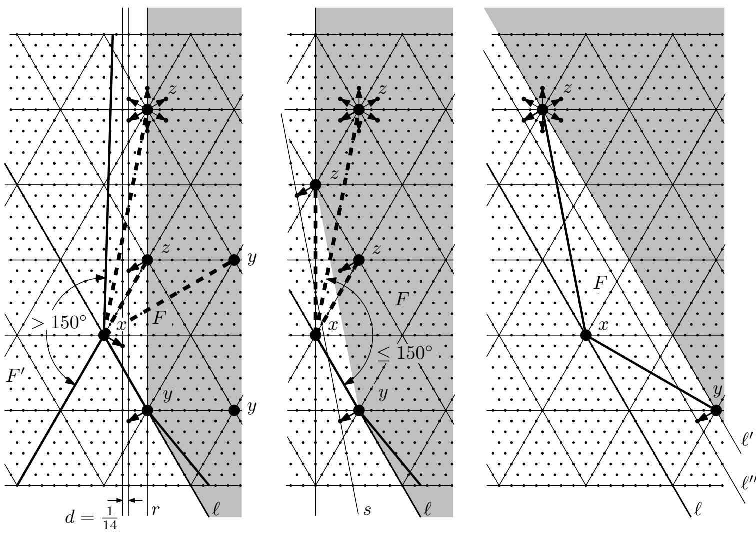
Documenta Mathematica

Journal der

Deutschen Mathematiker-Vereinigung

Gegründet 1996



(a) Case I (b) Case IIa (c) Case IIb

On Planar Graphs, cf. page 375

Band 11 · 2006

Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung, veröffentlicht Forschungsarbeiten aus allen mathematischen Gebieten und wird in traditioneller Weise referiert. Es wird indiziert durch Mathematical Reviews, Science Citation Index Expanded, Zentralblatt für Mathematik.

Artikel können als TEX-Dateien per E-Mail bei einem der Herausgeber eingereicht werden. Hinweise für die Vorbereitung der Artikel können unter der unten angegebenen WWW-Adresse gefunden werden.

Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung, publishes research manuscripts out of all mathematical fields and is refereed in the traditional manner. It is indexed in Mathematical Reviews, Science Citation Index Expanded, Zentralblatt für Mathematik.

Manuscripts should be submitted as TEX -files by e-mail to one of the editors. Hints for manuscript preparation can be found under the following WWW-address.

`http://www.math.uni-bielefeld.de/documenta`

ISSN 1431-0635 (Print), ISSN 1431-0643 (Internet)

SPARC
Leading Edge

Documenta Mathematica is a Leading Edge Partner of SPARC, the Scholarly Publishing and Academic Resource Coalition of the Association of Research Libraries (ARL), Washington DC, USA.

Documenta Mathematica

Band 11, 2006

Statistics of Lattice Points in Thin Annuli for Generic Lattices

Igor Wigman

Received: August 22, 2005

Communicated by Friedrich Götze

Abstract. We study the statistical properties of the counting function of lattice points inside thin annuli. By a conjecture of Bleher and Lebowitz, if the width shrinks to zero, but the area converges to infinity, the distribution converges to the Gaussian distribution. If the width shrinks slowly to zero, the conjecture was proven by Hughes and Rudnick for the standard lattice, and in our previous paper for generic rectangular lattices. We prove this conjecture for arbitrary lattices satisfying some generic Diophantine properties, again assuming the width of the annuli shrinks slowly to zero. One of the obstacles of applying the technique of Hughes-Rudnick on this problem is the existence of so-called close pairs of lattice points. In order to overcome this difficulty, we bound the rate of occurence of this phenomenon by extending some of the work of Eskin-Margulis-Mozes on the quantitative Openheim conjecture.

2000 Mathematics Subject Classification: Primary: 11H06, Secondary: 11J25

Keywords and Phrases: Lattice, Counting Function, Circle, Ellipse, Annulus, Two-Dimensional Torus, Gaussian Distribution, Diophantine approximation

1 Introduction

We consider a variant of the circle problem. Let $\Lambda \subset \mathbb{R}^2$ be a planar lattice, with $\det \Lambda$ the area of its fundamental cell. Let

$$N_\Lambda(t) = \{x \in \Lambda : |x| \leq t\},$$

denote its counting function, that is, we are counting Λ-points inside a disc of radius t.
As well known, as $t \to \infty$, $N_\Lambda(t) \sim \frac{\pi}{\det \Lambda} t^2$. Denoting the remainder or the error term

$$\Delta_\Lambda(t) = N_\Lambda(t) - \frac{\pi}{\det \Lambda} t^2,$$

it is a conjecture of Hardy that

$$|\Delta_\Lambda(t)| \ll_\epsilon t^{1/2+\epsilon}.$$

Another problem one could study is the *statistical* behavior of the value distribution of Δ_Λ normalized by $\sqrt{t}$, namely of

$$F_\Lambda(t) := \frac{\Delta_\Lambda(t)}{\sqrt{t}}.$$

Heath-Brown [HB] shows that for the standard lattice $\Lambda = \mathbb{Z}^2$, the value distribution of F_Λ, weakly converges to a non-Gaussian distribution with density $p(x)$. Bleher [BL3] established an analogue of this theorem for a more general setting, where in particular it implies a non-Gaussian limiting distribution of F_Λ, for any lattice $\Lambda \subset \mathbb{Z}^2$.
However, the object of our interest is slightly different. Rather than counting lattice points in the circle of varying radius t, we will do the same for *annuli.* More precisely, we define

$$N_\Lambda(t,\, \rho) := N_\Lambda(t+\rho) - N_\Lambda(t),$$

that is, the number of Λ-points inside the annulus of inner radius t and width ρ. The "expected" value is the area $\frac{\pi}{\det \Lambda}(2t\rho + \rho^2)$, and the corresponding normalized remainder term is

$$S_\Lambda(t,\, \rho) := \frac{N_\Lambda(t+\rho) - N_\Lambda(t) - \frac{\pi}{\det \Lambda}(2t\rho + \rho^2)}{\sqrt{t}}.$$

The statistics of $S_\Lambda(t,\, \rho)$ vary depending to the size of $\rho(t)$. Of our particular interest is the *intermediate* or *macroscopic regime*. Here $\rho \to 0$, but $\rho t \to \infty$. A particular case of the conjecture of Bleher and Lebowitz [BL4] states that $S_\Lambda(t,\, \rho)$ has a Gaussian distribution. In 2004 Hughes and Rudnick [HR] established the Gaussian distribution for the unit circle, under an additional assumption that $\rho(t) \gg t^{-\epsilon}$ for every $\epsilon > 0$.
By a rotation and dilation (which does not effect the counting function), we may assume, with no loss of generality, that Λ admits a basis one of whose elements is the vector $(1, 0)$, that is $\Lambda = \left\langle 1,\, \alpha + i\beta \right\rangle$ (we make the natural identification of i with $(0,\, 1)$). In a previous paper [W] we already dealt with the problem of investigating the statistical properties of the error term for rectangular lattice $\Lambda = \left\langle 1,\, i\beta \right\rangle$. We established the limiting Gaussian distribution for the "generic" case in this 1-parameter family.

Some of the work done in [W] extends quite naturally for the 2-parameter family of planar lattices $\langle 1,\, \alpha + i\beta \rangle$. That is, in the current work we will require the algebraic independence of α and β, as well as a strong Diophantine property of the pair $(\alpha,\, \beta)$ (to be defined), rather than the transcendence and a strong Diophantine property of the aspect ratio of the ellipse, as in [W].
We say that a real number ξ is *strongly Diophantine*, if for every *fixed* natural n, there exists $K_1 > 0$, such that for integers a_j with $\sum\limits_{j=0}^{n} a_j \xi^j \neq 0$,

$$\left| \sum_{j=0}^{n} a_j \xi^j \right| \gg_n \frac{1}{\left(\max\limits_{0 \le j \le n} |a_j| \right)^{K_1}}.$$

It was shown by Mahler [MAH], that this property holds for a "generic" real number. We say that a pair of numbers $(\alpha,\, \beta)$ is *strongly Diophantine*, if for every *fixed* natural n, there exists a number $K_1 > 0$, such that for every integral polynomial $p(x,\, y) = \sum\limits_{i+j \le n} a_{i,\, j} x^i y^j$ of degree $\le n$, we have

$$|p(\alpha,\, \beta)| \gg_n \frac{1}{\max\limits_{i+j \le n} |a_{i,\, j}|^{K_1}},$$

whenever $p(\alpha, \beta) \neq 0$. This holds for almost all real pairs $(\alpha,\, \beta)$, see section 2.2.

Theorem 1.1. *Let $\Lambda = \langle 1,\, \alpha + i\beta \rangle$ where $(\alpha,\, \beta)$ is algebraically independent and strongly Diophantine pair of real numbers. Assume that $\rho = \rho(T) \to 0$, but for every $\delta > 0$, $\rho \gg T^{-\delta}$. Then for every interval $\mathcal{A}$,*

$$\lim_{T \to \infty} \frac{1}{T} meas \left\{ t \in [T,\, 2T] : \; \frac{S_\Lambda(t,\, \rho)}{\sigma} \in \mathcal{A} \right\} = \frac{1}{\sqrt{2\pi}} \int\limits_{\mathcal{A}} e^{-\frac{x^2}{2}} dx, \qquad (1)$$

where the variance is given by

$$\sigma^2 := \frac{4\pi}{\beta} \cdot \rho. \qquad (2)$$

Remark: Note that the variance σ^2 is α-independent, since the determinant $\det(\Lambda) = \beta$.
One of the features of a rectangular lattice is that it is quite easy to show that the number of so-called close pairs of lattice points or pairs of points lying within a narrow annulus is bounded by essentially its average (see lemma 5.2 of [W]). This particular feature of the rectangular lattices was exploited while reducing the computation of the moments to the ones of a smooth counting function (we call it "unsmoothing"). In order to prove an analogous bound for a general lattice, we extend a result from Eskin, Margulis and Mozes [EMM] for our needs to obtain proposition 3.1. We believe that this proposition is of independent interest.

2 The distribution of $\tilde{S}_{\Lambda,\,M,\,L}$

We apply the same smoothing as in [HR] and [W]: let χ be the indicator function of the unit disc and ψ a nonnegative, smooth, even function on the real line, of total mass unity, whose Fourier transform, $\hat{\psi}$ is smooth and has compact support. Introduce a rotationally symmetric function Ψ on $\mathbb{R}^2$ by setting $\hat{\Psi}(\vec{y}) = \hat{\psi}(|\vec{y}|)$, where $|\cdot|$ denotes the standard Euclidian norm. For $\epsilon > 0$, set

$$\Psi_\epsilon(\vec{x}) = \frac{1}{\epsilon^2}\Psi\left(\frac{\vec{x}}{\epsilon}\right).$$

Define a *smooth* counting function

$$\tilde{N}_{\Lambda,M}(t) = \sum_{\vec{n}\in\Lambda} \chi_\epsilon\left(\frac{\vec{n}}{t}\right), \tag{3}$$

with $\epsilon = \epsilon(M)$ and $\chi_\epsilon = \chi * \Psi_\epsilon$, the convolution of χ with Ψ_ϵ. In what will follow,

$$\epsilon = \frac{1}{t\sqrt{M}}, \tag{4}$$

where $M = M(T)$ is the smoothing parameter, which tends to infinity with t. In this section, we are interested in the distribution of the smooth version of $S_\Lambda(t,\,\rho)$, denoted $\tilde{S}_{\Lambda,\,M,\,L}(t)$, where $L := \frac{1}{\rho}$, defined by

$$\tilde{S}_{\Lambda,\,M,\,L}(t) = \frac{\tilde{N}_{\Lambda,\,M}(t+\frac{1}{L}) - \tilde{N}_{\Lambda,\,M}(t) - \frac{\pi}{d}(\frac{2t}{L}+\frac{1}{L^2})}{\sqrt{t}}, \tag{5}$$

We assume that for every $\delta > 0$, $L = L(T) = O(T^\delta)$, which corresponds to the assumption of theorem 1.1 regarding $\rho := \frac{1}{L}$.
Rather than drawing t at random from $[T,\,2T]$ with a uniform distribution, we prefer to work with smooth densities: introduce $\omega \geq 0$, a smooth function of total mass unity, such that both ω and $\hat{\omega}$ are rapidly decaying, namely

$$|\omega(t)| \ll \frac{1}{(1+|t|)^A},\ \ |\hat{\omega}(t)| \ll \frac{1}{(1+|t|)^A},$$

for every $A > 0$. Define the averaging operator

$$\langle f\rangle_T = \frac{1}{T}\int\limits_{-\infty}^{\infty} f(t)\omega(\frac{t}{T})dt,$$

and let $\mathbb{P}_{\omega,\,T}$ be the associated probability measure:

$$\mathbb{P}_{\omega,\,T}(f\in\mathcal{A}) = \frac{1}{T}\int\limits_{-\infty}^{\infty} 1_{\mathcal{A}}(f(t))\omega(\frac{t}{T})dt.$$

REMARK: In what follows, we will suppress the explicit dependency on T, whenever convenient.

THEOREM 2.1. *Suppose that $M(T)$ and $L(T)$ are increasing to infinity with T, such that $M = O(T^\delta)$ for all $\delta > 0$, and $L/\sqrt{M} \to 0$. Then if (α, β) is an* algebraically independent strongly Diophantine *pair, we have for $\Lambda = \langle 1, \alpha + i\beta \rangle$,*

$$\lim_{T\to\infty} \mathbb{P}_{\omega, T}\left\{ \frac{\tilde{S}_{\Lambda, M, L}}{\sigma} \in \mathcal{A} \right\} = \frac{1}{\sqrt{2\pi}} \int\limits_{\mathcal{A}} e^{-\frac{x^2}{2}} dx,$$

for any interval $\mathcal{A}$, where

$$\sigma^2 := \frac{4\pi}{\beta L}. \tag{6}$$

DEFINITION: A tuple of real numbers $(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ is called *Diophantine*, if there exists a number $K > 0$, such that for every integer tuple $\{a_i\}_{i=0}^n$,

$$\left| a_0 + \sum_{i=1}^{n} a_i \alpha_i \right| \gg \frac{1}{q^K}, \tag{7}$$

with $q = \max\limits_{0\le i\le n} |a_i|$, whenever the LHS of the inequality doesn't vanish. Khintchine proved that *almost all* tuples in $\mathbb{R}^n$ are Diophantine (see, e.g. [S], pages 60-63).

Denote the dual lattice

$$\Lambda^* = \langle 1, \gamma + i\delta \rangle$$

with $\gamma = -\frac{\alpha}{\beta}$ and $\delta = \frac{1}{\beta}$. In the rest of the current section, we assume, that, unless specified otherwise, the set of the squared lengths of vectors in Λ^* satisfy the Diophantine property. That means, that $(\alpha^2, \alpha\beta, \beta^2)$ is a Diophantine triple of real numbers. We may assume $(\alpha^2, \alpha\beta, \beta^2)$ being Diophantine, since theorem 1.1 (and theorem 2.1) assume (α, β) is *strongly Diophantine*, which is, obviously, a stronger assumption.

We use the following approximation to $\tilde{N}_{\Lambda,M}(t)$ (see e.g [W], lemma 4.1), which holds unconditionally on any Diophantine assumption:

LEMMA 2.2. *As $t \to \infty$,*

$$\tilde{N}_{\Lambda,M}(t) = \frac{\pi t^2}{\beta} - \frac{\sqrt{t}}{\beta\pi} \sum_{\vec{k}\in\Lambda^*\setminus\{0\}} \frac{\cos\left(2\pi t|\vec{k}| + \frac{\pi}{4}\right)}{|\vec{k}|^{\frac{3}{2}}} \cdot \hat{\psi}\left(\frac{|\vec{k}|}{\sqrt{M}}\right) + O\left(\frac{1}{\sqrt{t}}\right), \tag{8}$$

where, again, Λ^* is the dual lattice.

By the definition of $\tilde{S}_{\Lambda, M, L}$ in (5) and appropriately manipulating the sum in (8) we obtain the following

COROLLARY 2.3.

$$\tilde{S}_{\Lambda,\,M,\,L}(t) = \frac{2}{\beta\pi} \sum_{\vec{k}\in\Lambda^*\setminus\{0\}} \frac{\sin\left(\frac{\pi|\vec{k}|}{L}\right)}{|\vec{k}|^{\frac{3}{2}}} \sin\left(2\pi\big(t+\frac{1}{2L}\big)|\vec{k}| + \frac{\pi}{4}\right)\hat{\psi}\left(\frac{|\vec{k}|}{\sqrt{M}}\right) + O\left(\frac{1}{\sqrt{t}}\right). \tag{9}$$

One should note that $\hat{\psi}$ being compactly supported means that the sum essentially truncates at $|\vec{k}| \approx \sqrt{M}$.
Unlike the standard lattice, clearly there are no nontrivial multiplicities in Λ, that is

LEMMA 2.4. *Let $\vec{a_j} = m_j + n_j(\alpha + i\beta) \in \Lambda$, $j = 1, 2$, with an irrational α such that $\beta \notin \mathbb{Q}(\alpha)$. Then if $|\vec{a_1}| = |\vec{a_2}|$, either $n_1 = n_2$ and $m_1 = m_2$ or $n_1 = -n_2$ and $n_2 = -m_2$.*

Proof of theorem 2.1. We will show that the moments of $\tilde{S}_{\Lambda,\,M,\,L}$ corresponding to the smooth probability space converge to the moments of the normal distribution with zero mean and variance which is given by theorem 2.1. This allows us to deduce that the distribution of $\tilde{S}_{\Lambda,\,M,\,L}$ converges to the normal distribution as $T \to \infty$, precisely in the sense of theorem 2.1.
First, we show that the mean is $O(\frac{1}{\sqrt{T}})$. Since ω is real,

$$\left|\left\langle \sin\left(2\pi\big(t+\frac{1}{2L}\big)|\vec{k}| + \frac{\pi}{4}\right)\right\rangle\right| = \left|\Im m\left\{\hat{\omega}\big(-T|\vec{k}|\big)e^{i\pi(\frac{|\vec{k}|}{L}+\frac{1}{4})}\right\}\right| \ll \frac{1}{T^A|\vec{k}|^A}$$

for any $A > 0$, where we have used the rapid decay of $\hat{\omega}$. Thus

$$\left|\left\langle \tilde{S}_{\Lambda,\,M,\,L}\right\rangle\right| \ll \sum_{\vec{k}\in\Lambda^*\setminus\{0\}} \frac{1}{T^A|\vec{k}|^{A+3/2}} + O\left(\frac{1}{\sqrt{T}}\right) \ll O\left(\frac{1}{\sqrt{T}}\right),$$

due to the convergence of $\sum\limits_{\vec{k}\in\Lambda^*\setminus\{0\}} \frac{1}{|\vec{k}|^{A+3/2}}$, for $A > \frac{1}{2}$
Now define

$$\mathcal{M}_{\Lambda,\,m} := \left\langle \left(\frac{2}{\beta\pi} \sum_{\vec{k}\in\Lambda^*\setminus\{0\}} \frac{\sin\left(\frac{\pi|\vec{k}|}{L}\right)}{|\vec{k}|^{\frac{3}{2}}} \sin\left(2\pi\big(t+\frac{1}{2L}\big)|\vec{k}| + \frac{\pi}{4}\right)\hat{\psi}\big(\frac{|\vec{k}|}{\sqrt{M}}\big)\right)^m\right\rangle \tag{10}$$

Then from (9), the binomial formula and the Cauchy-Schwartz inequality,

$$\left\langle \big(\tilde{S}_{\Lambda,\,M,\,L}\big)^m\right\rangle = \mathcal{M}_{\Lambda,\,m} + O\left(\sum_{j=1}^{m}\binom{m}{j}\frac{\sqrt{\mathcal{M}_{2m-2j}}}{T^{j/2}}\right)$$

Proposition 2.5 together with proposition 2.8 allow us to deduce the result of theorem 2.1 for an algebraically independent strongly Diophantine $(\xi,\,\eta) := (-\frac{\alpha}{\beta},\,\frac{1}{\beta})$. Clearly, $(\alpha,\,\beta)$ being algebraically independent and strongly Diophantine is sufficient. □

2.1 The variance

The computation of the variance is done in two steps. First, we reduce the main contribution to the *diagonal* terms, using the assumption on the pair $(\alpha,\,\beta)$ (i.e. $(\alpha^2,\,\alpha\beta,\,\beta^2)$ is *Diophantine*). Then we compute the contribution of the *diagonal* terms. Both these steps are very close to the corresponding ones in [W].

Suppose that the triple $(\alpha^2,\,\alpha\beta,\,\beta^2)$ satisfies (7).

Proposition 2.5. *If $M = O\big(T^{1/(K+1/2+\delta)}\big)$ for fixed $\delta > 0$, then the variance of $\tilde{S}_{\Lambda,\,M,\,L}$ is asymptotic to*

$$\sigma^2 := \frac{4}{\beta^2\pi^2}\sum_{\vec{k}\in\Lambda^*\setminus\{0\}}\frac{\sin^2\left(\frac{\pi|\vec{k}|}{L}\right)}{|\vec{k}|^3}\hat{\psi}^2\left(\frac{|\vec{k}|}{\sqrt{M}}\right)$$

If $L\to\infty$, but $L/\sqrt{M}\to 0$, then

$$\sigma^2 \sim \frac{4\pi}{\beta L} \tag{11}$$

Remark: In the formulation of proposition 2.5, K is implicitly given by (7).

Proof. Expanding out (10), we have

$$\mathcal{M}_{\Lambda,\,2} = \frac{4}{\beta^2\pi^2}\sum_{\vec{k},\vec{l}\in\Lambda^*\setminus\{0\}}\frac{\sin\left(\frac{\pi|\vec{k}|}{L}\right)\sin\left(\frac{\pi|\vec{l}|}{L}\right)\hat{\psi}(\frac{|\vec{k}|}{\sqrt{M}})\hat{\psi}(\frac{|\vec{l}|}{\sqrt{M}})}{|\vec{k}|^{\frac{3}{2}}|\vec{l}|^{\frac{3}{2}}} \times\left\langle\sin\left(2\pi\left(t+\frac{1}{2L}\right)|\vec{k}|+\frac{\pi}{4}\right)\sin\left(2\pi\left(t+\frac{1}{2L}\right)|\vec{l}|+\frac{\pi}{4}\right)\right\rangle \tag{12}$$

It is easy to check that the average of the second line of the previous equation is:

$$\begin{aligned}\frac{1}{4}\Big[&\hat{\omega}\big(T(|\vec{k}|-|\vec{l}|)\big)e^{i\pi(1/L)(|\vec{l}|-|\vec{k}|)}+\\ &\hat{\omega}\big(T(|\vec{l}|-|\vec{k}|)\big)e^{i\pi(1/L)(|\vec{k}|-|\vec{l}|)}+\\ &\hat{\omega}\big(T(|\vec{k}|+|\vec{l}|)\big)e^{-i\pi(1/2+(1/L)(|\vec{k}|+|\vec{l}|))}-\\ &\hat{\omega}\big(-T(|\vec{k}|+|\vec{l}|)\big)e^{i\pi(1/2+(1/L)(|\vec{k}|+|\vec{l}|))}\Big]\end{aligned} \tag{13}$$

Recall that the support condition on $\hat{\psi}$ means that $\vec{k}$ and $\vec{l}$ are both constrained to be of length $O(\sqrt{M})$. Thus the off-diagonal contribution (that is for $|\vec{k}| \neq |\vec{l}|$) of the first two lines of (13) is

$$\ll \sum_{\substack{\vec{k},\vec{l}\in\Lambda^*\setminus\{0\} \\ |\vec{k}|,\,|\vec{k}'|\le\sqrt{M}}} \frac{M^{A(K+1/2)}}{T^A} \ll \frac{M^{A(K+1/2)+2}}{T^A} \ll T^{-B},$$

for every $B > 0$, since $(\alpha,\,\alpha\beta,\,\beta^2)$ is Diophantine.
Obviously, the contribution to (12) of the two last lines of (13) is negligible both in the diagonal and off-diagonal cases, justifying the diagonal approximation of (12) in the first statement of the proposition. To compute the asymptotics, we write we take a large parameter $Y = Y(T) > 0$ (to be chosen later), and write:

$$\sum_{\vec{k}\in\Lambda^*\setminus\{0\}} \frac{\sin^2\left(\frac{\pi|\vec{k}|}{L}\right)}{|\vec{k}|^3}\hat{\psi}^2\left(\frac{|\vec{k}|}{\sqrt{M}}\right) = \sum_{\substack{\vec{k}\in\Lambda^*\setminus\{0\} \\ |\vec{k}|^2\le Y}} + \sum_{\substack{\vec{k}\in\Lambda^*\setminus\{0\} \\ |\vec{k}|^2> Y}} := I_1 + I_2,$$

Now for $Y = o(M)$, $\hat{\psi}^2\big(\frac{|\vec{k}|}{\sqrt{M}}\big) \sim 1$ within the constraints of I_1, and so

$$I_1 \sim \sum_{\substack{\vec{k}\in\Lambda^*\setminus\{0\} \\ |\vec{k}|^2\le Y}} \frac{\sin^2\left(\frac{\pi|\vec{k}|}{L}\right)}{|\vec{k}|^3}.$$

Recall that $\Lambda^* = \langle 1,\,\gamma + i\delta\rangle$. The sum in

$$\sum_{\substack{\vec{k}\in\Lambda^*\setminus\{0\} \\ |\vec{k}|^2\le Y}} \frac{\sin^2\left(\frac{\pi|\vec{k}|}{L}\right)}{|\vec{k}|^3} = \frac{1}{L}\sum_{\substack{\vec{k}\in\Lambda^*\setminus\{0\} \\ |\vec{k}|^2\le Y}} \frac{\sin^2\left(\frac{\pi|\vec{k}|}{L}\right)}{\big(\frac{|\vec{k}|}{L}\big)^3}\frac{1}{L^2}.$$

is a 2-dimensional Riemann sum of the integral

$$\iint\limits_{1/L^2\ll(x+y\gamma)^2+(\delta y)^2\le Y/L^2} \frac{\sin^2\left(\pi\sqrt{(x+y\gamma)^2+(\delta y)^2}\right)}{|(x+y\gamma)^2+(\delta y)^2|^{3/2}}dxdy$$

$$\sim \frac{2\pi}{\delta}\int\limits_{\frac{1}{L}}^{\frac{\sqrt{Y}}{L}} \frac{\sin^2(\pi r)}{r^2}dr \to \beta\pi^3,$$

provided that $Y/L^2 \to \infty$, since $\int_0^\infty \frac{\sin^2(\pi r)}{r^2} dr = \frac{\pi^2}{2}$. We changed the coordinates appropriately. And so,

$$I_1 \sim \frac{\beta\pi^3}{L}$$

Next we will bound I_2. Since $\hat{\psi} \ll 1$, we may use the same change of variables to obtain:

$$\begin{aligned} I_2 &\ll \frac{1}{L} \iint\limits_{(x+y\gamma)^2+(\delta y)^2 \geq Y/L^2} \frac{\sin^2\left(\pi\sqrt{(x+y\gamma)^2+(\delta y)^2}\right)}{|(x+y\gamma)^2+(\delta y)^2|^{3/2}} dxdy \\ &\ll \frac{1}{L} \int\limits_{\sqrt{Y}/L}^{\infty} \frac{dr}{r^2} = o\left(\frac{1}{L}\right). \end{aligned}$$

This concludes the proposition, provided we have managed to choose Y with $L^2 = o(Y)$ and $Y = o(M)$. Such a choice is possible by the assumption of the proposition regarding L.

□

2.2 The higher moments

In order to compute the higher moments we will prove that the main contribution comes from the so-called *diagonal* terms (to be explained later). Our bound for the contribution of the *off-diagonal* terms holds for a *strongly Diophantine* pair of real numbers, which is defined below. In order to show that the strongly Diophantine pairs are "generic", we use theorem 2.6 below, which is a consequence of the work of Kleinbock and Margulis [KM]. The contribution of the diagonal terms is computed exactly in the same manner it was done in [W], and so we will omit it here.

Definition: We call the pair (ξ, η) *strongly Diophantine*, if for all natural n there exists a number $K_1 = K_1(\xi, \eta, n) \in \mathbb{N}$ such that for every integral polynomial of 2 variables $p(x, y) = \sum\limits_{i+j \leq n} a_{i,j} x^i y^j$ of degree $\leq n$, we have

$$\left|p(\xi, \eta)\right| \gg h^{-K_1}, \tag{14}$$

where $h = \max\limits_{i+j \leq n} |a_{i,j}|$ is the height of p. The constant involved in the " $\gg$ " notation may depend only on ξ, η, n and K_1.

Theorem 2.6. *Let an integer n be given. Then almost all pairs of real numbers $(\xi, \eta) \in \mathbb{R}^2$ satisfy the following property: there exists a number $K_1 = K_1(n) \in \mathbb{N}$ such that for every integer polynomial of 2 variables $p(x, y) = \sum\limits_{i+j \leq n} a_{i,j} x^i y^j$ of degree $\leq n$, (14) is satisfied.*

Theorem 2.6 states that almost all real pairs of numbers are strongly Diophantine.

REMARK: Theorem A in [KM] is much more general than the result we are using. As a matter of fact, we have the inequality

$$\left|b_0 + b_1 f_1(x) + \ldots + b_n f_n(x)\right| \gg_\epsilon \frac{1}{h^{n+\epsilon}}$$

with $b_i \in \mathbb{Z}$ and

$$h := \max_{0\le i\le n} |b_i|.$$

The inequality above holds for every $\epsilon > 0$ for a wide class of functions $f_i : U \to \mathbb{R}$, for almost all $x \in U$, where $U \subset \mathbb{R}^m$ is an open subset. Here we use this inequality for the monomials.

REMARK: Simon Kristensen [KR] has recently shown, that the set of all pairs $(\xi, \eta) \in \mathbb{R}^2$ which fail to be strongly Diophantine has Hausdorff dimension 1. Obviously, if (ξ, η) is strongly Diophantine, then any n-tuple of real numbers, which consists of a set of monomials in ξ and η, is Diophantine. Moreover, (ξ, η) is strongly Diophantine iff $(-\frac{\xi}{\eta}, \frac{1}{\eta})$ is such.
We have the following analogue of lemma 4.7 in [W], which will eventually allow us to exploit the strong Diophantine assumption of (α, β).

LEMMA 2.7. *If (ξ, η) is strongly Diophantine, then it satisfies the following property: for any fixed natural m, there exists $K \in \mathbb{N}$, such that if*

$$z_j = a_j^2 + b_j^2\xi^2 + 2a_jb_j\xi + b_j^2\eta^2 \ll M,$$

and $\epsilon_j = \pm 1$ for $j = 1, \ldots, m$, with integral a_j, b_j and if $\sum\limits_{j=1}^{m} \epsilon_j\sqrt{z_j} \neq 0$, then

$$\Big|\sum_{j=1}^{m} \epsilon_j\sqrt{z_j}\Big| \gg M^{-K}, \tag{15}$$

where the constant involved in the " $\gg$ " notation depends only on η and m.

The proof is essentially the same as the one of lemma 4.7 from [W], considering the product Q of numbers of the form $\sum\limits_{j=1}^{m} \delta_j\sqrt{z_j}$ over all possible signs δ_j. Here we use the Diophantine condition of the real tuple (ξ, η) rather than of a single real number.

PROPOSITION 2.8. *Let $m \in \mathbb{N}$ be given. Suppose that $\Lambda = \langle 1, \alpha+i\beta\rangle$, such that the pair $(\xi, \eta) := (-\frac{\alpha}{\beta}, \frac{1}{\beta})$ is algebraically independent strongly Diophantine, which satisfy the property of lemma 2.7 for the given m, with $K = K_m$. Then if $M = O\big(T^{\frac{1-\delta}{K_m}}\big)$ for some $\delta > 0$, and if $L \to \infty$ such that $L/\sqrt{M} \to 0$, the following holds:*

$$\frac{\mathcal{M}_{\Lambda,m}}{\sigma^m} = \begin{cases} \frac{m!}{2^{m/2}\left(\frac{m}{2}\right)!} + O\big(\frac{\log L}{L}\big), & m \text{ is even} \\ O\big(\frac{\log L}{L}\big), & m \text{ is odd}\end{cases}$$

Proof. Expanding out (10), we have

$$\mathcal{M}_{\Lambda,\,m} = \frac{2^m}{\beta^m \pi^m} \sum_{\vec{k_1},\ldots,\,\vec{k_m} \in \Lambda^* \setminus \{0\}} \prod_{j=1}^{m} \frac{\sin\left(\frac{\pi|\vec{k_j}|}{L}\right)\hat{\psi}\left(\frac{|\vec{k_j}|}{\sqrt{M}}\right)}{|\vec{k_j}|^{\frac{3}{2}}} \times \left\langle \prod_{j=1}^{m} \sin\left(2\pi\left(t+\frac{1}{2L}\right)|\vec{k_1}|+\frac{\pi}{4}\right)\right\rangle \tag{16}$$

Now,

$$\left\langle \prod_{j=1}^{m} \sin\left(2\pi\left(t+\frac{1}{2L}\right)|\vec{k_1}|+\frac{\pi}{4}\right)\right\rangle = \sum_{\epsilon_j=\pm 1} \frac{\prod_{j=1}^{m}\epsilon_j}{2^m i^m} \hat{\omega}\left(-T\sum_{j=1}^{m}\epsilon_j|\vec{k_j}|\right) e^{\pi i \sum_{j=1}^{m}\epsilon_j\left((1/L)|\vec{k_j}|+1/4\right)}$$

We call a term of the summation in (16) with $\sum_{j=1}^{m}\epsilon_j|\vec{k_j}| = 0$ *diagonal*, and *off-diagonal* otherwise. Due to lemma 2.7, the contribution of the *off-diagonal* terms is:

$$\ll \sum_{\substack{\vec{k_1},\ldots,\,\vec{k_m}\in\Lambda^*\setminus\{0\} \\ |\vec{k_1}|,\,\ldots,\,|\vec{k_m}|\le\sqrt{M}}} \left(\frac{T}{M^{K_m}}\right)^{-A} \ll M^m T^{-A\delta},$$

for every $A > 0$, by the rapid decay of $\hat{\omega}$ and our assumption regarding M. Since m is constant, this allows us to reduce the sum to the *diagonal terms*. In order to be able to sum over all the diagonal terms we need the following analogue of a well-known theorem due to Besicovitch [BS] about incommensurability of square roots of integers.

Proposition 2.9. *Suppose that ξ and η are algebraically independent, and*

$$z_j = a_j^2 + 2a_jb_j\xi + b_j^2(\xi^2+\eta), \tag{17}$$

such that $(a_j,\, b_j) \in \mathbb{Z}_+^2$ are all different primitive vectors, for $1 \le j \le m$. Then $\{\sqrt{z_j}\}_{j=1}^m$ are linearly independent over $\mathbb{Q}$.

The last proposition is an immediate consequence of a theorem proved in the appendix of [BL2].

DEFINITION: We say that a term corresponding to $\{\vec{k_1},\ldots,\vec{k_m}\} \in \Big(\Lambda^* \setminus \{0\}\Big)^m$ and $\{\epsilon_j\} \in \{\pm 1\}^m$ is a *principal diagonal* term if there is a partition $\{1,\ldots,m\} = \bigsqcup\limits_{i=1}^{l} S_i$, such that for each $1 \le i \le l$ there exists a primitive $\vec{n_i} \in \Lambda^* \setminus \{0\}$, with non-negative coordinates, that satisfies the following property: for every $j \in S_i$, there exist $f_j \in \mathbb{Z}$ with $|\vec{k_j}| = f_j |\vec{n_i}|$. Moreover, for each $1 \le i \le l$, $\sum\limits_{j\in S_i} \epsilon_j f_j = 0$.

Obviously, the principal diagonal is contained within the diagonal. However, the meaning of proposition 2.9 is, that in our situation, the converse also is true:

COROLLARY 2.10. *Every diagonal term is a principle diagonal term whenether ξ and η are algebraically independent.*

Computing the contribution of the principal diagonal terms is done literally the same way it was done in [W], and we sketch it here. As in [W], one can show that the contribution of a particular partition $\{1,\ldots,m\} = \bigsqcup\limits_{i=1}^{l} S_i$ is negligible, unless $m = 2l$ is even and $\#S_i = 2$ for all $1 \le i \le l$.

In the latter case, the contribution is asymptotic to 1. Therefore, the m-th moment is asymptotic to 0, if m is *odd*, and to the number of partitions $\{1,\ldots,m\} = \bigsqcup\limits_{i=1}^{l} S_i$ with $\#S_i = 2$ for all i, $m = 2l$. This number equals to $\frac{m!}{2^{m/2}\left(\frac{m}{2}\right)!}$, which is also the m-th moment of the standard Gaussian distribution.

□

3 BOUNDING THE NUMBER OF CLOSE PAIRS OF LATTICE POINTS

Roughly speaking, we say that a pair of lattice points, n and n' is *close*, if $\big||n| - |n'|\big|$ is *small*. We would like to show that this phenomenon is *rare*. This is closely related to the Oppenheim conjecture, as $|n|^2 - |n'|^2$ is a quadratic form on the coefficients of n and n'.

In order to establish a quantative result, we use a technique developed in a paper by Eskin, Margulis and Mozes [EMM]. Note that the proof is unconditional on any Diophantine assumptions.

3.1 STATEMENT OF THE RESULTS

The ultimate goal of this section is to establish the following

PROPOSITION 3.1. *Let Λ be a lattice and denote*

$$A(R,\delta) := \{(\vec{k},\vec{l}) \in \Lambda \times \Lambda : \; R \le |\vec{k}|^2 \le 2R,\; |\vec{k}|^2 \le |\vec{l}|^2 \le |\vec{k}|^2 + \delta\}. \qquad (18)$$

Then if $\delta > 1$, such that $\delta = o(R)$, we have

$$\#A(R,\delta) \ll R\delta \cdot \log R$$

In order to prove this result, we note that evaluating the size of $A(R, \delta)$ is equivalent to counting integer points $\vec{v} \in \mathbb{R}^4$ with $T \leq \|\vec{v}\| \leq 2T$ such that

$$0 \leq Q_1(v) \leq \delta,$$

where Q_1 is a quadratic form of signature (2, 2), given explicitly by

$$Q_1(\vec{v}) = (v_1 + v_2\alpha)^2 + (v_2\beta)^2 - (v_3 + v_4\alpha)^2 - (v_4\beta)^2. \tag{19}$$

For a fixed $\delta > 0$ and a large R, this situation was considered extensively by Eskin, Margulis and Mozes [EMM]. The authors give an asymptotical upper bound in this situation. We will examine how the constants involved in their bound depend on δ, and find out that there is a linear dependency, which is what we essentially need. The author wishes to thank Alex Eskin for his assistance with this matter.

Remarks: 1. In a more recent paper, Eskin Margulis and Mozes [EMM1] prove that for "generic" lattice Λ, there is a constant $c > 0$, such that for any *fixed* $\delta > 0$, as $R \to \infty$, $\#A(R, \delta)$ is asymptotic to $c\delta R$.
2. For our purposes we need a weaker result:

$$\#A(R,\delta) \ll_\epsilon R\delta \cdot R^\epsilon,$$

for every $\epsilon > 0$. If Λ is a rectangular lattice (i.e. $\alpha = 0$), then this result follows from properties of the divisor function (see e.g. [BL], lemma 3.2).
Theorem 2.3 in [EMM] considers a more general setting than proposition 3.1. We state here theorem 2.3 from [EMM] (see theorem 3.2). It follows from theorem 3.3 from [EMM], which will be stated as well (see theorem 3.3). Then we give an outline of the proof of theorem 2.3 of [EMM], and inspect the dependency on δ of the constants involved.

3.2 Theorems 2.3 and 3.3 from [EMM]

Let Δ be a lattice in $\mathbb{R}^n$. We say that a subspace $L \subset \mathbb{R}^n$ is Δ-rational, if $L \cap \Delta$ is a lattice in L. We need the following definitions:

Definitions:

$$\alpha_i(\Delta) := \sup\left\{ \frac{1}{d_\Delta(L)} \,\middle|\, L \text{ is a } \Delta-\text{rational subspace of dimension } i \right\},$$

where

$$d_\Delta(L) := vol(L/(L \cap \Delta)).$$

Also

$$\alpha(\Delta) := \max_{0\le i\le n} \alpha_i(\Delta).$$

Since the space of unimodular lattices is canonically isomorphic to $SL(n,\,\mathbb{R})/SL(n,\,\mathbb{Z})$, the notation $\alpha(g)$ makes sense for $g \in G := SL(n,\,\mathbb{R})$. For a bounded function $f : \mathbb{R}^n \to \mathbb{R}$, with $|f| \le M$, which vanishes outside a ball $B(0,\,R)$, define $\tilde{f} : SL(n,\,\mathbb{R}) \to \mathbb{R}$ by the following formula:

$$\tilde{f}(g) := \sum_{v\in\mathbb{Z}^n} f(gv).$$

Lemma 3.1 in [S2] implies that

$$\tilde{f}(g) < c\alpha(g), \tag{20}$$

where $c = c(f)$ is an explicit constant constant

$$c(f) = c_0 M \max(1, R^n),$$

for some constant $c_0 = c_0(n)$, independent on f. In section 3.4 we prove a stronger result, assuming some additional information about the support of f. Let Q_0 be a quadratic form defined by

$$Q_0(\vec{v}) = 2v_1v_n + \sum_{i=2}^{p} v_i^2 - \sum_{i=p+1}^{n-1} v_i^2.$$

Since

$$v_1v_n = \frac{(v_1+v_n)^2 - (v_1-v_n)^2}{2},$$

Q_0 is of signature $p,\,q$. Obviously, $G := SL(n,\mathbb{R})$ acts on the space of quadratic forms of signature $(p,\,q)$, and discriminant ± 1, $\mathcal{O} = \mathcal{O}(p,\,q)$ by:

$$Q^g(v) := Q(gv).$$

Moreover, by the well known classification of quadratic forms, $\mathcal{O}$ is the orbit of Q_0 under this action.
In our case the signature is $(p,\,q) = (2,\,2)$ and $n = 4$. We fix an element $h_1 \in G$ with $Q^{h_1} = Q_1$, where Q_1 is given by (19). There exists a constant $\tau > 0$, such that for every $v \in \mathbb{R}^4$,

$$\tau^{-1}\|v\| \le \|h_1 v\| \le \tau\|v\|. \tag{21}$$

We may assume, with no loss of generality that $\tau \ge 1$.
Let $H := Stab_{Q_0}(G)$. Then the natural mophism $H\backslash G \to \mathcal{O}(p,q)$ is a homeomorphism. Define a 1-parameter family $a_t \in G$ by:

$$a_t e_i = \begin{cases} e^{-t}e_1, & i = 1 \\ e_i, & i = 2,\dots,n-1 \\ e^t e_n, & i = n \end{cases}.$$

Clearly, $a_t \in H$. Furthermore, let $\hat{K}$ be the subgroup of G consisting of orthogonal matrices, and denote $K := H \cap \hat{K}$.
Let $(a,\, b) \in \mathbb{R}^2$ be given and let $Q : \mathbb{R}^n \to \mathbb{R}$ be any quadratic form. The object of our interest is:

$$V_{(a,\, b)}(\mathbb{Z}) = V^Q_{(a,\, b)}(\mathbb{Z}) = \{x \in \mathbb{Z}^n :\, a < Q(x) < b\}.$$

Theorem 2.3 states, in our case:

Theorem 3.2 (Theorem 2.3 from [EMM]). *Let $\Omega = \{v \in \mathbb{R}^4 |\; \|v\| < \nu(v/\|v\|)\}$, where ν is a nonnegative continuous function on S^3. Then we have:*

$$\# V^{Q_1}_{(a,\, b)}(\mathbb{Z}) \cap T\Omega < cT^2 \log T,$$

where the constant c depends only on $(a,\, b)$.

The proof of theorem 3.2 relies on theorem 3.3 from [EMM], and we give here a particular case of this theorem

Theorem 3.3 (Theorem 3.3 from [EMM]). *For any (fixed) lattice Δ in $\mathbb{R}^4$,*

$$\sup_{t>1} \frac{1}{t} \int\limits_K \alpha(a_t k \Delta) dm(k) < \infty,$$

where the upper bound is universal.

3.3 Outline of the proof of theorem 3.2:

Step 1: Define

$$J_f(r, \zeta) = \frac{1}{r^2} \int\limits_{\mathbb{R}^2} f(r, x_2,\, x_3,\, x_4) dx_2 dx_3, \tag{22}$$

where

$$x_4 = \frac{\zeta - x_2^2 + x_3^2}{2r}$$

Lemma 3.6 in [EMM] states that J_f is approximable by means of an integral over the compact subgroup K. More precisely, there is some constant $C > 0$, such that for every $\epsilon > 0$,

$$\left| C \cdot e^{2t} \int\limits_K f(a_t k v) \nu(k^{-1} e_1) dm(k) - J_f\big(\|v\| e^{-t},\, Q_0(v)\big) \nu(\frac{v}{\|v\|}) \right| < \epsilon \tag{23}$$

with e^t, $\|v\| > T_0$ for some $T_0 > 0$.

Step 2: Choose a continuous nonnegative function f on $\mathbb{R}^4_+ = \{x_1 > 0\}$ which vanishes outside a compact set so that

$$J_f(r, \zeta) \geq 1 + \epsilon$$

on $[\tau^{-1},\, 2\tau] \times [a,\, b]$. We will show later, how one can choose f.

Step 3: Denote $T = e^t$, and suppose that $T \le \|v\| \le 2T$ and $a \le Q_0(h_1 v) \le b$. Then by (21), $J_f\big(\|h_1 v\| T^{-1}, Q_0(h_1 v)\big) \ge 1+\epsilon$, and by (23), for a sufficiently large t,

$$C \cdot T^2 \int\limits_K f(a_t k h_1 v) dm(k) \ge 1, \tag{24}$$

for $T \le \|v\| \le 2T$ and

$$a \le Q_0^x(v) \le b. \tag{25}$$

Step 4: Summing (24) over all $v \in \mathbb{Z}^4$ with (25) and $T \le \|v\| \le 2T$, we obtain:

$$\begin{aligned} \#V_{(a,\,b)}(\mathbb{Z}) \cap [T,\, 2T]S^3 &\le \sum_{v \in \mathbb{Z}^n} C \cdot T^2 \int\limits_K f(a_t k h_1 v) dm(k) \\ &= C \cdot T^2 \int\limits_K \tilde{f}(a_t k h_1) dm(k) \end{aligned} \tag{26}$$

using the nonnegativity of f.

Step 5: By (20), (26) is

$$\le C \cdot c(f) \cdot T^2 \int\limits_K \alpha(a_t k h_1) dm(k).$$

Step 6: The result of theorem 2.3 is obtained by using theorem 3.3 on the last expression.

3.4 δ-dependency:

In this section we assume that $(a,\, b) = (0,\, \delta)$, which suits the definition of the set $A(R,\, \delta)$, (18). One should notice that there only 3 δ-dependent steps:
• Choosing f in step 2, such that $J_f \ge 1 + \epsilon$ on $[\tau^{-1},\, 2\tau] \times [0,\, \delta]$. We will construct a family of functions f_δ with an universal bound $|f_\delta| \le M$, such that f_δ vanishes outside of a compact set which is only slightly larger than

$$V(\delta) = [\tau^{-1},\, 2\tau] \times [-1,\, -1]^2 \times [0,\, \frac{\delta\tau}{2}]. \tag{27}$$

This is done in section 3.4.1.
• The dependency of T_0 of step 3, so that the usage of lemma 3.6 in [EMM] is legitimate. For this purpose we will have to examine the proof of this lemma. This is done in section 3.4.2.
• The constant c in (20). We would like to establish a *linear* dependency on δ. This is straightforward, once we are able to control the number of integral points in a domain defined by (27). This is done in section 3.4.3.

3.4.1 Choosing f_δ:

Notation: For a set $U \subset \mathbb{R}^n$, and $\epsilon > 0$, denote

$$U_\epsilon := \{x \in \mathbb{R}^n : \max_{1\le i\le n} |x_i - y_i| \le \epsilon, \text{ for some } y \in U\}.$$

Choose a nonnegative continuous function f_0, on $\mathbb{R}^4_+$, which vanishes outside a compact set, such that its support, E_{f_0}, slightly exceeds the set $V(1)$. More precisely, $V(1) \subset E_{f_0} \subset V(1)_{\delta_0}$ for some $\delta_0 > 0$. By the uniform continuity of f, there are $\epsilon_0,\, \delta_0 > 0$, such that if $\max_{1\le i\le 4} |x_i - x_i^0| \le \delta_0$, then $f(x) > \epsilon_0$, for every $x^0 = (x_1^0, 0,\, 0,\, x_4^0) \in V(1)$.
Thus for $(r,\, \zeta) \in [\tau^{-1},\, 2\tau] \times [0,\, \delta]$, the contribution of $[-\delta_0,\, \delta_0]^2$ to J_{f_0} is $\ge \epsilon_0 \cdot (2\delta_0)^2$. Multiplying f_0 by a suitable factor, and by the linearity of J_{f_0}, we may assume that this contribution is at least $1 + \epsilon$.
Now define $f_\delta(x_1,\, \dots,\, x_4) := f_0(x_1,\, x_2,\, x_3,\, \frac{x_4}{\delta})$. We have for $\delta \ge 1$

$$\frac{\zeta - x_2^2 + x_3^2}{2r\delta} = \frac{\zeta/2r}{\delta} - \frac{(x_2/\sqrt{\delta})^2}{2r} + \frac{(x_3/\sqrt{\delta})^2}{2r}.$$

Thus for $\delta \ge 1$, if $(r,\, \zeta) \in [\tau^{-1},\, 2\tau] \times [0,\, \delta]$ and for $i = 2,\, 3$, $|x_i| < \delta_0$, f_δ satisfies:

$$f_\delta(r,\, x_2,\, x_3,\, x_4) > \epsilon_0,$$

and therefore the contribution of this domain to J_{f_δ} is

$$\ge \epsilon_0 (2\delta)^2 \ge 1 + \epsilon$$

by our assumption.
By the construction, the family $\{f_\delta\}$ has a universal upper bound M which is the one of f_0.

3.4.2 How large is T_0

The proof of lemma 3.6 from [EMM] works well along the same lines, as long as

$$f(a_t x) \ne 0 \tag{28}$$

implies that for $t \to \infty$, $x/\|x\|$ converges to $e_1 = (1,\, 0,\, 0,\, 0)$. Now, since a_t preserves $x_1 x_4$, (28) implies for the particular choice of $f = f_\delta$ in section 3.4.1:

$$|x_1 x_4| = O(\delta); \quad x_1 \gg T.$$

Thus

$$\|x\| = x_1 + O\left(\frac{\delta}{T}\right) + O(1),$$

and so, as long as $\delta = O(T)$, $x/\|x\|$ indeed converges to e_1.

3.4.3 BOUNDING INTEGRAL POINTS IN V_δ:

LEMMA 3.4. *Let $V(\delta)$ defined by*

$$V(\delta) = [\tau^{-1},\, 2\tau] \times [-1,\, -1]^{n-2} \times [0,\, \frac{\delta\beta}{2}]. \tag{29}$$

for some constant τ and $n \geq 3$. Let $g \in SL(n,\, \mathbb{R})$ and denote

$$N(g,\, \delta) := \# V(\delta) \cap g\mathbb{Z}^n.$$

Then for $\delta \geq 1$,

$$\left| N(g,\, \delta) - \frac{2^{n-2}(2\tau - \tau^{-1})\delta}{\det g} \right| \leq c_5 \delta \sum_{i=1}^{n-1} \frac{1}{vol(L_i/(g\mathbb{Z}^n \cap L_i)}$$

for some g-rational subspaces L_i of $\mathbb{R}^4$ of dimension i, where $c_5 = c_5(n)$ depends only on n.

A direct consequence of lemma 3.4 is the following

COROLLARY 3.5. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a nonnegative function which vanishes outside a compact set E. Suppose that $E \subset V_\epsilon(\delta)$ for some $\epsilon > 0$. Then for $\delta \geq 1$, (20) is satisfied with*

$$c(f) = c_3 \cdot M\delta,$$

where the constant c_3 depends on n only.

In order to prove lemma 3.4, we shall need the following:

LEMMA 3.6. *Let $\Lambda \subset \mathbb{R}^n$ be a m-dimensional lattice, and let*

$$A_t = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & t \end{pmatrix} \tag{30}$$

an n-dimensional linear transformation. Then for $t > 0$ we have

$$\det A_t\Lambda \leq t \det \Lambda. \tag{31}$$

Proof. We may assume that $m < n$, since if $m = n$, we obviously have an equality. Let $v_1,\, \ldots,\, v_m$ the basis of Λ and denote for every i, $u_i \in \mathbb{R}^{n-1}$ the vector, which consists of first $n-1$ coordinates of v_i. Also, let $x_i \in \mathbb{R}$ be the last coordinate of v_i. By switching vectors, if necessary, we may assume $x_1 \neq 0$. We consider the function

$$f(t) := (\det A_t\Lambda)^2,$$

as a function of $t \in \mathbb{R}$.
Obviously,

$$f(t) = \det\left(\langle u_i,\, u_j\rangle + x_i x_j t^2\right)_{1\le i,\, j\le m}.$$

Substracting $\frac{x_i}{x_1}$ times the first row from any other, we obtain:

$$f(t) = \begin{vmatrix} \langle u_1,\, u_j\rangle + x_1 x_j t^2 \\ \langle u_2,\, u_j\rangle - \frac{x_2}{x_1}\langle u_1,\, u_j\rangle \\ \vdots \\ \langle u_m,\, u_j\rangle - \frac{x_m}{x_1}\langle u_1,\, u_j\rangle \end{vmatrix},$$

and by the multilinearity property of the determinant, f is a linear function of t^2. Write

$$f(t) = a(t^2-1) + bt^2.$$

Thus

$$b = f(1); \quad a = -f(0),$$

and so $b = \det\Lambda$, and $a = -\det\left(\langle u_i,\, u_j\rangle\right) \le 0$, being minus the determinant of a Gram matrix. Therefore,

$$(\det A_t\Lambda)^2 - t^2\det\Lambda = a(t^2-1) \le 0$$

for $t \ge 1$, implying (30). □

Proof of lemma 3.4. We will prove the lemma, assuming $\beta = 2$. However, it implies the result of the lemma for any β, affecting only c_5. Let $\delta > 0$. Trivially,

$$N(g,\,\delta) = N(g_0,\,1),$$

where $g_0 = A_\delta^{-1}g$ with A_δ given by (30). Let $\lambda_1 \le \lambda_2 \le \ldots \le \lambda_n$ be the successive minima of g_0, and pick linearly independent lattice points $v_1, \ldots, v_n$ with $\|v_i\| = \lambda_i$. Denote M_i the linear space spanned by $v_1, \ldots, v_i$ and the lattice $\Lambda_i = g_0\mathbb{Z}^n \cap M_i$.
First, assume that $\lambda_n \le \sqrt{\tau^2 + (n-1)} =: r$. Now, by Gauss' argument,

$$\left| N(g_0,\,1) - \frac{2^{n-1}(2\tau - \tau^{-1})\delta}{\det g}\right| \le \frac{1}{\det g_0} vol(\Sigma),$$

where

$$\Sigma := \{x :\ dist(x,\,\partial V(1)) \le n\lambda_n\}.$$

Now, for $\lambda_n \le r$,

$$vol(\Sigma) \ll \lambda_n,$$

where the constant implied in the " $\ll$ "-notation depends on n only (this is obvious for $\lambda_n \le \frac{1}{2n}$, and trivial otherwise, since for $\lambda_n \le r$, $vol(\Sigma) = O(1)$).

Thus,

$$\left| N(g_0,\,1) - \frac{2^{n-1}(2\tau-\tau^{-1})\delta}{\det g} \right| \ll \frac{\lambda_n}{\det g_0} \ll \frac{1}{\det \Lambda_{n-1}}$$
$$= \frac{1}{vol(M_{n-1}/M_{n-1}\cap g_0\mathbb{Z}^n)} \le \frac{\delta}{vol(A_\delta M_{n-1}/A_\delta M_{n-1}\cap g\mathbb{Z}^n)}$$

Next, suppose that $\lambda_n > r$. Then,

$$V(\delta)\cap g_0\mathbb{Z}^n \subset V(\delta)\cap \Lambda_{n-1}.$$

Thus, by the induction hypothesis, the number of such points is:

$$\le c_4\sum_{i=0}^{k-1}\frac{1}{\det(\Lambda_i)} = \sum_{i=0}^{k-1}\frac{1}{vol(M_i/M_i\cap g_0\mathbb{Z}^n)}$$
$$\le \delta\sum_{i=0}^{k-1}\frac{1}{vol(A_\delta M_i/A_\delta \mathcal{M}_i\cap g\mathbb{Z}^n)}.$$

Since $\lambda_n > r$, we have

$$\frac{1}{\det g} = \frac{1}{\lambda_n}\frac{1}{\det g/\lambda_n} \ll \frac{1}{\det g/\lambda_n} \ll \frac{1}{\lambda_1\cdot\ldots\cdot\lambda_{n-1}},$$

and we're done by defining $L_i := A_\delta M_i$. □

4 UNSMOOTHING

4.1 AN ASYMPTOTIC FORMULA FOR N_Λ

We need an asymptotic formula for the *sharp* counting function N_Λ. Unlike the case of the standard lattice, $\mathbb{Z}^2$, in order to have a good control over the error terms we should use some Diophantine properties of the lattice we are working with. We adapt the following notations:
Let $\Lambda = \langle 1,\,\alpha+i\beta\rangle$, be a lattice, $d := \det\Lambda = \beta$ its determinant, and $t > 0$ a real variable. Denote the set of squared norms of Λ by

$$SN_\Lambda = \{|\vec{n}|^2:\ n\in\Lambda\}.$$

Suppose we have a function $\delta_\Lambda : SN_\Lambda \to \mathbb{R}$, such that given $\vec{k}\in\Lambda$, there are no vectors $\vec{n}\in\Lambda$ with $0 < ||\vec{n}|^2 - |\vec{k}|^2| < \delta_\Lambda(|\vec{k}|^2)$. That is,

$$\Lambda\cap\{\vec{n}\in\Lambda:\ |\vec{k}|^2-\delta_\Lambda(|\vec{k}|^2) < |\vec{n}|^2 < |\vec{k}|^2+\delta_\Lambda(|\vec{k}|^2)\} = A_{|\vec{k}|},$$

where

$$A_y := \{\vec{n}\in\Lambda:\ |\vec{n}| = y\}.$$

Extend δ_Λ to $\mathbb{R}$ by defining $\delta_\Lambda(x) := \delta_\Lambda(|\vec{k}|^2)$, where $\vec{k}\in\Lambda$ minimizes $|x-|\vec{k}|^2|$ (in the case there is any ambiguity, that is if $x = \frac{|\vec{n_1}|^2+|\vec{n_2}|^2}{2}$ for vectors $\vec{n_1},\,\vec{n_2}\in\Lambda$ with consecutive increasing norms, choose $\vec{k} := \vec{n_1}$). We have the following lemma:

Lemma 4.1. *For every* $a > 0$, $c > 1$,

$$N_\Lambda(t) = \frac{\pi}{\beta} t^2 - \frac{\sqrt{t}}{\beta\pi} \sum_{\substack{\vec{k} \in \Lambda^* \setminus \{0\} \\ |\vec{k}| \le \sqrt{N}}} \frac{\cos\left(2\pi t |\vec{k}| + \frac{\pi}{4}\right)}{|\vec{k}|^{\frac{3}{2}}} + O(N^a)$$
$$+ O\left(\frac{t^{2c-1}}{\sqrt{N}}\right) + O\left(\frac{t}{\sqrt{N}} \cdot \left(\log t + \log(\delta_\Lambda(t^2))\right)\right)$$
$$+ O\left(\log N + \log(\delta_{\Lambda^*}(t^2))\right)$$

As a typical example of such a function, δ_Λ, for $\Lambda = \langle 1, \alpha + i\beta \rangle$, with a Diophantine $(\alpha, \alpha^2, \beta^2)$, we may choose $\delta_\Lambda(y) = \frac{c}{y^K}$, where c is a constant. In this example, if $\Lambda \ni \vec{k} = (a, b)$, then by lemma 2.4, $A_{|\vec{k}|} = \pm(a, b)$, provided that $\beta \notin \mathbb{Q}(\alpha)$.

Sketch of proof. The proof of this lemma is essentially the same as the one of lemma 5.1 in [W]. We start from

$$\mathcal{Z}_\Lambda(s) := \frac{1}{2} \sum_{\vec{k} \in \Lambda \setminus 0} \frac{1}{|\vec{k}|^{2s}} = \sum_{(m,\, n) \in \mathbb{Z}_+^2 \setminus 0} \frac{1}{\left((m + n\alpha)^2 + (\beta n)^2\right)^s},$$

where the series is convergent for $\Re s > 1$.
The function $\mathcal{Z}_\Lambda$ has an analytic continuation to the whole complex plane, except for a single pole at $s = 1$, defined by the formula

$$\Gamma(s)\pi^{-s}\mathcal{Z}_\Lambda(s) = \int_1^\infty x^{s-1}\psi_\Lambda(x)dx + \frac{1}{d}\int_1^\infty x^{-s}\psi_{\Lambda^*}(x)dx - \frac{s - d(s-1)}{2ds(1-s)},$$

where

$$\psi_\Lambda(x) := \frac{1}{2} \sum_{\vec{k} \in \Lambda \setminus 0} e^{-\pi |\vec{k}|^2 x}.$$

Moreover, $\mathcal{Z}_\Lambda$ satisfies the following functional equation:

$$\mathcal{Z}_\Lambda(s) = \frac{1}{d}\chi(s)\mathcal{Z}_{\Lambda^*}(1-s), \tag{32}$$

with

$$\chi(s) = \pi^{2s-1}\frac{\Gamma(1-s)}{\Gamma(s)}. \tag{33}$$

The connection between N_Λ and $\mathcal{Z}_\Lambda$ is given in the following formula, which is satisfied for every $c > 1$:

$$\frac{1}{2}N_\Lambda(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \mathcal{Z}_\Lambda(s)\frac{x^s}{s}ds.$$

The result of the current lemma follows from moving the contour of the integration to the left, collecting the residue at $s = 1$ (see [W] for details). $\square$

PROPOSITION 4.2. *Let a lattice $\Lambda = \langle 1, \alpha + i\beta \rangle$ with a Diophantine triple of numbers $(\alpha^2, \alpha\beta, \beta^2)$ be given. Suppose that $L \to \infty$ as $T \to \infty$ and choose M, such that $L/\sqrt{M} \to 0$, but $M = O\big(T^\delta\big)$ for every $\delta > 0$ as $T \to \infty$. Suppose furthermore, that $M = O(L^{s_0})$ for some (fixed) $s_0 > 0$. Then*

$$\left\langle \left| S_\Lambda(t,\, \rho) - \tilde{S}_{\Lambda,\, M,\, L}(t) \right|^2 \right\rangle \ll \frac{1}{\sqrt{M}}$$

The proof of proposition 4.2 proceeds along the same lines as the one of proposition 5.1 in [W], using again an asymptotic formula for the sharp counting function, given by lemma 4.1. The only difference is that here we use proposition 3.1 rather than lemma 5.2 from [W].
Once we have proposition 4.2 in our hands, the proof of our main result, namely, theorem 1.1 proceeds along the same lines as the one of theorem 1.1 in [W].

ACKNOWLEDGEMENT. This work was supported in part by the EC TMR network *Mathematical Aspects of Quantum Chaos*, EC-contract no HPRN-CT-2000-00103 and the Israel Science Foundation founded by the Israel Academy of Sciences and Humanities. This work was carried out as part of the author's PHD thesis at Tel Aviv University, under the supervision of prof. Zeév Rudnick. The author wishes to thank Alex Eskin for his help as well as the anonymous referees. A substantial part of this work was done during the author's visit to the university of Bristol.

REFERENCES

[BL] Pavel M. Bleher and Joel L. Lebowitz *Variance of Number of Lattice Points in Random Narrow Elliptic Strip* Ann. Inst. Henri Poincare, Vol 31, n. 1, 1995, pages 27-58.

[BL2] Pavel M. Bleher *Distribution of the Error Term in the Weyl Asymptotics for the Laplace Operator on a Two-Dimensional Torus and Related Lattice Problems* Duke Mathematical Journal, Vol. 70, No. 3, 1993

[BL3] Bleher, Pavel *On the distribution of the number of lattice points inside a family of convex ovals* Duke Math. J. 67 (1992), no. 3, pages 461-481.

[BL4] Bleher, Pavel M. ; Lebowitz, Joel L. *Energy-level statistics of model quantum systems: universality and scaling in a lattice-point problem* J. Statist. Phys. 74 (1994), no. 1-2, pages 167-217.

[BS] A.S. Besicovitch *On the linear independence of fractional powers of integers* J. London Math. Soc. 15 (1940), pages 3-6.

[EMM] Eskin, Alex; Margulis, Gregory; Mozes, Shahar *Upper bounds and asymptotics in a quantitative version of the Oppenheim conjecture* Ann. of Math. (2) 147 (1998), no. 1, pages 93-141.

[EMM1] Eskin, Alex; Margulis, Gregory; Mozes, Shahar *Quadratic forms of signature (2,2) and eigenvalue spaces on rectangular 2-tori* , Ann. of Math. 161 (2005), no. 4, pages 679-721

[HB] Heath-Brown, D. R. *The distribution and moments of the error term in the Dirichlet divisor problem* Acta Arith. 60 (1992), no. 4, pages 389-415.

[HR] C. P. Hughes and Z. Rudnick *On the Distribution of Lattice Points in Thin Annuli* International Mathematics Research Notices, no. 13, 2004, pages 637-658.

[KM] Kleinbock, D. Y., Margulis, G. A. *Flows on homogeneous spaces and Diophantine approximation on manifolds* Ann. of Math. (2) 148 (1998), no. 1, pages 339-360.

[KR] S. Kristensen, *Strongly Diophantine pairs*, private communication.

[MAH] K. Mahler *Über das Mass der Menge aller S-Zahlen* Math. Ann. 106 (1932), pages 131-139.

[S] Wolfgang M. Schmidt *Diophantine approximation* Lecture Notes in Mathematics, vol. 785. Springer, Berlin, 1980.

[S2] Schmidt, Wolfgang M. *Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height* Duke Math. J. 35 1968 327-339.

[W] I. Wigman *The distribution of lattice points in elliptic annuli*, to be published in Quarterly Journal of Mathematics, Oxford, available online in http://qjmath.oxfordjournals.org/cgi/content/abstract/hai017v1

Igor Wigman
School of Mathematical Sciences
Tel Aviv University
Tel Aviv 69978
Israel
igorv@post.tau.ac.il

Automorphism Groups of Shimura Varieties

Haruzo Hida

Received: April 14, 2003
Revised: February 5, 2006

Communicated by Don Blasius

Abstract. In this paper, we determine the scheme automorphism group of the reduction modulo p of the integral model of the connected Shimura variety (of prime-to-p level) for reductive groups of type A and C. The result is very close to the characteristic 0 version studied by Shimura, Deligne and Milne-Shih.

2000 Mathematics Subject Classification: 11G15, 11G18, 11G25
Keywords and Phrases: Shimura variety, reciprocity law

There are two aspects of the Artin reciprocity law. One is representation theoretic, for example,

$$\mathrm{Hom}_{cont}(\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}), \mathbb{C}^\times) \cong \mathrm{Hom}_{cont}((\mathbb{A}^{(\infty)})^\times/\mathbb{Q}_+^\times, \mathbb{C}^\times)$$

via the identity of L–functions. Another geometric one is:

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong GL_1(\mathbb{A}^{(\infty)})/\mathbb{Q}_+^\times.$$

They are equivalent by duality, and the first is generalized by Langlands in non-abelian setting. Geometric reciprocity in non-abelian setting would be via Tannakian duality; so, it involves Shimura varieties.

Iwasawa theory is built upon the geometric reciprocity law. The cyclotomic field $\mathbb{Q}(\mu_{p^\infty})$ is the maximal p–ramified extension of $\mathbb{Q}$ fixed by $\widehat{\mathbb{Z}}^{(p)} \subset \mathbb{A}^\times/\mathbb{Q}^\times\mathbb{R}_+^\times$ removing the p–inertia toric factor $\mathbb{Z}_p^\times$. We then try to study arithmetically constructed modules X out of $\mathbb{Q}(\mu_{p^\infty}) \subset \mathbb{Q}^{ab}$. The main idea is to regard X as a module over over the Iwasawa algebra (which is a completed Hecke algebra relative to $\frac{GL_1(\mathbb{A}^{(\infty)})}{GL_1(\widehat{\mathbb{Z}}^{(p)})\mathbb{Q}_+^\times}$), and ring theoretic techniques are used to determine X.

If one wants to get something similar in a non-abelian situation, we really need a scheme whose automorphism group has an identification with $G(\mathbb{A}^{(\infty)})/\overline{Z(\mathbb{Q})}$ for a reductive algebraic group G. If $G = GL(2)_{/\mathbb{Q}}$, the tower $V_{/\mathbb{Q}^{ab}}$ of modular curves has $\mathrm{Aut}(V_{/\mathbb{Q}})$ identified with $GL_2(\mathbb{A}^{(\infty)})/Z(\mathbb{Q})$ as Shimura proved. The decomposition group of (p) is given by $B(\mathbb{Q}_p) \times SL_2(\mathbb{A}^{(p\infty)})/\{\pm 1\}$ for a Borel subgroup B, and I have been studying various arithmetically constructed modules over the Hecke algebra of $\frac{GL_2(\mathbb{A}^{(\infty)})}{GL_2(\widehat{\mathbb{Z}}^{(p)})U(\mathbb{Z}_p)\mathbb{Q}_+^\times}$, relative to the unipotent subgroup $U(\mathbb{Z}_p) \subset B(\mathbb{Z}_p)$ (removing the toric factor from the decomposition group). Such study has yielded a p–adic deformation theory of automorphic forms (see [PAF] Chapter 1 and 8), and it would be therefore important to study the decomposition group at p of a given Shimura variety, which is basically the automorphism group of the mod p Shimura variety.

Iwasawa theoretic applications (if any) are the author's motivation for the investigation done in this paper. However the study of the automorphism group of a given Shimura variety has its own intrinsic importance. As is clear from the construction of Shimura varieties done by Shimura ([Sh]) and Deligne ([D1] 2.4-7), their description of the automorphism group (of Shimura varieties of characteristic 0) is deeply related to the geometric reciprocity laws generalizing classical ones coming from class field theory and is almost equivalent to the existence of the canonical models defined over a canonical algebraic number field. Except for the modulo p modular curves and Shimura curves studied by Y. Ihara, the author is not aware of a single determination of the automorphism group of the integral model of a Shimura variety and of its reduction modulo p, although Shimura indicated and emphasized at the end of his introduction of the part I of [Sh] a good possibility of having a canonical system of automorphic varieties over finite fields described by the adelic groups such as the ones studied in this paper.

We shall determine the automorphism group of mod p Shimura varieties of PEL type coming from symplectic and unitary groups.

1 Statement of the theorem

Let B be a central simple algebra over a field M with a positive involution ρ (thus $\mathrm{Tr}_{B/\mathbb{Q}}(xx^\rho) > 0$ for all $0 \neq x \in B$). Let F be the subfield of M fixed by ρ. Thus F is a totally real field, and either $M = F$ or M is a CM quadratic extension of F. We write O (resp. R) for the integer ring of F (resp. M). We fix an algebraic closure $\mathbb{F}$ of the prime field $\mathbb{F}_p$ of characteristic $p > 0$. Fix a proper subset Σ of rational places including ∞ and p. Let $F_+^\times$ be the subset of totally positive elements in F, and $O_{(\Sigma)}$ denotes the localization of O at Σ (disregarding the infinite place in Σ) and O_Σ is the completion of O at Σ (again disregarding the infinite place). We write $O_{(\Sigma)+}^\times = F_+^\times \cap O_{(\Sigma)}$. We have an exact sequence

$$1 \to B^\times/M^\times \to \mathrm{Aut}_{alg}(B) \to \mathrm{Out}(B) \to 1,$$

and by a theorem of Skolem-Noether, $\mathrm{Out}(B) \subset \mathrm{Aut}(M)$. Here $b \in B^\times$ acts on B by $x \mapsto bxb^{-1}$. Since B is central simple, any simple B-module N is isomorphic each other. Take one such simple B-module. Then $\mathrm{End}_B(N)$ is a division algebra D°. Taking a base of N over D° and identifying $N \cong (D^\circ)^r$, we have $B = \mathrm{End}_{D^\circ}(N) \cong M_r(D)$ for the opposite algebra D of D°. Letting $\mathrm{Aut}_{alg}(D)$ act on $b \in M_r(D)$ entry-by-entry, we have $\mathrm{Aut}_{alg}(D) \subset \mathrm{Aut}_{alg}(B)$, and $\mathrm{Out}(D) = \mathrm{Out}(B)$ under this isomorphism.

Let O_B be a maximal order of B. Let L be a projective O_B–module with a non-degenerate F-linear alternating form $\langle\ ,\ \rangle : L_{\mathbb{Q}} \times L_{\mathbb{Q}} \to F$ for $L_A = L \otimes_{\mathbb{Z}} A$ such that $\langle bx, y\rangle = \langle x, b^\rho y\rangle$ for all $b \in B$. Identifying $L_{\mathbb{Q}}$ with a product of copies of the column vector space D^r on which $M_r(D)$ acts via matrix multiplication, we can let $\sigma \in \mathrm{Aut}_{alg}(D)$ act component-wise on $L_{\mathbb{Q}}$ so that $\sigma(bv) = \sigma(b)\sigma(v)$ for all $\sigma \in \mathrm{Aut}_{alg}(D)$.

Let C be the opposite algebra of $C^\circ = \mathrm{End}_B(L_{\mathbb{Q}})$. Then C is a central simple algebra and is isomorphic to $M_s(D)$, and hence $\mathrm{Out}(C) \cong \mathrm{Out}(D) = \mathrm{Out}(B)$. We write $C_A = C \otimes_{\mathbb{Q}} A$, $B_A = B \otimes_{\mathbb{Q}} A$ and $F_A = F \otimes_{\mathbb{Q}} A$. The algebra C has involution $*$ given by $\langle cx, y\rangle = \langle x, c^* y\rangle$ for $c \in C$, and this involution "$*$" of C extends to an involution again denoted by "$*$" of $\mathrm{End}_{\mathbb{Q}}(L_{\mathbb{Q}})$ given by $\mathrm{Tr}_{F/\mathbb{Q}}(\langle gx, y\rangle) = \mathrm{Tr}_{F/\mathbb{Q}}(\langle x, g^* y\rangle)$ for $g \in \mathrm{End}_{\mathbb{Q}}(L_{\mathbb{Q}})$. The involution $*$ (resp. ρ) induces the involution $* \otimes 1$ (resp. $\rho \otimes 1$) on C_A (resp. on B_A) which we write as $*$ (resp. ρ) simply. Define an algebraic group $G_{/\mathbb{Q}}$ by

$$G(A) = \left\{ g \in C_A \middle| \nu(g) := gg^* \in (F_A)^\times \right\} \quad \text{for } \mathbb{Q}\text{-algebras } A \tag{1.1}$$

and an extension $\widetilde{G}$ of G by the following subgroup of the opposite group $\mathrm{Aut}^\circ_A(L_A)$ of the A-linear automorphism group $\mathrm{Aut}_A(L_A)$:

$$\widetilde{G}(A) = \left\{ g \in \mathrm{Aut}^\circ_A(L_A) \middle| gC_Ag^{-1} = C_A \ \text{ and } \ \nu(g) := gg^* \in (F_A)^\times \right\}. \tag{1.2}$$

Since $C^\circ = \mathrm{End}_B(L_{\mathbb{Q}})$, we have $B^\circ = \mathrm{End}_C(L_{\mathbb{Q}})$, and from this we find that $gBg^{-1} = B \Leftrightarrow gCg^{-1} = C$ for $g \in \mathrm{Aut}_{\mathbb{Q}}(L_{\mathbb{Q}})$, and if this holds for g, then $gg^* \in F^\times \Leftrightarrow gx^\rho g^{-1} = (gxg^{-1})^\rho$ for all $x \in B$ and $gy^*g^{-1} = (gyg^{-1})^*$ for all $y \in C$. Then G is a normal subgroup of $\widetilde{G}$ of finite index, and $\widetilde{G}(\mathbb{Q})/G(\mathbb{Q}) = \mathrm{Out}_{\mathbb{Q}\text{-alg}}(C,*)$. Here $\mathrm{Out}_{\mathbb{Q}\text{-alg}}(C,*)$ is the outer automorphism group of C commuting with $*$; in other words, it is the quotient of the group of automorphisms of C commuting with $*$ by the group of inner automorphisms commuting with $*$. Thus we have $\mathrm{Out}_{\mathbb{Q}\text{-alg}}(C,*) \subset H^0(\langle * \rangle, \mathrm{Out}_{\mathbb{Q}\text{-alg}}(C)) \subset \mathrm{Out}_{\mathbb{Q}\text{-alg}}(C) \subset \mathrm{Aut}(M/\mathbb{Q})$. All the four groups are equal if $G_{/\mathbb{Q}}$ is quasi-split but are not equal in general. We put $PG = G/Z$ and $P\widetilde{G} = \widetilde{G}/Z$ for the center Z of G.

We write G_1 for the derived group of G; thus, $G_1 = \{g \in G | N_C(g) = \nu(g) = 1\}$ for the reduced norm N_C of C over M. We write $Z^G = G/G_1$ for the cocenter of G. Then $g \mapsto (\nu(g), N_C(g))$ identifies Z^G with a sub-torus of $\mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_m \times \mathrm{Res}_{M/\mathbb{Q}}\mathbb{G}_m$. If $M = F$, G_1 is equal to the kernel of the similitude map $g \mapsto \nu(g)$; so, in this case, we ignore the right factor $\mathrm{Res}_{M/\mathbb{Q}}\mathbb{G}_m$ and regard $Z^G \subset \mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_m$. By a result of Weil ([W]) combined with an observation in [Sh] II (4.2.1), the automorphism group $\mathrm{Aut}_{A\text{-alg}}(C_A, *)$ of the algebra C_A preserving the involution $*$ is given by $P\widetilde{G}(A)$. In other words, we have an exact sequence of $\mathbb{Q}$-algebraic groups

$$1 \to PG(A) \to \mathrm{Aut}_{A\text{-alg}}(C_A, *)(= P\widetilde{G}(A)) \to \mathrm{Out}_{A\text{-alg}}(B_A, \rho) \to 1. \quad (1.3)$$

We write

$$\pi : \widetilde{G}(A) \to \widetilde{G}(A)/G(A) = \mathrm{Out}_{A\text{-alg}}(B_A, \rho) \subset \mathrm{Out}_{A\text{-alg}}(B_A)$$

for the projection.

The automorphism group of the Shimura variety of level away from Σ is a quotient of the following locally compact subgroup of $\widetilde{G}(\mathbb{A}^{(\Sigma)})$:

$$\mathcal{G}^{(\Sigma)} = \left\{ x \in \widetilde{G}(\mathbb{A}^{(\Sigma)}) \middle| \pi(x) \in \mathrm{Out}_{\mathbb{Q}\text{-alg}}(B, \rho) \right\}, \quad (1.4)$$

where we embed $\mathrm{Out}_{\mathbb{Q}\text{-alg}}(B, \rho)$ into $\prod_{\ell \notin \Sigma} \mathrm{Out}_{\mathbb{Q}_\ell\text{-alg}}(B_\ell) = \mathrm{Out}_{\mathbb{A}^{(\Sigma)}\text{-alg}}(B \otimes_{\mathbb{Q}} \mathbb{A}^{(\Sigma)})$ by the diagonal map ($B_\ell = B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$).

We suppose to have an $\mathbb{R}$–algebra homomorphism $h : \mathbb{C} \to C_{\mathbb{R}}$ such that $h(\overline{z}) = h(z)^*$ and

(h1) $(x, y) = \langle x, h(i)y \rangle$ induces a positive definite hermitian form on $L_{\mathbb{R}}$.

We define X to be the conjugacy classes of h under $G(\mathbb{R})$. Then X is a finite disjoint union of copies of the hermitian symmetric domain isomorphic to $G(\mathbb{R})^+/C_h$, where C_h is the stabilizer of h and the superscript "+" indicates the identity connected component of the Lie group $G(\mathbb{R})$. Then the pair (G, X) satisfies the three axioms (see [D1] 2.1.1.1-3) specifying the data for defining the Shimura variety Sh (and its field of definition, the reflex field E; see [Ko] Lemma 4.1). In [D1], two more axioms are stated to simplify the situation: (2.1.1.4-5). These two extra axioms may not hold generally for our choice of (G, X) (see [M] Remark 2.2).

The complex points of Sh are given by

$$Sh(\mathbb{C}) = G(\mathbb{Q}) \backslash \left(G(\mathbb{A}^{(\infty)}) \times X \right) / \overline{Z(\mathbb{Q})}.$$

This variety can be characterized as a moduli variety of abelian varieties up to isogeny with multiplication by B. For each $x \in X$, we have $h_x : \mathbb{C} \to C_{\mathbb{R}}$ given by $z \mapsto g \cdot h(z)g^{-1}$ for $g \in G(\mathbb{R})/C_h$ sending h to x. Then $v \mapsto h_x(z)v$ for $z \in \mathbb{C}$ gives rise to a complex vector space structure on $L_{\mathbb{R}}$, and $\mathbb{X}_x(\mathbb{C}) = L_{\mathbb{R}}/L$ is an abelian variety, because by (h1), $\langle\ ,\ \rangle$ induces a Riemann form on L. The multiplication by $b \in O_B$ is given by $(v \mod L) \mapsto (b \cdot v \mod L)$.

We suppose

(h2) all rational primes in Σ are unramified in $M/\mathbb{Q}$, and Σ contains ∞ and p;

(h3) For every prime $\ell \in \Sigma$, $O_{B,\ell} = O_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong M_n(R_\ell)$ for $R_\ell = R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$;

(h4) For every prime $\ell \in \Sigma$, $\langle\ ,\ \rangle$ induces $L_\ell = L \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{Hom}(L_\ell, O_\ell)$;

(h5) The derived subgroup G_1 is simply connected; so, $G_1(\mathbb{R})$ is of type A (unitary groups) or of type C (symplectic groups).

Let $G(\mathbb{Z}_\Sigma) = \{g \in G(\mathbb{Q}_\Sigma) | g \cdot L_\Sigma = L_\Sigma\}$ for $\mathbb{Q}_\Sigma = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_\Sigma$ and $L_\Sigma = L \otimes_{\mathbb{Z}} \mathbb{Z}_\Sigma$. We define $Sh^{(\Sigma)} = Sh/G(\mathbb{Z}_\Sigma)$. This moduli interpretation (combined with (h1-4)) allows us to have a well defined p–integral model of level away from Σ (see below for a brief description of the moduli problem, and a more complete description can be found in [PAF] 7.1.3). In other words,

$$Sh^{(\Sigma)}(\mathbb{C}) = G(\mathbb{Q})\backslash \left(G(\mathbb{A}^{(\infty)}) \times X\right) / \overline{Z(\mathbb{Q})} G(\mathbb{Z}_\Sigma)$$

has a well defined smooth model over $O_{E,(p)} := O_E \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ which is again a moduli scheme of abelian varieties up to prime-to–Σ isogenies. We write $Sh^{(p)}$ for $Sh^{(\Sigma)}$ when $\Sigma = \{p, \infty\}$. We also write $\mathbb{Q}_\Sigma^{(p)} = \mathbb{Q}_\Sigma/\mathbb{Q}_p$ and $\mathbb{Z}_\Sigma^{(p)} = \mathbb{Z}_\Sigma/\mathbb{Z}_p$.

We have taken full polarization classes under scalar multiplication by $O^\times_{(\Sigma)+}$ in our moduli problem (while Kottwitz's choice in [Ko] is a partial class of multiplication by $\mathbb{Z}^\times_{(\Sigma)+}$). By our choice, the group G is the full similitude group, while Kottwitz choice is a partial rational similitude group. Our choice is convenient for our purpose because G has cohomologically trivial center, and the special fiber at p of the characteristic 0 Shimura variety $Sh/G(\mathbb{Z}_\Sigma)$ gives rise to the mod p moduli of abelian varieties of the specific type we study (as shown in [PAF] Theorem 7.5), while Kottwitz's mod p moduli is a disjoint union of the reduction modulo p of finitely many characteristic 0 Shimura varieties associated to finitely many different pairs (G_i, X_i) with G_i locally isomorphic each other at every place ([Ko] Section 8).

We fix a strict henselization $\mathcal{W} \subset \overline{\mathbb{Q}}$ of $\mathbb{Z}_{(p)}$. Thus $\mathcal{W}$ is an unramified valuation ring with residue field $\mathbb{F} = \overline{\mathbb{F}}_p$. Under these five conditions (h1-5), combining (and generalizing) the method of Chai-Faltings [DAV] for Siegel modular varieties and that of [Ra] for Hilbert modular varieties, Fujiwara ([F] Theorem in §0.4) proved the existence of a smooth toroidal compactification of $Sh^{(p)}_S = Sh^{(p)}/S$ for sufficiently small principal congruence subgroups S with respect to L in $G(\mathbb{A}^{(p)})$ as an algebraic space over a suitable open subscheme of $Spec(O_E)$ containing $Spec(\mathcal{W} \cap E)$. Although our moduli problem is slightly different from the one Kottwitz considered in [Ko], as was done in [PAF] 7.1.3, following [Ko] closely, the p-integral moduli $Sh^{(p)}$ over $O_{E,(p)}$ is proven to be a quasi-projective scheme; so, Fujiwara's algebraic space is a projective scheme (if we choose the toroidal compactification data well). If the reader is not familiar with Fujiwara's work, the reader can take the existence of the smooth toroidal compactification (which is generally believed to be true) as an assumption of our main result.

Since p is unramified in $M/\mathbb{Q}$, $O_{E,(p)}$ is contained in $\mathcal{W}$. We fix a geometrically connected component $V_{/\overline{\mathbb{Q}}}$ of $Sh^{(\Sigma)} \times_E \overline{\mathbb{Q}}$ and write $V_{/\mathcal{W}}$ for the schematic closure of $V_{/\overline{\mathbb{Q}}}$ in $Sh^{(\Sigma)}_{/\mathcal{W}} := Sh^{(\Sigma)}_{/O_{E,(p)}} \otimes_{O_{E,(p)}} \mathcal{W}$. By Zariski's connectedness theorem combined with the existence of a normal projective compactification (either minimal or smooth) of $Sh^{(\Sigma)}_{/\mathcal{W}}$, the reduction $V_{/\mathbb{F}} = V \times_{\mathcal{W}} \mathbb{F}$ is a geometrically irreducible component of $Sh^{(\Sigma)}_{/\mathcal{W}} \otimes_{\mathcal{W}} \mathbb{F}$. The scheme $Sh^{(\Sigma)}_{/S}$ classifies, for any S–scheme T, quadruples $(A, \overline{\lambda}, i, \phi^{(\Sigma)})_{/T}$ defined as follows: A is an abelian scheme of dimension $\frac{1}{2}\operatorname{rank}_{\mathbb{Z}} L$ for which we define the Tate module $\mathcal{T}(A) = \varprojlim_N A[N]$, $\mathcal{T}^{(\Sigma)}(A) = \mathcal{T}(A) \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(\Sigma)}$, $\mathcal{T}_\Sigma(A) = \mathcal{T}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\Sigma$ and $V^{(\Sigma)}(A) = \mathcal{T}(A) \otimes_{\mathbb{Z}} \mathbb{A}^{(\Sigma)}$; The symbol i stands for an algebra embedding $i : O_B \hookrightarrow \operatorname{End}(A)$ taking the identity to the identity map on A; $\phi^{(\Sigma)}$ is a level structure away from Σ, that is, an O_B–linear $\phi^{(p)} : L \otimes_{\mathbb{Q}} \mathbb{A}^{(p)} \cong V^{(p)}(A)$ modulo $G(\mathbb{Z}_\Sigma)$, where we require that $\phi^{(p)}_\Sigma : L \otimes_{\mathbb{Z}} \mathbb{Q}^{(p)}_\Sigma \cong \mathcal{T}_\Sigma(A) \otimes_{\mathbb{Z}} \mathbb{Q}^{(p)}_\Sigma$ send $L \otimes_{\mathbb{Z}} \mathbb{Z}^{(p)}_\Sigma$ isomorphically onto $\mathcal{T}_\Sigma(A) \otimes_{\mathbb{Z}} \mathbb{Z}^{(p)}_\Sigma$; $\overline{\lambda}$ is a class of polarizations λ up to scalar multiplication by $i(O^\times_{(\Sigma)+})$ which induces the Riemann form $\langle\cdot,\cdot\rangle$ on L up to scalar multiplication by $O^\times_{(\Sigma)+}$. There is one more condition (cf. [Ko] Section 5 or [PAF] 7.1.1 (det)) specifying the module structure of $\Omega_{A/T}$ over $O_B \otimes_{\mathbb{Z}} \mathcal{O}_T$ (which we do not recall).

The group $G(\mathbb{A}^{(\Sigma)})$ acts on $Sh^{(\Sigma)}$ by $\phi^{(\Sigma)} \mapsto \phi^{(\Sigma)} \circ g$. We can extend the action of $G(\mathbb{A}^{(\Sigma)})$ to the extension $\mathcal{G}^{(\Sigma)}$. Each element $g \in \mathcal{G}^{(\Sigma)}$ with projection $\pi(g) = \sigma_g$ in $\operatorname{Out}_{\mathbb{Q}\text{-alg}}(B, \rho)$ acts also on $Sh^{(\Sigma)}$ by $(A, \overline{\lambda}, i, \phi^{(\Sigma)})_{/T} \mapsto (A, \overline{\lambda}, i \circ \sigma_g, \phi^{(\Sigma)} \circ g)_{/T}$.

The reduced norm map $N_C : C^\times \to M^\times$ extends uniquely to a homomorphism $N_C : \widetilde{G} \to \operatorname{Res}_{M/\mathbb{Q}}\mathbb{G}_m$ of algebraic groups. Indeed, we have an isomorphism $\widetilde{G}(A) \cong \operatorname{Out}_{A\text{-alg}}(C_A, *) \ltimes G(A)$ for a suitable finite extension field A of M, and the norm map N_C factoring through the right factor $G(A)$ descends to $N_C : \widetilde{G}(\mathbb{Q}) \to M^\times$ (which determines

$N_C : \widetilde{G} \to \mathrm{Res}_{M/\mathbb{Q}}\mathbb{G}_m$ independently of the choice of A). The diagonal map $\mu : \widetilde{G} \ni g \mapsto (\nu(g), N_C(g)) \in (\mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_m \times \mathrm{Res}_{M/\mathbb{Q}}\mathbb{G}_m)$ factors through the cocenter Z^G of G; so, we have a homomorphism $\mu : \widetilde{G} \to Z^G$ of algebraic $\mathbb{Q}$-groups. We write $Z^G(\mathbb{R})^+$ for the identity connected component of $Z^G(\mathbb{R})$ and put $Z^G(\mathbb{Z}_{(\Sigma)})^+ = Z^G(\mathbb{R})^+ \cap \left(O^\times_{(\Sigma)} \times R^\times_{(\Sigma)}\right)$; so, $Z^G(\mathbb{Z}_{(\Sigma)})^+ = O^\times_{(\Sigma)+}$ if $M = F$. Similarly, we identify Z with $\mathrm{Res}_{R/\mathbb{Z}}\mathbb{G}_m$ so that $Z(\mathbb{Z}_{(\Sigma)}) = R^\times_{(\Sigma)}$.

We now state the main result:

Theorem 1.1. *Suppose* (h1-5)*. Then the field automorphism group* $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$ *of the function field* $\mathbb{F}(V)$ *over* $\mathbb{F}$ *is given by the stabilizer the connected component* V *(in* $\pi_0(Sh^{(\Sigma)}_{/\mathbb{F}})$*) inside* $\mathcal{G}^{(\Sigma)}/\overline{Z(\mathbb{Z}_{(\Sigma)})}$*. The stabilizer is given by*

$$\mathcal{G}_V = \frac{\left\{g \in \mathcal{G}^{(\Sigma)} \middle| \mu(g) \in \overline{Z^G(\mathbb{Z}_{(\Sigma)})^+}\right\}}{\overline{Z(\mathbb{Z}_{(\Sigma)})}},$$

where $\overline{Z^G(\mathbb{Z}_{(\Sigma)})^+}$ *(resp.* $\overline{Z(\mathbb{Z}_{(\Sigma)})}$*) is the topological closure of* $Z^G(\mathbb{Z}_{(\Sigma)})^+$ *(resp.* $Z(\mathbb{Z}_{(\Sigma)})$*)in* $Z^G(\mathbb{A}^{(\Sigma)})$ *(resp. in* $G(\mathbb{A}^{(\Sigma)})$*). In particular, this implies that the scheme automorphism group* $\mathrm{Aut}(V_{/\mathbb{F}})$ *coincides with the field automorphism group* $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$ *and is given as above.*

This type of theorems in characteristic 0 situation has been proven mainly by Shimura, Deligne and Milne-Shih (see [Sh] II, [D1] 2.4-7 and [MS] 4.13), whose proof uses the topological fundamental group of V and the existence of the analytic universal covering space. Our proof uses the algebraic fundamental group of V and the solution of the Tate conjecture on endomorphisms of abelian varieties over function fields of characteristic p due to Zarhin (see [Z], [DAV] Theorem V.4.7 and [RPT]). The characteristic 0 version of the finiteness theorem due to Faltings (see [RPT]) yields a proof in characteristic 0, arguing slightly more, but we have assumed for simplicity that the characteristic of the base field is positive (see [PAF] for the argument in characteristic 0). We shall give the proof in the following section and prove some group theoretic facts necessary in the proof in the section following the proof. Our original proof was longer and was based on a density result of Chai (which has been proven under some restrictive conditions on G), and Ching-Li Chai suggested us a shorter proof via the results of Zarhin and Faltings (which also eliminated the extra assumptions we imposed). The author is grateful for his comments.

2 Proof of the theorem

We start with

Proposition 2.1. *Suppose* (h1-5)*. Let* $\sigma \in \mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$*. Let* $U \subset V$ *be a connected open dense subscheme on which* $\sigma \in \mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$ *induces an* *isomorphism* $U \cong \sigma(U)$. *For* $x \in (U \cap \sigma(U))(\mathbb{F})$, *the two abelian varieties* $\mathbb{X}_x$ *and* $\mathbb{X}_{\sigma(x)}$ *are isogenous over* $\mathbb{F}$, *where* $\mathbb{X}_x$ *is the abelian variety sitting over* x.

Proof. We recall the subgroup in the theorem:

$$\mathcal{G}_V = \frac{\left\{g \in \mathcal{G}^{(\Sigma)} \middle| \mu(g) \in \overline{Z^G(\mathbb{Z}_{(\Sigma)})^+}\right\}}{\overline{Z(\mathbb{Z}_{(\Sigma)})}}.$$

By characteristic 0 theory in [D] Theorem 2.4 or [MS] p.929 (or [PAF] 7.2.3), the action of $\widetilde{G}(\mathbb{A}^{(\Sigma)})/\overline{Z(\mathbb{Z}_{(\Sigma)})}$ on $\pi_0(Sh^{(\Sigma)}_{/\overline{\mathbb{Q}}})$ factors through the homomorphism $\widetilde{G}(\mathbb{A}^{(\Sigma)})/\overline{Z(\mathbb{Z}_{(\Sigma)})} \to Z^G(\mathbb{A}^{(\Sigma)})/\overline{Z^G(\mathbb{Z}_{(\Sigma)})^+}$ induced by μ. The idele class group of cocenter $Z^G(\mathbb{A}^{(\Sigma)})/\overline{Z^G(\mathbb{Z}_{(\Sigma)})^+}$ acts on $\pi_0(Sh^{(\Sigma)}_{/\overline{\mathbb{Q}}})$ faithfully.

Since each geometrically connected component of $Sh^{(\Sigma)}$ is defined over the field $\mathcal{K}$ of fractions of $\mathcal{W}$, by the existence of a normal projective compactification (either smooth toroidal or minimal) over $\mathcal{W}$ (and Zariski's connectedness theorem), we have a bijection between geometrically connected components over $\mathcal{K}$ and over the residue field $\mathbb{F}$ induced by reduction modulo p. Then the stabilizer in $\widetilde{G}(\mathbb{A}^{(\Sigma)})/\overline{Z(\mathbb{Z}_{(\Sigma)})}$ of V in $\pi_0(Sh^{(\Sigma)}_{/\mathbb{F}})$ is given by $\mathcal{G}_V$.

The scheme theoretic automorphism group $\mathrm{Aut}(V/\mathbb{F})$ is a subgroup of the field automorphism group $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$. By a generalization due to N. Jacobson of the Galois theory (see [IAT] 6.3) to field automorphism groups, the Krull topology of $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$ is defined by a system of open neighborhoods of the identity, which is made up of the stabilizers of subfields of $\mathbb{F}(V)$ finitely generated over $\mathbb{F}$. For an open compact subgroups K in $G(\mathbb{A}^{(\Sigma)})/\overline{Z(\mathbb{Z}_{(\Sigma)})}$, we consider the image V_K of V in $Sh^{(\Sigma)}/K$. Then we have $V_K = V/\overline{K}_V$ for $\overline{K}_V = K \cap \mathcal{G}_V$, and $\overline{K}_V$ is isomorphic to the scheme theoretic Galois group $\mathrm{Gal}(V/V_{K/\mathbb{F}})$, which is in turn isomorphic to $\mathrm{Gal}(\mathbb{F}(V)/\mathbb{F}(V_K))$. Since all sufficiently small open compact subgroups of $\mathcal{G}_V$ are of the form $\overline{K}_V$ for open compact subgroups K of $G(\mathbb{A}^{(\Sigma)})/\overline{Z(\mathbb{Z}_{(\Sigma)})}$, the $\overline{K}_V$'s for open compact subgroups K of $G(\mathbb{A}^{(\Sigma)})/\overline{Z(\mathbb{Z}_{(\Sigma)})}$ give a fundamental system of open neighborhoods of the identity of $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$ under the Krull topology. In other words, the scheme theoretic automorphism group $\mathrm{Aut}(V_{/\mathbb{F}})$ is an open subgroup of $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$. If we choose K sufficiently small depending on $\sigma \in \mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$, we have ${}^{\sigma}\overline{K}_V = \sigma\overline{K}_V\sigma^{-1}$ still inside $\mathcal{G}_V$ in $G(\mathbb{A}^{(\Sigma)})/\overline{Z(\mathbb{Z}_{(\Sigma)})}$. We write U_K (resp. $U_{{}^{\sigma}K}$) for the image of U (resp. of $\sigma(U)$) in V_K (resp. in $V_{{}^{\sigma}K}$).

By the above description of the stabilizer of V, the image of $G_1(\mathbb{A}^{(\Sigma)})$ in the scheme automorphism group $\mathrm{Aut}(Sh^{(\Sigma)}_{/\mathbb{F}})$ is contained in the stabilizer $\mathrm{Aut}(V_{/\mathbb{F}})$ and hence in the field automorphism group $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$. Let $\overline{G}_1(\mathbb{A}^{(\Sigma)})$ be the image of $G_1(\mathbb{A}^{(\Sigma)})$ in $\mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$ (so $\overline{G}_1(\mathbb{A}^{(\Sigma)})$ is isomorphic to the quotient of $G_1(\mathbb{A}^{(\Sigma)})$ by the center of $G_1(\mathbb{Z}_{(\Sigma)})$). We take a sufficiently small open compact subgroup S of $G(\mathbb{A}^{(\Sigma)})$. We write $S_1 = G_1(\mathbb{A}^{(\Sigma)}) \cap S$ and $\overline{S}_1$ for the image of S_1 in $\overline{G}_1(\mathbb{A}^{(\Sigma)})$ with $\overline{G}_1(\mathbb{A}^{(\Sigma)})$. Shrinking S if necessary, we may assume that $S_1 \cong \overline{S}_1$, that V/V_S is étale, that $\mathrm{Gal}(V/V_{S/\mathbb{F}}) = \overline{S}_1$, that $S = \prod_\ell S_\ell$ with $S_\ell = S \cap G(\mathbb{Q}_\ell)$ for primes $\ell \notin \Sigma$ and that ${}^\sigma\overline{S}_1 := \sigma\overline{S}_1\sigma^{-1} \subset \overline{G}_1(\mathbb{A}^{(\Sigma)})$. We identify $Sh^{(p)}/\widetilde{S} = Sh^{(\Sigma)}/S$ for $\widetilde{S} = S \times G(\mathbb{Z}_\Sigma^{(p)})$, where $\mathbb{Z}_\Sigma^{(p)} = \prod_{\ell \in \Sigma - \{p,\infty\}} \mathbb{Z}_\ell$. Since $S_1 \cong \overline{S}_1$, we hereafter identify the two groups.

Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{W}$ and we write $\kappa = O_E/(O_E \cap \mathfrak{m})$ for the reflex field E. Since $Sh^{(\Sigma)}_{/\mathbb{F}}$ is a scalar extension relative to $\mathbb{F}/\kappa$ of the model $Sh^{(\Sigma)}_{/\kappa}$ defined over the finite field κ, the Galois group $\mathrm{Gal}(\mathbb{F}/\kappa)$ acts on the underlying topological space of $Sh^{(\Sigma)}/S$. Since $\pi_0((Sh^{(\Sigma)}/S)_{/\overline{\mathbb{Q}}})$ is finite, $\pi_0((Sh^{(\Sigma)}/S)_{/\mathbb{F}})$ is finite, and we have therefore a finite extension $\mathbb{F}_q$ of the prime field $\mathbb{F}_p$ such that $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ gives the stabilizer of V_S in $\pi_0((Sh^{(\Sigma)}/S)_{/\mathbb{F}})$. We may assume that (as varieties) U_S and $U_{^\sigma S}$ are defined over $\mathbb{F}_q$ and that $U_S \times_{\mathbb{F}_q} \mathbb{F}$ and $U_{^\sigma S} \times_{\mathbb{F}_q} \mathbb{F}$ are irreducible. Since $\sigma \in \mathrm{Hom}(U_S, U_{^\sigma S})$, the Galois group $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ acts on σ by conjugation. By further extending $\mathbb{F}_q$ if necessary, we may assume that σ is fixed by $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$, $x \in U_S(\mathbb{F}_q)$ and $\sigma(x) \in U_{^\sigma S}(\mathbb{F}_q)$. Thus σ descends to an isomorphism $\sigma_S : U_S \cong U_{^\sigma S}$ defined over $\mathbb{F}_q$.

Let $\mathbb{X}_{S/\mathbb{F}_q} \to U_{S/\mathbb{F}_q}$ be the universal abelian scheme with the origin $\mathbf{0}$. We write $(\mathbb{X}_x, \mathbf{0}_x)$ for the fiber of $(\mathbb{X}_S, \mathbf{0})$ over x and fix a geometric point $\overline{x} \in V(\mathbb{F})$ above x. The prime-to-p part $\pi_1^{(p)}(\mathbb{X}_x, \mathbf{0}_{\overline{x}})$ of $\pi_1(\mathbb{X}_x, \mathbf{0}_{\overline{x}})$ is canonically isomorphic to the prime to-p part $\mathcal{T}^{(p)}(\mathbb{X}_{\overline{x}/\mathbb{F}})$ of the Tate module $\mathcal{T}(\mathbb{X}_{\overline{x}/\mathbb{F}})$, and the p-part of $\pi_1(\mathbb{X}_x, \mathbf{0}_{\overline{x}})$ is the discrete p-adic Tate module of $\mathbb{X}_{x/\mathbb{F}}$ which is the inverse limit of the reduced part of $\mathbb{X}_x[p^n](\mathbb{F})$ (e.g. [ABV] page 171). We can make the quotient $\pi_1^{\{p\}}(\mathbb{X}_{S/\mathbb{F}}, \mathbf{0}_{\overline{x}})$ by the image of the p-part of $\pi_1(\mathbb{X}_x, \mathbf{0}_{\overline{x}})$. Then we have the following exact sequence ([SGA] 1.X.1.4):

$$\mathcal{T}^{(p)}(\mathbb{X}_{\overline{x}}) \xrightarrow{i} \pi_1^{\{p\}}(\mathbb{X}_{S/\mathbb{F}_q}, \mathbf{0}_{\overline{x}}) \to \pi_1(U_{S/\mathbb{F}_q}, \overline{x}) \to 1.$$

This sequence is split exact, because of the zero section $\mathbf{0} : U_S \to \mathbb{X}_S$. The multiplication by N: $\mathbb{X} \to \mathbb{X}$ (for N prime to p) is an irreducible étale covering, and we conclude that $\mathcal{T}^{(p)}(\mathbb{X}_x)$ injects into $\pi_1^{\{p\}}(\mathbb{X}_{S/\mathbb{F}}, \mathbf{0}_{\overline{x}})$. We make the quotient $\pi_1^\Sigma(\mathbb{X}_{S/\mathbb{F}_q}, \mathbf{0}_{\overline{x}}) = \pi_1^{\{p\}}(\mathbb{X}_{S/\mathbb{F}_q}, \mathbf{0}_{\overline{x}})/i(\mathcal{T}_\Sigma^{(p)}(\mathbb{X}_{\overline{x}}))$, and we get a split short exact sequence:

$$0 \to \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}}) \to \pi_1^\Sigma(\mathbb{X}_{S/\mathbb{F}_q}, \mathbf{0}_{\overline{x}}) \to \pi_1(U_{S/\mathbb{F}_q}, \overline{x}) \to 1. \tag{2.1}$$

By this exact sequence, $\pi_1(U_{S/\mathbb{F}_q}, \overline{x})$ acts by conjugation on $\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}})$. Recall that we have chosen S sufficiently small so that $V \twoheadrightarrow V_S$ is étale. We have a canonical surjection $\pi_1(U_{K/\mathbb{F}_q}, \overline{x}) \twoheadrightarrow \mathrm{Gal}(U/U_S)$. We write $S_V = \mathrm{Gal}(U/U_S)$, which is an extension of $\overline{S}_V$ by $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ generated by the Frobenius automorphism over $\mathbb{F}_q$. Since $\mathbb{X}_{\overline{x}}[N]$ for all integers N outside Σ gets trivialized over

U, the action of $\pi_1(U_{S/\mathbb{F}_q}, \overline{x})$ on $\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}})$ factors through $\pi_1(U_{S/\mathbb{F}_q}, \overline{x}) \twoheadrightarrow S_V$.

We now have another split exact sequence:

$$0 \to \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) \to \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}_q}, \mathbf{0}_{\sigma(\overline{x})}) \to \pi_1(U_{{}^\sigma S/\mathbb{F}_q}, \sigma(\overline{x})) \to 1. \tag{2.2}$$

Again the action of $\pi_1(U_{{}^\sigma S/\mathbb{F}_q}, \sigma(\overline{x}))$ on $\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})})$ factors through $\mathrm{Gal}(U/U_{{}^\sigma S}) = {}^\sigma S_V$. We fix a path in $U_{{}^\sigma S}$ from $\sigma(\overline{x})$ to $\overline{x}$ and lift it to a path from $\sigma(\mathbf{0}_{\overline{x}})$ to $\mathbf{0}_{\overline{x}}$ in $\mathbb{X}_{{}^\sigma S}$, which induces canonical isomorphisms ([SGA] V.7):

$$\iota^\sigma : \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) \cong \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\overline{x}}) \text{ and } \iota_\sigma : \pi_1(U_{{}^\sigma S}, \mathbf{0}_{\sigma(\overline{x})}) \cong \pi_1(U_{{}^\sigma S}, \overline{x}).$$

The isomorphism ι^σ in turn induces an isomorphism $\iota : \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) \to \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}})$ of ${}^\sigma S_1$–modules.

We want to have the following commutative diagram

$$\begin{array}{ccccc}
\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}}) & \xrightarrow{\hookrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{S/\mathbb{F}}, \mathbf{0}_{\overline{x}}) & \xrightarrow{\twoheadrightarrow} & \pi_1(U_{S/\mathbb{F}}, \overline{x}) \\
{\scriptstyle ?}\downarrow & & \downarrow{\scriptstyle ?} & & {\scriptstyle \sigma_*}\downarrow \\
\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) & \xrightarrow{\hookrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) & \xrightarrow{\twoheadrightarrow} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \sigma(\overline{x})) \\
{\scriptstyle \iota}\downarrow & & {\scriptstyle \iota^\sigma}\downarrow & & \downarrow{\scriptstyle \iota_\sigma} \\
\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}}) & \xrightarrow[\hookrightarrow]{} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\overline{x}}) & \xrightarrow[\twoheadrightarrow]{} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \overline{x}),
\end{array}$$

and we will find homomorphisms of topological groups fitting into the spot indicated by "?". In other words, we ask if we can find a linear endomorphism $\mathcal{L} \in \mathrm{End}_{\mathbb{A}^{(\Sigma)}}(\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}}) \otimes \mathbb{Q})$ such that $\mathcal{L}(s \cdot v) = {}^\sigma s \cdot \mathcal{L}(v)$ for all $s \in S_1$ and $v \in \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}})$, where ${}^\sigma s = \sigma s \sigma^{-1}$ is the image of $\iota_\sigma(\sigma_*(s))$ in ${}^\sigma S_1$ for any lift $s \in \pi_1(V_S, \overline{x})$ inducing $s \in S_1$. Since $\mathrm{Hom}(G_1(\mathbb{Z}_\ell), G_1(\mathbb{Z}_{\ell'}))$ is a singleton made of the zero-map (taking the entire $G_1(\mathbb{Z}_\ell)$ to the identity of $G_1(\mathbb{Z}_{\ell'})$) if two primes ℓ and ℓ' are large and distinct (see Section 3 (S3) for a proof of this fact), $s \mapsto {}^\sigma s$ sends $S_{1,\ell}$ into ${}^\sigma S_{1,\ell}$ for almost all primes ℓ, where $S_{1,\ell} = G_1(\mathbb{Q}_\ell) \cap S_\ell$. If we shrink S further if necessary for exceptional finitely many primes, we achieve that S_ℓ is ℓ–profinite for exceptional ℓ and the logarithm $\log_\ell : S_{1,\ell} \to Lie(S_{1,\ell})$ given by $\log_\ell(s) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{(s-1)^n}{n}$ is an ℓ-adically continuous isomorphism. Then by a result of Lazard [GAN] IV.3.2.6 (see Section 3 (S1)), σ induces by $\log_\ell \circ \sigma = [\sigma]_\ell \circ \log_\ell$ an automorphism $[\sigma]_\ell$ of the Lie algebra $Lie(S_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ over $\mathbb{Q}_\ell$. Note that

$$Lie(S_{1,\ell}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \left\{ x \in C_\ell \middle| \rho(x) = -x \text{ and } \mathrm{Tr}(x) = 0 \right\},$$

where $\mathrm{Tr} : C_\ell \to M_\ell$ is the reduced trace map. Extending scalar to a finite Galois extension of $K/\mathbb{Q}_\ell$, $Lie(S_\ell) \otimes_{\mathbb{Z}_\ell} K$ becomes split semi-simple over K, and therefore $[\sigma]_\ell$ is induced by an element of $P\widetilde{G}(K)$ (the Lie algebra version of (S2) in the following section), which implies by Galois descent that $[\sigma]_\ell$ is induced by an element of $P\widetilde{G}(\mathbb{Q}_\ell)$. Thus for all $\ell \notin \Sigma$, $s \mapsto {}^\sigma s$ sends $S_{1,\ell}$ into ${}^\sigma S_{1,\ell}$ and that the isomorphism: $s \mapsto {}^\sigma s$ is induced by an element $\overline{\mathcal{L}}$ of the group fitting into the middle term of the exact sequence (1.3):

$$1 \to PG(\mathbb{A}^{(\Sigma)}) \to P\widetilde{G}(\mathbb{A}^{(\Sigma)}) \to \mathrm{Aut}(M_{\mathbb{A}}^{(\Sigma)}/\mathbb{A}^{(\Sigma)}).$$

The element $\overline{\mathcal{L}}$ in $\mathrm{Aut}(G_1(\mathbb{A}^{(\Sigma)}))$ is in turn induced by an endomorphism $\mathcal{L} \in \mathrm{End}_{\mathbb{A}^{(\Sigma)}}(\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}}) \otimes \mathbb{Q})$. Define $g(\sigma) = \iota^{-1} \circ \mathcal{L}$. Then $g(\sigma)$ is an element of $\mathrm{Hom}_{\overline{S}_1}(\mathcal{T}^{(\Sigma)}\mathbb{X}_x, \mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(x)})$ invertible in $\mathrm{Hom}_{\overline{S}_1}(\mathcal{T}^{(\Sigma)}\mathbb{X}_x, \mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(x)}) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $g(\sigma)$ is S_1–linear in the sense that $g(\sigma)(sx) = {}^\sigma s \cdot g(\sigma)(x)$ for all $s \in \overline{S}_1$. Though $\mathcal{L}$ may depends on the choice of the path from x to $\sigma(x)$, the isomorphism $g(\sigma)$ (modulo the centralizer of S_1) is independent of the choice of the path; so, we will forget about the path hereafter. Applying this argument to $\Sigma = \{p, \infty\}$, we have the following commutative diagram

$$\begin{array}{ccc} \mathcal{T}^{(p)}(\mathbb{X}_x) \otimes_{\mathbb{Z}} \mathbb{A}^{(p)} & \xrightarrow{g(\sigma)} & \mathcal{T}^{(p)}(\mathbb{X}_{\sigma(x)}) \otimes_{\mathbb{Z}} \mathbb{A}^{(p)} \\ \wr\uparrow \phi_x^{(p)} & & \wr\uparrow \phi_{\sigma(x)}^{(p)} \\ L \otimes_{\mathbb{Z}} \mathbb{A}^{(p)} & \xrightarrow[g_\sigma]{} & L \otimes_{\mathbb{Z}} \mathbb{A}^{(p)} \end{array} \tag{2.3}$$

for $g_\sigma \in \widetilde{G}(\mathbb{A}^{(p)})$. Thus $g_\sigma^{(\Sigma)}$ has the projection $\pi(g_\sigma^{(\Sigma)}) \in \mathrm{Out}_{\mathbb{A}^{(\Sigma)}\text{-alg}}(B_{\mathbb{A}}^{(\Sigma)}, \rho)$.

Consider the relative Frobenius map $\pi_S : U_S \to U_S$ over $\mathbb{F}_q$. Since $\sigma : U_S \cong U_{{}^\sigma S}$ is defined over $\mathbb{F}_q$ by our choice, σ satisfies $\sigma_S \circ \pi_S = \pi_{{}^\sigma S} \circ \sigma_S$. If $X \to U_S$ is an étale irreducible covering, $X \times_{U_S, \pi_S} U_S \to U_S$ is étale irreducible, and $\pi_S : U_S \to U_S$ induces an endomorphism $\pi_{S,*} : \pi_1(U_S, \overline{x}) \to \pi_1(U_S, \overline{x})$. We have a diagram:

$$\begin{array}{ccccc} \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) & \xrightarrow{\hookrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) & \xrightarrow{\twoheadrightarrow} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \sigma(\overline{x})) \\ g(\sigma)^{-1}\downarrow & & \downarrow g(\sigma)^{-1} \ltimes \sigma_{S,*}^{-1} & & \downarrow \sigma_{S,*}^{-1} \\ \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}}) & \xrightarrow{\hookrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{S/\mathbb{F}}, \mathbf{0}_{\overline{x}}) & \xrightarrow{\twoheadrightarrow} & \pi_1(U_{S/\mathbb{F}}, \overline{x}) \\ \pi_x\downarrow & & \downarrow \pi_x \ltimes \pi_{S,*} & & \downarrow \pi_{S,*} \\ \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\overline{x}}) & \xrightarrow{\hookrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{S/\mathbb{F}}, \mathbf{0}_{\overline{x}}) & \xrightarrow{\twoheadrightarrow} & \pi_1(U_{S/\mathbb{F}}, \overline{x}) \\ g(\sigma)\downarrow & & \downarrow g(\sigma) \ltimes \sigma_{S,*} & & \downarrow \sigma_{S,*} \\ \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) & \xrightarrow[\hookrightarrow]{} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) & \xrightarrow[\twoheadrightarrow]{} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \sigma(\overline{x})), \end{array}$$

where π_x is the relative Frobenius endomorphism of $\mathbb{X}_x$ over $\mathbb{F}_q$. The middle horizontal three squares of the above diagram are commutative, because $(\pi_x \ltimes$

$\pi_{S,*}$) is induced by the relative Frobenius endomorphism of $\mathbb{X}_{S/\mathbb{F}_q}$. The top and the bottom three squares are commutative by construction; so, the entire diagram is commutative. In short, we have the following commutative diagram:

$$\begin{array}{ccccc} \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) & \xrightarrow{\hookrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) & \xrightarrow{\twoheadrightarrow} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \sigma(\overline{x})) \\ {\scriptstyle g(\sigma)\pi_x g(\sigma)^{-1}}\downarrow & & \downarrow & & {\scriptstyle \pi_{{}^\sigma S,*}}\downarrow \\ \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) & \underset{\hookrightarrow}{\longrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) & \underset{\twoheadrightarrow}{\longrightarrow} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \sigma(\overline{x})), \end{array}$$

because $\sigma_S \pi_S \sigma_S^{-1} = \pi_{{}^\sigma S}$. Since $\pi_{\sigma(x)}$ also gives a similar commutative diagram:

$$\begin{array}{ccccc} \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) & \xrightarrow{\hookrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) & \xrightarrow{\twoheadrightarrow} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \sigma(\overline{x})) \\ {\scriptstyle \pi_{\sigma(x)}}\downarrow & & \downarrow & & \downarrow{\scriptstyle \pi_{{}^\sigma S,*}} \\ \mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}) & \underset{\hookrightarrow}{\longrightarrow} & \pi_1^{\Sigma}(\mathbb{X}_{{}^\sigma S/\mathbb{F}}, \mathbf{0}_{\sigma(\overline{x})}) & \underset{\twoheadrightarrow}{\longrightarrow} & \pi_1(U_{{}^\sigma S/\mathbb{F}}, \sigma(\overline{x})), \end{array}$$

we find out that $g(\sigma)\pi_x g(\sigma)^{-1}\pi_{\sigma(x)}^{-1}$ commutes with the action of ${}^\sigma\overline{S}_1$, and hence it is in the center of $\mathrm{Aut}_R(\mathcal{T}^{(\Sigma)}(\mathbb{X}_{\sigma(\overline{x})}))$. In other words, $g(\sigma)\pi_x g(\sigma)^{-1} = z\pi_{\sigma(x)}$ for $z \in (\widehat{R}^{(\Sigma)})^\times$. Taking the determinant with respect to $\bigwedge^g \mathcal{T}_\ell(\mathbb{X}_{\sigma(\overline{x})})$ for the rank $g = \mathrm{rank}_{R_\ell} \mathcal{T}_\ell(\mathbb{X}_{\sigma(\overline{x})})$ with a prime $\ell \notin \Sigma$, we find that $\det(\pi_x) = z^g \det(\pi_{\sigma(x)})$. Since $\det(\pi_x) = N(\pi_x)^r$ with a positive integer r for the reduced norm map $N : B \to M$, we find that $\det(\pi_x) = \det(\pi_{\sigma(x)})$, and hence z is a g–th root of unity in $(\widehat{R}^{(\Sigma)})^\times$ (purity of the Weil number π_x). Then $g(\sigma) \in \mathrm{Hom}(\mathcal{T}^{(p)}\mathbb{X}_x, \mathcal{T}^{(p)}\mathbb{X}_{\sigma(x)})$ satisfies $g(\sigma) \circ \pi_x^g = \pi_{\sigma(x)}^g \circ g(\sigma)$, and hence $g(\sigma)$ is an isogeny of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_{q^g})$–modules. Then by a result of Tate ([T]),

$$\mathrm{Hom}_{\mathrm{Gal}(\mathbb{F}/\mathbb{F}_{q^g})}(\mathcal{T}^{(\Sigma)}\mathbb{X}_x, \mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(x)}) = \mathrm{Hom}(\mathbb{X}_{x/\mathbb{F}_{q^g}}, \mathbb{X}_{\sigma(x)/\mathbb{F}_{q^g}}) \otimes_{\mathbb{Z}} \mathbb{A}^{(\Sigma)},$$

we find that $\mathbb{X}_x$ and $\mathbb{X}_{\sigma(x)}$ are isogenous over $\mathbb{F}_{q^g}$. □

We have a canonical projection $\mathrm{Aut}_{\text{top group}}(\overline{G}_1(\mathbb{A}^{(\Sigma)})) \to \mathrm{Out}_{\mathbb{A}^{(\Sigma)}\text{-alg}}(B_{\mathbb{A}}^{(\Sigma)}, \rho)$ (induced by π) whose kernel is given by $PG(\mathbb{A}^{(\Sigma)})$. Thus $\sigma \in \mathrm{Aut}(\mathbb{F}(V)_{/\mathbb{F}})$ has projection $\pi(g_\sigma^{(\Sigma)})$ (for g_σ in (2.3)) in

$$\mathrm{Out}_{\mathbb{A}^{(\Sigma)}\text{-alg}}(B_{\mathbb{A}}^{(\Sigma)}, \rho) \subset \mathrm{Aut}_{\mathbb{A}^{(\Sigma)}\text{-alg}}(M_{\mathbb{A}}^{(\Sigma)}) = \prod_{\ell \notin \Sigma} \mathrm{Aut}_{\mathbb{Q}_\ell\text{-alg}}(M_\ell)$$

which will be written as $\sigma_B = \pi(g_\sigma^{(\Sigma)})$.

Corollary 2.2. *If $\sigma \in \mathrm{Aut}(\mathbb{F}(V)/\mathbb{F})$, we have $\sigma_B \in \mathrm{Out}_{\mathbb{Q}\text{-}alg}(B, \rho)$, where the group $\mathrm{Out}_{\mathbb{Q}\text{-}alg}(B, \rho)$ is diagonally embedded into $\prod_{\ell \notin \Sigma} \mathrm{Aut}_{\mathbb{Q}_\ell\text{-}alg}(M_\ell)$.*

Proof. The element $g(\sigma) = \iota^{-1} \circ \mathcal{L} \in \mathrm{Hom}_S(\mathcal{T}^{(\Sigma)}\mathbb{X}_x, \mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(x)})$ in the proof of Proposition 2.1 acts on $G_1(\mathbb{A}^{(\Sigma)})$ by conjugation of $g_\sigma \in \widetilde{G}(\mathbb{A}^{(\Sigma)})$ in (2.3); so, its projection $\pi(g_\sigma)$ in $\mathrm{Out}_{\mathbb{A}^{(\Sigma)}\text{-alg}}(B^{(\Sigma)}_{\mathbb{A}}, \rho)$ inside $\mathrm{Aut}(M^{(\Sigma)}_{\mathbb{A}}/\mathbb{A}^{(\Sigma)})$ is given by σ_B. By the proof of Proposition 2.1, $g(\sigma)$ is induced by $\xi \in \mathrm{Hom}_{O_B}(\mathbb{X}_x, \mathbb{X}_{\sigma(x)})$ modulo $Z(\mathbb{Z}_{(\Sigma)})S$. Choose a rational prime q outside Σ. We have $B_q \cap \mathrm{End}(\mathbb{X}_x) = O_B$. Note that $b \mapsto g(\sigma)^{-1} \circ b \circ g(\sigma)$ sends B_q into itself and that the conjugation by ξ sends $B_q \cap (\mathrm{End}(\mathbb{X}_x) \otimes_{\mathbb{Z}} \mathbb{Q}) = B$ into itself. Since the image of the conjugation by $g(\sigma)$ in $\mathrm{Out}_{\mathbb{Q}_q\text{-alg}}(B_q)$ and the image of the conjugation by ξ in $\mathrm{Out}(\mathrm{End}(\mathbb{X}_x) \otimes_{\mathbb{Z}} \mathbb{Q})$ coincide, we conclude $\sigma_B \in \mathrm{Out}_{\mathbb{Q}\text{-alg}}(B)$. Since $\sigma_B \in \mathrm{Out}_{\mathbb{A}^{(\Sigma)}\text{-alg}}(B^{(\Sigma)}_{\mathbb{A}}, \rho) \cap \mathrm{Out}_{\mathbb{Q}\text{-alg}}(B)$, we get $\sigma_B \in \mathrm{Out}_{\mathbb{Q}\text{-alg}}(B, \rho)$. □

Corollary 2.3. *For the generic point η of V_S, $\mathbb{X}_\eta$ and $\mathbb{X}_{\sigma(\eta)}$ are isogenous. In particular, if σ_B is the identity in $\mathrm{Out}_{\mathbb{Q}\text{-}alg}(B, \rho)$, we find $a_S \in G(\mathbb{A}^{(\Sigma)})$ inducing σ on $\mathbb{F}(V_S)$ for all sufficiently small open compact subgroups S of $G(\mathbb{A}^{(\Sigma)})$.*

Proof. We choose S sufficiently small as in the proof of Proposition 2.1. We replace q in the proof of Proposition 2.1 by q^g at the end of the proof in order to simplify the symbols.

Suppose that σ_S induces $U_S \cong U_{\sigma S}$ for an open dense subscheme $U_S \subset V_S$. Again we use the exact sequence:$0 \to \mathcal{T}^{(\Sigma)}\mathbb{X}_{\overline{\eta}} \to \pi_1^{\Sigma}(\mathbb{X}_{/\mathbb{F}_q}, \mathbf{0}_{\overline{\eta}}) \to \pi_1(U_{S/\mathbb{F}_q}, \overline{\eta}) \to 1$. By the same argument as above, we find $g_\eta(\sigma) \in \mathrm{Hom}_{\pi_1(U_{S/\mathbb{F}}, \overline{\eta})}(\mathcal{T}^{(\Sigma)}\mathbb{X}_\eta, \mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(\eta)})$. Since $\mathbb{X}_\eta[\ell^\infty]$ gets trivialized over U for a prime $\ell \notin \Sigma$, fixing a path from η to x for a closed point $x \in U_S(\mathbb{F}_q)$ and taking its image from $\sigma(\eta)$ to $\sigma(x)$, we may identify $\pi(U_{S/\mathbb{F}_q}, \overline{x})$ (resp. $\mathcal{T}^{(\Sigma)}\mathbb{X}_x$ and $\mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(x)}$) with the Galois group $\mathrm{Gal}(\mathbb{F}(\widetilde{U})/\mathbb{F}_q(U_S))$ for the universal covering $\widetilde{U}$ (resp. with the generic Tate modules $\mathcal{T}^{(\Sigma)}\mathbb{X}_\eta$ and $\mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(\eta)}$). By the universality, $\sigma : U \cong {}^\sigma U$ extends to $\widetilde{\sigma} : \widetilde{U} \cong {}^\sigma\widetilde{U}$. Writing D_x for the decomposition group of the closed point $x \in U_S(\mathbb{F}_q)$, the points $x : Spec(\mathbb{F}_q) \hookrightarrow U_S$ and $\sigma(x) : Spec(\mathbb{F}_q) \hookrightarrow U_{\sigma S}$ induce isomorphisms $D_x \cong \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q) \cong D_{\sigma(x)} = \widetilde{\sigma} D_x \widetilde{\sigma}^{-1}$ (choosing the extension $\widetilde{\sigma}$ suitably) and splittings: $\mathrm{Gal}(\mathbb{F}(\widetilde{U})/\mathbb{F}_q(U_S)) = D_x \ltimes \mathrm{Gal}(\mathbb{F}(\widetilde{U})/\mathbb{F}(U_S))$ and $\mathrm{Gal}(\mathbb{F}({}^\sigma\widetilde{U})/\mathbb{F}_q(U_{\sigma S})) = D_{\sigma(x)} \ltimes \mathrm{Gal}(\mathbb{F}({}^\sigma\widetilde{U})/\mathbb{F}(U_{\sigma S}))$. The morphism $g(\sigma) : \mathcal{T}^{(\Sigma)}\mathbb{X}_x \to \mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(x)}$ induces a morphism $g_\eta(\sigma) : \mathcal{T}^{(\Sigma)}\mathbb{X}_\eta \to \mathcal{T}^{(\Sigma)}\mathbb{X}_{\sigma(\eta)}$ satisfying $g_\eta(\sigma)(sx) = {}^\sigma s \cdot g_\eta(\sigma)(x)$ for all $s \in S_V$. Thus $g_\eta(\sigma)$ is a morphism of $\pi_1(U_{S/\mathbb{F}_q}, \overline{\eta})$–modules (not just that of $\pi_1^{\Sigma}(U_{S/\mathbb{F}}, \overline{\eta})$–modules). Then by a result of Zarhin (see [RPT] Chapter VI, [Z] and also [ARG] Chapter II), $\mathbb{X}_{\eta/\mathbb{F}_q(V_S)}$ and $\mathbb{X}_{\sigma(\eta)/\mathbb{F}_q(V_{\sigma S})}$ are isogenous. Here we note that the field $\mathbb{F}_q(V_S) = \mathbb{F}_q(U_S)$ is finitely generated over $\mathbb{F}_p$ (which has to be the case in order to apply Zarhin's result). Thus we can find an isogeny $\alpha_\eta : \mathbb{X}_\eta \to \mathbb{X}_{\sigma(\eta)}$, which extends to an isogeny $\mathbb{X}_S \to \sigma^*\mathbb{X}_{\sigma S} = \mathbb{X}_{\sigma S} \times_{U_{\sigma S}, \sigma} U_S$ over U_S. We write $\alpha : \mathbb{X}_S \to \mathbb{X}_{\sigma S}$ for the composite of the above isogeny with the projection $\mathbb{X}_{\sigma S} \times_{U_{\sigma S}, \sigma} U_S \to \mathbb{X}_{\sigma S}$.

We then have the commutative diagram:

$$\begin{array}{ccc} \mathbb{X}_S & \xrightarrow{\alpha} & \mathbb{X}_{^\sigma S} \\ \downarrow & & \downarrow \\ U_S & \xrightarrow[\sigma]{} & U_{^\sigma S}. \end{array}$$

Assume that $\sigma_B = 1$. Then α is B-linear. Suppose we have another B-linear isogeny $\alpha' : \mathbb{X}_S \to \sigma^*\mathbb{X}_{^\sigma S}$ inducing $g_\eta(\sigma)$. Then $\alpha^{-1}\alpha'$ commutes with the action of $\mathrm{Gal}(\mathbb{F}(\widetilde{U})/\mathbb{F}(U_S))$ and hence with the action of S. Thus we find $\xi = \phi^{-1}\alpha^{-1}\alpha'\phi \in \mathrm{End}_S(L_{\mathbb{A}^{(\Sigma)}})$ for the level structure $\phi = \phi^{(\Sigma)} : L_{\mathbb{A}^{(\Sigma)}} \to V^{(\Sigma)}(\mathbb{X}_\eta)$. This implies B-linear ξ commutes with the action of C, and hence in the center of $B \subset \mathrm{End}_C(L_{\mathbb{Q}})$. We thus find $\xi \in Z(\mathbb{Q})G(\mathbb{Z}_\Sigma^{(p)})S$. We consider the commutative diagram similar to (2.3):

$$\begin{array}{ccc} \mathcal{T}^{(p)}(\mathbb{X}_\eta) \otimes_{\mathbb{Z}} \mathbb{A}^{(p)} & \xrightarrow{\alpha_\eta} & \mathcal{T}^{(p)}(\mathbb{X}_{\sigma(\eta)}) \otimes_{\mathbb{Z}} \mathbb{A}^{(p)} \\ \wr\uparrow \phi_\eta^{(p)} & & \wr\uparrow \phi_{\sigma(\eta)}^{(p)} \\ L \otimes_{\mathbb{Z}} \mathbb{A}^{(p)} & \xrightarrow[g_\sigma]{} & L \otimes_{\mathbb{Z}} \mathbb{A}^{(p)}. \end{array} \tag{2.4}$$

The prime-to-Σ component of g_σ^{-1} eventually gives a_S in the corollary. By the above fact, $g_\sigma^{(\Sigma)}$ is uniquely determined in $\widetilde{G}(\mathbb{A}^{(\Sigma)})/Z(\mathbb{Q})S$.

Note that $\sigma^*(\mathbb{X}_{^\sigma S}, \overline{\lambda}_{^\sigma S}, i_{^\sigma S}, \phi_{\sigma(\eta)}^{(p)} \circ g_\sigma^{(\Sigma)})_{/U_S}$ is a quadruple classified by $Sh_{/S}^{(\Sigma)} = Sh^{(p)}/G(\mathbb{Z}_\Sigma^{(p)})S$. By the universality of $Sh_{/S}^{(\Sigma)}$ (proven under (h2-4)), we have a morphism $\tau : U_S \to U_S \subset Sh^{(\Sigma)}/S$ with a prime-to-Σ and B-linear isogeny $\beta : \sigma^*\mathbb{X}_{^\sigma S} \to \tau^*\mathbb{X}_S$ over U_S. Identifying $\mathrm{Gal}(U/U_S)$ with a subgroup S_V of $S \subset G(\mathbb{A}^{(\Sigma)})$, the actions of $s \in S_V$ on $\phi_1 = \phi_{\sigma(\eta)}^{(\Sigma)} \circ g_\sigma$ and on $\phi_2 = \phi_\eta^{(\Sigma)}$ have identical effect: $s \circ \phi_j = \phi_j \circ s$ $(j = 1, 2)$. Thus the effect of τ (and $\beta\alpha_\eta$) on $\mathcal{T}^{(\Sigma)}(\mathbb{X}_\eta)$ commutes with the action of S_V, and the action of B-linear $\beta\alpha_\eta$ on the Tate module $\mathcal{T}^{(\Sigma)}(\mathbb{X}_\eta)$ commutes with the action of S_V. Therefore it is in the center $Z(\mathbb{Q})$. Thus the isogeny α between $\sigma^*(\mathbb{X}_{^\sigma S})$ and $\mathbb{X}_S$ can be chosen (after modification by a central element) to be a prime-to-Σ isogeny. This τ could be non-trivial without the three assumptions (h2-4), and if this is the case, the action of τ is induced by an element of $G(\mathbb{Q}_\Sigma^{(p)})$ normalizing $G(\mathbb{Z}_\Sigma^{(p)})$. Under (h2-4), τ is determined by its effect on $\mathcal{T}^{(\Sigma)}(\mathbb{X}_\eta)$ and is the identity map (see the following two paragraphs), and we may assume that α is a prime-to-Σ isogeny (after modifying by an element of $Z(\mathbb{Q})$). Thus $g_\sigma^{(\Sigma)}$ is uniquely determined in $\mathcal{G}_V$ modulo S.

We add here a few words on this point related to the universality of $Sh^{(\Sigma)}$. Without the assumptions (h2-4), the effect of σ on the restriction of each level structure $\phi^{(p)}$ to $L_{\mathbb{A}^{(\Sigma)}}$ may not be sufficient to uniquely determine σ. In other words, in the definition of our moduli problem, we indeed have the datum of $\phi^{(p)}_{\Sigma}$ modulo $G(\mathbb{Z}^{(p)}_{\Sigma})$, which we cannot forget. To clarify this, take a (characteristic 0) geometrically connected component V_0 of $Sh_{/E}$ whose image $V_0^{(\Sigma)}$ in $Sh^{(\Sigma)}_{/E} = Sh/G(\mathbb{Z}_\Sigma)$ giving rise to $V_{/\mathbb{F}}$ after extending scalar to $\mathcal{W}$ and then taking reduction modulo p. By the description of $\pi_0(Sh_{/\overline{\mathbb{Q}}})$ at the beginning of the proof of Proposition 2.1, the stabilizer in $G(\mathbb{A}^{(\infty)})/\overline{Z(\mathbb{Q})}$ of $V_{0/\overline{\mathbb{Q}}} \in \pi_0(Sh_{/\overline{\mathbb{Q}}})$ is given by

$$\mathcal{G}_0 = \frac{\left\{g \in G(\mathbb{A}^{(\infty)}) \middle| \mu(g) \in \overline{Z^G(\mathbb{Q})^+}\right\}}{\overline{Z(\mathbb{Q})}}.$$

Inside this group, every element $g \in G(\mathbb{A}^{(\infty)})$ inducing an automorphism of $V_0^{(\Sigma)}$ has its ℓ-component g_ℓ for a prime $\ell \in \Sigma$ in the normalizer of $G(\mathbb{Z}_\ell)$. Under (h2-4), as is well known, the normalizer of $G(\mathbb{Z}_\ell)$ in $G(\mathbb{Q}_\ell)$ is $Z(\mathbb{Q}_\ell)G(\mathbb{Z}_\ell)$ (see [Ko] Lemma 7.2, which is one of the key points of the proof of the universality of $Sh^{(\Sigma)}$). By (h2-4), $G(\mathbb{Q}_\ell)$ is quasi-split over $\mathbb{Q}_\ell$, and we have the Iwasawa decomposition $G(\mathbb{Q}_\ell) = P_0(\mathbb{Q}_\ell)G(\mathbb{Z}_\ell)$ for $\ell \in \Sigma$ with a minimal parabolic subgroup P_0 of G, from which we can easily prove that the normalizer of $G(\mathbb{Z}_\ell)$ is $Z(\mathbb{Q}_\ell)G(\mathbb{Z}_\ell)$. An elementary proof of the Iwasawa decomposition (for a unitary group or a symplectic group acting on M_ℓ^r keeping a skew-hermitian form relative to M_ℓ/F_ℓ) can be found in [EPE] Section 5, particularly pages 36-37. By (h3-4), $G(\mathbb{Q}_\ell)$ is isomorphic to a unitary or symplectic group acting on $M_\ell^n = \varepsilon L_{\mathbb{Q}_\ell}$ for an idempotent ε (for example, $\varepsilon = \mathrm{diag}[1, 0, \dots, 0]$ fixed by ρ) of $O_{B_\ell} \cong M_n(R_\ell)$ with respect to the skew-hermitian form on $\varepsilon L_{\mathbb{Q}_\ell}$ induced by $\langle \cdot, \cdot \rangle$; so, the result in [EPE] Section 5 applies to our case.

Suppose that $g \in G(\mathbb{A}^{(\infty)})$ preserves the quotient $V_0^{(\Sigma)}$ of V_0. If Σ is finite, we can therefore choose $\xi \in Z(\mathbb{Q})$ so that $(\xi g)_\ell$ is in $G(\mathbb{Z}_\ell)$ for all $\ell \in \Sigma$, and the action of $(\xi g)^{(\Sigma)} \in \mathcal{G}_V$ on $V_0^{(\Sigma)}$ induces the action of g. Suppose that Σ is infinite. Since α_η is a prime-to-Σ isogeny, $(g_\sigma)_\Sigma$ is contained in $G(\mathbb{Z}^{(p)}_\Sigma)$. Thus σ is induced by $(g_\sigma^{(\Sigma)})^{-1}$ even if Σ is infinite. This fact can be also shown in a group theoretic way as in the case of finite Σ: Modifying g by an element in $G(\mathbb{Z}_\Sigma)$, we may assume that $g_\ell \in Z(\mathbb{Q}_\ell)$ for all $\ell \in \Sigma$. Taking an increasing sequence of finite sets Σ_i so that $\Sigma = \bigcup_i \Sigma_i$ and choosing $\xi_i \in Z(\mathbb{Q})$ so that the action of $(\xi_i g)^{(\Sigma_i)}$ induces the action of g on $V_0^{(\Sigma_i)}$, we find $\xi_i g \in G(\mathbb{Z}_{\Sigma_i})G(\mathbb{A}^{(\Sigma_i)})$ whose action on $V_0^{(\Sigma)}$ is identical to that of g. We write $\mathcal{F}_i$ for the closed subset of elements in $G(\mathbb{Z}_{\Sigma_i})G(\mathbb{A}^{(\Sigma_i)})$ whose action on $V_0^{(\Sigma)}$ is identical to that of g. In the locally compact group $G(\mathbb{A}^{(\infty)})$, the filter $\{\mathcal{F}_i\}_i$ has a nontrivial intersection $\bigcap_i \mathcal{F}_i \neq \emptyset$. Thus the action of g on $V_0^{(\Sigma)}$ is represented by an element in $G(\mathbb{A}^{(\Sigma)})$. In other words, an element of $G(\mathbb{A}^{(\infty)})$ in the stabilizer of the connected component $V_0^{(\Sigma)} \in \pi_0(Sh^{(\Sigma)}_{/\overline{\mathbb{Q}}})$ is represented by an element in the group $G(\mathbb{A}^{(\Sigma)})$ without Σ-component. Since $\pi_0(Sh^{(\Sigma)}_{/\overline{\mathbb{Q}}})$ is in bijection with $\pi_0(Sh^{(\Sigma)}_{/\mathbb{F}})$, any element in the stabilizer in $\widetilde{G}(\mathbb{A}^{(p)})$ of $V \in \pi_0(Sh^{(\Sigma)}_{/\mathbb{F}})$ is represented by an element in $G(\mathbb{A}^{(\Sigma)})$. By this fact, under (h2-4), the effect of σ on $\phi^{(p)}_{\Sigma}$ is determined by $g^{(\Sigma)}_{\sigma}$ outside Σ. Thus we can really forget about the Σ-component.

Writing the prime-to-Σ level structures of $\mathbb{X}_\eta$ and $\mathbb{X}_{\sigma(\eta)}$ as $\phi^{(\Sigma)}_\eta$ and $\phi^{(\Sigma)}_{\sigma(\eta)}$, respectively, we now find that $\alpha_\eta \circ \phi^{(\Sigma)}_\eta = \phi^{(\Sigma)}_{\sigma(\eta)} \circ a_S^{-1}$ for $a_S^{-1} = g^{(\Sigma)}_\sigma \in \widetilde{G}(\mathbb{A}^{(\Sigma)})$. Since the effect of σ on $\mathcal{T}^{(\Sigma)}(\mathbb{X}_\eta)$ determines σ, we have $a_S^{-1}(\sigma(\eta)) = \eta$, which implies that $a_S = \sigma$ on the Zariski open dense subset U_S of V_S, and hence, they are equal on the entire V_S. □

By the smoothness of $Sh^{(\Sigma)}$ over $\mathcal{W}$, Zariski's connectedness theorem (combined with the existence of a projective compactification normal over $\mathcal{W}$), we have a bijection $\pi_0(Sh^{(\Sigma)}_{/\mathbb{F}}) \cong \pi_0(Sh^{(\Sigma)}_{/\overline{\mathbb{Q}}})$ as described at the beginning of the proof of Proposition 2.1. Since our group G has cohomologically trivial center (cf., [MS] 4.12), the stabilizer of $V^{(\Sigma)}_0 \in \pi_0(Sh^{(\Sigma)}_{/\overline{\mathbb{Q}}})$ in $\frac{G(\mathbb{A}^{(\Sigma)})}{Z(\mathbb{Z}_{(\Sigma)})}$ has a simple expression given by the subgroup $\mathcal{G}_V$ in the theorem (see [D1] 2.1.6, 2.1.16, 2.6.3 and [MS] Theorem 4.13), and the above corollaries finish the proof of the theorem because σ on V is then induced by $a = \lim_{S\to 1} a_S$ in $\frac{G(\mathbb{A}^{(\Sigma)})}{Z(\mathbb{Z}_{(\Sigma)})}$. Since a fixes $V \in \pi_0(Sh^{(\Sigma)}_{/\mathbb{F}})$, we conclude $a \in \mathcal{G}_V$. The description of the stabilizer of V in the theorem necessitates the strong approximation theorem (which follows from noncompactness of $G_1(\mathbb{R})$ combined with simply connectedness of G_1: [Kn]).

3 Automorphism groups of quasi-split classical groups

In the above proof of the theorem, we have used the following facts:

(S) *For an open compact subgroups $S, S' \subset G_1(\mathbb{A}^{(\Sigma)})$, if $\sigma : S \cong S'$ is an isomorphism of groups, replacing S by an open subgroup and replacing S' accordingly by the image of σ, σ is induced by the conjugation by an element $g(\sigma) \in \widetilde{G}(\mathbb{A}^{(\Sigma)})$ as in* (1.2).

We may modify σ by $g \in \widetilde{G}(\mathbb{A}^{(\Sigma)})$ so that $\sigma_B = 1$. Then this assertion (S) follows from the following three assertions for σ with $\sigma_B = 1$:

(S1) *For open subgroups S_ℓ and ${S'}_\ell$ of $G_1(\mathbb{Q}_\ell)$ (for every prime ℓ), an isomorphism $\sigma_\ell : S_\ell \cong {S'}_\ell$ is induced by conjugation $s \mapsto g_\ell(\sigma) s g_\ell(\sigma)^{-1}$ for $g_\ell(\sigma) \in G(\mathbb{Q}_\ell)$ after replacing S_ℓ by an open subgroup of S_ℓ and replacing S'_ℓ by the image of the new S_ℓ;*

(S2) *For a prime ℓ at which $G_{1/\mathbb{Z}_\ell}$ is smooth quasi-split (so for a sufficiently large rational prime ℓ), we have*

$$\mathrm{Aut}(G_1(\mathbb{Z}_\ell)) = \mathrm{Aut}(M_\ell/\mathbb{Q}_\ell) \ltimes PG(\mathbb{Z}_\ell)$$

and

$$\mathrm{Aut}(G_1(\mathbb{Q}_\ell)) = \mathrm{Aut}(M_\ell/\mathbb{Q}_\ell) \ltimes PG(\mathbb{Q}_\ell),$$

(S3) *For sufficiently large distinct rational primes p and ℓ, any group homomorphism $\phi : G_1(\mathbb{Z}_p) \to G_1(\mathbb{Z}_\ell))$ is trivial* (that is, $\mathrm{Ker}(\phi) = G_1(\mathbb{Z}_p)$).

The assertion (S1) follows directly from a result of Lazard on ℓ–adic Lie groups (see [GAN] IV.3.2.6), because the automorphism of the Lie algebra of S (hence of S') are all inner up to the automorphism of the field (in our case). The assertion (S2) for finite fields is an old theorem of Steinberg (see [St] 3.2), and as remarked in [CST] in the comments (in page 587) on [St], (S2) for general infinite fields follows from a very general result in [BT] 8.14. Since the paper [BT] is a long paper and treats only algebraic groups over an infinite field (not over a valuation ring like $\mathbb{Z}_\ell$), for the reader's convenience, we will give a self-contained proof of (S2) restricting ourselves to unitary groups and symplectic groups.

Since the assertions (S3) concerns only sufficiently large primes, we may always assume

(QS) *$G_1(\mathbb{Z}_p)$ and $G_1(\mathbb{Z}_\ell)$ are quasi-split.*

We now prove the assertion (S3). Let $\phi : G_1(\mathbb{Z}_p) \to G_1(\mathbb{Z}_\ell)$ be a homomorphism. Since $G_1(\mathbb{Z}_p)$ is quasi split, $G_1(\mathbb{Z}_p)$ is generated by unipotent elements (see Proposition 3.1), and its unipotent radical U is generated by an additive subgroup U_α corresponding to a simple root α.

If $G_1 = SL(n)_{/\mathbb{Z}}$, for example, we may assume that U_α is made of diagonal matrices

$$\mathrm{diag}[1_j, \left(\begin{smallmatrix}1 & u\\ 0 & 1\end{smallmatrix}\right), 1_{n-j-2}] := \begin{pmatrix} 1_j & 0 & 0 \\ 0 & \left(\begin{smallmatrix}1 & u\\ 0 & 1\end{smallmatrix}\right) & 0 \\ 0 & 0 & 1_{n-j-2} \end{pmatrix}$$

with $u \in \mathbb{Z}_p$ for an index j (with $1 \leq j \leq n$), where 1_j is the $j \times j$ identity matrix.

In general, U and U_α are p-profinite. We consider the normalizer $N(U_\alpha)$ and the centralizer $Z(U_\alpha)$ of U_α in G_1. Then by conjugation, $N(U_\alpha)/Z(U_\alpha)$ acts on U_α. Since ϕ is a group homomorphism, the quotient $N(U_\alpha)/Z(U_\alpha)$ keeps acting on the image $\phi(U_\alpha)$ in $G_1(\mathbb{Z}_\ell)$ through conjugation by elements in $\phi(N(U_\alpha))$. If $p \neq \ell$, every element of $\phi(U_\alpha)$ is semi-simple (because unipotent radical of $G_1(\mathbb{Z}_\ell)$ is ℓ-profinite). Thus the centralizer (resp. the normalizer) of $\phi(U_\ell)$ is given by $Z(\mathbb{Z}_\ell)$ (resp. $N(\mathbb{Z}_\ell)$) for a reductive subgroup Z (resp. N)

of G_1. Then $N(\mathbb{Z}_\ell)/Z(\mathbb{Z}_\ell)$ is a finite subgroup of the Weyl group W_1 of $G_{1/\mathbb{C}}$ which is independent of ℓ.

For example, if $G_1 = SL(n)_{/\mathbb{Z}}$, and if $\phi(U_\alpha)$ is made of diagonal matrices $\mathrm{diag}[\zeta_1 1_{m_1}, \zeta_2 1_{m_2}, \dots, \zeta_r 1_{m_r}]$ for generically distinct ζ_j, Z is given by the subgroup

$$SL(n) \cap (GL(m_1) \times GL(m_2) \times \cdots \times GL(m_r)),$$

where $GL(m_1) \times GL(m_2) \times \cdots \times GL(m_r)$ is embedded in $GL(n)$ diagonally. The quotient N/Z in this case is isomorphic to the subgroup of permutation matrices preserving Z.

If $\phi(U_\alpha)$ is nontrivial, the image of $N(U_\alpha)/Z(U_\alpha)$ in $\mathrm{Aut}(\phi(U_\alpha))$ grows at least on the order of p as p grows. In the above example of $G_1 = SL(n)_{/\mathbb{Z}}$, if $\phi(U_\alpha) \cong \mathbb{Z}/p^m\mathbb{Z}$ for $m > 0$, all elements in $\mathrm{Aut}(\phi(U_\alpha)) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$ come from $N(U_\alpha)/Z(U_\alpha) \cong \mathbb{Z}_p^\times$. This is impossible if $p \gg |W_1|$. Thus $\phi(U_\alpha) = 1$. Since $G_1(\mathbb{Z}_p)$ for large enough p is generated by U_α for all simple roots α, ϕ has to be trivial for p large enough. □

Since we assume to have the strong approximation theorem, we need to assume that G_1 is simply connected; so, we may restrict ourselves to symplectic and unitary groups (those groups of types A and C). We shall give a detailed exposition of how to prove (S2) for general linear groups and split symplectic groups and give a sketch for quasi split unitary groups.

Write $\chi : G \to Z^G = G/G_1$ for the projection map for the cocenter Z^G. In the following subsection, we assume that the base field K is either a number field or a nonarchimedean field of characteristic 0 (often a p-adic field). When K is nonarchimedean, we suppose that the classical group G is defined over $\mathbb{Z}_p$, and if K is a number field, G is defined over $\mathbb{Q}$. We write O for the maximal compact ring of K if K is nonarchimedean (so, O is the p-adic integer ring if K is p-adic). We equip the natural locally compact topology (resp. the discrete topology) on $G(A)$ for $A = K$ or O if K is a local field (resp. a number field). Then we define, for $A = K$ and O, $\mathrm{Aut}_\chi(G(A))$ by the group of continuous automorphisms of the group $G(A)$ which preserve χ up to automorphisms induced on Z^G by the field automorphisms of K. Thus

$$\mathrm{Aut}_\chi(G(A)) = \{\sigma \in \mathrm{Aut}(G(A)) | \chi(\sigma(g)) = \tau(\chi(g)) \ \text{ for } \exists\ \tau \in \mathrm{Aut}(K)\}.$$

For a subgroup H with $G_1(A) \subset H \subset G(A)$ and a section s of $\chi : H \to Z^G(A)$, we write $\mathrm{Aut}_s(H)$ for the group of continuous automorphisms of H preserving s up to field automorphisms and inner automorphisms (in [PAF] 4.4.3, the symbol $\mathrm{Aut}_{\det}(GL_2(A))$ means the group Aut_s here for a section s of $\det : GL(2) \to \mathbb{G}_m$).

3.1 General linear groups

Let $L_j \subset \mathbf{P}^{n-1}$ be the hyperplane of the projective space $\mathbf{P}^{n-1}(K)$ defined by the vanishing of the j–th homogeneous coordinate x_j. We start with the following well known fact:

Proposition 3.1. *Let P be the maximal parabolic subgroup of $GL(n)$ fixing the infinity hyperplane L_n of $\mathbf{P}^{n-1}$. For an infinite field K, $SL_n(K)$ is generated by conjugates of $U_P(K)$, where U_P is the unipotent radical of P.*

Proof. Let H be a subgroup generated by all conjugates of U_P. Thus H is a normal subgroup of $SL_n(K)$. Since $SL_n(K)$ is almost simple, we find that $SL_n(K) = H$. □

Proposition 3.2. *For an open compact subgroup S of $SL_n(K)$ for a p–adic local field K, the unipotent radical U of a Borel subgroup B_1 of $SL_n(K)$ and S generate $SL_n(K)$. Similarly S and a Borel subgroup B of $GL_n(K)$ generate $GL_n(K)$.*

Proof. We may assume that U is upper triangular. Thus $U \supset U_P$ for the maximal parabolic subgroup P in Proposition 3.1. We consider the subgroup H generated by S and U_P. The group U_P acts transitively on the affine space $\mathbf{A}^{n-1}(K) = \mathbf{P}^{n-1}(K) - L_n$. For any $g \in S - B_1$ for the upper triangular Borel subgroup B_1, gUg^{-1} acts transitively on $\mathbf{P}^{n-1}(K) - g(L_n)$. Note that $\bigcap_{g\in S} g(L_n)$ is empty, because intersection of n transversal hyperplanes is empty. Thus we find that H acts transitively on $\mathbf{P}^{n-1}(K)$. Since $\mathbf{P}^{n-1}(K)$ is in bijection with the set of all unipotent subgroups conjugate to U_P in $SL_n(K)$, H contains all conjugates of U_P in $SL_n(K)$; so, $H = SL_n(K)$ by Proposition 3.1. From this, generation of $GL_n(K)$ by B and S is clear because $GL_n(K) = B \cdot SL_n(K)$. □

In this case of GL_n, we have $\chi = \det$ and $Z^G = \mathbb{G}_m$. Thus, for $A = K$ or O, $\mathrm{Aut}_{\det}(GL_n(A))$ is the automorphism group of the group $GL_n(A)$ preserving the determinant map up to field automorphisms of K, that is, $\sigma \in \mathrm{Aut}_{\det}(GL_n(A))$ satisfies $\det(\sigma(g)) = \tau(\det(g))$ for a field automorphism $\tau \in \mathrm{Aut}(K)$. More generally, for a subgroup $H \subset GL_n(A)$ containing $SL_n(A)$, we define $\mathrm{Aut}_{\det}(H)$ for the automorphism group of H preserving $\det : H \to A^\times$ up to field automorphisms of K. Fixing a section $s : A^\times \to GL_n(A)$ of the determinant map, that is, $\det(s(x)) = x$, we recall $\mathrm{Aut}_s(GL_n(A)) = \{\sigma \in \mathrm{Aut}(GL_n(A)) | \sigma(s(x)) = g \cdot s(\tau(x))g^{-1}\}$ for some $g \in GL_n(A)$ and $\tau \in \mathrm{Aut}(K)$. Similarly, we define $\mathrm{Aut}_s(H)$ for a section s of the determinant map $\det : H \to A^\times$. We write $Z(SL_n(A))$ for the center of $SL_n(A)$, which is the finite group $\mu_n(A)$ of n-th roots of unity.

We now prove (S2) for $SL_n(A)$:

Proposition 3.3. *If $A = K$, assume that K is either a local field of characteristic 0 or a number field. If $A = O$, assume that K is a local field of characteristic 0. Then we have*

1. *The continuous automorphism groups* $\mathrm{Aut}(PGL_n(A))$, $\mathrm{Aut}(PSL_n(A))$ *and* $\mathrm{Aut}(SL_n(A))$ *are all canonically isomorphic to*

$$\begin{cases} (\mathrm{Aut}(K) \times \langle J \rangle) \ltimes PGL_n(A) & \text{if } n \geq 3, \\ \mathrm{Aut}(K) \ltimes PGL_n(A) & \text{if } n = 2, \end{cases}$$

where $J(x) = w_0{}^t x^{-1} w_0^{-1}$ *for* $w_0 = (\delta_{i,n+1-j}) \in GL(n)$ *and* $\mathrm{Aut}(K)$ *is the continuous field automorphism group of* K.

2. *If* $H \supset SL_n(A)$ *is a subgroup of* $GL_n(A)$*, we have*

$$\mathrm{Aut}_s(H) = \{g \in \mathrm{Aut}(PGL_n(A)) | \tau_g(\det(H)) = \det(H)\},$$

where τ_g *indicates the projection of* g *to* $\mathrm{Aut}(K)$.

3. *We have a canonical split exact sequence*

$$1 \to \mathrm{Hom}(A^\times, Z(SL_n(A))) \to \mathrm{Aut}_{\det}(GL_n(A)) \to \mathrm{Aut}(SL_n(A)) \to 1.$$

In other words, for $\sigma \in \mathrm{Aut}_{\det}(GL_n(A))$*, there exists* $g \in GL_n(A)$ *and* $\tau \in \mathrm{Aut}(K)$ *with* $\sigma(x) = \zeta(\det(x)) g \tau(x) g^{-1}$ *for* $\zeta \in \mathrm{Hom}(A^\times, Z(SL_n(A)))$.

If K is a local field, we put the natural locally compact topology on the group, and if K is a global field, we put the discrete topology on the group. We shall give a computational proof for GL_n, because it describes well the mechanism of how an automorphism is determined entry by entry (of the matrices involved).

Proof. We first deal with the case where A is the field K. We first study $PGL_n(K)$. We have an exact sequence:

$$1 \to PGL_n(K) \xrightarrow{i} \mathrm{Aut}(PGL_n(K)) \to \mathrm{Out}(PGL_n(K)) \to 1,$$

where $i(x)(g) = xgx^{-1}$. We write B (resp. U) for the upper triangular Borel subgroup (resp. the upper triangular unipotent subgroup) of $GL_n(K)$. Their image in $PGL_n(K)$ will be denoted by $\overline{B}$ and $\overline{U}$.

Let $\mathcal{A}$ be a subgroup of $GL_n(K)$ isomorphic to the additive group K; so, we have an isomorphism $a : K \cong \mathcal{A}$. Consider the image $a(1)$ of $1 \in K$ in $\mathcal{A}$. Replacing K by a finite extension containing an eigenvalue α of $a(1)$, let $V_\alpha \subset K^n$ be the eigenspace of $a(1)$ with eigenvalue α. Then $a(\frac{1}{m})$ acts on V_α and $a(\frac{1}{m})^m = a(1) = \alpha \in \mathrm{End}(V_\alpha)$. Thus we have an algebra homomorphism: $K[x]/(x^m - \alpha) \to \mathrm{End}_K(V_\alpha)$ for all $0 < m \in \mathbb{Z}$. If K is a p–adic local field, $\bigcap_m (K^\times)^{m!} = \{1\}$. By using this, we find $\bigcap_m (K^\times)^m = \{1\}$ for a number field

K. Thus if K is a non-archimedean local field or a number field, we find that α has to be 1. Thus $\mathcal{A}$ is made up of commuting unipotent elements; so, by conjugation, we can embed $\mathcal{A}$ into U.

Since $\overline{U} \cong U$ is generated by unipotent subgroups isomorphic to K, by the above argument, $\sigma(\overline{U})$ for $\sigma \in \mathrm{Aut}(PGL_n(K))$ is again a unipotent subgroup of $PGL_n(K)$. Since $\overline{B}$ is the normalizer of $\overline{U}$, again $\sigma(\overline{B})$ is the normalizer of $\sigma(\overline{U})$; so, $\sigma(\overline{B})$ is a Borel subgroup. We find $g \in GL_n(K)$ such that $\sigma(\overline{B}) = g\overline{B}g^{-1}$. Thus we may assume that σ fixes $\overline{B}$. Applying the same argument to $\overline{U}$, we may assume that σ fixes $\overline{U}$. Since we have a unique filtration:

$$\overline{U} = U_1 \supset U_2 \supset U_3 \supset \cdots \supset U_{n-1} \supset \{1\} = U_n$$

with $[U_j, U_j] = U_{j+1}$ and $U_j/U_{j+1} \cong K^{n-j}$, σ preserves this filtration. We fix an isomorphism $a_j : K^{n-j} \hookrightarrow U_j$ given by

$$a_j(\alpha_1, \ldots, \alpha_{n-j}) = 1 + \alpha_1 E_{1,j+1} + \alpha_2 E_{2,j+2} + \cdots + \alpha_{n-j} E_{n-j,n},$$

where $E_{i,j}$ is the matrix having non-zero entry 1 only at the (i,j)-spot. Then a_j induces $K^{n-j} \cong U_j/U_{j+1}$. Since $\sigma([u,u']) = [\sigma(u), \sigma(u')]$ for $u, u' \in U_j$ and $[\sigma(u), \sigma(u')] \mod U_{j+2}$ is uniquely determined by the cosets uU_{j+1} and $u'U_{j+1}$, $\sigma : \overline{U} \cong \overline{U}$ is uniquely determined by $\sigma_1 : U_1/U_2 \cong U_1/U_2$ induced by σ.

Each subquotient U_j/U_{j+1} is a K-vector space and is a direct sum of one-dimensional eigenspaces under the conjugate action of $\overline{T} := \overline{B}/\overline{U}$. Define an isomorphism $t : (K^\times)^n/K^\times \cong T$ by $t(\alpha_1, \ldots, \alpha_n) = \mathrm{diag}[\alpha_1, \ldots, \alpha_n]$, and we write $\alpha_j(t) = \alpha_j$ if $t = \mathrm{diag}[\alpha_1, \ldots, \alpha_n]$. Then $U_{ij} \subset \overline{U}$ $(j > i)$ generated by $u_{ij} = 1 + E_{i,j}$ is the eigen-subgroup (isomorphic to one dimensional vector space over K) on which $t \in \overline{T}$ acts via the multiplication by $\chi_{ij}(t) = \alpha_i \alpha_j^{-1}(t)$. The automorphism σ also induces an automorphism $\overline{\sigma}$ of $T = \overline{B}/\overline{U}$. Thus σ permutes the eigen-subgroups U_{ij} of $\overline{U}$.

Let $k = \mathbb{Q}$ if K is a number field and $k = \mathbb{Q}_p$ if K is a p-adic field. Then σ induces a k-linear automorphism on U_j/U_{j+1} for all j. We first assume $K = k$. Write $\sigma(a_1(1, \ldots, 1)) = a_1(\alpha_1, \ldots, \alpha_{n-1}) \mod U_2$. Solve $a_j a_{j+1}^{-1} = \alpha_j$ for $j = 1, \ldots, n-1$. Then changing σ by $x \mapsto t\sigma(x)t^{-1}$ for $t = \mathrm{diag}[a_1, a_2, \ldots, a_n]$, we may assume that $\sigma_1(a_1(\mathbf{1})) \equiv a_1(\mathbf{1}) \mod U_2$ for $\mathbf{1} = (1, 1, \ldots, 1) \in K^{n-1}$. Further by conjugating σ by an element in $\overline{U}$, we may assume that $\sigma(a_1(\mathbf{1})) = a_1(\mathbf{1})$. Thus $\sigma(a_1(r \cdot \mathbf{1})) = a_1(r \cdot \mathbf{1})$ for all $r \in \mathbb{Q}$. By taking commutators of $a_1(r \cdot \mathbf{1})$, we have a nontrivial element in U_j/U_{j+1} fixed by σ for all j. In particular, σ fixes $U_{n-1} \cong k$ and hence fixes the character χ_{1n}. If $n \geq 3$, looking at $U_{n-2}/U_{n-1} = U_{1,n-1} \oplus U_{2,n}$, we conclude that σ either interchanges the two eigenspaces or fixes each. If σ interchange the two, replacing σ by $\sigma \circ J$ for the automorphism $J = J_n$ of $GL_n(K)$ given by $J(x) = w_0{}^t x^{-1} w_0^{-1}$, we may assume σ fix each $\overline{T}$-eigenspace of U_{n-2}/U_{n-1}. By the commutator relation $[u_{ij}, u_{jk}] = u_{ik}$ if $i < j < k$, we conclude that

σ has to fix all eigen-subgroups U_{ij} of $\overline{U}$. Since $tu_{ij}t^{-1} = \chi_{ij}(t)u_{ij}$ and σ commutes with the multiplication by $\chi_{ij}(t) \in k$ on U_{ij}, we find by the K-linearity of σ that $\chi_{ij}(\overline{\sigma}(t))\sigma(u_{ij}) = \sigma(\chi_{ij}(t)u_{ij}) = \chi_{ij}(t)\sigma(u_{ij})$. Thus σ acts trivially on $\overline{T}$. Since $a_1(\mathbf{1})$ has non-trivial projection to all $\overline{T}$-eigenspaces in U_1/U_2, we conclude that $\sigma(u_{i,i+1}) = u_{i,i+1}$. Then $\overline{U}$ is fixed by σ again by the commutator relation $[u_{ij}, u_{jk}] = u_{ik}$ if $i < j < k$. Thus, modifying σ further by an inner automorphism and J, we may assume that σ fixes B element-by-element.

Now we assume that $K \supsetneq k$. Modifying σ as above by composing an inner automorphism and the action of J if necessary, we assume that σ preserves the eigen subgroups U_{ij} for all $i < j$. We are going to show that $\chi_{ij} \circ \overline{\sigma} = \widetilde{\sigma} \circ \chi_{ij}$ (for all $i < j$) for a continuous field automorphism $\widetilde{\sigma}$ of K. Since σ induces a k-linear automorphism of $U_{ij} \cong K$ and $\chi_{ij}(t) \in \mathrm{Im}(\chi_{ij}) = K^\times$ acts on U_{ij} through the multiplication by $\chi_{ij}(t) \in K^\times$, we find an automorphism $\widetilde{\sigma}_{ij} \in \mathrm{Aut}(K)$ of the field K such that $\chi_{ij} \circ \overline{\sigma} = \widetilde{\sigma}_{ij} \circ \chi_{ij}$. This field automorphism $\widetilde{\sigma} = \widetilde{\sigma}_{ij}$ does not depend on (i,j) by the commutator relation $[u_{ij}, u_{jk}] = u_{ik}$ for all $i < j < k$. Thus modifying σ further by an element of $\mathrm{Aut}(K)$, we may assume that σ fixes B.

We are going to prove that σ inducing the identity map on B is the identity on the entire group. For the moment, we suppose that K is p–adic. Then by [GAN] IV.3.2.6, for a sufficiently small open compact subgroup $S \subset PGL_n(K)$, $\sigma : S \cong \sigma(S)$ induces an automorphism Φ_σ of the Lie algebra $\mathfrak{G}_{\mathbb{Q}_p}$ of $PGL_n(K)$ over $\mathbb{Q}_p$. Since $\dim_{\mathbb{Q}_p} \mathfrak{G}_{\mathbb{Q}_p} = \dim_{\mathbb{Q}_p} \mathfrak{G}_K$ for the Lie algebra $\mathfrak{G}_K$ of $PGL_n(K)$ over K, we find that $\mathrm{Aut}_K(\mathfrak{G}_K) \subset \mathrm{Aut}_{\mathbb{Q}_p} \mathfrak{G}_{\mathbb{Q}_p}$ has the same dimension over $\mathbb{Q}_p$ as a Lie group over $\mathbb{Q}_p$ (cf. [BLI] VIII.5.5). Thus $\Phi_\sigma \in \mathfrak{G}_K$ is induced by $g \in GL_n(K)$ through the adjoint action (cf. [BLI] VIII.13). Since σ fixes B, we find that g commutes with B and, hence, g is in the center. Therefore, shrinking S further if necessary, we conclude $\sigma = 1$ on S and on B. Since B and S generate $PGL_n(K)$ (see Proposition 3.2), we find σ is the identity map over entire $PGL_n(K)$. This shows that, under the condition that $n \geq 3$,

$$\mathrm{Out}(PGL_n(K)) \cong \mathrm{Aut}(K) \times \langle J \rangle \quad \text{and} \quad \mathrm{Aut}(PGL_n(K)) = (\mathrm{Aut}(K) \times \langle J \rangle) \ltimes PGL_n(K)$$

if K is a local p–adic field. If $n = 2$, we need to remove the factor $\langle J \rangle$ from the above formula. If $K = \mathbb{R}$ or $\mathbb{C}$, the above fact is well known (see [BLI] III.10.2).

Suppose now that K is a number field. Write O for the integer ring of K. Take a prime $\mathfrak{p}$ such that $O_\mathfrak{p} \cong \mathbb{Z}_p$. Since σ fixes B, for the diagonal torus T, σ fixes its normalizer $N(T)$. Since $N(T) = W \ltimes T$, we find that $\sigma(w) = tw$ for an element $t \in T$. Since $PGL_n(K) = \bigsqcup_{w \in W} BwB$, we find that σ is continuous with respect to the $\mathfrak{p}$–adic topology. Thus σ induces $\mathrm{Aut}(PGL_n(K_\mathfrak{p}))$ fixing B, and we find that $\sigma = 1$, which shows again $\mathrm{Out}(PGL_n(K)) \cong (\mathrm{Aut}(K) \times \langle J \rangle)$

and $\mathrm{Aut}(PGL_n(K)) = (\mathrm{Aut}(K) \times \langle J \rangle) \ltimes PGL_n(K)$ for a number field K.

We can apply the same argument to $\mathrm{Aut}(PSL_n(K))$ and $\mathrm{Aut}(SL_n(K))$. Modifying σ by inner automorphisms, J and an element in $\mathrm{Aut}(K)$, we may assume that σ leaves $\overline{B}_1$ fixed. Then by the same argument as above, we conclude $\sigma = 1$ and hence we find that, if $n > 2$,

$$\mathrm{Aut}(SL_n(K)) = \mathrm{Aut}(PSL_n(K)) = (\mathrm{Aut}(K) \times \langle J \rangle) \ltimes PGL_n(K).$$

If $n = 2$, again we need to remove the factor $\langle J \rangle$ from the above formulas.

Now we look at $\mathrm{Aut}_s(H)$ for a section s of $\det : H \to K^\times$. Since $\sigma \in \mathrm{Aut}_{\det}(H)$ preserves the section s up to field and inner automorphisms, modifying σ by such an automorphism, we may assume that σ fixes $\mathrm{Im}(s)$. Then σ is determined by its restriction to $SL_n(K) \subset H$ and, hence, comes from and element in $\mathrm{Aut}(K) \ltimes PGL_2(K)$ preserving H.

To see the last assertion (3) for $A = K$, we consider the restriction map

$$\mathrm{Res} : \mathrm{Aut}_{\det}(GL_n(K)) \to \mathrm{Aut}(SL_n(K)).$$

Since $\mathrm{Aut}(SL_n(K))$ acts naturally on $GL_n(K)$ by the result already proven, the homomorphism Res is surjective. Take $\sigma \in \mathrm{Ker}(\mathrm{Res})$, and fix a section $s : K^\times \to GL_n(K)$ of the determinant map. Then for $x \in SL_n(K)$, we have $s(a)xs(a)^{-1} = \sigma(s(a)xs(a)^{-1}) = \sigma(s(a))x\sigma(s(a))^{-1}$, because $\mathrm{Res}(\sigma)$ is the identity map. Thus $\sigma(s(a))s(a)^{-1}$ commutes with $SL_n(K)$. Taking the determinant of $\sigma(s(a))s(a)^{-1}$, we find that $\sigma(s(a))s(a)^{-1} \in Z(SL_n(K))$ and $a \mapsto \zeta(a) = \sigma(s(a))s(a)^{-1}$ is a homomorphism of the group $K^\times$ into $Z(SL_2(K))$.

For any $g \in GL_n(K)$, we can write uniquely $g = s(\det(g))u$ with $u \in SL_n(K)$. For a homomorphism $\zeta : K^\times \to Z(SL_n(K))$,

$$\sigma(g) = \sigma(s(\det(g))u) = \zeta(\det(g))s(\det(g))u = \zeta(\det(g))g$$

gives an endomorphism of $GL_n(K)$. It is an automorphism because σ induces the identity on $SL_n(K)$ and $K^\times = \det(GL_n(K))$. Thus we get the desired exact sequence.

We now assume $A = O$. Since the argument is the same as in the case of the field K, we only indicates some essential points. Let $U(O) = U \cap SL_n(O)$ for the subgroup U of upper unipotent matrices. Since $\mathbf{P}^{n-1}(O) = \mathbf{P}^{n-1}(K)$, all Borel subgroups of $SL_n(O)$ are conjugate each other. Since $B_1(O) = SL_n(O) \cap B$ is a semi-direct product of $T_1(O)$ and $U(O)$, all unipotent subgroups are conjugate each other. By the same argument in the case of the field, we may assume that $\sigma \in \mathrm{Aut}(PGL_n(O))$ leaves $U(O)$ stable. Writing b_j for $(0, \ldots, \overset{j}{b_j}, 0, \ldots, 0) \in$

O^{n-1} with $b_j \in O$, we have $t(\alpha)a_1(b_j)t(\alpha)^{-1} = a_1(\alpha_j b_j \alpha_{j+1}^{-1})$ for $a_1 : O^{n-1} \cong U(O)/[U(O), U(O)]$ and $t : (O^\times)^n \cong T(O)$ as in the proof of Proposition 3.3. Then applying σ to the above formula, we see that $\overline{\sigma}$ preserves the coordinates α_j, and $\overline{\sigma}(t(\alpha))\sigma(a_1(b_j))\overline{\sigma}(t(\alpha)^{-1}) = \sigma(a_1(\alpha_j b_j \alpha_{j+1}^{-1}))$ for $\alpha = (\alpha_j) \in (O^\times)^n$. If $\sigma(a_1(e_j)) \in \mathfrak{m}$ for $e_j = (0, \dots, \overset{j}{1}, 0, \dots, 0) \in O^{n-1}$, then

$$\overline{\sigma}(t(\alpha))\sigma(a_1(e_j))\overline{\sigma}(t(\alpha))^{-1} = \sigma(a_1(\alpha e_j \alpha^{-1}))$$

has entry in $\mathfrak{m}$ at $(j, j+1)$. However $\sigma(U/U_2) = U/U_2 \cong O^{n-1}$ by $a_1(b) \leftrightarrow b$, we find $O \subset \mathfrak{m}$, a contradiction. Thus we have $\sigma(a_1(\mathbf{1})) = a_1(\alpha)$ for an element in $\alpha \in (O^\times)^{n-1}$. Then $t(\alpha) \in GL_n(O)$,and modifying σ by the conjugation of $t(\alpha)$, we may assume that $\sigma(a_1(\mathbf{1})) = a_1(\mathbf{1})$. Then proceeding in exactly the same way in the case of the field, we find that

$$\mathrm{Aut}(PGL_n(O)) = \begin{cases} (\mathrm{Aut}(O) \times \langle J \rangle) \ltimes PGL_n(O) & \text{if } n \geq 3, \\ \mathrm{Aut}(O) \ltimes PGL_2(O) & \text{if } n = 2. \end{cases}$$

From this, again we obtain the desired result for all other automorphism groups listed in the proposition. □

Let $M = K \oplus K$ be a semi-simple algebra with involution $c(x, y) = (y, x)$. Then we can realize $SL_n(K)$ as a special unitary group with respect to the hermitian form $(u, v) = \mathrm{Tr}({}^t u^c w_0 v)$ $(u, v \in M^n)$:

$$G_1(K) = \left\{\alpha \in SL_n(M) \middle| (\alpha u, \alpha v) = (u, v)\right\}.$$

Indeed $SL_n(K) \cong G_1(K)$ by $x \mapsto (x, J(x))$. Then we have $\mathrm{Aut}(M) \cong \mathrm{Aut}(K) \times \langle J \rangle$, and the results in Propositions 3.3 for $A = O$ and K can be restated as

$$\mathrm{Aut}(G_1(A)) = \mathrm{Aut}(M) \ltimes PG(A)$$

for the unitary group G with respect to $(\cdot, \cdot)$. We used in the proof of the theorem this version of the result in this section when K is a completion of the totally real field F at a prime $\mathfrak{l}$ splitting in the CM field M; so, $M_{\mathfrak{l}} = K_{\mathfrak{l}} \oplus K_{\mathfrak{l}}$ and c is induced by complex conjugation c of M.

3.2 Symplectic groups

We start with a general fact valid for quasi-split almost simple connected groups G_1 not necessarily a symplectic group.

Proposition 3.4. *Let K be a p–adic local field. Let S be an open subgroup of $G_1(K)$ of a classical almost simple connected group G_1 quasi-split over K. Let P_0 be a minimal parabolic subgroup of G_1 defined over K with unipotent radical U. Then S and $U(K)$ generate $G_1(K)$.*

The proof is similar to that of Proposition 3.2. Here is a sketch. Taking the universal covering of G_1, we may assume that G_1 is simply connected and is given by a Chevalley group G_1 inside $GL(n)$ for an appropriate n defined over O. Thus $G_1(K)$ is almost simple. We may assume that $P_0 = B \cap G_1$ for the upper-triangular Borel subgroup B of $GL(n)$. Thus G_1 acts on the projective space $\mathbf{P}^{n-1}$ through the embedding $G_1 \subset GL(n)$. Take the stabilizer $P \subset G_1$ of the infinity hyperplane L_n of $\mathbf{P}^{n-1}$. Then P is a maximal parabolic subgroup of G_1 containing P_0. Since $G_1(K)$ is almost simple, $G_1(K)$ is generated by conjugates of the unipotent radical $U_P(K)$ of P. The flag variety $\mathbf{P} = G_1/P$ is an irreducible closed subscheme of $\mathbf{P}^{n-1}$, and $U_P(K)$ acts transitively on $\mathbf{P} - L_n$. Since $\mathbf{P}$ is covered by finitely many affine open subschemes of the form $\mathbf{P} - g(L_n)$ (on which gU_Pg^{-1} acts transitively), the subgroup H generated by S and $U_P(K)$ acts transitively on $\mathbf{P}$ and hence contains all conjugates of $U_P(K)$. This shows that $G_1(K)$ is generated by S and $U_P(K)$. □

Let I_n be the antidiagonal $I_n = (\delta_{n+1-i,j}) \in M_n(\mathbb{Q})$ and $J_n = \left(\begin{smallmatrix} 0 & -I_g \\ I_g & 0 \end{smallmatrix}\right)$ for $n = 2g$ is an anti-diagonal alternating matrix. In this subsection, we deal with the split symplectic group defined over $\mathbb{Q}$ given by

$$G(A) = GSp_{2g}(A) = \left\{\alpha \in GL_n(A) \middle| \alpha J_{2g}{}^t\alpha = \nu(\alpha)J_{2g} \ \text{ for } \nu(\alpha) \in A^\times\right\},$$

and $G_1 = Sp_{2g} = \mathrm{Ker}(\nu)$. We write Z for the center of GSp_{2g}. We write B for the upper triangular Borel subgroup of GSp_{2g}. We write U for the unipotent radical of B. For the diagonal torus T, we have $B = T \ltimes U$, and B is the normalizer of $U(K)$ in $GSp_{2g}(K)$ for a field extension K of $\mathbb{Q}$. We take a standard parabolic subgroup $P \supset B$ of $GSp_{2g}(K)$ with unipotent radical U_P contained in U.

In this symplectic case, $\chi : G \to Z^G$ is the similitude map $\nu : GSp_{2n} \to \mathbb{G}_m$; so, we have $\mathrm{Aut}_\nu(GSp_{2n}(A))$ and $\mathrm{Aut}_s(H)$ for a subgroup H with $Sp_{2n}(A) \subset H \subset GSp_{2n}(A)$ and a section s of $\nu : H \to K^\times$. Here $A = K$ or O.

Proposition 3.5. *Let K be a local or global field of characteristic 0. Then we have*

1. $\mathrm{Aut}(Sp_{2g}(K)) = \mathrm{Aut}(PGSp_{2n}(K)) = \mathrm{Aut}(K) \ltimes PGSp_{2g}(K)$*, where we define* $PGSp_{2g}(K) = GSp_{2n}(K)/Z(K)$.
2. *For a section s of $\nu : H \to K^\times$ for a closed subgroup H with $Sp_{2n}(K) \subset H \subset GSp_{2n}(K)$, $\mathrm{Aut}_s(H)$is given by*
$$\{(\tau, g) \in \mathrm{Aut}(K) \ltimes PGSp_{2g}(K) \big| \tau(\nu(H)) = \nu(H)\}.$$
3. *We have a canonical split exact sequence*
$$1 \to \mathrm{Hom}(K^\times, Z(Sp_{2n}(K))) \to \mathrm{Aut}_\nu(GSp_{2n}(K)) \to \mathrm{Aut}(Sp_{2n}(K)) \to 1,$$
where $Z(Sp_{2n}(K))$ is the center $\{\pm 1\}$ of $Sp_{2n}(K)$.

We describe here a shorter argument proving the assertion (1) for GSp_{2g} (than the computational one for $GL(n)$) using the theory of root systems (although this is just an interpretation of the computational argument in terms of a slightly more sophisticated language). The assertions (2) and (3) follow from the assertion (1) by the same argument as in the case of $GL_n(K)$.

Proof. By [BLI] III.10.2, we may assume that K is either p–adic local or a number field. Write simply $B = B(K)$, $U = U(K)$ and $T = T(K)$. Let $\sigma \in \mathrm{Aut}(G(K))$. In the same manner as in the case of $GL(n)$, we verify that σ sends unipotent elements to unipotent elements. Write $\mathfrak{N} = \log(U)$ which is a maximal nilpotent subalgebra of the Lie algebra $\mathfrak{G}$ of $Sp_{2g}(K)$.

Let $k = \mathbb{Q}$ if K is global and $k = \mathbb{Q}_p$ if K is a p–adic field. Since $\sigma(U)$ is generated by unipotent matrices, we have $\log(\sigma(U))$ (which we write $\sigma(\mathfrak{N})$) is a nilpotent subalgebra of $\mathfrak{G}$, and $\dim_k \sigma(\mathfrak{N}) = \dim_k(\mathfrak{N})$. Thus $\sigma(\mathfrak{N})$ is a maximal nilpotent subalgebra of $\mathfrak{G}$; so, it is a conjugate of $\mathfrak{N}$ by $a \in Sp_{2g}(K)$. This implies $\sigma(\mathfrak{N}) = a\mathfrak{N}a^{-1}$. Conjugating back by a, we may assume that $\sigma(\mathfrak{N}) = \mathfrak{N}$. Then $\sigma(U) = U$ and hence $\sigma(B) = B$ because B is the normalizer of U. Thus σ induces an automorphism $\overline{\sigma}$ of $B/U \cong T$. We have weight spaces $\mathfrak{N}_\alpha$ and $\mathfrak{N} = \bigoplus_\alpha \mathfrak{N}_\alpha$. From this, we conclude that σ permutes $\mathfrak{N}_\alpha$: $\sigma(\mathfrak{N}_\alpha) = \mathfrak{N}_{\alpha\circ\overline{\sigma}}$.

Suppose $K = k$. Then σ is K–linear; in particular, σ induces a permutation of roots which has to give rise to a K–linear automorphism of the Lie algebra $\mathfrak{G}$. Modifying σ by the action of Weyl group (conjugation by a permutation matrix), we find that the permutation has to be trivial or an outer automorphism of the Dynkin diagram of Sp_{2g} (e.g. [Tt] 3.4.2 or [BLI] VIII.13). Since the Dynkin diagram of Sp_{2g} does not have any non-trivial automorphism, we find that the permutation is the identity map. Since on $\mathfrak{N}_\alpha$, T acts by a character $\alpha : T \to K^\times$, we find that $\alpha(t) = \alpha(\overline{\sigma}(t))$; so, $\overline{\sigma}$ is also the identity map.

We now assume that $K \neq k$. For the set of simple roots Δ of T with respect to $\mathfrak{N}$, $\bigoplus_{\alpha\in\Delta} \mathfrak{N}_\alpha \hookrightarrow \mathfrak{N}$ induces an isomorphism $\bigoplus_{\alpha\in\Delta} \mathfrak{N}_\alpha \cong \mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$. In other words, $\{\mathfrak{N}_\alpha|\alpha \in \Delta\}$ generates $\mathfrak{N}$ over K. The K–vector space structure of $\mathfrak{N}$ induces an embedding $i_1 : K \hookrightarrow \mathrm{End}_k(\mathfrak{N})$ of k–algebras. Since σ induces $\sigma_\mathfrak{N} \in \mathrm{End}_k(\mathfrak{N})$, we have another embedding $i_2 = \sigma_\mathfrak{N}^{-1} i_1 \sigma_\mathfrak{N}$ of K into $\mathrm{End}_k(\mathfrak{N})$. In $\mathrm{End}_k(\mathfrak{N}/[\mathfrak{N},\mathfrak{N}])$, the subalgebra A_1 generated by $i_1(K)$ and the action of T is a maximal commutative k–subalgebra. The subtorus T_0 given by the connected component of

$$\{t \in T|\alpha(t) = \beta(t) \text{ for all } \alpha, \beta \in \Delta\}$$

is dimension 1 and acts on $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ by scalar multiplication. This property characterizes T_0. Since the fact that T_0 acts by scalar multiplication on $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ does not change after applying $\overline{\sigma}$, we have $\overline{\sigma}(T_0) = T_0$. The image of $i_j(K)$ in $\mathrm{End}_k(\mathfrak{N}/[\mathfrak{N},\mathfrak{N}])$ is generated over k by the action of T_0; so, they coincide. Since $\sigma \in \mathrm{Aut}_k(\mathfrak{N})$ is an automorphism of the Lie algebra, the action of σ on $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ determines the action of σ on $\mathfrak{N}$. In particular, we conclude $i_1(K) = i_2(K)$, and we can think of $\tau = i_2^{-1} \circ i_1 \in \mathrm{Aut}(K)$. Hence, σ is τ–linear for $\tau \in \mathrm{Aut}(K)$ (that is, $\sigma(\xi v) = \xi^\tau \sigma(v)$ for $\xi \in K$). Thus modifying by τ, we may assume that $\sigma : \mathfrak{N} \to \mathfrak{N}$ is K–linear. Then σ induces a permutation of roots which has to give rise to an automorphism of the Lie algebra of Sp_{2g}. Then by the same argument as in the case where $K = k$, we conclude that σ induces identity map on B/U and U. Taking T to be diagonal, we may assume that $\sigma(T) = u_\sigma T u_\sigma^{-1}$ for $u_\sigma \in U$. Thus by modifying σ by the inner automorphism of u_σ, we may assume that σ is the identity on B.

Suppose that K is p–adic, then σ sends an open compact subgroup S to $\sigma(S)$, which induces an endomorphism of the Lie algebra of $Sp_{2g}(O)$ for the p–adic integer ring O and induces the identity map on the Lie algebra of B; in particular, σ is a O–linear map on the Lie algebra. Since an automorphism of the Lie algebra is inner induced by conjugation by an element $g \in Sp_{2g}(K)$, we have $gbg^{-1} = b$ for $b \in B$. Since the centralizer of B is the center of G, we find that σ is the identity on S.
Since S and U generate $G_1 = Sp_{2g}$, we find that σ is the identity over G. This proves the desired result for G_1 and p–adic fields K.

We can proceed in exactly the same way as in the case of $GL(n)$ when K is a number field and conclude the result. □

We then get the following integral analogue in a manner similar to Proposition 3.3:

Proposition 3.6. *If K is a finite extension of $\mathbb{Q}_p$ for $p > 2$ with integer ring O, we have*

$$\mathrm{Aut}(Sp_n(O)) = \mathrm{Aut}(PGSp_n(O)) = \mathrm{Aut}(K) \ltimes PGL_n(O),$$

and a canonical split exact sequence

$$1 \to \mathrm{Hom}(O^\times, Z(Sp_{2n}(O))) \to \mathrm{Aut}_\nu(GSp_n(O)) \to \mathrm{Aut}(Sp_{2n}(O)) \to 1,$$

where $Z(Sp_{2n}(O)) = \{\pm 1\}$ is the center of $Sp_{2n}(O)$.

3.3 Quasi-split unitary groups

Let M/K be a p–adic quadratic extension with p–adic integer rings R/O, and consider the quasi split unitary group

$$G(K) = \left\{\alpha \in GL_n(M) \middle| \alpha I_n {}^t\alpha^c = \nu(\alpha) I_n\right\} \quad \text{and} \quad G(O) = GL_n(R) \cap G(K),$$

where c is the generator of $\mathrm{Gal}(M/K)$, $\nu : G \to K^\times$ is the similitude map, $I_n = w_0$ if n is odd and $I_{2m} = \left(\begin{smallmatrix} 1_m & 0 \\ 0 & -1_m \end{smallmatrix}\right) w_0$ if $n = 2m$ is even. We may assume that $n \geq 3$ because in the case of $n = 2$, we have $PG \cong PGL_2$ (so, the desired result in this case has been proven already in 3.1).

We write G_1 for the derived group of G. Thus

$$G_1(K) = \{g \in G(K) | \det(g) = \nu(g) = 1\}.$$

Define the cocenter $Z^G = G/G_1$ and write $\mu : G \to Z^G$ for the projection. We may identify μ with $\det \times \nu$ and Z^G with its image in $\mathrm{Res}_{M/\mathbb{Q}_p}\mathbb{G}_m \times \mathrm{Res}_{K/\mathbb{Q}_p}\mathbb{G}_m$. We consider $\mathrm{Aut}_\mu(G(A))$ for $A = O$ and K made up of group automorphisms σ of $G(A)$ satisfying $\mu \circ \sigma = \mu$. We suppose that the nontrivial automorphism c of M over K is induced by an order 2 automorphism of the Galois closure M^{gal} of $M/\mathbb{Q}_p$ in the center of $\mathrm{Gal}(M^{gal}/\mathbb{Q}_p)$.

Write $\mathfrak{G}_A$ for the Lie algebra of $G_1(A)$ for $A = K$, O, M and R. Since $G_1(M) \cong SL_n(M)$, by Proposition 3.3, the Lie algebra automorphism group $\mathrm{Aut}(\mathfrak{G}_M)$ is isomorphic to $(\mathrm{Aut}(M) \times \langle J \rangle) \ltimes PG(M)$. Since $\mathfrak{G}_K \otimes_K M = \mathfrak{G}_M$, any automorphism of $\mathfrak{G}_K$ extends to an automorphism of $\mathfrak{G}_M$; so, $\mathrm{Aut}_K(\mathfrak{G}_K) \subset \mathrm{Aut}(\mathfrak{G}_M)$, and by this inclusion sends $\sigma \in \mathrm{Aut}(M) \subset \mathrm{Aut}(\mathfrak{G}_K)$ to an element $(\sigma, 1) \in (\mathrm{Aut}(M) \times \langle J \rangle)$. By this fact, at the level of the Lie algebra, all automorphisms of $\mathfrak{G}_A$ for $A = O$ and K are inner up to automorphism of M, and we have $\mathrm{Aut}(\mathfrak{G}_A) = \mathrm{Aut}(A) \ltimes PG(A)$.

We now study the automorphism group of the p-adic Lie group $G(K)$ and $G(O)$.

PROPOSITION 3.7. *Let $A = O$ or K for a p-adic field K. We assume that $p > 2$ and $K/\mathbb{Q}_p$ is unramified if $A = O$. Then we have*

1. $\mathrm{Aut}(G_1(A)) = \mathrm{Aut}(PG(A)) = \mathrm{Aut}(M) \ltimes PG(A)$,
2. *We have a canonical split exact sequence:*

$$1 \to \mathrm{Hom}(Z^G(A), Z(G_1(A))) \to \mathrm{Aut}_\mu(G(A)) \to \mathrm{Aut}(G_1(A)) \to 1,$$

where $Z(G_1(A))$ is the center of $G_1(A)$ and is isomorphic to $\mu_n(A)$.

Proof. We start with a brief sketch of the argument. A standard Borel subgroup of G (i.e., a standard minimal parabolic subgroup) is given by the subgroup B made up of all upper triangular matrices. We consider the subgroup $U \subset B$ made up of upper unipotent matrices. If $\sigma \in \mathrm{Aut}_\mu(G(K))$, $\sigma(U)$ is again generated by unipotent elements. Thus by [B] 6.5, $\sigma(U)$ is a conjugate of U in $G(K)$. Then by the same argument in the case of $GL(n)$, modifying σ by an element in $\mathrm{Aut}(M) \ltimes G(K)$, we may assume that σ fixes B. Again by the same argument as in the case of $GL(n)$, we conclude that $\sigma = 1$. Thus $\mathrm{Aut}(PG(K))$ and $\mathrm{Aut}(G_1(K))$ are given by $\mathrm{Aut}(M) \ltimes PG(K)$, and further assuming that p is odd and unramified in $M/\mathbb{Q}_p$, $\mathrm{Aut}(PG(O))$ and $\mathrm{Aut}(G_1(O))$ are given by $\mathrm{Aut}(M) \ltimes PG(O)$. If $\sigma \in \mathrm{Aut}_\mu(G(A))$, then we can write $\sigma(g) = h_\sigma \tau(g) h_\sigma^{-1}$ with a unique $h_\sigma \in PG(A)$ and $\tau \in \mathrm{Aut}(M)$ for all $x \in G_1(A)$. Since $\mathrm{Aut}(PG(A)) = \mathrm{Aut}(M) \ltimes PG(A)$, we find $\sigma(g) = \zeta(g) h_\sigma \tau(g) h_\sigma^{-1}$ with $\zeta(g) \in Z(G(A))$ for all $g \in G(A)$. Applying μ and noting that $\mu(\sigma(g)) = \tau(\mu(g))$, we find $\tau(\mu(g)) = \mu(\zeta(g))\tau(\mu(g))$; so, $\zeta(g) \in Z(G_1(A))$. Since σ is an automorphism, $\zeta : G(A) \to Z(G_1(A))$ is a homomorphism. By our assumption on p, $G_1(A)$ is the derived group of the topological group $G(A)$, and hence, ζ factors through $Z^G(A) = G(A)/G_1(A)$, since $Z(G_1(A))$ is abelian. This shows that the assertion (2) follows from the assertion (1).

Let us fill in the proof of the assertion (1) with some more details, assuming first for simplicity that $n = 3$. In this case, by computation, we have

$$U(K) = \left\{ u(x,y) = \begin{pmatrix} 1 & x & y \\ 0 & 1 & -x^c \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(M) \middle| xx^c + (y + y^c) = 0 \right\}.$$

The diagonal torus $T(K) \subset G$ is made of $t(a,b) = \mathrm{diag}[a, b, a^{-c}bb^c]$ for $a \in M^\times$ and $b \in M^\times$. Thus writing $\mathfrak{N} = \log(U(K))$, we have $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}] \cong M$ by $u(x,y) \mapsto x$ and $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ is a one-dimensional vector space over M (so, it is two-dimensional over the field of definition K) on which $t(a,b)$ acts through the multiplication by ab^c: $t(a,b)u(x,y)t(a,b)^{-1} = u(ab^c x, (ab^{-1})(ab^{-1})^c y)$. By the above argument in the general case, we may assume that $\sigma(B) = B$ for $\sigma \in \mathrm{Aut}_\mu(G(K))$. Then we have $\sigma(u(1,y)) = u(a, y')$ for $a \in M^\times$ and $t(a,1)^{-1}\sigma(u(1,y))t(a,1) = u(1, y'')$ for some $y', y'' \in M$. Thus modifying σ by an inner automorphism of an element in $T(K)$ and identifying $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ with M by $u(x,*) \mod [\mathfrak{N},\mathfrak{N}] \mapsto x$, we find that σ induces an automorphism of the field $M = \mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ and the same automorphism on $T(K) = B(K)/U(K)$ coordinate-wise. Thus again modifying σ by an element in $\mathrm{Aut}(K)$ and by an inner automorphism of an element of $U(K)$, we may assume that σ induces the identity map on B. We then conclude that σ is the identity map on $G(K)$ by the same argument as in the case of $GL(n)$ and $GSp(2n)$.

Next, we suppose that $n = 4$. Again by computation, we have

$$U(K) = \left\{ u(w,y,x,z) = \begin{pmatrix} 1 & w & x & z \\ 0 & 1 & y & x^c - yw^c \\ 0 & 0 & 1 & -w^c \\ 0 & 0 & 0 & 1 \end{pmatrix} \in GL_4(M) \middle| \begin{matrix} y = y^c \text{ and} \\ z^c - z = xw^c - wx^c \end{matrix} \right\}.$$

The diagonal torus $T(K) \subset G$ is made of $t(a,b,\nu) = \mathrm{diag}[a\nu, b\nu, b^{-c}, a^{-c}]$ for $a, b \in M^\times$ and $\nu \in K^\times$. We have

$$t(a,b,\nu)u(w,y,x,z)t(a,b,\nu)^{-1} = u(ab^{-1}w, bb^c\nu y, ab^c\nu x, aa^c\nu z).$$

Thus writing $\mathfrak{N} = \log(U(K))$, we have $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}] \cong M \oplus K$ by $u(w,y,x,z) \mapsto (w,y)$ and $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ is a three-dimensional vector space over K on which $t(a,b,\nu)$ acts through $(w,y) \mapsto (ab^{-1}w, bb^c\nu y)$. By the above argument at the level of the Lie algebra, we may assume that $\sigma(B) = B$ for $\sigma \in \mathrm{Aut}_\mu(G(K))$ and that σ preserves the root space decomposition $M \oplus K$ of $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$. We write σ_M (resp. σ_K) for the $\mathbb{Q}_p$-linear map induced by σ on M (resp. K). Thus modifying σ by conjugation of $t \in T(K)$, we may assume that $\sigma(1,1) = (1,1)$ for $(1,1) \in M \oplus K$. Writing the character of T giving the action of T on M (resp. K) by χ_M (resp. χ_K), we have $\chi_M(t(a,b,\nu)) = ab^{-1}$ and $\chi_K(t(a,b,\nu)) = bb^c\nu$. Then on M (resp. on K), the action of T gives rise to the multiplication by elements of $M^\times = \mathrm{Im}(\chi_M)$ (resp. in $K^\times = \mathrm{Im}(\chi_K)$), which is preserved by σ_M (resp. by σ_K); that is, we have $\sigma_M(\chi_M(t)w) = \chi_M(\sigma(t))\sigma_M(w)$ and $\sigma_K(\chi_K(t)y) = \chi_K(\sigma(t))\sigma_K(y)$. Since σ fixes $(1,1)$, we find that $\sigma_M \in \mathrm{Aut}(M)$ and $\sigma_K \in \mathrm{Aut}(K)$ satisfying $\chi_M \circ \sigma = \sigma_M \circ \chi_M$ and $\chi_K \circ \sigma = \sigma_K \circ \chi_K$. By the commutator relation $[u(w,y,*,*), u(w',y',*,*)] = u(0,0,wy'-w'y,*)$, we find that $\sigma_M|_K = \sigma_K$. Then modifying σ by the element $\sigma_M \in \mathrm{Aut}(M)$, we find that σ fixes $\overline{T} = B/U$, and again modifying σ by the conjugation by an element in $U(K)$, we bring σ to preserve $T \subset B$; so, σ induces the identity map on B. Out of this, we conclude that σ is the identity map on $G(K)$ by the same argument as in the case of $GL(n)$ and $GSp(2n)$, because σ coincides with an inner automorphism on an open neighborhood of the identity in $G(K)$ (by the argument at the level of the Lie algebra).

In the general case of $n > 4$, if $n = 2m+1$ is odd, we may identify $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}] = M^m$ as M-vector space by $(u_{i,j}) \in \mathfrak{N} \mapsto (u_{1,2},\dots,u_{m,m+1})$. On the j-th factor, $t = \mathrm{diag}[a_1,\dots,a_n] \in T(K)$ acts through the multiplication by $a_j a_{j+1}^{-1} \in M^\times$. If $n = 2m$ is even, $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}] \cong M^{m-1} \oplus K$ by sending upper unipotent matrices $(u_{i,j}) \in U(K)$ to $(u_{1,2},\dots,u_{m,m+1})$. On the first j-th factors with $j < m$, $t = \mathrm{diag}[\nu a_1,\dots,\nu a_m, a_m^{-c},\dots,a_1^{-c}] \in T(K)$ ($a_j \in M^\times$ and $\nu \in K^\times$ acts through the multiplication by $a_j a_{j+1}^{-1} \in M^\times$ and on the m-th factor, t acts through the multiplication by $\nu a_m a_m^c \in K^\times$). More generally, writing $\mathfrak{N}_j = [\mathfrak{N}_{j-1},\mathfrak{N}_{j-1}]$ starting with $\mathfrak{N}_1 = [\mathfrak{N},\mathfrak{N}]$, $\mathfrak{N}_j/\mathfrak{N}_{j+1}$ is a $T(K)$-module under the conjugation action. We go in the same way as in the case of $GL(n)$: modifying σ by an inner automorphism of an element of T, we may assume that σ fixes $\mathbf{1} = (1,\dots,1) \in M^m$ if $n = 2m+1$ and that if $n = 2m$, σ fixes $\mathbf{1} = (1,\dots,1,1) \in M^{m-1} \oplus K$. Once σ is normalized in this way, we see that σ on B/U and σ on $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$ are the action of an element of $\mathrm{Aut}(M)$ coordinate-wise. The action of $\mathrm{Aut}(M)$ is faithful if $n \geq 3$ because we have a factor M in $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$. We modify σ therefore by an element of $\mathrm{Aut}(M)$; then, σ is $T(K)$-linear on $\mathfrak{N}/[\mathfrak{N},\mathfrak{N}]$. Once this is established, we verify, using commutator relations, that σ commutes with the conjugation action of T on $\mathfrak{N}_j/\mathfrak{N}_{j+1}$ for all j. Then modifying again by conjugation of an element of $U(K)$, we conclude that σ is the identity on B, and the rest is the same as the proof in the case of $GL(n)$ and $GSp(2n)$.

If p is odd and unramified in $M/\mathbb{Q}_p$, the nilpotent Lie algebra $\mathfrak{N}_{/O}$ is the direct sum of its root spaces as $T(O)$-modules. Then the above argument done over the field K can be checked word-by-word over O, and we get the same assertion for $A = O$. □

References

Books

[ABV] D. Mumford, *Abelian Varieties*, TIFR Studies in Mathematics, Oxford University Press, New York, 1994.

[ARG] G. Cornell and J. H. Silverman, edited, *Arithmetic Geometry*, Springer, 1986

[BLI] N. Bourbaki, *Groupes et Algébres de Lie*, Hermann, Paris, 1972–85

[CST] R. Steinberg, *Robert Steinberg collected papers*, AMS 1997

[DAV] G. Faltings and C.-L. Chai, *Degeneration of Abelian Varieties*, Springer, 1990

[EPE] G. Shimura, *Euler Products and Eisenstein Series*, CBMS Regional Conference Series 93, American Mathematical Society, Providence, RI, 1997.

[GAN] M. Lazard, *Groupes Analytiques p–Adiques*, Publications IHES 26, 1965

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press and Iwanami Shoten, 1971, Princeton-Tokyo

[PAF] H. Hida, *p–Adic Automorphic Forms on Shimura Varieties*, Monographs in Mathematics, Springer, 2004

[RPT] G. Faltings and G. Wüstholtz, edited, *Rational Points: seminar Bonn/Wuppertal 1983/84*, Aspects of mathematics. E6, 1992

[SGA] A. Grothendieck, *Revetements Étale et Groupe Fondamental*, Séminaire de geometrie algébrique 1, Lecture notes in Math. 224, 1971, Springer

Articles

[B] A. Borel, Linear algebraic groups, Proc. Symp. Pure Math. IX (1966), 3–19

[BT] A. Borel and J. Tits, Homomorphismes “abstraits” de groupes algébriques simples, Ann. of Math. 97 (1973), 499–571

[D] P. Deligne, Travaux de Shimura, Sem. Bourbaki, Exp. 389, Lecture notes in Math. 244 (1971), 123–165

[D1] P. Deligne, Variétés de Shimura: interprétation modulaire, et techniques de construction de modéles canoniques, Proc. Symp. Pure Math. 33.2 (1979), 247–290

[F] K. Fujiwara, Arithmetic compactifications of Shimura varieties, Master's Thesis (University of Tokyo), 1989.

[Kn] M. Kneser, Strong approximation, Proc. Symp. Pure Math. IX (1966), 187–196

[Ko] R. Kottwitz, Points on Shimura varieties over finite fields, J. Amer. Math. Soc. 5 (1992), 373–444

[M] J. Milne, Canonical models of (mixed) Shimura varieties and automorphic vector bundles, Perspective Math. 10 (1990), 283–414.

[MS] J. Milne and K-y. Shih, Automorphism groups of Shimura varieties and reciprocity laws, Amer. J. Math. 103 (1981), 911-935

[Ra] M. Rapoport, Compactifications de l'espace de modules de Hilbert–Blumenthal, Comp. Math. 36 (1978), 255–335.

[Sh] G. Shimura, On canonical models of arithmetic quotients of bounded symmetric domains, Ann. of Math. 91 (1970), 144-222; II, 92 (1970), 528-549

[St] R. Steinberg, Automorphisms of finite linear groups, Canad. J. Math. 12 (1960) 606–615

[T] J. Tate, Endomorphisms of abelian varieties over finite fields, Inventiones Math. 2 (1966), 134–144

[Tt] J. Tits Classification of algebraic semisimple groups, Proc. Symp. Pure Math. IX (1966), 33–70

[W] A. Weil, Algebras with involutions and the classical groups, J. Ind. Math. Soc. 24 (1960), 589–623

[Z] J. G. Zarhin, Endomorphisms of abelian varieties over fields of finite characteristics, Math. USSR Izvestija 9 (2) (1975), 255-260

Haruzo Hida
Department of Mathematics
UCLA
Los Angeles, CA 90095-1555
hida@math.ucla.edu

Compactification de Schémas Abéliens Dégénérant au-dessus d'un Diviseur Régulier

Sandra Rozensztajn

Received: September 9, 2005
Revised: Novmber 16, 2005

Communicated by Peter Schneider

Abstract. We consider a semiabelian scheme G over a regular base scheme S, which is generically abelian, such that the points of the base where the scheme is not abelian form a regular divisor S_0. We construct a compactification of G, that is a proper flat scheme P over the base scheme, containing G as a dense open set, such that P_{S_0} is a divisor with normal crossings in P. We also show that given an isogeny between two such semiabelian schemes, we can construct the compactifications so that the isogeny extends to a morphism between the compactifications.

2000 Mathematics Subject Classification: 11G10, 11G18, 14G35, 14K05

Introduction

Dans l'article [Mum72], Mumford construit une variété abélienne dégénérante, c'est-à-dire un schéma semi-abélien qui est génériquement abélien à partir d'un ensemble de données, dites données de dégénérescences, qui consistent en un tore déployé de rang constant sur une base complète, et en un groupe de périodes. Il obtient au cours de sa construction une compactification du schéma semi-abélien, c'est-à-dire un schéma propre contenant le schéma semi-abélien comme ouvert dense, et muni d'une action de celui-ci prolongeant son action sur lui-même par translation.
Faltings et Chai dans [CF90] utilisent cette construction pour obtenir des compactifications des variétés de Siegel et de leur schéma abélien universel. Ils exposent ce faisant comment associer à un schéma abélien dégénérant l'ensemble des données de dégénérescence qui permettent de le retrouver en utilisant la technique de Mumford.

Grâce à ces méthodes, Künnemann, dans [Kün98], construit des compactifications régulières de schémas semi-abéliens sur un anneau de valuation discrète dont la fibre générique est abélienne. Généralisant sa technique, nous construisons des compactifications de schémas abéliens sur une base régulière dégénérant le long d'un diviseur régulier. La méthode requiert l'utilisation d'un faisceau inversible symétrique ample sur le schéma semi-abélien. En vertu du corollaire XI 1.16 de [Ray70], tout schéma semi-abélien de fibre générique abélienne sur une base régulière peut être muni d'un tel faisceau, nous n'introduisons donc pas de restriction en imposant son existence.
Notre construction a pour application de permettre une compactification des variétés de Shimura associées à certains groupes unitaires et de leur schéma abélien universel, donnant ainsi des résultats similaires à ceux de Chai et Faltings pour les variétés de Shimura associées aux groupes symplectiques exposés dans [CF90].
Avant d'énoncer le théorème, introduisons les définitions suivantes.

DÉFINITION 1. *S est un schéma régulier noethérien, et S_0 un diviseur régulier de S, W l'ouvert complémentaire de S_0. G est un schéma semi-abélien sur S, qui est de rang constant sur S_0, et tel que G_W est un schéma abélien, et $\mathcal{L}$ est un faisceau inversible symétrique ample sur G.*

REMARQUE 1. Comme G est de rang constant sur S_0, il y est globalement extension d'un schéma abélien par un tore, d'après le corollaire 2.11 de [CF90].

DÉFINITION 2. *On appelle compactification de G la donnée d'un schéma P propre, plat et régulier sur S tel que $G \subset P$, possédant les propriétés suivantes :*

1. *G est dense dans P, et agit sur P par prolongement de son action par translation sur lui-même.*
2. *G et P coïncident sur W*
3. *il existe un entier k positif tel que $\mathcal{L}^{\otimes k}$ se prolonge en un faisceau $\mathcal{L}_P$ ample sur P*
4. *P_0 est un diviseur à croisements normaux dans P*

Le théorème s'énonce alors :

THÉORÈME 1. *Il existe des compactifications de G.*

On a même la propriété suivante de prolongement des morphismes :

THÉORÈME 2. *Soit G_1 et G_2 comme dans la définition 1, et f un morphisme de S-schémas en groupes $G_1 \to G_2$, qui induit une isogénie $f_\eta : G_{1\eta} \to G_{2\eta}$. Alors il existe deux compactifications P_1, P_2 de G_1 et G_2 et un morphisme $\bar{f} : P_1 \to P_2$ prolongeant f.*

L'énoncé ne fait aucune hypothèse d'existence de faisceaux amples sur G_1 et G_2, qui résulte en fait des autres conditions du théorème : d'après la preuve de la proposition XI 1.2 de [Ray70], du fait que f_η est de noyau fini, il existe un faisceau inversible ample symétrique $\mathcal{L}_2$ sur G_2 tel que $\mathcal{L}_1 = f^*\mathcal{L}_2$ soit aussi ample. Nous supposerons dorénavant deux tels faisceaux fixés.

Pour prouver ces théorèmes, nous allons d'abord étudier une situation locale (base affine, complète) dans le paragraphe 2, puis voir comment on peut déduire le résultat global d'un résultat local, dans le paragraphe 3.

1 Découpage du problème

Dans tout ce paragraphe on va se placer dans un cas particulier : le cas où la base S est irréductible et est complète par rapport au sous-schéma S_0.
Le passage du cas complet au cas non complet est expliqué au paragraphe 3.3. D'autre part, S étant régulier, les composantes irréductibles de S correspondent à ses composantes connexes, on peut donc travailler composante par composante. Observons enfin que S étant complet par rapport à S_0, S est irréductible si et seulement si S_0 l'est.

1.1 Cas d'un seul groupe

S étant complet par rapport à S_0, on a une extension associée à G, appelée extension de Raynaud (pour la construction de cette extension voir [CF90] p. 33, ou [Mor85]) :

$$0 \to T \to \tilde{G} \xrightarrow{\pi} A \to 0$$

et sur $\tilde{G}$ on a un faisceau inversible ample $\tilde{\mathcal{L}}$ provenant de $\mathcal{L}$. $\tilde{G}$ est caractérisé par le fait que c'est un schéma semi-abélien de rang constant sur S dont le complété formel le long de S_0 est le même que celui de G.

Définition 3. *On dit que l'extension est déployée si le tore T est déployé, de groupe des caractères constant, et si $\tilde{\mathcal{L}}$ se descend en un faisceau inversible ample $\mathcal{M}$ sur A.*

Lemme 3. *Il existe un recouvrement étale fini S' de S tel que l'extension de Raynaud du groupe sur S' obtenu par changement de base soit déployée.*

Démonstration. En effet, d'après [D$^+$70], théorème X 5.16, il existe un tel S' qui permette d'obtenir un tore déployé à groupe de caractères constant, car S est normal et localement noethérien. Pour ce qui est de l'existence de $\mathcal{M}$, on se réfère à [Mor85], I.7.2.3. □

Définition 4. *On appelle dégénérescence déployée la donnée d'un triplet $(G, \mathcal{L}, \mathcal{M})$ où $(G, \mathcal{L})$ est comme dans les données et a une extension de Raynaud associée déployée, et $\mathcal{M}$ est un faisceau cubique inversible sur A tel que $\tilde{\mathcal{L}} = \pi^*\mathcal{M}$.*

Notons que nous appelons ici dégénéréscence ce qui serait appelé dans [CF90] dégénérescence ample.

Définition 5. *Un morphisme entre dégénérescences déployées* $(G, \mathcal{L}, \mathcal{M})$ *et* $(G', \mathcal{L}', \mathcal{M}')$ *est la donnée de* $f = (f_G, f_{\mathcal{L}}, f_A, f_{\mathcal{M}})$*, où* f_G *est un morphisme* $G \to G'$*,* $f_{\mathcal{L}}$ *est un isomorphisme* $f_G^* \mathcal{L}' \to \mathcal{L}$*,* $f_A : A \to A'$ *est déduit de* f_G*,* $f_{\mathcal{M}}$ *est un isomorphisme* $f_A^* \mathcal{M}' \to \mathcal{M}$*, et enfin* $f_{\mathcal{L}}$ *et* $f_{\mathcal{M}}$ *induisent le même morphisme* $f_{\tilde{G}}^* \tilde{\mathcal{L}}' \to \tilde{\mathcal{L}}$*.*

Pour nos données $(G, \mathcal{L})$ sur le schéma S de départ, il existe donc (d'après le lemme 3) une extension étale finie S' de S telle que les données $(G', \mathcal{L}')$ sur S' obtenues par changement de base forment une dégénérescence déployée (pour un certain faisceau $\mathcal{M}'$). Comme nous le démontrerons dans le paragraphe 3.2, on peut déduire une compactification sur S d'une compactification sur S', ce qui explique que l'on s'intéresse au cas particulier des dégénérescences déployées.

1.2 Cas d'un morphisme

Plaçons-nous maintenant dans les hypothèses du théorème 2. La construction de Raynaud étant fonctorielle, f induit f_A, f_T, $f_{\tilde{G}}$ qui font commuter le diagramme suivant :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_1 & \longrightarrow & \tilde{G}_1 & \longrightarrow & A_1 & \longrightarrow & 0 \\ & & f_T \downarrow & & f_{\tilde{G}} \downarrow & & f_A \downarrow & & \\ 0 & \longrightarrow & T_2 & \longrightarrow & \tilde{G}_2 & \longrightarrow & A_2 & \longrightarrow & 0 \end{array}$$

Définition 6. *On appelle morphisme d'extensions une telle flèche.*

Lemme 4. *Il existe une extension finie comme dans le lemme 3 qui convienne à la fois à* G_1 *et à* G_2*.*

Démonstration. En effet, si S_1 convient à G_1 et S_2 convient à G_2, $S_1 \times_S S_2$ convient à G_1 et G_2. □

Après une telle extension, on obtient un morphisme de dégénérescences déployées $(G_1, \mathcal{L}_1, \mathcal{M}_1) \to (G_2, \mathcal{L}_2, \mathcal{M}_2)$. Remarquons que comme f_η est une isogénie, le noyau de f est quasi-fini, de sorte que f_T et f_A sont aussi des isogénies.

2 Compactifications locales

Introduisons dès à présent des notations. On notera $S = \mathrm{Spec} R$, I l'idéal définissant S_0 et η le point générique de S. On notera $S_n = \mathrm{Spec} R/I^{n+1}$.
On se restreint dans ce paragraphe au cas où S est irréductible, complet par rapport à S_0 et affine. On se donne une dégénérescence déployée $(G, \mathcal{L}, \mathcal{M})$, et un morphisme de dégénérescences déployées $f : (G_1, \mathcal{L}_1, \mathcal{M}_1) \to (G_2, \mathcal{L}_2, \mathcal{M}_2)$.

2.1 Compactifications équivariantes

Dans ce cadre plus restrictif que celui de départ, nous allons démontrer un théorème légèrement plus fort.
Soit H un groupe fini agissant sur S, c'est-à-dire qu'à chaque $h \in H$ est associé un automorphisme $h_S : S \to S$, et ce de manière compatible. On suppose que H laisse S_0 stable.

Définition 7. *On dit que H agit sur la dégénérescence déployée $(G, \mathcal{L}, \mathcal{M})$, si à chaque $h \in H$ est associé un morphisme de dégénérescences déployées $(G, \mathcal{L}, \mathcal{M}) \to h_S^*(G, \mathcal{L}, \mathcal{M})$, ces morphismes étant compatibles entre eux.*

Définition 8. *L'action de H étant donnée, on dit qu'une compactification est équivariante si on peut définir sur $(P, \mathcal{L}_P)$ une action de H prolongeant celle sur $(G, \mathcal{L})$.*

Théorème 5. *Soit S un schéma irréductible, affine, complet par rapport à S_0, $(G, \mathcal{L}, \mathcal{M})$ une dégénérescence déployée sur S, et H un groupe fini agissant sur cette dégénérescence. Alors il existe des compactifications équivariantes de $(G, \mathcal{L})$.*

Théorème 6. *Soit S un schéma irréductible, affine, complet par rapport à S_0, $(G_1, \mathcal{L}_1, \mathcal{M}_1)$ et $(G_2, \mathcal{L}_2, \mathcal{M}_2)$ deux dégénérescences déployées sur S, et f un morphisme de dégénérescences H-équivariant et tel que f induise une isogénie $G_{1\eta} \to G_{2\eta}$. Alors il existe des compactifications équivariantes P_1 et P_2 de G_1 et G_2, et un prolongement H-équivariant de f en un morphisme $P_1 \to P_2$.*

La suite du paragraphe est consacrée à la preuve de ces théorèmes.

2.2 Données de dégénérescence

On peut associer fonctoriellement à une dégénérescence déployée un ensemble de données, appelé données de dégénérescence. Ici aussi nous appelons simplement données de dégénérescence ce qui serait appelé données de dégénérescences amples dans [CF90]. On a en fait une équivalence de catégories entre dégénérescences et données de dégénérescence. L'obtention des données de dégénérescence à partir de la dégénérescence est l'objet du chapitre II de [CF90]. La construction inverse, due à Mumford ([Mum72]), est reprise en partie ici pour obtenir une compactification.

2.2.1 Liste des données

Une donnée de dégénérescence consiste en un ensemble :
$(A, \underline{X}, \underline{Y}, \varphi, c, c^t, \tilde{G}, \iota, \tau, \tilde{\mathcal{L}}, \mathcal{M}, \lambda_A, \psi)$, tel que :

1. A est une variété abélienne sur S.
2. $\underline{X}$ et $\underline{Y}$ sont des faisceaux étales en groupes abéliens libres de même rang fini r, qui sont constants de valeur X et Y.

3. φ est un homomorphisme injectif $Y \to X$ (et donc de conoyau fini).
4. c est un morphisme $X \to A^t$ et c^t un morphisme $Y \to A$.

   Soit T le tore déployé de groupe des caractères X. L'opposé du morphisme c détermine une extension :

$$0 \to T \to \tilde{G} \xrightarrow{\pi} A \to 0$$

   On fixe un faisceau de Poincaré $\mathcal{P}$ sur $A \times_S A^t$.
5. ι est un morphisme $Y \to \tilde{G}$ au-dessus de c^t. Le morphisme ι correspond à une trivialisation $\tau : \mathbf{1}_{Y\times X} \xrightarrow{\sim} (c \times c^t)^* \mathcal{P}_\eta^{-1}$, qui est donnée par un système compatible de sections $\tau(y,\mu) = \tau(\mathbf{1}_{y,\mu}) \in \Gamma(\eta, (c^t(y), c(\mu))^* \mathcal{P}_\eta^{-1})$ pour $y \in Y$ et $\mu \in X$.

   ι définit une action de $y \in Y$ sur $\tilde{G}_\eta$ par translation, qu'on note S_y.
6. un faisceau cubique inversible $\mathcal{M}$ sur A tel que la polarisation associée $\lambda_A : A \to A^t$ vérifie $\lambda_A \circ c^t = c \circ \varphi$.
7. $\tilde{\mathcal{L}} = \pi^* \mathcal{M}$.

   On a une trivialisation $\tau \circ (\mathrm{id}_Y \times \varphi) : \mathbf{1}_{Y\times X} \xrightarrow{\sim} (c \times (c \circ \varphi))^* \mathcal{P}_\eta^{-1}$.
8. $\psi : \mathbf{1}_{Y_\eta} \xrightarrow{\sim} \iota^* \tilde{\mathcal{L}}_\eta^{-1}$ est une trivialisation compatible avec τ.

On notera pour simplifier $\psi(y)$ pour $\psi(\mathbf{1}_y)$ et $\tau(y,\mu)$ pour $\tau(\mathbf{1}_{(y,\mu)})$.
La trivialisation ψ vérifie la condition suivante : pour presque tout $y \in Y$, $\psi(y)$ s'étend en une section de $\iota^* \tilde{\mathcal{L}}^{-1}$ congrue à 0 modulo I. De plus, pour tout $y \in Y, y \neq 0$, $\tau(y, \varphi(y))$ s'étend en une section congrue à 0 modulo I.
Les deux trivialisations ψ et τ définissent des idéaux fractionnaires de R : I_y défini par $\psi(y)$, et $I_{y,\mu}$ défini par $\tau(y,\mu)$, avec la relation $I_{y+z} = I_y I_z I_{z,\varphi(y)}$.

Rappelons comment on obtient certaines de ces données. Étant donnée une dégénérescence déployée $(G, \mathcal{L}, \mathcal{M})$, on forme son extension de Raynaud $0 \to T \to \tilde{G} \to A \to 0$, ce qui fournit $\tilde{G}$, A, et $\underline{X}$ le groupe des caractères de T, qui est constant puisque on a supposé la dégénérescence déployée. D'autre part on a un schéma semi-abélien G^t tel que G^t_W est le schéma abélien dual de G_W, il forme aussi une dégénérescence déployée, d'extension de Raynaud associée $0 \to T^t \to \tilde{G}^t \to A^t \to 0$, où A^t est bien le schéma abélien dual de A. Ceci nous donne $\underline{Y}$ qui est le groupe des caractères de T^t, et est le dual de $\underline{X}$.

2.2.2 Morphismes de données

Un morphisme entre les données de dégénérescences

$$(A, \underline{X}, \underline{Y}, \varphi, c, c^t, \tilde{G}, \iota, \tau, \tilde{\mathcal{L}}, \mathcal{M}, \lambda_A, \psi)$$

et

$$(A', \underline{X}', \underline{Y}', \varphi', c', c^{t\prime}, \tilde{G}', \iota', \tau', \tilde{\mathcal{L}}', \mathcal{M}', \lambda'_A, \psi')$$

est la donnée d'un ensemble de morphismes $f_A : A \to A'$, $f_X : \underline{X} \to \underline{X}'$, $f_Y : \underline{Y} \to \underline{Y}'$, $f_{\tilde{G}} : \tilde{G} \to \tilde{G}'$, un isomorphisme $f_{\mathcal{L}} : f_{\tilde{G}}^* \tilde{\mathcal{L}}' \to \tilde{\mathcal{L}}$, et un isomorphisme $f_{\mathcal{M}} : f_A^* \mathcal{M}' \to \mathcal{M}$, ces morphismes vérifiant toutes les conditions de compatibilité.
Par fonctorialité de la construction de données de dégénérescence, à partir d'un morphisme $f : (G_1, \mathcal{L}_1, \mathcal{M}_1) \to (G_2, \mathcal{M}_2, \mathcal{L}_2)$, de dégénérescences déployées, on obtient un morphisme entre les données de dégénérescences associées, et en particulier $f_{\tilde{G}} : \tilde{G}_1 \to \tilde{G}_2$ et $f_A : A_1 \to A_2$ (comme dans le paragraphe 1.2), $f_X : X_2 \to X_1$ provenant de $f_T : T_1 \to T_2$, et $f_Y : Y_1 \to Y_2$.

2.2.3 Propriétés particulières au cas étudié

Les idéaux I_y et $I_{y,\mu}$ ont une forme particulière dans notre cas.

PROPOSITION 7. *Il existe une fonction $b : Y \times X \to \mathbb{Z}$ bilinéaire, et $a : Y \to \mathbb{Z}$ telles que $I_y = I^{a(y)}$ et $I_{y,\mu} = I^{b(y,\mu)}$*

Démonstration. Dans notre cas particulier, G ne dégénère que sur S_0 : sur W, c'est un schéma abélien. Rappelons le résultat de [CF90], corollaire 7.5 p. 77. Soit s un point de S, correspondant donc à un idéal premier $\mathfrak{p}$ de R. Soit Y_s le sous-groupe de Y formé des éléments $y \in Y$ pour lesquels $I_{y,\varphi(y)}$ n'est pas contenu dans $\mathfrak{p}$. Alors le groupe des caractères de la partie torique de G_s^t (fibre de G^t au-dessus de s) est Y/Y_s.
G^t étant abélien sur W, si $s \notin S_0$, la partie torique de G_s^t est nulle, et donc $Y = Y_s$, ce qui se traduit par $\forall y \in Y, s \notin V(I_{y,\varphi(y)})$. Ceci étant vrai pour tout $s \notin S_0$, on en déduit que pour tout y, on a $V(I_{y,\varphi(y)}) \subset V(I)$. Comme on sait que $I_{y,\varphi(y)} \subset I$ à cause de la condition sur $\tau(y, \varphi(y))$, on en déduit que $V(I_{y,\varphi(y)}) = V(I)$. I étant engendré par un élément irréductible ϖ, $I_{y,\varphi(y)}$ est donc de la forme (ϖ^k) pour un $k \in \mathbb{Z}$. Les idéaux I_y et $I_{y,\mu}$ sont donc aussi de la forme (ϖ^k) pour un $k \in \mathbb{Z}$. Il existe donc bien une fonction $b : Y \times X \to \mathbb{Z}$ bilinéaire, et $a : Y \to \mathbb{Z}$ telles que $I_y = I^{a(y)}$ et $I_{y,\mu} = I^{b(y,\mu)}$. □

Tous les idéaux que nous voyons apparaître sont donc des puissances de I. Tout se passe donc comme si nous étions dans un anneau de valuation discrète, ce qui est exactement la situation étudiée dans [Kün98], ce qui explique que nous puissions nous inspirer largement de cet article.

2.2.4 Données de dégénérescence équivariantes

Soit H un groupe fini agissant sur S, de façon que chaque $h \in H$ induise un morphisme de dégénérescences déployées $h : (G, \mathcal{L}, \mathcal{M}) \to (G, \mathcal{L}, \mathcal{M})$. On obtient pour tout $h \in H$ une action sur $\tilde{G}$ et sur $\tilde{\mathcal{L}}$, qu'on note $h_{\tilde{G}}$ et $h_{\tilde{\mathcal{L}}}$. Ces actions sont compatibles avec l'action de Y, au sens où : $h_{\tilde{G}_\eta} \circ S_y = S_{h(y)} \circ h_{\tilde{G}_\eta}$ et $\tilde{S}_y \circ S_y^*(h_{\tilde{\mathcal{L}}_\eta}) = h_{\tilde{\mathcal{L}}_\eta} \circ h_{\tilde{G}_\eta}^*(\tilde{S}_{h(y)})$. Ceci nous permet de définir une action de $\Gamma = Y \rtimes H$ sur $\tilde{G}_\eta$ et $\tilde{\mathcal{L}}_\eta$ par les formules $S_\gamma = S_y \circ h_{\tilde{G}_\eta}$ et $\tilde{S}_\gamma = h_{\tilde{\mathcal{L}}_\eta} \circ h_{\tilde{G}_\eta}^*(\tilde{S}_y)$ pour $\gamma = (y, h)$.

2.3 Modèle relativement complet

2.3.1 Définition

Étant donnée une donnée de dégénérescence, on peut définir un modèle relativement complet.

Définition 9. *Un modèle relativement complet est la donnée de :*

1. $\tilde{\pi} : \tilde{P} \to A$ *localement de type fini tel que* $\tilde{P}$ *est intègre et contient* $\tilde{G}$ *comme ouvert dense.*
2. $\tilde{\mathcal{L}}_{\tilde{P}}$ *un faisceau inversible sur* $\tilde{P}$ *dont la restriction à* $\tilde{G}$ *coïncide avec* $\tilde{\mathcal{L}}$.
3. *une action de* $\tilde{G}$ *sur* $(\tilde{P}, \tilde{\mathcal{N}})$*, où* $\tilde{\mathcal{N}} = \tilde{\mathcal{L}}_{\tilde{P}} \otimes \tilde{\pi}^* \mathcal{M}^{-1}$*, qui étend l'action de* $\tilde{G}$ *sur* $(\tilde{G}, \mathcal{O}_{\tilde{G}})$ *par translation.*
4. *une action de* Y *sur* $(\tilde{P}, \tilde{\mathcal{L}}_{\tilde{P}})$ *notée* $(S_y, \tilde{S}_y)$ *qui étend l'action de* Y *sur* $(\tilde{G}_\eta, \tilde{\mathcal{L}}_\eta)$.

vérifiant les conditions suivantes :

1. *il existe un ouvert* U *de* $\tilde{P}$ *qui soit* $\tilde{G}$*-invariant, de type fini sur* S*, et tel que* $\tilde{P} = \cup_{y \in Y} S_y(U)$.
2. $\tilde{\mathcal{L}}_{\tilde{P}}$ *est ample sur* $\tilde{P}$.
3. *condition de complétude : pour une valuation* v *de* $K(\tilde{G})$ *positive sur* R*, on note* x_v *le centre de* v *sur* A*. Alors* v *a un centre sur* $\tilde{P}$ *si et seulement si,* $\forall \mu \in X, \exists y \in Y, v(I_{y,\mu} \mathcal{O}_{\mu, x_v}) \geq 0$.

Définition 10. *Étant donné un morphisme de données de dégénérescences* $\tilde{f} : \tilde{G}_1 \to \tilde{G}_2$*, et* $\tilde{P}_1$ *et* $\tilde{P}_2$ *des modèles relativement complets de* $\tilde{G}_1$ *et* $\tilde{G}_2$ *respectivement, on appelle morphisme de modèles relativement complets un prolongement de* $\tilde{f}$ *(noté toujours* $\tilde{f}$*) en un morphisme entre* $\tilde{P}_1$ *et* $\tilde{P}_2$ *tel que* $f_A \circ \tilde{\pi}_2 = \tilde{\pi}_1 \circ \tilde{f}$*, et* $\tilde{f}$ *commute aux actions de* Y_1 *et* Y_2.

2.4 Compactifications toriques

Pour construire notre modèle relativement complet, nous allons construire une compactification torique Z de T.
Soit T un tore déployé sur S, et X son groupe des caractères, de sorte que $T = \mathrm{Spec} R[\mathcal{X}^\alpha]_{\alpha \in X} / (\mathcal{X}^\alpha \mathcal{X}^\beta - \mathcal{X}^{\alpha+\beta}, \mathcal{X}^0 - 1)$

2.4.1 Décomposition en cônes

Soit Y un groupe abélien libre de rang r. Un cône rationnel polyédral de $Y^*_{\mathbb{R}}$ est un sous-ensemble de $Y^*_{\mathbb{R}}$ qui ne contient pas de droite, et qui peut s'écrire sous la forme $\sigma = \mathbb{R}_+ l_1 + \dots \mathbb{R}_+ l_n$ pour les $l_i \in Y^*$.
Une décomposition d'une partie $\mathcal{C}$ de $Y^*_{\mathbb{R}}$ en cônes rationnels polyédraux, ou éventail, est la donnée d'une famille (éventuellement infinie) $\{\sigma_\alpha\}_{\alpha \in I}$ de cônes rationnels polyédraux de $Y^*_{\mathbb{R}}$ telle que chaque face d'un σ_α est un σ_β pour un

$\beta \in I$, et que l'intersection de deux cônes dans cet ensemble est une face de chacun des deux cônes, et enfin que la réunion de tous les cônes de la famille est égale à $\mathcal{C}$.
Étant donnée une décomposition de $\mathcal{C}$ en cônes, on appelle fonction de support une fonction $\Phi : \mathcal{C} \to \mathbb{R}$ qui soit continue, linéaire par morceaux, prenant des valeurs entières sur $\mathcal{C} \cap Y^*$, et vérifie $\Phi(al) = a\Phi(l)$ pour tout $a \in \mathbb{R}_+, l \in \mathcal{C}$. Une telle fonction est dite strictement convexe si pour tout cône σ de la famille, il existe un entier $\mathbb{N}$ et $y \in Y$ tels que $< y, . >|_{\mathcal{C}} \geq n\Phi$ et $\sigma = \{l \in \mathcal{C}, < y, l >= n\Phi(l)\}$. Une fonction de support qui est strictement convexe et linéaire sur chaque cône de la famille est appelée fonction de polarisation.
Le cône dual $\breve{\sigma}$ est le cône de l'ensemble des éléments de $Y_{\mathbb{R}}$ sur lesquels les éléments de σ prennent des valeurs positives.
Le cône σ est appelé simplexe si on peut choisir les l_i linéairement indépendants. On appelle alors Y^*_σ le sous-groupe de Y^* engendré par les éléments de Y^* qui appartiennent à une face de dimension 1 de σ. On appelle multiplicité de σ l'indice de Y^*_σ dans $Y^* \cap (Y^*_\sigma \otimes_{\mathbb{Z}} \mathbb{Q})$. Un simplexe de multiplicité 1 est dit lisse.

2.4.2 Construction d'immersions toriques

On va appliquer cela à $Y = X^* \times \mathbb{Z} = \tilde{X}$. Soit $\sigma \subset X^*_{\mathbb{R}} \times \mathbb{R}_+$ un cône. On pose $Z(\sigma) = \mathrm{Spec} A_\sigma$, où :

$$A_\sigma = R[\pi^k \mathcal{X}^m]_{(m,k) \in \tilde{X} \cap \breve{\sigma}} / (\mathcal{X}^\alpha \mathcal{X}^\beta - \mathcal{X}^{\alpha+\beta}, \mathcal{X}^0 - 1)$$

Si τ est une face de σ, on a un morphisme naturel $Z(\tau) \to Z(\sigma)$ qui identifie $Z(\tau)$ à un ouvert affine de $Z(\sigma)$.
Étant donnée une décomposition $\{\sigma_\alpha\}$ de $X^*_{\mathbb{R}} \times \mathbb{R}_+$, on en déduit par recollement des immersions correspondant à chaque cône une immersion $T_W \to Z$. On note que $T_W \to T$ correspond au cône $\{0\} \times \mathbb{R}_+$, donc dès que ce cône apparaît dans la décomposition, l'immersion se prolonge en $T \to Z$.
Z est régulier si la décomposition est lisse, et $(Z_0)_{red}$ est un diviseur à croisements normaux stricts.

2.4.3 Construction de faisceaux

Soit φ une fonction de support $\cup_\alpha \sigma_\alpha \to \mathbb{R}$. Alors φ définit un faisceau T-équivariant $\mathcal{F}$ sur Z de la façon suivante. Sur $Z(\sigma)$, on définit le faisceau $\mathcal{F}_\sigma$ comme correspondant au $\Gamma(Z(\sigma), \mathcal{O}_{Z(\sigma)})$-module :

$$\sum_{(m,k) \in \tilde{X}, <(m,k), \_ >|_\sigma \geqslant \varphi|_\sigma} I^k \mathcal{X}^m$$

On dit que le faisceau $\mathcal{F}$ est ample si les sections de $\mathcal{L}^{\otimes n}$, $n \geq 1$, définissent une base de la topologie Zariski de Z. Alors $\mathcal{F}$ est ample si φ est strictement convexe, d'après [Kün98] 1.18.

2.4.4 Fonctorialité

Soit maintenant S' un ouvert affine de S rencontrant S_0, T' le tore sur S' obtenu à partir de T par changement de base. T' ayant même groupe des caractères que T, on peut fabriquer une compactification torique Z' de T' sur S' à partir de la même décomposition en cônes que celle utilisée pour construire Z. Alors on observe que Z' est obtenu à partir de Z par changement de base de S à S'. De même pour les faisceaux inversibles obtenus à partir d'une même fonction de support.

2.4.5 Morphismes entre immersions toriques

Soit T et T' deux tores sur S, g un morphisme de T vers T', $\mathcal{S}$ et $\mathcal{S}'$ deux éventails de $\tilde{X}$ et $\tilde{X}'$ respectivement. Alors g induit un morphisme entre les immersions toriques associées à ces décompositions si et seulement si pour tout $\sigma \in \mathcal{S}$, il existe $\sigma' \in \mathcal{S}'$ tel que $g(\sigma) \subset \sigma'$.

2.5 Choix d'une bonne décomposition

Il s'agit donc maintenant de trouver un bon éventail qui fasse de $\tilde{P} = \tilde{G} \times^T Z$ un modèle relativement complet. L'article [Kün98] fournit une telle décomposition dans le cas où R est un anneau de valuation discrète complet. Expliquons précisément ce que l'on obtient.
On part de

1. X et Y groupes abéliens libres de rang r
2. $\varphi : Y \to X$ morphisme injectif
3. $b : Y \times X \to \mathbb{Z}$ bilinéaire telle que $b(., \varphi(.))$ est symétrique définie positive.
4. $a : Y \to \mathbb{Z}$ telle que $a(0) = 0$ et $a(y + y') - a(y) - a(y') = b(y, \varphi(y'))$.
5. H groupe fini d'automorphismes de (X, Y, φ, a, b) agissant à gauche sur X et à droite sur Y, c'est-à-dire la donnée pour tout h de (h_X, h_Y) tels que $\varphi = h_X \circ \varphi \circ h_Y$, $a \circ h_Y = a$, et $b(h_Y(.), .) = b(., h_X(.))$.

Posons $\Gamma = Y \rtimes H$, la composition étant donnée par :

$$(y, h)(y', h') = (y + h(y'), hh')$$

Alors Γ agit à gauche sur $\tilde{X} = X^* \times \mathbb{Z}$ par :

$$S_{(y,h)}(l, s) = (l \circ h(.) + sb(y, .), s)$$

Notons que $\mathcal{C} = (X^*_{\mathbb{R}} \times \mathbb{R}^*_+) \cup \{0\}$ est stable par l'action de Γ.
On définit la fonction $\chi : \Gamma \times \tilde{X}_{\mathbb{R}} \to \mathbb{R}$ par $\chi((y, h), (l, s)) = sa(y) + l \circ \varphi \circ h^{-1}(y)$.

Définition 11. *On dit qu'un éventail de $\mathcal{C}$ est Γ-admissible si l'ensemble des cônes est Γ-invariant, et qu'il n'y a qu'un nombre fini d'orbites.*

Définition 12. *Soit k un entier > 0. On dit qu'une fonction de polarisation Φ est k-tordue et Γ-admissible si pour tout $\gamma \in \Gamma$, on a $\Phi(.) - \Phi \circ S_\gamma(.) = k\chi(\gamma, .)$.*

Alors la proposition 3.3 de [Kün98] donne le résultat suivant :

Proposition 8. *Il existe un éventail* Γ*-admissible* $\{\sigma_\alpha\}_{\alpha\in I}$ *muni d'une fonction de polarisation* Φ Γ*-admissible et* k*-tordu pour un certain* k*, qui soit lisse, qui contienne le cône* $\sigma_T = \{0\} \times \mathbb{R}_+$*, et qui vérifie* $S_y(\sigma_\alpha) \cap \sigma_\alpha = \{0\}$ *pour tout* $y \in Y \setminus \{0\}$ *et tout* $\alpha \in I$*.*

On dira qu'un tel éventail est convenable. Revenons à notre cas.

Lemme 9. *Il existe un éventail convenable dans* $\tilde{X}$*.*

Démonstration. Soit R' l'anneau local de S au point générique de S_0, et $I' = IR'$. Alors R' est un anneau de valuation discrète complet d'idéal maximal I'. Soit G' déduit de G par changement de base de S à $S' = \mathrm{Spec} R'$, et T' son tore, alors T' est aussi déduit de T par ce changement de base, ils ont donc même groupe de caractères X. On peut donc utiliser les résultats de [Kün98] pour mettre sur $\tilde{X}$ un éventail convenable. □

Remarque 2. Si (X, Y, φ, a, b) provient de $(G, \mathcal{L}, \mathcal{M})$, alors pour un entier $k > 0$, c'est $(X, Y, k\varphi, ka, b)$ qui est associé à $(G, \mathcal{L}^{\otimes k}, \mathcal{M}^{\otimes k})$. Supposons que l'on ait trouvé pour (X, Y, φ, a, b) une décomposition de $\mathcal{C}$ avec une fonction de polarisation Φ qui soit k-tordue, alors cette même fonction est 1-tordue pour $(X, Y, k\varphi, ka, b)$. Ainsi, quitte à remplacer $\mathcal{L}$ et $\mathcal{M}$ par une certaine puissance, on peut toujours supposer qu'on a associé à (X, Y, φ, a, b) une décomposition munie d'une fonction de polarisation 1-tordue.

Intéressons-nous maintenant au cas d'un morphisme $f : G_1 \to G_2$ H-équivariant. f induit donc des morphismes $f_Y : Y_1 \to Y_2$, et $f_X : X_2 \to X_1$ commutant à l'action de H, d'où $f_{\tilde{X}} : \tilde{X}_1 \to \tilde{X}_2$. Comme f_η est une isogénie, f_X et f_Y sont des injections.
Fixons un éventail convenable de $\tilde{X}_2$. On veut trouver un éventail convenable de $\tilde{X}_1$ vérifiant la condition énoncée en 2.4.5, de façon à obtenir $Z_1 \to Z_2$ prolongeant $T_1 \to T_2$. Considérons les images réciproques des cônes constituant l'éventail de $\tilde{X}_2$. Comme f induit une injection de conoyau fini de X_2 dans X_1, on peut identifier $\tilde{X}_1$ à $\tilde{X}_2$ muni d'une structure entière plus fine (c'est-à-dire $X_1^* \times \mathbb{Z} \subset X_2^* \times \mathbb{Z}$). L'éventail construit pour $\tilde{X}_2$ forme donc un éventail pour $\tilde{X}_1$, qui est convenable sauf qu'il peut ne pas être lisse. Il suffit donc de prendre un raffinement de cet éventail pour obtenir un éventail dans $\tilde{X}_1$ qui soit convenable et lisse.
Deux tels éventails seront dits compatibles.

2.6 Obtention d'un modèle relativement complet

On prend ensuite la compactification torique Z de T obtenue à partir de cette décomposition de X, et on fait le produit contracté de cette compactification avec $\tilde{G}$, c'est-à-dire $\tilde{P} = \tilde{G} \times^T Z$. Autrement dit $\tilde{P}$ est obtenu en recollant les $\tilde{P}(\sigma_\alpha) = \tilde{G} \times^T Z(\sigma_\alpha)$.

On obtient ainsi un modèle relativement complet de $\tilde{G}$, et muni d'une action de H. La vérification est identique à celle de l'article [Kün98], paragraphe 3.7. Nous avons ainsi construit $(\tilde{P}, \tilde{\mathcal{L}}_{\tilde{P}})$ dont le quotient donnera une compactification équivariante de $(G, \mathcal{L})$.
Soit $f : G_1 \to G_2$ H-équivariant, et deux éventails compatibles de $\tilde{X}_1$ et $\tilde{X}_2$, alors f induit un morphisme entre les modèles relativement complets associés aux éventails.

2.7 Du modèle relativement complet à la compactification

Le passage du modèle relativement complet à la compactification est décrit dans [CF90]. Rappelons-en le principe.
Soit $\tilde{P}_n$ le changement de base de $\tilde{P}$ à S_n (notation définie au début du paragraphe 2). Alors il existe un morphisme étale surjectif $\pi_n : \tilde{P}_n \to P_n$ tel que P_n soit un quotient de $\tilde{P}_n$ sous l'action de Y comme faisceau fpqc. $\tilde{\mathcal{L}}_n$ se descend en un faisceau ample $\mathcal{L}_n$ sur P_n.
En effet, il existe un ensemble fini $E \subset Y$ tel que pour tout y hors de E, on ait $S_y(U_0) \cap U_0 = \emptyset$, où $U_0 = U \times_S S_0$ (cela se déduit des propriétés du modèle relativement complet, et dans notre cas cela se verra directement sur la construction), autrement dit Y agit librement sur $\tilde{P}_0$. Alors on définit facilement le quotient P'_n de $\tilde{P}_n$ par mY pour un m assez grand. Ensuite, Y/mY agit librement sur P'_n qui est projectif donc on peut définir le quotient P_n.
Les $(P_n, \mathcal{L}_n)$ forment un système projectif, d'où $(P_{for}, \mathcal{L}_{for})$ avec $\mathcal{L}_{for}$ ample sur P_{for}. $(P_{for}, \mathcal{L}_{for})$ s'algébrise en $(P, \mathcal{L}_P)$, avec $\mathcal{L}_P$ ample sur P.
P est régulier et plat sur S, car c'est le cas pour $\tilde{P}$ (voir [Kün98], proposition 2.15).
Il s'agit ensuite de vérifier que P_0 est bien un diviseur à croisements normaux dans P. $\tilde{P}$ est muni d'une stratification, car c'est une immersion torique, chaque cône de l'éventail correspondant à une strate, et $\tilde{P}_0$ est un diviseur à croisements normaux dans $\tilde{P}$ parce qu'on a supposé l'éventail lisse. Lorsque on passe au quotient cette propriété est préservée, de plus l'hypothèse que $S_y(\sigma_\alpha) \cap \sigma_\alpha = \{0\}$ pour tout $y \in Y \setminus \{0\}$ et tout $\alpha \in I$ assure que P_0 est muni d'une stratification indexée par les orbites de Y dans l'ensemble des cônes, de sorte que $(P_0)_{red}$ est un diviseur à croisements normaux stricts.
P est alors une compactification de G, ce qui prouve le théorème 5.
D'autre part, si $\tilde{f} : \tilde{P}_1 \to \tilde{P}_2$ est un morphisme de modèles relativement complets, f passe au quotient (car on a supposé que $\tilde{f}$ commutait à l'action de Y_1 et Y_2), et on obtient $\bar{f} : P_1 \to P_2$ prolongeant $f : G_1 \to G_2$. Ainsi on a prouvé le théorème 6.

3 Recollements

Il s'agit maintenant d'utiliser divers théorèmes de descente pour montrer que l'existence de compactifications dans le cas d'une base complète, avec une extension déployée, suffit à obtenir l'existence de compactifications dans le cas général. La partie difficile est de redescendre les objets, ensuite les morphismes descendent automatiquement aussi, donc le théorème 2 va apparaître naturellement comme conséquence de la fin de la preuve du théorème 1.

3.1 Cas non affine

Proposition 10. *Supposons que S est complet par rapport à S_0 et que $(G, \mathcal{L})$ forme une dégénérescence déployée $(G, \mathcal{L}, \mathcal{M})$. Supposons de plus que nous avons une action d'un groupe fini H sur S et sur $(G, \mathcal{L}, \mathcal{M})$, telle que S peut être recouvert par des ouverts affines stables par H. Alors il existe des compactifications équivariantes.*

Démonstration. Pour chaque ouvert affine de S stable par H rencontrant S_0, on peut faire la compactification localement par la méthode expliquée précédemment. Les compactifications locales obtenues sont compatibles car elles proviennent de la même décomposition de X (car tous les ouverts affines considérés contiennent le point générique de S_0).
La condition d'être un diviseur à croisement normaux et la condition de propreté étant locales sur la base, le recollement des compactifications est bien une compactification. □

3.2 Cas où l'extension n'est pas déployée

Proposition 11. *Supposons S complet par rapport à S_0. Alors il existe des compactifications.*

Démonstration. Il existe une extension finie étale S' de S telle que $(G', \mathcal{L}', \mathcal{M}')$ sur S' déduite de celle sur S soit déployée. On peut supposer que $S' \xrightarrow{u} S$ est galoisienne.
Soit H le groupe de Galois de S' sur S. Soit S'_0 la préimage de S_0 par u.
Supposons d'abord que S'_0 est irréductible. Le groupe H agit sur la dégénérescence $(G', \mathcal{L}', \mathcal{M}')$ par son action sur S'. Observons que u est affine puisque finie. En particulier, la préimage d'un ouvert affine de S est un ouvert affine de S' stable par H. On peut donc appliquer le résultat du paragraphe 3.1 à S', S'_0 et H. On obtient une compactification sur S' munie de l'action du groupe de Galois, ce qui constitue une donnée de descente. Comme on cherche à redescendre un schéma P' qui est quasi-compact sur S' et muni d'un faisceau inversible ample $\mathcal{L}'$, on est dans une situation où toute donnée de descente est effective. On peut donc redescendre P' en un P sur S (cf.[BLR90]).
Comme P' se déduit de P par un changement de base fini, P est propre sur S si et seulement si P' est propre sur S'. D'autre part P' étant étale sur P, et $(P'_0)_{red}$ étant un diviseur à croisements normaux stricts dans P', P_0 est un diviseur à croisements normaux dans P.
Dans le cas où S'_0 n'est pas irréductible, notons que pour S' (et aussi pour S'_0) les composantes irréductibles correspondent aux composantes connexes, du fait de la propriété de régularité. D'autre part, S' étant complet par rapport à S'_0,

chaque composante connexe de S' contient exactement une composante connexe de S'_0. Alors n'importe quelle composante connexe de S' est une extension galoisienne de S, on est donc ramené au cas précédent. $\square$

3.3 Cas où la base n'est pas complète

Pour finir la preuve du théorème 1, il nous faut regarder le cas où S n'est pas nécessairement complet.
On rappelle le résultat suivant ([BL95]) :

Théorème. *Soit A un anneau, f un élément simplifiable de A, F un A_f-module, G un $\hat{A}$-module f-régulier, un isomorphisme $\hat{A}_f$-linéaire $\varphi : \hat{A} \otimes_A F \to G_f$.*
Il existe alors un A-module f-régulier M et des isomorphismes $\alpha : M_f \to F$ et $\beta : \hat{A} \otimes_A M \to G$ tels que φ soit l'application composée $\beta_f \circ (1 \otimes \alpha^{-1})$.
Le triplet (M, α, β) est unique à isomorphisme unique près.
Si F est plat sur A_f et G plat sur $\hat{A}$, alors M est plat sur A.

Par unicité de M, ce théorème s'étend en une situation globale sur S, donnant un théorème de descente pour les faisceaux quasi-cohérents vérifiant les conditions sur la torsion, donc en particulier pour les faisceaux plats sur S. D'où un théorème de descente pour les schémas plats munis d'un faisceau ample.
Soit $(\hat{G}, \hat{\mathcal{L}})$ obtenu par changement de base au complété $\hat{S}$ de S par rapport à S_0. D'après la proposition 11, il existe une compactification $(\hat{P}, \hat{\mathcal{L}}_P)$ de $(\hat{G}, \hat{\mathcal{L}})$, où $\hat{\mathcal{L}}_p$ prolonge $\hat{\mathcal{L}}^{\otimes k}$. $(\hat{P}, \hat{\mathcal{L}}_P)$ et $(G_{|W}, \mathcal{L}_{|W}^{\otimes k})$ deviennent isomorphes après passage à $\hat{S} \times_S W$, et $\hat{P}$ est plat sur $\hat{S}$, on déduit du résultat de [BL95] l'existence d'un $(P, \mathcal{L}_P)$ sur S, dont nous allons montrer que c'est une compactification de $(G, \mathcal{L})$.

Lemme 12. *P_0 est un diviseur à croisement normaux dans P.*

Démonstration. Cette condition se lit sur les anneaux locaux des points de P au-dessus de S_0. Soit x un point de $P_0 = \hat{P}_0$ au-dessus du point $s \in S_0$. Alors $\mathcal{O}_{\hat{P},x} = \mathcal{O}_{P,x} \otimes_{\mathcal{O}_{S,s}} \mathcal{O}_{\hat{S},s}$. Comme $\mathcal{O}_{\hat{S},s}$ est le complété de $\mathcal{O}_{S,s}$ selon un certain idéal, les anneaux locaux $\mathcal{O}_{\hat{P},x}$ et $\mathcal{O}_{P,x}$ ont même complété. La régularité de l'un est donc équivalent à la régularité de l'autre. D'autre part la propriété d'être réduit et les propriétés de dimension sont clairement conservées. $\square$

Lemme 13. *P est propre sur S.*

Démonstration. Il s'agit du corollaire 4.8 de l'exposé VIII de [Gro70] : la descente fpqc conserve la propreté, or $\hat{P}$ est propre sur $\hat{S}$ et $G_{|W}$ est propre sur W. $\square$

Ainsi $(P, \mathcal{L}_P)$ vérifie toutes les conditions nécessaires pour être une compactification de $(G, \mathcal{L})$. Une telle compactification existe donc bien.

Références

[BL95] Arnaud Beauville and Yves Laszlo, *Un lemme de descente*, C. R. Acad. Sci. Paris Sér. I Math. 320 (1995), 335–340.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron Models*, Springer-Verlag, 1990.

[CF90] Ching-Li Chai and Gerd Faltings, *Degeneration of Abelian Varieties*, Springer-Verlag, 1990.

[D$^+$70] Michel Demazure et al., *SGA 3/2*, Lecture Notes in Mathematics, vol. 152, Springer-Verlag, 1970.

[Gro70] Alexander Grothendieck, *SGA 1*, Lecture Notes in Mathematics, vol. 224, Springer-Verlag, 1970.

[Kün98] Klaus Künnemann, *Projective regular models for abelian varieties, semistable reduction, and the height pairing*, Duke Math. J. 95 (1998), 161–212.

[Mor85] Laurent Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérisque 129 (1985), 1–266.

[Mum72] David Mumford, *An analytic construction of degenerating abelian varieties over a complete local ring*, Compos. Math. 24 (1972), 239–272.

[Ray70] Michel Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes*, Lecture Notes in Mathematics, vol. 119, Springer-Verlag, 1970.

Sandra Rozensztajn
LAGA, Institut Galilée
Université Paris 13
99 avenue J.-B. Clément, 94340
Villetaneuse, France
rozenszt@math.univ-paris13.fr

On the Equivariant Tamagawa Number Conjecture for Abelian Extensions of a Quadratic Imaginary Field

W. Bley

Received: October 17, 2005

Communicated by Peter Schneider

Abstract. Let k be a quadratic imaginary field, p a prime which splits in $k/\mathbb{Q}$ and does not divide the class number h_k of k. Let L denote a finite abelian extension of k and let K be a subextension of L/k. In this article we prove the p-part of the Equivariant Tamagawa Number Conjecture for the pair $(h^0(\mathrm{Spec}(L)), \mathbb{Z}[\mathrm{Gal}(L/K)])$.

2000 Mathematics Subject Classification: 11G40, 11R23, 11R33, 11R65

Keywords and Phrases: L-functions, Iwasawa theory, Euler systems

1 Introduction

The aim of this paper is to provide new evidence for the validity of the Equivariant Tamagawa Number Conjectures (for short ETNC) as formulated by Burns and Flach in [4]. We recall that these conjectures generalize and refine the Tamagawa Number Conjectures of Bloch, Kato, Fontaine, Perrin-Riou et al. In the special case of the untwisted Tate motive the conjecture also refines and generalizes the central conjectures of classical Galois module theory as developed by Fröhlich, Chinburg, Taylor et al (see [2]). Moreover, in many cases it implies refinements of Stark-type conjectures formulated by Rubin and Popescu and the 'refined class number formulas' of Gross. For more details in this direction see [3].

Let k denote a quadratic imaginary field. Let L be a finite abelian extension of k and let K be any subfield of L/k. Let p be a prime number which does not divide the class number h_k of k and which splits in $k/\mathbb{Q}$. Then we prove the 'p-part' of the ETNC for the pair $(h^0(\mathrm{Spec}(L), \mathbb{Z}[\mathrm{Gal}(L/K)]))$ (see Theorem 4.2).

To help put the main result of this article into context we recall that so far the ETNC for Tate motives has only been verified for abelian extensions of the rational numbers $\mathbb{Q}$ and certain quaternion extensions of $\mathbb{Q}$. The most important result in this context is due to Burns and Greither [5] and establishes the validity of the ETNC for the pair $(h^0(\mathrm{Spec}(L)(r), \mathbb{Z}[\frac{1}{2}][\mathrm{Gal}(L/K)]))$, where $L/\mathbb{Q}$ is abelian, $\mathbb{Q} \subseteq K \subseteq L$ and $r \le 0$. The 2-part was subsequently dealt with by Flach [8], who also gives a nice survey on the general theory of the ETNC, including a detailed outline of the proof of Burns and Greither. Shortly after Burns and Greither, the special case $r = 0$ was independently shown (up to the 2-part) by Ritter and Weiss [22] using different methods.

In order to prove our main result we follow very closely the strategy of Burns and Greither, which was inspired by previous work of Bloch, Kato, Fontaine and Perrin-Riou. In particular, in [13] Kato formulates a conjecture whose proof is one of the main achievements in the work of Burns and Greither.

Roughly speaking, we will replace cyclotomic units by elliptic units. More concretely, the ETNC for the pair $(h^0(\mathrm{Spec}(L), \mathbb{Z}[\mathrm{Gal}(L/K)]))$ conjecturally describes the leading coefficient in the Laurant series of the equivariant Dirichlet L-function at $s = 0$ as the determinant of a canonical complex. By Kronecker's limit formula we replace L-values by sums of logarithms of elliptic units. In this formulation we may pass to the limit along a $\mathbb{Z}_p$-extension and recover (an analogue) of a conjecture which was formulated by Kato in [13]. As in [5] we will deduce this limit conjecture from the Main Conjecture of Iwasawa Theory and the triviality of certain Iwasawa μ-invariants (see Theorem 5.1). Combining the validity of the limit theorem with Iwasawa-theoretic descent considerations we then achieve the proof of our main result.

The Main Conjecture in the elliptic setting was proved by Rubin in [24], but only in semi-simple case (i.e. $p \nmid [L : k]$). Following Greither's exposition [10] we adapt Rubin's proof and obtain the full Main Conjecture (see Theorem 3.1) for ray class fields L and primes p which split in $k/\mathbb{Q}$ and do not divide the class number h_k of k.

The triviality of μ-invariants in the elliptic setting is known from work of Gillard [9], but again only in the ordinary case when p is split in $k/\mathbb{Q}$.

The descent considerations are particularly involved in the presence of 'trivial zeros' of the associated p-adic L-functions. In this case we make crucial use of a recently published result of the author [1] concerning valuative properties of certain elliptic p-units.

As in the cyclotomic case it is possible to use the Iwasawa-theoretic result of Theorem 5.1 and Iwasawa descent to obtain the p-part of the ETNC for $(h^0(\mathrm{Spec}(L)(r), \mathbb{Z}[\mathrm{Gal}(L/K)]))$, $r < 0$. We refer to thesis of Johnson [12] who deals with this case.

We conclude this introduction with some remarks on the non-split situation. Generically this case is more complicated because the corresponding Iwasawa extension is of type $\mathbb{Z}_p^2$. The main issue, if one tries to apply the above described strategy in the non-split case, is to prove $\mu = 0$. Note that we already use the triviality of μ in our proof of the Iwasawa Main Conjecture (see Remark 3.9).

During the preparation of this manuscript I had the pleasure to spend three months at the department of mathematics in Besançon and three weeks at the department of mathematics at Caltech, Pasadena. My thanks go to the algebra and number theory teams at both places for their hospitality and the many interesting mathematical discussions.

2 Elliptic units

The aim of this section is to define the elliptic units that we will use in this paper. Our main references are [20], [21] and [1].
We let $L \subseteq \mathbb{C}$ denote a $\mathbb{Z}$-lattice of rank 2 with complex multiplication by the ring of integers of a quadratic imaginary field k. We write $N = N_{k/\mathbb{Q}}$ for the norm map from k to $\mathbb{Q}$. For any $\mathcal{O}_k$-ideal $\mathfrak{a}$ satisfying $(N(\mathfrak{a}), 6) = 1$ we define a meromorphic function

$$\psi(z; L, \mathfrak{a}) := \tilde{F}(z; L, \mathfrak{a}^{-1}L), \quad z \in \mathbb{C},$$

where $\tilde{F}$ is defined in [20, Théorème principale, (15)]. This function ψ coincides with the function $\theta(z; \mathfrak{a})$ used by Rubin in [23, Appendix] and it is a canonical 12th root of the function $\theta(z; L, \mathfrak{a})$ defined in [6, II.2].
The basic arithmetical properties of special values of ψ are summarized in [1, §2].
We choose a $\mathbb{Z}$-basis w_1, w_2 of the complex lattice L such that $\mathrm{Im}(w_1/w_2) > 0$ and write $\eta(\tau)$, $\mathrm{Im}(\tau) > 0$, for the Dedekind η-function. Let η_1, η_2 denote the quasi-periods of the Weierstrass ζ-function and for any $z = a_1w_1 + a_2w_2 \in \mathbb{C}, a_1, a_2 \in \mathbb{R}$, put $z^* = a_1\eta_1 + a_2\eta_2$. Writing $\sigma(z; L)$ for the Weierstrass σ-function attached to L we define

$$\varphi(z; w_1, w_2) := 2\pi i e^{-zz^*/2}\sigma(z; L)\eta^2\left(\frac{w_1}{w_2}\right) w_2^{-1}. \tag{1}$$

Note that φ is exactly the function defined in [20, (4)]. The function φ is not a function of lattices but depends on the choice of a basis w_1, w_2. Its 12th power does not depend on this choice and we will also write $\varphi^{12}(z; L)$. We easily deduce from [20, Sec. 3, Lemme] and its proof that the relation between φ and ψ is given by

$$\psi^{12}(z; L, \mathfrak{a}) = \frac{\varphi^{12N(\mathfrak{a})}(z; L)}{\varphi^{12}(z; \mathfrak{a}^{-1}L)}. \tag{2}$$

3 The Iwasawa main conjecture

For any $\mathcal{O}_k$-ideal $\mathfrak{b}$ we write $k(\mathfrak{b})$ for the ray class field of conductor $\mathfrak{b}$. In this notation $k(1)$ denotes the Hilbert class field. We let $w(\mathfrak{b})$ denote the number of roots of unity in k which are congruent to 1 modulo $\mathfrak{b}$. Hence $w(1)$ is the number of roots of unity in k. This number will also be denoted by w_k.

Let p denote an odd rational prime which splits in $k/\mathbb{Q}$, and let $\mathfrak{p}$ be a prime ideal of k lying over p. We assume $p \nmid h_k$. For each $n \geq 0$ we write

$$\mathrm{Gal}(k(\mathfrak{p}^{n+1})/k) = \mathrm{Gal}(k(\mathfrak{p}^{n+1})/k(\mathfrak{p})) \times H,$$

where H is isomorphic to $\mathrm{Gal}(k(\mathfrak{p})/k)$ by restriction. We set

$$k_n := k(\mathfrak{p}^{n+1})^H, \quad k_\infty := \bigcup_{n\geq 0} k_n,$$

and note that k_∞/k is a $\mathbb{Z}_p$-extension. More precisely, k_∞/k is the unique $\mathbb{Z}_p$-extension of k which is unramified outside $\mathfrak{p}$. The prime $\mathfrak{p}$ is totally ramified in k_∞/k.

Let now $\mathfrak{f}$ be any integral ideal of k such that $(\mathfrak{f}, \mathfrak{p}) = 1$. Let $F = k(\mathfrak{f}\mathfrak{p})$ denote the ray class field of conductor $\mathfrak{f}\mathfrak{p}$. We set $K_n := Fk_n = k(\mathfrak{f}\mathfrak{p}^{n+1})$ and $K_\infty := \cup_{n\geq 0} K_n$. Then K_∞/K_0 is a $\mathbb{Z}_p$-extension in which each prime divisor of $\mathfrak{p}$ is totally ramified.

For any number field L we denote the p-part of the ideal class group of L by $A(L)$. Set $A_\infty := \varprojlim_n A(K_n)$, the inverse limit formed with respect to the norm maps. We write $\mathcal{E}_n$ for the group of global units of K_n. For a divisor $\mathfrak{g}$ of $\mathfrak{f}$ we let $\mathcal{C}_{n,\mathfrak{g}}$ denote the subgroup of primitive Robert units of conductor $\mathfrak{f}\mathfrak{p}^{n+1}$, $n \geq 0$. If $\mathfrak{g} \neq (1)$, then $\mathcal{C}_{n,\mathfrak{g}}$ is generated by all $\psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a})$ with $(\mathfrak{a}, \mathfrak{g}\mathfrak{p}) = 1$ and the roots of unity in K_n. If $\mathfrak{g} = (1)$, then the elements $\psi(1; \mathfrak{p}^{n+1}, \mathfrak{a})$ are no longer units. By [1, Th. 2.4] a product of the form $\prod \psi(1; \mathfrak{p}^{n+1}, \mathfrak{a})^{m(\mathfrak{a})}$ is a unit, if and only if $\sum m(\mathfrak{a})(N(\mathfrak{a}) - 1) = 0$. We let $\mathcal{C}_{n,\mathfrak{g}}$ denote the group generated by all such products and the roots of unity in K_n. We let $\mathcal{C}_n$ be the group of units generated by the subgroups $\mathcal{C}_{n,\mathfrak{g}}$ with $\mathfrak{g}$ running over the divisors of $\mathfrak{f}$.

We let U_n denote the semi-local units of $K_n \otimes_k k_\mathfrak{p}$ which are congruent to 1 modulo all primes above $\mathfrak{p}$, and let $\bar{\mathcal{E}}_n$ and $\bar{\mathcal{C}}_n$ denote the closures of $\mathcal{E}_n \cap U_n$ and $\mathcal{C}_n \cap U_n$, respectively, in U_n. Finally we define

$$\bar{\mathcal{E}}_\infty := \varprojlim_n \bar{\mathcal{E}}_n, \quad \bar{\mathcal{C}}_\infty := \varprojlim_n \bar{\mathcal{C}}_n,$$

both inverse limits formed with respect to the norm maps.

We let

$$\Lambda = \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(K_n/k)]$$

denote the completed group ring and for a finitely generated Λ-module and any abelian character χ of $\Delta := \mathrm{Gal}(K_0/k)$ we define the χ-quotient of M by

$$M_\chi := M \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi),$$

where $\mathbb{Z}_p(\chi)$ denotes the ring extension of $\mathbb{Z}_p$ generated by the values of χ. For the basic properties of the functor $M \mapsto M_\chi$ the reader is referred to [30, §2]. The ring Λ_χ is (non-canonically) isomorphic to the power series ring $\mathbb{Z}_p(\chi)[[T]]$. If M_χ is a finitely generated torsion Λ_χ-module, then we write $\mathrm{char}(M_\chi)$ for the characteristic ideal.

Theorem 3.1 *Let p be an odd rational prime which splits into two distinct primes in $k/\mathbb{Q}$. Then*

$$\mathrm{char}(A_{\infty,\chi}) = \mathrm{char}((\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty)_\chi).$$

Remarks 3.2 a) If $p \nmid [F:k]$ and p does not divide the number of roots of unity in $k(1)$, then the result of Theorem 3.1 is already proved by Rubin, see [24, Th. 4.1(i)].
b) The Main Conjecture of Iwasawa theory for abelian extensions of $\mathbb{Q}$ was first proved by Mazur and Wiles [16] using deep methods from algebraic geometry. They proved the version which identifies the characteristic power series of the projective limit over the p-class groups with a p-adic L-function. These methods were further developed by Wiles [32] who in 1990 established the Main Conjecture for $p \neq 2$ and Galois extensions L/K of a totally real base field K. Under the condition that $p \nmid |\mathrm{Gal}(L/\mathbb{Q})|$ the result of Mazur and Wiles implies a second version of the Main Conjecture where the p-adic L-function is replaced by the characteristic power series of "units modulo cyclotomic units". It is this version which is needed in the context of this manuscript.
Due to work of Kolyvagin and Rubin there is a much more elementary proof of the Main Conjecture for abelian extension $L/\mathbb{Q}$ with $p \nmid |\mathrm{Gal}(L/\mathbb{Q})|$. This approach uses the Euler system of cyclotomic units. Replacing cyclotomic units by elliptic units (amongst many other things) Rubin achieves the result mentioned in part a) of this remark.
In 1992 Greither [10] refined the method of Rubin and used the Euler system of cyclotomic units to give an elementary (but technical) proof of the second version of the Main Conjecture for $L/\mathbb{Q}$ abelian and all primes p. Our proof of Theorem 3.1 will closely follow Greither's exposition.
Finally we mention recent work of Huber and Kings [11]. They apply the machinery of Euler systems and simultaneously prove the Main Conjecture and the Bloch-Kato conjecture for all primes $p \neq 2$ and all abelian extensions $L/\mathbb{Q}$.

The rest of this section is devoted to the proof of Theorem 3.1. Let $\mathcal{C}(\mathfrak{f})$ denote the Iwasawa module of elliptic units as defined in [6, III.1.6]. Then $\mathcal{C}(\mathfrak{f}) \subseteq \bar{\mathcal{C}}_\infty$, so that $\mathrm{char}((\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty)_\chi)$ divides $\mathrm{char}((\bar{\mathcal{E}}_\infty/\mathcal{C}(\mathfrak{f}))_\chi)$. By [6, III.2.1, Theorem] it suffices to show that $\mathrm{char}(A_{\infty,\chi})$ divides $\mathrm{char}((\bar{\mathcal{E}}_\infty/\mathcal{C}(\mathfrak{f}))_\chi)$ for all characters χ of $\Delta = \mathrm{Gal}(K_0/k)$ in order to prove the equality $\mathrm{char}(A_{\infty,\chi}) = \mathrm{char}((\bar{\mathcal{E}}_\infty/\mathcal{C}(\mathfrak{f}))_\chi)$. Hence it is enough for us to prove

$$\mathrm{char}(A_{\infty,\chi}) \text{ divides } \mathrm{char}((\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty)_\chi) \tag{3}$$

for all characters χ of Δ.
For an abelian character χ of Δ we write

$$e_\chi := \frac{1}{|\Delta|}\sum_{\delta\in\Delta}\mathrm{Tr}(\chi(\delta))\delta^{-1}$$

for the idempotent of $\mathbb{Q}_p[\Delta]$ corresponding to χ with Tr denoting the trace map from $\mathbb{Z}_p(\chi)$ to $\mathbb{Z}_p$. We also set $\mathrm{Tr}_\Delta = \sum_{\delta\in\Delta}\delta$.
For any $\mathbb{Z}_p[\Delta]$-module M we have an epimorphism

$$M_\chi = M\otimes_{\mathbb{Z}_p[\Delta]}\mathbb{Z}_p(\chi) \longrightarrow |\Delta|e_\chi M, \quad m\otimes\alpha \mapsto |\Delta|\lambda_\alpha e_\chi m,$$

where $\lambda_\alpha \in \mathbb{Z}_p[\Delta]$ is an element which maps to α under $\mathbb{Z}_p[\Delta] \to \mathbb{Z}_p(\chi)$. If Z denotes the kernel, then it is easily seen that $|\Delta|Z = 0$.
Let now $M = A_\infty$ and $\chi = 1$. Then

$$Z \longrightarrow A_{\infty,\chi} \longrightarrow \mathrm{Tr}_\Delta A_\infty \longrightarrow 0$$

is exact. Since $\mathrm{Tr}_\Delta A_n$ is contained in the p-Sylow subgroup of the ideal class group of k_n, which is trivial by our assumption $p \nmid h_k$ and [31, Th. 10.4], we see that $A_{\infty,\chi}$ is annihilated by $|\Delta|$. By the main result of [9] the Iwasawa μ-invariant of $A_{\infty,\chi}$ is trivial. From this we deduce $\mathrm{char}(A_{\infty,\chi}) = (1)$, thus establishing (3) for the trivial character.

The rest of this section is devoted to the proof of the divisibility relation (3) for non-trivial characters χ. As already mentioned we will closely follow Greither's exposition [10]. Whenever there are only minor changes we shall be very brief, but emphasize those arguments which differ from the cyclotomic situation.
To see the Euler system method applied in an easy setting the reader is advised to have a look at [26]. The strategy of the proof of our Theorem 3.1 is essentially the same, but there are additional difficulties because we allow p to divide $|\Delta|$. If $p \nmid |\Delta|$, the functor $M \mapsto M_\chi$ is exact and the Euler system machinery directly produces a divisibility result of the form $\mathrm{char}(A_{\infty,\chi}) \mid \mathrm{char}((\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty)_\chi)$. If $p \mid |\Delta|$, the functor $M \mapsto M_\chi$ is no longer exact, but Greither's paper [10] shows how to adapt the Euler system method to produce a weaker divisibility relation of the form $\mathrm{char}(A_{\infty,\chi}) \mid \eta\,\mathrm{char}((\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty)_\chi)$ with an additional factor $\eta \in \Lambda_\chi$which is essentially a product of powers of p and $\gamma-1$. Because of Lemma 3.7 and the triviality of the μ-invariant of $A_{\infty,\chi}$, the factor η is coprime with $\mathrm{char}(A_{\infty,\chi})$, so that we again derive a clean divisibility result as in the case $p \nmid |\Delta|$.
We will need some notation from Kolyvagin's theory. Let M be a large power of p and define $\mathcal{L} = \mathcal{L}_{F,M}$ to be the set of all primes $\mathfrak{l}$ of k satisfying

$$\begin{aligned} (i) &\qquad \mathfrak{l} \text{ splits completely in } F/k,\\ (ii) &\qquad N_{k/\mathbb{Q}}(\mathfrak{l}) \equiv 1 (\mathrm{mod}\ M). \end{aligned}$$

By [24, Lem. 1.1] there exists a unique extension $F(\mathfrak{l})$ of F of degree M in $Fk(\mathfrak{l})$. Further $F(\mathfrak{l})/F$ is cyclic, totally ramified at all primes above $\mathfrak{l}$ and unramified at all other primes.
We write $J = \oplus_\lambda \mathbb{Z}\lambda$ for the group of fractional ideals of F and for every prime $\mathfrak{l}$ of k we let $J_\mathfrak{l} = \oplus_{\lambda|\mathfrak{l}}\mathbb{Z}\lambda$ denote the subgroup of J generated by the prime divisors of $\mathfrak{l}$. If $y \in F^\times$ we let $(y)_\mathfrak{l} \in J_\mathfrak{l}$ denote the support of the principal ideal $(y) = y\mathcal{O}_F$ above $\mathfrak{l}$. Analogously we write $[y] \in J/MJ$ and $[y]_\mathfrak{l} \in J_\mathfrak{l}/MJ_\mathfrak{l}$.

For $\mathfrak{l} \in \mathcal{L}$ we let

$$\varphi_{\mathfrak{l}} : \frac{(\mathcal{O}_F/\mathfrak{l}\mathcal{O}_F)^\times}{\left((\mathcal{O}_F/\mathfrak{l}\mathcal{O}_F)^\times\right)^M} \longrightarrow J_{\mathfrak{l}}/MJ_{\mathfrak{l}}$$

denote the $\mathrm{Gal}(F/k)$-equivariant isomorphism defined by [24, Prop. 2.3]. For every $\mathfrak{l} \in \mathcal{L}$ we also write $\varphi_{\mathfrak{l}}$ for the induced map

$$\varphi_{\mathfrak{l}} : \{y \in F^\times / \left(F^\times\right)^M : [y]_{\mathfrak{l}} = 0\} \longrightarrow J_{\mathfrak{l}}/MJ_{\mathfrak{l}}, \quad y \mapsto \varphi_{\mathfrak{l}}(u),$$

where $y = z^M u, z \in F^\times$, u a unit at all places above $\mathfrak{l}$.
We write $\mathcal{S} = \mathcal{S}_{F,M}$ for the set of squarefree integral ideals of k which are only divisible by primes $\mathfrak{l} \in \mathcal{L}$. If $\mathfrak{a} \in \mathcal{S}$, $\mathfrak{a} = \prod_{i=1}^k \mathfrak{l}_i$, we write $F(\mathfrak{a})$ for the compositum $F(\mathfrak{l}_1)\cdots F(\mathfrak{l}_k)$ and $F(\mathcal{O}_k) = F$. For every ideal $\mathfrak{g}$ of $\mathcal{O}_k$ let $\mathcal{S}(\mathfrak{g}) \subseteq \mathcal{S}$ be the subset $\{\mathfrak{a} \in \mathcal{S} : (\mathfrak{a}, \mathfrak{g}) = 1\}$. We write $\bar{F}$ for the algebraic closure of F and let $\mathcal{U}(\mathfrak{g})$ denote the set of all functions

$$\alpha : \mathcal{S}(\mathfrak{g}) \longrightarrow \bar{F}^\times$$

satisfying the properties (1a)-(1d) of [24]. Any such function will be called an Euler system. Define $\mathcal{U}_F = \mathcal{U}_{F,M} = \coprod \mathcal{U}(\mathfrak{g})$. For $\alpha \in \mathcal{U}_F$ we write $\mathcal{S}(\alpha)$ for the domain of α, i.e. $\mathcal{S}(\alpha) = \mathcal{S}(\mathfrak{g})$ if $\alpha \in \mathcal{U}(\mathfrak{g})$.
Given any Euler system $\alpha \in \mathcal{U}_F$, we let $\kappa = \kappa_\alpha : \mathcal{S}(\alpha) \longrightarrow F^\times / \left(F^\times\right)^M$ be the map defined in [24, Prop. 2.2].
Then we have:

Proposition 3.3 *Let $\alpha \in \mathcal{U}_F$, $\kappa = \kappa_\alpha$, $\mathfrak{a} \in \mathcal{S}(\alpha), \mathfrak{a} \neq 1$, and $\mathfrak{l}$ a prime of k. If $\mathfrak{a} = \mathfrak{l}$ we also assume that $\alpha(1)$ satisfies $v_\lambda(\alpha(1)) \equiv 0 (\mathrm{mod}\ M)$ for all $\lambda \mid \mathfrak{l}$ in F/k. Then:*

$$\text{If } \mathfrak{l} \nmid \mathfrak{a}, \text{ then } [\kappa(\mathfrak{a})]_{\mathfrak{l}} = 0.$$
$$\text{If } \mathfrak{l} \mid \mathfrak{a}, \text{ then } [\kappa(\mathfrak{a})]_{\mathfrak{l}} = \varphi_{\mathfrak{l}}(\kappa(\mathfrak{a}/\mathfrak{l})).$$

Proof See [24, Prop. 2.4]. Note that the additional assumption in the case $\mathfrak{a} = \mathfrak{l}$ is needed in (ii), both for its statement ($\varphi_{\mathfrak{l}}(\kappa(1))$ may not be defined in general) and for its proof. □

We now come to the technical heart of Kolyvagin's induction procedure, the application of Chebotarev's theorem.

Theorem 3.4 *Let K/k be an abelian extension, $G = \mathrm{Gal}(K/k)$. Let M denote a (large enough) power of p. Assume that we are given an ideal class $\mathfrak{c} \in A(K)$, a finite $\mathbb{Z}[G]$-module $W \subseteq K^\times / \left(K^\times\right)^M$, and a G-homomorphism*

$$\psi : W \longrightarrow \left(\mathbb{Z}/M\mathbb{Z}\right)[G].$$

Let $\bar{\mathfrak{p}}^c$ be the precise power of $\bar{\mathfrak{p}}$ which divides the conductor $\mathfrak{f}$ of K. Then there are infinitely many primes λ of K such that

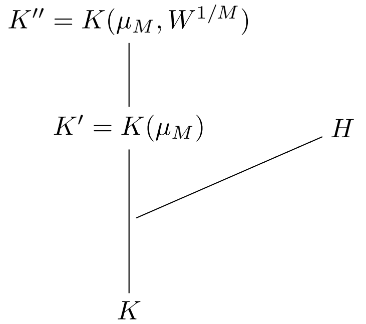
(1) $[\lambda] = p^{3c+3}\mathfrak{c}$ *in* $A(K)$.

(2) If $\mathfrak{l} = k \cap \lambda$, *then* $N\mathfrak{l} \equiv 1(\mathrm{mod}\ M)$, *and* $\mathfrak{l}$ *splits completely in* K.

(3) For all $w \in W$ *one has* $[w]_{\mathfrak{l}} = 0$ *in* $J_{\mathfrak{l}}/MJ_{\mathfrak{l}}$ *and there exists a unit* $u \in (\mathbb{Z}/M\mathbb{Z})^{\times}$ *such that*

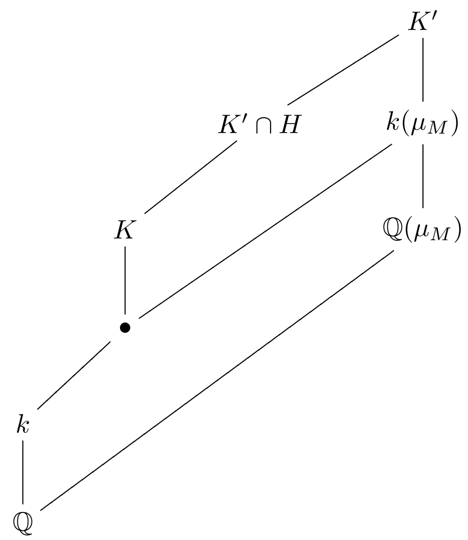
$$\varphi_{\mathfrak{l}}(w) = p^{3c+3}u\psi(w)\lambda.$$

Proof We follow the strategy of Greither's proof of [10, Th. 3.7], but have to change some technical details. Let H denote the Hilbert p-class field of K. For a natural number n we write μ_n for the nth roots of unity in an algebraic closure of K. We consider the following diagram of fields



Claim (a) $[H \cap K' : K] \leq p^c$

Proof: The situation is clarified by the following diagram



We write $\varphi_{\mathbb{Z}}$ (resp. $\varphi_{\mathcal{O}_k}$) for the Euler function in $\mathbb{Z}$ (resp. $\mathcal{O}_k$). Obviously $\bar{\mathfrak{p}}$ is totally ramified in $k(\mu_M)/k$. Hence $\bar{\mathfrak{p}}$ ramifies in K'/k of exponent at least $\varphi_{\mathbb{Z}}(M)$. On the other hand, $\bar{\mathfrak{p}}$ is ramified in K/k of exponent at most

$\varphi_{\mathcal{O}_k}(\bar{\mathfrak{p}}^c)$. Therefore any prime divisor of $\bar{\mathfrak{p}}$ ramifies in K'/K of degree at least $\varphi_{\mathbb{Z}}(M)/\varphi_{\mathcal{O}_k}(\bar{\mathfrak{p}}^c)$. Since $K' \cap H/K$ is unramified and $[K' : K] \leq \varphi_{\mathbb{Z}}(M)$, we derive $[K' \cap H : K] \leq \varphi_{\mathcal{O}_k}(\bar{\mathfrak{p}}^c)$. Since p is split in $k/\mathbb{Q}$ we obtain $\varphi_{\mathcal{O}_k}(\bar{\mathfrak{p}}^c) = (p-1)p^{c-1} < p^c$, so that the claim is shown.
In order to follow Greither's core argument for the proof of Theorem 3.4 we establish the following two claims.
Claim (b) $\mathrm{Gal}(H \cap K''/K)$ is annihilated by p^{2c+1}.
Claim (c) The cokernel of the canonical map from Kummer theory

$$\mathrm{Gal}(K''/K') \hookrightarrow \mathrm{Hom}(W, \mu_M)$$

is annihilated by p^{c+2}.

We write $M = p^m$. Since divisors of $\bar{\mathfrak{p}}$ are totally ramified in $k(\mu_M)/k$ of degree $\varphi_{\mathbb{Z}}(M)$ and at most ramified in K/k of degree $\varphi_{\mathcal{O}_k}(\bar{\mathfrak{p}}^c)$, one has

$$[k(\mu_M) : K \cap k(\mu_M)] \geq \frac{\varphi_{\mathbb{Z}}(M)}{\varphi_{\mathcal{O}_k}(\bar{\mathfrak{p}}^c)} = \begin{cases} p^{m-c}, & \text{if } c \geq 1, \\ (p-1)p^{m-1}, & \text{if } c = 0. \end{cases}$$

Since $k(\mu_M)/k$ is cyclic, there exists an element $j \in \mathrm{Gal}(k(\mu_M)/K \cap k(\mu_M))$ of exact order $a = p^{m-c-1}$. Let $r \in \mathbb{Z}$ such that $j(\zeta_M) = \zeta_M^r$. Then $r^a \equiv 1 (\mathrm{mod}\ M)$ and $r^b \not\equiv 1 (\mathrm{mod}\ M)$ for all $0 < b < a$. We also write $j \in \mathrm{Gal}(K'/K)$ for the unique extension of j to K' with $j|_K = id$. Let $\sigma \in \mathrm{Gal}(K''/K')$ and $\alpha \in K''$ such that $\alpha^M = w \in W$. Then there exists an integer t_w such that $\sigma(\alpha) = \zeta_M^{t_w}\alpha$. Since $W \subseteq K^\times/\left(K^\times\right)^M$, there is an extension of j to K''/K such that $j(\alpha) = \alpha$ for all $\alpha \in K''$ such that $\alpha^M \in W$. Therefore, for any such α,

$$j\sigma j^{-1}(\alpha) = j\sigma(\alpha) = j(\zeta_M^{t_w}\alpha) = \zeta_M^{rt_w}\alpha.$$

Hence j acts as $\sigma \mapsto \sigma^r$ on $\mathrm{Gal}(K''/K')$. Since $\mathrm{Gal}(K'/K)$ acts trivially on $\mathrm{Gal}(K'' \cap K'H/K')$ this implies that $r-1$ annihilates $\mathrm{Gal}(K'' \cap K'H/K')$. On the other hand $\mathrm{Gal}(K'' \cap K'H/K')$ is an abelian group of exponent M, so that also $\gcd(M, r-1)$ annihilates. Suppose that p^d divides $r-1$ with $d \geq 1$. By induction one easily shows that $r^{p^{m-d}} \equiv 1 (\mathrm{mod}\ p^m)$. Hence $a = p^{m-c-1}$ divides p^{m-d}, which implies $d \leq c+1$. As a consequence, p^{c+1} annihilates $\mathrm{Gal}(K'' \cap K'H/K') \simeq \mathrm{Gal}(K'' \cap H/K' \cap H)$. Together with claim (a) this proves (b).

We now proceed to demonstrate claim (c). Let $W' \subseteq K'^\times/\left(K'^\times\right)^M$ denote the image of W under the homomorphism

$$K^\times/\left(K^\times\right)^M \longrightarrow K'^\times/\left(K'^\times\right)^M. \tag{4}$$

Since $\mathrm{Gal}(K''/K') \simeq \mathrm{Hom}(W', \mu_M)$, it suffices to show that the kernel U of the map in (4) is annihilated by p^{c+2}. By Kummer theory U is isomorphic to $H^1(K'/K, \mu_M)$.

The extension K'/K is cyclic and a Herbrand quotient argument shows

$$\#H^1(K'/K,\mu_M) = \#H^0(K'/K,\mu_M) = \#\frac{\mu_M(K)}{N_{K'/K}(\mu_M)}.$$

From [20, Lem. 7] we deduce that $\#\mu_M(K)$ divides p^{c+2}. Hence U is annihilated by p^{c+2}.

Now that claim (b) and (c) are proved, the core argument runs precisely as in [10, pg.473/474] (using Greiter's notation the proof has to be adapted in the following way: $p^{c+2}\iota\psi$ has preimage $\gamma \in \mathrm{Gal}(K''/K')$; $\gamma_1 = p^{c+2}\left(\frac{\mathfrak{c}}{H/K}\right) \in \mathrm{Gal}(H/K)$; $\delta \in \mathrm{Gal}(K''H/K)$ with $\delta|_H = p^{2c+1}\gamma_1, \delta|_{K''} = p^{2c+1}\gamma$.)

$\square$

Recall the notation introduced at the beginning of this section. In addition, we let $\Delta = \mathrm{Gal}(K_0/k)$, $G_n = \mathrm{Gal}(K_n/k)$, $G_\infty = \mathrm{Gal}(K_\infty/k)$ and $\Gamma_n = \mathrm{Gal}(K_n/K_0)$. We fix a topological generator γ of $\Gamma = \mathrm{Gal}(K_\infty/K_0)$, and abbreviate the p^nth power of γ by γ_n.

For any abelian character χ of Δ we write $\Lambda_\chi = \mathbb{Z}_p(\chi)[[T]]$ for the usual Iwasawa algebra. Note that $\Lambda \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi) \simeq \mathbb{Z}_p(\chi)[[T]]$, so that our notation is consistent. We choose a generator $h_\chi \in \Lambda_\chi$ of char $\left((\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty)_\chi\right)$. By the general theory of finitely generated Λ_χ-modules there is a quasi-isomorphism

$$\tau : A_{\infty,\chi} \longrightarrow \bigoplus_{i=1}^{k} \Lambda_\chi/(g_i)$$

with $g_i \in \Lambda_\chi$, and by definition, $\mathrm{char}(A_{\infty,\chi}) = (g)$ with $g := g_1 \cdots g_k$.

As in [10] we need the following lemmas providing the link to finite levels.

Lemma 3.5 *Let $\chi \neq 1$ be an abelian character of Δ. Then there exist constants $n_0 = n_0(F), c_i = c_i(F), i = 1,2$, a divisor h'_χ of h_χ (all independent of n) and G_n-homomorphisms*

$$\vartheta_n : \bar{\mathcal{E}}_{n,\chi} \longrightarrow \Lambda_{n,\chi} := \Lambda_\chi/(1-\gamma_n)\Lambda_\chi$$

such that

(i) h'_χ is relatively prime to $\gamma_n - 1$ for all n

(ii) $(\gamma_{n_0} - 1)^{c_1} p^{c_2} h'_\chi \Lambda_{n,\chi} \subseteq \vartheta_n(im(\bar{\mathcal{C}}_{n,\chi}))$

where here $im(\bar{\mathcal{C}}_{n,\chi})$ denotes the image of $\bar{\mathcal{C}}_{n,\chi}$ in $\bar{\mathcal{E}}_{n,\chi}$.

Proof We mainly follow Greither's proof of [10, Lem. 3.9].
We let

$$\pi_n : \bar{\mathcal{E}}_\infty/(1-\gamma_n)\bar{\mathcal{E}}_\infty \longrightarrow \bar{\mathcal{E}}_n$$

denote the canonical map and first prove

Claim 1: There exists an integer κ (independent of n) such that

$$(\gamma-1)p^{\kappa}\ker(\pi_n)=0 \text{ and } (\gamma-1)p^{\kappa}\mathrm{cok}(\pi_n)=0$$

This is shown as in Greither's proof of [10, Lem. 3.9]. He uses [25, Lem. 1.2], which is stated under the additional assumption $p\nmid|\Delta|$. As already remarked by Greither, this hypothesis is not necessary.

Next we define $U_\infty := \varprojlim_n U_n$ and proceed to prove
Claim 2 $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}U_\infty\simeq\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\Lambda=\Lambda[\frac{1}{p}]$.
This can be proved similarly as [18, Th. 11.2.5]. The assumption $p\nmid|\Delta|$ of loc.cit. is not needed, since we invert p. Alternatively, Claim 2 follows from [6, Prop. III.1.3], together with Exercise (iii) of [6, III.1.1].

It follows that $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}U_{\infty,\chi}$ is free cyclic over $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\Lambda_\chi=\Lambda_\chi[\frac{1}{p}]$. Since $\Lambda_\chi[\frac{1}{p}]$ is a principal ideal domain, the submodule $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\bar{\mathcal{E}}_{\infty,\chi}$ is also free cyclic over $\Lambda_\chi[\frac{1}{p}]$. It follows that there exists a pseudo-isomorphism

$$f:\bar{\mathcal{E}}_{\infty,\chi}\longrightarrow C:=\bigoplus_i\Lambda_\chi/p^{n_i}\Lambda_\chi\oplus\Lambda_\chi.$$

If we apply the snake lemma to the diagram

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & \bar{\mathcal{E}}_{\infty,\chi} & \xrightarrow{=} & \bar{\mathcal{E}}_{\infty,\chi} & \longrightarrow & 0\\
 & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle pr\circ f=:\alpha} & & \\
0 & \longrightarrow & \oplus\Lambda_\chi/p^{n_i}\Lambda_\chi & \longrightarrow & C & \xrightarrow{pr} & \Lambda_\chi & \longrightarrow & 0
\end{array}$$

we see that $\ker(\alpha)$ is annihilated by some power of p and $\mathrm{cok}(\alpha)$ is finite.
We note that for any G_∞-module X one has

$$\left(X/(1-\gamma_n)X\right)_\chi\simeq X_\chi/(1-\gamma_n)X_\chi.$$

Let W_n denote the image of π_n and set $T:=\mathrm{Tor}_{\mathbb{Z}_p[\Delta]}(\mathrm{cok}(\pi_n),\mathbb{Z}_p(\chi))$. Then we have a commutative diagram (with exact lines)

$$\begin{array}{ccccccccc}
 & & T & \xrightarrow{\varphi} & W_{n,\chi} & \longrightarrow & \bar{\mathcal{E}}_{n,\chi} & \longrightarrow & \mathrm{cok}(\pi_n)_\chi \longrightarrow 0\\
 & & & & \downarrow{\scriptstyle =} & & & & \\
\ker(\pi_n)_\chi & \xrightarrow{\tau} & \frac{\bar{\mathcal{E}}_{\infty,\chi}}{(1-\gamma_n)\bar{\mathcal{E}}_{\infty,\chi}} & \xrightarrow{\pi_n} & W_{n,\chi} & \longrightarrow & 0 & &
\end{array}$$

We write $\pi_{n,\chi}$ for the composite map and obtain the exact sequence

$$0 \longrightarrow \ker(\pi_{n,\chi}) \longrightarrow \frac{\bar{\mathcal{E}}_{\infty,\chi}}{(1-\gamma_n)\bar{\mathcal{E}}_{\infty,\chi}} \stackrel{\pi_{n,\chi}}{\longrightarrow} \bar{\mathcal{E}}_{n,\chi} \longrightarrow \mathrm{cok}(\pi_n)_\chi \longrightarrow 0$$

We claim that $\ker(\pi_{n,\chi})$ is annihilated by $(\gamma-1)^2 p^{2\kappa}$: Let $e \in \ker(\pi_{n,\chi})$. Then

$$\begin{aligned} & \pi_n(e) = \varphi(t) \text{ for some } t \in \mathrm{Tor}_{\mathbb{Z}_p[\Delta]}(\mathrm{cok}(\pi_n), \mathbb{Z}_p(\chi)) \\ \Longrightarrow\quad & \pi_n((\gamma-1)p^\kappa e) = \varphi((\gamma-1)p^\kappa t) = 0 \\ \Longrightarrow\quad & \tau(c) = (\gamma-1)p^\kappa e \text{ for some } c \in \ker(\pi_n)_\chi \\ \Longrightarrow\quad & 0 = \tau((\gamma-1)p^\kappa c) = (\gamma-1)^2 p^{2\kappa} e \end{aligned}$$

So both $\ker(\pi_{n,\chi})$ and $\mathrm{cok}(\pi_{n,\chi})$ are annihilated by $(\gamma-1)^2 p^{2\kappa}$.
Consider now the following commutative diagram

$$\begin{array}{ccc} \bar{\mathcal{E}}_{\infty,\chi} & \xrightarrow{(\gamma-1)^4 p^{4\kappa}\alpha} & \Lambda_\chi \\ \downarrow{\scriptstyle \pi_{n,\chi}} & & \downarrow \\ \bar{\mathcal{E}}_{n,\chi} & \xrightarrow{\vartheta_n} & \Lambda_{n,\chi} = \Lambda_\chi/(1-\gamma_n)\Lambda_\chi \end{array}$$

where we define ϑ_n in the following manner: for $e \in \bar{\mathcal{E}}_{n,\chi}$ there exists $z \in \bar{\mathcal{E}}_{\infty,\chi}$ such that $\pi_{n,\chi}(z) = (\gamma-1)^2 p^{2\kappa} e$. We then set

$$\vartheta_n(e) := (\gamma-1)^2 p^{2\kappa}\alpha(z) (\mathrm{mod}\ (1-\gamma_n)\Lambda_\chi).$$

On the other hand, we have the exact sequence

$$\bar{\mathcal{C}}_{\infty,\chi} \longrightarrow \bar{\mathcal{E}}_{\infty,\chi} \longrightarrow \left(\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty\right)_\chi \longrightarrow 0$$

so that

$$\bar{\mathcal{E}}_{\infty,\chi}/\mathrm{im}(\bar{\mathcal{C}}_{\infty,\chi}) \hookrightarrow \left(\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty\right)_\chi.$$

The structure theorem of Λ_χ-torsion modules implies that $h_\chi\left(\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty\right)_\chi$ is finite. Since $\alpha(\bar{\mathcal{E}}_{\infty,\chi})/\alpha(\mathrm{im}\bar{\mathcal{C}}_{\infty,\chi})$ is a quotient of $\bar{\mathcal{E}}_{\infty,\chi}/\mathrm{im}(\bar{\mathcal{C}}_{\infty,\chi})$, the module $h_\chi\left(\alpha(\bar{\mathcal{E}}_{\infty,\chi})/\alpha(\mathrm{im}\bar{\mathcal{C}}_{\infty,\chi})\right)$ is also finite. Since $\mathrm{cok}(\alpha)$ is finite, there exists a power p^s such that $p^s \in \alpha(\bar{\mathcal{E}}_{\infty,\chi})$ and $p^s h_\chi \alpha(\bar{\mathcal{E}}_{\infty,\chi}) \subseteq \alpha(\mathrm{im}(\bar{\mathcal{C}}_{\infty,\chi})))$. Therefore $p^{2s}h_\chi \in \alpha(\mathrm{im}(\bar{\mathcal{C}}_{\infty,\chi}))$ and we conclude further:

$$\begin{aligned} & p^{2s+4\kappa}(\gamma-1)^4 h_\chi = p^{4\kappa}(\gamma-1)^4\alpha(z) \text{ for some } z \in \mathrm{im}(\bar{\mathcal{C}}_{\infty,\chi}) \\ \Longrightarrow\quad & \vartheta_n(z_n) = p^{2s+4\kappa}(\gamma-1)^4 h_\chi \text{ with } z_n = \pi_{n,\chi}(z) \in \mathrm{im}(\bar{\mathcal{C}}_{n,\chi}) \\ \Longrightarrow\quad & p^{2s+4\kappa}(\gamma-1)^4 h_\chi \Lambda_{n,\chi} \subseteq \vartheta_n(\mathrm{im}(\bar{\mathcal{C}}_{n,\chi})) \end{aligned} \tag{5}$$

Since $\gamma_n - 1$ divides $\gamma_{n+1} - 1$ for all n there exists a positive integer n_0 and a divisor h'_χ of h_χ such that h_χ divides $(\gamma_{n_0} - 1)h'_\chi$ and such that h'_χ is relatively prime with $\gamma_n - 1$ for all n. The assertions of the lemma are now immediate from (5).

□

Lemma 3.6 *Let $\chi \neq 1$ be a character of Δ. Then there exists a constant $c_3 = c_3(F)$ (independent of n) and G_n-homomorphisms*

$$\tau_n : A_{n,\chi} \longrightarrow \bigoplus_{i=1}^{k} \Lambda_{n,\chi}/(\bar{g}_i)$$

such that $p^{c_3}\mathrm{cok}\tau_n = 0$ for all $n \geq 0$. Here $\bar{g}_i$ denotes the image of $g_i \in \Lambda_\chi$ in $\Lambda_{n,\chi}$.

Proof The proof is identical to Greither's proof of [10, Lem. 3.10]. It is based on the following sublemma which will be used again at the end of the section.

□

Lemma 3.7 *For $n \geq 0$ the kernel and cokernel of multiplication with $\gamma_n - 1$ on A_∞ are finite.*

Proof See [25, pg. 705]. It is remarkable that one uses the known validity of Leopoldt's conjecture in this proof. □

The following technical lemma is the analogue of [10, Lem. 3.12].

Lemma 3.8 *Let K/k be an abelian extension, $G = \mathrm{Gal}(K/k)$ and Δ a subgroup of G. Let χ denote a character of Δ, M a power of p, $\mathfrak{a} = \mathfrak{l}_1 \cdots \mathfrak{l}_i \in \mathcal{S}_{M,K}$. Let $\mathfrak{l} = \mathfrak{l}_i$ and let λ be a fixed prime divisor of $\mathfrak{l}$ in K. We write $\mathfrak{c}$ for the class of λ and assume that $\mathfrak{c} \in A = A(K)$, where as usual $A(K)$ denotes the p-Sylow subgroup of the ideal class group of K.*
Let $B \subseteq A$ denote the subgroup generated by classes of prime divisors of $\mathfrak{l}_1, \ldots, \mathfrak{l}_{i-1}$. Let $x \in K^\times/\left(K^\times\right)^M$ such that $[x]_\mathfrak{q} = 0$ for all primes $\mathfrak{q}$ not dividing $\mathfrak{a}$, and let $W \subseteq K^\times/\left(K^\times\right)^M$ denote the $\mathbb{Z}_p[G]$-span of x. Assume that there exist elements

$$E, g, \eta \in \mathbb{Z}_p[G]$$

satisfying

(i) $E \cdot \mathrm{ann}_{(\mathbb{Z}_p[G])_\chi}(\bar{\mathfrak{c}}_\chi) \subseteq g \cdot \left(\mathbb{Z}_p[G]\right)_\chi$*, where $\bar{\mathfrak{c}}_\chi$ is the image of $\mathfrak{c}$ under $A \to A/B \to (A/B)_\chi$.*

(ii) $\#\left(\left(\mathbb{Z}_p[G]\right)_\chi / g\left(\mathbb{Z}_p[G]\right)_\chi\right) < \infty$

(iii) $M \geq |A_\chi| \left|\eta\left(\frac{J_\mathfrak{l}/MJ_\mathfrak{l}}{[W]_\mathfrak{l}}\right)_\chi\right|$*, where $[W]_\mathfrak{l}$ denotes the subgroup of $J_\mathfrak{l}/MJ_\mathfrak{l}$ generated by elements $[w]_\mathfrak{l}, w \in W$.*

Then there exists a G-homomorphism

$$\psi : W_\chi \longrightarrow ((\mathbb{Z}/M\mathbb{Z})\,[G])_\chi$$

such that

$$g\psi(x)\lambda_\chi = (E\cdot\eta[x]_{\mathfrak{l}})_\chi$$

in $(J_{\mathfrak{l}}/MJ_{\mathfrak{l}})_\chi$.

Proof Completely analoguous to the proof of [10, Lem. 3.12]. ∎

We will now sketch the main argument of the proof of Theorem 3.1. We fix a natural number $n \ge 1$ and let $K = K_n = Fk_n$. We view Δ as a subgroup of $G = \mathrm{Gal}(K/k)$.
We let M denote a large power of p which we will specify in course of the proof. By Lemma 3.6 there exists for each $i = 1, \dots, k$ an ideal class $\mathfrak{c}_i \in A_\chi$ such that

$$\tau_n(\mathfrak{c}_i) = (0, \dots, 0, p^{c_3}, 0, \dots, 0)$$

in $\bigoplus_{i=1}^k \Lambda_{n,\chi}/(\bar{g}_i)$ with p^{c_3} at the ith position. Choose $\mathfrak{c}_{k+1}$ arbitrary. By Lemma 3.5 there exists an element $\xi' \in \mathrm{im}(\bar{\mathcal{C}}_{n,\chi})$ such that $\vartheta_n(\xi') = (\gamma_{n_0} - 1)^{c_1}p^{c_2}h'_\chi$ in $\Lambda_{n,\chi}$. It is now easy to show that there exists an actual elliptic unit $\xi \in \mathcal{C}_n$ such that

$$\vartheta_n(\xi) = (\gamma_{n_0} - 1)^{c_1}p^{c_2}h'_\chi (\mathrm{mod}\ M\Lambda_{n,\chi}). \tag{6}$$

By [24, Prop. 1.2] there exists an Euler system $\alpha \in \mathcal{U}_{K,M}$ such that $\alpha(1) = \xi$. Set $d := 3c+3$, where c was defined in Theorem 3.4. Following Greither we will use Theorem 3.4 to construct inductively prime ideals λ_i of K, $1 \le i \le k+1$, such that

(a) $[\lambda_i]_\chi = p^d\mathfrak{c}_i$

(b) $\mathfrak{l}_i = \lambda_i \cap k \subseteq \mathcal{S}_{M,K}$

(c) one has the equalities

$$\begin{aligned}(v_{\lambda_1}(\kappa(\mathfrak{l}_1)))_\chi &= u_1|\Delta|(\gamma_{n_0}-1)^{c_1}p^{d+c_2}h'_\chi,\\ (g_{i-1}v_{\lambda_i}(\kappa(\mathfrak{l}_1\cdots\mathfrak{l}_i)))_\chi &= u_i|\Delta|(\gamma_{n_0}-1)^{c_1^{i-1}}p^{d+c_3}\left(v_{\lambda_{i-1}}(\kappa(\mathfrak{l}_1\cdots\mathfrak{l}_{i-1}))\right)_\chi\end{aligned}$$

for $2 \le i \le k+1$. These are equalities in $\Lambda_{n,\chi}/M\Lambda_{n,\chi}$. The elements u_i are units in $\mathbb{Z}/M\mathbb{Z}$ and $v_\lambda(x) \in (\mathbb{Z}/M\mathbb{Z})\,[G] \simeq \Lambda_n/M\Lambda_n$ is defined by $v_\lambda(x)\lambda = [x]_{\mathfrak{l}}$ in $J_{\mathfrak{l}}/MJ_{\mathfrak{l}}$, if $\mathfrak{l} = \lambda \cap k \in \mathcal{L}_{M,K}$.

We briefly descibe this induction process. For $i = 1$ we let $\mathfrak{c} \in A$ be a preimage of $\mathfrak{c}_1$ under the canonical epimorphism $A \to A_\chi$. We apply Theorem 3.4 with the data $\mathfrak{c}$, $W = \mathcal{E}/\mathcal{E}^M$ (with $\mathcal{E} := \mathcal{O}_K^\times$) and

$$\psi : W \xrightarrow{v} \bar{\mathcal{E}}_{n,\chi}/\bar{\mathcal{E}}_{n,\chi}^M \xrightarrow{\vartheta_n} \Lambda_{n,\chi}/M\Lambda_{n,\chi} \xrightarrow{\varepsilon_\chi} (\mathbb{Z}/M\mathbb{Z})\,[G]$$

where $v \in (\mathbb{Z}/M\mathbb{Z})^\times$ is such that each unit $x \in K \otimes k_\mathfrak{p}$ satisfies $x^v \equiv 1$ modulo all primes above $\mathfrak{p}$. The map ε_χ is defined in [10, Lemma 3.13]. Theorem 3.4 provides a prime ideal $\lambda = \lambda_1$ which obviously satisfies (a) and (b) and, in addition,

$$\varphi_\mathfrak{l}(w) = p^d u\psi(w)\lambda \text{ for all } w \in \mathcal{E}/\mathcal{E}^M.$$

From this equality we conclude further

$$\begin{aligned} v_\lambda(\kappa(\mathfrak{l}))\lambda &= [\kappa(\mathfrak{l})]_\mathfrak{l} = \varphi_\mathfrak{l}(\kappa(1)) = \varphi_\mathfrak{l}(\xi) \\ &= p^d u\psi(\xi)\lambda = \left(p^d uv(\varepsilon_\chi \circ \vartheta_n)(\xi)\right)\lambda \end{aligned}$$

in $J_\mathfrak{l}/MJ_\mathfrak{l} = (\mathbb{Z}/M\mathbb{Z})[G]\lambda$. Projecting the equality $v_\lambda(\kappa(\mathfrak{l})) = p^d uv(\varepsilon_\chi \circ \vartheta_n)(\xi)$ to $((\mathbb{Z}/M\mathbb{Z})[G])_\chi = \Lambda_{n,\chi}/M\Lambda_{n,\chi}$ and using [10, Lemma 3.13] together with (6) we obtain equality (c) for $i = 1$.
For the induction step $i-1 \mapsto i$ we set $\mathfrak{a}_{i-1} := \mathfrak{l}_1 \cdots \mathfrak{l}_{i-1}$. Using (c) inductively we see that $\left(v_{\lambda_{i-1}}(\kappa(\mathfrak{a}_{i-1}))\right)_\chi$ divides

$$\left(\underbrace{|\Delta|^{i-1}p^{(i-2)(d+c_3)+(d+c_2)}}_{=:D_i}(\gamma_{n_0}-1)^{c_1+\sum_{s=1}^{i-2}c_1^s}h'_\chi\right)_\chi.$$

Without loss of generality we may assume that $c_1 \geq 2$. Then one has $c_1 + \sum_{i=1}^{i-2} c_1^s \leq c_1^{i-1}$, so that $\left(v_{\lambda_{i-1}}(\kappa(\mathfrak{a}_{i-1}))\right)_\chi$ also divides $D_i(\gamma_{n_0}-1)^{t_i}h'_\chi$ with $t_i := c_1^{i-1}$. The module

$$N = (\gamma_{n_0}-1)^{t_i}\left(J_{\mathfrak{l}_{i-1}}/\left(M, [\kappa(\mathfrak{a}_{i-1})]_{\mathfrak{l}_{i-1}}\right)\right)_\chi$$

is a cyclic as a $\Lambda_{n,\chi}$-module and annihilated by $D_i h'_\chi$. Consequently

$$|N| \leq |\Lambda_{n,\chi}/(D_i)| \cdot |\Lambda_{n,\chi}/(h'_\chi)|.$$

Note that by the definition of h'_χ the quotient $\Lambda_{n,\chi}/(h'_\chi)$ is finite. If we choose M such that

$$M \geq \max\left(|A_\chi| \cdot |\Lambda_{n,\chi}/(D_{k+1})| \cdot |\Lambda_{n,\chi}/(h'_\chi)|, p^n\right)$$

then one has $|N| \leq M|A_\chi|^{-1}$.
We now apply Lemma 3.8 with $\mathfrak{a} = \mathfrak{a}_{i-1}, g = g_{i-1}, x = \kappa(\mathfrak{a}_{i-1}), E = p^{c_3}$ and $\eta = (\gamma_{n_0}-1)^{t_i}$. Following Greither it is straight forward to check the hypothesis (a), (b) and (c) of Lemma 3.8. Note that for (b) one has to use the fact that $\mathrm{char}(A_{\infty,\chi})$ is relatively prime to $\gamma_n - 1$ for all n, which is an immediate consequence of Lemma 3.5. We let W denote the $\mathbb{Z}_p[G]$-span of $\kappa(\mathfrak{a}_{i-1})$ in $K^\times/\left(K^\times\right)^M$ and obtain a homomorphism

$$\psi_i : W_\chi \longrightarrow ((\mathbb{Z}/M\mathbb{Z})[G])_\chi$$

such that $g_{i-1}\psi_i(\kappa(\mathfrak{a}_{i-1})) = \big(p^{c_3}(\gamma_{n_0}-1)^{t_i} v_{\lambda_{i-1}}(\kappa(\mathfrak{a}_{i-1}))\big)_\chi$. We let $\mathfrak{c}$ denote a preimage of $\mathfrak{c}_i$ and consider the homomorphism

$$\psi : W \longrightarrow W_\chi \xrightarrow{\psi_i} \Lambda_{n,\chi}/M\Lambda_{n,\chi} \xrightarrow{\varepsilon_\chi} (\mathbb{Z}/M\mathbb{Z})\,[G]$$

We again apply Theorem 3.4 and obtain λ_i satifying (a), (b) and also

$$\varphi_{\mathfrak{l}_i}(\kappa(\mathfrak{a}_{i-1})) = p^d u \psi(\kappa(\mathfrak{a}_{i-1}))\lambda_i.$$

As in the case $i = 1$ one now establishes equality (c). This concludes the inductive construction of $\lambda_1, \ldots, \lambda_{k+1}$.
Using (c) successively we obtain (suppressing units in $\mathbb{Z}/M\mathbb{Z}$)

$$\big(g_1 \cdots g_k v_{\lambda_{k+1}}(\kappa(\mathfrak{l}_1 \cdots \mathfrak{l}_{k+1}))\big) = \eta h'_\chi$$

(as an equality in $\Lambda_{n,\chi}/M\Lambda_{n,\chi}$) with

$$\eta = \Big(|\Delta|^{k+1} p^{k(d+c_3)+d+c_2}(\gamma_{n_0}-1)^{c_1+\sum_{s=1}^k c_1^s}\Big)_\chi .$$

Therefore $g = g_1 \cdots g_k$ divides $\eta h'_\chi$ in $\Lambda_{n,\chi}/M\Lambda_{n,\chi}$, and since $p^n \mid M$ we also see that g divides $\eta h'_\chi$ in $\Lambda_{n,\chi}/p^n\Lambda_{n,\chi}$. As in [31, page 371, last but one paragraph] we deduce that g divides $\eta h'_\chi$ in Λ_χ.
By [6, III.2.1, Theorem] (together with [6, III.1.7, (13)]) we know that the μ-invariant of $A_{\infty,\chi}$ is trivial. Hence $g = \mathrm{char}(A_{\infty,\chi})$ is coprime with p. By Lemma 3.7 it is also coprime with $\gamma_{n_0} - 1$, and consequently $|\Lambda_\chi/(g,\eta)| < \infty$. Therefore there exist $\alpha, \beta \in \Lambda_\chi$ and $N \in \mathbb{N}$ such that $p^N = \alpha g + \beta\eta$ and we see that g divides $p^N h'_\chi$. Since g is prime to p we obtain $g \mid h'_\chi$.

Remark 3.9 There are several steps in the proof where we use the assumption that p splits in $k/\mathbb{Q}$. Among these the vanishing of $\mu(A_{\infty,\chi})$ is most important. The proof of this uses an important result of Gillard [9]. If p is not split in $k/\mathbb{Q}$ our knowledge about $\mu(A_{\infty,\chi})$ seems to be quite poor.

4 The conjecture

In this section we fix an integral $\mathcal{O}_k$-ideal $\mathfrak{f}$ such that $w(\mathfrak{f}) = 1$ and write

$$M = h^0(\mathrm{Spec}(k(\mathfrak{f}))), \quad A = \mathbb{Q}[G_\mathfrak{f}], \quad \mathfrak{A} = \mathbb{Z}[G_\mathfrak{f}],$$

where for any $\mathcal{O}_k$-ideal $\mathfrak{m}$ we let $G_\mathfrak{m}$ denote the Galois group $\mathrm{Gal}(k(\mathfrak{m})/k)$.
For any commutative ring R we write $\mathcal{D}(R)$ for the derived category of the homotopy category of bounded complexes of R-modules and $\mathcal{D}^p(R)$ for the full triangulated subcategory of perfect complexes of R-modules. We write $\mathcal{D}^{pis}(R)$ for the subcategory of $\mathcal{D}^p(R)$ in which the objects are the same, but the morphisms are restricted to quasi-isomorphisms.

We let $\mathcal{P}(R)$ denote the category of graded invertible R-modules. If R is reduced, we write Det_R for the functor from $\mathcal{D}^{pis}(R)$ to $\mathcal{P}(R)$ introduced by Knudsen and Mumford [14]. To be more precise, we define

$$\mathrm{Det}_R(P) := \left(\bigwedge_R^{\mathrm{rk}_R(P)} P, \mathrm{rk}_R(P) \right) \quad \in \quad \mathrm{Ob}(\mathcal{P}(R))$$

for any finitely generated projective R-module P and for a bounded complex $P^\bullet$ of such modules we set

$$\mathrm{Det}_R(P^\bullet) := \bigotimes_{i\in\mathbb{Z}} \mathrm{Det}_R^{(-1)^i}(P^i).$$

If R is reduced, then this functor extends to a functor from $\mathcal{D}^{pis}(R)$ to $\mathcal{P}(R)$. For more information and relevant properties the reader is refered to [5, §2], or the original papers [14] and [15].
For any finite set S of places of k we define $Y_S = Y_S(k(\mathfrak{f})) = \oplus_{w\in S(k(\mathfrak{f}))}\mathbb{Z}w$. Here $S(k(\mathfrak{f}))$ denotes the set of places of $k(\mathfrak{f})$ lying above places in S. We let $X_S = X_S(k(\mathfrak{f}))$ denote the kernel of the augmentation map $Y_S \to \mathbb{Z}, w \mapsto 1$.
The fundamental line $\Xi({}_AM)$ is given by

$$\Xi({}_AM)^\# = \mathrm{Det}_A^{-1}\left(\mathcal{O}_{k(\mathfrak{f})}^\times \otimes_{\mathbb{Z}} \mathbb{Q}\right) \otimes_A \mathrm{Det}_A\left(X_{\{v|\infty\}} \otimes_{\mathbb{Z}} \mathbb{Q}\right),$$

where the superscript $\#$ means twisting the action of $G_\mathfrak{f}$ by $g \mapsto g^{-1}$. We let

$$\begin{aligned} R = R_{k(\mathfrak{f})} : \mathcal{O}_{k(\mathfrak{f})}^\times \otimes_{\mathbb{Z}} \mathbb{R} \quad &\longrightarrow \quad X_{\{v|\infty\}} \otimes_{\mathbb{Z}} \mathbb{R}, \\ u \quad &\mapsto \quad -\sum_{v|\infty} \log|u|_v \cdot v \end{aligned}$$

denote the Dirichlet regulator map. Let

$${}_A\vartheta_\infty : \mathbb{R}[G_\mathfrak{f}] \longrightarrow \Xi({}_AM)^\# \otimes_{\mathbb{Q}} \mathbb{R}$$

be the inverse of the canonical isomorphism

$$\begin{aligned} & \mathrm{Det}_{\mathbb{R}[G_\mathfrak{f}]}^{-1}\left(\mathcal{O}_{k(\mathfrak{f})}^\times \otimes_{\mathbb{Z}} \mathbb{R}\right) \otimes_{\mathbb{R}[G_\mathfrak{f}]} \mathrm{Det}_{\mathbb{R}[G_\mathfrak{f}]}\left(X_{\{v|\infty\}} \otimes_{\mathbb{Z}} \mathbb{R}\right) \\ \xrightarrow{\det(R)\otimes 1} \quad & \mathrm{Det}_{\mathbb{R}[G_\mathfrak{f}]}^{-1}\left(X_{\{v|\infty\}} \otimes_{\mathbb{Z}} \mathbb{R}\right) \otimes_{\mathbb{R}[G_\mathfrak{f}]} \mathrm{Det}_{\mathbb{R}[G_\mathfrak{f}]}\left(X_{\{v|\infty\}} \otimes_{\mathbb{Z}} \mathbb{R}\right) \\ \xrightarrow{\mathrm{eval}} \quad & (\mathbb{R}[G_\mathfrak{f}], 0). \end{aligned}$$

Following [19] we define for integral $\mathcal{O}_k$-ideals $\mathfrak{g}, \mathfrak{g}_1$ with $\mathfrak{g} \mid \mathfrak{g}_1$ and each abelian character η of $G_\mathfrak{g} \simeq \mathrm{cl}(\mathfrak{g})$ ($\mathrm{cl}(\mathfrak{g})$ denoting the ray class group modulo $\mathfrak{g}$)

$$S_\mathfrak{g}(\eta, \mathfrak{g}_1) = \sum_{c\in\mathrm{cl}(\mathfrak{g}_1)} \eta(c^{-1}) \log|\varphi_\mathfrak{g}(c)|,$$

where η is regarded as a character of $\mathrm{cl}(\mathfrak{g}_1)$ via inflation. For the definition of the ray class invariants $\varphi_{\mathfrak{g}}(c)$ we choose an integral ideal $\mathfrak{c}$ in the class c and set

$$\varphi_{\mathfrak{g}}(c) = \varphi_{\mathfrak{g}}(\mathfrak{c}) = \begin{cases} \varphi^{12N(\mathfrak{g})}(1; \mathfrak{g}\mathfrak{c}^{-1}), & \text{if } \mathfrak{g} \neq 1, \\ \left| \frac{N(\mathfrak{c}^{-1})^6 \Delta(\mathfrak{c}^{-1})}{(2\pi)^{12}} \right|, & \text{if } \mathfrak{g} = 1, \end{cases}$$

where φ was defined in (1). Note that this definition does not depend on the choice of the ideal $\mathfrak{c}$ (see [20, pp. 15/16]).

For an abelian character η of $\mathrm{cl}(\mathfrak{g})$ we write $\mathfrak{f}_\eta$ for its conductor. We write $L^*(\eta)$ for the leading term of the Taylor expansion of the Dirichlet L-function $L(s, \eta)$ at $s = 0$.

From [20, Th. 3] and the functional equation satisfied by Dirichlet L-functions we deduce

$$L^*(\eta^{-1}) = -\frac{S_{\mathfrak{f}_\eta}(\eta, \mathfrak{f}_\eta)}{6N(\mathfrak{f}_\eta) w(\mathfrak{f}_\eta)}. \tag{7}$$

We denote by $\hat{G}_{\mathfrak{f}}^{\mathbb{Q}}$ the set of $\mathbb{Q}$-rational characters associated with the $\mathbb{Q}$-irreducible representations of $G_{\mathfrak{f}}$. For $\chi \in \hat{G}_{\mathfrak{f}}^{\mathbb{Q}}$ we set $e_\chi = \sum_{\eta \in \chi} e_\eta \in A$, where we view χ as an $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$-orbit of absolutely irreducible characters of $G_{\mathfrak{f}}$. Then the Wedderburn decompostion of A is given by

$$A \simeq \prod_{\chi \in \hat{G}_{\mathfrak{f}}^{\mathbb{Q}}} \mathbb{Q}(\chi). \tag{8}$$

Here, by a slight abuse of notation, $\mathbb{Q}(\chi)$ denotes the extension generated by the values of η for any $\eta \in \chi$. For any character $\chi \in \hat{G}_{\mathfrak{f}}^{\mathbb{Q}}$ the conductor $\mathfrak{f}_\chi$, defined by $\mathfrak{f}_\chi := \mathfrak{f}_\eta$ for any $\eta \in \chi$, is well defined.

We put $L^*(\chi) := \sum_{\eta \in \chi} L^*(\eta) e_\eta$ and note that $L^*(\chi)^\# := \sum_{\eta \in \chi} L^*(\eta^{-1}) e_\eta$. The statement $L^*(\chi)^\# \in A e_\chi$ (compare to [8, page 8]) is not obvious, but needs to be proved. This is essentially Stark's conjecture.

We fix a prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$ and also choose an auxiliary ideal $\mathfrak{a}$ of $\mathcal{O}_k$ such that $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}) = 1$. For each $\eta \neq 1$ we define elements

$$\xi_\eta := \begin{cases} \psi(1; \mathfrak{f}_\eta, \mathfrak{a}), & \text{if } \mathfrak{f}_\eta \neq 1, \\ \frac{\delta(\mathcal{O}_k, \mathfrak{a}^{-1})}{\delta(\mathfrak{p}, \mathfrak{p}\mathfrak{a}^{-1})}, & \text{if } \mathfrak{f}_\eta = 1, \eta \neq 1, \end{cases} \tag{9}$$

where δ denotes the function of lattices defined in [21, Th. 1]. We set $\xi_\chi := \xi_\eta$ for any $\eta \in \chi$.

We fix an embedding $\sigma : \mathbb{Q}^c \hookrightarrow \mathbb{C}$ and write $w_\infty = \sigma|_{k(\mathfrak{f})}$. A standard computation leads to

$$\begin{aligned} & R(e_\eta \xi_\eta) \\ = & \begin{cases} (N\mathfrak{a} - \eta(\mathfrak{a})) w(\mathfrak{f}_\eta) [k(\mathfrak{f}) : k(\mathfrak{f}_\eta)] L^*(\eta^{-1}) e_\eta w_\infty, & \mathfrak{f}_\eta \neq 1, \\ (1 - \eta(\mathfrak{p})^{-1})(N\mathfrak{a} - \eta(\mathfrak{a})) w(1) [k(\mathfrak{f}) : k(1)] L^*(\eta^{-1}) e_\eta w_\infty, & \mathfrak{f}_\eta = 1, \eta \neq 1. \end{cases} \end{aligned} \tag{10}$$

For the reader's convenience we briefly sketch the computation for characters $\eta \neq 1$ with $\mathfrak{f}_\eta = 1$. By definition of the Dirichlet regulator map and [21, Cor. 2] we obtain

$$R(e_\eta \xi_\eta) = -\frac{1}{6}[k(\mathfrak{f}) : k(1)] \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \frac{\Delta(\mathfrak{c})^{N\mathfrak{a}} \Delta(\mathfrak{a}^{-1}\mathfrak{c}\mathfrak{p})}{\Delta(\mathfrak{a}^{-1}\mathfrak{c})\Delta(\mathfrak{c}\mathfrak{p})^{N\mathfrak{a}}} \right| \eta(\mathfrak{c}) e_\eta w_\infty. \tag{11}$$

Since $\sum_{\mathfrak{c}\in \mathrm{cl}(1)} C\eta(\mathfrak{c}) = 0$ for any constant C we compute further

$$\begin{aligned}
& \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \frac{\Delta(\mathfrak{c})^{N\mathfrak{a}} \Delta(\mathfrak{a}^{-1}\mathfrak{c}\mathfrak{p})}{\Delta(\mathfrak{a}^{-1}\mathfrak{c})\Delta(\mathfrak{c}\mathfrak{p})^{N\mathfrak{a}}} \right| \eta(\mathfrak{c}) \\
= & \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \left(\frac{(N\mathfrak{c})^6 \Delta(\mathfrak{c})}{(2\pi)^{12}} \right)^{N\mathfrak{a}} \right| \eta(\mathfrak{c}) + \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \frac{(N\mathfrak{a}^{-1}\mathfrak{c}\mathfrak{p})^6 \Delta(\mathfrak{a}^{-1}\mathfrak{c}\mathfrak{p})}{(2\pi)^{12}} \right| \eta(\mathfrak{c}) - \\
& - \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \left(\frac{(N\mathfrak{c}\mathfrak{p})^6 \Delta(\mathfrak{c}\mathfrak{p})}{(2\pi)^{12}} \right)^{N\mathfrak{a}} \right| \eta(\mathfrak{c}) - \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \frac{(N\mathfrak{a}^{-1}\mathfrak{c})^6 \Delta(\mathfrak{a}^{-1}\mathfrak{c})}{(2\pi)^{12}} \right| \eta(\mathfrak{c}) \\
= & N\mathfrak{a} \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \varphi_1(\mathfrak{c}^{-1}) \right| \eta(\mathfrak{c}) + \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \varphi_1(\mathfrak{a}\mathfrak{c}^{-1}\mathfrak{p}^{-1}) \right| \eta(\mathfrak{c}) - \\
& - N\mathfrak{a} \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \varphi_1(\mathfrak{p}^{-1}\mathfrak{c}^{-1}) \right| \eta(\mathfrak{c}) - \sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \varphi_1(\mathfrak{a}\mathfrak{c}^{-1}) \right| \eta(\mathfrak{c}).
\end{aligned}$$

Recalling that $\varphi_{\mathfrak{g}}(c)$ is a class invariant we obtain

$$\sum_{\mathfrak{c} \in \mathrm{cl}(1)} \log \left| \frac{\Delta(\mathfrak{c})^{N\mathfrak{a}} \Delta(\mathfrak{a}^{-1}\mathfrak{c}\mathfrak{p})}{\Delta(\mathfrak{a}^{-1}\mathfrak{c})\Delta(\mathfrak{c}\mathfrak{p})^{N\mathfrak{a}}} \right| \eta(\mathfrak{c}) = (N\mathfrak{a} - \eta(\mathfrak{a}))(1 - \eta(\mathfrak{p})^{-1}) S_1(\eta, 1) e_\eta w_\infty,$$

so that (10) is an immediate consequence of (7) and (11).
According to the decomposition (8) we decompose $\Xi({}_AM)^{\#}$ character by character and obtain a canonical isomorphism

$$\Xi({}_AM)^{\#} \longrightarrow \left(\prod_{\chi \in \hat{G}_{\mathfrak{f}}^{\mathbb{Q}}} \left(\mathrm{Det}^{-1}_{\mathbb{Q}(\chi)} (\mathcal{O}^\times_{k(\mathfrak{f})} \otimes_{\mathfrak{A}} \mathbb{Q}(\chi)) \otimes_{\mathbb{Q}(\chi)} \mathrm{Det}_{\mathbb{Q}(\chi)} (X_{\{v|\infty\}} \otimes_{\mathfrak{A}} \mathbb{Q}(\chi)) \right) \right).$$

As in the cyclotomic case one has

$$\dim_{\mathbb{Q}(\chi)} e_\chi \left(\mathcal{O}^\times_{k(\mathfrak{f})} \otimes_{\mathfrak{A}} \mathbb{Q}(\chi) \right) = \dim_{\mathbb{Q}(\chi)} e_\chi \left(X_{\{v|\infty\}} \otimes_{\mathfrak{A}} \mathbb{Q}(\chi) \right) = \begin{cases} 1, & \chi \neq 1, \\ 0, & \chi = 1. \end{cases} \tag{12}$$

Upon recalling that $\mathrm{Det}_{\mathbb{Q}}(0) = (\mathbb{Q}, 0)$ in $\mathcal{P}(\mathbb{Q})$ we get a canonical isomorphism

$$\Xi({}_AM)^{\#} \quad \longrightarrow \quad \mathbb{Q} \times \left(\prod_{\chi \neq 1} \left((\mathcal{O}^\times_{k(\mathfrak{f})} \otimes_{\mathfrak{A}} \mathbb{Q}(\chi))^{(-1)} \otimes_{\mathbb{Q}(\chi)} (X_{\{v|\infty\}} \otimes_{\mathfrak{A}} \mathbb{Q}(\chi)) \right) \right).$$

From (10) we deduce

$$\begin{aligned}&\left({}_A\vartheta_\infty(L^*({}_AM,0)^{-1})\right)_\chi\\ =&\begin{cases} w(\mathfrak{f}_\chi)[k(\mathfrak{f}):k(\mathfrak{f}_\chi)](N\mathfrak{a}-\sigma(\mathfrak{a}))e_\chi\xi_\chi^{-1}\otimes w_\infty, & \mathfrak{f}_\chi\neq 1,\\ w(1)[k(\mathfrak{f}):k(1)](1-\sigma(\mathfrak{p})^{-1})(N\mathfrak{a}-\sigma(\mathfrak{a}))e_\chi\xi_\chi^{-1}\otimes w_\infty, & \mathfrak{f}_\chi=1,\chi\neq 1\\ L(\chi,0)^{-1}, & \chi=1.\end{cases}\end{aligned}$$

In particular, this proves the equivariant version of [8, Conjecture 2].
We fix a prime p and put $A_p := A\otimes_{\mathbb{Q}}\mathbb{Q}_p = \mathbb{Q}_p[G_\mathfrak{f}]$, $\mathfrak{A}_p := \mathfrak{A}\otimes_{\mathbb{Z}}\mathbb{Z}_p = \mathbb{Z}_p[G_\mathfrak{f}]$. Let $S = S_{\mathrm{ram}}\cup S_\infty$ be the union of the set of ramified places and the set of archimedean places of k. Let $S_p = S\cup\{\mathfrak{p}\mid p\}$ and put

$$\Delta(k(\mathfrak{f})) := R\mathrm{Hom}_{\mathbb{Z}_p}(R\Gamma_c(\mathcal{O}_{k(\mathfrak{f}),S_p},\mathbb{Z}_p),\mathbb{Z}_p)[-3]$$

Then $\Delta(k(\mathfrak{f}))$ can be represented by a perfect complex of $\mathfrak{A}_p$-modules whose cohomology groups $H^i(\Delta(k(\mathfrak{f}))$ are trivial for $i\neq 1,2$. For $i=1$ one finds

$$H^1(\Delta(k(\mathfrak{f}))\simeq\mathcal{O}^\times_{k(\mathfrak{f}),S_p}\otimes_{\mathbb{Z}}\mathbb{Z}_p,$$

and H^2 fits into an short exact sequence

$$0\longrightarrow\mathrm{Pic}(\mathcal{O}_{k(\mathfrak{f}),S_p})\otimes_{\mathbb{Z}}\mathbb{Z}_p\longrightarrow H^2(\Delta(k(\mathfrak{f})))\longrightarrow X_{\{w\mid\mathfrak{f}p\infty\}}\otimes_{\mathbb{Z}}\mathbb{Z}_p\longrightarrow 0$$

We have an isomorphism

$${}_A\vartheta_p:\Xi({}_AM)^{\#}\otimes_{\mathbb{Q}}\mathbb{Q}_p\longrightarrow\mathrm{Det}_{A_p}\left(\Delta(k(\mathfrak{f}))\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\right)$$

given by the composite

$$\begin{aligned}&\mathrm{Det}^{-1}_{A_p}(\mathcal{O}^\times_{k(\mathfrak{f})}\otimes_{\mathbb{Z}}\mathbb{Q}_p)\otimes_{A_p}\mathrm{Det}_{A_p}(X_{\{v\mid\infty\}}\otimes_{\mathbb{Z}}\mathbb{Q}_p)\\ \xrightarrow{\varphi_1}\;&\mathrm{Det}^{-1}_{A_p}(\mathcal{O}^\times_{k(\mathfrak{f}),S_p}\otimes_{\mathbb{Z}}\mathbb{Q}_p)\otimes_{A_p}\mathrm{Det}_{A_p}(X_{\{v\mid\mathfrak{f}p\infty\}}\otimes_{\mathbb{Z}}\mathbb{Q}_p)\\ \xrightarrow{\varphi_2}\;&\mathrm{Det}^{-1}_{A_p}(\mathcal{O}^\times_{k(\mathfrak{f}),S_p}\otimes_{\mathbb{Z}}\mathbb{Q}_p)\otimes_{A_p}\mathrm{Det}_{A_p}(X_{\{v\mid\mathfrak{f}p\infty\}}\otimes_{\mathbb{Z}}\mathbb{Q}_p)\\ \xrightarrow{\varphi_3}\;&\mathrm{Det}_{A_p}\left(\Delta(k(\mathfrak{f}))\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\right).\end{aligned}$$

Here φ_1 is induced by the split short exact sequences

$$0\longrightarrow\mathcal{O}^\times_{k(\mathfrak{f})}\otimes_{\mathbb{Z}}\mathbb{Q}_p\longrightarrow\mathcal{O}^\times_{k(\mathfrak{f}),S_p}\otimes_{\mathbb{Z}}\mathbb{Q}_p\longrightarrow Y_{\{w\mid\mathfrak{f}p\}}\otimes_{\mathbb{Z}}\mathbb{Q}_p\longrightarrow 0 \qquad (13)$$

$$0\longrightarrow X_{\{w\mid\infty\}}\otimes_{\mathbb{Z}}\mathbb{Q}_p\longrightarrow X_{\{w\mid\mathfrak{f}p\infty\}}\otimes_{\mathbb{Z}}\mathbb{Q}_p\longrightarrow Y_{\{w\mid\mathfrak{f}p\}}\otimes_{\mathbb{Z}}\mathbb{Q}_p\longrightarrow 0 \qquad (14)$$

The isomorphism φ_2 is multiplication with the Euler factor $\prod_{v\in S_p}\mathcal{E}_v^{\#}\in A^\times$ where $\mathcal{E}_v$ is defined by

$$\mathcal{E}_v=\sum_{\eta|_{D_v}=1}|D_v/I_v|\,e_\eta+\sum_{\eta|_{D_v}\neq 1}(1-\eta(f_v))^{-1}\,e_\eta, \qquad (15)$$

where $f_v \in D_v$ denotes a lift of the Frobenius element in D_v/I_v and $I_v \subseteq D_v \subseteq G_{\mathfrak{f}}$ are the inertia and decomposition subgroups for a place $w \mid v$ in $k(\mathfrak{f})/k$. Finally φ_3 arises from the explicit description of the cohomology groups $H^i(\Delta(k(\mathfrak{f})))$, $i = 1, 2$, and the canonical isomorphism

$$\mathrm{Det}_{A_p}(\Delta(k(\mathfrak{f}))\otimes_{\mathfrak{A}_p}\mathbb{Q}_p) \simeq \bigotimes_{i\in\mathbb{Z}} \mathrm{Det}_{A_p}^{(-1)^i}\left(H^i(\Delta(k(\mathfrak{f}))\otimes_{\mathfrak{A}_p}\mathbb{Q}_p)\right) \tag{16}$$

([14, Rem. b) following Th. 2]).

We are now in position to give a very explicit description of the equivariant version of [8, Conjecture 3].

CONJECTURE 4.1 ${}_A\vartheta_p\left({}_A\vartheta_\infty(L^*({}_AM, 0)^{-1})\right)\mathfrak{A}_p = \mathrm{Det}_{\mathfrak{A}_p}(\Delta(k(\mathfrak{f})))$.

The main result of this article reads:

THEOREM 4.2 *Let k denote a quadratic imaginary field and let p be an odd prime which splits in $k/\mathbb{Q}$ and which does not divide the class number h_k of k. Then Conjecture 4.1 holds.*

COROLLARY 4.3 *Let k denote a quadratic imaginary field and let p be an odd prime which splits in $k/\mathbb{Q}$ and which does not divide the class number h_k of k. Let L be a finite abelian extension of k and $k \subseteq K \subseteq L$. Then the p-part of the ETNC holds for the pair $(h^0(\mathrm{Spec}(L), \mathbb{Z}[\mathrm{Gal}(L/K)]))$.*

PROOF This is implied by well known functorial properties of the ETNC. □

5 THE LIMIT THEOREM

Following [8] or [5] we will deduce Theorem 4.2 from an Iwasawa theoretic result which we will describe next. Let now $p = \mathfrak{p}\bar{\mathfrak{p}}$ denote a split rational prime and $\mathfrak{f}$ an integral $\mathcal{O}_k$-ideal such that $w(\mathfrak{f}) = 1$. In addition, we assume that $\bar{\mathfrak{p}}$ divides $\mathfrak{f}$ whenever $\mathfrak{p}$ divides $\mathfrak{f}$. We write $\mathfrak{f} = \mathfrak{f}_0\mathfrak{p}^\nu, \mathfrak{p} \nmid \mathfrak{f}_0$. We put $\Delta := \mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p})/k) = G_{\mathfrak{f}_0\mathfrak{p}}$ and let

$$\Lambda = \varprojlim_n \mathbb{Z}_p[G_{\mathfrak{f}\mathfrak{p}^n}] \simeq \mathbb{Z}_p[\Delta][[T]]$$

denote the completed group ring. The element $T = \gamma - 1$ depends on the choice of a topological generator γ of $\Gamma := \mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p}^\infty)/k(\mathfrak{f}_0\mathfrak{p})) \simeq \mathbb{Z}_p$.

We will work in the derived category $\mathcal{D}^p(\Lambda)$ and define

$$\Delta^\infty := \varprojlim_n \Delta(k(\mathfrak{f}_0\mathfrak{p}^n)).$$

Then Δ_∞ can be represented by a perfect complex of Λ-modules. For its cohomology groups one obtains $H^i(\Delta^\infty) = 0$ for $i \neq 1, 2$,

$$H^1(\Delta^\infty) \simeq U_{S_p}^\infty := \varprojlim_n \left(\mathcal{O}_{k(\mathfrak{f}_0\mathfrak{p}^n),S_p}^\times \otimes_\mathbb{Z} \mathbb{Z}_p\right)$$

and $H^2(\Delta^\infty)$ fits into the short exact sequence

$$0 \longrightarrow P_{S_p}^\infty \longrightarrow H^2(\Delta^\infty) \longrightarrow X_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}^\infty \longrightarrow 0,$$

where

$$P_{S_p}^\infty := \lim_{\overleftarrow{n}} \left(\mathrm{Pic}(\mathcal{O}_{k(\mathfrak{f}_0\mathfrak{p}^n),S_p}) \otimes_{\mathbb{Z}} \mathbb{Z}_p\right),$$
$$X_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}^\infty := \lim_{\overleftarrow{n}} \left(X_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}(k(\mathfrak{f}_0\mathfrak{p}^n)) \otimes_{\mathbb{Z}} \mathbb{Z}_p\right).$$

The limits over the unit and Picard groups are taken with respect to the norm maps; the transition maps for the definition of $X_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}^\infty$ are defined by sending each place to its restriction.
For $\mathfrak{g} \mid \mathfrak{f}_0$ we put

$$\begin{aligned} \eta_{\mathfrak{g}} &:= \left\{\psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a})\right\}_{n\geq 0} \in U_{S_p}^\infty, \\ \sigma_\infty &:= \left\{\sigma|_{k(\mathfrak{f}_0\mathfrak{p}^{n+1})}\right\}_{n\geq 0} \in Y_{\{w|\mathfrak{f}p\infty\}}^\infty, \end{aligned}$$

where σ is our fixed embedding $\mathbb{Q}^c \hookrightarrow \mathbb{C}$.
For any commutative ring R we write $Q(R)$ for its total ring of fractions. Then $Q(\Lambda)$ is a finite product of fields,

$$Q(\Lambda) \simeq \prod_{\psi \in \hat{\Delta}^{\mathbb{Q}_p}} Q(\psi), \tag{17}$$

where $\hat{\Delta}^{\mathbb{Q}_p}$ denotes the set of $\mathbb{Q}_p$-rational characters of Δ which are associated with the set of $\mathbb{Q}_p$-irreducible representations of Δ. For each $\psi \in \hat{\Delta}^{\mathbb{Q}_p}$ one has

$$Q(\psi) = Q\left(\mathbb{Z}_l(\psi)[[T]][\frac{1}{p}]\right).$$

As in [8] one shows that for each $\psi \in \hat{\Delta}^{\mathbb{Q}_p}$ one has

$$\dim_{Q(\psi)}\left(U_{S_p}^\infty \otimes_\Lambda Q(\psi)\right) = \dim_{Q(\psi)}\left(Y_{\{w|\mathfrak{f}p\infty\}}^\infty \otimes_\Lambda Q(\psi)\right) = 1$$

It follows that the element $e_\psi(\eta_{\mathfrak{f}_0}^{-1} \otimes \sigma_\infty)$ is a $Q(\psi)$-basis of

$$\mathrm{Det}_{Q(\psi)}(\Delta^\infty \otimes_\Lambda Q(\psi)) \simeq \mathrm{Det}_{Q(\psi)}^{-1}(U_{S_p}^\infty \otimes_\Lambda Q(\psi)) \otimes \mathrm{Det}_{Q(\psi)}(X_{\{w|\mathfrak{f}p\infty\}}^\infty \otimes_\Lambda Q(\psi)).$$

Theorem 5.1 *$\Lambda \cdot \mathcal{L} = \mathrm{Det}_\Lambda(\Delta^\infty)$ with $\mathcal{L} = (N\mathfrak{a} - \sigma(\mathfrak{a}))\left(\eta_{\mathfrak{f}_0}^{-1} \otimes \sigma_\infty\right)$.*

Proof By [8, Lem. 5.3] it suffices to show that the equality

$$\Lambda_{\mathfrak{q}} \cdot \mathcal{L} = \mathrm{Det}_{\Lambda_{\mathfrak{q}}}(\Delta^\infty \otimes_\Lambda \Lambda_{\mathfrak{q}}) \tag{18}$$

holds for all height 1 prime ideals of Λ. Such a height 1 prime is called regular (resp. singular) if $p \notin \mathfrak{q}$ (resp. $p \in \mathfrak{q}$).
We first assume that $\mathfrak{q}$ is a regular prime. Then $\Lambda_\mathfrak{q}$ is a discrete valuation ring, in particular, a regular ring. Hence we can work with the cohomology groups of Δ^∞, and in this way, the equality $\Lambda_\mathfrak{q} \cdot \mathcal{L} = \mathrm{Det}_{\Lambda_\mathfrak{q}}(\Delta^\infty \otimes_\Lambda \Lambda_\mathfrak{q})$ is equivalent to

$$\begin{aligned} & (N\mathfrak{a} - \sigma(\mathfrak{a}))\mathrm{Fitt}_{\Lambda_\mathfrak{q}}(\mathbb{Z}_{p,\mathfrak{q}})\,\mathrm{Fitt}_{\Lambda_\mathfrak{q}}\left(U^\infty_{S_p,\mathfrak{q}}/\eta_{\mathfrak{f}_0}\Lambda_\mathfrak{q}\right) \\ = \;& \mathrm{Fitt}_{\Lambda_\mathfrak{q}}\left(P^\infty_{S_p,\mathfrak{q}}\right)\mathrm{Fitt}_{\Lambda_\mathfrak{q}}\left(Y^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\},\mathfrak{q}}/\Lambda_\mathfrak{q}\sigma_\infty\right). \end{aligned} \tag{19}$$

Attached to each regular prime $\mathfrak{q}$ there is a unique character $\psi = \psi_\mathfrak{q} \in \hat{\Delta}^{\mathbb{Q}_p}$. To understand this notion we recall that

$$\Lambda[\frac{1}{p}] \simeq \prod_{\psi \in \hat{\Delta}^{\mathbb{Q}_p}} (\mathbb{Z}_p(\psi)[[T]])\,[\frac{1}{p}].$$

If $p \notin \mathfrak{q}$, then $\Lambda_\mathfrak{q}$ is just a further localisation of $\Lambda[\frac{1}{p}]$, so that exactly one of the above components survives the localization process.
We set

$$\begin{aligned} U^\infty &:= \lim_{\overleftarrow{n}} \left(\mathcal{O}^\times_{k(\mathfrak{f}_0\mathfrak{p}^n)} \otimes_\mathbb{Z} \mathbb{Z}_p\right), \\ P^\infty &:= \lim_{\overleftarrow{n}} \left(\mathrm{Pic}(\mathcal{O}_{k(\mathfrak{f}_0\mathfrak{p}^n)}) \otimes_\mathbb{Z} \mathbb{Z}_p\right). \end{aligned}$$

Remark 5.2 Note that, using the notation of Section 3, one has $P^\infty = A_\infty$. We put $K_n := k(\mathfrak{f}_0\mathfrak{p}^{n+1})$. Mimicking the proof of Leopoldt's conjecture, one can show that for each $n \geq 0$ the natural map $\mathcal{O}^\times_{K_n} \otimes_\mathbb{Z} \mathbb{Z}_p \to U_n$ (semi-local units in $K_n \otimes_k k_\mathfrak{p}$ which are congruent to 1 mod $\mathfrak{p}$) is an injection. It follows that $U^\infty = \bar{\mathcal{E}}_\infty$, where $\bar{\mathcal{E}}_\infty$ is, as in Section 3, the projective limit over the closures of the global units.

There is an exact sequence of Λ-modules

$$0 \longrightarrow U^\infty \longrightarrow U^\infty_{S_p} \longrightarrow Y^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\},\beta} \longrightarrow P^\infty \longrightarrow P^\infty_{S_p} \longrightarrow 0, \tag{20}$$

where

$$Y^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\},\beta} = \lim_{\overleftarrow{n}} \left(Y_{\{w|\mathfrak{f}_0\mathfrak{p}\}}(k(\mathfrak{f}_0\mathfrak{p}^n)) \otimes \mathbb{Z}_p\right)$$

with respect to the transition maps

$$Y_{\{w|\mathfrak{f}_0\mathfrak{p}\}}(k(\mathfrak{f}_0\mathfrak{p}^{n+1}) \overset{\beta_{n+1/n}}{\longrightarrow} Y_{\{w|\mathfrak{f}_0\mathfrak{p}\}}(k(\mathfrak{f}_0\mathfrak{p}^n))$$

induced by $w \mapsto f_{w|v}v$, if v denotes the restriction of w and $f_{w|v}$ the residue degree.
If now $\mathfrak{b}$ is a prime divisor of $\mathfrak{f}_0$ and $n_0 \in \mathbb{N}$ such that there is no further splitting of primes above $\mathfrak{b}$ in $k(\mathfrak{f}_0\mathfrak{p}^\infty)/k(\mathfrak{f}_0\mathfrak{p}^{n_0})$, then $\beta_{m|n}(w) = p^{m-n}w|_{k(\mathfrak{f}_0\mathfrak{p}^{n+1})}$ for all

$m \geq n \geq n_0$. Letting m tend to infinity this shows that $Y^\infty_{\{w|\mathfrak{b}\},\beta} = 0$. Hence we have an exact sequence of Λ-modules

$$0 \longrightarrow U^\infty \longrightarrow U^\infty_{S_p} \longrightarrow Y^\infty_{\{w|\mathfrak{p}\},\beta} \longrightarrow P^\infty \longrightarrow P^\infty_{S_p} \longrightarrow 0. \tag{21}$$

In addition, one has the exact sequence

$$0 \longrightarrow X^\infty_{\{w|\mathfrak{f}_0\}} \longrightarrow X^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}} \longrightarrow Y^\infty_{\{w|\mathfrak{p}\}} \oplus Y^\infty_{\{w|\infty\}} \longrightarrow 0. \tag{22}$$

Remark 5.3 Note that the transition maps in the first two limits are induced by restriction, which coincides with $\beta_{n+1|n}$ for the places above $\mathfrak{p}$ and ∞. Hence $Y_{\{w|\infty\}} = Y_{\{w|\infty\},\beta}$ and $Y_{\{w|\mathfrak{p}\}} = Y_{\{w|\mathfrak{p}\},\beta}$.

We observe that $Y^\infty_{\{w|\infty\},\mathfrak{q}} = \Lambda_\mathfrak{q} \cdot \sigma_\infty$. Putting together (21) and (22) we therefore deduce that (19) is equivalent to

$$(N\mathfrak{a} - \sigma(\mathfrak{a}))\mathrm{Fitt}_{\Lambda_\mathfrak{q}}\left(U^\infty_\mathfrak{q}/\eta_{\mathfrak{f}_0}\Lambda_\mathfrak{q}\right) = \mathrm{Fitt}_{\Lambda_\mathfrak{q}}\left(P^\infty_\mathfrak{q}\right)\mathrm{Fitt}_{\Lambda_\mathfrak{q}}\left(X_{\{w|\mathfrak{f}_0\},\mathfrak{q}}\right). \tag{23}$$

Let $\mathfrak{d}$ be a divisor of $\mathfrak{f}_0$ such that $\psi_\mathfrak{q}$ has conductor $\mathfrak{d}$ or $\mathfrak{d}\mathfrak{p}$. For any prime divisor $\mathfrak{l} \mid \mathfrak{f}_0$ we write $I_\mathfrak{l} \subseteq D_\mathfrak{l} \subseteq G_{\mathfrak{f}_0\mathfrak{p}^\infty}$ for the inertia and decomposition subgroups at $\mathfrak{l}$. Let $\mathrm{Fr}_\mathfrak{l}$ denote a lift of the Frobenius element in $D_\mathfrak{l}/I_\mathfrak{l}$. We view ψ as a character of $G_{\mathfrak{f}_0\mathfrak{p}^\infty}$ via inflation and note that if $\mathfrak{l} \nmid \mathfrak{d}$ (i.e. $\psi|_{I_\mathfrak{l}} = 1$), then $\mathrm{Fr}_\mathfrak{l}$ is a well defined element in $\Lambda_\mathfrak{q}$.

Lemma 5.4 *Let*

$$\varepsilon = \begin{cases} 0, & \psi \neq 1, \\ 1, & \psi = 1. \end{cases}$$

Then:

$$\mathrm{Fitt}_{\Lambda_\mathfrak{q}}(\Lambda_\mathfrak{q} T^\varepsilon \eta_\mathfrak{d}/\Lambda_\mathfrak{q}\eta_{\mathfrak{f}_0}) = T^{-\varepsilon}\prod_{\mathfrak{l}|\mathfrak{f}_0, \mathfrak{l}\nmid\mathfrak{d}} (1 - \mathrm{Fr}_\mathfrak{l}^{-1})\Lambda_\mathfrak{q} = \mathrm{Fitt}_{\Lambda_\mathfrak{q}}(X^\infty_{\{w|\mathfrak{f}_0\},\mathfrak{q}}).$$

Lemma 5.5

$$\mathrm{Fitt}_{\Lambda_\mathfrak{q}}(U^\infty_\mathfrak{q}/\Lambda_\mathfrak{q} T^\varepsilon \eta_\mathfrak{d}) = (N\mathfrak{a} - \sigma(\mathfrak{a}))\mathrm{Fitt}_{\Lambda_\mathfrak{q}}(P^\infty_\mathfrak{q})$$

Proof of Lemma 5.5: Let $\psi = \psi_\mathfrak{q}$. By the Iwasawa main conjecture (Theorem 3.1) and Remark 5.2 we have

$$\mathrm{char}(P^\infty_\psi) = \mathrm{char}\left((U^\infty/\bar{\mathcal{C}}_\infty)_\psi\right),$$

where (again by a slight abuse of notation) for a Λ-module M we set $M_\psi := M_\eta$ for any $\eta \in \psi$.

The corollary to [16, App. Prop. 2] implies that

$$\mathrm{Fitt}_{\Lambda_\mathfrak{q}}(P^\infty_\mathfrak{q}) = \mathrm{Fitt}_{\Lambda_\mathfrak{q}}\left((U^\infty/\bar{\mathcal{C}}_\infty)_\mathfrak{q}\right).$$

Hence it suffices to show that

$$\bar{\mathcal{C}}_\infty(\mathfrak{a})_\mathfrak{q} = \Lambda_\mathfrak{q} \cdot T^\varepsilon \eta_\mathfrak{d}, \tag{24}$$

$$\mathrm{Fitt}_{\Lambda_\mathfrak{q}}(\bar{\mathcal{C}}_{\infty,\mathfrak{q}}/\bar{\mathcal{C}}_\infty(\mathfrak{a})_\mathfrak{q}) = (N\mathfrak{a} - \sigma(\mathfrak{a}))\Lambda_\mathfrak{q}. \tag{25}$$

Here $\bar{\mathcal{C}}_\infty(\mathfrak{a})$ is the projective limit over

$$\bar{\mathcal{C}}_n(\mathfrak{a}) = \text{ closure of } \langle \psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a})\colon \mathfrak{g} \mid \mathfrak{f}_0 \rangle_{\mathbb{Z}[\mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p}^{n+1})/k)]} \cap \mathcal{E}_n.$$

(Note that $\Lambda_\mathfrak{q}\eta_\mathfrak{d}$ is for $\psi \neq 1$ a group of units. This is true even for $\mathfrak{d} = 1$, because $\Lambda_\mathfrak{q}\eta_1 = \Lambda_\mathfrak{q} e_\psi \eta_1$ and e_ψ has augmentation 0.)
In order to prove (24) we set

$$\psi_n := \psi(1; \mathfrak{d}\mathfrak{p}^{n+1}, \mathfrak{a}), \quad G_n := \mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p}^{n+1})/k), \quad \Lambda_n := \mathbb{Z}_p[G_n].$$

If $\mathfrak{b}_n$ denotes the annihilator of ψ_n in Λ_n, then we have the following exact sequence of inverse systems of finitely generated $\mathbb{Z}_p$-modules

$$0 \longrightarrow (\Lambda_n/\mathfrak{b}_n)_n \longrightarrow \left(\bar{\mathcal{C}}_n(\mathfrak{a})\right)_n \longrightarrow \left(\bar{\mathcal{C}}_n(\mathfrak{a})/\Lambda_n\psi_n\right)_n \longrightarrow 0.$$

The topology of $\mathbb{Z}_p$ induces on each of these modules the structure of a compact topological group, so that [27, Prop. B.1.1] implies that $\varprojlim_n$ is exact. Hence we obtain the short exact sequence of Λ-modules

$$0 \longrightarrow \varprojlim_n (\Lambda_n/\mathfrak{b}_n) \longrightarrow \bar{\mathcal{C}}_\infty(\mathfrak{a}) \longrightarrow \varprojlim_n \left(\bar{\mathcal{C}}_n(\mathfrak{a})/\Lambda_n\psi_n\right) \longrightarrow 0.$$

Again by [27, Prop. B.1.1] we obtain

$$\varprojlim_n (\Lambda_n/\mathfrak{b}_n) \simeq \Lambda/\varprojlim_n \mathfrak{b}_n \simeq \Lambda\eta_\mathfrak{d},$$

so that

$$\bar{\mathcal{C}}_\infty(\mathfrak{a})/\Lambda\eta_\mathfrak{d} \simeq \varprojlim_n (\bar{\mathcal{C}}_n(\mathfrak{a})/\Lambda\psi_n). \tag{26}$$

For $\mathfrak{d} \mid \mathfrak{f}_0$ we identify $\mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p}^{n+1})/k(\mathfrak{d}\mathfrak{p}^{n+1}))$ and $\mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{d}\mathfrak{p}))$. Then one has (in additive notation) for any $\mathfrak{g}$ with $\mathfrak{d} \mid \mathfrak{g} \mid \mathfrak{f}_0$ the distribution relation

$$\begin{aligned} & N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{d}\mathfrak{p})}\left(\psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a})\right) \\ = \; & [k(\mathfrak{f}_0\mathfrak{p}) : k(\mathfrak{g}\mathfrak{p})] \left(\prod_{\mathfrak{l} \mid \mathfrak{g}, \mathfrak{l} \nmid \mathfrak{d}} (1 - \mathrm{Fr}_\mathfrak{l}^{-1}) \right) \psi(1; \mathfrak{d}\mathfrak{p}^{n+1}, \mathfrak{a}). \end{aligned} \tag{27}$$

In addition, one obviously has

$$[k(\mathfrak{f}_0\mathfrak{p}) : k(\mathfrak{g}\mathfrak{p})]\psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a}) = N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{g}\mathfrak{p})}\left(\psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a})\right). \tag{28}$$

Note that for $\psi \neq 1$ and $\mathfrak{d} \nmid \mathfrak{g}$ one has $\psi(N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{g}\mathfrak{p})}) = 0$. Hence, if $\psi \neq 1$, then (27), (28) and (26) show that

$$A := \left(\prod_{\mathfrak{g} | \mathfrak{f}_0, \mathfrak{d} \nmid \mathfrak{g}} [k(\mathfrak{f}_0\mathfrak{p}) : k(\mathfrak{g}\mathfrak{p})] \right) \cdot N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{d}\mathfrak{p})}$$

annihilates $\bar{\mathcal{C}}_\infty(\mathfrak{a})/\Lambda\eta_{\mathfrak{d}}$. Since $\psi(A) \in \mathbb{Z}_p$ is non-trivial and p is invertible in $\Lambda_{\mathfrak{q}}$, the element A is a actually a unit in $\Lambda_{\mathfrak{q}}$, which implies $\bar{\mathcal{C}}_\infty(\mathfrak{a})_{\mathfrak{q}} = \Lambda_{\mathfrak{q}}\eta_{\mathfrak{d}}$.
If $\psi = 1$ we proceed in almost the same way, but now set $\psi_n := \psi(1; \mathfrak{p}^{n+1}, \mathfrak{a})^{\gamma - 1}$. In this case we have $\mathfrak{d} = 1$.

Sublemma: Let $\{C_n, f_n\}_{n \geq 0}$ be a projective system of finitely generated $\mathbb{Z}_p[G_n]$-modules and set $C_\infty = \varprojlim_n C_n$. Let $\mathfrak{q}$ denote a regular prime and let $\psi = \psi_{\mathfrak{q}}$. Then:

$$C_{\infty,\mathfrak{q}} \simeq (\varprojlim_n C_{n,\psi})_{\mathfrak{q}}.$$

Proof of Sublemma: The natural map $C_n \longrightarrow \oplus_{\chi \in \hat{\Delta}^{\mathbb{Q}_p}} C_{n,\chi}$ has kernel and cokernel annihilated by $|\Delta|$. Passing to the limit we obtain (again by [27, B.1.1]) an exact sequence of Λ-modules

$$0 \longrightarrow W_\infty \longrightarrow C_\infty \longrightarrow \bigoplus_{\chi \in \hat{\Delta}^{\mathbb{Q}_p}} \varprojlim_n C_{n,\chi} \longrightarrow X_\infty \longrightarrow 0,$$

where W_∞ and X_∞ are annihilated by $|\Delta|$. Since $|\Delta| \in \Lambda_{\mathfrak{q}}^\times$ we obtain

$$C_{\infty,\mathfrak{q}} \simeq \left(\bigoplus_{\chi \in \hat{\Delta}^{\mathbb{Q}_p}} \varprojlim_n C_{n,\chi} \right)_{\mathfrak{q}} = \left(\varprojlim_n C_{n,\psi} \right)_{\mathfrak{q}}.$$

□

Arguing as in the case $\psi \neq 1$ and applying the Sublemma we obtain

$$\left(\bar{\mathcal{C}}_\infty(\mathfrak{a})/\Lambda T \eta_{\mathfrak{d}}\right)_{\mathfrak{q}} \simeq \left(\varprojlim_n (\bar{\mathcal{C}}_n(\mathfrak{a})/\Lambda_n \psi_n) \right)_{\mathfrak{q}} \simeq \left(\varprojlim_n (\bar{\mathcal{C}}_n(\mathfrak{a})/\Lambda_n \psi_n)_\psi \right)_{\mathfrak{q}}.$$

Hence it suffices to show that each of the modules $(\bar{\mathcal{C}}_n(\mathfrak{a})/\Lambda_n\psi_n)_\psi$ is annihilated by the unit $N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{p})}$. If

$$\prod_{\mathfrak{g} \neq 1} \psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a})^{\alpha_{\mathfrak{g}}} \cdot \psi(1; \mathfrak{p}^{n+1}, \mathfrak{a})^{\alpha_1} \text{ with } \alpha_1, \alpha_{\mathfrak{g}} \in \mathbb{Z}_p[G_n]$$

is a unit in $K_n = k(\mathfrak{f}_0\mathfrak{p}^{n+1})$, then the prime ideal factorization of the singular values $\psi(1; \mathfrak{g}\mathfrak{p}^{n+1}, \mathfrak{a})$ (see [1, Th. 2.4]) implies that α_1 has augmentation 0. It follows that $\psi(\alpha_1) \in \mathbb{Z}_p[\mathrm{Gal}(K_n/K_0)]$ is divisible by $\gamma - 1$. For any element $\sigma \in G_n$ we write $\sigma = \gamma(\sigma)\delta(\sigma)$ according to the decomposition $G_n = \mathrm{Gal}(K_n/K_0) \times \Delta$. If $\mathfrak{g} \neq 1$ each of the factors $\psi(1 - \mathrm{Fr}_{\mathfrak{l}}^{-1}) = 1 - \gamma(\mathrm{Fr}_{\mathfrak{l}})^{-1}$ in (27) is divisible by $\gamma - 1$.

Altogether this implies that $N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{p})}$ annihilates $\left(\bar{\mathcal{C}}_\infty(\mathfrak{a})/\Lambda T\eta_{\mathfrak{d}}\right)_{\mathfrak{q}}$, hence $\bar{\mathcal{C}}_\infty(\mathfrak{a})_{\mathfrak{q}} = \Lambda_{\mathfrak{q}} T\eta_{\mathfrak{d}}$.

It finally remains to prove (25). For any integral ideal $\mathfrak{m}$ and any two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $(\mathfrak{ab}, 6\mathfrak{m}) = 1$ one has the relation

$$\psi(1; \mathfrak{m}, \mathfrak{a})^{N\mathfrak{b} - \sigma(\mathfrak{b})} = \psi(1; \mathfrak{m}, \mathfrak{b})^{N\mathfrak{a} - \sigma(\mathfrak{a})}. \tag{29}$$

This is a straightforward consequence of [1, Prop. 2.2] and the definition of ψ, see in particular [20, Théorème principal (b) and Remarque 1 (g)]. Equality (29) shows that $N\mathfrak{a} - \sigma(\mathfrak{a})$ annihilates $\bar{\mathcal{C}}_{\infty,\mathfrak{q}}/\bar{\mathcal{C}}_\infty(\mathfrak{a})_{\mathfrak{q}}$. Using the same arguments as in the proof of Lemma 3.5 (see that paragraph following Claim 2), one shows that this module is generated by one element. By [16, App. 3 and 8] it therefore suffices to show that $(N\mathfrak{a} - \sigma(\mathfrak{a}))\Lambda_{\mathfrak{q}}$ is the exact annihilator. From Lemma 5.6 below we obtain finitely many ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_s$ and $n_1, \dots, n_s \in \Lambda_{\mathfrak{q}}$ such that

$$1 = \sum_{i=1}^{s} n_i(N\mathfrak{a}_i - \sigma(\mathfrak{a}_i)).$$

Consider the element $\eta := T^\varepsilon \prod_{i=1}^s \eta_{\mathfrak{d}}(\mathfrak{a}_i)^{n_i}$, where $\eta_{\mathfrak{d}}(\mathfrak{a}_i) := \{\psi(1; \mathfrak{d}\mathfrak{p}^{n+1}, \mathfrak{a}_i)\}_{n=0}^\infty$. One has

$$\eta^{N\mathfrak{a} - \sigma(\mathfrak{a})} = T^\varepsilon \eta_{\mathfrak{d}}.$$

As a consequence of Lemma 3.5, Claim 2, the module $\bar{\mathcal{C}}_\infty(\mathfrak{a})_{\mathfrak{q}} = \Lambda_{\mathfrak{q}} T^\varepsilon \eta_{\mathfrak{d}}$ is $\Lambda_{\mathfrak{q}}$-free. It follows that no divisor of $N\mathfrak{a} - \sigma(\mathfrak{a})$ annihilates the quotient $\bar{\mathcal{C}}_{\infty,\mathfrak{q}}/\bar{\mathcal{C}}_\infty(\mathfrak{a})_{\mathfrak{q}}$.

To complete the proof for the localization at regular primes $\mathfrak{q}$ we add the following

Lemma 5.6 *Let $\psi \in \hat{\Delta}^{\mathbb{Q}_p}$, $\eta \in \psi$ and write $R = \mathbb{Z}_l(\psi) = \mathbb{Z}_l(\eta)$. Let I denote the ideal of $\Lambda_\psi = R[[\Gamma]]$ generated by the elements $N\mathfrak{a} - \sigma(\mathfrak{a}) = N\mathfrak{a} - \eta(\mathfrak{a})\gamma(\mathfrak{a})$, where $\mathfrak{a}$ runs through the integral ideals of $\mathcal{O}_k$ such that $(\mathfrak{a}, 6\mathfrak{f}\mathfrak{p}) = 1$. Then $I\Lambda_\psi[\frac{1}{p}] = \Lambda_\psi[\frac{1}{p}]$.*

Proof As usual we identify $R[[\Gamma]]$ with $R[[T]]$ by identifying γ with $1 + T$. We note that $\Lambda_\psi[\frac{1}{p}]$ is a principal ideal domain whose irreducible elements are given by the irreducible distinguished polynomials $f \in R[T]$. We fix such f and write

$$f(T) = \gamma^s + a_{s-1}\gamma^{s-1} + \ldots + a_1\gamma + a_0, \quad a_i \in R.$$

For any n there exist ideals $\mathfrak{a}_0, \dots, \mathfrak{a}_s$ (depending on n) such that $(\mathfrak{a}_i, 6\mathfrak{f}\mathfrak{p}) = 1$ and $\sigma(\mathfrak{a}_i)|_{K_n} = \gamma^i|_{K_n}$. In particular, this implies $\eta(\mathfrak{a}_i) = \gamma^i$ and

$$\sum_{i=0}^{s} a_i(N\mathfrak{a}_i - \sigma(\mathfrak{a}_i)) \equiv \sum_{i=0}^{s} a_i N\mathfrak{a}_i - f(T) (\mathrm{mod}\ (\gamma^{p^n} - 1)\Lambda_\psi).$$

Inverting p we derive

$$\sum_{i=0}^{s} a_i'(N\mathfrak{a}_i - \sigma(\mathfrak{a}_i)) \equiv 1 - cf(T)(\mathrm{mod}\ (\gamma^{p^n} - 1)\Lambda_\psi[\frac{1}{p}])$$

with $a_1', \dots, a_s', c \in \mathbb{Q}_p(\psi) = \mathbb{Q}_p(\eta)$. Therefore

$$1 \in I\Lambda_\psi[\frac{1}{p}] + f\Lambda_\psi[\frac{1}{p}] + \bigcap_n (\gamma^{p^n} - 1)\Lambda_\psi[\frac{1}{p}].$$

Since $(\gamma^{p^n} - 1)\Lambda_\psi[\frac{1}{p}]$ is a strictly decreasing sequence of ideals in a principal ideal domain we obtain $\bigcap_n (\gamma^{p^n} - 1)\Lambda_\psi[\frac{1}{p}] = (0)$. Consequently, $I\Lambda_\psi[\frac{1}{p}] + f\Lambda_\psi[\frac{1}{p}] = \Lambda_\psi[\frac{1}{p}]$ for every irreducible distinguished polynomial f and the lemma is proved. □

We now assume that $\mathfrak{q}$ is a singular prime. We write $\Delta = \Delta' \times P$ with $p \nmid |\Delta'|$ and note that the singular primes $\mathfrak{q}$ are in one-to-one correspondence with the $\mathbb{Q}_p$-rational irreducible characters of Δ' ([5, Lem. 6.2(i)]). Assume that in this way $\mathfrak{q}$ is associated with $\psi \in \hat{\Delta}'^{\mathbb{Q}_p}$ and set $\chi = \psi \times \eta$, where $\eta \in \hat{P}$ is arbitrarily chosen. From [6, III,2.1 Theorem] and [6, III,1.7 (13)] we know that the μ-invariant of $P_\chi^\infty := P^\infty \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)$ vanishes. By [8, Lem. 5.6] it follows that $P_\mathfrak{q}^\infty = 0$. The module $X_{\{w|\mathfrak{f}_0\mathfrak{p}\}}^\infty$ is $\mathbb{Z}_p[[T]]$-torsion and free over $\mathbb{Z}_p$, hence has vanishing μ-invariant (as $\mathbb{Z}_p[[T]]$-module). Again by [8, Lem. 5.6] we derive $X_{\{w|\mathfrak{f}_0\mathfrak{p}\},\mathfrak{q}}^\infty = 0$. Since $P_{S_p}^\infty$ is an epimorphic image of P^∞ and because of the exactness of

$$0 \longrightarrow X_{\{w|\mathfrak{f}_0\mathfrak{p}\}}^\infty \longrightarrow X_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}^\infty \longrightarrow Y_{\{w|\infty\}}^\infty \longrightarrow 0$$

we derive

$$H^2(\Delta^\infty)_\mathfrak{q} = Y_{\{w|\infty\},\mathfrak{q}}^\infty \simeq \Lambda_\mathfrak{q}\sigma_\infty.$$

We now compute $H^1(\Delta^\infty)_\mathfrak{q}$. Consider the filtration

$$\Lambda \cdot \eta_{\mathfrak{f}_0} \subseteq \bar{\mathcal{C}}_\infty(\mathfrak{a}) \subseteq \bar{\mathcal{C}}_\infty \subseteq U^\infty \subseteq U_{S_p}^\infty = H^1(\Delta^\infty).$$

By (21) the quotient $U_{S_p}^\infty / U^\infty$ injects into $Y_{\{w|\mathfrak{p}\}}^\infty$. This module is a finite free $\mathbb{Z}_p$-module and hence has vanishing μ-invariant. The module $U^\infty/\bar{\mathcal{C}}_\infty$ (or rather any of its χ-components) also has vanishing μ-invariant by [6, III, 2.1 Theorem and 1.7 (13)]. As shown above, the graded piece $\bar{\mathcal{C}}_\infty/\bar{\mathcal{C}}_\infty(\mathfrak{a})$ is annihilated by $N\mathfrak{a} - \sigma(\mathfrak{a})$. We claim that $N\mathfrak{a} - \sigma(\mathfrak{a}) \in \Lambda_\mathfrak{q}^\times$. In order to prove the claim we note that $N\mathfrak{a} - \sigma(\mathfrak{a}) = N\mathfrak{a} - \delta(\mathfrak{a})(1+T)^w$ with $w \in \mathbb{Z}_p$ and $w \neq 0$ (since $\sigma(\mathfrak{a})$ has infinite order in $G_{\mathfrak{f}_0\mathfrak{p}^\infty}$). Let π denote a prime element in $\mathbb{Z}_p(\psi)$. Then the explicit description of $\mathfrak{q}$ given in [5, Lem. 6.2] easily implies $\mathfrak{q} = (\pi, \Delta P)[[T]]$, where ΔP is the kernel of the augmentation map $\mathbb{Z}_p(\psi)[P] \to \mathbb{Z}_p(\psi)$. Therefore $\Lambda/\mathfrak{q} \simeq (\mathbb{Z}_p(\psi)/\pi))[[T]]$. Hence it suffices to show that the image of $N\mathfrak{a} - \sigma(\mathfrak{a})$ under

$$\Lambda \longrightarrow \mathbb{Z}_p(\psi)[[T]] \longrightarrow (\mathbb{Z}_p(\psi)/\pi)\,[[T]] = \Lambda/\mathfrak{q}$$

given by $N\mathfrak{a} - \psi(\mathfrak{a})(1+T)^w$ is non-trivial. This, in turn, is an easy exercise. Finally we will use the distribution relation

$$N_{k(\mathfrak{f}_0\mathfrak{p}^{n+1})/k(frg\mathfrak{p}^{n+1})}\psi(1;\mathfrak{f}_0\mathfrak{p}^{n+1},\mathfrak{a}) = \left(\prod_{\mathfrak{l}|\mathfrak{f}_0,\mathfrak{l}\nmid\mathfrak{g}}(1-\mathrm{Fr}_{\mathfrak{l}}^{-1})\right)\psi(1;\mathfrak{g}\mathfrak{p}^{n+1},\mathfrak{a}) \quad (30)$$

to show that $\bar{\mathcal{C}}_\infty(\mathfrak{a})_\mathfrak{q}/\Lambda_\mathfrak{q}\eta_{\mathfrak{f}_0}$ is trivial. Indeed, a statement similar to (26) shows that this quotient is annihilated by $\prod_{\mathfrak{l}|\mathfrak{f}_0}(1-\mathrm{Fr}_{\mathfrak{l}}^{-1})$, which is a unit in $\Lambda_\mathfrak{q}$ (same argument as with $N\mathfrak{a}-\sigma(\mathfrak{a})$ as above).
In conclusion, we have now shown that $\Delta_\mathfrak{q}^\infty$ has perfect cohomology, so that again (18) is equivalent to (19), which is trivially valid because all modules involved have trivial μ-invariants. □

In the following we want to deduce Conjecture 4.1 from Theorem 5.1. Again we can almost word by word rely on Flach's exposition [8].
We have a ring homomorphism

$$\Lambda \longrightarrow \mathbb{Z}_p[G_\mathfrak{f}] = \mathfrak{A}_p \subseteq A_p = \prod_{\chi\in\hat{G}_\mathfrak{f}^{\mathbb{Q}_p}} \mathbb{Q}_p(\chi),$$

a canonical isomorphism of complexes

$$\Delta^\infty \otimes_\Lambda^{\mathbf{L}} \mathfrak{A}_p \simeq \Delta(k(\mathfrak{f})), \quad (31)$$

and a canonical isomorphism of determinants

$$(\mathrm{Det}_\Lambda\Delta^\infty)\otimes_\Lambda\mathfrak{A}_p \simeq \mathrm{Det}_{\mathfrak{A}_p}(\Delta(k(\mathfrak{f})))$$

It remains to verify that the image of the element $\mathcal{L}\otimes 1$ in $\mathrm{Det}_{\mathfrak{A}_p}(\Delta(k(\mathfrak{f}))) \subseteq \mathrm{Det}_{A_p}\left(\Delta(k(\mathfrak{f}))\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\right)$ agrees with ${}_A\vartheta_p\left({}_A\vartheta_\infty(L^*({}_AM,0)^{-1})\right)$. Let δ denote the morphism such that the following diagram commutes

$$\begin{array}{ccc}
\mathrm{Det}_{Q(\Lambda)}(\Delta^\infty\otimes_\Lambda Q(\Lambda))\otimes_{Q(\Lambda)}A_p & \xrightarrow{\simeq} & \mathrm{Det}_{Q(\Lambda)}(H^\bullet(\Delta^\infty\otimes_\Lambda Q(\Lambda)))\otimes_{Q(\Lambda)}A_p \\
\simeq\downarrow & & \downarrow\delta \\
\mathrm{Det}_{A_p}(\Delta(k(\mathfrak{f}))\otimes_{\mathbb{Z}_p}\mathbb{Q}_p) & \xrightarrow{\simeq} & \mathrm{Det}_{A_p}(H^\bullet(\Delta(k(\mathfrak{f}))\otimes_{\mathbb{Z}_p}\mathbb{Q}_p))
\end{array}$$

We let

$$\begin{aligned}
\phi \quad : \quad & \mathrm{Det}_{\mathbb{Q}_p(\chi)}\left(\Delta(k(\mathfrak{f}))\otimes_{\mathfrak{A}_p}\mathbb{Q}_p(\chi)\right) \\
\simeq \quad & \begin{cases} \mathrm{Det}^{-1}_{\mathbb{Q}_p(\chi)}(\mathcal{O}^\times_{k(\mathfrak{f})}\otimes_{\mathfrak{A}_p}\mathbb{Q}_p(\chi))\otimes_{\mathbb{Q}_p(\chi)}\mathrm{Det}_{\mathbb{Q}_p(\chi)}(X_{\{v|\infty\}}\otimes_{\mathfrak{A}_p}\mathbb{Q}_p(\chi)), & \chi\neq 1, \\ \mathbb{Q}, & \chi = 1 \end{cases}
\end{aligned}$$

denote the isomorphism induced by φ_1^{-1} and φ_3^{-1} (see (13), (14) and (16)). Note that ϕ is defined in terms of cohomology. Then we have to show that

$$\left(\prod_{v\in S_p}\left(\mathcal{E}_v^{\#}\right)^{-1}\right)\phi(\delta(\mathcal{L}\otimes 1)) \tag{32}$$
$$= \begin{cases} w(\mathfrak{f}_\chi)[k(\mathfrak{f}):k(\mathfrak{f}_\chi)](N\mathfrak{a}-\chi(\mathfrak{a}))e_\chi\xi_\chi^{-1}\otimes w_\infty, & \mathfrak{f}_\chi\neq 1,\\ w(1)[k(\mathfrak{f}):k(1)](1-\chi(\mathfrak{p})^{-1})(N\mathfrak{a}-\chi(\mathfrak{a}))e_\chi\xi_\chi^{-1}\otimes w_\infty, & \mathfrak{f}_\chi=1,\chi\neq 1\\ L(\chi,0)^{-1}, & \chi=1.\end{cases}$$

By abuse of notation we also write χ for the composite ring homomorphism $\Lambda\to\mathbb{Q}_p(\chi)$ and denote its kernel by $\mathfrak{q}_\chi$. Then $\mathfrak{q}_\chi$ is a regular prime of Λ and $\Lambda_{\mathfrak{q}_\chi}$ is a discrete valuation ring with residue field $\mathbb{Q}_p(\chi)$. We consider χ as a character of $\mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p}^\infty)/k)$. If $\chi=\psi\times\eta$ with $\psi\in\hat{\Delta}$ and η a character of $\mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p}^\infty)/k(\mathfrak{f}_0\mathfrak{p}))$, then the quotient field of $\Lambda_{\mathfrak{q}_\chi}$ is given by $Q(\psi)$ (notation as in (17)). We set

$$\mathfrak{f}_1=\begin{cases}\mathfrak{f}, & \text{if } \mathfrak{p}\mid\mathfrak{f},\\ \mathfrak{f}\mathfrak{p}, & \text{if } \mathfrak{p}\nmid\mathfrak{f}.\end{cases}$$

Let p^n be the degree of $k(\mathfrak{f}_1)/k(\mathfrak{f}_0\mathfrak{p})$.

Lemma 5.7 *The element $\bar{\omega}:=1-\gamma^{p^n}$ is a uniformizing element for $\Lambda_{\mathfrak{q}_\chi}$.*

Proof We have to show that after localisation at $\mathfrak{q}_\chi$ the kernel of χ is generated by $\bar{\omega}$. Since the idempotents e_ψ and e_η associated with ψ and η, respectively, are units in $\Lambda_{\mathfrak{q}_\chi}$, one has $\left(\Lambda[\frac{1}{p}]\right)_{\mathfrak{q}_\chi}=\left((\mathbb{Z}_p(\psi)[[T]][\frac{1}{p}]\right)_{\mathfrak{q}_\chi}$ and $(\mathbb{Q}_p(\psi)][\Gamma_n])_{\mathfrak{q}_\chi}=\mathbb{Q}_p(\chi)$. This immediately implies the result. ∎

We apply [8, Lem. 5.7] to

$$R=\Lambda_{\mathfrak{q}_\chi},\quad \Delta=\Delta^\infty_{\mathfrak{q}_\chi},\quad \bar{\omega}=1-\gamma^{p^n}.$$

For a R-module M we put $M_{\bar{\omega}}:=\{m\in M\mid \bar{\omega}m=0\}$ and $M/\bar{\omega}:=M/\bar{\omega}M$. As we already know, the cohomology of Δ is concentrated in degrees 1 and 2. We will see that the R-torsion subgroup of $H^i(\Delta), i=1,2$, is annihilated by $\bar{\omega}$, hence $H^i(\Delta)_{\mathrm{tors}}=H^i(\Delta)_{\bar{\omega}}$. We define free R-modules M^i, $i=1,2$, by the short exact sequences

$$0\longrightarrow H^i(\Delta)_{\bar{\omega}}\longrightarrow H^i(\Delta)\longrightarrow M^i\longrightarrow 0,$$

and consider the exact sequences of $\mathbb{Q}_p(\chi)$-vector spaces

$$0\longrightarrow H^i(\Delta)/\bar{\omega}\longrightarrow H^i(\Delta\otimes^{\mathbf{L}}_R\mathbb{Q}_p(\chi))\longrightarrow H^{i+1}(\Delta)_{\bar{\omega}}\longrightarrow 0$$

induced by the distinguished triangle

$$\Delta\xrightarrow{\bar{\omega}}\Delta\longrightarrow\Delta\otimes^{\mathbf{L}}_R\mathbb{Q}_p(\chi)\longrightarrow\Delta[1].$$

Then the map $\phi_{\bar\omega}$ of [8, Lem. 5.7] is induced by the exact sequence of $\mathbb{Q}_p(\chi)$-vector spaces

$$0 \longrightarrow M^1/\bar\omega \longrightarrow H^1(\Delta \otimes^{\mathbf{L}}_R \mathbb{Q}_p(\chi)) \xrightarrow{\beta_{\bar\omega}} H^2(\Delta \otimes^{\mathbf{L}}_R \mathbb{Q}_p(\chi)) \longrightarrow M^2/\bar\omega \longrightarrow 0, \tag{33}$$

where the Bockstein map $\beta_{\bar\omega}$ is given by the composite

$$H^1(\Delta \otimes^{\mathbf{L}}_R \mathbb{Q}_p(\chi)) \longrightarrow H^2(\Delta)_{\bar\omega} \longrightarrow H^2(\Delta)/\bar\omega \longrightarrow H^2(\Delta \otimes^{\mathbf{L}}_R \mathbb{Q}_p(\chi)).$$

Note that for the exactness of (33) on the left we need to show that $H^1(\Delta)$ is torsion-free.
We recall that $\mathrm{Gal}(k(\mathfrak{f}_0\mathfrak{p}^{n+1})/k(\mathfrak{f}_0\mathfrak{p})) = \mathrm{Gal}(K_n/K_0)$ is isomorphic to $(1+\mathfrak{f}_0\mathfrak{p})/(1+\mathfrak{f}_0\mathfrak{p}^{n+1}) \simeq (1+p\mathbb{Z}_p)/(1+p^{n+1}\mathbb{Z}_p)$ via the Artin map. As before we denote this isomorphism by $\sigma : (1+p\mathbb{Z}_p)/(1+p^{n+1}\mathbb{Z}_p) \to \mathrm{Gal}(K_n/K_0)$ and also write $\sigma : 1+p\mathbb{Z}_p \to \Gamma$. Passing to the limit we obtain a character

$$\chi_{\mathrm{ell}} \colon \Gamma \longrightarrow 1+p\mathbb{Z}_p$$

uniquely defined by $\sigma(\chi_{\mathrm{ell}}(\tau) \bmod (1+p^{n+1}\mathbb{Z}_p)) = \tau|_{K_n}$ for all $\tau \in \Gamma$. Note that one has

$$\psi(1;\mathfrak{f}_0\mathfrak{p}^{n+1},\mathfrak{a})^\tau = \psi(\chi_{\mathrm{ell}}(\tau);\mathfrak{f}_0\mathfrak{p}^{n+1},\mathfrak{a})$$

for all $n \geq 0$ and $\tau \in \Gamma$.
For a place $w \mid \mathfrak{p}$ in $k(\mathfrak{f})/k$ and $u \in k(\mathfrak{f})$ we write $u_w = \sigma_w(u)$, where $\sigma_w : \mathbb{Q}^c \to \mathbb{Q}_p^c$ defines w.

Lemma 5.8 *Define for $\mathfrak{l} \mid \mathfrak{f}_0$ the element $c_\mathfrak{l} \in \mathbb{Z}_p$ by $\gamma^{c_\mathfrak{l} p^n} = \mathrm{Fr}_\mathfrak{l}^{-f_\mathfrak{l}}$, where $f_\mathfrak{l} \in \mathbb{Z}$ is the residue degree at $\mathfrak{l}$ of $k(\mathfrak{f})/k$. Put $c_\mathfrak{p} = \log_p(\chi_{\mathrm{ell}}(\gamma^{p^n}))^{-1} \in \mathbb{Q}_p$. Then $\beta_{\bar\omega}$ is induced by the map*

$$H^1(\Delta(k(\mathfrak{f})))\otimes\mathbb{Q}_p = \mathcal{O}^\times_{k(\mathfrak{f}),S_p}\otimes\mathbb{Q}_p \longrightarrow X_{\{w\mid\mathfrak{f}\mathfrak{p}\infty\}}\otimes\mathbb{Q}_p = H^2(\Delta(k(\mathfrak{f})))\otimes\mathbb{Q}_p$$

given by

$$u \mapsto \sum_{\mathfrak{l}\mid\mathfrak{f}_0} c_\mathfrak{l} \sum_{w\mid\mathfrak{l}} \mathrm{ord}_w(u)\cdot w + c_\mathfrak{p} \sum_{w\mid\mathfrak{p}} \mathrm{Tr}_{k(\mathfrak{f})_w/\mathbb{Q}_p}\left(\log_p(u_w)\right)\cdot w.$$

Proof As in [8, Lem. 5.8]. □

Let $\mathfrak{a}_1, \mathfrak{a}_2$ denote integral $\mathcal{O}_k$-ideals and set $\mathfrak{b} = \mathrm{lcm}(\mathfrak{a}_1,\mathfrak{a}_2), \mathfrak{c} = \gcd(\mathfrak{a}_1,\mathfrak{a}_2)$. In the following we will frequently apply the formulas

$$[k(\mathfrak{b}) : k(\mathfrak{a}_1)k(\mathfrak{a}_2)] = \frac{w(\mathfrak{b})w(\mathfrak{c})}{w(\mathfrak{a}_1)w(\mathfrak{a}_2)}, \quad k(\mathfrak{a}_1)\cap k(\mathfrak{a}_2) = k(\mathfrak{c}),$$

which follow easily from [28, (15)]. Without loss of generality we may assume that $w(\mathfrak{f}_0) = 1$. We also note that $w(\mathfrak{p}) = 1$, because $\mathfrak{p} \nmid 2$ and $\mathfrak{p} \neq \bar{\mathfrak{p}}$. This implies $w(\mathfrak{g}) = 1$ for any multiple $\mathfrak{g}$ of $\mathfrak{f}_0$ or $\mathfrak{p}$.

After these preparations we will now prove equality (32). Recall that this equality is equivalent to the statement that the image of $\mathcal{L}\otimes 1$ in $\mathrm{Det}_{\mathfrak{A}_p}\left(\Delta(k(\mathfrak{f}))\right) \subseteq \mathrm{Det}_{A_p}\left(\Delta(k(\mathfrak{f}))\otimes_{\mathbb{Z}_p}\mathbb{Q}_p\right)$ is equal to ${}_A\vartheta_p\left({}_A\vartheta_\infty(L^*({}_AM,0)^{-1})\right)$. This suggests to think of $\mathcal{L}$ as a p-adic L-function. The connection with the usual p-adic L-function is hidden in the fact that for each character χ the characteristic power series of the module of "semi-local units modulo elliptic units" is generated by the p-adic L-function (see [24, Remark after Theorem 4.1]).
It is therefore intuitively clear that our descent considerations will be most difficult (and interesting) in the case of "trivial zeros" of the associated p-adic L-function.

The case of $\chi|_{D_\mathfrak{p}} \neq 1$. We let $\chi \in \hat{G}_\mathfrak{f}^{\mathbb{Q}_p}$ be a non-trivial character such that $\chi|_{D_\mathfrak{p}} \neq 1$. This should be considered as the case of no trivial zeros.
We first show that $P_{\mathfrak{q}_\chi}^\infty = 0$. From Lemma 3.7 we know that multiplication by $\gamma^{p^n} - 1$ on P^∞ has finite kernel and cokernel. It follows that the characteristic power series $h \in \mathbb{Z}_p[[\Gamma]]$ of P^∞ (considered as a module over $\mathbb{Z}_p[[\Gamma]]$) is coprime with $\gamma^{p^n} - 1$. Hence h is a unit in $\Lambda_{\mathfrak{q}_\chi}$ which annihilates $P_{\mathfrak{q}_\chi}^\infty$.
From (21) and Remark 5.3 we obtain the short exact sequence

$$0 \longrightarrow U_{\mathfrak{q}_\chi}^\infty \longrightarrow U_{S_p,\mathfrak{q}_\chi}^\infty \longrightarrow Y_{\{w|\mathfrak{p}\},\mathfrak{q}_\chi}^\infty \longrightarrow 0$$

Moreover, $Y_{\{w|\mathfrak{p}\}}^\infty = \mathbb{Z}_p[G_\infty/D_\mathfrak{p}]$, so that $\chi|_{D_\mathfrak{p}} \neq 1$ implies $Y_{\{w|\mathfrak{p}\},\mathfrak{q}_\chi}^\infty = 0$. It follows that $H^1(\Delta) = U_{S_p,\mathfrak{q}_\chi}^\infty \simeq U_{\mathfrak{q}_\chi}^\infty$ and Lemma 5.5 implies

$$U_{\mathfrak{q}_\chi}^\infty = (N\mathfrak{a} - \sigma(\mathfrak{a}))(1-\gamma)^\varepsilon \eta_{\mathfrak{f}_{\chi,0}} \cdot \Lambda_{\mathfrak{q}_\chi},$$

where $\mathfrak{f}_{\chi,0}$ is the divisor of $\mathfrak{f}_0$ such that ψ has conductor $\mathfrak{f}_{\chi,0}$ or $\mathfrak{f}_{\chi,0}\mathfrak{p}$. Recall also that

$$\varepsilon = \begin{cases} 0, & \psi \neq 1, \\ 1, & \psi = 1. \end{cases}$$

If $\psi = 1$, then $\eta \neq 1$ and $1 - \chi(\gamma) = 1 - \eta(\gamma) \neq 0$, so that $1 - \gamma$ is a unit in $\Lambda_{\mathfrak{q}_\chi}$. Since also $N\mathfrak{a} - \sigma(\mathfrak{a}) \in \Lambda_{\mathfrak{q}_\chi}^\times$, we may choose $\beta_1 = \eta_{\mathfrak{f}_{\chi,0}}$ as $\Lambda_{\mathfrak{q}_\chi}$-basis of $M^1 = U_{\mathfrak{q}_\chi}^\infty$.
Since $P_{\{w|\mathfrak{f}\mathfrak{p}\}}^\infty$ is a quotient of P^∞ we obtain $P_{\{w|\mathfrak{f}\mathfrak{p}\},\mathfrak{q}_\chi}^\infty = 0$. Therefore $H^2(\Delta) = X_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\},\mathfrak{q}_\chi}^\infty$. From the short exact sequence

$$0 \longrightarrow X_{\{w|\mathfrak{f}_0\mathfrak{p}\}}^\infty \longrightarrow X_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}^\infty \longrightarrow Y_{\{w|\infty\}}^\infty \longrightarrow 0$$

together with the fact that $X_{\{w|\mathfrak{f}_0\mathfrak{p}\}}^\infty$ is Λ-torsion, we derive

$$M^2 = Y_{\{w|\infty\}}^\infty = \Lambda_{\mathfrak{q}_\chi} \cdot \beta_2 \text{ with } \beta_2 = \sigma_\infty.$$

We now apply [8, Lem. 5.7] with $\bar{\omega} = 1 - \gamma^{p^n}$. Recall that $H^2(\Delta)_{\mathrm{tors}} = X_{\{w|\mathfrak{f}_0\mathfrak{p}\},\mathfrak{q}_\chi}^\infty$ and this module is annihilated by $\bar{\omega}$. Indeed, $\bar{\omega} \sim 1 - \gamma^{p^m}$ for

$m \geq n$. For large m one has $\gamma^{p^m} \in D_{\mathfrak{l}}$ for each $\mathfrak{l} \mid \mathfrak{f}_0\mathfrak{p}$. It follows that $1-\gamma^{p^m}$ annihilates $X^{\infty}_{\{w|\mathfrak{f}_0\mathfrak{p}\}}$, so that the assumptions of [8, Lem. 5.7] are satisfied. The element $\bar{\beta}_1 \in M^1/\bar{\omega}$ is the image of the norm-compatible system

$$\eta_{\mathfrak{f}_{\chi,0}} = \left\{\psi(1;\mathfrak{f}_{\chi,0}\mathfrak{p}^{n+1},\mathfrak{a})\right\}_{n\geq 0}$$

in $M^1/\bar{\omega} \subseteq \mathcal{O}^{\times}_{k(\mathfrak{f}),S_p}\otimes_{\mathbb{Z}[G_{\mathfrak{f}}]}\mathbb{Q}_p(\chi)$. We write

$$\mathfrak{f} = \mathfrak{f}_0\mathfrak{p}^{\nu}, \quad \mathfrak{f}_\chi = \mathfrak{f}_{\chi,0}\mathfrak{p}^{\nu'}.$$

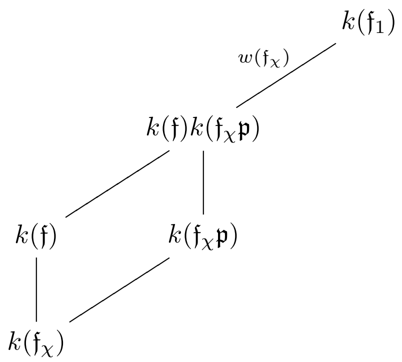
and recall the definition of ξ_χ in (9). We will show that

$$\bar{\beta}_1 = T_\chi\xi_\chi\otimes[k(\mathfrak{f}):k(\mathfrak{f}_0\mathfrak{p}^{\nu'})]^{-1}$$

with

$$T_\chi = \begin{cases} (1-\chi^{-1}(\mathfrak{p})), & \text{if } \mathfrak{f}_\chi \neq 1, \\ 1, & \text{if } \mathfrak{f}_\chi = 1. \end{cases}$$

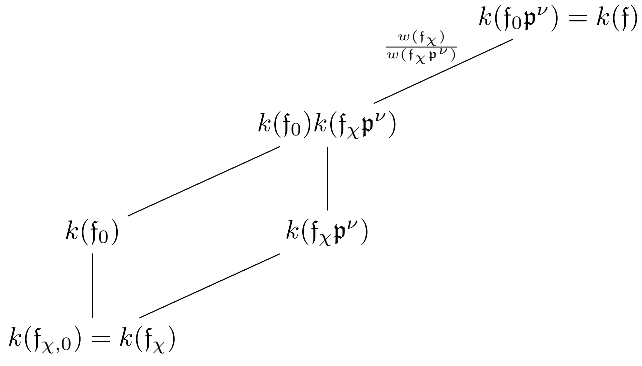
If $\nu = 0$, then $\mathfrak{f}_1 = \mathfrak{f}\mathfrak{p}, \mathfrak{f}_{\chi,0} = \mathfrak{f}_\chi$ and we have the following diagram of fields



Hence we obtain from[1, Th. 2.3]

$$\bar{\beta}_1 \quad = \quad N_{k(\mathfrak{f}_1)/k(\mathfrak{f})}\psi(1;\mathfrak{f}_\chi\mathfrak{p},\mathfrak{a})\otimes 1 = T_\chi\xi_\chi\otimes 1.$$

Note that in this case $[k(\mathfrak{f}):k(\mathfrak{f}_0\mathfrak{p}^{\nu'})] = 1$.
If $\nu > 0$ and $\nu' = 0$ we obtain the diagram



Writing $|G_{\mathfrak{f}}|e_\chi = t_\chi$ and $\bar{t}_\chi$ for the image of t_χ in $\mathbb{Z}[\mathrm{Gal}(k(\mathfrak{f}_\chi)/k)]$ we therefore have

$$\begin{aligned}\bar\beta_1 &= \psi(1;\mathfrak{f}_\chi\mathfrak{p}^\nu,\mathfrak{a})\otimes 1\\ &= t_\chi\psi(1;\mathfrak{f}_\chi\mathfrak{p}^\nu,\mathfrak{a})\otimes 1/|G_{\mathfrak{f}}|\\ &= \bar{t}_\chi T_\chi\xi_\chi\otimes\frac{w(\mathfrak{f}_\chi\mathfrak{p}^\nu)}{w(\mathfrak{f}_\chi)}\frac{1}{[k(\mathfrak{f}_\chi\mathfrak{p}^\nu):k]}\\ &= T_\chi\xi_\chi\otimes\frac{w(\mathfrak{f}_\chi\mathfrak{p}^\nu)}{w(\mathfrak{f}_\chi)}\frac{1}{[k(\mathfrak{f}_\chi\mathfrak{p}^\nu):k(\mathfrak{f}_\chi)]}\\ &= T_\chi\xi_\chi\otimes[k(\mathfrak{f}):k(\mathfrak{f}_0)]^{-1}.\end{aligned}$$

The case $\nu,\nu'>0$ is similar. Note that in this case $\chi(\mathfrak{p})=0$.
For each $\mathfrak{l}\mid\mathfrak{f}_0$ we choose a place $w_{\mathfrak{l}}$ above $\mathfrak{l}$ in $k(\mathfrak{f})/k$. It is easy to see that

$$Y_{\{w|\mathfrak{l}\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)=\begin{cases}0, & \chi|_{D_{\mathfrak{l}}}\neq 1,\\ \mathbb{Q}_p(\chi)\cdot w_{\mathfrak{l}}, & \chi|_{D_{\mathfrak{l}}}=1.\end{cases}$$

We choose for each $\mathfrak{l}\mid\mathfrak{f}_0$ with $\chi|_{D_{\mathfrak{l}}}=1$ an element $x_{\mathfrak{l}}\in k(\mathfrak{f})^\times$ such that

$$\begin{aligned}\mathrm{ord}_{w_{\mathfrak{l}}}(x_{\mathfrak{l}}) &\neq 0\\ \mathrm{ord}_{w}(x_{\mathfrak{l}}) &= 0 \text{ for all } w\neq w_{\mathfrak{l}}.\end{aligned}$$

Then $\mathbb{Q}_p(\chi)x_{\mathfrak{l}}\xrightarrow{\mathrm{val}}Y_{\{w|\mathfrak{l}\}}\otimes_{\mathbb{Z}_p[G_{\mathfrak{f}}]}\mathbb{Q}_p(\chi)=\mathbb{Q}_p(\chi)w_{\mathfrak{l}}$ is an isomorphism. We set

$$J=\{\mathfrak{l}\mid\mathfrak{f}_0\colon \chi|_{D_{\mathfrak{l}}}=1\},\quad x_J:=\bigwedge_{\mathfrak{l}\in J}x_{\mathfrak{l}},\quad w_J:=\bigwedge_{\mathfrak{l}\in J}w_{\mathfrak{l}}\text{ and } c_\chi:=\prod_{\mathfrak{l}\in J}c_{\mathfrak{l}}.$$

Since $\mathcal{O}_{k(\mathfrak{f})}^\times\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)$ is a $\mathbb{Q}_p(\chi)$-vector space of of dimension 1, the element $\bar\beta_1$ is necessarily a generator. Therefore $\{\bar\beta_1\}\cup\{x_{\mathfrak{l}}\colon\mathfrak{l}\in J\}$ is a $\mathbb{Q}_p(\chi)$-basis of $H^1(\Delta\otimes_R^{\mathbf{L}}\mathbb{Q}_p(\chi))=\mathcal{O}_{k(\mathfrak{f}),S_p}^\times\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)$. Moreover, $\{\bar\beta_2\}\cup\{w_{\mathfrak{l}}\colon\mathfrak{l}\in J\}$ is a $\mathbb{Q}_p(\chi)$-basis of $Y_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)$. Finally note that $\bar\beta_2=\sigma|_{k(\mathfrak{f})}$. From (33) we deduce

$$(\phi\circ\phi_{\bar\omega}^{-1})(\bar\beta_1^{-1}\otimes\bar\beta_2)=\phi(\bar\beta_1^{-1}\wedge x_J^{-1}\otimes\beta_{\bar\omega}(x_J)\wedge\bar\beta_2)$$

Applying Lemma 5.8 we obtain further

$$\begin{aligned}(\phi\circ\phi_{\bar\omega}^{-1})(\bar\beta_1^{-1}\otimes\bar\beta_2) &= c_\chi\phi(\bar\beta_1^{-1}\wedge x_J^{-1}\otimes\mathrm{val}(x_J)\wedge\bar\beta_2)\\ &= c_\chi(\bar\beta_1^{-1}\otimes\bar\beta_2)\\ &= \underbrace{c_\chi[k(\mathfrak{f}):k(\mathfrak{f}_0\mathfrak{p}^{\nu'})]T_\chi^{-1}\xi_\chi^{-1}\otimes\sigma|_{k(\mathfrak{f})}}_{=:A}.\end{aligned}\tag{34}$$

In order to apply [8, Lem. 5.7] we compute the exponent e such that $\bar{\omega}^e\beta_1^{-1}\otimes\beta_2$ is a $\Lambda_{\mathfrak{q}_\chi}$-basis of $\mathrm{Det}_{\Lambda_{\mathfrak{q}_\chi}}(\Delta^\infty_{\mathfrak{q}_\chi})$. By the proof of [8, Lem. 5.7] one has

$$\begin{aligned} e &= \sum_{i\in\mathbb{Z}}(-1)^{i+1}\dim_{\mathbb{Q}_p(\chi)}\left(H^i(\Delta)_{\bar{\omega}}\right)\\ &= -\dim_{\mathbb{Q}_p(\chi)}\left(X^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)\right)\\ &\overset{\chi\neq 1}{=} -\dim_{\mathbb{Q}_p(\chi)}\left(\bigoplus_{\mathfrak{l}|\mathfrak{f}_0\mathfrak{p}}\mathbb{Z}_p[G_\infty/D_\mathfrak{l}]\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)\right)\\ &= -|J|. \end{aligned}$$

As elements of $\left(\mathrm{Det}_\Lambda(\Delta^\infty)\right)_{\mathfrak{q}_\chi}$ we have

$$\begin{aligned} \mathcal{L} &= (N\mathfrak{a}-\sigma(\mathfrak{a}))\eta_{\mathfrak{f}_0}^{-1}\otimes\sigma_\infty\\ &= (N\mathfrak{a}-\sigma(\mathfrak{a}))[k(\mathfrak{f}_0\mathfrak{p}):k(\mathfrak{f}_{\chi,0}\mathfrak{p})][\mathrm{Tr}_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{f}_{\chi,0}\mathfrak{p})}\eta_{\mathfrak{f}_0}]^{-1}\otimes\sigma_\infty, \end{aligned}$$

because $\mathrm{Tr}_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{f}_{\chi,0}\mathfrak{p})} = [k(\mathfrak{f}_0\mathfrak{p}):k(\mathfrak{f}_{\chi,0}\mathfrak{p})]$ as elements of $\Lambda_{\mathfrak{q}_\chi}$ (multiply both sides with e_χ). From the distribution relation we derive further

$$\begin{aligned} \mathcal{L} &= (N\mathfrak{a}-\sigma(\mathfrak{a}))[k(\mathfrak{f}_0\mathfrak{p}):k(\mathfrak{f}_{\chi,0}\mathfrak{p})]\prod_{\mathfrak{l}|\mathfrak{f}_0,\mathfrak{l}\nmid\mathfrak{f}_{\chi,0}}\frac{1}{1-\mathrm{Fr}_\mathfrak{l}^{-1}}\eta_{\mathfrak{f}_{\chi,0}}^{-1}\otimes\sigma_\infty\\ &= \underbrace{(N\mathfrak{a}-\sigma(\mathfrak{a}))[k(\mathfrak{f}_0\mathfrak{p}):k(\mathfrak{f}_{\chi,0}\mathfrak{p})]\prod_{\substack{\mathfrak{l}|\mathfrak{f}_0,\mathfrak{l}\nmid\mathfrak{f}_{\chi,0}\\ \chi(\mathfrak{l})\neq 1}}\frac{1}{1-\mathrm{Fr}_\mathfrak{l}^{-1}}\prod_{\mathfrak{l}\in J}\frac{\bar{\omega}}{1-\mathrm{Fr}_\mathfrak{l}^{-1}}}_{=:B}\left(\bar{\omega}^e\beta_1^{-1}\otimes\beta_2\right). \end{aligned}$$

Now [8, Lem. 5.7] implies

$$\phi_{\bar{\omega}}(B^{-1}(\mathcal{L}\otimes 1)) = \bar{\beta}_1^{-1}\otimes\bar{\beta}_2,$$

which in conjunction with (34) shows that $\phi(B^{-1}(\mathcal{L}\otimes 1)) = A$ or $\phi(\mathcal{L}\otimes 1) = AB$. For $\mathfrak{l}\in J$ we have by definition of $c_\mathfrak{l}$ the equality $\mathrm{Fr}_\mathfrak{l}^{-f_\mathfrak{l}} = \gamma^{c_\mathfrak{l}p^n}$ and therefore

$$\chi\left(\frac{\bar{\omega}}{1-\mathrm{Fr}_\mathfrak{l}^{-1}}\right) = \chi\left(\frac{(1-\gamma^{p^n})(1+\mathrm{Fr}_\mathfrak{l}^{-1}+\ldots+\mathrm{Fr}_\mathfrak{l}^{-f_\mathfrak{l}+1})}{1-\gamma^{c_\mathfrak{l}p^n}}\right) = \frac{f_\mathfrak{l}}{c_\mathfrak{l}}. \qquad (35)$$

Using $[k(\mathfrak{f}):k(\mathfrak{f}_0\mathfrak{p}^{\nu'})][k(\mathfrak{f}_0\mathfrak{p}):k(\mathfrak{f}_{\chi,0}\mathfrak{p})] = w(\mathfrak{f}_\chi)[k(\mathfrak{f}):k(\mathfrak{f}_\chi)]$ it follows that

$$AB =$$

$$(N\mathfrak{a}-\sigma(\mathfrak{a}))w(\mathfrak{f}_\chi)[k(\mathfrak{f}):k(\mathfrak{f}_\chi)]\left(\prod_{\substack{\mathfrak{l}|\mathfrak{f}_0,\mathfrak{l}\nmid\mathfrak{f}_{\chi,0}\\ \chi(\mathfrak{l})\neq 1}}\frac{1}{1-\mathrm{Fr}_\mathfrak{l}^{-1}}\right)\left(\prod_{\mathfrak{l}\in J}f_\mathfrak{l}\right)T_\chi^{-1}\xi_\chi^{-1}\otimes\sigma|_{k(\mathfrak{f})}.$$

Recalling the definition of the elements $\mathcal{E}_v$ from (15) we observe that this is exactly the equality (32).

The case of $\chi \neq 1$ and $\chi|_{D_\mathfrak{p}} = 1$. We let $\chi \in \hat{G}_\mathfrak{f}^{\mathbb{Q}_p}$ be a non-trivial character such that $\chi|_{D_\mathfrak{p}} = 1$. This should be considered as the case of trivial zeros. Note that in this case $\mathfrak{p} \nmid \mathfrak{f}_\chi$, i.e. $\mathfrak{f}_{\chi,0} = \mathfrak{f}_\chi$.
Before going into detail we brievely explain the strategy of the proof. We first point out that in one respect the elliptic case is easier than the cyclotomic case: there is no distinction between odd and even characters. Indeed, in the elliptic setting every non-trivial character behaves like an even character. Nevertheless, the strategy of the proof becomes most clear, if one recalls what happens in the cyclotomic case for odd characters. In order to avoid the trivial zero one divides the p-adic L-function by $\gamma - 1$. As a consequence of a theorem of Ferrero and Greenberg [7] (which gives a formula for the first derivative of the p-adic L-function) one obtains that this quotient interpolates essentially the global L-function $L(\chi^{-1}, s)$ at $s = 0$ (for more details see [8, Lemma 5.11]).
For even characters the strategy can be motivated by the fact that the p-adic L-function is closely related to norm-coherent sequences of cyclotomic (or in our case, of elliptic) units. In order to "avoid the trivial zero" we again divide by $\gamma - 1$, which means that we have to take the $(\gamma - 1)$-st root of a norm-coherent sequence of cyclotomic or elliptic units. In the cyclotomic case this is achieved by using a result of Solomon [29] which also provides enough information to work out the relation to the value of $L(\chi^{-1}, s)$ at $s = 0$. In the elliptic case we will use an analoguous result proved by the author in [1].
For any subgroup H of G_∞ we define J_H to be the kernel of the canonical map $\mathbb{Z}_p[[G_\infty]] \to \mathbb{Z}_p[[G_\infty/H]]$.
As in the case of no trivial zeros we can show that $P_{\mathfrak{q}_\chi}^\infty = 0$. From (21) we obtain the short exact sequence

$$0 \longrightarrow U_{\mathfrak{q}_\chi}^\infty \longrightarrow U_{S_p,\mathfrak{q}_\chi}^\infty \longrightarrow Y_{\{w|\mathfrak{p}\},\mathfrak{q}_\chi}^\infty \longrightarrow 0 \tag{36}$$

where now $Y_{\{w|\mathfrak{p}\},\mathfrak{q}_\chi}^\infty \simeq \mathbb{Z}_p[G_\infty/D_\mathfrak{p}]\otimes_\Lambda \Lambda_{\mathfrak{q}_\chi} \simeq \Lambda/J_{D_\mathfrak{p}} \otimes_\Lambda \Lambda_{\mathfrak{q}_\chi} \simeq \Lambda_{\mathfrak{q}_\chi}/J_{D_\mathfrak{p}}\Lambda_{\mathfrak{q}_\chi}$. Since $\Gamma \subseteq D_\mathfrak{p}$ one has $\gamma^{p^n} - 1 \sim \gamma - 1$. It follows that $Y_{\{w|\mathfrak{p}\},\mathfrak{q}_\chi}^\infty \simeq \mathbb{Q}_p(\chi)$, and in addition, the structure theorem for modules over principal ideal rings implies $(\gamma - 1)U_{S_p,\mathfrak{q}_\chi}^\infty = U_{\mathfrak{q}_\chi}^\infty$.
For a finite set S of places of k we set $U_{k(\mathfrak{f}_\chi),S}^\infty = \varprojlim_n \left(\mathcal{O}_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+1}),S}^\times \otimes_\mathbb{Z} \mathbb{Z}_p\right)$.

Lemma 5.9 *a) The sequence*

$$0 \longrightarrow U_{k(\mathfrak{f}_\chi),S_p}^\infty \xrightarrow{\gamma-1} U_{k(\mathfrak{f}_\chi),S_p}^\infty \longrightarrow U_{k(\mathfrak{f}_\chi),S_p,\Gamma}^\infty \longrightarrow 0$$

is exact.
b) The canonical map $U_{k(\mathfrak{f}_\chi),S_p,\Gamma}^\infty \longrightarrow \mathcal{O}_{k(\mathfrak{f}_\chi\mathfrak{p}),S_p}^\times \otimes_\mathbb{Z} \mathbb{Z}_p$ *is injective.*

Proof One has $\left(U^{\infty}_{k(\mathfrak{f}_\chi),S_p}\right)^{\Gamma} = \varprojlim_n \left(\mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}),S_p}\otimes_{\mathbb{Z}}\mathbb{Z}_p\right) = 0$. Hence a) is immediate. For b) one has to prove

$$(\gamma-1)U^{\infty}_{k(\mathfrak{f}_\chi),S_p} = \{u \in U^{\infty}_{k(\mathfrak{f}_\chi),S_p} \mid u_0 = 1\}.$$

The inclusion "$\subseteq$" is obvious. Suppose that $u_0 = 1$. Then for each n Hilbert's Theorem 90 provides an element $\beta_n \in k(\mathfrak{f}_\chi\mathfrak{p}^{n+1})^{\times}/k(\mathfrak{f}_\chi\mathfrak{p})^{\times}$ such that

$$\beta_n^{\gamma-1} = u_n \quad \text{and} \quad N_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+2})/k(\mathfrak{f}_\chi\mathfrak{p}^{n+1})}(\beta_{n+1}) \equiv \beta_n (\mathrm{mod}\ k(\mathfrak{f}_\chi\mathfrak{p})^{\times}).$$

Let S be a finite set of places of k containing S_p and such that $\mathrm{Pic}(\mathcal{O}_{k(\mathfrak{f}_\chi\mathfrak{p}),S}) = 0$. Then we may assume that

$$\beta_n \in \mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+1}),S}/\mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}),S}.$$

In the following diagram all vertical maps are induced by the norm,

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}),S}\otimes\mathbb{Z}_p & \longrightarrow & \mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+2}),S}\otimes\mathbb{Z}_p & \longrightarrow & \dfrac{\mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+2}),S}\otimes\mathbb{Z}_p}{\mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}),S}\otimes\mathbb{Z}_p} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}),S}\otimes\mathbb{Z}_p & \longrightarrow & \mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+1}),S}\otimes\mathbb{Z}_p & \longrightarrow & \dfrac{\mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+1}),S}\otimes\mathbb{Z}_p}{\mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}),S}\otimes\mathbb{Z}_p} & \longrightarrow & 0
\end{array}$$

The natural topology of $\mathbb{Z}_p$ induces on each finitely generated $\mathbb{Z}_p$-module the structure of a compact topological group. By [17, Satz IV.2.7] the functor $\varprojlim_n$ is therefore exact on the above exact sequence of projective systems. In addition, the projective limit over the modules on the left hand side is obviously trivial and therefore

$$U^{\infty}_{k(\mathfrak{f}_\chi),S} \simeq \varprojlim_n \frac{\mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}^{n+1}),S}\otimes\mathbb{Z}_p}{\mathcal{O}_{k(\mathfrak{f}_\chi\mathfrak{p}),S}\otimes\mathbb{Z}_p}.$$

Moreover, the argument used to prove (21) also shows that $U^{\infty}_{k(\mathfrak{f}_\chi),S} \simeq U^{\infty}_{k(\mathfrak{f}_\chi),S_p} \simeq U^{\infty}_{k(\mathfrak{f}_\chi),\{w|\mathfrak{p}\infty\}}$ for any set $S \supseteq S_p$, so that the inclusion "$\supseteq$" follows. ∎

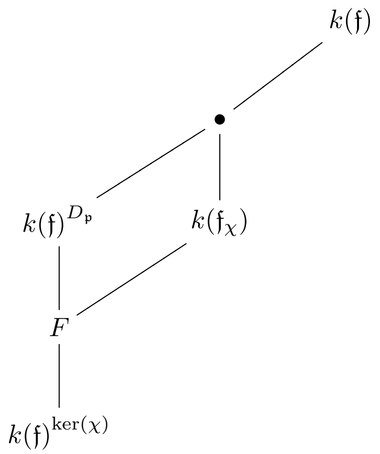
We now choose an auxiliary prime ideal $\mathfrak{b}$ of $\mathcal{O}_k$ such that

$$(\mathfrak{b}, \mathfrak{f}\mathfrak{p}) = 1, \quad w(\mathfrak{b}) = 1, \quad \chi(\mathfrak{b}) \neq 1.$$

In order to be able to deal also with the case $\mathfrak{f}_\chi = 1$ we introduce the element

$$\eta = \{\psi(1; \mathfrak{f}_\chi\mathfrak{b}\mathfrak{p}^{n+1}, \mathfrak{a})\}_{n=0}^{\infty} \in \varprojlim_n \mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p}^{n+1})}.$$

With respect to the injection $U^{\infty}_{k(\mathfrak{f}_\chi),S_p,\Gamma} \longrightarrow \mathcal{O}^{\times}_{k(\mathfrak{f}_\chi\mathfrak{p}),S_p}\otimes\mathbb{Z}_p$ the element $N_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p})/F}(\eta)$ maps to $N_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p})/F}(\eta^0)$, where here F denotes the decomposition subfield at $\mathfrak{p}$ in $k(\mathfrak{f}_\chi)/k$. One has the following diagram of fields



Since by definition of F one has $\sigma(\mathfrak{p})|_F = id$, we derive from the distribution relation

$$N_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p})/F}(\eta^0) = (1-\sigma(\mathfrak{p})^{-1})N_{k(\mathfrak{f}_\chi\mathfrak{b})/F}\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a}) = 1,$$

so that Lemma 5.9 yields a unique element $z^\infty \in U^\infty_{k(\mathfrak{f}_\chi),S_p}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ such that

$$(\gamma-1)z^\infty = \frac{1}{[k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p}):F]}N_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p})/F}(\eta). \tag{37}$$

From Lemma 5.5 and $N\mathfrak{a}-\sigma(\mathfrak{a})\sim 1$ we deduce $U^\infty_{\mathfrak{q}_\chi} = \Lambda_{\mathfrak{q}_\chi}\eta_{\mathfrak{f}_\chi}$. Again from the distribution relations [1, Th. 2.3] we deduce

$$N_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p})/F}\eta = (1-Fr_\mathfrak{b}^{-1})N_{k(\mathfrak{f}_\chi\mathfrak{p})/F}\eta_{\mathfrak{f}_\chi}.$$

Combining (36) and (37) we see that

$$H^1(\Delta) = U^\infty_{S_p,\mathfrak{q}_\chi} = \Lambda_{\mathfrak{q}_\chi}\cdot\beta_1 \text{ with } \beta_1 = z^\infty.$$

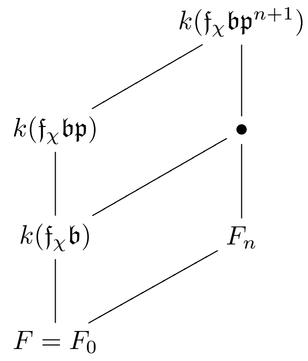
Note that

$$\bar\beta_1 = \begin{cases} z_\mu, & \text{if } \mathfrak{p}\mid\mathfrak{f}, \mathfrak{f}=\mathfrak{f}_0\mathfrak{p}^{\mu+1}, \mu\ge 0,\\ N_{k(\mathfrak{f}\mathfrak{p})/k(\mathfrak{f})}(z_0), & \text{if } \mathfrak{p}\nmid\mathfrak{f},\end{cases}$$

when we regard $\bar\beta_1$ as an element in $\mathcal{O}^\times_{k(\mathfrak{f}),S_p}\otimes\mathbb{Z}_p$.
Let v denote a place of $k(\mathfrak{f})$ above w, where $w\mid\mathfrak{p}$ in F/k. Using the above diagram we compute

$$\begin{aligned} & \mathrm{Tr}_{k(\mathfrak{f})_v/\mathbb{Q}_p}\left(\log_p\left(N_{k(\mathfrak{f}_\chi\mathfrak{b})/k(\mathfrak{f}_\chi)}\left(\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a})\right)\right)\right)\\ = & \frac{|D_\mathfrak{p}|}{[k(\mathfrak{f}_\chi):F]}\log_p\left(N_{k(\mathfrak{f}_\chi\mathfrak{b})/F}(\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a}))\right)\\ = & \frac{|D_\mathfrak{p}|}{[k(\mathfrak{f}_\chi):F]}\log_p(\chi_{\mathrm{ell}}(\gamma))\underbrace{\frac{1}{\log_p(\chi_{\mathrm{ell}}(\gamma))}\log_p\left(N_{k(\mathfrak{f}_\chi\mathfrak{b})/F}(\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a}))\right)}_{=:B}\end{aligned}$$

By the main result of [1] the quantity B is well known. We briefly recall the construction of [1]. Let k_∞ denote the unique $\mathbb{Z}_p$-extension of k which is unramified outside $\mathfrak{p}$. Let $k_n \subseteq k_\infty$ denote the extension of degree p^n above k. We put $F_n := Fk_n$ and consider the diagram of fields



For each n Hilbert's Theorem 90 provides an element $\beta_n \in F_n^\times / F^\times$ such that

$$\beta_n^{\gamma - 1} = N_{k(\mathfrak{f}_\chi \mathfrak{b}\mathfrak{p}^{n+1})/F_n} \left(\psi(1; \mathfrak{f}_\chi \mathfrak{b}\mathfrak{p}^{n+1}, \mathfrak{a}) \right).$$

If we put $\kappa_n := N_{F_n/F}(\beta_n) \in F^\times / (F^\times)^{p^n}$ and $\kappa^\infty := \{\kappa_n\}_{n=0}^\infty \in \lim F^\times / (F^\times)^{p^n}$, then the main result of [1] says

$$B = \mathrm{ord}_w(\kappa^\infty).$$

From the construction of z^∞ it is clear that one has

$$\beta_n = N_{k(\mathfrak{f}_\chi \mathfrak{b}\mathfrak{p}^{n+1})/F_n}(z_n) \text{ in } F_n^\times / F^\times,$$

and consequently,

$$\kappa^\infty = \{N_{k(\mathfrak{f}_\chi \mathfrak{b}\mathfrak{p})/F}(z_0)\}_{n=0}^\infty.$$

We let $w' \mid w$ denote the place in $k(\mathfrak{f}_\chi)/F$ defined by v and set $c_{\mathfrak{p}}(\gamma) :=$

$\log_p(\chi_{\mathrm{ell}}(\gamma))^{-1}$. Then

$$\begin{aligned}
& \mathrm{Tr}_{k(\mathfrak{f})_v/\mathbb{Q}_p}\left(\log_p\left(N_{k(\mathfrak{f}_\chi\mathfrak{b})/k(\mathfrak{f}_\chi)}\left(\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a})\right)\right)\right)\\
= & \frac{|D_\mathfrak{p}|}{[k(\mathfrak{f}_\chi):F]}c_\mathfrak{p}(\gamma)^{-1}\mathrm{ord}_w(N_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p})/F}z_0)\\
= & \frac{|D_\mathfrak{p}|c_\mathfrak{p}(\gamma)^{-1}}{[k(\mathfrak{f}_\chi):F]}\mathrm{ord}_w(N_{k(\mathfrak{f}_\chi\mathfrak{p})/F}N_{k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p})/k(\mathfrak{f}_\chi\mathfrak{p})}z_0)\\
= & \frac{|D_\mathfrak{p}|c_\mathfrak{p}(\gamma)^{-1}[k(\mathfrak{f}_\chi\mathfrak{b}\mathfrak{p}):k(\mathfrak{f}_\chi\mathfrak{p})]}{[k(\mathfrak{f}_\chi):F]}\mathrm{ord}_w(N_{k(\mathfrak{f}_\chi\mathfrak{p})/F}z_0)\\
= & \frac{|D_\mathfrak{p}|c_\mathfrak{p}(\gamma)^{-1}w(1)[k(\mathfrak{b}):k(1)]}{[k(\mathfrak{f}_\chi):F]}\mathrm{ord}_w(N_{k(\mathfrak{f}_\chi)/F}(N_{k(\mathfrak{f}_\chi\mathfrak{p})/k(\mathfrak{f}_\chi)}z_0))\\
= & \frac{|D_\mathfrak{p}|c_\mathfrak{p}(\gamma)^{-1}w(1)[k(\mathfrak{b}):k(1)]}{[k(\mathfrak{f}_\chi):F]}f_{w'/w}\mathrm{ord}_{w'}(N_{k(\mathfrak{f}_\chi\mathfrak{p})/k(\mathfrak{f}_\chi)}z_0)\\
= & |D_\mathfrak{p}|c_\mathfrak{p}(\gamma)^{-1}w(1)[k(\mathfrak{b}):k(1)]e_{v/w'}^{-1}\mathrm{ord}_v(N_{k(\mathfrak{f}_\chi\mathfrak{p})/k(\mathfrak{f}_\chi)}z_0)\\
= & f_\mathfrak{p}c_\mathfrak{p}(\gamma)^{-1}w(1)[k(\mathfrak{b}):k(1)]\mathrm{ord}_v(N_{k(\mathfrak{f}_\chi\mathfrak{p})/k(\mathfrak{f}_\chi)}z_0)
\end{aligned}$$

We now apply Lemma 5.8. The congruence in the following computation is modulo $Y_{\{w|\mathfrak{f}_0\}}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$.

$$\begin{aligned}
& \beta_{\bar\omega}\left(N_{k(\mathfrak{f}_\chi\mathfrak{b})/k(\mathfrak{f}_\chi)}(\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a}))\right)\\
\equiv & c_\mathfrak{p}\sum_{v|\mathfrak{p}}\mathrm{Tr}_{k(\mathfrak{f})_v/\mathbb{Q}_p}\left(\log_p(N_{k(\mathfrak{f}_\chi\mathfrak{b})/k(\mathfrak{f}_\chi)}(\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a})))\right)\cdot v\\
= & \frac{c_\mathfrak{p}}{c_\mathfrak{p}(\gamma)}f_\mathfrak{p}w(1)[k(\mathfrak{b}):k(1)]\sum_{v|\mathfrak{p}}\mathrm{ord}_v\left(N_{k(\mathfrak{f}_\chi\mathfrak{p})/k(\mathfrak{f}_\chi)}(z_0)\right)\cdot v\\
= & \begin{cases}\frac{f_\mathfrak{p}}{p^n}[k(\mathfrak{b}):k(1)]\frac{w(1)}{w(\mathfrak{f}_\chi)}\sum_{v|\mathfrak{p}}\mathrm{ord}_v(N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{f}_0)}z_0)\cdot v, & \text{if } \mathfrak{p}\nmid\mathfrak{f},\\ \frac{f_\mathfrak{p}}{p^n}w(1)[k(\mathfrak{b}):k(1)][k(\mathfrak{f}_\chi\mathfrak{p}):k(\mathfrak{f}_\chi)]\sum_{v|\mathfrak{p}}\mathrm{ord}_v(z_0)\cdot v, & \text{if } \mathfrak{p}\mid\mathfrak{f}\end{cases}\\
= & \begin{cases}\frac{f_\mathfrak{p}}{p^n}[k(\mathfrak{b}):k(1)]\frac{w(1)}{w(\mathfrak{f}_\chi)}\sum_{v|\mathfrak{p}}\mathrm{ord}_v(N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{f}_0)}z_0)\cdot v, & \text{if } \mathfrak{p}\nmid\mathfrak{f},\\ \frac{f_\mathfrak{p}}{p^n}w(1)[k(\mathfrak{b}):k(1)][k(\mathfrak{f}_\chi\mathfrak{p}):k(\mathfrak{f}_\chi)][k(\mathfrak{f}_\chi\mathfrak{p}^{\mu+1}):k(\mathfrak{f}_\chi\mathfrak{p})]\sum_{v|\mathfrak{p}}\mathrm{ord}_v(z_\mu)\cdot v, & \\ & \text{if } \mathfrak{p}\mid\mathfrak{f}\end{cases}\\
= & \begin{cases}\frac{f_\mathfrak{p}}{p^n}[k(\mathfrak{b}):k(1)]\frac{w(1)}{w(\mathfrak{f}_\chi)}\sum_{v|\mathfrak{p}}\mathrm{ord}_v(N_{k(\mathfrak{f}_0\mathfrak{p})/k(\mathfrak{f}_0)}z_0)\cdot v, & \text{if } \mathfrak{p}\nmid\mathfrak{f},\\ \frac{f_\mathfrak{p}}{p^n}w(1)[k(\mathfrak{b}):k(1)][k(\mathfrak{f}_\chi\mathfrak{p}^{\mu+1}):k(\mathfrak{f}_\chi)]\sum_{v|\mathfrak{p}}\mathrm{ord}_v\left(\bar\beta_1\right)\cdot v, & \text{if } \mathfrak{p}\mid\mathfrak{f}\end{cases}\\
= & \begin{cases}\frac{f_\mathfrak{p}}{p^n}\frac{w(1)}{w(\mathfrak{f}_\chi)}[k(\mathfrak{b}):k(1)]\sum_{v|\mathfrak{p}}\mathrm{ord}_v(\bar\beta_1)\cdot v, & \text{if } \mathfrak{p}\nmid\mathfrak{f},\\ \frac{f_\mathfrak{p}}{p^n}w(1)[k(\mathfrak{b}):k(1)][k(\mathfrak{f}_\chi\mathfrak{p}^{\nu}):k(\mathfrak{f}_\chi)]\sum_{v|\mathfrak{p}}\mathrm{ord}_v\left(\bar\beta_1\right)\cdot v, & \text{if } \mathfrak{p}\mid\mathfrak{f}\end{cases}
\end{aligned}$$

We first assume that $\mathfrak{p} \mid \mathfrak{f}$ and use this data to compute

$$\begin{aligned}
& (\phi \circ \phi_{\bar{\omega}}^{-1})(\bar{\beta}_1^{-1} \otimes \bar{\beta}_2) \\
= \ & \phi\big(\bar{\beta}_1^{-1} \wedge [N_{k(\mathfrak{f}_\chi \mathfrak{b})/k(\mathfrak{f}_\chi)} \psi(1; \mathfrak{f}_\chi \mathfrak{b}, \mathfrak{a})]^{-1} \\
& \qquad \wedge x_J^{-1} \otimes \beta_{\bar{\omega}}(x_J) \wedge \beta_{\bar{\omega}}(N_{k(\mathfrak{f}_\chi \mathfrak{b})/k(\mathfrak{f}_\chi)}(\psi(1; \mathfrak{f}_\chi \mathfrak{b}, \mathfrak{a}))) \wedge \bar{\beta}_2\big) \\
= \ & c_\chi \frac{f_\mathfrak{p}}{p^n} w(1)[k(\mathfrak{b}) : k(1)][k(\mathfrak{f}_\chi \mathfrak{p}^\nu) : k(\mathfrak{f}_\chi)] \times \\
& \phi\big(\bar{\beta}_1^{-1} \wedge [N_{k(\mathfrak{f}_\chi \mathfrak{b})/k(\mathfrak{f}_\chi)}(\psi(1; \mathfrak{f}_\chi \mathfrak{b}, \mathfrak{a}))]^{-1} \wedge x_J^{-1} \otimes \mathrm{val}(x_J) \wedge \mathrm{val}(\bar{\beta}_1) \wedge \bar{\beta}_2\big) \\
= \ & \underbrace{-c_\chi \frac{f_\mathfrak{p}}{p^n} w(1)[k(\mathfrak{b}) : k(1)][k(\mathfrak{f}_\chi \mathfrak{p}^\nu) : k(\mathfrak{f}_\chi)][N_{k(\mathfrak{f}_\chi \mathfrak{b})/k(\mathfrak{f}_\chi)}(\psi(1; \mathfrak{f}_\chi \mathfrak{b}, \mathfrak{a}))]^{-1} \otimes \sigma_\infty|_{k(\mathfrak{f})}}_{=:A}.
\end{aligned}$$

On the other hand we note that $\mathfrak{f}_\chi = \mathfrak{f}_{\chi,0}$ and compute

$$\mathcal{L} \ = \ (N\mathfrak{a} - \sigma(\mathfrak{a}))[k(\mathfrak{f}_0 \mathfrak{p}) : k(\mathfrak{f}_\chi \mathfrak{p})] \prod_{\mathfrak{l} \mid \mathfrak{f}_0, \mathfrak{l} \nmid \mathfrak{f}_\chi} \frac{1}{1 - \mathrm{Fr}_\mathfrak{l}^{-1}} \eta_{\mathfrak{f}_\chi}^{-1} \otimes \sigma_\infty.$$

In addition, one has

$$(\gamma - 1)\beta_1 = (\gamma - 1) z^\infty = \frac{1}{[k(\mathfrak{f}_\chi \mathfrak{b} \mathfrak{p}) : F]} N_{k(\mathfrak{f}_\chi \mathfrak{b} \mathfrak{p})/F}(\eta)$$

and

$$\frac{\bar{\omega}}{1 - \gamma} = T := 1 + \gamma + \ldots + \gamma^{p^n - 1}.$$

This implies the equality

$$\begin{aligned}
\bar{\omega}\beta_1 \ &= \ (1 - \gamma) T \beta_1 = -T \frac{1}{[k(\mathfrak{f}_\chi \mathfrak{b} \mathfrak{p}) : k(\mathfrak{f}_\chi \mathfrak{p})]} N_{k(\mathfrak{f}_\chi \mathfrak{b} \mathfrak{p})/k(\mathfrak{f}_\chi \mathfrak{p})}(\eta) \\
&= \ -T \frac{1}{[k(\mathfrak{f}_\chi \mathfrak{b} \mathfrak{p}) : k(\mathfrak{f}_\chi \mathfrak{p})]} (1 - \sigma(\mathfrak{b})^{-1}) \eta_{\mathfrak{f}_\chi} \\
&= \ -T \frac{1}{w(1)[k(\mathfrak{b}) : k(1)]} (1 - \sigma(\mathfrak{b})^{-1}) \eta_{\mathfrak{f}_\chi}
\end{aligned}$$

in $U^\infty_{S_p, \mathfrak{q}_\chi}$. Since $e = -(|J| + 1)$ we obtain $\mathcal{L} = B\bar{\omega}^e(\beta_1^{-1} \otimes \beta_2)$ with

$$\begin{aligned}
B \ = \ & -T(N\mathfrak{a} - \sigma(\mathfrak{a}))[k(\mathfrak{f}_0 \mathfrak{p}) : k(\mathfrak{f}_\chi \mathfrak{p})](w(1)[k(\mathfrak{b}) : k(1)])^{-1} \times \\
& (1 - \sigma(\mathfrak{b})^{-1}) \prod_{\substack{\mathfrak{l} \mid \mathfrak{f}_0, \mathfrak{l} \nmid \mathfrak{f}_\chi \\ \chi(\mathfrak{l}) \neq 1}} \frac{1}{1 - \mathrm{Fr}_\mathfrak{l}^{-1}} \prod_{\mathfrak{l} \in J} \frac{\bar{\omega}}{1 - \mathrm{Fr}_\mathfrak{l}^{-1}}.
\end{aligned}$$

Again we deduce from [8, Lem. 5.7] that $\phi(\mathcal{L} \otimes 1) = AB$. From

$$[k(\mathfrak{f}_\chi \mathfrak{p}^\nu) : k(\mathfrak{f}_\chi)][k(\mathfrak{f}_0 \mathfrak{p} : k(\mathfrak{f}_\chi \mathfrak{p})] = [k(\mathfrak{f}) : k(\mathfrak{f}_\chi)]$$

(recall again that $w(\mathfrak{p}) = w(\mathfrak{f}) = 1$) and

$$N_{k(\mathfrak{f}_\chi\mathfrak{b})/k(\mathfrak{f}_\chi)}(\psi(1;\mathfrak{f}_\chi\mathfrak{b},\mathfrak{a})^{w(\mathfrak{f}_\chi)}) = \begin{cases} (1-\sigma(\mathfrak{b})^{-1})\psi(1;\mathfrak{f}_\chi,\mathfrak{a}), & \text{if } \mathfrak{f}_\chi \neq 1, \\ \frac{\delta(\mathcal{O}_k,\mathfrak{a}^{-1})}{\delta(\mathfrak{b},\mathfrak{a}^{-1}\mathfrak{b})}, & \text{if } \mathfrak{f}_\chi = 1, \end{cases}$$

we compute

$$\begin{aligned} & AB = \\ = \ & w(\mathfrak{f}_\chi)[k(\mathfrak{f}):k(\mathfrak{f}_\chi)](N\mathfrak{a}-\sigma(\mathfrak{a})) \prod_{\substack{\mathfrak{l}\mid\mathfrak{f}_0 \\ \chi(\mathfrak{l})\neq 1}} \frac{1}{1-\mathrm{Fr}_{\mathfrak{l}}^{-1}} \prod_{\mathfrak{l}\in J\cup\{\mathfrak{p}\}} f_{\mathfrak{l}} \times \\ & \begin{cases} \psi(1;\mathfrak{f}_\chi,\mathfrak{a})^{-1}\otimes\sigma_\infty|_{k(\mathfrak{f})}, & \text{if } \mathfrak{f}_\chi \neq 1, \\ (1-\sigma(\mathfrak{b})^{-1})\frac{\delta(\mathcal{O}_k,\mathfrak{a}^{-1})}{\delta(\mathfrak{b},\mathfrak{a}^{-1}\mathfrak{b})}\otimes\sigma_\infty|_{k(\mathfrak{f})}, & \text{if } \mathfrak{f}_\chi = 1. \end{cases} \end{aligned}$$

Finally we use in the case $\mathfrak{f}_\chi = 1$ the relation

$$\left(\frac{\delta(\mathcal{O}_k,\mathfrak{a}^{-1})}{\delta(\mathfrak{b},\mathfrak{a}^{-1}\mathfrak{b})}\right)^{1-\sigma(\mathfrak{p})^{-1}} = \left(\frac{\delta(\mathcal{O}_k,\mathfrak{a}^{-1})}{\delta(\mathfrak{p},\mathfrak{a}^{-1}\mathfrak{p})}\right)^{1-\sigma(\mathfrak{b})^{-1}}$$

and recover the equation (32). The case $\mathfrak{p} \nmid \mathfrak{f}$ is completely analogous.

The case of the trivial character In this case $\beta_1 = \eta_1$ and we first have to compute $\bar\beta_1$. If $\mathfrak{p} \nmid \mathfrak{f}$, the $\bar\beta_1 = N_{k(\mathfrak{f}\mathfrak{p})/k(\mathfrak{f})}(\psi(1;\mathfrak{q},\mathfrak{a}))$ and the distribution relation [1, Th. 2.3 b)] implies

$$\bar\beta_1 = N_{k(\mathfrak{q})/k(1)}(\psi(1;\mathfrak{q},\mathfrak{a})^{w(1)}) = \frac{\delta(\mathcal{O}_k,\mathfrak{a}^{-1})}{\delta(\mathfrak{p},\mathfrak{p}\mathfrak{a}^{-1})},$$

where δ denotes the function of lattices defined in [21, Th. 1]. We recall that

$$\delta(L,\underline{L})^{12} = \frac{\Delta(L)^{[\underline{L}:L]}}{\Delta(\underline{L})}.$$

If $\mathfrak{p} \mid \mathfrak{f}$, then $\bar\beta_1 = \psi(1;\mathfrak{p}^\nu,\mathfrak{a})$, where again $\mathfrak{f} = \mathfrak{f}_0\mathfrak{p}^\nu$.
We now want to compute $(\phi\circ\phi_{\bar\omega}^{-1})(\bar\beta_1^{-1}\otimes\bar\beta_2)$. Since χ is now trivial we no longer have $X_{\{w|\infty\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi) = Y_{\{w|\infty\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)$, and therefore have to take into account the short exact sequence

$$0 \longrightarrow X^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\}} \longrightarrow X^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}} \longrightarrow Y^\infty_{\{w|\infty\}} \longrightarrow 0 \tag{38}$$

in the definition of $\phi_{\bar\omega}$. Recall here that $H^2(\Delta) = X^\infty_{\{w|\mathfrak{f}_0\mathfrak{p}\infty\}}$ and $Y^\infty_{\{w|\infty\}} = M^2$. A lift of $\sigma|_{k(\mathfrak{f})} \in M^2/\bar\omega = Y_{\{w|\infty\}}$ is given by $\sigma|_{k(\mathfrak{f})} - w_{\mathfrak{p}}$, where $w_{\mathfrak{p}}$ denotes a fixed place of $k(\mathfrak{f})$ above $\mathfrak{p}$. We obtain

$$\begin{aligned} (\phi\circ\phi_{\bar\omega}^{-1})(\bar\beta_1^{-1}\otimes\bar\beta_2) &= \phi(\bar\beta_1^{-1}\wedge x_J^{-1}\otimes\beta_{\bar\omega}(x_J)\wedge(\sigma|_{k(\mathfrak{f})}-w_{\mathfrak{p}})) \\ &= c_\chi\phi(\bar\beta_1^{-1}\wedge x_J^{-1}\otimes\mathrm{val}(x_J)\wedge(\sigma|_{k(\mathfrak{f})}-w_{\mathfrak{p}})) \end{aligned}$$

Next, we compute $\operatorname{val}(\bar\beta_1)$ and express the result in terms of $\sigma|_{k(\mathfrak{f})} - w_{\mathfrak{p}}$. If $\mathfrak{p} \nmid \mathfrak{f}$, then

$$\operatorname{val}(\bar\beta_1) = \frac{1}{12}(N\mathfrak{a}-1)\operatorname{val}\left(\frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{p})}\right).$$

We use $\Delta(\mathcal{O}_k)/\Delta(\mathfrak{p}) \sim \mathfrak{p}^{12}$ and obtain in $Y_{\{w|\mathfrak{f}_0\mathfrak{p}\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)$

$$\begin{aligned}
\operatorname{val}(\bar\beta_1) &= (N\mathfrak{a}-1)\sum_{w|\mathfrak{p}}\operatorname{ord}_w(\mathfrak{p})\cdot w \\
&= (N\mathfrak{a}-1)|I_{\mathfrak{p}}|\sum_{w|\mathfrak{p}} w \\
&= (N\mathfrak{a}-1)|I_{\mathfrak{p}}|\frac{|G_{\mathfrak{f}}|}{|D_{\mathfrak{p}}|}w_{\mathfrak{p}} \\
&= (N\mathfrak{a}-1)\frac{[k(\mathfrak{f}):k]}{f_{\mathfrak{p}}}w_{\mathfrak{p}}
\end{aligned}$$

An explicit splitting of the short exact sequence (14) is given by

$$w \mapsto w - \frac{1}{[k(\mathfrak{f}):k]}\operatorname{Tr}_{k(\mathfrak{f})/k}\sigma|_{k(\mathfrak{f})}.$$

Under this map $\operatorname{val}(\bar\beta_1)$ maps to $-(N\mathfrak{a}-1)\frac{[k(\mathfrak{f}):k]}{f_{\mathfrak{p}}}(\sigma|_{k(\mathfrak{f})} - w_{\mathfrak{p}})$ in $X_{\{w|\mathfrak{f}\mathfrak{p}\infty\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)$.

Recall that $\varphi_{\mathcal{O}_k}$ denotes the Euler function attached to the ring $\mathcal{O}_k$. In the case $\mathfrak{p} \mid \mathfrak{f}$ we compute from [1, Th. 2.4]

$$\begin{aligned}
\operatorname{val}(\bar\beta_1) &= \frac{N\mathfrak{a}-1}{\varphi_{\mathcal{O}_k}(\mathfrak{p}^\nu)}\sum_{w|\mathfrak{p}}\operatorname{ord}_w(\mathfrak{p})\cdot w \\
&= \frac{N\mathfrak{a}-1}{\varphi_{\mathcal{O}_k}(\mathfrak{p}^\nu)}\frac{[k(\mathfrak{f}):k]}{f_{\mathfrak{p}}}w_{\mathfrak{p}}.
\end{aligned}$$

So we derive the closed formula

$$\operatorname{val}(\bar\beta_1) = -\frac{N\mathfrak{a}-1}{\varphi_{\mathcal{O}_k}(\mathfrak{p}^\nu)}\frac{[k(\mathfrak{f}):k]}{f_{\mathfrak{p}}}(\sigma|_{k(\mathfrak{f})} - w_{\mathfrak{p}})$$

as elements of $X_{\{w|\mathfrak{f}\mathfrak{p}\infty\}}\otimes_{\mathfrak{A}}\mathbb{Q}_p(\chi)$.

This implies

$$(\phi\circ\phi_{\bar\omega}^{-1})(\bar\beta_1^{-1}) = \underbrace{-c_\chi\frac{\varphi_{\mathcal{O}_k}(\mathfrak{p}^\nu)}{N\mathfrak{a}-1}\frac{f_{\mathfrak{p}}}{[k(\mathfrak{f}):k]}}_{=:A}$$

On the other hand we compute for $\mathcal{L}\otimes 1$

$$\begin{aligned}
\mathcal{L}\otimes 1 &= (N\mathfrak{a}-\sigma(\mathfrak{a}))\eta_{\mathfrak{f}_0}^{-1}\otimes\sigma \\
&= (N\mathfrak{a}-\sigma(\mathfrak{a}))\,[k(\mathfrak{f}_0):k(1)]\,\frac{w(1)}{w(\mathfrak{f}_0)}\left[\mathrm{Tr}_{k(\mathfrak{f}_0\mathfrak{p}^{n+1})/k(\mathfrak{p}^{n+1})}\eta_{\mathfrak{f}_0}^{-1}\right]^{-1}\otimes\sigma \\
&= (N\mathfrak{a}-\sigma(\mathfrak{a}))\,[k(\mathfrak{f}_0):k(1)]\,\frac{w(1)}{w(\mathfrak{f}_0)}\prod_{\mathfrak{l}\mid\mathfrak{f}_0}\frac{1}{1-\mathrm{Fr}_{\mathfrak{l}}^{-1}}\eta_1^{-1}\otimes\sigma \\
&= \underbrace{(N\mathfrak{a}-\sigma(\mathfrak{a}))\,[k(\mathfrak{f}_0):k(1)]\,\frac{w(1)}{w(\mathfrak{f}_0)}\prod_{\mathfrak{l}\mid\mathfrak{f}_0}\frac{\bar\omega}{1-\mathrm{Fr}_{\mathfrak{l}}^{-1}}}_{=:B}\,\bar\omega^{e}(\beta_1^{-1}\otimes\bar\beta_2).
\end{aligned}$$

It follows from (35) together with

$$[k(\mathfrak{f}):k]=h_k\frac{w(\mathfrak{f})}{w(1)}\varphi_{\mathcal{O}_k}(\mathfrak{f}),\quad [k(\mathfrak{f}_0):k(1)]=\frac{w(\mathfrak{f}_0)}{w(1)}\varphi_{\mathcal{O}_k}(\mathfrak{f}_0)$$

that $\phi(\mathcal{L}\otimes 1)=AB=-f_{\mathfrak{p}}\left(\prod_{\mathfrak{l}\mid\mathfrak{f}_0}f_{\mathfrak{l}}\right)\frac{w(1)}{h_k}$. Since $\zeta_k^*(0)=-\frac{h_k}{w(1)}$ this concludes the proof.

References

[1] W. Bley, *Wild Euler systems of elliptic units and the Equivariant Tamagawa Number Conjecture*, J. Reine Angew. Math. 577 (2004) 117-146.

[2] M. Breuning, D. Burns, *Leading terms of Artin L-functions at $s=0$ and $s=1$*, preprint 2005, submitted for publication.

[3] D. Burns, *Congruences between derivatives of abelian L-functions at $s=0$*, preprint 2005, submitted for publication.

[4] D. Burns, M. Flach, *Tamagawa Numbers for motives with (non-commutative) coefficients*, Doc. Math., J. DMV 6 (2001) 501-570.

[5] D. Burns, C. Greither, *On the Equivariant Tamagawa Number Conjecture for Tate motives*, Invent. math. 153 (2003) 303-359.

[6] E. deShalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication* , Perspectives in Math. Vol. 3, Academic Press 1987.

[7] B. Ferrero, R. Greenberg, *On the behaviour of p-adic L-series at $s=0$*, Inv. Math. 50 (1978) 91-102.

[8] M. Flach, *The Equivariant Tamagawa Number Conjecture: A survey*, Stark's conjecture: recent work and new directions, Contemp. Math. 358 (2004) 79-125.

[9] R. Gillard, *Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes*, J. Reine Angew. Math. 358 (1986) 76-91.

[10] C. Greither, *Class groups of abelian fields and the main conjecture*, Ann. Inst. Fourier, 42 (1992) 449-499.

[11] A. Huber, G. Kings, *Bloch-Kato Conjecture and Main Conjecture of Iwasawa teory for Dirichlet characters*, Duke Math. J. 119 (2003) 393-464.

[12] J.M. Johnson, *Artin L-functions for abelian extensions of imaginary quadratic fields*, Thesis, California Institute of Technology, Pasadena, California 2005

[13] K. Kato, *Lectures on the approach to Iwasawa theory of Hasse-Weil L-functions via B_{dR}*, Part I, In: Arithmetical algebraic Geometry, Ballico, E. (eds.) Lect.Notes Math. 1553, 50 - 163, New York, Springer 1993.

[14] F. Knudsen, D. Mumford, *The projectivity of the moduli space of stable curves I: Preliminaries on 'det' and 'Div'*, Math. Scand. 39 (1976) 19-55.

[15] F. Knudsen, *Determinant functors on exact categories and their extensions to categories of bounded complexes*, Michigan Math.J. 50 (2002) 407-444.

[16] B. Mazur, A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76 (1984) 179-330.

[17] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Heidelberg, 1992.

[18] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, Springer, Berlin Heidelberg, 2000.

[19] G. Robert, *Unités elliptiques*, Bull.Soc.Math.France, Mémoire 36 (1973).

[20] G. Robert, *Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe*, Invent. math. 100 (1990) 231-257.

[21] G. Robert, *La racine* 12*-ième canonique de* $\Delta(L)^{[\underline{L}:L]}/\Delta(\underline{L})$, Séminaire de Théorie des Nombres Paris (1989-90) 209-232.

[22] J. Ritter, A. Weiss, *Toward equivariant Iwasawa theory*, munuscrpita mathematica 109 (2002) 131-146.

[23] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent.Math. 89 (1987), 527–560.

[24] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent.Math. 103 (1991), 25–68.

[25] K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent.Math. 93 (1988), 701–713.

[26] K. Rubin, *The main conjecture*, Appendix to the second edition of Serge Lang: Cyclotomic fields, Springer Verlag, 1990.

[27] K. Rubin, *Euler Systems*, Annals of mathematics studies 147, Princeton University Press, 2000.

[28] R. Schertz, *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, J. Reine Angew. Math. 398 (1989), 105–129.

[29] D. Solomon, *On a construction of p-units in abelian fields*, Invent. math. 109 (1992) 329-350.

[30] T. Tsuji, *Semi-local Units modulo Cyclotomic Units* , J.Number Theory. 78 (1999) 1-26.

[31] L. Washington, *Introduction to cyclotomic fields*, Springer Verlag 1998.

[32] A. Wiles, *The Iwasawa conjecture for totally real fields* , Ann. Math. 131 (1990) 493-540.

W. Bley
Universität Kassel
Fachbereich 17
D-34109 Kassel
Germany
bley@mathematik.uni-kassel.de

The Distribution of Group Structures on Elliptic Curves over Finite Prime Fields

Ernst-Ulrich Gekeler

Received: April 12, 2006

Communicated by Peter Schneider

Abstract. We determine the probability that a randomly chosen elliptic curve $E/\mathbb{F}_p$ over a randomly chosen prime field $\mathbb{F}_p$ has an ℓ-primary part $E(\mathbb{F}_p)[\ell^\infty]$ isomorphic with a fixed abelian ℓ-group $H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$.

Probabilities for "$|E(\mathbb{F}_p)|$ divisible by n", "$E(\mathbb{F}_p)$ cyclic" and expectations for the number of elements of precise order n in $E(\mathbb{F}_p)$ are derived, both for unbiased $E/\mathbb{F}_p$ and for $E/\mathbb{F}_p$ with $p \equiv 1$ (ℓ^r).

2000 Mathematics Subject Classification: 11 N 45, 11 G 20, 11 S 80
Keywords and Phrases: Elliptic curves over finite fields, group structures, counting functions

1. Introduction

Given an elliptic curve E over the finite field $\mathbb{F}_q$ with q elements, the set $E(\mathbb{F}_q)$ of rational points forms an abelian group, which satisfies

$$|E(\mathbb{F}_q) - (q+1)| \leq 2q^{1/2} \quad \text{(Hasse)} \tag{1.1}$$

and

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m \times \mathbb{Z}/n \tag{1.2}$$

with well-defined numbers m, n and $m|n$. Our aim is to study the statistics of such group structures if $E/\mathbb{F}_q$ varies through an infinite family $\mathcal{F}$. In the present article, we consider

$$\mathcal{F} = \{\mathbb{F}_p\text{-isomorphism classes of elliptic curves } E/\mathbb{F}_p \text{ over finite prime fields } \mathbb{F}_p\} \tag{1.3}$$

but note that a similar study may be performed for elliptic curves $E/\mathbb{F}_q$ over arbitrary finite fields, or for $E/\mathbb{F}_q$ where q runs through the powers of the fixed prime number p.

Given any algebraic property (A) of $E/\mathbb{F}_p$ (or any subset A of $\mathcal{F}$), we define its "probability" in $\mathcal{F}$ as

$$(1.4)\qquad P(\mathcal{F},A) := \lim_{x\to\infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p\le x,\ E/\mathbb{F}_p \text{ has property } A\}|}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \le x\}|},$$

provided the limit exists. Then $P(\mathcal{F},\cdot)$ is a "content" on $\mathcal{F}$, i.e., it satisfies the usual axioms of a probability measure except that the condition of σ-additivity (= countable additivity) is relaxed to finite additivity. In a similar fashion, we may define other notions of probability theory for $\mathcal{F}$, for example the conditional probability $P(\mathcal{F},A|B)$ for property A under condition B, or the expectation $E(\mathcal{F},f)$ for a function f on $\mathcal{F}$.

It is obvious from (1.1) that $P(\mathcal{F},A)=0$ for any property like

$$\text{(A)}\qquad E(\mathbb{F}_p)\cong \mathbb{Z}/m\times\mathbb{Z}/n \quad \text{with } m,n \text{ fixed};$$

i.e., such probabilities are meaningless. Instead, the typical question we will deal with is:

1.5 Question: Let a prime number ℓ and a finite abelian ℓ-group

$$H = H_{\alpha,\beta}^{(\ell)} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$$

with $0\le\alpha\le\beta$ be given. How likely (cf. (1.4)) is it that the ℓ-primary part $E(\mathbb{F}_p)[\ell^\infty]$ of $E(\mathbb{F}_p)$ is isomorphic with H, if $E/\mathbb{F}_p$ is randomly chosen in $\mathcal{F}$?

(Instead of fixing one prime ℓ and the finite ℓ-group H, we could fix a finite set L of primes and a finite abelian L-group H of rank less or equal to 2, and ask for the probability that the L-part of $E(\mathbb{F}_p)$ is isomorphic with H.)

In Theorem 3.15, using results of E. Howe [7], we show that the corresponding $P(\mathcal{F},$ "$E(\mathbb{F}_p)[\ell^\infty]\cong H_{\alpha,\beta}^{(\ell)}$") always exists, and give its value, along with an error term $O_{\ell,\alpha,\beta}(x^{-1/2})$. As prescribed by Serre's "Čebotarev theorem" ([8], Theorem 7), that probability agrees with the (non-vanishing) Haar volume $g^{(\ell)}(\alpha,\beta)$ of a certain subset $X^{(\ell)}(\alpha,\beta)$ of $\mathrm{GL}(2,\mathbb{Z}_\ell)$. The relevant Haar measures are provided by Theorem 2.3, the proof of which forms the contents of section 2.

Actually, we will see in section 4 that $P(\mathcal{F},\cdot)$ defines a probability measure (in the usual sense, that is, even σ-additive) on the discrete set of isomorphism classes of abelian groups of shape $H_{\alpha,\beta}^{(\ell)}=\mathbb{Z}/\ell^\alpha\times\mathbb{Z}/\ell^\beta$ $(0\le\alpha\le\beta)$, and that these measures for varying primes ℓ are stochastically independent.

We use the preceding to derive (both without restrictions on p, or under congruence conditions for p) the exact values of

(a) the probability $P(\mathcal{F},$ "$n|\ |E(\mathbb{F}_p)|$") that $|E(\mathbb{F}_p)|$ is divisible by the fixed natural number n (Proposition 5.1, Corollary 5.2);
(b) the expectation $E(\mathcal{F},\kappa_n)$ for the number $\kappa_n(E(\mathbb{F}_p))$ of elements of precise order n in $E(\mathbb{F}_p)$ (Proposition 5.6);
(c) the probability $P(\mathcal{F},$ "$E(\mathbb{F}_p)$ is cyclic") of cyclicity of $E(\mathbb{F}_p)$ (Theorem 5.9).

Items (a) and (c) are related to results of Howe (Theorem 1.1 of [5]) and S.G. Vladut (Theorem 6.1 of [7]), the difference being that the cited authors consider elliptic curves E over one fixed finite field $\mathbb{F}_q$, while (a),(b),(c) are results averaged over all $\mathbb{F}_p$ (or all $\mathbb{F}_p$ where p lies in some arithmetic progression).

Given $E/\mathbb{F}_p$ and a prime number ℓ different from p, we let $F_\ell = F_\ell(E/\mathbb{F}_p)$ be its Frobenius element, an element of $\mathrm{GL}(2, \mathbb{Z}_\ell)$ well-defined up to conjugation ($\mathbb{Z}_\ell = \ell$-adic integers). Its characteristic polynomial $\chi_{F_\ell}(X) = X^2 - \mathrm{tr}(F_\ell)X + \det(F_\ell)$ satisfies

$$\det(F_\ell) = p,\ \mathrm{tr}(F_\ell) = p + 1 - |E(\mathbb{F}_p)|; \tag{1.6}$$

in particular, it has integral coefficients independent of ℓ. It is related with the group structure on $E(\mathbb{F}_p)$ through

$$E(\mathbb{F}_p)[\ell^\infty] \cong \mathrm{cok}(F_\ell - 1), \tag{1.7}$$

where "cok" is the cokernel of a matrix regarded as an endomorphism on $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ (see e.g. [3], appendix, Proposition 2).

In order to avoid technical problems irrelevant for our purposes, we exclude for the moment the primes $p = 2$ and 3 from our considerations, that is, $\mathcal{F} = \{E/\mathbb{F}_p \mid p \geq 5 \text{ prime}\}$. Then we define

$$w(E/\mathbb{F}_p) = 2|\mathrm{Aut}_{\mathbb{F}_p}(E/\mathbb{F}_p)|^{-1} = \begin{cases} \frac{1}{3},\ p \equiv 1\ (3),\ j(E) = 0 \\ \frac{1}{2},\ p \equiv 1\ (4),\ j(E) = 12^3 \\ 1\ ,\quad \text{otherwise.} \end{cases} \tag{1.8}$$

Thus in "most" cases, $w(E/\mathbb{F}_p) = 1$. For well-known philosophical reasons not addressed here, we will count subsets of $\mathcal{F}$ not by ordinary cardinality, but by cardinality weighted with w. That is, for a finite subset $\mathcal{F}'$ of $\mathcal{F}$, we define its weighted cardinality as

$$|\mathcal{F}'|^* = \sum_{E/\mathbb{F}_p \in \mathcal{F}'} w(E/\mathbb{F}_p). \tag{1.9}$$

Then we have for example

$$|\{E/\mathbb{F}_p\}|^* = 2p \tag{1.10}$$

for the number* of isomorphism classes of elliptic curves over a fixed prime field $\mathbb{F}_p$. Accordingly, we redefine probabilities $P(\mathcal{F}, A)$ as in (1.4), replacing ordinary "$|\ |$" by weighted cardinalities "$|\ |^*$". Of course, it doesn't matter whether or not we include the finite number of $E/\mathbb{F}_p$ with $p = 2, 3$ into $\mathcal{F}$.

With each $E/\mathbb{F}_p \in \mathcal{F}$, we associate its total Frobenius element

$$F(E/\mathbb{F}_p) = (\ldots, F_\ell(E/\mathbb{F}_p), \ldots) \in \Pi_{\ell\ \mathrm{prime}} \mathrm{GL}(2, \mathbb{Z}_\ell)$$

(well-defined up to conjugation, and neglecting for the moment the question of the p-component of F). As usual, we let

$$\hat{\mathbb{Z}} = \varprojlim_{N \in \mathbb{N}} \mathbb{Z}/N = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$$

be the profinite completion of $\mathbb{Z}$. Then $\mathrm{GL}(2, \hat{\mathbb{Z}}) = \prod \mathrm{GL}(2, \mathbb{Z}_\ell)$ is a compact group provided with a canonical projection "(mod$N$)" onto $\mathrm{GL}(2, \mathbb{Z}/N)$ for each $N \in \mathbb{N}$.

Led by the Čebotarev and other equidistribution theorems or conjectures, in particular, the "Cohen-Lenstra philosophy" [2], we make the following hypothesis:

(H) The series $(F(E/\mathbb{F}_p))_{E/\mathbb{F}_p \in \mathcal{F}}$ is equidistributed in $\mathrm{GL}(2, \hat{\mathbb{Z}})$.

In more detailed terms, this means:

(1.11) Given $N \in \mathbb{N}$ and any conjugacy class $\mathcal{C}$ in $\mathrm{GL}(2, \mathbb{Z}/N)$, the limit

$$\lim_{x \to \infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid F(E/\mathbb{F}_p)(\mathrm{mod} N) \text{ lies in } \mathcal{C} \text{ and } p \leq x\}|^*}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*}$$

exists and equals $|\mathcal{C}|/|\mathrm{GL}(2, \mathbb{Z}/N)|$.

Note that in the form just given, the hypothesis does not require specifying the p-component of $F(E/\mathbb{F}_p)$, since for given N and $\mathcal{C}$ we may omit the finite number of terms indexed by $E/\mathbb{F}_p$ with $p|N$ without changing the limit. Note also that the number of $E/\mathbb{F}_p$ with $w(E/\mathbb{F}_p) \neq 1$ over a fixed $\mathbb{F}_p$ is uniformly bounded, and is therefore negligible for large p. That is, though (1.11) appears to be the "right" formula, the limit (provided it exists) doesn't change upon replacing weighted by unweighted cardinalities.

Now (H) may be derived from the general "Čebotarev theorem" (Theorem 7 of [8]) of Serre, applied to the moduli scheme of elliptic curves endowed with a level-N structure, and also from Theorem 3.1 of [1]. We thus regard (H) as established, although our proofs are independent of its validity.

In [6], we studied the frequency of $E/\mathbb{F}_p$ with a fixed Frobenius trace $\mathrm{tr}(E/\mathbb{F}_p) \in \mathbb{Z}$. The results (*loc. cit.*, Theorems 5.5 and 6.4) turned out to be those expected by (H) (and other known properties of $E/\mathbb{F}_p$, like the result of [2]). On the other hand, (H) in the form (1.11) applied to prime powers $N = \ell^n$ along with (1.7) predicts that for each group $H^{(\ell)}_{\alpha,\beta} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$, the probability $P(\mathcal{F}, \text{"}E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\text{"})$ equals the Haar volume in $\mathrm{GL}(2, \mathbb{Z}_\ell)$ of $\{\gamma \in \mathrm{GL}(2, \mathbb{Z}_\ell) \mid \mathrm{cok}(\gamma - 1) \cong H^{(\ell)}_{\alpha,\beta}\}$. Our Theorem 3.15 states an effective version of that identity, i.e., including the error term.

Notation. Apart from standard mathematical symbols, we use the following notation.

$\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ and $\mathbb{P} = \{2, 3, 5, \ldots\}$ denote the sets of natural, of non-negative integral, of prime numbers, respectively, and $|X|$ the cardinality of the set X. For $m, n \in \mathbb{N}$, "$m|n$" means "m divides n" and "$m\|n$" that m is an exact divisor of n, i.e., $m|n$ and m is coprime with n/m.

$\mathbb{Z}/n$ is the residue class group $\mathbb{Z}/n\mathbb{Z}$, and for each abelian group A and $n \in \mathbb{N}$, $A[n] = \{x \in A \mid nx = 0\}$. Further, for $\ell \in \mathbb{P}$, $A[\ell^\infty] = \bigcup_{r \in \mathbb{N}} A[\ell^r]$.

The symbols p and ℓ always stand for primes, and e.g. "$\sum_{p \le x} \cdots$" means the sum over all primes $p \le x$.

If f and g are functions defined on suitable subsets of $\mathbb{R}$, then

$$f \sim g :\Leftrightarrow \lim_{x \to \infty} f(x)/g(x) = 1;$$

$f = O(g) :\Leftrightarrow$ there exists a constant $C > 0$ such that $f(x) \le Cg(x)$. We write $f = O_{\alpha,\beta}(g)$ to indicate that C might depend on the parameters $\alpha, \beta, \ldots$

2. Some Haar measures in $\mathrm{GL}(2, \mathbb{Z}_\ell)$.

In the present section, we calculate the volumes with respect to Haar measure of certain subsets of $\mathrm{GL}(2, \mathbb{Z}_\ell)$ relevant for our purposes.

(2.1) Fix a prime number ℓ, and let

$M = \mathrm{Mat}(2, \mathbb{Z}_\ell)$ be the ring of 2×2-matrices over $\mathbb{Z}_\ell$, and

$G = \mathrm{GL}(2, \mathbb{Z}_\ell)$, with normalized Haar measures μ on M and ν on G, respectively.

For each natural number n, we put

$$M_n = \mathrm{Mat}(2, \mathbb{Z}/\ell^n) \text{ and } G_n = \mathrm{GL}(2, \mathbb{Z}/\ell^n).$$

By abuse of language, and if the context allows for no ambiguity, we often write "a" for the image of $a \in \mathbb{Z}_\ell$ (or of $a \in \mathbb{Z}/\ell^m$ with $m \ge n$) in $\mathbb{Z}/\ell^n$, etc. The reduction mapping $a \longmapsto \overline{a} : \mathbb{Z}_\ell \longrightarrow \mathbb{F}_\ell = \mathbb{Z}/\ell$ and everything derived from it will be denoted by a bar, e.g. $\gamma \longmapsto \overline{\gamma} : M \longrightarrow M_1$. Finally, v_ℓ denotes both the ℓ-adic valuation on $\mathbb{Z}_\ell$ and the truncated valuation $\mathbb{Z}/\ell^n \longrightarrow \{0, 1, \ldots, n\}$.

(2.2) The possible ℓ-torsion of an elliptic curve over a finite field is of shape

$$H = H_{\alpha,\beta} = H_{\alpha,\beta}^{(\ell)} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta,$$

where $0 \le \alpha \le \beta$ are well-defined by H. (We omit some ℓ's in the notation.) For reasons explained in the introduction, we are interested in the volumes (with respect to ν) of the subsets

$$X(\alpha, \beta) = \{\gamma \in G \mid \mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta}\}$$

and

$$X_r(\alpha, \beta) = \{\gamma \in G \mid \mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta},\ v_\ell(\det(\gamma) - 1) = r\}$$

of G. Here $\mathrm{cok}(\delta) = \mathbb{Z}_\ell^2/\delta(\mathbb{Z}_\ell^2)$ is the module determined by the matrix $\delta \in M$. We will show:

2.3 Theorem.

(i) *Given* $\alpha, \beta \in \mathbb{N}_0$ *with* $\alpha \leq \beta$, *we have* $\mathrm{vol}_\nu(X(\alpha,\beta)) = g(\alpha,\beta)$ *with*

$$g(\alpha,\beta) = \begin{cases} \frac{\ell^3-2\ell^2-\ell+3}{(\ell^2-1)(\ell-1)}, & 0=\alpha=\beta \\ \frac{\ell^2-\ell-1}{(\ell-1)\ell}\ell^{-\beta}, & 0=\alpha<\beta \\ \ell^{-4\alpha}, & 0<\alpha=\beta \\ \frac{\ell+1}{\ell}\ell^{-\beta-3\alpha}, & 0<\alpha<\beta\ . \end{cases}$$

(ii) *Given* $\alpha \leq \beta$ *and* $r \in \mathbb{N}_0$, $X_r(\alpha,\beta)$ *is empty if* $r < \alpha$. *Otherwise,* $\mathrm{vol}_\nu(X_r(\alpha,\beta))$ *is given by the following table.*

$\mathrm{vol}_\nu(X_r(\alpha,\beta))$	$r=\alpha$	$r>\alpha$
$0=\alpha=\beta$	$(\frac{\ell-2}{\ell-1})^2$	$\frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-r}$
$0=\alpha<\beta$	$\frac{\ell-2}{\ell-1}\ell^{-\beta}$	$\frac{\ell-1}{\ell}\ell^{-\beta-r}$
$0<\alpha=\beta$	$\frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-4\alpha}$	$\frac{\ell}{\ell+1}\ell^{-3\alpha-r}$
$0<\alpha<\beta$	$\ell^{-\beta-3\alpha}$	$\frac{\ell+1}{\ell}\ell^{-\beta-2\alpha-r}$

We need some preparations to prove the theorem. We start with three simple observations, stated without proof, where we always assume that $0 \leq \alpha \leq \beta$.

(2.4) For $\delta \in M$ we have the equivalence

$$\mathrm{cok}(\delta) \cong H_{\alpha,\beta} \quad \Leftrightarrow \quad \begin{array}{l}\delta \equiv 0\ (\ell^\alpha),\ \delta \not\equiv 0\ (\ell^{\alpha+1}) \text{ and} \\ v_\ell(\det\ \delta) = \alpha+\beta.\end{array}$$

(2.5) If $\delta \in M$ satisfies $\mathrm{cok}(\delta) \cong H_{\alpha,\beta}$ and $\delta \equiv \delta'(\ell^n)$ with $n > \beta$ then $\mathrm{cok}(\delta') \cong H_{\alpha,\beta}$.

As a consequence we get:

(2.6) If $n > \beta$ then

$$\mathrm{vol}_\mu\{\delta \in M \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\} = \ell^{-4n}|\{\delta \in M_n \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\}|.$$

That number is easy to determine.

2.7 Proposition.

$$\mathrm{vol}_\mu\{\delta \in M \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\} = \begin{cases} (1-\ell^{-1})(1-\ell^{-2})\ell^{-4\alpha}, & 0 \leq \alpha = \beta \\ (1-\ell^{-2})^2\ell^{-\beta-3\alpha}, & 0 \leq \alpha < \beta. \end{cases}$$

Proof. In view of (2.4) and the bijection $\delta \longmapsto \ell^{-\alpha}\delta$ of $\{\delta \in M_n \mid \mathrm{cok}(\delta) \cong H_{\alpha,\beta}\}$ with $\{\epsilon \in M_{n-\alpha} \mid \mathrm{cok}(\epsilon) \cong H_{0,\beta-\alpha}\}$, valid for $n > \beta$, the proof boils down to counting of matrices ϵ in $M_{n-\alpha}$ with $\overline{\epsilon} \neq 0$ and given value of $v_\ell(\det\ \epsilon)$. We omit the details. □

2.8 Remark. The volume of $\{\delta \in \mathrm{Mat}(n, \mathbb{Z}_\ell) \mid \mathrm{cok}(\delta) \cong H\}$ has been calculated by Friedman and Washington in full generality, i.e., for arbitrary n and abelian ℓ-groups H (see Proposition 3.1 of [5]). In our special case however, it is less complicated to apply the simple proof scheme given above than to extract (2.7) from the general result.

Similar to (2.6) we have

$$(2.9)\quad \begin{array}{rcl} \mathrm{vol}_\nu(X(\alpha,\beta)) &=& |G_n|^{-1}|\{\gamma \in G_n \mid \mathrm{cok}(\gamma-1) \cong H_{\alpha,\beta}\}| \\ \text{and} && \\ \mathrm{vol}_\nu(X_r(\alpha,\beta)) &=& |G_n|^{-1}|\{\gamma \in G_n \mid \mathrm{cok}(\gamma-1) \cong H_{\alpha,\beta}, \\ && \qquad v_\ell(\det(\gamma)-1) = r\}|, \end{array}$$

where $n > \beta$ in the first and $n > \max(\beta, r)$ in the second case.

Note that

$$(2.10)\qquad |G_n| = |G_1|\ell^{4(n-1)} = (\ell^2-1)(\ell-1)\ell^{4n-3}.$$

Thus (2.3) will be established as soon as we determine the numerators in (2.9).

Let $\gamma \in G$ with residue class $\overline{\gamma} \in G_1 = \mathrm{GL}(2, \mathbb{F}_\ell)$ be given, and suppose that $\mathrm{cok}(\gamma - 1) \cong H_{\alpha,\beta}$ with $0 \le \alpha \le \beta$.

2.11 Lemma. *We have*

(I) $0 = \alpha = \beta \Leftrightarrow 1$ *is not an eigenvalue of* $\overline{\gamma}$. *There are* $\ell(\ell^3 - 2\ell^2 - \ell + 3)$ *such elements* $\overline{\gamma} \in G_1$, *among which there are* $\ell(\ell^2 - \ell - 1)$ *with determinant* 1;

(II) $0 = \alpha < \beta \Leftrightarrow \overline{\gamma} - 1$ *has rank* 1
$\Leftrightarrow \overline{\gamma}$ *is conjugate to* $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ *(case* IIa*)* *or*
$\overline{\gamma}$ *is conjugate to* $\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)$ *with* $d \in \mathbb{F}_\ell - \{0,1\}$ *(case* IIb*).*
There are $\ell^2 - 1$ *(case* IIa*) and* $(\ell+1)\ell(\ell-2)$ *(case* IIb*) such* $\overline{\gamma} \in G_1$;

(III) $0 < \alpha \le \beta \Leftrightarrow \overline{\gamma} = 1$.

Proof. For $\delta = \gamma - 1$ we have $\mathrm{cok}(\delta)/\ell\,\mathrm{cok}(\delta) = \mathrm{cok}(\overline{\delta})$, and thus the equivalences are obvious. Now the centralizer of $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ (resp. of $\left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)$) in G_1 consists of the matrices of shape $\left(\begin{smallmatrix}a&b\\0&a\end{smallmatrix}\right)$ (resp. the diagonal matrices) in G_1, from which we find the numbers of $\overline{\gamma}$ subject to condition IIa (resp. IIb) and, finally, of $\overline{\gamma}$ subject to I. There are $\ell^3 - \ell$ elements $\overline{\gamma}$ of determinant 1, of which $\ell^2 - 1$ (resp. 1) are of type II (resp. III), thus $\ell^3 - \ell^2 - \ell$ of type I. □

Next, we need a series of lemmas that count numbers of matrices in M_n with various properties.

2.12 Lemma. (i) *The number of* $\overline{\delta} \in M_1$ *such that* $\det(\overline{\delta}) \neq 0$ *equals* $\ell(\ell^2 - 1)(\ell - 1)$. *A share of* $\ell \cdot (\ell^2 - 1)^{-1}$, *i.e., precisely* $\ell^2(\ell - 1)$ *of them, satisfy* $\mathrm{tr}(\overline{\delta}) = 0$.

(ii) *The number of* $0 \neq \overline{\delta} \in M_1$ *such that* $\det(\overline{\delta}) = 0$ *equals* $(\ell-1)(\ell+1)^2$. *A share of* $(\ell+1)^{-1}$, *i.e., precisely* $\ell^2 - 1$ *of them, satisfy* $\mathrm{tr}(\overline{\delta}) = 0$.

Proof. Omitted. □

2.13 Lemma. *Let* $n \in \mathbb{N}$ *and* $\delta_n \in M_n = \mathrm{Mat}(2, \mathbb{Z}/\ell^n)$ *be given, and suppose that*

$$\mathrm{tr}(\delta_n) + \det(\delta_n) \equiv 0 \ (\ell^n).$$

Then there are precisely ℓ^3 *elements* $\delta_{n+1} \in M_{n+1}$ *such that* $\delta_{n+1} \equiv \delta_n(\ell^n)$ *and*

$$\mathrm{tr}(\delta_{n+1}) + \det(\delta_{n+1}) \equiv 0 \ (\ell^{n+1}).$$

Proof. Writing $\delta_n = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}/\ell^n$, we have

$$(*) \qquad a + d + ad - bc = 0.$$

If $\overline{a} \neq -1$, we write the left hand side as $d(1+a) + a - bc$, choose arbitrary lifts $\tilde{a}, \tilde{b}, \tilde{c}$ of a, b, c in $\mathbb{Z}/\ell^{n+1}$ and solve for $\tilde{d}$ such that $(*)$ holds for $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}$. If $\overline{a} = -1$ but $\overline{d} \neq -1$, we may exchange the parts of a and d. If both $\overline{a}$ and $\overline{d}$ equal -1 then $\overline{b}\overline{c} = -1$, we may arbitrarily choose lifts $\tilde{a}, \tilde{b}, \tilde{d}$ of a, b, d and solve for $\tilde{c}$. In any case, we get precisely ℓ^3 matrices $\delta_{n+1} = \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{smallmatrix}\right) \in M_{n+1}$ as required. □

2.14 Lemma. *Let* $0 < \beta < n$ *and* $\overline{d} \in \mathbb{F}_\ell - \{0\}$ *be fixed. The number of matrices* $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_n$ *such that* $\overline{\delta} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & \overline{d} \end{smallmatrix}\right)$ *and* $v_\ell(ad - bc) = \beta$ *is* $(\ell-1)\ell^{4n-4-\beta}$.

Proof. For each of the $(\ell-1)\ell^{n-1-\beta}$ possible values of "det" in $\mathbb{Z}/\ell^n$ with $v_\ell(\det) = \beta$, the quantities b, c and d may be freely chosen subject to $\overline{b} = 0 = \overline{c}$ and $d \equiv \overline{d}(\ell)$, and then $a = d^{-1}(\det + bc)$. □

2.15 Lemma. *Let* $t, u \in \mathbb{Z}/\ell^n$ *be given with* $\overline{t} = 0 = \overline{u}$. *There are precisely* $(\ell^2-1)\ell^{2(n-1)}$ *elements* $\epsilon = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *of* M_n *such that* $\overline{\epsilon} \neq 0$, $\mathrm{tr}(\epsilon) = t$ *and* $\det(\epsilon) = u$.

Proof. Choose $a \in \mathbb{Z}/\ell^n$, which determines $d = t - a$. If $\overline{a} \neq 0$ then $\overline{d} \neq 0$, and we may freely choose $b \in (\mathbb{Z}/\ell^n)^*$ and solve for c in

$$(*) \qquad ad - u = bc.$$

If $\overline{a} = 0$ then $\overline{d} = 0$, either b or c is invertible, and we may solve for the other one in $(*)$. Counting the number of possible choices yields the stated value. □

Now we are ready for the

Proof of Theorem 2.3. At several occasions, we will use the trivial identity

$$(1) \qquad \det(1 + \delta) = 1 + \mathrm{tr}(\delta) + \det(\delta)$$

for 2×2-matrices δ. Among other things, it implies (together with (2.4)) that $X_r(\alpha, \beta)$ is empty for $r < \alpha$.

Case $\boxed{\boxed{0 = \alpha = \beta}}$ From (2.9), putting $n = 1$, and (2.11), we see after a little calculation that the volumes of $X(0,0)$ and $X_0(0,0)$ are as asserted. Let $\overline{\gamma} = 1+\overline{\delta} \in G_1$ be such that $\overline{\delta}$ also belongs to G_1. By (2.11), there are precisely $\ell(\ell^2-\ell-1)$ such $\overline{\gamma}$ with determinant 1, i.e., using (1), such that $\mathrm{tr}(\overline{\delta}) + \det(\overline{\delta}) = 0$. By induction on n, using (2.13), we see that among the $\ell^{4(n-1)}$ lifts $\gamma_n = 1+\delta_n$ of $\overline{\gamma}$ to G_n, there are precisely $\ell^{3(n-1)}$ that satisfy $\det(\gamma_n) \equiv 1\ (\ell^n)$, if $n \geq 2$. For $r \geq 1$ and $n := r+1$, (2.9) yields

$$\mathrm{vol}(X_r(0,0)) = \frac{\ell(\ell^2-\ell-1)\ell^{3(r-1)}(\ell^4-\ell^3)}{(\ell^2-1)(\ell-1)l^{4r+1}} = \frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-r}.$$

Case $\boxed{\boxed{0 = \alpha < \beta}}$ According to (2.4) and (2.9), we have for $n > \beta$

$$\mathrm{vol}(X(0,\beta)) = |G_n|^{-1}|\{\gamma \in G_n \mid \overline{\gamma} \neq 1,\ v_\ell(\det(\gamma-1)) = \beta\}|.$$

Any $\gamma = 1+\delta$ as above satisfies (see (2.11)):

- $\overline{\gamma} \in G_1$ is conjugate to $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, which happens ℓ^2-1 times, or
- $\overline{\gamma}$ is conjugate to $\left(\begin{smallmatrix}1&0\\0&d'\end{smallmatrix}\right)$, which happens $(\ell+1)\ell(\ell-2)$ times.

Thus we have to count the number of lifts $\gamma \in G_n$ of $\overline{\gamma}$ such that $v_\ell(\det(\gamma-1)) = \beta$, i.e., of lifts δ of $\overline{\delta}$ with $v_\ell(\det\delta) = \beta$. Clearly, that number is invariant under conjugation, so we may assume that

- $\overline{\gamma} = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, i.e., $\overline{\delta} = \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, or
- $\overline{\gamma} = \left(\begin{smallmatrix}1&0\\0&d'\end{smallmatrix}\right)$, i.e., $\overline{\delta} = \left(\begin{smallmatrix}0&0\\0&d\end{smallmatrix}\right)$ with $d = d'-1 \in \mathbb{F}_\ell - \{0,-1\}$.

In both cases, Lemma 2.14 (after possibly permuting the rows of $\overline{\delta}$) yields the same number $(\ell-1)\ell^{4n-4-\beta}$ of lifts of the wanted type. Therefore,

$$\begin{aligned}\mathrm{vol}(X(0,\beta)) &= |G_n|^{-1}[\ell^2-1+(\ell+1)\ell(\ell-2)](\ell-1)\ell^{4n-4-\beta}\\ &= \tfrac{\ell^2-\ell-1}{(\ell-1)\ell}\ell^{-\beta}.\end{aligned}$$

In order to find $\mathrm{vol}(X_r(0,\beta))$, we must determine the number of lifts γ as above that moreover satisfy

$$\det\gamma \equiv 1\ (\ell^r),\ \not\equiv 1\ (\ell^{r+1}),\ \text{ where } r < n, \text{ i.e., } n > \max(\beta, r).$$

Suppose $\boxed{r > 0}$ and $\overline{\gamma}$ conjugate to $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, without restriction, $\overline{\gamma} = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, $\overline{\delta} = \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$. The number of lifts is the number of $\delta = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \in M_n$ such that

(2) $a \equiv c \equiv d \equiv 0$, $b \equiv 1\ (\ell)$
(3) $a+d+ad-bc = \mathrm{tr}(\delta)+\det(\delta) \equiv 0\ (\ell^r)$, $\not\equiv 0\ (\ell^{r+1})$
(4) $v_\ell(\det\delta) = \beta$

hold. Now there are

- $(\ell-1)\ell^{n-\beta-1}$ choices of $\det(\delta)$ subject to (4);
- ℓ^{n-1} free choices for a and b each subject to (2);
- $(\ell-1)\ell^{n-r-1}$ choices for d compatible with (2), (3) and the choices made of $\det(\delta)$ and a,

which together determine $c = b^{-1}(ad - \det(\delta))$. Therefore, $\overline{\gamma}$ has $(\ell-1)^2\ell^{4(n-1)-r-\beta}$ lifts of the wanted type. If, on the other hand, $\overline{\gamma}$ is conjugate to $\left(\begin{smallmatrix}1&0\\0&d'\end{smallmatrix}\right)$ with $d' \neq 0,1$, then any lift γ satisfies $\det(\gamma) \not\equiv 1\ (\ell^r)$. Hence

$$\operatorname{vol}(X_r(0,\beta)) = |G_n|^{-1}(\ell^2-1)(\ell-1)^2\ell^{4(n-1)-r-\beta} = \tfrac{\ell-1}{\ell}\ell^{-\beta-r}.$$

Suppose $\boxed{r=0}$. If $\overline{\gamma}$ is unipotent, no lifts of the wanted type exist. Thus let $\overline{\gamma} = \left(\begin{smallmatrix}1&0\\0&d'\end{smallmatrix}\right)$ with $d' \in \mathbb{F}_\ell - \{0,1\}$. Any lift $\gamma \in G_n$ of $\overline{\gamma}$ satisfies $\det(\gamma) \not\equiv 1\ (\ell)$, so we have for $n > \beta$

$$\operatorname{vol}(X_0(0,\beta)) = |G_n|^{-1}(\ell+1)\ell(\ell-2)(\ell-1)\ell^{4n-4-\beta} = \tfrac{\ell-2}{\ell-1}\ell^{-\beta}.$$

It remains to treat the

Case $\boxed{\boxed{0<\alpha\le\beta}}$. Here, for $n > \beta$,

$$\operatorname{vol}(X(\alpha,\beta)) = |G_n|^{-1}|\{\gamma \in M_n \mid \overline{\gamma} = 1,\ \operatorname{cok}(\gamma-1) \cong H_{\alpha,\beta}\}|.$$

The condition on $\gamma = 1+\delta$ is equivalent with $\overline{\delta} = 0$, $\operatorname{cok}(\delta) \cong H_{\alpha,\beta}$, i.e., with $\operatorname{cok}(\delta') \cong H_{\alpha-1,\beta-1}$ for $\delta' := \ell^{-1}\delta \in M_{n-1}$. The number of such δ' is given by (2.6) and (2.7), and yields the stated result for $\operatorname{vol}(X(\alpha,\beta))$.

Now to find $\operatorname{vol}(X_r(\alpha,\beta))$, where $r \ge \alpha$, we need to analyze the condition

(5) $\operatorname{cok}(\delta) \cong H_{\alpha,\beta}$, $\det(1+\delta) \equiv 1\ (\ell^r)$, $\not\equiv 1\ (\ell^{r+1})$ for $\delta \in M_n$ and $n > \max(\beta,r)$. Note that $\operatorname{cok}(\delta) \cong H_{\alpha,\beta}$ implies $\delta \equiv 0\ (\ell^\alpha)$, $\not\equiv 0\ (\ell^{\alpha+1})$. Thus, letting $\epsilon := \ell^{-\alpha}\delta \in M_{n-\alpha}$, (5) is equivalent with

(6) $\overline{\epsilon} \neq 0$, $v_\ell(\det\epsilon) = \beta-\alpha$, $\operatorname{tr}(\epsilon) + \ell^\alpha\det(\epsilon) \equiv 0\ (\ell^{r-\alpha})$, $\not\equiv 0\ (\ell^{r-\alpha+1})$.

Suppose $\boxed{\alpha=\beta}$. If $\boxed{r=\alpha}$ then (6) is equivalent with $\epsilon \in G_{n-\alpha}$, $\operatorname{tr}(\overline{\epsilon}) \neq 0$, and the volume of $X_\alpha(\alpha,\alpha)$ comes out by (2.9) along with (2.12), putting $n = \alpha+1$.

Each of the $\ell^2(\ell-1)$ elements $\delta = \delta_{\alpha+1} \in M_{\alpha+1}$ subject to

$$\operatorname{cok}(\delta) \cong H_{\alpha,\alpha},\ \operatorname{tr}(\delta) \equiv 0\ (\ell^{\alpha+1})$$

has precisely $\ell^{3(n-\alpha-1)}$ lifts δ_n to M_n $(n \ge \alpha+1)$ such that

$$\operatorname{tr}(\delta_n) + \det(\delta_n) \equiv 0\ (\ell^n),$$

by (2.13). Therefore, for $\boxed{r>\alpha}$,

$$\begin{aligned}|\{\delta \in M_{r+1} \mid \operatorname{cok}(\delta) \cong H_{\alpha,\alpha},\ \operatorname{tr}(\delta)+\det(\delta) \equiv 0\ (\ell^r),\ \not\equiv 0\ (\ell^{r+1})\}|\\ = \ell^2(\ell-1)\ell^{3(r-\alpha-1)}(\ell^4-\ell^3),\end{aligned}$$

which together with (2.9) yields the stated result for $\operatorname{vol}(X_r(\alpha,\alpha))$.

Suppose $\boxed{\alpha<\beta}$. By virtue of Lemma 2.15, we have for $r > \alpha$ and $n >$

$\max(\beta, r)$:

$$\begin{aligned}&|\{\epsilon \in M_{n-\alpha} \mid \bar{\epsilon} \neq 0,\ v_\ell(\det \epsilon) = \beta - \alpha,\ \mathrm{tr}(\epsilon) + \ell^\alpha \det(\epsilon) \equiv 0\ (\ell^{r-\alpha}),\\ &\qquad \not\equiv 0\ (\ell^{r-\alpha+1})\}|\\ &= (\ell^2 - 1)\ell^{2(n-\alpha-1)} \mid \{(t,u) \in \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n \mid (t,u) \text{ subject to (7)}\}|\end{aligned}$$

with the condition

(7) $\bar{t} = 0 = \bar{u},\ v_\ell(u) = \beta - \alpha,\ t + \ell^\alpha u \equiv 0\ (\ell^{r-\alpha}),\ \not\equiv 0\ (\ell^{r-\alpha+1})$.

For the number of these pairs (t,u), we find $(\ell-1)^2\ell^{2n-\beta-r-2}$, which yields $\mathrm{vol}(X_r(\alpha,\beta))$ for $r > \alpha$. Finally,

$$\mathrm{vol}(X_\alpha(\alpha,\beta)) = \mathrm{vol}(X(\alpha,\beta)) - \sum_{r>\alpha} \mathrm{vol}(X_r(\alpha,\beta)),$$

which allows to fill in the last missing entry in the statement of Theorem 2.3. □

(2.16) Put $X_r := \{\gamma \in G \mid v_\ell(\det(\gamma) - 1) = r\}$. We have the obvious formula

$$\mathrm{vol}_\nu(X_r) = \begin{cases} \frac{\ell-2}{\ell-1}, & r = 0 \\ \ell^{-r}, & r > 0. \end{cases}$$

Then we may interpret Theorem 2.3 as follows. Define for $0 \leq \alpha \leq \beta$, $r \geq 0$ and $(r,\ell) \neq (0,2)$:

$$g_r(\alpha,\beta) := \frac{\mathrm{vol}_\nu(X_r(\alpha,\beta))}{\mathrm{vol}_\nu(X_r)}, \tag{2.17}$$

and recall that $g(\alpha,\beta) = \mathrm{vol}_\nu(X(\alpha,\beta))$. Then

$$g(\alpha,\beta) = \text{probability of } \gamma \in G \text{ to satisfy } \mathrm{cok}(\gamma - 1) \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$$

and

$$g_r(\alpha,\beta) = \text{probability for the same event under the assumption } v_\ell(\det(\gamma) - 1) = r.$$

2.18 COROLLARY. *The conditional probability $g_r(\alpha,\beta)$ is zero if $r < \alpha$, and otherwise is given by the table below, where the two entries marked with "$*$" are undefined for $\ell = 2$.*

$g_r(\alpha,\beta)$	$r = \alpha$	$r > \alpha$
$0 = \alpha = \beta$	$\frac{\ell-2}{\ell-1}$ $*$	$\frac{\ell^2-\ell-1}{\ell^2-1}$
$0 = \alpha < \beta$	$\ell^{-\beta}$ $*$	$\frac{\ell-1}{\ell}\ell^{-\beta}$
$0 < \alpha = \beta$	$\frac{\ell^2-\ell-1}{\ell^2-1}\ell^{-3\alpha}$	$\frac{\ell}{\ell+1}\ell^{-3\alpha}$
$0 < \alpha < \beta$	$\ell^{-\beta-2\alpha}$	$\frac{\ell-1}{\ell}\ell^{-\beta-2\alpha}$

That is, we have $g_r(\alpha,\beta) = \pi_r(\alpha,\beta)\ell^{-\beta-2\alpha}$ with some factor $\pi_r(\alpha,\beta) \in \{0, \frac{\ell-2}{\ell-1}, \frac{\ell^2-\ell-1}{\ell^2-1}, \frac{\ell-1}{\ell}, \frac{\ell}{\ell+1}, 1\}$. Note that

(2.19) $\pi_r(\alpha,\alpha)$ *increases* if $r = \alpha$ is replaced with $r > \alpha$. On the other hand, if α is less than β then $\pi_r(\alpha,\beta)$ *decreases* upon enlarging r from α to $r > \alpha$. In any case, $g_r(\alpha,\beta)$ is independent of r as long as $r > \alpha$.

3. Probabilities of group structures.

We first summarize some results of E. Howe from [7], which will play a crucial role.

(3.1) Define the multiplicative arithmetic functions φ and ψ through their values on prime powers ℓ^α, $\alpha \geq 1$:

$$\varphi(\ell^\alpha) = \ell^{\alpha-1}(\ell-1), \quad \psi(\ell^\alpha) = \ell^{\alpha-1}(\ell+1),$$

i.e., φ is the Euler function. Further, given a prime number $p \geq 5$ and $m, n \in \mathbb{N}$ with $m|n$, put

$$w_p(m,n) = \frac{1}{2} \sum_{E(\mathbb{F}_p)[n] \cong \mathbb{Z}/m \times \mathbb{Z}/n} w(E/\mathbb{F}_p),$$

where E runs through the $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with the property that $E(\mathbb{F}_p)[n] \cong \mathbb{Z}/m \times \mathbb{Z}/n$. Up to the factor $\frac{1}{2}$ (introduced to be in keeping with [7]), $w_p(m,n)$ is a weighted cardinality $|\ |^*$ in the sense of (1.9). Howe defines the approximation

$$\hat{w}_p(m,n) = p\frac{\psi(n/m)}{m\varphi(n)\psi(n)} \prod_{\ell|\gcd(n,p-1)/m} (1-\ell^{-1}), \tag{3.2}$$

where ℓ runs through the prime divisors of $\gcd(n, p-1)/m$, if $m|p-1$, and $\hat{w}_p(m,n) = 0$ otherwise. Note that

$$p^{-1}w_p(1,1) = p^{-1}\hat{w}_p(1,1) = 1. \tag{3.3}$$

On p. 245 of [7], he obtains the inequality

$$|w_p(m,n) - \hat{w}_p(m,n)| \leq C(m,n)p^{1/2} \tag{3.4}$$

with the constant

$$C(m,n) = (1/12 + 5/6\sqrt{2})\psi(n/m)2^{\omega(n)}$$

independent of p. Here $\omega(n) :=$ number of different prime divisors of n. Briefly,

$$w_p(m,n) = \hat{w}_p(m,n) + O_{m,n}(p^{1/2}).$$

It is obvious that the 2-variable function $p^{-1}\hat{w}_p(m,n)$ localizes, that is

$$p^{-1}\hat{w}_p(m,n) = \prod_\ell p^{-1}\hat{w}_p(\ell^{\alpha_\ell}, \ell^{\beta_\ell}) \tag{3.5}$$

if $m = \prod_\ell \ell^{\alpha_\ell}$, $n = \prod_\ell \ell^{\beta_\ell}$, $0 \leq \alpha_\ell \leq \beta_\ell$ with pairwise different prime numbers ℓ. The factors on the right hand side are simple functions of ℓ, α_ℓ, β_ℓ and

$$r(p,\ell) := r \in \mathbb{N}_0 \text{ such that } \ell^r \| p-1,$$

i.e., the dependence on p is via $r(p,\ell)$ only. We therefore define for $0 \leq \alpha \leq \beta$:

$$h_r^{(\ell)}(\alpha,\beta) := p^{-1}\hat{w}_p(\ell^\alpha, \ell^\beta), \tag{3.6}$$

where $r = r(p,\ell)$. It vanishes for $r < \alpha$; otherwise, its values are given by the following table.

3.7 TABLE for $h_r^{(\ell)}(\alpha,\beta)$.

	$r=\alpha$	$r>\alpha$
$0=\alpha=\beta$	1	1
$0=\alpha<\beta$	$\frac{\ell}{\ell-1}\ell^{-\beta}$	$\ell^{-\beta}$
$0<\alpha=\beta$	$\frac{\ell^2}{\ell^2-1}\ell^{-3\alpha}$	$\frac{\ell}{\ell+1}\ell^{-3\alpha}$
$0<\alpha<\beta$	$\frac{\ell}{\ell-1}\ell^{-\beta-2\alpha}$	$\ell^{-\beta-2\alpha}$

Fix ℓ, α and β for the moment, and let

$$H = H_{\alpha,\beta}^{(\ell)} = \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta.$$

From the above, replacing w_p by its approximation $\hat{w}_p$, and taking (1.9) into account, we may regard

$$h_r^{(\ell)}(\alpha,\beta) \approx \frac{|\{E/\mathbb{F}_p \mid E(\mathbb{F}_p)[\ell^\beta] \cong H\}|^*}{|\{E/\mathbb{F}_p\}|^*}$$

as the probability that a randomly chosen $E/\mathbb{F}_p$ (with our *fixed* p subject to $r(p,\ell) = r$) satisfies "$E(\mathbb{F}_p)[\ell^\beta] \cong H$". The associated probability of "$E(\mathbb{F}_p)[\ell^\infty] \cong H$" is

$$(3.8)\qquad \begin{aligned} g_r^{(\ell)}(\alpha,\beta) \quad &:= \quad h_r^{(\ell)}(\alpha,\beta) - h_r^{(\ell)}(\alpha,\beta+1), \\ &\qquad r=0 \text{ or } r>0,\ \alpha<\beta \\ &= \quad h_r^{(\ell)}(\alpha,\alpha) - h_r^{(\ell)}(\alpha,\alpha+1) - h_r^{(\ell)}(\alpha+1,\alpha+1), \\ &\qquad r>0,\ \alpha=\beta \end{aligned}$$

since, e.g., the event "$E(\mathbb{F}_p)[\ell^\infty] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$" for $\alpha<\beta$ is equivalent with: "$E(\mathbb{F}_p)[\ell^\beta] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$" but not "$E(\mathbb{F}_p)[\ell^{\beta+1}] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^{\beta+1}$".

More precisely, we get from (3.4) that

$$(3.9)\qquad \frac{|\{E/\mathbb{F}_p \mid E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^*}{|\{E/\mathbb{F}_p\}|^*} = g_r^{(\ell)}(\alpha,\beta) + O_{\ell,\alpha,\beta}(p^{-1/2}),$$

where the constant implied by the O-symbol depends only on ℓ,α,β (and may easily be determined). Evaluating (3.8) by means of (3.7), which requires a number of case distinctions, we find:

(3.10) The present $g_r^{(\ell)}(\alpha,\beta)$ agrees with the conditional probability (where ℓ,α,β are fixed) $g_r(\alpha,\beta)$ defined in (2.17) and described by the table in (2.18).

So far, p has been fixed. Letting p vary subject to $r(p,\ell) = r$ with some fixed r and taking (1.10) into account yields for $p \le x \in \mathbb{R}$:

$$(3.11)\qquad \begin{aligned} &|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \le x,\ r(p,\ell) = r,\ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^* \\ &= 2g_r^{(\ell)}(\alpha,\beta)\sum p + O_{\ell,\alpha,\beta}(\sum p^{1/2}), \end{aligned}$$

where the sum in both cases ranges through

$$\{p \in \mathbb{P} \mid p \le x,\ r(p,\ell) = r\} = \{p \le x \mid \ell^r \| p-1\}.$$

(Strictly speaking, we had to assume that $p \geq 5$, but including $p = 2, 3$ doesn't change the asymptotic behavior. Thus we will neglect from now on the restriction of $p \geq 5$.)

We need a well-known fact from analytic number theory, an explicit reference of which is nonetheless difficult to find.

3.12 Proposition. *Let $\gamma > -1$ be a real number and a, m coprime natural numbers. Then*

$$\sum_{\substack{p \leq x \text{ prime} \\ p \equiv a \ (m)}} p^\gamma \sim \frac{1}{\varphi(m)} \frac{1}{1+\gamma} \frac{x^{1+\gamma}}{\log x},$$

where "$\sim$" denotes asymptotic equivalence.

Proof (sketch). Note that the assertion includes the prime number theorem ($\gamma = 0$, $m = 1$) and Dirichlet's theorem on primes in arithmetic progressions ($\gamma = 0$). The general case ($\gamma > -1$ arbitrary) results from the case $\gamma = 0$ by Abel summation (see the instructions and notation given in [9] pp. 3,4) of the series $\sum_{n \leq x} a_n b(n)$ with

$$a_n = \begin{cases} 1, & n \equiv a(m), \ n \text{ prime} \\ 0, & \text{otherwise}, \end{cases}$$

and the C^1-function b with $b(x) = x^\gamma$. □

In particular,

$$\sum_{\substack{p \leq x \\ r(p,\ell) = r}} p^{1/2} \sim \frac{2}{3}\left(\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})}\right)\frac{x^{3/2}}{\log x},$$

so the expression in (3.11) becomes

$$2g_r^{(\ell)}(\alpha, \beta) \sum p + \left(\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})}\right) O_{\ell,\alpha,\beta}\left(\frac{x^{3/2}}{\log x}\right).$$

Applying (3.12) also to the first sum $\sum p$ in (3.11) yields

(3.13)
$$\begin{aligned} &\frac{|\{E/\mathbb{F}_p \mid p \leq x, \ r(p,\ell) = r, \ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x, \ r(p,\ell) = r\}|^*} \\ &= g_r^{(\ell)}(\alpha, \beta) + O_{\ell,\alpha,\beta}(x^{-1/2}), \end{aligned}$$

where the implied constant depends only on ℓ, α, β but not on r. Apart from the condition "$r(p, \ell) = r$", this expresses $g_r^{(\ell)}(\alpha, \beta)$ as a probability in the sense of (1.4). It remains to evaluate

$$P\{\mathcal{F}, \text{“}E(\mathbb{F}_p)[\ell^\infty] \cong H\text{”}\} = \lim_{x \to \infty} \frac{|\{E/\mathbb{F}_p \mid p \leq x, \ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*}.$$

It is tempting to calculate it via the conditional probabilities $g_r^{(\ell)}(\alpha, \beta)$ simply as

$$\sum_{r \geq 0}\left(\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})}\right) g_r^{(\ell)}(\alpha, \beta),$$

where $\frac{1}{\varphi(\ell^r)} - \frac{1}{\varphi(\ell^{r+1})} = \mathrm{vol}_\nu(X_r)$ (see (2.16)) is the probability of p to satisfy $r(p,\ell) = r$. This will turn out to be true, but requires reversing the order in which we evaluate a double limit, and needs to be justified.

We have

$$|\{E/\mathbb{F}_p \mid p \le x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^* \\ = \sum_{r\ge 0}[2g_r^{(\ell)}(\alpha,\beta)\sum_{\substack{p\le x\\ r(p,\ell)=r}} p + (\tfrac{1}{\varphi(\ell^{r+1})} - \tfrac{1}{\varphi(\ell^{r+1})})O_{\ell,\alpha,\beta}(\tfrac{x^{3/2}}{\log x})].$$

Now $g_r^{(\ell)}(\alpha,\beta) = 0$ if $r < \alpha$ and $g_r^{(\ell)}(\alpha,\beta) = g_{\alpha+1}^{(\ell)}(\alpha,\beta)$ for $r > \alpha$. Therefore, the above is

$$2g_\alpha^{(\ell)}(\alpha,\beta)\sum_{\substack{p\le x\\ r(p,\ell)=\alpha}} p + 2g_{\alpha+1}^{(\ell)}(\alpha,\beta)\sum_{\substack{p\le x\\ r(p,\ell)>\alpha}} p + O_{\ell,\alpha,\beta}(x^{3/2}/\log x).$$

From (3.12) and (2.17) we find that

$$\begin{aligned} 2g_\alpha^{(\ell)}(\alpha,\beta)\sum_{\substack{p\le x\\ r(p,\ell)=\alpha}} p &\sim \mathrm{vol}_\nu(X_\alpha(\alpha,\beta))x^2/\log x,\\ 2g_{\alpha+1}^{(\ell)}(\alpha,\beta)\sum_{\substack{p\le x\\ r(p,\ell)>\alpha}} p &\sim \tfrac{\ell}{\ell-1}\mathrm{vol}_\nu(X_{\alpha+1}(\alpha,\beta))x^2/\log x. \end{aligned}$$

Comparing with (2.3) yields in all the four cases

$$\mathrm{vol}_\nu(X_\alpha(\alpha,\beta)) + \tfrac{\ell}{\ell-1}\mathrm{vol}_\nu(X_{\alpha+1}(\alpha,\beta)) = g^{(\ell)}(\alpha,\beta).$$

Thus, dividing by $|\{E/\mathbb{F}_p \mid p \le x\}|^* = 2\sum_{p\le x} p \sim x^2/\log x$, we finally get

$$(3.14) \qquad \frac{|\{E/\mathbb{F}_p \mid p \le x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H\}|^*}{|\{E/\mathbb{F}_p \mid p \le x\}|^*} = g^{(\ell)}(\alpha,\beta) + O_{\ell,\alpha,\beta}(x^{-\frac{1}{2}}).$$

Hence, in fact

$$P(\mathcal{F}, \text{“}E(\mathbb{F}_p)[\ell^\infty] \cong H\text{”}) = g^{(\ell)}(\alpha,\beta) = \mathrm{vol}_\nu(X(\alpha,\beta)),$$

where $X(\alpha,\beta) = X^{(\ell)}(\alpha,\beta)$ is the ℓ-adic set defined in (2.2).

We may summarize our results (3.13) and (3.14) as follows.

3.15 Theorem. *Let a prime number ℓ and $0 \le \alpha \le \beta$ be given.*

- (i) *The probability $P(\mathcal{F}$, “$E(\mathbb{F}_p)[\ell^\infty] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$”) in the sense of* (1.4) *exists and equals the value $g^{(\ell)}(\alpha,\beta)$ given in* (2.3).
- (ii) *Fix moreover a non-negative integer r. The conditional probability $P(\mathcal{F}$, “$E(\mathbb{F}_p)[\ell^\infty] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$” | “$\ell^r \| p-1$”) for “$E(\mathbb{F}_p)[\ell^\infty] \cong \mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$” under the assumption “$\ell^r \| p-1$” exists and equals the value of $g_r^{(\ell)}(\alpha,\beta)$ given in* (2.18).

In both cases the error terms are $O_{\ell,\alpha,\beta}(x^{-1/2})$.

Note that the probabilities thus found are those predicted by the hypothesis (H) formulated in the introduction.

3.16 Example. We consider the probability that the 2-part of $E(\mathbb{F}_p)$ is isomorphic with $H = \mathbb{Z}/4 \times \mathbb{Z}/4$ under congruence conditions for p. According to (3.15), it is

$$1/3 \cdot 2^{-6} \quad \text{for } p \equiv 5\ (8)$$

and *increases* to

$$2/3 \cdot 2^{-6} \quad \text{for } p \equiv 1\ (8).$$

If we replace H by $H' = \mathbb{Z}/4 \times \mathbb{Z}/8$, the probability is

$$2^{-7} \quad \text{for } p \equiv 5\ (8)$$

and *decreases* to

$$2^{-8} \quad \text{for } p \equiv 1\ (8).$$

4. The probability spaces.

Theorem 3.15 has the drawback that it relies on the ad hoc notion (1.4) of probability and does not involve probability spaces in the ordinary sense. Here we will remedy this defect and put (3.15) in the framework of "ordinary" probability theory.

(4.1) For what follows, we fix a prime ℓ and put $\mathfrak{X}^{(\ell)}$ for the set of all pairs (H, r), where H is a group of shape $\mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$ with $0 \le \alpha \le \beta$ and $\alpha \le r \in \mathbb{N}_0$. Hence elements of $\mathfrak{X}^{(\ell)}$ correspond bijectively to triples $(\alpha, \beta, r) \in \mathbb{N}_0^3$ with $\alpha \le \min(\beta, r)$, which we often use as an identification. By (2.3), the function

$$P^{(\ell)} : (\alpha, \beta, r) \longmapsto \mathrm{vol}_\nu(X_r^{(\ell)}(\alpha, \beta))$$

turns $\mathfrak{X}^{(\ell)}$ into a discrete probability space (d.p.s.). (By a d.p.s. we understand a countable set provided with a probability measure in which each non-empty subset is measurable with positive volume.)

Given $(H_{\alpha,\beta}^{(\ell)}, r) = (\alpha, \beta, r) \in \mathfrak{X}^{(\ell)}$, we define

$$A_{\alpha,\beta,r} := \{E/\mathbb{F}_p \in \mathcal{F} \mid E(\mathbb{F}_p)[\ell^\infty] \cong H_{\alpha,\beta}^{(\ell)},\ r(p, \ell) = r\}.$$

We further let $\mathfrak{A}^{(\ell)}$ be the σ-algebra of subsets of $\mathcal{F}$ generated by all the sets $A_{\alpha,\beta,r}$. Hence the elements of $\mathfrak{A}^{(\ell)}$ are the subsets $A_\mathfrak{Y}$ of $\mathcal{F}$, where $\mathfrak{Y}$ is an arbitrary (finite or countably infinite) subset of $\mathfrak{X}^{(\ell)}$ and

$$A_\mathfrak{Y} = \bigcup_{(\alpha,\beta,r)\in\mathfrak{Y}} A_{\alpha,\beta,r} \quad \text{(disjoint union)}.$$

4.2 Proposition. *For each subset $\mathfrak{Y}$ of $\mathfrak{X}^{(\ell)}$, the limit $P(\mathcal{F}, A_\mathfrak{Y})$ as in* (1.4) *exists, and is given as $\sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r})$.*

Here $P(\mathcal{F}, A_{\alpha,\beta,r}) = P(\mathcal{F},$ *"*$E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta},\ r(p,\ell)=r$*"*$) = \mathrm{vol}_\nu(X_r^{(\ell)}(\alpha,\beta))$ *by* (3.15).

Proof. We must check the identity

$$(?)\qquad \lim_{x\to\infty} \frac{|\{E/\mathbb{F}_p\in\mathcal{F}\ |\ p\le x,\ (E(\mathbb{F}_p)[\ell^\infty],\ r(p,\ell))\in\mathfrak{Y}\}|^*}{|\{E/\mathbb{F}_p\in\mathcal{F}\ |\ p\le x\}|^*} = \sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r}),$$

which is obvious from (3.15) if $\mathfrak{Y}$ is finite. Let $f_{\mathfrak{Y}}(x)$ be the argument of the limit in the left hand side of (?). Then for each finite subset $\mathfrak{Y}_0$ of $\mathfrak{Y}$,

$$\liminf_{x\to\infty} f_{\mathfrak{Y}}(x) \ge \sum_{(\alpha,\beta,r)\in\mathfrak{Y}_0} P(\mathcal{F}, A_{\alpha,\beta,r}),$$

thus

$$\liminf_{x\to\infty} f_{\mathfrak{Y}}(x) \ge \sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r}).$$

If $\mathfrak{Y}^c$ denotes the complement $\mathfrak{X}^{(\ell)} - \mathfrak{Y}$ of $\mathfrak{Y}$, we have $A_{\mathfrak{Y}^c} = \mathcal{F} - A_{\mathfrak{Y}}$ and $f_{\mathfrak{Y}^c}(x) = 1 - f_{\mathfrak{Y}}(x)$. Thus reversing the parts of $\mathfrak{Y}$ and $\mathfrak{Y}^c$ yields

$$\limsup_{x\to\infty} f_{\mathfrak{Y}}(x) \le \sum_{(\alpha,\beta,r)\in\mathfrak{Y}} P(\mathcal{F}, A_{\alpha,\beta,r}).$$

□

As a consequence of (4.2), the function $P(\mathcal{F},\cdot)$ is countably additive on $\mathfrak{A}^{(\ell)}$ and therefore a probability measure. The following is then obvious.

4.3 Corollary. *The σ-algebra $\mathfrak{A}^{(\ell)}$ provided with its probability measure $P(\mathcal{F},\cdot)$ is canonically isomorphic with the discrete probability space* $(\mathfrak{X}^{(\ell)}, P^{(\ell)})$.

It is easy to generalize the preceding to cover the case of events that involve a finite number of primes ℓ. Thus let $L \subset \mathbb{P}$ be a finite set of primes. The cartesian product

$$\mathfrak{X}^{(L)} = \prod_{\ell\in L} \mathfrak{X}^{(\ell)}$$

provided with the product measure $P^{(L)}$ is itself a d.p.s. On the other hand, given $\mathbf{x} = (\alpha_\ell, \beta_\ell, r_\ell)_{\ell\in L} \in \mathfrak{X}^{(L)}$, we define

$$A_{\mathbf{x}} := \{E/\mathbb{F}_p \in \mathcal{F} \mid \forall \ell\in L : E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha_\ell,\beta_\ell},\ r(p,\ell) = r_\ell\}$$

and let $\mathfrak{A}^{(L)}$ be the σ-algebra in $\mathcal{F}$ generated by all the $A_{\mathbf{x}}$, $\mathbf{x}\in\mathfrak{X}^{(L)}$. Then $\mathfrak{A}^{(L)} = \{A_{\mathfrak{Y}} \mid \mathfrak{Y}\subset\mathfrak{X}^{(L)}\}$ with the obvious definition $A_{\mathfrak{Y}} := \bigcup_{\mathbf{x}\in\mathfrak{Y}} A_{\mathbf{x}}$.

4.4 Proposition.

(i) *For* $\mathbf{x} = (\alpha_\ell, \beta_\ell, r_\ell)_{\ell\in L} \in \mathfrak{X}^{(L)}$,

$$P(\mathcal{F}, A_{\mathbf{x}}) = \prod_{\ell\in L} P(\mathcal{F}, A_{\alpha_\ell,\beta_\ell,r_\ell})$$

holds.

(ii) *For each subset* $\mathfrak{Y}$ *of* $\mathfrak{X}^{(L)}$*, the limit* $P(\mathcal{F}, A_{\mathfrak{Y}})$ *exists, and is given as* $\sum_{\mathbf{x}\in\mathfrak{Y}} P(\mathcal{F}, A_{\mathbf{x}})$.

Proof. (i) is a formal consequence of (3.4), (3.5) and (3.15). We omit the details. The proof of (ii) is then identical to that of (4.2). □

As in the case of one single prime, (4.4)(ii) implies that $P(\mathcal{F}, \cdot)$ is a probability measure on $\mathcal{A}^{(L)}$. In view of (4.4)(i) we get:

4.5 Corollary. *The* σ*-algebra* $\mathfrak{A}^{(L)}$ *provided with its probability measure* $P(\mathcal{F}, \cdot)$ *is canonically isomorphic with the d.p.s.* $(\mathfrak{X}^{(L)}, P^{(L)})$*. In particular, the restrictions of* $P(\mathcal{F}, \cdot)$ *to the various* $\mathfrak{A}^{(\ell)}$ $(\ell \in L)$ *are stochastically independent on* $\mathfrak{A}^{(L)}$.

4.6 Remark. For a number of reasons, no simple generalizations of (4.4) and (4.5) to infinite subsets $L \subset \mathbb{P}$ are in sight. For example, the union $\bigcup_{L_0 \in L \text{ finite}} \mathfrak{A}^{(L_0)}$ is not a σ-algebra, $\prod_{\ell\in L} \mathfrak{X}^{(\ell)}$ is uncountable, and problems on the convergence of infinite products and their commutation with limits arise. Therefore, events in $\mathcal{F}$ that involve an infinite number of primes ℓ are a priori not covered by the above, and are more difficult to study. In (5.9), we investigate a significant instance of such an event, namely the property of cyclicity of $E(\mathbb{F}_p)$.

5. Some applications.

We use the preceding results to derive probabilities/expectations associated with some elementary properties of $E/\mathbb{F}_p \in \mathcal{F}$.

We start with divisibility by a fixed $n \in \mathbb{N}$.

5.1 Proposition. *Let a prime power* ℓ^a *and* $r \in \mathbb{N}_0$ *be given.*

(i) *The probability that* ℓ^a *divides* $|E(\mathbb{F}_p)|$ *equals*

$$P(\mathcal{F}, \text{“}\ell^a \mid |E(\mathbb{F}_p)|\text{”}) = \ell^{-a}\frac{\ell^3 - \ell - \ell^{2-a}}{(\ell^2-1)(\ell-1)}.$$

(ii) *The conditional probability for the same event under the assumption* $\ell^r \| p-1$ *equals*

$$P(\mathcal{F}, \text{“}\ell^a \mid |E(\mathbb{F}_p)|\text{”} \mid \text{“}\ell^r\|p-1\text{”}) = \begin{cases} \ell^{-a}\frac{\ell}{\ell-1}, & r < a/2 \\ \ell^{-a}\frac{\ell^2+\ell-\ell^{1-(a-1)/2}}{\ell^2-1}, & r > a/2,\ a \text{ odd} \\ \ell^{-a}\frac{\ell^2+\ell-\ell^{1-a/2}}{\ell^2-1}, & r \geq a/2,\ a \text{ even.} \end{cases}$$

Proof. By virtue of (4.2), $P(\mathcal{F}, \text{“}\ell^a \mid |E(\mathbb{F}_p)|\text{”})$ exists and is given by $\sum g^{(\ell)}(\alpha,\beta)$, where $0 \leq \alpha \leq \beta$ and $\alpha+\beta \geq a$. The conditional probability in (ii) is given by the same expression, but $g^{(\ell)}(\alpha,\beta)$ replaced by $g_r^{(\ell)}(\alpha,\beta)$.

The stated formulae result from a lengthy but elementary calculation using (2.3) and (2.18), which will be omitted. □

5.2 COROLLARY. *For arbitrary $n \in \mathbb{N}$ with factorization $n = \prod \ell^{a_\ell}$ into primes ℓ, $P(\mathcal{F}, $ "$n \mid |E(\mathbb{F}_p)|$"$)$ is given by*

$$n^{-1} \prod_{\ell \mid n} \frac{\ell^3 - \ell - \ell^{2-a_\ell}}{(\ell^2-1)(\ell-1)}.$$

Note that all the probabilities figuring in (5.1) and (5.2) are slightly larger than n^{-1}, the value naively expected. The probability of "$n \mid |E(\mathbb{F}_q)|$" over a *fixed* field $\mathbb{F}_q$ (i.e., the share of those $E/\mathbb{F}_q$ with the divisibility property) has been determined by Howe in [7].

(5.3) For any function $f : \mathcal{F} \longrightarrow \mathbb{R}$, we define the expectation $E(\mathcal{F}, f)$ (provided the limit exists) as

$$E(\mathcal{F}, f) = \lim_{x \to \infty} \frac{\sum f(E/\mathbb{F}_p) w(E/\mathbb{F}_p)}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*},$$

where the sum in the numerator is over all objects $E/\mathbb{F}_p \in \mathcal{F}$ with $p \leq x$. Restricting the domain $\mathcal{F}$ (for example by requiring congruence conditions on p), we may also define the expectation of f on subsets $\mathcal{F}'$ of $\mathcal{F}$. Given a prime number ℓ, we call f

- OF TYPE ℓ, if $f(E/\mathbb{F}_p)$ depends only on $E(\mathbb{F}_p)[\ell^\infty]$;
- WEAKLY OF TYPE ℓ, if $f(E/\mathbb{F}_p)$ depends only on $E(\mathbb{F}_p)[\ell^\infty]$ and $r(p, \ell)$.

If these conditions hold, we regard f as a function on the set of groups of shape $H^{(\ell)}_{\alpha,\beta}$ (or on the set $\mathfrak{X}^{(\ell)}$, respectively), see (4.1). More concretely, ℓ being fixed, f is a function on pairs (α, β) with $0 \leq \alpha \leq \beta$ if it is of type ℓ, and is a function on triples (α, β, r) with $0 \leq \alpha \leq \min(\beta, r)$ if it is weakly of type ℓ.

5.4 LEMMA.

(i) *Suppose that f is bounded and of type ℓ. Then $E(\mathcal{F}, f)$ is defined and agrees with the sum*

$$\sum_{\substack{\alpha,\beta \in \mathbb{N}_0 \\ \alpha \leq \beta}} f(\alpha, \beta) g^{(\ell)}(\alpha, \beta).$$

(ii) *Suppose that f is bounded and weakly of type ℓ, and let $r \in \mathbb{N}_0$ be given. Then the expectation $E(\mathcal{F}, f,$ "$\ell^r \| p-1$"$)$ of f on $\{E/\mathbb{F}_p \mid \ell^r \| p-1\}$ is defined and agrees with*

$$\sum_{\substack{\alpha,\beta \in \mathbb{N}_0 \\ \alpha \leq \min(\beta, r)}} f(\alpha, \beta, r) g_r^{(\ell)}(\alpha, \beta).$$

Proof. We restrict to showing (i); the proof of (ii) is similar. Let E be the value of the absolutely convergent sum

$$\sum_{0 \leq \alpha \leq \beta} f(\alpha, \beta) g^{(\ell)}(\alpha, \beta),$$

and let $\epsilon > 0$ be given. In view of the absolute convergence, there exists a finite subset $\mathfrak{Y} \subset \{(\alpha, \beta) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid \alpha \leq \beta\}$ such that

$$\sum_{(\alpha,\beta)\notin\mathfrak{Y}} |f(\alpha,\beta)| g^{(\ell)}(\alpha,\beta) < \frac{\epsilon}{3}.$$

Let $n = |\mathfrak{Y}|$ and let x_0 be chosen sufficiently large such that for each $(\alpha, \beta) \in \mathfrak{Y}$ and each $x \geq x_0$, we have

$$|f(\alpha,\beta)| \mid g^{(\ell)}(\alpha,\beta) - \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\}|^*}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*}| \leq \epsilon/3n.$$

Then for $x \geq x_0$,

$$|\sum_{(\alpha,\beta)\in\mathfrak{Y}} f(\alpha,\beta) \frac{|\{E/\mathbb{F}_p \mid p \leq x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*} - E| < 2\epsilon/3$$

holds. According to (4.2), and since $f(\alpha, \beta)$ is bounded, we find x_1 such that for $x \geq x_1$, we have

$$\sum_{(\alpha,\beta)\notin\mathfrak{Y}} |f(\alpha,\beta)| \frac{|\{E/\mathbb{F}_p \mid p \leq x,\ E(\mathbb{F}_p)[\ell^\infty] \cong H^{(\ell)}_{\alpha,\beta}\}|^*}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*} < \epsilon/3.$$

Thus for $x \geq \max(x_0, x_1)$,

$$\frac{\sum_{p\leq x} f(E/\mathbb{F}_p) w(E/\mathbb{F}_p)}{|\{E/\mathbb{F}_p \mid p \leq x\}|^*}$$

differs by less than ϵ from E. □

We apply (5.4) to the function $\kappa_n : \mathcal{F} \longrightarrow \mathbb{R}$ defined by

(5.5) $\kappa_n(E/\mathbb{F}_p)$ = number of points of precise order n in $E(\mathbb{F}_p)$ for $n \in \mathbb{N}$.

5.6 Proposition. *Let a prime power $n = \ell^a$ and a non-negative integer r be given. The expectation $E(\mathcal{F}, \kappa_n, \text{“}\ell^r \| p-1\text{”})$ for κ_n on $\{E/\mathbb{F}_p \mid \ell^r \| p-1\}$ exists and equals* 1 *independently of r. Thus the total expectation $E(\mathcal{F}, \kappa_n)$ exists on $\mathcal{F}$ and equals* 1.

Proof. κ_n is bounded by $n^2 = \ell^{2a}$ and of type ℓ, thus by (5.4),

$$E(\mathcal{F}, \kappa_n, \text{“}\ell^r \| p-1\text{”}) = \sum_{\substack{\alpha,\beta\in\mathbb{N}_0 \\ \alpha\leq\min(\beta,r)}} \kappa_n(\alpha,\beta) g_r^{(\ell)}(\alpha,\beta).$$

Now $\kappa_n(\alpha, \beta)$ = number of elements of precise order ℓ^a in $\mathbb{Z}/\ell^\alpha \times \mathbb{Z}/\ell^\beta$ is easily determined; we refrain from writing down the result. Evaluating after that the right hand side above is an elementary but - due to the numerous cases - laborious exercise in summing multiple geometric series. In each of the cases, the result turns out to 1. □

5.7 Corollary. *For each natural number n, the expectation $E(\mathcal{F}, \kappa_n)$ exists and equals* 1.

Proof. Since only the finitely many prime divisors ℓ of n are involved and κ_n is multiplicative in n, (4.4) allows to reduce the general case to (5.6). We omit the details. □

5.8 REMARK. The just established results on $E(\mathcal{F}, \kappa)$ are "formal facts" that can be seen by "pure thought", and avoiding the extended calculations with the values of $g_r^{(\ell)}(\alpha, \beta)$. Namely, taking into account that $\kappa_n(E/\mathbb{F}_p)$ equals the number of fixed points of Frobenius on the points of precise order n of $E(\overline{\mathbb{F}}_p)$, (5.7) is almost immediate from (H) and Burnside's lemma. I owe that hint to Bas Edixhoven [4].

We conclude with determining the asymptotic probability of the property "$E(\mathbb{F}_p)$ is a cyclic group". Since it cannot be studied entirely in the framework of the probability spaces $\mathfrak{A}^{(L)}$ or $\mathfrak{X}^{(L)}$ of section 4 with finite sets of primes, some more preparations are needed. We will finally prove the following.

5.9 THEOREM. *The probability $P(\mathcal{F}$, "$E(\mathbb{F}_p)$ is cyclic") exists and is given by*

$$\prod_{\ell \text{ prime}} \left(1 - \tfrac{1}{(\ell^2-1)\ell(\ell-1)}\right) \approx 0.81377.$$

5.10 REMARK. Vladut in [10] described the share of the cyclic ones among all the $E/\mathbb{F}_q$ over the fixed finite field $\mathbb{F}_q$. It depends strongly on the prime decomposition of $q-1$. In contrast, (5.9) is an average over all primes $p = q$, which balances local fluctuations.

We first determine the probability of local cyclicity.

5.11 LEMMA. *Fix a prime number ℓ and $r \geq 0$.*

(i) *The probability $P(\mathcal{F}$, "$E(\mathbb{F}_p)[L^\infty]$ is cyclic")* equals

$$\tau_\ell := 1 - \tfrac{1}{(\ell^2-1)\ell(\ell-1)}.$$

(ii) *The conditional probability under the assumption $r(p, \ell) = r$ for $E(\mathbb{F}_p)[\ell^\infty]$ to be cyclic equals* 1 *if $r = 0$ and*

$$\sigma_\ell := 1 - \tfrac{1}{(\ell^2-1)\ell}$$

if $r > 0$.

Proof. By (4.2), the first value is given by $\sum_{\beta \geq 0} g^{(\ell)}(\alpha, \beta)$, the second one by $\sum_{\beta \geq 0} g_r^{(\ell)}(0, \beta)$. □

For any $\lambda \in \mathbb{R}$, we call $E(\mathbb{F}_p)$ λ-cyclic if its ℓ-parts are cyclic for each prime $\ell \leq \lambda$. From the lemma and (4.4) we get:

5.12 COROLLARY. $P(\mathcal{F}$, *"$E(\mathbb{F}_p)$ is λ-cyclic"*) $= \prod_{\ell \leq \lambda} \tau_\ell$.

Hence (5.9) is established as soon as we have ensured that the limit for $\lambda \longrightarrow \infty$ commutes with the limit underlying the definition (1.4) of $P(\mathcal{F}, \cdot)$.

Since cyclicity implies λ-cyclicity, at least

$$\limsup_{x\to\infty} \frac{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x,\ E(\mathbb{F}_p) \text{ cyclic}\}|^*}{|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x\}|^*} \leq \prod_{\ell \text{ prime}} \tau_\ell$$

holds. Thus we must find lower estimates for the left hand side. Put for each prime p

$$c(p) := \prod_{\ell | p-1} \sigma_\ell. \tag{5.13}$$

Then it is an easy consequence of (3.4) and the inclusion/exclusion principle (see Theorem 6.1 of [10]) that for each $\epsilon > 0$ and each fixed prime p, we have

$$|\{E/\mathbb{F}_p \mid E(\mathbb{F}_p) \text{ cyclic}\}|^* = 2pc(p) + O_\epsilon(p^{1/2+\epsilon}).$$

Hence

$$|\{E/\mathbb{F}_p \in \mathcal{F} \mid p \leq x, E(\mathbb{F}_p) \text{ cyclic}\}|^* = 2\sum_{p\leq x} pc(p) + O_\epsilon(\sum_{p \leq x} p^{1/2+\epsilon}). \tag{5.14}$$

5.15 LEMMA. *Suppose that the average*

$$C := \lim_{x\to\infty} \pi(x)^{-1} \sum_{p \leq x} c(p)$$

exists, where $\pi(x) \sim x/\log x$ *is the prime number function. Then*

$$2\sum_{p\leq x} pc(p) \sim Cx^2/\log x$$

and therefore $P(\mathcal{F}$, *"*$E(\mathbb{F}_p)$ *is cyclic"*$) = C$.

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be the series defined by $a_n = c(p)$ if $n = p \in \mathbb{P}$ and $a_n = 0$ otherwise, and $A(x) = \sum_{n\leq x} a_n = \sum_{p\leq x} c(p)$. Abel summation with $b(x) = x$ yields

$$\sum_{p\leq x} pc(p) = xA(x) - \int_1^x A(s)ds \sim 1/2\ Cx^2/\log x,$$

since by assumption, $A(x) \sim Cx/\log x$ and any primitive F of $x/\log x$ satisfies $F \sim 1/2\ x^2/\log x$. The last assertion follows from (5.14) and

$$\sum_{p\leq x} p^{1/2+\epsilon} \sim \frac{1}{3/2+\epsilon} x^{3/2+\epsilon}/\log x.$$

□

We are left to verifying the hypothesis of (5.15), which no longer involves elliptic curves. Put

$$\begin{aligned} c_\lambda(p) &= \textstyle\prod_{\ell|p-1,\ \ell\leq\lambda} \sigma_\ell \\ C_\lambda(x) &= \pi(x)^{-1} \textstyle\sum_{p\leq x} c_\lambda(p) \\ C(x) &= \pi(x)^{-1} \textstyle\sum_{p\leq x} c(p), \end{aligned} \tag{5.16}$$

the quantity whose limit we need to find. Now, since $c_\lambda(p)$ depends only on the class of p modulo $n := \prod_{\ell\le\lambda}\ell$, Dirichlet's theorem implies that for λ fixed,

$$(5.17)\qquad \begin{aligned} C_\lambda &:= \lim_{x\to\infty} C_\lambda(x) = \text{average of } c_\lambda \text{ over } (\mathbb{Z}/n)^* \\ &= \prod_{\ell\le\lambda} (\text{average of } \tilde\sigma_\ell \text{ over } (\mathbb{Z}/\ell)^*) = \prod_{\ell\le\lambda}\tau_\ell. \end{aligned}$$

Here $\tilde\sigma_\ell(x) = \sigma_\ell$, ($\tilde\sigma_\ell(x) = 1$) if $x \equiv 1$, ($x \not\equiv 1$) modulo ℓ, respectively (see Lemma 5.11(ii)).

In view of $c(p) \le c_\lambda(p)$, we have for each λ

$$\limsup_{x\to\infty} C(x) \le C_\lambda,$$

hence

$$\limsup C(x) \le \prod_{\ell \text{ prime}} \tau_\ell.$$

5.18 Claim. We have in fact

$$C := \lim_{x\to\infty} C(x) = \prod_{\ell \text{ prime}} \tau_\ell.$$

Proof of claim. Let $\lambda_0 \in \mathbb{R}$ and $\epsilon > 0$ be given. Choose x_0 large enough such that for $x \ge x_0$

$$|C_{\lambda_0}(x) - C_{\lambda_0}| < \epsilon$$

holds. For such x and $\lambda \ge \lambda_0$, we have

$$C_\lambda(x) \ge (\prod_{\lambda_0<\ell\le\lambda}\sigma_\ell)C_{\lambda_0}(x) > (\prod_{\lambda_0<\ell\le\lambda}\sigma_\ell)(C_{\lambda_0}-\epsilon).$$

Letting $\lambda \longrightarrow \infty$, we find

$$C(x) \ge (\prod_{\ell>\lambda_0}\sigma_\ell)(C_{\lambda_0}-\epsilon)$$

for each $x \ge x_0$, and therefore

$$\liminf_{x\to\infty} C(x) \ge (\prod_{\ell>\lambda_0}\sigma_\ell)C_{\lambda_0} = \prod_{\ell\le\lambda_0}\tau_\ell\prod_{\ell>\lambda_0}\sigma_\ell.$$

Since this holds for any λ_0, and $\sigma_\ell \le \tau_\ell$ for each ℓ, we finally get

$$\liminf_{x\to\infty} C(x) \ge \prod_{\ell \text{ prime}} \tau_\ell,$$

i.e., the claim. Together with (5.15), this also concludes the proof of Theorem 5.9. □

References

[1] J.D. Achter: The distribution of class groups of function fields. J. Pure and Appl. Algebra 204 (2006), 316–333.
[2] B.J. Birch: How the number of points of an elliptic curve over a fixed prime field varies. J. London Math. Soc. 43 (1968), 57–60.
[3] H. Cohen–H.W. Lenstra, Jr.: Heuristics on class groups of number fields. In: Lecture Notes in Mathematics 1068, 33–62, Springer–Verlag 1984.
[4] B. Edixhoven: personal communication.
[5] E. Friedman–L.C. Washington: On the distribution of divisor class groups of curves over a finite field. In: Théorie des Nombres/Number Theory Laval 1987 (J.-M. De Koninck–C. Levesque eds.), De Gruyter 1989.
[6] E.-U. Gekeler: Frobenius distributions of elliptic curves over finite prime fields. Int. Math. Res. Notices 37 (2003), 1999–2018.
[7] E.W. Howe: On the group orders of elliptic curves over finite fields. Comp. Math. 85 (1993), 229–247.
[8] J-P. Serre: Zeta and L functions. Arithmetical Algebraic Geometry, 82–92, Harper and Row 1965.
[9] G. Tenenbaum: Introduction à la théorie analytique et probabiliste des nombres. Soc. Math. France 1995.
[10] S.G. Vladut: Cyclicity statistics for elliptic curves over finite fields. Finite Fields Appl. 5 (1999), 13–25.

Ernst-Ulrich Gekeler
FR 6.1 Mathematik
Universität des Saarlandes
D-66041 Saarbrücken
Germany
gekeler@math.uni-sb.de

Galois coverings, Morita Equivalence and Smash Extensions of Categories over a Field[1]

Claude Cibils and Andrea Solotar

Received: September 29, 2005

Communicated by Max Karoubi

Abstract. Algebras over a field k generalize to categories over k in order to considers Galois coverings. Two theories presenting analogies, namely smash extensions and Galois coverings with respect to a finite group are known to be different. However we prove in this paper that they are Morita equivalent. For this purpose we need to describe explicit processes providing Morita equivalences of categories which we call contraction and expansion. A structure theorem is obtained: composition of these processes provides any Morita equivalence up to equivalence, a result which is related with the karoubianisation (or idempotent completion) and additivisation of a k-category.

2000 Mathematics Subject Classification: 16W50, 18E05, 16W30, 16S40, 16D90.
Keywords and Phrases: Hopf algebra, Galois covering, k-category, Morita theory, smash product, completion, karoubianisation.

1 Introduction

Let k be a field. The observation that a k-algebra A is a category with one object and endomorphisms given by A leads to Galois coverings given by categories with more than one object, see for instance [3]. In this context the universal cover of the polynomial algebra in one variable is the free category

[1]This work has been supported by the projects Conicet-Cnrs:"Metodos Homologicos en Representaciones y Algebra de Hopf", Pics 1514, Pict 08280 (Anpcyt), Ubacytx169 and Pip-Conicet 02265. The second author is a research member of Conicet (Argentina) and a Regular Associate of ICTP Associate Scheme.

over k generated by the infinite quiver with integer vertices and one arrow from i to $i+1$ for each integer i.

A category $\mathcal{C}$ over a field k has a set of objects $\mathcal{C}_0$ and each morphism set ${}_y\mathcal{C}_x$ from an object x to an object y is a k-vector space, the composition of maps of $\mathcal{C}$ is k-bilinear. In particular each endomorphism set ${}_x\mathcal{C}_x$ is an associative k-algebra. Such categories are called k-categories, they have been considered extensively and are considered as algebras with several objects, see [13, 14].

This work has a two-fold main purpose.

In one direction we show that there is a coincidence up to Morita equivalence between Galois coverings of k-categories and smash extensions for a finite group. More precisely we associate to each Galois covering of a k-category with finite group G a smash extension with the same group, having the property that the categories involved are Morita equivalent to the starting ones. In particular from a full and dense functor we obtain a faithful one. Conversely, a smash extension of categories gives rise to a Galois covering, with categories actually equivalent to the original ones. Consequently both procedures are mutual inverses up to Morita equivalence.

This Theorem explains the analogous spectral sequence arising in cohomology for both theories, see [5] and the generalisation [16], and [12].

We emphasize that similar results for an arbitrary group G can be obtained considering coalgebras and comodule categories. This approach will be detailed in a subsequent paper.

In the other direction, motivated by the above problem, we study the Morita equivalence of k-categories, obtaining a complete description of these equivalences. In other words, a Morita theorem for linear categories.

We consider modules over a k-category $\mathcal{C}$, that is k-functors from $\mathcal{C}$ to the category of k-vector spaces *i.e.* collections of vector spaces attached to the objects with "actions" of morphisms transforming vectors at the source of the morphism to vectors at the target. Notice that if $\mathcal{C}$ is a finite object set k-category it is well known and easy to prove that modules over $\mathcal{C}$ coincide with usual modules over the "matrix algebra" $a(\mathcal{C}) = \oplus_{x,y\in\mathcal{C}}\, {}_y\mathcal{C}_x$.

We introduce in this paper a general framework for Morita theory for k-categories. More precisely we establish processes which provide categories Morita equivalent to a starting one. We prove in the Appendix that up to equivalence of categories any Morita equivalence of k-categories is a composition of contractions and expansions of a given k-category, where contraction and expansion are processes generalizing a construction considered in [5]. More precisely, given a partition E of the set of objects of a k-category $\mathcal{C}$ by means of finite sets, the *contracted category* $\mathcal{C}_E$ along E has set of objects the sets of the partition while morphisms are provided by the direct sum of all the morphism spaces involved between two sets of the partition. The reverse construction is called *expansion.* Another process is related to the classical Morita theory for algebras, that is for each vertex we provide an endomorphism algebra Morita equivalent to the given one together with a corresponding Morita context, which enables us to modify the morphisms of the original category. In particular the

matrix category of a given category is obtained in this way. A discussion of this processes in relation with karoubianisation and additivisation (see for instance [1, 18]) is also presented in the Appendix. We thank Alain Bruguières and Mariano Suarez Alvarez for useful conversations concerning this point.
Usually smash extensions are considered for algebras, see for instance [15]. We begin by extending this construction to k-categories, namely given a Hopf algebra H we consider a Hopf module structure on a k-category $\mathcal{C}$ which is provided by an H-module structure on each morphism space such that the composition maps of $\mathcal{C}$ are H-module maps - in particular the endomorphism algebra of each object is required to be an usual H-module algebra. Given a Hopf module k-category $\mathcal{C}$ we define the *smash category* $\mathcal{C}\#H$ in a coherent way with the algebra case.
We need this extension of the usual algebra setting to the categorical one in order to relate smash extensions to Galois coverings of k-categories as considered for instance in [3, 5, 7].
Notice that we can consider, as in the algebra case, a smash extension of a category as a Hopf Galois extension with the normal basis property and with trivial map σ, see [15, p. 101] and also [2, 11, 17]. It would be interesting to relate non trivial maps σ to an extended class of coverings of categories accordingly, we will not initiate this study in the present paper.
We define a *smash extension* of an H-module category $\mathcal{C}$ to be the natural functor from $\mathcal{C}$ to $\mathcal{C}\#H$. An expected compatibility result holds, namely if the number of objects of $\mathcal{C}$ is finite, the corresponding matrix algebra $a(\mathcal{C})$ has an usual smash extension provided by $a(\mathcal{C}\#H)$. The later algebra can indeed be considered since the category $\mathcal{C}\#H$ has also a finite number of objects, namely the set of objects of $\mathcal{C}$. Moreover, we have that $a(\mathcal{C})\#H = a\,(\mathcal{C}\#H)$.
We consider also Galois coverings of k-categories given by a group G, that is a k-category with a free G-action and the projection functor to the corresponding quotient category. More precisely, by definition a G-k-category $\mathcal{C}$ has a set action of G on the set of objects, and has linear maps ${}_y\mathcal{C}_x \to {}_{sy}\mathcal{C}_{sx}$ for each element s of G and each couple of objects x and y, verifying the usual axioms that we recall in the text. In other words we have a group morphism from G to the autofunctors of $\mathcal{C}$. In case $\mathcal{C}$ is object-finite, we infer a usual action of G by automorphisms of the algebra $a(\mathcal{C})$. A G-k-category is called *free* in case the set action on the objects is free, namely $sx = x$ implies $s = 1$. The quotient category is well defined only in this case and we recall its construction, see [3, 9, 7, 5, 4].
The group algebra kG is a Hopf algebra, hence we can consider kG-module categories. Notice that G-k-categories form a wider class than kG-module categories. In fact kG-module categories are G-k-categories which have trivial action of G on the set of objects.
First we establish a comparison between two constructions obtained when starting with a graded category $\mathcal{C}$ over a finite group G. From one side the smash product category $\mathcal{C}\#k^G$ is defined in the present paper, and from the other side a smash product category $\mathcal{C}\#G$ has been considered in [4], actually the later

is the Galois covering of $\mathcal{C}$ corresponding to the grading. We show that $\mathcal{C}\#k^G$ and $\mathcal{C}\#G$ are not equivalent but Morita equivalent categories.
We note that starting with a Galois covering $\mathcal{C}$ of a category $\mathcal{B}$, the covering category $\mathcal{C}$ is $\mathcal{B}\#G$ (see [4] and the grading of $\mathcal{B}$ introduced there, first considered by E. Green in [10] for presented k-categories by a quiver with relations). Unfortunately $\mathcal{B}\#G$ has no natural kG-module category structure. However $\mathcal{B}\#G$ and $\mathcal{B}\#k^G$ are Morita equivalent and we perform the substitution. The later is a kG-module category using the left kG-module structure of k^G provided by $t\delta_s = \delta_{st^{-1}}$. In this way we associate to the starting Galois covering the smash extension $(\mathcal{B}\#k^G)\#kG$ of $\mathcal{B}\#k^G$.
The important point is that the later is Morita equivalent to $\mathcal{C}$ while $(\mathcal{B}\#k^G)\#kG$ is isomorphic to a matrix category that we introduce, which in turn is Morita equivalent to $\mathcal{B}$. Notice that this result is a categorical version of the Cohen Montgomery duality Theorem, see [6]. Hence we associate to the starting Galois covering $\mathcal{C} \to \mathcal{B}$ a smash extension with the same group and where the categories are replaced by Morita equivalent ones.
Second we focus to the reverse procedure, namely given a smash extension of categories with finite group G – that is a kG-module category $\mathcal{B}$ and the inclusion $\mathcal{B} \to \mathcal{C} = \mathcal{B}\#kG$ – we intend to associate a Galois covering to this data. For this purpose we consider the *inflated category* $I_F\mathcal{B}$ of a category $\mathcal{B}$ along a sequence $F = \{F_x\}$ of sets associated to the vertices of the original category : each object x of $\mathcal{B}_0$ provides $\mid F_x \mid$ new objects while the set of morphisms from (x, i) to (y, j) is precisely the vector space ${}_y\mathcal{B}_x$ with the obvious composition. For a finite group G the inflated category of a kG-module category – using the constant sequence of sets G – has a natural structure of a free G-k-category. The inflated category $I_G\mathcal{B}$ is Morita equivalent to the matrix category $M_{|G|}(\mathcal{B})$ by contraction and in turn the later is Morita equivalent to $\mathcal{B}$.
Moreover the categorical quotient of $I_G\mathcal{C}$ exists and in this way we obtain a Galois covering having the required properties with respect to the starting smash extension.

2 Hopf module categories

In this section we introduce the smash product of a category with a Hopf algebra and we specify this construction in case the Hopf algebra is the function algebra of a finite group G. We will obtain that the later is Morita equivalent to the smash product category defined in [4].
We recall (see for instance [15]) that for a Hopf algebra H over k, an H-module algebra A is a k-algebra which is simultaneously an H-module in such a way that the product map of A is a morphism of H-modules, where $A \otimes A$ is considered as an H-module through the comultiplication of H. Moreover we require that $h1_A = \epsilon(h)1_A$ for every $h \in H$.
We provide an analogous definition for a k-category $\mathcal{C}$ instead of an algebra.

Definition 2.1 *A k-category $\mathcal{C}$ is an H-*module category *if each morphism* *space is an H-module, each endomorphism algebra is an H-module algebra and composition maps are morphisms of H-modules, where as before the tensor product of H-modules is considered as an H-module via the comultiplication of H.*

Notice that analogously we may consider the structure of an H-comodule category. In case H is a finite dimensional Hopf algebra, we recall from [15] that there is a bijective vector space preserving correspondence between right H-modules and left H^*-comodules.

Remark 2.2 *Given a finite k-category $\mathcal{C}$, let $a(\mathcal{C})$ be the k-algebra obtained as the direct sum of all k-module morphisms of $\mathcal{C}$ equipped with the usual matrix product combined with the composition of $\mathcal{C}$. In case $\mathcal{C}$ is an H-module category $a(\mathcal{C})$ is an H-module algebra.*

Let $\mathcal{C}$ be an H-module category. We define the k-category $\mathcal{C}\#H$ as follows. The objets remain the same, while given two objects x and y we put ${}_y(\mathcal{C}\#H)_x = {}_y\mathcal{C}_x \otimes_k H$. The composition map for morphisms

$$ {}_z(\mathcal{C}\#H)_y \ \otimes \ {}_y(\mathcal{C}\#H)_x \longrightarrow {}_z(\mathcal{C}\#H)_x $$

is given by

$$ ({}_z\varphi_y \otimes h) \circ ({}_y\psi_x \otimes h') = \sum {}_z\varphi_y \circ (h_1 \ {}_y\psi_x) \otimes h_2 h', $$

where the comultiplication Δ of H is given by $\Delta(h) = \sum h_1 \otimes h_2$ and $\circ$ denotes composition in $\mathcal{C}$. As before we have an immediate coherence result:

Proposition 2.3 *Let $\mathcal{C}$ be a finite object H-module category $\mathcal{C}$. Then the k-algebras $a(\mathcal{C})\#H$ and $a(\mathcal{C}\#H)$ are canonically isomorphic.*

Let now G be a group. A G-graded k-category $\mathcal{C}$ (see for instance [4]) is a k-category $\mathcal{C}$ such that each morphism space ${}_y\mathcal{C}_x$ is the direct sum of sub-vector spaces ${}_y\mathcal{C}_x^s$, indexed by elements $s \in G$ such that ${}_z\mathcal{C}_y{}^t \ {}_y\mathcal{C}_x{}^s \subseteq {}_y\mathcal{C}_x{}^{ts}$ for all $x, y \in \mathcal{C}$ and for all $s, t \in G$.

Notice that as in the algebra case, gradings of a k-category $\mathcal{C}$ by means of a group G are in one-to-one correspondence with kG-comodule category structures on $\mathcal{C}$. Let now G be a finite group, $\mathcal{C}$ be a G-graded k-category and consider the function algebra $k^G = (kG)^*$ which is a Hopf algebra. The category $\mathcal{C}$ is a k^G-module category, hence according to our previous definition we can consider $\mathcal{C}\#k^G$.

We want to compare this category with another construction of a k-category denoted $\mathcal{C}\#G$ which can be performed for an arbitrary group G, see [4] : the set of objects is $\mathcal{C}_0 \times G$ while the morphisms from (x, s) to (y, t) is the vector space ${}_y\mathcal{C}_x{}^{(t^{-1}s)}$. The composition of morphisms is well-defined as an immediate consequence of the definition of a graded category.

Notice that given a graded algebra A considered as a single object G-graded k-category, the preceding construction provides a category with as many objects as elements of G, even if G is infinite. If G is finite, the associated algebra is known to be the usual smash product algebra $A\#k^G$, see [4].
We will recall below the definition of the module category of a k-category in order to prove that in case of a finite group G the module categories over $\mathcal{C}\#k^G$ and $\mathcal{C}\#G$ are equivalent.
First we introduce a general setting which is interesting by itself.

Definition 2.4 *Let $\mathcal{D}$ be a k-category equipped with a partition E of the set of objects $\mathcal{D}_0$ by means of finite sets $\{E_i\}_{i\in I}$. Then $\mathcal{D}_E$ is a new k-category obtained by* contraction *along the partition, more precisely I is the set of objects of $\mathcal{D}_E$ and morphisms are given by*

$$_j(\mathcal{D}_E)_i = \bigoplus_{y\in E_j \quad x\in E_i} {}_y\mathcal{D}_x.$$

Composition is given by matrix product combined with composition of the original category. Notice that the identity map of an object i is given by $\sum_{z\in E_i} {}_z1_z$, which makes sense since E_i is finite.

Example 2.5 *Let A be an algebra and let F be a complete finite family of orthogonal idempotents in A (we don't require that the idempotents are primitive). Consider the category $\mathcal{D}$ with set of objects F and morphisms ${}_y\mathcal{D}_x = yAx$. Then the contracted category along the trivial partition with only one subset is a single object category having endomorphism algebra $\bigoplus_{x,y\in F} {}_y\mathcal{D}_x = \bigoplus_{x,y\in F} yAx = A$.*

We also observe that for a finite object k-category $\mathcal{C}$, the contracted category along the trivial partition is a single object category with endomorphism algebra precisely $a(\mathcal{C})$. More generally let E be a partition of $\mathcal{C}_0$, then the k-algebras $a(\mathcal{C})$ and $a(\mathcal{C}_E)$ are equal.
We will establish now a relation between $\mathcal{D}$ and $\mathcal{D}_E$ at the representation theory level of these categories. In order to do so we recall the definition of modules over a k-category.

Definition 2.6 *Let $\mathcal{C}$ be a k-category. A left $\mathcal{C}$-module $\mathcal{M}$ is a collection of k-modules $\{{}_x\mathcal{M}\}_{x\in\mathcal{C}_0}$ provided with a left* action *of the k-modules of morphisms of $\mathcal{C}$, given by k-module maps ${}_y\mathcal{C}_x \otimes_k {}_x\mathcal{M} \to {}_y\mathcal{M}$, where the image of ${}_yf_x \otimes {}_xm$ is denoted ${}_yf_x\ {}_xm$, verifying the usual axioms:*

- ${}_zf_y\ ({}_yg_x\ {}_xm) = ({}_zf_y\ {}_yg_x)\ {}_xm$,
- ${}_x1_x\ {}_xm = {}_xm$.

In other words $\mathcal{M}$ is a covariant k-functor from $\mathcal{C}$ to the category of k-modules, the preceding explicit definition is useful for some detailed constructions. We denote by $\mathcal{C}-\mathrm{Mod}$ the category of left $\mathcal{C}$-modules. In case of a k-algebra A it is clear that A-modules considered as k-vector spaces equipped with an action of A coincide with $\mathbb{Z}$-modules provided with an A-action. Analogously, $\mathcal{C}$-modules as defined above are the same structures than $\mathbb{Z}$-functors from $\mathcal{C}$ to the category of $\mathbb{Z}$-modules.

Definition 2.7 *Two k-categories are said to be* Morita equivalent *if their left module categories are equivalent.*

Proposition 2.8 *Let $\mathcal{D}$ be a k-category and let E be a partition of the objects of $\mathcal{D}$ by means of finite sets. Then $\mathcal{D}$ and the contracted category $\mathcal{D}_E$ are Morita equivalent.*

We notice that this result is an extension of the well known fact that the category of modules over an algebra is isomorphic to the category of functors over the category of projective left modules provided by a direct sum decomposition of the free rank one left module, obtained for instance through a complete system of orthogonal idempotents of the algebra.
Proof. Let $\mathcal{M}$ be a $\mathcal{D}$-module and let $F\mathcal{M}$ be the following $\mathcal{D}_E$-module:

$$_iF\mathcal{M} = \bigoplus_{x\in E_i} {}_x\mathcal{M} \text{ for each } i \in I,$$

the action of a morphism $_jf_i = ({}_yf_x)_{x\in E_i, y\in E_j} \in {}_j(\mathcal{D}_E)_i$ on $_im = ({}_xm)_{x\in E_i} \in {}_iF(\mathcal{M})$ is obtained as a matrix by a column product, namely:

$$_jf_i\ {}_im = (\sum_{x\in E_i} {}_yf_x\ {}_xm)_{y\in E_j}.$$

A $\mathcal{D}-\text{Mod}$ morphism $\phi : \mathcal{M} \to \mathcal{M}'$ is a natural transformation between both functors, *i.e.* a collection of k-maps $_x\phi : {}_x\mathcal{M} \to {}_x\mathcal{M}'$, satisfying compatibility conditions. We define $F\phi : F\mathcal{M} \to F\mathcal{M}'$ by:

$$_i(F\phi) = \bigoplus_{x\in E_i} {}_x\phi.$$

Conversely given a $\mathcal{D}_E$-module $\mathcal{N}$, let $G\mathcal{N} \in (\mathcal{D}-\text{Mod})$ be the functor given by $_x(G\mathcal{N}) = e_x\,({}_i\mathcal{N})$, where i is unique element in I such that $x \in E_i$, and where e_x is the idempotent $|E_i| \times |E_i|$ - matrix with one in the (x,x) entry and zero elsewhere.
The action of $_yf_x \in {}_y\mathcal{D}_x$ on $_x(G\mathcal{N})$ is obtained as follows: let $i,j \in I$ be such that $x \in E_i$ and $y \in E_j$. Let $\overline{{}_yf_x} \in {}_j(\mathcal{D}_E)_i$ be the matrix with $_yf_x$ in the (y,x) entry and zero elsewhere. Then, for $e_xn \in {}_x(G\mathcal{N})$ we put $({}_yf_x)(e_xn) = {}_j(\overline{{}_yf_x})_i\ {}_i(e_xn) \in e_y\,({}_j\mathcal{N}) = {}_y(G\mathcal{N})$.
It is easy to verify that both compositions of F and G are the corresponding identity functors.

We will now apply the preceding result to the situation $\mathcal{D} = \mathcal{C}\#G$ using the partition provided by the orbits of the free G-action on the objects.

Theorem 2.9 *The k-categories $\mathcal{C}\#G$ and $\mathcal{C}\#k^G$ are Morita equivalent.*

Proof. We consider the contraction of $\mathcal{C}\#G$ along the partition provided by the orbits, namely for $x \in \mathcal{C}_0$ we put $E_x = \{(x,g) \mid g \in G\}$. Observe that for all $x \in \mathcal{C}_0$ the set E_x is finite since its cardinal is the order of the group G. Moreover the set of objects $((\mathcal{C}\#G)_E)_0$ of the contracted category is identified to $\mathcal{C}_0$.
The morphisms from x to y in the contracted category are $\bigoplus_{s,t\in G} {}_y\mathcal{C}_x{}^{t^{-1}s}$. On the other hand

$${}_y(\mathcal{C}\#k^G)_x = {}_y\mathcal{C}_x \otimes k^G = \bigoplus_{v\in G} {}_y\mathcal{C}_x{}^v \otimes k^G.$$

We assert that the contracted category $(\mathcal{C}\#G)_E$ and $\mathcal{C}\#k^G$ are isomorphic. The sets of objects already coincide. We define the functor L on the morphisms as follows. Let ${}_{(y,t)}f_{(x,s)}$ be an elementary matrix morphism of the contracted category. We put

$$L\left({}_{(y,t)}f_{(x,s)}\right) = f \otimes \delta_s \in {}_y\mathcal{C}_x{}^{t^{-1}s} \otimes k^G.$$

It is not difficult to check that L is an isomorphism preserving composition.

Remark 2.10 *The categories $\mathcal{C}\#G$ and $\mathcal{C}\#k^G$ are not equivalent in general as the following simple example already shows : let A be the group algebra kC_2 of the cyclic group of order two C_2 and let $\mathcal{C}_A$ be the single object C_2-graded k-category with A as endomorphism algebra. The category $\mathcal{C}\#C_2$ has two objects that we denote $(*,1)$ and $(*,t)$, while $\mathcal{C}\#k^{C_2}$ has only one object $*$. If $\mathcal{C}\#G$ and $\mathcal{C}\#k^G$ were equivalent categories the algebras $End_{\mathcal{C}\#C_2}((*,1))$ and $End_{\mathcal{C}\#k^{C_2}}(*))$ would be isomorphic. However the former is isomorphic to k while the latter is the four dimensional algebra $End_{\mathcal{C}\#k^{C_2}}(*) = (k\bigoplus kt)\otimes k^{C_2}$.*

3 kG-module categories

Let G be a group and let $\mathcal{C}$ be a kG-module category. Using the Hopf algebra structure of kG and the preceding definitions we are able to construct the smash category $\mathcal{C}\#kG$. We have already noticed that if $\mathcal{C}$ is an object finite k-category then the algebra $a(\mathcal{C}\#kG)$ is the classical smash product algebra $a(\mathcal{C})\#kG$.
According to [4] a G-k-category $\mathcal{D}$ is a k-category with an action of G on the set of objects and, for each $s \in G$, a k-linear map $s : {}_y\mathcal{D}_x \to {}_{sy}\mathcal{D}_{sx}$ such that $s(gf) = s(g)s(f)$ and $t(sf) = (ts)f$ for any composable couple of morphisms g, f and any elements s, t of G. Such a category is called a free G-k-category in case the action of G on the objects is a free action, namely the only group element acting trivially on the category is the trivial element of G.

Remark 3.1 *Notice that kG-module categories are G-k-categories verifying that the action of G on the set of objects is trivial.*

We need to associate a free G-k-category to a kG-module category $\mathcal{C}$, in order to perform the quotient category as considered in [4]. For this purpose we consider *inflated categories* as follows.

Definition 3.2 *Let $\mathcal{C}$ be a k-category and let $F = (F_x)_{x\in\mathcal{C}_0}$ be a sequence of sets associated to the objects of $\mathcal{C}$. The set of objects of the inflated category $I_F\mathcal{C}$ is*

$$\{(x,i) \mid x \in \mathcal{C}_0 \text{ and } i \in F_x\}$$

while ${}_{(y,j)}(I_F\mathcal{C})_{(x,i)} = {}_y\mathcal{C}_x$ with the obvious composition provided by the composition of $\mathcal{C}$. Alternatively, consider F as a map φ from a set to $\mathcal{C}_0$ such that the fiber over each object x is F_x. The set of objects of the inflated category is the fiber product of $\mathcal{C}_0$ with this set over φ.

Remark 3.3 *Clearly an inflated category is equivalent to the original category since all the objects with the same first coordinate are isomorphic. Hence a choice of one object in each set $\{(x,i) \mid i \in F_x\}$ provides a full sub-category of $I_F\mathcal{C}$ which is isomorphic to $\mathcal{C}$.*

In case $\mathcal{C}$ is a kG-module category we use the constant sequence of sets provided by the underlying set of G. We obtain a free action of G on the objects of the inflated category $I_G\mathcal{C}$ by translation on the second coordinate. Moreover the original action of G on each morphism set of $\mathcal{C}$ provides a free G-k-category structure on the inflated category. More precisely the G-action on the category $I_G\mathcal{C}$ is obtained through maps for each $u \in G$ as follows:

$$u : {}_{(y,t)}I_G\mathcal{C}_{(x,s)} \to {}_{(y,ut)}I_G\mathcal{C}_{(x,us)}$$

$$u\left({}_{(y,t)}f_{(x,s)}\right) = {}_{(y,ut)}(u\left({}_y f_x\right))_{(x,us)}.$$

As a next step we notice that the free G-k-category $I_G\mathcal{C}$ has a skew category $(I_G\mathcal{C})[G]$ associated to it. In fact any G-k-category has a related skew category defined in [4]. We recall that $(I_G\mathcal{C})[G]_0 = (I_G\mathcal{C})_0 = \mathcal{C}_0 \times G$. For $x, y \in \mathcal{C}_0$ $t, s \in G$ we have

$${}_{(y,t)}(I_G\mathcal{C})[G]_{(x,s)} = \bigoplus_{u\in G} {}_{(y,ut)}(I_G\mathcal{C})_{(x,s)} = \bigoplus_{u\in G} {}_y\mathcal{C}_x = {}_y\mathcal{C}_x \times G.$$

We are going to compare the categories $\mathcal{C}\#kG$ and $(I_G\mathcal{C})[G]$. In order to do so we consider the intermediate quotient category $(I_G\mathcal{C})/G$ (see [4, Definition 2.1]). We recall the definition of $\mathcal{D}/G$, where $\mathcal{D}$ is a free G-k-category: the set of objects is the set of G-orbits of $\mathcal{D}_0$, while the k-module of morphisms in $\mathcal{D}/G$ from the orbit α to the orbit β is

$${}_\beta(\mathcal{D}/G)_\alpha = \left(\bigoplus_{b\in\beta, a\in\alpha} {}_b\mathcal{D}_a\right)/G.$$

Recall that X/G denotes the module of coinvariants of a kG-module X, namely the quotient of X by $(\operatorname{Ker}\epsilon)X$ where $\epsilon : kG \to k$ the augmentation map. Composition is well defined precisely because the action of G is free on the objects, more explicitly, for $g \in {}_d\mathcal{D}_c$ and $f \in {}_b\mathcal{D}_a$ where b and c are objects in the same G-orbit, let s be the unique element of G such that $sb = c$. Then $[g][f] = [g\ (sf)] = [(s^{-1}g)\ f]$.

Lemma 3.4 *The k-categories $\mathcal{C}\#kG$ and $(I_G\mathcal{C})/G$ are isomorphic.*

Proof. Clearly the set of objects can be identified. Given a morphism $({}_yf_x \otimes u) \in {}_y(\mathcal{C}\#kG)_x$ we associate to it the class $[f]$ of the morphism $f \in {}_{(y,1)}(I_G\mathcal{C})_{(x,u)}$. Notice that in the smash category we have

$$({}_zg_y \otimes v)({}_yf_x \otimes u) = {}_zg_y\ v({}_yf_x) \otimes vu$$

which has image $[{}_zg_y\ v({}_yf_x)]$. The composition in the quotient provides precisely $[g][f] = [g\ vf]$. The inverse functor is also clear.

Since $(I_G\mathcal{C})/G$ and $(I_G\mathcal{C})[G]$ are equivalent (see [4]), we obtain the following:

Proposition 3.5 *The categories $\mathcal{C}\#kG$ and $(I_G\mathcal{C})[G]$ are equivalent.*

4 From Galois coverings to smash extensions and vice versa

Our aim is to relate kG-smash extensions and Galois coverings for a finite group G. Recall that it has been proved in [4] that any Galois covering with group G of a k-category $\mathcal{B}$ is obtained *via* a G-grading of $\mathcal{B}$, we have that $\mathcal{C} = \mathcal{B}\#G$ is the corresponding Galois covering of $\mathcal{B}$. We have already noticed that for a finite group G a G-grading of a k-category $\mathcal{B}$ is the same thing than a k^G-module category structure on $\mathcal{B}$.
However neither $\mathcal{B}$ nor $\mathcal{B}\#G$ have a natural kG-module category structure which could provide a smash extension. We have proven before that $\mathcal{B}\#k^G$ is Morita equivalent to the category $\mathcal{B}\#G$. The advantage of $\mathcal{B}\#k^G$ is that it has a natural kG-module category structure provided by the left kG-module structure of k^G given by $t\delta_s = \delta_{st^{-1}}$.
In this way we associate to the starting Galois covering $\mathcal{B}\#G$ of $\mathcal{B}$ the smash extension $(\mathcal{B}\#k^G) \to (\mathcal{B}\#k^G)\#kG$. In [17] the authors describe when a given Hopf-Galois extension is of this type (in the case of algebras). We will prove that the later is isomorphic to an *ad-hoc* category $M_{|G|}(\mathcal{B})$ which happens to be Morita equivalent to $\mathcal{B}$.

Definition 4.1 *Let $\mathcal{B}$ be a k-category and let n be a sequence of positive integers $(n_x)_{x\in\mathcal{B}_0}$. The objects of the matrix category $M_n(\mathcal{B})$ remain the same objects of $\mathcal{B}$. The set of morphisms from x to y is the vector space of n_x-columns and n_y-rows rectangular matrices with entries in ${}_y\mathcal{B}_x$. Composition of morphisms is given by the matrix product combined with the composition in $\mathcal{B}$.*

Remark 4.2 *In case the starting category $\mathcal{B}$ is a single object category provided by an algebra B, the matrix category has one object with endomorphism algebra precisely the usual algebra of matrices $M_n(B)$.*
Notice that the matrix category that we consider is not the category $\mathrm{Mat}(\mathcal{C})$ *defined by Mitchell in [13]. In fact* $\mathrm{Mat}(\mathcal{C})$ *corresponds to the additivisation of* $\mathcal{C}$ *(see the Appendix).*

We need the next result in order to have that the smash extension associated to a Galois covering has categories Morita equivalent to the original ones. In fact this result is also a categorical generalization of Cohen Montgomery duality Theorem [6].

Lemma 4.3 *Let $\mathcal{B}$ be a G-graded category and let n be the order of G. Then the categories $(\mathcal{B}\#k^G)\#kG$ and $M_n(\mathcal{B})$ are isomorphic.*

Proof. Both sets of objects coincide. Given two objects x and y we define two linear maps:

$$\phi : {}_y\mathcal{B}_x \otimes k^G \otimes kG \to {}_y(M_n(\mathcal{B}))_x\,,$$
$$\psi : {}_y(M_n(\mathcal{B}))_x \to {}_y\mathcal{B}_x \otimes k^G \otimes kG.$$

Given an homogeneous element

$$(f \otimes \delta_g \otimes h) \in {}_y\mathcal{B}_x \otimes k^G \otimes kG,$$

where f has degree r and $g, h \in G$ we put

$$\phi(f \otimes \delta_g \otimes h) = f\ {}_{rg}E_{gh},$$

where ${}_{rg}E_{gh}$ is the elementary matrix with 1 in the (rg, gh)-spot and 0 elsewhere. It is straightforward to verify that ϕ is well-behaved with respect to compositions.
We also define ψ on elementary morphisms as follows:

$$\psi(f\ {}_gE_h) = f \otimes \delta_{r^{-1}g} \otimes g^{-1}rh,$$

where r is the degree of f.

Next we have to prove that $M_n(\mathcal{B})$ is Morita equivalent to $\mathcal{B}$. In order to do so we develop some Morita theory for k-categories which is interesting by itself. When we restrict the following theory to a particular object, it will coincide with the classical theory, see for instance [19, p.326]. Moreover, in case of a finite object set k-categories both Morita theories coincide using the associated algebras that we have previously described.
Let $\mathcal{C}$ be a k-category. For simplicity for a given object x we denote by A_x the k-algebra ${}_x\mathcal{C}_x$. For each x, let B_x be a k-algebra such that there is a (B_x, A_x)-bimodule P_x and a (A_x, B_x)-bimodule Q_x verifying that $P_x \otimes_{A_x} Q_x \cong B_x$ as B_x-bimodules and $Q_x \otimes_{B_x} P_x \cong A_x$ as A_x-bimodules. In other words for each

object we assume that we have a Morita context providing that A_x and B_x are Morita equivalent. Note that it follows from the assumptions that P_x is projective and finitely generated on both sides, see for instance [19].
Using the preceding data we modify the morphisms in order to define a new k-category $\mathcal{D}$ which will be Morita equivalent to $\mathcal{C}$. In particular the endomorphism algebra of each object x will turn out to be B_x.
More precisely the set of objects of $\mathcal{D}$ remains the set of objects of $\mathcal{C}$ while for morphisms we put

$$_y\mathcal{D}_x = P_y \otimes_{A_y} {_y\mathcal{C}_x} \otimes_{A_x} Q_x.$$

Notice that for $x = y$ we have $_x\mathcal{D}_x \cong B_x$. In order to define composition in $\mathcal{D}$ we need to provide a map

$$(P_z \otimes_{A_z} {_z\mathcal{C}_y} \otimes_{A_y} Q_y) \otimes_k (P_y \otimes_{A_y} {_y\mathcal{C}_y} \otimes_{A_x} Q_x) \longrightarrow P_z \otimes_{A_z} {_z\mathcal{C}_x} \otimes_{A_x} Q_x,$$

For this purpose let φ_x be a fixed A_x-bimodule isomorphism from $Q_x \otimes_{B_x} P_x$ to A_x and consider ϕ_x the composition the projection $Q_x \otimes_k P_x \to Q_x \otimes_{B_x} P_x$ followed by φ_x. Then composition is defined as follows

$$(p_z \otimes g \otimes q_y)(p_y \otimes f \otimes q_x) = p_z \otimes g\, [\phi_y(q_y \otimes p_y)]\, f \otimes q_x.$$

This composition is associative since the use of the morphisms ϕ do not interfere in case of composition of three maps.

PROPOSITION 4.4 *Let $\mathcal{C}$ and $\mathcal{D}$ be k-categories as above. Then $\mathcal{C}$ and $\mathcal{D}$ are Morita equivalent.*

PROOF. For a $\mathcal{C}$-module $\mathcal{M}$ we define the $\mathcal{D}$-module $F\mathcal{M}$ as follows:

$$_x(F\mathcal{M}) = P_x \otimes_{A_x} {_x\mathcal{M}}, \text{ which is already a left } B_x\text{-module.}$$

The left action $_y\mathcal{D}_x \otimes {_x(F\mathcal{M})} \to {_y(F\mathcal{M})}$ is obtained using the following morphism induced by ϕ_x

$$\big(P_y \otimes_{A_y} {_y\mathcal{C}_x} \otimes_{A_x} Q_x\big) \otimes_k (P_x \otimes_{A_x} {_x\mathcal{M}}) \longrightarrow P_y \otimes_{A_y} {_y\mathcal{C}_x} \otimes_k A_x \otimes_k {_x\mathcal{M}}$$

and the actions of A_x and of $_y\mathcal{C}_x$ on $_x\mathcal{M}$. We then obtain a map with target $_y(F\mathcal{M})$. This defines clearly a $\mathcal{D}$-module structure.
Similarly we obtain a functor G in the reverse direction which is already an equivalent inverse for F.

We apply now this Proposition to a k-category $\mathcal{C}$ and the category obtained from $\mathcal{C}$ by replacing each endomorphism algebra by matrix algebras over it. For each object x in $\mathcal{C}_0$ consider the k-algebra $B_x = M_n(A_x)$. The bimodule $_{M_n(A_x)}(P_x)_{A_x}$ is the left ideal of $M_n(A_x)$ given by the first column and zero elsewhere, while $_{A_x}(Q_x)_{M_n(A_x)}$ is given by the analogous right ideal provided by the first row. Then the category $\mathcal{D}$ defined above is precisely $M_n(\mathcal{C})$.

Corollary 4.5 *$\mathcal{C}$ and $M_n(\mathcal{C})$ are Morita equivalent.*

Remark 4.6 *An analogous Morita equivalence still hold when the integer n is replaced by a sequence of positive integers $(n_x)_{x\in\mathcal{C}_0}$.*

The applications of Morita theory for categories developed above covers a larger spectra than the one considered in this paper. We have produced several sorts of Morita equivalences for categories, namely expansion, contraction and the Morita context for categories described above. We will prove the next result in the Appendix.

Theorem 4.7 *Let $\mathcal{C}$ and $\mathcal{D}$ be Morita equivalent k-categories. Up to equivalence of categories, $\mathcal{D}$ is obtained from $\mathcal{C}$ by contractions and expansions.*

Example 4.8 *Let A be a k-algebra and $\mathcal{C}_A$ the corresponding single object category. It is well known that the following k-category $M\mathcal{C}_A$ is Morita equivalent to $\mathcal{C}_A$: objects are all the positive integers $[n]$ and the morphisms from $[n]$ to $[m]$ are the matrices with n columns, m rows, and with A entries.*
At each object [n] choose the system of n idempotents provided by the elementary matrices which are zero except in a diagonal spot where the value is the unit of the algebra. The expansion process through this choice provides a category with numerable set of objects, morphisms are A between any couple of objects, they are all isomorphic, consequently this category is equivalent to $\mathcal{C}_A$. This way a Morita equivalence (up to equivalence) between $\mathcal{C}_A$ and $M\mathcal{C}_A$ is obtained using the expansion process.
Conversely, in order to obtain $M\mathcal{C}_A$ from $\mathcal{C}_A$, first inflate $\mathcal{C}_A$ using the set of positive integers. Then consider the partition by means of the finite sets having all the positive integers cardinality, namely $\{1\}, \{2, 3\}, \{4, 5, 6\}, \ldots$. Finally the contraction along this partition provides precisely $M\mathcal{C}_A$.

We provide now an alternative proof of the fact that a matrix category is Morita equivalent to the original one. It provides also evidence for Theorem 4.7 concerning the structure of the Morita equivalence functors. First consider the inflated category using the sequence of positive integers defining the matrix category. We have shown before that this category is equivalent to the original one. Secondly perform the contraction of this inflated category along the finite sets partition provided by couples having the same first coordinate. This category is the matrix category. Since we know that a contracted category is Morita equivalent to the original one, this provides a proof that a matrix category is Morita equivalent to the the starting category, avoiding the use of Morita contexts. The alternative proof we have presented indicate how classical Morita equivalence between algebras can be obtained by means of contractions, expansions and equivalences of categories. More precisely Theorem 4.7 states that classical Morita theory can be replaced by those processes.
The results that we have obtained provide the following

Theorem 4.9 *Let $\mathcal{C} \longrightarrow \mathcal{B}$ be a Galois covering of categories with finite group G. The associated smash extension $\mathcal{B}\#k^G \longrightarrow (\mathcal{B}\#k^G)\#kG$ verifies that $\mathcal{B}\#k^G$ is Morita equivalent to $\mathcal{C}$ and $(\mathcal{B}\#k^G)\#kG$ is Morita equivalent to $\mathcal{B}$.*

Finally notice that the proof of a converse for this result is a direct consequence of the discussion we have made in the previous section:

Theorem 4.10 *Let $\mathcal{C} \longrightarrow \mathcal{B}$ be a smash extension with finite group G. The corresponding Galois covering $I_G\mathcal{C} \longrightarrow (I_G\mathcal{C})/G$ verifies that $I_G\mathcal{C}$ is equivalent to $\mathcal{C}$ and that $(I_G\mathcal{C})/G$ is equivalent to $\mathcal{B}$.*

Proof. Indeed an inflated category is isomorphic to the original one; moreover $\mathcal{B} = \mathcal{C}\#kG$ and by Lemma 3.4 this category is isomorphic to $(I_G\mathcal{C})/G$.

5 Appendix: Morita equivalence of categories over a field

We have considered in this paper several procedures that we can apply to a k-category. We briefly recall and relate them with the karoubianisation (also called idempotent completion) and the additivisation (or additive completion), see for instance the appendix of [18].
The *inflation* procedure clearly provides an equivalent category : given a set F_x over each object x of the k-category $\mathcal{C}$, the objects of the inflated category $I_F\mathcal{C}$ are the couples (x, i) with $i \in F_x$. Morphisms from (x, i) to (y, j) remain the morphisms from x to y. Consequently objects with the same first coordinate are isomorphic in the inflated category. Choosing one of them above each object of the original category $\mathcal{C}$ provides a full subcategory of the inflated one, which is isomorphic to $\mathcal{C}$.
The *skeletonisation* procedure consists in choosing precisely one object in each isomorphism set of objects and considering the corresponding full subcategory. Clearly any category is isomorphic to an inflation of its skeleton. Skeletons of the same category are isomorphic, as well as skeletons of equivalent categories. Those remarks show that up to isomorphism of categories, any equivalence of categories is the composition of a skeletonisation and an inflation procedure.
Concerning Morita equivalence, we have used *contraction* and *expansion*. In order to contract we need a partition of the objects of the k-category $\mathcal{C}$ by means of finite sets. The sets of the partition become the objects of the contracted category, and morphisms are provided by matrices of morphisms of $\mathcal{C}$. Conversely, in order to expand we choose a complete system of orthogonal idempotents for each endomorphism algebra at each object of the k-category (the trivial choice is given by just the identity morphism at each object). The set of objects of the expanded category is the disjoint union of all those finite sets of idempotents. Morphisms from e to f are $f_y\mathcal{C}_x e$, assuming e is an idempotent at x and f is an idempotent at y. Composition is given by the composition of $\mathcal{C}$.
We assert that the karoubianisation and the additivisation (see for instance [1, 18]) can be obtained through the previous procedures.

Recall that the karoubianisation of $\mathcal{C}$ replaces each object of $\mathcal{C}$ by *all* the idempotents of its endomorphism algebra, while the morphisms are defined as for the expansion process above.

Consider now the partition of the objects of the karoubianisation of $\mathcal{C}$ given by an idempotent and its complement, namely the sets $\{e, 1-e\}$ for each idempotent at each object of $\mathcal{C}$. The contraction along this partition provides a category equivalent to $\mathcal{C}$, since all the objects over a given object of $\mathcal{C}$ are isomorphic in the contraction of the karoubianisation. Concerning the additivisation, notice first that two constructions are in force which provide equivalent categories as follows.

The larger category is obtained from $\mathcal{C}$ by considering all the finite sequences of objects, and morphisms given through matrix morphisms of $\mathcal{C}$. Observe that two objects (i.e. two finite sequences) which differ by a transposition are isomorphic in this category, using the evident matrix morphism between them. Consequently the objects of the smaller construction are the objects of the previous one modulo permutation, namely the set of objects are finite sets of objects of $\mathcal{C}$ with positive integers coefficients attached. In other words objects are maps from $\mathcal{C}_0$ to $\mathbb{N}$ with finite support. Morphisms are once again matrix morphisms.

The observation above concerning finite sequences differing by a transposition shows that the larger additivisation completion is equivalent to the smaller one.

Finally the smaller additivisation of $\mathcal{C}$ can be expanded: choose the canonical complete orthogonal idempotent system at each object provided by the matrix endomorphism algebra. Of course the expanded category have several evident isomorphic objects which keeps trace of the original objects. A choice provides a full subcategory equivalent to $\mathcal{C}$.

It follows from this discussion that karoubianisation and additivisation provide Morita equivalent categories to a given category, using contraction and expansion processes, up to isomorphism of categories.

We denote $\widehat{\mathcal{C}}$ the completion of $\mathcal{C}$, namely the additivisation of the karoubianisation (or *vice-versa* since those procedures commute). We notice that two categories are Morita equivalent if and only if their completions are Morita equivalent.

Recall that a k-category is called *amenable* if it has finite coproducts and if idempotents split, see for instance [8]. It is well known and easy to prove that the completion $\widehat{\mathcal{C}}$ is amenable.

We provide now a proof of Theorem 4.7. We have shown that the completion of a k-category is obtained (up to equivalence) by expansions and contractions of the original one. Notice that $\widehat{\mathcal{C}}$ and $\widehat{\mathcal{D}}$ are Morita equivalent amenable categories. We recall now the proof that this implies that the categories $\widehat{\mathcal{C}}$ and $\widehat{\mathcal{D}}$ are already equivalent (a result known as "Freyd's version of Morita equivalence", see [13, p.18]): consider the full subcategory of representable $\widehat{\mathcal{C}}$-modules, namely modules of the form ${}_{-}\widehat{\mathcal{C}}_x$. This category is isomorphic to the opposite of the original one (this is well known and immediate to prove using

Yoneda's Lemma). Since $\widehat{\mathcal{C}}$ is amenable, representable $\widehat{\mathcal{C}}$-modules are precisely the small (or finitely generated) projective ones, see for instance [8, p. 119]. Finally the small projective modules are easily seen to be preserved by any equivalence of categories; consequently the opposite categories of $\widehat{\mathcal{C}}$ and $\widehat{\mathcal{D}}$ are equivalent, hence the categories themselves are also equivalent.

References

[1] Balmer, P; Schlichting, M.: Idempotent completion of triangulated categories. J. Algebra 236 (2001), 819–834.

[2] Beattie, M.; Torrecillas, B.: Twistings and Hopf Galois extensions. J. Algebra 232 (2000), 673–696.

[3] Bongartz, K.; Gabriel, P.: Covering spaces in representation-theory. Invent. Math. 65 (1981/82), 331–378.

[4] Cibils, C.; Marcos E. N.: Skew categories, Galois coverings and smash product of a k-category. Proc. Amer. Math. Soc., 134 (2006), 39–50.

[5] Cibils, C.; Redondo M. J.: Cartan-Leray spectral sequence for Galois coverings of linear categories. J. Algebra 284 (2005), 310-325.

[6] Cohen, M.; Montgomery, S.: Group-graded rings, smash products, and group actions. Trans. Amer. Math. Soc. 282 (1984), 237–258.

[7] Drozd, Y.A.; Ovsienko, S.A.: Coverings of tame boxes and algebras. Preprints of the Max-Planck-Institut für Mathematik. MPI 2000 - 26.

[8] Freyd, P.: Abelian categories. An introduction to the theory of functors. Harper's Series in Modern Mathematics. New York-Evanston-London: Harper and Row, Publishers, 1964.
http://www.tac.mta.ca/tac/reprints/articles/3/tr3.pdf

[9] Gabriel, P.: The universal cover of a representation-finite algebra. Representations of algebras (Puebla, 1980), pp. 68–105, Lecture Notes in Math., 903, Springer, Berlin-New York, 1981.

[10] Green, E. L.: Graphs with relations, coverings, and group-graded algebras. Trans. Amer. Math. Soc., 279, (1983), 297-310.

[11] Kreimer, H. F.: Normal bases for Hopf-Galois algebras. Proc. Amer. Math. Soc. 130 (2002), 2853–2856.

[12] Lorenz, M. : On the homology of graded algebras. Comm. Algebra 20 (1992), 489–507.

[13] Mitchell, B.: Rings with several objects. Adv. in Math. 8 (1972), 1–161.

[14] Mitchell, B.: Separable algebroids. AMS Memoirs 333 (1985).

[15] Montgomery, S.: Hopf algebras and their actions on rings. CBMS Regional Conference Series in Mathematics, 82. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993.

[16] Redondo, M.-J.; Pirashvili, T.: Cohomology of the Grothendieck construction. http://arxiv.org/abs/math/0504282

[17] Raianu, Ş; Saorín, M.: Finite Hopf-Galois extensions equivalent to crossed products. Comm. Algebra 29 (2001), 4871–4882.

[18] Tillmann, U.: S-structures for k-linear categories and the definition of a modular functor. J. Lond. Math. Soc. II. 58 (1998), 208–228.

[19] Weibel, C.: An introduction to homological algebra. Cambridge Studies in Advanced Mathematics. 38. Cambridge: Cambridge University Press, 1994.

Claude Cibils
Département de Mathématiques
Université de Montpellier 2
F–34095 Montpellier cedex 5
France
Claude.Cibils@math.univ-montp2.fr

Andrea Solotar
Departemento de Matemática
Facultad de Ciencias
Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria, Pabellón 1
1428, Buenos Aires, Argentina
asolotar@dm.uba.ar

Sobolev Spaces on Lie Manifolds and Regularity for Polyhedral Domains

Bernd Ammann, Alexandru D. Ionescu, Victor Nistor

Received: January 4, 2006
Revised: June 8, 2006

Communicated by Heinz Siedentop

Abstract. We study some basic analytic questions related to differential operators on Lie manifolds, which are manifolds whose large scale geometry can be described by a a Lie algebra of vector fields on a compactification. We extend to Lie manifolds several classical results on Sobolev spaces, elliptic regularity, and mapping properties of pseudodifferential operators. A tubular neighborhood theorem for Lie submanifolds allows us also to extend to regular open subsets of Lie manifolds the classical results on traces of functions in suitable Sobolev spaces. Our main application is a regularity result on polyhedral domains $\mathbb{P} \subset \mathbb{R}^3$ using the weighted Sobolev spaces $\mathcal{K}_a^m(\mathbb{P})$. In particular, we show that there is no loss of $\mathcal{K}_a^m$–regularity for solutions of strongly elliptic systems with smooth coefficients. For the proof, we identify $\mathcal{K}_a^m(\mathbb{P})$ with the Sobolev spaces on $\mathbb{P}$ associated to the metric $r_{\mathbb{P}}^{-2} g_E$, where g_E is the Euclidean metric and $r_{\mathbb{P}}(x)$ is a smoothing of the Euclidean distance from x to the set of singular points of $\mathbb{P}$. A suitable compactification of the interior of $\mathbb{P}$ then becomes a regular open subset of a Lie manifold. We also obtain the well-posedness of a non-standard boundary value problem on a smooth, bounded domain with boundary $\mathcal{O} \subset \mathbb{R}^n$ using weighted Sobolev spaces, where the weight is the distance to the boundary.

2000 Mathematics Subject Classification: 35J40 (Primary) 33J55, 35J70, 35J25, 47G30 (Secondary)
Keywords and Phrases: regularity, polyhedral domains, Lie manifolds, analysis on complete manifolds

Contents

Introduction

We study some basic analytic questions on non-compact manifolds. In order to obtain stronger results, we restrict ourselves to "Lie manifolds," a class of manifolds whose large scale geometry is determined by a compactification to a manifold with corners and a Lie algebra of vector fields on this compactification (Definition 1.3). One of the motivations for studying Lie manifolds is the loss of (classical Sobolev) regularity of solutions of elliptic equations on non-smooth domains. To explain this loss of regularity, let us recall first that the Poisson problem

$$\Delta u = f \in H^{m-1}(\Omega), \quad m \in \mathbb{N} \cup \{0\},\ \Omega \subset \mathbb{R}^n \text{ bounded}, \tag{1}$$

has a unique solution $u \in H^{m+1}(\Omega)$, $u = 0$ on $\partial\Omega$, provided that $\partial\Omega$ *is smooth*. In particular, u will be smooth up to the boundary if $\partial\Omega$ and f are smooth (in the following, when dealing with functions defined on an open set, by "smooth," we shall mean "smooth up to the boundary"). See the books of Evans [16], or Taylor [58] for a proof of this basic well-posedness result.

This well-posedness result is especially useful in practice for the numerical approximation of the solution u of Equation (1) [8]. However, in practice, it is only rarely the case that Ω is smooth. The lack of smoothness of the domains interesting in applications has motivated important work on Lipschitz domains, see for instance [23, 40] or [65]. These papers have extended to Lipschitz domains some of the classical results on the Poisson problem on smooth, bounded domains, using the classical Sobolev spaces

$$H^m(\Omega) := \{u,\ \partial^\alpha u \in L^2(\Omega),\ |\alpha| \leq m\}.$$

It turns out that, if $\partial\Omega$ is *not* smooth, then the smoothness of f on $\overline{\Omega}$ (i. e., up to the boundary) does not imply that the solution u of Equation (1) is smooth as well on $\overline{\Omega}$. This is the *loss of regularity* for elliptic problems on non-smooth domains mentioned above.

The loss of regularity can be avoided, however, by a conformal blowup of the singular points. This conformal blowup replaces a neighborhood of each connected component of the set of singular boundary points by a complete, but non-compact end. (Here "complete" means complete as a metric space, not geodesically complete.) It can be proved then that the resulting Sobolev spaces are the "Sobolev spaces with weights" considered for instance in [25, 26, 35, 46]. Let $f > 0$ be a smooth function on a domain Ω, we then define the *mth Sobolev space with weight* f by

$$\text{(2)}\quad \mathcal{K}_a^m(\Omega; f) := \{u,\ f^{|\alpha|-a}\partial^\alpha u \in L^2(\Omega),\ \ |\alpha| \leq m\}, \quad m \in \mathbb{N} \cup \{0\},\ a \in \mathbb{R}.$$

Indeed, if $\Omega = \mathbb{P} \subset \mathbb{R}^2$ is a polygon, and if we choose

$$\text{(3)}\qquad f(x) = \vartheta(x) = \text{ the } \textit{distance to the non-smooth boundary points of } \mathbb{P},$$

then there is no loss of regularity in the spaces $\mathcal{K}_a^m(\Omega) := \mathcal{K}_a^m(\Omega; \vartheta)$ [26, Theorem 6.6.1]. In this paper, we extend this regularity result to polyhedral domains in three dimensions, Theorem 6.1, with the same choice of the weight (in three dimensions the weight is the distance to the edges). The analogous result in arbitrary dimensions leads to topological difficulties [9, 66].

Our regularity result requires us first to study the weighted Sobolev spaces $\mathcal{K}_a^m(\Omega) := \mathcal{K}_a^m(\Omega; \vartheta)$ where $\vartheta(x)$ is the distance to the set of singular points on the boundary. Our approach to Sobolev spaces on polyhedral domains is to show first that $\mathcal{K}_a^m(\Omega)$ is isomorphic to a Sobolev space on a certain non-compact Riemannian manifold M with smooth boundary. This non-compact manifold M is obtained from our polyhedral domain by replacing the Euclidean metric g_E with

$$\text{(4)}\qquad r_{\mathbb{P}}^{-2} g_E, \quad r_{\mathbb{P}} \text{ a smoothing of } \vartheta,$$

which blows up at the faces of codimension two or higher, that is, at the set of singular boundary points. (The metric $r_{\mathbb{P}}^{-2} g_E$ is Lipschitz equivalent to $\vartheta^{-2} g_E$, but the latter is not smooth.) The resulting non-compact Riemannian manifold turns out to be a regular open subset in a "Lie manifold." (see Definition 1.3, Subsection 1.6, and Section 6 for the precise definitions). A *Lie manifold* is a compact manifold with corners M together with a $C^\infty(M)$-module $\mathcal{V}$ whose elements are vector fields on M. The space $\mathcal{V}$ must satisfy a number of axioms, in particular, $\mathcal{V}$ is required to be closed under the Lie bracket of vector fields. This property is the origin of the name *Lie* manifold. The $C^\infty(M)$-module $\mathcal{V}$ can be identified with the sections of a vector bundle A over M. Choosing a metric on A defines a complete Riemannian metric on the interior of M. See Section 1 or [4] for details.

The framework of Lie manifolds is quite convenient for the study of Sobolev spaces, and in this paper we establish, among other things, that the main results on the classical Sobolev spaces remain true in the framework of Lie manifolds. The regular open sets of Lie manifolds then play in our framework the role played by smooth, bounded domains in the classical theory.

Let $\mathbb{P} \subset \mathbb{R}^n$ be a polyhedral domain. We are especially interested in describing the spaces $\mathcal{K}^{m-1/2}_{a-1/2}(\partial\mathbb{P})$ of restrictions to the boundary of the functions in the weighted Sobolev space $\mathcal{K}^m_a(\mathbb{P};\vartheta) = \mathcal{K}^m_a(\mathbb{P};r_{\mathbb{P}})$ on $\mathbb{P}$. Using the conformal change of metric of Equation (4), the study of restrictions to the boundary of functions in $\mathcal{K}^m_a(\mathbb{P})$ is reduced to the analogous problem on a suitable regular open subset $\Omega_{\mathbb{P}}$ of some Lie manifold. More precisely, $\mathcal{K}^m_a(\mathbb{P}) = r_{\mathbb{P}}^{a-n/2} H^m(\Omega_{\mathbb{P}})$. A consequence of this is that

$$\mathcal{K}^{m-1/2}_{a-1/2}(\partial\mathbb{P}) = \mathcal{K}^{m-1/2}_{a-1/2}(\partial\mathbb{P};\vartheta) = r_{\mathbb{P}}^{a-n/2} H^{m-1/2}(\partial\Omega_{\mathbb{P}}). \tag{5}$$

(In what follows, we shall usually simply denote $\mathcal{K}^m_a(\mathbb{P}) := \mathcal{K}^m_a(\mathbb{P};\vartheta) = \mathcal{K}^m_a(\mathbb{P};r_{\mathbb{P}})$ and $\mathcal{K}^m_a(\partial\mathbb{P}) := \mathcal{K}^m_a(\partial\mathbb{P};\vartheta) = \mathcal{K}^m_a(\partial\mathbb{P};r_{\mathbb{P}})$, where, we recall, $\vartheta(x)$ is the distance from x to the set of non-smooth boundary points and $r_{\mathbb{P}}$ is a smoothing of ϑ that satisfies $r_{\mathbb{P}}/\vartheta \in [c, C]$, $c, C > 0$.)

Equation (5) is one of the motivations to study Sobolev spaces on Lie manifolds. In addition to the non-compact manifolds that arise from polyhedral domains, other examples of Lie manifolds include the Euclidean spaces $\mathbb{R}^n$, manifolds that are Euclidean at infinity, conformally compact manifolds, manifolds with cylindrical and polycylindrical ends, and asymptotically hyperbolic manifolds. These classes of non-compact manifolds appear in the study of the Yamabe problem [32, 48] on compact manifolds, of the Yamabe problem on asymptotically cylindrical manifolds [2], of analysis on locally symmetric spaces, and of the positive mass theorem [49, 50, 67], an analogue of the positive mass theorem on asymptotically hyperbolic manifolds [6]. Lie manifolds also appear in Mathematical Physics and in Numerical Analysis. Classes of Sobolev spaces on non-compact manifolds have been studied in many papers, of which we mention only a few [15, 18, 27, 30, 34, 36, 39, 37, 38, 51, 52, 53, 63, 64] in addition to the works mentioned before. Our work can also be used to unify some of the various approaches found in these papers.

Let us now review in more detail the contents of this paper. A large part of the technical material in this paper is devoted to the study of Sobolev spaces on Lie manifolds (with or without boundary). If M is a *compact* manifold with corners, we shall denote by ∂M the union of all boundary faces of M and by $M_0 := M \smallsetminus \partial M$ the interior of M. We begin in Section 1 with a review of the definition

of a structural Lie algebra of vector fields $\mathcal{V}$ on a manifold with corners M. This Lie algebra of vector fields will provide the derivatives appearing in the definition of the Sobolev spaces. Then we define a Lie manifold as a pair $(M, \mathcal{V})$, where M is a compact manifold with corners and $\mathcal{V}$ is a structural Lie algebra of vector fields that is unrestricted in the interior M_0 of M. We will explain the above mentioned fact that the interior of M carries a complete metric g. This metric is unique up to Lipschitz equivalence (or quasi-isometry). We also introduce in this section Lie manifolds with (true) boundary and, as an example, we discuss the example of a Lie manifold with true boundary corresponding to curvilinear polygonal domains. In Section 2 we discuss Lie submanifolds, and most importantly, the global tubular neighborhood theorem. The proof of this global tubular neighborhood theorem is based on estimates on the second fundamental form of the boundary, which are obtained from the properties of the structural Lie algebra of vector fields. This property distinguishes Lie manifolds from general manifolds with boundary and bounded geometry, for which a global tubular neighborhood is part of the definition. In Section 3, we define the Sobolev spaces $W^{s,p}(M_0)$ on the interior M_0 of a Lie manifold M, where either $s \in \mathbb{N} \cup \{0\}$ and $1 \le p \le \infty$ or $s \in \mathbb{R}$ and $1 < p < \infty$. We first define the spaces $W^{s,p}(M_0)$, $s \in \mathbb{N} \cup \{0\}$ and $1 \le p \le \infty$, by differentiating with respect to vector fields in $\mathcal{V}$. This definition is in the spirit of the standard definition of Sobolev spaces on $\mathbb{R}^n$. Then we prove that there are two alternative, but equivalent ways to define these Sobolev spaces, either by using a suitable class of partitions of unity (as in [54, 55, 62] for example), or as the domains of the powers of the Laplace operator (for $p = 2$). We also consider these spaces on open subsets $\Omega_0 \subset M_0$. The spaces $W^{s,p}(M_0)$, for $s \in \mathbb{R}$, $1 < p < \infty$ are defined by interpolation and duality or, alternatively, using partitions of unity. In Section 4, we discuss regular open subsets $\Omega \subset M$. In the last two sections, several of the classical results on Sobolev spaces on smooth domains were extended to the spaces $W^{s,p}(M_0)$. These results include the density of smooth, compactly supported functions, the Gagliardo-Nirenberg-Sobolev inequalities, the extension theorem, the trace theorem, the characterization of the range of the trace map in the Hilbert space case ($p = 2$), and the Rellich-Kondrachov compactness theorem.
In Section 5 we include as an application a regularity result for strongly elliptic boundary value problems, Theorem 5.1. This theorem gives right away the following result, proved in Section 6, which states that there is no loss of regularity for these problems within weighted Sobolev spaces.

Theorem 0.1. *Let $\mathbb{P} \subset \mathbb{R}^3$ be a polyhedral domain and P be a strongly elliptic, second order differential operator with coefficients in $\mathcal{C}^\infty(\overline{\mathbb{P}})$. Let $u \in \mathcal{K}^1_{a+1}(\mathbb{P})$, $u = 0$ on $\partial\mathbb{P}$, $a \in \mathbb{R}$. If $Pu \in \mathcal{K}^{m-1}_{a-1}(\mathbb{P})$, then $u \in \mathcal{K}^{m+1}_{a+1}(\mathbb{P})$ and there exists $C > 0$ independent of u such that*

$$\|u\|_{\mathcal{K}^{m+1}_{a+1}(\mathbb{P})} \le C\big(\|Pu\|_{\mathcal{K}^{m-1}_{a-1}(\mathbb{P})} + \|u\|_{\mathcal{K}^{0}_{a+1}(\mathbb{P})}\big), \quad m \in \mathbb{N} \cup \{0\}.$$

The same result holds for strongly elliptic systems.

Note that the above theorem does not constitute a Fredholm (or normal solvability) result, because the inclusion $\mathcal{K}^{m+1}_{a+1}(\mathbb{P}) \to \mathcal{K}^0_{a+1}(\mathbb{P})$ is *not compact.* See also [25, 26, 35, 46] and the references therein for similar results.
In Section 7, we obtain a "non-standard boundary value problem" on a smooth domain $\mathcal{O}$ in weighted Sobolev spaces with weight given by the distance to the boundary. The boundary conditions are thus replaced by growth conditions. Finally, in the last section, Section 8, we obtain mapping properties for the pseudodifferential calculus $\Psi^\infty_{\mathcal{V}}(M)$ defined in [3] between our weighted Sobolev spaces $\rho^s W^{r,p}(M)$. We also obtain a general elliptic regularity result for elliptic pseudodifferential operators in $\Psi^\infty_{\mathcal{V}}(M)$.

Acknowledgements: We would like to thank Anna Mazzucato and Robert Lauter for useful comments. The first named author wants to thank MSRI, Berkeley, CA for its hospitality.

1. Lie manifolds

As explained in the Introduction, our approach to the study of weighted Sobolev spaces on polyhedral domains is based on their relation to Sobolev spaces on Lie manifolds with true boundary. Before we recall the definition of a Lie manifold and some of their basic properties, we shall first look at the following example, which is one of the main motivations for the theory of Lie manifolds.

Example 1.1. Let us take a closer look at the local structure of the Sobolev space $\mathcal{K}^m_a(\mathbb{P})$ associated to a polygon $\mathbb{P}$ (recall (2)). Consider $\Omega := \{(r,\theta) \,|\, 0 < \theta < \alpha\}$, which models an angle of $\mathbb{P}$. Then the distance to the vertex is simply $\vartheta(x) = r$, and the *weighted Sobolev spaces* associated to Ω, $\mathcal{K}^m_a(\Omega)$, can alternatively be described as

(6) $$\mathcal{K}^m_a(\Omega) = \mathcal{K}^m_a(\Omega;\vartheta) := \{u \in L^2_{loc}(\Omega),\ r^{-a}(r\partial_r)^i\partial^j_\theta u \in L^2(\Omega),\ \ i+j \leq m\}.$$

The point of the definition of the spaces $\mathcal{K}^m_a(\Omega)$ was the replacement of the local basis $\{r\partial_x, r\partial_y\}$ with the local basis $\{r\partial_r, \partial_\theta\}$ that is easier to work with on the desingularization $\Sigma(\Omega) := [0,\infty)\times[0,\alpha] \ni (r,\theta)$ of Ω. By further writing $r = e^t$, the vector field $r\partial_r$ becomes ∂_t. Since $dt = r^{-1}dr$, the space $\mathcal{K}^m_1(\Omega)$ then identifies with $H^m(\mathbb{R}_t \times (0,\alpha))$. The weighted Sobolev space $\mathcal{K}^m_1(\Omega)$ has thus become a classical Sobolev space on the cylinder $\mathbb{R}\times(0,\alpha)$, as in [25].

The aim of the following definitions is to define such a desingularisation in general. The desingularisation will carry the structure of a Lie manifold, defined in the next subsection.
We shall introduce a further, related definition, namely the definition of a "Lie submanifolds of a Lie manifold" in Section 4.

1.1. Definition of Lie manifolds.

At first, we want to recall the definition of manifolds with corners. A *manifold with corners* is a closed subset M of a differentiable manifold such that every point $p \in M$ lies in a coordinate chart whose restriction to M is a diffeomorphism to $[0,\infty)^k \times \mathbb{R}^{n-k}$, for some $k = 0, 1, \ldots, n$ depending on p. Obviously, this definition includes the property

that the transition map of two different charts are smooth up to the boundary. If $k = 0$ for all $p \in M$, we shall say that M is a *smooth manifold.* If $k \in \{0, 1\}$, we shall say that M is a *smooth manifold with smooth boundary.*
Let M be a *compact* manifold with corners. We shall denote by ∂M the union of all boundary faces of M, that is, ∂M is the union of all points not having a neighborhood diffeomorphic to $\mathbb{R}^n$. Furthermore, we shall write $M_0 := M \smallsetminus \partial M$ for the *interior* of M. In order to avoid confusion, we shall use this notation and terminology only when M is compact. Note that our definition allows ∂M to be a smooth manifold, possibly empty.
As we shall see below, a Lie manifold is described by a Lie algebra of vector fields satisfying certain conditions. We now discuss some of these conditions.

Definition 1.2. A subspace $\mathcal{V} \subseteq \Gamma(M; TM)$ of the Lie algebra of all smooth vector fields on M is said to be a *structural Lie algebra of vector fields on M* provided that the following conditions are satisfied:

(i) $\mathcal{V}$ is closed under the Lie bracket of vector fields;
(ii) every $V \in \mathcal{V}$ is tangent to all boundary hyperfaces of M;
(iii) $\mathcal{C}^\infty(M)\mathcal{V} = \mathcal{V}$; and
(iv) each point $p \in M$ has a neighborhood U_p such that

$$\mathcal{V}_{U_p} := \{X|_{\overline{U}_p} \,|X \in \mathcal{V}\} \simeq C^\infty(\overline{U}_p)^k$$

in the sense of $C^\infty(\overline{U}_p)$-modules.

The condition (iv) in the definition above can be reformulated as follows:

(iv') For every $p \in M$, there exist a neighborhood $U_p \subset M$ of p and vector fields $X_1, X_2, \ldots, X_k \in \mathcal{V}$ with the property that, for any $Y \in \mathcal{V}$, there exist functions $f_1, \ldots, f_k \in \mathcal{C}^\infty(M)$, uniquely determined on U_p, such that

$$Y = \sum_{j=1}^{k} f_j X_j \quad \text{on } U_p. \tag{7}$$

We now have defined the preliminaries for the following important definition.

Definition 1.3. A *Lie structure at infinity* on a smooth manifold M_0 is a pair $(M, \mathcal{V})$, where M is a compact manifold with interior M_0 and $\mathcal{V} \subset \Gamma(M; TM)$ is a structural Lie algebra of vector fields on M with the following property: If $p \in M_0$, then any local basis of $\mathcal{V}$ in a neighborhood of p is also a local basis of the tangent space to M_0.

It follows from the above definition that the constant k of Equation (7) equals to the dimension n of M_0.
A *manifold with a Lie structure at infinity* (or, simply, a *Lie manifold*) is a manifold M_0 together with a Lie structure at infinity $(M, \mathcal{V})$ on M_0. We shall sometimes denote a Lie manifold as above by $(M_0, M, \mathcal{V})$, or, simply, by $(M, \mathcal{V})$, because M_0 is determined as the interior of M. (In [4], only the term "manifolds with a Lie structure at infinity" was used.)

Example 1.4. If $F \subset TM$ is a sub-bundle of the tangent bundle of a smooth manifold (so M has no boundary) such that $\mathcal{V}_F := \Gamma(M; F)$ is closed under the Lie bracket, then $\mathcal{V}_F$ is a structural Lie algebra of vector fields. Using the Frobenius theorem it is clear that such vector bundles are exactly the tangent bundles of k-dimensional foliations on M, $k = \operatorname{rank} F$. However, $\mathcal{V}_F$ does not define a Lie structure at infinity, unless $F = TM$.

Remark 1.5. We observe that Conditions (iii) and (iv) of Definition 1.2 are equivalent to the condition that $\mathcal{V}$ be a projective $\mathcal{C}^\infty(M)$-module. Thus, by the Serre-Swan theorem [24], there exists a vector bundle $A \to M$, unique up to isomorphism, such that $\mathcal{V} = \Gamma(M; A)$. Since $\mathcal{V}$ consists of vector fields, that is $\mathcal{V} \subset \Gamma(M; TM)$, we also obtain a natural vector bundle morphism $\varrho_M : A \to TM$, called the *anchor map*. The Condition (ii) of Definition 1.3 is then equivalent to the fact that ϱ_M is an isomorphism $A|_{M_0} \simeq TM_0$ on M_0. We will take this isomorphism to be an identification, and thus we can say that A is *an extension* of TM_0 to M (that is, $TM_0 \subset A$).

1.2. Riemannian metric. Let $(M_0, M, \mathcal{V})$ be a Lie manifold. By definition, a *Riemannian metric on M_0 compatible with the Lie structure at infinity* $(M, \mathcal{V})$ is a metric g_0 on M_0 such that, for any $p \in M$, we can choose the basis $X_1, \dots, X_k$ in Definition 1.2 (iv') (7) to be orthonormal with respect to this metric everywhere on $U_p \cap M_0$. (Note that this condition is a restriction only for $p \in \partial M := M \smallsetminus M_0$.) Alternatively, we will also say that (M_0, g_0) is a *Riemannian Lie manifold*. Any Lie manifold carries a compatible Riemannian metric, and any two compatible metrics are bi-Lipschitz to each other.

Remark 1.6. Using the language of Remark 1.5, g_0 is a compatible metric on M_0 if, and only if, there exists a metric g on the vector bundle $A \to M$ which restricts to g_0 on $TM_0 \subset A$.

The geometry of a Riemannian manifold (M_0, g_0) with a Lie structure $(M, \mathcal{V})$ at infinity has been studied in [4]. For instance, (M_0, g_0) is necessarily complete and, if $\partial M \neq \emptyset$, it is of infinite volume. Moreover, all the covariant derivatives of the Riemannian curvature tensor are bounded. Under additional mild assumptions, we also know that the injectivity radius is bounded from below by a positive constant, i. e., (M_0, g_0) is of bounded geometry. (A *manifold with bounded geometry* is a Riemannian manifold with positive injectivity radius and with bounded covariant derivatives of the curvature tensor, see [54] and references therein).

On a Riemannian Lie manifold $(M_0, M, \mathcal{V}, g_0)$, the exponential map $\exp : TM_0 \to M_0$ is well-defined for all $X \in TM_0$ and extends to a differentiable map $\exp : A \to M$. A convenient way to introduce the exponential map is via the geodesic spray, as done in [4]. Similarly, any vector field $X \in \mathcal{V} = \Gamma(M; A)$ is integrable and will map any (connected) boundary face of M to itself. The resulting diffeomorphism of M_0 will be denoted ψ_X.

1.3. Examples. We include here two examples of Lie manifolds together with compatible Riemannian metrics. The reader can find more examples in [4, 31].

Examples 1.7.

(a) Take $\mathcal{V}_b$ to be the set of all vector fields tangent to all faces of a manifold with corners M. Then $(M, \mathcal{V}_b)$ is a Lie manifold. This generalizes Example 1.1. See also Subsection 1.6 and Section 6. Let $r \geq 0$ to be a smooth function on M that is equal to the distance to the boundary in a neighborhood of ∂M, and is > 0 outside ∂M (i. e., on M_0). Let h be a smooth metric on M, then $g_0 = h + (r^{-1}dr)^2$ is a compatible metric on M_0.

(b) Take $\mathcal{V}_0$ to be the set of all vector fields vanishing on all faces of a manifold with corners M. Then $(M, \mathcal{V}_0)$ is a Lie manifold. If ∂M is a smooth manifold (i. e., if M is a smooth manifold with boundary), then $\mathcal{V}_0 = r\Gamma(M; TM)$, where r is as in (a).

1.4. $\mathcal{V}$-differential operators. We are especially interested in the analysis of the differential operators generated using only derivatives in $\mathcal{V}$. Let $\mathrm{Diff}^*_{\mathcal{V}}(M)$ be the algebra of differential operators on M generated by multiplication with functions in $\mathcal{C}^\infty(M)$ and by differentiation with vector fields $X \in \mathcal{V}$. The space of order m differential operators in $\mathrm{Diff}^*_{\mathcal{V}}(M)$ will be denoted $\mathrm{Diff}^m_{\mathcal{V}}(M)$. A differential operator in $\mathrm{Diff}^*_{\mathcal{V}}(M)$ will be called a $\mathcal{V}$-differential operator.

We can define $\mathcal{V}$-differential operators acting between sections of smooth vector bundles $E, F \to M$, $E, F \subset M \times \mathbb{C}^N$ by

$$\mathrm{Diff}^*_{\mathcal{V}}(M; E, F) := e_F M_N(\mathrm{Diff}^*_{\mathcal{V}}(M)) e_E \,, \tag{8}$$

where $M_N(\mathrm{Diff}^*_{\mathcal{V}}(M))$ is the algebra of $N \times N$-matrices over the ring $\mathrm{Diff}^*_{\mathcal{V}}(M)$, and where $e_E, e_F \in M_N(\mathcal{C}^\infty(M))$ are the projections onto E and, respectively, onto F. It follows that $\mathrm{Diff}^*_{\mathcal{V}}(M; E) := \mathrm{Diff}^*_{\mathcal{V}}(M; E, E)$ is an algebra. It is also closed under taking adjoints of operators in $L^2(M_0)$, where the volume form is defined using a compatible metric g_0 on M_0.

1.5. Regular open sets. *We assume from now on that* $r_{\mathrm{inj}}(M_0)$*, the injectivity radius of* (M_0, g_0)*, is positive.*

One of the main goals of this paper is to prove the results on weighted Sobolev spaces on polyhedral domains that are needed for regularity theorems. We shall do that by reducing the study of weighted Sobolev spaces to the study of Sobolev spaces on "regular open subsets" of Lie manifolds, a class of open sets that plays in the framework of Lie manifolds the role played by domains with smooth boundaries in the framework of bounded, open subsets of $\mathbb{R}^n$. Regular open subsets are defined below in this subsection.

Let $N \subset M$ be a submanifold of codimension one of the Lie manifold $(M, \mathcal{V})$. Note that this implies that N is a closed subset of M. We shall say that N is a *regular* submanifold of $(M, \mathcal{V})$ if we can choose a neighborhood V of N in M and a compatible metric g_0 on M_0 that restricts to a product-type metric on $V \cap M_0 \simeq (\partial N_0) \times (-\varepsilon_0, \varepsilon_0)$, $N_0 = N \smallsetminus \partial N = N \cap M_0$. Such neighborhoods will be called *tubular neighborhoods*.

In Section 2, we shall show that a codimension one manifold is regular if, and only if, it is a tame submanifold of M; this gives an easy, geometric, necessary

and sufficient condition for the regularity of a codimension one submanifold of M. This is relevant, since the study of manifolds with boundary and bounded geometry presents some unexpected difficulties [47].
In the following, it will be important to distinguish properly between the boundary of a topological subset, denoted by $\partial_{\rm top}$, and the boundary in the sense of manifolds with corners, denoted simply by ∂.

Definition 1.8. Let $(M, \mathcal{V})$ be a Lie manifold and $\Omega \subset M$ be an open subset. We shall say that Ω is a *regular open subset* in M if, and only if, Ω is connected, Ω and $\overline{\Omega}$ have the same boundary, $\partial_{\rm top}\Omega$ (in the sense of subsets of the topological space M), and $\partial_{\rm top}\Omega$ is a regular submanifold of M.

Let $\Omega \subset M$ be a regular open subset. Then $\overline{\Omega}$ is a compact manifold with corners. The reader should be aware of the important fact that $\partial_{\rm top}\Omega = \partial_{\rm top}\overline{\Omega}$ is contained in $\partial\overline{\Omega}$, but in general $\partial\overline{\Omega}$ and $\partial_{\rm top}\Omega$ are not equal. The set $\partial_{\rm top}\Omega$ will be called the *true boundary* of $\overline{\Omega}$. Furthermore, we introduce $\partial_\infty\Omega := \partial\overline{\Omega} \cap \partial M$, and call it the *boundary at infinity* of $\overline{\Omega}$. Obviously, one has $\partial\overline{\Omega} = \partial_{\rm top}\overline{\Omega} \cup \partial_\infty\overline{\Omega}$. The true boundary and the boundary at infinity intersect in a (possibly empty) set of codimension ≥ 2. See Figure 1. We will also use the notation $\partial\Omega_0 := \partial_{\rm top}\Omega \cap M_0 = \partial\overline{\Omega} \cap M_0$.

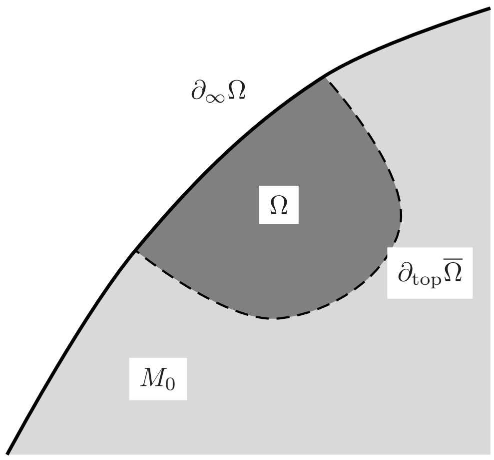


Figure 1. A regular open set Ω. Note that the interior of $\partial_\infty\overline{\Omega}$ is contained in Ω, but the true boundary $\partial_{\rm top}\Omega = \partial_{\rm top}\overline{\Omega}$ is not contained in Ω

The space of restrictions to Ω or $\overline{\Omega}$ of order m differential operators in $\mathrm{Diff}^*_{\mathcal{V}}(M)$ will be denoted $\mathrm{Diff}^m_{\mathcal{V}}(\Omega)$, respectively $\mathrm{Diff}^m_{\mathcal{V}}(\overline{\Omega})$. Similarly, we shall denote by $\mathcal{V}(\Omega)$ the space of restrictions to $\overline{\Omega}$ of vector fields in $\mathcal{V}$, the structural Lie algebra of vector fields on M.
Let $F \subset \partial\Omega$ be any boundary hyperface of $\overline{\Omega}$ of codimension 1. Such a face is either contained in $\partial_{\rm top}\overline{\Omega}$ or in $\partial_\infty\overline{\Omega}$. If $F \subset \partial_\infty\Omega$, then the restrictions of all

vector fields in $\mathcal{V}$ to F are tangent to F. However, if $F \subset \partial_{\text{top}}\overline{\Omega}$ the regularity of the boundary implies that there are vector fields in $\mathcal{V}$ whose restriction to F is not tangent to F. In particular, the true boundary $\partial_{\text{top}}\overline{\Omega}$ of $\overline{\Omega}$ is uniquely determined by $(\overline{\Omega}, \mathcal{V}(\Omega))$, and hence so is $\Omega = \overline{\Omega} \smallsetminus \partial_{\text{top}}\overline{\Omega}$. We therefore obtain a one-to-one correspondence between Lie manifolds with true boundary and regular open subsets (of some Lie manifold M).

Assume we are given Ω, $\overline{\Omega}$ (the closure in M), and $\mathcal{V}(\Omega)$, with Ω a regular open subset of some Lie manifold $(M, \mathcal{V})$. In the cases of interest, for example if $\partial_{\text{top}}\overline{\Omega}$ is a tame submanifold of M (see Subsection 2.3 for the definition of tame submanifolds), we can replace the Lie manifold $(M, \mathcal{V})$ in which Ω is a regular open set with a Lie manifold $(N, \mathcal{W})$ canonically associated to $(\Omega, \overline{\Omega}, \mathcal{V}(\Omega))$ as follows. Let N be obtained by gluing two copies of $\overline{\Omega}$ along $\partial_{\text{top}}\overline{\Omega}$, the so-called *double* of $\overline{\Omega}$, also denoted $\overline{\Omega}^{db} = N$. A smooth vector field X on $\overline{\Omega}^{db}$ will be in $\mathcal{W}$, the structural Lie algebra of vector fields $\mathcal{W}$ on $\overline{\Omega}^{db}$ if, and only if, its restriction to each copy of $\overline{\Omega}$ is in $\mathcal{V}(\Omega)$. Then Ω will be a regular open set of the Lie manifold $(N, \mathcal{W})$. For this reason, the pair $(\overline{\Omega}, \mathcal{V}(\Omega))$ will be called a *Lie manifold with true boundary.* In particular, the true boundary of a Lie manifold with true boundary is a tame submanifold of the double. The fact that the double is a Lie manifold is justified in Remark 2.10.

1.6. Curvilinear polygonal domains. We conclude this section with a discussion of a curvilinear polygonal domain $\mathbb{P}$, an example that generalizes Example 1.1 and is one of the main motivations for considering Lie manifolds. To study function spaces on $\mathbb{P}$, we shall introduce a "desingularization" $(\Sigma(\mathbb{P}), \kappa)$ of $\mathbb{P}$ (or, rather, of $\overline{\mathbb{P}}$), where $\Sigma(\mathbb{P})$ is a compact manifold with corners and $\kappa : \Sigma(\mathbb{P}) \to \overline{\mathbb{P}}$ is a continuous map that is a diffeomorphism from the interior of $\Sigma(\mathbb{P})$ to $\mathbb{P}$ and maps the boundary of $\Sigma(\mathbb{P})$ onto the boundary of $\mathbb{P}$.

Let us denote by B^k the open unit ball in $\mathbb{R}^k$.

Definition 1.9. An open, connected subset $\mathbb{P} \subset M$ of a two dimensional manifold M will be called a *curvilinear polygonal domain* if, by definition, $\overline{\mathbb{P}}$ is compact and for every point $p \in \partial\mathbb{P}$ there exists a diffeomorphism $\phi_p : V_p \to B^2$, $\phi_p(p) = 0$, defined on a neighborhood $V_p \subset M$ such that

$$(9) \quad \phi_j(V_p \cap \mathbb{P}) = \{(r\cos\theta, r\sin\theta),\ 0 < r < 1,\ 0 < \theta < \alpha_p\}, \quad \alpha_p \in (0, 2\pi).$$

A point $p \in \partial\mathbb{P}$ for which $\alpha_p \neq \pi$ will be called a *vertex of* $\mathbb{P}$. The other points of $\partial\mathbb{P}$ will be called *smooth boundary points.* It follows that every curvilinear polygonal domain has finitely many vertices and its boundary consists of a finite union of smooth curves γ_j (called the *edges* of $\mathbb{P}$) which have no other common points except the vertices. Moreover, every vertex belongs to exactly two edges.

Let $\{P_1, P_2, \dots, P_k\} \subset \overline{\mathbb{P}}$ be the vertices of $\mathbb{P}$. The cases $k = 0$ and $k = 1$ are also allowed. Let $V_j := V_{P_j}$ and $\phi_j := \phi_{P_j} : V_j \to B^2$ be the diffeomorphisms defined by Equation (9). Let $(r, \theta) : \mathbb{R}^2 \smallsetminus \{(0,0)\} \to (0, \infty) \times [0, 2\pi)$ be the polar coordinates. We can assume that the sets V_j are disjoint and define $r_j(x) = r(\phi_j(x))$ and $\theta_j(x) = \theta(\phi_j(x))$.

The *desingularization* $\Sigma(\mathbb{P})$ of $\mathbb{P}$ will replace each of the vertices P_j, $j = 1, \dots, k$ of $\mathbb{P}$ with a segment of length $\alpha_j = \alpha_{P_j} > 0$. Assume that $\mathbb{P} \subset \mathbb{R}^2$. We can realize $\Sigma(\mathbb{P})$ in $\mathbb{R}^3$ as follows. Let ψ_j be smooth functions supported on V_j with $\psi_j = 1$ in a neighborhood of P_j.

$$\Phi : \overline{\mathbb{P}} \smallsetminus \{P_1, P_2, \dots, P_k\} \to \mathbb{R}^2 \times \mathbb{R}, \quad \Phi(p) = \big(p\,, \sum_j \psi_j(p)\theta_j(p)\big).$$

Then $\Sigma(\mathbb{P})$ is (up to a diffeomorphism) the closure of $\Phi(\mathbb{P})$ in $\mathbb{R}^3$. The desingularization map is $\kappa(p, z) = p$.

The structural Lie algebra of vector fields $\mathcal{V}(\mathbb{P})$ on $\Sigma(\mathbb{P})$ is given by (the lifts of) the smooth vector fields X on $\overline{\mathbb{P}} \smallsetminus \{P_1, P_2, \dots, P_k\}$ that, on V_j, can be written as

$$X = a_r(r_j, \theta_j) r_j \partial_{r_j} + a_\theta(r_j, \theta_j)\partial_{\theta_j},$$

with a_r and a_θ smooth functions of (r_j, θ_j), $r_j \geq 0$. Then $(\Sigma(\mathbb{P}), \mathcal{V}(\mathbb{P}))$ is a Lie manifold with true boundary.

To define the structural Lie algebra of vector fields on $\Sigma(\mathbb{P})$, we now choose a smooth function $r_{\mathbb{P}} : \mathbb{P} \to [0, \infty)$ with the following properties

(i) $r_{\mathbb{P}}$ is continuous on $\overline{\mathbb{P}}$,
(ii) $r_{\mathbb{P}}$ is smooth on $\mathbb{P}$,
(iii) $r_{\mathbb{P}}(x) > 0$ on $\overline{\mathbb{P}} \smallsetminus \{P_1, P_2, \dots, P_k\}$,
(iv) $r_{\mathbb{P}}(x) = r_j(x)$ if $x \in V_j$.

Note that $r_{\mathbb{P}}$ lifts to a *smooth positive function* on $\Sigma(\mathbb{P})$. Of course, $r_{\mathbb{P}}$ is determined only up to a smooth positive function ψ on $\Sigma(\mathbb{P})$ that equals to 1 in a neighborhood of the vertices.

Definition 1.10. A function of the form $\psi r_{\mathbb{P}}$, with $\psi \in \mathcal{C}^\infty(\Sigma(\mathbb{P}))$, $\psi > 0$ will be called a *canonical weight function of* $\mathbb{P}$.

In what follows, we can replace $r_{\mathbb{P}}$ with any canonical weight function. Canonical weight functions will play an important role again in Section 6. Canonical weights are example of "admissible weights," which will be used to define weighted Sobolev spaces.

Then an alternative definition of $\mathcal{V}(\mathbb{P})$ is

$$\mathcal{V}(\mathbb{P}) := \{\, r_{\mathbb{P}}\,(\psi_1\partial_1 + \psi_2\partial_2)\,\}, \quad \psi_1, \psi_2 \in \mathcal{C}^\infty(\Sigma(\mathbb{P})). \tag{10}$$

Here ∂_1 denotes the vector field corresponding to the derivative with respect to the first component. The vector field ∂_2 is defined analogously. In particular,

$$r_{\mathbb{P}}(\partial_j r_{\mathbb{P}}) = r_{\mathbb{P}} \frac{\partial r_{\mathbb{P}}}{\partial x_j} \in \mathcal{C}^\infty(\Sigma(\mathbb{P})), \tag{11}$$

which is useful in establishing that $\mathcal{V}(\mathbb{P})$ is a Lie algebra. Also, let us notice that both $\{r_{\mathbb{P}}\partial_1, r_{\mathbb{P}}\partial_2\}$ and $\{r_{\mathbb{P}}\partial_{r_{\mathbb{P}}}, \partial_\theta\}$ are local bases for $\mathcal{V}(\mathbb{P})$ on V_j. The transition functions lift to smooth functions on $\Sigma(\mathbb{P})$ defined in a neighborhood of $\kappa^{-1}(P_j)$, but cannot be extended to smooth functions defined in a neighborhood of P_j in $\overline{\mathbb{P}}$.

Then $\partial_{\rm top}\Sigma(\mathbb{P})$, the true boundary of $\Sigma(\mathbb{P})$, consists of the disjoint union of the edges of $\mathbb{P}$ (note that the interiors of these edges have disjoint closures in $\Sigma(\mathbb{P})$). Anticipating the definition of a Lie submanifold in Section 2, let us notice that $\partial_{\rm top}\Sigma(\mathbb{P})$ is a Lie submanifold, where the Lie structure consists of the vector fields on the edges that vanish at the end points of the edges.
The function ϑ used to define the Sobolev spaces $\mathcal{K}_a^m(\mathbb{P}) := \mathcal{K}_a^m(\mathbb{P};\vartheta)$ in Equation (2) is closely related to the function $r_{\mathbb{P}}$. Indeed, $\vartheta(x)$ is the distance from x to the vertices of $\mathbb{P}$. Therefore $\vartheta/r_{\mathbb{P}}$ will extend to a continuous, nowhere vanishing function on $\Sigma(\mathbb{P})$, which shows that

$$\mathcal{K}_a^m(\mathbb{P};\vartheta) = \mathcal{K}_a^m(\mathbb{P};r_{\mathbb{P}}). \tag{12}$$

If P is an order m differential operator with smooth coefficients on $\mathbb{R}^2$ and $\mathbb{P} \subset \mathbb{R}^2$ is a polygonal domain, then $r_{\mathbb{P}}^m P \in \mathrm{Diff}_{\mathcal{V}}^m(\Sigma(\mathbb{P}))$, by Equation (10). However, in general, $r_{\mathbb{P}}^m P$ will not define a smooth differential operator on $\overline{\mathbb{P}}$.

2. SUBMANIFOLDS

In this section we introduce various classes of submanifolds of a Lie manifold. Some of these classes were already mentioned in the previous sections.

2.1. GENERAL SUBMANIFOLDS. We first introduce the most general class of submanifolds of a Lie manifold.
We first fix some notation. Let $(M_0, M, \mathcal{V})$ and $(N_0, N, \mathcal{W})$ be Lie manifolds. We know that there exist vector bundles $A \to M$ and $B \to N$ such that $\mathcal{V} \simeq \Gamma(M;A)$ and $\mathcal{W} \simeq \Gamma(N;B)$, see Remark 1.5. We can assume that $\mathcal{V} = \Gamma(M;A)$ and $\mathcal{W} = \Gamma(N;B)$ and write (M,A) and (N,B) instead of $(M_0, M, \mathcal{V})$ and $(N_0, N, \mathcal{W})$.

DEFINITION 2.1. Let (M,A) be a Lie manifold with anchor map $\varrho_M : A \to TM$. A Lie manifold (N,B) is called a *Lie submanifold* of (M,A) if

(i) N is a closed submanifold of M (possibly with corners, no transversality at the boundary required),
(ii) $\partial N = N \cap \partial M$ (that is, $N_0 \subset M_0$, $\partial N \subset \partial M$), and
(iii) B is a sub vector bundle of $A|_N$, and
(iv) the restriction of ϱ_M to B is the anchor map of $B \to N$.

Remark 2.2. An alternative form of Condition (iv) of the above definition is

$$\begin{aligned} \mathcal{W} = \Gamma(N;B) &= \{X|_N \mid X \in \Gamma(M;A) \text{ and } X|_N \text{ tangent to } N\} \\ &= \{X \in \Gamma(N;A|_N) \mid \varrho_M \circ X \in \Gamma(N;TN)\}. \end{aligned} \tag{13}$$

We have the following simple corollary that justifies Condition (iv) of Definition 2.1.

COROLLARY 2.3. *Let g_0 be a metric on M_0 compatible with the Lie structure at infinity on M_0. Then the restriction of g_0 to N_0 is compatible with the Lie structure at infinity on N_0.*

Proof. Let g be a metric on A whose restriction to TM_0 defines the metric g_0. Then g restricts to a metric h on B, which in turn defines a metric h_0 on N_0. By definition, h_0 is the restriction of g_0 to N_0. □

We thus see that any submanifold (in the sense of the above definition) of a Riemannian Lie manifold is itself a Riemannian Lie manifold.

2.2. Second fundamental form. We define the A-*normal bundle* of the Lie submanifold (N, B) of the Lie manifold (M, A) as $\nu^A = (A|_N)/B$ which is a bundle over N. Then the anchor map ϱ_M defines a map $\nu^A \to (TM|_N)/TN$, called the *anchor map of* ν^A, which is an isomorphism over N_0.
We denote the Levi-Civita-connection on A by ∇^A and the Levi-Civita connection on B by ∇^B [4]. Let $X, Y, Z \in \mathcal{W} = \Gamma(N; B)$ and $\tilde{X}, \tilde{Y}, \tilde{Z} \in \mathcal{V} = \Gamma(M; A)$ be such that $X = \tilde{X}|_N$, $Y = \tilde{Y}|_N$, $Z = \tilde{Z}|_N$. Then $\nabla^A_{\tilde{X}} \tilde{Y}|_N$ depends only on $X, Y \in \mathcal{W} = \Gamma(N; B)$ and will be denoted $\nabla^A_X Y$ in what follows. Furthermore, the Koszul formula gives

$$\begin{aligned}
2g(\tilde{Z}, \nabla^A_{\tilde{Y}} \tilde{X}) =& \partial_{\varrho_M(\tilde{X})} g(\tilde{Y}, \tilde{Z}) + \partial_{\varrho_M(\tilde{Y})} g(\tilde{Z}, \tilde{X}) - \partial_{\varrho_M(\tilde{Z})} g(\tilde{X}, \tilde{Y}) \\
& - g([\tilde{X}, \tilde{Z}], \tilde{Y}) - g([\tilde{Y}, \tilde{Z}], \tilde{X}) - g([\tilde{X}, \tilde{Y}], \tilde{Z}), \\
2g(Z, \nabla^B_Y X) =& \partial_{\varrho_M(X)} g(Y, Z) + \partial_{\varrho_M(Y)} g(Z, X) - \partial_{\varrho_M(Z)} g(X, Y) \\
& - g([X, Z], Y) - g([Y, Z], X) - g([X, Y], Z).
\end{aligned}$$

As this holds for arbitrary sections Z of $\Gamma(N; B)$ with extensions $\tilde{Z}$ on $\Gamma(M; A)$, we see that $\nabla^B_X Y$ is the tangential part of $\nabla^A_X Y|_N$.
The normal part of ∇^A then gives rise to the *second fundamental form* II defined as

$$\mathrm{II} : \mathcal{W} \times \mathcal{W} \to \Gamma(\nu^A), \quad \mathrm{II}(X, Y) := \nabla^A_X Y - \nabla^B_X Y.$$

The Levi-Civita connections ∇^A and ∇^B are torsion free, and hence II is symmetric because

$$\mathrm{II}(X, Y) - \mathrm{II}(Y, X) = [\tilde{X}, \tilde{Y}]|_N - [X, Y] = 0.$$

A direct computation reveals also that $\mathrm{II}(X, Y)$ is tensorial in X, and hence, because of the symmetry, it is also tensorial in Y. ("Tensorial" here means $\mathrm{II}(fX, Y) = f\mathrm{II}(X, Y) = \mathrm{II}(X, fY)$, as usual.) Therefore the second fundamental form is a vector bundle morphism $\mathrm{II} : B \otimes B \to \nu^A$, and the endomorphism at $p \in M$ is denoted by $\mathrm{II}_p : B_p \otimes B_p \to A_p$. It then follows from the compactness of N that

$$\|\mathrm{II}_p(X_p, Y_p)\| \le C \|X_p\| \, \|Y_p\|,$$

with a constant C independent of $p \in N$. Clearly, on the interior $N_0 \subset M_0$ the second fundamental form coincides with the classical second fundamental form.

Corollary 2.4. *Let (N, B) be a submanifold of (M, A) with a compatible metric. Then the (classical) second fundamental form of N_0 in M_0 is uniformly bounded.*

2.3. Tame submanifolds. We now introduce tame manifolds. Our main interest in tame manifolds is the global tubular neighborhood theorem, Theorem 2.7, which asserts that a tame submanifold of a Lie manifold has a tubular neighborhood in a strong sense. In particular, we will obtain that a tame submanifold of codimension one is regular. This is interesting because being tame is an algebraic condition that can be easily verified by looking at the structural Lie algebras of vector fields. On the other hand, being a regular submanifold is an analytic condition on the metric that may be difficult to check directly.

Definition 2.5. Let (N, B) be a Lie submanifold of the Lie manifold (M, A) with anchor map $\varrho_M : A \to TM$. Then (N, B) is called a *tame submanifold of* M if T_pN and $\varrho_M(A_p)$ span T_pM for all $p \in \partial N$.

Let (N, B) be a tame submanifold of the Lie manifold (M, A). Then the anchor map $\varrho_M : A \to TM$ defines an isomorphism from A_p/B_p to T_pM/T_pN for any $p \in N$. In particular, the anchor map ϱ_M maps $B^\perp$, the orthogonal complement of B in A, injectively into $\varrho_M(A) \subset TM$. For any boundary face F and $p \in F$ we have $\varrho_M(A_p) \subset T_pF$. Hence, for any $p \in N \cap F$, the space T_pM is spanned by T_pN and T_pF. As a consequence, $N \cap F$ is a submanifold of F of codimension $\dim M - \dim N$. The codimension of $N \cap F$ in F is therefore independent of F, in particular independent of the dimension of F.

Examples 2.6.
(1) Let M be any compact manifold (without boundary). Fix a $p \in M$. Let (N, B) be a manifold with a Lie structure at infinity. Then $(N_0 \times \{p\}, N \times \{p\}, B)$ is a tame submanifold of $(N_0 \times M, N \times M, B \times TM)$.
(2) If $\partial N \neq \emptyset$, the diagonal N is a submanifold of $N \times N$, but not a tame submanifold.
(3) Let N be a submanifold with corners of M such that N is transverse to all faces of M. We endow these manifolds with the b-structure at infinity $\mathcal{V}_b$ (see Example 1.7 (i)). Then $(N, \mathcal{V}_b)$ is a tame Lie submanifold of $(M, \mathcal{V}_b)$.
(4) A regular submanifold (see section 1) is a also a tame submanifold.

We now prove the main theorem of this section. Note that this theorem is not true for a general manifold of bounded geometry with boundary (for a manifold with bounded geometry and boundary, the existence of a global tubular neighborhood of the boundary is part of the definition, see [47]).

Theorem 2.7 (Global tubular neighborhood theorem). *Let (N, B) be a tame submanifold of the Lie manifold (M, A). For $\epsilon > 0$, let $(\nu^A)_\epsilon$ be the set of all vectors normal to N of length smaller than ϵ. If $\epsilon > 0$ is sufficiently small, then the normal exponential map* $\exp^\nu$ *defines a diffeomorphism from $(\nu^A)_\epsilon$ to an open neighborhood V_ϵ of N in M. Moreover, dist*$(\exp^\nu(X), N) = |X|$ *for* $|X| < \epsilon$.

Proof. Recall from [4] that the exponential map $\exp : TM_0 \to M_0$ extends to a map $\exp : A \to M$. The definition of the normal exponential function $\exp^\nu$ is obtained by identifying the quotient bundle ν^A with $B^\perp$, as discussed earlier.

This gives

$$\exp^\nu : (\nu^A)_\epsilon \to M.$$

The differential $d\exp^\nu$ at $0_p \in \nu^A_p$, $p \in N$ is the restriction of the anchor map to $B^\perp \cong \nu^A$, hence any point $p \in N$ has a neighborhood $U(p)$ and $\tau_p > 0$ such that

$$\exp^\nu : (\nu^A)_{\tau_p}|_{U_p} \to M \tag{14}$$

is a diffeomorphism onto its image. By compactness $\tau_p \geq \tau > 0$. Hence, $\exp^\nu$ is a local diffeomorphism of $(\nu^A)_\tau$ to a neighborhood of N in M. It remains to show that it is injective for small $\epsilon \in (0, \tau)$.

Let us assume now that there is no $\epsilon > 0$ such that the theorem holds. Then there are sequences $X_i, Y_i \in \nu^A$, $i \in \mathbb{N}$, $X_i \neq Y_i$ such that $\exp^\nu X_i = \exp^\nu Y_i$ with $|X_i|, |Y_i| \to 0$ for $i \to \infty$. After taking a subsequence we can assume that the basepoints p_i of X_i converge to p_∞ and the basepoints q_i of Y_i converge to q_∞. As the distance in M of p_i and q_i converges to 0, we conclude that $p_\infty = q_\infty$. However, $\exp^\nu$ is a diffeomorphism from $(\nu^A)_\tau|_{U(p_\infty)}$ into a neighborhood of $U(p_\infty)$. Hence, we see that $X_i = Y_i$ for large i, which contradicts the assumptions. □

We now prove that every tame codimension one Lie submanifold is regular.

Proposition 2.8. *Let (N, B) be a tame submanifold of codimension one of (M, A). We fix a unit length section X of ν^A. Theorem 2.7 states that*

$$\begin{array}{rcl} \exp^\nu : (\nu^A)_\epsilon \cong N \times (-\epsilon, \epsilon) & \to & \{x \mid d(x, N) < \epsilon\} =: V_\epsilon \\ (p, t) & \mapsto & \exp\big(tX(p)\big) \end{array}$$

is a diffeomorphism for small $\epsilon > 0$. Then M_0 carries a compatible metric g_0 such that $(\exp^\nu)^* g_0$ is a product metric, i. e., $(\exp^\nu)^* g_0 = g_N + dt^2$ on $N \times (-\epsilon/2, \epsilon/2)$.

Proof. Choose any compatible metric g_1 on M_0. Let g_2 be a metric on U_ϵ such that $(\exp^\nu)^* g_2 = g_1|_N + dt^2$ on $N \times (-\epsilon, \epsilon)$. Let $d(x) := dist(x, N)$. Then

$$g_0 = (\chi \circ d)\, g_1 + (1 - \chi \circ d)\, g_2,$$

has the desired properties, where the cut-off function $\chi : \mathbb{R} \to [0, 1]$ is 1 on $(-\epsilon/2, \epsilon/2)$ and has support in $(-\epsilon, \epsilon)$, and satisfies $\chi(-t) = \chi(t)$. □

The above definition shows that any tame submanifold of codimension 1 is a regular submanifold. Hence, the concept of a tame submanifold of codimension 1 is the same as that of a regular submanifolds. We hence obtain a new criterion for deciding that a given domain in a Lie manifold is regular.

Proposition 2.9. *Assume the same conditions as the previous proposition. Then $d\exp^\nu\left(\frac{\partial}{\partial t}\right)$ defines a smooth vector field on $V_{\epsilon/2}$. This vector field can be extended smoothly to a vector field Y in $\mathcal{V}$. The restriction of A to $V_{\epsilon/2}$ splits in the sense of smooth vector bundles as $A = A_1 \oplus A_2$ where $A_1|_N = \nu^A$ and $A_2|_N = B$. This splitting is parallel in the direction of Y with respect to the*

Levi-Civita connection of the product metric g_0, i.e. if Z is a section of A_i, then $\nabla_Y Z$ is a section of A_i as well.

Proof. Because of the injectivity of the normal exponential map, the vector field $Y_1 := d\exp^\nu\left(\frac{\partial}{\partial t}\right)$ is well-defined, and the diffeomorphism property implies smoothness on V_ϵ. At first, we want to argue that $Y_1 \in \mathcal{V}(V_\epsilon)$. Let $\pi : S(A) \to M$ be the bundle of unit length vectors in A. Recall from [4], section 1.2 that $S(A)$ is naturally a Lie manifold, whose Lie structure is given by the *thick pullback* $\pi^\#(A)$ of A. Now the flow lines of Y_1 are geodesics, which yield in coordinates solutions to a second order ODE in t. In [4], section 3.4 this ODE was studied on Lie manifolds. The solutions are integral lines of the geodesic spray $\sigma : S(A) \to f^\#(A)$. As the integral lines of this flow stay in $S(A) \subset A$ and as they depend smoothly on the initial data and on t, we see that Y_1 is a smooth section of constant length one of $A|_{V_\epsilon}$.
Multiplying with a suitable cutoff-function with support in V_ϵ one sees that we obtain the desired extension $Y \in \mathcal{V}$. Using parallel transport in the direction of Y, the splitting $A|_N = \nu^A \oplus TN$ extends to a small neighborhood of N. This splitting is clearly parallel in the direction of Y. □

Remark 2.10. Let $N \subset M$ be a tame submanifold of the Lie manifold $(M, \mathcal{V})$ and $Y \in \mathcal{V}$ as above. If Y has length one in a neighborhood of N and is orthogonal to N, then $V := \bigcup_{|t|<\epsilon} \phi_t(N)$ will be a tubular neighborhood of N. According to the previous proposition the restriction of $A \to M$ to V has a natural product type decomposition. This justifies, in particular, that the double of a Lie manifold with boundary is again a Lie manifold, and that the Lie structure defined on the double satisfies the natural compatibility conditions with the Lie structure on a Lie manifold with boundary.

3. Sobolev spaces

In this section we study Sobolev spaces on Lie manifolds without boundary. These results will then be used to study Sobolev spaces on Lie manifolds with true boundary, which in turn, will be used to study weighted Sobolev spaces on polyhedral domains. The goal is to extend to these classes of Sobolev spaces the main results on Sobolev spaces on smooth domains.

Conventions. *Throughout the rest of this paper, $(M_0, M, \mathcal{V})$ will be a fixed Lie manifold. We also fix a compatible metric g on M_0, i. e., a metric compatible with the Lie structure at infinity on M_0, see Subsection 1.2. To simplify notation we denote the compatible metric by g instead of the previously used g_0. By Ω we shall denote an open subset of M and $\Omega_0 = \Omega \cap M_0$. The letters C and c will be used to denote possibly different constants that may depend only on (M_0, g) and its Lie structure at infinity $(M, \mathcal{V})$.*

We shall denote the volume form (or measure) on M_0 associated to g by $d\,\mathrm{vol}_g(x)$ or simply by dx, when there is no danger of confusion. Also, we shall denote by $L^p(\Omega_0)$ the resulting L^p-space on Ω_0 (i. e., defined with respect to the volume form dx). These spaces are independent of the choice of the compatible metric g on M_0, but their norms, denoted by $\| \cdot \|_{L^p}$, do depend upon this choice, although this is not reflected in the notation. Also, we shall use the fixed metric g on M_0 to trivialize all density bundles. Then the space $\mathcal{D}'(\Omega_0)$ of distributions on Ω_0 is defined, as usual, as the dual of $\mathcal{C}^\infty_{\mathrm{c}}(\Omega_0)$. The spaces $L^p(\Omega_0)$ identify with spaces of distributions on Ω_0 via the pairing

$$\langle u, \phi\rangle = \int_{\Omega_0} u(x)\phi(x)dx, \quad \text{where } \phi \in \mathcal{C}^\infty_{\mathrm{c}}(\Omega_0) \text{ and } u \in L^p(\Omega_0).$$

3.1. Definition of Sobolev spaces using vector fields and connections. We shall define the Sobolev spaces $W^{s,p}(\Omega_0)$ in the following two cases:

- $s \in \mathbb{N} \cup \{0\}$, $1 \leq p \leq \infty$, and arbitrary open sets Ω_0 or
- $s \in \mathbb{R}$, $1 < p < \infty$, and $\Omega_0 = M_0$.

We shall denote $W^{s,p}(\Omega) = W^{s,p}(\Omega_0)$ and $W^{s,p}(M) = W^{s,p}(M_0)$. If Ω is a regular open set, then $W^{s,p}(\overline{\Omega}) = W^{s,p}(\Omega_0)$. In the case $p = 2$, we shall often write H^s instead of $W^{s,2}$. We shall give several definitions for the spaces $W^{s,p}(\Omega_0)$ and show their equivalence. This will be crucial in establishing the equivalence of various definitions of weighted Sobolev spaces on polyhedral domains. The first definition is in terms of the Levi-Civita connection ∇ on TM_0. We shall denote also by ∇ the induced connections on tensors (i. e., on tensor products of TM_0 and T^*M_0).

Definition 3.1 (∇-definition of Sobolev spaces). The Sobolev space $W^{k,p}(\Omega_0)$, $k \in \mathbb{N} \cup \{0\}$, is defined as the space of distributions u on $\Omega_0 \subset M_0$ such that

$$\|u\|^p_{\nabla, W^{k,p}} := \sum_{l=1}^{k} \int_{\Omega_0} |\nabla^l u(x)|^p dx < \infty\,, \quad 1 \leq p < \infty. \tag{15}$$

For $p = \infty$ we change this definition in the obvious way, namely we require that,

$$\|u\|_{\nabla, W^{k,\infty}} := \sup |\nabla^l u(x)| < \infty\,, \quad 0 \leq l \leq k. \tag{16}$$

We introduce an alternative definition of Sobolev spaces.

Definition 3.2 (vector fields definition of Sobolev spaces). Let again $k \in \mathbb{N} \cup \{0\}$. Choose a finite set of vector fields $\mathcal{X}$ such that $\mathcal{C}^\infty(M)\mathcal{X} = \mathcal{V}$. This condition is equivalent to the fact that the set $\{X(p), X \in \mathcal{X}\}$ generates A_p linearly, for any $p \in M$. Then the system $\mathcal{X}$ provides us with the norm

$$\|u\|^p_{\mathcal{X}, W^{k,p}} := \sum \|X_1 X_2 \ldots X_l u\|^p_{L^p}\,, \quad 1 \leq p < \infty, \tag{17}$$

the sum being over all possible choices of $0 \leq l \leq k$ and all possible choices of not necessarily distinct vector fields $X_1, X_2, \ldots, X_l \in \mathcal{X}$. For $p = \infty$, we change this definition in the obvious way:

$$\|u\|_{\mathcal{X}, W^{k,\infty}} := \max \|X_1 X_2 \ldots X_l u\|_{L^\infty}\,, \tag{18}$$

the maximum being taken over the same family of vector fields.

In particular,

$$W^{k,p}(\Omega_0) = \{u \in L^p(\Omega_0),\ Pu \in L^p(\Omega_0),\ \text{for all } P \in \mathrm{Diff}^k_{\mathcal{V}}(M)\} \tag{19}$$

Sometimes, when we want to stress the Lie structure $\mathcal{V}$ on M, we shall write $W^{k,p}(\Omega_0; M, \mathcal{V}) := W^{k,p}(\Omega_0)$.

Example 3.3. Let $\mathbb{P}$ be a curvilinear polygonal domain in the plane and let $\Sigma(\mathbb{P})^{db}$ be the "double" of $\Sigma(\mathbb{P})$, which is a Lie manifold without boundary (see Subsection 1.6). Then $\mathbb{P}$ identifies with a regular open subset of $\Sigma(\mathbb{P})^{db}$, and we have

$$\mathcal{K}_1^m(\mathbb{P}) = W^{m,2}(\mathbb{P}) = W^{m,2}(\mathbb{P}; \Sigma(\mathbb{P})^{db}, \mathcal{V}(\mathbb{P})).$$

The following proposition shows that the second definition yields equivalent norms.

Proposition 3.4. *The norms $\|\cdot\|_{\mathcal{X},W^{k,p}}$ and $\|\cdot\|_{\nabla,W^{k,p}}$ are equivalent for any choice of the compatible metric g on M_0 and any choice of a system of the finite set $\mathcal{X}$ such that $\mathcal{C}^\infty(M)\mathcal{X} = \mathcal{V}$. The spaces $W^{k,p}(\Omega_0)$ are complete Banach spaces in the resulting topology. Moreover, $H^k(\Omega_0) := W^{k,2}(\Omega_0)$ is a Hilbert space.*

Proof. As all compatible metrics g are bi-Lipschitz to each others, the equivalence classes of the $\|\cdot\|_{\mathcal{X},W^{k,p}}$-norms are independent of the choice of g. We will show that for any choice $\mathcal{X}$ and g, $\|\cdot\|_{\mathcal{X},W^{k,p}}$ and $\|\cdot\|_{\nabla,W^{k,p}}$ are equivalent. It is clear that then the equivalence class of $\|\cdot\|_{\mathcal{X},W^{k,p}}$ is independent of the choice of $\mathcal{X}$, and the equivalence class of $\|\cdot\|_{\nabla,W^{k,p}}$ is independent of the choice of g.
We argue by induction in k. The equivalence is clear for $k = 0$. We assume now that the $W^{l,p}$-norms are already equivalent for $l = 0, \ldots, k-1$. Observe that if $X, Y \in \mathcal{V}$, then the Koszul formula implies $\nabla_X Y \in \mathcal{V}$ [4]. To simplify notation, we define inductively $\mathcal{X}^0 := \mathcal{X}$, and $\mathcal{X}^{i+1} = \mathcal{X}^i \cup \{\nabla_X Y \mid X, Y \in \mathcal{X}^i\}$. By definition any $V \in \Gamma(M; T^*M^{\otimes k})$ satisfies $(\nabla\nabla V)(X,Y) = \nabla_X \nabla_Y V - \nabla_{\nabla_X Y} V$. This implies for $X_1, \ldots, X_k \in \mathcal{X}$

$$(\underbrace{\nabla \ldots \nabla f}_{k\text{-times}})(X_1, \ldots, X_k) = X_1 \ldots X_k f + \sum_{l=0}^{k-1} \sum_{Y_j \in \mathcal{X}^{k-l}} a_{Y_1,\ldots,Y_l} Y_1 \ldots Y_l\, f,$$

for appropriate choices of $a_{Y_1,\ldots,Y_l} \in \mathbb{N} \cup \{0\}$. Hence,

$$\|(\underbrace{\nabla \ldots \nabla f}_{k\text{-times}})\|_{L^p} \le C \sum \|\nabla \ldots \nabla f(X_1, \ldots, X_k)\|_{L^p} \le C\|f\|_{\mathcal{X},W^{k,p}}.$$

By induction, we know that $\|Y_1, \dots, Y_l f\|_{L^p} \leq C\|f\|_{\nabla, W^{l,p}}$ for $Y_i \in \mathcal{X}^{k-l}$, $0 \leq l \leq k-1$, and hence

$$\|X_1 \dots X_k f\|_{L^p} \leq \underbrace{\|\nabla \dots \nabla f\|_{L^p} \|X_1\|_{L^\infty} \cdots \|X_k\|_{L^\infty}}_{\leq C\|f\|_{\nabla, W^{k,p}}} + \underbrace{\sum_{l=0}^{k-1} \sum_{Y_1,\dots,Y_l \in \mathcal{X}^{k-l}} a_{Y_1,\dots,Y_l} Y_1 \dots Y_l f}_{\leq C\|f\|_{\nabla, W^{k-1,p}}}.$$

This implies the equivalence of the norms.
The proof of completeness is standard, see for example [16, 60]. □

We shall also need the following simple observation.

Lemma 3.5. *Let $\Omega' \subset \Omega \subset M$ be open subsets, $\Omega_0 = \Omega \cap M_0$, and $\Omega_0' = \Omega' \cap M_0$, $\Omega' \neq \emptyset$. The restriction then defines continuous operators $W^{s,p}(\Omega_0) \to W^{s,p}(\Omega_0')$. If the various choices $(\mathcal{X}, g, x_j)$ are done in the same way on Ω and Ω', then the restriction operator has norm 1.*

3.2. Definition of Sobolev spaces using partitions of unity. Yet another description of the spaces $W^{k,p}(\Omega_0)$ can be obtained by using suitable partitions of unity as in [54, Lemma 1.3], whose definition we now recall. See also [13, 18, 51, 52, 55, 62].

Lemma 3.6. *For any $0 < \epsilon < r_{\text{inj}}(M_0)/6$ there is a sequence of points $\{x_j\} \subset M_0$, and a partition of unity $\phi_j \in \mathcal{C}_c^\infty(M_0)$, such that, for some N large enough depending only on the dimension of M_0), we have*

(i) $\operatorname{supp}(\phi_j) \subset B(x_j, 2\epsilon)$;
(ii) $\|\nabla^k \phi_j\|_{L^\infty(M_0)} \leq C_{k,\epsilon}$, *with $C_{k,\epsilon}$ independent of j; and*
(iii) *the sets $B(x_j, \epsilon/N)$ are disjoint, the sets $B(x_j, \epsilon)$ form a covering of M_0, and the sets $B(x_j, 4\epsilon)$ form a covering of M_0 of finite multiplicity, i. e.,*

$$\sup_{y \in M_0} \#\{x_j \mid y \in B(x_j, 4\epsilon)\} < \infty.$$

Fix $\epsilon \in (0, r_{\text{inj}}(M_0)/6)$. Let $\psi_j : B(x_j, 4\epsilon) \to B_{\mathbb{R}^n}(0, 4\epsilon)$ normal coordinates around x_j (defined using the exponential map $\exp_{x_j} : T_{x_j} M_0 \to M_0$). The uniform bounds on the Riemann tensor R and its derivatives $\nabla^k R$ imply uniform bounds on $\nabla^k d\exp_{x_j}$, which directly implies that all derivatives of ψ_j are uniformly bounded.

Proposition 3.7. *Let ϕ_i and ψ_i be as in the two paragraphs above. Let $U_j = \psi_j(\Omega_0 \cap B(x_j, 2\epsilon)) \subset \mathbb{R}^n$. We define*

$$\nu_{k,\infty}(u) := \sup_j \|(\phi_j u) \circ \psi_j^{-1}\|_{W^{k,\infty}(U_j)}$$

and, for $1 \leq p < \infty$,

$$\nu_{k,p}(u)^p := \sum_j \|(\phi_j u) \circ \psi_j^{-1}\|_{W^{k,p}(U_j)}^p.$$

Then $u \in W^{k,p}(\Omega_0)$ if, and only if, $\nu_{k,p}(u) < \infty$. Moreover, $\nu_{k,p}(u)$ defines an equivalent norm on $W^{k,p}(\Omega_0)$.

Proof. We shall assume $p < \infty$, for simplicity of notation. The case $p = \infty$ is completely similar. Consider then $\mu(u)^p = \sum_j \|\phi_j u\|^p_{W^{k,p}(\Omega_0)}$. Then there exists $C_{k,\varepsilon} > 0$ such that

$$C_{k,\varepsilon}^{-1}\|u\|_{W^{k,p}(\Omega_0)} \leq \mu(u) \leq C_{k,\varepsilon}\|u\|_{W^{k,p}(\Omega_0)}, \tag{20}$$

for all $u \in W^{k,p}(\Omega_0)$, by Lemma 3.6 (i. e., the norms are equivalent). The fact that all derivatives of $\exp_{x_j}$ are bounded uniformly in j further shows that μ and $\nu_{k,p}$ are also equivalent. □

The proposition gives rise to a third, equivalent definition of Sobolev spaces. This definition is similar to the ones in [54, 55, 62, 61] and can be used to define the spaces $W^{s,p}(\Omega_0)$, for any $s \in \mathbb{R}$, $1 < p < \infty$, and $\Omega_0 = M_0$. The cases $p = 1$ or $p = \infty$ are more delicate and we shall not discuss them here.
Recall that the spaces $W^{s,p}(\mathbb{R}^n)$, $s \in \mathbb{R}$, $1 < p < \infty$ are defined using the powers of $1 + \Delta$, see [56, Chapter V] or [60, Section 13.6].

Definition 3.8 (Partition of unity definition of Sobolev spaces). Let $s \in \mathbb{R}$, and $1 < p < \infty$. Then we define

$$\|u\|^p_{W^{s,p}(M_0)} := \sum_j \|(\phi_j u) \circ \psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)}, \quad 1 < p < \infty. \tag{21}$$

By Proposition 3.7, this norm is equivalent to our previous norm on $W^{s,p}(M_0)$ when s is a nonnegative integer.

Proposition 3.9. *The space $\mathcal{C}^\infty_c(M_0)$ is dense in $W^{s,p}(M_0)$, for $1 < p < \infty$ and $s \in \mathbb{R}$, or $1 \leq p < \infty$ and $s \in \mathbb{N} \cup \{0\}$.*

Proof. For $s \in \mathbb{N} \cup \{0\}$, the result is true for any manifold with bounded geometry, see [7, Theorem 2] or [19, Theorem 2.8], or [20]. For $\Omega_0 = M_0$, $s \in \mathbb{R}$, and $1 < p < \infty$, the definition of the norm on $W^{s,p}(M_0)$ allows us to reduce right away the proof to the case of $\mathbb{R}^n$, by ignoring enough terms in the sum defining the norm (21). (We also use a cut-off function $0 \leq \chi \leq 1$, $\chi \in \mathcal{C}^\infty_c(B_{\mathbb{R}^n}(0, 4\epsilon))$, $\chi = 1$ on $B_{\mathbb{R}^n}(0, 4\epsilon)$.) □

We now give a characterization of the spaces $W^{s,p}(M_0)$ using interpolation, $s \in \mathbb{R}$. Let $k \in \mathbb{N} \cup \{0\}$ and let $\widetilde{W}^{-k,p}(M_0)$ be the set of distributions on M_0 that extend by continuity to linear functionals on $W^{k,q}(M_0)$, $p^{-1} + q^{-1} = 1$, using Proposition 3.9. That is, let $\widetilde{W}^{-k,p}(M_0)$ be the set of distributions on M_0 that define continuous linear functionals on $W^{k,q}(M_0)$, $p^{-1} + q^{-1} = 1$. We let

$$\widetilde{W}^{\theta k,k,p}(M_0) := [\widetilde{W}^{0,p}(M_0), W^{k,p}(M_0)]_\theta\,, \quad 0 \leq \theta \leq 1\,,$$

be the complex interpolation spaces. Similarly, we define

$$\widetilde{W}^{-\theta k,k,p}(M_0) = [\widetilde{W}^{0,p}(M_0), W^{-k,p}(M_0)]_\theta.$$

(See [12] or [58, Chapter 4] for the definition of the complex interpolation spaces.)
The following proposition is an analogue of Proposition 3.7. Its main role is to give an intrinsic definition of the spaces $W^{s,p}(M_0)$, a definition that is independent of choices.

PROPOSITION 3.10. *Let $1 < p < \infty$ and $k > |s|$. Then we have a topological equality $\widetilde{W}^{s,k,p}(M_0) = W^{s,p}(M_0)$. In particular, the spaces $W^{s,p}(M_0)$, $s \in \mathbb{R}$, do not depend on the choice of the covering $B(x_j, \epsilon)$ and of the subordinated partition of unity and we have*

$$[W^{s,p}(M_0), W^{0,p}(M_0)]_\theta = W^{\theta s,p}(M_0)\,, \quad 0 \leq \theta \leq 1\,.$$

Moreover, the pairing between functions and distributions defines an isomorphism $W^{s,p}(M_0)^* \simeq W^{-s,q}(M_0)$, where $1/p + 1/q = 1$.

Proof. This proposition is known if $M_0 = \mathbb{R}^n$ with the usual metric [60][Equation (6.5), page 23]. In particular, $\widetilde{W}^{s,p}(\mathbb{R}^n) = W^{s,p}(\mathbb{R}^n)$. As in the proof of Proposition 3.7 one shows that the quantity

$$\nu_{s,p}(u)^p := \sum_j \|(\phi_j u) \circ \psi_j^{-1}\|^p_{\tilde{W}^{s,p}(\mathbb{R}^n)}, \tag{22}$$

is equivalent to the norm on $\tilde{W}^{s,p}(M_0)$. This implies $\tilde{W}^{s,p}(M_0) = W^{s,p}(M_0)$. Choose k large. Then we have

$$\begin{aligned}[W^{s,p}(M_0), W^{0,p}(M_0)]_\theta &= [W^{s,k,p}(M_0), W^{0,k,p}(M_0)]_\theta \\ &= W^{\theta s,k,p}(M_0) = W^{\theta s,p}(M_0).\end{aligned}$$

The last part follows from the compatibility of interpolation with taking duals. This completes the proof. □

The above proposition provides us with several corollaries. First, from the interpolation properties of the spaces $W^{s,p}(M_0)$, we obtain the following corollary.

COROLLARY 3.11. *Let $\phi \in W^{k,\infty}(M_0)$, $k \in \mathbb{N} \cup \{0\}$, $p \in (1, \infty)$, and $s \in \mathbb{R}$ with $k \geq |s|$. Then multiplication by ϕ defines a bounded operator on $W^{s,p}(M_0)$ of norm at most $C_k \|\phi\|_{W^{k,\infty}(M_0)}$. Similarly, any differential operator $P \in \mathrm{Diff}^m_{\mathcal{V}}(M)$ defines continuous maps $P : W^{s,p}(M_0) \to W^{s-m,p}(M_0)$.*

Proof. For $s \in \mathbb{N} \cup \{0\}$, this follows from the definition of the norm on $W^{k,\infty}(M_0)$ and from the definition of $\mathrm{Diff}^m_{\mathcal{V}}(M)$ as the linear span of differential operators of the form $fX_1 \ldots X_k$, ($f \in \mathcal{C}^\infty(M) \subset W^{k,\infty}$, $X_j \in \mathcal{V}$, and $0 \leq k \leq m$), and from the definition of the spaces $W^{k,p}(\Omega_0)$.
For $s \leq m$, the statement follows by duality. For the other values of s, the result follows by interpolation. □

Next, recall that an isomorphism $\phi : M \to M'$ of the Lie manifolds $(M_0, M, \mathcal{V})$ and $(M_0', M', \mathcal{V}')$ is defined to be a diffeomorphism such that $\phi_*(\mathcal{V}) = \mathcal{V}'$. We then have the following invariance property of the Sobolev spaces that we have introduced.

Corollary 3.12. *Let $\phi : M \to M'$ be an isomorphism of Lie manifolds, $\Omega_0 \subset M_0$ be an open subset and $\Omega' = \phi(\Omega)$. Let $p \in [1, \infty]$ if $s \in \mathbb{N} \cup \{0\}$, and $p \in (1, \infty)$ if $s \notin \mathbb{N} \cup \{0\}$. Then $f \to f \circ \phi$ extends to an isomorphism $\phi^* : W^{s,p}(\Omega') \to W^{s,p}(\Omega)$ of Banach spaces.*

Proof. For $s \in \mathbb{N} \cup \{0\}$, this follows right away from definitions and Proposition 3.4. For $-s \in \mathbb{N} \cup \{0\}$, this follows by duality, Proposition (3.10). For the other values of s, the result follows from the same proposition, by interpolation. □

Recall now that M_0 is complete [4]. Hence the Laplace operator $\Delta = \nabla^*\nabla$ is essentially self-adjoint on $\mathcal{C}_c^\infty(M_0)$ by [17, 45]. We shall define then $(1+\Delta)^{s/2}$ using the spectral theorem.

Proposition 3.13. *The space $H^s(M_0) := W^{s,2}(M_0)$, $s \geq 0$, identifies with the domain of $(1+\Delta)^{s/2}$, if we endow the latter with the graph topology.*

Proof. For $s \in \mathbb{N} \cup \{0\}$, the result is true for any manifold of bounded geometry, by [7, Proposition 3]. For $s \in \mathbb{R}$, the result follows from interpolation, because the interpolation spaces are compatible with powers of operators (see, for example, the chapter on Sobolev spaces in Taylor's book [58]). □

The well known Gagliardo–Nirenberg–Sobolev inequality [7, 16, 19] holds also in our setting.

Proposition 3.14. *Denote by n the dimension of M_0. Assume that $1/p = 1/q - m/n$, $1 < q \leq p < \infty$, where $m \geq 0$. Then $W^{s,q}(M_0)$ is continuously embedded in $W^{s-m,p}(M_0)$.*

Proof. If s and m are integers, $s \geq m \geq 0$, the statement of the proposition is true for manifolds with bounded geometry, [7, Theorem 7] or [19, Corollary 3.1.9]. By duality (see Proposition 3.10), we obtain the same result when $s \leq 0$, $s \in \mathbb{Z}$. Then, for integer s, m, $0 < s < m$ we obtain the corresponding embedding by composition $W^{s,q}(M_0) \to W^{0,r}(M_0) \to W^{s-m,p}(M_0)$, with $1/r = 1/q - s/n$. This proves the result for integral values of s. For non-integral values of s, the result follows by interpolation using again Proposition 3.10. □

The Rellich-Kondrachov's theorem on the compactness of the embeddings of Proposition 3.14 for $1/p > 1/q - m/n$ is true if M_0 is compact [7, Theorem 9]. This happens precisely when $M = M_0$, which is a trivial case of a manifold with a Lie structure at infinity. On the other hand, it is easily seen (and well known) that this compactness cannot be true for M_0 non-compact. We will nevertheless obtain compactness in the next section by using Sobolev spaces with weights, see Theorem 4.6.

4. Sobolev spaces on regular open subsets

Let $\Omega \subset M$ be an open subset. Recall that Ω is a regular open subset in M if, and only if, Ω and $\overline{\Omega}$ have the same boundary in M, denoted $\partial_{\text{top}}\overline{\Omega}$,, and if $\partial_{\text{top}}\overline{\Omega}$ is a regular submanifold of M. Let $\Omega_0 = \Omega \cap M_0$. Then $\partial\Omega_0 := (\partial\Omega) \cap M_0 = \partial_{\text{top}}\overline{\Omega} \cap M_0$ is a smooth submanifold of codimension one of M_0 (see Figure 1). We shall denote $W^{s,p}(\overline{\Omega}) = W^{s,p}(\Omega) = W^{s,p}(\Omega_0)$. Throughout this section Ω will denote a regular open subset of M.

We have the following analogue of the classical extension theorem.

Theorem 4.1. *Let $\Omega \subset M$ be a regular open subset. Then there exists a linear operator E mapping measurable functions on Ω_0 to measurable functions on M_0 with the properties:*

(i) *E maps $W^{k,p}(\Omega_0)$ continuously into $W^{k,p}(M_0)$ for every $p \in [1,\infty]$ and every integer $k \geq 0$, and*

(ii) *$Eu|_{\Omega_0} = u$.*

Proof. Since $\partial\Omega_0$ is a regular submanifold we can fix a compatible metric g on M_0 and a tubular neighborhood V_0 of $\partial\Omega_0$ such that $V_0 \simeq (\partial\Omega_0) \times (-\varepsilon_0, \varepsilon_0)$, $\varepsilon_0 > 0$. Let $\varepsilon = \min(\varepsilon_0, r_{\text{inj}}(M_0))/20$, where $r_{\text{inj}}(M_0) > 0$ is the injectivity radius of M_0. By Zorn's lemma and the fact that M_0 has bounded geometry we can choose a maximal, countable set of disjoint balls $B(x_i, \varepsilon)$, $i \in I$. Since this family of balls is maximal we have $M_0 = \cup_i B(x_i, 2\varepsilon)$. For each i we fix a smooth function η_i supported in $B(x_i, 3\varepsilon)$ and equal to 1 in $B(x_i, 2\varepsilon)$. This can be done easily in local coordinates around the point x_i; since the metric g is induced by a metric g on A we may also assume that all derivatives of order up to k of η_i are bounded by a constant $C_{k,\varepsilon}$ independent of i. We then set $\tilde{\eta}_i := \big(\sum_{j\in I} \eta_j^2\big)^{-1/2}\eta_i$. Then $\sum_{i\in I} \tilde{\eta}_i^2 = 1$, $\tilde{\eta}_i$ equals 1 on $B(x_i, \epsilon)$ and is supported in $B(x_i, 3\epsilon)$.

Following [56, Ch. 6] we also define two smooth cutoff functions adapted to the set Ω_0. We start with a function $\psi : \mathbb{R} \to [0,1]$ which is equal to 1 on $[-3,3]$ and which has support in $[-6,6]$

Let $\varphi = (\varphi_1, \varphi_2)$ denote the isomorphism between V_0 and $\partial\Omega_0 \times (-\varepsilon_0, \varepsilon_0)$, where $\varphi_1 : V_0 \to \partial\Omega_0$ and $\varphi_2 : V_0 \to (-\varepsilon_0, \varepsilon_0)$. We define

$$\Lambda_+(x) := \begin{cases} 0 & \text{if } x \in M_0 \setminus V_0 \\ \psi(\varphi_2(x)/\varepsilon) & \text{if } x \in V_0, \end{cases}$$

and $\Lambda_-(x) := 1 - \Lambda_+(x)$. Clearly Λ_+ and Λ_- are smooth functions on M_0 and $\Lambda_+(x) + \Lambda_-(x) = 1$. Obviously, Λ_+ is supported in a neighborhood of $\partial\Omega_0$ and Λ_- is supported in the complement of a neighborhood of $\partial\Omega_0$.

Let $\partial\Omega_0 = A_1 \cup A_2 \cup \ldots$ denote the decomposition of $\partial\Omega_0$ into connected components. Let $V_0 = B_1 \cup B_2 \cup \ldots$ denote the corresponding decomposition of V_0 into connected components, namely, $B_j = \varphi^{-1}(A_j \times (-\varepsilon_0, \varepsilon_0))$. Since $\partial\Omega_0 = \partial\overline{\Omega}_0$, we have $\varphi(\Omega_0 \cap B_j) = A_j \times (-\varepsilon_0, 0)$ or $\varphi(\Omega_0 \cap B_j) = A_j \times (0, \varepsilon_0)$. Thus, if necessary, we may change the sign of φ on some of the connected components of V_0 in such a way that

$$\varphi(\Omega_0 \cap V_0) = \partial\Omega_0 \times (0, \varepsilon_0).$$

Let ψ_0 denote a fixed smooth function, $\psi_0 : \mathbb{R} \to [0,1]$, $\psi_0(t) = 1$ if $t \geq -\varepsilon$ and $\psi_0(t) = 0$ if $t \leq -2\varepsilon$, and let

$$\Lambda_0(x) = \begin{cases} 1 & \text{if } x \in \Omega_0 \setminus V_0 \\ 0 & \text{if } x \in M_0 \setminus (\Omega_0 \cup V_0) \\ \psi_0(\varphi_2(x)) & \text{if } x \in V_0. \end{cases}$$

We look now at the points x_i defined in the first paragraph of the proof. Let $J_1 = \{i \in I : d(x_i, \partial\Omega_0) \leq 10\varepsilon\}$ and $J_2 = \{i \in I : d(x_i, \partial\Omega_0) > 10\varepsilon\}$. For every point x_i, $i \in J_1$, there is a point $y_i \in \partial\Omega_0$ with the property that $B(x_i, 4\varepsilon) \subset B(y_i, 15\varepsilon)$. Let $B_{\partial\Omega_0}(y_i, 15\varepsilon)$ denote the ball in $\partial\Omega_0$ of center y_i and radius 15ε (with respect to the induced metric on $\partial\Omega_0$). Let $h_i : B_{\partial\Omega_0}(y_i, 15\varepsilon) \to B_{\mathbb{R}^{n-1}}(0, 15\varepsilon)$ denote the normal system of coordinates around the point y_i. Finally let $g_i : B_{\mathbb{R}^{n-1}}(0, 15\varepsilon) \times (-15\varepsilon, 15\varepsilon) \to V_0$ denote the map $g_i(v,t) = \varphi^{-1}(h_i^{-1}(v), t)$.
Let $E_{\mathbb{R}^n}$ denote the extension operator that maps $W^{k,p}(\mathbb{R}^n_+)$ to $W^{k,p}(\mathbb{R}^n)$ continuously, where $\mathbb{R}^n_+$ denotes the half-space $\{x : x_n > 0\}$. Clearly, $E_{\mathbb{R}^n} u|_{\mathbb{R}^n_+} = u$. The existence of this extension operator is a classical fact, for instance, see [56, Chapter 6]. For any $u \in W^{k,p}(\Omega_0)$ and $i \in J_1$ the function $(\tilde{\eta}_i u) \circ g_i$ is well defined on $\mathbb{R}^n_+$ simply by setting it equal to 0 outside the set $B_{\mathbb{R}^{n-1}}(0, 15\varepsilon) \times (0, 15\varepsilon)$. Clearly, $(\tilde{\eta}_i u) \circ g_i \in W^{k,p}(\mathbb{R}^n_+)$. We define the extension Eu by the formula
(23)

$$Eu(x) = \Lambda_0(x)\Lambda_-(x)u(x) + \Lambda_0(x)\Lambda_+(x) \sum_{i \in J_1} \tilde{\eta}_i(x) \Big(E_{\mathbb{R}^n}[(\tilde{\eta}_i u) \circ g_i] \Big)(g_i^{-1} x) \, .$$

Notice that for all $i \in J_2$, the function $\tilde{\eta}_i$ vanishes on the support of Λ_+, and hence

$$\sum_{i \in J_1} \tilde{\eta}_i^2(x) = \sum_{i \in I} \tilde{\eta}_i^2(x) = 1 \text{ in } \operatorname{supp} \Lambda_+. \tag{24}$$

This formula implies $Eu|_{\Omega_0} = u$. It remains to verify that

$$\|Eu\|_{W^{k,p}(M_0)} \leq C_k \|u\|_{W^{k,p}(\Omega_0)}.$$

This follows as in [56] using (24), the fact that the extension $E_{\mathbb{R}^n}$ satisfies the same bound, and the definition of the Sobolev spaces using partitions of unity (Proposition 3.7). □

Let Ω be a regular open subset of M and $\Omega_0 = \Omega \cap M$, as before. We shall denote by $\overline{\Omega}_0$ the closure of Ω_0 in M_0.

Theorem 4.2. *The space $\mathcal{C}_c^\infty(\overline{\Omega}_0)$ is dense in $W^{k,p}(\Omega_0)$, for $1 \leq p < \infty$.*

Proof. For any $u \in W^{k,p}(\Omega_0)$ let Eu denote its extension from Theorem 4.1, $Eu \in W^{k,p}(M_0)$. By Proposition 3.9, there is a sequence of functions $f_j \in \mathcal{C}_c^\infty(M_0)$ with the property that

$$\lim_{j\to\infty} f_j = Eu \text{ in } W^{k,p}(M_0).$$

Thus $\lim_{j\to\infty} f_j|_{\Omega_0} = u$ in $W^{k,p}(\Omega_0)$, as desired. □

Theorem 4.3. *The restriction map $\mathcal{C}_c^\infty(\overline{\Omega}_0) \to \mathcal{C}_c^\infty(\partial\Omega_0)$ extends to a continuous map $T : W^{k,p}(\Omega_0) \to W^{k-1,p}(\partial\Omega_0)$, for $1 \le p \le \infty$.*

Proof. The case $p = \infty$ is obvious. In the case $1 \le p < \infty$, we shall assume that the compatible metric on M_0 restricts to a product type metric on V_0, our distinguished tubular neighborhood of $\partial\Omega_0$. As the curvature of M_0 and the second fundamental form of $\partial\Omega_0$ in M_0 are bounded (see Corollary 2.4), there is an $\epsilon_1 > 0$ such that, in normal coordinates, the hypersurface $\partial\Omega_0$ is the graph of a function on balls of radius $\le \epsilon_1$.
We use the definitions of the Sobolev spaces using partitions of unity, Proposition 3.7 and Lemma 3.6 with $\varepsilon = \min(\epsilon_1, \epsilon_0, r_{\rm inj}(M_0))/10$. Let $B(x_j, 2\varepsilon)$ denote the balls in the cover of M_0 in Lemma 3.6, let $\psi_j : B(\epsilon, x_j) \to B(\epsilon, 0)$ denote normal coordinates based in x_j, and let $1 = \sum_j \phi_j$ be a corresponding partition of unity. Then $\widetilde{\phi}_j = \phi_j|_{\partial\Omega_0}$ form a partition of unity on $\partial\Omega_0$.
Start with a function $u \in W^{k,p}(\Omega_0)$ and let $u_j = (u\phi_j)\circ\psi_j^{-1}$, $u_j \in W^{k,p}(\psi_j(\Omega_0 \cap B(x_j, 4\varepsilon)))$. In addition $u_j \equiv 0$ outside the set $\psi_j(\Omega_0 \cap B(x_j, 2\varepsilon))$. If $B(x_j, 4\varepsilon) \cap \partial\Omega_0 = \emptyset$ let $\widetilde{T}(u_j) = 0$. Otherwise notice that $B(x_j, 4\varepsilon)$ is included in V_0, the tubular neighborhood of $\partial\Omega_0$, thus the set $\psi_j(\partial\Omega_0 \cap B(x_j, 4\varepsilon))$ is the intersection of a graph and the ball $B_{\mathbb{R}^n}(0, 4\varepsilon)$. We can then let $\widetilde{T}(u_j)$ denote the Euclidean restriction of u_j to $\psi_j(\partial\Omega_0 \cap B(x_j, 4\varepsilon))$ (see [16, Section 5.5]). Clearly $\widetilde{T}(u_j)$ is supported in $\psi_j(\partial\Omega_0 \cap B(x_j, 2\varepsilon))$ and

$$\|\widetilde{T}(u_j) \circ \widetilde{\psi}_j\|_{W^{k-1,p}(\partial\Omega_0)} \le C\|u_j\|_{W^{k,p}(\psi_j(\Omega_0 \cap B(x_j,4\varepsilon)))},$$

where $\widetilde{\psi}_j = \psi_j|_{\Omega_0}$ and the constant C is independent of j (recall that $\psi_j(\partial\Omega_0 \cap B(x_j, 4\varepsilon))$ is the intersection of a hyperplane and the ball $B_{\mathbb{R}^n}(0, 4\varepsilon)$). Let

$$Tu = \sum_j \widetilde{T}(u_j) \circ \widetilde{\psi}_j.$$

Since the sum is uniformly locally finite, Tu is well-defined and we have

$$\begin{aligned}\|Tu\|^p_{W^{k-1,p}(\partial\Omega_0)} &\le C \sum_j \|\widetilde{T}(u_j) \circ \widetilde{\psi}_j\|^p_{W^{k-1,p}(\partial\Omega_0)} \\ &\le C \sum_j \|u_j\|^p_{W^{k,p}(\psi_j(\Omega_0 \cap B(x_j,4\varepsilon)))} \le C\|u\|^p_{W^{k,p}(\Omega_0)},\end{aligned}$$

with constants C independent of u. The fact that $Tu|_{\mathcal{C}_c^\infty(\Omega_0)}$ is indeed the restriction operator follows immediately from the definition. □

We shall see that if $p = 2$, we get a surjective map $W^{s,2}(\Omega_0) \to W^{s-1/2,2}(\partial\Omega_0)$ (Theorem 4.7).
In the following, ∂_ν denotes derivative in the normal direction of the hypersurface $\partial\Omega_0 \subset M_0$.

Theorem 4.4. *The closure of $\mathcal{C}_c^\infty(\Omega_0)$ in $W^{k,p}(\Omega_0)$ is the intersection of the kernels of $T \circ \partial_\nu^j : W^{k,p}(\Omega_0) \to W^{k-j-1,p}(\Omega_0)$, $0 \leq j \leq k-1$, $1 \leq p < \infty$.*

Proof. The proof is reduced to the Euclidean case [1, 16, 33, 58] following the same pattern of reasoning as in the previous theorem. □

The Gagliardo–Nirenberg–Sobolev theorem holds also for manifolds with boundary.

Theorem 4.5. *Denote by n the dimension of M and let $\Omega \subset M$ be a regular open subset in M. Assume that $1/p = 1/q - m/n > 0$, $1 \leq q < \infty$, where $m \leq k$ is an integer. Then $W^{k,q}(\Omega_0)$ is continuously embedded in $W^{k-m,p}(\Omega_0)$.*

Proof. This can be proved using Proposition 3.14 and Theorem 4.1. Indeed, denote by

$$j : W^{k,q}(M_0) \to W^{k-m,p}(M_0)$$

the continuous inclusion of Proposition 3.14. Also, denote by r the restriction maps $W^{k,p}(M_0) \to W^{k,p}(\Omega_0)$. Then the maps

$$W^{k,q}(\Omega_0) \xrightarrow{E} W^{k,q}(M_0) \xrightarrow{j} W^{k-m,p}(M_0) \xrightarrow{r} W^{k-m,p}(\Omega_0)$$

are well defined and continuous. Their composition is the inclusion of $W^{k,q}(\Omega_0)$ into $W^{k-m,p}(\Omega_0)$. This completes the proof. □

For the proof of a variant of Rellich–Kondrachov's compactness theorem, we shall need Sobolev spaces with weights. Let $\Omega \subset M$ be a regular open subset. Let $a_H \in \mathbb{R}$ be a parameter associated to each boundary hyperface (i. e., face of codimension one) of the manifold with corners $\overline{\Omega}$. Fix for any boundary hyperface $H \subset \overline{\Omega}$ a defining function ρ_H, that is a function $\rho_H \geq 0$ such that $H = \{\rho_H = 0\}$ and $d\rho_H \neq 0$ on H. Let

$$\rho = \prod \rho_H^{a_H}, \tag{25}$$

the product being taken over all boundary hyperfaces of $\overline{\Omega}$. A function of the form $\psi\rho$, with $\psi > 0$, ψ smooth on $\overline{\Omega}$, and ρ as in Equation (25) will be called an *admissible weight* of $\overline{\Omega}$ (or simply an admissible weight when Ω is understood). We define then the weighted Sobolev space $W^{k,p}(\Omega_0)$ by

$$\rho W^{k,p}(\Omega_0) := \{\rho u, u \in W^{k,p}(\Omega_0)\}, \tag{26}$$

with the norm $\|\rho^s u\|_{\rho^s W^{k,p}(\Omega_0)} := \|u\|_{W^{k,p}(\Omega_0)}$.
Note that in the definition of an admissible weight of $\overline{\Omega}$, for a regular open subset $\Omega \subset M$ of the Lie manifold $(M, \mathcal{V})$, we allow also powers of the defining functions of the boundary hyperfaces contained in $\partial\Omega = \partial_{\mathrm{top}}\overline{\Omega}$, the true boundary of $\overline{\Omega}$. In the next compactness theorem, however, we shall allow only the powers of the defining functions of M, or, which is the same thing, only

powers of the defining functions of the boundary hyperfaces of $\overline{\Omega}$ whose union is $\partial_\infty \overline{\Omega}$ (see Figure 1).

Theorem 4.6. *Denote by n the dimension of M and let $\Omega \subset M$ be a regular open subset, $\Omega_0 = \Omega \cap M_0$. Assume that $1/p > 1/q - m/n > 0$, $1 \leq q < \infty$, where $m \in \{1, \ldots, k\}$ is an integer, and that $s > s'$ are real parameters. Then $\rho^s W^{k,q}(\Omega_0)$ is compactly embedded in $\rho^{s'} W^{k-m,p}(\Omega_0)$ for any admissible weight $\rho := \prod_H \rho_H^{a_H}$ of M such that $a_H > 0$ for any boundary hyperface H of M.*

Proof. The same argument as that in the proof of Theorem 4.5 allows us to assume that $\Omega_0 = M_0$. The norms are chosen such that $W^{k,p}(\Omega_0) \ni u \mapsto \rho^s u \in \rho^s W^{k,p}(\Omega_0)$ is an isometry. Thus, it is enough to prove that $\rho^s : W^{k,q}(\Omega_0) \to W^{k-m,p}(\Omega_0)$, $s > 0$, is a compact operator.
For any defining function ρ_H and any $X \in \mathcal{V}$, we have that $X(\rho_H)$ vanishes on H, since X is tangent to H. We obtain that $X(\rho^s) = \rho^s f_X$, for some $f_X \in \mathcal{C}^\infty(M)$. Then, by induction, $X_1 X_2 \ldots X_k(\rho^s) = \rho^s g$, for some $g \in \mathcal{C}^\infty(M)$.
Let $\chi \in \mathcal{C}^\infty([0,\infty)$ be equal to 0 on $[0, 1/2]$, equal to 1 on $[1,\infty)$, and non-negative everywhere. Define $\phi_\epsilon = \chi(\epsilon^{-1}\rho^s)$. Then

$$\|X_1 X_2 \ldots X_k\big(\rho^s \phi_\epsilon - \rho^s\big)\|_{L^\infty} \to 0\,, \quad \text{as } \epsilon \to 0,$$

for any $X_1, X_2, \ldots, X_k \in \mathcal{V}$. Corollary 3.11 then shows that $\rho^s \phi_\epsilon \mapsto \rho^s$ in the norm of bounded operators on $W^{s,p}(\Omega_0)$. But multiplication by $\rho^s \phi_\epsilon$ is a compact operator, by the Rellich-Kondrachov's theorem for compact manifolds with boundary [7, Theorem 9]. This completes the proof. □

We end with the following generalization of the classical restriction theorem for the Hilbertian Sobolev spaces $H^s(M_0) := W^{s,2}(M_0)$.

Theorem 4.7. *Let $N_0 \subset M_0$ be a tame submanifold of codimension k of the Lie manifold $(M_0, M, \mathcal{V})$. Restriction of smooth functions extends to a bounded, surjective map*

$$H^s(M_0) \to H^{s-k/2}(N_0),$$

for any $s > k/2$. In particular, $H^s(\Omega_0) \to H^{s-1/2}(\partial\Omega_0)$ is continuous and surjective.

Proof. Let $B \to N$ be the vector bundle defining the Lie structure at infinity (N, B) on N_0 and $A \to M$ be the vector bundle defining the Lie structure at infinity (M, A) on M_0. (See Section 2 for further explanation of this notation.) The existence of tubular neighborhoods, Theorem 2.7, and a partition of unity argument, allows us to assume that $M = N \times S^1$ and that $A = B \times TS^1$ (external product). Since the Sobolev spaces $H^s(M_0)$ and $H^{s-1/2}(N_0)$ do not depend on the metric on A and B, we can assume that the circle S^1 is given the invariant metric making it of length 2π and that M_0 is given the product metric. The rest of the proof now is independent of the way we obtain the product metric on M_0.
Let S^1 be the unit circle in the plane. Let us denote by Δ_M, Δ_N, and Δ_{S^1} the Laplace operators on M_0, N_0, and S^1, respectively. Then $\Delta_M = \Delta_N + \Delta_{S^1}$

and $\Delta_{S^1} = -\partial^2/\partial\theta^2$ has spectrum $\{4\pi^2 n^2 \,|\, n \in \mathbb{N} \cup \{0\}\}$. We can decompose $L^2(N_0 \times S^1)$ according to the eigenvalues $n \in \mathbb{Z}$ of $-\frac{1}{2\pi\imath}\partial_\theta$:

$$L^2(N_0 \times S^1) \simeq \bigoplus_{n\in\mathbb{Z}} L^2(N_0 \times S^1)_n \simeq \bigoplus_{n\in\mathbb{Z}} L^2(N_0),$$

where the isomorphism $L^2(N_0 \times S^1)_n \simeq L^2(N_0)$ is obtained by restricting to $N_0 = N_0 \times \{1\}$, $1 \in S^1$. We use this isomorphism to identify the above spaces in what follows.

Let $\xi \in L^2(N_0 \times S^1)$. Then ξ identifies with a sequence (ξ_n) under the above isomorphism. By Proposition 3.13, we have that $\xi \in H^s(N_0 \times S^1)$ if, and only if, $(1+\Delta_M)^{s/2}\xi = \sum_n \big((1+n^2+\Delta_N)^{s/2}\xi_n\big) \in \bigoplus_{n\in\mathbb{Z}} L^2(N_0) \simeq L^2(N_0 \times S^1)$. The restriction of ξ to N_0 is then given by $\sum_n \xi_n$. We want to show that $\sum_n \xi_n \in H^{s-1/2}(N_0)$, which is equivalent to $(1+\Delta_N)^{s/2-1/4}\big(\sum \xi_n\big) \in L^2(N_0)$. The spectral spaces of Δ_N corresponding to $[m, m+1) \subset \mathbb{R}$, $m \in \mathbb{N} \cup \{0\}$ give an orthogonal direct sum decomposition of $L^2(N_0)$.

We decompose $\xi_n = \sum_m \xi_{mn}$, with ξ_{mn} in the spectral space corresponding to $[m, m+1)$ of Δ_N. Note that ξ_{mn} is orthogonal to $\xi_{m'n}$ for $m \neq m'$. Denote $h = (1+m^2)^{-1/2}$, $f(t) = (1+t^2)^{-s}$, and $C = 1 + \int_{\mathbb{R}} f(t)dt$. Then an application of the Cauchy–Schwartz inequality gives

$$\begin{aligned}(27)\quad & (1+m^2)^{s-1/2}\Big(\sum_n \|\xi_{mn}\|\Big)^2 \\ & \leq (1+m^2)^{s-1/2}\Big(\sum_n (1+n^2+m^2)^{-s}\Big) \sum_n \|(1+n^2+m^2)^{s/2}\xi_{mn}\|^2 \\ & \leq h\Big(\sum_n f(nh)\Big) \sum_n \|(1+n^2+m^2)^{s/2}\xi_{mn}\|^2 \leq C_s \sum_n \|(1+n^2+m^2)^{s/2}\xi_{mn}\|^2.\end{aligned}$$

The constant C_s is independent of m (but depends on s). We sum over m and obtain

$$\begin{aligned}(28)\quad & \|\sum_n (1+\Delta_N)^{s/2-1/4}\xi_n\|^2 = \sum_m \|\sum_n (1+\Delta_N)^{s/2-1/4}\xi_{nm}\|^2 \\ & \leq \sum_m (1+(m+1)^2)^{s-1/2}\Big(\sum_n \|\xi_{nm}\|\Big)^2 \leq 2^s \sum_m (1+m^2)^{s-1/2}\Big(\sum_n \|\xi_{nm}\|\Big)^2 \\ & \leq 2^s C_s \sum_{n,m} \|(1+n^2+m^2)^{s/2}\xi_{nm}\|^2 \leq 2^s C_s \sum_{n,m} \|(1+n^2+\Delta_N)^{s/2}\xi_{nm}\|^2 \\ & = 2^s C_s \sum_n \|(1+n^2+\Delta_N)^{s/2}\xi_n\|^2,\end{aligned}$$

with the same constant C_s as in Equation (27). This shows that $\zeta := \sum_n \xi_n \in H^{s-1/2}(N_0)$ if $\xi = (\xi_n) \in \bigoplus_n L^2(N_0) \simeq L^2(N_0 \times S^1)$ is a *finite* sequence such that $\|\xi\|_{H^s} := \sum_n \|(1+n^2+\Delta_N)^{s/2}\xi_n\|^2_{L^2(N_0)} < \infty$, and that ζ depends continuously on $\xi \in H^s(N_0 \times S^1)$. This completes the proof. □

We finally obtain the following consequences for a curvilinear polygonal domain $\mathbb{P}$ (see Subsection 1.6). First, recall that the distance $\vartheta(x)$ from x to the vertices of a curvilinear polygon $\mathbb{P}$ and $r_{\mathbb{P}}$ have bounded quotients, and hence define the same weighted Sobolev spaces (Equation (12)). Moreover, the function $r_{\mathbb{P}}$ is an admissible weight. Recall that $\mathbb{P}$ has a compactification $\Sigma(\mathbb{P})$ that is a Lie manifold with boundary (that is, the closure of a regular open subset of a Lie manifold M). Let us write $W^{m,p}(\Sigma(\mathbb{P})) := W^{m,p}(\mathbb{P})$ the Sobolev spaces defined by the structural Lie algebra of vector fields on $\Sigma(\mathbb{P})$. Then

$$\mathcal{K}_a^m(\mathbb{P};\vartheta) = r_\Omega^{a-1}\mathcal{K}_1^m(\mathbb{P};r_{\mathbb{P}}) = r_{\mathbb{P}}^{a-1}W^{m,2}(\Sigma(\mathbb{P})). \tag{29}$$

This identifies the weighted Sobolev spaces on $\mathbb{P}$ with a weighted Sobolev space of the form $\rho W^{k,p}(\Omega_0)$.
Motivated by Equation (29), we now define

$$\mathcal{K}_a^m(\partial\mathbb{P}) = \mathcal{K}_a^m(\partial\mathbb{P};\vartheta) = \mathcal{K}_a^m(\partial\mathbb{P};r_{\mathbb{P}}) = r_{\mathbb{P}}^{a-1/2}W^{m,2}(\partial\mathbb{P}). \tag{30}$$

More precisely, let us notice that we can identify each edge with $[0,1]$. Then $\mathcal{K}_a^m(\partial\mathbb{P})$ consists of the functions $f:\partial\mathbb{P}\to\mathbb{C}$ that, on each edge, are such that $t^k(1-t)^kf^{(k)}\in L^2([0,1])$, $0\le k\le m$ (here we identify that edge with $[0,1]$). This last condition is equivalent to $[t(1-t)\partial_t]^kf\in L^2([0,1])$, $0\le k\le m$.

Proposition 4.8. *Let $\mathbb{P}\subset\mathbb{R}^2$ be a curvilinear polygonal domain and P be a differential operator of order m with coefficients in $\mathcal{C}^\infty(\overline{\mathbb{P}})$. Then $P_\lambda := r_{\mathbb{P}}^\lambda P r_{\mathbb{P}}^{-\lambda}$ defines a continuous family of bounded maps $P_\lambda:\mathcal{K}_a^s(\mathbb{P})\to\mathcal{K}_{a-m}^{s-m}(\mathbb{P})$, for any $s,a\in\mathbb{R}$. Let $\mathbb{P}'$ be $\overline{\mathbb{P}}$ with the vertices removed. Then $\mathcal{C}_c^\infty(\mathbb{P}')$ is dense in $\mathcal{K}_a^m(\mathbb{P})$. Also, the restriction to the boundary extends to a continuous, surjective trace map $\mathcal{K}_a^s(\mathbb{P})\to\mathcal{K}_{a-1/2}^{s-1/2}(\partial\mathbb{P})$. If $s=1$, then the kernel of the trace map is the closure of $\mathcal{C}_c^\infty(\mathbb{P})$ in $\mathcal{K}_a^1(\mathbb{P})$.*

The above proposition, except maybe for the description of the restrictions to the boundary, is well known in two dimensions. It will serve as a model for the results in three dimensions that we present in the last section.

5. A regularity result

We include in this section an application to the regularity of boundary value problems, Theorem 5.1. Its proof is reduced to the Euclidean case using a partition of unity argument and the tubular neighborhood theorem 2.7, both of which require some non-trivial input from differential geometry.
Let us introduce some notation first that will be also useful in the following. Let $\exp: TM_0 \longrightarrow M_0\times M_0$ be given by $\exp(v) := (x,\exp_x(v))$, $v\in T_xM_0$. If E is a real vector bundle with a metric, we shall denote by $(E)_r$ the set of all vectors v of E with $|v|<r$. Let $(M_0^2)_r := \{(x,y), x,y\in M_0,\ d(x,y)<r\}$. Then the exponential map defines a diffeomorphism $\exp:(TM_0)_r\to(M_0^2)_r$. We shall also need the admissible weight function ρ defined in Equation (25) and the weighted Sobolev spaces $\rho^sW^{k,p}(\Omega_0) := \{\rho^su, u\in W^{k,p}(\Omega_0)\}$ introduced in Equation 26.

Recall [58], Chapter 5, Equation (11.79), that a differential operator P of order m is called *strongly elliptic* if there exists $C > 0$ such that $Re\big(\sigma^{(m)}(P)(\xi)\big) \geq C\|\xi\|^m$ for all ξ.

Theorem 5.1. *Let $\Omega \subset M$ be a regular open subset of the Lie manifold $(M, \mathcal{V})$. Let $P \in \mathrm{Diff}^2_{\mathcal{V}}(M)$ be an order 2 strongly elliptic operator on M_0 generated by $\mathcal{V}$ and $s \in \mathbb{R}$, $t \in \mathbb{Z}$, $1 < p < \infty$. Then there exists $C > 0$ such that, for any $u \in \rho^s W^{1,p}(\Omega_0)$, $u|_{\partial\Omega_0} = 0$, we have*

$$\|u\|_{\rho^s W^{t+2,p}(\Omega_0)} \leq C(\|Pu\|_{\rho^s W^{t,p}(\Omega_0)} + \|u\|_{\rho^s L^p(\Omega_0)}).$$

In particular, let $u \in \rho^s W^{1,p}(\Omega_0)$ be such that $Pu \in \rho^s W^{t,p}(\Omega_0)$, and $u|_{\partial\Omega_0} = 0$, then $u \in \rho^s W^{t+2,p}(\Omega_0)$.

Proof. Note that, locally, this is a well known statement. In particular, $\phi u \in W^{t+2,p}(\Omega_0)$, for any $\phi \in \mathcal{C}^\infty_{\mathrm{c}}(M_0)$. The result will follow then if we prove that

$$\|u\|_{\rho^s W^{t+2,p}(M_0)} \leq C(\|Pu\|_{\rho^s W^{t,p}(M_0)} + \|u\|_{\rho^s L^p(M_0)}) \tag{31}$$

for any $u \in W^{t+2,p}_{\mathrm{loc}}(\Omega_0)$. Here, of course, $\|u\|_{\rho^s L^p(M_0)} = \|\rho^{-s} u\|_{L^p(M_0)}$ (see Equation (26)).

Let $r < r_{\mathrm{inj}}(M_0)$ and let $\exp : (TM_0)_r \to (M_0^2)_r$ be the exponential map. The statement is trivially true for $t \leq -2$, so we will assume $t \geq -1$ in what follows. Also, we will assume first that $s = 0$. The general case will be reduced to this one at the end. Assume first that $\Omega_0 = M_0$.

Let P_x be the differential operators defined on $B_{T_xM_0}(0, r)$ obtained from P by the local diffeomorphism $\exp : B_{T_xM_0}(0, r) \to M_0$. We claim that there exists a constant $C > 0$, independent of $x \in M_0$ such that

$$\|u\|^p_{W^{t+2,p}(T_xM_0)} \leq C\big(\|P_x u\|^p_{W^{t,p}(T_xM_0)} + \|u\|^p_{L^p(T_xM_0)}\big), \tag{32}$$

for any function $u \in \mathcal{C}^\infty_{\mathrm{c}}(B_{T_xM_0}(0, r))$. This is seen as follows. We can find a constant $C_x > 0$ with this property for any $x \in M_0$ by the ellipticity of P_x. (For $p = 2$, a complete proof can be found in [58], Propositions 11.10 and 11.16. For general p, the result can be proved as [16], Theorem 1 in subsection 5.8.1, page 275.) Choose C_x to be the least such constant. Let $\pi : A \to M$ be the extension of the tangent bundle of M_0, see Remark 1.5 and let $A_x = \pi^{-1}(x)$. The family P_x, $x \in M_0$, extends to a family P_x, $x \in M$, that is smooth in x. The smoothness of the family P_x in $x \in M$ shows that C_x is upper semi-continuous (i. e., the set $\{C_x < \eta\}$ is open for any x). Since M is compact, C_x will attain its maximum, which therefore must be positive. Let C be that maximum value.

Let now ϕ_j be the partition of unity and ψ_j be the diffeomorphisms appearing in Equation (22), for some $0 < \epsilon < r/6$. In particular, the partition of unity ϕ_j satisfies the conditions of Lemma 3.6, which implies that $\mathrm{supp}(\phi_j) \subset B(x_j, 2\epsilon)$ and the sets $B(x_j, 4\epsilon)$ form a covering of M_0 of finite multiplicity. Let $\eta_j = 1$

on the support of ϕ_j, $\mathrm{supp}(\eta_j) \subset B(x_j, 4\epsilon)$. We then have

$$\begin{aligned}\nu_{t+2,p}(u)^p := \sum_j \|(\phi_j u)\circ \psi_j^{-1}\|^p_{W^{t+2,p}(\mathbb{R}^n)} \\ \leq C \sum_j \Big(\|P_x(\phi_j u)\|^p_{W^{t,p}(T_xM_0)} + \|\phi_j u\|^p_{L^p(T_xM_0)}\Big) \\ \leq C\sum_j \Big(\|\phi_j P_x u\|^p_{W^{t,p}(T_xM_0)} + \|[P_x,\phi_j]u\|^p_{W^{t,p}(T_xM_0)} + \|\phi_j u\|^p_{L^p(T_xM_0)}\Big) \\ \leq C\sum_j \Big(\|\phi_j P_x u\|^p_{W^{t,p}(T_xM_0)} + \|\eta_j u\|^p_{W^{t+1,p}(T_xM_0)} + \|\phi_j u\|^p_{L^p(T_xM_0)}\Big) \\ \leq C\big(\nu_{t,p}(Pu)^p + \nu_{t+1}(u)^p\big).\end{aligned}$$

The equivalence of the norm $\nu_{s,p}$ with the standard norm on $W^{s,p}(M_0)$ (Propositions 3.7 and 3.10) shows that $\|u\|_{W^{t+2,p}(M_0)} \leq C(\|Pu\|_{W^{t,p}(M_0)} + \|u\|_{W^{t+1,p}(M_0)})$, for any $t \geq -1$. This is known to imply

$$\|u\|_{W^{t+2,p}(M_0)} \leq C(\|Pu\|_{W^{t,p}(M_0)} + \|u\|_{L^p(M_0)}) \tag{33}$$

by a boot-strap procedure, for any $t \geq -1$. This proves our statement if $s = 0$ and $\Omega_0 = M_0$.

The case of arbitrary domains Ω_0 follows in exactly the same way, but using a product type metric in a neighborhood of $\partial_{\mathrm{top}}\Omega_0$ and the analogue of Equation (32) for a half-space, which shows that Equation (31) continues to hold for M_0 replaced with Ω_0.

The case of arbitrary $s \in \mathbb{R}$ is obtained by applying Equation (33) to the elliptic operator $\rho^{-s}P\rho^s \in \mathrm{Diff}^2_{\mathcal{V}}(M)$ and to the function $\rho^{-s}u \in W^{k,p}(\Omega_0)$, which then gives Equation (31) right away. □

For $p = 2$, by combining the above theorem with Theorem 4.7, we obtain the following corollary.

Corollary 5.2. *We keep the assumptions of Theorem 5.1. Let $u \in \rho^s H^1(\Omega_0)$ be such that $Pu \in \rho^s H^t(\Omega_0)$ and $u|_{\partial\Omega_0} \in \rho^s H^{t+3/2}(\Omega_0)$, $s \in \mathbb{R}$, $t \in \mathbb{Z}$. Then $u \in \rho^s H^{t+2}(\Omega_0)$ and*

$$\|u\|_{\rho^s H^{t+2}(\Omega_0)} \leq C(\|Pu\|_{\rho^s H^t(\Omega_0)} + \|u\|_{\rho^s L^2(\Omega_0)} + \|u|_{\partial\Omega_0}\|_{\rho^s H^{t+3/2}(\Omega_0)}). \tag{34}$$

Proof. For $u|_{\partial\Omega_0} = 0$, the result follows from Theorem 5.1. In general, choose a suitable $v \in H^{t+2}(\Omega_0)$ such that $v|_{\partial\Omega_0} = u|_{\partial\Omega_0}$, which is possible by Theorem 4.7. Then we use our result for $u - v$. □

6. Polyhedral domains in three dimensions

We now include an application of our results to polyhedral domains $\mathbb{P} \subset \mathbb{R}^3$. A *polyhedral domain in* $\mathbb{P} \subset \mathbb{R}^3$ is a bounded, connected open set such that $\partial\mathbb{P} = \partial\overline{\mathbb{P}} = \bigcup \overline{D}_j$ where

- each D_j is a polygonal domain with straight edges contained in an affine 2-dimensional subspace of $\mathbb{R}^3$

• each edge is contained in exactly two closures of polygonal domains $\overline{D}_j$.

(See Subsection 1.6 for the definition of a polygonal domain.)

The vertices of the polygonal domains D_j will form the vertices of $\mathbb{P}$. The edges of the polygonal domains D_j will form the edges of $\mathbb{P}$. For each vertex P of $\mathbb{P}$, we choose a small open ball V_P centered in P. We assume that the neighborhoods V_P are chosen to be disjoint. For each vertex P, there exists a unique closed polyhedral cone C_P with vertex at P, such that $\overline{\mathbb{P}} \cap V_P = C_P \cap V_P$. Then $\mathbb{P} \subset \bigcup C_P$.

We now proceed to define canonical weight functions of $\mathbb{P}$ in analogy with the definition of canonical weights of curvilinear polygonal domains, Definition 1.10. We want to define first a continuous function $r_{\mathbb{P}} : \overline{\Omega} \to [0, \infty)$ that is positive and differentiable outside the edges. Let $\vartheta(x)$ be the distance from x to the edges of $\mathbb{P}$, as before. We want $r_{\mathbb{P}}(x) = \vartheta(x)$ close to the edges but far from the vertices and we want the quotients $r_{\mathbb{P}}(x)/\vartheta(x)$ and $\vartheta(x)/r_{\mathbb{P}}(x)$ to extend to continuous functions on $\overline{\Omega}$. Using a smooth partition of unity, in order to define $r_{\mathbb{P}}$, we need to define it close to the vertices.

Let us then denote by $\{P_k\}$ the set of vertices of $\mathbb{P}$. Choose a continuous function $r : \overline{\mathbb{P}} \to [0, \infty)$ such that $r(x)$ is the distance from x to the vertex P if $x \in V_P \cap \mathbb{P}$, and such that $r(x)$ is differentiable and positive on $\overline{\mathbb{P}} \smallsetminus \{P_k\}$. Let S^2 be the unit sphere centered at P and let r_P be a canonical weight associated to the curvilinear polygon $C_P \cap S^2$ (see Definition 1.10). We extend this function to C_P to be constant along the rays, except at P, where $r_P(P) = 0$. Finally, we let $r_{\mathbb{P}}(x) = r(x) r_P(x)$, for x close to P. Then a *canonical weight of* $\mathbb{P}$ is any function of the form $\psi r_{\mathbb{P}}$, where ψ is a smooth, nowhere vanishing function on $\overline{\mathbb{P}}$.

For any canonical weight $r_{\mathbb{P}}$, we then we have the following analogue of Equation (12)

$$\mathcal{K}_a^m(\mathbb{P}) := \mathcal{K}_a^m(\mathbb{P}; \vartheta) = \mathcal{K}_a^m(\mathbb{P}; r_{\mathbb{P}}). \tag{35}$$

Let us define, for every vertex P of $\mathbb{P}$, a spherical coordinate map $\Theta_P : \mathbb{P} \smallsetminus \{P\} \to S^2$ by $\Theta_P(x) = |x - P|^{-1}(x - P)$. Then, for each edge $e = [AB]$ of $\mathbb{P}$ joining the vertices A and B, we define a generalized cylindrical coordinate system (r_e, θ_e, z_e) to satisfy the following properties:

(i) $r_e(x)$ be the distance from x to the line containing e.

(ii) A as the origin (i. e., $r_e(A) = z_e(A) = 0$),

(iii) $\theta_e = 0$ on one of the two faces containing e, and

(iv) $z_e \geq 0$ on the edge e.

Let $\psi : S^2 \to [0, 1]$ be a smooth function on the unit sphere that is equal to 1 in a neighborhood of $(0, 0, 1) = \{\phi = 0\} \cap S^2$ and is equal to 0 in a neighborhood of $(0, 0, -1) = \{\phi = \pi\} \cap S^2$. Then we let

$$\tilde{\theta}_e(x) = \theta_e(x) \psi(\Theta_A(x)) \psi(-\Theta_B(x))$$

where $\theta_e(x)$ is the θ coordinate of x in a cylindrical coordinate system (r, θ, z) in which the point A corresponds to the origin (i. e., $r = 0$ and $z = 0$) and the edge AB points in the positive direction of the z axis (i. e., B corresponds to

$r = 0$ and $z > 0$). By choosing ψ to have support small enough in S^2 we may assume that the function $\tilde{\theta}_e$ is defined everywhere on $\mathbb{P} \smallsetminus e$. (This is why we need the cut-off function ψ.)
We then consider the function

$$\Phi : \mathbb{P} \to \mathbb{R}^N, \quad \Phi(x) = (x, \Theta_P(x), r_e(x), \tilde{\theta}_e(x)),$$

with $N = 3 + 3n_v + 2n_e$, n_v being the number of vertices of $\mathbb{P}$ and n_e being the number of edges of $\mathbb{P}$. Finally, we define $\Sigma(\mathbb{P})$ to be the closure of $\Phi(\mathbb{P})$ in $\mathbb{R}^N$. Then $\Sigma(\mathbb{P})$ is a manifold with corners that can be endowed with the structure of a Lie manifold with true boundary as follows. (Recall that a Lie manifold with boundary Σ is the closure $\overline{\Omega}$ of a regular open subset Ω in a Lie manifold M and the *true boundary* of Σ is the topological boundary $\partial_{\mathrm{top}}\Omega$.) The true boundary $\partial_{\mathrm{top}}\Sigma(\Omega)$ of $\Sigma(\Omega)$ is defined as the union of the closures of the faces D_j of $\mathbb{P}$ in $\Sigma(\mathbb{P})$. (Note that the closures of D_j in $\Sigma(\mathbb{P})$ are disjoint.) We can then take M to be the union of two copies of $\Sigma(\mathbb{P})$ with the true boundaries identified (i. e., the double of $\Sigma(\mathbb{P})$) and $\Omega = \Sigma(\mathbb{P}) \smallsetminus \partial_{\mathrm{top}}\Sigma(\mathbb{P})$. In particular, $\Omega_0 := \Omega \cap M_0$ identifies with $\mathbb{P}$.
To complete the definition of the Lie manifold with true boundary on $\Sigma(\mathbb{P})$, we now define the structural Lie algebra of vector fields $\mathcal{V}(\mathbb{P})$ of $\Sigma(\mathbb{P})$ by

$$\mathcal{V}(\mathbb{P}) := \{r_{\mathbb{P}}(\phi_1\partial_1 + \phi_2\partial_2 + \phi_3\partial_3),\ \phi_j \in \mathcal{C}^\infty(\Sigma(\mathbb{P}))\}. \tag{36}$$

(Here ∂_j are the standard unit vector fields. Also, the vector fields in $\mathcal{V}(\mathbb{P})$ are determined by their restrictions to $\mathbb{P}$.) This is consistent with the fact that $\partial_{\mathrm{top}}\Sigma(\mathbb{P})$, the true boundary of $\Sigma(\mathbb{P})$, is defined as the union of the boundary hyperfaces of $\Sigma(\mathbb{P})$ to which not all vector fields are tangent. This completes the definition of the structure of Lie manifold with boundary on $\Sigma(\mathbb{P})$.
The function $r_{\mathbb{P}}$ is easily seen to be an admissible weight on $\Sigma(\mathbb{P})$. It hence satisfies

$$r_{\mathbb{P}}(\partial_j r_{\mathbb{P}}) = r_{\mathbb{P}} \frac{\partial r_{\mathbb{P}}}{\partial x_j} \in \mathcal{C}^\infty(\Sigma(\mathbb{P})),$$

which is equivalent to the fact that $\mathcal{V}(\mathbb{P})$ is a Lie algebra. This is the analogue of Equation (11).
To check that $\Sigma(\mathbb{P})$ is a Lie manifold, let us notice first that $g = r_{\mathbb{P}}^{-2} g_E$ is a compatible metric on $\Sigma(\mathbb{P})$, where g_E is the Euclidean metric on $\mathbb{P}$. Then, let us denote by ν the outer unit normal to $\mathbb{P}$ (where it is defined), then $r_{\mathbb{P}}\partial_\nu$ is the restriction to $\partial_{\mathrm{top}}\Sigma(\Omega)$ of a vector field in $\mathcal{V}(\mathbb{P})$. Moreover $r_{\mathbb{P}}\partial_\nu$ is of length one and orthogonal to the true boundary in the compatible metric $g = r_{\mathbb{P}}^{-2} g_E$. The definition of $\mathcal{V}(\mathbb{P})$ together with our definition of Sobolev spaces on Lie manifolds using vector fields shows that

$$\mathcal{K}_a^m(\mathbb{P}) = r_{\mathbb{P}}^{a-3/2} W^{m,2}(\Sigma(\mathbb{P})) = r_{\mathbb{P}}^{a-3/2} H^m(\Sigma(\mathbb{P})). \tag{37}$$

The induced Lie manifold structure on $\Sigma(\mathbb{P})$ consists of the vector fields on the faces D_j that vanish on the boundary of D_j. The Soblev spaces on the boundary are

$$\mathcal{K}_a^m(\partial\mathbb{P}) = r_{\mathbb{P}}^{a-1} W^{m,2}(\partial_{\mathrm{top}}\Sigma(\mathbb{P})) = r_{\mathbb{P}}^{a-1} H^m(\partial_{\mathrm{top}}\Sigma(\mathbb{P})). \tag{38}$$

The factors $-3/2$ and -1 in the powers of $r_{\mathbb{P}}$ appearing in the above two equations are due to the fact that the volume elements on $\mathbb{P}$ and $\Sigma(\mathbb{P})$ differ by these factors.
If P is an order m differential operator with smooth coefficients on $\mathbb{R}^3$ and $\mathbb{P} \subset \mathbb{R}^3$ is a polyhedral domain, then $r_{\mathbb{P}}^m P \in \mathrm{Diff}_{\mathcal{V}}^m(\Sigma(\mathbb{P}))$, by Equation (10). However, in general, $r_{\mathbb{P}}^m P$ will not define a smooth differential operator on $\overline{\mathbb{P}}$. In particular, we have the following theorem, which is a direct analog of Proposition 4.8, if we replace "vertices" with "edges:"

Theorem 6.1. *Let $\mathbb{P} \subset \mathbb{R}^3$ be a polyhedral domain and P be a differential operator of order m with coefficients in $\mathcal{C}^\infty(\overline{\mathbb{P}})$. Then $P_\lambda := r_{\mathbb{P}}^\lambda P r_{\mathbb{P}}^{-\lambda}$ defines a continuous family of bounded maps $P_\lambda : \mathcal{K}_a^s(\mathbb{P}) \to \mathcal{K}_{a-m}^{s-m}(\mathbb{P})$, for any $s, a \in \mathbb{R}$. Let $\mathbb{P}'$ be $\overline{\mathbb{P}}$ with the* edges *removed. Then $\mathcal{C}_c^\infty(\mathbb{P}')$ is dense in $\mathcal{K}_a^m(\mathbb{P})$. Also, the restriction to the boundary extends to a continuous, surjective trace map $\mathcal{K}_a^s(\mathbb{P}) \to \mathcal{K}_{a-1/2}^{s-1/2}(\partial\mathbb{P})$. If $s = 1$, then the kernel of the trace map is the closure of $\mathcal{C}_c^\infty(\mathbb{P})$ in $\mathcal{K}_a^1(\mathbb{P})$.*

See [11] for applications of these results, especially of the above theorem.
Theorem 5.1 and the results of this section immediately lead to the proof of Theorem 0.1 formulated in the Introduction.

7. A non-standard boundary value problem

We present in this section a non-standard boundary value problem on a smooth manifold with boundary. Let $\mathcal{O}$ be a smooth manifold with boundary. We shall assume that $\mathcal{O}$ is connected and that the boundary is not empty.
Let $r : \overline{\mathcal{O}} \to [0, \infty)$ be a smooth function that close to the boundary is equal to the distance to the boundary and is > 0 on $\mathcal{O}$. Then we recall [14] that there exists a constant depending only on $\mathcal{O}$ such that

$$\int_{\mathcal{O}} r^{-2} |u(x)|^2 dx \leq C \int_{\mathcal{O}} |\nabla u(x)|^2 dx \tag{39}$$

for any $u \in H^1(\mathcal{O})$ that vanishes at the boundary. If we denote, as in Equation (2),

$$\mathcal{K}_a^m(\mathcal{O}; r) := \{u \in L^2_{loc}(\mathcal{O}),\ r^{|\alpha|-a}\partial^\alpha u \in L^2(\mathcal{O}),\ \ |\alpha| \leq m\},\ m \in \mathbb{N} \cup \{0\},\ a \in \mathbb{R},$$

with norm $\|\cdot\|_{\mathcal{K}_a^m}$, the Equation (39) implies that $\|u\|_{\mathcal{K}_1^1} \leq C\|\nabla u\|_{L^2}$.
Let $M = \overline{\mathcal{O}}$ with the structural Lie algebra of vector fields

$$\mathcal{V} = \mathcal{V}_0 := \{X, X = 0 \text{ at } \partial\mathcal{O}\} = r\Gamma(M; TM),$$

(see Example 1.7). Recall from Subsection 1.4 that $\mathrm{Diff}_{\mathcal{V}}^m(M)$ is the space of order m differential operators on M generated by multiplication with functions in $\mathcal{C}^\infty(M)$ and by differentiation with vector fields $X \in \mathcal{V}$. It follows that

$$r^m P \in \mathrm{Diff}_{\mathcal{V}}^m(M) \tag{40}$$

for any differential operator P of order m with smooth coefficients on M.

Lemma 7.1. *The pair $(M, \mathcal{V})$ is a Lie manifold with $M_0 = \mathcal{O}$ satisfying*

$$\mathcal{K}^m_a(\mathcal{O}; r) = r^{a-n/2} H^m(M). \tag{41}$$

If P is a differential operator with smooth coefficients on M, then $r^m P$ is a differential operator generated by $\mathcal{V}$, and hence $P_\lambda := r^\lambda P r^{-\lambda}$ gives rise to a continuous family of bounded maps $P_\lambda : \mathcal{K}^s_a(\mathcal{O}; r) \to \mathcal{K}^{s-m}_{a-m}(\mathcal{O}; r)$.

Because of the above lemma, it makes sense to define $\mathcal{K}^s_a(\mathcal{O}; r) = r^{a-n/2} H^s(M)$, for all $s, a \in \mathbb{R}$, with norm denoted $\|\cdot\|_{\mathcal{K}^s_a}$. The regularity result (Theorem 5.1) then gives

Lemma 7.2. *Let P be an order m elliptic differential operator with smooth coefficients defined in a neighborhood of $M = \overline{\mathcal{O}}$. Then, for any $s, t \in \mathbb{R}$, there exists $C = C_{st} > 0$ such that*

$$\|u\|_{\mathcal{K}^s_a} \leq C\big(\|Pu\|_{\mathcal{K}^{s-m}_{a-m}} + \|u\|_{\mathcal{K}^t_a}\big).$$

In particular, let $u \in \mathcal{K}^t_a(\mathcal{O}; r)$ be such that $Pu \in \mathcal{K}^{s-m}_{a-m}(\mathcal{O}; r)$, then $u \in \mathcal{K}^s_a(\mathcal{O}; r)$. The same result holds for elliptic systems.

Proof. We first notice that $r^m P \in \mathrm{Diff}^m_{\mathcal{V}}(M)$ is an *elliptic operator* in the usual sense (that is, its principal symbol $\sigma^{(m)}(r^m P)$ does not vanish outside the zero section of A^*). For this we use that $\sigma^{(m)}(r^m P) = r^m \sigma^{(m)}(P)$ and that A^* is defined such that multiplication by r^m defines an isomorphism $\mathcal{C}^\infty(T^*M) \to \mathcal{C}^\infty(A^*)$ that maps order m elliptic symbols to elliptic symbols. Then the proof is exactly the same as that of Theorem 5.1, except that we do not need strong ellipticity, because we do not have boundary conditions (and hence we have no condition of the form $u = 0$ on the boundary). □

An alternative proof of our lemma is obtained using pseudodifferential operators generated by $\mathcal{V}$ [3] and their L^p–continuity.

Theorem 7.3. *There exists $\eta > 0$ such that $\Delta : \mathcal{K}^{a+1}_{s+1}(\mathcal{O}; r) \to \mathcal{K}^{a-1}_{s-1}(\mathcal{O}; r)$ is an isomorphism for all $s \in \mathbb{R}$ and all $|a| < \eta$.*

Proof. The proof is similar to that of Theorem 2.1 in [10], so we will be brief. Consider

$$B : \mathcal{K}^1_1(\mathcal{O}; r) \times \mathcal{K}^1_1(\mathcal{O}; r) \to \mathbb{C}, \quad B(u, v) = \int_{\mathcal{O}} \nabla u \cdot \nabla \overline{v} dx.$$

Then $|B(u, v)| \leq \|u\|_{\mathcal{K}^1_1} \|v\|_{\mathcal{K}^1_1}$, so B is continuous.
On the other hand, by Equation (39), $B(u, u) \geq \theta \|u\|^2_{\mathcal{K}^1_1}$, for all u with compact support on $\mathcal{O}$ and for some $\theta > 0$ independent of u. Since $\mathcal{C}^\infty_{\mathrm{c}}(\mathcal{O})$ is dense in $\mathcal{K}^1_1(\mathcal{O}; r)$, by Theorem 4.2, the Lax-Milgram Lemma can be used to conclude that

$$\Delta : \mathcal{K}^1_1(\mathcal{O}; r) \to \mathcal{K}^{-1}_{-1}(\mathcal{O}; r) := \mathcal{K}^1_1(\mathcal{O}; r)^*$$

is an isomorphism. Since multiplication by $r^a : \mathcal{K}^1_1(\mathcal{O}; r) \to \mathcal{K}^1_{a+1}(\mathcal{O}; r)$ is an isomorphism and the family $r^a \Delta r^{-a}$ depends continuously on a by Lemma 7.1,

we obtain that $\Delta : \mathcal{K}^1_{a+1}(\mathcal{O}; r) \to \mathcal{K}^{-1}_{a-1}(\mathcal{O}; r)$ is an isomorphism for $|a| < \eta$, for some $\eta > 0$ small enough.
Fix now a, $|a| < \eta$. We obtain that $\Delta : \mathcal{K}^{s+1}_{a+1}(\mathcal{O}; r) \to \mathcal{K}^{s-1}_{a-1}(\mathcal{O}; r)$ is a continuous, injective map, for all $s \geq 0$. The first part of the proof (for $a = 0$) together with the regularity result of Lemma 7.2 show that this map is also surjective. The Open Mapping Theorem therefore completes the proof for $s \geq 0$. For $s \leq 0$, the result follows by considering duals. □

It can be shown as in [10] that η is the least value for which $\Delta : \mathcal{K}^1_{\eta+1}(\mathcal{O}; r) \to \mathcal{K}^{-1}_{\eta-1}(\mathcal{O}; r)$ is not Fredholm. This, in principle, can be decided by using the Fredholm conditions in [43] that involve looking at the L^2 invertibility of the same differential operators when M is the half-space $\{x_{n+1} \geq 0\}$. See also [5] for some non-standard boundary value problems on exterior domains in weighted Sobolev spaces.

8. Pseudodifferential operators

We now recall the definition of pseudodifferential operators on M_0 generated by a Lie structure at infinity $(M, \mathcal{V})$ on M_0.

8.1. Definition. We fix in what follows a compatible Riemannian metric g on M_0 (that is, a metric coming by restriction from a metric on the bundle $A \to M$ extending TM_0), see Section 1. In order to simplify our discussion below, we shall use the metric g to trivialize all density bundles on M. Recall that M_0 with the induced metric is complete [4]. Also, recall that $A \to M$ is a vector bundle such that $\mathcal{V} = \Gamma(A)$.
Let $\exp_x : T_xM_0 \to M_0$ be the exponential map, which is everywhere defined because M_0 is complete. We let

$$\Phi : TM_0 \longrightarrow M_0 \times M_0, \quad \Phi(v) := (x, \exp_x(-v)),\ v \in T_xM_0, \tag{42}$$

If E is a real vector bundle with a metric, we shall denote by $(E)_r$ the set of all vectors v of E with $|v| < r$. Let $(M_0^2)_r := \{(x, y), x, y \in M_0,\ d(x, y) < r\}$. Then the map Φ of Equation (42) restricts to a diffeomorphism $\Phi : (TM_0)_r \to (M_0^2)_r$, for any $0 < r < r_{\mathrm{inj}}(M_0)$, where $r_{\mathrm{inj}}(M_0)$ is the injectivity radius of M_0, which was assumed to be positive. The inverse of Φ is of the form

$$(M_0^2)_r \ni (x, y) \longmapsto (x, \tau(x, y)) \in (TM_0)_r\,.$$

We shall denote by $S^m_{1,0}(E)$ the space of symbols of order m and type $(1, 0)$ on E (in Hörmander's sense) and by $S^m_{cl}(E)$ the space of classical symbols of order m on E [21, 42, 57, 59]. See [3] for a review of these spaces of symbols in our framework.
Let $\chi \in \mathcal{C}^\infty(A^*)$ be a smooth function that is equal to 1 on $(A^*)_r$ and is equal to 0 outside $(A^*)_{2r}$, for some $r < r_{\mathrm{inj}}(M_0)/3$. Then, following [3], we define

$$q(a)u(x) = (2\pi)^{-n} \int_{T^*M_0} e^{i\tau(x,y)\cdot\eta} \chi(x, \tau(x, y)) a(x, \eta) u(y)\, d\eta\, dy\,.$$

This integral is an oscillatory integral with respect to the symplectic measure on T^*M_0 [22]. Alternatively, we consider the measures on M_0 and on $T^*_xM_0$ defined by some choice of a metric on A and we integrate first in the fibers $T^*_xM_0$ and then on M_0. The map $\sigma_{tot} : S^m_{1,0}(A^*) \to \Psi^m(M_0)/\Psi^{-\infty}(M_0)$,

$$\sigma_{tot}(a) := q(a) + \Psi^{-\infty}(M_0)$$

is independent of the choice of the function $\chi \in \mathcal{C}^\infty_c((A)_r)$ [3].
We now enlarge the class of order $-\infty$ operators that we consider. Any $X \in \mathcal{V} = \Gamma(A)$ generates a global flow $\Psi_X : \mathbb{R} \times M \to M$ because X is tangent to all boundary faces of M and M is compact. Evaluation at $t = 1$ yields a diffeomorphism

$$\psi_X := \Psi_X(1, \cdot) : M \to M. \tag{43}$$

We now define the pseudodifferential calculus on M_0 that we will consider following [3]. See [28, 29, 41, 44] for the connections between this calculus and groupoids.

Definition 8.1. Fix $0 < r < r_{\mathrm{inj}}(M_0)$ and $\chi \in \mathcal{C}^\infty_c((A)_r)$ such that $\chi = 1$ in a neighborhood of $M \subseteq A$. For $m \in \mathbb{R}$, the space $\Psi^m_{1,0,\mathcal{V}}(M_0)$ of *pseudodifferential operators generated by the Lie structure at infinity* $(M, \mathcal{V})$ is defined to be the linear space of operators $\mathcal{C}^\infty_c(M_0) \to \mathcal{C}^\infty_c(M_0)$ generated by $q(a)$, $a \in S^m_{1,0}(A^*)$, and $q(b)\psi_{X_1} \dots \psi_{X_k}$, $b \in S^{-\infty}(A^*)$ and $X_j \in \Gamma(A)$, $\forall j$.
Similarly, the space $\Psi^m_{cl,\mathcal{V}}(M_0)$ of *classical pseudodifferential operators generated by the Lie structure at infinity* $(M, \mathcal{V})$ is obtained by using classical symbols a in the construction above.

We have that $\Psi^{-\infty}_{cl,\mathcal{V}}(M_0) = \Psi^{-\infty}_{1,0,\mathcal{V}}(M_0) =: \Psi^{-\infty}_{\mathcal{V}}(M_0)$ (we dropped some subscripts).

8.2. Properties. We now review some properties of the operators in $\Psi^m_{1,0,\mathcal{V}}(M_0)$ and $\Psi^m_{cl,\mathcal{V}}(M_0)$ from [3]. These properties will be used below. Let $\Psi^\infty_{1,0,\mathcal{V}}(M_0) = \bigcup_{m\in\mathbb{Z}} \Psi^m_{1,0,\mathcal{V}}(M_0)$ and $\Psi^\infty_{cl,\mathcal{V}}(M_0) = \bigcup_{m\in\mathbb{Z}} \Psi^m_{cl,\mathcal{V}}(M_0)$.
First of all, each operator $P \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ defines continuous maps $\mathcal{C}^\infty_c(M_0) \to \mathcal{C}^\infty(M_0)$, and $\mathcal{C}^\infty(M) \to \mathcal{C}^\infty(M)$, still denoted by P. An operator $P \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ has a distribution kernel k_P in the space $I^m(M_0 \times M_0, M_0)$ of distributions on $M_0 \times M_0$ that are conormal of order m to the diagonal, by [22]. If $P = q(a)$, then k_P has support in $(M_0 \times M_0)_r$. If we extend the exponential map $(TM_0)_r \to M_0 \times M_0$ to a map $A \to M$, then the distribution kernel of $P = q(a)$ is the restriction of a distribution, also denoted k_P in $I^m(A, M)$.
If $\mathcal{P}$ denotes the space of polynomial symbols on A^* and $\mathrm{Diff}(M_0)$ denotes the algebra of differential operators on M_0, then

$$\Psi^\infty_{1,0,\mathcal{V}}(M_0) \cap \mathrm{Diff}(M_0) = \mathrm{Diff}^\infty_{\mathcal{V}}(M) = q(\mathcal{P}). \tag{44}$$

The spaces $\Psi^m_{1,0,\mathcal{V}}(M_0)$ and $\Psi^m_{1,0,\mathcal{V}}(M_0)$ are independent of the choice of the metric on A and the function χ used to define it, but depend, in general, on the Lie structure at infinity (M, A) on M_0. They are also closed under multiplication, which is a quite non-trivial fact.

Theorem 8.2. *The spaces* $\Psi^{\infty}_{1,0,\mathcal{V}}(M_0)$ *and* $\Psi^{\infty}_{cl,\mathcal{V}}(M_0)$ *are filtered algebras that are closed under adjoints.*

For $\Psi^m_{1,0,\mathcal{V}}(M_0)$, the meaning of the above theorem is that

$$\Psi^m_{1,0,\mathcal{V}}(M_0)\Psi^{m'}_{1,0,\mathcal{V}}(M_0) \subseteq \Psi^{m+m'}_{1,0,\mathcal{V}}(M_0) \text{ and } \big(\Psi^m_{1,0,\mathcal{V}}(M_0)\big)^* = \Psi^m_{1,0,\mathcal{V}}(M_0)$$

for all $m, m' \in \mathbb{C} \cup \{-\infty\}$.
The usual properties of the principal symbol remain true.

Proposition 8.3. *The principal symbol establishes isomorphisms*

$$\sigma^{(m)} : \Psi^m_{1,0,\mathcal{V}}(M_0)/\Psi^{m-1}_{1,0,\mathcal{V}}(M_0) \to S^m_{1,0}(A^*)/S^{m-1}_{1,0}(A^*) \tag{45}$$

and

$$\sigma^{(m)} : \Psi^m_{cl,\mathcal{V}}(M_0)/\Psi^{m-1}_{cl,\mathcal{V}}(M_0) \to S^m_{cl}(A^*)/S^{m-1}_{cl}(A^*). \tag{46}$$

Moreover, $\sigma^{(m)}(q(a)) = a + S^{m-1}_{1,0}(A^*)$ *for any* $a \in S^m_{1,0}(A^*)$ *and* $\sigma^{(m+m')}(PQ) = \sigma^{(m)}(P)\sigma^{(m')}(Q)$, *for any* $P \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ *and* $Q \in \Psi^{m'}_{1,0,\mathcal{V}}(M_0)$.

We shall need also the following result.

Proposition 8.4. *Let* ρ *be a defining function of some hyperface of* M. *Then* $\rho^s\Psi^m_{1,0,\mathcal{V}}(M_0)\rho^{-s} = \Psi^m_{1,0,\mathcal{V}}(M_0)$ *and* $\rho^s\Psi^m_{cl,\mathcal{V}}(M_0)\rho^{-s} = \Psi^m_{cl,\mathcal{V}}(M_0)$ *for any* $s \in \mathbb{C}$.

8.3. Continuity on $W^{s,p}(M_0)$. The preparations above will allow us to prove the continuity of the operators $P \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ between suitable Sobolev spaces. This is the main result of this section. Some of the ideas and constructions in the proof below have already been used in 5.1, which the reader may find convenient to review first. Let us recall from Equation (25) that an admissible weight ρ of M is a function of the form $\rho := \prod_H \rho_H^{a_H}$, where $a_H \in \mathbb{R}$ and ρ_H is a defining function of H.

Theorem 8.5. *Let* ρ *be an admissible weight of* M *and let* $P \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ *and* $p \in (0,\infty)$. *Then* P *maps* $\rho^r W^{s,p}(M_0)$ *continuously to* $\rho^r W^{s-m,p}(M_0)$ *for any* $r, s \in \mathbb{R}$.

Proof. We have that P maps $\rho^r W^{s,p}(M_0)$ continuously to $\rho^r W^{s-m,p}(M_0)$ if, and only if, $\rho^{-r}P\rho^r$ maps $W^{s,p}(M_0)$ continuously to $W^{s-m,p}(M_0)$. By Proposition 8.4 it is therefore enough to check our result for $r = 0$.
We shall first prove our result if the Schwartz kernel of P has support close enough to the diagonal. To this end, let us choose $\epsilon < r_{\mathrm{inj}}(M_0)/9$ and assume that the distribution kernel of P is supported in the set $(M_0^2)_\epsilon := \{(x,y), d(x,y) < \epsilon\} \subset M_0^2$. This is possible by choosing the function χ used to define the spaces $\Psi^m_{1,0,\mathcal{V}}(M_0)$ to have support in the set $(M_0^2)_\epsilon$. There will be no loss of generality then to assume that $P = q(a)$.
Then choose a smooth function $\eta : [0,\infty) \to [0,1]$, $\eta(t) = 1$ if $t \le 6\epsilon$, $\eta(t) = 0$ if $t \ge 7\epsilon$. Let $\psi_x : B(x, 8\epsilon) \to B_{T_xM_0}(0, 8\epsilon)$ denote the normal system of

coordinates induced by the exponential maps $\exp_x : T_xM_0 \to M_0$. Denote $\pi : A \to M$ be the natural (vector bundle) projection and

$$B := A \times_M A := \{(\xi_1, \xi_2) \in A \times A, \pi(\xi_1) = \pi(\xi_2)\}, \tag{47}$$

which defines a vector bundle $B \to M$. In the language of vector bundles, $B := A \oplus A$. For any $x \in M_0$, let η_x denote the function $\eta \circ \exp_x$, and consider the operator $\eta_x P \eta_x$ on $B(x, 13\epsilon)$. The diffeomorphism ψ_x then will map this operator to an operator P_x on $B_{T_xM_0}(0, 8\epsilon)$. Then P_x maps continuously $W^{s,p}(T_xM_0) \to W^{s-m,p}(T_xM_0)$, by the continuity of pseudodifferential operators on $\mathbb{R}^n$ [60, XIII, §5] or [56].

The distribution kernel k_x of P_x is a distribution with compact support on

$$T_xM_0 \times T_xM_0 = A_x \times A_x = B_x$$

If $P = q(a) \in \Psi^m_{1,0,\mathcal{V}}(M_0)$, then the distributions k_x can be determined in terms of the distribution $k_P \in I^m(A, M)$ associated to P. This shows that the distributions k_x extend to a smooth family of distributions on the fibers of $B \to M$. From this, it follows that the family of operators $P_x : W^{s,p}(A_x) \to W^{s-m,p}(A_x)$, $x \in M_0$, extends to a family of operators defined for $x \in M$ (recall that $A_x = T_xM_0$ if $x \in M_0$). This extension is obtained by extending the distribution kernels. In particular, the resulting family P_x will depend smoothly on $x \in M$. Since M is compact, we obtain, in particular, that the norms of the operators P_x are uniformly bounded for $x \in M_0$.

By abuse of notation, we shall denote by $P_x : W^{s,p}(M_0) \to W^{s-m,p}(M_0)$ the induced family of pseudodifferential operators, and we note that it will still be a smooth family that is uniformly bounded in norm. Note that it is possible to extend P_x to an operator on M_0 because its distribution kernel has compact support.

Then choose the sequence of points $\{x_j\} \subset M_0$ and a partition of unity $\phi_j \in \mathcal{C}^\infty_c(M_0)$ as in Lemma 3.6. In particular, ϕ_j will have support in $B(x_j, 2\epsilon)$. Also, let $\psi_j : B(x_j, 4\epsilon) \to B_{\mathbb{R}^n}(0, 4\epsilon)$ denote the normal system of coordinates induced by the exponential maps $\exp_x : T_xM_0 \to M_0$ and some fixed isometries $T_xM_0 \simeq \mathbb{R}^n$. Then all derivatives of $\psi_j \circ \psi_k^{-1}$ are bounded on their domain of definition, with a bound that may depend on ϵ but does not depend on j and k [13, 54].

Let

$$\nu_{s,p}(u)^p := \sum_j \|(\phi_j u) \circ \psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)}.$$

be one of the several equivalent norms defining the topology on $W^{s,p}(M_0)$ (see Proposition 3.10 and Equation (21). It is enough to prove that

$$\nu_{s,p}(Pu)^p := \sum_j \|(\phi_j Pu) \circ \psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)} \le C \sum_j \|(\phi_j u) \circ \psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)} =: C\nu_{s,p}(u)^p, \tag{48}$$

for some constant C independent of u.

We now prove this statement. Indeed, for the reasons explained below, we have the following inequalities.

$$\sum_j \|(\phi_j Pu)\circ\psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)} \le C\sum_{j,k}\|(\phi_j P\phi_k u)\circ\psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)}$$
$$= C\sum_{j,k}\|(\phi_j P_{x_j}\phi_k u)\circ\psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)} \le C\sum_{j,k}\|(\phi_j\phi_k u)\circ\psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)}$$
$$\le C\sum_j \|(\phi_j u)\circ\psi_j^{-1}\|^p_{W^{s,p}(\mathbb{R}^n)} = C\nu_{s,p}(u)^p.$$

Above, the first and last inequalities are due to the fact that the family ϕ_j is uniformly locally finite, that is, there exists a constant κ such that at any given point x, at most κ of the functions $\phi_j(x)$ are different from zero. The first equality is due to the support assumptions on ϕ_j, ϕ_k, and P_{x_j}. Finally, the second inequality is due to the fact that the operators P_{x_j} are continuous, with norms bounded by a constant independent of j, as explained above. We have therefore proved that $P = q(a) \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ defines a bounded operator $W^{s,p}(M_0) \to W^{s-m,p}(M_0)$, provided that the Schwartz kernel of P has support in a set of the $(M_0^2)_\epsilon$, for $\epsilon < r_{\mathrm{inj}}(M_0)/9$.
Assume now that $P \in \Psi^{-\infty}_{\mathcal{V}}(M_0)$. We shall check that P is bounded as a map $W^{2k,p}(M_0) \to W^{-2k,p}(M_0)$. For $k = 0$, this follows from the fact that the Schwartz kernel of P is given by a smooth function $k(x, y)$ such that $\int_{M_0} |k(x, y)| d\,\mathrm{vol}_g(x)$ and $\int_{M_0} |k(x, y)| d\,\mathrm{vol}_g(y)$ are uniformly bounded in x and y. For the other values of k, it is enough to prove that the bilinear form

$$W^{2k,p}(M_0) \times W^{2k,p}(M_0) \ni (u, v) \mapsto \langle Pu, v\rangle \in \mathbb{C}$$

is continuous. Choose Q a parametrix of Δ^k and let $R = 1 - Q\Delta^k$ be as above. Let $R' = 1 - \Delta^k Q \in \Psi^{-\infty}_{\mathcal{V}}(M_0)$. Then

$$\langle Pu, v\rangle = \langle (QPQ)\Delta^k u, \Delta^k v\rangle + \langle (QPR)u, \Delta^k v\rangle + \langle (R'PQ)\Delta^k u, v\rangle + \langle (R'PR)u, v\rangle,$$

which is continuous since $QPQ, QPR, R'PQ$, and $R'PR$ are in $\Psi^{-\infty}_{\mathcal{V}}(M_0)$ and hence they are continuous on $L^p(M_0)$ and because $\Delta^k : W^{2k,p}(M_0) \to L^p(M_0)$ is continuous.
Since any $P \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ can be written $P = P_1 + P_2$ with $P_2 \in \Psi^{-\infty}_{\mathcal{V}}(M_0)$ and $P_1 = q(a) \in \Psi^m_{1,0,\mathcal{V}}(M_0)$ with support arbitrarily close to the diagonal in M_0, the result follows. □

We obtain the following standard description of Sobolev spaces.

Theorem 8.6. *Let $s \in \mathbb{R}_+$ and $p \in (1, \infty)$. We have that $u \in W^{s,p}(M_0)$ if, and only if, $u \in L^p(M_0)$ and $Pu \in L^p(M_0)$ for any $P \in \Psi^s_{1,0,\mathcal{V}}(M_0)$. The norm $u \mapsto \|u\|_{L^p(M_0)} + \|Pu\|_{L^p(M_0)}$ is equivalent to the original norm on $W^{s,p}(M_0)$ for any elliptic $P \in \Psi^s_{1,0,\mathcal{V}}(M_0)$.*
Similarly, the map $T : L^p(M_0)\oplus L^p(M_0) \ni (u, v) \mapsto u+Pv \in W^{-s,p}(M_0)$ is surjective and identifies $W^{-s,p}(M_0)$ with the quotient $(L^p(M_0)\oplus L^p(M_0))/\ker(T)$.

Proof. Clearly, if $u \in W^{s,p}(M_0)$, then $Pu, u \in L^p(M_0)$. Let us prove the converse. Assume $Pu, u \in L^p(M_0)$. Let $Q \in \Psi^{-s}_{1,0,\mathcal{V}}(M_0)$ be a parametrix of P and let $R, R' \in \Psi^{-\infty}_{\mathcal{V}}(M_0)$ be defined by $R := 1 - QP$ and $R' = 1 - PQ$. Then $u = QPu + Ru$. Since both $Q, R : L^p(M_0) \to W^{s,p}(M_0)$ are defined and bounded, $u \in W^{s,p}(M_0)$ and $\|u\|_{W^{s,p}(M_0)} \le C\big(\|u\|_{L^p(M_0)} + \|Pu\|_{L^p(M_0)}\big)$. This proves the first part.
To prove the second part, we observe that the mapping

$$W^{s,q}(M_0) \ni u \mapsto (u, Pu) \in L^q(M_0) \oplus L^q(M_0), \qquad q^{-1} + p^{-1} = 1,$$

is an isomorphism onto its image. The result then follows by duality using also the Hahn-Banach theorem. □

We conclude our paper with the sketch of a regularity results for solutions of elliptic equations. Recall the Sobolev spaces with weights $\rho^s W^{s,p}(\Omega_0)$ introduced in Equation (26).

Theorem 8.7. *Let $P \in \mathrm{Diff}^m_{\mathcal{V}}(M)$ be an order m elliptic operator on M_0 generated by $\mathcal{V}$. Let $u \in \rho^s W^{r,p}(M_0)$ be such that $Pu \in \rho^s W^{t,p}(M_0)$, $s, r, t \in \mathbb{R}$, $1 < p < \infty$. Then $u \in \rho^s W^{t+m,p}(M_0)$.*

Proof. Let $Q \in \Psi^{-\infty}_{\mathcal{V}}(M_0)$ be a parametrix of P. Then $R = I - QP \in \Psi^{-\infty}_{\mathcal{V}}(M_0)$. This gives $u = Q(Pu) + Ru$. But $Q(Pu) \in \rho^s W^{t+m,p}(M_0)$, by Theorem 8.5, because $Pu \in \rho^s W^{t,p}(M_0)$. Similarly, $Ru \in \rho^s W^{t+m,p}(M_0)$. This completes the proof. □

Note that the above theorem was already proved in the case $t \in \mathbb{Z}$ and $m = 2$, using more elementary methods, as part of Theorem 5.1. The proof here is much shorter, however, it attests to the power of pseudodifferential operator algebra techniques.

References

[1] R. A. Adams. *Sobolev spaces.* Pure and Applied Mathematics, Vol. 65. Academic Press, New York-London, 1975.

[2] K. Akutagawa and B. Botvinnik. Yamabe metrics on cylindrical manifolds. *Geom. Funct. Anal.*, 13(2):259–333, 2003.

[3] B. Ammann, R. Lauter, and V. Nistor. Pseudodifferential operators on manifolds with a Lie structure at infinity. To appear in Annals of Math.

[4] B. Ammann, R. Lauter, and V. Nistor. On the geometry of Riemannian manifolds with a Lie structure at infinity. *Int. J. Math. Math. Sci.*, (1-4):161–193, 2004.

[5] C. Amrouche, V. Girault, and J. Giroire. Dirichlet and Neumann exterior problems for the n-dimensional Laplace operator: an approach in weighted Sobolev spaces. *J. Math. Pures Appl. (9)*, 76(1):55–81, 1997.

[6] L. Andersson and M. Dahl. Scalar curvature rigidity for asymptotically locally hyperbolic manifolds. *Ann. Global Anal. Geom.*, 16(1):1–27, 1998.

[7] T. Aubin. Espaces de Sobolev sur les variétés riemanniennes. *Bull. Sc. math.*, 100:149–173, 1970.

[8] I. Babuška and A. K. Aziz. Survey lectures on the mathematical foundations of the finite element method. In *The mathematical foundations of the finite element method with applications to partial differential equations (Proc. Sympos., Univ. Maryland, Baltimore, Md., 1972)*, pages 1–359. Academic Press, New York, 1972. With the collaboration of G. Fix and R. B. Kellogg.

[9] C. Bacuta, V. Nistor, and L. Zikatanov. Boundary value problems and regularity on polyhedral domains. IMA preprint #1984, August 2004.

[10] C. Bacuta, V. Nistor, and L. Zikatanov. Improving the rate of convergence of 'high order finite elements' on polygons and domains with cusps. *Numerische Mathematik*, 100:165–184, 2005.

[11] C. Bacuta, V. Nistor, and L. Zikatanov. Improving the rate of convergence of high-order finite elements on polyhedra. I. A priori estimates. *Numer. Funct. Anal. Optim.*, 26(6):613–639, 2005.

[12] J. Bergh and J. Löfström. *Interpolation spaces. An introduction.* Springer-Verlag, Berlin, 1976. Grundlehren der Mathematischen Wissenschaften, No. 223.

[13] M. Cheeger, J. Gromov and M. Taylor. Finite propagation speed, kernel estimates for functions of the Laplace operator, and the geometry of complete Riemannian manifolds. *J. Differential Geom.*, 17(1):15–53, 1982.

[14] H. Donnelly. Spectrum of domains in Riemannian manifolds. *Illinois J. Math.*, 31(4):692–698, 1987.

[15] A. K. Erkip and E. Schrohe. Normal solvability of elliptic boundary value problems on asymptotically flat manifolds. *J. Funct. Anal.*, 109:22–51, 1992.

[16] L. C. Evans. *Partial differential equations*, volume 19 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 1998.

[17] M. P. Gaffney. The harmonic operator for exterior differential forms. *Proc. Nat. Acad. Sci. U. S. A.*, 37:48–50, 1951.

[18] G. Grubb. *Functional calculus of pseudodifferential boundary problems*, volume 65 of *Progress in Mathematics.* Birkhäuser Boston Inc., Boston, MA, second edition, 1996.

[19] E. Hebey. *Sobolev spaces on Riemannian manifolds*, volume 1635 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1996.

[20] E. Hebey. *Nonlinear analysis on manifolds: Sobolev spaces and inequalities*, volume 5 of *Courant Lecture Notes in Mathematics.* New York University Courant Institute of Mathematical Sciences, New York, 1999.

[21] L. Hörmander. *Pseudo-differential operators and hypoelliptic equations*, volume X of *Proc. Symp. in Pure Math. – Singular Integrals*, pages 138–183. Amer. Math. Soc., Providence, Rhode Island, 1967.

[22] L. Hörmander. *The analysis of linear partial differential operators,* vol. 3. *Pseudo-differential operators*, volume 274 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin - Heidelberg - New York, 1985.

[23] D. Jerison and C. E. Kenig. The inhomogeneous Dirichlet problem in Lipschitz domains. *J. Funct. Anal.*, 130(1):161–219, 1995.

[24] M. Karoubi. Homologie cyclique et K-theorie. *Asterisque*, 149:1–147, 1987.

[25] V. A. Kondrat′ev. Boundary value problems for elliptic equations in domains with conical or angular points. *Transl. Moscow Math. Soc.*, 16:227–313, 1967.

[26] V. A. Kozlov, V. G. Maz′ya, and J. Rossmann. *Elliptic boundary value problems in domains with point singularities*, volume 52 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[27] R. Lauter. Pseudodifferential analysis on conformally compact spaces. *Mem. Amer. Math. Soc.*, 163(777), 2003.

[28] R. Lauter, B. Monthubert, and V. Nistor. Pseudodifferential analysis on continuous family groupoids. *Doc. Math.*, 5:625–655 (electronic), 2000.

[29] R. Lauter, B. Monthubert, and V. Nistor. Spectral invariance for certain algebras of pseudodifferential operators. Preprint Nr. 1/02, Fachbereich Mathematik, Johannes Gutenberg-Universität Mainz, January 2002.

[30] R. Lauter and S. Moroianu. Homology of pseudodifferential operators on manifolds with fibered cusps. *Trans. Amer. Math. Soc.*, 355(8):3009–3046 (electronic), 2003.

[31] R. Lauter and V. Nistor. Analysis of geometric operators on open manifolds: a groupoid approach. In N. P. Landsman, M. Pflaum, and M. Schlichenmaier, editors, *Quantization of Singular Symplectic Quotients*, volume 198 of *Progress in Mathematics*, pages 181–229. Birkhäuser, Basel - Boston - Berlin, 2001.

[32] J. M. Lee and T. H. Parker. The Yamabe problem. *Bull. Am. Math. Soc., New Ser.*, 17:37–91, 1987.

[33] J.-L. Lions and E. Magenes. *Non-homogeneous boundary value problems and applications. Vol. I.* Springer-Verlag, New York, 1972. Translated from the French by P. Kenneth, Die Grundlehren der mathematischen Wissenschaften, Band 181.

[34] L. Maniccia and P. Panarese. Eigenvalue asymptotics for a class of md-elliptic ψdo's on manifolds with cylindrical exits. *Ann. Mat. Pura Appl. (4)*, 181(3):283–308, 2002.

[35] V. Maz'ya and J. Rossmann. Weighted L_p estimates of solutions to boundary value problems for second order elliptic systems in polyhedral domains. *ZAMM Z. Angew. Math. Mech.*, 83(7):435–467, 2003.

[36] R. Mazzeo. Elliptic theory of differential edge operators. I. *Commun. Partial Differ. Equations*, 16(10):1615–1664, 1991.

[37] R. B. Melrose. Pseudodifferential operators, corners and singular limits. In *Proceeding of the International Congress of Mathematicians, Kyoto*, pages 217–234, Berlin - Heidelberg - New York, 1990. Springer-Verlag.

[38] R. B. Melrose. *The Atiyah-Patodi-Singer index theorem.* Research Notes in Mathematics (Boston, Mass.). 4. Wellesley, MA: A. K. Peters, Ltd., 1993.

[39] R. B. Melrose. *Geometric scattering theory.* Stanford Lectures. Cambridge University Press, Cambridge, 1995.

[40] M. Mitrea and M. Taylor. Boundary layer methods for Lipschitz domains in Riemannian manifolds. *J. Funct. Anal.*, 163(2):181–251, 1999.

[41] B. Monthubert. Pseudodifferential calculus on manifolds with corners and groupoids. *Proc. Amer. Math. Soc.*, 127(10):2871–2881, 1999.

[42] A. Nagel and E. Stein. *Lectures on pseudodifferential operators: regularity theorems and applications to nonelliptic problems*, volume 24 of *Mathematical Notes.* Princeton University Press, Princeton, N.J., 1979.

[43] V. Nistor. Pseudodifferential opearators on non-compact manifolds and analysis on polyhedral domains. In *Workshop on Spectral Geometry of Manifolds with Boundary and Decomposition of Manifolds, Roskilde University*, pages 307–328, 2005.

[44] V. Nistor, A. Weinstein, and P. Xu. Pseudodifferential operators on groupoids. *Pacific J. Math.*, 189:117–152, 1999.

[45] W. Roelcke. Über den Laplace-Operator auf Riemannschen Mannigfaltigkeiten mit diskontinuierlichen Gruppen. *Math. Nachr.*, 21:131–149, 1960.

[46] J. Rossmann. On two classes of weighted Sobolev-Slobodetskiĭ spaces in a dihedral angle. In *Partial differential equations, Part 1, 2 (Warsaw, 1990)*, volume 2 of *Banach Center Publ., 27, Part 1*, pages 399–424. Polish Acad. Sci., Warsaw, 1992.

[47] T. Schick. Manifolds with boundary and of bounded geometry. *Math. Nachr.*, 223:103–120, 2001.

[48] R. Schoen. Conformal deformation of a Riemannian metric to constant scalar curvature. *J. Diff. Geom.*, 20:479–495, 1984.

[49] R. Schoen and S.-T. Yau. On the proof of the positive mass conjecture in general relativity. *Comm. Math. Phys.*, 65:45–76, 1979.

[50] R. Schoen and S.-T. Yau. Proof of the positive mass theorem. II. *Comm. Math. Phys.*, 79:231–260, 1981.

[51] E. Schrohe. Spectral invariance, ellipticity, and the Fredholm property for pseudodifferential operators on weighted Sobolev spaces. *Ann. Global Anal. Geom.*, 10(3):237–254, 1992.

[52] E. Schrohe. Fréchet algebra techniques for boundary value problems: Fredholm criteria and functional calculus via spectral invariance. *Math. Nachr.*, 199:145–185, 1999.

[53] E. Schrohe and B.-W. Schulze. Boundary value problems in Boutet de Monvel's algebra for manifolds with conical singularities II. In *Boundary value problems, Schrödinger operators, deformation quantization*, volume 8 of *Math. Top.* Akademie Verlag, Berlin, 1995.

[54] M. A. Shubin. Spectral theory of elliptic operators on noncompact manifolds. *Astérisque*, 207:5, 35–108, 1992. Méthodes semi-classiques, Vol. 1 (Nantes, 1991).

[55] L. Skrzypczak. Mapping properties of pseudodifferential operators on manifolds with bounded geometry. *J. London Math. Soc. (2)*, 57(3):721–738, 1998.
[56] E. Stein. *Singular integrals and differentiability properties of functions*. Princeton Mathematical Series, No. 30. Princeton University Press, Princeton, N.J., 1970.
[57] M. Taylor. *Pseudodifferential operators*, volume 34 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1981.
[58] M. Taylor. *Partial differential equations I, Basic theory*, volume 115 of *Applied Mathematical Sciences*. Springer-Verlag, New York, 1995.
[59] M. Taylor. *Partial differential equations II, Qualitative studies of linear equations*, volume 116 of *Applied Mathematical Sciences*. Springer-Verlag, New York, 1996.
[60] M. Taylor. *Partial differential equations III, Nonlinear equations*, volume 117 of *Applied Mathematical Sciences*. Springer-Verlag, New York, 1997.
[61] H. Triebel. Spaces of Besov-Hardy-Sobolev type on complete Riemannian manifolds. *Ark. Mat.*, 24(2):299–337, 1986.
[62] H. Triebel. Characterizations of function spaces on a complete Riemannian manifold with bounded geometry. *Math. Nachr.*, 130:321–346, 1987.
[63] A. Vasy. Propagation of singularities in many-body scattering. *Ann. Sci. École Norm. Sup. (4)*, 34(3):313–402, 2001.
[64] A. Vasy and M. Zworski. Semiclassical estimates in asymptotically Euclidean scattering. *Comm. Math. Phys.*, 212(1):205–217, 2000.
[65] G. C. Verchota. Layer potentials and regularity for the Dirichlet problem for Laplace's equation in Lipschitz domains. *J. Funct. Anal.*, 59(3):572–611, 1984.
[66] G. C. Verchota and A. L. Vogel. A multidirectional Dirichlet problem. *J. Geom. Anal.*, 13(3):495–520, 2003.
[67] E. Witten. A new proof of the positive energy theorem. *Comm. Math. Phys.*, 80:381–402, 1981.

Bernd Ammann
Institut Élie Cartan
Université Henri Poincaré
Nancy 1, B.P. 239
54506 Vandoeuvre-Les-Nancy
France
bernd.ammann@gmx.net

Alexandru D. Ionescu
University of Wisconsin
Department of Mathematics
Madison, WI 53705
USA
ionescu@math.wisc.edu

Victor Nistor
Pennsylvania State University
Math. Dept. University Park
PA 16802 USA
nistor@math.psu.edu

Acyclicity Versus Total Acyclicity for Complexes over Noetherian Rings

Srikanth Iyengar[1], Henning Krause

Received: October 4, 2005
Revised: June 14, 2006

Communicated by Max Karoubi

Abstract. It is proved that for a commutative noetherian ring with dualizing complex the homotopy category of projective modules is equivalent, as a triangulated category, to the homotopy category of injective modules. Restricted to compact objects, this statement is a reinterpretation of Grothendieck's duality theorem. Using this equivalence it is proved that the (Verdier) quotient of the category of acyclic complexes of projectives by its subcategory of totally acyclic complexes and the corresponding category consisting of injective modules are equivalent. A new characterization is provided for complexes in Auslander categories and in Bass categories of such rings.

2000 Mathematics Subject Classification: Primary: 16E05; Secondary: 13D05, 16E10, 18E30
Keywords and Phrases: Totally acyclic complex, dualizing complex, Gorenstein dimension, Auslander category, Bass category

Introduction

Let R be a commutative noetherian ring with a dualizing complex D; in this article, this means, in particular, that D is a bounded complex of injective R-modules; see Section 3 for a detailed definition. The starting point of the work described below was a realization that $\mathbf{K}(\operatorname{Prj} R)$ and $\mathbf{K}(\operatorname{Inj} R)$, the homotopy categories of complexes of projective R-modules and of injective R-modules, respectively, are equivalent. This equivalence comes about as follows: D consists of injective modules and, R being noetherian, direct sums of injectives are injective, so $D \otimes_R -$ defines a functor from $\mathbf{K}(\operatorname{Prj} R)$ to $\mathbf{K}(\operatorname{Inj} R)$. This

[1]S. I. was partly supported by NSF grant DMS 0442242

functor factors through $\mathbf{K}(\operatorname{Flat} R)$, the homotopy category of flat R-modules, and provides the lower row in the following diagram:

$$\mathbf{K}(\operatorname{Prj} R) \underset{\mathsf{inc}}{\overset{\mathsf{q}}{\rightleftarrows}} \mathbf{K}(\operatorname{Flat} R) \underset{D\otimes_R -}{\overset{\operatorname{Hom}_R(D,-)}{\rightleftarrows}} \mathbf{K}(\operatorname{Inj} R)$$

The triangulated structures on the homotopy categories are preserved by inc and $D\otimes_R -$. The functors in the upper row of the diagram are the corresponding right adjoints; the existence of q is proved in Proposition (2.4). Theorem (4.2) then asserts:

Theorem I. *The functor* $D\otimes_R -\colon \mathbf{K}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Inj} R)$ *is an equivalence of triangulated categories, with quasi-inverse* $\mathsf{q}\circ \operatorname{Hom}_R(D,-)$.

This equivalence is closely related to, and may be viewed as an extension of, Grothendieck's duality theorem for $\mathbf{D}^f(R)$, the derived category of complexes whose homology is bounded and finitely generated. To see this connection, one has to consider the classes of compact objects – the definition is recalled in (1.2) – in $\mathbf{K}(\operatorname{Prj} R)$ and in $\mathbf{K}(\operatorname{Inj} R)$. These classes fit into a commutative diagram of functors:

$$\begin{array}{ccc} \mathbf{K}^c(\operatorname{Prj} R) & \xrightarrow{D\otimes_R -} & \mathbf{K}^c(\operatorname{Inj} R) \\ {\scriptstyle \mathsf{P}}\downarrow{\scriptstyle\wr} & & {\scriptstyle\wr}\downarrow{\scriptstyle \mathsf{I}} \\ \mathbf{D}^f(R) & \xrightarrow{\mathbf{R}\operatorname{Hom}_R(-,D)} & \mathbf{D}^f(R) \end{array}$$

The functor P is induced by the composite

$$\mathbf{K}(\operatorname{Prj} R) \xrightarrow{\operatorname{Hom}_R(-,R)} \mathbf{K}(R) \xrightarrow{\mathsf{can}} \mathbf{D}(R)\,,$$

and it is a theorem of Jørgensen [11] that P is an equivalence of categories. The equivalence I is induced by the canonical functor $\mathbf{K}(R) \to \mathbf{D}(R)$; see [14]. Given these descriptions it is not hard to verify that $D\otimes_R -$ preserves compactness; this explains the top row of the diagram. Now, Theorem I implies that $D\otimes_R -$ restricts to an equivalence between compact objects, so the diagram above implies $\mathbf{R}\operatorname{Hom}_R(-,D)$ is an equivalence; this is one version of the duality theorem; see Hartshorne [9]. Conversely, given that $\mathbf{R}\operatorname{Hom}_R(-,D)$ is an equivalence, so is the top row of the diagram; this is the crux of the proof of Theorem I.

Theorem I appears in Section 4. The relevant definitions and the machinery used in the proof of this result, and in the rest of the paper, are recalled in Sections 1 and 2. In the remainder of the paper we develop Theorem (4.2) in two directions. The first one deals with the difference between the category of acyclic complexes in $\mathbf{K}(\operatorname{Prj} R)$, denoted $\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R)$, and its subcategory consisting of totally acyclic complexes, denoted $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)$. We consider also the injective counterparts. Theorems (5.3) and (5.4) are the main new results in this context; here is an extract:

Theorem II. *The quotients*

$$\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R)/\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R) \text{ and } \mathbf{K}_{\mathrm{ac}}(\operatorname{Inj} R)/\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)$$

are compactly generated, and there are, up to direct factors, equivalences

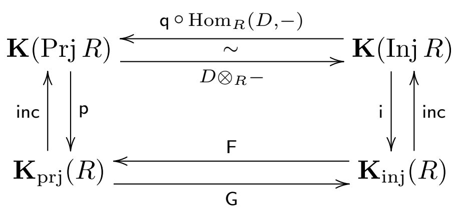
$$\operatorname{Thick}(R,D)/\operatorname{Thick}(R) \xrightarrow{\sim} \big[\big(\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R)/\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)\big)^{c}\big]^{\mathrm{op}}$$
$$\operatorname{Thick}(R,D)/\operatorname{Thick}(R) \xrightarrow{\sim} \big(\mathbf{K}_{\mathrm{ac}}(\operatorname{Inj} R)/\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)\big)^{c}.$$

In this result, $\operatorname{Thick}(R,D)$ is the thick subcategory of $\mathbf{D}^f(R)$ generated by R and D, while $\operatorname{Thick}(R)$ is the thick subcategory generated by R; that is to say, the subcategory of complexes of finite projective dimension. The quotient $\operatorname{Thick}(R,D)/\operatorname{Thick}(R)$ is a subcategory of the category $\mathbf{D}^f(R)/\operatorname{Thick}(R)$, which is sometimes referred to as the stable category of R. Since a dualizing complex has finite projective dimension if and only if R is Gorenstein, one corollary of the preceding theorem is that R is Gorenstein if and only if every acyclic complex of projectives is totally acyclic, if and only if every acyclic complex of injectives is totally acyclic.

Theorem II draws attention to the category $\operatorname{Thick}(R,D)/\operatorname{Thick}(R)$ as a measure of the failure of a ring R from being Gorenstein. Its role is thus analogous to that of the full stable category with regards to regularity: $\mathbf{D}^f(R)/\operatorname{Thick}(R)$ is trivial if and only if R is regular. See (5.6) for another piece of evidence that suggests that $\operatorname{Thick}(R,D)/\operatorname{Thick}(R)$ is an object worth investigating further.

In Section 6 we illustrate the results from Section 5 on local rings whose maximal ideal is square-zero. Their properties are of interest also from the point of view of Tate cohomology; see (6.5).

Sections 7 and 8 are a detailed study of the functors induced on $\mathbf{D}(R)$ by those in Theorem I. This involves two different realizations of the derived category as a subcategory of $\mathbf{K}(R)$, both obtained from the localization functor $\mathbf{K}(R) \to \mathbf{D}(R)$: one by restricting it to $\mathbf{K}_{\mathrm{prj}}(R)$, the subcategory of K-projective complexes, and the other by restricting it to $\mathbf{K}_{\mathrm{inj}}(R)$, the subcategory of K-injective complexes. The inclusion $\mathbf{K}_{\mathrm{prj}}(R) \to \mathbf{K}(\operatorname{Prj} R)$ admits a right adjoint p; for a complex X of projective modules the morphism $\mathsf{p}(X) \to X$ is a K-projective resolution. In the same way, the inclusion $\mathbf{K}_{\mathrm{inj}}(R) \to \mathbf{K}(\operatorname{Inj} R)$ admits a left adjoint i, and for a complex Y of injectives the morphism $Y \to \mathsf{i}(Y)$ is a K-injective resolution. Consider the functors $\mathsf{G} = \mathsf{i}\circ(D \otimes_R -)$ restricted to $\mathbf{K}_{\mathrm{prj}}(R)$, and $\mathsf{F} = \mathsf{p}\circ\mathsf{q}\circ\operatorname{Hom}_R(D,-)$ restricted to $\mathbf{K}_{\mathrm{inj}}(R)$. These functors better visualized as part of the diagram below:



It is clear that (G, F) is an adjoint pair of functors. However, the equivalence in the upper row of the diagram does not imply an equivalence in the lower one. Indeed, given Theorem I and the results in Section 5 it is not hard to prove:

The natural morphism $X \to \mathsf{FG}(X)$ is an isomorphism if and only if the mapping cone of the morphism $(D \otimes_R X) \to \mathsf{i}(D \otimes_R X)$ is totally acyclic.

The point of this statement is that the mapping cones of resolutions are, in general, only acyclic. Complexes in $\mathbf{K}_{\mathrm{inj}}(R)$ for which the morphism $\mathsf{GF}(Y) \to Y$ is an isomorphism can be characterized in a similar fashion; see Propositions (7.3) and (7.4). This is the key observation that allows us to describe, in Theorems (7.10) and (7.11), the subcategories of $\mathbf{K}_{\mathrm{prj}}(R)$ and $\mathbf{K}_{\mathrm{inj}}(R)$ where the functors G and F restrict to equivalences.

Building on these results, and translating to the derived category, we arrive at:

Theorem III. *A complex X of R-modules has finite G-projective dimension if and only if the morphism $X \to \mathbf{R}\mathrm{Hom}_R(D, D \otimes^{\mathbf{L}}_R X)$ in $\mathbf{D}(R)$ is an isomorphism and $H(D \otimes^{\mathbf{L}}_R X)$ is bounded on the left.*

The notion of finite G-projective dimension, and finite G-injective dimension, is recalled in Section 8. The result above is part of Theorem (8.1); its counterpart for G-injective dimensions is Theorem (8.2). Given these, it is clear that Theorem I restricts to an equivalence between the category of complexes of finite G-projective dimension and the category of complexes of finite G-injective dimension.

Theorems (8.1) and (8.2) recover recent results of Christensen, Frankild, and Holm [6], who arrived at them from a different perspective. The approach presented here clarifies the connection between finiteness of G-dimension and (total) acyclicity, and uncovers a connection between Grothendieck duality and the equivalence between the categories of complexes of finite G-projective dimension and of finite G-injective dimension by realizing them as different shadows of the same equivalence: that given by Theorem I.

So far we have focused on the case where the ring R is commutative. However, the results carry over, with suitable modifications in the statements and with nearly identical proofs, to non-commutative rings that possess dualizing complexes; the appropriate comments are collected towards the end of each section. We have chosen to present the main body of the work, Sections 4–8, in the commutative context in order to keep the underlying ideas transparent, and unobscured by notational complexity.

Notation. The following symbols are used to label arrows representing functors or morphisms: $\sim$ indicates an equivalence (between categories), $\cong$ an isomorphism (between objects), and $\simeq$ a quasi-isomorphism (between complexes).

1. Triangulated categories

This section is primarily a summary of basic notions and results about triangulated categories used frequently in this article. For us, the relevant examples of triangulated categories are homotopy categories of complexes over noetherian rings; they are the focus of the next section. Our basic references are Weibel [23], Neeman [19], and Verdier [22].

1.1. Triangulated categories. Let $\mathcal{T}$ be a triangulated category. We refer the reader to [19] and [22] for the axioms that define a triangulated category. When we speak of subcategories, it is implicit that they are full.

A non-empty subcategory $\mathcal{S}$ of $\mathcal{T}$ is said to be *thick* if it is a triangulated subcategory of $\mathcal{T}$ that is closed under retracts. If, in addition, $\mathcal{S}$ is closed under all coproducts allowed in $\mathcal{T}$, then it is *localizing*; if it is closed under all products in $\mathcal{T}$ it is *colocalizing.*

Let $\mathcal{C}$ be a class of objects in $\mathcal{T}$. The intersection of the thick subcategories of $\mathcal{T}$ containing $\mathcal{C}$ is a thick subcategory, denoted $\mathrm{Thick}(\mathcal{C})$. We write $\mathrm{Loc}(\mathcal{C})$, respectively, $\mathrm{Coloc}(\mathcal{C})$, for the intersection of the localizing, respectively, colocalizing, subcategories containing $\mathcal{C}$. Note that $\mathrm{Loc}(\mathcal{C})$ is itself localizing, while $\mathrm{Coloc}(\mathcal{C})$ is colocalizing.

1.2. Compact objects and generators. Let $\mathcal{T}$ be a triangulated category admitting arbitrary coproducts. An object X of $\mathcal{T}$ is *compact* if $\mathrm{Hom}_{\mathcal{T}}(X,-)$ commutes with coproducts; that is to say, for each coproduct $\coprod_i Y_i$ of objects in $\mathcal{T}$, the natural morphism of abelian groups

$$\coprod_i \mathrm{Hom}_{\mathcal{T}}(X, Y_i) \longrightarrow \mathrm{Hom}_{\mathcal{T}}\big(X, \coprod_i Y_i\big)$$

is bijective. The compact objects form a thick subcategory that we denote $\mathcal{T}^c$. We say that a class of objects $\mathcal{S}$ *generates* $\mathcal{T}$ if $\mathrm{Loc}(\mathcal{S}) = \mathcal{T}$, and that $\mathcal{T}$ is *compactly generated* if there exists a generating set consisting of compact objects.

Let $\mathcal{S}$ be a class of compact objects in $\mathcal{T}$. Then $\mathcal{S}$ generates $\mathcal{T}$ if and only if for any object Y of $\mathcal{T}$, we have $Y = 0$ provided that $\mathrm{Hom}_{\mathcal{T}}(\Sigma^n S, Y) = 0$ for all S in $\mathcal{S}$ and $n \in \mathbb{Z}$; see [18, (2.1)].

Adjoint functors play a useful, if technical, role in this work, and pertinent results on these are collected in the following paragraphs. MacLane's book [15, Chapter IV] is the basic reference for this topic; see also [23, (A.6)].

1.3. Adjoint functors. Given categories $\mathcal{A}$ and $\mathcal{B}$, a diagram

$$\mathcal{A} \underset{\mathsf{F}}{\overset{\mathsf{G}}{\leftrightarrows}} \mathcal{B}$$

indicates that F and G are adjoint functors, with F left adjoint to G; that is to say, there is a natural isomorphism $\mathrm{Hom}_{\mathcal{B}}(\mathsf{F}(A), B) \cong \mathrm{Hom}_{\mathcal{A}}(A, \mathsf{G}(B))$ for $A \in \mathcal{A}$ and $B \in \mathcal{B}$.

1.4. Let $\mathcal{T}$ be a category, $\mathcal{S}$ a full subcategory of $\mathcal{T}$, and $\mathsf{q}\colon \mathcal{T} \to \mathcal{S}$ a right adjoint of the inclusion $\mathsf{inc}\colon \mathcal{S} \to \mathcal{T}$. Then $\mathsf{q} \circ \mathsf{inc} \cong \mathsf{id}_{\mathcal{S}}$. Moreover, for each T in $\mathcal{T}$, an object P in $\mathcal{S}$ is isomorphic to $\mathsf{q}(T)$ if and only if there is a morphism $P \to T$ with the property that the induced map $\mathrm{Hom}_{\mathcal{T}}(S, P) \to \mathrm{Hom}_{\mathcal{T}}(S, T)$ is bijective for each $S \in \mathcal{S}$.

1.5. Let $\mathsf{F}\colon \mathcal{S} \to \mathcal{T}$ be an exact functor between triangulated categories such that $\mathcal{S}$ is compactly generated.

(1) The functor F admits a right adjoint if and only if it preserves coproducts.
(2) The functor F admits a left adjoint if and only if it preserves products.
(3) If F admits a right adjoint G, then F preserves compactness if and only if G preserves coproducts.

For (1), we refer to [18, (4.1)]; for (2), see [19, (8.6.1)]; for (3), see [18, (5.1)].

1.6. Orthogonal classes. Given a class $\mathcal{C}$ of objects in a triangulated category $\mathcal{T}$, the full subcategories

$$\begin{aligned} \mathcal{C}^{\perp} &= \{Y \in \mathcal{T} \mid \operatorname{Hom}_{\mathcal{T}}(\Sigma^n X, Y) = 0 \quad \text{for all } X \in \mathcal{C} \text{ and } n \in \mathbb{Z}\}\,, \\ {}^{\perp}\mathcal{C} &= \{X \in \mathcal{T} \mid \operatorname{Hom}_{\mathcal{T}}(X, \Sigma^n Y) = 0 \quad \text{for all } Y \in \mathcal{C} \text{ and } n \in \mathbb{Z}\}\,. \end{aligned}$$

are called the classes *right orthogonal* and *left orthogonal* to $\mathcal{C}$, respectively. It is elementary to verify that $\mathcal{C}^{\perp}$ is a colocalizing subcategory of $\mathcal{T}$, and equals $\operatorname{Thick}(\mathcal{C})^{\perp}$. In the same vein, ${}^{\perp}\mathcal{C}$ is a localizing subcategory of $\mathcal{T}$, and equals ${}^{\perp}\operatorname{Thick}(\mathcal{C})$.
Caveat: Our notation for orthogonal classes conflicts with the one in [19].

An additive functor $\mathsf{F}\colon \mathcal{A} \to \mathcal{B}$ between additive categories is an *equivalence up to direct factors* if F is full and faithful, and every object in $\mathcal{B}$ is a direct factor of some object in the image of F.

Proposition 1.7. *Let $\mathcal{T}$ be a compactly generated triangulated category and let $\mathcal{C} \subseteq \mathcal{T}$ be a class of compact objects.*

(1) *The triangulated category $\mathcal{C}^{\perp}$ is compactly generated. The inclusion $\mathcal{C}^{\perp} \to \mathcal{T}$ admits a left adjoint which induces, up to direct factors, an equivalence*
$$\mathcal{T}^c/\operatorname{Thick}(\mathcal{C}) \xrightarrow{\sim} (\mathcal{C}^{\perp})^c\,.$$
(2) *For each class $\mathcal{B} \subseteq \mathcal{C}$, the triangulated category $\mathcal{B}^{\perp}/\mathcal{C}^{\perp}$ is compactly generated. The canonical functor $\mathcal{B}^{\perp} \to \mathcal{B}^{\perp}/\mathcal{C}^{\perp}$ induces, up to direct factors, an equivalence*
$$\operatorname{Thick}(\mathcal{C})/\operatorname{Thick}(\mathcal{B}) \xrightarrow{\sim} (\mathcal{B}^{\perp}/\mathcal{C}^{\perp})^c\,.$$

Proof. First observe that $\mathcal{C}$ can be replaced by a set of objects because the isomorphism classes of compact objects in $\mathcal{T}$ form a set. Neeman gives in [17, (2.1)] a proof of (1); see also [17, p. 553 ff]. For (2), consider the following diagram

$$\begin{array}{ccccc} \mathcal{T}^c & \xrightarrow{\ \mathsf{can}\ } & \mathcal{T}^c/\operatorname{Thick}(\mathcal{B}) & \xrightarrow{\ \mathsf{can}\ } & \mathcal{T}^c/\operatorname{Thick}(\mathcal{C}) \\ \downarrow{\scriptstyle \mathsf{inc}} & & \downarrow & & \downarrow \\ \mathcal{T} & \underset{\mathsf{a}}{\overset{\mathsf{inc}}{\rightleftarrows}} & \mathcal{B}^{\perp} & \underset{\mathsf{b}}{\overset{\mathsf{inc}}{\rightleftarrows}} & \mathcal{C}^{\perp} \end{array}$$

where a and b denote adjoints of the corresponding inclusion functors and unlabeled functors are induced by a and b respectively. The localizing subcategory

$\mathrm{Loc}(\mathcal{C})$ of $\mathcal{T}$ is generated by $\mathcal{C}$ and hence it is compactly generated and its full subcategory of compact objects is precisely $\mathrm{Thick}(\mathcal{C})$; see [17, (2.2)]. Moreover, the composite

$$\mathrm{Loc}(\mathcal{C}) \xrightarrow{\mathsf{inc}} \mathcal{T} \xrightarrow{\mathsf{can}} \mathcal{T}/\mathcal{C}^{\perp}$$

is an equivalence. From the right hand square one obtains an analogous description of $\mathcal{B}^{\perp}/\mathcal{C}^{\perp}$, namely: the objects of $\mathcal{C}$ in $\mathcal{T}^c/\mathrm{Thick}(\mathcal{B})$ generate a localizing subcategory of $\mathcal{B}^{\perp}$, and this subcategory is compactly generated and equivalent to $\mathcal{B}^{\perp}/\mathcal{C}^{\perp}$. Moreover, the full subcategory of compact objects in $\mathcal{B}^{\perp}/\mathcal{C}^{\perp}$ is equivalent to the thick subcategory generated by $\mathcal{C}$ which is, up to direct factors, equivalent to $\mathrm{Thick}(\mathcal{C})/\mathrm{Thick}(\mathcal{B})$. □

2. Homotopy categories

We begin this section with a recapitulation on the homotopy category of an additive category. Then we introduce the main objects of our study: the homotopy categories of projective modules, and of injective modules, over a noetherian ring, and establish results which prepare us for the development in the ensuing sections.

Let $\mathcal{A}$ be an additive category; see [23, (A.4)]. We grade complexes cohomologically, thus a complex X over $\mathcal{A}$ is a diagram

$$\cdots \longrightarrow X^n \xrightarrow{\partial^n} X^{n+1} \xrightarrow{\partial^{n+1}} X^{n+2} \longrightarrow \cdots$$

with X^n in $\mathcal{A}$ and $\partial^{n+1} \circ \partial^n = 0$ for each integer n. For such a complex X, we write ΣX for its suspension: $(\Sigma X)^n = X^{n+1}$ and $\partial_{\Sigma X} = -\partial_X$.

Let $\mathbf{K}(\mathcal{A})$ be the homotopy category of complexes over $\mathcal{A}$; its objects are complexes over $\mathcal{A}$, and its morphisms are morphisms of complexes modulo homotopy equivalence. The category $\mathbf{K}(\mathcal{A})$ has a natural structure of a triangulated category; see [22] or [23].

Let R be a ring. Unless stated otherwise, modules are left modules; right modules are sometimes referred to as modules over R^{op}, the opposite ring of R. This proclivity for the left carries over to properties of the ring as well: when we say noetherian without any further specification, we mean left noetherian, etc. We write $\mathbf{K}(R)$ for the homotopy category of complexes over R; it is $\mathbf{K}(\mathcal{A})$ with $\mathcal{A}$ the category of R-modules. The paragraphs below contain basic facts on homotopy categories required in the sequel.

2.1. Let $\mathcal{A}$ be an additive category, and let X and Y complexes over $\mathcal{A}$. Set $\mathbf{K} = \mathbf{K}(\mathcal{A})$. Let d be an integer. We write $X^{\geqslant d}$ for the subcomplex

$$\cdots \to 0 \to X^d \to X^{d+1} \to \cdots$$

of X, and $X^{\leqslant d-1}$ for the quotient complex $X/X^{\geqslant d}$. In $\mathbf{K}$ these fit into an exact triangle

$$(*) \qquad X^{\geqslant d} \longrightarrow X \longrightarrow X^{\leqslant d-1} \longrightarrow \Sigma X^{\geqslant d}$$

This induces homomorphisms $\operatorname{Hom}_{\mathbf{K}}(X,Y) \to \operatorname{Hom}_{\mathbf{K}}(X^{\geqslant d},Y)$ and $\operatorname{Hom}_{\mathbf{K}}(X^{\leqslant d-1},Y) \to \operatorname{Hom}_{\mathbf{K}}(X,Y)$ of abelian groups. These have the following properties.

(1) One has isomorphisms of abelian groups:

$$H^d(\operatorname{Hom}_{\mathcal{A}}(X,Y)) \cong \operatorname{Hom}_{\mathbf{K}}(X,\Sigma^d Y) \cong \operatorname{Hom}_{\mathbf{K}}(\Sigma^{-d}X,Y)\,.$$

(2) If $Y^n = 0$ for $n \geq d$, then the map $\operatorname{Hom}_{\mathbf{K}}(X^{\leqslant d},Y) \to \operatorname{Hom}_{\mathbf{K}}(X,Y)$ is bijective.

(3) If $Y^n = 0$ for $n \leq d$, then the map $\operatorname{Hom}_{\mathbf{K}}(X,Y) \to \operatorname{Hom}_{\mathbf{K}}(X^{\geqslant d},Y)$ is bijective.

There are also versions of (2) and (3), where the hypothesis is on X.
Indeed, these remarks are all well-known, but perhaps (2) and (3) less so than (1). To verify (2), note that (1) implies

$$H^0(\operatorname{Hom}_{\mathcal{A}}(X^{\geqslant d+1},Y)) = 0 = H^1(\operatorname{Hom}_{\mathcal{A}}(X^{\geqslant d+1},Y))\,,$$

so applying $\operatorname{Hom}_{\mathcal{A}}(-,Y)$ to the exact triangle $(*)$ yields that the induced homomorphism of abelian groups

$$H^0(\operatorname{Hom}_{\mathcal{A}}(X^{\leqslant d},Y)) \longrightarrow H^0(\operatorname{Hom}_{\mathcal{A}}(X,Y))$$

is bijective, which is as desired. The argument for (3) is similar.

Now we recall, with proof, a crucial observation from [14, (2.1)]:

2.2. Let R be a ring, M an R-module, and let $\mathsf{i}M$ be an injective resolution of M. Set $\mathbf{K} = \mathbf{K}(R)$. If Y is a complex of injective R-modules, the induced map

$$\operatorname{Hom}_{\mathbf{K}}(\mathsf{i}M,Y) \longrightarrow \operatorname{Hom}_{\mathbf{K}}(M,Y)$$

is bijective. In particular, $\operatorname{Hom}_{\mathbf{K}}(\mathsf{i}R,Y) \cong H^0(Y)$.
Indeed, one may assume $(\mathsf{i}M)^n = 0$ for $n \leq -1$, since all injective resolutions of M are isomorphic in $\mathbf{K}$. The inclusion $M \to \mathsf{i}M$ leads to an exact sequence of complexes

$$0 \longrightarrow M \longrightarrow \mathsf{i}M \longrightarrow X \longrightarrow 0$$

with $X^n = 0$ for $n \leq -1$ and $H(X) = 0$. Therefore for $d = -1, 0$ one has isomorphisms

$$\operatorname{Hom}_{\mathbf{K}}(\Sigma^d X,Y) \cong \operatorname{Hom}_{\mathbf{K}}(\Sigma^d X,Y^{\geqslant -1}) = 0\,,$$

where the first one holds by an analogue of (2.1.2), and the second holds because $Y^{\geqslant -1}$ is a complex of injectives bounded on the left. It now follows from the exact sequence above that the induced map $\operatorname{Hom}_{\mathbf{K}}(\mathsf{i}M,Y) \to \operatorname{Hom}_{\mathbf{K}}(M,Y)$ is bijective.

The results below are critical ingredients in many of our arguments. We write $\mathbf{K}^{-,b}(\operatorname{prj} R)$ for the subcategory of $\mathbf{K}(R)$ consisting of complexes X of finitely generated projective modules with $H(X)$ bounded and $X^n = 0$ for $n \gg 0$, and $\mathbf{D}^f(R)$ for its image in $\mathbf{D}(R)$, the derived category of R-modules.

2.3. Let R be a (not necessarily commutative) ring.

(1) When R is coherent on both sides and flat R-modules have finite projective dimension, the triangulated category $\mathbf{K}(\operatorname{Prj} R)$ is compactly generated and the functors $\operatorname{Hom}_R(-,R)\colon \mathbf{K}(\operatorname{Prj} R) \to \mathbf{K}(R^{\mathrm{op}})$ and $\mathbf{K}(R^{\mathrm{op}}) \to \mathbf{D}(R^{\mathrm{op}})$ induce equivalences

$$\mathbf{K}^c(\operatorname{Prj} R) \xrightarrow{\sim} \mathbf{K}^{-,b}(\operatorname{prj} R^{\mathrm{op}})^{\mathrm{op}} \xrightarrow{\sim} \mathbf{D}^f(R^{\mathrm{op}})^{\mathrm{op}}.$$

(2) When R is noetherian, the triangulated category $\mathbf{K}(\operatorname{Inj} R)$ is compactly generated, and the canonical functor $\mathbf{K}(\operatorname{Inj} R) \to \mathbf{D}(R)$ induces an equivalence

$$\mathbf{K}^c(\operatorname{Inj} R) \xrightarrow{\sim} \mathbf{D}^f(R)$$

Indeed, (1) is a result of Jørgensen [11, (2.4)] and (2) is a result of Krause [14, (2.3)].

In the propositions below $d(R)$ denotes the supremum of the projective dimensions of all flat R-modules.

PROPOSITION 2.4. *Let R be a two-sided coherent ring such that $d(R)$ is finite. The inclusion $\mathbf{K}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Flat} R)$ admits a right adjoint:*

$$\mathbf{K}(\operatorname{Prj} R) \underset{\mathsf{inc}}{\overset{\mathsf{q}}{\rightleftarrows}} \mathbf{K}(\operatorname{Flat} R)$$

Moreover, the category $\mathbf{K}(\operatorname{Prj} R)$ admits arbitrary products.

Proof. By Proposition (2.3.1), the category $\mathbf{K}(\operatorname{Prj} R)$ is compactly generated. The inclusion inc evidently preserves coproducts, so (1.5.1) yields the desired right adjoint q. The ring R is right coherent, so the (set-theoretic) product of flat modules is flat, and furnishes $\mathbf{K}(\operatorname{Flat} R)$ with a product. Since inc is an inclusion, the right adjoint q induces a product on $\mathbf{K}(\operatorname{Prj} R)$: the product of a set of complexes $\{P_\lambda\}_{\lambda\in\Lambda}$ in $\mathbf{K}(\operatorname{Prj} R)$ is the complex $\mathsf{q}\big(\prod_\lambda P_\lambda\big)$. □

The proof of Theorem 2.7 below uses homotopy limits in the homotopy category of complexes; its definition is recalled below.

2.5. HOMOTOPY LIMITS. Let R be a ring and let $\cdots \to X(r+1) \to X(r)$ be a sequence of morphisms in $\mathbf{K}(R)$. The *homotopy limit* of the sequence $\{X(i)\}$, denoted $\operatorname{holim} X(i)$, is defined by an exact triangle

$$\operatorname{holim} X(i) \longrightarrow \prod_{i\geqslant r} X(i) \xrightarrow{\mathrm{id}-\mathrm{shift}} \prod_{i\geqslant r} X(i) \longrightarrow \Sigma \operatorname{holim} X(i)\,.$$

The homotopy limit is uniquely defined, up to an isomorphism in $\mathbf{K}(R)$; see [4] for details.

The result below identifies, in some cases, a homotopy limit in the homotopy category with a limit in the category of complexes.

LEMMA 2.6. *Let R be a ring. Consider a sequence of complexes of R-modules:*

$$\cdots \longrightarrow X(i) \xrightarrow{\varepsilon(i)} X(i-1) \longrightarrow \cdots \longrightarrow X(r+1) \xrightarrow{\varepsilon(r+1)} X(r)\,.$$

If for each degree n, there exists an integer s_n such that $\varepsilon(i)^n$ is an isomorphism for $i \geq s_n + 1$, then there exists a degree-wise split-exact sequence of complexes

$$0 \longrightarrow \varprojlim X(i) \longrightarrow \prod_i X(i) \xrightarrow{\text{id} - \text{shift}} \prod_i X(i) \longrightarrow 0\,.$$

In particular, it induces in $\mathbf{K}(R)$ an isomorphism holim $X(i) \cong \varprojlim X(i)$.

Proof. To prove the desired degree-wise split exactness of the sequence, it suffices to note that if $\cdots \longrightarrow M(r+1) \xrightarrow{\delta(r+1)} M(r)$ is a sequence of R-modules such that $\delta(i)$ is an isomorphism for $i \geq s+1$, for some integer s, then one has a split exact sequence of R-modules:

$$0 \longrightarrow M(s) \xrightarrow{\eta} \prod_i M(i) \xrightarrow{\text{id} - \text{shift}} \prod_i M(i) \longrightarrow 0\,,$$

where the morphism η is induced by $\eta_i \colon M(s) \to M(i)$ with

$$\eta_i = \begin{cases} \delta(i+1)\cdots\delta(s) & \text{if } i \leq s-1 \\ \text{id} & \text{if } i = s \\ \delta(i)^{-1}\cdots\delta(s+1)^{-1} & \text{if } i \geq s+1\,. \end{cases}$$

Indeed, in the sequence above, the map $(\text{id} - \text{shift})$ is surjective since the system $\{M_i\}$ evidently satisfies the Mittag-Leffler condition, see [23, (3.5.7)]. Moreover, a direct calculation shows that $\text{Im}(\eta) = \text{Ker}(\text{id} - \text{shift})$. It remains to note that the morphism $\pi\colon \prod M(i) \to M(s)$ defined by $\pi(a_i) = a_s$ is such that $\pi\eta = \text{id}$.
Finally, it is easy to verify that degree-wise split exact sequences of complexes induce exact triangles in the homotopy category. Thus, by the definition of homotopy limits, see (2.5), and the already established part of the lemma, we deduce: holim $X(i) \cong \varprojlim X(i)$ in $\mathbf{K}(R)$, as desired. □

The result below collects some properties of the functor $\mathsf{q}\colon \mathbf{K}(\text{Flat}\,R) \to \mathbf{K}(\text{Prj}\,R)$. It is noteworthy that the proof of part (3) describes an explicit method for computing the value of q on complexes bounded on the left. As usual, a morphism of complexes is called a *quasi-isomorphism* if the induced map in homology is bijective.

Theorem 2.7. *Let R be a two-sided coherent ring with $d(R)$ finite, and let F be a complex of flat R-modules.*

(1) *The morphism $\mathsf{q}(F) \to F$ is a quasi-isomorphism.*
(2) *If $F^n = 0$ for $n \gg 0$, then $\mathsf{q}(F)$ is a projective resolution of F.*
(3) *If $F^n = 0$ for $n \leq r$, then $\mathsf{q}(F)$ is isomorphic to a complex P with $P^n = 0$ for $n \leq r - d(R)$.*

Proof. (1) For each integer n, the map $\text{Hom}_{\mathbf{K}}(\Sigma^n R, \mathsf{q}(F)) \to \text{Hom}_{\mathbf{K}}(\Sigma^n R, F)$, induced by the morphism $\mathsf{q}(F) \to F$, is bijective; this is because R is in $\mathbf{K}(\text{Prj}\,R)$. Therefore (2.1.1) yields $H^{-n}(\mathsf{q}(F)) \cong H^{-n}(F)$, which proves (1).

(2) When $F^n = 0$ for $n \geq r$, one can construct a projective resolution $P \to F$ with $P^n = 0$ for $n \geq r$. Thus, for each $X \in \mathbf{K}(\operatorname{Prj} R)$ one has the diagram below

$$\operatorname{Hom}_{\mathbf{K}}(X^{\leqslant r}, P) = \operatorname{Hom}_{\mathbf{K}}(X, P) \to \operatorname{Hom}_{\mathbf{K}}(X, F) = \operatorname{Hom}_{\mathbf{K}}(X^{\leqslant r}, F)\,.$$

where equalities hold by (2.1.2). The complex $X^{\leqslant r}$ is K-projective, so the composed map is an isomorphism; hence the same is true of the one in the middle. This proves that $\mathsf{q}(F) \cong P$; see (1.4).

(3) We may assume $d(R)$ is finite. The construction of the complex P takes place in the category of complexes of R-modules. Note that $F^{>i}$ is a subcomplex of F for each integer $i \geq r$; denote $F(i)$ the quotient complex $F/F^{>i}$. One has surjective morphisms of complexes of R-modules

$$\cdots \longrightarrow F(i) \xrightarrow{\varepsilon(i)} F(i-1) \longrightarrow \cdots \longrightarrow F(r+1) \xrightarrow{\varepsilon(r+1)} F(r) = 0$$

with $\operatorname{Ker}(\varepsilon(i)) = \mathsf{\Sigma}^i F^i$. The surjections $F \to F(i)$ are compatible with the $\varepsilon(i)$, and the induced map $F \to \varprojlim F(i)$ is an isomorphism. The plan is to construct a commutative diagram in the category of complexes of R-modules

$$(\dagger)\qquad \begin{array}{ccccccccc}
\cdots \longrightarrow & P(i) & \xrightarrow{\delta(i)} & P(i-1) & \longrightarrow \cdots \longrightarrow & P(r+1) & \xrightarrow{\delta(r+1)} & P(r) = 0 \\
& \Big\downarrow{\scriptstyle \kappa(i)} & & \Big\downarrow{\scriptstyle \kappa(i-1)} & & \Big\downarrow{\scriptstyle \kappa(r+1)} & & \\
\cdots \longrightarrow & F(i) & \xrightarrow{\varepsilon(i)} & F(i-1) & \longrightarrow \cdots \longrightarrow & F(r+1) & \xrightarrow{\varepsilon(r+1)} & F(r) = 0
\end{array}$$

with the following properties: for each integer $i \geq r+1$ one has that

(a) $P(i)$ consists of projectives R-modules and $P(i)^n = 0$ for $n \notin (r - d(R), i]$;
(b) $\delta(i)$ is surjective, and $\operatorname{Ker} \delta(i)^n = 0$ for $n < i - d(R)$;
(c) $\kappa(i)$ is a surjective quasi-isomorphism.

The complexes $P(i)$ and the attendant morphisms are constructed iteratively, starting with $\kappa(r+1)\colon P(r+1) \to F(r+1) = \mathsf{\Sigma}^{r+1} F^{r+1}$ a surjective projective resolution, and $\delta(r+1) = 0$. One may ensure $P(r+1)^n = 0$ for $n \geq r+2$, and also for $n \leq r - d(R)$, because the projective dimension of the flat R-module F^{r+1} is at most $d(R)$. Note that $P(r+1)$, $\delta(r+1)$, and $\kappa(r+1)$ satisfy conditions (a)–(c).

Let $i \geq r+2$ be an integer, and let $\kappa(i-1)\colon P(i-1) \to F(i-1)$ be a homomorphism with the desired properties. Build a diagram of solid arrows

$$\begin{array}{ccccccccc}
0 \longrightarrow & Q & \dashrightarrow & P(i) & \overset{\delta(i)}{\dashrightarrow} & P(i-1) & \longrightarrow 0 \\
& \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \kappa(i)} & & \Big\downarrow{\scriptstyle \kappa(i-1)} & \\
0 \longrightarrow & \mathsf{\Sigma}^i F^i & \xrightarrow{\iota} & F(i) & \xrightarrow{\varepsilon(i)} & F(i-1) & \longrightarrow 0
\end{array}$$

where ι is the canonical injection, and $\theta\colon Q \to \mathsf{\Sigma}^i F^i$ is a surjective projective resolution, chosen such that $Q^n = 0$ for $n < i - d(R)$. The Horseshoe Lemma now yields a complex $P(i)$, with underlying graded R-module $Q \oplus P(i-1)$, and dotted morphisms that form the commutative diagram above; see [23, (2.2.8)].

It is clear that $P(i)$ and $\delta(i)$ satisfy conditions (a) and (b). As to (c): since both θ and $\kappa(i-1)$ are surjective quasi-isomorphisms, so is $\kappa(i)$. This completes the construction of the diagram (†).

Set $P = \varprojlim P(i)$; the limit is taken in the category of complexes. We claim that P is a complex of projectives and that $\mathsf{q}(F) \cong P$ in $\mathbf{K}(\operatorname{Prj} R)$.

Indeed, by property (b), for each integer n the map $P(i+1)^n \to P(i)^n$ is bijective for $i > n + d(R)$, so $P^n = P(n + d(R))^n$, and hence the R-module P^n is projective. Moreover $P^n = 0$ for $n \le r - d(R)$, by (a).

The sequences of complexes $\{P(i)\}$ and $\{F(i)\}$ satisfy the hypotheses of Lemma (2.6); the former by construction, see property (b), and the latter by definition. Thus, Lemma (2.6) yields the following isomorphisms in $\mathbf{K}(R)$:

$$\operatorname{holim} P(i) \cong P \qquad \text{and} \qquad \operatorname{holim} F(i) \cong F\,.$$

Moreover, the $\kappa(i)$ induce a morphism $\kappa\colon \operatorname{holim} P(i) \to \operatorname{holim} F(i)$ in $\mathbf{K}(R)$. Let X be a complex of projective R-modules. To complete the proof of (3), it suffices to prove that for each integer i the induced map

$$\operatorname{Hom}_{\mathbf{K}}(X, \kappa(i))\colon \operatorname{Hom}_{\mathbf{K}}(X, P(i)) \longrightarrow \operatorname{Hom}_{\mathbf{K}}(X, F(i))$$

is bijective. Then, a standard argument yields that $\operatorname{Hom}_{\mathbf{K}}(X, \kappa)$ is bijective, and in turn this implies $P \cong \operatorname{holim} P(i) \cong \mathsf{q}(\operatorname{holim} F(i)) \cong \mathsf{q}(F)$, see (1.4).

Note that, since $\kappa(i)$ is a quasi-isomorphism and $P(i)^n = 0 = F(i)^n$ for $n \ge i+1$, the morphism $\kappa(i)\colon P(i) \to F(i)$ is a projective resolution. Since projective resolutions are isomorphic in the homotopy category, it follows from (2) that $P(i) \cong \mathsf{q}(F(i))$, and hence that the map $\operatorname{Hom}_{\mathbf{K}}(X, \kappa(i))$ is bijective, as desired. Thus, (3) is proved. □

3. Dualizing complexes

Let R be a commutative noetherian ring. In this article, a *dualizing complex* for R is a complex D of R-modules with the following properties:

(a) the complex D is bounded and consists of injective R-modules;
(b) the R-module $H^n(D)$ is finitely generated for each n;
(c) the canonical map $R \to \operatorname{Hom}_R(D, D)$ is a quasi-isomorphism.

See Hartshorne [9, Chapter V] for basic properties of dualizing complexes. The presence of a dualizing complex for R implies that its Krull dimension is finite. As to the existence of dualizing complexes: when R is a quotient of a Gorenstein ring Q of finite Krull dimension, it has a dualizing complex: a suitable representative of the complex $\mathbf{R}\operatorname{Hom}_Q(R, Q)$ does the job. On the other hand, Kawasaki [13] has proved that if R has a dualizing complex, then it is a quotient of a Gorenstein ring.

3.1. A dualizing complex induces a contravariant equivalence of categories:

$$\mathbf{D}^f(R) \underset{\operatorname{Hom}_R(-,D)}{\overset{\operatorname{Hom}_R(-,D)}{\rightleftarrows}} \mathbf{D}^f(R)$$

This property characterizes dualizing complexes: if C is a complex of R-modules such that $\mathbf{R}\mathrm{Hom}_R(-,C)$ induces a contravariant self-equivalence of $\mathbf{D}^f(R)$, then C is isomorphic in $\mathbf{D}(R)$ to a dualizing complex for R; see [9, (V.2)]. Moreover, if D and E are dualizing complexes for R, then E is quasi-isomorphic to $P \otimes_R D$ for some complex P which is locally free of rank one; that is to say, for each prime ideal $\mathfrak{p}$ in R, the complex $P_\mathfrak{p}$ is quasi-isomorphic $\Sigma^n R_\mathfrak{p}$ for some integer n; see [9, (V.3)].

Remark 3.2. Let R be a ring with a dualizing complex. Then, as noted above, the Krull dimension of R is finite, so a result of Gruson and Raynaud [20, (II.3.2.7)] yields that the projective dimension of each flat R-module is at most the Krull dimension of R. The upshot is that Proposition (2.4) yields an adjoint functor

$$\mathbf{K}(\mathrm{Prj}\,R) \underset{\mathsf{inc}}{\overset{\mathsf{q}}{\rightleftarrows}} \mathbf{K}(\mathrm{Flat}\,R)$$

and this has properties described in Theorem (2.7). In the remainder of the article, this remark will be used often, and usually without comment.

In [6], Christensen, Frankild, and Holm have introduced a notion of a dualizing complex for a pair of, possibly non-commutative, rings:

3.3. Non-commutative rings. In what follows $\langle S, R\rangle$ denotes a pair of rings, where S is left noetherian and R is left coherent and right noetherian. This context is more restrictive than that considered in [6, Section 1], where it is not assumed that R is left coherent. We make this additional hypothesis on R in order to invoke (2.3.1).

3.3.1. A *dualizing complex* for the pair $\langle S, R\rangle$ is complex D of S-R bimodules with the following properties:

(a) D is bounded and each D^n is an S-R bimodule that is injective both as an S-module and as an R^{op}-module;
(b) $H^n(D)$ is finitely generated as an S-module and as an R^{op}-module for each n;
(c) the following canonical maps are quasi-isomorphisms:

$$R \longrightarrow \mathrm{Hom}_S(D,D) \quad \text{and} \quad S \longrightarrow \mathrm{Hom}_{R^{\mathrm{op}}}(D,D)$$

When R is commutative and $R = S$ this notion of a dualizing complex coincides with the one recalled in the beginning of this section. The appendix in [6] contains a detailed comparison with other notions of dualizing complexes in the non-commutative context.
The result below implies that the conclusion of Remark (3.2): existence of a functor q with suitable properties, applies also in the situation considered in (3.3).

Proposition 3.4. *Let D be a dualizing complex for the pair of rings $\langle S, R\rangle$, where S is left noetherian and R is left coherent and right noetherian.*

(1) *The projective dimension of each flat R-module is finite.*

(2) *The complex D induces a contravariant equivalence:*

$$\mathbf{D}^f(R^{\mathrm{op}}) \underset{\mathrm{Hom}_{R^{\mathrm{op}}}(-,D)}{\overset{\mathrm{Hom}_S(-,D)}{\rightleftarrows}} \mathbf{D}^f(S)$$

Indeed, (1) is contained in [6, (1.5)]. Moreover, (2) may be proved as in the commutative case, see [9, (V.2.1)], so we provide only a

Sketch of a proof of (2). By symmetry, it suffices to prove that for each complex X of right R-modules if $H(X)$ is bounded and finitely generated in each degree, then so is $H(\mathrm{Hom}_{R^{\mathrm{op}}}(X,D))$, as an S-module, and that the biduality morphism

$$\theta(X)\colon X \longrightarrow \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(X,D),D))$$

is a quasi-isomorphism. To begin with, since $H(X)$ is bounded, we may pass to a quasi-isomorphic complex and assume X is itself bounded, in which case the complex $\mathrm{Hom}_{R^{\mathrm{op}}}(X,D)$, and hence its homology, is bounded.
For the remainder of the proof, by replacing X by a suitable projective resolution, we assume that each X^i is a finitely generated projective module, with $X^i = 0$ for $i \gg 0$. In this case, for any bounded complex Y of S-R bimodules, if the S-module $H(Y)$ is finitely generated in each degree, then so is the S-module $H(\mathrm{Hom}_{R^{\mathrm{op}}}(X,Y))$; this can be proved by an elementary induction argument, based on the number

$$\sup\{i \mid H^i(Y) \neq 0\} - \inf\{i \mid H^i(Y) \neq 0\}\,,$$

keeping in mind that S is noetherian. Applied with $Y = D$, one obtains that each $H^i(\mathrm{Hom}_{R^{\mathrm{op}}}(X,D))$ is finitely generated, as desired.
As to the biduality morphism: fix an integer n, and pick an integer $d \leq n$ such that the morphism of complexes

$$\mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(X^{\geqslant d},D),D)) \longrightarrow \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(X,D),D))$$

is bijective in degrees $\geq n-1$; such a d exists because D is bounded. Therefore, $H^n(\theta(X))$ is bijective if and only if $H^n(\theta(X^{\geqslant d}))$ is bijective. Thus, passing to $X^{\geqslant d}$, we may assume that $X^i = 0$ when $|i| \gg 0$. One has then a commutative diagram of morphisms of complexes

$$\begin{array}{ccc} X \otimes_R R & \xrightarrow{X\otimes_R\theta(R)} & X \otimes_R \mathrm{Hom}_S(D,D) \\ \cong\downarrow & & \downarrow\cong \\ X & \xrightarrow[\simeq]{\theta(X)} & \mathrm{Hom}_S(\mathrm{Hom}_{R^{\mathrm{op}}}(X,D),D) \end{array}$$

The isomorphism on the right holds because X is a finite complex of finitely generated projectives; for the same reason, since $\theta(R)$ is a quasi-isomorphism, see (3.3.1.c), so is $X \otimes_R \theta(R)$. Thus, $\theta(X)$ is a quasi-isomorphism. This completes the proof. □

4. An equivalence of homotopy categories

The standing assumption in the rest of this article is that R is a *commutative* noetherian ring. Towards the end of each section we collect remarks on the extensions of our results to the non-commutative context described in (3.3).

The main theorem in this section is an equivalence between the homotopy categories of complexes of projectives and complexes of injectives. As explained in the discussion following Theorem I in the introduction, it may be viewed as an extension of the Grothendieck duality theorem, recalled in (3.1). Theorem (4.2) is the basis for most results in this work.

Remark 4.1. Let D be a dualizing complex for R; see Section 3.

For any flat module F and injective module I, the R-module $I \otimes_R F$ is injective; this is readily verified using Baer's criterion. Thus, $D \otimes_R -$ is a functor between $\mathbf{K}(\operatorname{Prj} R)$ and $\mathbf{K}(\operatorname{Inj} R)$, and it factors through $\mathbf{K}(\operatorname{Flat} R)$. If I and J are injective modules, the R-module $\operatorname{Hom}_R(I, J)$ is flat, so $\operatorname{Hom}_R(D, -)$ defines a functor from $\mathbf{K}(\operatorname{Inj} R)$ to $\mathbf{K}(\operatorname{Flat} R)$; evidently it is right adjoint to $D \otimes_R -\colon \mathbf{K}(\operatorname{Flat} R) \to \mathbf{K}(\operatorname{Inj} R)$.

Here is the announced equivalence of categories. The existence of q in the statement below is explained in Remark (3.2), and the claims implicit in the right hand side of the diagram are justified by the preceding remark.

Theorem 4.2. *Let R be a noetherian ring with a dualizing complex D. The functor $D \otimes_R -\colon \mathbf{K}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Inj} R)$ is an equivalence. A quasi-inverse is $\mathsf{q} \circ \operatorname{Hom}_R(D, -)$:*

$$\mathbf{K}(\operatorname{Prj} R) \underset{\mathsf{inc}}{\overset{\mathsf{q}}{\rightleftarrows}} \mathbf{K}(\operatorname{Flat} R) \underset{D\otimes_R -}{\overset{\operatorname{Hom}_R(D,-)}{\rightleftarrows}} \mathbf{K}(\operatorname{Inj} R)$$

where q denotes the right adjoint of the inclusion $\mathbf{K}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Flat} R)$.

4.3. The functors that appear in the theorem are everywhere dense in the remainder of this article, so it is expedient to abbreviate them: set

$$\mathsf{T} = D \otimes_R - : \mathbf{K}(\operatorname{Prj} R) \longrightarrow \mathbf{K}(\operatorname{Inj} R) \qquad \text{and}$$
$$\mathsf{S} = \mathsf{q} \circ \operatorname{Hom}_R(D, -)\colon \mathbf{K}(\operatorname{Inj} R) \longrightarrow \mathbf{K}(\operatorname{Prj} R)\,.$$

The notation 'T' should remind one that this functor is given by a tensor product. The same rule would call for an 'H' to denote the other functor; unfortunately, this letter is bound to be confounded with an 'H', so we settle for an 'S'.

Proof. By construction, $(\mathsf{inc}, \mathsf{q})$ and $(D \otimes_R -, \operatorname{Hom}_R(D, -))$ are adjoint pairs of functors. It follows that their composition (T, S) is an adjoint pair of functors as well. Thus, it suffices to prove that T is an equivalence: this would imply that S is its quasi-inverse, and hence also an equivalence.

Both $\mathbf{K}(\operatorname{Prj} R)$ and $\mathbf{K}(\operatorname{Inj} R)$ are compactly generated, by Proposition (2.3), and T preserves coproducts. It follows, using a standard argument, that it suffices to verify that T induces an equivalence $\mathbf{K}^c(\operatorname{Prj} R) \to \mathbf{K}^c(\operatorname{Inj} R)$. Observe that each complex P of finitely generated projective R-modules satisfies

$$\operatorname{Hom}_R(P, D) \cong D \otimes_R \operatorname{Hom}_R(P, R)\,.$$

Thus one has the following commutative diagram

$$\begin{array}{ccccc}
\mathbf{K}^{-,b}(\operatorname{prj} R) & \xrightarrow[\sim]{\operatorname{Hom}_R(-,R)} & \mathbf{K}^c(\operatorname{Prj} R) & \xrightarrow{\mathsf{T}} & \mathbf{K}^+(\operatorname{Inj} R) \\
\big\downarrow \wr & & & & \big\downarrow \wr \\
\mathbf{D}^f(R) & & \xrightarrow[\operatorname{Hom}_R(-,D)]{} & & \mathbf{D}^+(R)
\end{array}$$

By (2.3.2), the equivalence $\mathbf{K}^+(\operatorname{Inj} R) \to \mathbf{D}^+(R)$ identifies $\mathbf{K}^c(\operatorname{Inj} R)$ with $\mathbf{D}^f(R)$, while by (3.1), the functor $\operatorname{Hom}_R(-, D)$ induces an auto-equivalence of $\mathbf{D}^f(R)$. Hence, by the commutative diagram above, T induces an equivalence $\mathbf{K}^c(\operatorname{Prj} R) \to \mathbf{K}^c(\operatorname{Inj} R)$. This completes the proof. □

In the proof above we utilized the fact that $\mathbf{K}(\operatorname{Prj} R)$ and $\mathbf{K}(\operatorname{Inj} R)$ admit coproducts compatible with T. The categories in question also have products; this is obvious for $\mathbf{K}(\operatorname{Inj} R)$, and contained in Proposition (2.4) for $\mathbf{K}(\operatorname{Prj} R)$. The equivalence of categories established above implies:

Corollary 4.4. *The functors* T *and* S *preserve coproducts and products.*

Remark 4.5. Let $\mathsf{i}R$ be an injective resolution of R, and set $D^* = \mathsf{S}(\mathsf{i}R)$. Injective resolutions of R are uniquely isomorphic in $\mathbf{K}(\operatorname{Inj} R)$, so the complex $\mathsf{S}(\mathsf{i}R)$ is independent up to isomorphism of the choice of $\mathsf{i}R$, so one may speak of D^* without referring to $\mathsf{i}R$.

Lemma 4.6. *The complex* D^* *is isomorphic to the image of* D *under the composition*

$$\mathbf{D}^f(R) \xrightarrow{\sim} \mathbf{K}^{-,b}(\operatorname{prj} R) \xrightarrow{\operatorname{Hom}_R(-,R)} \mathbf{K}(\operatorname{Prj} R)\,.$$

Proof. The complex D is bounded and has finitely generated homology modules, so we may choose a projective resolution P of D with each R-module P^n finitely generated, and zero for $n \gg 0$. In view of Theorem (4.2), it suffices to verify that $\mathsf{T}(\operatorname{Hom}_R(P, R))$ is isomorphic to $\mathsf{i}R$. The complex $\mathsf{T}(\operatorname{Hom}_R(P, R))$, that is to say, $D \otimes_R \operatorname{Hom}_R(P, R)$ is isomorphic to the complex $\operatorname{Hom}_R(P, D)$, which consists of injective R-modules and is bounded on the left. Therefore $\operatorname{Hom}_R(P, D)$ is K-injective. Moreover, the composite

$$R \longrightarrow \operatorname{Hom}_R(D, D) \longrightarrow \operatorname{Hom}_R(P, D)$$

is a quasi-isomorphism, and one obtains that in $\mathbf{K}(\operatorname{Inj} R)$ the complex $\operatorname{Hom}_R(P, D)$ is an injective resolution of R. □

The objects in the subcategory $\operatorname{Thick}(\operatorname{Prj} R)$ of $\mathbf{K}(\operatorname{Prj} R)$ are exactly the complexes of finite projective dimension; those in the subcategory $\operatorname{Thick}(\operatorname{Inj} R)$ of $\mathbf{K}(\operatorname{Inj} R)$ are the complexes of finite injective dimension. It is known that the functor $D \otimes_R -$ induces an equivalence between these categories; see, for instance, [1, (1.5)]. The result below may be read as the statement that this equivalence extends to the full homotopy categories.

Proposition 4.7. *Let R be a noetherian ring with a dualizing complex D. The equivalence $\mathsf{T}\colon \mathbf{K}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Inj} R)$ restricts to an equivalence between* $\operatorname{Thick}(\operatorname{Prj} R)$ *and* $\operatorname{Thick}(\operatorname{Inj} R)$. *In particular,* $\operatorname{Thick}(\operatorname{Inj} R)$ *equals* $\operatorname{Thick}(\operatorname{Add} D)$.

Proof. It suffices to prove that the adjoint pair of functors (T, S) in Theorem (4.2) restrict to functors between $\operatorname{Thick}(\operatorname{Prj} R)$ and $\operatorname{Thick}(\operatorname{Inj} R)$.
The functor T maps R to D, which is a bounded complex of injectives and hence in $\operatorname{Thick}(\operatorname{Inj} R)$. Therefore T maps $\operatorname{Thick}(\operatorname{Prj} R)$ into $\operatorname{Thick}(\operatorname{Inj} R)$.
Conversely, given injective R-modules I and J, the R-module $\operatorname{Hom}_R(I, J)$ is flat. Therefore $\operatorname{Hom}_R(D, -)$ maps $\operatorname{Thick}(\operatorname{Inj} R)$ into $\operatorname{Thick}(\operatorname{Flat} R)$, since D is a bounded complex of injectives. By Theorem (2.7.2), for each flat R-module F, the complex $\mathsf{q}(F)$ is a projective resolution of F. The projective dimension of F is finite since R has a dualizing complex; see (3.2). Hence q maps $\operatorname{Thick}(\operatorname{Flat} R)$ to $\operatorname{Thick}(\operatorname{Prj} R)$. □

4.8. Non-commutative rings. Consider a pair of rings $\langle S, R\rangle$ as in (3.3), with a dualizing complex D. Given Proposition (3.4), the proof of Theorem (4.2) carries over verbatim to yield:

Theorem. *The functor $D \otimes_R -\colon \mathbf{K}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Inj} S)$ is an equivalence, and the functor $\mathsf{q} \circ \operatorname{Hom}_S(D, -)$ is a quasi-inverse.* □

This basic step accomplished, one can readily transcribe the remaining results in this section, and their proofs, to apply to the pair $\langle S, R\rangle$; it is clear what the corresponding statements should be.

5. Acyclicity versus total acyclicity

This section contains various results concerning the classes of (totally) acyclic complexes of projectives, and of injectives. We start by recalling appropriate definitions.

5.1. Acyclic complexes. A complex X of R-modules is *acyclic* if $H^n X = 0$ for each integer n. We denote $\mathbf{K}_{\mathrm{ac}}(R)$ the full subcategory of $\mathbf{K}(R)$ formed by acyclic complexes of R-modules. Set

$$\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R) = \mathbf{K}(\operatorname{Prj} R) \cap \mathbf{K}_{\mathrm{ac}}(R) \quad \text{and} \quad \mathbf{K}_{\mathrm{ac}}(\operatorname{Inj} R) = \mathbf{K}(\operatorname{Inj} R) \cap \mathbf{K}_{\mathrm{ac}}(R)\,.$$

Evidently acyclicity is a property intrinsic to the complex under consideration. Next we introduce a related notion which depends on a suitable subcategory of $\operatorname{Mod} R$.

5.2. Total acyclicity. Let $\mathcal{A}$ be an additive category. A complex X over $\mathcal{A}$ is *totally acyclic* if for each object $A \in \mathcal{A}$ the following complexes of abelian groups are acyclic.

$$\operatorname{Hom}_{\mathcal{A}}(A, X) \quad \text{and} \quad \operatorname{Hom}_{\mathcal{A}}(X, A)$$

We denote by $\mathbf{K}_{\text{tac}}(\mathcal{A})$ the full subcategory of $\mathbf{K}(\mathcal{A})$ consisting of totally acyclic complexes. Specializing to $\mathcal{A} = \operatorname{Prj} R$ and $A = \operatorname{Inj} R$ one gets the notion of a *totally acyclic complex of projectives* and a *totally acyclic complex of injectives*, respectively.

Theorems (5.3) and (5.4) below describe various properties of (totally) acyclic complexes. In what follows, we write $\mathbf{K}^c_{\text{ac}}(\operatorname{Prj} R)$ and $\mathbf{K}^c_{\text{ac}}(\operatorname{Inj} R)$ for the class of compact objects in $\mathbf{K}_{\text{ac}}(\operatorname{Prj} R)$ and $\mathbf{K}_{\text{ac}}(\operatorname{Inj} R)$, respectively; in the same way, $\mathbf{K}^c_{\text{tac}}(\operatorname{Prj} R)$ and $\mathbf{K}^c_{\text{tac}}(\operatorname{Inj} R)$ denote compacts among the corresponding totally acyclic objects.

THEOREM 5.3. *Let R be a noetherian ring with a dualizing complex D.*

(1) *The categories $\mathbf{K}_{\text{ac}}(\operatorname{Prj} R)$ and $\mathbf{K}_{\text{tac}}(\operatorname{Prj} R)$ are compactly generated.*
(2) *The equivalence $\mathbf{D}^f(R) \to \mathbf{K}^c(\operatorname{Prj} R)^{\text{op}}$ induces, up to direct factors, equivalences*

$$\mathbf{D}^f(R)/\operatorname{Thick}(R) \xrightarrow{\sim} \mathbf{K}^c_{\text{ac}}(\operatorname{Prj} R)^{\text{op}}$$
$$\mathbf{D}^f(R)/\operatorname{Thick}(R,D) \xrightarrow{\sim} \mathbf{K}^c_{\text{tac}}(\operatorname{Prj} R)^{\text{op}}.$$

(3) *The quotient $\mathbf{K}_{\text{ac}}(\operatorname{Prj} R)/\mathbf{K}_{\text{tac}}(\operatorname{Prj} R)$ is compactly generated, and one has, up to direct factors, an equivalence*

$$\operatorname{Thick}(R,D)/\operatorname{Thick}(R) \xrightarrow{\sim} \big[\big(\mathbf{K}_{\text{ac}}(\operatorname{Prj} R)/\mathbf{K}_{\text{tac}}(\operatorname{Prj} R)\big)^c\big]^{\text{op}}.$$

The proof of this result, and also of the one below, which is an analogue for complexes of injectives, is given in (5.10). It should be noted that, in both cases, part (1) is not new: for the one above, see the proof of [12, (1.9)], and for the one below, see [14, (7.3)].

THEOREM 5.4. *Let R be a noetherian ring with a dualizing complex D.*

(1) *The categories $\mathbf{K}_{\text{ac}}(\operatorname{Inj} R)$ and $\mathbf{K}_{\text{tac}}(\operatorname{Inj} R)$ are compactly generated.*
(2) *The equivalence $\mathbf{D}^f(R) \to \mathbf{K}^c(\operatorname{Inj} R)$ induces, up to direct factors, equivalences*

$$\mathbf{D}^f(R)/\operatorname{Thick}(R) \xrightarrow{\sim} \mathbf{K}^c_{\text{ac}}(\operatorname{Inj} R)$$
$$\mathbf{D}^f(R)/\operatorname{Thick}(R,D) \xrightarrow{\sim} \mathbf{K}^c_{\text{tac}}(\operatorname{Inj} R).$$

(3) *The quotient $\mathbf{K}_{\text{ac}}(\operatorname{Inj} R)/\mathbf{K}_{\text{tac}}(\operatorname{Inj} R)$ is compactly generated, and we have, up to direct factors, an equivalence*

$$\operatorname{Thick}(R,D)/\operatorname{Thick}(R) \xrightarrow{\sim} \big(\mathbf{K}_{\text{ac}}(\operatorname{Inj} R)/\mathbf{K}_{\text{tac}}(\operatorname{Inj} R)\big)^c.$$

Here is one consequence of the preceding results. In it, one cannot restrict to complexes (of projectives or of injectives) of finite modules; see the example in Section 6.

COROLLARY 5.5. *Let R be a noetherian ring with a dualizing complex. The following conditions are equivalent.*

(a) *The ring R is Gorenstein.*
(b) *Every acyclic complex of projective R-modules is totally acyclic.*

(c) *Every acyclic complex of injective R-modules is totally acyclic.*

Proof. Theorems (5.3.3) and (5.4.3) imply that (b) and (c) are equivalent, and that they hold if and only if D lies in $\operatorname{Thick}(R)$, that is to say, if and only if D has finite projective dimension. This last condition is equivalent to R being Gorenstein; see [5, (3.3.4)]. ☐

Remark 5.6. One way to interpret Theorems (5.3.3) and (5.4.3) is that the category $\operatorname{Thick}(R, D)/\operatorname{Thick}(R)$ measures the failure of the Gorenstein property for R. This invariant of R appears to possess good functorial properties. For instance, let R and S be local rings with dualizing complexes D_R and D_S, respectively. If a local homomorphism $R \to S$ is quasi-Gorenstein, in the sense of Avramov and Foxby [1, Section 7], then tensoring with S induces an equivalence of categories, up to direct factors:

$$- \otimes^{\mathbf{L}}_R S\colon \operatorname{Thick}(R, D_R)/\operatorname{Thick}(R) \xrightarrow{\sim} \operatorname{Thick}(S, D_S)/\operatorname{Thick}(S)$$

This is a quantitative enhancement of the ascent and descent of the Gorenstein property along such homomorphisms.

The notion of total acyclicity has a useful expression in the notation of (1.6).

LEMMA 5.7. *Let $\mathcal{A}$ be an additive category. One has $\mathbf{K}_{\mathrm{tac}}(\mathcal{A}) = \mathcal{A}^{\perp} \cap {}^{\perp}\mathcal{A}$, where $\mathcal{A}$ is identified with complexes concentrated in degree zero.*

Proof. By (2.1.1), for each A in $\mathcal{A}$ the complex $\operatorname{Hom}_{\mathcal{A}}(X, A)$ is acyclic if and only if $\operatorname{Hom}_{\mathbf{K}(\mathcal{A})}(X, \Sigma^n A) = 0$ for every integer n; in other words, if and only if X is in ${}^{\perp}\mathcal{A}$. By the same token, $\operatorname{Hom}_{\mathcal{A}}(A, X)$ is acyclic if and only if X is in $\mathcal{A}^{\perp}$. ☐

5.8. Let R be a ring. The following identifications hold:

$$\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R) = \mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R) \cap {}^{\perp}(\operatorname{Prj} R)$$
$$\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R) = (\operatorname{Inj} R)^{\perp} \cap \mathbf{K}_{\mathrm{ac}}(\operatorname{Inj} R)\,.$$

Indeed, both equalities are due to (5.7), once it is observed that for any complex X of R-modules, the following conditions are equivalent: X is acyclic; $\operatorname{Hom}_R(P, X)$ is acyclic for each projective R-module P; $\operatorname{Hom}_R(X, I)$ is acyclic for each injective R-module I.

In the presence of a dualizing complex total acyclicity can be tested against a pair of objects, rather than against the entire class of projectives, or of injectives, as called for by the definition. This is one of the imports of the result below. Recall that $\mathsf{i}R$ denotes an injective resolution of R, and that $D^* = \mathsf{S}(\mathsf{i}R)$; see (4.5).

PROPOSITION 5.9. *Let R be a noetherian ring with a dualizing complex D.*

(1) *The functor T restricts to an equivalence of $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)$ with $\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)$.*
(2) $\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R) = \{R\}^{\perp}$ *and* $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R) = \{R, D^*\}^{\perp}$.
(3) $\mathbf{K}_{\mathrm{ac}}(\operatorname{Inj} R) = \{\mathsf{i}R\}^{\perp}$ *and* $\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R) = \{\mathsf{i}R, D\}^{\perp}$.

Proof. (1) By Proposition (4.7), the equivalence induced by T identifies Thick(Prj R) with Thick(Inj R). This yields the equivalence below:

$$\begin{aligned}\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R) &= \operatorname{Thick}(\operatorname{Prj} R)^{\perp} \cap {}^{\perp}\operatorname{Thick}(\operatorname{Prj} R)\\ &\xrightarrow{\sim} \operatorname{Thick}(\operatorname{Inj} R)^{\perp} \cap {}^{\perp}\operatorname{Thick}(\operatorname{Inj} R) = \mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)\end{aligned}$$

The equalities are by Lemma (5.7).
(3) That $\mathbf{K}_{\mathrm{ac}}(\operatorname{Inj} R)$ equals $\{\mathsf{i}R\}^{\perp}$ follows from (2.2). Given this, the claim on $\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)$ is a consequence of (5.8) and the identifications

$$\{D\}^{\perp} = \operatorname{Thick}(\operatorname{Add} D)^{\perp} = \operatorname{Thick}(\operatorname{Inj} R)^{\perp} = (\operatorname{Inj} R)^{\perp},$$

where the second one is due to Proposition (4.7).
(2) The equality involving $\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R)$ is immediate from (2.1.1). Since $R \otimes_R D \cong D$ and $D^* \otimes_R D \cong \mathsf{i}R$, the second claim follows from (1) and (3). □

5.10. Proof of Theorems (5.4) and (5.3). The category $\mathcal{T} = \mathbf{K}(\operatorname{Inj} R)$ is compactly generated, the complexes $\mathsf{i}R$ and D are compact, and one has a canonical equivalence $\mathcal{T}^c \xrightarrow{\sim} \mathbf{D}^f(R)$; see (2.3.2). Therefore, Theorem (5.4) is immediate from Proposition (5.9.3), and Proposition (1.7) applied with $\mathcal{B} = \{\mathsf{i}R\}$ and $\mathcal{C} = \{\mathsf{i}R, D\}$.
To prove Theorem (5.3), set $\mathcal{T} = \mathbf{K}(\operatorname{Prj} R)$. By (2.3.1), this category is compactly generated, and in it R and D^* are compact; for D^* one requires also the identification in (4.5). Thus, in view of Proposition (5.9.2), Proposition (1.7) applied with $\mathcal{B} = \{R\}$ and $\mathcal{C} = \{R, D^*\}$ yields that the categories $\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R)$ and $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)$, and their quotient, are compactly generated. Furthermore, it provides equivalences up to direct factors

$$\mathbf{K}^c(\operatorname{Prj} R)/\operatorname{Thick}(R) \xrightarrow{\sim} \mathbf{K}^c_{\mathrm{ac}}(\operatorname{Prj} R)$$

$$\mathbf{K}^c(\operatorname{Prj} R)/\operatorname{Thick}(R, D^*) \xrightarrow{\sim} \mathbf{K}^c_{\mathrm{tac}}(\operatorname{Prj} R)$$

$$\operatorname{Thick}(R, D^*)/\operatorname{Thick}(R) \xrightarrow{\sim} \big(\mathbf{K}_{\mathrm{ac}}(\operatorname{Prj} R)/\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)\big)^c.$$

Combining these with the equivalence $\mathbf{D}^f(R) \to \mathbf{K}^c(\operatorname{Prj} R)^{\mathrm{op}}$ in (2.3.1) yields the desired equivalences. □

Remark 5.11. Proposition (5.9.3) contains the following result: a complex of injectives X is totally acyclic if and only if both X and $\operatorname{Hom}_R(D, X)$ are acyclic. We should like to raise the question: if both $\operatorname{Hom}_R(X, D)$ and $\operatorname{Hom}_R(D, X)$ are acyclic, is then X acyclic, and hence totally acylic? An equivalent formulation is: if X is a complex of projectives and X and $\operatorname{Hom}_R(X, R)$ are acyclic, is then X totally acyclic?
In an earlier version of this article, we had claimed an affirmative answer to this question, based on a assertion that if X is a complex of R-modules such that $\operatorname{Hom}_R(X, D)$ is acyclic, then X is acyclic. This assertion is false. Indeed, let R be a complete local domain, with field of fractions Q. A result of Jensen [10, Theorem 1] yields $\operatorname{Ext}^i_R(Q, R) = 0$ for $i \geq 1$, and it is easy to check that $\operatorname{Hom}_R(Q, R) = 0$ as well. Thus, $\operatorname{Hom}_R(Q, \mathsf{i}R)$ is acyclic. It remains to recall that when R is Gorenstein, $\mathsf{i}R$ is a dualizing complex for R.

5.12. Non-commutative rings. Theorems (5.3) and (5.4), and Proposition (5.9), all carry over, again with suitable modifications in the statements, to the pair of rings $\langle S, R\rangle$ from (3.3). The analogue of Corollary (5.5) is especially interesting:

Corollary. *The following conditions are equivalent.*

(a) *The projective dimension of D is finite over R^{op}.*
(b) *The projective dimension of D is finite over S.*
(c) *Every acyclic complex of projective R-modules is totally acyclic.*
(d) *Every acyclic complex of injective S-modules is totally acyclic.* □

6. An example

Let A be a commutative noetherian local ring, with maximal ideal $\mathfrak{m}$, and residue field $k = A/\mathfrak{m}$. Assume that $\mathfrak{m}^2 = 0$, and that $\operatorname{rank}_k(\mathfrak{m}) \geq 2$. Observe that A is *not* Gorenstein; for instance, its socle is $\mathfrak{m}$, and hence of rank at least 2. Let E denote the injective hull of the R-module k; this is a dualizing complex for A.

Proposition 6.1. *Set $\mathbf{K} = \mathbf{K}(\operatorname{Prj} A)$ and let X be a complex of projective A-modules.*

(1) *If X is acyclic and the A-module X^d is finite for some d, then $X \cong 0$ in $\mathbf{K}$.*
(2) *If X is totally acyclic, then $X \cong 0$ in $\mathbf{K}$.*
(3) *The cone of the homothety $A \to \operatorname{Hom}_A(P, P)$, where P is a projective resolution of D, is an acyclic complex of projectives, but it is not totally acyclic.*
(4) *In the derived category of A, one has $\operatorname{Thick}(A, D) = \mathbf{D}^f(A)$, and hence*

$$\operatorname{Thick}(A, D)/\operatorname{Thick}(A) = \mathbf{D}^f(A)/\operatorname{Thick}(A)\,.$$

The proof is given in (6.4). It hinges on some properties of minimal resolutions over A, which we now recall. Since A is local, each projective A-module is free. The Jacobson radical $\mathfrak{m}$ of A is square-zero, and in particular, nilpotent. Thus, Nakayama's lemma applies to each A-module M, hence it has a projective cover $P \to M$, and hence a minimal projective resolution; see [7, Propositions 3 and 15]. Moreover, $\Omega = \operatorname{Ker}(P \to M)$, the first syzygy of M, satisfies $\Omega \subseteq \mathfrak{m}P$, so that $\mathfrak{m}\Omega \subseteq \mathfrak{m}^2 P = 0$, so $\mathfrak{m}\Omega = 0$. In what follows, $\ell_A(-)$ denotes length.

Lemma 6.2. *Let M be an A-module; set $b = \ell_A(M)$, $c = \ell_A(\Omega)$.*

(1) *If M is finite, then its Poincaré series is*

$$P^A_M(t) = b + \frac{ct}{1 - et}$$

In particular, $\beta^A_n(M)$, the nth Betti number of M, equals ce^{n-1}, for $n \geq 1$.

(2) *If $\operatorname{Ext}^n_A(M, A) = 0$ for some $n \geq 2$, then M is free.*

Proof. (1) This is a standard calculation, derived from the exact sequences

$$0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow k \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow \Omega \longrightarrow P \longrightarrow M \longrightarrow 0$$

The one on the left implies $P_k^A(t) = 1 + etP_k^A(t)$, so $P_k^A(t) = (1-et)^{-1}$, while the one on the right yields $P_M^A(t) = b + ctP_k^A(t)$, since $\mathfrak{m}\Omega = 0$.
(2) If M is not free, then $\Omega \neq 0$ and hence has k as a direct summand. In this case, since $\operatorname{Ext}_A^{n-1}(\Omega, A) \cong \operatorname{Ext}_A^n(M, A) = 0$, one has $\operatorname{Ext}_A^{n-1}(k, A) = 0$, which in turn implies that A is Gorenstein; a contradiction. □

The following test to determine when an acyclic complex is homotopically trivial is surely known. Note that it applies to any (commutative) noetherian ring of finite Krull dimension, and, in particular, to the ring A that is the focus of this section.

Lemma 6.3. *Let R be a ring whose finitistic global dimension is finite. An acyclic complex X of projective R-modules is homotopically trivial if and only if for some integer s the R-module* $\operatorname{Coker}(X^{s-1} \to X^s)$ *is projective.*

Proof. For each integer n set $M(n) = \operatorname{Coker}(X^{n-1} \to X^n)$. It suffices to prove that the R-module $M(n)$ is projective for each n. This is immediate for $n \leq s$ because $M(s)$ is projective so that the sequence $\cdots \to X^{s-1} \to X^s \to M(s) \to 0$ is split exact.
We may now assume that $n \geq s+1$. By hypothesis, there exists an integer d with the following property: for any R-module M, if its projective dimension, $\operatorname{pd}_R M$ is finite, then $\operatorname{pd}_R M \leq d$. It follows from the exact complex

$$0 \longrightarrow M(s) \longrightarrow X^{s+1} \longrightarrow \cdots \longrightarrow X^{n+d} \longrightarrow M(n+d) \longrightarrow 0$$

that $\operatorname{pd}_R M(n+d)$ is finite. Thus, $\operatorname{pd}_R M(n+d) \leq d$, and another glance at the exact complex above reveals that $M(n)$ must be projective, as desired. □

Now we are ready for the

6.4. Proof of Proposition (6.1). In what follows, set $M(s) = \operatorname{Coker}(X^{s-1} \to X^s)$.
(1) Pick an integer $n \geq 1$ with $e^{n-1} \geq \operatorname{rank}_A(X^d) + 1$. Since X is acyclic, $\Sigma^{-d-n} X^{\leqslant d+n}$ is a free resolution of the A-module $M(n+d)$. Let Ω be the first syzygy of $M(n+d)$. One then obtains the first one of the following equalities:

$$\operatorname{rank}_A(X^d) \geq \beta_n^A(M(n+d)) \geq \ell_A(\Omega)e^{n-1} \geq \ell_A(\Omega)(\operatorname{rank}_A(X^d)+1)$$

The second equality is Lemma (6.2.1) applied to $M(n+d)$ while the last one is by the choice of n. Thus $\ell_A(\Omega) = 0$, so $\Omega = 0$ and $M(n+d)$ is free. Now Lemma (6.3) yields that X is homotopically trivial.
(2) Fix an integer d. Since $\Sigma^{-d} X^{\leqslant d}$ is a projective resolution of $M(d)$, total acyclicity of X implies that the homology of $\operatorname{Hom}_A(\Sigma^{-d}X^{\leqslant d}, A)$ is zero in degrees ≥ 1, so $\operatorname{Ext}_A^n(M(d), A) = 0$ for $n \geq 1$. Lemma (6.2.2) established above implies $M(d)$ is free. Once again, Lemma (6.3) completes the proof.
(3) Suppose that the cone of $A \to \operatorname{Hom}_A(P, P)$ is totally acyclic. This leads to a contradiction: (2) implies that the cone is homotopic to zero, so $A \cong$

$\operatorname{Hom}_A(P,P)$ in $\mathbf{K}$. This entails the first of the following isomorphisms in $\mathbf{K}(A)$; the others are standard.

$$\begin{aligned}\operatorname{Hom}_A(k,A) &\cong \operatorname{Hom}_A(k,\operatorname{Hom}_A(P,P))\\ &\cong \operatorname{Hom}_A(P\otimes_A k, P)\\ &\cong \operatorname{Hom}_k(P\otimes_A k,\operatorname{Hom}_A(k,P))\\ &\cong \operatorname{Hom}_k(P\otimes_A k,\operatorname{Hom}_A(k,A)\otimes_A P)\\ &\cong \operatorname{Hom}_k(P\otimes_A k,\operatorname{Hom}_A(k,A)\otimes_k (k\otimes_A P))\end{aligned}$$

Passing to homology and computing ranks yields $H(k\otimes_A P)\cong k$, and this implies $D\cong A$. This cannot be for $\operatorname{rank}_k \operatorname{soc}(D)=1$, while $\operatorname{rank}_k \operatorname{soc}(A)=e$ and $e\geq 2$.
(4) Combining Theorem (5.3.2) and (3) gives the first part. The second part then follows from the first. A direct and elementary argument is also available: As noted above the A-module D is not free; thus, the first syzygy module Ω of D is non-zero, so has k as a direct summand. Since Ω is in $\operatorname{Thick}(A,D)$, we deduce that k, and hence every homologically finite complex of A-modules, is in $\operatorname{Thick}(A,D)$.

Remark 6.5. Let A be the ring introduced at the beginning of this section, and let X and Y be complexes of A-modules.
The Tate cohomology of X and Y, in the sense of Jørgensen [12], is the homology of the complex $\operatorname{Hom}_A(T,Y)$, where T is a complete projective resolution of X; see (7.6). By Proposition (6.1.2) any such T, being totally acyclic, is homotopically trivial, so the Tate cohomology modules of X and Y are all zero. The same is true also of the version of Tate cohomology introduced by Krause [14, (7.5)] via complete injective resolutions. This is because A has no non-trivial totally acyclic complexes of injectives either, as can be verified either directly, or by appeal to Proposition (5.9.1).
These contrast drastically with another generalization of Tate cohomology over the ring A, introduced by Vogel and described by Goichot [8]. Indeed, Avramov and Veliche [3, (3.3.3)] prove that for an arbitrary commutative local ring R with residue field k, if the Vogel cohomology with $X=k=Y$ has finite rank even in a *single* degree, then R is Gorenstein.

7. Auslander categories and Bass categories

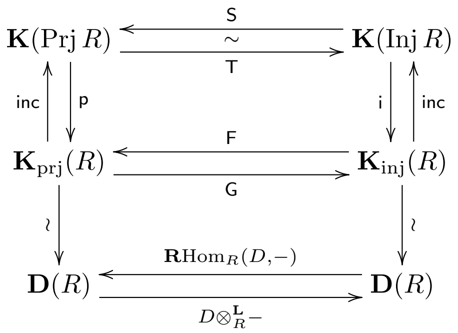
Let R be a commutative noetherian ring with a dualizing complex D. We write $\mathbf{K}_{\mathrm{prj}}(R)$ for the subcategory of $\mathbf{K}(\operatorname{Prj} R)$ consisting of K-projective complexes, and $\mathbf{K}_{\mathrm{inj}}(R)$ for the subcategory of $\mathbf{K}(\operatorname{Inj} R)$ consisting of K-injective complexes. This section is motivated by the following considerations: One has adjoint pairs of functors

$$\mathbf{K}_{\mathrm{prj}}(R) \underset{\mathsf{inc}}{\overset{\mathsf{p}}{\rightleftarrows}} \mathbf{K}(\operatorname{Prj} R) \quad\text{and}\quad \mathbf{K}(\operatorname{Inj} R) \underset{\mathsf{i}}{\overset{\mathsf{inc}}{\rightleftarrows}} \mathbf{K}_{\mathrm{inj}}(R)$$

and composing these functors with those in Theorem (4.2) gives functors

$$\mathsf{G} = (\mathsf{i} \circ \mathsf{T})\colon \mathbf{K}_{\mathrm{prj}}(R) \longrightarrow \mathbf{K}_{\mathrm{inj}}(R) \quad \text{and} \quad \mathsf{F} = (\mathsf{p} \circ \mathsf{S})\colon \mathbf{K}_{\mathrm{inj}}(R) \longrightarrow \mathbf{K}_{\mathrm{prj}}(R)\,.$$

These functors fit into the upper half of the picture below:



The vertical arrows in the lower half are obtained by factoring the canonical functor $\mathbf{K}(\operatorname{Prj} R) \to \mathbf{D}(R)$ through p, and similarly $\mathbf{K}(\operatorname{Inj} R) \to \mathbf{D}(R)$ through i. A straightforward calculation shows that the functors in the last row of the diagram are induced by those in the middle. Now, while T and S are equivalences – by Theorem (4.2) – the functors G and F need not be; indeed, they are equivalences if and only if R is Gorenstein; see Corollary (7.5) ahead. The results in this section address the natural:

Question. Identify subcategories of $\mathbf{K}_{\mathrm{prj}}(R)$ and $\mathbf{K}_{\mathrm{inj}}(R)$ on which G and F restrict to equivalences.

Given the equivalences in the lower square of the diagram an equivalent problem is to characterize subcategories of $\mathbf{D}(R)$ on which the functors $D \otimes^{\mathbf{L}}_R -$ and $\mathbf{R}\mathrm{Hom}_R(D,-)$ induce equivalences. This leads us to the following definitions:

7.1. AUSLANDER CATEGORY AND BASS CATEGORY. Consider the categories

$$\begin{aligned}\widehat{\mathcal{A}}(R) =& \{X \in \mathbf{D}(R) \mid \text{the natural map} \\ & \qquad X \to \mathbf{R}\mathrm{Hom}_R(D, D \otimes^{\mathbf{L}}_R X) \text{ is an isomorphism.}\} \\ \widehat{\mathcal{B}}(R) =& \{Y \in \mathbf{D}(R) \mid \text{the natural map} \\ & \qquad D \otimes^{\mathbf{L}}_R \mathbf{R}\mathrm{Hom}_R(D,Y) \to Y \text{ is an isomorphism.}\}\end{aligned}$$

The notation is intended to be reminiscent of the ones for the *Auslander category* $\mathcal{A}(R)$ and the *Bass category* $\mathcal{B}(R)$, introduced by Avramov and Foxby [1], which are the following subcategories of the derived category:

$$\mathcal{A}(R) = \{X \in \widehat{\mathcal{A}}(R) \mid X \text{ and } D \otimes^{\mathbf{L}}_R X \text{ are homologically bounded.}\}$$

$$\mathcal{B}(R) = \{Y \in \widehat{\mathcal{B}}(R) \mid Y \text{ and } \mathbf{R}\mathrm{Hom}_R(D,Y) \text{ are homologically bounded.}\}$$

The definitions are engineered to lead immediately to the following

Proposition 7.2. *The adjoint pair of functors* (G,F) *restrict to equivalences of categories between* $\widehat{\mathcal{A}}(R)$ *and* $\widehat{\mathcal{B}}(R)$*, and between* $\mathcal{A}(R)$ *and* $\mathcal{B}(R)$*.* □

In what follows, we identify $\widehat{\mathcal{A}}(R)$ and $\widehat{\mathcal{B}}(R)$ with the subcategories of $\mathbf{K}_{\mathrm{prj}}(R)$ and $\mathbf{K}_{\mathrm{inj}}(R)$ on which $\mathsf{S}\circ\mathsf{T}$ and $\mathsf{T}\circ\mathsf{S}$, respectively, restrict to equivalences. The Auslander category and the Bass category are identified with appropriate subcategories.

The main task then is describe the complexes in the categories being considered. In this section we provide an answer in terms of the categories of K-projectives and K-injectives; in the next one, it is translated to the derived category. Propositions (7.3) and (7.4) below are the first step towards this end. In them, the *cone* of a morphism $U\to V$ in a triangulated category refers to an object W obtained by completing the morphism to an exact triangle: $U\to V\to W\to \Sigma U$. We may speak of *the* cone because they exist and are all isomorphic.

Proposition 7.3. *Let X be a complex of projective R-modules. If X is K-projective, then it is in $\widehat{\mathcal{A}}(R)$ if and only if the cone of the morphism* $\mathsf{T}(X)\to \mathsf{iT}(X)$ *in* $\mathbf{K}(\mathrm{Inj}\,R)$ *is totally acyclic.*

Remark. The cone in question is always acyclic, because $\mathsf{T}(X)\to\mathsf{iT}(X)$ is an injective resolution; the issue thus is the difference between acyclicity and total acyclicity.

Proof. Let $\eta\colon \mathsf{T}(X)\to\mathsf{iT}(X)$ be a K-injective resolution. In $\mathbf{K}(\mathrm{Prj}\,R)$ one has then a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\ \kappa\ } & \mathsf{FG}(X) \\ {\scriptstyle\cong}\downarrow & & \downarrow{\scriptstyle\simeq} \\ \mathsf{ST}(X) & \xrightarrow{\ \mathsf{S}(\eta)\ } & \mathsf{SiT}(X) \end{array}$$

of adjunction morphisms, where the isomorphism is by Theorem (4.2). It is clear from the diagram above that

$$\begin{aligned} X \text{ is in } \widehat{\mathcal{A}}(R) &\iff \kappa \text{ is a quasi-isomorphism} \\ &\iff \mathsf{S}(\eta) \text{ is a quasi-isomorphism} \end{aligned}$$

It thus remains to prove that the last condition is equivalent to total acyclicity of the cone of η. In $\mathbf{K}(\mathrm{Inj}\,R)$ complete η to an exact triangle:

$$\mathsf{T}(X) \xrightarrow[\simeq]{\ \eta\ } \mathsf{iT}(X) \longrightarrow C \longrightarrow \Sigma\mathsf{T}(X)$$

From this triangle one obtains that $\mathsf{S}(\eta)$ is a quasi-isomorphism if and only if $\mathsf{S}(C)$ is acyclic. Now $\mathsf{S}(C)$ is quasi-isomorphic to $\mathrm{Hom}_R(D,C)$, see Theorem (2.7.1), and the acyclicity of $\mathrm{Hom}_R(D,C)$ is equivalent to C being in $\{D\}^{\perp}$, in $\mathbf{K}(\mathrm{Inj}\,R)$. However, C is already acyclic, and hence in $\{\mathsf{i}R\}^{\perp}$. Therefore Proposition (5.9.3) implies that $\mathsf{S}(C)$ is acyclic if and only if C is totally acyclic, as desired. □

An analogous proof yields:

Proposition 7.4. *Let Y be a complex of injective R-modules. If Y is K-injective, then it is in $\widehat{\mathcal{B}}(R)$ if and only if the cone of the morphism $\mathsf{pS}(Y) \to \mathsf{S}(Y)$ in $\mathbf{K}(\operatorname{Prj} R)$ is totally acyclic.* □

Corollary 7.5. *Let R be a noetherian ring with a dualizing complex. The ring R is Gorenstein if and only if $\widehat{\mathcal{A}}(R) = \mathbf{K}_{\mathrm{prj}}(R)$, if and only if $\widehat{\mathcal{B}}(R) = \mathbf{K}_{\mathrm{inj}}(R)$.*

Proof. Combine Propositions (7.3) and (7.4) with Corollary (5.5). □

One shortcoming in Propositions (7.3) and (7.4) is they do not provide a structural description of objects in the Auslander and Bass categories. Addressing this issue requires a notion of complete resolutions.

7.6. Complete resolutions. The subcategory $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)$ of $\mathbf{K}(\operatorname{Prj} R)$ is closed under coproducts; moreover, it is compactly generated, by Theorem (5.3.1). Thus, the inclusion $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Prj} R)$ admits a right adjoint:

$$\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R) \underset{\mathsf{inc}}{\overset{\mathsf{t}}{\rightleftarrows}} \mathbf{K}(\operatorname{Prj} R)$$

For each complex X in $\mathbf{K}(\operatorname{Prj} R)$ we call $\mathsf{t}(X)$ the *complete projective resolution* of X. In $\mathbf{K}(\operatorname{Prj} R)$, complete the natural morphism $\mathsf{t}(X) \to X$ to an exact triangle:

$$\mathsf{t}(X) \longrightarrow X \longrightarrow \mathsf{u}(X) \longrightarrow \Sigma\mathsf{t}(X)$$

Up to an isomorphism, this triangle depends only on X.
Similar considerations show that the inclusion $\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R) \to \mathbf{K}(\operatorname{Inj} R)$ admits a left adjoint. We denote it s, and for each complex Y of injectives call $\mathsf{s}(Y)$ the *complete injective resolution* of Y. This leads to an exact triangle in $\mathbf{K}(\operatorname{Inj} R)$:

$$\mathsf{v}(Y) \longrightarrow Y \longrightarrow \mathsf{s}(Y) \longrightarrow \Sigma\mathsf{v}(Y)$$

Relevant properties of complete resolutions and the corresponding exact triangles are summed up in the next two result; the arguments are standard, and details are given for completeness.

Lemma 7.7. *Let X be a complex of projectives R-modules.*

1. *The morphism $X \to \mathsf{u}(X)$ is a quasi-isomorphism and $\mathsf{u}(X)$ is in $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)^{\perp}$.*
2. *Any exact triangle $T \to X \to U \to \Sigma T$ in $\mathbf{K}(\operatorname{Prj} R)$ where T is totally acyclic and U is in $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)^{\perp}$ is isomorphic to $\mathsf{t}(X) \to X \to \mathsf{u}(X) \to \Sigma\mathsf{t}(X)$.*

Proof. (1) By definition, one has an exact triangle

$$\mathsf{t}(X) \longrightarrow X \longrightarrow \mathsf{u}(X) \longrightarrow \Sigma\mathsf{t}(X)\,.$$

Since the complex $\mathsf{t}(X)$ is acyclic, the homology long exact sequence arising from this triangle proves that $X \to \mathsf{u}(X)$ is an quasi-isomorphism, as claimed.

Moreover, for each totally acyclic complex T the induced map below is bijective:

$$(\dagger) \qquad \operatorname{Hom}_{\mathbf{K}}(T, \mathsf{t}(X)) \longrightarrow \operatorname{Hom}_{\mathbf{K}}(T, X)$$

This holds because t is a right adjoint to the inclusion $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R) \to \mathbf{K}(\operatorname{Prj} R)$. Since $\mathsf{t}(-)$ commutes with translations, the morphism $\Sigma^n \mathsf{t}(X) \to \Sigma^n X$ coincides with the morphism $\mathsf{t}(\Sigma^n X) \to \Sigma^n X$. Thus, from (†) one deduces that the induced map

$$\operatorname{Hom}_{\mathbf{K}}(T, \mathsf{t}(\Sigma^n X)) \longrightarrow \operatorname{Hom}_{\mathbf{K}}(T, \Sigma^n X)$$

is bijective for each integer n. It is now immediate from the exact triangle above that $\operatorname{Hom}_{\mathbf{K}}(T, \mathsf{u}(X)) = 0$; this settles (1), since $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)$ is stable under translations.

(2) Given such an exact triangle, the induced map $\operatorname{Hom}_{\mathbf{K}}(-, T) \to \operatorname{Hom}_{\mathbf{K}}(-, X)$ is bijective on $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)$, since $\operatorname{Hom}_{\mathbf{K}}(-, U)$ vanishes on $\mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)$. Thus, there is an isomorphism $\alpha\colon T \to \mathsf{t}(X)$, by (1.4), and one obtains a commutative diagram

$$\begin{array}{ccccccccc}
T & \longrightarrow & X & \longrightarrow & U & \longrightarrow & \Sigma T & \longrightarrow & \cdots \\
\downarrow{\scriptstyle \alpha} & & \| & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \Sigma\alpha} & & \\
\mathsf{t}(X) & \longrightarrow & X & \longrightarrow & \mathsf{u}(X) & \longrightarrow & \Sigma \mathsf{t}(X) & \longrightarrow & \cdots
\end{array}$$

of morphisms in $\mathbf{K}(\operatorname{Prj} R)$. Since the rows are exact triangles, and we are in a triangulated category, there exists a β as above that makes the diagram commute. Moreover, since α is an isomorphism, so is β; this is the desired result. □

One has also a version of Lemma (7.7) for complexes of injectives; proving it calls for a new ingredient, provided by the next result. Recall that $\mathsf{i}R$ denotes an injective resolution of R and $D^* = \mathsf{S}(\mathsf{i}R)$; see (4.5).

Lemma 7.8. ${}^{\perp}\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R) = \operatorname{Loc}(\mathsf{i}R, D)$

Proof. Proposition (5.9.3) implies that $\mathsf{i}R$ and D are contained in ${}^{\perp}\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)$, and hence so is $\operatorname{Loc}(\mathsf{i}R, D)$. To see that the reverse inclusion also holds note that $\operatorname{Loc}(\mathsf{i}R, D)$ is compactly generated (by $\mathsf{i}R$ and D) and closed under coproducts. Thus, by (1.5.1), the inclusion $\operatorname{Loc}(\mathsf{i}R, D) \to \mathbf{K}(\operatorname{Inj} R)$ admits a right adjoint, say r. Let X be a complex of injectives. Complete the canonical morphism $\mathsf{r}(X) \to X$ to an exact triangle

$$\mathsf{r}(X) \longrightarrow X \longrightarrow C \longrightarrow \Sigma \mathsf{r}(X)$$

For each integer n the induced map $\operatorname{Hom}_{\mathbf{K}}(-, \Sigma^n \mathsf{r}(X)) \to \operatorname{Hom}_{\mathbf{K}}(-, \Sigma^n X)$ is bijective on $\{\mathsf{i}R, D\}$, so the exact triangle above yields that $\operatorname{Hom}_{\mathbf{K}}(\mathsf{i}R, \Sigma^n C) = 0 = \operatorname{Hom}_{\mathbf{K}}(D, \Sigma^n C)$. Therefore, C is totally acyclic, by Proposition (5.9.3). In particular, when X is in ${}^{\perp}\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)$, one has $\operatorname{Hom}_{\mathbf{K}}(X, C) = 0$, so the exact triangle above is split, that is to say, X is a direct summand of $\mathsf{r}(X)$, and hence in $\operatorname{Loc}(\mathsf{i}R, D)$, as claimed. □

Here is the analogue of Lemma (7.7) for complexes of injectives; it is a better result for it provides a structural description of $\mathsf{v}(Y)$.

Lemma 7.9. *Let Y be a complex of injective R-modules.*

(1) *The morphism $\mathsf{v}(Y) \to Y$ is a quasi-isomorphism and $\mathsf{v}(Y)$ is in* $\operatorname{Loc}(\mathsf{i}R, D)$.
(2) *Any exact triangle $V \to X \to T \to \Sigma V$ in $\mathbf{K}(\operatorname{Inj} R)$ where T is totally acyclic and V is in $\operatorname{Loc}(\mathsf{i}R, D)$ is isomorphic to $\mathsf{v}(Y) \to Y \to \mathsf{s}(Y) \to \Sigma\mathsf{v}(Y)$.*

Proof. An argument akin to the proof of Lemma (7.7.1) yields that $\mathsf{v}(Y) \to Y$ is a quasi-isomorphism and that $\mathsf{v}(Y)$ is in ${}^{\perp}\mathbf{K}_{\mathrm{tac}}(\operatorname{Inj} R)$, which equals $\operatorname{Loc}(\mathsf{i}R, D)$, by Lemma (7.8). Given this, the proof of part (2) is similar to that of Lemma (7.7.2). □

Our interest in complete resolutions is due to Theorems (7.11) and (7.10), which provide one answer to the question raised at the beginning of this section.

Theorem 7.10. *Let R be a noetherian ring with a dualizing complex D, and let X be a complex of projective R-modules. If X is K-projective, then the following conditions are equivalent.*

(a) *The complex X is in $\widehat{\mathcal{A}}(R)$.*
(b) *The complex $\mathsf{u}(X)$ is in* $\operatorname{Coloc}(\operatorname{Prj} R)$.
(c) *In $\mathbf{K}(\operatorname{Prj} R)$, there exists an exact triangle $T \to X \to U \to \Sigma U$ where T is totally acyclic and U is in* $\operatorname{Coloc}(\operatorname{Prj} R)$.

Proof. Let $\mathsf{t}(X) \to X \to \mathsf{u}(X) \to \Sigma\mathsf{t}(X)$ be the exact triangle associated to the complete projective resolution of X; see (7.6). Let $\eta\colon \mathsf{T}(X) \to \mathsf{iT}(X)$ be a K-injective resolution, and consider the commutative diagram

$$\begin{array}{ccc} \mathsf{T}(X) & \xrightarrow[\simeq]{\eta} & \mathsf{iT}(X) \\ {\scriptstyle\simeq}\downarrow & & \| \\ \mathsf{Tu}(X) & \xrightarrow[\simeq]{\kappa} & \mathsf{iT}(X) \end{array}$$

arising as follows: the vertical map on the left is a quasi-isomorphism because it sits in the exact triangle with third vertex $\mathsf{Tt}(X)$, which is acyclic since $\mathsf{t}(X)$ is totally acyclic; see Proposition (5.9.1). Since $\mathsf{iT}(X)$ is K-injective, η extends to yield κ, which is a quasi-isomorphism because the other maps in the square are.

Note that the cone of the morphism $\mathsf{T}(X) \to \mathsf{Tu}(X)$ is $\Sigma\,\mathsf{Tt}(X)$, so applying the octahedral axiom to the commutative square above gives us an exact triangle

$$\Sigma\mathsf{Tt}(X) \longrightarrow \operatorname{Cone}(\eta) \longrightarrow \operatorname{Cone}(\kappa) \longrightarrow \Sigma^2\,\mathsf{Tt}(X)$$

where $\operatorname{Cone}(-)$ refers to the cone of the morphism in parenthesis. Since $\mathsf{t}(X)$ is totally acyclic, so is $\mathsf{Tt}(X)$, by Proposition (5.9.1). Hence the exact triangle above yields:

(†) Cone(η) is totally acyclic if and only if Cone(κ) is totally acyclic.

This observation is at the heart of the equivalence one has set out to establish.
(a) ⇒ (b): Proposition (7.3) yields that Cone(η) is totally acyclic, and hence so is Cone(κ), by (†). Consider the exact triangle

$$\mathsf{Tu}(X) \xrightarrow[\simeq]{\kappa} \mathsf{iT}(X) \longrightarrow \mathrm{Cone}(\kappa) \longrightarrow \Sigma\mathsf{Tu}(X)$$

According to Lemma (7.7.1) the complex $\mathsf{u}(X)$ is in $\mathbf{K}_{\mathrm{tac}}(\mathrm{Prj}\,R)^{\perp}$, so Proposition (5.9) yields that $\mathsf{Tu}(X)$ is in $\mathbf{K}_{\mathrm{tac}}(\mathrm{Inj}\,R)^{\perp}$, and hence the total acyclicity of Cone(κ) implies

$$\mathrm{Hom}_{\mathbf{K}}(\mathrm{Cone}(\kappa), \mathsf{Tu}(X)) = 0$$

Thus the triangle above is split exact, and $\mathsf{Tu}(X)$ is a direct summand of $\mathsf{iT}(X)$. Consequently $\mathsf{Tu}(X)$ is in $\mathrm{Coloc}(\mathrm{Inj}\,R)$, so, by Theorem (4.2) and Corollary (4.4), one obtains that $\mathsf{u}(X)$ is in $\mathrm{Coloc}(\mathrm{Prj}\,R)$, as desired.
(b) ⇒ (a): By Corollary (4.4), as $\mathsf{u}(X)$ is in $\mathrm{Coloc}(\mathrm{Prj}\,R)$ the complex $\mathsf{Tu}(X)$ is in $\mathrm{Coloc}(\mathrm{Inj}\,R)$, that is to say, it is K-injective. The map $\kappa\colon \mathsf{Tu}(X) \to \mathsf{iT}(X)$, being a quasi-isomorphism between K-injectives, is an isomorphism. Therefore $\mathrm{Cone}(\kappa) \cong 0$ so (†) implies that Cone(η) is totally acyclic. It remains to recall Proposition (7.3).
That (b) implies (c) is patent, and (c) ⇒ (b) follows from Lemma (7.7), because $\mathbf{K}_{\mathrm{tac}}(\mathrm{Prj}\,R)^{\perp} \supseteq \mathrm{Coloc}(\mathrm{Prj}\,R)$. The completes the proof of the theorem. □

An analogous argument yields a companion result for complexes of injectives:

Theorem 7.11. *Let R be a noetherian ring with a dualizing complex D, and let Y be a complex of injective R-modules. If Y is K-injective, then the following conditions are equivalent.*

(a) *The complex Y is in $\widehat{\mathcal{B}}(R)$.*
(b) *The complex $\mathsf{v}(Y)$ is in $\mathrm{Loc}(D)$.*
(c) *In $\mathbf{K}(\mathrm{Inj}\,R)$, there exists an exact triangle $V \to Y \to T \to \Sigma V$ where V is in $\mathrm{Loc}(D)$ and T is totally acyclic.* □

Section 8 translates Theorems (7.11) and (7.10) to the derived category of R.

7.12. Non-commutative rings. Consider a pair of rings $\langle S, R\rangle$ with a dualizing complex D, defined in (3.3). As in (7.1), one can define the Auslander category of R and the Bass category of S; these are equivalent via the adjoint pair of functors $(D \otimes_R -, \mathsf{q} \circ \mathrm{Hom}_S(D, -))$. The analogues of Theorems (7.10) and (7.11) extend to the pair $\langle S, R\rangle$, and they describe the complexes in $\widehat{\mathcal{A}}(R)$ and $\widehat{\mathcal{B}}(S)$.

8. Gorenstein dimensions

Let R be a commutative noetherian ring, and let X be a complex of R-modules. We say that X has *finite Gorenstein projective dimension*, or, in short: *finite G-projective dimension*, if there exists an exact sequence of complexes of projective

R-modules

$$0 \longrightarrow U \longrightarrow T \longrightarrow \mathsf{p}X \longrightarrow 0$$

where T is totally acyclic, $\mathsf{p}X$ is a K-projective resolution of X, and $U^n = 0$ for $n \ll 0$.

Similarly, a complex Y of R-modules has *finite G-injective dimension* if there exists an exact sequence of complexes of injective R-modules

$$0 \longrightarrow \mathsf{i}Y \longrightarrow T \longrightarrow V \longrightarrow 0$$

where T is totally acyclic, $\mathsf{i}Y$ is a K-injective resolution of Y, and $V^n = 0$ for $n \gg 0$.

The preceding definitions are equivalent to the usual ones, in terms of G-projective and G-injective resolutions; see Veliche [21], and Avramov and Martsinkovsky [2].

The theorem below contains a recent result of Christensen, Frankild, and Holm; more precisely, the equivalence of (i) and (ii) in [6, (4.1)], albeit in the case when R is commutative; however, see (8.3).

Theorem 8.1. *Let R be a noetherian ring with a dualizing complex D, and X a complex of R-modules. The following conditions are equivalent:*

(a) *X has finite G-projective dimension.*
(b) *$\mathsf{p}X$ is in $\widehat{\mathcal{A}}(R)$ and $D \otimes^{\mathbf{L}}_R X$ is homologically bounded on the left.*
(c) *$\mathsf{u}(\mathsf{p}X)$ is isomorphic, in $\mathbf{K}(\operatorname{Prj} R)$, to a complex U with $U^n = 0$ for $n \ll 0$.*

When $H(X)$ is bounded, these conditions are equivalent to: X is in $\mathcal{A}(R)$.

Proof. Substituting X with $\mathsf{p}X$, one may assume that X is K-projective and that $D \otimes^{\mathbf{L}}_R X$ is quasi-isomorphic to $D \otimes_R X$, that is to say, to $\mathsf{T}(X)$.

(a) $\Rightarrow$ (b): By definition, there is an exact sequence of complexes of projectives $0 \to U \to T \to X \to 0$ where T is totally acyclic and $U^n = 0$ for $n \ll 0$. Passing to $\mathbf{K}(\operatorname{Prj} R)$ gives rise to an exact triangle

$$U \longrightarrow T \longrightarrow X \longrightarrow \Sigma U$$

Since T is totally acyclic, $\mathsf{T}(X)$ is quasi-isomorphic to $\mathsf{T}(\Sigma U)$; the latter is bounded on the left as a complex, hence the former is homologically bounded on the left, as claimed. This last conclusion yields also that $\mathsf{T}(\Sigma U)$ is in $\operatorname{Coloc}(\operatorname{Inj} R)$. Thus, by Theorem (4.2) and Corollary (4.4), the complex ΣU is in $\operatorname{Coloc}(\operatorname{Prj} R)$, so the exact triangle above and Theorem (7.10) imply that X is in $\widehat{\mathcal{A}}(R)$.

(b) $\Rightarrow$ (c): By Theorem (7.10), there is an exact triangle

$$T \longrightarrow X \longrightarrow U \longrightarrow \Sigma T$$

with T totally acyclic and U in $\operatorname{Coloc}(\operatorname{Prj} R)$. The first condition implies that $\mathsf{T}(U)$ is quasi-isomorphic to $\mathsf{T}(X)$, and hence homologically bounded on the left, while the second implies, thanks to Corollary (4.4), that it is in $\operatorname{Coloc}(\operatorname{Inj} R)$, that is to say, it is K-injective. Consequently $\mathsf{T}(U)$ is isomorphic to a complex of injectives I with $I^n = 0$ for $n \ll 0$. This implies that the complex of flat R-modules $\operatorname{Hom}_R(D, \mathsf{T}(U))$ is bounded on the left. Theorem (2.7.3) now yields that the complex $\mathsf{q}(\operatorname{Hom}_R(D, \mathsf{T}(U)))$, that is to say, $\mathsf{ST}(U)$, is bounded on the left; thus, the same is true of U as it is isomorphic to $\mathsf{ST}(U)$, by Theorem (4.2). It remains to note that $\operatorname{Coloc}(\operatorname{Prj} R) \subseteq \mathbf{K}_{\mathrm{tac}}(\operatorname{Prj} R)^{\perp}$, so $\mathsf{u}(X) \cong U$ by Lemma (7.7).

(c) ⇒ (a): Lift the morphism $X \to \mathsf{u}(X) \cong U$ in $\mathbf{K}(\operatorname{Prj} R)$ to a morphism $\alpha\colon X \to U$ of complexes of R-modules. In the mapping cone exact sequence

$$0 \longrightarrow U \longrightarrow \operatorname{Cone}(\alpha) \longrightarrow \Sigma X \longrightarrow 0$$

$\operatorname{Cone}(\alpha)$ is homotopic to $\mathsf{t}(X)$, and hence totally acyclic, while $U^n = 0$ for $n \ll 0$, by hypothesis. Thus, the G-projective dimension of ΣX, and hence of X, is finite.

Finally, when $H(X)$ is bounded, $D \otimes^{\mathbf{L}}_R X$ is always bounded on the right. It is now clear from definitions that the condition that X is in $\mathcal{A}(R)$ is equivalent to (b). □

Here is a characterization of complexes in $\mathbf{D}(R)$ that are in the Bass category. For commutative rings, it recovers [6, (4.4)]; see (8.3). The basic idea of the proof is akin the one for the theorem above, but the details are dissimilar enough to warrant exposition.

Theorem 8.2. *Let R be a noetherian ring with a dualizing complex D, and Y a complex of R-modules. The following conditions are equivalent:*

(a) *Y has finite G-injective dimension.*

(b) *$\mathsf{i}Y$ is in $\widehat{\mathcal{B}}(R)$ and $\mathbf{R}\operatorname{Hom}_R(D, Y)$ is homologically bounded on the right.*

(c) *$\mathsf{v}(\mathsf{i}Y)$ is isomorphic, in $\mathbf{K}(\operatorname{Inj} R)$, to a complex V with $V^n = 0$ for $n \gg 0$.*

When $H(Y)$ is bounded, these conditions are equivalent to: Y is in $\mathcal{B}(R)$.

Proof. Replacing Y with $\mathsf{i}Y$ we assume that Y is K-injective, so $\mathbf{R}\operatorname{Hom}_R(D, Y)$ is quasi-isomorphic to $\operatorname{Hom}_R(D, Y)$. In the argument below the following remark is used without comment: in $\mathbf{K}(\operatorname{Inj} R)$, given an exact triangle

$$Y_1 \longrightarrow Y_2 \longrightarrow T \longrightarrow \Sigma Y_1$$

if T is totally acyclic, then one has a sequence

$$\operatorname{Hom}_R(D, Y_1) \xleftarrow{\simeq} \mathsf{S}(Y_1) \xrightarrow{\simeq} \mathsf{S}(Y_2) \xrightarrow{\simeq} \operatorname{Hom}_R(D, Y_2)\,.$$

of quasi-isomorphisms. Indeed, the first and the last quasi-isomorphism hold by Theorem (2.7.1), while the middle one holds because $\mathsf{S}(T)$ is totally acyclic, by Theorem (4.2).

(a) ⇒ (b): The defining property of complexes of finite G-injective dimension provides an exact sequence of complexes of injectives $0 \to Y \to T \to V \to 0$ where T is totally acyclic and $V^n = 0$ for $n \gg 0$. Passing to $\mathbf{K}(\operatorname{Inj} R)$ gives rise to an exact triangle

$$\Sigma^{-1} V \longrightarrow Y \longrightarrow T \longrightarrow V$$

Since T is totally acyclic, $\operatorname{Hom}_R(D, \Sigma^{-1} V)$ is quasi-isomorphic to $\operatorname{Hom}_R(D, Y)$; the former is bounded on the right as a complex, so the latter is homologically bounded on the right, as claimed. Furthermore, since V is bounded on the right, so is $\mathrm{Hom}_R(D, \Sigma^{-1}V)$. Theorem (2.7.2) then yields that $\mathsf{S}(\Sigma^{-1}V)$ is its projective resolution, and hence it is in $\mathrm{Loc}(R)$. Thus, by Theorem (4.2), the complex $\Sigma^{-1}V$ is in $\mathrm{Loc}(D)$, so the exact triangle above and Theorem (7.11) imply that Y is in $\widehat{\mathcal{B}}(R)$.

(b) $\Rightarrow$ (c): By hypothesis and Theorem (7.11) there exists and exact triangle

$$V \longrightarrow Y \longrightarrow T \longrightarrow \Sigma V$$

in $\mathbf{K}(\mathrm{Inj}\, R)$, where V lies in $\mathrm{Loc}(D)$ and T is totally acyclic. Thus $\mathsf{S}(V)$ is in $\mathrm{Loc}(R)$, that is to say, it is K-projective, and it is quasi-isomorphic to $\mathrm{Hom}_R(D, Y)$, and hence it is homologically bounded on the right. Therefore, $\mathsf{S}(V)$ is isomorphic to a complex of projectives P with $P^n = 0$ for $n \gg 0$. By Theorem (4.2), this implies that V is isomorphic to $\mathsf{T}(P)$, which is bounded on the right.

(c) $\Rightarrow$ (a): Lift the morphism $V \cong \mathsf{v}(Y) \to Y$ in $\mathbf{K}(\mathrm{Inj}\, R)$ to a morphism $\alpha \colon V \to Y$ of complexes of R-modules. In the mapping cone exact sequence

$$0 \longrightarrow Y \longrightarrow \mathrm{Cone}(\alpha) \longrightarrow \Sigma V \longrightarrow 0$$

the complex $\mathrm{Cone}(\alpha)$ is homotopic to $\mathsf{s}(Y)$, and hence totally acyclic, while $V^n = 0$ for $n \gg 0$, by hypothesis. Thus, the G-injective dimension of Y is finite.

Finally, when Y is homologically bounded, $\mathbf{R}\mathrm{Hom}_R(D, Y)$ is bounded on the left, so Y is in $\mathcal{B}(R)$ if and only if it satisfies condition (b). □

8.3. Non-commutative rings. Following the thread in (3.3), (4.8), (5.12), and (7.12), the development of this section also carries over to the context of a pair of rings $\langle S, R\rangle$ with a dualizing complex D. In this case, the analogues of Theorems (8.1) and (8.2) identify complexes of finite G-projective dimension over R and of finite G-injective dimension over S as those in the Auslander category of R and the Bass category of S, respectively. These results contain [6, (4.1),(4.4)], but only when one assumes that the ring R is left coherent as well; the reason for this has already been given in (3.3).

Acknowledgments

This project was initiated in June 2004, when Srikanth Iyengar was visiting the University of Paderborn. He thanks the Department of Mathematics at Paderborn and its algebra group for hospitality. The authors thank Lucho Avramov for his comments and suggestions, Lars Winther Christensen for numerous discussions on [6] which motivates the results in Section 8, and Amnon Neeman for a careful reading of the manuscript.

References

[1] L. Avramov, H.-B. Foxby: Ring homomorphisms and finite Gorenstein dimension. Proc. London Math. Soc. (3) 75 (1997), no. 2, 241–270.

[2] L. Avramov, A. Martsinkovsky: Absolute, relative, and Tate cohomology of modules of finite Gorenstein dimension. Proc. London Math. Soc. (3) 85 (2002), 393-440.

[3] L. Avramov, O. Veliche: Stable cohomology over local rings. ArXiv: math.AC/0508021.

[4] M. Bökstedt, A. Neeman: Homotopy limits in triangulated categories. Compositio Math. 86 (1993), 209–234.

[5] L. W. Christensen: Gorenstein dimensions. Lecture Notes Math. 1747, Springer, Berlin, 2000.

[6] L. W. Christensen, A. Frankild, H. Holm: On Gorenstein projective, injective and flat dimensions – A functorial description with applications. J. Algebra 302 (2006), 231–279.

[7] S. Eilenberg: Homological dimensions of syzygies. Ann. of Math. 64 (1956), 328–336.

[8] F. Goichot:, Homologie de Tate-Vogel équivariante. J. Pure Appl. Algebra 82 (1992), 39–64.

[9] R. Hartshorne: Residues and Duality. Springer Lecture Notes Math. 20 (1966).

[10] C. U. Jensen: On the vanishing of $\varprojlim^{(i)}$. J. Algebra 15 (1970), 151–166.

[11] P. Jørgensen: The homotopy category of complexes of projective modules. Adv. Math. 193 (2005), 223–232.

[12] P. Jørgensen: Existence of Gorenstein projective resolutions and Tate cohomology. J. Eur. Math. Soc. (to appear).

[13] T. Kawasaki: On arithmetic Macaulayfication of Noetherian rings. Trans. Amer. Math. Soc. 354 (2002), 123–149.

[14] H. Krause: The stable derived category of a noetherian scheme. Compositio Math. 141 (2005), 1128–1162.

[15] S. MacLane: Categories for the working mathematician. second ed. Graduate Texts Math., 5, Springer-Verlag, New York, 1998

[16] A. Neeman: The chromatic tower for $D(R)$, With an appendix by Marcel Bökstedt. Topology 31 (1992), 519–532.

[17] A. Neeman: The Connection between the K-theory localization theorem of Thomason, Trobaugh and Yao and the smashing subcategories of Bousfield and Ravenel. Ann. Sci. École Norm. Sup. 25 (1992), 547–566.

[18] A. Neeman: The Grothendieck duality theorem via Bousfield's techniques and Brown representability. J. Amer. Math. Soc. 9 (1996), 205–236.

[19] A. Neeman: Triangulated categories. Annals of Mathematics Studies 148, Princeton University Press (2001).

[20] M. Raynaud, L. Gruson: Critères de platitude et de projectivité. Techniques de "platification" d'un module. Invent. Math. 13 (1971), 1–89.

[21] O. VELICHE: Gorenstein projective dimension for complexes. Trans. Amer. Math. Soc. 358 (2006), 1257–1283.
[22] J. L. VERDIER: Des catégories dérivées des catégories abéliennes. Astérisque 239 (1996).
[23] C. WEIBEL: An introduction to homological algebra, Cambridge Stud. Adv. Math. 38, Cambridge Univ. Press, Cambridge, 1994.

Srikanth Iyengar
Department of Mathematics
University of Nebraska
Lincoln, NE - 68588
U.S.A.
iyengar@math.unl.edu

Henning Krause
Institut für Mathematik
Universität Paderborn
33095 Paderborn
Germany.
hkrause@math.uni-paderborn.de

Erratum to: Cohomology of Arithmetic Groups with Infinite Dimensional Coefficient Spaces cf. Documenta Math. 10, (2005) 199–216

Anton Deitmar and Joachim Hilgert

Received: May 8, 2006

Communicated by Patrick Delorme

Abstract. A correction of an error in the proof of Lemma 5.3 is given.

2000 Mathematics Subject Classification: 11F75

In the first paragraph of the proof of Lemma 5.3 of the above paper it is claimed that $C^\infty(G,\pi)$ is nuclear for π an irreducible admissible representation of G. This does not hold, for it implies that the subspace of constant functions, i.e., π itself, is also nuclear. Now π can be a Hilbert-representation and a Hilbert space is only nuclear if it is finite dimensional.
It was the aim of that paragraph to give a proof that π^∞ is nuclear. This can be seen as follows: First assume that π is induced from a minimal parabolic. Then π^∞ may, in the compact model, be interpreted as the space of smooth sections of a vector bundle over the compact manifold K/M. Hence π^∞ is nuclear. By the results of Casselman [10], every π^∞ may be embedded topologically into an induced representation as above, therefore is nuclear.

Anton Deitmar
Mathematisches Institut
Auf der Morgenstelle 10
72076 Tübingen
Germany
deitmar@uni-tuebingen.de

Joachim Hilgert
Universität Paderborn
Fakultät für Elektrotechnik,
Informatik und Mathematik
Warburger Str. 100
33098 Paderborn, Germany
hilgert@math.uni-paderborn.de

Koszul Duality and Equivariant Cohomology

Matthias Franz

Received: June 26, 2005
Revised: May 6, 2006

Communicated by Eckhard Meinrenken

Abstract. Let G be a topological group such that its homology $H(G)$ with coefficients in a principal ideal domain R is an exterior algebra, generated in odd degrees. We show that the singular cochain functor carries the duality between G-spaces and spaces over BG to the Koszul duality between modules up to homotopy over $H(G)$ and $H^*(BG)$. This gives in particular a Cartan-type model for the equivariant cohomology of a G-space with coefficients in R. As another corollary, we obtain a multiplicative quasi-isomorphism $C^*(BG) \to H^*(BG)$. A key step in the proof is to show that a differential Hopf algebra is formal in the category of A_∞ algebras provided that it is free over R and its homology an exterior algebra.

2000 Mathematics Subject Classification: Primary 16S37, 55N91; Secondary 16E45, 55N10

1. Introduction

Let G be a topological group. A space over the classifying space BG of G is a map $Y \to BG$. There are canonical ways to pass from left G-spaces to spaces over BG and back: The Borel construction $\boldsymbol{t}X = EG \times_G X$ is a functor

$$\boldsymbol{t}\colon G\text{-}\boldsymbol{Space} \to \boldsymbol{Space}\text{-}BG,$$

and pulling back the universal right G-bundle $EG \to BG$ along $Y \to BG$ and passing to a left action gives a functor in the other direction,

$$\boldsymbol{h}\colon \boldsymbol{Space}\text{-}BG \to G\text{-}\boldsymbol{Space}.$$

These functors are essentially inverse to each other in the sense that $\boldsymbol{ht}X$ and $\boldsymbol{th}Y$ are homotopy-equivalent in the category of spaces to X and Y, respectively, cf. [3].

Goresky–Kottwitz–MacPherson [8] have related this to an algebraic phenomenon called Koszul duality (see also Alekseev–Meinrenken [1] and Allday–Puppe [2]). Let $\mathbf{\Lambda}$ be an exterior algebra over some ring R with generators $x_1, \ldots, x_r$ of odd degrees, and $\mathbf{S}^*$ the symmetric R-algebra with generators $\xi_1, \ldots, \xi_r$ dual to the x_i and with degrees shifted by 1. We will denote the categories of bounded below differential graded modules over $\mathbf{\Lambda}$ and $\mathbf{S}^*$ by $\mathbf{\Lambda}$-*Mod* and $\mathbf{S}^*$-*Mod*, respectively. The Koszul functors

$$\mathbf{t}\colon \mathbf{\Lambda}\text{-}\mathit{Mod} \to \mathbf{S}^*\text{-}\mathit{Mod} \quad \text{and} \quad \mathbf{h}\colon \mathbf{S}^*\text{-}\mathit{Mod} \to \mathbf{\Lambda}\text{-}\mathit{Mod}$$

are defined by

$$\text{(1.1)} \qquad \mathbf{t}N = \mathbf{S}^* \otimes N, \qquad d(\sigma \otimes n) = \sigma \otimes dn + \sum_{i=1}^{r} \xi_i \sigma \otimes x_i n$$

and

$$\text{(1.2)} \qquad \mathbf{h}M = \mathbf{\Lambda}^* \otimes M, \qquad d(\alpha \otimes m) = (-1)^{|\alpha|} \alpha \otimes dm - \sum_{i=1}^{r} x_i \cdot \alpha \otimes \xi_i m.$$

Here $\mathbf{\Lambda}$ acts on $\mathbf{\Lambda}^*$ by contraction. Koszul duality refers to the fact that $\mathbf{ht}N$ and $\mathbf{th}M$ are homotopy-equivalent in the category of R-modules to N and M, respectively.

Now let $\mathbf{\Lambda} = H(G)$ be the homology of the compact connected Lie group G (with the Pontryagin product induced from the group multiplication) and $\mathbf{S}^* = H^*(BG)$ the cohomology of its classifying space BG. We take real coefficients, so that $\mathbf{\Lambda}$ and $\mathbf{S}^*$ are of the form described above. Goresky–Kottwitz–MacPherson and Alekseev-Meinrenken have shown that for certain G-spaces X, for instance for G-manifolds, $\mathbf{t}\Omega^*(X)^G$ computes the equivariant cohomology of X as $\mathbf{S}^*$-module, and $\mathbf{h}\Omega^*(\boldsymbol{t}X)$ the ordinary cohomology of X as $\mathbf{\Lambda}$-module. Here $\Omega^*(X)^G$ denotes the G-invariant differential forms on X, and $\Omega^*(\boldsymbol{t}X)$ the (suitably defined) differential forms on the Borel construction of X.

For the case of torus actions, the author has shown in [5] how to generalise this to arbitrary spaces and, more importantly, to an arbitrary coefficient ring R instead of $\mathbf{R}$. Differential forms are thereby replaced by singular cochains. The main problem one has to face is that the action of $\mathbf{S}^*$ on $H^*(Y)$, Y a space over BG, does not lift to an action on $C^*(Y)$ because the cup product of cochains is not commutative – unlike that of differential forms. The solution comes in form of "modules up to homotopy". Although modules up to homotopy – or *weak modules*, as we will call them – have a long history in Differential Homological Algebra (cf. for instance [17] or [18]), they are not familiar to many mathematicians in other areas. They will be defined precisely in Section 2; in the following paragraphs we just explain their main features and why they are useful for us.

A weak $\mathbf{S}^*$-module is a bounded below differential graded module over a differential graded R-algebra A together with elements $a_\pi \in A$, $\emptyset \neq \pi \subset \{1, \ldots, r\}$, such that

$$d(\alpha \otimes m) = (-1)^{|\alpha|}\alpha \otimes dm + \sum_{\pi \neq \emptyset} (-1)^{|x_\pi|} x_\pi \cdot \alpha \otimes a_\pi m \tag{1.3}$$

is a differential on $\mathbf{\Lambda}^* \otimes M$. Here (x_π) denotes the canonical R-basis of $\mathbf{\Lambda}$ consisting of the monomials in the x_i. If $A = \mathbf{S}^*$, one can simply set $a_i = \xi_i$ and all higher elements equal to zero. This shows that any $\mathbf{S}^*$-module is also a weak $\mathbf{S}^*$-module. In general, equation (1.3) puts certain conditions on the elements a_π. For instance, the element a_{12} must satisfy the relation

$$(da_{12})m = (a_1 a_2 - a_2 a_1)m \quad \text{for all } m \in M. \tag{1.4}$$

In other words, it compensates for the lack of commutativity between a_1 and a_2. Gugenheim–May [10] have shown how to construct suitable elements $a_\pi \in A = C^*(BG)$ starting from representatives a_i of the $\xi_i \in \mathbf{S}^*$. As a consequence, the cochains on any space Y over BG admit the structure of a weak $\mathbf{S}^*$-module. One then defines the Koszul dual of the weak $\mathbf{S}^*$-module $C^*(Y)$ to be the $\mathbf{\Lambda}$-module $\mathbf{\Lambda}^* \otimes C^*(Y)$ with differential (1.3), and in [5] it was shown that for tori this computes the cohomology of $\boldsymbol{h}Y$ as $\mathbf{\Lambda}$-module. (That this complex gives the right cohomology as R-module appears already in Gugenheim–May [10].)

A fancier way to define a weak $\mathbf{S}^*$-module is to say that it is an A-module as above together with a so-called twisting cochain $u\colon \mathbf{\Lambda}^* \to A$. The elements a_π then are the images under u of the R-basis of $\mathbf{\Lambda}^*$ dual to the basis (x_π). It follows from equation (1.4) that the cohomology of a weak $\mathbf{S}^*$-module admits itself a (strict) $\mathbf{S}^*$-action. Similarly, a weak $\mathbf{\Lambda}$-module is a module N over some algebra A together with a twisting cochain $\mathbf{S} \to A$, where $\mathbf{S}$ denotes the coalgebra dual to $\mathbf{S}^*$. Its cohomology is canonically a $\mathbf{\Lambda}$-module.

For torus actions there is no need to consider weak $\mathbf{\Lambda}$-modules because the $\mathbf{\Lambda}$-action on cohomology can be lifted to an honest action on cochains. In fact, since $C(G)$ is graded commutative in this case, it suffices to choose representatives $c_i \in C(G)$ of the generators $x_i \in \mathbf{\Lambda}$ in order to construct a quasi-isomorphism of algebras $\mathbf{\Lambda} \to C(G)$. In [8, Sec. 12] it is claimed that a lifting is possible for any compact connected Lie group, but the proof given there is wrong. The mistake is that it is not possible in general to find conjugation-invariant representatives of the generators x_i because all singular simplices appearing in a conjugation-invariant chain c_i necessarily map to the centre of G. The example $G = SU(3)$ shows that passing to subanalytic chains (which are also used in [8]) is of no help: apart from the finite centre, all conjugation classes of $SU(3)$ have dimension 4 or 6. Hence, there can be no conjugation-invariant subanalytic set supporting a representative of the 3-dimensional generator.

In the present paper, we extend the approach of [5] to non-commutative topological groups G by constructing a weak $\mathbf{\Lambda}$-structure on the cochain complex of a G-space X. We then show that the normalised singular cochain functor C^* transforms the topological equivalence between G-spaces and spaces over BG, up to quasi-isomorphism, to the Koszul duality between modules up to homotopy over the homology $\mathbf{\Lambda} = H(G)$ and the cohomology $\mathbf{S}^* = H^*(BG)$. The only assumptions are that coefficients are in a principal ideal domain R and that $H(G)$ is an exterior algebra on finitely many generators of odd degrees or, equivalently, that $H^*(BG)$ a symmetric algebra on finitely many generators of even degrees.

A priori, the isomorphism $H(G) \cong \bigwedge(x_1, \dots, x_r)$ must be one of Hopf algebras[1] with primitive generators x_i. But the Samelson–Leray theorem asserts that in our situation any isomorphism of algebras (or coalgebras) can be replaced by one which is Hopf. In characteristic 0 it suffices by Hopf's theorem to check that G is connected and $H(G)$ free of finite rank over R. In particular, the condition is satisfied for $U(n)$, $SU(n)$ and $Sp(n)$ and arbitrary R, and for an arbitrary compact connected Lie group if the order of the Weyl group is invertible in R.

Under the assumptions on $H(G)$ and $H^*(BG)$ mentioned above, we prove the following:

PROPOSITION 1.1. *There are twisting cochains $v\colon \mathbf{S} \to C(G)$ and $u\colon \mathbf{\Lambda}^* \to C^*(BG)$ such that the $\mathbf{\Lambda}$-action on the homology of a $C(G)$-module, viewed as weak $\mathbf{\Lambda}$-module, is the canonical one over $H(G) = \mathbf{\Lambda}$, and analogously for u.*

The cochains on a G-space are canonically a $C(G)$-module and the cochains on a space over BG a $C^*(BG)$-module. Hence we may consider C^* as a functor from G-spaces to weak $\mathbf{\Lambda}$-modules, and from spaces over BG to weak $\mathbf{S}^*$-modules.

We say that two functors to a category of complexes are quasi-isomorphic if they are related by a zig-zag of natural transformations which become isomorphisms after passing to homology.

THEOREM 1.2. *The functors $C^* \circ \boldsymbol{t}$ and $\mathbf{t} \circ C^*$ from G-spaces to weak $\mathbf{S}^*$-modules are quasi-isomorphic, as are the functors $C^* \circ \boldsymbol{h}$ and $\mathbf{h} \circ C^*$ from spaces over BG to weak $\mathbf{\Lambda}$-modules.*

Hence, the equivariant cohomology $H_G^*(X)$ of a G-space X is naturally isomorphic, as $\mathbf{S}^*$-module, to the homology of the "singular Cartan model"

$$\mathbf{t}C^*(X) = \mathbf{S}^* \otimes C^*(X) \tag{1.5a}$$

with differential

$$d(\sigma \otimes \gamma) = \sigma \otimes d\gamma + \sum_{i=1}^{r} \xi_i \sigma \otimes c_i \cdot \gamma + \sum_{i \le j} \xi_i \xi_j \sigma \otimes c_{ij} \cdot \gamma + \cdots , \tag{1.5b}$$

where the ξ_i are generators of the symmetric algebra $\mathbf{S}^*$ and the $c_i \in C(G)$ representatives of the generators $x_i \in \mathbf{\Lambda}$. They are, like the higher order terms c_{ij} etc., encoded in the twisting cochain v. The sum, which runs over all non-constant monomials of $\mathbf{S}^*$, is well-defined for degree reasons.

Similarly, the cohomology of the pull back of EG along $Y \to BG$ is isomorphic to the homology of the $\mathbf{\Lambda}$-module $\mathbf{h}C^*(Y) = \mathbf{\Lambda}^* \otimes C^*(Y)$, again with a twisted differential. (See Section 3 for precise formulas for the differentials.) That the complex $\mathbf{h}C^*(Y)$ gives the right cohomology as R-module is already due to Gugenheim–May [10]. The correctness of the $\mathbf{\Lambda}$-action is new.

[1] Note that $H(G)$ has a well-defined diagonal because it is free over R.

Along the way, we obtain the following result, which was previously only known for tori, and for other Eilenberg–Mac Lane spaces if $R = \mathbf{Z}_2$ (Gugenheim–May [10, §4]):

Proposition 1.3. *There exists a quasi-isomorphism of algebras $C^*(BG) \to H^*(BG)$ between the cochains and the cohomology of the simplicial construction of the classifying space of G.*

Any such map has an A_∞ map as homotopy inverse (cf. Lemma 4.1). So we get as another corollary the well-known existence of an A_∞ quasi-isomorphism $H^*(BG) \Rightarrow C^*(BG)$. The original proof (Stasheff–Halperin [22]) uses the homotopy-commutativity of the cup product and the fact that $H^*(BG)$ is free commutative. Here it is based, like most of the paper, on the following result, which is of independent interest and should be considered as dual to the theorem of Stasheff and Halperin.

Theorem 1.4. *Let A be a differential $\mathbf{N}$-graded Hopf algebra, free over R and such that its homology is an exterior algebra on finitely many generators of odd degrees. Then there are A_∞ quasi-isomorphisms $A \Rightarrow H(A)$ and $H(A) \Rightarrow A$.*

It is essentially in order to use Theorem 1.4 (and a similar argument in Section 7) that we assume R to be a principal ideal domain. A look at the proofs will show that once Proposition 1.1, Theorem 1.2 and Proposition 1.3 are established for such an R, they follow by extension of scalars for any commutative R-algebra R' instead of R.
Johannes Huebschmann has informed the author that he has been aware of the singular Cartan model and of Theorem 1.4 since the 1980's, cf. [14]. Instead of adapting arguments from his habilitation thesis [13, Sec. 4.8], we shall base the proof of Theorem 1.4 on an observation due to Stasheff [21].

The paper is organised as follows: Notation and terminology is fixed in Section 2. Section 3 contains a review of Koszul duality between modules up to homotopy over symmetric and exterior algebras. Theorem 1.4 is proved in Section 4. The proofs of the other results stated in the introduction appear in Sections 5 to 7. In Section 8 we discuss equivariantly formal spaces and in Section 9 the relation between the singular Cartan model and other models, in particular the classical Cartan model. In an appendix we prove the versions of the theorems of Samelson–Leray and Hopf mentioned above because they are not readily available in the literature.

Acknowledgements. The author thanks Stéphane Guillermou, Johannes Huebschmann, Tomasz Maszczyk and Andrzej Weber for stimulating discussions and comments.

2. Preliminaries

Throughout this paper, the letter R denotes a principal ideal domain. All complexes are over R. Differentials always lower degree, hence cochain complexes and cohomology are negatively graded. All (co)algebras and (co)modules are graded and have differentials (which might be trivial). Let A and B be complexes. The dual $f^* \in \operatorname{Hom}(B^*, A^*)$ of a map $f \in \operatorname{Hom}(A, B)$ is defined by

$$f^*(\beta)(a) = (-1)^{|f||\beta|}\,\beta(f(a)).$$

Algebras will be associative and coalgebras coassociative, and both have units and counits (augmentations). Morphisms of (co)algebras preserve these structures. We denote the augmentation ideal of an algebra A by $\bar{A}$. An $\mathbf{N}$-graded algebra A is called connected if $\bar{A}_0 = 0$, and an $\mathbf{N}$-graded coalgebra C simply connected if $C_0 = R$ and $C_1 = 0$. Hopf algebras are algebras which are also coalgebras with a multiplicative diagonal, cf. [18, Def. 4.39]. (Note that we do not require the existence of an antipode, though there will always be one for our examples.)

Let C be a coalgebra, A an algebra and $t\colon C \to A$ a twisting cochain. For a right C-comodule M and a left A-module N, we define the twisted tensor product $M \otimes_t N$ with differential

$$d_t = d \otimes 1 + 1 \otimes d + (1 \otimes \mu_N)(1 \otimes t \otimes 1)(\Delta_M \otimes 1).$$

Here $\Delta_M\colon M \to M \otimes C$ and $\mu_N\colon A \otimes N \to N$ denote the structure maps of M and N, respectively. Readers unfamiliar with twisting cochains can take the fact that d is a well-defined differential (say, on $C \otimes_t A$) as the definition of a twisting cochain, plus the normalisation conditions $t\iota_C = 0$ and $\varepsilon_A t = 0$, where ι_C is the unit of C and ε_A the augmentation of A. Suppose that C and A are $\mathbf{N}$-graded. We will regularly use the fact that twisting cochains $C \to A$ correspond bijectively to coalgebra maps $C \to BA$ and to algebra maps $\Omega C \to A$. Here BA denotes the normalised bar construction of A and ΩC the normalised cobar construction of C. In particular, the functors Ω and B are adjoint. (See for instance [15, Sec. II] for more about twisting cochains and the (co)bar construction.)

We agree that an exterior algebra is one on finitely many generators of odd positive degrees. Let A be an $\mathbf{N}$-graded algebra such that $\mathbf{\Lambda} = H(A) = \bigwedge(x_1, \dots, x_r)$ is an exterior algebra. Then $H(BA) = H(B\mathbf{\Lambda}) = \mathbf{S}$ is a symmetric coalgebra on finitely many cogenerators y_i of even degrees $|y_i| = |x_i| + 1$, cf. [18, Thm. 7.30]. (The converse is true as well.) We assume that the y_i are chosen such that they can be represented by the cycles $[x_i] \in B\mathbf{\Lambda}$ and $[c_i] \in BA$, where the $c_i \in A$ are any representatives of the generators $x_i \in \mathbf{\Lambda}$. We denote by x_π, $\pi \subset \{1, \dots, r\}$, the canonical R-basis of $\mathbf{\Lambda}$ generated by the x_i, and the dual basis of $\mathbf{\Lambda}^*$ by ξ_π. The R-basis of $\mathbf{S}$ induced by the y_i is written as y_α, $\alpha \in \mathbf{N}^r$. The dual $\mathbf{S}^*$ of $\mathbf{S}$ is a symmetric algebra on generators ξ_i dual to the y_i.

We work in the simplicial category. We denote by $C(X)$ the normalised chain complex of the simplicial set X. (If X comes from a topological space, then $C(X)$ is the complex of normalised singular chains.) The (negatively graded) dual complex of normalised cochains is denoted by $C^*(X)$. If G is a connected (topological or simplicial) group, then the inclusion of the simplicial subgroup consisting of the simplices with all vertices at $1 \in G$ is a quasi-isomorphism. We may therefore assume that G has only one vertex. Then $C(G)$ is a connected Hopf algebra and $C(BG)$ a simply connected coalgebra. In both cases, the diagonal is the Alexander–Whitney map, and the Pontryagin product of $C(G)$ is the composition of the shuffle map $C(G) \otimes C(G) \to C(G \times G)$ with the map $C(G \times G) \to C(G)$ induced by the multiplication of G. Analogously, $C(X)$ is a left $C(G)$-module if X is a left G-space. The left $C(G)$-action on cochains is defined by

$$(a \cdot \gamma)(c) = (-1)^{|a||\gamma|}\,\gamma(\lambda_*(a) \cdot c) \tag{2.1}$$

where $\lambda\colon G \to G$ denotes the group inversion. If $p\colon Y \to BG$ is a space over BG, then $C^*(Y)$ is a left $C^*(BG)$-module by $\beta \cdot \gamma = p^*(\beta) \cup \gamma$.

3. Koszul duality

Koszul duality is most elegantly expressed as a duality between $\mathbf{\Lambda}$-modules and comodules over the symmetric coalgebra $\mathbf{S}$ dual to $\mathbf{S}^*$, see [5, Sec. 2]. It hinges on the fact that the Koszul complex $\mathbf{S} \otimes_w \mathbf{\Lambda}$ is acyclic, where $w\colon \mathbf{S} \to \mathbf{\Lambda}$ is the canonical twisting cochain which sends each y_i to x_i and annihilates all other y_α. In this paper, though, we adopt a cohomological viewpoint. This makes definitions look rather ad hoc, but it is better suited to our discussion of equivariant cohomology in Section 8.

We denote the categories of bounded above weak modules over $\mathbf{\Lambda}$ and $\mathbf{S}^*$ by $\mathbf{\Lambda}$-$\mathcal{M}od$ and $\mathbf{S}^*$-$\mathcal{M}od$, respectively. (Recall that we grade cochain complexes negatively.) Note that any (strict) module over $\mathbf{\Lambda}$ or $\mathbf{S}^*$ is also a weak module because of the canonical twisting cochain w and its dual $w^*\colon \mathbf{\Lambda}^* \to \mathbf{S}^*$. The homology of a weak $\mathbf{\Lambda}$-module (N, v) is a $\mathbf{\Lambda}$-module by setting $x_i \cdot [n] = [v(y_i) \cdot n]$, and $\mathbf{S}^*$ acts on the homology of a weak $\mathbf{S}^*$-module (M, u) by $\xi_i \cdot [m] = [u(\xi_i) \cdot m]$. Before describing morphisms of weak modules, we say how the Koszul functors act on objects.

The Koszul dual of $(N, v) \in \mathbf{\Lambda}$-$\mathcal{M}od$ is defined as the bounded above $\mathbf{S}^*$-module $\mathbf{t}N = \mathbf{S}^* \otimes N$ with differential

$$d(\sigma \otimes n) = \sigma \otimes dn + \sum_{\alpha > 0} \xi^\alpha \sigma \otimes v(y_\alpha) \cdot n. \tag{3.1}$$

(This is well-defined because N is bounded above.)

The Koszul dual of $(M, u) \in \mathbf{S}^*$-$\mathcal{M}od$ is the bounded above $\mathbf{\Lambda}$-module $\mathbf{h}M = \mathbf{\Lambda}^* \otimes M$ with differential

$$d(\alpha \otimes m) = (-1)^{|\alpha|} \alpha \otimes dm + \sum_{\pi \neq \emptyset} (-1)^{|x_\pi|} x_\pi \cdot \alpha \otimes u(\xi_\pi) \cdot m \tag{3.2}$$

and $\mathbf{\Lambda}$-action coming from that on $\mathbf{\Lambda}^*$, which is defined similarly to (2.1),

$$(a \cdot \alpha)(a') = (-1)^{|a|(|\alpha|+1)} \alpha(a \wedge a').$$

A morphism f between two weak $\mathbf{\Lambda}$-modules N and N' is a morphism of (strict) $\mathbf{S}^*$-modules $\mathbf{t}N \to \mathbf{t}N'$. Its "base-component"

$$N = 1 \otimes N \hookrightarrow \mathbf{S}^* \otimes N \xrightarrow{f} \mathbf{S}^* \otimes N' \twoheadrightarrow 1 \otimes N' = N'$$

is a chain map inducing a $\mathbf{\Lambda}$-equivariant map in homology. If the latter is an isomorphism, we say that f is a quasi-isomorphism. The definitions for weak $\mathbf{S}^*$-modules are analogous. The Koszul dual of a morphism of weak modules is what one expects.
The Koszul functors preserve quasi-isomorphisms and are quasi-inverse to each other, cf. [5, Sec. 2.6]. Note that our (left) weak $\mathbf{S}^*$-modules correspond to *left* weak $\mathbf{S}$-comodules and not to right ones as used in [5]. This detail, which is crucial for the present paper, does not affect Koszul duality.

In the rest of this section we generalise results of [8, Sec. 9] to weak modules.

Following [8], we call a weak $\mathbf{S}^*$-module M is called *split and extended* if it is quasi-isomorphic to its homology and if the latter is of the form $\mathbf{S}^* \otimes L$ for some graded R-module L. If M it is quasi-isomorphic to its homology and if the $\mathbf{S}^*$-action on $H(M)$ is trivial, we say that M is *split and trivial.* Similar definitions apply to weak $\mathbf{\Lambda}$-modules. (Note that it does not make a difference whether we require the homology of a split and free $\mathbf{\Lambda}$-module to be isomorphic to $\mathbf{\Lambda} \otimes L$ or to $\mathbf{\Lambda}^* \otimes L$.)

PROPOSITION 3.1. *Under Koszul duality, split and trivial weak modules correspond to split and extended ones.*

Proof. That the Koszul functors carry split and trivial weak modules to split and extended ones is almost a tautology. The other direction follows from the fact that the Koszul functors are quasi-inverse to each other and preserve quasi-isomorphisms because a split and extended weak module is by definition quasi-isomorphic to the Koszul dual of a module with zero differential and trivial action. □

PROPOSITION 3.2. *Let M be in $\mathbf{S}^*$-$\mathcal{M}od$. If $H(M)$ is extended, then M is split and extended.*

Proof. We may assume that M has a strict $\mathbf{S}^*$-action because any weak $\mathbf{S}^*$-module M is quasi-isomorphic to a strict one (for instance, to $\mathbf{th}M$). By assumption, $H(M) \cong \mathbf{S}^* \otimes L$ for some graded R-module L. Since we work over a principal ideal domain, there exists a free resolution

$$0 \longleftarrow L \longleftarrow P^0 \longleftarrow P^1 \longleftarrow 0$$

of L with P^0, P^1 bounded above. Tensoring it with $\mathbf{S}^*$ gives a free resolution of the $\mathbf{S}^*$-module $H(M)$ and therefore the (not uniquely determined) $\mathbf{S}^*$-equivariant vertical maps in the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longleftarrow & \mathbf{S}^* \otimes L & \longleftarrow & \mathbf{S}^* \otimes P^0 & \longleftarrow & \mathbf{S}^* \otimes P^1 & \longleftarrow & 0 \\
 & & \downarrow \cong & & \downarrow & & \downarrow & & \\
0 & \longleftarrow & H(M) & \longleftarrow & Z(M) & \xleftarrow{\;d\;} & M. & &
\end{array}$$

This implies that the total complex $\mathbf{S}^* \otimes P$ is quasi-isomorphic to both $H(M)$ and M. □

4. Proof of Theorem 1.4

In this section all algebras are **N**-graded and connected unless otherwise stated. Recall that an A_∞ map $f\colon A \Rightarrow A'$ between two algebras is a map of coalgebras $BA \to BA'$, see [18, Sec. 8.1] or [17] for example. It is called strict if it is induced from an algebra map $A \to A'$. If $f\colon A \Rightarrow A'$ is A_∞, then its base component $f_1\colon B_1A \to B_1A'$ between the elements of external degree 1 is a chain map, multiplicative up to homotopy. We denote the induced algebra map in homology by $H(f)\colon H(A) \to H(A')$. If it is an isomorphism, we call f an A_∞ quasi-isomorphism.
In order to prove Theorem 1.4, it is sufficient to construct an A_∞ quasi-isomorphism $A \Rightarrow H(A) = \bigwedge(x_1, \dots, x_r) = \mathbf{\Lambda}$, due to the following result:

Lemma 4.1. *Let A be an algebra with A and $H(A)$ free over R, and let $f\colon A \Rightarrow H(A)$ be an A_∞ map inducing the identity in homology. Then f has an A_∞ quasi-inverse, i. e., there is an A_∞ map $g\colon H(A) \Rightarrow A$ also inducing the identity in homology.*

(At least over fields one can do better: there any A_∞ quasi-isomorphism between two algebras – even A_∞ algebras – is an A_∞ homotopy equivalence, cf. [20] or [17, Sec. 3.7].)

Proof. According to [19, Prop. 2.2], the claim is true if f is strict. (Here we use that over a principal ideal domain any quasi-isomorphism $A \to H(A)$ of free modules comes from a "trivialised extension" in the sense of [19, §2.1].) To reduce the general case to this, we consider the cobar construction ΩBA of BA. Coalgebra maps $h\colon BA \to BA'$ correspond bijectively to algebra maps $\tilde{h}\colon \Omega BA \to A'$. For h, the identity of A, the map $\tilde{h}$ is a quasi-isomorphism [15, Thm II.4.4] with quasi-inverse (in the category of complexes), the canonical inclusion $A \hookrightarrow \Omega BA$. The composition of this map with $\tilde{f}\colon \Omega BA \to H(A)$ is essentially f_1, which is a quasi-isomorphism by hypothesis. Hence $\tilde{f}$ is so, too. Now compose any A_∞ quasi-inverse of it with the projection $\Omega BA \to A$. □

Recall that for any complex C a cycle in $C^q = \operatorname{Hom}_{-q}(C, R)$ is the same as a chain map $C \to R[-q]$. (Here $R[-q]$ denotes the complex R, shifted to degree q.) The crucial observation, made in a topological context by Stasheff [21, Thm. 5.1], is the following:

Lemma 4.2. *A_∞ maps $A \Rightarrow \bigwedge(x)$, $|x| = q > 0$, correspond bijectively to cocycles in $(BA)^{q+1}$.*

Proof. Note that the augmentation ideal of $\bigwedge(x)$ is $R[-q]$ (with vanishing product). An A_∞ map $f\colon A \Rightarrow \bigwedge(x)$ is given by components $f_p\colon \bar{A}^{\otimes p} \to R[-q]$ of degree $p-1$ such that for all $[a_1, \dots, a_p] \in B_p(A)$,

$$f_p(d[a_1, \dots, a_p]) = -f_{p-1}(\delta[a_1, \dots, a_p]),$$

where $d\colon B_p(A)\to B_p(A)$ denotes the "internal" differential and $\delta\colon B_p(A)\to B_{p-1}(A)$ the "external" one, cf. [18, Thm. 8.18]. In other words, $d(f_p) = -\delta(f_{p-1})$, where δ and d now denote the dual differentials. But this is the condition for a cycle in the double complex $((BA)^*, d, \delta)$ dual to BA. $\square$

By our assumptions, $H^*(BA) = \mathbf{S}^*$ is a (negatively graded) polynomial algebra. Taking representatives of the generators ξ_i gives A_∞ maps $f^{(i)}\colon A \Rightarrow \bigwedge(x_i)$. By [19, Prop. 3.3 & 3.7], they assemble into an A_∞ map

$$f^{(1)}\otimes\cdots\otimes f^{(r)}\colon A^{\otimes r} \Rightarrow \bigwedge(x_1)\otimes\cdots\otimes\bigwedge(x_r) = \mathbf{\Lambda}$$

whose base component is the tensor product of the base components $f_1^{(i)}$. Since A is a Hopf algebra, the r-fold diagonal $\Delta^{(r)}\colon A\to A^{\otimes r}$ is a morphism of algebras. A test on the generators x_i reveals that the composition $(f^{(1)}\otimes\cdots\otimes f^{(r)})\Delta^{(r)}\colon A \Rightarrow \mathbf{\Lambda}$ induces an isomorphism in homology, hence is the A_∞ quasi-isomorphism we are looking for.

REMARK 4.3. Since we have not really used the coassociativity of Δ, Theorem 1.4 holds even for quasi-Hopf algebras in the sense of [15, §IV.5].

5. THE TWISTING COCHAIN $v\colon \mathbf{S}\to C(G)$

This is now easy: Compose the map $\mathbf{S}\to B\mathbf{\Lambda}$ determined by the canonical twisting cochain $w\colon \mathbf{S}\to\mathbf{\Lambda}$ with the map $B\mathbf{\Lambda}\to BC(G)$. This corresponds to a twisting cochain $\mathbf{S}\to C(G)$ mapping each cogenerator $y_i\in\mathbf{S}$ to a representative of $x_i\in\mathbf{\Lambda}$. Since these elements are used to define the $\mathbf{\Lambda}$-action in the homology of a weak $\mathbf{\Lambda}$-module, we get the usual action of $\mathbf{\Lambda} = H(G)$ there.
Note that by dualisation we obtain a quasi-isomorphism of algebras $(BC(G))^*\to\mathbf{S}^*$. This is not exactly the same as the quasi-isomorphism of algebras $C^*(BG)\to\mathbf{S}^*$ from Proposition 1.3, which we are going to construct next.

6. PROOF OF THEOREM 1.2 (FIRST PART) AND OF PROPOSITION 1.3

In this section we construct maps

$$\Psi_X\colon \mathbf{S}\otimes_v C(X)\to C(EG\underset{G}{\times} X) = C(\boldsymbol{t}X),$$

natural in $X\in G$-***Space***. We will show that $\psi := \Psi_{\mathrm{pt}}\colon \mathbf{S}\to C(BG)$ is a quasi-isomorphism of coalgebras and that Ψ_X, which maps from an $\mathbf{S}$-comodule to a $C(BG)$–comodule, is a ψ-equivariant quasi-isomorphism. Taking duals then gives Proposition 1.3 and the first half of Theorem 1.2.
Recall that the differential on $\mathbf{S}\otimes_v C(X)$ is

$$d(y_\alpha\otimes c) = y_\alpha\otimes dc + \sum_{\beta<\alpha} y_\beta\otimes c_{\alpha-\beta}\cdot c,$$

where we have abbreviated $v(y_{\alpha-\beta})$ to $c_{\alpha-\beta}$. The summation runs over all β strictly smaller than α in the canonical partial ordering of $\mathbf{N}^r$.

To begin with, we define a map

$$f\colon \mathbf{S}\otimes_v C(G)\to C(EG)$$

by recursively setting

$$f(1\otimes a)=e_0\cdot a,$$
$$f(y_\alpha\otimes a)=\Big(Sf\big(d(y_\alpha\otimes 1)\big)\Big)\cdot a$$

for $\alpha>0$. Here e_0 is the canonical base point of the simplicial construction of the right G-space EG and S its canonical contracting homotopy, cf. [5, Sec. 3.7].

Lemma 6.1. *This f is a quasi-morphism of right $C(G)$-modules.*

Proof. The map is equivariant by construction. By induction, one has for $\alpha>0$

$$d\,f(y_\alpha\otimes 1)=d\,Sf\big(d(y_\alpha\otimes 1)\big)=f\big(d(y_\alpha\otimes 1)\big)-S\,d\,f\big(d(y_\alpha\otimes 1)\big)=f\big(d(y_\alpha\otimes 1)\big),$$

which shows that it is a chain map. That it induces an isomorphism in homology follows from the acyclicity of $\mathbf{S}\otimes_v C(G)$: Filter the complex according to the number of factors ξ_i appearing in an element $\xi^\alpha\otimes a$, i.e., by $\alpha_1+\cdots+\alpha_r$. Then the E^1 term of the corresponding spectral sequence is the Koszul complex $\mathbf{S}\otimes_w \mathbf{\Lambda}$, hence acyclic. □

We will also need the following result:

Lemma 6.2. *The image of $f(y_\alpha\otimes 1)$, $\alpha\in\mathbf{N}^r$, under the diagonal Δ of the coalgebra $C(EG)$ is*

$$\Delta f(y_\alpha\otimes 1)\equiv\sum_{\beta+\gamma=\alpha} f(y_\beta\otimes 1)\otimes f(y_\gamma\otimes 1),$$

up to terms of the form $c\cdot a\otimes c'$ with c, $c'\in C(EG)$ and $a\in C(G)$, $|a|>0$.

Proof. We proceed by induction, the case $\alpha=0$ being trivial. For $\alpha>0$ we have

$$\Delta f(y_\alpha\otimes 1)=\Delta Sf\big(d\,(y_\alpha\otimes 1)\big)=\sum_{\beta<\alpha}\Delta S\big(f(y_\beta\otimes 1)\cdot c_{\alpha-\beta}\big)$$

We now use the identity $\Delta S(c)=Sc\otimes 1+(1\otimes S)AW(c)$ [5, Prop. 3.8] and the $C(G)$-equivariance of the Alexander–Whitney map to get

$$=f(y_\alpha\otimes 1)\otimes 1+(1\otimes S)\sum_{\beta<\alpha}\Delta f(y_\beta\otimes 1)\cdot\Delta c_{\alpha-\beta},$$

where the second diagonal is of course that of $C(G)$. By induction and the fact that $\Delta c_{\alpha-\beta}\equiv 1\otimes c_{\alpha-\beta}$ up to terms $a\otimes a'$ with $|a|>0$, we find

$$\equiv f(y_\alpha\otimes 1)\otimes 1+(1\otimes S)\sum_{\beta+\gamma<\alpha} f(y_\beta\otimes 1)\otimes f(y_\gamma\otimes 1)\cdot c_{\alpha-(\beta+\gamma)}$$
$$=f(y_\alpha\otimes 1)\otimes 1+\sum_{\substack{\beta<\alpha\\ \gamma<\alpha-\beta}} f(y_\beta\otimes 1)\otimes Sf(y_\gamma\otimes c_{(\alpha-\beta)-\gamma}),$$

which simplifies by the definition of f to

$$= f(y_\alpha \otimes 1) \otimes 1 + \sum_{\beta<\alpha} f(y_\beta \otimes 1) \otimes f(y_{\alpha-\beta} \otimes 1),$$

as was to be shown. □

For a G-space X we define the map

$$\Psi_X \colon \mathbf{t}C(X) = \mathbf{S} \otimes_v C(X) \to C(EG \underset{G}{\times} X) = C(\boldsymbol{t}X)$$

as the bottom row of the commutative diagram

$$\begin{array}{ccccccc}
 & & \mathbf{S} \otimes_v C(G) \otimes C(X) & \xrightarrow{f\otimes 1} & C(EG) \otimes C(X) & \xrightarrow{\nabla} & C(EG \times X) \\
 & & \downarrow & & \downarrow & & \downarrow \\
\mathbf{S} \otimes_v C(X) & = & \mathbf{S} \otimes_v C(G) \underset{C(G)}{\otimes} C(X) & \longrightarrow & C(EG) \underset{C(G)}{\otimes} C(X) & \longrightarrow & C(EG \underset{G}{\times} X),
\end{array}$$

where ∇ denotes the shuffle map. Ψ_X is obviously natural in X.
It follows from the preceding lemma that $\psi = \Psi_{\mathrm{pt}} \colon \mathbf{S} \to C(BG)$ is a morphism of coalgebras because terms of the form $c \cdot a$ with $|a| > 0$ are annihilated by the projection $C(EG) \to C(BG)$. (We are working with normalised chains!)
Using naturality and the commutativity of the diagram

$$\begin{array}{ccc}
C(EG) \otimes C(X) & \xrightarrow{\quad\nabla\quad} & C(EG \times X) \\
\Big\downarrow {\scriptstyle \Delta_{C(EG)} \otimes 1} & & \Big\downarrow {\scriptstyle \Delta_{C(EG\times X)}} \\
C(BG) \otimes C(EG) \otimes C(X) & \xrightarrow[1\otimes\nabla]{} & C(BG) \otimes C(EG \times X),
\end{array}$$

one proves similarly that Ψ_X is a ψ-equivariant morphism of comodules. To see that it induces an isomorphism in homology, consider the diagram

$$\begin{array}{ccccc}
\mathrm{Tor}^{C(G)}\big(\mathbf{S} \otimes_v C(G), C(X)\big) & \longrightarrow & H\big(\mathbf{S} \otimes_v C(G) \underset{C(G)}{\otimes} C(X)\big) & = & H(\mathbf{S} \otimes_v C(X)) \\
\Big\downarrow {\scriptstyle \mathrm{Tor}^{\mathrm{id}}(f,\mathrm{id})} & & \Big\downarrow & & \Big\downarrow {\scriptstyle H(\Psi_X)} \\
\mathrm{Tor}^{C(G)}\big(C(EG), C(X)\big) & \longrightarrow & H\big(C(EG) \underset{C(G)}{\otimes} C(X)\big) & \longrightarrow & H(EG \underset{G}{\times} X).
\end{array}$$

The composition along the bottom row is an isomorphism by Moore's theorem [18, Thm. 7.27],[2] and the top row is so because $\mathbf{S} \otimes_v C(G)$ is $C(G)$-flat. Since $\mathrm{Tor}^{\mathrm{id}}(f, \mathrm{id})$ is an isomorphism by Lemma 6.1, $H(\Psi_X)$ is so, too.

[2] In fact, each single arrow is an isomorphism. This follows from the twisted Eilenberg–Zilber theorem, see [9] for example.

7. The twisting cochain $u\colon \mathbf{\Lambda}^* \to C^*(BG)$ and the end of the proof of Theorem 1.2

The map $\psi\colon \mathbf{S} \to C(BG)$ is a quasi-isomorphism of simply connected coalgebras. Similar to the first step in the proof of Lemma 4.1, it comes from a trivialised extension (or "Eilenberg–Zilber data" in the terminology of [11]). By [11, Thm. 4.1*], there is an algebra map $F\colon \Omega C(BG) \to \Omega\mathbf{S}$ whose base component $F_{-1}\colon \Omega_{-1}C(BG) \to \Omega_{-1}\mathbf{S}$ is essentially the chosen homotopy inverse to ψ. Composing such an F with the canonical map $g\colon \Omega\mathbf{S} \to \mathbf{\Lambda}$, we get a twisting cochain $\tilde{u}\colon C(BG) \to \mathbf{\Lambda}$. Write

$$\tilde{u} = \sum_{\emptyset\neq\pi\subset\{1,\ldots,r\}} x_\pi \otimes \gamma_\pi \in \mathbf{\Lambda} \otimes C^*(BG) = \operatorname{Hom}(C(BG), \mathbf{\Lambda}). \tag{7.1}$$

Then γ_i is a representative of the generator $\xi_i \in \mathbf{S}^*$ because it is a cocycle (cf. [5, eq. (2.12)]) and

$$\tilde{u}(\psi(y_i)) = g(F([\psi(y_i)])) = g(y_i) = x_i.$$

The dual $u = \tilde{u}^*\colon \mathbf{\Lambda}^* \to C^*(BG)$ is again a cochain, which corresponds under the isomorphism $\operatorname{Hom}(\mathbf{\Lambda}^*, C^*(BG)) = C^*(BG) \otimes \mathbf{\Lambda}$ to the transposition of factors of (7.1). Therefore, the induced action of $\mathbf{S}^*$ on a $C^*(BG)$-module, considered as weak $\mathbf{S}^*$-module, is given by $\xi_i \cdot [m] = [\gamma_i \cdot m]$, as desired.

For a given G-space X, we now look at the map Ψ^*_X as a quasi-isomorphism of $C^*(BG)$-modules, where the module structure of $\mathbf{t}C^*(X)$ is induced by ψ^*. By naturality, it is a morphism of weak $\mathbf{S}^*$-modules. This new weak $\mathbf{S}^*$-action on $\mathbf{t}C^*(X)$ coincides with the (strict) old one because the composition

$$(\Omega\mathbf{S})^* \xrightarrow{F^*} (\Omega C(BG))^* \xrightarrow{\psi^*} (\Omega\mathbf{S})^*$$

is the identity. This proves that Ψ^*_X is a quasi-isomorphism of weak $\mathbf{S}^*$-modules, hence that the functors $C^* \circ \boldsymbol{t}$ and $\mathbf{t} \circ C^*$ are quasi-isomorphic.
The corresponding result for the functors $\boldsymbol{h}$ and $\mathbf{h}$ is a formal consequence of this because they are quasi-inverse to $\boldsymbol{t}$ and $\mathbf{t}$, respectively. This finishes the proof of Theorem 1.2.

Remark 7.1. For $G = (S^1)^r$ a torus (and a reasonable choice of v) one may also take the twisting cochain $\mathbf{\Lambda}^* \to C^*(BG)$ of Gugenheim–May [10, Example 2.2], which is defined using iterated cup_1 products of (any choice of) representatives $\gamma_i \in C^*(BG)$ of the $\xi_i \in \mathbf{S}^*$. (This follows for example from [5, Cor. 4.4].) It would be interesting to know whether this remains true in general if one chooses the γ_i carefully enough.

8. Equivariantly formal spaces

An important class of G-spaces are the equivariantly formal ones. Their equivariant cohomology is particularly simple, which is often exploited in algebraic or symplectic geometry or combinatorics.
We say that X is *R-equivariantly formal* if the following conditions hold.

Proposition 8.1. *For a G-space X, the following are equivalent:*

(1) *$H^*_G(X)$ is extended.*
(2) *$C^*(X_G)$ is split and extended.*
(3) *$C^*(X)$ is split and trivial.*
(4) *The canonical map $H^*_G(X) \to H^*(X)$ admits a section of graded R-modules.*
(5) *$H^*_G(X)$ is isomorphic, as $\mathbf{S}^*$-module, to the E_2 term $\mathbf{S}^* \otimes H^*(X)$ of the Leray–Serre spectral sequence for X_G (which therefore degenerates).*

Note that if R is a field, condition (1) means that $H^*_G(X)$ is free over $\mathbf{S}^*$, and condition (4) that $H^*_G(X) \to H^*(X)$ is surjective. A space X with the latter property is traditionally called "totally non-homologous to zero in X_G with respect to R". We stress the fact that for some of the above conditions we really need the assumption that R is a principal ideal domain.
In [6] (see also [7]) it is shown that a compact symplectic manifold X with a Hamiltonian torus action is $\mathbf{Z}$-equivariantly formal if $X^T = X^{T_p}$ for each prime p that kills elements in $H^*(X^T)$. Here $T_p \cong \mathbf{Z}_p^r$ denotes the maximal p-torus contained in the torus T. In particular, a compact Hamiltonian T-manifold is $\mathbf{Z}$-equivariantly formal if the isotropy group of each non-fixed point is contained in a proper subtorus.

Proof. (5) $\Rightarrow$ (1) is trivial. (1) $\Rightarrow$ (2) follows from Proposition 3.2, and (2) $\Rightarrow$ (3) from Proposition 3.1 because $C^*(X)$ and $C^*(X_G)$ are Koszul dual by Theorem 1.2. (4) $\Rightarrow$ (5) is the Leray–Hirsch theorem. (Note that it holds here for arbitrary X because $H^*(BG) = \mathbf{S}^*$ is of finite type.)
(3) $\Rightarrow$ (4): The (in the simplicial setting canonical) map $C^*(X_G) \to C^*(X)$ is the composition of Ψ^*_X with the canonical projection $\mathbf{t}C^*(X) \to C^*(X)$. Since $C^*(X)$ is split, we can pass from $C^*(X)$ to $H^*(X)$ by a sequence of commutative diagrams

$$\begin{array}{ccc} \mathbf{t}N & \longrightarrow & N \\ \downarrow & & \downarrow \\ \mathbf{t}N' & \longrightarrow & N' \end{array}$$

where the vertical arrow on the right is the base component of the quasi-isomorphism of weak $\mathbf{\Lambda}$-modules given on the left. But for the projection $\mathbf{S}^* \otimes H^*(X) \to H^*(X)$ the assertion is obvious because $\mathbf{\Lambda}$ acts trivially on $H^*(X)$, which means that there are no differentials any more. $\square$

9. Relation to the Cartan model

In differential geometry and differential homological algebra many different complexes ("models") are known that compute the equivariant cohomology of a space. We content ourselves with indicating the relation between our construction and the probably best-known one, the so-called Cartan model. We use real or complex coefficients.

Let G be a compact connected Lie group and X a G-manifold. The Cartan model of X is the complex

$$\Big(\mathrm{Sym}(\mathfrak{g}^*) \otimes \Omega(X)\Big)^G \tag{9.1a}$$

of G-invariants with differential

$$d(\sigma \otimes \omega) = \sigma \otimes d\omega + \sum_{j=1}^{s} \zeta_j \sigma \otimes z_j \cdot \omega. \tag{9.1b}$$

Here $\mathrm{Sym}(\mathfrak{g}^*)$ denotes the (evenly graded) polynomial functions on the Lie algebra $\mathfrak{g}$ of G, (z_j) a basis of $\mathfrak{g}$ with dual basis (ζ_j), and $z_j \cdot \omega$ the contraction of the form ω with the generating vector field associated with z_j. The Cartan model computes $H^*_G(X)$ as algebra and as $\mathbf{S}^*$-module, cf. [12].

As mentioned in the introduction, Goresky, Kottwitz and MacPherson [8] have found an even smaller complex giving the $\mathbf{S}^*$-module $H^*_G(X)$, namely $\mathbf{t}\Omega(X)^G$, or explicitly

$$\mathrm{Sym}(\mathfrak{g}^*)^G \otimes \Omega(X)^G, \tag{9.2a}$$

where $\Omega(X)^G$ denotes the complex of G-invariant differential forms on X. The differential

$$d(\sigma \otimes \omega) = \sigma \otimes d\omega + \sum_{i=1}^{r} \xi_i \sigma \otimes x_i \cdot \omega \tag{9.2b}$$

is similar to (9.1b), but the summation now runs over a system of generators of $\mathbf{S}^* = H^*(BG) = \mathrm{Sym}(\mathfrak{g}^*)^G$. (This is of course differential (3.1) for strict $\mathbf{\Lambda}$-modules.) Alekseev and Meinrenken [1] have proved that the complexes (9.1) and (9.2) are quasi-isomorphic as $\mathbf{S}^*$-modules.

For the case of torus actions (where (9.1) and (9.2) coincide), Goresky–Kottwitz–MacPherson [8, Sec. 12] have shown that one may replace $\Omega(X)^T$ by singular cochains together with the "sweep action", which is defined by restricting the action of $C(T)$ along a quasi-isomorphism of algebras $\mathbf{\Lambda} = H(T) \to C(T)$. The latter is easy to construct, as explained in the introduction. Now all ingredients are defined for an arbitrary topological T-space X and an arbitrary coefficient ring R, and the resulting complex does indeed compute $H^*_T(X)$ as algebra and as $\mathbf{S}^*$-module in this generality, see Félix–Halperin–Thomas [4, Sec. 7.3].

Appendix: The theorems of Samelson–Leray and Hopf

All differentials are zero in this section. Recall that an element a of a Hopf algebra A is called primitive if $\Delta a = a \otimes 1 + 1 \otimes a$ or, equivalently, if the projection of Δa to $\bar{A} \otimes \bar{A}$ is zero.

Let A be a Hopf algebra over a field, isomorphic as algebra to an exterior algebra. Then A is primitively generated (Samelson–Leray). If R is a field of characteristic 0 and A a connected commutative Hopf algebra, finite-dimensional over R, then multiplicatively it is an exterior algebra (Hopf), hence also primitively generated. (A good reference for our purposes is [16, §§1, 2].)
We now show that the analogous statements hold over any principal ideal domain. Denote for a Hopf algebra A over R the extension of coefficients to the quotient field of R by $A_{(0)}$.

PROPOSITION 9.1. *Let A be a Hopf algebra, free over R and such that $A_{(0)}$ is a primitively generated exterior algebra. Then A is a primitively generated exterior algebra.*

Proof. Let A' be the sub Hopf algebra generated by the free submodule of primitive elements of A. Then $A'_{(0)} = A_{(0)}$ (Samelson–Leray), hence A' is a primitively generated exterior algebra and A/A' is R-torsion. Take an $a \in A \backslash A'$ of smallest degree. Then $ka \in A'$ for some $0 \neq k \in R$, and the image of Δa in $\bar{A} \otimes \bar{A}$ already lies in $\bar{A}' \otimes \bar{A}'$. Write $ka = a_1 + a_2$ with $a_1 \in A'$ primitive and $a_2 \in \bar{A}' \cdot \bar{A}'$. Note that the image of Δa_2 in $\bar{A}' \otimes \bar{A}'$ is divisible by k. This implies that a_2 is divisible by k in A'. (Look at how the various products of the generators of a primitively generated exterior algebra behave under the diagonal.) Since $a - a_2/k$ is primitive, it lies in A', hence a as well. Therefore, $A = A'$. □

Added in proof. Suppose that G is a compact connected Lie group and let $T \subset G$ be a maximal torus. In their recent preprint "Torsion and abelianization in equivariant cohomology" (math.AT/0607069), T. Holm and R. Sjamaar show that in this situation $H^*_G(X)$ consists of the Weyl group invariants of $H^*_T(X)$. Their assumption on the coefficient ring R is essentially the same as ours. Together with the explicit Cartan model for torus actions [5], this gives another model for $H^*_G(X)$.

REFERENCES

[1] A. Alekseev and E. Meinrenken. Equivariant cohomology and the Maurer-Cartan equation. *Duke Math. J.* 130, 479-522.

[2] C. Allday and V. Puppe. On a conjecture of Goresky, Kottwitz and MacPherson. *Canad. J. Math.* 51 (1999), 3–9.

[3] E. Dror, W. G. Dwyer, D. M. Kan. Equivariant maps which are self homotopy equivalences. *Proc. AMS* 80 (1980), 670–672.

[4] Y. Felix, S. Halperin, and J.-C. Thomas. Differential graded algebras in topology. Ch. 16 in: I. M. James (ed.), *Handbook of algebraic topology*, Elsevier, Amsterdam 1995.

[5] M. Franz. Koszul duality and equivariant cohomology for tori. *Int. Math. Res. Not.* 42, 2255-2303 (2003).

[6] M. Franz and V. Puppe. Exact sequences for equivariantly formal spaces. ArXiv e-print math.AT/0307112.

[7] M. Franz and V. Puppe. Exact cohomology sequences with integral coefficients for torus actions. To appear in *Transformation Groups*.
[8] M. Goresky, R. Kottwitz, and R. MacPherson. Equivariant cohomology, Koszul duality, and the localization theorem. *Invent. Math.* 131 (1998), 25–83.
[9] V. K. A. M. Gugenheim. On the chain-complex of a fibration. *Illinois J. Math.* 16 (1972), 398–414.
[10] V. K. A. M. Gugenheim and J. P. May. On the theory and applications of differential torsion products. *Mem. Am. Math. Soc.* 142 (1974).
[11] V. K. A. M. Gugenheim and H. J. Munkholm. On the extended functoriality of Tor and Cotor. *J. Pure Appl. Algebra* 4 (1974), 9–29.
[12] V. W. Guillemin and S. Sternberg. *Supersymmetry and equivariant de Rham theory.* Springer, Berlin 1999.
[13] J. Huebschmann. Perturbation theory and small models for the chains of certain induced fibre spaces. Habilitationsschrift, Universität Heidelberg 1984.
[14] J. Huebschmann. Homological perturbations, equivariant cohomology, and Koszul duality. ArXiv math.AT/0401160.
[15] D. H. Husemoller, J. C. Moore, and J. Stasheff. Differential homological algebra and homogeneous spaces. *J. Pure Appl. Algebra* 5 (1974), 113–185.
[16] R. M. Kane. *The homology of Hopf spaces.* North-Holland, Amsterdam 1988.
[17] B. Keller. Introduction to A-infinity algebras and modules. *Homology Homotopy Appl.* 3 (2001), 1–35. Addendum *ibid.* 4 (2002), 25–28.
[18] J. McCleary. *A user's guide to spectral sequences*, 2nd ed., Cambridge University Press, Cambridge 2001.
[19] H. J. Munkholm. The Eilenberg–Moore spectral sequence and strongly homotopy multiplicative maps. *J. Pure Appl. Algebra* 5 (1974), 1–50.
[20] H. J. Munkholm. shm maps of differential algebras, I. A characterization up to homotopy. *J. Pure Appl. Algebra* 9 (1976), 39–46.
[21] J. D. Stasheff. Homotopy associativity of H-spaces. II. *Trans. AMS* 108 (1963), 293–312.
[22] J. Stasheff and S. Halperin. Differential algebra in its own rite. Pages 567–577 in *Proc. Adv. Study Inst. Alg. Top. (Aarhus 1970)*, Vol. III. Various Publ. Ser. 13, Mat. Inst. Aarhus Univ., Aarhus 1970.

Matthias Franz
Fachbereich Mathematik
Universität Konstanz
78457 Konstanz
Germany
matthias.franz@ujf-grenoble.fr

Derived Categories of Coherent Sheaves on Rational Homogeneous Manifolds

Christian Böhning

Received: February 14, 2006
Revised: May 15, 2006

Communicated by Thomas Peternell

Abstract. One way to reformulate the celebrated theorem of Beilinson is that $(\mathcal{O}(-n), \dots, \mathcal{O})$ and $(\Omega^n(n), \dots, \Omega^1(1), \mathcal{O})$ are strong complete exceptional sequences in $D^b(Coh\, \mathbb{P}^n)$, the bounded derived category of coherent sheaves on $\mathbb{P}^n$. In a series of papers ([Ka1], [Ka2], [Ka3]) M. M. Kapranov generalized this result to flag manifolds of type A_n and quadrics. In another direction, Y. Kawamata has recently proven existence of complete exceptional sequences on toric varieties ([Kaw]).
Starting point of the present work is a conjecture of F. Catanese which says that on every rational homogeneous manifold $X = G/P$, where G is a connected complex semisimple Lie group and $P \subset G$ a parabolic subgroup, there should exist a complete strong exceptional poset (cf. def. 2.1.7 (B)) and a bijection of the elements of the poset with the Schubert varieties in X such that the partial order on the poset is the order induced by the Bruhat-Chevalley order (cf. conjecture 2.2.1 (A)). An answer to this question would also be of interest with regard to a conjecture of B. Dubrovin ([Du], conj. 4.2.2) which has its source in considerations concerning a hypothetical mirror partner of a projective variety Y: There is a complete exceptional sequence in $D^b(Coh\, Y)$ if and only if the quantum cohomology of Y is generically semisimple (the complete form of the conjecture also makes a prediction about the Gram matrix of such a collection). A proof of this conjecture would also support M. Kontsevich's homological mirror conjecture, one of the most important open problems in applications of complex geometry to physics today (cf. [Kon]).
The goal of this work will be to provide further evidence for F. Catanese's conjecture, to clarify some aspects of it and to supply new techniques. In section 2 it is shown among other things that

the length of every complete exceptional sequence on X must be the number of Schubert varieties in X and that one can find a complete exceptional sequence on the product of two varieties once one knows such sequences on the single factors, both of which follow from known methods developed by Rudakov, Gorodentsev, Bondal et al. Thus one reduces the problem to the case $X = G/P$ with G simple. Furthermore it is shown that the conjecture holds true for the sequences given by Kapranov for Grassmannians and quadrics. One computes the matrix of the bilinear form on the Grothendieck K-group $K_\circ(X)$ given by the Euler characteristic with respect to the basis formed by the classes of structure sheaves of Schubert varieties in X; this matrix is conjugate to the Gram matrix of a complete exceptional sequence. Section 3 contains a proof of theorem 3.2.7 which gives complete exceptional sequences on quadric bundles over base manifolds on which such sequences are known. This enlarges substantially the class of varieties (in particular rational homogeneous manifolds) on which those sequences are known to exist. In the remainder of section 3 we consider varieties of isotropic flags in a symplectic resp. orthogonal vector space. By a theorem due to Orlov (thm. 3.1.5) one reduces the problem of finding complete exceptional sequences on them to the case of isotropic Grassmannians. For these, theorem 3.3.3 gives generators of the derived category which are homogeneous vector bundles; in special cases those can be used to construct complete exceptional collections. In subsection 3.4 it is shown how one can extend the preceding method to the orthogonal case with the help of theorem 3.2.7. In particular we prove theorem 3.4.1 which gives a generating set for the derived category of coherent sheaves on the Grassmannian of isotropic 3-planes in a 7-dimensional orthogonal vector space. Section 4 is dedicated to providing the geometric motivation of Catanese's conjecture and it contains an alternative approach to the construction of complete exceptional sequences on rational homogeneous manifolds which is based on a theorem of M. Brion (thm. 4.1.1) and cellular resolutions of monomial ideals à la Bayer/Sturmfels. We give a new proof of the theorem of Beilinson on $\mathbb{P}^n$ in order to show that this approach might work in general. We also prove theorem 4.2.5 which gives a concrete description of certain functors that have to be investigated in this approach.

2000 Mathematics Subject Classification: 14M15, 14F05; 18E30

Keywords and Phrases: flag varieties, rational homogeneous manifolds, derived category

Contents

1 Introduction

The concept of derived category of an Abelian category $\mathcal{A}$, which gives a transparent and compact way to handle the totality of cohomological data attached to $\mathcal{A}$ and puts a given object of $\mathcal{A}$ and all of its resolutions on equal footing, was conceived by Grothendieck at the beginning of the 1960's and their internal structure was axiomatized by Verdier through the notion of triangulated category in his 1967 thesis (cf. [Ver1], [Ver2]). Verdier's axioms for distinguished triangles still allow for some pathologies (cf. [GeMa], IV.1, 7) and in [BK] it was suggested how to replace them by more satisfactory ones, but since the former are in current use, they will also be the basis of this text. One may consult [Nee] for foundational questions on triangulated categories.
However, it was only in 1978 that people laid hands on "concrete" derived categories of geometrical significance (cf. [Bei] and [BGG2]), and A. A. Beilinson constructed strong complete exceptional sequences of vector bundles for $D^b(Coh\,\mathbb{P}^n)$, the bounded derived category of coherent sheaves on $\mathbb{P}^n$. The terminology is explained in section 2, def. 2.1.7, below, but roughly the simplification brought about by Beilinson's theorem is analogous to the construction of a semi-orthonormal basis $(e_1, \dots, e_d)$ for a vector space equipped with a non-degenerate (non-symmetric) bilinear form χ (i.e., $\chi(e_i, e_i) = 1\ \forall i$, $\chi(e_j, e_i) = 0\ \forall j > i$)).
Beilinson's theorem represented a spectacular breakthrough and, among other things, his technique was applied to the study of moduli spaces of semi-stable sheaves of given rank and Chern classes on $\mathbb{P}^2$ and $\mathbb{P}^3$ by Horrocks,

Barth/Hulek, Drézet/Le Potier (cf. [OSS], [Po] and references therein).
Recently, A. Canonaco has obtained a generalization of Beilinson's theorem to weighted projective spaces and applied it to the study of canonical projections of surfaces of general type on a 3-dimensional weighted projective space (cf. [Can], cf. also [AKO]).
From 1984 onwards, in a series of papers [Ka1], [Ka2], [Ka3], M. M. Kapranov found strong complete exceptional sequences on Grassmannians and flag varieties of type A_n and on quadrics. Subsequently, exceptional sequences alongside with some new concepts introduced in the meantime such as helices, mutations, semi-orthogonal decompositions etc. were intensively studied, especially in Russia, an account of which can be found in the volume [Ru1] summarizing a series of seminars conducted by A. N. Rudakov in Moscow (cf. also [Bo], [BoKa], [Or]). Nevertheless, despite the wealth of new techniques introduced in the process, many basic questions concerning exceptional sequences are still very much open. These fall into two main classes: first questions of existence: E.g., do complete exceptional sequences always exist on rational homogeneous manifolds? (For toric varieties existence of complete exceptional sequences was proven very recently by Kawamata, cf. [Kaw].) Secondly, one often does not know if basic intuitions derived from semi-orthogonal linear algebra hold true in the framework of exceptional sequences, and thus one does not have enough flexibility to manipulate them, e.g.: Can every exceptional bundle on a variety X on which complete exceptional sequences are known to exist (projective spaces, quadrics...) be included in a complete exceptional sequence?
To round off this brief historical sketch, one should not forget to mention that derived categories have proven to be of geometrical significance in a lot of other contexts, e.g. through Fourier-Mukai transforms and the reconstruction theorem of Bondal-Orlov for smooth projective varieties with ample canonical or anti-canonical class (cf. [Or2]), in the theory of perverse sheaves and the generalized Riemann-Hilbert correspondence (cf. [BBD]), or in the recent proof of T. Bridgeland that birational Calabi-Yau threefolds have equivalent derived categories and in particular the same Hodge numbers (cf. [Brid]). Interest in derived categories was also extremely stimulated by M. Kontsevich's proposal for homological mirror symmetry ([Kon]) on the one side and by new applications to minimal model theory on the other side.
Let me now describe the aim and contents of this work. Roughly speaking, the problem is to give as concrete as possible a description of the (bounded) derived categories of coherent sheaves on rational homogeneous manifolds $X = G/P$, G a connected complex semisimple Lie group, $P \subset G$ a parabolic subgroup. More precisely, the following set of main questions and problems, ranging from the modest to the more ambitious, have served as programmatic guidelines:

P 1. Find generating sets of $D^b(Coh\, X)$ with as few elements as possible. (Here a set of elements of $D^b(Coh\, X)$ is called a *generating set* if the smallest full triangulated subcategory containing this set is equivalent to $D^b(Coh\, X)$).

We will see in subsection 2.3 below that the number of elements in a generating set is always bigger or equal to the number of Schubert varieties in X.
In the next two problems we mean by a complete exceptional sequence an ordered tuple $(E_1, \dots, E_n)$ of objects $E_1, \dots, E_n$ of $D^b(Coh\, X)$ which form a generating set and such that moreover $R^\bullet \mathrm{Hom}(E_i, E_j) = 0$ for all $i > j$, $R^\bullet \mathrm{Hom}(E_i, E_i) = \mathbb{C}$ (in degree 0) for all i. If in addition all extension groups in nonzero degrees between the elements E_i vanish we speak of a strong complete exceptional sequence. See section 2, def. 2.1.7, for further discussion.

P 2. Do there always exist complete exceptional sequences in $D^b(Coh\, X)$?

P 3. Do there always exist strong complete exceptional sequences in $D^b(Coh\, X)$?

Besides the examples found by Kapranov mentioned above, the only other substantially different examples I know of in answer to P 3. is the one given by A. V. Samokhin in [Sa] for the Lagrangian Grassmannian of totally isotropic 3-planes in a 6-dimensional symplectic vector space and, as an extension of this, some examples in [Kuz].
In the next problem we mean by a complete strong exceptional poset a set of objects $\{E_1, \dots, E_n\}$ of $D^b(Coh\, X)$ that generate $D^b(Coh\, X)$ and satisfy $R^\bullet \mathrm{Hom}(E_i, E_i) = \mathbb{C}$ (in degree 0) for all i and such that all extension groups in nonzero degrees between the E_i vanish, together with a partial order $\le$ on $\{E_1, \dots, E_n\}$ subject to the condition: $\mathrm{Hom}(E_j, E_i) = 0$ for $j \ge i$, $j \ne i$ (cf. def. 2.1.7 (B)).

P 4. Catanese's conjecture: On any $X = G/P$ there exists a complete strong exceptional poset $(\{E_1, \dots, E_n\}, \le)$ together with a bijection of the elements of the poset with the Schubert varieties in X such that $\le$ is the partial order induced by the Bruhat-Chevalley order (cf. conj. 2.2.1 (A)).

P 5. Dubrovin's conjecture (cf. [Du], conj. 4.2.2; slightly modified afterwards in [Bay]; cf. also [B-M]): The (small) quantum cohomology of a smooth projective variety Y is generically semi-simple if and only if there exists a complete exceptional sequence in $D^b(Coh\, Y)$ (Dubrovin also relates the Gram matrix of the exceptional sequence to quantum-cohomological data but we omit this part of the conjecture).

Roughly speaking, quantum cohomology endows the usual cohomology space with complex coefficients $H^*(Y)$ of Y with a new commutative associative multiplication $\circ_\omega : H^*(Y) \times H^*(Y) \to H^*(Y)$ depending on a complexified Kähler class $\omega \in H^2(Y, \mathbb{C})$, i.e. the imaginary part of ω is in the Kähler cone of Y (here we assume $H^{odd}(Y) = 0$ to avoid working with supercommutative rings). The condition that the quantum cohomology of Y is generically semi-simple means that for generic values of ω the resulting algebra is semi-simple. The validity of this conjecture would provide further evidence for the famous homological mirror conjecture by Kontsevich ([Kon]). However, we will not

deal with quantum cohomology in this work.
Before stating the results, a word of explanation is in order to clarify why we narrow down the focus to rational homogeneous manifolds:

- Exceptional vector bundles need not always exist on an arbitrary smooth projective variety; e.g., if the canonical class of Y is trivial, they never exist (see the explanation following definition 2.1.3).
- $D^b(Coh\, Y)$ need not be finitely generated, e.g., if Y is an Abelian variety (see the explanation following definition 2.1.3).
- If we assume that Y is Fano, then the Kodaira vanishing theorem tells us that all line bundles are exceptional, so we have at least some *a priori* supply of exceptional bundles.
- Within the class of Fano manifolds, the rational homogeneous spaces $X = G/P$ are distinguished by the fact that they are amenable to geometric, representation-theoretic and combinatorial methods alike.

Next we will state right away the main results obtained, keeping the numbering of the text and adding a word of explanation to each.
Let V be a $2n$-dimensional symplectic vector space and $\mathrm{IGrass}(k, V)$ the Grassmannian of k-dimensional isotropic subspaces of V with tautological subbundle $\mathcal{R}$. $\Sigma^\bullet$ denotes the Schur functor (see subsection 2.2 below for explanation).

Theorem 3.3.3. *The derived category $D^b(Coh(\mathrm{IGrass}(k, V)))$ is generated by the bundles $\Sigma^\nu \mathcal{R}$, where ν runs over Young diagrams Y which satisfy*

$$\begin{gathered}(\text{number of columns of } Y) \leq 2n-k\,,\\ k \geq (\text{number of rows of } Y) \geq (\text{number of columns of } Y) - 2(n-k)\,.\end{gathered}$$

This result pertains to P 1. Moreover, we will see in subsection 3.3 that P 2. for isotropic flag manifolds of type C_n can be reduced to P 2. for isotropic Grassmannians. Through examples 3.3.6-3.3.8 we show that theorem 3.3.3 gives a set of bundles which is in special cases manageable enough to obtain from it a complete exceptional sequence. In general, however, this last step is a difficult combinatorial puzzle relying on Bott's theorem for the cohomology of homogeneous bundles and Schur complexes derived from tautological exact sequences on the respective Grassmannians.
For the notion of semi-orthogonal decomposition in the next theorem we refer to definition 2.1.17 and for the definition of spinor bundles Σ, $\Sigma^{\pm}$ for the orthogonal vector bundle $\mathcal{O}_{\mathcal{Q}}(-1)^{\perp}/\mathcal{O}_{\mathcal{Q}}(-1)$ we refer to subsection 3.2.

Theorem 3.2.7. *Let X be a smooth projective variety, $\mathcal{E}$ an orthogonal vector bundle of rank $r+1$ on X (i.e., $\mathcal{E}$ comes equipped with a quadratic form $q \in \Gamma(X, \mathrm{Sym}^2\mathcal{E}^\vee)$ which is non-degenerate on each fibre), $\mathcal{Q} \subset \mathbb{P}(\mathcal{E})$ the associated* *quadric bundle, and let $\mathcal{E}$ admit spinor bundles (see subsection 3.2). Then there is a semiorthogonal decomposition*

$$D^b(\mathcal{Q}) = \langle D^b(X)\otimes\Sigma(-r+1), D^b(X)\otimes\mathcal{O}_{\mathcal{Q}}(-r+2), \\ \dots, D^b(X)\otimes\mathcal{O}_{\mathcal{Q}}(-1), D^b(X)\rangle$$

for $r+1$ odd and

$$D^b(\mathcal{Q}) = \langle D^b(X)\otimes\Sigma^+(-r+1), D^b(X)\otimes\Sigma^-(-r+1), \\ D^b(X)\otimes\mathcal{O}_{\mathcal{Q}}(-r+2), \dots, D^b(X)\otimes\mathcal{O}_{\mathcal{Q}}(-1), D^b(X)\rangle$$

for $r+1$ even.

This theorem is an extension to the relative case of a theorem of [Ka2]. It enlarges substantially the class of varieties (especially rational-homogeneous varieties) on which complete exceptional sequences are proven to exist (P 2). It will also be the substantial ingredient in subsection 3.4: Let V be a 7-dimensional orthogonal vector space, $\mathrm{IGrass}(3,V)$ the Grassmannian of isotropic 3-planes in V, $\mathcal{R}$ the tautological subbundle on it; L denotes the ample generator of $\mathrm{Pic}(\mathrm{IGrass}(3,V))\simeq\mathbb{Z}$ (a square root of $\mathcal{O}(1)$ in the Plücker embedding). For more information cf. subsection 3.4.

Theorem 3.4.1. *The derived category $D^b(Coh\,\mathrm{IGrass}(3,V))$ is generated as triangulated category by the following 22 vector bundles:*

$$\bigwedge^2\mathcal{R}(-1),\ \mathcal{O}(-2),\ \mathcal{R}(-2)\otimes L,\ \mathrm{Sym}^2\mathcal{R}(-1)\otimes L,\ \mathcal{O}(-3)\otimes L, \\ \bigwedge^2\mathcal{R}(-2)\otimes L,\ \Sigma^{2,1}\mathcal{R}(-1)\otimes L,\ \mathcal{R}(-1),\ \mathcal{O}(-2)\otimes L,\ \mathcal{O}(-1), \\ \mathcal{R}(-1)\otimes L,\ \bigwedge^2\mathcal{R}(-1)\otimes L,\ \Sigma^{2,1}\mathcal{R}\otimes L,\ \mathrm{Sym}^2\mathcal{R}^\vee(-2)\otimes L,\ \bigwedge^2\mathcal{R},\ \mathcal{O}, \\ \Sigma^{2,1}\mathcal{R},\ \mathrm{Sym}^2\mathcal{R}^\vee(-2),\ \mathcal{O}(-1)\otimes L,\ \mathrm{Sym}^2\mathcal{R}^\vee(-1),\ \bigwedge^2\mathcal{R}\otimes L,\ \mathcal{R}\otimes L.$$

This result pertains to P 1. again. It is worth mentioning that the expected number of elements in a complete exceptional sequence for $D^b(Coh\,\mathrm{IGrass}(3,V))$ is 8, the number of Schubert varieties in $\mathrm{IGrass}(3,V)$. In addition, one should remark that P 2. for isotropic flag manifold of type B_n or D_n can again be reduced to isotropic Grassmannians. Moreover, the method of subsection 3.4 applies to all orthogonal isotropic Grassmannians alike, but since the computations tend to become very large, we restrict our attention to a particular case.

Beilinson proved his theorem on $\mathbb{P}^n$ using a resolution of the structure sheaf of the diagonal and considering the functor $Rp_{2*}(p_1^*(-)\otimes^L\mathcal{O}_\Delta)\simeq\mathrm{id}_{D^b(Coh\,\mathbb{P}^n)}$ (here $p_1,p_2:\mathbb{P}^n\times\mathbb{P}^n\to\mathbb{P}^n$ are the projections onto the two factors). The situation is complicated on general rational homogeneous manifolds X because resolutions of the structure sheaf of the diagonal $\Delta\subset X\times X$ analogous to those used in [Bei], [Ka1], [Ka2], [Ka3] to exhibit complete exceptional sequences, are not known. The preceding theorems are proved by "fibrational techniques". Section 4 outlines an alternative approach: In fact, M. Brion ([Bri]) constructed, for any rational homogeneous manifold X, a degeneration of the diagonal Δ_X into $\mathfrak{X}_0$, which is a union, over the Schubert varieties in X, of the products of a Schubert variety with its opposite Schubert variety (cf. thm. 4.1.1). It turns out that it is important to describe the functors $Rp_{2*}(p_1^*(-)\otimes^L \mathcal{O}_{\mathfrak{X}_0})$ which, contrary to what one might expect at first glance, are no longer isomorphic to the identity functor by Orlov's representability theorem [Or2], thm. 3.2.1 (but one might hope to reconstruct the identity out of $Rp_{2*}(p_1^*(-)\otimes^L \mathcal{O}_{\mathfrak{X}_0})$ and some infinitesimal data attached to the degeneration). For $\mathbb{P}^n$ this is accomplished by the following

Theorem 4.2.5. *Let $\{pt\} = L_0 \subset L_1 \subset \cdots \subset L_n = \mathbb{P}^n$ be a full flag of projective linear subspaces of $\mathbb{P}^n$ (the Schubert varieties in $\mathbb{P}^n$) and let $L^0 = \mathbb{P}^n \supset L^1 \supset \cdots \supset L^n = \{pt\}$ be a complete flag in general position with respect to the L_j.*
For $d \geq 0$ one has in $D^b(Coh\,\mathbb{P}^n)$

$$Rp_{2*}(p_1^*(\mathcal{O}(d))\otimes^L \mathcal{O}_{\mathfrak{X}_0}) \simeq \bigoplus_{j=0}^{n} \mathcal{O}_{L_j}\otimes H^0(L^j,\mathcal{O}(d))^\vee / H^0(L^{j+1},\mathcal{O}(d))^\vee \,.$$

Moreover, one can also describe completely the effect of $Rp_{2*}(p_1^*(-)\otimes^L \mathcal{O}_{\mathfrak{X}_0})$ on morphisms (cf. subsection 4.2 below).

The proof uses the technique of cellular resolutions of monomial ideals of Bayer and Sturmfels ([B-S]). We also show in subsection 4.2 that Beilinson's theorem on $\mathbb{P}^n$ can be recovered by our method with a proof that uses only $\mathfrak{X}_0$ (see remark 4.2.6).
It should be added that we will not completely ignore the second part of P 4. concerning Hom-spaces: In section 2 we show that the conjecture in P 4. is valid in full for the complete strong exceptional sequences found by Kapranov on Grassmannians and quadrics (cf. [Ka3]). In remark 2.3.8 we discuss a possibility for relating the Gram matrix of a strong complete exceptional sequence on a rational homogeneous manifold with the Bruhat-Chevalley order on Schubert cells.
Additional information about the content of each section can be found at the beginning of the respective section.
Acknowledgements. I would like to thank my thesis advisor Fabrizio Catanese for posing the problem and several discussions on it. Special thanks also to Michel Brion for filling in my insufficient knowledge of representation theory and algebraic groups on a number of occasions and for fruitful suggestions and discussions.

2 Tools and background: getting off the ground

This section supplies the concepts and dictionary that will be used throughout the text. We state a conjecture due to F. Catanese which was the motivational backbone of this work and discuss its relation to work of M. M. Kapranov. Moreover, we prove some results that are useful in the study of the derived categories of coherent sheaves on rational homogeneous varieties, but do not yet tackle the problem of constructing complete exceptional sequences on them: This will be the subject matter of sections 3 and 4.

2.1 Exceptional sequences

Throughout the text we will work over the ground field $\mathbb{C}$ of complex numbers. The classical theorem of Beilinson (cf. [Bei]) can be stated as follows.

Theorem 2.1.1. *Consider the following two ordered sequences of sheaves on* $\mathbb{P}^n = \mathbb{P}(V)$, V *an* $n+1$ *dimensional vector space:*

$$\mathfrak{B} = (\mathcal{O}(-n), \dots, \mathcal{O}(-1), \mathcal{O})$$
$$\mathfrak{B}' = \left(\Omega^n(n), \dots, \Omega^1(1), \mathcal{O}\right).$$

Then $D^b(Coh\mathbb{P}^n)$ *is equivalent as a triangulated category to the homotopy category of bounded complexes of sheaves on* $\mathbb{P}^n$ *whose terms are finite direct sums of sheaves in* $\mathfrak{B}$ *(and the same for* $\mathfrak{B}$ *replaced with* $\mathfrak{B}'$*).*
Moreover, one has the following stronger assertion: If $\Lambda = \bigoplus_{i=0}^{n+1} \wedge^i V$ *and* $S = \bigoplus_{i=0}^{\infty} \mathrm{Sym}^i V^*$ *are the* $\mathbb{Z}$*-graded exterior algebra of* V*, resp. symmetric algebra of* V^**, and* $K^b_{[0,n]}\Lambda$ *resp.* $K^b_{[0,n]}S$ *are the homotopy categories of bounded complexes whose terms are finite direct sums of free modules* $\Lambda[i]$*, resp.* $S[i]$*, for* $0 \le i \le n$*, and whose morphisms are homogeneous graded of degree* 0*, then*

$$K^b_{[0,n]}\Lambda \simeq D^b(Coh\mathbb{P}^n) \quad K^b_{[0,n]}S \simeq D^b(Coh\mathbb{P}^n)$$

as triangulated categories, the equivalences being given by sending $\Lambda[i]$ *to* $\Omega^i(i)$ *and* $S[i]$ *to* $\mathcal{O}(-i)$ *(*$\Lambda[i]$*,* $S[i]$ *have their generator in degree* i*).*

One would like to have an analogous result on any rational homogeneous variety X, i.e. a rational projective variety with a transitive Lie group action or equivalently (cf. [Akh], 3.2, thm. 2) a coset manifold G/P where G is a connected semisimple complex Lie group (which can be assumed to be simply connected) and $P \subset G$ is a parabolic subgroup. However, to give a precise meaning to this wish, one should first try to capture some formal features of Beilinson's theorem in the form of suitable definitions; thus we will recall next a couple of notions which have become standard by now, taking theorem 2.1.1 as a model.
Let $\mathcal{A}$ be an Abelian category.

Definition 2.1.2. A class of objects $\mathcal{C}$ *generates* $D^b(\mathcal{A})$ if the smallest full triangulated subcategory containing the objects of $\mathcal{C}$ is equivalent to $D^b(\mathcal{A})$. If $\mathcal{C}$ is a set, we will also call $\mathcal{C}$ a *generating set* in the sequel.

Unravelling this definition, one finds that this is equivalent to saying that, up to isomorphism, every object in $D^b(\mathcal{A})$ can be obtained by successively enlarging $\mathcal{C}$ through the following operations: Taking finite direct sums, shifting in $D^b(\mathcal{A})$ (i.e., applying the translation functor), and taking a cone Z of a morphism $u : X \to Y$ between objects already constructed: This means we complete u to a distinguished triangle $X \xrightarrow{u} Y \longrightarrow Z \longrightarrow X[1]$.
The sheaves $\Omega^i(i)$ and $\mathcal{O}(-i)$ in theorem 2.1.1 have the distinctive property of being "exceptional".

Definition 2.1.3. An object E in $D^b(\mathcal{A})$ is said to be *exceptional* if

$$\mathrm{Hom}(E,E) \simeq \mathbb{C} \quad \text{and} \quad \mathrm{Ext}^i(E,E) = 0 \; \forall i \neq 0.$$

If Y is a smooth projective variety of dimension n, exceptional objects need not always exist (e.g., if Y has trivial canonical class this is simply precluded by Serre duality since then $\mathrm{Hom}(E,E) \simeq \mathrm{Ext}^n(E,E) \neq 0$).
What is worse, $D^b(Coh\, Y)$ need not even possess a finite generating set: In fact we will see in subsection 2.3 below that if $D^b(Coh\, Y)$ is finitely generated, then $A(Y) \otimes \mathbb{Q} = \bigoplus_{r=0}^{\dim Y} A^r(Y) \otimes \mathbb{Q}$, the rational Chow ring of Y, is finite dimensional (here $A^r(Y)$ denotes the group of cycles of codimension r on Y modulo rational equivalence). But, for instance, if Y is an Abelian variety, $A^1(Y) \otimes \mathbb{Q} \simeq \mathrm{Pic}\, Y \otimes \mathbb{Q}$ does not have finite dimension.
Recall that a vector bundle $\mathcal{V}$ on a rational homogeneous variety $X = G/P$ is called *G-homogeneous* if there is a G-action on $\mathcal{V}$ which lifts the G-action on X and is linear on the fibres. It is well known that this is equivalent to saying that $\mathcal{V} \simeq G \times_\varrho V$, where $\varrho : P \to \mathrm{GL}(V)$ is some representation of the algebraic group P and $G \times_\varrho V$ is the quotient of $G \times V$ by the action of P given by $p \cdot (g,v) := (gp^{-1}, \varrho(p)v)$, $p \in P$, $g \in G$, $v \in V$. The projection to G/P is induced by the projection of $G \times V$ to G; this construction gives a 1-1 correspondence between representations of the subgroup P and homogeneous vector bundles over G/P (cf. [Akh], section 4.2).
Then we have the following result (mentioned briefly in a number of places, e.g. [Ru1], 6., but without a precise statement or proof).

Proposition 2.1.4. *Let $X = G/P$ be a rational homogeneous manifold with G a simply connected semisimple group, and let $\mathcal{F}$ be an exceptional sheaf on X. Then $\mathcal{F}$ is a G-homogeneous bundle.*

Proof. Let us first agree that a deformation of a coherent sheaf $\mathcal{G}$ on a complex space Y is a triple $(\tilde{\mathcal{G}}, S, s_0)$ where S is another complex space (or germ), $s_0 \in S$, $\tilde{\mathcal{G}}$ is a coherent sheaf on $Y \times S$, flat over S, with $\tilde{\mathcal{G}}\,|_{Y\times\{s_0\}} \simeq \mathcal{G}$ and $\mathrm{Supp}\, \tilde{\mathcal{G}} \to S$ proper. Then one knows that, for the deformation with base a complex space germ, there is a versal deformation and its tangent space at the marked point

is $\mathrm{Ext}^1(\mathcal{G},\mathcal{G})$ (cf. [S-T]).
Let $\sigma : G\times X \to X$ be the group action; then $(\sigma^*\mathcal{F}, G, \mathrm{id}_G)$ is a deformation of $\mathcal{F}$ (flatness can be seen e.g. by embedding X equivariantly in a projective space (cf. [Akh], 3.2) and noting that the Hilbert polynomial of $\sigma^*\mathcal{F}\mid_{\{g\}\times X}= \tau_g^*\mathcal{F}$ is then constant for $g\in G$; here $\tau_g : X\to X$ is the automorphism induced by g). Since $\mathrm{Ext}^1(\mathcal{F},\mathcal{F})=0$ one has by the above that $\sigma^*\mathcal{F}$ will be locally trivial over G, i.e. $\sigma^*\mathcal{F}\simeq \mathrm{pr}_2^*\mathcal{F}$ locally over G where $\mathrm{pr}_2 : G\times X\to X$ is the second projection ($\mathcal{F}$ is "rigid"). In particular $\tau_g^*\mathcal{F}\simeq\mathcal{F}\ \forall g\in G$.
Since the locus of points where $\mathcal{F}$ is not locally free is a proper algebraic subset of X and invariant under G by the preceding statement, it is empty because G acts transitively. Thus $\mathcal{F}$ is a vector bundle satisfying $\tau_g^*\mathcal{F}\simeq\mathcal{F}\ \forall g\in G$. Since G is semisimple and assumed to be simply connected, this is enough to imply that $\mathcal{F}$ is a G-homogeneous bundle (a proof of this last assertion due to A. Huckleberry is presented in [Ot2] thm. 9.9). □

Remark 2.1.5. In proposition 2.1.4 one must insist that G be simply connected as an example in [GIT], ch.1, §3 shows : The exceptional bundle $\mathcal{O}_{\mathbb{P}^n}(1)$ on $\mathbb{P}^n$ is SL_{n+1}-homogeneous, but not homogeneous for the adjoint form PGL_{n+1} with its action $\sigma : PGL_{n+1}\times\mathbb{P}^n\to\mathbb{P}^n$ since the SL_{n+1}-action on $H^0(\mathcal{O}_{\mathbb{P}^n}(1))$ does not factor through PGL_{n+1}.

Remark 2.1.6. It would be interesting to know which rational homogeneous manifolds X enjoy the property that exceptional objects in $D^b(Coh\,X)$ are actually just shifts of exceptional sheaves. It is straightforward to check that this is true on $\mathbb{P}^1$. This is because, if C is a curve, $D^b(Coh\,C)$ is not very interesting: In fancy language, the underlying abelian category is *hereditary* which means $\mathrm{Ext}^2(\mathcal{F},\mathcal{G})=0\ \forall\mathcal{F},\mathcal{G}\in\mathrm{obj}\,(Coh\,C)$. It is easy to see (cf. [Ke], 2.5) that then every object Z in $D^b(Coh\,C)$ is isomorphic to the direct sum of shifts of its cohomology sheaves $\bigoplus_{i\in\mathbb{Z}} H^i(Z)[-i]$ whence morphisms between objects Z_1 and Z_2 correspond to tuples $(\varphi_i, e_i)_{i\in\mathbb{Z}}$ with $\varphi_i : H^i(Z_1)\to H^i(Z_2)$ a sheaf morphism and $e_i\in\mathrm{Ext}^1(H^i(Z_1), H^{i-1}(Z_2))$ an extension class . Exceptional objects are indecomposable since they are simple.
The same property holds on $\mathbb{P}^2$ (and more generally on any Del Pezzo surface) by [Gor], thm. 4.3.3, and is conjectured to be true on $\mathbb{P}^n$ in general ([Gor], 3.2.7).

The sequences $\mathfrak{B}$ and $\mathfrak{B}'$ in theorem 2.1.1 are examples of complete strong exceptional sequences (cf. [Ru1] for the development of this notion).

Definition 2.1.7. (A) An n-tuple $(E_1,\dots,E_n)$ of exceptional objects in $D^b(\mathcal{A})$ is called an *exceptional sequence* if

$$\mathrm{Ext}^l(E_j,E_i)=0\quad \forall 1\le i<j\le n\ \text{ and }\ \forall l\in\mathbb{Z}\,.$$

If in addition

$$\mathrm{Ext}^l(E_j,E_i)=0\quad \forall 1\le i,j\le n\ \text{ and }\ \forall l\neq 0$$

we call $(E_1, \dots, E_n)$ a *strong exceptional sequence.* The sequence is *complete* if $E_1, \dots, E_n$ generate $D^b(\mathcal{A})$.

(B) In order to phrase conjecture 2.2.1 below precisely, it will be convenient to introduce also the following terminology: A set of exceptional objects $\{E_1, \dots, E_n\}$ in $D^b(\mathcal{A})$ that generates $D^b(\mathcal{A})$ and such that $\mathrm{Ext}^l(E_j, E_i) = 0$ for all $1 \le i, j \le n$ and all $l \neq 0$ will be called a *complete strong exceptional set.* A partial order $\le$ on a complete strong exceptional set is *admissible* if $\mathrm{Hom}(E_j, E_i) = 0$ for all $j \ge i, i \neq j$. A pair $(\{E_1, \dots, E_n\}, \le)$ consisting of a complete strong exceptional set and an admissible partial order on it will be called a *complete strong exceptional poset.*

(C) A *complete very strong exceptional poset* is a pair $(\{E_1, \dots, E_n\}, \le)$ where $\{E_1, \dots, E_n\}$ is a complete strong exceptional set and $\le$ is a partial order on this set such that $\mathrm{Hom}(E_j, E_i) = 0$ unless $i \ge j$.

Obviously every complete strong exceptional sequence is a complete strong exceptional poset (with the partial order being in fact a total order). I think it might be possible that for complete strong exceptional posets in $D^b(Coh\, X)$ which consist of vector bundles, X a rational homogeneous manifold, the converse holds, i.e. any admissible partial order can be refined to a total order which makes the poset into a complete strong exceptional sequence. But I cannot prove this.

Moreover, every complete very strong exceptional poset is in particular a complete strong exceptional poset. If we choose a total order refining the partial order on a complete very strong exceptional poset, we obtain a complete strong exceptional sequence.

Let me explain the usefulness of these concepts by first saying what kind of analogues of Beilinson's theorem 2.1.1 we can expect for $D^b(\mathcal{A})$ once we know the existence of a complete strong exceptional set.

Look at a complete strong exceptional set $\{E_1, \dots, E_n\}$ in $D^b(\mathcal{A})$ consisting of objects E_i, $1 \le i \le n$, of $\mathcal{A}$. If $K^b(\{E_1, \dots, E_n\})$ denotes the homotopy category of bounded complexes in $\mathcal{A}$ whose terms are finite direct sums of the E_i's, it is clear that the natural functor

$$\Phi_{(E_1,\dots,E_n)} : K^b(\{E_1, \dots, E_n\}) \to D^b(\mathcal{A})$$

(composition of the inclusion $K^b(\{E_1, \dots, E_n\}) \hookrightarrow K^b(\mathcal{A})$ with the localization $Q : K^b(\mathcal{A}) \to D^b(\mathcal{A})$) is an equivalence; indeed $\Phi_{(E_1,\dots,E_n)}$ is essentially surjective because $\{E_1, \dots, E_n\}$ is complete and $\Phi_{(E_1,\dots,E_n)}$ is fully faithful because $\mathrm{Ext}^p(E_i, E_j) = 0$ for all $p > 0$ and all i and j implies

$$\mathrm{Hom}_{K^b(\{E_1,\dots,E_n\})}(A, B) \simeq \mathrm{Hom}_{D^b(\mathcal{A})}(\Phi_{(E_1,\dots,E_n)}\, A, \Phi_{(E_1,\dots,E_n)}\, B)$$
$$\forall A,\, B \in \mathrm{obj}\, K^b(\{E_1, \dots, E_n\})$$

(cf. [AO], prop. 2.5).
Returning to derived categories of coherent sheaves and dropping the hypothesis that the E_i's be objects of the underlying Abelian category, we have the following stronger theorem of A. I. Bondal:

Theorem 2.1.8. *Let X be a smooth projective variety and $(E_1,\dots,E_n)$ a strong complete exceptional sequence in $D^b(Coh\,X)$. Set $E := \bigoplus_{i=1}^n E_i$, let $A := \mathrm{End}(E) = \bigoplus_{i,j}\mathrm{Hom}(E_i,E_j)$ be the algebra of endomorphisms of E, and denote $\mathrm{mod}-A$ the category of right modules over A which are finite dimensional over $\mathbb{C}$.*
Then the functor

$$R\mathrm{Hom}^\bullet(E,-) : D^b(Coh\,(X)) \to D^b(\mathrm{mod}-A)$$

is an equivalence of categories (note that, for any object Y of $D^b(Coh\,(X))$, $R\mathrm{Hom}^\bullet(E,Y)$ has a natural action from the right by $A=\mathrm{Hom}(E,E)$).
Moreover, the indecomposable projective modules over A are (up to isomorphism) exactly the $P_i := \mathrm{id}_{E_i}\cdot A$, $i=1,\dots,n$. We have $\mathrm{Hom}_{D^b(Coh\,(X))}(E_i,E_j) \simeq \mathrm{Hom}_A(P_i,P_j)$ and an equivalence

$$K^b(\{P_1,\dots,P_n\}) \xrightarrow{\sim} D^b(\mathrm{mod}-A)$$

where $K^b(\{P_1,\dots,P_n\})$ is the homotopy category of complexes of right A-modules whose terms are finite direct sums of the P_i's.

For a proof see [Bo], §§5 and 6. Thus whenever we have a strong complete exceptional sequence in $D^b(Coh\,(X))$ we get an equivalence of the latter with a homotopy category of projective modules over the algebra of endomorphisms of the sequence. For the sequences $\mathfrak{B}$, $\mathfrak{B}'$ in theorem 2.1.1 we recover Beilinson's theorem (although the objects of the module categories $K^b(\{P_1,\dots,P_n\})$ that theorem 2.1.8 produces in each of these cases will be different from the objects in the module categories $K^b_{[0,n]}S$, resp. $K^b_{[0,n]}\Lambda$, in theorem 2.1.1, the morphisms correspond and the respective module categories are equivalent).
Next suppose that $D^b(Coh\,X)$ on a smooth projective variety X is generated by an exceptional sequence $(E_1,\dots,E_n)$ that is not necessarily strong. Since extension groups in nonzero degrees between members of the sequence need not vanish in this case, one cannot expect a description of $D^b(Coh\,X)$ on a homotopy category level as in theorem 2.1.8. But still the existence of $(E_1,\dots,E_n)$ makes available some very useful computational tools, e.g. Beilinson type spectral sequences. To state the result, we must briefly review some basic material on an operation on exceptional sequences called *mutation*. Mutations are also needed in subsection 2.2 below. Moreover, the very concept of exceptional sequence as a weakening of the concept of strong exceptional sequence was first introduced because strong exceptionality is in general not preserved by mutations, cf. [Bo], introduction p.24 (exceptional sequences are also more flexible in other situations, cf. remark 3.1.3 below).

For $A, B \in \operatorname{obj} D^b(Coh\, X)$ set $\operatorname{Hom}^\times(A,B) := \bigoplus_{k\in\mathbb{Z}} \operatorname{Ext}^k(A,B)$, a graded $\mathbb{C}$-vector space. For a graded $\mathbb{C}$-vector space V, $(V^\vee)^i := \operatorname{Hom}_{\mathbb{C}}(V^{-i},\mathbb{C})$ defines the grading of the dual, and if $X \in \operatorname{obj} D^b(Coh\, X)$, then $V \otimes X$ means $\bigoplus_{i\in\mathbb{Z}} V^i \otimes X[-i]$ where $V^i \otimes X[-i]$ is the direct sum of $\dim V^i$ copies of $X[-i]$.

Definition 2.1.9. Let (E_1, E_2) be an exceptional sequence in $D^b(Coh\, X)$. The *left mutation* $L_{E_1}E_2$ (resp. the *right mutation* $R_{E_2}E_1$) is the object defined by the distinguished triangles

$$L_{E_1}E_2 \longrightarrow \operatorname{Hom}^\times(E_1,E_2)\otimes E_1 \xrightarrow{\text{can}} E_2 \longrightarrow L_{E_1}E_2[1]$$
$$(\text{resp.}\quad R_{E_2}E_1[-1] \longrightarrow E_1 \xrightarrow{\text{can}'} \operatorname{Hom}^\times(E_1,E_2)^\vee\otimes E_2 \longrightarrow R_{E_2}E_1 \quad).$$

Here can resp. can′ are the canonical morphisms ("evaluations").

Theorem 2.1.10. *Let $\mathfrak{E} = (E_1, \dots, E_n)$ be an exceptional sequence in $D^b(Coh\, X)$. Set, for $i = 1, \dots, n-1$,*

$$R_i\mathfrak{E} := \left(E_1, \dots, E_{i-1}, E_{i+1}, R_{E_{i+1}}E_i, E_{i+2}, \dots, E_n\right),$$
$$L_i\mathfrak{E} := (E_1, \dots, E_{i-1}, L_{E_i}E_{i+1}, E_i, E_{i+2}, \dots, E_n).$$

Then $R_i\mathfrak{E}$ and $L_i\mathfrak{E}$ are again exceptional sequences. R_i and L_i are inverse to each other; the R_i's (or L_i's) induce an action of Bd_n, the Artin braid group on n strings, on the class of exceptional sequences with n terms in $D^b(Coh\, X)$. If moreover $\mathfrak{E}$ is complete, so are all the $R_i\mathfrak{E}$'s and $L_i\mathfrak{E}$'s.

For a proof see [Bo], §2.
We shall see in example 2.1.13 that the two exceptional sequences $\mathfrak{B}$, $\mathfrak{B}'$ of theorem 2.1.1 are closely related through a notion that we will introduce next:

Definition 2.1.11. Let $(E_1, \dots, E_n)$ be a complete exceptional sequence in $D^b(Coh\, X)$. For $i = 1, \dots, n$ define

$$E_i^\vee := L_{E_1}L_{E_2}\dots L_{E_{n-i}}E_{n-i+1},$$
$${}^\vee E_i := R_{E_n}R_{E_{n-1}}\dots R_{E_{n-i+2}}E_{n-i+1}.$$

The complete exceptional sequences $(E_1^\vee, \dots, E_n^\vee)$ resp. $({}^\vee E_1, \dots, {}^\vee E_n)$ are called the *right* resp. *left dual* of $(E_1, \dots, E_n)$.

The name is justified by the following

Proposition 2.1.12. *Under the hypotheses of definition 2.1.11 one has*

$$\operatorname{Ext}^k({}^\vee E_i, E_j) = \operatorname{Ext}^k(E_i, E_j^\vee) = \begin{cases} \mathbb{C} & \text{if } i+j = n+1,\ i = k+1 \\ 0 & \text{otherwise} \end{cases}$$

Moreover the right (resp. left) dual of $(E_1, \dots, E_n)$ is uniquely (up to unique isomorphism) defined by these equations.

The proof can be found in [Gor], subsection 2.6.

Example 2.1.13. Consider on $\mathbb{P}^n = \mathbb{P}(V)$, the projective space of lines in the vector space V, the complete exceptional sequence $\mathfrak{B}' = (\Omega^n(n), \dots, \Omega^1(1), \mathcal{O})$ and for $1 \le p \le n$ the truncation of the p-th exterior power of the Euler sequence

$$0 \longrightarrow \Omega^p_{\mathbb{P}^n} \longrightarrow \left(\bigwedge^p V^\vee\right) \otimes \mathcal{O}_{\mathbb{P}^n}(-p) \longrightarrow \Omega^{p-1}_{\mathbb{P}^n} \longrightarrow 0\,.$$

Let us replace $\mathfrak{B}'$ by $\big(\Omega^n(n), \dots, \Omega^2(2), \mathcal{O}, R_{\mathcal{O}}\Omega^1(1)\big)$, i.e., mutate $\Omega^1(1)$ to the right across $\mathcal{O}$. But in the exact sequence

$$0 \longrightarrow \Omega^1(1) \longrightarrow V^\vee \otimes \mathcal{O} \longrightarrow \mathcal{O}(1) \longrightarrow 0$$

the arrow $\Omega^1(1) \to V^\vee \otimes \mathcal{O}$ is nothing but the canonical morphism $\Omega^1(1) \to \mathrm{Hom}(\Omega^1(1), \mathcal{O})^\vee \otimes \mathcal{O}$ from definition 2.1.9. Therefore $R_{\mathcal{O}}\Omega^1(1) \simeq \mathcal{O}(1)$.
Now in the mutated sequence $(\Omega^n(n), \dots, \Omega^2(2), \mathcal{O}, \mathcal{O}(1))$ we want to mutate in the next step $\Omega^2(2)$ across $\mathcal{O}$ and $\mathcal{O}(1)$ to the right. In the sequence

$$0 \longrightarrow \Omega^2(2) \longrightarrow \bigwedge^2 V^\vee \otimes \mathcal{O} \longrightarrow \Omega^1(2) \longrightarrow 0$$

the arrow $\Omega^2(2) \to \bigwedge^2 V^\vee \otimes \mathcal{O}$ is again the canonical morphism $\Omega^2(2) \to \mathrm{Hom}(\Omega^2(2), \mathcal{O})^\vee \otimes \mathcal{O}$ and $R_{\mathcal{O}}\Omega^2(2) \simeq \Omega^1(2)$ and then

$$0 \longrightarrow \Omega^1(2) \longrightarrow V^\vee \otimes \mathcal{O}(1) \longrightarrow \mathcal{O}(2) \longrightarrow 0$$

gives $R_{\mathcal{O}(1)}R_{\mathcal{O}}\Omega^2(2) \simeq \mathcal{O}(2)$.
Continuing this pattern, one transforms our original sequence $\mathfrak{B}'$ by successive right mutations into $(\mathcal{O}, \mathcal{O}(1), \mathcal{O}(2), \dots, \mathcal{O}(n))$ which, looking back at definition 2.1.11 and using the braid relations $R_iR_{i+1}R_i = R_{i+1}R_iR_{i+1}$, one identifies as the left dual of $\mathfrak{B}'$.

Here is Gorodentsev's theorem on generalized Beilinson spectral sequences.

Theorem 2.1.14. *Let X be a smooth projective variety and let $D^b(Coh\,X)$ be generated by an exceptional sequence $(E_1, \dots, E_n)$. Let $F : D^b(Coh\,X) \to \mathcal{A}$ be a covariant cohomological functor to some Abelian category $\mathcal{A}$.
For any object A in $D^b(Coh\,X)$ there is a spectral sequence*

$$E_1^{p,q} = \bigoplus_{i+j=q} \mathrm{Ext}^{n+i-1}({}^\vee E_{n-p}, A) \otimes F^j(E_{p+1})$$
$$= \bigoplus_{i+j=q} \mathrm{Ext}^{-i}(A, E_{n-p}^\vee)^\vee \otimes F^j(E_{p+1}) \implies F^{p+q}(A)$$

(with possibly nonzero entries for $0 \le p, q \le n-1$ only).

For the proof see [Gor], 2.6.4 (actually one can obtain A as a convolution of a complex over $D^b(Coh\, X)$ whose terms are computable once one knows the $\mathrm{Ext}^i({}^\vee E_j, A)$, but we don't need this).
In particular, taking in theorem 2.1.14 the dual exceptional sequences in example 2.1.13 and for F the functor that takes an object in $D^b(Coh\, \mathbb{P}^n)$ to its zeroth cohomology sheaf, we recover the classical Beilinson spectral sequence.
It is occasionally useful to split a derived category into more manageable building blocks before starting to look for complete exceptional sequences. This is the motivation for giving the following definitions.

Definition 2.1.15. Let $\mathcal{S}$ be a full triangulated subcategory of a triangulated category $\mathcal{T}$. The *right orthogonal* to $\mathcal{S}$ in $\mathcal{T}$ is the full triangulated subcategory $\mathcal{S}^\perp$ of $\mathcal{T}$ consisting of objects T such that $\mathrm{Hom}(S,T)=0$ for all objects S of $\mathcal{S}$. The *left orthogonal* ${}^\perp\mathcal{S}$ is defined similarly.

Definition 2.1.16. A full triangulated subcategory $\mathcal{S}$ of $\mathcal{T}$ is *right-* (resp. *left-*) *admissible* if for every $T \in \mathrm{obj}\, \mathcal{T}$ there is a distinguished triangle

$$S \longrightarrow T \longrightarrow S' \longrightarrow S[1] \quad \text{with} \quad S \in \mathrm{obj}\, \mathcal{S}\,,\ S' \in \mathrm{obj}\, \mathcal{S}^\perp$$
$$(\text{resp.} \quad S'' \longrightarrow T \longrightarrow S \longrightarrow S''[1] \quad \text{with} \quad S \in \mathrm{obj}\, \mathcal{S}\,,\ S'' \in \mathrm{obj}\, {}^\perp\mathcal{S}\,)$$

and *admissible* if it is both right- and left-admissible.

Other useful characterizations of admissibility can be found in [Bo], lemma 3.1 or [BoKa], prop. 1.5.

Definition 2.1.17. An n-tuple of admissible subcategories $(\mathcal{S}_1, \dots, \mathcal{S}_n)$ of a triangulated category $\mathcal{T}$ is *semi-orthogonal* if $\mathcal{S}_j$ belongs to $\mathcal{S}_i^\perp$ whenever $1 \le j < i \le n$. If $\mathcal{S}_1, \dots, \mathcal{S}_n$ generate $\mathcal{T}$ one calls this a *semi-orthogonal decomposition of* $\mathcal{T}$ and writes

$$\mathcal{T} = \langle \mathcal{S}_1, \dots, \mathcal{S}_n \rangle \ .$$

To conclude, we give a result that describes the derived category of coherent sheaves on a product of varieties.

Proposition 2.1.18. *Let X and Y be smooth, projective varieties and*

$$(\mathcal{V}_1, \dots, \mathcal{V}_m)$$

resp.

$$(\mathcal{W}_1, \dots, \mathcal{W}_n)$$

be (strong) complete exceptional sequences in $D^b(Coh(X))$ resp. $D^b(Coh(Y))$ where $\mathcal{V}_i$ and $\mathcal{W}_j$ are vector bundles on X resp. Y. Let π_1 resp. π_2 be the projections of $X \times Y$ on the first resp. second factor and put $\mathcal{V}_i \boxtimes \mathcal{W}_j := \pi_1^*\mathcal{V}_i \otimes \pi_2^*\mathcal{W}_j$. Let $\prec$ be the lexicographic order on $\{1, \dots, m\} \times \{1, \dots, n\}$. Then

$$(\mathcal{V}_i \boxtimes \mathcal{W}_j)_{(i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}}$$

is a (strong) complete exceptional sequence in $D^b(Coh(X \times Y))$ where $\mathcal{V}_{i_1} \boxtimes \mathcal{W}_{j_1}$ precedes $\mathcal{V}_{i_2} \boxtimes \mathcal{W}_{j_2}$ iff $(i_1, j_1) \prec (i_2, j_2)$.

Proof. The proof is a little less straightforward than it might be expected at first glance since one does not know explicit resolutions of the structure sheaves of the diagonals on $X \times X$ and $Y \times Y$.
First, by the Künneth formula,

$$\begin{aligned}\mathrm{Ext}^k(\mathcal{V}_{i_2} \boxtimes \mathcal{W}_{j_2}, \mathcal{V}_{i_1} \boxtimes \mathcal{W}_{j_1}) &\simeq H^k(X \times Y, (\mathcal{V}_{i_1} \otimes \mathcal{V}_{i_2}^\vee) \boxtimes (\mathcal{W}_{j_1} \otimes \mathcal{W}_{j_2}^\vee)) \\ &\simeq \bigoplus_{k_1+k_2=k} H^{k_1}(X, \mathcal{V}_{i_1} \otimes \mathcal{V}_{i_2}^\vee) \otimes H^{k_2}(Y, \mathcal{W}_{j_1} \otimes \mathcal{W}_{j_2}^\vee) \\ &\simeq \bigoplus_{k_1+k_2=k} \mathrm{Ext}^{k_1}(\mathcal{V}_{i_2}, \mathcal{V}_{i_1}) \otimes \mathrm{Ext}^{k_2}(\mathcal{W}_{j_2}, \mathcal{W}_{j_1})\end{aligned}$$

whence it is clear that $(\mathcal{V}_i \boxtimes \mathcal{W}_j)$ will be a (strong) exceptional sequence for the ordering $\prec$ if $(\mathcal{V}_i)$ and $(\mathcal{W}_j)$ are so.
Therefore we have to show that $(\mathcal{V}_i \boxtimes \mathcal{W}_j)$ generates $D^b(Coh(X \times Y))$ (see [BoBe], lemma 3.4.1). By [Bo], thm. 3.2, the triangulated subcategory $\mathcal{T}$ of $D^b(Coh(X \times Y))$ generated by the $\mathcal{V}_i \boxtimes \mathcal{W}_j$'s is admissible, and thus by [Bo], lemma 3.1, it suffices to show that the right orthogonal $\mathcal{T}^\perp$ is zero. Let $Z \in \mathrm{obj}\, \mathcal{T}^\perp$ so that we have

$$\mathrm{Hom}_{D^b(Coh(X\times Y))}(\mathcal{V}_i \boxtimes \mathcal{W}_j, Z[l_1+l_2]) = 0 \quad \forall i \in \{1, \dots, m\}, \\ \forall j \in \{1, \dots, n\} \, \forall l_1, l_2 \in \mathbb{Z}.$$

But

$$\begin{aligned}&\mathrm{Hom}_{D^b(Coh(X\times Y))}(\mathcal{V}_i \boxtimes \mathcal{W}_j, Z[l_1+l_2]) \\ &\quad \simeq \mathrm{Hom}_{D^b(Coh(X\times Y))}\left(\pi_1^*\mathcal{V}_i, R\mathcal{H}om^\bullet_{D^b(Coh(X\times Y))}(\pi_2^*\mathcal{W}_j, Z[l_1])[l_2]\right) \\ &\quad \simeq \mathrm{Hom}_{D^b(Coh(X))}\left(\mathcal{V}_i, R\pi_{1*}R\mathcal{H}om^\bullet_{D^b(Coh(X\times Y))}(\pi_2^*\mathcal{W}_j, Z[l_1])[l_2]\right)\end{aligned}$$

using the adjointness of $\pi_1^* = L\pi_1^*$ and $R\pi_{1*}$. But then

$$R\pi_{1*}R\mathcal{H}om^\bullet_{D^b(Coh(X\times Y))}(\pi_2^*\mathcal{W}_j, Z[l_1]) = 0 \quad \forall j \in \{1, \dots, m\} \, \forall l_1 \in \mathbb{Z}$$

because the $\mathcal{V}_i$ generate $D^b(Coh(X))$ and hence there is no non-zero object in the right orthogonal to $\langle \mathcal{V}_1, \dots, \mathcal{V}_n \rangle$. Let $U \subset X$ and $V \subset Y$ be affine open sets. Then

$$\begin{aligned}0 &= R\Gamma\left(U, R\pi_{1*}R\mathcal{H}om^\bullet_{D^b(Coh(X\times Y))}(\pi_2^*\mathcal{W}_j, Z[l+l_1])\right) \\ &\simeq R\mathrm{Hom}^\bullet\left(\mathcal{W}_j, R\pi_{2*}(Z[l]\mid_{U\times Y})[l_1]\right) \; \forall l, l_1 \in \mathbb{Z}\end{aligned}$$

whence $R\pi_{2*}(Z[l]\mid_{U\times Y}) = 0$ since the $\mathcal{W}_j$ generate $D^b(Coh(Y))$ (using thm. 2.1.2 in [BoBe]). Therefore we get

$$R\Gamma(U \times V, Z) = 0\,.$$

But $R^i\Gamma(U \times V, Z) = \Gamma(U \times V, H^i(Z))$ and thus all cohomology sheaves of Z are zero, i.e. $Z = 0$ in $D^b(Coh(X \times Y))$. □

Remark 2.1.19. This proposition is very useful for a treatment of the derived categories of coherent sheaves on rational homogeneous spaces from a systematic point of view. For if $X = G/P$ with G a connected semisimple complex Lie group, $P \subset G$ a parabolic subgroup, it is well known that one has a decomposition

$$X \simeq S_1/P_1 \times \ldots \times S_N/P_N$$

where $S_1, \ldots, S_N$ are connected simply connected simple complex Lie groups and $P_1, \ldots, P_N$ corresponding parabolic subgroups (cf. [Akh], 3.3, p. 74). Thus for the construction of complete exceptional sequences on any G/P one can restrict oneself to the case where G is simple.

2.2 Catanese's conjecture and the work of Kapranov

First we fix some notation concerning rational homogenous varieties and their Schubert varieties that will remain in force throughout the text unless otherwise stated. References for this are [Se2], [Sp].

G is a complex semi-simple Lie group which is assumed to be connected and simply connected with Lie algebra $\mathfrak{g}$.
$H \subset G$ is a fixed maximal torus in G with Lie algebra the Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$.
$R \subset \mathfrak{h}^*$ is the root system associated to $(\mathfrak{g}, \mathfrak{h})$ so that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^{\alpha}$$

with $\mathfrak{g}^{\alpha}$ the eigen-subspace of $\mathfrak{g}$ corresponding to $\alpha \in \mathfrak{h}^*$. Choose a base $S = \{\alpha_1, \ldots, \alpha_r\}$ for R; R^+ denotes the set of positive roots w.r.t. S, $R^- := -R^+$, so that $R = R^+ \cup R^-$, and ϱ is the half-sum of the positive roots.
$\mathrm{Aut}(\mathfrak{h}^*) \supset W := \langle s_\alpha \mid s_\alpha$ the reflection with vector α leaving R invariant$\rangle \simeq N(H)/H$ is the Weyl group of R.
Let $\mathfrak{b} := \mathfrak{h} \oplus \bigoplus_{\alpha > 0} \mathfrak{g}^{\alpha}$, $\mathfrak{b}^- := \mathfrak{h} \oplus \bigoplus_{\alpha < 0} \mathfrak{g}^{\alpha}$ be opposite Borel subalgebras of $\mathfrak{g}$ corresponding to $\mathfrak{h}$ and S, and $\mathfrak{p} \supset \mathfrak{b}$ a parabolic subalgebra corresponding uniquely to a subset $I \subset S$ (then

$$\mathfrak{p} = \mathfrak{p}(I) = \mathfrak{h} \oplus \bigoplus_{\alpha \in R^+} \mathfrak{g}^{\alpha} \oplus \bigoplus_{\alpha \in R^-(I)} \mathfrak{g}^{\alpha}$$

where $R^-(I) := \{\alpha \in R^- \mid \alpha = \sum_{i=1}^r k_i \alpha_i$ with $k_i \le 0$ for all i and $k_j = 0$ for all $\alpha_j \in I\}$). Let B, B^-, $P = P(I) \supset B$ be the corresponding connected subgroups of G with Lie algebras $\mathfrak{b}$, $\mathfrak{b}^-$, $\mathfrak{p}$.
$X := G/P$ is the rational homogeneous variety corresponding to G and P.

$l(w)$ is the length of an element $w \in W$ relative to the set of generators $\{s_\alpha \mid \alpha \in S\}$, i.e. the least number of factors in a decomposition

$$w = s_{\alpha_{i_1}} s_{\alpha_{i_2}} \dots s_{\alpha_{i_l}} \, , \ \alpha_{i_j} \in S \, ;$$

A decomposition with $l = l(w)$ is called reduced. One has the Bruhat order $\le$ on W, i.e. $x \le w$ for $x, w \in W$ iff x can be obtained by erasing some factors of a reduced decomposition of w.
W_P is the Weyl group of P, the subgroup of W generated by the simple reflections s_α with $\alpha \notin I$. In each coset $wW_P \in W/W_P$ there exists a unique element of minimal length and W^P denotes the set of minimal representatives of W/W^P. One has $W^P = \{w \in W \mid l(ww') = l(w) + l(w') \, \forall w' \in W_P\}$.
For $w \in W^P$, C_w denotes the double coset BwP/P in X, called a Bruhat cell, $C_w \simeq \mathbb{A}^{l(w)}$. Its closure in X is the Schubert variety X_w. $C_w^- = B^- wP/P$ is the opposite Bruhat cell of codimension $l(w)$ in X, $X^w = \overline{C_w^-}$ is the Schubert variety opposite to X_w.
There is the extended version of the Bruhat decomposition

$$G/P = \bigsqcup_{w \in W^P} C_w$$

(a paving of X by affine spaces) and for $v, \ w \in W^P$: $v \le w \Leftrightarrow X_v \subseteq X_w$; we denote the boundaries $\partial X_w := X_w \backslash C_w$, $\partial X^w := X^w \backslash C_w^-$, which have pure codimension 1 in X_w resp. X^w.

Moreover, we need to recall some facts and introduce further notation concerning representations of the subgroup $P = P(I) \subset G$, which will be needed in subsection 3 below. References are [A], [Se2], [Sp], [Ot2], [Stei].

The spaces $\mathfrak{h}_\alpha := [\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}] \subset \mathfrak{h}$, $\alpha \in R$, are 1-dimensional, one has $\mathfrak{g} = \bigoplus_{\alpha \in S} \mathfrak{h}_\alpha \oplus \bigoplus_{\alpha \in R^+} \mathfrak{g}^\alpha \oplus \bigoplus_{\alpha \in R^-} \mathfrak{g}^\alpha$ and there is a unique $H_\alpha \in \mathfrak{h}_\alpha$ such that $\alpha(H_\alpha) = 2$.
Then we have the weight lattice $\Lambda := \{\omega \in \mathfrak{h}^* \mid \omega(H_\alpha) \in \mathbb{Z} \, \forall \alpha \in R\}$ (which one identifies with the character group of H) and the set of dominant weights $\Lambda^+ := \{\omega \in \mathfrak{h}^* \mid \omega(H_\alpha) \in \mathbb{N} \, \forall \alpha \in R\}$. $\{\omega_1, \dots, \omega_r\}$ denotes the basis of $\mathfrak{h}^*$ dual to the basis $\{H_{\alpha_1}, \dots, H_{\alpha_r}\}$ of $\mathfrak{h}$. The ω_i are the fundamental weights. If $(\cdot, \cdot)$ is the inner product on $\mathfrak{h}^*$ induced by the Killing form, they can also be characterized by the equations $2(\omega_i, \alpha_j)/(\alpha_j, \alpha_j) = \delta_{ij}$ (Kronecker delta). It is well known that the irreducible finite dimensional representations of $\mathfrak{g}$ are in one-to-one correspondence with the $\omega \in \Lambda^+$, these ω occurring as highest weights.
I recall the Levi-Malčev decomposition of $P(I)$ (resp. $\mathfrak{p}(I)$): The algebras

$$\mathfrak{s}_P := \bigoplus_{\alpha \in S \backslash I} \mathfrak{h}_\alpha \oplus \bigoplus_{\alpha \in R^-(I)} (\mathfrak{g}^\alpha \oplus \mathfrak{g}^{-\alpha})$$

resp.

$$\mathfrak{l}_P := \bigoplus_{\alpha \in S} \mathfrak{h}_\alpha \oplus \bigoplus_{\alpha \in R^-(I)} (\mathfrak{g}^\alpha \oplus \mathfrak{g}^{-\alpha})$$

are the semisimple resp. reductive parts of $\mathfrak{p}(I)$ containing $\mathfrak{h}$, the corresponding connected subgroups of G will be denoted S_P resp. L_P. The algebra

$$\mathfrak{u}_P := \bigoplus_{\alpha \in R^- \backslash R^-(I)} \mathfrak{g}^{-\alpha}$$

is an ideal of $\mathfrak{p}(I)$, $\mathfrak{p}(I) = \mathfrak{l}_P \oplus \mathfrak{u}_P$, and the corresponding normal subgroup $R_u(P)$ is the unipotent radical of P. One has

$$P = L_P \ltimes R_u(P)\,,$$

the Levi-Malčev decomposition of P. The center Z of the Levi subgroup L_P is $Z = \{g \in H \,|\, \alpha(g) = 1\, \forall \alpha \in S \backslash I\}$. The connected center corresponds to the Lie algebra $\bigoplus_{\alpha \in I} \mathfrak{h}_\alpha$ and is isomorphic to the torus $(\mathbb{C}^*)^{|I|}$. One has

$$P = Z \cdot S_P \ltimes R_u(P)\,.$$

Under the hypothesis that G is simply connected, also S_P is simply connected.
If $r : P \to \mathrm{GL}(V)$ is an irreducible finite-dimensional representation, $R_u(P)$ acts trivially, and thus those r are in one-to-one correspondence with irreducible representations of the reductive Levi-subgroup L_P and as such possess a well-defined highest weight $\omega \in \Lambda$. Then the irreducible finite dimensional representations of $P(I)$ correspond bijectively to weights $\omega \in \mathfrak{h}^*$ such that ω can be written as $\omega = \sum_{i=1}^r k_i\omega_i$, $k_i \in \mathbb{Z}$, such that $k_j \in \mathbb{N}$ for all j such that $\alpha_j \notin I$. We will say that such an ω is the highest weight of the representation $r : P \to \mathrm{GL}(V)$.
The homogeneous vector bundle on G/P associated to r will be $G \times_r V := G \times V / \{(g, v) \sim (gp^{-1}, r(p)v)\,,\ p \in P,\ g \in G,\ v \in V\}$ as above. However, for a character $\chi : H \to \mathbb{C}$ (which will often be identified with $d\chi \in \mathfrak{h}^*$), $\mathcal{L}(\chi)$ will denote the homogeneous line bundle on G/B whose fibre at the point $e \cdot B$ is the one-dimensional representation of B corresponding to the character $-\chi$. This has the advantage that $\mathcal{L}(\chi)$ will be ample iff $d\chi = \sum_{j=1}^r k_j\omega_j$ with $k_j > 0$, $k_j \in \mathbb{Z}$ for all j, and it will also prove a reasonable convention in later applications of Bott's theorem.

The initial stimulus for this work was a conjecture due to F. Catanese. This is variant (A) of conjecture 2.2.1. Variant (B) is a modification of (A) due to the author, but closely related.

Conjecture 2.2.1. (A) On any rational homogeneous variety $X = G/P$ there exists a complete strong exceptional poset (cf. def. 2.1.7 (B)) and a bijection of the elements of the poset with the Schubert varieties in X such that the partial order of the poset is the one induced by the Bruhat-Chevalley order.

(B) For any $X = G/P$ there exists a strong complete exceptional sequence $\mathfrak{E} = (E_1, \dots, E_n)$ in $D^b(Coh\, X)$ with $n = |W^P|$, the number of Schubert varieties in X (which is the topological Euler characteristic of X).
Moreover, since there is a natural partial order $\le_{\mathfrak{E}}$ on the set of objects in $\mathfrak{E}$ by defining that $E' \le_{\mathfrak{E}} E$ for objects E and E' of $\mathfrak{E}$ iff there are objects $F_1, \dots, F_r$ of $\mathfrak{E}$ such that $\mathrm{Hom}(E', F_1) \neq 0$, $\mathrm{Hom}(F_1, F_2) \neq 0, \dots,$ $\mathrm{Hom}(F_r, E) \neq 0$ (the order of the exceptional sequence $\mathfrak{E}$ itself is a total order refining $\le_{\mathfrak{E}}$), there should be a relation between the Bruhat order on W^P and $\le_{\mathfrak{E}}$ (for special choice of $\mathfrak{E}$).
If $P = P(\alpha_i)$, some $i \in \{1, \dots, r\}$, is a maximal parabolic subgroup in G and G is simple, then one may conjecture more precisely: There exists a strong complete exceptional sequence $\mathfrak{E} = (E_1, \dots, E_n)$ in $D^b(Coh\, X)$ and a bijection

$$b : \{E_1, \dots, E_n\} \to \{X_w \,|\, w \in W^P\}$$

such that

$$\mathrm{Hom}(E_i, E_j) \neq 0 \iff b(E_j) \subseteq b(E_i)\,.$$

We would like to add the following two questions:

(C) Does there always exist on X a complete very strong exceptional poset (cf. def. 2.1.7 (C)) and a bijection of the elements of the poset with the Schubert varieties in X such that the partial order of the poset is the one induced by the Bruhat-Chevalley order?

(D) Can we achieve that the E_i's in (A), (B) and/or (C) are homogeneous vector bundles?

It is clear that, if the answer to (C) is positive, this implies (A). Moreover, the existence of a complete very strong exceptional poset entails the existence of a complete strong exceptional sequence.
For P maximal parabolic, part (B) of conjecture 2.2.1 is stronger than part (A). We will concentrate on that case in the following.
In the next subsection we will see that, at least upon adopting the right point of view, it is clear that the number of terms in any complete exceptional sequence in $D^b(Coh\, X)$ must equal the number of Schubert varieties in X.
To begin with, let me show how conjecture 2.2.1 can be brought in line with results of Kapranov obtained in [Ka3] (and [Ka1], [Ka2]) which are summarized in theorems 2.2.2, 2.2.3, 2.2.4 below.
One more piece of notation: If L is an m-dimensional vector space and $\lambda =$

$(\lambda_1, \dots, \lambda_m)$ is a non-increasing sequence of integers, then $\Sigma^\lambda L$ will denote the space of the irreducible representation $\varrho_\lambda : \mathrm{GL}(L) \to \mathrm{GL}(\Sigma^\lambda L)$ of $\mathrm{GL}(L) \simeq \mathrm{GL}_m\mathbb{C}$ with highest weight λ. Σ^λ is called the Schur functor associated to λ; if $\mathcal{E}$ is a rank m vector bundle on a variety Y, $\Sigma^\lambda\mathcal{E}$ will denote the vector bundle $P_{\mathrm{GL}}(\mathcal{E}) \times_{\varrho_\lambda} \Sigma^\lambda(L) := P_{\mathrm{GL}}(\mathcal{E}) \times \Sigma^\lambda(L)/\{(f,w) \sim (fg^{-1}, \varrho_\lambda(g)w),\ f \in P_{\mathrm{GL}}(\mathcal{E}),\ w \in \Sigma^\lambda L,\ g \in \mathrm{GL}_m\mathbb{C}\}$ where $P_{\mathrm{GL}}(\mathcal{E})$ is the principal $\mathrm{GL}_m\mathbb{C}$- bundle of local frames in $\mathcal{E}$.

Theorem 2.2.2. *Let* $\mathrm{Grass}(k, V)$ *be the Grassmanian of* k*-dimensional subspaces of an* n*-dimensional vector space* V*, and let* $\mathcal{R}$ *be the tautological rank* k *subbundle on* $\mathrm{Grass}(k, V)$*. Then the bundles* $\Sigma^\lambda\mathcal{R}$ *where* λ *runs over* $Y(k, n-k)$*, the set of Young diagrams with no more than* k *rows and no more than* $n-k$ *columns, are all exceptional, have no higher extension groups between each other and generate* $D^b(Coh\,\mathrm{Grass}(k, V))$*.*
Moreover, $\mathrm{Hom}(\Sigma^\lambda\mathcal{R}, \Sigma^\mu\mathcal{R}) \neq 0$ *iff* $\lambda_i \geq \mu_i\ \forall i = 1, \dots, k$*. (Thus these* $\Sigma^\lambda\mathcal{R}$ *form a strong complete exceptional sequence in* $D^b(Coh\,\mathrm{Grass}(k, V))$ *when appropriately ordered).*

Theorem 2.2.3. *If* V *is an* n*-dimensional vector space,* $1 \leq k_1 < \dots < k_l \leq n$ *a strictly increasing sequence of integers, and* $\mathrm{Flag}(k_1, \dots, k_l; V)$ *the variety of flags of subspaces of type* $(k_1, \dots, k_l)$ *in* V*, and if* $\mathcal{R}_{k_1} \subset \dots \subset \mathcal{R}_{k_l}$ *denotes the tautological flag of subbundles, then the bundles*

$$\Sigma^{\lambda_1}\mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_l}\mathcal{R}_{k_l}$$

where λ_j*,* $j = 1, \dots, l-1$*, runs over* $Y(k_j, k_{j+1} - k_j)$*, the set of Young diagrams with no more than* k_j *rows and no more than* $k_{j+1} - k_j$ *columns, and* λ_l *runs over* $Y(k_l, n - k_l)$*, form a strong complete exceptional sequence in* $D^b(Coh\,\mathrm{Flag}(k_1, \dots, k_l; V)$ *if we order them as follows:*
Choose a total order $\prec_j$ *on each of the sets* $Y(k_j, k_{j+1} - k_j)$ *and* $\prec_l$ *on* $Y(k_l, n - k_l)$ *such that if* $\lambda \prec_j \mu$ *(or* $\lambda \prec_t \mu$*) then the Young diagram of* λ *is not contained in the Young diagram of* μ*; endow the set* $Y = Y(k_l, n - k_l) \times Y(k_{l-1}, k_l - k_{l-1}) \times \dots \times Y(k_1, k_2 - k_1)$ *with the resulting lexicographic order* $\prec$*. Then* $\Sigma^{\lambda_1}\mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_l}\mathcal{R}_{k_l}$ *precedes* $\Sigma^{\mu_1}\mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\mu_l}\mathcal{R}_{k_l}$ *iff* $(\lambda_l, \dots, \lambda_1) \prec (\mu_l, \dots, \mu_1)$*.*

Theorem 2.2.4. *Let* V *be again an* n*-dimensional vector space and* $Q \subset \mathbb{P}(V)$ *a nonsingular quadric hypersurface.*
If n *is odd and* Σ *denotes the spinor bundle on* Q*, then the following constitutes a strong complete exceptional sequence in* $D^b(Coh\,Q)$*:*

$$(\Sigma(-n+2),\ \mathcal{O}_Q(-n+3), \dots, \mathcal{O}_Q(-1),\ \mathcal{O}_Q)$$

and $\mathrm{Hom}(\mathcal{E}, \mathcal{E}') \neq 0$ *for two bundles* $\mathcal{E}$*,* $\mathcal{E}'$ *in this sequence iff* $\mathcal{E}$ *precedes* $\mathcal{E}'$ *in the ordering of the sequence.*
If n *is even and* Σ^+*,* Σ^- *denote the spinor bundles on* Q*, then*

$$(\Sigma^+(-n+2),\ \Sigma^-(-n+2),\ \mathcal{O}_Q(-n+3), \dots, \mathcal{O}_Q(-1),\ \mathcal{O}_Q)$$

is a strong complete exceptional sequence in $D^b(Coh\, Q)$ *and* $\mathrm{Hom}(\mathcal{E}, \mathcal{E}') \neq 0$ *for two bundles* $\mathcal{E}$, $\mathcal{E}'$ *in this sequence iff* $\mathcal{E}$ *precedes* $\mathcal{E}'$ *in the ordering of the sequence with the one exception that* $\mathrm{Hom}(\Sigma^+(-n+2), \Sigma^-(-n+2)) = 0$.

Here by Σ (resp. Σ^+, Σ^-), we mean the homogeneous vector bundles on $Q = \mathrm{Spin}_n\mathbb{C}/P(\alpha_1)$, α_1 the simple root corresponding to the first node in the Dynkin diagram of type B_m, $n = 2m+1$, (resp. the Dynkin diagram of type D_m, $n = 2m$), that are the duals of the vector bundles associated to the irreducible representation of $P(\alpha_1)$ with highest weight ω_m (resp. highest weights ω_m, ω_{m-1}). We will deal more extensively with spinor bundles in subsection 3.2 below.

First look at theorem 2.2.2. It is well known (cf. [BiLa], section 3.1) that if one sets

$$I_{k,n} := \{\underline{i} = (i_1, \dots, i_k) \in \mathbb{N}^k \mid 1 \le i_1 < \dots < i_k \le n\}$$

and if $V_i := \langle v_1, \dots, v_i \rangle$ where $(v_1, \dots, v_n)$ is a basis for V, then the Schubert varieties in $\mathrm{Grass}(k, V)$ can be identified with

$$X_{\underline{i}} := \left\{ L \in \mathrm{Grass}(k,V) \mid \dim(L \cap V_{i_j}) \ge j \quad \forall 1 \le j \le k \right\}, \quad \underline{i} \in I_{k,n}$$

and the Bruhat order is reflected by

$$X_{\underline{i}} \subseteq X_{\underline{i'}} \iff i_j \le i'_j \quad \forall 1 \le j \le k;$$

and the $\underline{i} \in I_{k,n}$ bijectively correspond to Young diagrams in $Y(k, n-k)$ by associating to $\underline{i}$ the Young diagram $\lambda(\underline{i})$ defined by

$$\lambda(\underline{i})_t := i_{k-t+1} - (k-t+1) \quad \forall 1 \le t \le k\,.$$

Then containment of Schubert varieties corresponds to containment of associated Young diagrams. Thus conjecture 2.2.1 (B) is verified by the strong complete exceptional sequence of theorem 2.2.2.

In the case of $\mathrm{Flag}(k_1, \dots, k_l; V)$ (theorem 2.2.3) one can describe the Schubert subvarieties and the Bruhat order as follows (cf. [BiLa], section 3.2): Define

$$I_{k_1,\dots,k_l} = \left\{ \left(\underline{i}^{(1)}, \dots, \underline{i}^{(l)}\right) \in I_{k_1,n} \times \dots \times I_{k_l,n} \mid \underline{i}^{(j)} \subset \underline{i}^{(j+1)} \quad \forall 1 \le j \le l-1 \right\}$$

Then the Schubert varieties in $\mathrm{Flag}(k_1, \dots, k_l; V)$ can be identified with the

$$\begin{aligned} X_{\left(\underline{i}^{(1)},\dots,\underline{i}^{(l)}\right)} := \{(L_1, \dots, L_l) \in \mathrm{Flag}(k_1, \dots, k_l; V) \subset \mathrm{Grass}(k_1, V) \times \dots \\ \dots \times \mathrm{Grass}(k_l, V) \mid L_j \in X_{\underline{i}^{(j)}} \quad \forall 1 \le j \le l \right\} \end{aligned}$$

for $\left(\underline{i}^{(1)}, \dots, \underline{i}^{(l)}\right)$ running over $I_{k_1,\dots,k_l}$ (keeping the preceding notation for the Grassmannian). The Bruhat order on the Schubert varieties may be identified with the following partial order on $I_{k_1,\dots,k_l}$:

$$\left(\underline{i}^{(1)}, \dots, \underline{i}^{(l)}\right) \le \left(\underline{j}^{(1)}, \dots, \underline{j}^{(l)}\right) \iff i^{(t)} \le j^{(t)} \quad \forall 1 \le t \le l.$$

To set up a natural bijection between the set Y in theorem 2.2.3 and $I_{k_1,\dots,k_l}$ associate to $\mathbf{i} := \left(\underline{i}^{(1)}, \dots, \underline{i}^{(l)}\right)$ the following Young diagrams: $\lambda_l(\mathbf{i}) \in Y(k_l, n-k_l)$ is defined by

$$(\lambda_l(\mathbf{i}))_t := i^{(l)}_{k_l-t+1} - (k_l - t + 1) \quad \forall 1 \le t \le k_l.$$

Now since $\underline{i}^{(j)} \subset \underline{i}^{(j+1)} \quad \forall 1 \le j \le l-1$ one can write

$$i^{(j)}_s = i^{(j+1)}_{r(s)}, \; s = 1, \dots, k_j$$

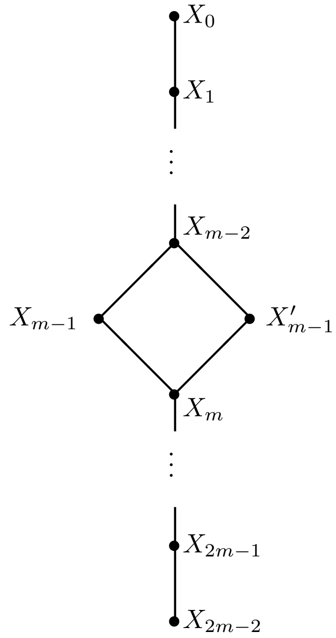
where $1 \le r(1) < \dots < r(k_j) \le k_{j+1}$. One then defines $\lambda_j(\mathbf{i}) \in Y(k_j, k_{j+1}-k_j)$ by

$$(\lambda_j(\mathbf{i}))_t := r(k_j - t + 1) - (k_j - t + 1) \quad \forall 1 \le t \le k_j.$$

However it is not clear to me in this case how to relate the Bruhat order on $I_{k_1,\dots,k_l}$ with the vanishing or non-vanishing of Hom-spaces between members of the strong complete exceptional sequence in theorem 2.2.3 (there is an explicit combinatorial criterion for the non-vanishing of

$$\mathrm{Hom}\left(\Sigma^{\lambda_1}\mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_l}\mathcal{R}_{k_l}, \Sigma^{\mu_1}\mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\mu_l}\mathcal{R}_{k_l}\right)$$

formulated in [Ka3], 3.12, but if this relates in any perspicuous way to the Bruhat order is not clear). In this respect, for the time being, conjecture 2.2.1 (parts (A) and (B)) must remain within the confines of wishful thinking.
If in the set-up of theorem 2.2.4 $Q \subset \mathbb{P}(V)$, $\dim V = n = 2m+1$ odd, is a smooth quadric hypersurface, then there are $2m$ Schubert varieties in Q and the Bruhat order on them is linear (cf. [BiLa], pp. 139/140), so the strong complete exceptional sequence of theorem 2.2.4 satisfies conjecture 2.2.1. (B).
The case of a smooth quadric hypersurface $Q \subset \mathbb{P}(V)$ with $\dim V = n = 2m$ even, is more interesting. The Bruhat order on the set of Schubert varieties can be depicted in the following way (cf. [BiLa], p. 142/143):



Here $X_0, \dots, X_{m-2}$, X_{m-1}, X'_{m-1}, $X_m, \dots, X_{2m-2}$ are labels for the Schubert varieties in Q and the subscript denotes the codimension in Q. The strong complete exceptional sequence

$$(\Sigma^+(-2m+2),\ \Sigma^-(-2m+2),\ \mathcal{O}_Q(-2m+3), \dots, \mathcal{O}_Q(-1),\ \mathcal{O}_Q)$$

does not verify conjecture 2.2.1 (B), but we claim that there is a strong complete exceptional sequence in the same braid group orbit (see thm. 2.1.10) that does. In fact, by [Ott], theorem 2.8, there are two natural exact sequences on Q

$$0 \longrightarrow \Sigma^+(-1) \longrightarrow \mathrm{Hom}(\Sigma^+(-1), \mathcal{O}_Q)^\vee \otimes \mathcal{O}_Q \longrightarrow \Sigma^- \longrightarrow 0$$
$$0 \longrightarrow \Sigma^-(-1) \longrightarrow \mathrm{Hom}(\Sigma^-(-1), \mathcal{O}_Q)^\vee \otimes \mathcal{O}_Q \longrightarrow \Sigma^+ \longrightarrow 0$$

where the (injective) arrows are the canonical morphisms of definition 2.1.9; one also has $\dim \mathrm{Hom}(\Sigma^+(-1), \mathcal{O}_Q)^\vee = \dim \mathrm{Hom}(\Sigma^-(-1), \mathcal{O}_Q)^\vee = 2^{m-1}$. (Caution: the spinor bundles in [Ott] are the duals of the bundles that are called spinor bundles in this text which is clear from the discussion in [Ott], p.305!). It follows that if in the above strong complete exceptional sequence we mutate $\Sigma^-(-2m+2)$ across $\mathcal{O}_Q(-2m+3), \dots, \mathcal{O}_Q(-m+1)$ to the right and afterwards mutate $\Sigma^+(-2m+2)$ across $\mathcal{O}_Q(-2m+3), \dots, \mathcal{O}_Q(-m+1)$ to the right, we will obtain the following complete exceptional sequences in $D^b(Coh\, Q)$:

If m is odd:

$$\big(\mathcal{O}_Q(-2m+3), \dots, \mathcal{O}_Q(-m+1),\ \Sigma^+(-m+1),\ \Sigma^-(-m+1),$$
$$\mathcal{O}_Q(-m+2), \dots, \mathcal{O}_Q(-1),\ \mathcal{O}_Q\big),$$

if m is even:

$$\big(\mathcal{O}_Q(-2m+3), \dots, \mathcal{O}_Q(-m+1),\ \Sigma^-(-m+1),\ \Sigma^+(-m+1),\\ \mathcal{O}_Q(-m+2), \dots, \mathcal{O}_Q(-1),\ \mathcal{O}_Q\big).$$

One finds (e.g. using theorem 2.2.4 and [Ott], thm.2.3 and thm. 2.8) that these exceptional sequences are again strong and if we let the bundles occurring in them (in the order given by the sequences) correspond to $X_0, \dots, X_{m-2},\ X_{m-1},\ X'_{m-1},\ X_m, \dots, X_{2m-2}$ (in this order), then the above two strong complete exceptional sequences verify conjecture 2.2.1. (B).

2.3 Information detected on the level of K-theory

The cellular decomposition of X has the following impact on $D^b(Coh\, X)$.

PROPOSITION 2.3.1. *The structure sheaves $\mathcal{O}_{X_w}$, $w \in W^P$, of Schubert varieties in X generate $D^b(Coh\, X)$ as a triangulated category.*

Since we have the Bruhat decomposition and each Bruhat cell is isomorphic to an affine space, the proof of the proposition will follow from the next lemma.

LEMMA 2.3.2. *Let Y be a reduced algebraic scheme, $U \subset Y$ an open subscheme with $U \simeq \mathbb{A}^d$, for some $d \in \mathbb{N}$, $Z := Y \backslash U$, $i : U \hookrightarrow Y$, $j : Z \hookrightarrow Y$ the natural embeddings. Look at the sequence of triangulated categories and functors*

$$D^b(Coh\, Z) \xrightarrow{\ j_*\ } D^b(Coh\, Y) \xrightarrow{\ i^*\ } D^b(Coh\, U)$$

(thus j_* is extension by 0 outside Z which is exact, and i^* is the restriction to U, likewise exact). Suppose $Z_1, \dots, Z_n \in \operatorname{obj} D^b(Coh\, Z)$ generate $D^b(Coh\, Z)$. Then $D^b(Coh\, Y)$ is generated by $j_*Z_1, \dots, j_*Z_n$, $\mathcal{O}_Y$.

Proof. $D^b(Coh\, Y)$ is generated by $Coh\, Y$ so it suffices to prove that each coherent sheaf $\mathcal{F}$ on Y is isomorphic to an object in the triangulated subcategory generated by $j_*Z_1, \dots, j_*Z_n$, $\mathcal{O}_Y$. By the Hilbert syzygy theorem $i^*\mathcal{F}$ has a resolution

$$(*) \quad 0 \to \mathcal{L}_t \to \dots \to \mathcal{L}_0 \to i^*\mathcal{F} \to 0$$

where the $\mathcal{L}_i$ are finite direct sums of $\mathcal{O}_U$. We recall the following facts (cf. [FuLa] , VI, lemmas 3.5, 3.6, 3.7):

(1) For any coherent sheaf $\mathcal{G}$ on U there is a coherent extension $\overline{\mathcal{G}}$ to Y.

(2) Any short exact sequence of coherent sheaves on U is the restriction of an exact sequence of coherent sheaves on Y.

(3) If $\mathcal{G}$ is coherent on U and $\overline{\mathcal{G}}_1$, $\overline{\mathcal{G}}_2$ are two coherent extensions of $\mathcal{G}$ to Y, then there are a coherent sheaf $\overline{\mathcal{G}}$ on Y and homomorphisms $\overline{\mathcal{G}} \xrightarrow{f} \overline{\mathcal{G}}_1$, $\overline{\mathcal{G}} \xrightarrow{g} \overline{\mathcal{G}}_2$ which restrict to isomorphisms over U.

Note that in the set-up of the last item we can write

$$0 \to \ker(f) \to \overline{\mathcal{G}} \xrightarrow{f} \overline{\mathcal{G}}_1 \to \operatorname{coker}(f) \to 0\,,$$
$$0 \to \ker(g) \to \overline{\mathcal{G}} \xrightarrow{g} \overline{\mathcal{G}}_2 \to \operatorname{coker}(g) \to 0$$

and $\ker(f)$, $\operatorname{coker}(f)$, $\ker(g)$, $\operatorname{coker}(g)$ are sheaves with support in Z, i.e. in the image of j_*. Thus they will be isomorphic to an object in the subcategory generated by $j_*Z_1, \dots, j_*Z_n$. In conclusion we see that if one coherent extension $\overline{\mathcal{G}}_1$ of $\mathcal{G}$ is isomorphic to an object in the subcategory generated by $j_*Z_1, \dots, j_*Z_n$, $\mathcal{O}_Y$, the same will be true for any other coherent extension $\overline{\mathcal{G}}_2$. The rest of the proof is now clear: We split $(*)$ into short exact sequences and write down extensions of these to Y by item (2) above. Since the $\mathcal{L}_i$ are finite direct sums of $\mathcal{O}_U$ one deduces from the preceding observation that $\mathcal{F}$ is indeed isomorphic to an object in the triangulated subcategory generated by $j_*Z_1, \dots, j_*Z_n$, $\mathcal{O}_Y$. □

Remark 2.3.3. On $\mathbb{P}^n$ it is possible to prove Beilinson's theorem with the help of proposition 2.3.1. Indeed the structure sheaves of a flag of linear subspaces $\{\mathcal{O}_{\mathbb{P}^n}, \mathcal{O}_{\mathbb{P}^{n-1}}, \dots, \mathcal{O}_{\mathbb{P}^1}, \mathcal{O}_{\mathbb{P}^0}\}$ admit the Koszul resolutions

$$0 \to \mathcal{O}(-1) \to \mathcal{O} \to \mathcal{O}_{\mathbb{P}^{n-1}} \to 0$$
$$0 \to \mathcal{O}(-2) \to \mathcal{O}(-1)^{\oplus 2} \to \mathcal{O} \to \mathcal{O}_{\mathbb{P}^{n-2}} \to 0$$
$$\vdots$$
$$0 \to \mathcal{O}(-n) \to \mathcal{O}(-(n-1))^{\oplus n} \to \dots \to \mathcal{O}(-1)^{\oplus n} \to \mathcal{O} \to \mathcal{O}_{\mathbb{P}^0} \to 0$$

from which one concludes inductively that $(\mathcal{O}(-n), \dots, \mathcal{O}(-1), \mathcal{O})$ generates $D^b(Coh\,\mathbb{P}^n)$.

Next we want to explain a point of view on exceptional sequences that in particular makes obvious the fact that the number of terms in any complete exceptional sequence on $X = G/P$ equals the number $|W^P|$ of Schubert varieties in X.

Definition 2.3.4. Let $\mathcal{T}$ be a triangulated category. The *Grothendieck group* $K_\circ(\mathcal{T})$ *of* $\mathcal{T}$ is the quotient of the free abelian group on the isomorphism classes $[A]$ of objects of $\mathcal{T}$ by the subgroup generated by expressions

$$[A] - [B] + [C]$$

for every distinguished triangle $A \longrightarrow B \longrightarrow C \longrightarrow A[1]$ in $\mathcal{T}$.

If $\mathcal{T} = D^b(\mathcal{A})$, $\mathcal{A}$ an Abelian category, then we also have $K_\circ(\mathcal{A})$ the Grothendieck group of $\mathcal{A}$, i.e. the free abelian group on the isomorphism classes of objects of $\mathcal{A}$ modulo relations $[D'] - [D] + [D'']$ for every short exact sequence $0 \to D' \to D \to D'' \to 0$ in $\mathcal{A}$, and it is clear that in this case $K_\circ(D^b(\mathcal{A})) \simeq K_\circ(\mathcal{A})$ (to a complex $A \in \operatorname{obj} D^b(\mathcal{A})$ one associates

$\sum_{i\in\mathbb{Z}}(-1)^i[H^i(A)] \in K_\circ(\mathcal{A})$ which is a map that is additive on distinguished triangles by the long exact cohomology sequence and hence descends to a map $K_\circ(D^b(\mathcal{A})) \to K_\circ(\mathcal{A})$; the inverse map is induced by the embedding $\mathcal{A} \hookrightarrow D^b(\mathcal{A})$).
Let now Y be some smooth projective variety. Then to $Z_1, Z_2 \in \mathrm{obj}\, D^b(Coh\, Y)$ one can assign the integer $\sum_{i\in\mathbb{Z}}(-1)^i \dim_{\mathbb{C}} \mathrm{Ext}^i(Z_1, Z_2)$, a map which is biadditive on distinguished triangles. Set $K_\circ(Y) := K_\circ(Coh\, Y)$.

DEFINITION 2.3.5. The (in general nonsymmetric) bilinear pairing

$$\begin{aligned} \chi : K_\circ(Y) \times K_\circ(Y) &\to \mathbb{Z} \\ ([Z_1],[Z_2]) &\mapsto \sum_{i\in\mathbb{Z}}(-1)^i \dim_{\mathbb{C}} \mathrm{Ext}^i(Z_1, Z_2) \end{aligned}$$

is called the *Euler bilinear form* (cf.[Gor]).

PROPOSITION 2.3.6. *Suppose that the derived category $D^b(Coh\, Y)$ of a smooth projective variety Y is generated by an exceptional sequence $(E_1, \dots, E_n)$. Then $K_\circ(Y) \simeq \mathbb{Z}^n$ is a free $\mathbb{Z}$-module of rank n with basis given by $([E_1], \dots, [E_n])$. The Euler bilinear form χ is unimodular with Gram matrix with respect to the basis $([E_1], \dots, [E_n])$:*

$$\begin{pmatrix} 1 & & & & \\ 0 & 1 & & * & \\ 0 & 0 & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix};$$

in other words, $([E_1], \dots, [E_n])$ is a semi-orthonormal basis w.r.t. χ.
Moreover, $n = \mathrm{rk}\, K_\circ(Y) = \bigoplus_{r=0}^{\dim Y} \mathrm{rk}\, A^r(Y)$, where $A^r(Y)$ is the group of codimension r algebraic cycles on Y modulo rational equivalence (so that $A(Y) = \bigoplus_r A^r(Y)$ is the Chow ring of Y).

Proof. Since the E_i, $i = 1, \dots, n$, generate $D^b(Coh\, Y)$ in the sense of definition 2.1..2 it is clear that the $[E_i]$ generate $K_\circ(Y)$ (note that for X, X', $X'' \in \mathrm{obj}\, D^b(Coh\, Y)$ we have $[X[n]] = (-1)^n[X]$, $n \in \mathbb{Z}$, $[X' \oplus X''] = [X'] + [X'']$ and for every distinguished triangle $X' \to X \to X'' \to X'[1]$ one has $[X''] = [X] - [X']$).
$[E_1] \neq 0$ because $\chi([E_1],[E_1]) = 1$ since E_1 is exceptional. Assume inductively that $[E_1], \dots, [E_i]$ are linearly independent in $K_\circ(Y) \otimes \mathbb{Q}$. We claim $[E_{i+1}] \notin \langle [E_1], \dots, [E_i] \rangle_{\mathbb{Q}}$. Indeed otherwise $[E_{i+1}] = \sum_{j=1}^{i} \lambda_j [E_j]$; since $[E_{i+1}] \neq 0$ there is $l := \min\{j \mid \lambda_j \neq 0\}$. Then

$$\chi([E_{i+1}],[E_l]) = \chi(\sum_{j=l}^{i} \lambda_j [E_j],[E_l]) = \lambda_l \neq 0$$

(using $\mathrm{Ext}^k(E_j, E_i) = 0\ \forall k \in \mathbb{Z}\ \forall i < j$) contradicting the fact that $\chi([E_{i+1}],[E_l]) = 0$ since $l < i+1$. Thus the $([E_1], \dots, [E_n])$ form a free $\mathbb{Z}$-basis

of $K_\circ(Y)$. The remaining assertions concerning χ are obvious from the above arguments.
The last equality follows from the fact that the Grothendieck Chern character ch gives an isomorphism

$$\mathrm{ch} : K_\circ(Y) \otimes \mathbb{Q} \to A(Y) \otimes \mathbb{Q}$$

(cf. [Ful], 15.2.16 (b)). □

Corollary 2.3.7. *If $(E_1, \ldots, E_n)$ is an exceptional sequence that generates $D^b(Coh\, X)$, X a rational homogeneous variety, then $n = |W^P|$, the number of Schubert varieties X_w in X.*

Proof. It suffices to show that the $[\mathcal{O}_{X_w}]$'s likewise form a free $\mathbb{Z}$-basis of $K_\circ(X)$. One way to see this is as follows: By proposition 2.3.1 it is clear that the $[\mathcal{O}_{X_w}]$ generate $K_\circ(X)$. $K_\circ(X)$ is a ring for the product $[\mathcal{F}] \cdot [\mathcal{G}] := \sum_{i \in \mathbb{Z}} (-1)^i [\mathcal{T}or_i^X(\mathcal{F}, \mathcal{G})]$ and

$$\begin{aligned} \beta : K_\circ(X) \times K_\circ(X) &\to \mathbb{Z} \\ ([\mathcal{F}], [\mathcal{G}]) &\mapsto \sum_{i \in \mathbb{Z}} (-1)^i h^i(X, [\mathcal{F}] \cdot [\mathcal{G}]) \end{aligned}$$

is a symmetric bilinear form. One can compute that $\beta([\mathcal{O}_{X_x}], [\mathcal{O}_{X^y}(-\partial X^y)]) = \delta_x^y$ (Kronecker delta) for $x,\, y \in W^P$, cf. [BL], proof of lemma 6, for details. □

It should be noted at this point that the constructions in subsection 2.1 relating to semi-orthogonal decompositions, mutations etc. all have their counterparts on the K-theory level and in fact appear more natural in that context (cf. [Gor], §1).

Remark 2.3.8. Suppose that on $X = G/P$ we have a strong complete exceptional sequence $(E_1, \ldots, E_n)$. Then the Gram matrix Γ of χ w.r.t. the basis $([E_1], \ldots, [E_n])$ on $K_\circ(X) \simeq \mathbb{Z}^n$ is upper triangular with ones on the diagonal and (i,j)-entry equal to $\dim_{\mathbb{C}} \mathrm{Hom}(E_i, E_j)$. Thus with regard to conjecture 2.2.1 it would be interesting to know the Gram matrix Γ' of χ in the basis given by the $[\mathcal{O}_{X_w}]$'s, $w \in W^P$, since Γ and Γ' will be conjugate.
The following computation was suggested to me by M. Brion. Without loss of generality one may reduce to the case $X = G/B$ using the fibration $\pi : G/B \to G/P$: Indeed, the pull-back under π of the Schubert variety X_{wP}, $w \in W^P$, is the Schubert variety $X_{w\, w_{0,P}}$ in G/B where $w_{0,P}$ is the element of maximal length of W_P, and $\pi^* \mathcal{O}_{X_{wP}} = \mathcal{O}_{X_{w\, w_{0,P}}}$. Moreover, by the projection formula and because $R\pi_* \mathcal{O}_{G/B} = \mathcal{O}_{G/P}$, we have $R\pi_* \circ \pi^* \simeq \mathrm{id}_{D^b(Coh\, G/P)}$ and

$$\chi(\pi^* \mathcal{E}, \pi^* \mathcal{F}) = \chi(\mathcal{E}, \mathcal{F})$$

for any $\mathcal{E},\, \mathcal{F} \in \mathrm{obj}\, D^b(Coh\, G/P)$.
Therefore, let $X = G/B$ and let $x,\, y \in W$. The first observation is that

$X_y = w_0 X^{w_0 y}$ and $\chi(\mathcal{O}_{X_x}, \mathcal{O}_{X_y}) = \chi(\mathcal{O}_{X_x}, \mathcal{O}_{X^{w_0 y}})$. This follows from the facts that there is a connected chain of rational curves in G joining g to id_G (since G is generated by images of homomorphisms $\mathbb{C} \to G$ and $\mathbb{C}^* \to G$) and that flat families of sheaves indexed by open subsets of $\mathbb{A}^1$ yield the same class in $K_\circ(X)$, thus $[\mathcal{O}_{X^{w_0 y}}] = [\mathcal{O}_{w_0 X^{w_0 y}}]$. We have

$$\begin{aligned} R\mathrm{Hom}^\bullet(\mathcal{O}_{X_x}, \mathcal{O}_{X^{w_0 y}}) &\simeq R\Gamma(X, R\mathcal{H}om^\bullet(\mathcal{O}_{X_x}, \mathcal{O}_{X^{w_0 y}})) \\ &\simeq R\Gamma(X, R\mathcal{H}om^\bullet(\mathcal{O}_{X_x}, \mathcal{O}_X) \otimes^L \mathcal{O}_{X^{w_0 y}}) \end{aligned}$$

(cf. [Ha1], prop. 5.3/5.14). Now Schubert varieties are Cohen-Macaulay, in fact they have rational singularities (cf. [Ra1]), whence

$$\begin{aligned} R\mathcal{H}om^\bullet(\mathcal{O}_{X_x}, \mathcal{O}_X) &\simeq \mathcal{E}xt^{\mathrm{codim}(X_x)}(\mathcal{O}_{X_x}, \mathcal{O}_X)[-\mathrm{codim}(X_x)] \\ &\simeq \omega_{X_x} \otimes \omega_X^{-1}[-\mathrm{codim}(X_x)]\,. \end{aligned}$$

But $\omega_{X_x} \otimes \omega_X^{-1} \simeq \mathcal{L}(\varrho)|_{X_x}(-\partial X_x)$ ($\mathcal{L}(\varrho)$ is the line bundle associated to the character ϱ), cf. [Ra1], prop. 2 and thm. 4. Now X_x and $X^{w_0 y}$ are Cohen-Macaulay and their scheme theoretic intersection is proper in X and reduced ([Ra1], thm. 3) whence $\mathcal{T}or_i^X(\mathcal{O}_{X_x}, \mathcal{O}_{X^{w_0 y}}) = 0$ for all $i \ge 1$ (cf. [Bri], lemma 1). Since ∂X_x is likewise Cohen-Macaulay by [Bri], lemma 4, we get by the same reasoning $\mathcal{T}or_i^X(\mathcal{O}_{\partial X_x}, \mathcal{O}_{X^{w_0 y}}) = 0$ for all $i \ge 1$. Thus by the exact sequence

$$0 \to \mathcal{O}_{X_x}(-\partial X_x) \to \mathcal{O}_{X_x} \to \mathcal{O}_{\partial X_x} \to 0$$

and the long exact sequence of Tor's we see that $\mathcal{T}or_i^X(\mathcal{O}_{X_x}(-\partial X_x), \mathcal{O}_{X^{w_0 y}}) = 0$ for all $i \ge 1$.
Therefore

$$R\mathrm{Hom}^\bullet(\mathcal{O}_{X_x}, \mathcal{O}_{X^{w_0 y}}) \simeq R\Gamma(X, \mathcal{L}(\varrho)|_{X_x}(-\partial X_x)[-\mathrm{codim}(X_x)] \otimes \mathcal{O}_{X^{w_0 y}})$$

so that setting $X_x^{w_0 y} := X_x \cap X^{w_0 y}$ and $(\partial X_x)^{w_0 y} := \partial X_x \cap X^{w_0 y}$

$$\chi(\mathcal{O}_{X_x}, \mathcal{O}_{X_y}) = (-1)^{\mathrm{codim}(X_x)} \chi\left(\mathcal{L}(\varrho)|_{X_x^{w_0 y}}(-(\partial X_x)^{w_0 y})\right)\,.$$

This is 0 unless $w_0 y \le x$ (because $X_x^{w_0 y}$ is non-empty iff $w_0 y \le x$, see [BL], lemma 1); moreover if $w_0 y \le x$ there are no higher h^i in the latter Euler characteristic by [BL], prop. 2. In conclusion

$$\chi(\mathcal{O}_{X_x}, \mathcal{O}_{X_y}) = \begin{cases} (-1)^{\mathrm{codim}(X_x)} h^0\left(\mathcal{L}(\varrho)|_{X_x^{w_0 y}}(-(\partial X_x)^{w_0 y})\right) & \text{if} \quad w_0 y \le x \\ 0 \quad \text{otherwise} \end{cases}$$

though the impact of this on conjecture 2.2.1 ((A) or (B)) is not clear to me. Cf. also [Bri2] for this circle of ideas.

3 Fibrational techniques

The main idea pervading this section is that the theorem of Beilinson on the structure of the derived category of coherent sheaves on projective space ([Bei]) and the related results of Kapranov ([Ka1], [Ka2], [Ka3]) for Grassmannians, flag varieties and quadrics, generalize without substantial difficulty from the absolute to the relative setting, i.e. to projective bundles etc. For projective bundles, Grassmann and flag bundles this has been done in [Or]. We review these results in subsection 3.1; the case of quadric bundles is dealt with in subsection 3.2. Aside from being technically a little more involved, the result follows rather mechanically combining the techniques from [Ka3] and [Or]. Thus armed, we deduce information on the derived category of coherent sheaves on isotropic Grassmannians and flag varieties in the symplectic and orthogonal cases; we follow an idea first exploited in [Sa] using successions of projective and quadric bundles.

3.1 The theorem of Orlov on projective bundles

Let X be a smooth projective variety, $\mathcal{E}$ a vector bundle of rank $r+1$ on X. Denote by $\mathbb{P}(\mathcal{E})$ the associated projective bundle † and $\pi : \mathbb{P}(\mathcal{E}) \to X$ the projection. Set $D^b(\mathcal{E}) := D^b(Coh(\mathbb{P}(\mathcal{E})))$, $D^b(X) := D^b(Coh(X))$. There are the functors $R\pi_* : D^b(\mathcal{E}) \to D^b(X)$ (note that $R\pi_* : D^+(Coh(\mathbb{P}(\mathcal{E}))) \to D^+(Coh(X))$, where $D^+(-)$ denotes the derived category of complexes bounded to the left in an abelian category, maps $D^b(\mathcal{E})$ to $D^b(X)$ using $R^i\pi_*(\mathcal{F}) = 0 \, \forall i > \dim \mathbb{P}(\mathcal{E}) \, \forall \mathcal{F} \in \operatorname{Ob} Coh(\mathbb{P}(\mathcal{E}))$ and the spectral sequence in hypercohomology) and $\pi^* : D^b(X) \to D^b(\mathcal{E})$ (π is flat, hence π^* is exact and passes to the derived category without taking the left derived functor).
We identify $D^b(X)$ with a full subcategory in $D^b(\mathcal{E})$ via π^* (cf. [Or], lemma 2.1). More generally we denote by $D^b(X)\otimes\mathcal{O}_{\mathcal{E}}(m)$ for $m \in \mathbb{Z}$ the subcategory of $D^b(\mathcal{E})$ which is the image of $D^b(X)$ in $D^b(\mathcal{E})$ under the functor $\pi^*(-)\otimes\mathcal{O}_{\mathcal{E}}(m)$, where $\mathcal{O}_{\mathcal{E}}(1)$ is the relative hyperplane bundle on $\mathbb{P}(\mathcal{E})$. Then one has the following result (cf. [Or], thm. 2.6):

Theorem 3.1.1. *The categories $D^b(X)\otimes\mathcal{O}_{\mathcal{E}}(m)$ are all admissible subcategories of $D^b(\mathcal{E})$ and we have a semiorthogonal decomposition*

$$D^b(\mathcal{E}) = \left\langle D^b(X) \otimes \mathcal{O}_{\mathcal{E}}(-r), \dots, D^b(X) \otimes \mathcal{O}_{\mathcal{E}}(-1), D^b(X) \right\rangle .$$

We record the useful

Corollary 3.1.2. *If $D^b(X)$ is generated by a complete exceptional sequence*

$$(E_1, \dots, E_n) ,$$

then $D^b(\mathcal{E})$ is generated by the complete exceptional sequence

$$(\pi^* E_1 \otimes \mathcal{O}_{\mathcal{E}}(-r), \dots, \pi^* E_n \otimes \mathcal{O}_{\mathcal{E}}(-r), \pi^* E_1 \otimes \mathcal{O}_{\mathcal{E}}(-r+1), \\ \dots, \pi^* E_1, \dots, \pi^* E_n) .$$

† Here and in the following $\mathbb{P}(\mathcal{E})$ denotes $\operatorname{Proj}(\operatorname{Sym}^\bullet(\mathcal{E}^\vee))$, i.e. the bundle of 1-dimensional subspaces in the fibres of $\mathcal{E}$, and contrary to Grothendieck's notation NOT the bundle $\operatorname{Proj}(\operatorname{Sym}^\bullet \mathcal{E})$ of hyperplanes in the fibres of $\mathcal{E}$ which might be less intuitive in the sequel.

Proof. This is stated in [Or], cor. 2.7; for the sake of completeness and because the method will be used repeatedly in the sequel, we give a proof. One just checks that

$$\mathrm{Ext}^k(\pi^* E_i \otimes \mathcal{O}_{\mathcal{E}}(-r_1), \pi^* E_j \otimes \mathcal{O}_{\mathcal{E}}(-r_2)) = 0$$

$\forall k, \forall 1 \le i, j \le n \, \forall 0 \le r_1 < r_2 \le r$ and $\forall k$, $\forall 1 \le j < i \le n$, $r_1 = r_2$. Indeed,

$$\begin{aligned}\mathrm{Ext}^k(\pi^* E_i \otimes \mathcal{O}_{\mathcal{E}}(-r_1), \pi^* E_j \otimes \mathcal{O}_{\mathcal{E}}(-r_2)) &\simeq \mathrm{Ext}^k(\pi^* E_i, \pi^* E_j \otimes \mathcal{O}_{\mathcal{E}}(r_1 - r_2)) \\ &\simeq \mathrm{Ext}^k(E_i, E_j \otimes R\pi_*(\mathcal{O}_{\mathcal{E}}(r_1 - r_2)))\end{aligned}$$

where for the second isomorphism we use that $R\pi_*$ is right adjoint to π^*, and the projection formula (cf. [Ha2], II, prop. 5.6). When $r_1 = r_2$ and $i > j$ then $R\pi_*\mathcal{O}_{\mathcal{E}} \simeq \mathcal{O}_X$ and $\mathrm{Ext}^k(E_i, E_j) = 0$ for all k because $(E_1, \dots, E_n)$ is exceptional. If on the other hand $0 \le r_1 < r_2 \le r$ then $-r \le r_1 - r_2 < 0$ and $R\pi_*(\mathcal{O}_{\mathcal{E}}(r_1 - r_2)) = 0$.
It remains to see that each $\pi^* E_i \otimes \mathcal{O}_{\mathcal{E}}(-r_1)$ is exceptional. From the above calculation it is clear that this follows exactly from the exceptionality of E_i. □

Remark 3.1.3. From the above proof it is clear that even if we start in corollary 3.1.2 with a strong complete exceptional sequence $(E_1, \dots, E_n)$ (i.e. $\mathrm{Ext}^k(E_i, E_j) = 0 \forall i, j \forall k \neq 0$), the resulting exceptional sequence on $\mathbb{P}(\mathcal{E})$ need not again be strong: For example take $X = \mathbb{P}^1$ with strong complete exceptional sequence $(\mathcal{O}(-1), \mathcal{O})$ and $\mathcal{E} = \mathcal{O} \oplus \mathcal{O}(h)$, $h \ge 2$, so that $\mathbb{P}(\mathcal{E}) = \mathbb{F}_h \xrightarrow{\pi} \mathbb{P}^1$ is a Hirzebruch surface. Then $(\pi^*\mathcal{O}(-1) \otimes \mathcal{O}_{\mathcal{E}}(-1), \mathcal{O}_{\mathcal{E}}(-1), \pi^*\mathcal{O}(-1) \otimes \mathcal{O}_{\mathcal{E}}, \mathcal{O}_{\mathcal{E}})$ is an exceptional sequence on $\mathbb{F}_h$ that generates $D^b(Coh(\mathbb{F}_h))$, but it is not a strong one since $\mathrm{Ext}^1(\mathcal{O}_{\mathcal{E}}(-1), \mathcal{O}_{\mathcal{E}}) \simeq H^1(\mathbb{P}^1, \pi_* \mathcal{O}_{\mathcal{E}}(1)) \simeq H^1(\mathbb{P}^1, \mathcal{O} \oplus \mathcal{O}(-h)) \simeq \mathrm{Sym}^{h-2}\, \mathbb{C}^2 \neq 0$.

Analogous results hold for relative Grassmannians and flag varieties. Specifically, if $\mathcal{E}$ is again a rank $r+1$ vector bundle on a smooth projective variety X, denote by $\mathrm{Grass}_X(k, \mathcal{E})$ the relative Grassmannian of k-planes in the fibres of $\mathcal{E}$ with projection $\pi : \mathrm{Grass}_X(k, \mathcal{E}) \to X$ and tautological subbundle $\mathcal{R}$ of rank k in $\pi^*\mathcal{E}$. Denote by $Y(k, r+1-k)$ the set of partitions $\lambda = (\lambda_1, \dots, \lambda_k)$ with $0 \le \lambda_k \le \lambda_{k-1} \le \dots \le \lambda_1 \le r+1-k$ or equivalently the set of Young diagrams with at most k rows and no more than $r+1-k$ columns. For $\lambda \in V(k, r+1-k)$ we have the Schur functor Σ^λ and bundles $\Sigma^\lambda\mathcal{R}$ on $\mathrm{Grass}_X(k, \mathcal{E})$. Moreover, as before we can talk about full subcategories $D^b(X) \otimes \Sigma^\lambda\mathcal{R}$ of $D^b(Coh(\mathrm{Grass}_X(k, \mathcal{E})))$. Choose a total order $\prec$ on $Y(k, r+1-k)$ such that if $\lambda \prec \mu$ then the Young diagram of λ is not contained in the Young diagram of μ, i.e. $\exists i : \mu_i < \lambda_i$. Then one has (cf. [Or], p. 137):

Theorem 3.1.4. *There is a semiorthogonal decomposition*

$$D^b(Coh(\mathrm{Grass}_X(k, \mathcal{E}))) = \left\langle \dots, D^b(X) \otimes \Sigma^\lambda\mathcal{R}, \dots, D^b(X) \otimes \Sigma^\mu\mathcal{R}, \dots \right\rangle$$

$(\lambda \prec \mu)$.
If $(E_1, \dots, E_n)$ is a complete exceptional sequence in $D^b(X)$, then

$$\big(\dots, \pi^* E_1 \otimes \Sigma^\lambda \mathcal{R}, \dots, \pi^* E_n \otimes \Sigma^\lambda \mathcal{R},\\ \dots, \pi^* E_1 \otimes \Sigma^\mu \mathcal{R}, \dots, \pi^* E_n \otimes \Sigma^\mu \mathcal{R}, \dots\big)$$

is a complete exceptional sequence in $D^b(Coh(\mathrm{Grass}_X(k, \mathcal{E})))$. Here all $\pi^* E_i \otimes \Sigma^\lambda \mathcal{R}$, $i \in \{1, \dots, n\}$, $\lambda \in Y(k, r+1-k)$ occur in the list, and $\pi^* E_i \otimes \Sigma^\lambda \mathcal{R}$ precedes $\pi^* E_j \otimes \Sigma^\mu \mathcal{R}$ iff $\lambda \prec \mu$ or $\lambda = \mu$ and $i < j$.

More generally, we can consider for $1 \le k_1 < \dots < k_t \le r+1$ the variety $\mathrm{Flag}_X(k_1, \dots, k_t; \mathcal{E})$ of relative flags of type $(k_1, \dots, k_t)$ in the fibres of $\mathcal{E}$, with projection π and tautological subbundles $\mathcal{R}_{k_1} \subset \dots \subset \mathcal{R}_{k_t} \subset \pi^* \mathcal{E}$. If we denote again by $Y(a, b)$ the set of Young diagrams with at most a rows and b columns, we consider the sheaves $\Sigma^{\lambda_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_t} \mathcal{R}_{k_t}$ on $\mathrm{Flag}_X(k_1, \dots, k_t; \mathcal{E})$ with $\lambda_k \in Y(k_t, r+1-k_t)$ and $\lambda_j \in Y(k_j, k_{j+1} - k_j)$ for $j = 1, \dots, t-1$ and subcategories $D^b(X) \otimes \Sigma^{\lambda_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_t} \mathcal{R}_{k_t}$ of $D^b(Coh(\mathrm{Flag}_X(k_1, \dots, k_t; \mathcal{E})))$. Choose a total order $\prec_j$ on each of the sets $Y(k_j, k_{j+1} - k_j)$ and $\prec_t$ on $Y(k_t, r+1-k_t)$ with the same property as above for the relative Grassmannian, and endow the set $Y = Y(k_t, r+1-k_t) \times \dots \times Y(k_1, k_2 - k_1)$ with the resulting lexicographic order $\prec$.

Theorem 3.1.5. *There is a semiorthogonal decomposition*

$$D^b(Coh(\mathrm{Flag}_X(k_1, \dots, k_t; \mathcal{E}))) = \big\langle \dots, D^b(X) \otimes \Sigma^{\lambda_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_t} \mathcal{R}_{k_t},\\ \dots, D^b(X) \otimes \Sigma^{\mu_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\mu_t} \mathcal{R}_{k_t}, \dots \big\rangle$$

$((\lambda_t, \dots, \lambda_1) \prec (\mu_t, \dots, \mu_1))$.
If $(E_1, \dots, E_n)$ is a complete exceptional sequence in $D^b(X)$, then

$$\big(\dots, \pi^* E_1 \otimes \Sigma^{\lambda_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_t} \mathcal{R}_{k_t}, \dots, \pi^* E_n \otimes \Sigma^{\lambda_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_t} \mathcal{R}_{k_t}, \dots,\\ \pi^* E_1 \otimes \Sigma^{\mu_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\mu_t} \mathcal{R}_{k_t}, \dots, \pi^* E_n \otimes \Sigma^{\mu_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\mu_t} \mathcal{R}_{k_t}, \dots\big)$$

is a complete exceptional sequence in $D^b(Coh(\mathrm{Flag}_X(k_1, \dots, k_t; \mathcal{E})))$. Here all $\pi^* E_i \otimes \Sigma^{\lambda_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_t} \mathcal{R}_{k_t}$, $i \in \{1, \dots, n\}$, $(\lambda_t, \dots, \lambda_1) \in Y$ occur in the list, and $\pi^* E_i \otimes \Sigma^{\lambda_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\lambda_t} \mathcal{R}_{k_t}$ precedes $\pi^* E_j \otimes \Sigma^{\mu_1} \mathcal{R}_{k_1} \otimes \dots \otimes \Sigma^{\mu_t} \mathcal{R}_{k_t}$ iff $(\lambda_t, \dots, \lambda_1) \prec (\mu_t, \dots, \mu_1)$ or $(\lambda_t, \dots, \lambda_1) = (\mu_t, \dots, \mu_1)$ and $i < j$.

Proof. Apply theorem 3.1.4 iteratively to the succession of Grassmann bundles

$$\mathrm{Flag}_X(k_1, \dots, k_t; \mathcal{E}) = \mathrm{Grass}_{\mathrm{Flag}_X(k_2, \dots, k_t; \mathcal{E})}(k_1, \mathcal{R}_{k_2})\\ \to \mathrm{Flag}_X(k_2, \dots, k_t; \mathcal{E}) = \mathrm{Grass}_{\mathrm{Flag}_X(k_3, \dots, k_t; \mathcal{E})}(k_2, \mathcal{R}_{k_3}) \to \dots \to X$$

□

3.2 The theorem on quadric bundles

Let us now work out in detail how the methods of Orlov ([Or]) and Kapranov ([Ka2], [Ka3]) yield a result for quadric bundles that is analogous to theorems 3.1.1, 3.1.4, 3.1.5.
As in subsection 3.1, X is a smooth projective variety with a vector bundle $\mathcal{E}$ of rank $r+1$ endowed with a symmetric quadratic form $q \in \Gamma(X, \mathrm{Sym}^2 \mathcal{E}^\vee)$ which is nondegenerate on each fibre; $\mathcal{Q} := \{q = 0\} \subset \mathbb{P}(\mathcal{E})$ is the associated quadric bundle:

$$\begin{array}{ccc} \mathcal{Q} & \hookrightarrow & \mathbb{P}(\mathcal{E}) \\ & \pi = \Pi|_{\mathcal{Q}} \searrow & \downarrow \Pi \\ & & X \end{array}$$

Write $D^b(X) := D^b(Coh\, X)$, $D^b(\mathcal{Q}) := D^b(Coh\, \mathcal{Q})$, $D^b(\mathcal{E}) := D^b(Coh\, \mathbb{P}(\mathcal{E}))$.

Lemma 3.2.1. *The functor*

$$\pi^* = L\pi^* : D^b(X) \to D^b(\mathcal{Q})$$

is fully faithful.

Proof. Since $\mathcal{Q}$ is a locally trivial fibre bundle over X with rational homogeneous fibre, we have $\pi_* \mathcal{O}_{\mathcal{Q}} = \mathcal{O}_X$ and $R^i \pi_* \mathcal{O}_{\mathcal{Q}} = 0$ for $i > 0$. The right adjoint to $L\pi^*$ is $R\pi_*$, and $R\pi_* \circ L\pi^*$ is isomorphic to the identity on $D^b(X)$ because of the projection formula and $R\pi_* \mathcal{O}_{\mathcal{Q}} = \mathcal{O}_X$. Hence $L\pi^*$ is fully faithful (and equal to π^* since π is flat). $\square$

Henceforth $D^b(X)$ is identified with a full subcategory of $D^b(\mathcal{Q})$.
We will now define two bundles of graded algebras, $\mathcal{A} = \bigoplus_{n \geq 0} \mathcal{A}_n$ and $\mathcal{B} = \bigoplus_{n \geq 0} \mathcal{B}_n$, on X. Form the tensor algebra $\mathrm{T}^\bullet(\mathcal{E}[h])$ where h is an indeterminate with $\deg h = 2$ and germs of sections in $\mathcal{E}$ have degree 1 and take the quotient modulo the two-sided ideal $\mathcal{I}$ of relations with $\mathcal{I}(x) := \langle e \otimes e - q(e)h,\ e \otimes h - h \otimes e \rangle_{e \in \mathcal{E}(x)}$, $(x \in X)$. This quotient is $\mathcal{A}$, the bundle of graded Clifford algebras of the orthogonal vector bundle $\mathcal{E}$. On the other hand, $\mathcal{B}$ is simply defined as $\bigoplus_{n \geq 0} \pi_* \mathcal{O}_{\mathcal{Q}}(n)$, the relative coordinate algebra of the quadric bundle $\mathcal{Q}$.
For each graded left $\mathcal{A}$-module $\mathcal{M} = \bigoplus_{i \in \mathbb{Z}} \mathcal{M}_i$ with $\mathcal{M}_i$ vector bundles on X we get a complex $L^\bullet(\mathcal{M})$ of bundles on $\mathcal{Q}$

$$L^\bullet(\mathcal{M}) : \ldots \to \pi^* \mathcal{M}_j \otimes_{\mathbb{C}} \mathcal{O}_{\mathcal{Q}}(j) \xrightarrow{d^j} \pi^* \mathcal{M}_{j+1} \otimes_{\mathbb{C}} \mathcal{O}_{\mathcal{Q}}(j+1) \to \ldots$$

with differentials given as follows: For $x \in X$ and $e \in \mathcal{E}(x)$ we get a family of mappings

$$d^j(x,e) : \mathcal{M}_j(x) \to \mathcal{M}_{j+1}(x)$$

given by left multiplication by e on $\mathcal{M}_j(x)$ and linear in e which globalize to mappings $\Pi^*\mathcal{M}_j \otimes \mathcal{O}_{\mathcal{E}}(j) \to \Pi^*\mathcal{M}_{j+1} \otimes \mathcal{O}_{\mathcal{E}}(j+1)$. When restricted to $\mathcal{Q}$ two successive maps compose to 0 and we get the required complex.
We recall at this point the relative version of Serre's correspondence (cf. e.g. [EGA], II, §3):

Theorem 3.2.2. *Let $Mod_{\mathcal{E}}^X$ be the category whose objects are coherent sheaves over X of graded $\mathrm{Sym}^\bullet\mathcal{E}^\vee$-modules of finite type with morphisms*

$$\mathrm{Hom}_{Mod_{\mathcal{E}}^X}(\mathcal{M},\mathcal{N}) := \varinjlim_{n} \mathrm{Hom}_{\mathrm{Sym}^\bullet \mathcal{E}^\vee}(\bigoplus_{i\geq n}\mathcal{M}_i, \bigoplus_{i\geq n}\mathcal{N}_i)$$

(the direct limit running over the groups of homomorphisms of sheaves of graded modules over $\mathrm{Sym}^\bullet\,\mathcal{E}^\vee$ which are homogeneous of degree 0). If $\mathcal{F} \in \mathrm{obj}(Coh(\mathbb{P}(\mathcal{E})))$ set

$$\alpha(\mathcal{F}) := \bigoplus_{n=0}^{\infty} \Pi_*(\mathcal{F}(n))\,.$$

Then the functor $\alpha : Coh(\mathbb{P}(\mathcal{E}))) \to Mod_{\mathcal{E}}^X$ is an equivalence of categories with quasi-inverse $(-)^\sim$ which is an additive and exact functor.

The key remark is now that $L^\bullet(\mathcal{A}^\vee)$ is exact since it arises by applying the Serre functor $(-)^\sim$ to the complex $P^\bullet$ given by

$$\dots \xrightarrow{\ d\ } \mathcal{A}_2^\vee \otimes \mathcal{B}[-2] \xrightarrow{\ d\ } \mathcal{A}_1^\vee \otimes \mathcal{B}[-1] \xrightarrow{\ d\ } \mathcal{A}_0^\vee \otimes \mathcal{B} \to \mathcal{O}_X \to 0.$$

Here, if $(e_1, \dots, e_{r+1})$ is a local frame of $\mathcal{E} = \mathcal{A}_1$ and $(e_1^\vee, \dots, e_{r+1}^\vee)$ is the corresponding dual frame for $\mathcal{E}^\vee = \mathcal{B}_1$, the differential d is $\sum_{i=1}^{r+1} l_{e_i}^\vee \otimes l_{e_i^\vee}$, where $l_{e_i} : \mathcal{A}[-1] \to \mathcal{A}$ is left multiplication by e_i and analogously $l_{e_i^\vee} : \mathcal{B}[-1] \to \mathcal{B}$. This complex is exact since it is so fibrewise as a complex of vector bundles; the fibre over a point $x \in X$ is just Priddy's generalized Koszul complex associated to the dual quadratic algebras $\mathcal{B}(x) = \oplus_i H^0(\mathcal{Q}(x), \mathcal{O}_{\mathcal{Q}(x)}(i))$ and $\mathcal{A}(x)$, the graded Clifford algebra of the vector space $\mathcal{E}(x)$. See [Ka3], 4.1 and [Pri].
Define bundles Ψ_i, $i \geq 0$, on $\mathcal{Q}$ by a twisted truncation, i.e., by the requirement that

$$0 \to \Psi_i \to \pi^*\mathcal{A}_i^\vee \to \pi^*\mathcal{A}_{i-1}^\vee \otimes \mathcal{O}_{\mathcal{Q}}(1) \to \dots \to \pi^*\mathcal{A}_0^\vee \otimes \mathcal{O}_{\mathcal{Q}}(i) \to 0$$

be exact. Look at the fibre product

$$\begin{array}{ccc} \Delta \subset \mathcal{Q} \times_X \mathcal{Q} & \xrightarrow{\ p_2\ } & \mathcal{Q} \\ {\scriptstyle p_1}\downarrow & & {\scriptstyle \pi}\downarrow \\ \mathcal{Q} & \xrightarrow{\ \pi\ } & X \end{array}$$

together with the relative diagonal Δ. The goal is to cook up an infinite to the left but eventually periodic resolution of the sheaf $\mathcal{O}_\Delta$ on $\mathcal{Q}\times_X\mathcal{Q}$, then truncate it in a certain degree and identify the remaining kernel explicitly.
Write $\Psi_i\boxtimes\mathcal{O}(-i)$ for $p_1^*\Psi_i\otimes p_2^*\mathcal{O}_{\mathcal{Q}}(-i)$ and consider the maps $\Psi_i\boxtimes\mathcal{O}(-i)\to\Psi_{i-1}\boxtimes\mathcal{O}(-i+1)$ induced by the maps of complexes

$$\begin{array}{ccccc}
(\pi^*\mathcal{A}_i^\vee\otimes\mathcal{O})\boxtimes\mathcal{O}(-i) & \longrightarrow & (\pi^*\mathcal{A}_{i-1}^\vee\otimes\mathcal{O}(1))\boxtimes\mathcal{O}(-i) & \longrightarrow & \dots\\
\downarrow & & \downarrow & & \\
(\pi^*\mathcal{A}_{i-1}^\vee\otimes\mathcal{O})\boxtimes\mathcal{O}(-i+1) & \longrightarrow & (\pi^*\mathcal{A}_{i-2}^\vee\otimes\mathcal{O}(1))\boxtimes\mathcal{O}(-i+1) & \longrightarrow & \dots
\end{array}$$

where the vertical arrows are given by $\sum_{i=1}^{r+1}(\pi^*r_{e_i}^\vee\otimes\mathrm{id})\boxtimes\widetilde{l_{e_i^\vee}}$; here again we're using the local frames $(e_1,\dots,e_{r+1})$, resp. $(e_1^\vee,\dots,e_{r+1}^\vee)$, $r_{e_i}:\mathcal{A}[-1]\to\mathcal{A}$ is right multiplication by e_i and $\widetilde{l_{e_i^\vee}}$ is the map induced by $l_{e_i^\vee}:\mathcal{B}[-1]\to\mathcal{B}$ between the associated sheaves (via the Serre correspondence).
This is truly a map of complexes since right and left Clifford multiplication commute with each other. Moreover, we obtain a complex, infinite on the left side

$$R^\bullet:\dots\to\Psi_i\boxtimes\mathcal{O}(-i)\to\dots\to\Psi_2\boxtimes\mathcal{O}(-2)\to\Psi_1\boxtimes\mathcal{O}(-1)\to\mathcal{O}_{\mathcal{Q}\times_X\mathcal{Q}}.$$

Lemma 3.2.3. *The complex $R^\bullet$ is a left resolution of $\mathcal{O}_\Delta$, $\Delta\subset\mathcal{Q}\times_X\mathcal{Q}$ being the diagonal.*

Proof. Consider $\mathcal{B}^2:=\bigoplus_i\mathcal{B}_i\otimes_{\mathcal{O}_X}\mathcal{B}_i$, the "Segre product of $\mathcal{B}$ with itself" (i.e. the homogeneous coordinate ring of $\mathcal{Q}\times_X\mathcal{Q}$ under the (relative) Segre morphism). Look at the following double complex $D^{\bullet\bullet}$ of $\mathcal{B}^2$-modules:

$$\begin{array}{ccccccc}
\dots\longrightarrow & \bigoplus_i\mathcal{B}_{i+2}\otimes\mathcal{B}_{i-2} & & & & \\
 & \uparrow & & & & \\
\dots\longrightarrow & \bigoplus_i\mathcal{A}_1^\vee\otimes\mathcal{B}_{i+1}\otimes\mathcal{B}_{i-2} & \longrightarrow & \bigoplus_i\mathcal{B}_{i+1}\otimes\mathcal{B}_{i-1} & & \\
 & \uparrow & & \uparrow & & \\
\dots\longrightarrow & \bigoplus_i\mathcal{A}_2^\vee\otimes\mathcal{B}_i\otimes\mathcal{B}_{i-2} & \longrightarrow & \bigoplus_i\mathcal{A}_1^\vee\otimes\mathcal{B}_i\otimes\mathcal{B}_{i-1} & \longrightarrow & \bigoplus_i\mathcal{B}_i\otimes\mathcal{B}_i
\end{array}$$

Here the columns correspond to the right resolutions of $\Psi_0\boxtimes\mathcal{O}$, $\Psi_1\boxtimes\mathcal{O}(-1)$, $\Psi_2\boxtimes\mathcal{O}(-2)$ etc. (starting from the right) if we pass from complexes of coherent sheaves on $\mathcal{Q}\times_X\mathcal{Q}$ to complexes of graded $\mathcal{B}^2$-modules via Serre's theorem. For example, the left-most column in the above diagram arises from

$$\begin{aligned}(\pi^*\mathcal{A}_2^\vee\otimes\mathcal{O}_{\mathcal{Q}})\boxtimes\mathcal{O}(-2)&\to(\pi^*\mathcal{A}_1^\vee\otimes\mathcal{O}_{\mathcal{Q}}(1))\boxtimes\mathcal{O}(-2)\\&\to(\pi^*\mathcal{A}_0^\vee\otimes\mathcal{O}_{\mathcal{Q}}(2))\boxtimes\mathcal{O}(-2)\to 0\end{aligned}$$

The horizontal arrows in the above diagram then come from the morphisms of complexes defining the differentials in $R^\bullet$.
The associated total complex $Tot^\bullet(D^{\bullet\bullet})$ has a natural augmentation $a : Tot^\bullet(D^{\bullet\bullet}) \to \bigoplus_i \mathcal{B}_{2i}$ arising from the multiplication maps $\mathcal{B}_{i+j} \otimes \mathcal{B}_{i-j} \to \mathcal{B}_{2i}$ and corresponding to the augmentation $R^\bullet \to \mathcal{O}_\Delta$.
Claim: a is a quasi-isomorphism. For this note that $D^{\bullet\bullet}$ is the direct sum over i of double complexes

$$\begin{array}{ccccccc}
\ldots \longrightarrow & \mathcal{B}_{i+2} \otimes \mathcal{B}_{i-2} & & & & & \\
 & \uparrow & & & & & \\
\ldots \longrightarrow & \mathcal{A}_1^\vee \otimes \mathcal{B}_{i+1} \otimes \mathcal{B}_{i-2} & \longrightarrow & \mathcal{B}_{i+1} \otimes \mathcal{B}_{i-1} & & & \\
 & \uparrow & & \uparrow & & & \\
\ldots \longrightarrow & \mathcal{A}_2^\vee \otimes \mathcal{B}_i \otimes \mathcal{B}_{i-2} & \longrightarrow & \mathcal{A}_1^\vee \otimes \mathcal{B}_i \otimes \mathcal{B}_{i-1} & \longrightarrow & \mathcal{B}_i \otimes \mathcal{B}_i &
\end{array}$$

which are bounded ($\mathcal{B}$ is positively graded) and whose rows are just Priddy's resolution $P^\bullet$ in various degrees and thus the total complex of the above direct summand of $D^{\bullet\bullet}$ is quasi-isomorphic to $\mathcal{A}_0^\vee \otimes \mathcal{B}_{2i} \otimes \mathcal{B}_0 = \mathcal{B}_{2i}$. Thus $Tot^\bullet(D^{\bullet\bullet})$ is quasi-isomorphic to $\bigoplus_i \mathcal{B}_{2i}$. □

The next step is to identify the kernel of the map $\Psi_{r-2} \boxtimes \mathcal{O}(-r+2) \to \Psi_{r-3} \boxtimes \mathcal{O}(-r+3)$. For this we have to talk in more detail about spinor bundles.
Let $\mathrm{Cliff}(\mathcal{E}) = \mathcal{A}/(h-1)\mathcal{A}$ be the Clifford bundle of the orthogonal vector bundle $\mathcal{E}$. This is just $\mathrm{Cliff}(\mathcal{E}) := \mathrm{T}^\bullet\, \mathcal{E}/I(\mathcal{E})$ where $I(\mathcal{E})$ is the bundle of ideals whose fibre at $x \in X$ is the two-sided ideal $I(\mathcal{E}(x))$ in $T^\bullet(\mathcal{E}(x))$ generated by the elements $e \otimes e - q(e)1$ for $e \in \mathcal{E}(x)$. $\mathrm{Cliff}(\mathcal{E})$ inherits a $\mathbb{Z}/2$-grading, $\mathrm{Cliff}(\mathcal{E}) = \mathrm{Cliff}^{\mathrm{even}}(\mathcal{E}) \oplus \mathrm{Cliff}^{\mathrm{odd}}(\mathcal{E})$.
For $\boxed{r+1 \text{ odd}}$ we will now make the following assumption (A):

> There exists a bundle of irreducible $\mathrm{Cliff}^{\mathrm{even}}(\mathcal{E})$-modules $S(\mathcal{E})$,
> self-dual up to twist by a line bundle L on X, i.e.
> $S(\mathcal{E})^\vee \simeq S(\mathcal{E}) \otimes L$,
> together with an isomorphism of sheaves of algebras on X
> $\mathrm{Cliff}(\mathcal{E}) \simeq \mathcal{E}nd(S(\mathcal{E})) \oplus \mathcal{E}nd(S(\mathcal{E}))$
> such that
> $\mathrm{Cliff}^{\mathrm{even}}(\mathcal{E}) \simeq \mathcal{E}nd(S(\mathcal{E}))$.

For $\boxed{r+1 \text{ even}}$ we assume (A'):

There exist bundles of irreducible $\mathrm{Cliff}^{\mathrm{even}}(\mathcal{E})$-modules
$S^+(\mathcal{E})$, $S^-(\mathcal{E})$, which for $\boxed{r+1 \equiv 0(4)}$ satisfy
$S^+(\mathcal{E})^\vee \simeq S^+(\mathcal{E}) \otimes L$
$S^-(\mathcal{E})^\vee \simeq S^-(\mathcal{E}) \otimes L$
and for $\boxed{r+1 \equiv 2(4)}$ satisfy
$S^+(\mathcal{E})^\vee \simeq S^-(\mathcal{E}) \otimes L$
$S^-(\mathcal{E})^\vee \simeq S^+(\mathcal{E}) \otimes L$, L a line bundle on X,
together with an isomorphism of sheaves on algebras on X
$\mathrm{Cliff}(\mathcal{E}) \simeq \mathcal{E}nd(S^+(\mathcal{E}) \oplus S^-(\mathcal{E}))$
such that
$\mathrm{Cliff}^{\mathrm{even}}(\mathcal{E}) \simeq \mathrm{E}nd(S^+(\mathcal{E})) \oplus \mathcal{E}nd(S^-(\mathcal{E}))$.

We will summarize this situation by saying that the orthogonal vector bundle $\mathcal{E}$ *admits spinor bundles* $S(\mathcal{E})$ resp. $S^+(\mathcal{E})$, $S^-(\mathcal{E})$.
Conditions (A) resp. (A') will be automatically satisfied in the applications in subsection 3.4.
Then for $\boxed{r+1 \text{ even}}$

$$\mathcal{M}^- := S^-(\mathcal{E}) \oplus S^+(\mathcal{E}) \oplus S^-(\mathcal{E}) \oplus \dots$$

and

$$\mathcal{M}^+ := S^+(\mathcal{E}) \oplus S^-(\mathcal{E}) \oplus S^+(\mathcal{E}) \oplus \dots$$

are graded left $\mathcal{A}$-modules (the grading starting from 0); one defines bundles Σ^+, Σ^- on $\mathcal{Q}$ by the requirement that

$$0 \to (\Sigma^\pm)^\vee \to L^\bullet(\mathcal{M}^\pm) \text{ for } \boxed{r+1 \equiv 0(\mathrm{mod}\, 4)},$$
$$0 \to (\Sigma^\mp)^\vee \to L^\bullet(\mathcal{M}^\pm) \text{ for } \boxed{r+1 \equiv 2(\mathrm{mod}\, 4)}$$

be exact.
For $\boxed{r+1 \text{ odd}}$ let $\mathcal{M}$ be the graded left $\mathcal{A}$- module (grading starting from 0)

$$\mathcal{M} := S(\mathcal{E}) \oplus S(\mathcal{E}) \oplus S(\mathcal{E}) \oplus \dots$$

and define the bundle Σ on $\mathcal{Q}$ by the requirement that

$$0 \to (\Sigma)^\vee \to L^\bullet(\mathcal{M})$$

be exact.
From the definition

$$\Sigma^\pm =: \Sigma^\pm(\mathcal{O}_{\mathcal{Q}}(-1)^\perp/\mathcal{O}_{\mathcal{Q}}(-1)) \text{ resp. } \Sigma =: \Sigma(\mathcal{O}_{\mathcal{Q}}(-1)^\perp/\mathcal{O}_{\mathcal{Q}}(-1))$$

are spinor bundles for the orthogonal vector bundle $\mathcal{O}_{\mathcal{Q}}(-1)^\perp/\mathcal{O}_{\mathcal{Q}}(-1)$ on $\mathcal{Q}$.

LEMMA 3.2.4. *The kernel*

$$\ker(\Psi_{r-2} \boxtimes \mathcal{O}(-r+2) \to \Psi_{r-3} \boxtimes \mathcal{O}(-r+3))$$

is equal to

(i) for $\boxed{r+1}$ *odd:*

$$(\Sigma(-1) \otimes \pi^* \, L^{-1}) \boxtimes \Sigma(-r+1)$$

(ii) for $\boxed{r+1 \equiv 2(\mathrm{mod}\, 4)}$*:*

$$((\Sigma^+(-1) \otimes \pi^* \, L^{-1}) \boxtimes \Sigma^+(-r+1)) \oplus ((\Sigma^-(-1) \otimes \pi^* \, L^{-1}) \boxtimes \Sigma^-(-r+1))$$

(iii) and for $\boxed{r+1 \equiv 0(\mathrm{mod}\, 4)}$*:*

$$((\Sigma^+(-1) \otimes \pi^* \, L^{-1}) \boxtimes \Sigma^-(-r+1)) \oplus ((\Sigma^-(-1) \otimes \pi^* \, L^{-1}) \boxtimes \Sigma^+(-r+1))$$

Proof. For $i \geq r$ $\mathcal{A}_i \stackrel{\mathrm{mult}(h)}{\longrightarrow} \mathcal{A}_{i+2}$ is an isomorphism because $(e_{i_1} \cdot \ldots \cdot e_{i_k} h^m)$, $1 \leq i_1 < \ldots < i_k \leq r+1$, $m \in \mathbb{N}$ is a local frame for $\mathcal{A}$ if $(e_1, \ldots, e_{r+1})$ is one for $\mathcal{E}$, and the map $\mathcal{A}_i \to \mathrm{Cliff}^{\mathrm{par}(i)}(\mathcal{E})$ induced by $\mathcal{A} \to \mathcal{A}/(h-1)\mathcal{A}$ is then an isomorphism where

$$\mathrm{par}(i) := \begin{cases} \text{even}, & i \equiv 0(\mathrm{mod}\, 2) \\ \text{odd}, & i \equiv 1(\mathrm{mod}\, 2) \end{cases} .$$

Because $L^\bullet(\mathcal{A}^\vee)$ is exact, Ψ_i is also the cokernel of

$$(*) \quad \ldots \to \pi^* \mathcal{A}_{i+3}^\vee \otimes \mathcal{O}_{\mathcal{Q}}(-3) \to \pi^* \mathcal{A}_{i+2}^\vee \otimes \mathcal{O}_{\mathcal{Q}}(-2) \to \pi^* \mathcal{A}_{i+1}^\vee \otimes \mathcal{O}_{\mathcal{Q}}(-1)$$

Since $\ker(\Psi_{r-2} \boxtimes \mathcal{O}(-r+2) \to \Psi_{r-3} \boxtimes \mathcal{O}(-r+3)) = \mathrm{coker}(\Psi_r \boxtimes \mathcal{O}(-r) \to \Psi_{r-1} \boxtimes \mathcal{O}(-r+1))$ we conclude that a left resolution of the kernel in lemma 3.2.4 is given by $Tot^\bullet(E^{\bullet\bullet})$ where $E^{\bullet\bullet}$ is the following double complex:

$$\begin{array}{ccccc}
 & & \vdots & & \vdots \\
 & & \downarrow & & \downarrow \\
\ldots \to & (\pi^* \mathrm{Cliff}^{\mathrm{par}(r+2)} \mathcal{E}^\vee(-2)) \boxtimes \mathcal{O}(-r) & \longrightarrow & (\pi^* \mathrm{Cliff}^{\mathrm{par}(r+1)} \mathcal{E}^\vee(-2)) \boxtimes \mathcal{O}(-r+1) \\
 & \downarrow & & \downarrow \\
\ldots \to & (\pi^* \mathrm{Cliff}^{\mathrm{par}(r+1)} \mathcal{E}^\vee(-1)) \boxtimes \mathcal{O}(-r) & \longrightarrow & (\pi^* \mathrm{Cliff}^{\mathrm{par}(r)} \mathcal{E}^\vee(-1)) \boxtimes \mathcal{O}(-r+1)
\end{array}$$

Here the columns (starting from the right) are the left resolutions $(*)$ of $\Psi_{r-1} \boxtimes \mathcal{O}(-r+1)$, $\Psi_r \boxtimes \mathcal{O}(-r)$, etc. and the rows are defined through the morphisms of complexes defining the differentials $\Psi_{r-1} \boxtimes \mathcal{O}(-r+1) \to \Psi_r \boxtimes \mathcal{O}(-r)$ etc. in the resolution $R^\bullet$. For odd $r+1$ we have $\mathrm{Cliff}^{odd}(\mathcal{E}) \simeq \mathrm{Cliff}^{even}(\mathcal{E}) \simeq \mathcal{E}nd(S(\mathcal{E})) \simeq S(\mathcal{E})^\vee \otimes S(\mathcal{E})$ whence our double complex becomes

$$\begin{array}{ccccc}
 & & \vdots & & \vdots \\
 & & \downarrow & & \downarrow \\
\dots & \longrightarrow & \pi^*S(\mathcal{E})^\vee(-2)\boxtimes\pi^*S(\mathcal{E})(-r) & \longrightarrow & \pi^*S(\mathcal{E})^\vee(-2)\boxtimes\pi^*S(\mathcal{E})(-r+1) \\
 & & \downarrow & & \downarrow \\
\dots & \longrightarrow & \pi^*S(\mathcal{E})^\vee(-1)\boxtimes\pi^*S(\mathcal{E})(-r) & \longrightarrow & \pi^*S(\mathcal{E})^\vee(-1)\boxtimes\pi^*S(\mathcal{E})(-r+1)
\end{array}$$

and is thus isomorphic as a double complex to $L^\bullet(\mathcal{M})^\vee(-1)\boxtimes(L^\bullet(\mathcal{M})^\vee(-r+1)\otimes\pi^*L^{-1})\simeq(L^\bullet(\mathcal{M})^\vee(-1)\otimes\pi^*L^{-1})\boxtimes L^\bullet(\mathcal{M})^\vee(-r+1)$, i.e. quasi-isomorphic to $(\Sigma(-1)\otimes\pi^*L^{-1})\boxtimes\Sigma(-r+1)$. The cases for even $r+1$ are considered similarly. □

Lemma 3.2.5. *Consider the following two ordered sets of sheaves on $\mathcal{Q}$:*

$$\begin{aligned}
\mathfrak{S} &= \{\Sigma(-r+1)\prec\mathcal{O}_{\mathcal{Q}}(-r+2)\prec\dots\prec\mathcal{O}_{\mathcal{Q}}(-1)\prec\mathcal{O}_{\mathcal{Q}}\} \quad (r+1 \text{ odd}),\\
\mathfrak{S}' &= \left\{\Sigma^+(-r+1)\prec\Sigma^-(-r+1)\prec\dots\prec\mathcal{O}_{\mathcal{Q}}(-1)\prec\mathcal{O}_{\mathcal{Q}}\right\} \quad (r+1 \text{ even}).
\end{aligned}$$

If $\mathcal{V}$, $\mathcal{V}_1$, $\mathcal{V}_2\in\mathfrak{S}$ (resp.: $\in\mathfrak{S}'$) with $\mathcal{V}_1\prec\mathcal{V}_2$, $\mathcal{V}_1\neq\mathcal{V}_2$, we have the following identities

$$\begin{aligned}
R^i\pi_*(\mathcal{V}\otimes\mathcal{V}^\vee) &= 0\,,\quad \forall i\neq 0,\\
R^i\pi_*(\mathcal{V}_1\otimes\mathcal{V}_2^\vee) = 0\ \forall i\in\mathbb{Z},\quad & R^i\pi_*(\mathcal{V}_2\otimes\mathcal{V}_1^\vee)=0\ \forall i\neq 0\,.
\end{aligned}$$

and the canonical morphism $R^0\pi_*(\mathcal{V}\otimes\mathcal{V}^\vee)\to\mathcal{O}_X$ is an isomorphism.

Proof. In the absolute case (where the base X is a point) this is a calculation in [Ka3] , prop. 4.9., based on Bott's theorem. The general assertion follows from this by the base change formula because the question is local on X and we can check this on open sets $U\subset X$ which cover X and over which $\mathcal{Q}$ is trivial. □

As in subsection 3.1, for $\mathcal{V}\in\mathfrak{S}$ (resp. $\in\mathfrak{S}'$), we can talk about subcategories $D^b(X)\otimes\mathcal{V}$ of $D^b(\mathcal{Q})$ as the images of $D^b(X)$ in $D^b(\mathcal{Q})$ under the functor $\pi^*(-)\otimes\mathcal{V}$.

Proposition 3.2.6. *Let $\mathcal{V}$, $\mathcal{V}_1,\mathcal{V}_2$ be as in lemma 3.2.5. The subcategories $D^b(X)\otimes\mathcal{V}$ of $D^b(\mathcal{Q})$ are all admissible subcategories. Moreover, for $A\in\mathrm{obj}(D^b(X)\otimes\mathcal{V}_2)$, $B\in\mathrm{obj}(D^b(X)\otimes\mathcal{V}_1)$ we have $R\mathrm{Hom}(A,B)=0$.*

Proof. Let $A=\pi^*A'\otimes\mathcal{V}_2$, $B=\pi^*B'\otimes\mathcal{V}_1$. Using lemma 3.2.5 and the projection formula we compute

$$\begin{aligned}
R^i\mathrm{Hom}(\pi^*A'\otimes\mathcal{V}_2,\pi^*B'\otimes\mathcal{V}_1) &\simeq R^i\mathrm{Hom}(\pi^*A',\pi^*B'\otimes\mathcal{V}_1\otimes\mathcal{V}_2^\vee)\\
&\simeq R^i\mathrm{Hom}(A',B'\otimes R\pi_*(\mathcal{V}_1\otimes\mathcal{V}_2^\vee))\simeq 0\,.
\end{aligned}$$

If we repeat the same calculation with $\mathcal{V}$ instead of $\mathcal{V}_1$ and $\mathcal{V}_2$ we find that $R^i\mathrm{Hom}(\pi^*A' \otimes \mathcal{V}, \pi^*B' \otimes \mathcal{V}) \simeq R^i\mathrm{Hom}(A', B')$. This shows that the categories $D^b(X) \otimes \mathcal{V}$ are all equivalent to $D^b(X)$ as triangulated subcategories of $D^b(\mathcal{Q})$. It follows from [BoKa] , prop. 2.6 and thm. 2.14, together with lemma 3.2.1 that the $D^b(X) \otimes \mathcal{V}$ are admissible subcategories of $D^b(\mathcal{Q})$. □

Theorem 3.2.7. *Let X be a smooth projective variety, $\mathcal{E}$ an orthogonal vector bundle on X, $\mathcal{Q} \subset \mathbb{P}(\mathcal{E})$ the associated quadric bundle, and let assumptions (A) resp. (A') above be satisfied.*
Then there is a semiorthogonal decomposition

$$D^b(\mathcal{Q}) = \big\langle D^b(X) \otimes \Sigma(-r+1), D^b(X) \otimes \mathcal{O}_{\mathcal{Q}}(-r+2), \\ \dots, D^b(X) \otimes \mathcal{O}_{\mathcal{Q}}(-1), D^b(X)\big\rangle$$

for $r+1$ odd and

$$D^b(\mathcal{Q}) = \big\langle D^b(X) \otimes \Sigma^+(-r+1), D^b(X) \otimes \Sigma^-(-r+1), \\ D^b(X) \otimes \mathcal{O}_{\mathcal{Q}}(-r+2), \dots, D^b(X) \otimes \mathcal{O}_{\mathcal{Q}}(-1), D^b(X)\big\rangle$$

for $r+1$ even.

Proof. By proposition 3.2.6 the categories in question are semiorthogonal and it remains to see that they generate $D^b(\mathcal{Q})$. For ease of notation we will consider the case of odd $r+1$, the case of even $r+1$ being entirely similar.
From lemmas 3.2.3 and 3.2.4 we know that in the situation of the fibre product

$$\begin{array}{ccc} \Delta \subset \mathcal{Q} \times_X \mathcal{Q} & \xrightarrow{p_2} & \mathcal{Q} \\ {\scriptstyle p_1}\downarrow & & {\scriptstyle \pi}\downarrow \\ \mathcal{Q} & \xrightarrow{\pi} & X \end{array}$$

we have a resolution

$$0 \to (\Sigma(-1) \otimes \pi^* L^{-1}) \boxtimes \Sigma(-r+1) \to \Psi_{r-2} \boxtimes \mathcal{O}_{\mathcal{Q}}(-r+2) \to \dots \\ \dots \to \Psi_1 \boxtimes \mathcal{O}(-1) \to \mathcal{O}_{\mathcal{Q}\times_X\mathcal{Q}} \to \mathcal{O}_\Delta \to 0$$

and tensoring this with $p_1^*\mathcal{F}$ ($\mathcal{F}$ a coherent sheaf on $\mathcal{Q}$)

$$0 \to (\Sigma(-1) \otimes \pi^* L^{-1} \otimes \mathcal{F}) \boxtimes \Sigma(-r+1) \to (\Psi_{r-2} \otimes \mathcal{F}) \boxtimes \mathcal{O}_{\mathcal{Q}}(-r+2) \to \dots \\ \dots \to (\Psi_1 \otimes \mathcal{F}) \boxtimes \mathcal{O}(-1) \to \mathcal{F} \boxtimes \mathcal{O}_{\mathcal{Q}} \to p_1^*\mathcal{F}|_\Delta \to 0$$

and applying $Rp_{2\,*}$ we obtain a spectral sequence

$$\begin{aligned} E_1^{ij} &= R^i p_{2\,*}((\Psi_{-j} \otimes \mathcal{F}) \boxtimes \mathcal{O}_{\mathcal{Q}}(j)) \quad -r+2 < j \le 0 \\ &= R^i p_{2\,*}((\Sigma(-1) \otimes \pi^* L^{-1} \otimes \mathcal{F}) \boxtimes \Sigma(-r+1)) \quad j = -r+1 \\ &= 0 \quad \text{otherwise} \end{aligned}$$

and $E_1^{ij} \Rightarrow R^{i+j}p_{2\,*}(p_1^*\mathcal{F}|_\Delta)$ which is $=\mathcal{F}$ for $i+j=0$ and $=0$ otherwise. But since cohomology commutes with flat base extension (cf. [EGA], III, §1, prop. 1.4.15), we have $R^ip_{2\,*}p_1^*\mathcal{G} \simeq \pi^*R^i\pi_*\mathcal{G}$ for any coherent $\mathcal{G}$ on $\mathcal{Q}$. This together with the projection formula shows that all E_1^{ij} belong to one of the admissible subcategories in the statement of theorem 3.2.7. This finishes the proof because $D^b(\mathcal{Q})$ is generated by the subcategory $Coh(\mathcal{Q})$. □

Corollary 3.2.8. *If $D^b(X)$ is generated by a complete exceptional sequence*

$$(E_1, \dots, E_n)\,,$$

then $D^b(\mathcal{Q})$ is generated by the complete exceptional sequence

$$(\pi^*E_1 \otimes \Sigma(-r+1), \dots, \pi^*E_n \otimes \Sigma(-r+1), \pi^*E_1 \otimes \mathcal{O}_{\mathcal{Q}}(-r+2), \dots, \pi^*E_n)$$

for $r+1$ odd and

$$\big(\pi^*E_1 \otimes \Sigma^+(-r+1), \dots, \pi^*E_n \otimes \Sigma^+(-r+1), \dots, \pi^*E_1 \otimes \Sigma^-(-r+1), \\ \dots, \pi^*E_n \otimes \Sigma^-(-r+1), \pi^*E_1 \otimes \mathcal{O}_{\mathcal{Q}}(-r+2), \dots, \pi^*E_1, \dots, \pi^*E_n\big)$$

for $r+1$ even.

Proof. Using lemma 3.2.5, one proves this analogously to corollary 3.1.2; we omit the details. □

3.3 Application to varieties of isotropic flags in a symplectic vector space

We first fix some notation: Let V be a $\mathbb{C}$-vector space of even dimension $2n$ with a nondegenerate skew symmetric bilinear form $\langle\cdot,\cdot\rangle$. For $1 \le k_1 < \ldots < k_t \le n$ we denote $\mathrm{IFlag}(k_1,\dots,k_t;V) := \{(L_{k_1},\dots,L_{k_t}) \mid L_{k_1} \subset \ldots L_{k_t} \subset V$ isotropic subspaces of V with $\dim L_{k_j} = k_j,\ 1 \le j \le t\}$ the (partial) flag variety of isotropic flags of type $(k_1,\dots,k_t)$ in V; moreover, for $1 \le k \le n$, put $\mathrm{IGrass}(k,V) := \mathrm{IFlag}(k;V)$, the Grassmann manifold of isotropic k-planes in V. As usual, we have the tautological flag of subbundles $\mathcal{R}_{k_1} \subset \ldots \subset \mathcal{R}_{k_t} \subset V \otimes \mathcal{O}_{\mathrm{IFlag}(k_1,\dots,k_t;V)}$ on $\mathrm{IFlag}(k_1,\dots,k_t;V)$ and the tautological subbundle $\mathcal{R}$ on $\mathrm{IGrass}(k,V)$.

Remark 3.3.1. Via the projection $\mathrm{IFlag}(k_1,\dots,k_t;V) \to \mathrm{IGrass}(k_t,V)$, the variety $\mathrm{IFlag}(k_1,\dots,k_t;V)$ identifies with $\mathrm{Flag}_{\mathrm{IGrass}(k_t,V)}(k_1,\dots,k_{t-1};\mathcal{R})$, the relative variety of flags of type $(k_1,\dots,k_{t-1})$ in the fibres of the tautological subbundle $\mathcal{R}$ on $\mathrm{IGrass}(k_t,V)$. Therefore, by theorem 3.1.5, if we want to exhibit complete exceptional sequences in the derived categories of coherent sheaves on all possible varieties of (partial) isotropic flags in V, we can reduce to finding them on isotropic Grassmannians. Thus we will focus on the latter in the sequel.

Now look at the following diagram (the notation will be explained below)

$$\begin{array}{ccc}
\mathrm{IFlag}(1,2,\dots,k-1,k;V)\simeq\mathbb{P}(\mathcal{E}_{k-1})\simeq\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,2,\dots,k;\mathcal{R}) & & \\
\downarrow \pi_{k-1} & & \\
\mathrm{IFlag}(1,2,\dots,k-1;V)\simeq\mathbb{P}(\mathcal{E}_{k-2}) & & \\
\downarrow \pi_{k-2} & & \\
\vdots & \searrow \pi & \\
\downarrow \pi_2 & & \\
\mathrm{IFlag}(1,2;V)\simeq\mathbb{P}(\mathcal{E}_1) & & \\
\downarrow \pi_1 & & \\
\mathrm{IFlag}(1;V)\simeq\mathbb{P}(V) & & \mathrm{IGrass}(k,V)
\end{array}$$

Since for $1\le i\le j\le k-1$ the i-dimensional tautological subbundle on $\mathrm{IFlag}(1,2,\dots,j;V)$ pulls back to the i-dimensional tautological subbundle on $\mathrm{IFlag}(1,2,\dots,j+1;V)$ under π_j, we denote all of them by the same symbol $\mathcal{R}_i$ regardless of which space they live on, if no confusion can arise.
Since any line in V is isotropic, the choice of a 1-dimensional isotropic $L_1\subset V$ comes down to picking a point in $\mathbb{P}(V)$ whence the identification $\mathrm{IFlag}(1;V)\simeq\mathbb{P}(V)$ above; the space $L_1^{\perp}/L_1$ is again a symplectic vector space with skew form induced from $\langle\cdot,\cdot\rangle$ on V, and finding an isotropic plane containing L_1 amounts to choosing a line L_2/L_1 in $L_1^{\perp}/L_1$. Thus $\mathrm{IFlag}(1,2;V)$ is a projective bundle $\mathbb{P}(\mathcal{E}_1)$ over $\mathrm{IFlag}(1;V)$ with $\mathcal{E}_1=\mathcal{R}_1^{\perp}/\mathcal{R}_1$, and on $\mathbb{P}(\mathcal{E}_1)\simeq\mathrm{IFlag}(1,2;V)$ we have $\mathcal{O}_{\mathcal{E}_1}(-1)\simeq\mathcal{R}_2/\mathcal{R}_1$. Of course, $\mathrm{rk}\,\mathcal{E}_1=2n-2$.
Continuing this way, we successively build the whole tower of projective bundles over $\mathbb{P}(V)$ in the above diagram where

$$\mathcal{E}_j\simeq\mathcal{R}_j^{\perp}/\mathcal{R}_j\,,\quad j=1,\dots,k-1\,,\quad \mathrm{rk}\,\mathcal{E}_j=2n-2j$$
$$\text{and}\quad \mathcal{O}_{\mathcal{E}_j}(-1)\simeq\mathcal{R}_{j+1}/\mathcal{R}_j\,.$$

Moreover, $\mathrm{IFlag}(1,2,\dots,k-1,k;V)$ is just $\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,\dots,k;\mathcal{R})$, the relative variety of complete flags in the fibres of the tautological subbundle $\mathcal{R}$ on $\mathrm{IGrass}(k,V)$; the flag of tautological subbundles in $V\otimes\mathcal{O}_{\mathrm{IFlag}(1,\dots,k;V)}$ on $\mathrm{IFlag}(1,\dots,k;V)$ and the flag of relative tautological subbundles in $\pi^*\mathcal{R}$ on $\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,2,\dots,k;\mathcal{R})$ correspond to each other under this isomorphism, and we do not distinguish them notationally.
For $\lambda=(\lambda_1,\dots,\lambda_k)\in\mathbb{Z}^k$ define the line bundle $\mathcal{L}(\lambda)$ on the variety $\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,\dots,k;\mathcal{R})$ by

$$\mathcal{L}(\lambda):=(\mathcal{R}_1)^{\otimes(-\lambda_1)}\otimes(\mathcal{R}_2/\mathcal{R}_1)^{\otimes(-\lambda_2)}\otimes\dots\otimes(\pi^*\mathcal{R}/\mathcal{R}_{k-1})^{\otimes(-\lambda_k)}\,.$$

(This notation is consistent with that of $\mathcal{L}(\chi)$ in subsection 2.2 which will be further explained in the comment after the proof of lemma 3.3.2 below).

Repeatedly applying corollary 3.1.2 to the above tower of projective bundles, we find that the following sheaves constitute a complete exceptional sequence in $D^b(Coh\,(\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,\dots,k;\mathcal{R})))$:

$$(\sharp)\qquad (\mathcal{L}(\lambda)) \quad \text{with} \quad \begin{aligned} -2n+1 &\le \lambda_1 \le 0,\\ -2n+3 &\le \lambda_2 \le 0,\\ &\vdots\\ -2n+2k-1 &\le \lambda_k \le 0. \end{aligned}$$

Here $\mathcal{L}(\lambda)$ precedes $\mathcal{L}(\mu)$ according to the ordering of the exceptional sequence iff $(\lambda_k, \lambda_{k-1}, \dots, \lambda_1) \prec (\mu_k, \mu_{k-1}, \dots, \mu_1)$ where $\prec$ is the lexicographic order on $\mathbb{Z}^k$.

Let us record here the simple

Lemma 3.3.2. *The set of full direct images $R\pi_*\mathcal{L}(\lambda)$, as $\mathcal{L}(\lambda)$ varies among the bundles $(\sharp)$, generates the derived category $D^b(Coh(\mathrm{IGrass}(k,V)))$.*

Proof. As in lemma 3.2.1, $R\pi_*\mathcal{O}_{\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,\dots,k;\mathcal{R})} \simeq \mathcal{O}_{\mathrm{IGrass}(k,V)}$, and $R\pi_* \circ \pi^*$ is isomorphic to the identity functor on $D^b(Coh(\mathrm{IGrass}(k,V)))$ by the projection formula. Thus, since the bundles in $(\sharp)$ generate the derived category upstairs, if E is an object in $D^b(Coh(\mathrm{IGrass}(k,V)))$, π^*E will be isomorphic to an object in the smallest full triangulated subcategory containing the objects $(\sharp)$, i.e. starting from the set $(\sharp)$ and repeatedly enlarging it by taking finite direct sums, shifting in cohomological degree and completing distinguished triangles by taking a mapping cone, we can reach an object isomorphic to π^*E. Hence it is clear that the objects $R\pi_*\mathcal{L}(\lambda)$ will generate the derived category downstairs because $R\pi_*\pi^*E \simeq E$. □

Now the fibre of $\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,\dots,k;\mathcal{R})$ over a point $x \in \mathrm{IGrass}(k,V)$ is just the full flag variety $\mathrm{Flag}(1,\dots,k;\mathcal{R}(x))$ which is a quotient of $\mathrm{GL}_k\mathbb{C}$ by a Borel subgroup B; the $\lambda \in \mathbb{Z}^k$ can be identified with weights or characters of a maximal torus $H \subset B$ and the restriction of $\mathcal{L}(\lambda)$ to the fibre over x is just the line bundle associated to the character λ, i.e. $\mathrm{GL}_k\mathbb{C} \times_B \mathbb{C}_{-\lambda}$, where $\mathbb{C}_{-\lambda}$ is the one-dimensional B-module in which the torus H acts via the character $-\lambda$ and the unipotent radical $R_u(B)$ of B acts trivially, and $\mathrm{GL}_k\mathbb{C} \times_B \mathbb{C}_{-\lambda} := \mathrm{GL}_k\mathbb{C} \times \mathbb{C}_{-\lambda}/\{(g,v) \sim (gb^{-1}, bv)\,,\ b \in B\}$. Thus we can calculate the $R\pi_*\mathcal{L}(\lambda)$ by the following (relative) version of Bott's theorem (cf. [Wey], thm. 4.1.4 or [Akh], §4.3 for a full statement):

Let $\varrho := (k-1, k-2, \dots, 0)$ (the half sum of the positive roots) and let $W = \mathfrak{S}_k$, the symmetric group on k letters (the Weyl group), act on $\mathbb{Z}^k$ by permutation of entries:

$$\sigma((\lambda_1,\dots,\lambda_k)) := \left(\lambda_{\sigma(1)},\dots,\lambda_{\sigma(k)}\right)\,.$$

The dotted action of $\mathfrak{S}_k$ on $\mathbb{Z}^k$ is defined by

$$\sigma^\bullet(\lambda) := \sigma(\lambda+\varrho) - \varrho\,.$$

Then the theorem of Bott asserts in our case:

- Either there exists $\sigma \in \mathfrak{S}_k$, $\sigma \neq \mathrm{id}$, such that $\sigma^\bullet(\lambda) = \lambda$. Then $R^i\pi_*\mathcal{L}(\lambda) = 0 \; \forall i \in \mathbb{Z}$;
- or there exists a unique $\sigma \in \mathfrak{S}_k$ such that $\sigma^\bullet(\lambda) =: \mu$ is non-increasing (i.e., μ is a dominant weight). Then

$$R^i\pi_*\mathcal{L}(\lambda) = 0 \quad \text{for} \quad i \neq l(\sigma)\,,$$
$$R^{l(\sigma)}\pi_*\mathcal{L}(\lambda) = \Sigma^\mu \mathcal{R}^\vee\,,$$

  where $l(\sigma)$ is the length of the permutation σ (the smallest number of transpositions the composition of which gives σ) and Σ^μ is the Schur functor.

As a first consequence, note that the objects $R\pi_*\mathcal{L}(\lambda)$ all belong -up to shift in cohomological degree- to the abelian subcategory of $D^b(Coh(\mathrm{IGrass}(k,V)))$ consisting of coherent sheaves. We would like to determine the homogeneous bundles that arise as direct images of the bundles ($\sharp$) in this way. The following theorem gives us some information (though it is not optimal).

Theorem 3.3.3. *The derived category $D^b(Coh(\mathrm{IGrass}(k,V)))$ is generated by the bundles $\Sigma^\nu\mathcal{R}$, where ν runs over Young diagrams Y which satisfy*

$$(\text{number of columns of } Y) \leq 2n-k\,,$$
$$k \geq (\text{number of rows of } Y) \geq (\text{number of columns of } Y) - 2(n-k)\,.$$

Proof. Note that if λ satisfies the inequalities in ($\sharp$), then for $\delta := \lambda + \varrho$ we have

$$(\sharp\sharp) \qquad \begin{aligned} -(2n-k) &\leq \delta_1 \leq k-1\,,\\ -(2n-k-1) &\leq \delta_2 \leq k-2\,,\\ &\;\vdots\\ -(2n-2k+1) &\leq \delta_k \leq 0\,. \end{aligned}$$

First of all one remarks that for $\sigma^\bullet(\lambda) = \sigma(\delta) - \varrho$ to be non-increasing, it is necessary and sufficient that $\sigma(\delta)$ be strictly decreasing. We assume this to be the case in the following. Since the maximum possible value for $\sigma(\delta)_1$ is $k-1$, and the minimum possible value for $\sigma(\delta)_k$ is $-(2n-k)$, we find that for $\sigma^\bullet(\lambda) =: \mu$

$$0 \geq \mu_1 \geq \ldots \geq \mu_k \geq -(2n-k)\,;$$

putting $\nu = (\nu_1, \ldots, \nu_k) := (-\mu_k, -\mu_{k-1}, \ldots, -\mu_1)$ and noticing that $\Sigma^\mu\mathcal{R}^\vee \simeq \Sigma^\nu\mathcal{R}$, we find that the direct images $R^i\pi_*\mathcal{L}(\lambda)$, $i \in \mathbb{Z}$, $\mathcal{L}(\lambda)$ as in ($\sharp$), will form a subset of the set of bundles $\Sigma^\nu\mathcal{R}$ on $\mathrm{IGrass}(k,V)$ where ν runs over the set of Young diagrams with no more than $2n-k$ columns and no more than k rows.

But in fact we are only dealing with a proper subset of the latter: Suppose that

$$\sigma(\delta)_k = -(2n-k-a+1)\,, \quad 1 \le a \le k-1\,.$$

Then the maximum possible value for $\sigma(\delta)_a$ is $k-a-1$. For in any case an upper bound for $\sigma(\delta)_a$ is $k-a$ because $\sigma(\delta)_1$ can be at most $k-1$ and the sequence $\sigma(\delta)$ is strictly decreasing. But in case this upper bound for $\sigma(\delta)_a$ is attained, the sequence $\sigma(\delta)$ must start with

$$\sigma(\delta)_1 = k-1\,,\ \sigma(\delta)_2 = k-2\,, \dots,\ \sigma(\delta)_a = k-a\,,$$

in other words, we can only have

$$\sigma(\delta)_1 = \delta_1\,, \dots,\ \sigma(\delta)_a = \delta_a\,.$$

But this is impossible since $\delta_{a+1}, \dots, \delta_k$ are all $\ge -(2n-k-a) > -(2n-k-a+1)$ and thus we could not have $\sigma(\delta)_k = -(2n-k-a+1)$. Hence $\sigma(\delta)_a$ is at most $k-a-1$, that is to say in $\sigma^{\bullet}(\lambda) = \sigma(\delta) - \varrho = \mu$ we have $\mu_a = \sigma(\delta)_a - (k-a) < 0$; or in terms of $\nu = (-\mu_k, \dots, -\mu_1)$ we can say that if the Young diagram $Y(\nu)$ of ν has $2n-k-a+1$ columns, $1 \le a \le k-1$, it must have at least $k-a+1$ rows; or that the Young diagram $Y(\nu)$ satisfies

$$(\text{number of rows of } Y(\nu)) \ge (\text{number of columns of } Y(\nu)) - 2(n-k)$$

where the inequality is meaningless if the number on the right is ≤ 0. Thus by lemma 3.3.2 this concludes the proof of theorem 3.3.3. □

Remark 3.3.4. By thm. 2.2.2, in $D^b(Coh(\mathrm{Grass}(k,V)))$ there is a complete exceptional sequence consisting of the $\Sigma^{\tilde{\nu}}\tilde{\mathcal{R}}$ where $\tilde{\mathcal{R}}$ is the tautological subbundle on $\mathrm{Grass}(k,V)$ and $\tilde{\nu}$ runs over Young diagrams with at most $2n-k$ columns and at most k rows. Looking at $\mathrm{IGrass}(k,V)$ as a subvariety $\mathrm{IGrass}(k,V) \subset \mathrm{Grass}(k,V)$ we see that the bundles in theorem 3.3.3 form a proper subset of the restrictions of the $\Sigma^{\tilde{\nu}}\tilde{\mathcal{R}}$ to $\mathrm{IGrass}(k,V)$.

Before making the next remark we have to recall two ingredients in order to render the following computations transparent:
The first is the Littlewood-Richardson rule to decompose $\Sigma^{\lambda} \otimes \Sigma^{\mu}$ into irreducible factors where λ, μ are Young diagrams (cf. [FuHa], §A.1). It says the following: Label each box of μ with the number of the row it belongs to. Then expand the Young diagram λ by adding the boxes of μ to the rows of λ subject to the following rules:

(a) The boxes with labels $\le i$ of μ together with the boxes of λ form again a Young diagram;

(b) No column contains boxes of μ with equal labels.

(c) When the integers in the boxes added are listed from right to left and from top down, then, for any $0 \le s \le$ (number of boxes of μ), the first s entries of the list satisfy: Each label l ($1 \le l \le$ (number of rows of μ)-1) occurs at least as many times as the label $l+1$.

Then the multiplicity of Σ^ν in $\Sigma^\lambda \otimes \Sigma^\mu$ is the number of times the Young diagram ν can be obtained by expanding λ by μ according to the above rules, forgetting the labels.
The second point is the calculation of the cohomology of the bundles $\Sigma^\lambda\mathcal{R}$ on the variety $\mathrm{IGrass}(k,V)$, V a $2n$-dimensional symplectic vector space (cf. [Wey], cor. 4.3.4). Bott's theorem gives the following prescription:
Look at the sequence

$$\mu = (-\lambda_k, -\lambda_{k-1}, \dots, -\lambda_1, 0, \dots, 0) \in \mathbb{Z}^n$$

considered as a weight of the root system of type C_n. Let W be the Weyl group of this root system which is a semi-direct product of $(\mathbb{Z}/2\mathbb{Z})^n$ with the symmetric group $\mathfrak{S}_n$ and acts on weights by permutation and sign changes of entries. Let $\varrho := (n, n-1, \dots, 1)$ be the half sum of the positive roots for type C_n. The dotted action of W on weights is defined as above by $\sigma^\bullet(\mu) := \sigma(\mu+\varrho)-\varrho$. Then

- either there is $\sigma \in W$, $\sigma \neq \mathrm{id}$, such that $\sigma^\bullet(\mu) = \mu$. then all cohomology groups
$$H^\bullet(\mathrm{IGrass}(k,V), \Sigma^\lambda\mathcal{R}) = 0\,.$$
- or there is a unique $\sigma \in W$ such that $\sigma^\bullet(\mu) =: \nu$ is dominant (a non-increasing sequence of non-negative integers). Then the only non-zero cohomology group is
$$H^{l(\sigma)}(\mathrm{IGrass}(k,V), \Sigma^\lambda\mathcal{R}) = V_\nu\,,$$
where $l(\sigma)$ is the length of the Weyl group element σ and V_ν is the space of the irreducible representation of $\mathrm{Sp}_{2n}\mathbb{C}$ with highest weight ν.

Remark 3.3.5. The $R^i\pi_*\mathcal{L}(\lambda)$, $i \in \mathbb{Z}$, $\mathcal{L}(\lambda)$ as in ($\sharp$), are not in general exceptional: For example, take $k = n = 3$, so that we are dealing with $\mathrm{IGrass}(3,V)$, the Lagrangian Grassmannian of maximal isotropic subspaces in a 6-dimensional symplectic space V. Then $\mathcal{L}((0,-3,0))$ is in ($\sharp$). Adding $\varrho = (2,1,0)$ to $(0,-3,0)$ we get $(2,-2,0)$ and interchanging the last two entries and subtracting ϱ again, we arrive at $(0,-1,-2)$ which is non-increasing whence

$$R^1\pi_*\mathcal{L}((0,-3,0)) = \Sigma^{2,1,0}\mathcal{R}\,,$$

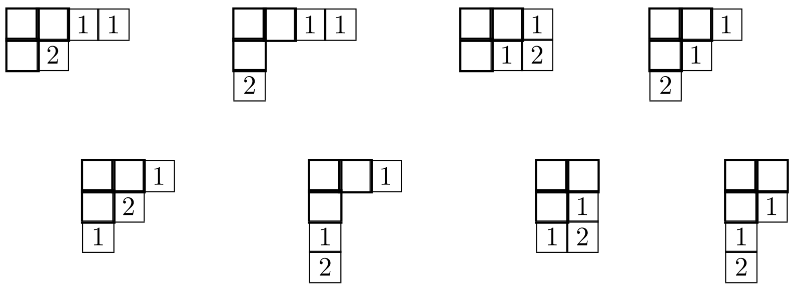
all other direct images being 0. To calculate

$$\begin{aligned}\mathrm{Ext}^\bullet\left(\Sigma^{2,1,0}\mathcal{R}, \Sigma^{2,1,0}\mathcal{R}\right) &= H^\bullet\left(\mathrm{IGrass}(3,V), \Sigma^{2,1,0}\mathcal{R}\otimes\Sigma^{0,-1,-2}\mathcal{R}\right)\\ &= H^\bullet\left(\mathrm{IGrass}(3,V), \Sigma^{2,1,0}\mathcal{R}\otimes\Sigma^{2,1,0}\mathcal{R}\otimes\left(\bigwedge^3\mathcal{R}^\vee\right)^{\otimes 2}\right)\end{aligned}$$

we use the Littlewood-Richardson rule and Bott's theorem as recalled above: One gets that

$$\begin{aligned}\Sigma^{2,1,0}\mathcal{R}\otimes\Sigma^{0,-1,-2}\mathcal{R} &= \Sigma^{2,0,-2}\mathcal{R}\oplus\Sigma^{2,-1,-1}\mathcal{R}\oplus\Sigma^{1,1,-2}\mathcal{R}\\ &\oplus(\Sigma^{1,0,-1}\mathcal{R})^{\oplus 2}\oplus\Sigma^{0,0,0}\mathcal{R}\end{aligned}$$

in view of the fact that if we expand $\lambda = (2,1,0)$ by $\mu = (2,1,0)$ we get the following Young diagrams according to the Littlewood-Richardson rule:



Thus calculating the cohomology of $\Sigma^{2,1,0}\mathcal{R} \otimes \Sigma^{0,-1,-2}\mathcal{R}$ by the version of Bott's theorem recalled above one finds that

$$\mathrm{Hom}\left(\Sigma^{2,1,0}\mathcal{R}, \Sigma^{2,1,0}\mathcal{R}\right) = \mathbb{C} \quad \mathrm{Ext}^1\left(\Sigma^{2,1,0}\mathcal{R}, \Sigma^{2,1,0}\mathcal{R}\right) = V_{1,1,0} \oplus V_{2,0,0} \neq 0$$

the other Ext groups being 0.

Next we want to show by some examples that, despite the fact that theorem 3.3.3 does not give a complete exceptional sequence on $\mathrm{IGrass}(k,V)$, it is sometimes -for small values of k and n- not so hard to find one with its help.

Example 3.3.6. Choose $k = n = 2$, i.e. look at $\mathrm{IGrass}(2,V)$, $\dim V = 4$. Remarking that $\mathcal{O}(1)$ on $\mathrm{IGrass}(2,V)$ in the Plücker embedding equals $\bigwedge^{\mathrm{top}} \mathcal{R}^\vee$ and applying theorem 3.3.3 one finds that the following five sheaves generate $D^b(Coh(\mathrm{IGrass}(2,V)))$:

$$\mathcal{O},\ \mathcal{R},\ \bigwedge^2 \mathcal{R} = \mathcal{O}(-1),\ \Sigma^{2,1}\mathcal{R} = \mathcal{R}(-1),\ \mathcal{O}(-2);$$

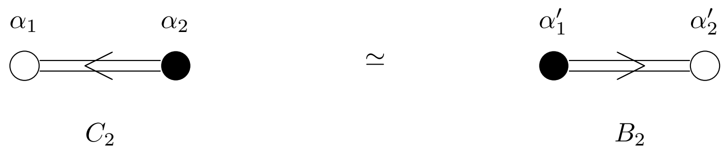
The real extra credit that one receives from working on the Lagrangian Grassmannian $\mathrm{IGrass}(2,V)$ is that $\mathcal{R} = \mathcal{R}^\perp$ and the tautological factor bundle can be identified with $\mathcal{R}^\vee \simeq \mathcal{R}(1)$, i.e. one has an exact sequence

$$0 \longrightarrow \mathcal{R} \longrightarrow V \otimes \mathcal{O} \longrightarrow \mathcal{R}(1) \longrightarrow 0.$$

Twisting by $\mathcal{O}(-1)$ in this sequence shows that of the above five sheaves, $\mathcal{R}(-1)$ is in the full triangulated subcategory generated by the remaining four; moreover, it is a straightforward computation with Bott's theorem that

$$(\mathcal{O}(-2),\ \mathcal{O}(-1),\ \mathcal{R},\ \mathcal{O})$$

is a strong exceptional sequence in $D^b(Coh(\mathrm{IGrass}(2,V)))$; but this is also complete, i.e., it generates this derived category by the preceding considerations. In fact, this does not come as a surprise. IGrass$(2, V)$ is isomorphic to a quadric hypersurface in $\mathbb{P}^4$, more precisely it is a hyperplane section of the Plücker quadric Grass$(2, V) \subset \mathbb{P}^5$. By [Ott], thm. 1.4 and ex. 1.5, the spinor bundles on the Plücker quadric are the dual of the tautological subbundle and the tautological factor bundle on Grass$(2, V)$ and these both restrict to the spinor bundle $\mathcal{R}^\vee$ on IGrass$(2, V) \subset \mathbb{P}^4$ (let us renew here the warning from subsection 2.2 that the spinor bundles in [Ott] are the duals of the bundles that we choose to call spinor bundles in this work). We thus recover the result of [Ka3], §4, in a special case. Note that the identification of IGrass$(2, V)$ with a quadric hypersurface in $\mathbb{P}^4$ also follows more conceptually from the isomorphism of marked Dynkin diagrams



corresponding to the isomorphism $\mathrm{Sp}_4\mathbb{C}/P(\alpha_2) \simeq \mathrm{Spin}_5\mathbb{C}/P(\alpha_1')$ (cf. [Stei], prop. p. 16 and [FuHa], §23.3). Recalling the one-to-one correspondence between conjugacy classes of parabolic subgroups of a simple complex Lie group G and subsets of the set of simple roots, the notations $P(\alpha_2)$ resp. $P(\alpha_1')$ are self-explanatory.

Example 3.3.7. Along the same lines which are here exposed in general, A. V. Samokhin treated in [Sa] the particular case of IGrass$(3, V)$, $\dim V = 6$, and using the identification of the tautological factor bundle with $\mathcal{R}^\vee$ on this Lagrangian Grassmannian and the exact sequence

$$0 \longrightarrow \mathcal{R} \longrightarrow V \otimes \mathcal{O} \longrightarrow \mathcal{R}^\vee \longrightarrow 0\,.$$

together with its symmetric and exterior powers found the following strong complete exceptional sequence for $D^b(Coh(\mathrm{IGrass}(3, V)))$:

$$(\mathcal{R}(-3),\, \mathcal{O}(-3),\, \mathcal{R}(-2),\, \mathcal{O}(-2),\, \mathcal{R}(-1),\, \mathcal{O}(-1),\, \mathcal{R},\, \mathcal{O})$$

and we refer to [Sa] for details of the computation.

In general I conjecture that on any Lagrangian Grassmannian IGrass(n, V), $\dim V = 2n$, every "relation" between the bundles in theorem 3.3.3 in the derived category $D^b(Coh\,\mathrm{IGrass}(n, V))$ (that is to say that one of these bundles is in the full triangulated subcategory generated by the remaining ones) should follow using the Schur complexes (cf. [Wey], section 2.4) derived from the exact sequence $0 \to \mathcal{R} \to V \otimes \mathcal{O} \to \mathcal{R}^\vee \to 0$ (and the Littlewood-Richardson rule).
Let us conclude this subsection by giving an example which, though we do not find a complete exceptional sequence in the end, may help to convey the sort of combinatorial difficulties that one encounters in general.

EXAMPLE 3.3.8. For a case of a non-Lagrangian isotropic Grassmannian, look at $\mathrm{IGrass}(2,V)$, $\dim V = 6$. Theorem 3.3.3 says that $D^b(Coh\,\mathrm{IGrass}(2,V))$ is generated by the following 14 bundles:

$$(*) \qquad \mathrm{Sym}^a\,\mathcal{R}(-b)\,, \quad 0 \le a \le 3\,, \quad 0 \le b \le 4-a\,.$$

By corollary 2.3.7, the number of terms in a complete exceptional sequence must be 12 in this case (in general for $\mathrm{IGrass}(k,V) = \mathrm{Sp}_{2n}\,\mathbb{C}/P(\alpha_k)$, $\dim V = 2n$, one has that $W^{P(\alpha_k)}$, the set of minimal representatives of the quotient $W/W_{P(\alpha_k)}$ can be identified with k-tuples of integers $(a_1,\dots,a_k)$ such that

$$1 \le a_1 < a_2 < \ldots < a_k \le 2n \text{ and}$$
$$\text{for } 1 \le i \le 2n\,,\ \text{if } i \in \{a_1,\dots,a_k\} \quad \text{then } 2n+1-i \notin \{a_1,\dots,a_k\}$$

(see [BiLa], §3.3) and these are

$$\frac{2n(2n-2)\dots(2n-2(k-1))}{1\cdot 2\cdot \dots \cdot k} = 2^k\binom{n}{k}$$

in number). Without computation, we know by a theorem of Ramanan (cf. [Ot2], thm 12.3) that the bundles in $(*)$ are all simple since they are associated to irreducible representations of the subgroup $P(\alpha_2) \subset \mathrm{Sp}_6\,\mathbb{C}$.
Moreover the bundles

$$\Sigma^{c_1,c_2}\mathcal{R} \ \text{ and } \ \Sigma^{d_1,d_2}\mathcal{R} \ \text{ with } 0 \le c_2 \le c_1 \le 3\,,\ 0 \le d_2 \le d_1 \le 3$$

have no higher extension groups between each other: By the Littlewood-Richardson rule, every irreducible summand $\Sigma^{e_1,e_2}\mathcal{R}$ occurring in the decomposition of $\Sigma^{d_1,d_2}\mathcal{R} \otimes \Sigma^{c_1,c_2}\mathcal{R}^\vee$ satisfies $-3 \le e_2 \le e_1 \le 3$ and hence for $\mu := (-e_2,-e_1,0) \in \mathbb{Z}^3$ and $\varrho = (3,2,1)$ we find that $\mu+\varrho$ is either a strictly decreasing sequence of positive integers or two entries in $\mu+\varrho$ are equal up to sign or one entry in $\mu+\varrho$ is 0. In each of these cases, Bott's theorem as recalled before remark 3.3.5 tells us that $H^i(\mathrm{IGrass}(2,V),\Sigma^{e_1,e_2}\mathcal{R}) = 0\ \forall i > 0$. Combining this remark with the trivial observation that for $\mathrm{Sym}^a\mathcal{R}(-b)$, $\mathrm{Sym}^c\mathcal{R}(-d)$ in the set $(*)$ with $b,d \ge 1$ we have

$$\mathrm{Ext}^i(\mathrm{Sym}^a\mathcal{R}(-b),\mathrm{Sym}^c\mathcal{R}(-d)) = \mathrm{Ext}^i(\mathrm{Sym}^a\mathcal{R}(-b+1),\mathrm{Sym}^c\mathcal{R}(-d+1)) \ \ \forall i$$

we infer that for $\mathcal{A}$, $\mathcal{B}$ bundles in the set $(*)$ we can only have

$$\mathrm{Ext}^j(\mathcal{A},\mathcal{B}) \neq 0, \ \text{ some } \ j > 0$$

if $\mathcal{A}$ occurs in the set

$$S_1 := \{\mathcal{O}(-4),\ \mathcal{R}(-3),\ \mathrm{Sym}^2\mathcal{R}(-2),\ \mathrm{Sym}^3\mathcal{R}(-1)\}$$

and $\mathcal{B}$ is in the set

$$S_2 := \{\mathcal{O},\ \mathcal{R},\ \mathrm{Sym}^2\mathcal{R},\ \mathrm{Sym}^3\mathcal{R}\}$$

or vice versa. By explicit calculation (which amounts to applying Bott's theorem another 32 more times) we find that the only non-vanishing higher extension groups between two bundles in $(*)$ are the following:

$$\mathrm{Ext}^1(\mathrm{Sym}^3\mathcal{R}, \mathcal{R}(-3)) = \mathbb{C}, \ \ \mathrm{Ext}^1(\mathrm{Sym}^2\mathcal{R}, \mathrm{Sym}^2\mathcal{R}(-2)) = \mathbb{C}$$
$$\mathrm{Ext}^1(\mathrm{Sym}^3\mathcal{R}, \mathrm{Sym}^2\mathcal{R}(-2)) = V, \ \ \mathrm{Ext}^1(\mathcal{R}, \mathrm{Sym}^3\mathcal{R}(-1)) = \mathbb{C}$$
$$\mathrm{Ext}^1(\mathrm{Sym}^2\mathcal{R}, \mathrm{Sym}^3\mathcal{R}(-1)) = V, \ \ \mathrm{Ext}^1(\mathrm{Sym}^3\mathcal{R}, \mathrm{Sym}^3\mathcal{R}(-1)) = V_{2,0,0}.$$

Thus in this case the set of bundles $(*)$ does not contain a strong complete exceptional sequence. It does not contain a complete exceptional sequence, either, since

$$\mathrm{Hom}(\mathcal{R}(-3), \mathrm{Sym}^3\mathcal{R}) \neq 0, \ \ \mathrm{Hom}(\mathrm{Sym}^2\mathcal{R}(-2), \mathrm{Sym}^2\mathcal{R}) \neq 0$$
$$\mathrm{Hom}(\mathrm{Sym}^2\mathcal{R}(-2), \mathrm{Sym}^3\mathcal{R}) \neq 0, \ \ \mathrm{Hom}(\mathrm{Sym}^3\mathcal{R}(-1), \mathcal{R}) \neq 0$$
$$\mathrm{Hom}(\mathrm{Sym}^3\mathcal{R}(-1), \mathrm{Sym}^2\mathcal{R}) \neq 0, \ \ \mathrm{Hom}(\mathrm{Sym}^3\mathcal{R}(-1), \mathrm{Sym}^3\mathcal{R}) \neq 0.$$

On the other hand one has on $\mathrm{IGrass}(2, V)$ the following exact sequences of vector bundles:

$$0 \to \mathcal{R}^\perp \to V \otimes \mathcal{O} \to \mathcal{R}^\vee \to 0 \tag{1}$$
$$0 \to \mathcal{R} \to \mathcal{R}^\perp \to \mathcal{R}^\perp/\mathcal{R} \to 0. \tag{2}$$

The second exterior power of the two term complex $0 \to \mathcal{R} \to \mathcal{R}^\perp$ gives an acyclic complex resolving $\bigwedge^2(\mathcal{R}^\perp/\mathcal{R})$ which is isomorphic to $\mathcal{O}_{\mathrm{IGrass}(2,V)}$ via the mapping induced by the symplectic form $\langle\cdot,\cdot\rangle$. Thus we get the exact sequence

$$0 \to \mathrm{Sym}^2\mathcal{R} \to \mathcal{R} \otimes \mathcal{R}^\perp \to \bigwedge^2 \mathcal{R}^\perp \to \mathcal{O} \to 0. \tag{3}$$

The second symmetric power of the two term complex $0 \to \mathcal{R}^\perp \to V \otimes \mathcal{O}$ yields the exact sequence

$$0 \to \bigwedge^2 \mathcal{R}^\perp \to \mathcal{R}^\perp \otimes V \to \mathrm{Sym}^2 V \otimes \mathcal{O} \to \mathrm{Sym}^2 \mathcal{R}^\vee \to 0. \tag{4}$$

Note also that $\mathcal{R}^\vee \simeq \mathcal{R}(1)$ and $\mathrm{Sym}^2 \mathcal{R}^\vee \simeq \mathrm{Sym}^2 \mathcal{R}(2)$. Since $\mathcal{R} \otimes \mathcal{R}(-1) \simeq \mathrm{Sym}^2 \mathcal{R}(-1) \oplus \mathcal{O}(-2)$ sequence (1) gives

$$0 \to \mathcal{R}^\perp \otimes \mathcal{R}(-2) \to V \otimes \mathcal{R}(-2) \to \mathrm{Sym}^2 \mathcal{R}(-1) \oplus \mathcal{O}(-2) \to 0 \tag{5}$$

and

$$0 \to \mathcal{R}^\perp(-2) \to V \otimes \mathcal{O}(-2) \to \mathcal{R}(-1) \to 0. \tag{6}$$

Moreover twisting by $\mathcal{O}(-2)$ in (3) and (4) yields

$$0 \to \mathrm{Sym}^2\mathcal{R}(-2) \to \mathcal{R} \otimes \mathcal{R}^\perp(-2) \to \bigwedge^2 \mathcal{R}^\perp(-2) \to \mathcal{O}(-2) \to 0 \tag{7}$$
$$0 \to \bigwedge^2 \mathcal{R}^\perp(-2) \to \mathcal{R}^\perp \otimes V(-2) \to \mathrm{Sym}^2 V \otimes \mathcal{O}(-2) \to \mathrm{Sym}^2 \mathcal{R} \to 0. \tag{8}$$

What (5), (6), (7), (8) tell us is that $\mathrm{Sym}^2\,\mathcal{R}(-2)$ is in the full triangulated subcategory generated by $\mathcal{O}(-2)$, $\mathrm{Sym}^2\,\mathcal{R}(-1)$, $\mathcal{R}(-2)$, $\mathrm{Sym}^2\,\mathcal{R}$, $\mathcal{R}(-1)$. Thus the derived category $D^b(Coh\,\mathrm{IGrass}(2,V))$ is generated by the bundles in $(*)$ without $\mathrm{Sym}^2\,\mathcal{R}(-2)$, which makes a total of 13 bundles.
But even in this simple case I do not know how to pass on to a complete exceptional sequence because there is no method at this point to decide which bundles in $(*)$ should be thrown away and what extra bundles should be let in to obtain a complete exceptional sequence.

3.4 Calculation for the Grassmannian of isotropic 3-planes in a 7-dimensional orthogonal vector space

In this section we want to show how the method of subsection 3.3 can be adapted -using theorem 3.2.7 on quadric bundles- to produce sets of vector bundles that generate the derived categories of coherent sheaves on orthogonal Grassmannians (with the ultimate goal to obtain (strong) complete exceptional sequences on them by appropriately modifying these sets of bundles). Since the computations are more involved than in the symplectic case, we will restrict ourselves to illustrating the method by means of a specific example:
Let V be a 7-dimensional complex vector space equipped with a non-degenerate symmetric bilinear form $\langle\cdot,\cdot\rangle$. $\mathrm{IFlag}(k_1,\dots,k_t;V)$ denotes the flag variety of isotropic flags of type $(k_1,\dots,k_t)$, $1\le k_1<\dots<k_t\le 3$, in V and $\mathrm{IGrass}(k,V)$, $1\le k\le 3$, the Grassmannian of isotropic k-planes in V; again in this setting we have the tautological flag of subbundles

$$\mathcal{R}_{k_1}\subset\dots\subset\mathcal{R}_{k_t}\subset V\otimes\mathcal{O}_{\mathrm{IFlag}(k_1,\dots,k_t;V)}$$

on $\mathrm{IFlag}(k_1,\dots,k_t;V)$ and the tautological subbundle $\mathcal{R}$ on $\mathrm{IGrass}(k,V)$.
Now consider $\mathrm{IGrass}(3,V)$ which sits in the diagram (D)

$$\begin{array}{lcl}
\mathbb{P}(\mathcal{E}_2)\supset\mathcal{Q}_2\simeq\mathrm{IFlag}(1,2,3;V)\simeq\mathrm{Flag}_{\mathrm{IGrass}(3,V)}(1,2,3;\mathcal{R}) & & \\
\quad\downarrow\pi_2 & & \\
\mathbb{P}(\mathcal{E}_1)\supset\mathcal{Q}_1\simeq\mathrm{IFlag}(1,2;V) & \searrow\pi & \\
\quad\downarrow\pi_1 & & \\
\mathbb{P}^6\supset Q\simeq\mathrm{IFlag}(1;V) & & \mathrm{IGrass}(3,V)
\end{array}\qquad (D)$$

The rank i tautological subbundle on $\mathrm{IFlag}(1,\dots,j;V)$ pulls back to the rank i tautological subbundle on $\mathrm{IFlag}(1,\dots,j+1;V)$ under π_j, $1\le i\le j\le 2$, and for ease of notation it will be denoted by $\mathcal{R}_i$ with the respective base spaces being tacitly understood in each case.
The choice of an isotropic line L_1 in V amounts to picking a point in the

quadric hypersurface $Q = \{[v] \in \mathbb{P}(V) \mid \langle v, v \rangle = 0\} \subset \mathbb{P}^6$. An isotropic plane L_2 containing L_1 is nothing but an isotropic line L_2/L_1 in the orthogonal vector space $L_1^{\perp}/L_1$. Thus $\mathrm{IFlag}(1,2;V)$ is a quadric bundle $\mathcal{Q}_1$ over $\mathrm{IFlag}(1;V)$ inside the projective bundle $\mathbb{P}(\mathcal{E}_1)$ of the orthogonal vector bundle $\mathcal{E}_1 := \mathcal{R}_1^{\perp}/\mathcal{R}_1$ on $\mathrm{IFlag}(1;V)$. Similarly, $\mathrm{IFlag}(1,2,3;V)$ is a quadric bundle $\mathcal{Q}_2 \subset \mathbb{P}(\mathcal{E}_2)$ over $\mathrm{IFlag}(1,2;V)$ where $\mathcal{E}_2 := \mathcal{R}_2^{\perp}/\mathcal{R}_2$, and at the same time $\mathrm{IFlag}(1,2,3;V)$ is isomorphic to the relative variety of complete flags $\mathrm{Flag}_{\mathrm{IGrass}(k,V)}(1,2,3;\mathcal{R})$ in the fibres of the tautological subbundle $\mathcal{R}$ on $\mathrm{IGrass}(3,V)$.
Moreover, $\mathcal{O}_Q(-1) \simeq \mathcal{R}_1$, $\mathcal{O}_{\mathcal{Q}_1}(-1) \simeq \mathcal{R}_2/\mathcal{R}_1$, $\mathcal{O}_{\mathcal{Q}_2}(-1) \simeq \mathcal{R}_3/\mathcal{R}_2$. We want to switch to a more representation-theoretic picture. For this, put $G := \mathrm{Spin}_7 \mathbb{C}$ and turning to the notation and set-up introduced at the beginning of subsection 2.2, rewrite diagram (D) as

$$\begin{array}{ccc} G/P(\alpha_1,\alpha_2,\alpha_3) = G/B & & \\ \downarrow \pi_2 & \searrow \pi & \\ G/P(\alpha_1,\alpha_2) & & \\ \downarrow \pi_1 & & \\ G/P(\alpha_1) & & G/P(\alpha_3) \end{array} \qquad \text{(D')}$$

The orthogonal vector bundles $\mathcal{R}_1^{\perp}/\mathcal{R}_1$ on $Q = G/P(\alpha_1)$ resp. $\mathcal{R}_2^{\perp}/\mathcal{R}_2$ on $\mathrm{IFlag}(1,2;V) = G/P(\alpha_1,\alpha_2)$ admit spinor bundles in the sense of assumption (A) in subsection 3.2:
In fact, on $G/P(\alpha_1)$ we will use the homogeneous vector bundle $S(\mathcal{R}_1^{\perp}/\mathcal{R}_1)$ which is associated to the irreducible representation r_1 of $P(\alpha_1)$ with highest weight the fundamental weight ω_3, and on $G/P(\alpha_1,\alpha_2)$ we will use the homogeneous vector bundle $S(\mathcal{R}_2^{\perp}/\mathcal{R}_2)$ which is the pull-back under the projection $G/P(\alpha_1,\alpha_2) \to G/P(\alpha_2)$ of the homogeneous vector bundle defined by the irreducible representation r_2 of $P(\alpha_2)$ with highest weight ω_3.
Therefore we can apply theorem 3.2.7 (or rather its corollary 3.2.8) iteratively to obtain the following assertion:
The bundles on $\mathrm{IFlag}(1,2,3;V)$

$$(\heartsuit) \qquad \mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C}$$

where $\mathcal{A}$ runs through the set

$$A := \{\Sigma(\mathcal{R}_1^{\perp}/\mathcal{R}_1) \otimes \mathcal{R}_1^{\otimes 5},\ \mathcal{R}_1^{\otimes 4},\ \mathcal{R}_1^{\otimes 3},\ \mathcal{R}_1^{\otimes 2},\ \mathcal{R}_1,\ \mathcal{O}\}$$

and $\mathcal{B}$ runs through

$$B := \{\Sigma(\mathcal{R}_2^{\perp}/\mathcal{R}_2) \otimes (\mathcal{R}_2/\mathcal{R}_1)^{\otimes 3},\ (\mathcal{R}_2/\mathcal{R}_1)^{\otimes 2},\ \mathcal{R}_2/\mathcal{R}_1,\ \mathcal{O}\}$$

and $\mathcal{C}$ runs through

$$C := \{\Sigma(\mathcal{R}_3^{\perp}/\mathcal{R}_3) \otimes (\mathcal{R}_3/\mathcal{R}_2),\ \mathcal{O}\}$$

generate $D^b(Coh\,\mathrm{IFlag}(1,2,3;V))$, and in fact form a complete exceptional sequence when appropriately ordered.
Here $\Sigma(\mathcal{R}_i^{\perp}/\mathcal{R}_i)$, $i = 1,\ 2,\ 3$, denote the bundles on $\mathrm{IFlag}(1,2,3;V)$ which are the pull-backs under the projections $G/B \to G/P(\alpha_i)$ of the vector bundles on $G/P(\alpha_i)$ which are *the duals* of the homogeneous vector bundles associated to the irreducible representations r_i of $P(\alpha_i)$ with highest weight the fundamental weight ω_3.
We know that the full direct images under π of the bundles in ($\heartsuit$) will generate $D^b(Coh\,\mathrm{IGrass}(3,V))$ downstairs. When one wants to apply Bott's theorem to calculate direct images the trouble is that $\Sigma(\mathcal{R}_1^{\perp}/\mathcal{R}_1)$ and $\Sigma(\mathcal{R}_2^{\perp}/\mathcal{R}_2)$, though homogeneous vector bundles on $\mathrm{IFlag}(1,2,3;V) = \mathrm{Spin}_7\mathbb{C}/B$, are not defined by irreducible representations, i.e. characters of, the Borel subgroup B. Therefore, one has to find Jordan-Hölder series for these, i.e. filtrations

$$0 = \mathcal{V}_0 \subset \mathcal{V}_1 \subset \mathcal{V}_2 \subset \cdots \subset \mathcal{V}_M = \Sigma(\mathcal{R}_1^{\perp}/\mathcal{R}_1)$$

and

$$0 = \mathcal{W}_0 \subset \mathcal{W}_1 \subset \cdots \subset \mathcal{W}_N = \Sigma(\mathcal{R}_2^{\perp}/\mathcal{R}_2)$$

by homogeneous vector subbundles $\mathcal{V}_i$ resp. $\mathcal{W}_j$ such that the quotients $\mathcal{V}_{i+1}/\mathcal{V}_i$, $i = 0, \dots, M-1$, resp. $\mathcal{W}_{j+1}/\mathcal{W}_j$, $j = 0, \dots, N-1$, are line bundles defined by characters of B.
Recall that in terms of an orthonormal basis $\epsilon_1, \dots, \epsilon_r$ of $\mathfrak{h}^*$ we can write the fundamental weights for $\mathfrak{so}_{2r+1}\mathbb{C}$ as $\omega_i = \epsilon_1 + \dots \epsilon_i$, $1 \le i < r$, $\omega_r = (1/2)(\epsilon_1 + \cdots + \epsilon_r)$, and simple roots as $\alpha_i = \epsilon_i - \epsilon_{i+1}$, $1 \le i < r$, $\alpha_r = \epsilon_r$, and that (cf. [FuHa], §20.1) the weights of the spin representation of $\mathfrak{so}_{2r+1}\mathbb{C}$ are just given by

$$\frac{1}{2}(\pm\epsilon_1 \pm \cdots \pm \epsilon_r)$$

(all possible 2^r sign combinations).
Therefore, on the level of Lie algebras, the weights of dr_1, dr_2, and dr_3 are given by:

$$dr_1 : \quad \frac{1}{2}(\epsilon_1 \pm \epsilon_2 \pm \epsilon_3), \quad dr_2 : \quad \frac{1}{2}(\epsilon_1 + \epsilon_2 \pm \epsilon_3),$$
$$dr_3 : \quad \frac{1}{2}(\epsilon_1 + \epsilon_2 + \epsilon_3).$$

(Indeed, if v_{ω_3} is a highest weight vector in the irreducible G-module of highest weight ω_3, then the span of $P(\alpha_i) \cdot v_{\omega_3}$, $i = 1, \dots, 3$, is the irreducible $P(\alpha_i)$-module of highest weights ω_3, and its weights are therefore those weights of the ambient irreducible G-module wich can be written as $\omega_3 - \sum_{j \neq i} c_j\alpha_j$, $c_j \in \mathbb{Z}^+$).

Therefore, the spinor bundle $\Sigma(\mathcal{R}_3^{\perp}/\mathcal{R}_3)$ on G/B is just the line bundle $\mathcal{L}(\omega_3) = \mathcal{L}(1/2, 1/2, 1/2)$ associated to ω_3 (viewed as a character of B), $\Sigma(\mathcal{R}_2^{\perp}/\mathcal{R}_2)$ has a Jordan-Hölder filtration of length 2 with quotients
$\mathcal{L}(1/2, 1/2, \pm 1/2)$, and $\Sigma(\mathcal{R}_1^{\perp}/\mathcal{R}_1)$ has a Jordan-Hölder filtration of length 4 with quotients the line bundles $\mathcal{L}(1/2, \pm 1/2, \pm 1/2)$.
In conclusion we get that $D^b(Coh\, G/B)$ is generated by the line bundles

$$(\heartsuit') \qquad \mathcal{A}' \otimes \mathcal{B}' \otimes \mathcal{C}'$$

where $\mathcal{A}'$ runs through the set

$$A' := \Big\{ \mathcal{L}(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}) \otimes \mathcal{L}(-5,0,0),\ \mathcal{L}(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}) \otimes \mathcal{L}(-5,0,0),$$
$$\mathcal{L}(\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}) \otimes \mathcal{L}(-5,0,0),\ \mathcal{L}(\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}) \otimes \mathcal{L}(-5,0,0),\ \mathcal{L}(-4,0,0),$$
$$\mathcal{L}(-3,0,0),\ \mathcal{L}(-2,0,0),\ \mathcal{L}(-1,0,0),\ \mathcal{L}(0,0,0) \}$$

and $\mathcal{B}'$ runs through

$$B' := \Big\{ \mathcal{L}(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}) \otimes \mathcal{L}(0,-3,0),\ \mathcal{L}(\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}) \otimes \mathcal{L}(0,-3,0),$$
$$\mathcal{L}(0,-2,0),\ \mathcal{L}(0,-1,0),\ \mathcal{L}(0,0,0) \}$$

and $\mathcal{C}'$ runs through

$$C' := \Big\{ \mathcal{L}(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}) \otimes \mathcal{L}(0,0,-1),\ \mathcal{L}(0,0,0) \Big\}.$$

Then we can calculate $R\pi_*(\mathcal{A}' \otimes \mathcal{B}' \otimes \mathcal{C}')$ by applying the relative version of Bott's theorem as explained in subsection 3.3 to each of the 90 bundles $\mathcal{A}' \otimes \mathcal{B}' \otimes \mathcal{C}'$; here of course one takes into account that $\mathcal{L}(1/2, 1/2, 1/2) = \pi^* L$, where for simplicity we denote by L the line bundle on $G/P(\alpha_3)$ defined by the one-dimensional representation of $P(\alpha_3)$ with weight $-\omega_3$ and one uses the projection formula. After a lengthy calculation one thus arrives at the following

Theorem 3.4.1. *The derived category $D^b(Coh\, \mathrm{IGrass}(3,V))$ is generated as triangulated category by the following 22 vector bundles:*

$$\bigwedge^2 \mathcal{R}(-1),\ \mathcal{O}(-2),\ \mathcal{R}(-2) \otimes L,\ \mathrm{Sym}^2\mathcal{R}(-1) \otimes L,\ \mathcal{O}(-3) \otimes L,$$
$$\bigwedge^2 \mathcal{R}(-2) \otimes L,\ \Sigma^{2,1}\mathcal{R}(-1) \otimes L,\ \mathcal{R}(-1),\ \mathcal{O}(-2) \otimes L,\ \mathcal{O}(-1),$$
$$\mathcal{R}(-1) \otimes L,\ \bigwedge^2 \mathcal{R}(-1) \otimes L,\ \Sigma^{2,1}\mathcal{R} \otimes L,\ \mathrm{Sym}^2\mathcal{R}^\vee(-2) \otimes L,\ \bigwedge^2 \mathcal{R},\ \mathcal{O},$$
$$\Sigma^{2,1}\mathcal{R},\ \mathrm{Sym}^2\mathcal{R}^\vee(-2),\ \mathcal{O}(-1) \otimes L,\ \mathrm{Sym}^2\mathcal{R}^\vee(-1),\ \bigwedge^2 \mathcal{R} \otimes L,\ \mathcal{R} \otimes L.$$

One should remark that the expected number of vector bundles in a complete exceptional sequence is 8 in this case since there are 8 Schubert varieties in $\mathrm{IGrass}(3,V)$ (cf. [BiLa], §3).

4 Degeneration techniques

Whereas in the preceding section a strategy for proving existence of complete exceptional sequences on rational homogeneous varieties was exposed which was based on the method of fibering them into simpler ones of the same type, here we propose to explain an idea for a possibly alternative approach to tackle this problem. It relies on a theorem due to M. Brion that provides a degeneration of the diagonal $\Delta \subset X \times X$, X rational homogeneous, into a union (over the Schubert varieties in X) of the products of a Schubert variety with its opposite Schubert variety.
We will exclusively consider the example of $\mathbb{P}^n$ and the main goal will be to compare resolutions of the structure sheaves of the diagonal and its degeneration product in this case. This gives a way of proving Beilinson's theorem on $\mathbb{P}^n$ without using a resolution of $\mathcal{O}_\Delta$ but only of the structure sheaf of the degeneration.

4.1 A theorem of Brion

The notation concerning rational homogeneous varieties introduced at the beginning of subsection 2.2 is retained.
The following theorem was proven by M. Brion (cf. [Bri], thm. 2).

Theorem 4.1.1. *Regard the simple roots $\alpha_1, \dots, \alpha_r$ as characters of the maximal torus H and put*

$$\mathfrak{X} := \text{closure of } \{(hx,\, x,\, \alpha_1(h), \dots, \alpha_r(h)) \,|\, x \in X = G/P,\ h \in H\} \\ \text{in } X \times X \times \mathbb{A}^r$$

with its projection $\mathfrak{X} \xrightarrow{\pi} \mathbb{A}^r$. If H acts on $\mathfrak{X}$ via its action on the ambient $X \times X \times \mathbb{A}^r$ given by

$$h \cdot (x_1,\, x_2,\, t_1, \dots, t_r) := (hx_1,\, x_2,\, \alpha_1(h)t_1, \dots, \alpha_r(h)t_r)$$

and acts in $\mathbb{A}^r$ with weights $\alpha_1, \dots, \alpha_r$, then π is equivariant, surjective, flat with reduced fibres such that

$$\mathfrak{X}_0 := \pi^{-1}((0, \dots, 0)) \simeq \bigcup_{w \in W^P} X_w \times X^w\,,$$

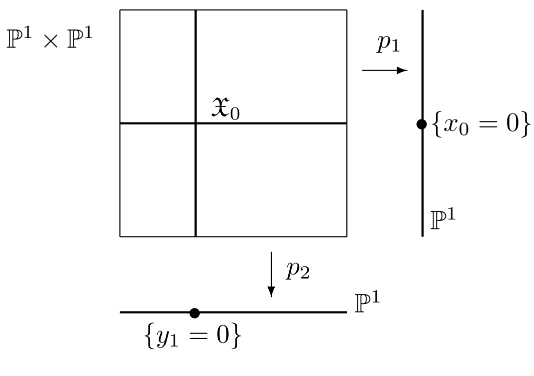
and is a trivial fibration over $H \cdot (1, \dots, 1)$, the complement of the union of all coordinate hyperplanes, with fibre the diagonal $\Delta = \Delta_X \subset X \times X$.

Now the idea to use this result for our purpose is as follows: In [Bei], Beilinson proved his theorem using an explicit resolution of $\mathcal{O}_{\Delta_{\mathbb{P}^n}}$. However, on a general rational homogeneous variety X a resolution of the structure sheaf of the diagonal is hard to come up with. The hope may be therefore that a resolution of

$\mathfrak{X}_0$ is easier to manufacture (by combinatorial methods) than one for $\mathcal{O}_\Delta$, and that one could afterwards lift the resolution of $\mathcal{O}_{\mathfrak{X}_0}$ to one of $\mathcal{O}_\Delta$ by flatness. If we denote by p_1 resp. p_2 the projections of $X \times X$ to the first resp. second factor, the preceding hope is closely connected to the problem of comparing the functors $Rp_{2*}(p_1^*(-) \otimes^L \mathcal{O}_{\mathfrak{X}_0})$ and $Rp_{2*}(p_1^*(-) \otimes^L \mathcal{O}_\Delta) \simeq \mathrm{id}_{D^b(Coh\,X)}$. In the next subsection we will present the computations to clarify these issues for projective space.

4.2 Analysis of the degeneration of the Beilinson functor on $\mathbb{P}^n$

Look at two copies of $\mathbb{P}^n$, one with homogeneous coordinates $x_0, \dots, x_n$, the other with homogeneous coordinates $y_0, \dots, y_n$. In this case $\mathfrak{X}_0 = \bigcup_{i=0}^n \mathbb{P}^i \times \mathbb{P}^{n-i}$, and $\mathfrak{X}_0$ is defined by the ideal $J = (x_i y_j)_{0 \le i < j \le n}$ and the diagonal by the ideal $I = (x_i y_j - x_j y_i)_{0 \le i < j \le n}$.
Consider the case of $\mathbb{P}^1$. The first point that should be noticed is that $Rp_{2*}(p_1^*(-) \otimes^L \mathcal{O}_{\mathfrak{X}_0})$ is no longer isomorphic to the identity: By Orlov's representability theorem (cf. [Or2], thm. 3.2.1) the identity functor is represented uniquely by the structure sheaf of the diagonal on the product (this is valid for any smooth projective variety and not only for $\mathbb{P}^1$). Here one can also see this in an easier way as follows. For $d >> 0$ the sheaf $p_1^*\mathcal{O}(d) \otimes \mathcal{O}_{\mathfrak{X}_0}$ is p_{2*}-acyclic and p_{2*} commutes with base extension whence $\dim_{\mathbb{C}} (p_{2*}(p_1^*\mathcal{O}(d) \otimes \mathcal{O}_{\mathfrak{X}_0}) \otimes \mathbb{C}_P) = d+1$ if P is the point $\{y_1 = 0\}$ and $= 1$ otherwise:



Thus $p_{2*}(p_1^*\mathcal{O}(d) \otimes \mathcal{O}_{\mathfrak{X}_0}) = Rp_{2*}(p_1^*\mathcal{O}(d) \otimes^L \mathcal{O}_{\mathfrak{X}_0})$ is not locally free in this case. We will give a complete description of the functor $Rp_{2*}(p_1^*(-) \otimes^L \mathcal{O}_{\mathfrak{X}_0})$ below for $\mathbb{P}^n$. If one compares the resolutions of $\mathcal{O}_{\mathfrak{X}_0}$ and $\mathcal{O}_\Delta$ on $\mathbb{P}^1$:

$$0 \longrightarrow \mathcal{O}(-1,-1) \xrightarrow{(x_0 y_1)} \mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1} \longrightarrow \mathcal{O}_{\mathfrak{X}_0} \longrightarrow 0$$
$$0 \longrightarrow \mathcal{O}(-1,-1) \xrightarrow{(x_0 y_1 - x_1 y_0)} \mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1} \longrightarrow \mathcal{O}_\Delta \longrightarrow 0$$

and on $\mathbb{P}^2$:

$$0\to\mathcal{O}(-2,-1)\oplus\mathcal{O}(-1,-2)\xrightarrow{A'}\mathcal{O}(-1,-1)^{\oplus 3}\xrightarrow{B'}\mathcal{O}_{\mathbb{P}^2\times\mathbb{P}^2}\to\mathcal{O}_{\mathfrak{X}_0}\to 0$$
$$0\to\mathcal{O}(-2,-1)\oplus\mathcal{O}(-1,-2)\xrightarrow{A}\mathcal{O}(-1,-1)^{\oplus 3}\xrightarrow{B}\mathcal{O}_{\mathbb{P}^2\times\mathbb{P}^2}\to\mathcal{O}_{\Delta}\to 0$$

where

$$A=\begin{pmatrix} x_0 & y_0\\ x_1 & y_1\\ x_2 & y_2\end{pmatrix}\quad A'=\begin{pmatrix} x_0 & 0\\ x_1 & y_1\\ 0 & y_2\end{pmatrix}$$
$$B=(x_2y_1-x_1y_2,\ x_0y_2-x_2y_0,\ x_1y_0-x_0y_1)\quad B=(-x_1y_2,\ x_0y_2,\ -x_0y_1)$$

(these being Hilbert-Burch type resolutions; here $\mathfrak{X}_0$ is no longer a local complete intersection!) one may wonder if on $\mathbb{P}^n$ there exist resolutions of $\mathcal{O}_{\mathfrak{X}_0}$ and $\mathcal{O}_\Delta$ displaying an analogous similarity. This is indeed the case, but will require some work.

Consider the matrix

$$\begin{pmatrix} x_0 & \dots & x_n\\ y_0 & \dots & y_n\end{pmatrix}$$

as giving rise to a map between free bigraded modules F and G over $\mathbb{C}[x_0,\dots,x_n;\,y_0,\dots,y_n]$ of rank $n+1$ and 2 respectively. Put $K_h:=\bigwedge^{h+2}F\otimes\mathrm{Sym}^h G^\vee$ for $h=0,\dots,n-1$. Choose bases $f_0,\dots,f_n$ resp. ξ, η for F resp. $G^\vee$. Define maps $d_h:K_h\to K_{h-1}$, $h=1,\dots,n-1$ by

$$d_h\left(f_{j_1}\wedge\dots\wedge f_{j_{h+2}}\otimes\xi^{\mu_1}\eta^{\mu_2}\right):=\sum_{l=1}^{h+2}(-1)^{l+1}x_{j_l}f_{j_1}\wedge\dots\wedge\hat{f}_{j_l}\wedge\dots\wedge f_{j_{h+2}}$$
$$\otimes\xi^{-1}(\xi^{\mu_1}\eta^{\mu_2})+\sum_{l=1}^{h+2}(-1)^{l+1}y_{j_l}f_{j_1}\wedge\dots\wedge\hat{f}_{j_l}\wedge\dots\wedge f_{j_{h+2}}\otimes\eta^{-1}(\xi^{\mu_1}\eta^{\mu_2})$$

where $0\le j_1<\dots<j_{h+2}\le n$, $\mu_1+\mu_2=h$ and the homomorphism ξ^{-1} (resp. η^{-1}) is defined by

$$\xi^{-1}(\xi^{\mu_1}\eta^{\mu_2}):=\begin{cases}\xi^{\mu_1-1}\eta^{\mu_2} & \text{if}\quad \mu_1\ge 1\\ 0 & \text{if}\quad \mu_1=0\end{cases}$$

(resp. analogously for η^{-1}). Then

$$0\longrightarrow K_{n-1}\xrightarrow{d_{n-1}}\dots\xrightarrow{d_1}K_0\longrightarrow I\longrightarrow 0$$

is a resolution of I which is the Eagon-Northcott complex in our special case (cf. [Nor], appendix C).

Proposition 4.2.1. *The ideal J has a resolution*

$$0\longrightarrow K_{n-1}\xrightarrow{d'_{n-1}}\dots\xrightarrow{d'_1}K_0\longrightarrow J\longrightarrow 0$$

where the differential $d'_h : K_h \to K_{h-1}$ *is defined by*

$$d'_h \left(f_{j_1} \wedge \dots \wedge f_{j_{h+2}} \otimes \xi^{\mu_1}\eta^{\mu_2}\right) := \sum_{l=1}^{h-\mu_2+1} (-1)^{l+1} x_{j_l} f_{j_1} \wedge \dots \wedge \hat{f}_{j_l} \wedge \dots \wedge f_{j_{h+2}}$$

$$\otimes \xi^{-1}(\xi^{\mu_1}\eta^{\mu_2}) + \sum_{l=\mu_1+2}^{h+2} (-1)^{l+1} y_{j_l} f_{j_1} \wedge \dots \wedge \hat{f}_{j_l} \wedge \dots \wedge f_{j_{h+2}} \otimes \eta^{-1}(\xi^{\mu_1}\eta^{\mu_2}) \,.$$

Intuitively the differentials d'_h are gotten by degenerating the differentials d_h. To prove proposition 4.2.1 we will use the fact that J is a monomial ideal. There is a combinatorial method for sometimes writing down resolutions for these by looking at simplicial or more general cell complexes from topology. The method can be found in [B-S]. We will recall the results we need in the following. Unfortunately the resolution of proposition 4.2.1 is not supported on a simplicial complex, one needs a more general cell complex.

Let X be a finite regular cell complex. This is a non-empty topological space X with a finite set Γ of subsets of X (the *cells* of X) such that

(a) $X = \bigcup_{e\in\Gamma} e$,

(b) the $e \in \Gamma$ are pairwise disjoint,

(c) $\emptyset \in \Gamma$,

(d) for each non-empty $e \in \Gamma$ there is a homeomorphism between a closed i-dimensional ball and the closure $\bar{e}$ which maps the interior of the ball onto e (i.e. e is an *open* i*-cell*).

We will also call the $e \in \Gamma$ *faces*. We will say that $e' \in \Gamma$ is a *face of* $e \in \Gamma$, $e \neq e'$, or that e contains e' if $e' \subset \bar{e}$. The maximal faces of e under containment are called its *facets*. 0- and 1-dimensional faces will be called *vertices* and *edges* respectively. The set of vertices is denoted $\mathfrak{V}$. A subset $\Gamma' \subset \Gamma$ such that for each $e \in \Gamma'$ all the faces of e are in Γ' determines a *subcomplex* $X_{\Gamma'} = \bigcup_{e\in\Gamma'} e$ of X. Moreover we assume in addition

(e) If e' is a codimension 2 face of e there are exactly two facets e_1, e_2 of e containing e'.

The prototypical example of a finite regular cell complex is the set of faces of a convex polytope for which property (e) is fulfilled. In general (e) is added as a kind of regularity assumption.

Choose an *incidence function* $\epsilon(e, e')$ on pairs of faces of e, e'. This means that ϵ takes values in $\{0, +1, -1\}$, $\epsilon(e, e') = 0$ unless e' is a facet of e, $\epsilon(v, \emptyset) = 1$ for all vertices $v \in \mathfrak{V}$ and moreover

$$\epsilon(e, e_1)\epsilon(e_1, e') + \epsilon(e, e_2)\epsilon(e_2, e') = 0$$

for e, e_1, e_2, e' as in (e).
Let now $M = (m_v)_{v \in \mathfrak{V}}$ be a monomial ideal (m_v monomials) in the polynomial ring $k[T_1, \dots, T_N]$, k some field. For multi-indices $\underline{a}$, $\underline{b} \in \mathbb{Z}^N$ we write $\underline{a} \le \underline{b}$ to denote $a_i \le b_i$ for all $i = 1, \dots, N$. $T^{\underline{a}}$ denotes $T_1^{a_1} \cdot \dots \cdot T_N^{a_N}$.
The oriented chain complex $\tilde{C}(X, k) = \bigoplus_{e \in \Gamma} ke$ (the homological grading is given by dimension of faces) with differential

$$\partial e := \sum_{e' \in \Gamma} \epsilon(e, e') e'$$

computes the *reduced cellular homology groups* $\tilde{H}^i(X, k)$ of X.
Think of the vertices $v \in \mathfrak{V}$ as labelled by the corresponding monomials m_v. Each non-empty face $e \in \Gamma$ will be identified with its set of vertices and will be labelled by the least common multiple m_e of its vertex labels. The *cellular complex* $F_{X,M}$ associated to (X, M) is the $\mathbb{Z}^N$-graded $k[T_1, \dots, T_N]$-module $\bigoplus_{e \in \Gamma, e \neq \emptyset} k[T_1, \dots, T_N]e$ with differential

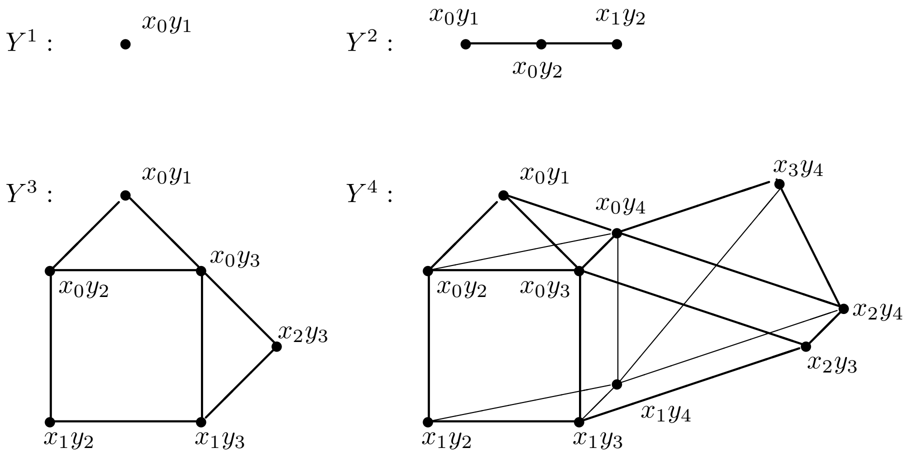
$$\partial e := \sum_{e' \in \Gamma, e' \neq \emptyset} \epsilon(e, e') \frac{m_e}{m_{e'}} e'$$

(where again the homological grading is given by the dimension of the faces).
For each multi-index $\underline{b} \in \mathbb{Z}^N$ let $X_{\le \underline{b}}$ be the subcomplex of X consisting of all the faces e whose labels m_e divide $T^{\underline{b}}$. We have

Proposition 4.2.2. *$F_{X,M}$ is a free resolution of M if and only if $X_{\le \underline{b}}$ is acyclic over k for all $\underline{b} \in \mathbb{Z}^N$ (i.e.$\tilde{H}_i(X_{\le \underline{b}}, k) = 0$ for all i).*

We refer to [B-S], prop. 1.2, for a proof.

Next we will construct appropriate cell complexes Y^n, $n = 1, 2, \dots$, that via the procedure described above give resolutions of $J = (x_i y_j)_{0 \le i < j \le n}$. We will apply proposition 4.2.2 by showing that for all $\underline{b} \in \mathbb{Z}^{2n+2}$ the subcomplexes $Y^n_{\le \underline{b}}$ are contractible.
It is instructive to look at the pictures of Y^1, Y^2, Y^3, Y^4 with their labellings first:



The general procedure for constructing Y^n geometrically is as follows: In $\mathbb{R}^{n-1}$ take the standard $(n-1)$-simplex P^1 on the vertex set $\{x_0y_1,\, x_0y_2, \dots,\, x_0y_n\}$. Then take an $(n-2)$-simplex on the vertex set $\{x_1y_2, \dots, x_1y_n\}$, viewed as embedded in the same $\mathbb{R}^{n-1}$, and join the vertices $x_1y_2, \dots, x_1y_n$, respectively, to the vertices $x_0y_2, \dots, x_0y_n$,, respectively, of P^1 by drawing an edge between x_0y_i and x_1y_i for $i = 2, \dots, n$. This describes the process of attaching a new $(n-1)$-dimensional polytope P^2 to the facet of P^1 on the vertex set $\{x_0y_2, \dots, x_0y_n\}$.

Assume that we have constructed inductively the $(n-1)$-dimensional polytope P^i, $2 \le i \le n-1$, with one facet on the vertex set $\{x_\mu y_\nu\}_{\substack{0\le\mu\le i-1\\ i+1\le\nu\le n}}$. Then take an $(n-i-1)$-simplex on the vertex set $\{x_iy_{i+1}, \dots, x_iy_n\}$, viewed as embedded in the same $\mathbb{R}^{n-1}$, and for every α with $1 \le \alpha \le n-i$ join the vertex $x_iy_{i+\alpha}$ of this simplex to the vertices $x_\mu y_{i+\alpha}$, $0 \le \mu \le i-1$, of P^i by an edge. This corresponds to attaching a new $(n-1)$-dimensional polytope P^{i+1} to the facet of P^i on the vertex set $\{x_\mu y_\nu\}_{\substack{0\le\mu\le i-1\\ i+1\le\nu\le n}}$.

In the end we get $(n-1)$-dimensional polytopes $P_1, \dots, P_n$ in $\mathbb{R}^{n-1}$ where P_j and P_{j+1}, $j = 1, \dots, n-1$, are glued along a common facet. These will make up our labelled cell complex Y^n.

The h-dimensional faces of Y^n will be called *h-faces* for short. We need a more convenient description for them:

Lemma 4.2.3. *There are natural bijections between the following sets:*

(i) $\{$*h-faces of* $Y^n\}$

(ii) *matrices*

$$\begin{pmatrix} x_{i_1}y_{i_{\mu_1+2}} & \cdots & x_{i_1}y_{i_{h+2}} \\ \vdots & \ddots & \vdots \\ x_{i_{\mu_1+1}}y_{i_{\mu_1+2}} & \cdots & x_{i_{\mu_1+1}}y_{i_{h+2}} \end{pmatrix}$$

with vertex labels of Y^n *as entries, where* $0 \le i_1 < i_2 < \ldots < i_{\mu_1+1} < i_{\mu_1+2} < \ldots < i_{h+2} \le n$ *and* $0 \le \mu_1 \le h$ *are integers. The* (κ, λ)*-entry of the above matrix is thus* $x_{i_\kappa} y_{i_{\mu_1+\lambda+1}}$*.*

(iii) *standard basis vectors*

$$f_{i_1} \wedge \ldots \wedge f_{i_{\mu_1+1}} \wedge f_{i_{\mu_1+2}} \wedge \ldots \wedge f_{i_{h+2}} \otimes \xi^{\mu_1}\eta^{\mu_2}, \quad 0 \le \mu_1 \le h,$$
$$0 \le i_1 < i_2 < \ldots < i_{\mu_1+1} < i_{\mu_1+2} < \ldots < i_{h+2} \le n$$

of $\bigwedge^{h+2} F \otimes \mathrm{Sym}^h G^\vee$*.*

Proof. The bijection between the sets in (*ii*) and (*iii*) is obvious: To $f_{i_1} \wedge \ldots \wedge f_{i_{h+2}} \otimes \xi^{\mu_1}\eta^{\mu_2}$ in $\bigwedge^{h+2} F \otimes \mathrm{Sym}^h G^\vee$ one associates the matrix

$$\begin{pmatrix} x_{i_1}y_{i_{\mu_1+2}} & \cdots & x_{i_1}y_{i_{h+2}} \\ \vdots & \ddots & \vdots \\ x_{i_{\mu_1+1}}y_{i_{\mu_1+2}} & \cdots & x_{i_{\mu_1+1}}y_{i_{h+2}} \end{pmatrix}.$$

To set up a bijection between the sets under (i) and (ii) the idea is to identify an h-face e of Y^n with its vertex labels and collect the vertex labels in a matrix of the form given in (ii). We will prove by induction on j that the h-faces e contained in the polytopes $P_1, \ldots, P_j$ are exactly those whose vertex labels may be collected in a matrix of the form written in (ii) satisfying the additional property $i_{\mu_1+1} \le j-1$. This will prove the lemma.

P_1 is an $(n-1)$-simplex on the vertex set $\{x_0y_1, \ldots, x_0y_n\}$ and its h-faces e can be identified with the subsets of cardinality $h+1$ of $\{x_0y_1, \ldots, x_0y_n\}$. We can write such a subset in matrix form

$$\begin{pmatrix} x_0y_{i_2} & x_0y_{i_3} & \cdots & x_0y_{i_{h+2}} \end{pmatrix}$$

with $0 \le i_2 < i_3 < \ldots < i_{h+2} \le n$. This shows that the preceding claim is true for $j = 1$.

For the induction step assume that the h-faces of Y^n contained in $P_1, \ldots, P_j$ are exactly those whose vertex labels may be collected in a matrix as in (ii) with $i_{\mu_1+1} \le j-1$. Look at the h-faces e contained in $P_1, \ldots, P_{j+1}$. If e is contained in $P_1, \ldots, P_j$ (which is equivalent to saying that none of the vertex labels of e involves the indeterminate x_j) then there is nothing to show. Now there are two types of h-faces contained in $P_1, \ldots, P_{j+1}$ but not in $P_1, \ldots, P_j$: The first type corresponds to h-faces e entirely contained in the simplex on the vertex set $\{x_jy_{j+1}, \ldots, x_jy_n\}$. These correspond to matrices

$$\begin{pmatrix} x_jy_{i_2} & \cdots & x_jy_{i_{h+2}} \end{pmatrix},$$

$0 \le i_2 < i_3 < \ldots < i_{h+2} \le n$, of the form given in (ii) which involve the indeterminate x_j and have only one row.
The second type of h-faces e is obtained as follows: We take an $(h-1)$-face e' contained in the facet on the vertex set $\{x_a y_b\}_{\substack{0\le a\le j-1\\ j+1\le b\le n}}$ which P_j and P_{j+1} have in common; by induction e' corresponds to a matrix

$$\begin{pmatrix} x_{i_1}y_{i_{\mu_1+2}} & \cdots & x_{i_1}y_{i_{h+1}} \\ \vdots & \ddots & \vdots \\ x_{i_{\mu_1+1}}y_{i_{\mu_1+2}} & \cdots & x_{i_{\mu_1+1}}y_{i_{h+1}} \end{pmatrix}$$

with $0 \le i_1 < i_2 < \ldots < i_{\mu_1+1} \le j-1$ and $j+1 \le i_{\mu_1+2} < \ldots < i_{h+1} \le n$, $0 \le \mu_1 \le h-1$. Then by construction of P_{j+1} there is a unique h-face e in $P_1, \ldots, P_{j+1}$, but not in $P_1, \ldots, P_j$, which contains the $(h-1)$-face e': It is the h-face whose vertex labels are the entries of the preceding matrix together with $\{x_j y_{i_{\mu_1+2}},\, x_j y_{i_{\mu_1+3}}, \ldots,\, x_j y_{i_{h+1}}\}$. Thus e corresponds to the matrix

$$\begin{pmatrix} x_{i_1}y_{i_{\mu_1+2}} & \cdots & x_{i_1}y_{i_{h+1}} \\ \vdots & \ddots & \vdots \\ x_{i_{\mu_1+1}}y_{i_{\mu_1+2}} & \cdots & x_{i_{\mu_1+1}}y_{i_{h+1}} \\ x_j y_{i_{\mu_1+2}} & \cdots & x_j y_{i_{h+1}} \end{pmatrix}.$$

This proves the lemma. □

Now we want to define an incidence function $\epsilon(e, e')$ on pairs of faces e, e' of Y^n. Of course if e' is not a facet of e , we put $\epsilon(e, e') = 0$ and likewise put $\epsilon(v, \emptyset) := 1$ for all vertices v of Y^n. Let now e be an h-face. Using lemma 4.2.3 it corresponds to a matrix

$$M(e) = \begin{pmatrix} x_{i_1}y_{i_{\mu_1+2}} & \cdots & x_{i_1}y_{i_{h+2}} \\ \vdots & \ddots & \vdots \\ x_{i_{\mu_1+1}}y_{i_{\mu_1+2}} & \cdots & x_{i_{\mu_1+1}}y_{i_{h+2}} \end{pmatrix}.$$

A facet e' of e corresponds to a submatrix $M(e')$ of $M(e)$ obtained from $M(e)$ by erasing either a row or a column. We define $\epsilon(e, e') := (-1)^l$ if $M(e')$ is obtained from $M(e)$ by erasing the lth row; we define $\epsilon(e, e') := (-1)^{\mu_1 + j}$ if $M(e')$ is obtained from $M(e)$ by erasing the jth column.
One must check that then $\epsilon(e, e_1)\epsilon(e_1, e'') + \epsilon(e, e_2)\epsilon(e_2, e'') = 0$ for a codimension 2 face e'' of e and e_1, e_2 the two facets of e containing e''. This is now a straightforward computation. There are 3 cases: The matrix $M(e'')$ is obtained from $M(e)$ by (i) deleting two rows, (ii) deleting two columns, (iii) erasing one row and one column:

(i) Let $l_1 < l_2$ and assume that $M(e_1)$ is $M(e)$ with l_1th row erased and $M(e_2)$ is $M(e)$ with l_2th row erased. Then

$$\epsilon(e, e_1) = (-1)^{l_1}, \quad \epsilon(e, e_2) = (-1)^{l_2}, \quad \epsilon(e_1, e'') = (-1)^{l_2 - 1}$$
$$\epsilon(e_2, e'') = (-1)^{l_1}.$$

(ii) This is the same computation as for (i) with the roles of rows and columns interchanged.

(iii) Assume that $M(e_1)$ is $M(e)$ with lth row erased and $M(e_2)$ is $M(e)$ with jth column erased. Then

$$\epsilon(e,e_1)=(-1)^l,\quad \epsilon(e,e_2)=(-1)^{\mu_1+j},\quad \epsilon(e_1,e'')=(-1)^{\mu_1-1+j}$$
$$\epsilon(e_2,e'')=(-1)^l.$$

Thus ϵ is an incidence function on Y^n. Now one has to compute the cellular complex $F_{Y^n,J}$: Indeed by lemma 4.2.3 we know that its term in homological degree h identifies with $\bigwedge^{h+2}F\otimes \mathrm{Sym}^h G^\vee$. If e is an h-face recall that the differential ∂ of $F_{Y^n,J}$ is given by

$$\partial e=\sum_{e'\text{ a facet of }e,\ e'\neq\emptyset}\epsilon(e,e')\frac{m_e}{m_{e'}}e'$$

and if e corresponds to $f_{i_1}\wedge\ldots\wedge f_{i_{h+2}}\otimes\xi^{\mu_1}\eta^{\mu_2}\in\bigwedge^{h+2}F\otimes\mathrm{Sym}^h G^\vee$ we find

$$\partial\left(f_{j_1}\wedge\cdots\wedge f_{j_{h+2}}\otimes\xi^{\mu_1}\eta^{\mu_2}\right)=\sum_{l=1}^{h-\mu_2+1}(-1)^{l+1}x_{j_l}f_{j_1}\wedge\cdots\wedge\hat{f}_{j_l}\wedge\cdots\wedge f_{j_{h+2}}$$
$$\otimes\xi^{-1}(\xi^{\mu_1}\eta^{\mu_2})+\sum_{l=\mu_1+2}^{h+2}(-1)^{l+1}y_{j_l}f_{j_1}\wedge\cdots\wedge\hat{f}_{j_l}\wedge\cdots\wedge f_{j_{h+2}}\otimes\eta^{-1}(\xi^{\mu_1}\eta^{\mu_2}).$$

Thus the complex $F_{Y^n,J}$ is nothing but the complex in proposition 4.2.1. Thus to prove proposition 4.2.1 it is sufficient in view of proposition 4.2.2 to prove the following

Lemma 4.2.4. *For all $\underline{b}\in\mathbb{Z}^{2n+2}$ the subcomplexes $Y^n_{\leq\underline{b}}$ of Y^n are contractible.*

Proof. Notice that it suffices to prove the following: If

$$x_{i_1}\ldots x_{i_k}y_{j_1}\ldots y_{j_l}\quad 0\leq i_1<\ldots i_k\leq n,\quad 0\leq j_1<\cdots<j_l\leq n$$

is a monomial that is the least common multiple of some subset of the vertex labels of Y^n then the subcomplex $\tilde{Y}^n$ of Y^n that consists of all the faces e whose label divides $x_{i_1}\ldots x_{i_k}y_{j_1}\ldots y_{j_l}$ is contractible. This can be done as follows:
Put $\kappa(i_d):=\min\{t\,:\,j_t>i_d\}$ for $d=1,\ldots,k$. Note that we have $\kappa(i_1)=1$ and $\kappa(i_1)\leq\kappa(i_2)\leq\cdots\leq\kappa(i_k)$. Choose a retraction of the face e^0 of $\tilde{Y}^n$ corresponding to the matrix

$$\begin{pmatrix} x_{i_1}y_{j_{\kappa(i_k)}} & \ldots & x_{i_1}y_{j_l}\\ \vdots & \ddots & \vdots\\ x_{i_k}y_{j_{\kappa(i_k)}} & \ldots & x_{i_k}y_{j_l}\end{pmatrix}$$

onto its facet $e^{0'}$ corresponding to

$$\begin{pmatrix} x_{i_1}y_{j_{\kappa(i_k)}} & \dots & x_{i_1}y_{j_l} \\ \vdots & \ddots & \vdots \\ x_{i_{k-1}}y_{j_{\kappa(i_k)}} & \dots & x_{i_{k-1}}y_{j_l} \end{pmatrix}.$$

Then choose a retraction of the face e^1 corresponding to

$$\begin{pmatrix} x_{i_1}y_{j_{\kappa(i_{k-1})}} & \dots & x_{i_1}y_{j_l} \\ \vdots & \ddots & \vdots \\ x_{i_{k-1}}y_{j_{\kappa(i_{k-1})}} & \dots & x_{i_{k-1}}y_{j_l} \end{pmatrix}$$

onto its facet $e^{1'}$ corresponding to

$$\begin{pmatrix} x_{i_1}y_{j_{\kappa(i_{k-1})}} & \dots & x_{i_1}y_{j_l} \\ \vdots & \ddots & \vdots \\ x_{i_{k-2}}y_{j_{\kappa(i_{k-1})}} & \dots & x_{i_{k-2}}y_{j_l} \end{pmatrix}.$$

Notice that $e^{0'}$ is contained in e^1. Continuing this pattern, one can finally retract the face corresponding to

$$\begin{pmatrix} x_{i_1}y_{j_{\kappa(i_1)}} & x_{i_1}y_{j_{\kappa(i_1)+1}} & \dots & x_{i_1}y_{j_l} \end{pmatrix},$$

i.e. a simplex, onto one of its vertices. Composing these retractions, one gets a retraction of $\tilde{Y}^n$ onto a point. □

In conclusion what we get from proposition 4.2.1 is that on $\mathbb{P}^n \times \mathbb{P}^n$ the sheaf $\mathcal{O}_{\mathfrak{X}_0}$ has a resolution

$$(*) \quad 0 \longrightarrow \bigoplus_{\substack{i+j=n-1 \\ i,j\geq 0}} \mathcal{O}(-i-1,-j-1) \xrightarrow{d'_{n-1}} \dots$$
$$\dots \xrightarrow{d'_{h+1}} \left(\bigoplus_{\substack{i+j=h \\ i,j\geq 0}} \mathcal{O}(-i-1,-j-1)\right)^{\oplus\binom{n+1}{h+2}} \xrightarrow{d'_h} \dots$$
$$\dots \xrightarrow{d'_1} \mathcal{O}(-1,-1)^{\oplus\binom{n+1}{2}} \longrightarrow \mathcal{O}_{\mathbb{P}^n\times\mathbb{P}^n} \longrightarrow \mathcal{O}_{\mathfrak{X}_0} \longrightarrow 0$$

where the differentials can be identified with the differentials in the complex of proposition 4.2.1, and $\mathcal{O}_\Delta$ has a resolution

$$(**) \quad 0 \longrightarrow \bigoplus_{\substack{i+j=n-1 \\ i,j\geq 0}} \mathcal{O}(-i-1,-j-1) \xrightarrow{d_{n-1}} \dots$$
$$\dots \xrightarrow{d_{h+1}} \left(\bigoplus_{\substack{i+j=h \\ i,j\geq 0}} \mathcal{O}(-i-1,-j-1)\right)^{\oplus\binom{n+1}{h+2}} \xrightarrow{d_h} \dots$$
$$\dots \xrightarrow{d_1} \mathcal{O}(-1,-1)^{\oplus\binom{n+1}{2}} \longrightarrow \mathcal{O}_{\mathbb{P}^n\times\mathbb{P}^n} \longrightarrow \mathcal{O}_\Delta \longrightarrow 0$$

which is an Eagon-Northcott complex.
The next theorem gives a complete description of the functor $Rp_{2*}(p_1^*(-)\otimes^L \mathcal{O}_{\mathfrak{X}_0}) : D^b(Coh\,\mathbb{P}^n) \to D^b(Coh\,\mathbb{P}^n)$ (recall that in $D^b(Coh\,\mathbb{P}^n)$ one has the strong complete exceptional sequence $(\mathcal{O},\, \mathcal{O}(1), \dots,\, \mathcal{O}(n))$).

THEOREM 4.2.5. *Let $\{pt\} = L_0 \subset L_1 \subset \dots \subset L_n = \mathbb{P}^n$ be a full flag of projective linear subspaces of $\mathbb{P}^n$ (the Schubert varieties in $\mathbb{P}^n$) and let $L^0 = \mathbb{P}^n \supset \dots \supset L^n = \{pt\}$ form a complete flag in general position with respect to the L_j ("L^j is the Schubert variety opposite to L_j").*
For $d \ge 0$ one has in $D^b(Coh\,\mathbb{P}^n)$

$$Rp_{2*}(p_1^*(\mathcal{O}(d))\otimes^L \mathcal{O}_{\mathfrak{X}_0}) \simeq \bigoplus_{j=0}^{n} \mathcal{O}_{L_j}\otimes H^0(L^j,\mathcal{O}(d))^\vee / H^0(L^{j+1},\mathcal{O}(d))^\vee \, .$$

In terms of the coordinates $x_0,\dots,x_n$, $y_0,\dots,y_n$ introduced above:

$$\begin{aligned} Rp_{2*}(p_1^*(\mathcal{O}(d))\otimes^L \mathcal{O}_{\mathfrak{X}_0}) &\simeq \mathcal{O}\oplus(\mathcal{O}/(y_n))^{\oplus d}\oplus(\mathcal{O}/(y_n,y_{n-1}))^{\oplus\frac{d(d+1)}{2}}\oplus\dots \\ &\dots\oplus(\mathcal{O}/(y_n,\dots,y_{n-i}))^{\oplus\binom{d+i}{d-1}}\oplus\dots\oplus(\mathcal{O}/(y_n,\dots,y_1))^{\oplus\binom{d+n-1}{d-1}}. \end{aligned}$$

Moreover for the map $\mathcal{O}(e)\xrightarrow{\cdot x_k}\mathcal{O}(e+1)$ ($e\ge 0$, $0\le k\le n$) one can describe the induced map $Rp_{2*}(p_1^*(\cdot x_k)\otimes^L \mathcal{O}_{\mathfrak{X}_0})$ as follows:
For each $d \ge 0$ and each $i = -1,\dots,n-1$ choose a bijection between the set of monomials M_i^d in the variables $x_{n-1-i}, x_{n-i},\dots,x_n$ of the form $x_{n-i-1}^{\alpha_1}x_{n-i}^{\alpha_2}\dots x_n^{\alpha_{i+2}}$ with $\alpha_1 > 0$ and $\sum\alpha_j = d$, and the set of copies of $\mathcal{O}/(y_n,\dots,y_{n-i})$ occuring in the above expression for $Rp_{2*}(p_1^*(\mathcal{O}(d))\otimes^L \mathcal{O}_{\mathfrak{X}_0})$. Then the copy of $\mathcal{O}/(y_n,\dots,y_{n-i})$ corresponding to a monomial $m\in M_i^e$ is mapped under $Rp_{2*}(p_1^*(\cdot x_k)\otimes^L \mathcal{O}_{\mathfrak{X}_0})$ identically to the copy of $\mathcal{O}/(y_n,\dots,y_{n-i})$ corresponding to the monomial $x_k m$ iff x_k occurs in m. If x_k does not occur in m then the copy of $\mathcal{O}/(y_n,\dots,y_{n-i})$ corresponding to the monomial $m\in M_i^e$ is mapped to the copy of $\mathcal{O}/(y_n,\dots,y_{k+1})$ corresponding to $x_k m$ via the natural surjection

$$\mathcal{O}/(y_n,\dots,y_{n-i}) \to \mathcal{O}/(y_n,\dots,y_{k+1}).$$

Proof. For $d\ge 0$ one tensors the resolution $(*)$ of $\mathcal{O}_{\mathfrak{X}_0}$ by $p_1^*\mathcal{O}(d)$ and notes that then all the bundles occuring in the terms of $(*)\otimes p_1^*\mathcal{O}(d)$ are p_{2*}-acyclic whence $Rp_{2*}(p_1^*(\mathcal{O}(d))\otimes^L \mathcal{O}_{\mathfrak{X}_0})$ is (as a complex concentrated in degree 0) the cokernel of the map

$$\Phi\,:\,\left(H^0(\mathbb{P}^n,\mathcal{O}(d-1))\otimes\mathcal{O}(-1)\right)^{\oplus\binom{n+1}{2}} \to H^0(\mathbb{P}^n,\mathcal{O}(d))\otimes\mathcal{O}$$

which on the various summands $H^0(\mathbb{P}^n,\mathcal{O}(d-1))\otimes\mathcal{O}(-1)$ of the domain is given by the maps

$$\begin{aligned} H^0(\mathbb{P}^n,\mathcal{O}(d-1))\otimes\mathcal{O}(-1) &\to H^0(\mathbb{P}^n,\mathcal{O}(d))\otimes\mathcal{O} \\ m\otimes\sigma &\mapsto x_i m\otimes y_j\sigma \end{aligned}$$

for $0 \le i < j \le n$. For $i = -1, \dots, n-1$ let M_i^d be as above the set of monomials in $x_{n-1-i}, x_{n-i}, \dots, x_n$ of the form $x_{n-i-1}^{\alpha_1} x_{n-i}^{\alpha_2} \dots x_n^{\alpha_{i+2}}$ with $\alpha_1 > 0$ and $\sum \alpha_j = d$. Then we have the identification

$$H^0(\mathbb{P}^n, \mathcal{O}(d)) \otimes \mathcal{O} \simeq \bigoplus_{i=-1}^{n-1} \left(\bigoplus_{m \in M_i^d} \mathcal{O} \right);$$

For given $m \in M_i^d$ write $\mathrm{cont}(m)$ for the subset of the variables $x_0, \dots, x_n$ that occur in m. Then the map Φ above is the direct sum of maps

$$\bigoplus_{x_i \in \mathrm{cont}(m)} \bigoplus_{n \ge j > i} \mathcal{O}(-1) \to \mathcal{O} \quad \forall i = -1, \dots, n-1 \, \forall m \in M_i^d$$

which on the summand $\mathcal{O}(-1)$ on the left side of the arrow corresponding to $x_{i_0} \in \mathrm{cont}(m)$ and $j_0 > i_0$ are multiplication by y_{j_0}. Since M_i^d has cardinality

$$\binom{d+i}{d-1} = \binom{d+i+1}{d} - \binom{d+i}{d}$$

one finds that the cokernel of Φ is indeed

$$\mathcal{O} \oplus (\mathcal{O}/(y_n))^{\oplus d} \oplus \dots \oplus (\mathcal{O}/(y_n, \dots, y_{n-i}))^{\oplus \binom{d+i}{d-1}} \oplus \\ \dots \oplus (\mathcal{O}/(y_n, \dots, y_1))^{\oplus \binom{d+n-1}{d-1}}$$

as claimed.
The second statement of the theorem is now clear because $Rp_{2*}(p_1^*(\cdot x_k) \otimes^L \mathcal{O}_{\mathfrak{X}_0})$ is induced by the map $H^0(\mathbb{P}^n, \mathcal{O}(e)) \otimes \mathcal{O} \to H^0(\mathbb{P}^n, \mathcal{O}(e+1)) \otimes \mathcal{O}$ which is multiplication by x_k. □

Remark 4.2.6. It is possible to prove Beilinson's theorem on $\mathbb{P}^n$ using only knowledge of the resolution $(*)$ of $\mathcal{O}_{\mathfrak{X}_0}$: Indeed by theorem 4.1.1 one knows a priori that one can lift the resolution $(*)$ of $\mathcal{O}_{\mathfrak{X}_0}$ to a resolution of $\mathcal{O}_\Delta$ of the form $(**)$ by flatness (cf. e.g. [Ar], part I, rem. 3.1). Since the terms in the resolution $(*)$ are direct sums of bundles $\mathcal{O}(-k,-l)$, $0 \le k, l \le n$, we find by the standard argument from [Bei](i.e., the decomposition $\mathrm{id} \simeq Rp_{2*}(p_1^*(-) \otimes^L \mathcal{O}_\Delta)$) that $D^b(Coh\, \mathbb{P}^n)$ is generated by $(\mathcal{O}(-n), \dots, \mathcal{O})$.

Finally it would be interesting to know if one could find a resolution of $\mathcal{O}_{\mathfrak{X}_0}$ on $X \times X$ for any rational homogeneous $X = G/P$ along the same lines as in this subsection, i.e. by first finding a "monomial description" of $\mathfrak{X}_0$ inside $X \times X$ (e.g. using standard monomial theory, cf. [BiLa]) and then using the method of cellular resolutions from [B-S]. Thereafter it would be even more important to see if one could obtain valuable information about $D^b(Coh\, X)$ by lifting the resolution of $\mathcal{O}_{\mathfrak{X}_0}$ to one of $\mathcal{O}_\Delta$.

References

[Akh] Akhiezer, D. N., *Lie Group Actions in Complex Analysis*, Aspects of Mathematics, vol. E 27, Braunschweig/Wiesbaden: Vieweg (1995)

[A] Ancona, V., *Fibrati vettoriali sopra le varietà omogenee razionali*, Bolletino U.M.I., (7), 2-A (1988), 299-317

[AO] Ancona, V. & Ottaviani, G., *An introduction to the derived category and the theorem of Beilinson*, Atti Accademia Peloritana dei Pericolanti, Classe I di Scienze Fis. Mat. et Nat. LXVII (1989), 99-110

[Ar] Artin, M., *Deformations of singularities*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics 54, Tata Inst. of Fund. Research, Bombay (1976)

[AKO] Auroux, D., Katzarkov, L., Orlov, D., *Mirror symmetry for weighted projective planes and their noncommutative deformations*, preprint (2004), available at `http://www.arXiv.org/abs/math.AG/0404281`

[Bay] Bayer, A., *Semisimple quantum cohomology and blow-ups*, preprint (2004), available at `http://www.arXiv.org/abs/math.AG/0403260`

[B-M] Bayer, A. & Manin, Y. I., *(Semi)simple exercises in quantum cohomology*, preprint (2001), available at `http://www.arXiv.org/abs/math.AG/0103164`

[B-S] Bayer, D. & Sturmfels, B., *Cellular resolutions of monomial modules*, J. reine angew. Math. 502 (1998), 123-140

[Bei] Beilinson, A. A., *Coherent sheaves on* $\mathbb{P}^n$ *and problems of linear algebra*, Funktsional. Anal. i Prilozhen. 12 (1978), no. 3, 68-69; English translation in Functional. Anal. Appl. 12 (1978)

[BBD] Beilinson, A. A., Bernstein, I. N., Deligne, P., *Faisceaux pervers*, Astérisque 100, 1981

[BGG1] Bernstein, I. N., Gelfand, I. M., Gelfand, S. I., *Schubert Cells and Cohomology of the Spaces* G/P, Russian Math. Surveys 28 (1973), 1-26

[BGG2] Bernstein, I. N., Gelfand, I. M., Gelfand, S. I., *Algebraic vector bundles on* $\mathbb{P}^n$ *and problems of linear algebra*, Funkcionalniy analiz i ego pril. 12 (1978), 66-67; English transl. in Functional. Anal. Appl. 12 (1978)

[BiLa] Billey, S., Lakshmibai, V., *Singular loci of Schubert varieties*, Progress in Mathematics 182, Birkhäuser Boston-Basel-Berlin (2000)

[Bo] Bondal, A. I., *Representation of associative algebras and coherent sheaves*, Izv. Akad. Nauk SSSR Ser. Mat. 53 (1989), 25-44; English transl. in Math. USSR Izv. 34 (1990), 23-42

[BoBe] Bondal, A. I. & van den Bergh, M. *Generators and representability of functors in commutative and noncommutative geometry*, Moscow Math. J. 3 (2003), no. 1, 1-36

[BoKa] Bondal, A. I. & Kapranov, M. M., *Representable functors, Serre functors, and mutations*, Izv. Akad. Nauk SSSR Ser. Mat. 53 (1989), 1183-1205; English transl. in Math. USSR Izv. 35 (1990)

[BK] Bondal, A. I. & Kapranov, M. M., *Enhanced triangulated categories*, Math. USSR Sb. 70 (1991), 93-107

[Brid] Bridgeland, T., *Flops and derived categories*, Invent. Math. 147 (2002), 613-632

[Bri] Brion, M., *Positivity in the Grothendieck group of complex flag varieties*, special issue in celebration of Claudio Procesi's 60th birthday, J. Algebra 258 (2002), no. 1, 137-159

[Bri2] Brion, M., *Lectures on the geometry of flag varieties*, preprint (2004), available at `http://www.arXiv.org/abs/math.AG/0410240`

[BL] Brion, M., Lakshmibai, V., *A geometric aproach to standard monomial theory*, Represent. Theory 7 (2003), 651-680 (electronic)

[Can] Canonaco, A., *The Beilinson complex and canonical rings of irregular surfaces*, to be published on the Memoirs of the A.M.S.

[CMR] Costa, L. & Miro-Roig, R., *Tilting sheaves on toric varieties*, Math. Z. 248 (2004), no. 4, 849-865

[Du] Dubrovin, B., *Geometry and analytic theory of Frobenius manifolds*, Proceedings of the International Congress of Mathematicians, Vol. II, Doc. Math. 1998, no. Extra Vol. II, Berlin, 1998, 315-326

[Ful] Fulton, W., *Intersection Theory*, Berlin-Heidelberg-New York: Springer (1984)

[FuHa] Fulton, W., Harris, J., *Representation Theory: A First Course*, Springer G.T.M./R.I.M. 129, Berlin-Heidelberg-New York: Springer (1991)

[FuLa] Fulton, W., Lang, S., *Riemann-Roch Algebra*, Grundl. der math. Wiss. 277, Berlin-Heidelberg-New York: Springer (1985)

[GeMa] Gelfand, S. I., Manin, Yu. I., *Methods of Homological Algebra*, 2nd ed., Springer monographs in math., Berlin-Heidelberg-New York: Springer (2003)

[Gor] Gorodentsev, A. L., *KIAS Lectures on The Helix Theory*, lectures given at Korea Institute for Advanced Study in May 2001, 45 pp.; available at `http://wwwth.itep.ru/~gorod/Math/start.html`

[EGA] Grothendieck, A. & Dieudonné, J., *Éléments de géométrie algébrique*, I. Grundlehren der Mathematik 166 (1971), Springer, Heidelberg; II-IV. Publ. Math. I.H.E.S. 8 (1961) 11 (1961) 17 (1963) 20 (1964) 24 (1965) 28 (1966) 32 (1967)

[Ha1] Hartshorne, R., *Residues and Duality*, Springer L.N.M. 20, Berlin-Heidelberg-New York: Springer (1966)

[Ha2] Hartshorne, R., *Algebraic Geometry*, Springer G.T.M. 52, Berlin-Heidelberg-New York: Springer (1977)

[Ka1] Kapranov, M. M., *On the derived category of coherent sheaves on Grassmann manifolds*, Izv. Akad. Nauk SSSR Ser. Mat. 48 (1984), 192-202; English translation in Math. USSR Izv. 24 (1985)

[Ka2] Kapranov, M. M., *The derived category of coherent sheaves on a quadric*, Funktsional. Anal. i Prilozhen. 20 (1986), no. 2, 67; English transl. in Functional Anal. Appl. 20 (1986)

[Ka3] Kapranov, M. M., *On the derived categories of coherent sheaves on some homogeneous spaces*, Invent. Math. 92, 479-508 (1988)

[Kaw] Kawamata, Y., *Derived Categories of Toric Varieties*, preprint (2005), available at `http://arXiv.org/abs/math.AG/0503102`

[Ke] Keller, B., *Derived categories and tilting*, preprint, available at `http://www.math.jussieu.fr/~keller/publ/`

[Kon] Kontsevich, M., *Homological algebra of mirror symmetry*, Proc. of the Int. Congress of Mathematicians, vol. 1,2 (Zürich 1994), Birkhäuser, Basel 1995, 120-139

[Kuz] Kuznetsov, A., *Hyperplane sections and derived categories*, preprint (2005), available at `http://arXiv.org/abs/math.AG/0503700`

[Man] Manin, Yu. I., *Lectures on the K-functor in algebraic geometry*, Russ. Math. Surveys 24, no. 5 (1969), 1-89

[GIT] Mumford, D., Fogarty, J., Kirwan, F., *Geometric Invariant Theory*, 3rd ed., Springer Berlin-Heidelberg-New York (1994)

[Nee] Neeman, A., *Triangulated categories*, Annals of math. studies 148, Princeton University Press (2001)

[Nor] Northcott, D. G., *Finite free resolutions*, Cambridge Tracts in Mathematics 71, Cambridge University Press (1976)

[OSS] Okonok, C., Schneider, M., Spindler, H.: *Vector bundles on complex projective spaces*, Progress in Math. 3, Birkhäuser, Boston (1980)

[Or] Orlov, D. O., *Projective bundles, monoidal transformations, and derived categories of coherent sheaves*, Izv. Akad. Nauk SSSR Ser. Mat. 56 (1992), 852-862; English transl. in Math. USSR Izv. 38 (1993), 133-141

[Or2] Orlov, D. O., *Derived categories of coherent sheaves and equivalences between them*, Russian Math. Surveys 58 (3) (2003), 511-591

[Ott] Ottaviani, G., *Spinor bundles on quadrics*, Trans. Am. Math. Soc. 307 (1988), 301-316

[Ot2] Ottaviani, G., *Rational Homogeneous Varieties*, notes of SMI course held in Cortona (1995), available at `http://www.math.unifi.it/ottavian`

[Po] Le Potier, J., *Lectures on vector bundles*, Cambridge studies in adv. math. *54*, Cambridge University Press (1997)

[Pri] Priddy, S., *Koszul resolutions*, Trans. Am. Math. Soc. 152 (1970), 39-60

[RaRa] Ramanan, S., Ramanathan, A., *Projective normality of flag varieties and Schubert varieties*, Invent. Math. 79 (1985), 217-234

[Ra1] Ramanathan, A., *Schubert varieties are arithmetically Cohen-Macaulay*, Invent. Math. 80 (1985), 283-294

[Ra2] Ramanathan, A., *Equations defining Schubert varieties and Frobenius splitting of diagonals*, Publ. Math. I.H.E.S. 65 (1987), 61-90

[Ru1] Rudakov, A. N. et al., *Helices and Vector Bundles: Séminaire Rudakov*, London Mathematical Society Lecture Note Series 148, Cambridge University Press (1990)

[Ru2] Rudakov, A. N., *Rigid and Exceptional Vector Bundles and Sheaves on a Fano Variety*, Proceedings of the International Congress of Mathematicians, Zürich, Switzerland 1994, vol.1, 697-705, Birkhäuser Verlag, Basel, Switzerland (1995)

[Sa] Samokhin, A. V., *The derived category of coherent sheaves on* $LG_3^{\mathbf{C}}$, Russ. Math. Surv., 2001, 56 (3), 592-594

[Se1] Serre, J.-P., *Lie Algebras and Lie Groups*, Springer L.N.M. 1500, Berlin-Heidelberg-New York: Springer (1992)

[Se2] Serre, J.-P., *Complex Semisimple Lie Algebras*, Springer monographs in math., Berlin-Heidelberg-New York: Springer (2001)

[S-T] Siu, Y. T. & Trautmann, G., *Deformations of coherent analytic sheaves with compact supports*, Mem. Amer. Math. Soc. 29 (1981), no. 238

[Sp] Springer, T. A., *Linear algebraic groups*, Progress in Math. 9, Birkhäuser (1998)

[Stei] Steinsieck, M., *Über homogen-rationale Mannigfaltigkeiten*, Schriftenr. Math. Inst. Univ. Münster (2) 23 (1982), 1-55

[Ta] Tate, J., *Homology of Noetherian rings and local rings*, Ill. J. Math. 1 (1957), 14-27

[Ver1] Verdier, Jean-Louis, *Catégories dérivées: État 0*, (rédigé en 1963, publié en 1976), Séminaire de Géométrie Algébrique 4 1/2, Cohomologie Étale, L.N.M. 569, 262-311, Springer (1977)

[Ver2] Verdier, Jean-Louis, *Des catégories dérivées des catégories abéliennes*, Astérisque 239, 1996

[Wey] Weyman, J. M., *Cohomology of Vector Bundles and Syzygies*, Cambridge Tracts in Math. 149, Cambridge Univ. Press (2003)

Christian Böhning
Mathematisches Institut
der Universität Göttingen
Bunsenstr. 3-5
D-37073 Göttingen
boehning@uni-math.gwdg.de

Integer-Valued Quadratic Forms and Quadratic Diophantine Equations

Goro Shimura

Received: September 12, 2006

Communicated by Don Blasius

Abstract. We investigate several topics on a quadratic form Φ over an algebraic number field including the following three: (A) an equation $\xi\Phi \cdot {}^t\xi = \Psi$ for another form Ψ of a smaller size; (B) classification of Φ over the ring of algebraic integers; (C) ternary forms. In (A) we show that the "class" of such a ξ determines a "class" in the orthogonal group of a form Θ such that $\Phi \approx \Psi \oplus \Theta$. Such was done in [S3] when Ψ is a scalar. We will treat the case of nonscalar Ψ, and prove a class number formula and a mass formula, both of new types. In [S5] we classified all genera of **Z**-valued Φ. We generalize this to the case of an arbitrary number field, which is topic (B). Topic (C) concerns some explicit forms of the formulas in (A) when Φ is of size 3 and Ψ is a scalar.

2000 Mathematics Subject Classification: 11E12 (primary), 11D09, 11E41 (secondary)

Introduction

A quadratic Diophantine equation in the title means an equation of the form $\xi\Phi \cdot {}^t\xi = \Psi$, where Φ and Ψ are symmetric matrices of size n and m, and ξ is an $(m \times n)$-matrix. We assume that $n > m$, $\det(\Phi)\det(\Psi) \neq 0$, and all these matrices have entries in an algebraic number field F. The purpose of this paper is to present various new ideas and new results on such an equation. In the simplest case $m = 1$, we take a vector space V of dimension n over F, take also a nondegenerate symmetric F-bilinear form $\varphi : V \times V \to F$, and put $\varphi[x] = \varphi(x, x)$ for $x \in V$. Then the equation can be written $\varphi[x] = q$ with $q \in F, \neq 0$. In our recent book [S3] we formulated a new arithmetic framework of such an equation. In the present paper we attempt to extend the theory so that equations of the type $\xi\Phi \cdot {}^t\xi = \Psi$ can be treated along the same line of ideas, and give essential improvements on the results in [S3], as well as some new results.

Let us first recall the basic ideas of [S3] on this topic. Let $\mathfrak{g}$ denote the ring of algebraic integers in F. For a $\mathfrak{g}$-lattice L in V and a fractional ideal $\mathfrak{b}$ in F we put

$$L[q,\,\mathfrak{b}] = \{\, x \in V \mid \varphi[x] = q,\ \varphi(x,\,L) = \mathfrak{b}\,\},$$
$$\Gamma(L) = \{\, \gamma \in SO^{\varphi}(V) \mid L\gamma = L\},$$
$$SO^{\varphi}(V) = \{\, \alpha \in SL(V,\,F) \mid \varphi[x\alpha] = \varphi[x] \quad \text{for every} \quad x \in V\}.$$

We call L *integral* if $\varphi[x] \in \mathfrak{g}$ for every $x \in L$, and call an integral lattice *maximal* if it is the only integral lattice containing itself.

Given $h \in L[q,\,\mathfrak{b}]$, put $G = SO^{\varphi}(V)$, $W = (Fh)^{\perp}$, that is,

$$W = \{x \in V \,\big|\, \varphi(x,\,h) = 0\},$$

and $H = SO^{\varphi}(W)$, where we use φ also for its restriction to W. Then in [S3] we proved, for a maximal L, that

(1a) *There is a bijection of* $\bigsqcup_{i\in I} \{L_i[q,\,\mathfrak{b}]/\Gamma(L_i)\}$ *onto* $H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)$, *and consequently*

(1b) $$\sum_{i\in I} \#\{L_i[q,\,\mathfrak{b}]/\Gamma(L_i)\} = \#\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)\}.$$

Here the subscript $\mathbf{A}$ means adelization, $C = \{x \in G_{\mathbf{A}} \,\big|\, Lx = L\}$, and $\{L_i\}_{i\in I}$ is a complete set of representatives for the classes in the genus of L with respect to G. If $F = \mathbf{Q}$, $\mathfrak{g} = \mathfrak{b} = \mathbf{Z}$, $L = \mathbf{Z}^3$, and φ is the sum of three squares, then the result is a reformulation of the result of Gauss that connects the number of primitive representations of an integer q as sums of three squares with the class number of primitive binary forms of discriminant $-q$. This result can be formulated as a statement about $\#L[q,\,\mathbf{Z}]$ for such φ and L as Gauss did, and also as another statement concerning $\#\{L[q,\,\mathfrak{b}]/\Gamma(L)\}$ as in (1b), which Gauss did not present in a clear-cut form. Though Eisenstein and Minkowski investigated $\#L[q,\,\mathbf{Z}]$ when φ is the sum of five squares, neither (1a) nor (1b) appears in their work. It seems that the idea of $L[q,\,\mathfrak{b}]/\Gamma(L)$ was taken up for the first time in [S3].

Now the major portion of this paper consists of several types of new results, which are the fruits of the ideas developed from (1a) and (1b). More explicitly, they can be described as follows.

I. The main theorems about $\#\{L[q,\,\mathfrak{b}]/\Gamma(L)\}$ in [S3], formula (1b) in particular, were proved under the following condition: if n is odd, then $\det(\varphi)\mathfrak{g}$ is a square ideal. We will show that this condition is unnecessary.

II. The same types of problems about the equation $\xi\Phi\cdot{}^t\xi = \Psi$ for $m > 1$ were discussed in [S3] to some extent, but mainly restricted to the case $m = n-1$. In Theorem 2.2 we will prove more general results for an arbitrary m formulated from a new viewpoint. Namely, we present the principle that the class of a solution ξ determines a class in the orthogonal group in dimension $n - m$, which is complementary to that of Ψ. We then obtain generalizations of (1a) and (1b).

III. In [S3] we proved a certain mass formula which connects the "mass" of the set $L[q,\,\mathfrak{b}]$ with the mass of H with respect to a subgroup of $H_{\mathbf{A}}$. If F is totally real and φ is totally definite, this can be given in the form

$$\sum_{i\in I}\#L_i[q,\,\mathfrak{b}]/\#\varGamma(L_i)=\sum_{\varepsilon\in E}[H\cap\varepsilon C\varepsilon^{-1}:1]^{-1}, \tag{2}$$

where E is a subset of $H_{\mathbf{A}}$ such that $H_{\mathbf{A}}=\bigsqcup_{\varepsilon\in E}H\varepsilon(H_{\mathbf{A}}\cap C)$. The right-hand side may be called the mass of H with respect to $H_{\mathbf{A}}\cap C$. In Theorem 3.2 we will generalize this to the case of $\xi\varPhi\cdot{}^t\xi=\varPsi$ with $m\geq 1$ and definite or indefinite φ. Our formulas are different from any of the mass formulas of Siegel. See the remark at the end of Section 3 for more on this point.

IV. For $n=3$, the right-hand side of (1b) can be written $[H_{\mathbf{A}}:H(H_{\mathbf{A}}\cap C)]$. In [S3] we gave an explicit formula for this index under the condition mentioned in I. In Theorem 5.7 of the present paper we prove the result without that condition. In general it is difficult to determine when $L[q,\,\mathfrak{b}]\neq\emptyset$. We will investigate this problem for a ternary form.

Every ternary space is isomorphic to a space of type $(B^\circ,\,\beta)$ obtained from a quaternion algebra B over F as follows. Denote by ι the main involution of B and put $B^\circ=\{x\in B\,|\,x^\iota=-x\}$ and $\beta[x]=dxx^\iota$ for $x\in B^\circ$ with $d\in F^\times$. Then we will determine for a maximal L exactly when $L[q,\,\mathbf{Z}]\neq\emptyset$ and give an explicit formula for $\#L[q,\,\mathbf{Z}]$ for $(B^\circ,\,\beta)$ over $\mathbf{Q}$ under the following conditions: (i) B is definite and the genus of maximal lattices in B° consists of a single class; (ii) the discriminant e of B is a prime number; (iii) d is one of the following four types: $d=1$, $d=e$, d is a prime $\neq e$, d/e is a prime $\neq e$ (Theorems 6.6 and 6.7). In fact there are exactly 30 positive definite ternary forms over $\mathbf{Q}$ satisfying these three conditions, including of course the case of the sum of three squares. If we drop conditions (ii) and (iii), then there are exactly 64 ternary quadratic spaces over $\mathbf{Q}$ of type (i). Though our methods are applicable to those 64 spaces, we impose the last two conditions in order to avoid complicated analysis.

Indeed, though the results about $L[q,\,\mathbf{Z}]$ are not so complicated, they are not of the type one can easily guess, even under all three conditions. Also, to make transparent statements, it is better to consider an equation $\xi\cdot\lambda\varPhi^{-1}\cdot{}^t\xi=s=\lambda q$ with a suitable λ, where $\varPhi$ is the matrix representing φ with respect to a $\mathbf{Z}$-basis of L. Take, for example, a ternary form $2x^2+3y^2-yz+z^2$. Then we consider the equation $\xi\cdot\lambda\varPhi^{-1}\cdot{}^t\xi=s$ for $s\in\mathbf{Z}$ with $\lambda=22$, which can be written

$$11x^2+8(y^2+yz+3z^2)=s. \tag{3}$$

We can show that there is a bijection of $L[s/22,\,\mathbf{Z}]$ for this φ onto the set of solutions $(x,\,y,\,z)$ of (3) such that $x\mathbf{Z}+y\mathbf{Z}+z\mathbf{Z}=\mathbf{Z}$. Moreover, such a solution exists if and only if $s=r^2m$ with a squarefree positive integer m such that $m-3\in 8\mathbf{Z}$ and an odd positive integer r such that $11|r$ if 11 remains prime in K, where $K=\mathbf{Q}(\sqrt{-m}\,)$. Thus $\#L[s/22,\,\mathbf{Z}]$ equals the number of such solutions of (3), and can be given as

$$2^{3-\mu_0-\mu_1}c \over w \cdot r\prod_{p|r}\left\{1-\left(\frac{-m}{p}\right)\right\}. \tag{4}$$

Here $\mu_0 = 0$ if 2 is unramified in K and $\mu_0 = 1$ otherwise; $\mu_1 = 0$ if $11|r$ or $11 \nmid m$, and $\mu_1 = 1$ otherwise; c is the class number of K; w is the number of roots of unity in K; $\prod_{p|r}$ is the product over all prime factors p of r. We can state similar results in the 30 cases mentioned above, and the same can be said, in principle, even in the 64 cases too, though we will not do so in the present paper. The condition that the class number is 1 is necessary, as the left-hand side of (2) has more than one term otherwise.

A much smaller portion of this paper, Section 4, is devoted to the classification of Φ over $\mathfrak{g}$. In [S5] we classified the genera of matrices that represent reduced **Z**-valued quadratic forms. Here a quadratic form is called *reduced* if it cannot be represented nontrivially over **Z** by another **Z**-valued quadratic form. This is different from Eisenstein's terminology for ternary forms. We will treat the same type of problem over the ring of algebraic integers of an arbitrary algebraic number field. For this we first have to define the genus of a symmetric matrix in a proper way, so that every genus of maximal lattices can be included. The formulation requires new concepts, and the classification has some interesting features. It should be noted that the obvious definition of a genus employed by Siegel applies only to a special case.

As a final remark we mention the article [S6], in which the reader will find a historical perspective of this topic that we do not include here. For example, [S6] contains a more detailed account of the work of Gauss and his predecessors, Lagrange and Legendre, and also comparisons of our formulas with Siegel's mass formulas. Therefore, [S6] is complementary to the present paper in that sense.

1. Basic symbols and a crucial local result

1.1. Throughout the paper we denote by V a finite-dimensional vector space over a field F and by φ a nondegenerate F-bilinear symmetric form $V \times V \to F$; we put then $\varphi[x] = \varphi(x, x)$ for $x \in V$, $n = \dim(V)$, and

$$O^\varphi(V) = \{\alpha \in GL(V) \mid \varphi[x\alpha] = \varphi[x] \text{ for every } x \in V\},$$
$$SO^\varphi(V) = O^\varphi(V) \cap SL(V).$$

For every subspace U of V on which φ is nondegenerate, we denote the restriction of φ to U also by φ, and use the symbols $O^\varphi(U)$ and $SO^\varphi(U)$. We denote by $A(V)$ the Clifford algebra of (V, φ), and define the *canonical automorphism* $\alpha \mapsto \alpha'$ and the *canonical involution* $\alpha \mapsto \alpha^*$ of $A(V)$ by the condition $-x' = x^* = x$ for every $x \in V$. We then put

$$A^+(V) = A^+(V, \varphi) = \{\alpha \in A(V) \mid \alpha' = \alpha\},$$
$$G^+(V) = \{\alpha \in A^+(V)^\times \mid \alpha^{-1}V\alpha = V\}.$$

We can define a homomorphism $\nu : G^+(V) \to F^\times$ by $\nu(\alpha) = \alpha\alpha^*$ and also a surjective homomorphism $\tau : G^+(V) \to SO^\varphi(V)$ by $x\tau(\alpha) = \alpha^{-1}x\alpha$ for $\alpha \in G^+(V)$ and $x \in V$. Then $\mathrm{Ker}(\tau) = F^\times$. We denote by $\delta(\varphi)$ the coset of $F^\times/F^{\times 2}$ represented by $(-1)^{n(n-1)/2}\det(\varphi)$, where $F^{\times 2} = \{a^2 \mid a \in F^\times\}$.

We note here an easy fact [S3, Lemma 1.5 (ii)]:

$$(1.1) \qquad \{k \in V \mid \varphi[k] = q\} = h \cdot SO^\varphi(V) \ \text{ if } \ n > 1,\ h \in V, \text{and } \varphi[h] = q \in F^\times.$$

1.2. We now consider symbols F and $\mathfrak{g}$ in the following two cases: (i) F is an algebraic number field of finite degree and $\mathfrak{g}$ is its maximal order; (ii) F and $\mathfrak{g}$ are the completions of those in Case (i) at a nonarchimedean prime. We call a field of type (i) a *global field,* and that of type (ii) a *local field.* In this paper, we employ the terms global and local fields only in these senses. If F is a local field, we denote by $\mathfrak{p}$ the maximal ideal of $\mathfrak{g}$. In both local and global cases, by a $\mathfrak{g}$-*lattice* (or simply a *lattice*) in a finite-dimensional vector space V over F, we mean a finitely generated $\mathfrak{g}$-module in V that spans V over F. When F is a global field, we denote by $\mathbf{a}$ and $\mathbf{h}$ the sets of archimedean primes and nonarchimedean primes of F respectively, and put $\mathbf{v} = \mathbf{a} \cup \mathbf{h}$. For each $v \in \mathbf{v}$ we denote by F_v the v-completion of F. Given an algebraic group G defined over F, we define an algebraic group G_v over F_v for each $v \in \mathbf{v}$ and the adelization $G_\mathbf{A}$ as usual, and view G and G_v as subgroups of $G_\mathbf{A}$. We then denote by $G_\mathbf{a}$ and $G_\mathbf{h}$ the archimedean and nonarchimedean factors of $G_\mathbf{A}$, respectively. In particular, $F_\mathbf{A}^\times$ is the idele group of F. For $v \in \mathbf{v}$ and $x \in G_\mathbf{A}$ we denote by x_v the v-component of x.

Given a $\mathfrak{g}$-lattice L in V and another $\mathfrak{g}$-lattice M contained in L in both local and global cases, we can find a finite set $\{\mathfrak{a}\}$ of integral ideals $\mathfrak{a}$ such that L/M as a $\mathfrak{g}$-module is isomorphic to $\bigoplus_{\mathfrak{a}\in\{\mathfrak{a}\}} \mathfrak{g}/\mathfrak{a}$. We then put $[L/M] = \prod_{\mathfrak{a}\in\{\mathfrak{a}\}} \mathfrak{a}$. For $x \in G_\mathbf{A}$ with G acting on V in the global case, we denote by Lx the $\mathfrak{g}$-lattice in V such that $(Lx)_v = L_v x_v$ for every $v \in \mathbf{h}$. We call the set of all such Lx the G-*genus* of L, and call the set of $L\alpha$ for all $\alpha \in G$ the G-*class* of L.

In our later treatment we will often use a quaternion algebra over a local or global field F. Whenever we deal with such an algebra B, we always denote by ι the main involution of B; we then put

$$(1.2) \qquad B^\circ = \{\, x \in B \mid x^\iota = -x \,\},$$

$\mathrm{Tr}_{B/F}(x) = x + x^\iota$, and $N_{B/F}(x) = xx^\iota$ for $x \in B$.

Given (V, φ) as in §1.1 over a local or global F, we call a $\mathfrak{g}$-lattice L in V *integral* if $\varphi[x] \in \mathfrak{g}$ for every $x \in L$, and call such an L *maximal* if L is the only integral lattice containing L. For an integral lattice L in V we denote by $A(L)$ the subring of $A(V)$ generated by $\mathfrak{g}$ and L, and put $A^+(L) = A(L) \cap A^+(V)$. For a $\mathfrak{g}$-lattice Λ in V, an element q in $F^\times$, and a fractional ideal $\mathfrak{b}$ in F, we put

$$(1.3\text{a}) \qquad \widetilde{\Lambda} = \{\, y \in V \mid 2\varphi(y, \Lambda) \subset \mathfrak{g} \,\},$$

$$(1.3\text{b}) \qquad \Lambda[q, \mathfrak{b}] = \{\, x \in V \mid \varphi[x] = q,\ \varphi(x, \Lambda) = \mathfrak{b} \,\},$$

(1.3c) $D(\Lambda) = \{\gamma \in O^\varphi(V) \mid \Lambda\gamma = \Lambda\}, \quad C(\Lambda) = D(\Lambda) \cap SO^\varphi(V) \quad (F \text{ local}).$

THEOREM 1.3. *If F is local, L is a maximal lattice in V, and $n > 2$, then* $\#\{L[q, \mathfrak{b}]/C(L)\} \le 1$.

This was given in [S3, Theorem 10.5] under the condition that *if n is odd, then $\delta(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$*; see [S3, (8.1)]. Our theorem says that this condition is unnecesary. It is sufficient to prove the case $\mathfrak{b} = 2^{-1}\mathfrak{g}$, since $cL[q, \mathfrak{b}] = L(c^2q, c\mathfrak{b}]$ for every $c \in F^\times$. We devote §§1.4 and 1.5 to the proof. To avoid possible misunderstandings, we note that a result which looks similar to the above theorem was stated in [E1, Satz 10.4]. This result of Eichler has no relevance to our theory, as it does not consider the set $\varphi(x, L)$, an essential ingredient of our theorem. Besides, we have $\#\{L[q, \mathfrak{b}]/C(L)\} = 2$ for certain nonmaximal L; see [S7, Theorem 4.2 and (4.3)].

1.4. Given (V, φ) over a local field F and a maximal lattice L in V, by Lemma 6.5 of [S3] we can find decompositions

$$V = Z \oplus U, \quad U = \sum_{i=1}^{r}(Fe_i + Ff_i), \quad \varphi(Z, U) = 0, \tag{1.4a}$$

$$L = M \oplus R, \quad R = \sum_{i=1}^{r}(\mathfrak{g}e_i + \mathfrak{g}f_i), \quad M = \{z \in Z \mid \varphi[z] \in \mathfrak{g}\}, \tag{1.4b}$$

$$2\varphi(e_i, f_j) = \delta_{ij}, \quad \varphi(e_i, e_j) = \varphi(f_i, f_j) = 0, \quad \varphi[z] \neq 0 \text{ for } 0 \neq z \in Z. \tag{1.4c}$$

We put $t = \dim(Z)$, and call it *the core dimension* of (V, φ). To prove Theorem 1.3, we assume hereafter until the end of §1.6 that n is odd and $\delta(\varphi)$ contains a prime element of F. Then t is 1 or 3. We denote by π any fixed prime element of F. We first note a few auxiliary facts:

(1.5) $\{x \in \mathfrak{g} \mid x - 1 \in 4\mathfrak{p}^m\} = \{a^2 \mid a - 1 \in 2\mathfrak{p}^m\}$ *if* $0 < m \in \mathbf{Z}$.

(1.6) *If* $k \in U$ *and* $2\varphi(k, R) = \mathfrak{g}$, *then* $k\alpha = e_1 + sf_1$ *with some* $\alpha \in D(R)$ *and* $s \in \mathfrak{g}$; α *can be taken from* $C(R)$ *if* $r > 1$.

(1.7) *If* $h \in L[q, 2^{-1}\mathfrak{g}]$, $\notin Z$, *then there exists an element* α *of* $C(L)$ *such that* $h\alpha = \pi^m(e_1 + sf_1) + z$ *with* $0 \le m \in \mathbf{Z}$, $s \in \mathfrak{g}$, *and* $z \in M$.

The first of these is [S3, Lemma 5.5 (i)]; (1.6) is proven in [S3, §10.7, (A1), (A2)]. Notice that the proof there is valid even when $\varphi[k] = 0$. Now let $h = k + w \in L[q, 2^{-1}\mathfrak{g}]$ with $k \in U$ and $w \in Z$. If $h \notin Z$, then $k \neq 0$, and we can put $2\varphi(k, R) = \mathfrak{p}^m$ with $0 \le m \in \mathbf{Z}$. By (1.6), there exists an element $\alpha_0 \in D(R)$ such that $\pi^{-m}k\alpha_0 = e_1 + sf_1$ with $s \in \mathfrak{g}$. Since $D(M)$ contains an element of determinant -1, we can extend α_0 to an element α of $C(L)$ such that $M\alpha = M$. This proves (1.7).

1.5. By virtue of (1.7), it is sufficient to prove Theorem 1.3 when $r \le 1$. If $r = 0$, then $L = M$ and $SO^\varphi(V) = C(L)$ by [S3, Lemma 6.4]. Therefore, if $n = t = 3$ and $\varphi[z] = \varphi[w]$ with $z, w \in V$, then by (1.1), $z = w\alpha$ with $\alpha \in C(L)$, which gives the desired fact. For this reason we hereafter assume that

$r = 1$, and write e and f for e_1 and f_1. We represent the elements of $O^\varphi(V)$ by $(n\times n)$-matrices with respect to $\{e, g_1, , \dots , g_t, f\}$, where $\{g_1, , \dots , g_t\}$ is a $\mathfrak{g}$-basis of M.

(A) Case $t = 1$. In this case $M = \mathfrak{g}g$ with an element g such that $\varphi[g]$ is a prime element of F. Thus we can take $\varphi[g]$ as π.

(a1) Suppose $L[q, 2^{-1}\mathfrak{g}] \cap Z \neq \emptyset$; let $w \in L[q, 2^{-1}\mathfrak{g}] \cap Z$ and $h \in L[q, 2^{-1}\mathfrak{g}]$. Then we can put $w = [0 \quad c \quad 0]$ with $c \in F$ such that $2c\mathfrak{p} = \mathfrak{g}$. By (1.1), $h = w\alpha$ with $\alpha \in SO^\varphi(V)$. Now $SO^\varphi(V) = PC(L)$ with the subgroup P of $SO^\varphi(V)$ consisting of the upper triangular elements; see [S3, Theorem 6.13 (ii)]. Put $\alpha = \beta\gamma$ with $\beta \in P$ and $\gamma \in C(L)$. The second row of β is of the form $[0 \quad 1 \quad j]$ with $j \in F$. Thus $h\gamma^{-1} = w\beta = [0 \quad c \quad cj]$, and so $cj \in \mathfrak{g}$. Since $2c\mathfrak{p} = \mathfrak{g}$, we can find an element p of $\mathfrak{g}$ such that $2c\pi p = cj$. Take the matrix

$$\eta = \begin{bmatrix} 1 & -p & -\pi p^2 \\ 0 & 1 & 2\pi p \\ 0 & 0 & 1 \end{bmatrix}. \tag{1.8}$$

Then $\eta \in C(L)$ and $w\eta = w\beta = h\gamma^{-1}$, which gives the desired fact.

(a2) Thus we assume that $L[q, 2^{-1}\mathfrak{g}] \cap Z = \emptyset$. Let $h \in L[q, 2^{-1}\mathfrak{g}]$. By (1.7) we can put $h = \pi^m(e + sf) + cg$ with $0 \le m \in \mathbf{Z}$ and $s, c \in \mathfrak{g}$. Then $q = \pi^{2m}s + \pi c^2$ and $\mathfrak{p}^m + 2c\mathfrak{p} = \mathfrak{g}$. Put $d = 2\pi c$. Suppose $d \in \mathfrak{g}^\times$. Then by (1.5), we can put $d^2 + 4\pi^{2m+1}s = d_1^2$ with $d_1 \in \mathfrak{g}^\times$. We easily see that $(2\pi)^{-1}d_1 g \in L[q, 2^{-1}\mathfrak{g}]$, a contradiction, as $g \in Z$. Thus $d \in \mathfrak{p}$, so that $m = 0$ and $h = e + sf + (2\pi)^{-1}dg$, and $q = s + (4\pi)^{-1}d^2$. Suppose we have another element $h_1 = e+s_1f+(2\pi)^{-1}d_1g$ with $s_1 \in \mathfrak{g}$ and $d_1 \in \mathfrak{p}$ such that $\varphi[h_1] = q$. Then $d_1^2 - d^2 = 4\pi(s - s_1) \in 4\mathfrak{p}$, and so $d_1 - d \in 2\mathfrak{p}$ or $d_1 + d \in 2\mathfrak{p}$. Since $-2d \in 2\mathfrak{p}$, we have $d_1 - d \in 2\mathfrak{p}$ in both cases. Let α be the element of (1.8) with $p = (d_1 - d)/(2\pi)$. Then $\alpha \in C(L)$ and $h = h_1\alpha \in h_1C(L)$. This completes the proof when $t = 1$.

(B) Case $t = 3$. As shown in [S3, §§7.3 and 7.7 (III)], there is a division quaternion algebra B over F with which we can put $Z = B^\circ$ and $2\varphi(x, y) = d\mathrm{Tr}_{B/F}(xy^\iota)$ for $x, y \in Z$, where d is an element of $F^\times$ that represents the determinant of the restriction of φ to Z. Thus we can take a prime element π of F as d; then $M = \{x \in Z \mid \pi xx^\iota \in \mathfrak{g}\}$. Let K be an unramified quadratic extension of F, $\mathfrak{r}$ the maximal order of K, and ρ the generator of $\mathrm{Gal}(K/F)$. We can put $B = K + K\eta$ with an element η such that $\eta^2 = \pi$ and $x\eta = \eta x^\rho$ for every $x \in K$. Take $u \in \mathfrak{r}$ so that $\mathfrak{r} = \mathfrak{g}[u]$ and put $\sigma = u - u^\rho$. Then $M = \mathfrak{g}\sigma + \mathfrak{r}\eta^{-1}$ and $\widetilde{M} = (2\mathfrak{p})^{-1}\sigma + \mathfrak{r}\eta^{-1}$. Since $r = 1$, φ is represented by a matrix

$$\begin{bmatrix} 0 & 0 & 2^{-1} \\ 0 & \zeta & 0 \\ 2^{-1} & 0 & 0 \end{bmatrix},$$

where ζ is an element of $\mathfrak{g}_3^3$ that represents the restriction of φ to Z. Define $\lambda = (\lambda_{ij}) \in \mathfrak{g}_3^3$ by $\lambda_{ii} = \zeta_{ii}$, $\lambda_{ij} = 2\zeta_{ij}$ if $i < j$ and $\lambda_{ij} = 0$ if $i > j$. Then $\lambda + {}^t\lambda = 2\zeta$. Let P be the subgroup of $SO^\varphi(V)$ consisting of the elements that send Ff onto itself, Then $SO^{\varphi}(V) = PC(L)$; see [S3, Theorem 6.13 (ii)].

(b1) Suppose $L[q,\, 2^{-1}\mathfrak{g}] \cap Z \neq \emptyset$. Let $h \in L[q,\, 2^{-1}\mathfrak{g}]$ and $w \in L[q,\, 2^{-1}\mathfrak{g}] \cap Z$. Identify w with a row vector $w = [0 \quad y \quad 0]$, where $y = (y_i)_{i=1}^{3}$ with $y_i \in \mathfrak{g}$. By (1.1), $h = w\alpha$ with $\alpha \in SO^{\varphi}(V)$. Put $\alpha = \beta\gamma$ with $\beta \in P$ and $\gamma \in C(L)$. The middle three rows of β can be written in the form $[0 \quad \varepsilon \quad j]$ with $\varepsilon \in SO^{\varphi}(Z)$ and a column vector j. Replacing γ by $\mathrm{diag}[1,\, \varepsilon,\, 1]\gamma$, we may assume that $\varepsilon = 1$. Then $h\gamma^{-1} = w\beta = [0 \quad y \quad yj]$ and $yj \in \mathfrak{g}$. Since $w \in L[q,\, 2^{-1}\mathfrak{g}]$, we see that $2y\zeta$ is primitive, and so we can find $p \in \mathfrak{g}_3^1$ such that $-2y\zeta \cdot {}^t p = yj$. Let

$$\psi = \begin{bmatrix} 1 & p & -p\lambda \cdot {}^t p \\ 0 & 1 & -2\zeta \cdot {}^t p \\ 0 & 0 & 1 \end{bmatrix}. \tag{1.9}$$

Then $\psi \in C(L)$ and $w\psi = w\beta = h\gamma^{-1}$, and so $h \in wC(L)$ as expected.

(b2) Let $h \in L[q,\, 2^{-1}\mathfrak{g}],\, \notin Z$. By (1.7) we may assume that $h = \pi^m(e + sf) + z$ with $0 \leq m \in \mathbf{Z}$, $s \in \mathfrak{g}$, and $z \in Z$. Put $z = (2\pi)^{-1}c\sigma + x\eta^{-1}$ with $c \in F$ and $x \in K$. Then $\mathfrak{g} = \mathfrak{p}^m + c\mathfrak{g} + \mathrm{Tr}_{K/F}(x\mathfrak{r})$, $q = \pi^{2m}s - \pi z^2$, and $\pi z^2 = (4\pi)^{-1}c^2\sigma^2 + xx^{\rho}$. Suppose $m > 0$; then $c \in \mathfrak{g}^{\times}$ or $x \in \mathfrak{r}^{\times}$. If $c \in \mathfrak{g}^{\times}$, then by (1.5) we can put $c^2 - 4\pi^{2m+1}\sigma^{-2}s = b^2$ with $b \in \mathfrak{g}^{\times}$. Put $w = (2\pi)^{-1}b\sigma + x\eta^{-1}$. Then we see that $w \in L[q,\, 2^{-1}\mathfrak{g}] \cap Z$. Next suppose $x \in \mathfrak{r}^{\times}$; then $xx^{\rho} - \pi^{2m}s \in \mathfrak{g}^{\times}$. Since $N_{K/F}(\mathfrak{r}^{\times}) = \mathfrak{g}^{\times}$, we can find $x_1 \in \mathfrak{r}^{\times}$ such that $x_1x_1^{\rho} = xx^{\rho} - \pi^{2m}s$. Put $x = (2\pi)^{-1}c\sigma + x_1\eta^{-1}$. Then $x \in L[q,\, 2^{-1}\mathfrak{g}] \cap Z$. Therefore, if $m > 0$, then the problem can be reduced to case (b1), which has been settled.

(b3) Thus if $L[q,\, 2^{-1}\mathfrak{g}] \cap Z = \emptyset$ and $h \in L[q,\, 2^{-1}\mathfrak{g}]$, then we may assume that $h = e + sf + z$ with $s \in \mathfrak{g}$ and $z \in Z$. Take another element $h_1 = e + s_1f + z_1 \in L[q,\, 2^{-1}\mathfrak{g}]$ with $s_1 \in \mathfrak{g}$ and $z_1 \in Z$. We have $z = (2\pi)^{-1}c\sigma + x\eta^{-1}$ and $z_1 = (2\pi)^{-1}c_1\sigma + x_1\eta^{-1}$ with $c,\, c_1 \in \mathfrak{g}$ and $x,\, x_1 \in \mathfrak{r}$. Since $s - \pi z^2 = s_1 - \pi z_1^2$, we have $(4\pi)^{-1}(c^2 - c_1^2) \in \mathfrak{g}$, so that $c^2 - c_1^2 \in 4\mathfrak{p}$. Then $c - c_1 \in 2\mathfrak{p}$ or $c + c_1 \in 2\mathfrak{p}$. Now the map $x\sigma + y\eta^{-1} \mapsto -x\sigma + y^{\rho}\eta^{-1}$ is an element of $C(M)$. Therefore, replacing z_1 by its image under this map if necessary, we may assume that $c - c_1 \in 2\mathfrak{p}$, which implies that $z - z_1 \in M$. Define ψ by (1.9) by taking p to be the vector that represents $z - z_1$. Then $h_1\psi = h$, which gives the desired fact.

1.6. We can now remove condition (8.1) from [S3, Lemma 10.8], which concerns the case where $t = 1$ and $r > 0$. To be precise, that lemma can be restated, without condition (8.1), as follows:

Let $L = \mathfrak{g}e_1 + \mathfrak{g}f_1 + \mathfrak{g}g$ with g such that $\mathfrak{p} \subset \varphi[g]\mathfrak{g} \subset \mathfrak{g}$, and let $h \in L[q,\, 2^{-1}\mathfrak{g}]$ with $q \in F^{\times}$. Then there exists an element γ of $C(L)$ such that $h\gamma = cg$ with c satisfying $2c\varphi[g]\mathfrak{g} = \mathfrak{g}$ or $h\gamma = ae_1 + f_1 + cg$ with $a \in \mathfrak{g}$ and $c \in 2^{-1}\mathfrak{g}$.

This follows from the discussions of (a1) and (a2) combined with (1.7).

1.7. Still asssuming F to be local, take the symbols as in (1.4a, b, c) with even or odd n, put $C = C(L)$ for simplicity, and define subgroups T and J of $G^{+}(V)$ by

$$T = \{\, \alpha \in G^+(V) \,|\, \tau(\alpha) \in C \},\tag{1.10}$$

$$J = \{\, \gamma \in T \,|\, \nu(\gamma) \in \mathfrak{g}^\times \,\}.\tag{1.11}$$

In [S3], Proposition 8.8, Theorems 8.6, and 8.9 we discussed the structure of $A(L)$, $A^+(L)$, $\nu(J)$, and the connection of $\tau(J)$ with C under the condition that $\delta(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$ if n is odd. Let us now prove the results in the cases in which the condition is not satisfied.

Theorem 1.8. *Suppose F is local, $1 < n-1 \in 2\mathbf{Z}$, and $\delta(\varphi)$ contains a prime element. Then the following assertions hold.*

(i) *If $t = 1$, then there exist an order $\mathfrak{O}$ in $M_2(F)$ of discriminant $\mathfrak{p}$ (see §5.1 for the definition) and an isomorphism θ of $A^+(V)$ onto $M_s\bigl(M_2(F)\bigr)$ that maps $A^+(L)$ onto $M_s(\mathfrak{O})$, where $s = 2^{r-1}$.*

(ii) *If $t = 3$, then there exist a division quaternion algebra B over F and an isomorphism $\xi : B^\circ \to Z$ such that $\varphi[x\xi] = dxx^\iota$ for every $x \in B^\circ$ with a prime element d of $F^\times$ independent of x, where B° is defined by (1.2). Moreover there exists an isomorphism θ of $A^+(V)$ onto $M_s(B)$ that maps $A^+(L)$ onto $M_s(\mathfrak{O})$, where $s = 2^r$ and $\mathfrak{O}$ is the unique maximal order in B.*

(iii) *In both cases $t = 1$ and $t = 3$ we have $\nu(J) = \mathfrak{g}^\times$, $C = \tau(T)$, $[C : \tau(J)] = 2$, and $T = F^\times(J \cup J\eta)$ with an element η such that $\eta \notin F^\times J$, $\eta^2 \in F^\times$, $J\eta = \eta J$, and $\nu(\eta)\mathfrak{g} = \mathfrak{p}$.*

This will be proved after the proof of Lemma 5.4.

Theorem 1.9. *In the setting of Theorem 1.3 with even or odd $n > 2$, let t be the core dimension of (V, φ) and let $\sigma : SO^\varphi(V) \to F^\times/F^{\times 2}$ be the spinor norm map of* [S3, (3.7)]. Then $\sigma(C) = \mathfrak{g}^\times F^{\times 2}$ in the following three cases: (i) $t = 0$; (ii) $t = 1$ *and* $\delta(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$; (iii) $t = 2$ *and* $\widetilde{L} = L$. *We have $\sigma(C) = F^\times$ in all the remaining cases.*

Proof. That $\sigma(C) = \mathfrak{g}^\times F^{\times 2}$ in the three cases specified above is shown by Proposition 8.8 (iii) and Theorem 8.9 (i) of [S3]. Therefore we assume that those cases do not apply. If $\delta(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$ or n is even, then Theorem 8.9 (ii) of [S3] shows that $\sigma(C) = F^\times$. If n is odd and $\delta(\varphi) \cap \mathfrak{g}^\times = \emptyset$, then from (iii) of Theorem 1.8 we obtain $\sigma(C) = \nu(T) = F^\times$, which completes the proof.

2. Global quadratic Diophantine equations

2.1. Let us now turn to the global case. The main theorems of [S3, Sections 11 through 13] were given under a condition stated in [S3, (9.2)]: *if n is odd, then $\delta(\varphi)$, at every nonarchimedean prime, contains a local unit.* By virtue of Theorem 1.3 we can now remove this condition from [S3, Theorem 11.6] and some others, which we will indicate in Remark 2.4 (3), (5), (6), and (7).

Throughout this section we assume that F is an algebraic number field. Given a quadratic space (V, φ) over F, we can define, for each $v \in \mathbf{v}$, the v-localization (V_v, φ_v) of (V, φ) as a quadratic space over F_v by putting $V_v = V \otimes_F F_v$ and extending φ to an F_v-valued quadratic form φ_v on V_v in a natural way.

In [S3, Section 13], we treated the equation $\varphi[h] = q$ not only for a scalar q, but also for a symmetric matrix q of size $n-1$. We now consider a more general case by taking a new approach. Given ${}^t q = q \in GL_m(F)$ and ${}^t\varphi = \varphi \in GL_n(F)$, we consider the solutions $h \in F_n^m$ of the equation $h\varphi \cdot {}^t h = q$. Here and throughout this and the next sections we assume that $n > 2$ and $n > m > 0$. More intrinsically, take (V, φ) as before and take also (X, q) with a nondegenerate quadratic form q on a vector space X over F of dimension m. We put

$$\mathscr{V} = \mathrm{Hom}(X, V), \tag{2.1}$$

and consider $h \in \mathscr{V}$ such that $\varphi[xh] = q[x]$ for every $x \in X$. Since q is nondegenerate, h must be injective. To simplify our notation, for every $k \in \mathscr{V}$ we denote by $\varphi[k]$ the quadratic form on X defined by $\varphi[k][x] = \varphi[xk]$ for every $x \in X$. Then our problem concerns the solutions $h \in \mathscr{V}$ of the equation $\varphi[h] = q$ for a fixed q. If $m = 1$ and $X = F$, then $q \in F^\times$, and an element h of V defines an element of $\mathscr{V}$ that sends c to ch for $c \in F$, and $\mathscr{V}$ consists of all such maps. Thus we can put $\mathscr{V} = V$ if $m = 1$ and the problem about $\varphi[h] = q$ with $q \in F^\times$ is the one-dimensional special case. For $m \geq 1$, if $h \in \mathscr{V}$ and $\det(\varphi[h]) \neq 0$, then

$$\{k \in \mathscr{V} \mid \varphi[k] = \varphi[h]\} = h \cdot SO^\varphi(V). \tag{2.2}$$

This is a generalization of (1.1) and follows easily from the Witt theorem; see [S3, Lemma 1.5 (i)].

For a fixed $h \in \mathscr{V}$ such that $\det\big(\varphi[h]\big) \neq 0$, put $W = (Xh)^\perp$, $G = SO^\varphi(V)$, and $H = SO^\varphi(W)$. We identify H with the subgroup of G consisting of the elements that are the identity map on Xh; thus

$$H = \{\alpha \in G \mid h\alpha = h\}. \tag{2.3}$$

For $\xi \in G_{\mathbf{A}}$ the symbol $h\xi$ is meaningful as an element of $\mathscr{V}_{\mathbf{A}}$, and so for a subset Ξ of $G_{\mathbf{A}}$ the symbol $h\Xi$ is meaningful as a subset of $\mathscr{V}_{\mathbf{A}}$.

THEOREM 2.2. *Let $D = D_0 G_{\mathbf{a}}$ with an open compact subgroup D_0 of $G_{\mathbf{h}}$. Then the following assertions hold.*

(i) *For $y \in G_{\mathbf{A}}$ we have $H_{\mathbf{A}} \cap GyD \neq \emptyset$ if and only if $\mathscr{V} \cap hDy^{-1} \neq \emptyset$.*

(ii) *Fixing $y \in G_{\mathbf{A}}$, for every $\varepsilon \in H_{\mathbf{A}} \cap GyD$ take $\alpha \in G$ so that $\varepsilon \in \alpha y D$. Then the map $\varepsilon \mapsto h\alpha$ gives a bijection of $H\backslash(H_{\mathbf{A}} \cap GyD)/(H_{\mathbf{A}} \cap D)$ onto $(\mathscr{V} \cap hDy^{-1})/\Gamma^y$, where $\Gamma^y = G \cap yDy^{-1}$.*

(iii) *Take $Y \subset G_{\mathbf{A}}$ so that $G_{\mathbf{A}} = \bigsqcup_{y \in Y} GyD$. Then*

$$\#\big\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)\big\} = \sum_{y \in Y} \#\big\{(\mathscr{V} \cap hDy^{-1})/\Gamma^y\big\}. \tag{2.4}$$

(iv) *In particular, suppose $m = 1$ and $n > 2$. With a fixed maximal lattice L in V put $C = \{\xi \in G_{\mathbf{A}} \mid L\xi = L\}$, $q = \varphi[h]$, and $\mathfrak{b} = \varphi(h, L)$. Then*

$$V \cap hCy^{-1} = (Ly^{-1})[q, \mathfrak{b}] \quad \textit{for every} \quad y \in G_{\mathbf{A}}. \tag{2.5}$$

Note: Since $H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)$ is a finite set, from (ii) we see that $(\mathscr{V} \cap hDy^{-1})/\Gamma^y$ is a finite set.

Proof. Let y, ε, and α be as in (ii); then clearly $h\alpha \in \mathscr{V} \cap hDy^{-1}$. If $\eta\varepsilon\zeta \in \beta yD$ with $\eta \in H$, $\zeta \in H_{\mathbf{A}} \cap D$, and $\beta \in G$, then $\beta^{-1}\eta\alpha \in G \cap yDy^{-1} = \Gamma^y$, and hence $h\alpha = h\eta\alpha \in h\beta\Gamma^y$. Thus our map is well defined. Next let $k \in \mathscr{V} \cap hDy^{-1}$. Then $k = h\delta y^{-1}$ with $\delta \in D$, and moreover, by (2.2), $k = h\xi$ with $\xi \in G$. Then $h = h\xi y\delta^{-1}$, so that $\xi y\delta^{-1} \in H_{\mathbf{A}}$ by (2.3). Thus $\xi y\delta^{-1} \in H_{\mathbf{A}} \cap GyD$. This shows that k is the image of an element of $H_{\mathbf{A}} \cap GyD$. To prove that the map is injective, suppose $\varepsilon \in \alpha yD \cap H_{\mathbf{A}}$ and $\delta \in \beta yD \cap H_{\mathbf{A}}$ with $\alpha, \beta \in G$, and $h\alpha = h\beta\sigma$ with $\sigma \in \Gamma^y$. Put $\omega = \beta\sigma\alpha^{-1}$. Then $h\omega = h$, so that $\omega \in H$. Since $\sigma \in yDy^{-1}$, we have $\beta yD = \beta\sigma yD = \omega\alpha yD$, and hence $\delta \in \beta yD \cap H_{\mathbf{A}} = \omega\alpha yD \cap H_{\mathbf{A}} = \omega(\alpha yD \cap H_{\mathbf{A}}) = \omega(\varepsilon D \cap H_{\mathbf{A}}) = \omega\varepsilon(D \cap H_{\mathbf{A}}) \subset H\varepsilon(D \cap H_{\mathbf{A}})$. This proves the injectivity, and completes the proof of (ii). At the same time we obtain (i).

Now $H_{\mathbf{A}} = \bigsqcup_{y\in Y}(H_{\mathbf{A}} \cap GyD)$, and so (iii) follows immediately from (ii). As for (iv), clearly $V \cap hC \subset L[q, \mathfrak{b}]$. Conversely, every element of $L[q, \mathfrak{b}]$ belongs to hC by virtue of Theorem 1.3. Thus

$$V \cap hC = L[q, \mathfrak{b}]. \tag{2.6}$$

Let $k \in V \cap hCy^{-1}$ with $y \in G_{\mathbf{A}}$; put $M = Ly^{-1}$. Then $\varphi[k] = q$, $\varphi\bigl(k, M\bigr) = \varphi(h, L) = \mathfrak{b}$, and $kyCy^{-1} = hCy^{-1}$. Taking k, M, and yCy^{-1} in place of h, L and C in (2.6), we obtain $V \cap hCy^{-1} = V \cap kyCy^{-1} = M[q, \mathfrak{b}] = (Ly^{-1})[q, \mathfrak{b}]$. This proves (2.5) when $V \cap hCy^{-1} \neq \emptyset$. To prove the remaining case, suppose $\ell \in (Ly^{-1})[q, \mathfrak{b}]$; then $\varphi(\ell y_v, L_v) = \mathfrak{b}_v = \varphi(h, L)_v$ for every $v \in \mathbf{h}$. By Theorem 1.3, $\ell y \in hC$, and hence $\ell \in hCy^{-1}$. This shows that if $(Ly^{-1})[q, \mathfrak{b}] \neq \emptyset$, then $V \cap hCy^{-1} \neq \emptyset$, and hence (2.5) holds for every $y \in G_{\mathbf{A}}$. This completes the proof.

If k and ℓ are two elements of $\mathscr{V} \cap hDy^{-1}$, then $k = \ell x_v$ with $x_v \in y_vD_vy_v^{-1}$ for every $v \in \mathbf{h}$. Therefore we are tempted to say that *k and ℓ belong to the same genus.* Then each orbit of $(\mathscr{V} \cap hDy^{-1})/\Gamma^y$ may be called a *class.* Thus (ii) of Theorem 2.2 connects such classes of elements of $\mathscr{V}$ with the classes of H with respect to $H_{\mathbf{A}} \cap D$.

Combining (2.4) with (2.5), we obtain, in the setting of (iv),

$$\#\bigl\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)\bigr\} = \sum_{y\in Y} \#\bigl\{(Ly^{-1})[q, \mathfrak{b}]/\Gamma^y\bigr\}. \tag{2.7}$$

This was stated in [S3, (11.7)] under the condition mentioned at the beginning of this section, which we can now remove.

The above theorem concerns $SO^\varphi\bigl((Xh)^\perp\bigr)$. Let us now show that we can formulate a result with respect to $SO^q(X)$ instead, when $m = n - 1$. The notation being as above, put $Y = Xh$ and $J = SO^\varphi(Y)$. We identify J with $\bigl\{\alpha \in G \bigm| \alpha = \text{id. on } W\bigr\}$. For every $\delta \in J$ there is a unique element δ' of $SO^q(X)$ such that $\delta' h = h\delta$, and $\delta \mapsto \delta'$ gives an isomorphism of J onto $SO^q(X)$. In this section we employ the symbol δ' always in this sense. We note a simple fact:

(2.8) *If $m = n - 1$ and $h\xi = h\eta$ for $\xi, \eta \in G_{\mathbf{A}}$, then $\xi = \eta$.*

Indeed, for each $v \in \mathbf{v}$ we have $h\xi_v\eta_v^{-1} = h$, and so $\xi_v\eta_v^{-1}$ is the identity map on $X_v h$. Since $m = n-1$, it must be the identity map on the whole V_v. Thus $\xi_v\eta_v^{-1} = 1$ for every $v \in \mathbf{v}$, which proves (2.8).

THEOREM 2.3. *Let $D = D_0 G_{\mathbf{a}}$ as in Theorem 2.2 and let $E = E_0 J_{\mathbf{a}}$ with an open compact subgroup E_0 of $J_{\mathbf{h}}$. Suppose $m = n-1$ and $J_{\mathbf{A}} \cap D \subset E$. Then for every $z \in J_{\mathbf{A}}$ and $y \in G_{\mathbf{A}}$ there exists a bijection*

$$J\backslash(JzE \cap GyD)/(J_{\mathbf{A}} \cap D) \longrightarrow \Delta'\backslash(\mathscr{V} \cap hzEDy^{-1})/\Gamma, \tag{2.9}$$

where $\Gamma = yDy^{-1} \cap G$ and $\Delta' = \{\delta' \mid \delta \in \Delta\}$, $\Delta = zEz^{-1} \cap J$.

Proof. Given $\sigma \in JzE \cap GyD$, take $\alpha \in G$ and $\beta \in J$ so that $\sigma \in \beta zE \cap \alpha yD$, and put $k = h\beta^{-1}\alpha$. Then $k \in \mathscr{V} \cap hzEDy^{-1}$. If $\sigma \in \beta_1 zE \cap \alpha_1 yD$ with $\alpha_1 \in G$ and $\beta_1 \in J$, then $\beta_1^{-1}\beta \in \Delta$ and $\alpha_1^{-1}\alpha \in \Gamma$, and so $\sigma \to h\beta^{-1}\alpha$ is a well-defined map as in (2.9). To show that it is surjective, take $k \in \mathscr{V} \cap hzEDy^{-1}$; then $\varphi[k] = q$, and so $k = h\alpha$ with $\alpha \in G$ by (2.2). We have also $k = hz\varepsilon\zeta y^{-1}$ with $\varepsilon \in E$ and $\zeta \in D$. By (2.8), $z\varepsilon\zeta y^{-1} = \alpha$, and so $z\varepsilon = \alpha y\zeta^{-1} \in zE \cap \alpha yD$. This shows that k is the image of $z\varepsilon$, which proves the surjectivity. To prove the injectivity, let $\sigma \in \beta zE \cap \alpha yD$ and $\sigma_1 \in \beta_1 zE \cap \alpha_1 yD$ with $\alpha, \alpha_1 \in G$ and $\beta, \beta_1 \in E$. Suppose $h\beta_1^{-1}\alpha_1 = \delta' h\beta^{-1}\alpha\gamma$ with $\delta \in \Delta$ and $\gamma \in \Gamma$. Then $\beta_1^{-1}\alpha_1 = \delta\beta^{-1}\alpha\gamma$ by (2.8). Put $\lambda = \alpha\gamma\alpha_1^{-1}$. Then $\lambda = \beta\delta^{-1}\beta_1^{-1} \in J$. Since $\gamma \in yDy^{-1}$, we have $\sigma \in \alpha yD = \alpha\gamma yD = \lambda\alpha_1 yD = \lambda\sigma_1 D \subset J\sigma_1 D$. Also, since $\sigma, \sigma_1 \in J_{\mathbf{A}}$, we have $\sigma \in J\sigma_1(J_{\mathbf{A}} \cap D)$. This proves the injectivity, and completes the proof.

REMARK 2.4. (1) We can take $E = J_{\mathbf{A}} \cap D$ in the above theorem. Then (2.9) takes a simpler form

$$J\backslash(JzE \cap GyD)/E \longrightarrow \Delta'\backslash(\mathscr{V} \cap hzDy^{-1})/\Gamma, \tag{2.10}$$

(2) Let $G_{\mathbf{A}} = \bigsqcup_{y \in Y} GyD$ as in Theorem 2.2 and let $J_{\mathbf{A}} = \bigsqcup_{z \in Z} JzE$ with a finite subset Z of $J_{\mathbf{A}}$. Then $J_{\mathbf{A}} = \bigsqcup_{z,y}(JzE \cap GyD)$. For each (z, y) such that $JzE \cap GyD \neq \emptyset$ pick $\xi \in JzE \cap GyD$ and denote by Ξ the set of all such ξ. Then $J_{\mathbf{A}} = \bigsqcup_{\xi \in \Xi}(J\xi E \cap G\xi D)$, and we obtain

$$\#\{J\backslash J_{\mathbf{A}}/(J_{\mathbf{A}} \cap D)\} = \sum_{\xi \in \Xi} \#\{\Delta'_\xi\backslash(\mathscr{V} \cap h\xi ED\xi^{-1})/\Gamma^\xi\}, \tag{2.11}$$

where $\Gamma^\xi = \xi D\xi^{-1} \cap G$ and $\Delta'_\xi = \{\delta' \mid \delta \in J \cap \xi E\xi^{-1}\}$.

(3) For $\ell \in V$ let us denote by $\varphi(h, \ell)$ the element of $\mathrm{Hom}(X, F)$ defined by $x\varphi(h, \ell) = \varphi(xh, \ell)$ for $x \in X$; then for a subset S of V let us put $\varphi(h, S) = \{\varphi(h, s) \mid s \in S\}$. Now, fixing a maximal lattice L in V, put $\Lambda = \widetilde{L}$, $\mathfrak{B} = \varphi(h, \Lambda)$, and $E = \{\varepsilon \in J_{\mathbf{A}} \mid \varepsilon'\mathfrak{B} = \mathfrak{B}\}$. Since $\mathfrak{B}$ is a $\mathfrak{g}$-lattice in $\mathrm{Hom}(X, F)$, we see that E is a subgroup of $J_{\mathbf{A}}$ of the type considered in Theorem 2.3. Then we can prove

$$\mathscr{V} \cap hzEDy^{-1} = \{k \in \mathscr{V} \mid \varphi[k] = q,\ \varphi(k, \Lambda y^{-1}) = z'\mathfrak{B}\}. \tag{2.12}$$

This is similar to (2.5), and proved in the proof of [S3, Theorem 13.10]. It should be noted that condition (9.2) imposed in that theorem and also (8.1) in [S3 Theorem 13.8] are unnecessary for the reason explained at the beginning of this section.

(4) Suppose $m = n - 1$ in the setting of Theorem 2.2; then $H = \{1\}$. Therefore $H_{\mathbf{A}} \cap GyD \neq \emptyset$ only when $GyD = GD$. Then (2.4) gives $\#\big\{(\mathscr{V} \cap hD)/(G \cap D)\big\} = 1$, but this is an immediate consequence of (2.2).

(5) Let us note some more statements in [S3] from which condition (9.2) of [S3] can be removed. First of all, that is the case with Theorem 9.26 of [S3]. In fact, we can state an improved version of that theorem as follows. Using the notation employed in the theorem, let $\mathfrak{I}'_\varphi$ be the subgroup of $\mathfrak{I}$ generated by $\mathfrak{I}_0$ and the prime ideals for which $\sigma(C_v) = F_v^\times$. (Such prime ideals are determined by Theorem 1.9.) *Then* $\#\{SO^\varphi\backslash SO^\varphi_{\mathbf{A}}/C) = [\mathfrak{I} : \mathfrak{I}'_\varphi]$ *for* C *of* [S3, (9.15)], which equals C of Theorem 2.2 (iv). The last group index is 1 if $F = \mathbf{Q}$, and so the genus of maximal lattices consists of a single class. Consequently we can state a clear-cut result as follows. Let $\mathfrak{S}_n$ denote the set of symmetric matrices of $GL_n(\mathbf{Q})$ that represent $\mathbf{Z}$-valued quadratic forms on $\mathbf{Z}^n$, and $\mathfrak{S}_n^0$ the subset of $\mathfrak{S}_n$ consisting of the reduced elements of $\mathfrak{S}_n$ in the sense of [S5], that is, the set of $\Phi \in \mathfrak{S}_n$ which cannot be represented nontrivially over $\mathbf{Z}$ by another element of $\mathfrak{S}_n$. For $\Phi \in \mathfrak{S}_n$ put $\sigma(\Phi) = p - q$ where Φ as a real matrix has p positive and q negative eigenvalues. Now the number of genera of $\Phi \in \mathfrak{S}_n^0$ with given $\sigma(\Phi)$ and $\det(2\Phi)$ was determined in [S5, Theorem 6.6]. If $n \geq 3$ and $\sigma(\Phi) \neq n$, then the number of genera of Φ given there equals the number of classes, as each genus of maximal lattices consists of a single class as explained above.

(6) Next, (9.2) is unnecessary in Theorem 12.1 of [S3]. What we need, in addition to Theorem 1.3, is the following fact: *If* $v \in \mathbf{h}$, $\varphi[h]\mathfrak{g}_v = \varphi(h,\, L_v)^2$, *then* $L_v \cap W_v$ *is maximal and* $C \cap H_v = \big\{\alpha \in H_v \,\big|\, (L_v \cap W_v)\alpha = L_v \cap W_v\big\}$. Here the notation is the same as in the proof of Theorem 12.1. The statement is valid irrespective of the nature of L_v and t_v. Indeed, replacing h by an element of $F^\times h$, we may assume that $\varphi[h]\mathfrak{g}_v = \varphi(h,\, L_v) = \mathfrak{g}_v$. Then, by Lemma 10.2 (i) of [S3], we have $L_v = \mathfrak{g}_v h \oplus (L_v \cap W_v)$, from which we immediately obtain the expected facts on $L_v \cap W_v$. Consequently, $\mathfrak{g}_v^\times \subset \sigma(C \cap H_v)$ by Theorem 1.9, as $n - 1 > 2$, and the original proof of Theorem 12.1 is valid without (9.2).

(7) In [S4] we proved a result of type (2.7) in terms of $G^+(V)$, but imposed the condition that *if* n *is odd, then* $\det(\varphi)\mathfrak{g}$ *is a square in the ideal group of* F; see Theorem 1.6 (iv) of [S4]. We can remove this condition by virtue of Theorem 1.3.

3. New mass formulas

3.1. We first recall the symbols $\mathfrak{m}(G, D)$ and $\nu(\Gamma)$ introduced in [S1] and [S2]. Here $G = SO^\varphi(V)$ and D is an open subgroup of $G_{\mathbf{A}}$ containing $G_{\mathbf{a}}$ and such that $D \cap G_{\mathbf{h}}$ is compact. Fixing such a D, we put $\Gamma^a = G \cap aDa^{-1}$ for every $a \in G_{\mathbf{A}}$. Let $C_{\mathbf{a}}$ be a maximal compact subgroup of $G_{\mathbf{a}}$ and let $\mathscr{Z} = G_{\mathbf{a}}/C_{\mathbf{a}}$.

Then $\mathscr{Z}$ is a symmetric space on which G acts through its projection into $G_{\mathbf{a}}$. Taking a complete set of representatives $\mathscr{B}$ for $G\backslash G_{\mathbf{A}}/D$, we put

$$\mathfrak{m}(G,\, D) = \mathfrak{m}(D) = \sum_{a\in\mathscr{B}} \nu(\Gamma^a). \tag{3.1}$$

Here $\nu(\Gamma)$ is a quantity defined by

$$\nu(\Gamma) = \begin{cases} [\Gamma:1]^{-1} & \text{if } G_{\mathbf{a}} \text{ is compact,} \\ \mathrm{vol}(\Gamma\backslash\mathscr{Z})/\#(\Gamma\cap\{\pm1\}) & \text{otherwise.} \end{cases} \tag{3.2}$$

We fix a Haar measure on $G_{\mathbf{a}}$, which determines a unique $G_{\mathbf{a}}$-invariant measure on $\mathscr{Z}$ by a well known principle. (In fact, $\mathfrak{m}(D)$ and $\nu(\Gamma)$ are the measure of $D\cap G_{\mathbf{a}}$ and that of $\Gamma\backslash G_{\mathbf{a}}$; see [S6, Theorem 9].) We easily see that $\mathfrak{m}(D)$ does not depend on the choice of $\mathscr{B}$. We call $\mathfrak{m}(G,\, D)$ *the mass of G relative to D*. If D' is a subgroup of $G_{\mathbf{A}}$ of the same type as D and $D'\subset D$, then, as proven in [S1, Lemma 24.2 (1)],

$$\mathfrak{m}(G,\, D') = [D:D']\mathfrak{m}(G,\, D). \tag{3.3}$$

Next, in the setting of §2.1 we consider a subset S of $\mathscr{V}$ of the form $S = \bigsqcup_{\zeta\in Z} h\zeta\Gamma$, where h is as in (2.2), Z is a finite subset of G, and $\Gamma = G\cap D$ with D as above. Then we put

$$\mathfrak{m}(S) = \sum_{\zeta\in Z} \nu(\Delta_\zeta)/\nu(\Gamma), \quad \Delta_\zeta = H\cap\zeta\Gamma\zeta^{-1}, \tag{3.4}$$

and call $\mathfrak{m}(S)$ the *mass* of S. Here, to define $\nu(\Delta_\zeta)$, we need to fix a measure on $H_{\mathbf{a}}$. Thus $\mathfrak{m}(S)$ depends on the choice of measures on $G_{\mathbf{a}}$ and $H_{\mathbf{a}}$, but $\mathfrak{m}(S)$ is independent of the choice of Z and Γ. (Let $\mathfrak{Y} = \{x\in\mathscr{V}_{\mathbf{a}} \,|\, \varphi[x] = q\}$. Since $\mathfrak{Y}$ can be identified with $H_{\mathbf{a}}\backslash G_{\mathbf{a}}$, once a measure on $G_{\mathbf{a}}$ is fixed, a measure on $\mathfrak{Y}$ determines a measure on $H_{\mathbf{a}}$, and vice versa. The replacement of h by an element of hG changes the group H, but that does not change $\mathfrak{m}(S)$ if we start with a fixed measure on $\mathfrak{Y}$. Notice also that an identification of $\mathscr{V}_{\mathbf{a}}$ with a Euclidean space determines a $G_{\mathbf{a}}$-invariant measure on $\mathfrak{Y}$.) Since the left-hand side of (2.4) is finite, we see that $(\mathscr{V}\cap hDy^{-1})/\Gamma^y$ is a finite set for every $y\in G_{\mathbf{A}}$. Thus we can define $\mathfrak{m}(\mathscr{V}\cap hDy^{-1})$ for every $y\in G_{\mathbf{A}}$.

If $G_{\mathbf{a}}$ is compact, we naturally take the measures of $G_{\mathbf{a}}$ and $H_{\mathbf{a}}$ to be 1. Then $\mathfrak{m}(S)$ can be defined in a unique way. We easily see that $S = \bigsqcup_{\zeta\in Z}\bigsqcup_{\gamma\in\Delta'_\zeta\backslash\Gamma} h\zeta\gamma$, where $\Delta'_\zeta = \zeta^{-1}\Delta_\zeta\zeta$, and so $\#S = \sum_{\zeta\in Z}[\Gamma:\Delta'_\zeta] = \mathfrak{m}(S)$ if $G_{\mathbf{a}}$ is compact. Thus we obtain

$$\mathfrak{m}(S) = \#(S) \quad \text{if } G_{\mathbf{a}} \text{ is compact.} \tag{3.5}$$

THEOREM 3.2. *The notation being the same as in Theorem 2.2, we have*

$$\mathfrak{m}(H,\, H_{\mathbf{A}}\cap D) = \sum_{y\in Y} \nu(\Gamma^y)\mathfrak{m}(\mathscr{V}\cap hDy^{-1}). \tag{3.6}$$

In particular if $m=1$ and the notation is as in (iv) *of Theorem 2.2, then*

(3.7) $$\mathfrak{m}(H,\, H_{\mathbf{A}}\cap C) = \sum_{y\in Y}\nu(\Gamma^y)\mathfrak{m}\bigl((Ly^{-1})[q,\, \mathfrak{b}]\bigr).$$

Proof. Let $E_y = H\backslash(H_{\mathbf{A}}\cap GyD)/(H_{\mathbf{A}}\cap D)$. For each $\varepsilon\in E_y$ take $\zeta_\varepsilon\in G$ so that $\varepsilon\in\zeta_\varepsilon yD$. By Theorem 2.2 (ii) we have $\mathscr{V}\cap hDy^{-1} = \bigsqcup_{\varepsilon\in E_y} h\zeta_\varepsilon\Gamma^y$ and $H\cap\varepsilon(H_{\mathbf{A}}\cap D)\varepsilon^{-1} = H\cap H_{\mathbf{A}}\cap\varepsilon D\varepsilon^{-1} = H\cap\zeta_\varepsilon yDy^{-1}\zeta_\varepsilon^{-1} = H\cap\zeta_\varepsilon\Gamma^y\zeta_\varepsilon^{-1}$, so that

$$\nu(\Gamma^y)\mathfrak{m}(\mathscr{V}\cap hDy^{-1}) = \sum_{\varepsilon\in E_y}\nu(H\cap\zeta_\varepsilon\Gamma^y\zeta_\varepsilon^{-1}) = \sum_{\varepsilon\in E_y}\nu(H\cap\varepsilon(H_{\mathbf{A}}\cap D)\varepsilon^{-1}).$$

Since $\bigsqcup_{y\in Y} E_y$ gives $H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}}\cap D)$, we obtain

$$\mathfrak{m}(H,\, H_{\mathbf{A}}\cap D) = \sum_{y\in Y}\sum_{\varepsilon\in E_y}\nu(H\cap\varepsilon(H_{\mathbf{A}}\cap D)\varepsilon^{-1}) = \sum_{y\in Y}\nu(\Gamma^y)\mathfrak{m}(\mathscr{V}\cap hDy^{-1}).$$

This proves (3.6), which combined with (2.5) gives (3.7).

Formula (3.7) was given in [S3, (13.17b)] under the condition mentioned at the beginning of Section 2. That condition can be removed by the above theorem.

It should be noted that (3.6) and (3.7) are different from any of the mass formulas of Siegel. Indeed, the left-hand side of (3.6) concerns an orthogonal group in dimension $n-m$, and the right-hand side concerns the space $\mathscr{V}$, whereas both sides of Siegel's formulas are defined with respect to matrices of the same size. See also [S3, p. 137] for a comment on the connection with the work of Eisenstein and Minkowski on the sums of five squares.

4. Classification and genera of quadratic forms in terms of matrices

4.1. Traditionally the genus and class of a quadratic form over $\mathbf{Q}$ were defined in terms of matrices, but it is easy to see that they are equivalent to those defined in terms of lattices. In the general case, however, there is a standard definition in terms of lattices, but the definition in terms of matrices is nontrivial. Also, we treated in [S5] the classification of quadratic forms over a number field, but gave explicit results in terms of matrices only when $\mathbf{Q}$ is the base field. Let us now discuss how we can handle such problems over an arbitrary number field, as the generalization is far from obvious and requires some new concepts. Before proceeding, we recall two basic facts: Given $(V,\, \varphi)$ over a global F and a lattice L in V, the $O^\varphi(V)$-genus of L is the same as the $SO^\varphi(V)$-genus of L; all the maximal lattices in V form a single $O^\varphi(V)$-genus; see [S3, Lemmas 6.8 and 6.9].

We take a global field F, and denote by F_n^1 the vector space of all n-dimensional row vectors with components in F, and by $\mathfrak{g}_n^1$ the set of elements of F_n^1 with components in $\mathfrak{g}$. Define subgroups E and E_ξ of $GL_n(F)_{\mathbf{A}}$ by

(4.1) $$E = GL_n(F)_{\mathbf{a}}\prod_{v\in\mathbf{h}} GL_n(\mathfrak{g}_v), \qquad E_\xi = \xi^{-1}E\xi \quad (\xi\in GL_n(F)_{\mathbf{A}}).$$

Put $L_0 = \mathfrak{g}_n^1$. An arbitrary $\mathfrak{g}$-lattice L in F_n^1 can be given as $L = L_0\xi$ with $\xi \in GL_n(F)_\mathbf{A}$; then $E_\xi = \{y \in GL_n(F)_\mathbf{A} \mid Ly = L\}$. It is well known that the map $x \mapsto \det(x)\mathfrak{g}$ gives a bijection of $E\backslash GL_n(F)_\mathbf{A}/GL_n(F)$ onto the ideal class group of F; see [S1, Lemma 8.14], for example. Thus the ideal class of $\det(\xi)\mathfrak{g}$ is determined by the $GL_n(F)$-class of $L_0\xi$, and vice versa. Consequently, L is isomorphic as a $\mathfrak{g}$-module to the direct sum of $\mathfrak{g}_{n-1}^1$ and $\det(\xi)\mathfrak{g}$.

To define the generalization of $\mathbf{Z}$-valued quadratic forms, we denote by S_n the set of all symmetric elements of $GL_n(F)$, fix an element ξ of $GL_n(F)_\mathbf{A}$, and denote by $S_n(\xi)$ the set of all $T \in S_n$ such that $xT \cdot {}^t x \in \mathfrak{g}$ for every $x \in L_0\xi$. We call such a T *reduced* (relative to ξ) if the following condition is satisfied:

$$T \in S_n(\zeta^{-1}\xi) \text{ with } \zeta \in GL_n(F)_\mathbf{h} \cap \prod_{v\in\mathbf{h}} M_n(\mathfrak{g}_v) \implies \zeta \in E. \tag{4.2}$$

We denote by $S_n^0(\xi)$ the set of all reduced elements of $S_n(\xi)$. These depend essentially on $E\xi GL_n(F)$, as will be seen in Proposition 4.3 (i) below.

4.2. To define the genus and class of an element of S_n, put

$$\Delta_\xi = E_\xi \cap GL_n(F), \qquad \Delta_\xi^1 = E_\xi \cap SL_n(F). \tag{4.3}$$

We say that two elements Φ and Ψ of $S_n(\xi)$ belong to the same *genus* (relative to ξ) if there exists an element ε of E_ξ such that $\varepsilon\Phi \cdot {}^t\varepsilon = \Psi$; they are said to belong to the same *O-class* (resp. *SO-class*) if $\alpha\Phi \cdot {}^t\alpha = \Psi$ for some $\alpha \in \Delta_\xi$ (resp. $\alpha \in \Delta_\xi^1$). These depend on the choice of $L = L_0\xi$, or rather, on the choice of the ideal class of $\det(\xi)\mathfrak{g}$. There is no reason to think that $\xi = 1$ is the most natural choice.

Given $\Phi \in S_n$, put $V = F_n^1$ and $\varphi[x] = x\Phi \cdot {}^t x$ for $x \in V$. Then we obtain a quadratic space (V, φ), which we denote by $[\Phi]$; we put then $O(\Phi) = O^\varphi(V)$ and $SO(\Phi) = SO^\varphi(V)$. Now put $L = L_0\xi$ with $\xi \in GL_n(F)_\mathbf{A}$. Clearly L is integral if $\Phi \in S_n(\xi)$, in which case L is maximal if and only if $\Phi \in S_n^0(\xi)$.

PROPOSITION 4.3. (i) *If $\eta \in E\xi\alpha$ with $\xi, \eta \in GL_n(F)_\mathbf{A}$ and $\alpha \in GL_n(F)$, then $S_n(\xi) = \alpha S_n(\eta) \cdot {}^t\alpha$ and $S_n^0(\xi) = \alpha S_n^0(\eta) \cdot {}^t\alpha$.*

(ii) *For $\Phi, \Psi \in S_n^0(\xi)$, $\xi \in GL_n(F)_\mathbf{A}$, the spaces $[\Phi]$ and $[\Psi]$ are isomorphic if and only if they belong to the same genus.*

(iii) *Let X be a complete set of representatives for $E\backslash GL_n(F)_\mathbf{A}/GL_n(F)$ and for each $\xi \in GL_n(F)_\mathbf{A}$ let Y_ξ be a complete set of representatives for the genera of the elements of $S_n^0(\xi)$. Then the spaces $[\Phi]$ obtained from $\Phi \in Y_\xi$ for all $\xi \in X$ exhaust all isomorphism classes of n-dimensional quadratic spaces over F without overlapping.*

Proof. Assertion (i) can be verified in a straightforward way. Let Φ and Ψ be elements of $S_n^0(\xi)$ belonging to the same genus. Then there exists an element $\varepsilon \in E_\xi$ such that $\varepsilon\Phi \cdot {}^t\varepsilon = \Psi$, and the Hasse principle guarantees an element α of $GL_n(F)$ such that $\Psi = \alpha\Phi \cdot {}^t\alpha$. Thus $[\Psi]$ is isomorphic to $[\Phi]$. Conversely, suppose $[\Phi]$ and $[\Psi]$ are isomorphic for $\Phi, \Psi \in S_n^0(\xi)$. Then $\Phi = \beta\Psi \cdot {}^t\beta$ for some $\beta \in GL_n(F)$. Now $L_0\xi$ is maximal in both $[\Phi]$ and $[\Psi]$, and $L_0\xi\beta$ is maximal in $[\Psi]$. Thus $L_0\xi\beta = L_0\xi\gamma$ with $\gamma \in O(\Psi)_{\mathbf{A}}$. Put $\zeta = \beta\gamma^{-1}$. Then $\zeta \in E_\xi$, and $\zeta\Psi \cdot {}^t\zeta = \Phi$. Therefore Ψ belongs to the genus of Φ. This proves (ii). As for (iii), clearly every n-dimensional quadratic space is isomorphic to $[\Psi]$ for some $\Psi \in S_n$. Putting $V = F_n^1$, pick a maximal lattice L in V and put $L = L_0\eta$ with $\eta \in GL_n(F)_{\mathbf{A}}$. Then $\eta \in E\xi GL_n(F)$ for some $\xi \in X$, and by (i) we can replace η by ξ. Take a member Φ of Y_ξ belonging to the genus of Ψ. Then by (ii), $[\Psi]$ is isomorphic to $[\Phi]$. Thus every n-dimensional quadratic space is isomorphic to $[\Phi]$ for some $\Phi \in Y_\xi$ with $\xi \in X$. To prove that there is no overlapping, take $\Phi_i \in Y_{\xi_i}$ with $\xi_i \in X$, $i = 1, 2$, and suppose that $[\Phi_1]$ is isomorphic to $[\Phi_2]$. Then $\Phi_1 = \alpha\Phi_2 \cdot {}^t\alpha$ with $\alpha \in GL_n(F)$. Now $L_0\xi_1$ is maximal in $[\Phi_1]$, and so $L_0\xi_1\alpha$ is maximal in $[\Phi_2]$. Therefore $L_0\xi_1\alpha = L_0\xi_2\gamma$ with $\gamma \in O(\Phi_2)_{\mathbf{A}}$. Then $\xi_1\alpha\gamma^{-1}\xi_2^{-1} \in E$, and so $\det(\xi_1\xi_2^{-1}) \in F^\times \det(E)$, which implies that $\xi_1 = \xi_2$, as $\xi_i \in X$. Thus both Φ_1 and Φ_2 belong to Y_{ξ_1}. By (ii) they must belong to the same genus. This completes the proof.

4.4. Take $\Phi \in S_n^0(\xi)$ and suppose another member Ψ of$S_n^0(\xi)$ belongs to the genus of Φ. Put $L = L_0\xi$. Then $\Psi = \varepsilon\Phi \cdot {}^t\varepsilon = \alpha\Phi \cdot {}^t\alpha$ with $\varepsilon \in E_\xi$ and $\alpha \in GL_n(F)$, as observed in the above proof. Clearly $\varepsilon^{-1}\alpha \in O(\Phi)_{\mathbf{A}}$. Since $L\alpha = L\varepsilon^{-1}\alpha$, we see that $L\alpha$ belongs to the genus of L. We associate the $O(\Phi)$-class of $L\alpha$ to the O-class of Ψ. We easily see that the class of $L\alpha$ is determined by the class of Ψ. Moreover, it gives a bijection of the set of O-classes in the genus of Φ onto the set of $O(\Phi)$-classes in the genus of $L_0\xi$. Indeed, let $M = L\sigma$ with $\sigma \in SO(\Phi)_{\mathbf{A}}$. Then $\det(\sigma)\mathfrak{g} = \mathfrak{g}$, and so $\sigma = \tau\beta$ with $\tau \in E_\xi$ and $\beta \in GL_n(F)$. Put $\Psi = \tau^{-1}\Phi \cdot {}^t\tau^{-1}$. Then $\Psi = \beta\Phi \cdot {}^t\beta$ and $M = L\beta$, which corresponds to Ψ. This proves the surjectivity. The injectivity can be easily verified too.

For $\Phi \in S_n^0(\xi)$ we define the *SO-genus* of Φ to be the set of all Ψ in the genus of Φ such that $\det(\Psi) = \det(\Phi)$. For $\Psi = \varepsilon\Phi \cdot {}^t\varepsilon = \alpha\Phi \cdot {}^t\alpha$ as above, suppose $\det(\Psi) = \det(\Phi)$; then $\det(\alpha)^2 = 1$. Since $-1 \in \det\big(O(\Phi)\big)$, changing α for $\alpha\gamma$ with a suitable $\gamma \in O(\Phi)$, we may assume that $\det(\alpha) = 1$. We then associate the $SO(\Phi)$-class of $L\alpha$ to Ψ We can easily verify that the set of all SO-classes in the SO-genus of Φ contained in $S_n^0(\xi)$ are in one-to-one correspondence with the set of $SO(\Phi)$-classes in the genus of L.

In general, if $\Psi = \varepsilon\Phi\cdot{}^t\varepsilon = \alpha\Phi\cdot{}^t\alpha$ as above, then $\det(\alpha)^2 = \det(\varepsilon)^2 \in \det(E_\xi)$, and so $\det(\alpha) \in \mathfrak{g}^\times$. Therefore, if $F = \mathbf{Q}$, then $\det(\Psi) = \det(\Phi)$, and the SO-genus of Φ coincides with the genus of Φ.

4.5. Define (V, φ) by $V = F_n^1$ and $\varphi[x] = x\Phi \cdot {}^tx$ as above with any $\Phi \in S_n$. Put $L = L_0\xi$ with $\xi \in GL_n(F)_{\mathbf{A}}$. We easily see that $\widetilde{L} = L_0(2\Phi \cdot {}^t\xi)^{-1}$, and so

$$[\widetilde{L}/L] = \det(2\Phi\xi^2)\mathfrak{g} \quad \text{if} \quad L = L_0\xi. \tag{4.4}$$

In order to state our main results, we need a basic fact on an algebraic extension K of F. Let $\mathfrak{r}$ be the maximal order of K, and $\mathfrak{d}$ the different of K relative to F; let $\mathfrak{d}_0 = N_{K/F}(\mathfrak{d})$, $m = [K : F]$, and $d(K/F) = \det\left[(\mathrm{Tr}_{K/F}(e_ie_j))_{i,j=1}^m\right]$ with an F-basis $\{e_i\}_{i=1}^m$ of K. Strictly speaking, $d(K/F)$ should be viewed as a coset in $F^\times/F^{\times 2}$ represented by that determinant, but we denote any number in that coset by $d(K/F)$. By the *characteristic ideal class* for the extension K/F we understand the ideal class $\mathfrak{k}$ in F determined by the property that $\mathfrak{r}$ is isomorphic as a $\mathfrak{g}$-module to $\mathfrak{g}^1_{m-1} \oplus \mathfrak{x}$ with an ideal $\mathfrak{x}$ belonging to $\mathfrak{k}$. Then we have

(4.5) *The characteristic ideal class for K/F contains an ideal $\mathfrak{x}$ such that $\mathfrak{d}_0 = d(K/F)\mathfrak{x}^2$.*

To prove this, take $V = K$, $\varphi(x, y) = \mathrm{Tr}_{K/F}(xy)$ for $x, y \in K$, and $L = \mathfrak{r}$ in (4.4). Then $\widetilde{L} = (2\mathfrak{d})^{-1}$, and (4.4) shows that $\mathfrak{d}_0 = d(K/F)\mathfrak{x}^2$ with $\mathfrak{x} = \det(\xi)\mathfrak{g}$, which proves (4.5). This fact was noted, in substance, by Artin in 1949; that $\mathfrak{d}$ defines a square ideal class in K is due to Hecke. We can easily generalize (4.5) to the case of a maximal order $\mathfrak{o}$ in a simple algebra over F. The ideal class which is an obvious analogue of $\mathfrak{k}$ is independent of the choice of $\mathfrak{o}$.

We also need a few more symbols. We denote by $\mathbf{r}$ the set of all real primes in $\mathbf{a}$. For $T \in S_n$ and $v \in \mathbf{r}$ we put $s_v(T) = p_v - q_v$ if T as a real symmetric matrix in $GL_n(F_v) = GL_v(\mathbf{R})$ has p_v positive and q_v negative eigenvalues. Given a quadratic space (V, φ), we denote by $Q(\varphi)$ the characteristic quaternion algebra of (V, φ) in the sense of [S5, §3.1]; if φ is obtained from $\Phi \in S_n$ as above, we put $\delta(\Phi) = \delta(\varphi)$ and $Q(\Phi) = Q(\varphi)$. In [S5, Theorem 4.4] we showed that the isomorphism class of (V, φ) is determined by $\{n, \delta(\varphi), Q(\varphi), \{s_v(\varphi)\}_{v\in\mathbf{r}}\}$. We will now state this fact in terms of the matrices Φ in $S^0_n(\xi)$.

THEOREM 4.6 (The case of even n). *Let the symbols n, $\{\sigma_v\}_{v\in\mathbf{r}}$, δ, K_0, $\mathfrak{e}_0$, $\mathfrak{e}_1$, and ξ be given as follows: $4 \le n \in 2\mathbf{Z}$, $\sigma_v \in 2\mathbf{Z}$, $|\sigma_v| \le n$; $\delta \in F^\times$, $K_0 = F(\sqrt{\delta})$; $\mathfrak{e}_0$ and $\mathfrak{e}_1$ are squarefree integral ideals in F; $\xi \in GL_n(F)_\mathbf{A}$. Let r be the number of prime factors of $\mathfrak{e}_0\mathfrak{e}_1$, and $\mathfrak{d}$ the different of K_0 relative to F; put $\mathfrak{d}_0 = \mathfrak{d}^2 \cap F$. Suppose that $\mathfrak{e}_0$ divides $\mathfrak{d}_0$, $\mathfrak{e}_1$ is prime to $\mathfrak{d}_0$, $(-1)^{\sigma_v/2}\delta > 0$ at each $v \in \mathbf{r}$, $\det(\xi)\mathfrak{e}_1^{-1}$ belongs to the characteristic ideal class for K_0/F, and*

$$r + \#\{v \in \mathbf{r} \,|\, \sigma_v \equiv 4 \text{ or } 6 \pmod 8\} \in 2\mathbf{Z}. \tag{4.6}$$

Then there exists an element Φ of $S^0_n(\xi)$ such that

$$\delta \in \delta(\Phi), \quad \det(2\Phi\xi^2)\mathfrak{g} = \mathfrak{d}_0\mathfrak{e}_1^2, \quad s_v(\Phi) = \sigma_v \text{ for every } v \in \mathbf{r}, \tag{4.7}$$

and $Q(\Phi)$ is ramified at $v \in \mathbf{h}$ if and only if $v|\mathfrak{e}_0\mathfrak{e}_1$. Moreover, every element of $S^0_n(\xi)$ is of this type, and its genus is determined by $(\{\sigma_v\}_{v\in\mathbf{r}}, \delta, \mathfrak{e}_0, \mathfrak{e}_1)$. These statements are true even for $n = 2$ under the following additional condition on $\mathfrak{e}_1$: if $\mathfrak{e}_1 \ne \mathfrak{g}$, then $K_0 \ne F$ and every prime factor of $\mathfrak{e}_1$ remains prime in K_0.

Proof. Given the symbols as in our theorem, let B be the quaternion algebra over F ramified exactly at the prime factos of $\mathfrak{e}_0\mathfrak{e}_1$ and at those $v \in \mathbf{r}$ for which $\sigma_v \equiv 4$ or $6 \pmod 8$. Such a B exists because of (4.6). By the main theorem of classification [S5, Theorem 4.4] there exists a quadratic space (V, φ) over F such that $B = Q(\varphi)$, $\delta \in \delta(\varphi)$, and $\sigma_v = s_v(\varphi)$ for every $v \in \mathbf{r}$. By Proposition 4.3 (ii) we can take $(V, \varphi) = [\Psi]$ with $\Psi \in S^0_n(\eta)$, $\eta \in GL_n(F)_\mathbf{A}$. Put $L = L_0\eta$. By [S5, Theorem 6.2 (ii)] we have $[\widetilde{L}/L] = \mathfrak{d}_0\mathfrak{e}_1^2$, which combined with (4.4) shows that $\det(2\Psi\eta^2)\mathfrak{g} = \mathfrak{d}_0\mathfrak{e}_1^2$. By our assumption on ξ and (4.5) we have $\mathfrak{d}_0\mathfrak{e}_1^2 = c^2\delta\det(\xi)^2\mathfrak{g}$ with $c \in F^\times$. Thus $\det(2\Psi\eta^2)\mathfrak{g} = c^2\delta\det(\xi)^2\mathfrak{g}$. Since $(-1)^{n/2}\delta = b^2\det(2\Psi)$ with $b \in F^\times$, we see that $\det(\eta)\mathfrak{g} = bc\det(\xi)\mathfrak{g}$, which implies that $\eta \in E\xi\alpha$ with $\alpha \in GL_n(F)$. Then by Proposition 4.3 (i) we can replace η by the given ξ, and we obtain the first part of our theorem.

Next, given $\Phi \in S_n^0(\xi)$, put $L = L_0\xi$. Let $\mathfrak{e}$ be the product of all the prime ideals in F ramified in $Q(\Phi)$ and let $K_0 = F(\sqrt{\delta})$ with $\delta \in \delta(\Phi)$. By [S5, (4.2b)], $Q(\Phi)$ is ramified at $v \in \mathbf{r}$ if and only if $s_v(\Phi) \equiv 4$ or $6 \pmod 8$. Put $\mathfrak{e} = \mathfrak{e}_0\mathfrak{e}_1$, where $\mathfrak{e}_0$ is the product of the prime factors of $\mathfrak{e}$ ramified in K_0. Then in [S5, Theorem 6.2 (ii)] we showed that $[\widetilde{L}/L] = \mathfrak{d}_0\mathfrak{e}_1^2$, where $\mathfrak{d}_0$ is defined for this K_0 as in our theorem. Combining this with (4.4) we obtain $\det(2\Phi\xi^2)\mathfrak{g} = \mathfrak{d}_0\mathfrak{e}_1^2$. We have $\mathfrak{d}_0 = \delta\mathfrak{x}^2$ with an ideal $\mathfrak{x}$ as in (4.5), and so $\det(\xi)\mathfrak{g} = \mathfrak{x}\mathfrak{e}_1$, if we take δ to be $(-1)^{n/2}\det(2\Phi)$. This proves the second part of our theorem. The last part concerning the case $n = 2$ follows from [S5, Theorem 4.4, (4.4b)].

THEOREM 4.7 (The case of odd n). *Let the symbols n, $\{\sigma_v\}_{v\in\mathbf{r}}$, δ, K_0, $\mathfrak{e}$, and ξ be given as follows: $0 < n-1 \in 2\mathbf{Z}$, $\sigma_v - 1 \in 2\mathbf{Z}$, $|\sigma_v| \le n$; $\delta \in F^\times$, $K_0 = F(\sqrt{\delta})$; $\mathfrak{e}$ is a squarefree integral ideal in F; $\xi \in GL_n(F)_\mathbf{A}$. Let r be the number of prime factors of $\mathfrak{e}$; let $\delta\mathfrak{g} = \mathfrak{a}\mathfrak{b}^2$ with a squarefree integral ideal $\mathfrak{a}$ and a fractional ideal $\mathfrak{b}$ in F; put $\mathfrak{e} = \mathfrak{e}_0\mathfrak{e}_1$ with $\mathfrak{e}_1 = \mathfrak{a} + \mathfrak{e}$. Suppose $(-1)^{(\sigma_v-1)/2}\delta > 0$ at each $v \in \mathbf{r}$, $\det(\xi)\mathfrak{b}$ belongs to the ideal class of $\mathfrak{e}_0$, and*

$$r + \#\{v \in \mathbf{r} \mid \sigma_v \equiv \pm 3 \pmod 8\} \in 2\mathbf{Z}. \tag{4.8}$$

Then there exists an element Φ of $S_n^0(\xi)$ such that

$$\delta \in \delta(\Phi), \quad \det(2\Phi\xi^2)\mathfrak{g} = 2\mathfrak{a}\mathfrak{e}_0^2, \quad s_v(\Phi) = \sigma_v \text{ for every } v \in \mathbf{r}, \tag{4.9}$$

and $Q(\Phi)$ is ramified at $v \in \mathbf{h}$ if and only if $v|\mathfrak{e}$. Moreover, every element of $S_n^0(\xi)$ is of this type, and its genus is determined by $(\{\sigma_v\}_{v\in\mathbf{r}}, \delta, \mathfrak{e})$.

Proof. In [S5, Theorem 6.2 (iii)] we showed that $[\widetilde{L}/L] = 2\mathfrak{a}^{-1}\mathfrak{e}^2 \cap 2\mathfrak{a}$ for a maximal lattice L if $\delta(\varphi)\mathfrak{g} = \mathfrak{a}\mathfrak{b}^2$ as above. We easily see that $2\mathfrak{a}^{-1}\mathfrak{e}^2 \cap 2\mathfrak{a} = 2\mathfrak{a}\mathfrak{e}_0^2$. Therefore the proof can be given in exactly the same fashion as for Theorem 4.6.

Remark. (1) Let $\mathfrak{x}$ be the ideal belonging to the characteristic ideal class for K_0/F such that $\mathfrak{d}_0 = \delta\mathfrak{x}^2$. Suppose Φ has the last two properties of (4.7) and $\det(\xi)\mathfrak{e}_1^{-1}$ belongs to the class of $\mathfrak{x}$. Then $b^2\det(2\Phi)\mathfrak{g} = \delta\mathfrak{g}$ with $b \in F^\times$, and so $(-1)^{n/2}\det(2\Phi) = b^{-2}\delta c$ with $c \in \mathfrak{g}^\times$. Since $s_v(\Phi) = \sigma_v$ for every $v \in \mathbf{r}$, we see that $c > 0$ at every $v \in \mathbf{r}$. Suppose an element of $\mathfrak{g}^\times$ positive at every $v \in \mathbf{r}$ is always a square. Then we obtain $\delta \in \delta(\Phi)$. Thus the first property of Φ in (4.7) follows from the assumption on $\det(\xi)\mathfrak{g}$ and the last two properties of (4.7) under that condition on $\mathfrak{g}^\times$. The same comment applies to (4.9).

(2) The last two statements of (1) apply to the case $F = \mathbf{Q}$. Therefore the above two theorems for $F = \mathbf{Q}$ are the same as [S5, Theorems 6.4 and 6.5]. The new features in the general case are that we need $\xi \in GL_n(F)_\mathbf{A}$ and we have to impose a condition on the ideal class of $\det(\xi)\mathfrak{g}$. In other words, the

coset $E\xi GL_n(F)$ is determined by $\{\sigma_v\}_{v\in\mathbf{r}}$, δ, and the characteristic quaternion algebra.

(3) A $\mathfrak{g}$-valued *symmetric* form is represented by an element of S_n with entries in $\mathfrak{g}$. This is different from the notion of a $\mathfrak{g}$-valued *quadratic* form, and so the classification of $\mathfrak{g}$-valued symmetric forms is different from that of $\mathfrak{g}$-valued quadratic forms. We refer the reader to [S7] for the classification of $\mathfrak{g}$-valued symmetric forms and its connection with the classification of quadratic forms.

5. Ternary forms

5.1. Before proceeding further, let us recall several basic facts on quaternion algebras. Let B be a quaternion algebra over a global field F, and $\mathfrak{O}$ an order in B containing $\mathfrak{g}$. For $\xi \in B_{\mathbf{A}}^\times$ the principle of §1.2 about the lattice Lx enables us to define $\mathfrak{O}\xi$ as a $\mathfrak{g}$-lattice in B. We call a $\mathfrak{g}$-lattice in B of this form a *proper left* $\mathfrak{O}$*-ideal.* Thus the $B^\times$-genus of $\mathfrak{O}$ consists of all proper left $\mathfrak{O}$-ideals, and the genus is stable under right multiplication by the elements of $B^\times$, and so a $B^\times$-class of proper left $\mathfrak{O}$-ideals is meaningful. Define a subgroup U of $B_{\mathbf{A}}^\times$ by $U = B_{\mathbf{a}}^\times \prod_{v\in\mathbf{h}} \mathfrak{O}_v^\times$. Then $\#(U\backslash B_{\mathbf{A}}^\times/B^\times)$ gives the number of $B^\times$-classes in this genus, which we call *the class number of* $\mathfrak{O}$. Next, for $x \in B_{\mathbf{A}}^\times$ we denote by $x\mathfrak{O}x^{-1}$ the order $\mathfrak{O}'$ in B such that $\mathfrak{O}'_v = x_v\mathfrak{O}_v x_v^{-1}$ for every $v \in \mathbf{h}$. By *the type number of* $\mathfrak{O}$ we mean $\#S$ for a minimal set S of such orders $\mathfrak{O}'$ with the property that every order of type $x\mathfrak{O}x^{-1}$ can be transformed to a member of S by an inner automorphism of B.

Given an order $\mathfrak{O}$ in B over a local or global F, put $\widetilde{\mathfrak{O}} = \{x \in B \,|\, \mathrm{Tr}_{B/F}(x\mathfrak{O}) \subset \mathfrak{g}\}$. It can be shown that $[\widetilde{\mathfrak{O}}/\mathfrak{O}]$ is a square of an integral ideal $\mathfrak{t}$. We call $\mathfrak{t}$ *the discriminant of* $\mathfrak{O}$. In the local case, if B is a division algebra, then $\mathfrak{O}$ is maximal if and only if the disriminant is the prime ideal of $\mathfrak{g}$. In the global case, if $\mathfrak{O}$ is maximal, then the discriminant of $\mathfrak{O}$ is the product of all the prime ideals where B is ramified. Thus we call it the *discriminant of* B. If $F = \mathbf{Q}$, then writing the discriminant of $\mathfrak{O}$ or of B in the form $t\mathbf{Z}$ with a positive integer t, we call t *the discriminant of* $\mathfrak{O}$ *or of* B. Let us quote here a result due to Eichler [E2, Satz 3]:

(5.1) *If F is local, B is isomorphic to $M_2(F)$, and the discriminant of an order $\mathfrak{O}$ in B is the prime ideal $\mathfrak{p}$ of $\mathfrak{g}$, then there is an isomorphism of B onto $M_2(F)$ that maps $\mathfrak{O}$ onto*

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathfrak{g}) \,\middle|\, c \in \mathfrak{p} \right\}. \tag{5.1a}$$

If $\mathfrak{O}$ is the order of (5.1a), then we can easily verify that

$$\widetilde{\mathfrak{O}} = \mathfrak{O}\eta^{-1} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \,\middle|\, a,\, c,\, d \in \mathfrak{g},\, b \in \mathfrak{p}^{-1} \right\}, \quad \eta = \begin{bmatrix} 0 & -1 \\ \pi & 0 \end{bmatrix}, \tag{5.1b}$$

where π is a prime element of F.

Let $\mathfrak{O}$ be an order in B in the global case, and let $\mathfrak{e}$ be the discriminant of B; suppose the discriminant of $\mathfrak{O}$ is squarefree. Then the discriminant of

$\mathfrak{O}$ is of the form $\mathfrak{a}_0\mathfrak{e}$ with a squarefree integral ideal $\mathfrak{a}_0$ prime to $\mathfrak{e}$. For each $v|\mathfrak{a}_0$ the order $\mathfrak{O}_v$ can be transformed to an order of type (5.1a). We will be considering such an order $\mathfrak{O}$ in the following treatment.

5.2. Let us now consider (V, φ) with $n = 3$ over a local or global F. As shown in [S3, §7.3], we can find a quaternion algebra B over F with which we can put $V = B^\circ\xi$, $A(V) = B + B\xi$, $A^+(V) = B$, $\varphi[x\xi] = dxx^\iota$ and $2\varphi(x\xi, y\xi) = d\mathrm{Tr}_{B/F}(xy^\iota)$ for $x, y \in B^\circ$, where B° is as in (1.2) and ξ is an element such that $\xi^2 = -d \in \delta(\varphi)$; $F + F\xi$ is the center of $A(V)$; $G^+(V) = B^\times$; $\nu(\alpha) = N_{B/F}(\alpha)$ and $x\xi\tau(\alpha) = \alpha^{-1}x\alpha\xi$ for $x \in B^\circ$ and $\alpha \in B^\times$.

Given $h \in V$ such that $\varphi[h] \neq 0$, take $k \in B^\circ$ so that $h = k\xi$. Put $W = (Fh)^\perp$ and $K = F + Fk$. It can easily be seen that $K = \{\alpha \in B \mid \alpha k = k\alpha\}$, and K is either a quadratic extension of F, or isomorphic to $F \times F$. In either case we can find an element ω of B such that

$$B = K + \omega K, \quad \omega^2 \in F^\times, \quad \omega k = -k\omega. \tag{5.2}$$

Then $B^\circ = Fk + \omega K$ and $\mathrm{Tr}_{B/F}(k\omega K) = 0$, and so $W = \omega K\xi = F\omega\xi + F\omega k\xi$, and $\varphi[\omega x\xi] = -d\omega^2 xx^\rho$ for $x \in K$, where ρ is the nontrivial automorphism of K over F. Since $-dk^2 = \varphi[h]$, we have $K = F \times F$ if $-d\varphi[h]$ is a square in F; otherwise $K = F(\kappa^{1/2})$ with $\kappa = -d\varphi[h]$. We easily see that

$$A^+(W) = K, \qquad G^+(W) = K^\times. \tag{5.3}$$

The group $SO^\varphi(W)$ can be identified with $\{b \in K^\times \mid bb^\rho = 1\}$, and the map $\tau : K^\times \to SO^\varphi(W)$ is given by $\tau(a) = a/a^\rho$ for $a \in K^\times$. To be precise, $\omega x\xi\tau(a) = \omega(a/a^\rho)x\xi$ for $x \in K$.

Clearly the isomorphism class of (V, φ) is determined by B and $dF^{\times 2}$, and vice versa. If F is a totally real number field and φ is positive definite at every $v \in \mathbf{a}$, then B is totally definite and d is totally positive.

Assuming F to be global, put $d\mathfrak{g} = \mathfrak{a}\mathfrak{x}^2$ with a squarefree integral ideal $\mathfrak{a}$ and a fractional ideal $\mathfrak{x}$; let $\mathfrak{e}$ be the product of all the prime ideals of F ramified in B. In general the pair $(\mathfrak{e}, \mathfrak{a})$ does not necessarily determine (V, φ), but it does if $F = \mathbf{Q}$ and φ is positive definite.

Lemma 5.3. *Suppose F is global; let (V, φ), B, $\mathfrak{a}$, and $\mathfrak{e}$ be as above. Put $\mathfrak{e}_1 = \mathfrak{a} + \mathfrak{e}$, $\mathfrak{e} = \mathfrak{e}_0\mathfrak{e}_1$, and $\mathfrak{a} = \mathfrak{a}_0\mathfrak{e}_1$. Let L be an integral lattice in V. Then the following assertions hold:*

(i) *L is maximal if and only if $[\widetilde{L}/L] = 2\mathfrak{a}\mathfrak{e}_0^2$.*

(ii) *If L is maximal, then there is a unique order of B $\bigl(= A^+(V)\bigr)$ of discriminant $\mathfrak{a}_0\mathfrak{e}$ containing $A^+(L)$.*

Proof. Let Λ be a maximal lattice containing L. Since $[\widetilde{L}/L] = [\widetilde{\Lambda}/\Lambda][\Lambda/L]^2$, the "if"-part of (i) follows from the "only if"-part. Clearly the problem can be reduced to the local case. In the local case, we may assume that $d\mathfrak{g}$ equals $\mathfrak{g}$ or the prime ideal $\mathfrak{p}$ of $\mathfrak{g}$. Let t and M be as in §1.4. Then $[\widetilde{L}/L] = [\widetilde{M}/M]$. If $t = 1$, we can easily find $[\widetilde{M}/M]$. Suppose $t = 3$; if $d\mathfrak{g} = \mathfrak{p}$, then the explicit forms of M and $\widetilde{M}$ given in §1.5, (B) show that $[\widetilde{M}/M] = 2\mathfrak{p}$. If $d\mathfrak{g} = \mathfrak{g}$. we have $[\widetilde{M}/M] = 2\mathfrak{p}^2$ as shown in [S3, (7.9)]. This proves (i).

Next, since all the maximal lattices form a genus, it is sufficient to prove (ii) for a special choice of L. We take an order $\mathfrak{O}$ in B of discriminant $\mathfrak{a}\mathfrak{e}_0$, and take the $\mathfrak{g}$-lattice $\mathfrak{M}$ in B such that $\mathfrak{M}_v = \widetilde{\mathfrak{O}}_v$ if $v|\mathfrak{a}$ and $\mathfrak{M}_v = \mathfrak{O}_v$ if $v\nmid\mathfrak{a}$. We then put

$$L = \mathfrak{x}^{-1}(\mathfrak{M} \cap B^\circ)\xi, \tag{5.4}$$

Our task is to show that L is maximal and to prove (ii) for this L. The problems can be reduced to the local case. For simplicity we fix $v \in \mathbf{h}$ and denote F_v and $\mathfrak{g}_v$ by F and $\mathfrak{g}$, suppressing the subscript v. We can take $\mathfrak{x} = \mathfrak{g}$, and $d\mathfrak{g}$ to be $\mathfrak{g}$ or $\mathfrak{p}$. If $B = M_2(F)$ and $d\mathfrak{g} = \mathfrak{g}$, then $\mathfrak{O} = \widetilde{\mathfrak{O}} = M_2(\mathfrak{g})$. If $B = M_2(F)$ and $d\mathfrak{g} = \mathfrak{p}$, then $\mathfrak{O}$ and $\widetilde{\mathfrak{O}}$ can be given by (5.1a, b). Thus, for either type of $d\mathfrak{g}$ we have

$$L = \left\{ \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \,\middle|\, a,\, c \in \mathfrak{g},\, b \in d^{-1}\mathfrak{g} \right\} \cdot \xi, \tag{5.5a}$$

$$\widetilde{L} = \left\{ \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \,\middle|\, a \in (2d)^{-1}\mathfrak{g},\, c \in \mathfrak{g},\, b \in d^{-1}\mathfrak{g} \right\} \cdot \xi, \tag{5.5b}$$

so that $[\widetilde{L}/L] = 2d\mathfrak{g}$, which together with (i) shows that L is maximal. If $v|\mathfrak{e}$, then there is a unique maximal lattice in V given in the form $\{x \in V \mid \varphi[x] \in \mathfrak{g}\}$. It can easily be seen that this coincides with (5.4). Now, in the local case we easily see that $A^+(L) = \mathfrak{O}$ except when B is a division algebra and $d\mathfrak{g} = \mathfrak{g}$, in which case B has a unique order of prime discriminant. This completes the proof.

LEMMA 5.4. *In the setting of Lemma 5.3 let L be a maximal lattice in V and let $\mathfrak{O}$ be the order in B of discriminat $\mathfrak{a}_0\mathfrak{e}$ established in Lemma 5.3 (ii). Put*

$$C = \{x \in SO^\varphi(V)_\mathbf{A} \mid Lx = L\}, \tag{5.6}$$

$$T = \{y \in B_\mathbf{A}^\times \mid y\mathfrak{O} = \mathfrak{O}y\}, \quad T_v = B_v^\times \cap T. \tag{5.7}$$

Then $C = \tau(T)$; moreover, for $v \in \mathbf{h}$ we have $T_v = B_v^\times$ if $v|\mathfrak{e}$, $T_v = F_v^\times\mathfrak{O}_v^\times$ if $v\nmid\mathfrak{a}_0\mathfrak{e}$, and $T_v = F_v^\times(\mathfrak{O}_v^\times \cup \mathfrak{O}_v^\times\eta_v)$ if $v|\mathfrak{a}_0$, where η_v is η of (5.1b). Furthermore,

$$\{\gamma \in SO^\varphi(V) \mid L\gamma = L\} = \tau(\{\alpha \in B^\times \mid \alpha\mathfrak{O} = \mathfrak{O}\alpha\}). \tag{5.8}$$

Proof. The statements about T_v are well known if $\mathfrak{O}_v$ is maximal, that is, if $v\nmid\mathfrak{a}_0$. If $v|\mathfrak{a}_0$, then $\mathfrak{O}_v$ is of type (5.1a), and the desired fact follows from [E2, Satz 5]. To prove $\tau(T) = C$, we first recall the equality $SO^\varphi(V) = \tau(G^+(V))$, which holds over any field. Thus it is sufficient to show that $\tau(T_v) = C_v$ for every $v \in \mathbf{h}$, where $C_v = C \cap SO^\varphi(V)_v$. This is trivial if $v|\mathfrak{e}$, as $C_v = SO^\varphi(V)_v$ and $T_v = B_v^\times$ then. For $v \in \mathbf{h}$ put $D_v = \{\alpha \in B_v^\times \mid \alpha^{-1}L_v\alpha = L_v\}$. Then $\tau(D_v) = C_v$. We have seen in the proof of Lemma 5.3 that $A^+(L_v) = \mathfrak{O}_v$ if $v\nmid\mathfrak{e}$. Therefore if $\alpha \in D_v$ for such a v, then $\alpha^{-1}\mathfrak{O}_v\alpha = \mathfrak{O}_v$, and so $\alpha \in T_v$. Conversely, if $\alpha \in T_v$, then $\alpha\mathfrak{O}_v = \mathfrak{O}_v\alpha$ and we easily see that $\alpha\widetilde{\mathfrak{O}}_v = \widetilde{\mathfrak{O}}_v\alpha$.

We may assume that L is of the form (5.4). Since $\mathfrak{M}_v$ is $\mathfrak{O}_v$ or $\widetilde{\mathfrak{O}}_v$, we have $\alpha^{-1}L_v\alpha = L_v$, and so $\alpha \in D_v$. Thus $T_v = D_v$. Since $\tau(D_v) = C_v$, we obtain $\tau(T) = C$. Since $\mathrm{Ker}(\tau) = F_{\mathbf{A}}^{\times} \subset T$, if $\tau(\alpha) \in C$ with $\alpha \in B^{\times}$, then $\alpha \in T \cap B^{\times}$, from which we obtain (5.8).

Proof of Theorem 1.8. Since $\tau\bigl(G^+(V)\bigr) = SO^{\varphi}(V)$, the equality $\tau(T) = C$ stated in (iii) is clear from the definition of T. To prove the remaining statements, we first consider the case $n = 3$. Then C of §1.7 and Theorem 1.8 is C_v of Lemma 5.4 with a divisor v of $\mathfrak{a}$, and $A^+(L) = \mathfrak{O}_v$ as noted at the end of the proof of Lemma 5.3. Moreover, by Lemma 5.4, we have $F_v^{\times} \subset T_v$ and $\tau(T_v) = C_v$, and so T_v coincides with T of our theorem. Thus $T = B_v^{\times}$ if $v|\mathfrak{e}$ and $T = F_v^{\times}(\mathfrak{O}_v^{\times} \cup \mathfrak{O}_v^{\times}\eta_v)$ if $v|\mathfrak{a}_0$. The last expression for T is valid even for $v|\mathfrak{e}$, if we take η_v to be an element of B_v such that η_v^2 is a prime element of F_v. Clearly $J = \mathfrak{O}_v^{\times}$ and $\nu(J) = \mathfrak{g}_v^{\times}$; also, all the other statements of our theorem can easily be verified.

Next suppose $n > 3$; using the symbols of (1.4a, b, c), put $W = Z$ and $N = M$ if $t = 3$; put $W = Z + Fe_r + Ff_r$ and $N = M + \mathfrak{g}e_r + \mathfrak{g}f_r$ if $t = 1$. Then $V = W + \sum_{i=1}^{u}(Fe_i + Ff_i)$ and $L = N + \sum_{i=1}^{u}(\mathfrak{g}e_i + \mathfrak{g}f_i)$, where $u = r$ if $t = 3$ and $u = r - 1$ if $t = 1$. Observe that N contains an element g such that $\varphi[g] \in \mathfrak{g}^{\times}$. Therefore, as shown in [S3, §8.2], there exists an isomorphism θ of $A^+(V)$ onto $M_2\bigl(A^+(W)\bigr)$ such that $\theta\bigl(A^+(L)\bigr) = M_s\bigl(A^+(N)\bigr)$, where $s = 2^u$. Thus (i) and (ii) of our theorem follow from what we proved in the case $n = 3$; namely, $A^+(L)$ can be identified with $M_s(\mathfrak{O})$ with an order $\mathfrak{O}$ as stated. As for (iii) in the general case, clearly $\nu(J) = \mathfrak{g}^{\times}$. We already found an element η of $G^+(W)$ such that $N\tau(\eta) = N$, $\eta^2 \in F^{\times}$, and $\nu(\eta)\mathfrak{g} = \mathfrak{p}$; also $\eta J = J\eta$ as can easily be seen. Put $T_0 = F^{\times}(J \cup J\eta)$. Then T_0 is a subgroup of $G^+(V)$, $\tau(T_0) \subset C$, and $\nu(T_0) = F^{\times}$. Let $\alpha \in T$. Take $\beta \in T_0$ so that $\nu(\alpha) = \nu(\beta)$. Then $\nu(\beta^{-1}\alpha) = 1$, and so $\beta^{-1}\alpha \in J$. Thus $\alpha \in \beta J \subset T_0$, and we obtain $T = T_0$ and $C = \tau(T_0) = \tau(J) \cup \tau(J\eta)$. If $\tau(\eta) \in \tau(J)$, then $\eta \in F^{\times}J$, which is impossible, as $\nu(\eta)\mathfrak{g} = \mathfrak{p}$. Thus $\tau(\eta) \notin \tau(J)$, and so $[C : \tau(J)] = 2$. This completes the proof.

5.5. We now return to (V, φ) over a global F of an odd dimension $n > 1$, and fix a maximal lattice L in V. For each $v \in \mathbf{h}$ we take an element $\varepsilon_v \in \delta(\varphi_v)$ that is either a unit or a prime element of F_v. Then $\varepsilon_v\mathfrak{g}_v^{\times 2}$ is determined by φ_v, where $\mathfrak{g}_v^{\times 2} = \bigl\{a^2 \bigm| a \in \mathfrak{g}_v^{\times}\bigr\}$. Given $h \in V$ such that $\varphi[h] \neq 0$, take an element $\beta_v \in F_v$ such that $\varphi(h, L_v) = \beta_v\mathfrak{g}_v$, and put $r_v(h) = \varepsilon_v^{-1}\varphi[h]\beta_v^{-2}$. Then $r_v(h)$ determines a coset of $F_v^{\times}/\mathfrak{g}_v^{\times 2}$, which depends only on φ_v, L, and $F_v^{\times}hC(L_v)$. Strictly speaking, $r_v(h)$ should be defined as a coset, but for simplicity we view it as an element of $F_v^{\times}$, and write $r_v(h) \in X$ or $r_v(h) \in X$ for any subset X of F_v stable under multiplication by the elements of $\mathfrak{g}_v^{\times 2}$. For example, we can take as X the set

$$\mathfrak{E}_v = \bigl\{u^2 + 4w \bigm| u,\, w \in \mathfrak{g}_v\bigr\}. \tag{5.9}$$

Then the condition $r_v(h) \in \mathfrak{E}_v$ is meaningful. Obviously $\mathfrak{E}_v = \mathfrak{g}_v$ if $v\nmid 2$. We can also define $r_v(h)$ for $h \in V_v$.

The following lemma concerns the local case, that is, v is fixed, and so we write $r(h)$ and $\mathfrak{E}$ for $r_v(h)$ and $\mathfrak{E}_v$.

LEMMA 5.6. *Let* (V, φ), B, ξ, d, *and* B° *be as in §5.2 with a local field* F *and* $B = M_2(F)$; *suppose* d *is a prime element of* F; *let* $\mathfrak{O}$ *be the order of (5.1a) and* L *be as in (5.5a); put* $C = \{\alpha \in SO^\varphi(V) \mid L\alpha = L\}$. *Fixing* $h = k\xi$ *as in §5.2, put* $K = F[k]$, $\mathfrak{f} = K \cap \mathfrak{O}$, $\mathfrak{y} = \widetilde{\mathfrak{O}} \cap K$, $W = (Fh)^\perp$, *and*

$$J = \{\alpha \in SO^\varphi(W) \mid (L \cap W)\alpha = L \cap W\}. \tag{5.10}$$

Then the following assertions hold:

(i) $\mathfrak{f}$ *is the order of* K *whose discriminant is* $r(h)\mathfrak{p}^2$.

(ii) *There exists an element* ω *of* $B^\times$ *such that (5.2) is satisfied,* $\tau(\omega) \in C$, $W = \omega K\xi$; $L \cap W = \omega\mathfrak{f}\xi$ *if* $r(h) \notin \mathfrak{p}^{-1}$, *and* $L \cap W = \omega\mathfrak{y}\xi$ *if* $r(h) \in \mathfrak{p}^{-1}$.

(iii) *If* $r(h) \notin \mathfrak{p}^{-1}$, *then* $K \cong F \times F$, $\mathfrak{f}$ *is the maximal order of* K, $L \cap W$ *is a maximal lattice in* W, *and* $J = SO^\varphi(W) \cap C = \tau(\mathfrak{f}^\times)$.

(iv) *If* $r(h) \in \mathfrak{E}$, *then* $\mathfrak{y}$ *is the order in* K *whose discriminant is* $r(h)\mathfrak{g}$, $\mathfrak{f}$ *is not maximal,* $J = \tau(\{a \in K^\times \mid a/a^\rho \in \mathfrak{y}^\times\})$, *and* $SO^\varphi(W) \cap C = \tau(\mathfrak{f}^\times)$.

(v) *If* $r(h) \in \mathfrak{p}^{-1}$ *and* $r(h) \notin \mathfrak{E}$, *then* K *is ramified over* F, $\mathfrak{f}$ *is the maximal order of* K, $J = \tau(\{a \in K^\times \mid a/a^\rho \in \mathfrak{f}^\times\})$, *and* $SO^\varphi(W) \cap C = \{x \in K \mid xx^\rho = 1\}$, *which has* $\tau(\mathfrak{f}^\times)$ *as a subgroup of index 2.*

(vi) *Cases* (iii), (iv), *and* (v) *cover all possibilities for* h, *and mutually exclusive.*

Proof. To prove our assertions, we can replace h by any element of $F^\times hC$. Indeed, if we replace h by $ch\tau(\alpha)$ with $c \in F^\times$ and α in the set T_v of (5.7), then K, $\mathfrak{f}$, and other symbols are replaced by their images under the inner asutomorphism $x \mapsto \alpha^{-1}x\alpha$ of $A(V)$. Thus we may assume that $2\varphi(h, L) = \mathfrak{g}$. We can take $\begin{bmatrix} 0 & -d^{-1} \\ 0 & 0 \end{bmatrix}\xi$, $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\xi$, and $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\xi$ as the elements e_1, f_1, and g of §1.6. Therefore the result there guaratees an element $\gamma \in C$ such that $h\gamma = j\xi$ with j of the following two types: (1) $j = \mathrm{diag}[c, -c]$, $2c\mathfrak{p} = \mathfrak{g}$; (2) $j = \begin{bmatrix} c & b \\ 1 & -c \end{bmatrix}$ with $b \in \mathfrak{p}^{-1}$ and $c \in 2^{-1}\mathfrak{g}$. Thus we may assume that $k = j$ with such a j. Take $\omega = \begin{bmatrix} 0 & d^{-1} \\ -1 & 0 \end{bmatrix}$ for type (1) and $\omega = \begin{bmatrix} -1 & 2c \\ 0 & 1 \end{bmatrix}$ for type (2). Then $\tau(\omega) \in C$ and $\omega^{-1}k\omega = -k$; also $W = \omega K\xi$ and $L \cap W = (\widetilde{\mathfrak{O}} \cap \omega K)\xi$. We now treat our problems according to the type of j.

Type (1). Put $\ell = \mathrm{diag}[2c, 0]$. Then $K = F + F\ell$, as $\ell = j + c$. Clearly K consists of the diagonal matrices, and $\mathfrak{f}$ is its maximal order. Since $2c\mathfrak{p} = \mathfrak{g}$, we have $\mathfrak{f} = \mathfrak{g}[d\ell]$. Now, $\widetilde{\mathfrak{O}} \cap \omega K = \omega(\mathfrak{O} \cap K) = \omega\mathfrak{f}$, so that $L \cap W = \omega\mathfrak{f}\xi$, which is a maximal lattice in W. It can easily be seen that $J = SO^\varphi(W) \cap C = \tau(\mathfrak{f}^\times)$. Also, $r(h)\mathfrak{g} = 4c^2\mathfrak{g} = \mathfrak{p}^{-2}$, so that $r(h) \notin \mathfrak{p}^{-1}$, and $r(h)\mathfrak{p}^2 = \mathfrak{g}$, which is the discriminant of $\mathfrak{f}$. Since $r(h) \in \mathfrak{p}^{-1}$ for type (2) as can easily be seen, we have type (1) if and only if $r(h) \notin \mathfrak{p}^{-1}$.

Type (2). For j of type (2), we have $r(h) \in \mathfrak{p}^{-1}$. We easily see that $r(h) \in \mathfrak{E}$ if $b \in \mathfrak{g}$. Conversely suppose $r(h) \in \mathfrak{E}$; then we have $-4\varphi[h] = d(u^2 + 4w)$

with $u,\,w\in\mathfrak{g}$. Put $h'=j'\xi$ with $j'=\begin{bmatrix}u/2 & w\\ 1 & -u/2\end{bmatrix}$. Then $\varphi[h']=\varphi[h]$ and $2\varphi(h',\,L)=\mathfrak{g}=2\varphi(h,\,L)$, so that $h'\in hC$ by Theorem 1.3. Thus if $r(h)\in\mathfrak{E}$, then we can put $h=j\xi$ with j of the above form such that $b\in\mathfrak{g}$. Without assuming $b\in\mathfrak{g}$, put $\ell=\begin{bmatrix}2c & b\\ 1 & 0\end{bmatrix}$. Then $\ell=c+j$ and $K=F+F\ell$. For $y,\,z\in F$ we have $y+z\ell=\begin{bmatrix}y+2cz & bz\\ z & y\end{bmatrix}$. This belongs to $\mathfrak{O}$ if and only if $y\in\mathfrak{g}$ and $z\in\mathfrak{p}$. Thus $\mathfrak{f}=\mathfrak{g}[d\ell]$. This has discriminant $4(b+c^2)\mathfrak{p}^2$, which equals $r(h)\mathfrak{p}^2$. Since $\omega^2=1$ and $\omega\in\mathfrak{O}^\times$, we have $L\cap W=\omega(\widetilde{\mathfrak{O}}\cap K)\xi$. We see that $y+z\ell\in\widetilde{\mathfrak{O}}$ if and only if $y\in\mathfrak{g}$ and $z\in\mathfrak{g}$. Thus $\mathfrak{y}=\mathfrak{g}+\mathfrak{g}\ell$ and $L\cap W=\omega\mathfrak{y}\xi$. For $x\in K$ and $a\in K^\times=G^+(W)$, we have $\omega x\xi\tau(a)=\omega ex\xi$, where $e=a/a^\rho$. Thus $(L\cap W)\tau(a)=L\cap W$ if and only if $(a/a^\rho)\mathfrak{y}=\mathfrak{y}$. Also $\tau(a)\in C$ if and only if $\tau(a)=\tau(s)$ with $s\in\mathfrak{O}^\times\cup\mathfrak{O}^\times\eta^{-1}$, as can be seen from Lemma 5.4. If $s\in\mathfrak{O}^\times$, then $a\in F^\times\mathfrak{O}^\times\cap K^\times=F^\times\mathfrak{f}^\times$, so that $\tau(a)\in\tau(\mathfrak{f}^\times)$. If $s\in\mathfrak{O}^\times\eta^{-1}$, then $s\in\mathfrak{O}^\times\eta^{-1}\cap K\subset\mathfrak{y}$.

Suppose now $r(h)\in\mathfrak{E}$; then we may assume that $b\in\mathfrak{g}$. Since $\ell^2=2c\ell+b$, we see that $\mathfrak{y}$ is an order, and so J is as in (iv). If $s\in\mathfrak{O}^\times\eta^{-1}$, then $dss^\iota\in\mathfrak{g}^\times$, which is impossible as $\mathfrak{y}$ is an order. Thus $SO^\varphi(W)\cap C=\tau(\mathfrak{f}^\times)$. Since $\mathfrak{f}=\mathfrak{g}[d\ell]\neq\mathfrak{g}[\ell]=\mathfrak{y}$, $\mathfrak{f}$ is not maximal and the discriminant of $\mathfrak{y}$ is $r(h)\mathfrak{g}$. This proves (iv).

Next suppose $r(h)\notin\mathfrak{E}$; then $b\notin\mathfrak{g}$ and $b\mathfrak{p}=\mathfrak{g}$. We easily see that $\ell\mathfrak{f}=\mathfrak{y}$, and so $e\mathfrak{y}=\mathfrak{y}$ if and only if $e\in\mathfrak{f}^\times$. Thus J is as in (v). Put $\pi=b^{-1}$ and $\sigma=\pi\ell$. Then $K=F[\sigma]$. Since $\sigma^2=2c\pi\sigma+\pi$, K is ramified over F and its maximal order is $\mathfrak{g}[\sigma]$, which coincides with $\mathfrak{f}$. Now $SO^\varphi(W)=\{x\in K^\times\mid xx^\rho=1\}$, which has $\tau(\mathfrak{f}^\times)$ as a subgroup of index 2 by a general principle [S3, Lemma 5.6 (iii)]. Since $\ell\in\mathfrak{O}^\times\eta^{-1}$, we have $\tau(\ell)\in SO^\varphi(W)\cap C$. If $\tau(\ell)\in\tau(\mathfrak{f}^\times)$, then $\ell\in F^\times\mathfrak{f}^\times$, which is impossible. Thus $\tau(\mathfrak{f}^\times)\subsetneqq SO^\varphi(W)\cap C\subset SO^\varphi(W)$, which proves (v). Finally (vi) is clear from the above discussion. This completes the proof, as (i) and (ii) have been proved.

If we apply (2.7) to the present setting, then $H=\{b\in K^\times\mid bb^\rho=1\}$ with $K=F+Fk$ as noted in §5.2. Thus H is commutative and the left-hand side of (2.7) becomes $[H_{\mathbf{A}}:H(H_{\mathbf{A}}\cap C)]$. We can determine this index explicitly as follows.

Theorem 5.7. *In the setting of §5.2 with a global F, let L be a maximal lattice in V, and $\mathfrak{e}$ the product of all the prime ideals in F ramified in B; put $d\mathfrak{g}=\mathfrak{a}\mathfrak{x}^2$ with a squarefree integral ideal $\mathfrak{a}$ and a fractional ideal $\mathfrak{x}$. Let $\mathfrak{O}$ be the order in B of discriminant $\mathfrak{a}\cap\mathfrak{e}$ containing $A^+(L)$. (See Lemma 5.3 (ii).) Given $h=k\xi\in V$ with $k\in B^\circ$ such that $\varphi[h]\neq 0$, put $K=F+Fk$; denote by $\mathfrak{r}$ the maximal order of K and by $\mathfrak{d}$ the different of K relative to F. Let $\mathfrak{a}^*$ be the product of the prime factors v of $\mathfrak{a}$ such that $v\nmid\mathfrak{e}$, $r_v(h)\in\mathfrak{p}_v^{-1}$, and $r_v(h)\notin\mathfrak{E}_v$, where $\mathfrak{p}_v$ is the local prime ideal at v. Then the order $\mathfrak{f}$ in K given by $\mathfrak{f}=K\cap\mathfrak{O}$ has conductor $\mathfrak{c}$, which can be determined by the condition that $\mathfrak{c}_v=\mathfrak{g}_v$ if $v|\mathfrak{a}^*\mathfrak{e}$ and $\mathfrak{c}_v^2N_{K/F}(\mathfrak{d})_v=\mathfrak{a}_v\varphi[h]\varphi(h,\,L)_v^{-2}$ if $v\nmid\mathfrak{e}$. Moreover,* *put* $H = SO^{\varphi}(W)$ *and identify* H *with* $\{\alpha \in K^\times \mid \alpha\alpha^{\iota} = 1\}$; *define* C *by (5.6). Suppose* K *is a field; then*

$$(5.11)\qquad [H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)] = (c_K/c_F) \cdot 2^{1-\mu-\nu}[\mathfrak{g}^\times : N_{K/F}(\mathfrak{r}^\times)] \cdot [U : U']^{-1} N(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \{1 - [K/F,\, \mathfrak{p}]N(\mathfrak{p})^{-1}\}.$$

Here c_K *resp.* c_F *is the class number of* K *resp.* F; μ *is the number of prime ideals dividing* $\mathfrak{a}^*\mathfrak{e}$ *and ramified in* K; ν *is the number of* $v \in \mathbf{a}$ *ramified in* K;

$$U = \{x \in \mathfrak{r}^\times \mid xx^\rho = 1\} \quad and \quad U' = \{x \in U \mid x - 1 \in \mathfrak{c}_v\mathfrak{d}_v \text{ for every } v \nmid \mathfrak{a}^*\mathfrak{e}\};$$

$\mathfrak{p}$ *runs over all prime factors of* $\mathfrak{c}$; $[K/F,\, \mathfrak{p}]$ *denotes* 1, -1, *or* 0 *according as* $\mathfrak{p}$ *splits in* K, *remains prime in* K, *or is ramified in* K.

Proof. If $d \in \mathfrak{g}^\times$, this is [S3, Theorem 12.3]. Our proof here is a modified version of the proof there. For $v|\mathfrak{e}$ we have $\mathfrak{r}_v \subset \mathfrak{O}_v$, so that $\mathfrak{f}_v = \mathfrak{r}_v$ and $\mathfrak{c}_v = \mathfrak{g}_v$. Next suppose $v \nmid \mathfrak{e}$; then we can put $B_v = M_2(F_v)$, and so [S3, Lemma 11.11] is applicable if $v \nmid \mathfrak{a}$; by (i) of that lemma, $\mathfrak{c}_v^2 N_{K/F}(\mathfrak{d})_v = \varphi[h]\varphi(h,\, L)_v^{-2}$. If $v|\mathfrak{a}$, then we use (i) of Lemma 5.6. If $v|\mathfrak{a}^*$, then $\mathfrak{c}_v = \mathfrak{g}_v$ by (v) of Lamma 5.6. Thus we obtain our assertion concerning $\mathfrak{c}$.

To prove (5.11), suppose K is a field. Then we have

$$[H_{\mathbf{A}} : HE] = (c_K/c_F) \cdot 2^{1-\kappa}[\mathfrak{g}^\times : N_{K/F}(\mathfrak{r}^\times)],$$

where $E = H_{\mathbf{a}} \prod_{v \in \mathbf{h}} E_v$ with $E_v = \mathfrak{r}_v^\times \cap H_v$ and κ is the number of $v \in \mathbf{v}$ ramified in K. Indeed, $[H_{\mathbf{A}} : HE]$ equals the number of classes in the genus of $\mathfrak{g}$-maximal lattices in W, and in [S3, (9.16)] we noted that it is the right-hand side of the above equality. Put $D = H_{\mathbf{A}} \cap C$ and $D_v = D \cap H_v$. If $v|\mathfrak{e}$, then φ_v is anisotropic, so that $C_v = G_v$; thus $D_v = H_v = E_v$ if $v|\mathfrak{e}$. If $v \nmid \mathfrak{a}^*\mathfrak{e}$, then, by [S3, Lemma 11.11 (iv)] and Lemma 5.6 (iii), (iv), we have $D_v = \tau(\mathfrak{f}_v^\times)$. If $v|\mathfrak{a}^*$, then $D_v = E_v$ by Lemma 5.6 (v). Thus $U \cap D = \{x \in U \mid x \in \tau(\mathfrak{f}_v^\times) \text{ for every } v \nmid \mathfrak{a}^*\mathfrak{e}\}$. Applying [S3, Lemma 11.10 (iii)] to $\tau(\mathfrak{f}_v^\times)$, we obtain $U \cap D = U'$. Now we have $U = E \cap H$,

$$[HE : HD] = [E : E \cap HD] = [E : UD] = [E : D]/[UD : D] = [E : D]/[U : U \cap D],$$

$$[E : D] = \prod_{v \nmid \mathfrak{a}^*\mathfrak{e}} [E_v : D_v] = \prod_{v \nmid \mathfrak{a}^*\mathfrak{e}} [E_v : \tau(\mathfrak{r}_v^\times)]\,[\tau(\mathfrak{r}_v^\times) : \tau(\mathfrak{f}_v^\times)].$$

By [S3, Lemma 5.6 (iii)], $[E_v : \tau(\mathfrak{r}_v^\times)] = 2$ if v is ramified in K, and $= 1$ otherwise. The index $[\tau(\mathfrak{r}_v^\times) : \tau(\mathfrak{f}_v^\times)]$ is given by [S3, Lemma 11.10 (i), (iv)]. Thus we obtain

$$[E : D] = 2^b N(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \{1 - [K/F,\, \mathfrak{p}]N(\mathfrak{p})^{-1}\},$$

where b is the number of the primes $v \nmid \mathfrak{a}^*\mathfrak{e}$ ramified in K. Now $[H_{\mathbf{A}} : HD] = [H_{\mathbf{A}} : HE][HE : HD]$. Combining all these, we obtain (5.11).

COROLLARY 5.8. *The notation and assumption being as in Theorem 5.7, let* $c(\mathfrak{f})$ *denote the class number of* $\mathfrak{f}$ *in the sense of* [S3, §12.5] *and let* $U_{\mathfrak{f}} = U \cap \mathfrak{f}^\times$. *Then* $U' \subset U_{\mathfrak{f}}$ *and*

$$(5.12)\quad \bigl[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)\bigr] = \bigl(c(\mathfrak{f})/c_F\bigr)\cdot 2^{1-\mu-\nu}\bigl[\mathfrak{g}^\times : N_{K/F}(\mathfrak{f}^\times)\bigr][U_{\mathfrak{f}} : U']^{-1}.$$

Proof. By [S3, Lemma 11.10 (ii)] we have $U_{\mathfrak{f}} = \bigl\{\, x \in U \,\big|\, x^\rho - x \in \mathfrak{c}\mathfrak{d} \,\bigr\}$. Since $\mathfrak{c}$ is prime to $\mathfrak{a}^*\mathfrak{e}$, for $x \in U$ we have $x^\rho - x \in \mathfrak{c}\mathfrak{d}$ if and only if $x^\rho - x \in \mathfrak{c}_v\mathfrak{d}_v$ for every $v \nmid \mathfrak{a}^*\mathfrak{e}$. We have also $x^\rho - x = (1-x)(1+x^\rho)$, and hence $U' \subset U_{\mathfrak{f}}$. Now we recall a well known formula (see [S3, (12.3)])

$$(5.13)\qquad c(\mathfrak{f}) = c_K \cdot [\mathfrak{r}^\times : \mathfrak{f}^\times]^{-1} N(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \bigl\{1 - [K/F,\, \mathfrak{p}]N(\mathfrak{p})^{-1}\bigr\}.$$

As shown in [S3, p. 117, line 7], we have

$$(5.14)\qquad [\mathfrak{r}^\times : \mathfrak{f}^\times] = [U : U_{\mathfrak{f}}]\bigl[N_{K/F}(\mathfrak{r}^\times) : N_{K/F}(\mathfrak{f}^\times)\bigr].$$

Combining (5.11), (5.13), and (5.14) together, we obtain (5.12).

Theorem 5.9. *In the setting of Lemma 5.4 and Theorem 5.7, the class number of the genus of maximal lattices in the ternary space (V, φ) equals the type number of $\mathfrak{O}$.*

Proof. We easily see that the type number of $\mathfrak{O}$ equals $\#\{B^\times\backslash B_{\mathbf{A}}^\times/T\}$ with T of (5.7). By Lemma 5.4, $\tau(T) = C$ and clearly $F_{\mathbf{A}}^\times \subset T$, and so τ gives a bijection of $B^\times\backslash B_{\mathbf{A}}^\times/T$ onto $SO^\varphi(V)\backslash SO^\varphi(V)_{\mathbf{A}}/C$. This proves our theorem.

This theorem should not be confused with the results in [Pe] (Satz 9 and its corollary), which concern the classes with respect to the group of similitudes.

Theorem 5.10. *In the setting of Theorem 5.7, suppose the genus of maximal lattices consists of a single class (which is the case if $\mathfrak{O}$ has type number 1). Put $\Gamma(L) = \bigl\{\gamma \in SO^\varphi(V) \,\big|\, L\gamma = L\bigr\}$. Then*

$$(5.15\text{a})\quad \#\bigl\{L[q,\, \mathfrak{b}]/\Gamma(L)\bigr\} = \bigl(c(\mathfrak{f})/c_F\bigr)\cdot 2^{1-\mu-\nu}\bigl[\mathfrak{g}^\times : N_{K/F}(\mathfrak{f}^\times)\bigr][U_{\mathfrak{f}} : U']^{-1}.$$

Moreover, if B is totally definite, then

$$(5.15\text{b})\quad \#L[q,\, \mathfrak{b}]/\#\Gamma(L) = \bigl(c(\mathfrak{f})/c_F\bigr)\cdot 2^{1-\mu-\nu}\bigl[\mathfrak{g}^\times : N_{K/F}(\mathfrak{f}^\times)\bigr]\#(U_{\mathfrak{f}})^{-1}.$$

Proof. The left-hand side of (2.7) in the present case is $\bigl[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)\bigr]$, as H is commutative; the right-hand side consists of a single term. Thus (2.7) combined with (5.12) gives (5.15a). Since $H \cap C = U \cap D = U'$, we have $\mathfrak{m}(H,\, H_{\mathbf{A}} \cap C) = \bigl[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)\bigr]\#(U')^{-1}$, which together with (3.7) and (5.15a) proves (5.15b).

Lemma 5.11. *Let B be a quaternion algebra over a global field F, and $\mathfrak{e}$ the product of all the prime ideals in F ramified in B; let $\mathfrak{a}_0$ be a squarefree integral ideal prime to $\mathfrak{e}$. Further let K be a quadratic extension of F contained in B and $\mathfrak{f}$ an order in K containing $\mathfrak{g}$ that has conductor $\mathfrak{c}$. Then there exists an order $\mathfrak{O}$ in B of discriminant $\mathfrak{a}_0\mathfrak{e}$ such that $\mathfrak{O} \cap K = \mathfrak{f}$ if and only if $\mathfrak{c} + \mathfrak{e} = \mathfrak{g}$ and every prime factor of $\mathfrak{a}_0$ not dividing $\mathfrak{c}$ does not remain prime in K.*

This is due to Eichler [E2, Satz 6].

LEMMA 5.12. *Let B, $\mathfrak{e}$, $\mathfrak{a}_0$, K, $\mathfrak{f}$ and $\mathfrak{c}$ be as in Lemma 5.11; let $\mathfrak{O}$ be an order in B of discriminant $\mathfrak{a}_0\mathfrak{e}$. Suppose that $\mathfrak{O}$ has type number 1, $\mathfrak{c}+\mathfrak{e}=\mathfrak{g}$ and every prime factor of $\mathfrak{a}_0$ not dividing $\mathfrak{c}$ does not remain prime in K. Then there exists an element α of $B^\times$ such that $\alpha^{-1}\mathfrak{O}\alpha\cap K=\mathfrak{f}$.*

Proof. Since $\mathfrak{O}$ has type number 1, every order in B of discriminant $\mathfrak{a}_0\mathfrak{e}$ is of the form $\alpha^{-1}\mathfrak{O}\alpha$ with $\alpha\in B^\times$. Therefore our assertion follows from Lemma 5.11.

6. POSITIVE DEFINITE TERNARY FORMS OVER $\mathbf{Q}$

6.1. Every positive definite ternary quadratic space $(V,\,\varphi)$ over $\mathbf{Q}$ is obtained by taking B to be a definite quaternion algebra over $\mathbf{Q}$ and d to be a squarefree positive integer in the setting of §5.2. If we represent φ with respect to a $\mathbf{Z}$-basis of an integral $\mathbf{Z}$-lattice L in V, then we obtain a $\mathbf{Z}$-valued ternary form. If L is maximal, then the form is *reduced* in the sense that it cannot be represented nontrivially by another $\mathbf{Z}$-valued ternary form, and vice versa. This definition of a reduced form is different from Eisenstein's terminology for ternary forms.

Define $\mathfrak{a}$ and $\mathfrak{e}$ as in §5.2. Then $\mathfrak{a}=d\mathbf{Z}$ and $\mathfrak{e}=e\mathbf{Z}$ with a squarefree positive integer e. We have $\mathfrak{e}\cap\mathfrak{a}=d_0e\mathbf{Z}$ with a positive divisor d_0 of d prime to e. Thus $\mathfrak{O}$ of Theorem 5.7 is an order of discriminant d_0e. The pair $(e,\,d)$ determines the isomorphism class of $(V,\,\varphi)$ and hence the genus of a reduced $\mathbf{Z}$-valued ternary form. If Φ is a matrix which represents a ternary form belonging to that genus, then $\det(2\Phi)=2d_0^2e^2/d$; this follows from Lemma 5.3 (i). As to the general theory of reduced forms and $\det(2\Phi)$ for an arbitrary n, the reader is referred to [S5]. Taking a maximal lattice L in V, put $C=\bigl\{SO^\varphi(V)_\mathbf{A}\bigm| L\alpha=L\bigr\}$. Then we have

LEMMA 6.2. $$\mathfrak{m}\bigl(SO^\varphi(V),\,C\bigr)=\frac{1}{12}\prod_{p|e}\frac{p-1}{2}\prod_{p|d_0}\frac{p+1}{2}.$$

Proof. Define a quadratic form β on B° by $\beta[x]=xx^\iota$ for $x\in B^\circ$; put $G=SO^\beta(B^\circ)$. Then $x\mapsto x\xi$ for $x\in B^\circ$ gives an isomorphism of $(B^\circ,\,d\beta)$ onto $(V,\,\varphi)$, and also an isomorphism of G onto $SO^\varphi(V)$. Moreover, for $\alpha\in B^\times$ we have $\alpha^{-1}x\alpha\xi=\alpha^{-1}x\xi\alpha$. Thus the symbol $\tau(\alpha)$ is consistent. We can identify C with the subgroup $\bigl\{\gamma\in G_\mathbf{A}\bigm|(\mathfrak{M}\cap B^\circ)\gamma=(\mathfrak{M}\cap B^\circ)\bigr\}$ of $G_\mathbf{A}$, where $\mathfrak{M}$ is as in (5.4). Let $\mathfrak{O}_0$ be a maximal order in B containing $\mathfrak{O}$; put $M=\mathfrak{O}_0\cap B^\circ$ and $D=\bigl\{\gamma\in G_\mathbf{A}\bigm| M\gamma=M\bigr\}$. Then M is a maximal lattice with respect to β, and from [S2, Theorem 5.8] we obtain

$$\mathfrak{m}(G,\,D)=\frac{1}{12}\prod_{p|e}\frac{p-1}{2}. \qquad (6.1)$$

By (3.3) we have $[C:C\cap D]\mathfrak{m}(G,\,C)=\mathfrak{m}(G,\,C\cap D)=[D:C\cap D]\mathfrak{m}(G,\,D)$. Clearly $D_p=C_p$ if $p\nmid d_0$. Suppose $p|d_0$; then we can put $B_p=M_2(\mathbf{Q}_p)$, $(\mathfrak{O}_0)_p=M_2(\mathbf{Z}_p)$, $D_p=\tau\bigl(GL_2(\mathbf{Z}_p)\bigr)$, and $\mathfrak{O}_p$ is of the type (5.1a). From Lemma 5.4 we obtain $[C_p:C_p\cap D_p]=2$ and $[D_p:C_p\cap D_p]=p+1$.

Thus $\mathfrak{m}(G, C) = \mathfrak{m}(G, D)\prod_{p|d_0}\{(p+1)/2\}$. Combining this with (6.1), we obtain our lemma.

6.3. Now Eichler gave a formula for the class number of $\mathfrak{O}$ and also a formula for the type number of $\mathfrak{O}$ in [E2, (64)]. However, his formula for the type number is not completely correct, and correct formulas were given by Peters in [Pe] and by Pizer in [Pi]. There is a table for the type number of $\mathfrak{O}$ for $d_0e \le 30$ in [Pe, p. 360]; a larger table for $d_0e \le 210$ is given at the end of [Pi]; in these papers, e and d_0 are denoted by q_1 and q_2. From these tables we see that the type number of $\mathfrak{O}$ for $d_0e \le 210$ is 1 exactly when (e, d_0) is one of the following 20 pairs:

$$(2, 1), (2, 3), (2, 5), (2, 7), (2, 11), (2, 23), (2, 15), (3, 1), (3, 2), (3, 5),$$
$$(3, 11), (5, 1), (5, 2), (7, 1), (7, 3), (13, 1), (30, 1), (42, 1), (70, 1), (78, 1).$$

Now d is d_0 times a factor of e. Therefore if e has exactly t prime factors, then there are 2^t choices for (e, d) with the same (e, d_0). Consequently there are exactly 64 choices for (e, d) obtained from the above 20 pairs of (e, d_0), and each (e, d) determines (V, φ); $\det(2\Phi) = 2d_0^2e^2/d$ as noted in §6.1. By Theorem 5.9, $\#\{SO^\varphi(V)\backslash SO^\varphi(V)_{\mathbf{A}}/C\} = 1$ in all these cases. We have actually

THEOREM 6.4. *The spaces (V, φ) obtained from these 64 pairs (e, d) exhaust all positive definite ternary quadratic spaces over $\mathbf{Q}$ for which the genus of maximal lattices has class number 1. In other words, there are exactly 64 genera of positive definite, $\mathbf{Z}$-valued, and reduced ternary forms consisting of a single class.*

Proof. Our task is to show that the class number is not 1 for $d_0e > 210$. If the inverse of the right-hand side of the equality of Lemma 6.2 is not an integer, then the class number cannot be 1. For $d_0e > 210$, the inverse is an integer exactly when (e, d_0) is one of the following six: $(2\cdot7\cdot17, 1)$, $(2\cdot5\cdot13, 3)$, $(2\cdot3\cdot17, 5)$, $(2\cdot3\cdot13, 7)$, $(2\cdot3\cdot5, 23)$, $(2\cdot3\cdot5, 11)$. The verification is easy, as the mass ≤ 1 for relatively few cases of (e, d_0). Among those six, the mass is 1/2 for the last one; in the other five cases the mass is 1. Now, by the formula in [Pe, p. 361] the type number of $\mathfrak{O}$ (which is the class number in question by virtue of Theorem 5.9) is given by $2^{-\kappa}\sum_t Sp\{P^*(t)\}$, where κ is the number of prime factors of d_0e, t runs over all positive divisors of d_0e, and $Sp\{P^*(t)\}$ is given on the same page. From the formulas there we can easily verify that $Sp\{P^*(1)\} = 2^\kappa$ and $Sp\{P^*(d_0e)\} > 0$ in the first five cases, and hence the type number is greater than 1. As for the last case $(2\cdot3\cdot5, 11)$, computing $Sp\{P^*(t)\}$ for all $t|d_0e$, we find that the type number is 2. Thus we obtain our theorem.

Remark. In the setting of §6.1, if $\det(2\Phi)/2$ is squarefree, then Φ must be reduced and $\det(2\Phi)/2 = d = d_0e$ with squarefree d_0 and e. If the genus of Φ has class number 1, then in view of the above theorem such a Φ is obtained from one of the pairs listed in §6.3 by taking $d = d_0e$. Thus there are exactly 20 genera of $\mathbf{Z}$-valued positive definite ternary forms with class number 1 such that $\det(2\Phi)/2$ is squarefree. This result was obtained by Watson [W], and we derived it from a stronger result, Theorem 6.4.

6.5. We are going to specialize Theorem 5.7 and (5.15b) to these cases, and give explicit formulas for $\#L[q, \mathbf{Z}]$. For simplicity, we consider only the cases in which e is a prime, and d_0 is 1 or a prime; thus we consider only 15 pairs (e, d_0), and consequently 30 pairs (e, d) with $d = d_0$ or $d = d_0 e$. In this setting we have

$$\#\{\Gamma(L)\} = 48/[(d_0+1)(e-1)]. \tag{6.2}$$

This is because $\#\{\Gamma(L)\}$ equals the inverse of the quantity of Lemma 6.2, as the class number is 1.

To study the nature of q for which $L[q, \mathbf{Z}] \neq \emptyset$, we consider the localization of B at e. Let $\mathfrak{r}$ denote the maximal order in the unramified quadratic extension of $\mathbf{Q}_e$. We can put $B_e^\circ = \mathbf{Q}_e\sigma + \mathbf{Q}_e\eta$, $\mathfrak{O}_e = \mathfrak{r} + \mathfrak{r}\eta$, and $\widetilde{\mathfrak{O}}_e = \mathfrak{r} + \mathfrak{r}\eta^{-1}$ with σ and η as in (B) of §1.5; we can take $\eta^2 = e$, though this is often unnecessary. We have $L = (\mathfrak{M} \cap B^\circ)\xi$, and so

$$L_e = (\mathbf{Z}_e\sigma + \mathfrak{r}\eta)\xi \quad \text{and} \quad \widetilde{L}_e = (2^{-1}\mathbf{Z}_e\sigma + \mathfrak{r}\eta^{-1})\xi \quad \text{if} \quad e \nmid d, \tag{6.3a}$$

$$L_e = (\mathbf{Z}_e\sigma + \mathfrak{r}\eta^{-1})\xi \quad \text{and} \quad \widetilde{L}_e = ((2e)^{-1}\mathbf{Z}_e\sigma + \mathfrak{r}\eta^{-1})\xi \quad \text{if} \quad e | d. \tag{6.3b}$$

Here is an easy fact: given an element η_0 of $B_e^\times$ such that η_0^2 is a prime element, we can find an element α of $B_e^\times$ such that (6.3a, b) are true with $(\alpha^{-1}\sigma\alpha, \alpha^{-1}\mathfrak{r}\alpha, \eta_0)$ in place of $(\sigma, \mathfrak{r}, \eta)$. Indeed, since $\eta_0^2/\eta^2 \in \mathbf{Z}_e^\times$, we have $\eta_0^2/\eta^2 = aa^\iota$ with $a \in \mathfrak{r}^\times$. Then $\eta_0^2 = (a\eta)^2$, and hence there exists an element α of $B_e^\times$ such that $\alpha^{-1}a\eta\alpha = \eta_0$. Since $\alpha^{-1}L_e\alpha = L_e$ and $\alpha^{-1}\widetilde{L}_e\alpha = \widetilde{L}_e$, we obtain the desired result.

Theorem 6.6. *Given $0 < q \in \mathbf{Q}$ in the setting of §6.5, put $K_0 = \mathbf{Q}(\sqrt{-dq}\,)$ and denote by δ the discriminant of K_0. Then the following assertions hold:*

(i) *$L[q, \mathbf{Z}] \neq \emptyset$ only if q is as follows:*

$$d_0eq = r^2m \quad \textit{when} \quad e \neq 2 \quad \textit{or} \quad e|d, \tag{6.4a}$$

$$d_0q = r^2m \quad \textit{when} \quad e = 2 \quad \textit{and} \quad e \nmid d. \tag{6.4b}$$

Here m is a squarefree positive integer such that e does not split in K_0, and also that $m - 3 \in 8\mathbf{Z}$ if $e = 2$ and $2|d$; r is a positive integer prime to e.

(ii) *Moreover, put $a^* = d_0$ in the following two cases:* (A) $d_0 \geq 2$, $d_0|m$, *and* $d_0 \nmid r$; (B) $d_0 = 2$, $r - 2 \in 2\mathbf{Z}$, *and* 2 *is ramified in* K_0; *put* $a^* = 1$ *if neither* (A) *nor* (B) *applies. Let $\mathfrak{C}$ be the set of all positive integers c prime to a^*e such that $d_0|c$ if d_0 is a prime that remains prime in K_0. (Thus $\mathfrak{C}$ depends on d, e, and q.) Then $r/2 \in \mathfrak{C}$ if $4|\delta$ and $e \neq 2$; $r \in \mathfrak{C}$ otherwise.*

(iii) *Conversely, given r and m satisfying all these conditions, determine q by (6.4a, b). Then $L[q, \mathbf{Z}] \neq \emptyset$.*

Notice that $K_0 = \mathbf{Q}(\sqrt{-m}\,)$ if $e|d$ or $e = 2$, and $K_0 = \mathbf{Q}(\sqrt{-em}\,)$ otherwise. Also, $\mathfrak{C} = \emptyset$ if a^* is a prime that remains prime in K_0.

Proof. Suppose $h = k\xi \in L[q, \mathbf{Z}]$ with $k \in B^\circ$; put $K = F[k]$ as in §5.2 and $\mathfrak{f} = K \cap \mathfrak{O}$; let c be the conductor of $\mathfrak{f}$. Then $K \cong K_0$ and $h \in 2\widetilde{L}$. Then from (6.3a, b) we see that $eq \in \mathbf{Z}_e$ if $e \neq 2$ or $e|d$, and $q \in \mathbf{Z}_e$ otherwise. The set $\widetilde{L}_p$ for $p \neq e$ can be given by (5.5b), and so $dq \in \mathbf{Z}_p$. Thus $d_0eq \in \mathbf{Z}$ if $e \neq 2$ or $e|d$; $d_0q \in \mathbf{Z}$ otherwise. Take $0 < r \in \mathbf{Z}$ and a squarefree positive integer m as in (6.4a, b). Define $\mathfrak{a}^*$ as in Theorem 5.7 and put $\mathfrak{a}^* = a^*\mathbf{Z}$ with $0 < a^* \in \mathbf{Z}$. Clearly $a^* = 1$ if $d_0 = 1$. Suppose d_0 is a prime number. To make our exposition easier, denote this prime by s; then $s \neq e$ and $r_s(h) = -d^{-1}q$. We can easily verify that $a^* = s$ exactly in Cases (A) and (B) stated in (ii) above. By Theorem 5.7 and Lemma 5.11, we see that $c \in \mathfrak{C}$. Notice that s is ramified in K_0 if $a^* = s$.

(1) We first consider the case $e|d$. Then $d = d_0e$ and $dq = d_0eq$ and so $K \cong \mathbf{Q}(\sqrt{-m})$. Suppose $e|r$; put $\ell = e^{-1}k$. Then $d^2\ell\ell^\iota = de^{-2}q = (r/e)^2m \in \mathbf{Z}$, and hence $d\ell \in \mathfrak{O}_e \cap B^\circ$. Thus $\ell \in e^{-1}\mathfrak{O}_e \cap B^\circ = e^{-1}\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r}$, and so $\ell\xi \in 2\widetilde{L}_e$ by (6.3b). Therefore $h = e\ell\xi \in 2e\widetilde{L}_e$, which implies that $\varphi(h, L)_e \subset e\mathbf{Z}_e$, a contradiction. Thus $e \nmid r$.

(2) Next suppose $e \nmid d$; then $d = d_0$. Assuming $e|r$, put $\ell = e^{-1}k$. Then $d^2\ell\ell^\iota = de^{-2}q \in e^{-1}\mathbf{Z}_e$, and hence $\ell \in \widetilde{\mathfrak{O}}_e \cap B^\circ = \mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r}$. Thus $\ell\xi \in 2\widetilde{L}_e$ by (6.3a), which leads to a contradiction for the same reason as in Case (1). Therefore $e \nmid r$ in this case too. This reasoning is valid even when $e = 2$.

(3) Since K_0 must be embeddable in B, the prime e cannot split in K_0. Suppose $e = 2$, $e|d$, and $e|m$. Since $kk^\iota = d^{-2}r^2m$, we have $k \in \eta^{-1}\mathfrak{O}_e^\times \cap B^\circ$, so that $k = a\sigma + \eta^{-1}b$ with $a \in \mathbf{Z}_e$ and $b \in \mathfrak{r}$. Since $\eta k \in \mathfrak{O}_e^\times$, we have $b \in \mathfrak{r}^\times$. By (6.3b), $2\varphi(h, L)_e = 2\mathrm{Tr}_{B/F}\big(k(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\big) = 4a\mathbf{Z}_e + \mathrm{Tr}_{K/\mathbf{Q}}(b\mathfrak{r}) = \mathbf{Z}_e$, a contradiction. Therefore m must be odd if $e = 2$ and $e|d$. In this case, $k \in 2^{-1}\mathfrak{O}_e^\times \cap B^\circ$, so that $2k = x\sigma + \eta y$ with $x \in \mathbf{Z}_e^\times$ and $y \in \mathfrak{r}$. Thus $2\mathbf{Z}_e = 2\varphi(h, L)_e = 2\mathrm{Tr}_{B/F}\big(k(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\big) = 2\mathbf{Z}_e + \mathrm{Tr}_{K/\mathbf{Q}}(y\mathfrak{r})$, so that $y \in 2\mathfrak{r}$. Now $r^2m = dq = d^2kk^\iota = -d_0^2(x^2\sigma^2 + 2yy^\iota)$. We can take $\mathfrak{r} \subset \mathbf{Q}_2(\sqrt{5})$ and $\sigma = \sqrt{5}$. Therefore we see that $m - 3 \in 8\mathbf{Z}$. Thus we obtain the condition on m as stated in our theorem.

(4) By Theorem 5.7, c is prime to a^*e and $c^2\delta\mathbf{Z}_p = d_0q\mathbf{Z}_p = r^2m\mathbf{Z}_p$ for every $p \neq e$. We have seen that r is prime to e. First suppose $4|\delta$ and $e \neq 2$. Then we see that $\delta\mathbf{Z}_p = 4m\mathbf{Z}_p$ for $p \neq e$, and so $4c^2\mathbf{Z}_p = r^2\mathbf{Z}_p$ for $p \neq e$. Since both $2c$ and r are prime to e, we obtain $2c = r$. Similarly we easily find that $c = r$ if $4 \nmid \delta$ or $e = 2$. Thus we obtain (ii). This completes the proof of the "if"-part.

(5) Conversely, suppose q is given with r and m as in our theorem; put $c = r/2$ or $c = r$ according as $r/2 \in \mathfrak{C}$ or $r \in \mathfrak{C}$. Let $\mathfrak{o}$ be the order in K_0 whose conductor is c. By Lemma 5.12, our conditions on r and m guarantees an injection θ of K_0 into B such that $\theta(\mathfrak{o}) = \theta(K_0) \cap \mathfrak{O}$. Our task is to find an element h such that $\varphi[h] = q$ and $\varphi(h, L) = \mathbf{Z}$. Put $\mu = \theta(\sqrt{-m})$ if $K_0 = \mathbf{Q}(\sqrt{-m})$.

(5a) First we consider the case $e|d$ and $|\delta| = m$. Then $d = d_0e$, $r = c$, and $K_0 = \mathbf{Q}(\sqrt{-m})$. Put $h = k\xi$ with $k = d^{-1}r\mu$. Then $\varphi[h] = q$ and by Theorem 5.7, $dq\varphi(h, L)_p^{-2} = c^2\delta\mathbf{Z}_p = r^2 m\mathbf{Z}_p$ for every $p \neq e$, so that $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq e$. Now $2\varphi(h, L)_e = d\mathrm{Tr}_{B/F}\bigl(k(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\bigr) = \mathrm{Tr}_{B/F}\bigl(\mu(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\bigr)$ by (6.3b). If $e|m$, then we can take μ as η, changing $\mathfrak{r}$ by an inner automorphism, as noted after (6.3b). (Since $|\delta| = m$, we have $e \neq 2$.) If $e \nmid m$, then we can take $\mathfrak{r} \subset \theta(K_0)_e$ and $\sigma = \mu$. In either case we easily see that $2\varphi(h, L)_e = 2\mathbf{Z}_e$. Thus $\varphi(h, L) = \mathbf{Z}$, and $L[q, \mathbf{Z}] \neq \emptyset$ as expected.

(5b) Next suppose $e|d$ and $|\delta| = 4m$; then $r = 2c$ if $e \neq 2$ and $r = c$ if $e = 2$. We have $K_0 = \mathbf{Q}(\sqrt{-m}\,)$ and we again take $h = k\xi$ with $k = d^{-1}r\mu$. Then $\varphi[h] = q$ and $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq e$ for the same reason as in (5a). If $e \neq 2$, the same argument as in (5a) shows that $\varphi(h, L)_e = \mathbf{Z}_e$, which leads to the desired result. Thus suppose $e = 2$. Then $m-3 \in 8\mathbf{Z}$ as stipulated in our theorem. We can take $\sigma = \sqrt{5}$ as we did in (3). Put $\mu = a\sigma + \eta b$ with $a \in \mathbf{Z}_e$ and $b \in \mathfrak{r}$. Then $a \in \mathbf{Z}_e^\times$ and $-m = a^2\sigma^2 + 2bb^\rho$. Since $m+\sigma^2 \in 8\mathbf{Z}_e$, we see that $b \in 2\mathfrak{r}$. Thus $2\varphi(h, L)_e = \mathrm{Tr}_{B/F}\bigl(\mu(\mathbf{Z}_e\sigma+\eta^{-1}\mathfrak{r})\bigr) = 2\mathbf{Z}_e + \mathrm{Tr}_{K/\mathbf{Q}}(b\mathfrak{r}) = 2\mathbf{Z}_e$, which gives the expected result.

(5c) Suppose $e \nmid d$ and $e = 2$. Then $d = d_0$ and $K_0 = \mathbf{Q}(\sqrt{-m}\,)$; we take $h = k\xi$ with $k = d^{-1}r\mu$. We find that $\varphi[h] = q$ and $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq 2$ in the same manner as in (5a). Now $2\varphi(h, L)_2 = \mathrm{Tr}_{B/F}\bigl(\mu(\mathbf{Z}_2\sigma + \eta\mathfrak{r})\bigr)$ by (6.3a). If $2|m$, then taking μ as η, we obtain $2\varphi(h, L)_2 = 2\mathbf{Z}_2$ as expected. Suppose $2 \nmid m$; then $\mu = a\sigma + \eta b$ with $a \in \mathbf{Z}_2^\times$ and $b \in \mathfrak{r}$, and so $\mathrm{Tr}_{B/F}\bigl(\mu(\mathbf{Z}_2\sigma + \eta\mathfrak{r})\bigr) = 2\mathbf{Z}_2$, which gives the desired result.

(5d) Finally suppose $e \nmid d$ and $e \neq 2$. Then $d = d_0$ and $K_0 = \mathbf{Q}(\sqrt{-em}\,)$; we take $h = k\xi$ with $k = \theta(d^{-1}e^{-1}r\sqrt{-em}\,)$; then $\varphi[h] = q$. For $p \neq e$, $\delta\mathbf{Z}_p$ equals $m\mathbf{Z}_p$ or $4m\mathbf{Z}_p$, and $r = c$ or $r = 2c$ accordingly. Then we easily see that $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq e$ in the same manner as in (5a). Now $2\varphi(h, L)_e = \mathrm{Tr}_{B/F}\bigl(e^{-1}\theta(\sqrt{-em}\,)(\mathbf{Z}_2\sigma + \eta\mathfrak{r})\bigr)$. If $e|m$, then we can put $\theta(\sqrt{-em}\,) = e(a\sigma + \eta b)$ with $a \in \mathbf{Z}_e^\times$ and $b \in \mathfrak{r}$, and obtain $\varphi(h, L)_e = \mathbf{Z}_e$. If $e \nmid m$. then taking $\eta = \theta(\sqrt{-em}\,)$, we obtain the desired result. This completes the proof.

THEOREM 6.7. *If $L[q, \mathbf{Z}] \neq \emptyset$ in the setting of Theorem 6.6, then*

$$\#L[q, \mathbf{Z}] = \frac{2^{1-\mu} \cdot 48 \cdot \mathbf{c}(K_0)}{(d_0+1)(e-1)w} \cdot c\prod_{p|c}\bigl\{1 - [K_0/\mathbf{Q},\, p]p^{-1}\bigr\}.$$

Here μ is the number of prime factors of a^*e ramified in K_0; $\mathbf{c}(K_0)$ is the class number of K_0; w is the number of roots of unity in K; $c = r/2$ if $4|\delta$ and $e \neq 2$; $c = r$ otherwise; $[K_0/\mathbf{Q}, p]$ is defined as in Theorem 5.7.

Proof. Specialize (5.15b) to the present case. Then $[U : 1] = w$ and $\#\Gamma(L)$ is given by (6.2); $c(\mathfrak{f})$ can be connected to $\mathbf{c}(K_0)$ by (5.13) and (5.14). Thus we obtain our formula.

6.8. Before discussing examples, let us insert here a remark applicable to (V, φ) over $\mathbf{Q}$ with an arbitrary n. If $F = \mathbf{Q}$ and $\mathfrak{g} = \mathbf{Z}$, it is natural to consider $L[q, \mathbf{Z}]$, but it is not always best to formulate the result with respect to a **Z**-basis of L. To see this, first take the standard basis $\{e_i\}_{i=1}^n$ of $\mathbf{Z}^n = L$, and define a matrix Φ by $\Phi = [\varphi(e_i, e_j)]_{i,j=1}^n$; put $f_i = e_i\Phi^{-1}$. Then $2\widetilde{L} = \sum_{i=1}^n \mathbf{Z}f_i$. Let $h \in L[q, \mathbf{Z}]$. Then $h \in 2\widetilde{L}$, and so $h = \sum_{i=1}^n a_i f_i$ with $a_i \in \mathbf{Z}$. We easily see that $\varphi(h, L) = \mathbf{Z}$ if and only if $\sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z}$, and also that $\Phi^{-1} = [\varphi(f_i, f_j)]_{i,j=1}^n$. This means that

$$(6.5)\quad L[q, \mathbf{Z}] = \left\{ \textstyle\sum_{i=1}^n a_i f_i \,\middle|\, a\Phi^{-1} \cdot {}^t a = q,\ \sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z}\right\}, \quad a = (a_i)_{i=1}^n.$$

Therefore if we follow the traditional definition of primitivity, we have to use the matrix Φ^{-1} instead of Φ. Recall that $\Gamma(L) = \Gamma(\widetilde{L})$. Thus $\Gamma(L)$ can be represented, with respect to the basis $\{f_i\}_{i=1}^n$, by the group

$$(6.6)\qquad \Gamma' = \left\{\gamma \in SL_n(\mathbf{Z}) \,\middle|\, \gamma\Phi^{-1} \cdot {}^t\gamma = \Phi^{-1}\right\}.$$

Consequently, $L[q, \mathbf{Z}]/\Gamma(L)$ corrresponds to the vectors a such that $a\Phi^{-1}\cdot{}^t a = q$ and $\sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z}$, considered modulo Γ'. We note here an easy fact:

$$(6.7)\qquad |\det(2\Phi)| = [\widetilde{L} : L].$$

6.9. Let us now illustrate Theorem 6.6 by considering five examples and formulating the results in terms of the matrix Φ^{-1} of §6.8. For $(e, d) = (2, 1)$ we obtain the result on sums of three squares, which Gauss treated; we do not include this in our examples, as it is easy and too special. Indeed, in this case we have $\Phi = \Phi^{-1}$, and so the result concerns the primitive solutions of $\sum_{i=1}^3 x_i^2 = q$. But in all other cases, $\Phi \neq \Phi^{-1}$, and the results have more interesting features. From Lemma 5.3 (i) and (6.7) we obtain $\det(2\Phi) = 2d_0^2e^2/d$. In each case we state only the condition for $L[q, \mathbf{Z}] \neq \emptyset$. We will dispense with the statement about $\#L[q, \mathbf{Z}]$, as it is merely a specialization of Theorem 6.7.

(1) We first take $e = d = 3$ in Theorem 6.6. Then

$$(6.8)\qquad 2\Phi = \operatorname{diag}\left[2,\ \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 3\Phi^{-1} = \operatorname{diag}\left[3,\ \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}\right].$$

These forms of matrices can be obtained by analyzing L of (5.4) in the present case. Alternatively, since $\det(2\Phi) = 6$ for Φ of (6.8), we can conclude that Φ is the matrix representing φ by the principle explained in [S5]. Theorem 6.6 (or the form of Φ^{-1}) in the present case shows that $L[q, \mathbf{Z}] \neq \emptyset$ only when $3q \in \mathbf{Z}$. Thus with $s = 3q \in \mathbf{Z}$, the principle of §6.8 says that $L[s/3, \mathbf{Z}]$ corresponds to the set of vectors (x, y, z) such that

$$(6.9)\qquad 3x^2 + 4(y^2 + yz + z^2) = s \quad \text{and} \quad x\mathbf{Z} + y\mathbf{Z} + z\mathbf{Z} = \mathbf{Z}.$$

Theorem 6.6 specialized to this case means that given $0 < s \in \mathbf{Q}$, we can find (x, y, z) satisfying (6.9) if and only if $s = r^2m$ with a squarefree positive integer m such that $m+1 \notin 3\mathbf{Z}$ and a positive integer r prime to 3 such that $2|r$ if $m + 1 \notin 4\mathbf{Z}$; $K_0 = \mathbf{Q}(\sqrt{-m}\,)$.

(2) Next we take $e = 3$ and $d = 1$. Then

$$(6.10)\qquad 2\Phi = \operatorname{diag}\left[6,\ \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 3\Phi^{-1} = \operatorname{diag}\left[1,\ \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}\right].$$

Therefore $L[s/3, \mathbf{Z}]$ corresponds to the set of vectors (x, y, z) such that

$$x^2 + 4(y^2 + yz + z^2) = s \quad \text{and} \quad x\mathbf{Z} + y\mathbf{Z} + z\mathbf{Z} = \mathbf{Z}. \tag{6.11}$$

Such vectors exist if and only if $s = r^2 m$ with a squarefree positive integer m such that 3 does not split in $K_0 = \mathbf{Q}(\sqrt{-3m}\,)$ and a positive integer r prime to 3 such that $2|r$ if 4 divides the discriminant of K_0.

In both cases (1) and (2) the group $\Gamma(L)$ has order 12. Represent $(x, y, z) \in \mathbf{Z}^3$ by (x, β) with $\beta = y + z\zeta$, where ζ is a primitive cubic root of unity. Then Γ' of (6.6) consists of the maps $(x, \beta) \mapsto (x, \varepsilon\beta)$ and $(x, \beta) \mapsto (-x, \varepsilon\overline{\beta})$, where ε is a sixth root of unity. Therefore a set of representatives for $L[q, \mathbf{Z}]/\Gamma(L)$ can be found numerically. For instance, take $s = m = 79$ in (6.9); then we easily find that $\#\bigl\{L[q, \mathbf{Z}]/\Gamma(L)\bigr\} = 5$, which combined with (5.15a) confirms that $\mathbf{Q}(\sqrt{-79}\,)$ has class number 5.

(3) Our third example concerns the case $e = d = 2$. We have

$$2\Phi = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix}, \quad 2\Phi^{-1} = \begin{bmatrix} 3 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 3 \end{bmatrix}. \tag{6.12}$$

Then $L[s/2, \mathbf{Z}]$ corresponds to the set of vectors $x = (x_i)_{i=1}^3 \in \mathbf{Z}^3$ such that

$$x \cdot 2\Phi^{-1} \cdot {}^t x = s \quad \text{and} \quad \textstyle\sum_{i=1}^3 x_i\mathbf{Z} = \mathbf{Z}. \tag{6.13}$$

Such vectors x exist if and only if $s = r^2 m$ with an odd integer r and a squarefree positive integer m such that $m - 3 \in 8\mathbf{Z}$. In this case, $K_0 = \mathbf{Q}(\sqrt{-m}\,)$.

(4) Take $e = d = 7$. We have then

$$2\Phi = \mathrm{diag}\left[2,\ \begin{bmatrix} 4 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 7\Phi^{-1} = \mathrm{diag}\left[7,\ \begin{bmatrix} 4 & 2 \\ 2 & 8 \end{bmatrix}\right], \tag{6.14}$$

and $L[s/7, \mathbf{Z}]$ with $s \in \mathbf{Z}$ corresponds to the set of vectors (x, y, z) such that

$$7x^2 + 4(y^2 + yz + 2z^2) = s \quad \text{and} \quad x\mathbf{Z} + y\mathbf{Z} + z\mathbf{Z} = \mathbf{Z}. \tag{6.15}$$

Such vectors exist if and only if $s = r^2 m$ with a positive integer r prime to 7 and a squarefree positive integer m such that 7 does not split in $K_0 = \mathbf{Q}(\sqrt{-m}\,)$; $2|r$ if $m + 1 \notin 4\mathbf{Z}$.

(5) Let us finally take $e = 2$ and $d = 22$. We have then

$$2\Phi = \mathrm{diag}\left[4,\ \begin{bmatrix} 6 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 22\Phi^{-1} = \mathrm{diag}\left[11,\ \begin{bmatrix} 8 & 4 \\ 4 & 24 \end{bmatrix}\right], \tag{6.16}$$

and the result about $L[s/22, \mathbf{Z}]$ is what we stated in the introduction.

References

[E1] M. Eichler, Quadratische Formen und orthogonale Gruppen, Springer, Berlin, 1952, 2nd ed. 1974.

[E2] M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, J. reine angew. Math. 195 (1956), 127–151.

[Pe] M. Peters, Ternäre und quaternäre quadratische Formen und Quaternionenalgebren, Acta Arithmetica 15 (1969), 329–365.

[Pi] A. Pizer, Type numbers of Eichler orders, J. reine angew. Math. 264 (1973), 76–102.

[S1] G. Shimura, Euler Products and Eisenstein series, CBMS Regional Conference Series in Mathematics, No. 93, Amer. Math. Soc. 1997.

[S2] G. Shimura, An exact mass formula for orthogonal groups, Duke Math. J. 97 (1999), 1–66 (=Collected Papers, IV, 509–574).

[S3] G. Shimura, Arithmetic and analytic theories of quadratic forms and Clifford groups, Mathematical Surveys and Monographs, vol. 109, Amer. Math. Soc. 2004.

[S4] G. Shimura, Quadratic Diophantine equations and orders in quaternion algebras, Amer. J. Math. 128 (2006), 481–518.

[S5] G. Shimura, Classification, construction, and similitudes of quadratic forms, to appear in Amer. J. Math. 128 (2006).

[S6] G. Shimura, Quadratic Diophantine equations, the class number, and the mass formula, Bulletin, Amer. Math. Soc. 43 (2006), 285–304.

[S7] G. Shimura, Classification of integer-valued symmetric forms, to appear in Amer. J. Math. 129 (2007).

[W] G. L. Watson, One-class genera of positive ternary quadratic forms, Mathematika 19 (1972), 96–104.

Goro Shimura
Department of Mathematics
Princeton University
Princeton, New Jersey 08544-1000
U.S.A.
goro@Math.Princeton.EDU

Strictly Convex Drawings of Planar Graphs

Imre Bárány and Günter Rote

Received: July 13, 2005
Revised: June 21, 2006

Communicated by Günter Ziegler

Abstract. Every three-connected planar graph with n vertices has a drawing on an $O(n^2) \times O(n^2)$ grid in which all faces are strictly convex polygons. These drawings are obtained by perturbing (not strictly) convex drawings on $O(n) \times O(n)$ grids. Tighter bounds are obtained when the faces have fewer sides. In the proof, we derive an explicit lower bound on the number of primitive vectors in a triangle.

2000 Mathematics Subject Classification: Primary 05C62; Secondary 52C05.
Keywords and Phrases: Graph drawing, planar graphs.

1 Introduction

A *strictly convex* drawing of a planar graph is a drawing with straight edges in which all faces, including the outer face, are strictly convex polygons, i. e., polygons whose interior angles are less than 180°.

Theorem 1. (i) *A three-connected planar graph with n vertices in which every face has at most k edges has a strictly convex drawing on an $O(nw) \times O(n^2k/w)$ grid of area $O(n^3k)$, for any choice of a parameter w in the range $1 \le w \le k$.*

(ii) *In particular, every three-connected planar graph with n vertices has a strictly convex drawing on an $O(n^2) \times O(n^2)$ grid, and on an $O(n) \times O(n^3)$ grid.*

(iii) *For $k \le 4$, an $O(n) \times O(n)$ grid suffices.*
The drawings can be constructed in linear time.

When referring to a $W \times H$ grid of width W and height H, the constant hidden in the O-notation is on the order of 100 for the width and on the order of 10000 for the height. This is far too much for applications where one wants to draw graphs on a computer screen, for example. For the case $w = 1$, the bound is tighter: the grid size is approximately $14n \times 30n^2k$. For part (iii) of the theorem, the grid size is at most $14n \times 14n$, and if the outer face is a triangle, it is $2n \times 2n$.

The main idea of the proof is to start with a (non-strictly) convex embedding, in which angles of 180° are allowed, and to perturb the vertices to obtain strict convexity. We will use an embedding with special properties that is provided by the so-called *Schnyder embeddings*, which are introduced in Section 2.

Historic context. The problem of drawing graphs with straight lines has a long history. It is related to realizing three-connected planar graphs as three-dimensional polyhedra. By a suitable projection on a plane, one obtains from a polyhedron a straight-line drawing, a so-called *Schlegel diagram.* The faces in such a drawing are automatically strictly convex. By a projective transformation, it can be arranged that the projection along a coordinate axis is possible, and hence a suitable realization as a grid polytope gives rise to a grid drawing of the graph. However, the problem of realizing a graph as a polytope is more restricted: not every drawing with strictly convex faces is the projection of a polytope. In fact, there is an exponential gap between the known grid size for strictly convex planar drawings and for polytopes in space.

The approaches for realizing a graph as a polytope or for drawing it in the plane come in several flavors. The classical methods of Steinitz (for polytopes) and Fáry and Wagner (for graphs) work incrementally, making local modifications to the graph and adapting the geometric structure accordingly. Tutte [15, 16] gave a "one-shot" approach for drawing graphs that sets up a system of equations. This method yields also a polytope via the Maxwell-Cremona correspondence, see [11]. All these methods give embeddings that can be drawn on an integer grid but require an exponential grid size (or even larger, if one is not careful).

The first methods for straight-line drawings of graphs on an $O(n) \times O(n)$ grid were proposed for triangulated graphs, independently by de Fraysseix, Pach and Pollack [7] and by Schnyder [13]. The method of de Fraysseix, Pach and Pollack [7] is incremental: it inserts vertices in a special order, and modifies a partial grid drawing to accommodate new vertices. In contrast, Schnyder's method is another "one-shot" method: it constructs some combinatorial structure in the graph, from which the coordinates of the embedding can be readily determined afterwards. Both methods work in linear time. $O(n) \times O(n)$ is still the best known asymptotic bound on the size of planar grid drawings.

If graphs are not triangulated, the first challenge is to get faces which are convex. (Without the convexity requirement one can just add edges until the graph becomes triangulated, draw the triangulated supergraph and remove the extra edges from the drawing.) Many algorithms are now known that construct convex (but not necessarily strictly convex) drawings with $O(n) \times O(n)$ size, for example by Chrobak and Kant [5] (à la Fraysseix, Pach and Pollack); or Schnyder and Trotter [14] and Felsner [8], see also [4] (à la Schnyder). Our algorithm builds on the output of Felsner's algorithm, which is described in the next section. Luckily, this embedding has some special features, which our algorithm uses.

The idea of getting a strictly convex drawing by perturbing a convex drawing was pioneered by Chrobak, Goodrich and Tamassia [6]. They claimed to construct strictly convex embeddings on an $O(n^3) \times O(n^3)$ grid, without giving full details, however. This was improved to $O(n^{7/3}) \times O(n^{7/3})$ in [12]. In this paper we further improve the "fine perturbation" step of [12] to obtain a bound of $O(n^2) \times O(n^2)$ for grid drawings. Theorem 1 gives better bounds when the faces have few sides, and we allow grids of different aspect ratios (keeping the same total area).

In the course of the proof, we need explicit (not just asymptotic) lower bounds on the number of primitive vectors in certain triangles. A primitive vector is an integer vector which is not a multiple of another integer vector; hence, primitive vectors can be used to characterize the directions of polygon edges. The existence of many short primitive vectors is the key to constructing strictly convex polygons with many sides. These lower bounds are derived in Section 5, based on elementary techniques from the geometry of numbers.

2 Preliminaries: Schnyder Embeddings of Three-Connected Plane Graphs

Felsner [8] (see also [9, 4]) has extended the straight-line drawing algorithm of Schnyder, which works for triangulated planar graphs, to arbitrary three-connected graphs. It constructs a drawing with special properties, beyond just having convex faces. These properties will be crucial for the perturbation step.

Felsner's algorithm works roughly as follows. The edges of the graph are covered by three directed trees which are rooted at three selected vertices a, b, c on the boundary, forming a *Schnyder wood*. The three trees define for each vertex v three paths from v to the respective root, which partition the graph into three regions. Counting the faces in each region gives three numbers x, y, z which can be used as barycentric coordinates for the point v with respect to the points a, b, and c. Selecting abc as an equilateral triangle of side length $f-1$ (the number of interior faces of the graph) yields vertices which lie on a hexagonal grid formed by equilateral triangles of side length 1, see Figure 1a. Since $f \leq 2n$ this yields a drawing on a grid of size $2n \times 2n$.

This straight-line embedding has the following important property (see [8, Lemma 4 and Figure 11], [4, Fact 5]):

> *The Three Wedges Property.* Every vertex except the corners a, b, c has exactly one incident edge in each of the three closed 60° wedges shown in Figure 2a.

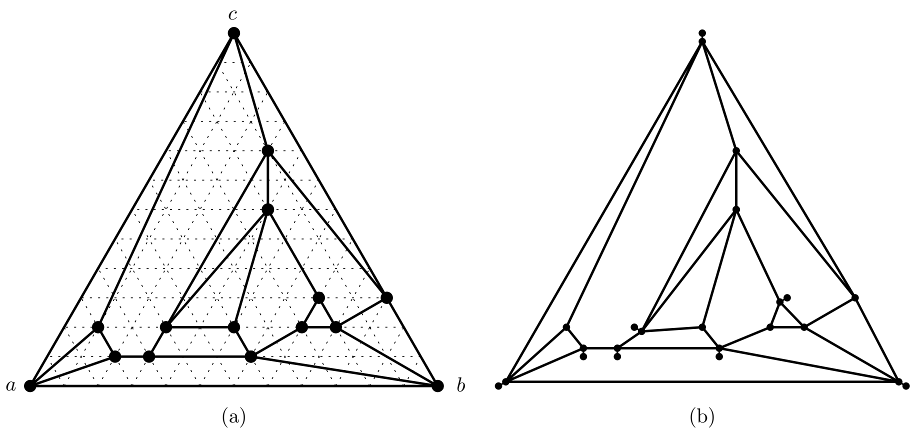


Figure 1: (a) A Schnyder embedding on a hexagonal grid and (b) on the refined grid after the initial (rough) perturbation

From this it follows immediately that there can be no angle larger than 180°, and hence all faces are convex. Moreover, it follows that the interior faces F have the *Enclosing Triangle Property*, see Figure 4a ([8, proof of Lemma 7], [4, Lemma 2]):

> *The Enclosing Triangle Property.* Consider the line x = const through the point of F with maximum x-coordinate, and similarly for the other three coordinate directions. These three lines form a triangle T_F which encloses F. Then all vertices of F lie on the boundary of T_F, but F contains none of the vertices of T_F.

It follows that interior faces with $k \leq 4$ sides are already strictly convex. Throughout, we will call T_F the *enclosing triangle* of the face F.

The Schnyder wood and the coordinates of the points can be calculated in linear time. Recently, Bonichon, Felsner, and Mosbah [4], have improved the grid size to $(n-2) \times (n-2)$. However, the resulting drawing does not have the Three Wedges Property. An alternative algorithm for producing an embedding with a property similarly to the Enclosing Triangle Property is sketched in Chrobak, Goodrich and Tamassia [6]. It proceeds incrementally in the spirit of the algorithm of de Fraysseix, Pach and Pollack [7] and takes linear time. From the details given in [6] it is not clear whether the embedding has also the Three Wedges Property, which we need for our algorithm. The original algorithm of Chrobak and Kant [5] achieves a weak form of the Three Wedges Property, where F is permitted to contain vertices of T_F. Maybe, this algorithm can be modified to obtain the Three Wedges Property, at the expense of a constant-factor blow-up in the grid size.

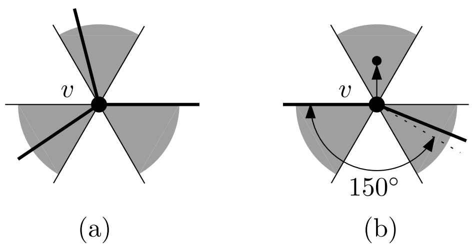


Figure 2: (a) Each closed shaded wedge contains exactly one edge incident to v. There may be additional edges in the interior of the white sectors. (b) A typical situation at a vertex which is perturbed.

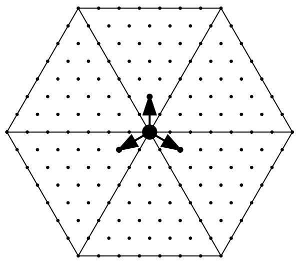


Figure 3: The three possible new positions for a single vertex in the rough perturbation. (Only the three boundary vertices a, b, c are pushed in directions opposite to these.)

3 Rough Perturbation

Before making all faces strictly convex, we perform an initial perturbation on a refined grid which is smaller by only a constant factor. This preparatory step will ensure that the subsequent "fine perturbation" can treat each face independently.

We overlay a triangular grid which is scaled by a factor of $1/7$, see Figures 3 and 5. A point may be moved to one of the three possible positions shown in Figure 3, by a distance of $\sqrt{3}/7$. The precise rules are as follows: A vertex v on an interior face F is moved if and only if the following two conditions hold.

(i) The interior angle of F at v is larger than 150° (including the possibility of a straight angle of 180°); and

(ii) v is incident to an edge of F which lies on the enclosing triangle T_F.

See Figure 2b for a typical case. Such a vertex is then pushed "out", perpendicular to the edge of T_F. We call the angle between the two edges incident

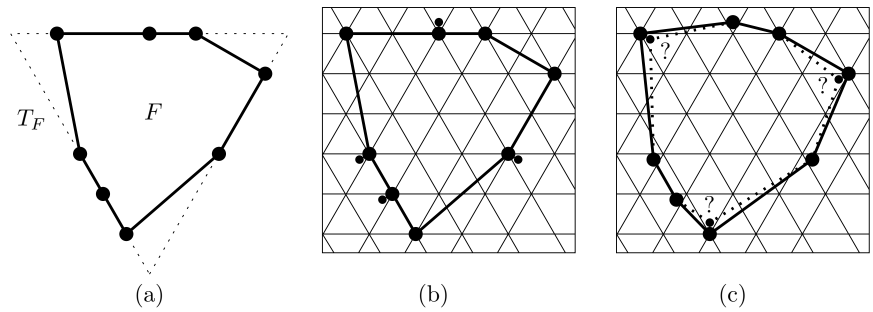


Figure 4: (a) A typical face F constructed by the convex embedding algorithm. (b) The new positions of the vertices of F which are pushed out are indicated. (c) The result of the rough perturbation. The perturbation of the vertices with question marks depends on the other faces incident to these vertices.

to F and v the *critical angle* of v. For a boundary vertex different from a, b, c, the exterior angle is the critical angle, but these vertices are not subject to the rough perturbation. The three corners a, b, and c are treated specially: they are pushed straight *into* the triangle by the rough perturbation, as illustrated in Figure 1. Examples can be seen in Figure 4b–c and Figure 5. The result of

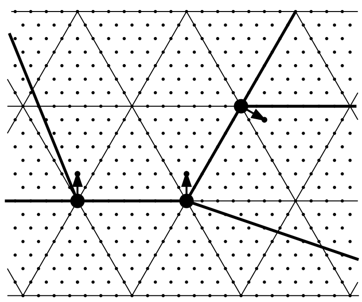


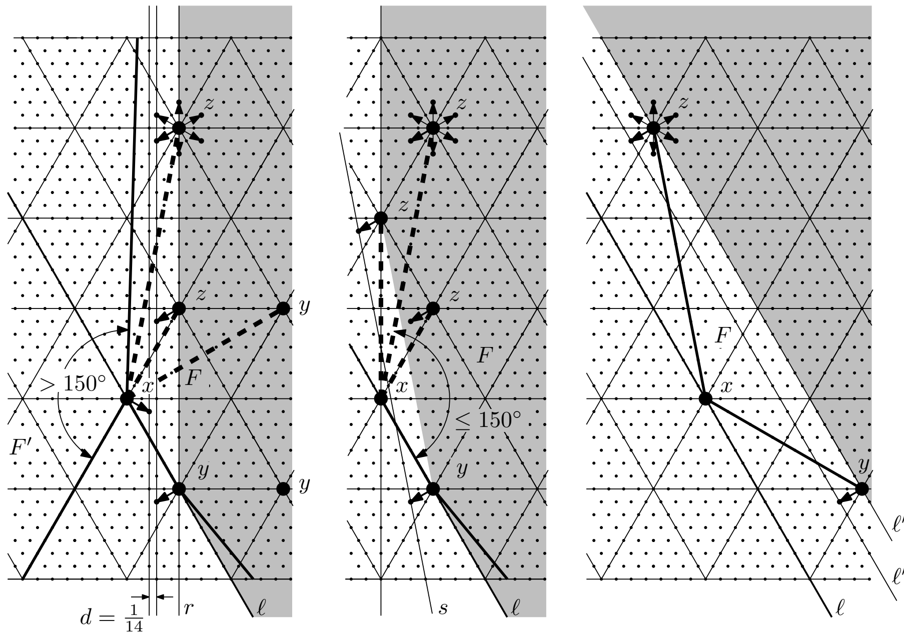
Figure 5: Example of the rough perturbation.

perturbing the example in Figure 1a is shown in Figure 1b.

There can be no conflict in applying the rules by regarding a vertex v as part of different faces: the bound of 150° on the angle, together with the Three Wedges Property ensures that there is at most one critical angle for every vertex (Figure 2b).

The result has the following properties:

Lemma 1. *After the rough perturbation, all faces are still convex. Moreover, if each vertex is additionally perturbed within a disk of radius* $1/30$*, the only concave angle that might arise at a vertex* v *is the critical angle of* v*.*



(a) Case I (b) Case IIa (c) Case IIb

Figure 6: The cases in the proof of Lemma 1. The figures show possible locations for the neighbors y and z of x.

Proof. It is evident that no critical angle can become bigger than 180°. For non-critical angles, this is also easy to see (cf. Figure 4c). (In fact, the second statement is a strengthening of this claim.)

We now prove this second statement of the lemma by considering different cases. The reader who is satisfied with the existence of *some* small enough perturbation bound $\varepsilon > 0$ may skip the rest of the proof. We continue to show that we can choose $\varepsilon = 1/30$.

Consider a non-critical angle yxz at a vertex x in a face F. We assume without loss of generality that x lies on the *lower left* edge ℓ of the enclosing triangle T_F.

Case I. The point x is incident to a critical angle of another face F', and thus x is pushed out of F'.

Without loss of generality, we can assume that x lies on the lower right edge of $T_{F'}$, and thus x is perturbed in the lower right direction, as in Figure 6a. (The other case, when x lies on the upper edge of $T_{F'}$ and is pushed vertically upward, is symmetric.) By the definition of critical angles, the angle in F' must be bigger than 150°. This excludes from F all points vertically above x or to the left of x. The upper neighbor z of x, which is a grid point, is therefore restricted to a closed halfplane right of a vertical line r at distance $1/2$ from x. The lower neighbor y must lie on or above the line ℓ that bounds the enclosing triangle T_F. Thus, y and z are restricted to the shaded area in Figure 6a. Even if all three points are perturbed by the rough perturbation, they are still separated by a vertical strip of width $d = \frac{1}{2} - 2 \cdot \frac{3}{14} = \frac{1}{14}$. An additional perturbation of $\frac{1}{30} < \frac{1}{2 \cdot 14}$ cannot make the angle at x larger than $180°$.

Case II. The point x not perturbed by the initial perturbation.

Case IIa. The point x has a neighbor on ℓ.

We can assume w.l.o.g. that it is the lower neighbor y, see Figure 6b. The angle yxz must be at most $150°$ because otherwise x would be critical. It means that z cannot lie to the left of x, and thus y and z are restricted to the shaded area in Figure 6b. Even if they are perturbed, they remain above the line s, which is obtained by offsetting the edge of the shaded region that is closest to x. The distance from x to s is $1/7 \cdot \sqrt{3/7} \approx 0.0935 > \frac{2}{30}$. Thus, there is enough space to additionally perturb the points x, y and z without creating a concave angle. (Actually, the vertex x will not even be perturbed in the fine perturbation.)

Case IIb. The point x has no neighbors on ℓ, see Figure 6c.

This means that y and z lie on or beyond the next grid line ℓ' parallel to ℓ. The rough perturbation can move them closer to ℓ, but they remain beyond another parallel line ℓ'' whose distance from x is $5/7 \cdot \sqrt{3/4} \approx 0.618$. This leaves plenty of space for additional perturbations of x, y, and z. □

After the rough perturbation, we will subject every vertex v that is incident to a critical angle to an additional small perturbation of a distance at most $1/30$. The lemma ensures that, in order to achieve convexity at v without destroying convexity at another place, we only have to take care of *one* incident face when we decide the final perturbation of v. We can thus work on each face independently to make it strictly convex.

4 Fine Perturbation

We will now discuss how we go about achieving strict convexity of all faces. The rough perturbation helps us to reduce this task to the case of regularly spaced points on a line (Section 4.1). In Section 4.2, we will describe in detail how the perturbed strictly convex chain is constructed for this special case.

4.1 The Setting after the Rough Perturbation

After the rough perturbation, we are in the following situation. Consider a maximal chain $v_2, v_3, \ldots, v_{K-1}$ of successive critical angles on a face F. These angles must be made strictly convex by perturbing them inside their little disks. (The two extreme angles at v_2 and v_{K-1} might already be convex.) The vertices $v_2, v_3, \ldots, v_{K-1}$ lie originally on a common edge of the enclosing triangle T_F, We first discuss the case when the vertices lie on the upper edge ℓ of T_F, forming a horizontal chain, as in Figure 7a. (The extension to the other two cases is discussed in Section 4.3.) According to Lemma 1 we have to

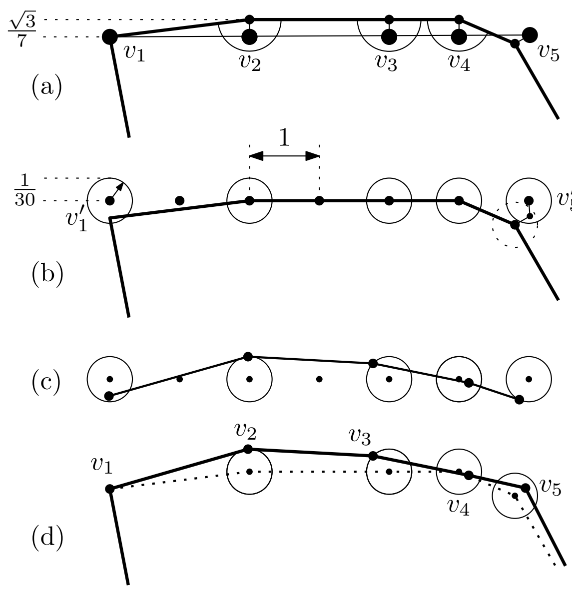


Figure 7: The setting of the fine perturbation process: (a) The initial situation after the rough perturbation. The angles in which it is necessary to ensure a convex angle are marked. (b) The circles in which the fine perturbation is performed. The size of the circles is exaggerated to make the perturbation more conspicuous. (c) A strictly convex polygon inside the circles. (d) The final result.

ensure that these critical angles are smaller than 180° after the perturbation. In Figure 7a, these are the vertices v_2, v_3, and v_4. Let us call these vertices *critical vertices*. In addition, we look at the two adjacent vertices v_1 and v_K on F. By the choice of a maximal chain, they are not critical for F. They may lie on the same line as the critical vertices, as the vertices v_1 and v_5 in Figure 7a, or they might lie below this line. To guide the perturbation of the points $v_2, \dots, v_{K-1}$, we pretend that v_1 and v_K are part of the chain, and we create *surrogate positions* v_1' and v_K' for these neighbors: First we move them from their original positions vertically upward to ℓ; if they don't land on a grid point, we move them outward by 1/2 unit. Since the angles at v_2 and v_{K-1} are bigger than 150°, we are sure that $v_1', v_2, \dots, v_{K-1}, v_K'$ lie on ℓ in this order. Finally, we subject v_1' and v_K' to the same rough perturbation as the critical vertices between them, and move them vertically upward.

We place a disk of radius 1/30 around every perturbed point on this edge, including the two surrogate positions, see Figure 7b. In the next step, to be described in Section 4.2, we find a strictly convex chain which selects one vertex out of each little disk, as shown in Figure 7c.

This will make all angles at $v_2, \dots, v_{K-1}$ strictly convex. Finally, we use these perturbed positions for our critical vertices, but for v_1 and v_K, we ignore their perturbed surrogate positions, see Figure 7d. The true position of v_1 or v_K may be determined by a different face in which it forms a critical angle (as is the case for v_5 in the example), or it might just keep its original position (like v_1 in the example). We only have to check that the angle at the left-most and right-most critical vertex (v_2 and v_4 in this case) remains convex:

Lemma 2. *Replacing the perturbed surrogate position v_1' and v_K' of the points v_1 and v_K by their true positions does not destroy convexity at their neighbors v_2 and v_{K-1} in F.*

Proof. We first show that the rough perturbation does not actually perturb v_1 and v_K to their surrogate positions v_1' or v_K'. It is conceivable that, say, v_1 lies on ℓ and is perturbed upwards because of its critical angle in a different face F', see Figure 8. However, this would contradict the Three Wedges Property for v_1 and F, creating two incident edges in a sector in which only a unique incident edge can exist.

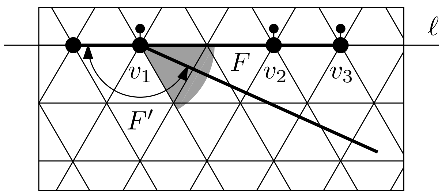


Figure 8: A neighbor of a critical vertex cannot be perturbed in the same direction.

Thus we conclude that v_1 and v_K lie below or on ℓ, and they are either perturbed not at all or in a direction below ℓ.
Vertices v_2 and v_4 in the example of Figure 7 represent the possible extreme cases that have to be considered. v_5 represents a vertex that is pushed downward in the rough perturbation, and then subjected to a fine perturbation anywhere in its little circle. For visual clarity, the circles in Figure 7 have been drawn with a much larger radius than 1/30. Since the circles are actually small enough, the angle at v_4 will be convex no matter where the point v_5 is placed in its own circle. (This position is determined when the critical face of v_5 is considered.) A similar statement holds at v_2, where the perturbed surrogate position of v_1 in Figure 7c is replaced by the *original* position of v_1; this will always turn the edge v_2v_1 counterclockwise and thus preserve convexity at v_2.
The argument works also for a chain of vertices on an exterior edge of the enclosing triangle. In this case, $v_2, v_3, \ldots, v_{K-1}$ are perturbed around their original position on ℓ, whereas the neighbors v_1 and v_K are moved inside the triangle and below ℓ. Geometrically, the situation looks similar as for vertex v_1 in Figure 7, except that v_1 is not pushed down straight but at a $-30°$ angle. This movement is large enough to ensure convexity at v_2. □

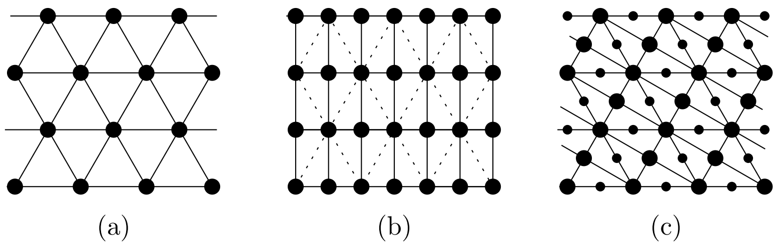


Figure 9: The hexagonal grid (a) is contained in a rectangular grid (b). A hexagonal grid twice refined (c) contains rectangular grids in three different directions. One of these rectangular grids is highlighted by thicker points.

4.2 Convex Chains in the Grid

We have a number K of vertices $0 = a_1 < a_2 < \cdots < a_K \leq 2n - 1$ on a horizontal line which form part of an array of $2n$ consecutive grid points. We want to perturb them into convex position. If the faces of the embedding have at most k sides, then $K \leq k$. It is more convenient to work with a rectangular grid. So we extend the hexagonal grid to a rectangular grid as shown in Figure 9. This grid will be refined sufficiently in order to allow a strictly convex chain to be drawn inside a sequence of circles. Figure 10 gives a schematic picture of the situation. (This drawing is not to scale.) It is more convenient to discuss the construction of an *upward* convex chain. Inside each disk (of radius 1/30) we fit a square of side length 1/50, which is subdivided into a subgrid of width w and height h. More precisely, we are looking for a sequence of points $p_i = (x_i, y_i)$ in these circles, whose coordinates measure the distance from the lower left corner of the first circle in units of little grid cells. Two successive circle centers at distance 1 in terms of the original grid have a distance of $S := 50w$ when measured in subgrid units. Thus we are looking for integer coordinates that satisfy $a_i \cdot S \leq x_i \leq a_i \cdot S + w$ and $0 \leq y_i \leq h$. Eventually, when the whole subgrid is scaled to the standard grid $\mathbb{Z} \times \mathbb{Z}$, x_i and y_i will become true distances again. The total size of the resulting integer grid will be $O(nw) \times O(nh)$.

The convex chain $p_1, p_2, \ldots, p_K$ has a descending part up to a point with minimum y-coordinate and an ascending part. We choose the two points with minimum y-coordinate to lie in the middle: We define $M := \lfloor K/2 \rfloor + 1$ and set $y_{M-1} = y_M = 0$. We will only describe the construction of the ascending chain from p_M to the right. The left half is constructed symmetrically.

The direction between two grid points is uniquely specified by a *primitive vector*, a vector whose components are relatively prime. We now take a sequence of primitive vectors $q_1, q_2, \ldots, q_{K-M}$, $q_i = (u_i, v_i)$ with $0 < u_i \leq w$ and $v_i > 0$, in order of increasing slope v_i/u_i. Then we choose the difference vectors Δp as appropriate multiples of these vectors, in the following way. We have already

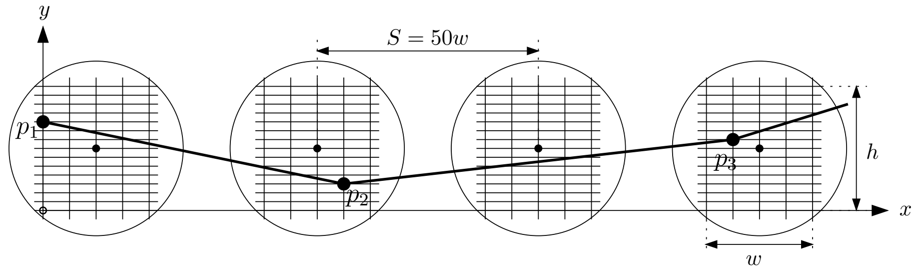


Figure 10: A convex chain formed by grid points in the circles. (Again, the radius of the circles is drawn much too large compared to their distance.)

defined $y_M := 0$, and we choose x_M arbitrarily within the permitted range of x-coordinates. Having defined p_{M+i-1}, we define

$$p_{M+i} := p_{M+i-1} + s \cdot q_i$$

by adding as many copies of q_i as are necessary to bring x_{M+i} into the desired box:

$$a_{M+i} \cdot S \le x_{M+i} \le a_{M+i} \cdot S + w$$

Since this box has width w, and $u_i \le w$, this is always possible.
We need $K - M \le K/2$ primitive vectors q_i (including the vector $(1,0)$ from p_{M-1} to p_M.) The following theorem ensures that we can find these vectors in a triangle of sufficiently large area.

Theorem 2. *The right triangle $T = (0,0),(w,0),(w,t)$, where $w \ge 1$, w integer, and $t \ge 2$, contains at least $wt/4$ primitive vectors.*

The general proof is given in Section 5. We can however easily give an explicit solution for the special case $t = 2$ (corresponding to the choice $w = k$ below, which leads to the most balanced grid dimensions): In this case, we can simply take the $1 + \lfloor w/2 \rfloor$ vectors $(w,1)$, $(w-1,1)$, …, $(\lceil w/2 \rceil, 1)$.
We use Theorem 2 as follows. We choose an arbitrary width $w \le k$ for the boxes. By Theorem 2, we can set $t := \max\{2, 2K/w\}$ to ensure that we find at least $K/2$ primitive vectors in the triangle T. The slope of these vectors is bounded by t/w. Let us estimate the necessary height h of the boxes. The last point p_K is connected to p_M by a chain of vectors with slope at most t/w. The distance of x-coordinates is at most the width of the whole grid on which the graph is embedded, i. e., at most $S \cdot 2n = O(wn)$; hence the difference in y-coordinates is at most $t/w \cdot O(wn) = O(tn) = O(kn/w)$. It follows that the height h of the boxes is $O(kn/w)$. The total height of the resulting grid is $O(hn) = O(kn^2/w)$.
This leads to part (i) of Theorem 1. Part (ii) is an easy corollary. As an extreme case, we can set $w = 1$ and perform only vertical perturbations. We get $h \le 2kn$ (without any additional constants depending on S).

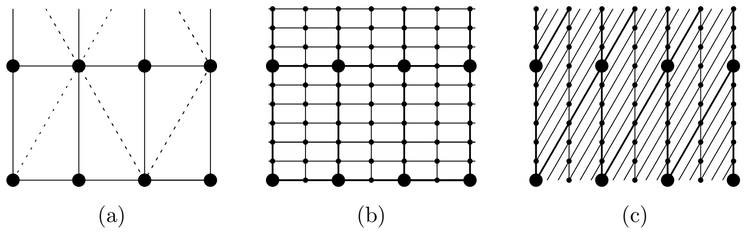


Figure 11: A rectangular grid (a), its 2×6 refinement (b), and a shearing (c) of the refined grid. Its grid-points coincide with the untransformed grid.

4.3 Perturbation of Vertices on Diagonal Lines

So far, we have treated only a sequence of vertices on a horizontal straight line. The same scheme can be applied to lines of the two other directions by applying the shearing transformation $\binom{x}{y} \mapsto \binom{x}{y+\sqrt{3}/2\cdot x}$ or $\binom{x}{y} \mapsto \binom{x}{y-\sqrt{3}/2\cdot x}$ which moves points only in vertical direction. If h is a multiple of w, the transformation will produce a grid like in Figure 11c which is contained in the original grid of Figure 11b. For the range of parameters which is interesting for the theorem ($w \le k$), the height h of the subgrid is never smaller than the width w; thus, the choice of h as a multiple of w does not change the asymptotic analysis. One needs to reduce the size of the little square subgrid to ensure that the sheared square still fits inside the circle, and one has to adjust the quantity S accordingly. In addition, we have to select h and w as multiples of 14, to accommodate the grid of the rough perturbation and the refined rectangular grid of Figure 9b. All of this changes the analysis only by a constant factor.

For the case of a uniform stretching of both dimensions ($w = h$), one referee has pointed out a simpler alternative method. After a blow-up by a factor of two, the original triangular grid contains rectangular grids in all three grid directions, Figure 9c. Two further refinements by the factor 7 (for the rough perturbation) and then by the factor w are sufficient to accommodate the fine perturbation. On the exterior edges, the points must of course be perturbed to form an *outward* convex chain.

For part (iii) of the theorem we have already mentioned that interior faces with $k \le 4$ sides are already strictly convex. If the outer face has 4 edges, it contains a single vertex on one of the sides of the outer triangle. The rough perturbation is thus sufficient to make the outer face strictly convex.

The whole procedure, as described above, is quite explicit and can be carried out with a linear number of arithmetic operations. We calculate the $O(k)$ primitive vectors q_i only once and store them in an array. Then, for every actual sequence of vertices on an edge, we can construct the perturbation very easily. The primitive vectors in the triangle $(0,0)$, $(w,0)$, (w,t) according to Theorem 2 can be selected from the $O(wt) = O(k)$ grid points in linear time with a sieve method.

	optimal		greedy	
$w = h$	n	$(w+1)/n$	n	$(w+1)/n$
0	2	0.5000	2	0.5000
1	4	0.5000	4	0.5000
2	6	0.5000	6	0.5000
4	10	0.5000	8	0.6250
6	14	0.5000	12	0.5833
8	16	0.5625	14	0.6429
10	20	0.5500	18	0.6111
12	22	0.5909	18	0.7222
20	32	0.6562	28	0.7500
40	58	0.7069	48	0.8542
100	122	0.8279	96	1.0521
200	212	0.9481	164	1.2256
400	366	1.0956	276	1.4529
1,000	758	1.3206	562	1.7811
2,000	1,292	1.5488	948	2.1108
4,000	2,206	1.8137	1,610	2.4851
10,000	4,468	2.2384	3,230	3.0963
20,000	7,592	2.6345	5,472	3.6552
40,000			9,250	4.3244
100,000			18,484	5.4101
200,000			31,192	6.4119
400,000			52,626	7.6008
1,000,000			105,012	9.5227
2,000,000			177,046	11.2965
4,000,000			299,494	13.3559

Table 1: The length of the longest strictly convex n-gon in a sequence of square cells of size $w \times w$, regularly spaced at distance $S = 50w$.

4.4 Numerical Experiments

We have presented a general systematic solution for finding a convex chain by selecting grid-points from a sequence of boxes. One can find the *optimal* (i.e., longest) convex chain in polynomial time by dynamic programming, as described in more detail below. Results of some experiments are shown in the first column of Table 1. We restrict ourselves to the standard situation of selecting an n-gon from n adjacent boxes ($K = n$) which are squares ($w = h$). For several different sizes w, we computed the largest n such that a strictly convex n-gon can be found in a sequence of cells of size $w \times w$. The factor $(w+1)/n$ determines the necessary grid size w in terms of n. (By the convention of Figure 10, a "$w \times w$" grid consists of $(w+1)^2$ vertices; thus we give the fraction $(w+1)/n$ instead of w/n.) Since the convex chain consists of a monotone decreasing and a monotone increasing part, connected by a horizontal segment in the middle, the necessary height $w+1$ is at least $0.5\,n$. We see that this trivial lower bound is achieved for small values of n. The factor $(w+1)/n$ increases with n, but not very fast. (The rectangular $w \times h$ boxes constructed in the proof of Theorem 1 would have $w/n = 1$, but $h/n = 100$.)

The dynamic programming algorithm computes, for each point p in the $w \times h$ box, and for each possible previous point p' in the adjacent box to the left, the longest ascending and strictly convex chain (of length i) for which $p_{i-1} = p'$ and $p_i = p$. Knowing p' and p, it can be determined which points in the next box are candidate endpoints p_{i+1} of a chain of length $i+1$. One can argue that, among these points p_{i+1} that are reachable as a continuation of $p'p$, only the $w+1$ lowest points on each vertical line are candidates for endpoints p_{i+1} that form part of an optimal chain. Theoretically, the complexity of this algorithm is therefore $O(w^3h^2)$. It turns out that, with few exceptions, every point p has only one predecessor point p' that must be considered: all other predecessor points p_{i-1} have either a larger slope of the vector $p - p_{i-1}$ or they are reached by a shorter chain. Therefore, the algorithm runs in $O(w^2h) = O(wkn)$ time, in practice.

A simple greedy approach for selecting the points p_i one by one gives already a very good solution: we choose p_{i+1} from the possible grid points in the appropriate box in such a way that the segment $p_{i+1} - p_i$ has the slope as small as possible while still forming a convex angle at p_i. The results in the right column of Table 1 indicate that this algorithm is quite competitive with the optimum solution. The running time is $O(kw)$.

5 Grid Points in a Triangle

In this section we prove Theorem 2. We denote by $\mathbb{P} := \{\, (x,y) \mid \gcd(x,y) = 1 \,\}$ the set of primitive vectors in the plane.

It is known that the proportion of primitive vectors among the integer vectors in some large enough area is approximately $1/\zeta(2) = 6/\pi^2$ [10, Chapters 16–18]. Thus, a "large" triangle T should contain roughly $3/\pi^2 \cdot wt \approx 0.304wt$ primitive points. However, for very wide or very high triangles, the fraction of primitive vectors may be different. In fact, for $t = 2$, the bound $wt/4$ is tight except for an additive slack of at most 2.

We will use special methods for counting primitive vectors when T is "very high" (i. e., w is fixed and below some threshold and t is unbounded, Section 5.1), when T is "very wide" (t is fixed and w is unbounded, Section 5.2), and for the case when both t and w are large (Section 5.3). We use the help of the computer for the first two cases, but we use a general bound for the last case.

5.1 Fixed width, unbounded height

For a fixed value of w, the function $f(t) := |T \cap \mathbb{P}|$ can be analyzed explicitly. It is periodically ascending:

$$f(t+w) = f(t) + C,$$

where $C = \sum_{i=1}^{w} \phi(i)$ is the number of primitive vectors in the triangle $(0,0)$, $(w,0)$, (w,w), excluding the point $(1,1)$. Euler's totient function $\phi(i)$ denotes the number of integers $1 \le j \le i$ that are relatively prime to i, or equivalently, the number of primitive vectors (i,j) on the vertical line segment from $(i,0)$ to $(i,i-1)$.

The reason for the periodic behavior is that the unimodular shearing transformation $(x,y) \mapsto (x, y+x)$ maps the triangle $(0,0)$, $(w,0)$, (w,t), to the triangle $(0,0)$, (w,w), $(w,w+t)$, which is equal to $(0,0)$, $(w,0)$, $(w,w+t)$ minus the triangle $(0,0)$, $(w,0)$, (w,w).

Therefore, it is sufficient to check that the "average slope" C/w of f is bigger than $w/4$, and to check

$$f(t) \ge tw/4 \tag{1}$$

for the initial interval $2 \le t \le 2 + w$. This can be done by computer: We sort all primitive vectors (x,y) with $0 \le x \le w$ and $0 \le y/x \le (w+2)/w$ by their slope y/x. We gradually increase t from 2 to $w+2$. The critical values of t for which (1) must be checked explicitly are when a new primitive vector is just about to enter the triangle.

We ran a lengthy computer check to establish (1) for $w = 1, 2, \dots, 250$ and for $2 \le t \le w+2$ (and hence for all t). In addition, we checked it for the range $w = 251, 252, \dots, 800$ and for $2 \le t \le 250$.

5.2 Large width

In this section we prove Theorem 2 for small t and large w. T intersects each horizontal line $y = i$ in a segment of length $w - (w/t)i$. In any set of i consecutive grid points on this line, there are precisely $\phi(i)$ primitive vectors. We can subdivide the grid points on $y = i$ into $\lfloor (w-(w/t)i)/i \rfloor \ge w/i - w/t - 1$ groups of i consecutive points, leading to a total of at least $(w/i - w/t - 1)\phi(i)$ primitive vectors:

$$|T \cap \mathbb{P}| \ge 1 + \sum_{i=1}^{\lfloor t \rfloor} \left(\frac{w}{i} - \frac{w}{t} - 1 \right) \phi(i)$$

For a given value of $\lfloor t \rfloor$, one can evaluate the expression

$$|T \cap \mathbb{P}| \ge 1 + \sum_{i=1}^{\lfloor t \rfloor} \Big(\frac{w}{i} - \frac{w}{t} - 1 \Big) \phi(i) \ge 1 + \sum_{i=1}^{\lfloor t \rfloor} \Big(\frac{w}{i} - \frac{w}{\lfloor t \rfloor} - 1 \Big) \phi(i) \tag{2}$$

explicitly. The right-hand side of this bound is a linear function $g(w)$:

$$g(w) = \sum_{i=1}^{\lfloor t\rfloor}\Big(\frac{w}{i} - \frac{w}{\lfloor t\rfloor} - 1\Big)\phi(i)$$

For example, for $\lfloor t\rfloor = 130$, we have $g(w) = w\cdot 39.514\ldots - 5153$. It follows that $g(w) > w\cdot 131/4 > wt/4$ for $w \geq 762$. Performing this calculation by computer for $\lfloor t\rfloor = 6, 7, \ldots, 130$ establishes Theorem 2 for $6 \leq t \leq 130$ and $w \geq 800$. The interval $4 \leq t < 6$ can be split into the ranges $4 \leq t < 4.5$, $4.5 \leq t < 5$, $5 \leq t < 5.5$, and $5.5 \leq t < 6$. For each range, we can use the above method with a tighter bound in (2) than $t \geq \lfloor t\rfloor$, and the estimate goes through in the same way.

So let us consider the remaining interval $2 \leq t \leq 4$: For $2 \leq t < 3$, we can evaluate $|T \cap \mathbb{P}|$ explicitly:

$$|T \cap \mathbb{P}| = 1 + (w + 1 - \lceil \tfrac{w}{t}\rceil) + (\lceil \tfrac{w}{2}\rceil - \lceil \tfrac{w}{t} - \tfrac{1}{2}\rceil), \tag{3}$$

counting the primitive vectors on the lines $y = 0$, $y = 1$, and $y = 2$, respectively. For $t \geq 3$, the right-hand side of (3) is still valid as a lower bound. We get

$$|T \cap \mathbb{P}| \geq 1 + \big(w + 1 - (\tfrac{w}{t} + 1)\big) + \big(\tfrac{w}{2} - (\tfrac{w}{t} - \tfrac{1}{2} + 1)\big) > w(\tfrac{3}{2} - \tfrac{2}{t})$$

The last expression is $\geq wt/4$ for $2 \leq t \leq 4$.

Thus we have proved the theorem for $2 \leq t \leq 130$ and $w \geq 800$.

5.3 Large triangles

LEMMA 3. *Let T' be an axis-aligned right triangle of width a' and height b', whose right angle lies on a grid point. Then*

$$\operatorname{area} T' \leq |T' \cap \mathbb{Z}^2| \leq \operatorname{area} T' + \lfloor a'\rfloor + \lfloor b'\rfloor + 1$$

Proof. This is simple. Suppose the right angle is at the right bottom corner of T', see Figure 12a. Each lattice point in T' is the right bottom vertex of a unit square and these squares cover T'. To bound the area from below, we must subtract the squares which are not contained in T'. These squares form a monotone chain along the longest side of T', and their number is $\lfloor a'\rfloor + \lfloor b'\rfloor + 1$. □

LEMMA 4. *Let T be the right triangle $(0,0)$, $(a,0)$, (a,b), with $a, b \geq 1$. Define T^* as $T \cap \{\,(x,y) : y \geq 1\,\}$. Then*

$$\frac{ab}{2} - a - b + \frac{a}{2b} \leq |T^* \cap \mathbb{Z}^2| \leq \frac{ab}{2} + b - \frac{a}{2b} \tag{4}$$

In particular,

$$\left| |T^* \cap \mathbb{Z}^2| - \frac{ab}{2} \right| \leq a + b$$

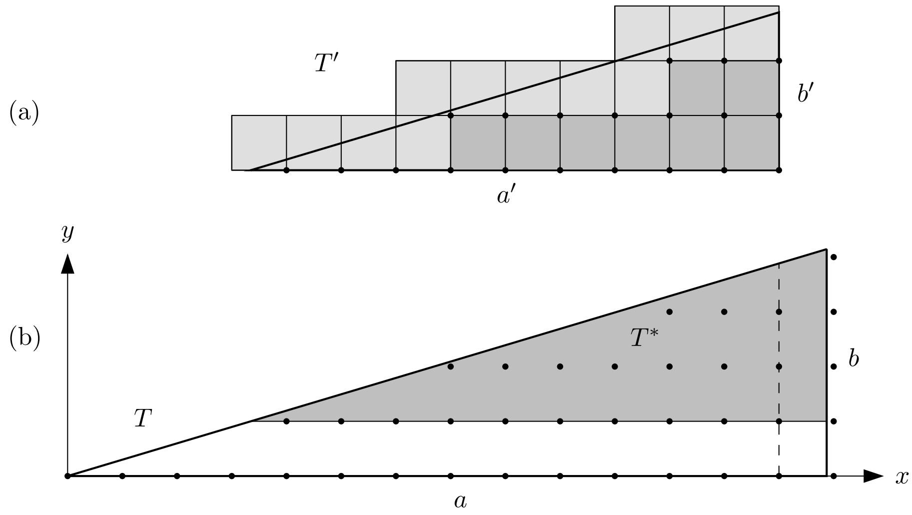


Figure 12: (a) The triangle T' in Lemma 3 and its covering by squares. (b) The triangles T and T^* (shaded) in Lemma 4.

Proof. See Figure 12b. The triangle T^* has length $a - a/b$, height $b-1$ and area $\frac{1}{2}(b-1)(a-a/b) = ab/2 - a + a/(2b)$. Let T' denote the part of T^* that lies left of the line $x = \lfloor a \rfloor$. This triangle contains the same grid points as T^*. We assume first that T' is a nonempty triangle. The difference in areas lies in a rectangle strip of width < 1 and height $b-1$:

$$\operatorname{area} T^* - (b-1) \le \operatorname{area} T' \le \operatorname{area} T^*$$

We can apply Lemma 3 to T' and obtain

$$|T^* \cap \mathbb{Z}^2| = |T' \cap \mathbb{Z}^2| \le \left(\frac{ab}{2} - a + \frac{a}{2b}\right) + \left(a - \frac{a}{b}\right) + (b-1) + 1,$$
$$|T^* \cap \mathbb{Z}^2| = |T' \cap \mathbb{Z}^2| \ge \operatorname{area} T' \ge \left(\frac{ab}{2} - a + \frac{a}{2b}\right) - (b-1),$$

from which the lemma follows.

The triangle T' may not exist, as in Figure 13. In this case, $T^* \cap \mathbb{Z}^2 = \emptyset$. Instead of arguing why the above derivation is valid also for this case, we establish the inequalities directly. Let $b' \ge b - b/a$ denote the vertical extent of T at $x = \lfloor a \rfloor$. Then the fact that T' is empty is equivalent to $b' < 1$.

Then, from $1 \ge b' \ge b - b/a$ we conclude that $ab < a + b$. It follows that the lower bound in (4) is at most 0:

$$\frac{ab}{2} + \frac{a}{2b} - a - b \le \frac{a+b}{2} + \frac{a}{2} - a - b \le 0$$

The claimed upper bound in (4) is always nonnegative, by the assumption $b \ge 1$. $\square$

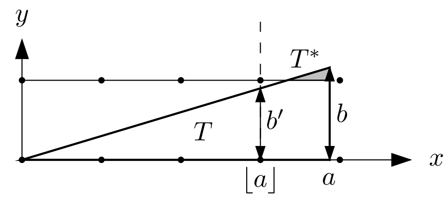


Figure 13: If T^* (shaded) contains no grid points, the triangle T' does not exist.

The number of primitive vectors can be estimated by an inclusion-exclusion formula, taking into account vectors which are multiples of single primes $2, 3, 5, 7, \ldots$, vectors which are jointly multiples of two primes, of three primes, and so on, see [10, Chapters 16–18]:

$$|T \cap \mathbb{P}| = 1 + |T^* \cap \mathbb{P}| = 1 + \sum_{i=1}^{S} \mu(i) \cdot \left|(\tfrac{1}{i} \cdot T^*) \cap \mathbb{Z}^2\right| = 1 + \sum_{i=1}^{S} \mu(i) \cdot \left|(\tfrac{1}{i}T)^* \cap \mathbb{Z}^2\right| \tag{5}$$

Here, $\mu(i)$ is the Möbius function: $\mu(i) = (-1)^k$ if i is the product of k distinct primes and $\mu(i) = 0$ otherwise. It is known that $\sum_{i=1}^{\infty} \frac{\mu(i)}{i^2} = 1/\zeta(2) = 6/\pi^2$, leading to the fact mentioned above that a fraction of approximately $6/\pi^2$ of the grid points in a large area are primitive vectors.
Our sum in (5) goes to $i = \infty$, but for $i > w$ or $i > t$, the set $(\frac{1}{i}T)^* \cap \mathbb{Z}^2$ is empty. Therefore, the formula is valid for $S := \min\{w, \lfloor t \rfloor\}$. We apply Lemma 4 and obtain

$$\begin{aligned} |T \cap \mathbb{P}| = 1 + \sum_{i=1}^{S} \mu(i) \cdot \left|(\tfrac{1}{i}T)^* \cap \mathbb{Z}^2\right| &\ge \frac{wt}{2} \sum_{i=1}^{S} \frac{\mu(i)}{i^2} - \sum_{i=1}^{S} \frac{w+t}{i} \\ &\ge \frac{wt}{2} \left(\frac{6}{\pi^2} - \frac{1}{S} \right) - H_S(w+t), \end{aligned}$$

where $H_S = 1{+}1/2{+}1/3{+}\cdots{+}1/S$ is the harmonic number. The last inequality comes from bounding the remainder $\sum_{i=S+1}^{\infty} \mu(i)/i^2 \le \sum_{i=S+1}^{\infty} 1/i^2 < 1/S$ of the infinite series, whose value is $6/\pi^2$.
We distinguish the two cases for S: Case 1: $w \le t$, and $S = w$. Then

$$|T \cap \mathbb{P}| \ge \frac{wt}{2} \left(\frac{6}{\pi^2} - \frac{1}{w} \right) - H_w(2t) = wt \left(\frac{3}{\pi^2} - \frac{1}{2w} - \frac{2H_w}{w} \right)$$

Case 2: $w \ge t$, and $S = \lfloor t \rfloor$.

$$\begin{aligned} |T \cap \mathbb{P}| &\ge \frac{wt}{2} \left(\frac{6}{\pi^2} - \frac{1}{\lfloor t \rfloor} \right) - H_{\lfloor t \rfloor}(w+t) \\ &\ge wt \left(\frac{3}{\pi^2} - \frac{1}{2(t-1)} - H_{\lfloor t \rfloor} \left(\frac{1}{t} + \frac{1}{w} \right) \right) \end{aligned} \tag{6}$$

Combining the two cases and setting $n := \min\{w,t\}$ gives

$$|T \cap \mathbb{P}| \geq wt\left(\frac{3}{\pi^2} - \frac{1}{2(n-1)} - \frac{2H_{\lfloor n \rfloor}}{n}\right)$$

Using the estimate $H_i \leq \gamma + \ln(i+1)$ with Euler's constant $\gamma \approx 0.57721$, it can be checked that this factor is bigger than $1/4$ for $n \geq 250$, thus proving the theorem for $w, t \geq 250$.
On the other hand, the factor in (6) is bigger than $1/4$ for $w \geq 800$ and $130 \leq t \leq 250$, proving the theorem also for this range.

Wrap-up. The proof of Theorem 2 is now complete. On a high level, we distinguish three ranges for w: $1 \leq w \leq 250$, $251 \leq w \leq 800$, and $w \geq 800$.

- Range 1: For $1 \leq w \leq 250$, the theorem has been established in Section 5.1.
- Range 2: $251 \leq w \leq 800$. For $251 \leq w \leq 800$ and $1 \leq t \leq 250$, the theorem has been established in Section 5.1 as well. For $251 \leq w \leq 800$ and $t \geq 250$, it has been proved in Section 5.3.
- Range 3: Finally, for $w \geq 800$, there is a division into three cases: Section 5.2 takes care of the range $2 \leq t \leq 130$. Section 5.3 proves the bound separately for the ranges $130 \leq t < 250$ and $t \geq 250$. □

6 Conclusion

In practice, the algorithm behaves much better than indicated by the rough worst-case bounds that we have proved. We have not attempted to optimize the constants in the proof. For example, if we don't take a 7×7 subgrid but an 11×11 subgrid, and with a more specialized treatment of the outer face, the permissible amount of perturbation in Lemma 1 increases from $1/30$ to $1/9$, but it would make the pictures of the rough perturbation harder to draw.
Bonichon, Felsner, and Mosbah [4] have used a technique of eliminating edges from the drawing that can later be inserted in order to reduce the necessary grid size for (non-strictly) convex drawings. This technique can also be applied in our case: remove interior edges as long as the graph remains three-connected. These edges can be easily reinserted in the end, after all faces are strictly convex. (For non-strictly convex drawings in [4], the selection of removable edges and their reinsertion is actually a more complicated issue.) This technique might be useful in practice for reducing the grid size.

Lower Bounds. The only known lower bound comes from the fact that a single convex n-gon on the integer grid needs $\Omega(n^3)$ area, see Bárány and Tokushige [3], or Acketa and Žunić [1, 2] for the easier case of a *square* grid. To achieve this area for an n-gon, one has to draw it in a quite round shape.

In contrast, the faces that are produced in our algorithm have a very restricted shape: when viewed from a distance, the look like the triangles, quadrilaterals, pentagons, or hexagons of the $n \times n$ grid drawing from which they were derived. To reduce the area requirement below $O(n^4)$ one has to come up with a new approach that also produces faces with a "rounder" shape.
Our bounds are however, optimal within the restricted class of algorithms that start with a Schnyder drawing or an arbitrary non-strictly convex drawing on an $O(n) \times O(n)$ grid and try to make it strictly convex by *local perturbations* only. Consider the case where $n-1$ vertices lie on the outer face, connected to a central vertex in the middle. The Schnyder drawing will place these vertices on the enclosing triangle, and at least $n/3$ vertices will lie on a common line. They have to be perturbed into convex position, as in Figures 7 or 10.
Let us focus on the standard situation when we want to perturb n equidistant vertices on a line, at distance 1 from each other. The $n-1$ edge vectors $p_{i+1}-p_i$ lie in a $2w \times 2h$ box; they must be non-parallel, and in particular, they must be *distinct*. If Δy is the average absolute vertical increment of these vectors, it follows that $\Delta y = \Omega(n/w)$, and the total necessary height h of the boxes is $\Omega(n(\Delta y)) = \Omega(n^2/w)$. Therefore, the total necessary area is $\Omega(hwn^2) = \Omega(n^4)$. The argument can be extended to the case when only $\Omega(n)$ selected grid vertices on a line of length $O(n)$ have to be perturbed. It can also be shown that our bounds in terms of k are optimal in this setting. The worst case occurs when there is a line of length n with $\Omega(k)$ consecutive grid points in the middle and two vertices at the extremes.

Extensions. The class of three-connected graphs is not the most general class of graphs which allow strictly convex embeddings. The simplest example of this is a single cycle. A planar graph, with a specified face cycle C as the outer boundary, has a strictly convex embedding if and only if it is three-connected to the boundary, i. e., if every interior vertex (not on C) has three vertex-disjoint paths to the boundary cycle. Equivalently, the graph becomes three-connected after adding a new vertex and connecting it to every vertex of C. These graphs cannot be treated directly by our approach, since the Schnyder embedding method of Felsner [8] does not apply. Partitioning the graph into three-connected components and putting them together at the end might work.

Acknowledgements. We thank the referees for helpful remarks which have lead to many clarifications in the presentation. Imre Bárány was partially supported by Hungarian National Science Foundation Grants No. T 037846 and T 046246.

References

[1] Dragan M. Acketa and Jovisa D. Žunić, *On the maximal number of edges of convex digital polygons included into a square grid*, počítače a umelá

inteligencia 1 (1982), no. 6, 549–558.

[2] ———, *On the maximal number of edges of convex digital polygons included into an $m \times m$-grid*, J. Comb. Theory, Ser. A 69 (1995), 358–368.

[3] Imre Bárány and Norihide Tokushige, *The minimum area of convex lattice n-gons*, Combinatorica 24 (2004), no. 2, 171–185.

[4] Nicolas Bonichon, Stefan Felsner, and Mohamed Mosbah, *Convex drawings of 3-connected plane graphs*, Graph Drawing: Proc. 12th International Symposium on Graph Drawing (GD 2004), September 29–October 2, 2004 (New York), János Pach, ed. Lecture Notes in Computer Science, vol. 3383, Springer-Verlag, 2005, pp. 60–70.

[5] M. Chrobak and G. Kant, *Convex grid drawings of 3-connected planar graphs*, Internat. J. Comput. Geom. Appl. 7 (1997), no. 3, 211–223.

[6] Marek Chrobak, Michael T. Goodrich, and Roberto Tamassia, *Convex drawings of graphs in two and three dimensions*, Proc. 12th Ann. Sympos. Comput. Geom., 1996, pp. 319–328.

[7] H. de Fraysseix, J. Pach, and R. Pollack, *How to draw a planar graph on a grid*, Combinatorica 10 (1990), no. 1, 41–51.

[8] Stefan Felsner, *Convex drawings of planar graphs and the order dimension of 3-polytopes*, Order 18 (2001), 19–37.

[9] ———, *Geodesic embeddings and planar graphs*, Order 20 (2003), 135–150.

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, 1979.

[11] Jürgen Richter-Gebert, *Realization Spaces of Polytopes*, Lecture Notes in Mathematics, vol. 1643, Springer-Verlag, 1997.

[12] Günter Rote, *Strictly convex drawings of planar graphs*, Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), Vancouver, 2005, pp. 728–734.

[13] W. Schnyder, *Embedding planar graphs on the grid*, Proc. 1st ACM-SIAM Sympos. Discrete Algorithms, 1990, pp. 138–148.

[14] W. Schnyder and W. T. Trotter, *Convex embeddings of 3-connected plane graphs*, Abstracts of the AMS 13 (1992), no. 5, 502.

[15] W. T. Tutte, *Convex representations of graphs*, Proceedings London Mathematical Society 10 (1960), no. 38, 304–320.

[16] ———, *How to draw a graph*, Proceedings London Mathematical Society 13 (1963), no. 52, 743–768.

Imre Bárány
Rényi Institute
Hungarian Academy of Sciences
PoB 127
Budapest 1364, Hungary
barany@renyi.hu
and
Department of Mathematics
University College London
Gower Street
London WC1E 6BT, UK

Günter Rote
Freie Universität Berlin
Institut für Informatik
Takustraße 9
D-14195 Berlin, Germany
rote@inf.fu-berlin.de

On Packing Spheres into Containers

About Kepler's Finite Sphere Packing Problem

Achill Schürmann

Received: June 3, 2005
Revised: July 21 2006

Communicated by Günter Ziegler

Abstract. In an Euclidean d-space, the container problem asks to pack n equally sized spheres into a minimal dilate of a fixed container. If the container is a smooth convex body and $d \geq 2$ we show that solutions to the container problem can not have a "simple structure" for large n. By this we in particular find that there exist arbitrary small $r > 0$, such that packings in a smooth, 3-dimensional convex body, with a maximum number of spheres of radius r, are necessarily not hexagonal close packings. This contradicts Kepler's famous statement that the cubic or hexagonal close packing "will be the tightest possible, so that in no other arrangement more spheres could be packed into the same container".

2000 Mathematics Subject Classification: 52C17; 01A45, 05B40
Keywords and Phrases: sphere packing, Kepler, container problem

1 Introduction

How many equally sized spheres can be packed into a given container? In 1611, Kepler discussed this question in his booklet [Kep11] and came to the following conclusion:

> "Coaptatio fiet arctissima, ut nullo praeterea ordine plures globuli in idem vas compingi queant."

> "The (cubic or hexagonal close) packing will be the tightest possible, so that in no other arrangement more spheres could be packed into the same container."

In this note we want to show that Kepler's assertion is false for many containers (see Section 5, Corollary 2). Even more general we show, roughly speaking, that the set of solutions to the finite container problem (see below) in an Euclidean space of dimension $d \geq 2$ has no "simple structure" (see Definition 1).

To make this precise, we consider the Euclidean d-space $\mathbb{R}^d$ endowed with inner product $\langle \cdot, \cdot \rangle$ and norm $|\cdot|$. Let $B^d = \{\boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| \leq 1\}$ denote the (solid) unit sphere and $S^{d-1} = \{\boldsymbol{x} \in \mathbb{R}^d : |\boldsymbol{x}| = 1\}$ its boundary. Then a discrete set $X \subset \mathbb{R}^d$ is a *packing set* and defines a *sphere packing* $X + \frac{1}{2}B^d = \{\boldsymbol{x} + \frac{1}{2}\boldsymbol{y} : \boldsymbol{x} \in X, \boldsymbol{y} \in B^d\}$, if distinct elements $\boldsymbol{x}$ and $\boldsymbol{x}'$ of X have distance $|\boldsymbol{x} - \boldsymbol{x}'| \geq 1$. The sphere packing is called *finite* if X is of finite cardinality $|X|$. Here we consider finite sphere packings contained in a convex body (*container*) C, that is, a compact, convex subset of $\mathbb{R}^d$ with nonempty interior. The *finite container problem* may be stated as follows.

PROBLEM. *Given $d \geq 2$, $n \in \mathbb{N}$ and a convex body $C \subset \mathbb{R}^d$, determine*

$$\lambda(C, n) = \min\{\lambda > 0 : \lambda C \supset X + \tfrac{1}{2}B^d \text{ a packing, } X \subset \mathbb{R}^d \text{ with } |X| = n\}$$

and packing sets X attaining the minimum.

Many specific instances of this container problem have been considered (see for example [Bez87], [BW04], [Fod99], [Mel97], [NÖ97],[Spe04], [SMC+06]). Independent of the particular choice of the container C, solutions tend to densest infinite packing arrangements for growing n (see Section 5, cf. [CS95]). In dimension 2 these packings are known to be arranged hexagonally. Nevertheless, although close, solutions to the container problem are not hexagonally arranged for all sufficiently large n and various convex disks C, as shown by the author in [Sch02], Theorem 9 (cf. [LG97] for corresponding computer experiments). Here we show that a similar phenomenon is true in arbitrary Euclidean spaces of dimension $d \geq 2$.

We restrict ourselves to *smooth convex bodies* C as containers. That is, we assume the *support function* $h_C(\boldsymbol{u}) = \sup\{\langle \boldsymbol{x}, \boldsymbol{u} \rangle : \boldsymbol{x} \in C\}$ of C is differentiable at all $\boldsymbol{u} \in \mathbb{R}^d \setminus \{\boldsymbol{0}\}$, or equivalently, we require that C has a unique *supporting hyperplane* through each boundary point (see [Sch93], Chapter 1.7).

Our main result shows that families of packing sets with a "simple structure" can not be solutions to the container problem if C is smooth and n sufficiently large. This applies for example to the family of solutions to the *lattice restricted container problem*. In it, we only consider packing sets which are isometric to a subset of some *lattice* (a discrete subgroup of $\mathbb{R}^d$).

THEOREM 1. *Let $d \geq 2$ and $C \subset \mathbb{R}^d$ a smooth convex body. Then there exists an $n_0 \in \mathbb{N}$, depending on C, such that $\lambda(C, n)$ is not attained by any lattice packing set for $n \geq n_0$.*

2 PACKING FAMILIES OF LIMITED COMPLEXITY

The result of Theorem 1 can be extended to a more general class of packing sets.

DEFINITION 1. *A family $\mathcal{F}$ of packing sets in $\mathbb{R}^d$ is of* limited complexity *(an* lc-family*), if*

(i) *there exist isometries $\mathcal{I}_X$, for each $X \in \mathcal{F}$, such that*

$$\{\boldsymbol{x} - \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{I}_X(X) \text{ and } X \in \mathcal{F}\} \tag{1}$$

has only finitely many accumulation points in any bounded region.

(ii) *there exists a $\varrho > 0$, such that for all $\boldsymbol{x} \in X$ with $X \in \mathcal{F}$, every affine subspace spanned by some elements of*

$$\{\boldsymbol{y} \in X : |\boldsymbol{x} - \boldsymbol{y}| = 1\}$$

either contains $\boldsymbol{x}$ or its distance to $\boldsymbol{x}$ is larger than ϱ.

Condition (i) shows that point configurations within an arbitrarily large radius around a point are (up to isometries of X and up to finitely many exceptions) arbitrarily close to one out of finitely many possibilities. Condition (ii) limits the possibilities for points at minimum distance further. Note that the existence of a $\varrho > 0$ in (ii) follows if (1) in (i) is finite within S^{d-1}.

An example of an lc-family in which isometries can be chosen so that (1) is finite in any bounded region, is the family of *hexagonal packing sets*. These are isometric copies of subsets of a *hexagonal lattice*, in which every point in the plane is at minimum distance 1 to six others. For the hexagonal packing sets, condition (ii) is satisfied for all $\varrho < \frac{1}{2}$. More general, isometric copies of subsets of a fixed lattice give finite sets (1) in any bounded region and satisfy (ii) for suitable small $\varrho > 0$. Similar is true for more general families of packing sets, as for example for the *hexagonal close configurations* in dimension 3 (see Section 5).

An example of an lc-family, in which the sets (1) are not necessarily finite in any bounded region, are the solutions to the lattice restricted container problem. As shown at the end of Section 3, condition (ii) in Definition 1 is nevertheless satisfied. Thus we are able to derive Theorem 1 from the following, more general result.

Theorem 2. *Let $d \geq 2$, $C \subset \mathbb{R}^d$ a smooth convex body and $\mathcal{F}$ an lc-family of packing sets in $\mathbb{R}^d$. Then there exists an $n_0 \in \mathbb{N}$, depending on $\mathcal{F}$ and C, such that $\lambda(C, n)$ is not attained by any packing set in $\mathcal{F}$ for $n \geq n_0$.*

Proofs are given in the next section. In Section 4 we briefly mention some possible extensions of Theorem 2. In Section 5 we discuss consequences for the quoted assertion of Kepler, if interpreted as a container problem (see Corollary 2).

3 Proofs

Idea. The proof of Theorem 2 is subdivided into four preparatory steps and corresponding propositions. These technical ingredients are brought together at the end of this section. Given an lc-family $\mathcal{F}$ of packing sets, the idea is the following: We show that packing sets $X \in \mathcal{F}$, with $|X|$ sufficiently large, allow the construction of packing sets X' with $|X'| = |X|$ and with $X' + \frac{1}{2}B^d$ fitting into a smaller dilate of C. Roughly speaking, this is accomplished in two steps. First we show that "rearrangements" of spheres near the boundary of C are possible for sufficiently large n. This allows us to obtain arbitrarily large regions in which spheres have no contact, respectively in which points of X' have distance greater than 1 to all other points (Proposition 2, depending on property (i) of Definition 1). Such an initial modification then allows rearrangements of all spheres (Proposition 3 and 4, depending on property (ii) of Definition 1), so that the resulting packing fits into a smaller dilate of C. For example, consider a hexagonal packing in the plane: It is sufficient to initially rearrange (or remove) two disks in order to subsequently rearrange all other disks, so that no disk is in contact with others afterwards (see Figure 1, cf. [Sch02]).

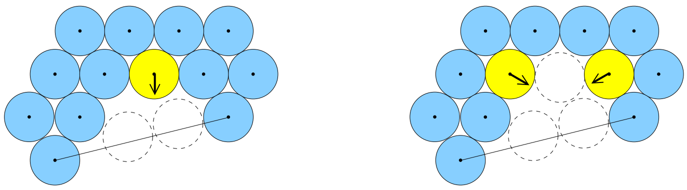


Figure 1: Local rearrangements in a hexagonal circle packing.

How do we know that the new sphere packings $X' + \frac{1}{2}B^d$ fit into a smaller dilate of C? Consider

$$\lambda(C, X) = \min\{\lambda > 0 : \lambda C \supset \boldsymbol{t} + X + \tfrac{1}{2}B^d \text{ for some } \boldsymbol{t} \in \mathbb{R}^d\}$$

for a fixed finite packing set X. Here and in the sequel we use $\boldsymbol{t} + X$ to abbreviate $\{\boldsymbol{t}\} + X$. Clearly

$$\lambda(C, n) = \min\{\lambda(C, X) : \ X \text{ is a packing set with } |X| = n\},$$

and $\lambda(C, X') < \lambda(C, X)$ whenever the *convex hull* $\operatorname{conv} X'$ of X' (and hence X' itself) is contained in the interior $\operatorname{int} \operatorname{conv} X$ of the convex hull of X. Thus in order to prove that X does not attain $\lambda(C, |X|)$ for any convex container C, it is sufficient to describe a way of attaining a packing set X' with $|X'| = |X|$ and

$$X' \subset \operatorname{int} \operatorname{conv} X. \tag{2}$$

I. Let us first consider the "shapes" of packing sets X_n attaining $\lambda(C, n)$. Here and in what follows, X_n denotes a packing set with $|X_n| = n$.
In order to define the "shape", let

$$R(M) = \min\{R \geq 0 : M \subset \boldsymbol{t} + RB^d \text{ for some } \boldsymbol{t} \in \mathbb{R}^d\}$$

denote the circumradius of a compact set $M \subset \mathbb{R}^d$ and let $\boldsymbol{c}(M)$ denote the center of its circumsphere. Hence $M \subseteq \boldsymbol{c}(M) + R(M)B^d$. Then the *shape* of M is defined by

$$\mathcal{S}(M) = (\operatorname{conv}(M) - \boldsymbol{c}(M)) / R(M) \subset B^d.$$

The family of nonempty compact subsets in $\mathbb{R}^d$ can be turned into a metric space, for example with the *Hausdorff metric* (cf. [Sch93]). Shapes of packing sets X_n attaining $\lambda(C,n)$ converge to the shape of C, that is,

$$\lim_{n\to\infty} \mathcal{S}\left(X_n\right) = \mathcal{S}(C). \tag{3}$$

This is seen by "reorganizing elements" in a hypothetical convergent subsequence of $\{X_n\}_{n\in\mathbb{N}}$ not satisfying (3).
The convergence of shapes leads for growing n to shrinking sets of *outer (unit) normals*

$$\{\boldsymbol{v} \in S^{d-1} : \langle \boldsymbol{v}, \boldsymbol{x}\rangle \geq \langle \boldsymbol{v}, \boldsymbol{y}\rangle \text{ for all } \boldsymbol{y} \in \operatorname{conv} X_n\} \tag{4}$$

at boundary points $\boldsymbol{x}$ of the *center polytope* $\operatorname{conv} X_n$. For general terminology and results on convex polytopes used here and in the sequel we refer to [Zie97].
Since C is smooth, the sets of outer normals (4) at boundary points of $\operatorname{conv} X_n$ become uniformly small for large n. Also, within a fixed radius around a boundary point, the boundary of $\operatorname{conv} X_n$ becomes "nearly flat" for growing n.

Proposition 1. *Let $d \geq 2$ and $C \subset \mathbb{R}^d$ a smooth convex body. Let $\{X_n\}$ be a sequence of packing sets in $\mathbb{R}^d$ attaining $\lambda(C,n)$. Then*

(i) for $\varepsilon > 0$ there exists an $n_1 \in \mathbb{N}$, depending on C and ε, such that for all $n \geq n_1$, outer normals $\boldsymbol{v}, \boldsymbol{v}' \in S^{d-1}$ of $\operatorname{conv} X_n$ at $\boldsymbol{x} \in X_n$ satisfy

$$|\boldsymbol{v} - \boldsymbol{v}'| < \varepsilon;$$

(ii) for $\varepsilon > 0$ and $r > 0$ there exists an $n_1 \in \mathbb{N}$, depending on C, ε and r, such that for all $n \geq n_1$, and for $\boldsymbol{x}, \boldsymbol{x}' \in \operatorname{bd}\operatorname{conv} X_n$ with $|\boldsymbol{x} - \boldsymbol{x}'| \leq r$, outer normals $\boldsymbol{v} \in S^{d-1}$ of $\operatorname{conv} X_n$ at $\boldsymbol{x}$ satisfy

$$\langle \boldsymbol{v}, \boldsymbol{x} - \boldsymbol{x}'\rangle > -\varepsilon.$$

II. In what follows we use some additional terminology. Given a packing set X, we say $\boldsymbol{x} \in X$ is in a *free position*, if the set

$$\mathcal{N}_X(\boldsymbol{x}) = \{\boldsymbol{y} \in X : |\boldsymbol{x} - \boldsymbol{y}| = 1\}$$

is empty. If some $\boldsymbol{x} \in X$ is not contained in $\operatorname{int}\operatorname{conv} \mathcal{N}_X(\boldsymbol{x})$, then it is possible to obtain a packing set $X' = X \setminus \{\boldsymbol{x}\} \cup \{\boldsymbol{x}'\}$ in which $\boldsymbol{x}'$ is in a free position. We say $\boldsymbol{x}$ is *moved to a free position* in this case (allowing $\boldsymbol{x}' = \boldsymbol{x}$). We say $\boldsymbol{x}$ is *moved into or within a set M* (to a free position), if $\boldsymbol{x}' \in M$. Note, in the resulting packing set X' less elements may have minimum distance 1 to others, and therefore possibly further elements can be moved to free positions.
Assuming $X \in \mathcal{F}$ attains $\lambda(C, |X|)$ with $|X|$ sufficiently large, the following proposition shows that it is possible to move elements of X into free positions within an arbitrarily large region, without changing the center polytope $\operatorname{conv} X$.

Proposition 2. *Let $d \geq 2$ and $R > 0$. Let $C \subset \mathbb{R}^d$ a smooth convex body and $\mathcal{F}$ a family of packing sets in $\mathbb{R}^d$ satisfying (i) of Definition 1. Then there exists an $n_2 \in \mathbb{N}$, depending on R, $\mathcal{F}$ and C, such that for all $X \in \mathcal{F}$ attaining $\lambda(C, |X|)$ with $|X| \geq n_2$, there exists a $\boldsymbol{t}_X \in \mathbb{R}^d$ with*

(i) $(\boldsymbol{t}_X + RB^d) \subset \operatorname{conv} X$*, and*

(ii) all elements of $X \cap \operatorname{int}(\boldsymbol{t}_X + RB^d)$ can be moved to free positions by subsequently moving elements of $X \cap \operatorname{int} \operatorname{conv} X$ to free positions within $\operatorname{int} \operatorname{conv} X$.

Proof. Preparations. By applying suitable isometries to the packing sets in $\mathcal{F}$ we may assume that

$$\{\boldsymbol{y} : \ \boldsymbol{y} \in X - \boldsymbol{x} \text{ with } |\boldsymbol{y}| < r \text{ for } \boldsymbol{x} \in X \text{ and } X \in \mathcal{F}\} \tag{5}$$

has only finitely many accumulation points for every $r > 1$. For each X, the container C is transformed to possibly different isometric copies. This is not a problem though, since the container is not used aside of Proposition 1, which is independent of the chosen isometries. Note that the smoothness of C is implicitly used here.
We say $\boldsymbol{x} \in X$ is *moved in direction* $\boldsymbol{v} \in S^{d-1}$, if it is replaced by an $\boldsymbol{x}'$ on the ray $\{\boldsymbol{x} + \lambda \boldsymbol{v} : \lambda \in \mathbb{R}_{>0}\}$. Note that it is possible to move $\boldsymbol{x}$ in direction $\boldsymbol{v} \in S^{d-1}$ to a free position, if

$$\mathcal{N}_X(\boldsymbol{x}, \boldsymbol{v}) = \{\boldsymbol{w} \in \mathcal{N}_X(\boldsymbol{x}) - \boldsymbol{x} : \langle \boldsymbol{v}, \boldsymbol{w} \rangle > 0\} \tag{6}$$

is empty. If we want a fixed $\boldsymbol{x} \in X$ to be moved to a free position, in direction $\boldsymbol{v} \in S^{d-1}$ say, we have to move the elements $\boldsymbol{y} \in \boldsymbol{x} + \mathcal{N}_X(\boldsymbol{x}, \boldsymbol{v})$ first. In order to do so, we move the elements of $\boldsymbol{y} + \mathcal{N}_X(\boldsymbol{y}, \boldsymbol{v})$ to free positions, and so on. By this we are lead to the definition of the *access cone*

$$\operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v}) = \operatorname{pos}\{\mathcal{N}_X(\boldsymbol{x}, \boldsymbol{v}) : \boldsymbol{x} \in X \text{ for } X \in \mathcal{F} \text{ with } |X| \geq n\} \tag{7}$$

of $\mathcal{F}$ and n in direction $\boldsymbol{v} \in S^{d-1}$. Here,

$$\operatorname{pos}(M) = \{\sum_{i=1}^{m} \lambda_i \boldsymbol{x}_i : m \in \mathbb{N}, \lambda_i \geq 0 \text{ and } \boldsymbol{x}_i \in M \text{ for } i = 1, \ldots, m\}$$

denotes the *positive hull* of a set $M \subset \mathbb{R}^d$, which is by definition a convex cone. Note that $\operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v})$ is contained in the halfspace $\{\boldsymbol{x} \in \mathbb{R}^d : \langle \boldsymbol{v}, \boldsymbol{x} \rangle \geq 0\}$ and that $\operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v}) \subseteq \operatorname{acc}_{\mathcal{F},n'}(\boldsymbol{v})$ whenever $n \geq n'$.
By the assumption that (5) has only finitely many accumulation points for $r > 1$, there exist only finitely many limits $\lim_{n\to\infty} \left(\operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v}) \cap B^d\right)$. Here, limits are defined using the Hausdorff metric on the set of nonempty compact subsets of $\mathbb{R}^d$ again.
Strategy. We choose a $\boldsymbol{v} \in S^{d-1}$ such that there exists an $\varepsilon > 0$ with

$$\lim_{n\to\infty} \left(\operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v}) \cap B^d\right) = \lim_{n\to\infty} \left(\operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v}') \cap B^d\right),$$

for all $\boldsymbol{v}'$ in the ε*-neighborhood* $S_\varepsilon(\boldsymbol{v}) = S^{d-1} \cap (\boldsymbol{v} + \varepsilon B^d)$ of $\boldsymbol{v} \in S^{d-1}$.
In order to prove the proposition, we show the following for every $X \in \mathcal{F}$, attaining $\lambda(C, |X|)$ with $|X|$ sufficiently large: There exists a $\boldsymbol{t}_X \in \mathbb{R}^d$ such that

(i') $(\boldsymbol{t}_X + RB^d) + \operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v})$ does not intersect $X \cap \operatorname{bd}\operatorname{conv} X$, while

(ii') $(\boldsymbol{t}_X + RB^d) \subset \operatorname{conv} X$.

It follows that $\operatorname{bd}\operatorname{conv} X$ has to intersect the unbounded set

$$(\boldsymbol{t}_X + RB^d) + \operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v}) \tag{8}$$

and by the definition of the access cone it is possible to move the elements in $X \cap \operatorname{int}(\boldsymbol{t}_X + RB^d)$ to free positions as asserted. For example, after choosing a direction $\boldsymbol{v}' \in S_\varepsilon(\boldsymbol{v})$, we may subsequently pick non-free elements $\boldsymbol{x}$ in (8) with maximal $\langle \boldsymbol{x}, \boldsymbol{v}' \rangle$. These elements can be moved to a free position within $\operatorname{int}\operatorname{conv} X$, since $\mathcal{N}_X(\boldsymbol{x}, \boldsymbol{v}')$ is empty by the definition of the access cone.

Bounding the boundary intersection. We first estimate the size of the intersection of (8) with $\operatorname{bd}\operatorname{conv} X$. For $\boldsymbol{v}' \in S_\varepsilon(\boldsymbol{v})$ and $n \in \mathbb{N}$, we consider the sets

$$M(\boldsymbol{v}', n) = \{\boldsymbol{x} \in RB^d + \operatorname{acc}_{\mathcal{F},n}(\boldsymbol{v}) : \langle \boldsymbol{x}, \boldsymbol{v}' \rangle = R\}.$$

By the definition of the access cones (7), $M(\boldsymbol{v}', n) \subseteq M(\boldsymbol{v}', n')$ for $n \geq n'$. We choose

$$r > \sup\{|\boldsymbol{x} - \boldsymbol{y}| : \boldsymbol{x}, \boldsymbol{y} \in M(\boldsymbol{v}', n) \text{ with } \boldsymbol{v}' \in S_\varepsilon(\boldsymbol{v})\},$$

as a common upper bound on the diameter of the sets $M(\boldsymbol{v}', n)$ with n sufficiently large, say $n \geq n'$. Note that R as well as $\mathcal{F}$, $\boldsymbol{v}$ and ε have an influence on the size of r and n'.

By Proposition 1 (ii) we can choose n' possibly larger to ensure the following for all $X \in \mathcal{F}$ attaining $\lambda(C, |X|)$ with $|X| \geq n'$: *The intersection of* (8) *with* $\operatorname{bd}\operatorname{conv} X$ *has a diameter less than* r*, no matter which* $\boldsymbol{t}_X \in \operatorname{conv} X$ *at distance* R *to* $\operatorname{bd}\operatorname{conv} X$ *we choose. Moreover,* $(\boldsymbol{t}_X + RB^d) \subset \operatorname{conv} X$.

Ensuring an empty intersection. It remains to show that for $X \in \mathcal{F}$, attaining $\lambda(C, |X|)$ with $|X|$ sufficiently large, $\boldsymbol{t}_X$ can be chosen such that (8) does not intersect $X \cap \operatorname{bd}\operatorname{conv} X$. For this we prove the following claim: *There exists an* n''*, depending on* r*,* $\boldsymbol{v}$ *and* ε*, such that for all* $X \in \mathcal{F}$ *with* $|X| \geq n''$*, there exists a vertex* $\boldsymbol{x}$ *of* $\operatorname{conv} X$ *with outer normal* $\boldsymbol{v}' \in S_\varepsilon(\boldsymbol{v})$ *and*

$$\{\boldsymbol{x}\} = X \cap (\operatorname{bd}\operatorname{conv} X) \cap (\boldsymbol{x} + rB^d). \tag{9}$$

Thus these vertices $\boldsymbol{x}$ have a distance larger than r to any other element of $X \cap \operatorname{bd}\operatorname{conv} X$. Therefore, by choosing $n_2 \geq \max\{n', n''\}$, we can ensure that there exists a $\boldsymbol{t}_X \in \mathbb{R}^d$ at distance R to $\operatorname{bd}\operatorname{conv} X$ such that (i') and (ii') are satisfied for all $X \in \mathcal{F}$ attaining $\lambda(C, |X|)$ with $|X| \geq n_2$. Note that n', n'', and hence n_2, depend on the choice of $\boldsymbol{v}$ and ε. But we may choose $\boldsymbol{v}$ and ε, depending on $\mathcal{F}$, so that n_2 can be chosen as small as possible. In this way we get an n_2 which solely depends on R, $\mathcal{F}$ and C.

It remains to prove the claim. Since (5) has only finitely many accumulation points, the set of normals $\boldsymbol{v}' \in S^{d-1}$ with hyperplane $\{\boldsymbol{y} \in \mathbb{R}^d : \langle \boldsymbol{v}', \boldsymbol{y} \rangle = 0\}$ running through

$\mathbf{0}$ and an accumulation point $\boldsymbol{y}$ of (5) all lie in the union $\mathcal{U}_r$ of finitely many linear subspaces of dimension $d-1$. Thus for any $\delta > 0$ the normals of these hyperplanes all lie in $\mathcal{U}_{r,\delta} = \mathcal{U}_r + \delta B^d$ if we choose $|X|$ sufficiently large, depending on δ. By choosing δ small enough, we find a $\boldsymbol{v}' \in S_\varepsilon(\boldsymbol{v})$ with $\boldsymbol{v}' \notin \mathcal{U}_{r,\delta}$. Moreover, there exists an $\varepsilon' > 0$ such that $S_{\varepsilon'}(\boldsymbol{v}') \cap \mathcal{U}_{r,\delta} = \emptyset$. Since every center polytope $\operatorname{conv} X$ has a vertex $\boldsymbol{x}$ with outer normal $\boldsymbol{v}'$, we may choose $|X|$ sufficiently large by Proposition 1 (i) (applied to $2\varepsilon'$), such that $\operatorname{conv} X$ has no outer normal in $\mathcal{U}_{r,\delta}$ at $\boldsymbol{x}$.
Moreover, for sufficiently large $|X|$, faces of $\operatorname{conv} X$ intersecting $\boldsymbol{x} + rB^d$ can not contain any vertex in $X \cap (\boldsymbol{x} + rB^d)$ aside of $\boldsymbol{x}$. Thus by construction, there exists an n'' such that (9) holds for all $X \in \mathcal{F}$ with $|X| \geq n''$. This proves the claim and therefore the proposition. □

Note that the proof offers the possibility to loosen the requirement on $\mathcal{F}$ a bit, for the price of introducing another parameter: For suitable large r, depending on $\mathcal{F}$, the proposition holds, if instead of (i) in Definition 1 we require

(i') there exist isometries $\mathcal{I}_X$ for each $X \in \mathcal{F}$, such that

$$\{\boldsymbol{x} - \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{I}_X(X) \text{ and } X \in \mathcal{F}\}$$

has only finitely many accumulation points within rB^d.

III. For all $X \in \mathcal{F}$ attaining $\lambda(C, |X|)$, with $|X|$ sufficiently large, we are able to obtain *contact free regions* $(\boldsymbol{t}_X + RB^d) \subset \operatorname{conv} X$, with R as large as we want, by Proposition 2. That is, we can modify these packing sets X by moving elements to free positions within $\operatorname{int}(\boldsymbol{t}_X + RB^d)$. By choosing R large enough, such an initial contact free region allows to move further elements to free positions. The following proposition takes care of interior points.

PROPOSITION 3. *Let $d \geq 2$ and $\mathcal{F}$ a family of packing sets in $\mathbb{R}^d$ satisfying (ii) in Definition 1 with $\varrho > 0$. Let $R \geq \frac{1}{\varrho}$, $X \in \mathcal{F}$ and $\boldsymbol{x} \in X \cap \operatorname{int}\operatorname{conv} X$. Let $\boldsymbol{t} \in \mathbb{R}^d$ with $|\boldsymbol{t} - \boldsymbol{x}| \leq R + \frac{\varrho}{2}$ and with all elements of $X \cap (\boldsymbol{t} + RB^d)$ in a free position. Then $\boldsymbol{x}$ can be moved to a free position within $\operatorname{int}\operatorname{conv} X$.*

Proof. Assume $\boldsymbol{x} \in \operatorname{int}\operatorname{conv} \mathcal{N}_X(\boldsymbol{x})$. By the assumption on $\mathcal{F}$,

$$\boldsymbol{x} + \varrho B^d \subset \operatorname{int}\operatorname{conv} \mathcal{N}_X(\boldsymbol{x}).$$

Thus there exists a $\boldsymbol{y} \in \mathcal{N}_X(\boldsymbol{x})$, such that the orthogonal projection $\boldsymbol{y}'$ of $\boldsymbol{y}$ onto the line through $\boldsymbol{x}$ and $\boldsymbol{t}$ satisfies $|\boldsymbol{y}' - \boldsymbol{x}| \geq \varrho$ and $|\boldsymbol{y}' - \boldsymbol{t}| \leq R - \frac{\varrho}{2}$. Then

$$|\boldsymbol{y} - \boldsymbol{t}|^2 = |\boldsymbol{y}' - \boldsymbol{t}|^2 + |\boldsymbol{y} - \boldsymbol{y}'|^2 \leq \left(R - \tfrac{\varrho}{2}\right)^2 + \left(1 - \varrho^2\right) < R^2.$$

Thus $\boldsymbol{y}$ is in a free position by the assumptions of the proposition, which contradicts $\boldsymbol{y} \in \mathcal{N}_X(\boldsymbol{x})$. □

IV. After Propositions 2 and 3 it remains to take care of points in $X \cap \operatorname{bd} \operatorname{conv} X$, for $X \in \mathcal{F}$ attaining $\lambda(C, |X|)$, and with $|X|$ sufficiently large. It turns out that these points can all be moved to free positions within $\operatorname{int} \operatorname{conv} X$. As a consequence we obtain the following.

Proposition 4. *Let $d \geq 2$, $C \subset \mathbb{R}^d$ a smooth convex body and $\mathcal{F}$ a family of packing sets in $\mathbb{R}^d$ satisfying (ii) of Definition 1. Then there exists an $n_4 \in \mathbb{N}$, depending on C and $\mathcal{F}$, such that $X \in \mathcal{F}$ with $|X| \geq n_4$ does not attain $\lambda(C, |X|)$, if all elements of $X \cap \operatorname{int} \operatorname{conv} X$ are in a free position.*

Proof. Let $\varrho > 0$ as in (ii) of Definition 1. We choose n_4 by Proposition 1 (ii), applied to $\varepsilon = \varrho$ and $r = 1$. Assume $X \in \mathcal{F}$ with $|X| \geq n_4$ attains $\lambda(C, |X|)$ and all elements of $X \cap \operatorname{int} \operatorname{conv} X$ are in a free position. We show that every element $\boldsymbol{x} \in X \cap \operatorname{bd} \operatorname{conv} X$ can be moved to a free position into $\operatorname{int} \operatorname{conv} X$. This gives the desired contradiction, because after moving (in an arbitrary order) all $X \cap \operatorname{bd} \operatorname{conv} X$ to free positions into $\operatorname{int} \operatorname{conv} X$, we obtain a packing set X' with $|X'| = |X|$ and $X' \subset \operatorname{int} \operatorname{conv} X$.
It is possible to move a given $\boldsymbol{x} \in X \cap \operatorname{bd} \operatorname{conv} X$ to a free position $\boldsymbol{x}' = \boldsymbol{x} + \delta \boldsymbol{v}$ for a (sufficiently small) $\delta > 0$, if $\boldsymbol{v} \in S^{d-1}$ is contained in the non-empty polyhedral cone

$$C_{\boldsymbol{x}} = \left\{ \boldsymbol{v} \in \mathbb{R}^d : \langle \boldsymbol{v}, \boldsymbol{y} - \boldsymbol{x} \rangle \leq 0 \text{ for all } \boldsymbol{y} \in \mathcal{N}_X(\boldsymbol{x}) \right\}.$$

If $\boldsymbol{v} \in C_{\boldsymbol{x}}$ can be chosen, so that $\boldsymbol{x}' \in \operatorname{int} \operatorname{conv} X$, the assertion follows. Otherwise, because $C_{\boldsymbol{x}}$ and $\operatorname{conv} X$ are convex, there exists a hyperplane through $\boldsymbol{x}$, with normal $\boldsymbol{w} \in S^{d-1}$, which separates $\operatorname{conv} X$ and $\boldsymbol{x} + C_{\boldsymbol{x}}$. That is, we may assume that

$$\boldsymbol{w} \in \operatorname{pos} \{ \boldsymbol{y} - \boldsymbol{x} : \boldsymbol{y} \in \mathcal{N}_X(\boldsymbol{x}) \}$$

and $-\boldsymbol{w}$ is an outer normal of $\operatorname{conv} X$ at $\boldsymbol{x}$.
Then for some $\delta > 0$, there exists a point $\boldsymbol{z} = \boldsymbol{x} + \delta \boldsymbol{w} \in \operatorname{bd} \operatorname{conv} \mathcal{N}_X(\boldsymbol{x})$, which is a convex combination of some $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_k \in \mathcal{N}_X(\boldsymbol{x})$. That is, there exist $\alpha_i \geq 0$ with $\sum_{i=1}^k \alpha_i = 1$ and $\boldsymbol{z} = \sum_{i=1}^k \alpha_i \boldsymbol{y}_i$. Therefore

$$\delta = \langle \boldsymbol{z} - \boldsymbol{x}, \boldsymbol{w} \rangle = \sum_{i=1}^k \alpha_i \langle \boldsymbol{y}_i - \boldsymbol{x}, \boldsymbol{w} \rangle < \varrho,$$

because $\langle \boldsymbol{y}_i - \boldsymbol{x}, \boldsymbol{w} \rangle < \varrho$ due to $|X| \geq n_4$ and $\boldsymbol{y}_i \in \operatorname{bd} \operatorname{conv} X$. This contradicts the assumption on $\mathcal{F}$ with respect to ϱ though. □

Finish. The proof of Theorem 2 reduces to the application of Propositions 1, 2, 3 and 4. Let $\mathcal{F}$ be an lc-family of packing sets in $\mathbb{R}^d$, with a $\varrho > 0$ as in (ii) of Definition 1. We choose $R \geq 1/\varrho$ and n_2 and n_4 according to Propositions 2 and 4. By Proposition 1 (ii), we choose n_1 such that packing sets X attaining $\lambda(C, |X|)$ with $|X| \geq n_1$ satisfy the following: For each $\boldsymbol{x} \in X$, there exists a $\boldsymbol{t} \in \mathbb{R}^d$ with $|\boldsymbol{x} - \boldsymbol{t}| = R + \frac{\varrho}{2}$ and $\boldsymbol{t} + RB^d \subset \operatorname{conv} X$.
We choose $n_0 \geq \max\{n_1, n_2, n_4\}$ and assume that $X \in \mathcal{F}$ with $|X| \geq n_0$ attains $\lambda(C, |X|)$. By Proposition 2 we can modify the packing set X to obtain a new packing

set X' with a contact free region $(\boldsymbol{t}_X + RB^d) \subset \operatorname{int}\operatorname{conv} X$, and with the same points $X' \cap \operatorname{bd}\operatorname{conv} X' = X \cap \operatorname{bd}\operatorname{conv} X$ on the boundary of the center polytope $\operatorname{conv} X' = \operatorname{conv} X$.
The following gives a possible order, in which we may subsequently move non-free elements $\boldsymbol{x} \in X \cap \operatorname{int}\operatorname{conv} X$ to free positions: By the choice of n_0 we can guarantee that for each $\boldsymbol{x} \in X \cap \operatorname{int}\operatorname{conv} X$, there exists a $\boldsymbol{t}$ with $|\boldsymbol{x} - \boldsymbol{t}| \leq R + \frac{\varrho}{2}$ and $\boldsymbol{t} + RB^d \subset \operatorname{conv} X$. Let $\boldsymbol{t}_{\boldsymbol{x}}$ be the $\boldsymbol{t}$ at minimal distance to $\boldsymbol{t}_X$. Then among the non-free $\boldsymbol{x} \in \operatorname{int}\operatorname{conv} X$, the one with minimal distance $|\boldsymbol{t}_{\boldsymbol{x}} - \boldsymbol{t}_X|$ satisfies the assumptions of Proposition 3, because a non-free element $\boldsymbol{y} \in X \cap (\boldsymbol{t}_{\boldsymbol{x}} + B^d)$ would satisfy $|\boldsymbol{t}_{\boldsymbol{y}} - \boldsymbol{t}_X| < |\boldsymbol{t}_{\boldsymbol{x}} - \boldsymbol{t}_X|$ due to $\operatorname{conv}\{\boldsymbol{t}_{\boldsymbol{x}}, \boldsymbol{t}_X\} + B^d \subset \operatorname{conv} X$.
Thus by Proposition 3 we can subsequently move the non-free elements within $X \cap \operatorname{int}\operatorname{conv} X$ to free positions. By this we obtain a contradiction to Proposition 4, which proves the theorem.

The lattice packing case. We end this section with the proof of Theorem 1. We may apply Theorem 2 after showing that the family of solutions to the lattice restricted container problem is of limited complexity. The space of lattices can be turned into a topological space (see [GL87]). The convergence of a sequence $\{\Lambda_n\}$ of lattices to a lattice Λ in particular involves that sets of lattice points within radius r around a lattice point tend to translates of $\Lambda \cap rB^d$ for growing n. As a consequence, a convergent sequence of packing lattices, as well as subsets of them, form an lc-family. Solutions to the lattice restricted container problem tend for growing n towards subsets of translates of *densest packing lattices* (see [Zon99]). These lattices are the solutions of the *lattice (sphere) packing problem*. Up to isometries, there exist only finitely many of these lattices in each dimension (see [Zon99]). Thus the assertion follows, since a finite union of lc-families is an lc-family.

4 Extensions

Let us briefly mention some possible extensions of Theorem 2. These have been treated in [Sch02] for the 2-dimensional case and could be directions for further research.

Packings of other convex bodies. Instead of sphere packings, we may consider packings $X + K$ for other convex bodies K. If the *difference body* $DK = K - K$ is strictly convex, then the proofs can be applied after some modifications: Instead of measuring distances with the norm $|\cdot|$ given by B^d, we use the norm $|\boldsymbol{x}|_{DK} = \min\{\lambda > 0 : \lambda\boldsymbol{x} \in DK\}$ given by DK. The strict convexity of DK is then used for the key fact, that elements $\boldsymbol{x}$ of a packing set X can be moved to a free position, whenever they are not contained in $\operatorname{int}\operatorname{conv} \mathcal{N}_X(\boldsymbol{x})$ (see II in Section 3). Note though that the sets in (6) and depending definitions have to be adapted for general convex bodies.

Packings in other containers. The restriction to smooth convex containers simplifies the proof, but we strongly believe that Theorem 2 is valid for other containers as well, e.g. certain polytopes. On the other hand there might exist containers for which

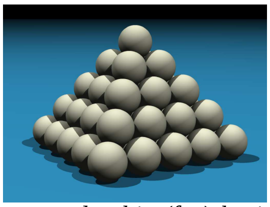
Theorem 2 is not true. In particular in dimension 3 it seems very likely that Theorem 2 is not true for polytopal containers C with all their facets lying in planes containing hexagonal sublattices of the *fcc lattice* (see Section 5). That is, for these polytopal containers C we conjecture the existence of infinitely many n, for which subsets of the *fcc lattice* attain $\lambda(C, n)$. An example for at least "local optimality" of sphere packings (with respect to differential perturbations) in suitable sized, but arbitrarily large tetrahedra was given by Dauenhauer and Zassenhaus [DZ87]. A proof of "global optimality" seems extremely difficult though, as it would provide a new proof of the sphere packing problem ("Kepler conjecture", see Section 5).

Other finite packing problems. Similar "phenomena" occur for other packing problems. For example, if we consider finite packing sets X with minimum diameter or surface area of $\operatorname{conv} X$, or maximum parametric density with large parameter (cf. [FCG91], [BHW94], [Bör04], [BP05]). This is due to the fact that the shapes of solutions tend to certain convex bodies, e.g. a sphere.

5 Kepler's assertion

Kepler's statement, quoted in the introduction, was later referred to as the origin of the famous sphere packing problem known as the *Kepler conjecture* (cf. e.g. [Hal02] p.5, [Hsi01] p.4). In contrast to the original statement, this problem asks for the maximum sphere packing density (see (10) below) of an infinite arrangement of spheres, where the "container" is the whole Euclidean space. As a part of Hilbert's famous problems [Hil01], it attracted many researchers in the past. Its proof by Hales with contributions of Ferguson (see [Hal02], [Hal05], [Hal06]), although widely accepted, had been a matter of discussion (cf. [Lag02], [Szp03], [FL06]).

Following Kepler [Kep11], the *cubic or hexagonal close packings* in $\mathbb{R}^3$ can be described via two dimensional layers of spheres, in which every sphere center belongs to a planar square grid, say with minimum distance 1. These layers are stacked (in a unique way) such that each sphere in a layer touches exactly four spheres of the layer above and four of the layer below.



The packing attained in this way is the well known *face centered cubic (fcc) lattice packing*. We can build up the fcc lattice by planar hexagonal layers as well, but then there are two choices for each new layer to be placed, and only one of them yields an fcc lattice packing. All of them, including the uncountably many non-lattice packings, are referred to as *hexagonal close packings (hc-packings)*. Note that the family of hc-packings is of limited complexity, because up to isometries they can be built from a fixed hexagonal layer.

Let

$$n(C) = \max\{|X| : C \supset X + \tfrac{1}{2}B^d \text{ is a packing }\}.$$

Then in our terminology Kepler asserts that, in $\mathbb{R}^3$, $n(C)$ is attained by hc-packings. His assertion, if true, would imply an "answer" to the sphere packing problem (Kepler conjecture), namely that the density of the densest infinite sphere packing

$$\delta_d = \limsup_{\lambda \to \infty} \frac{n(\lambda C) \cdot \mathrm{vol}(\frac{1}{2} B^d)}{\mathrm{vol}(\lambda C)} \tag{10}$$

is attained by hc-packings for $d = 3$; hence $\delta_3 = \pi/\sqrt{18}$. Note that this definition of density is independent of the chosen convex container C (see [Hla49] or [GL87]).
As a consequence of Theorem 2, Kepler's assertion turns out to be false though, even if we think of arbitrarily large containers. Consider for example the containers $\lambda(C, n)C$ for $n \geq n_0$.

COROLLARY 1. *Let $d \geq 2$, $C \subset \mathbb{R}^d$ a smooth convex body and $\mathcal{F}$ an lc-family of packing sets in $\mathbb{R}^d$. Then there exist arbitrarily large λ such that $n(\lambda C)$ is not attained by packing sets in $\mathcal{F}$.*

We may as well think of arbitrarily small spheres packed into a fixed container C. For $r > 0$, we call $X + rB^d$ a sphere packing if distinct elements $\boldsymbol{x}$ and $\boldsymbol{x}'$ of X have distance $|\boldsymbol{x} - \boldsymbol{x}'| \geq 2r$. Specializing to $\mathbb{R}^3$, the following corollary of Theorem 2 refers directly to Kepler's assertion.

COROLLARY 2. *Let $C \subset \mathbb{R}^3$ a smooth convex body. Then there exist arbitrarily small $r > 0$, such that*

$$\max\{|X| : C \supset X + rB^d \text{ is a packing }\}$$

is not attained by fcc or hexagonal close packing sets.

ACKNOWLEDGMENTS

I like to thank Thomas C. Hales, Tyrrell B. McAllister, Frank Vallentin, Jörg M. Wills, Günter M. Ziegler and the two anonymous referees for many helpful suggestions.

REFERENCES

[BHW94] U. Betke, M. Henk and J.M. Wills, *Finite and infinite packings*, J. Reine Angew. Math. 453 (1994), 165–191.

[Bez87] K. Bezdek, *Densest packing of small number of congruent spheres in polyhedra*, Ann. Univ. Sci. Budapest Eötvös Sect. Math., 30 (1987), 177–194.

[Bör04] K. Böröczky Jr., *Finite packing and covering*, Cambridge university press, Cambridge, 2004.

[BW04] K. Böröczky Jr., G. Wintsche, *Sphere packings in the regular crosspolytope*, Ann. Univ. Sci. Budapest Eötvös Sect. Math., 43 (2000), 151–157.

[BP05] P. Brass and J. Pach, *Problems in discrete geometry*, Springer, New York, 2005.

[CS95] J.H. Conway and N.J.A. Sloane, *What are all the best sphere packings in low dimensions?*, Discrete Comput. Geom., 13 (1995), 282–403.

[DZ87] M.H. Dauenhauer and H.J. Zassenhaus, *Local optimality of the critical lattice sphere-packing of regular tetrahedra*, Discrete Math. 64 (1987), 129–146.

[FCG91] K.J. Falconer H.T. Croft and R.K. Guy, *Unsolved problems in geometry*, Springer, New York, 1991.

[FL06] G. Fejes Tóth and J.C. Lagarias, *Guest Editors Foreword*, Discrete Comput. Geom., 36 (2006), 1–3.

[Fod99] F. Fodor, *The densest packing of 19 congruent circles in a circle*, Geom. Dedicata, 74 (1999), 139–145.

[GL87] P.M. Gruber and C.G. Lekkerkerker, *Geometry of numbers*, North-Holland, Amsterdam, 1987.

[Hal02] T.C. Hales, *An overview of the Kepler conjecture*, 16 pages, first in a series, arXiv:math.MG/9811071 (v2).

[Hal05] T.C. Hales, *A proof of the Kepler conjecture*, Ann. of Math (2), 162 (2005), 1065–1185.

[Hal06] T.C. Hales, *A proof of the Kepler conjecture (unabridged version)*, Discrete Comput. Geom., 36 (2006), 1–265.

[Hil01] D. Hilbert, *Mathematische Probleme*, Archiv Math. Physik 1 (1901), 44–63.

[Hla49] E. Hlawka, *Ausfüllung und Überdeckung konvexer Körper durch konvexe Körper.*, Monatsh. Math. 53 (1949), 81–131.

[Hsi01] W.Y. Hsiang, *Least action principle of crystal formation of dense packing type and Kepler's conjecture.*, World Scientific, Singapore, 2001.

[Kep11] J. Kepler, *Strena seu de nive sexangula*, Godefridum Tampach, Francofvrti Ad Moenum (Frankfurt), 1611, English translation: Hardy, *The six-cornered snowflake*, Clarendon Pr., Oxford, 1966.

[Lag02] J.C. Lagarias, *Bounds for local density of sphere packings and the Kepler conjecture.*, Discrete Comput. Geom. 27 (2002), 165–193.

[LG97] B.D. Lubachevsky and R.L. Graham, *Curved hexagonal packings of equal disks in a circle*, Discrete Comput. Geom. 18 (1997), 179–194.

[Mel97] J.B.M. Melissen, *Packing and covering with circles*, PhD thesis, University of Utrecht, 1997.

[NÖ97] K.J. Nurmela and P.R.J. Östergard, *More Optimal Packings of Equal Circles in a Square*, Discrete Comput. Geom. 22 (1999), 439–457.

[Sch93] R. Schneider, *Convex bodies: the Brunn-Minkowski theory.*, Cambridge University Press, Cambridge, 1993.

[Sch02] A. Schürmann, *On extremal finite packings*, Discrete Comput. Geom. 28 (2002), 389–403.

[Spe04] E. Specht, *Packomania*, `http://www.packomania.com/`.

[SMC+06] P.G. Szabó, M.Cs. Markót, T. Csendes, E. Specht, L.G. Casado, I. García, *New Approaches to Circle Packing in a Square*, Springer-Verlag, Berlin, to appear.

[Szp03] G. Szpiro, *Does the proof stack up?*, Nature 424 (2003), 12–13.

[Zie97] G.M. Ziegler, *Lectures on polytopes*, Springer-Verlag, New York, 1997.

[Zon99] C. Zong, *Sphere packings*, Springer-Verlag, New York, 1999.

Achill Schürmann
Mathematics Department
University of Magdeburg
39106 Magdeburg
Germany
achill@math.uni-magdeburg.de

A Symplectic Approach to Van Den Ban's Convexity Theorem

Philip Foth, Michael Otto

Received: June 2, 2006
Revised: September 25, 2006

Communicated by Eckhard Meinrenken

Abstract. Let G be a complex semisimple Lie group and τ a complex antilinear involution that commutes with a Cartan involution. If H denotes the connected subgroup of τ-fixed points in G, and K is maximally compact, each H-orbit in G/K can be equipped with a Poisson structure as described by Evens and Lu. We consider symplectic leaves of certain such H-orbits with a natural Hamiltonian torus action. A symplectic convexity theorem then leads to van den Ban's convexity result for (complex) semisimple symmetric spaces.

2000 Mathematics Subject Classification: 53D17, 53D20, 22E46
Keywords and Phrases: Lie group, real form, Poisson manifold, symplectic leaf, moment map, convex cone

1. Introduction

In 1982, Atiyah [1] and independently Guillemin and Sternberg [4] discovered a surprising connection between results in Lie theory and symplectic geometry. They proved a general symplectic convexity theorem of which Kostant's linear convexity theorem (for complex semisimple Lie groups) is a corollary. In this context, the orbits relevant for Kostant's theorem carry the natural symplectic structure of coadjoint orbits. The symplectic convexity theorem states that the image under the moment map of a compact connected symplectic manifold with Hamiltonian torus action is a convex polytope. Subsequently, Duistermaat [2] extended the symplectic convexity theorem in a way that it could be used to prove Kostant's linear theorem for real semisimple Lie groups as well.
Lu and Ratiu [10] found a way to put Kostant's nonlinear theorem into a symplectic framework. For a complex semisimple Lie group G with Iwasawa decomposition $G = NAK$, they regard the relevant K-orbits as symplectic

leaves of the Poisson Lie group AN, carrying the Lu-Weinstein Poisson structure. Kostant's nonlinear theorem for both complex and certain real groups then follows from the AGS-theorem or Duistermaat's theorem.

In this paper, we want to give a symplectic interpretation of van den Ban's convexity theorem for a complex semisimple symmetric space $(\mathfrak{g}, \tau)$, which is a generalization of Kostant's nonlinear theorem for complex groups. The theorem describes the image of the projection of a coset of G^τ onto $\mathfrak{a}^-$, the (-1)-eigenspace of τ. The image is characterized as the sum of a convex polytope and a convex polyhedral cone. For the precise statement of van den Ban's result we refer to Section 2. The main difference in view of our symplectic approach is that van den Ban's theorem is concerned with orbits of a certain subgroup $H \subset G$ that are in general neither symplectic nor compact. Since G is complex we can use a method due to Evens and Lu [3] to equip H-orbits in G/K with a certain Poisson structure. An H-orbit foliates into symplectic leaves, and on each leaf some torus acts in a Hamiltonian way. The corresponding moment map Φ turns out to be proper, and therefore the symplectic convexity theorem of Hilgert-Neeb-Plank [6] can be applied, which describes the image under Φ in terms of local moment cones. An analysis of those local moment cones shows that the image of Φ is the sum of a compact convex polytope and a convex polyhedral cone, just as in van den Ban's theorem.

The case of van den Ban's theorem for a real semisimple symmetric space is dealt with in a separate paper [12]. It follows the symplectic approach of Lu and Ratiu towards Kostant's nonlinear convexity theorem. The main tool is a generalized version of Duistermaat's theorem for non-compact manifolds.

Acknowledgments. We are grateful to the referee for the careful reading of the manuscript and many useful comments and suggestions.

2. Van den Ban's theorem

The purpose of this section is to fix notation and to recall the statement of van den Ban's theorem.

Let G be a real connected semisimple Lie group with finite center, equipped with an involution τ, i.e. τ is a smooth group homomorphism such that $\tau^2 = id$. Let $\mathfrak{g}$ be the Lie algebra of G. We write H for an open subgroup of G^τ, the τ-fixed points in G. Let K be a τ-stable maximal compact subgroup of G. The corresponding Cartan involution θ on $\mathfrak{g}$ commutes with τ and induces the Cartan decomposition $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$. If $\mathfrak{h}$ and $\mathfrak{q}$ denote the $(+1)$- and (-1)-eigenspace of $\mathfrak{g}$ with respect to τ one obtains

$$\mathfrak{g} = (\mathfrak{k} \cap \mathfrak{h}) + (\mathfrak{p} \cap \mathfrak{h}) + (\mathfrak{k} \cap \mathfrak{q}) + (\mathfrak{p} \cap \mathfrak{q}).$$

We fix a maximal abelian subalgebra $\mathfrak{a}^{-\tau}$ of $\mathfrak{p} \cap \mathfrak{q}$. (In [14] this subalgebra is denoted by $\mathfrak{a}_{pq}$.) In addition, we choose $\mathfrak{a}^\tau \subseteq \mathfrak{p} \cap \mathfrak{h}$ such that $\mathfrak{a} := \mathfrak{a}^\tau + \mathfrak{a}^{-\tau}$ is maximal abelian in $\mathfrak{p}$. Let $\Delta(\mathfrak{g}, \mathfrak{a}^{-\tau})$ and $\Delta(\mathfrak{g}, \mathfrak{a})$ denote the sets of roots for the root space decomposition of $\mathfrak{g}$ with respect to $\mathfrak{a}^{-\tau}$ and $\mathfrak{a}$, respectively.

Next, we choose a system of positive roots $\Delta^+(\mathfrak{g}, \mathfrak{a})$ and define

$$\Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}) = \{\alpha|_{\mathfrak{a}^{-\tau}} : \alpha \in \Delta^+(\mathfrak{g}, \mathfrak{a}), \alpha|_{\mathfrak{a}^{-\tau}} \neq 0\}.$$

This leads to an Iwasawa decomposition

$$\mathfrak{g} = \mathfrak{n} + \mathfrak{a} + \mathfrak{k} = \mathfrak{n}^1 + \mathfrak{n}^2 + \mathfrak{a} + \mathfrak{k},$$

where

$$\begin{aligned} \mathfrak{n} &= \sum_{\alpha \in \Delta^+(\mathfrak{g},\mathfrak{a})} \mathfrak{g}^\alpha, \\ \mathfrak{n}^1 &= \sum_{\alpha \in \Delta^+(\mathfrak{g},\mathfrak{a}), \alpha|_{\mathfrak{a}^{-\tau}} \neq 0} \mathfrak{g}^\alpha = \sum_{\beta \in \Delta^+(\mathfrak{g},\mathfrak{a}^{-\tau})} \mathfrak{g}^\beta, \\ \mathfrak{n}^2 &= \sum_{\alpha \in \Delta^+(\mathfrak{g},\mathfrak{a}), \alpha|_{\mathfrak{a}^{-\tau}} = 0} \mathfrak{g}^\alpha. \end{aligned}$$

Here $\mathfrak{g}^\alpha = \{X \in \mathfrak{g} : [H, X] = \alpha(H)X \ \forall H \in \mathfrak{a}\}$ for $\alpha \in \Delta(\mathfrak{g}, \mathfrak{a})$, and similarly $\mathfrak{g}^\beta$ is defined for $\beta \in \Delta(\mathfrak{g}, \mathfrak{a}^{-\tau})$.
Let N and A denote the analytic subgroups of G with Lie algebras $\mathfrak{n}$ and $\mathfrak{a}$, respectively. The Iwasawa decomposition $G = NAK$ on the group level has the middle projection $\mu : G \to A$. We write $pr_{\mathfrak{a}^{-\tau}} : \mathfrak{a} \to \mathfrak{a}^{-\tau}$ for the projection along $\mathfrak{a}^\tau$.
For $\beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau})$ define $H_\beta \in \mathfrak{a}^{-\tau}$ such that

$$H_\beta \perp \ker\beta, \quad \beta(H_\beta) = 1,$$

where $\perp$ means orthogonality with respect to the Killing form κ.
Note that the involution $\theta \circ \tau$ leaves each root space

$$\mathfrak{g}^\beta = \sum_{\alpha \in \Delta(\mathfrak{g},\mathfrak{a}), \alpha|_{\mathfrak{a}^{-\tau}} = \beta} \mathfrak{g}^\alpha$$

stable. Each $\mathfrak{g}^\beta = (\mathfrak{g}^\beta)_+ \oplus (\mathfrak{g}^\beta)_-$ decomposes into $(+1)$- and (-1)-eigenspace with respect to $\theta \circ \tau$.
For

$$\Delta_- := \{\beta \in \Delta(\mathfrak{g}, \mathfrak{a}^{-\tau}) : (\mathfrak{g}^\beta)_- \neq 0\},$$

let $\Delta_-^+ = \Delta_- \cap \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau})$. Define the closed cone

$$\Gamma(\Delta_-^+) = \sum_{\beta \in \Delta_-^+} \mathbb{R}_+ H_\beta.$$

Write $\mathcal{W}_{K\cap H}$ for the Weyl group

$$\mathcal{W}_{K\cap H} = N_{K\cap H}(\mathfrak{a}^{-\tau})/Z_{K\cap H}(\mathfrak{a}^{-\tau}).$$

The convex hull of a Weyl group orbit through $X \in \mathfrak{a}^{-\tau}$ will be denoted by $\mathrm{conv}(\mathcal{W}_{K\cap H}.X)$.

REMARK 2.1. *Consider the Lie algebra $\mathfrak{g}^{\theta\tau}$ of $\theta\tau$-fixed points in $\mathfrak{g}$. It is reductive and its semisimple part $\mathfrak{g}' = [\mathfrak{g}^{\theta\tau}, \mathfrak{g}^{\theta\tau}]$ admits a Cartan decomposition $\mathfrak{g}' = \mathfrak{k}' + \mathfrak{p}'$ with $\mathfrak{k}' \subset \mathfrak{k}$, $\mathfrak{p}' \subset \mathfrak{p}$. Due to our choice, $\mathfrak{a}^{-\tau}$ is a maximal abelian subalgebra of $\mathfrak{p}'$. The set of roots $\Delta(\mathfrak{g}', \mathfrak{a}^{-\tau})$ consists exactly of those reduced roots*

$\beta \in \Delta(\mathfrak{g}, \mathfrak{a}^{-\tau})$ for which $(\mathfrak{g}^\beta)_+ \neq 0$. Moreover, the Weyl group $\mathcal{W}'$ associated to $\mathfrak{g}'$ coincides with $\mathcal{W}_{K\cap H}$.

We can now state the central theorem.

THEOREM 2.2. (Van den Ban [14])
Let G be a real connected semisimple Lie group with finite center, equipped with an involution τ, and H a connected open subgroup of G^τ. For $X \in \mathfrak{a}^{-\tau}$, write $a = \exp X \in A^{-\tau}$. Then

$$(pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu)(Ha) = \mathrm{conv}(\mathcal{W}_{K\cap H}.X) - \Gamma(\Delta_-^+).$$

Remark 2.3.

- *The statement of the theorem above differs from the original in [14] by a minus sign in front of the conal part $\Gamma(\Delta_-^+)$. This is due to the fact that we consider the set Ha and an Iwasawa decomposition $G = NAK$, whereas in [14] the set $aH \subset G = KAN$ is considered. Indeed, if we denote the two middle projections by $\mu : NAK \to A$ and $\mu' : KAN \to A$, then $\Gamma(\Delta_-^+) = \log \circ \mu'(H) = -\log \circ \mu(H)$.*
- *Van den Ban proved his theorem under the weaker condition that H is an essentially connected open subgroup of G^τ (by reducing it to the connected case).*
- *If $\tau = \theta$ one obtains Kostant's (nonlinear) convexity theorem. Note that in this case the group H and the orbit Ha are compact.*

3. Poisson structure

Let G be a connected and simply connected semisimple complex Lie group with Lie algebra $\mathfrak{g}$. Cartan involutions on both group and Lie algebra level will be denoted by θ. In addition, let τ be a complex antilinear involution (on G and $\mathfrak{g}$) which commutes with θ.
The Lie algebra $\mathfrak{g}$ decomposes into $(+1)$- and (-1)-eigenspaces with respect to both involutions θ and τ.

$$\mathfrak{g} = \mathfrak{k} + \mathfrak{p} = \mathfrak{h} + \mathfrak{q},$$

where $\mathfrak{k}$ and $\mathfrak{h}$ denote the $(+1)$-eigenspaces with respect to θ and τ, respectively, and $\mathfrak{p}$ and $\mathfrak{q}$ denote the (-1)-eigenspaces.
The maximal compact subgroup K of G with Lie algebra $\mathfrak{k}$ is τ-stable. Let H denote the connected subgroup of G consisting of τ-fixed points. We will be interested in certain H-orbits in the symmetric space G/K. Each such orbit can be equipped with a Poisson structure as introduced by Evens and Lu. We briefly describe their method which can be found in [3, Section 2.2]. For details on Poisson Lie groups see e.g. [11].
Let (U, π_U) be a connected Poisson Lie group with tangent Lie bialgebra $(\mathfrak{u}, \mathfrak{u}^*)$ and double Lie algebra $\mathfrak{d} = \mathfrak{u} \bowtie \mathfrak{u}^*$. The pairing

$$\langle v_1 + \lambda_1, v_2 + \lambda_2 \rangle := \lambda_1(v_2) + \lambda_2(v_1) \quad \forall\, v_1, v_2 \in \mathfrak{u}, \lambda_1, \lambda_2 \in \mathfrak{u}^*,$$

defines a non-degenerate symmetric bilinear form and turns $(\mathfrak{d}, \mathfrak{u}, \mathfrak{u}^*)$ into a Manin triple. We will identify $\mathfrak{d}^*$ with $\mathfrak{d}$ via $\langle , \rangle$.

Consider the following bivector $R \in \wedge^2 \mathfrak{d}$:

$$R(v_1 + \lambda_1, v_2 + \lambda_2) = \lambda_2(v_1) - \lambda_1(v_2) \quad \forall\, v_1, v_2 \in \mathfrak{u}, \lambda_1, \lambda_2 \in \mathfrak{u}^*.$$

In terms of a basis $\{v_1, \ldots, v_n\}$ for $\mathfrak{u}$ and a dual basis $\{\lambda_1, \ldots, \lambda_n\}$ for $\mathfrak{u}^*$ the bivector is represented by $R = \sum_{i=1}^n \lambda_i \wedge v_i$.
Assume that D is a connected Lie group with Lie algebra $\mathfrak{d}$, and assume that U is a connected subgroup of D with Lie algebra $\mathfrak{u}$. Then D acts on the Grassmannian $\mathrm{Gr}(n, \mathfrak{d})$ of n-dimensional subspaces of $\mathfrak{d}$ via the adjoint action of D on $\mathfrak{d}$ and therefore defines a Lie algebra antihomomorphism

$$\eta : \mathfrak{d} \to \mathcal{X}(\mathrm{Gr}(n, \mathfrak{d})),$$

into the vector fields on $\mathrm{Gr}(n, \mathfrak{d})$. Using the symbol η also for its multilinear extension we can define a bivector field Π on $\mathrm{Gr}(n, \mathfrak{d})$ by

$$\Pi = \frac{1}{2}\eta(R).$$

Note that Π in general does not define a Poisson structure on the entire $\mathrm{Gr}(n, \mathfrak{d})$. However, it does so on the subvariety $\mathfrak{L}(\mathfrak{d})$ of Lagrangian subspaces (with respect to $\langle , \rangle$) on $\mathfrak{d}$, and on each D-orbit $D.\mathfrak{l} \subset \mathfrak{L}(\mathfrak{d})$.
The bivector R also gives rise to a Poisson structure π_- on D that makes (D, π_-) a Poisson Lie group:

$$\pi_-(d) = \frac{1}{2}(r_d R - l_d R) \quad \forall d \in D. \tag{1}$$

Here r_d and l_d denote the differentials of right and left translations by d. Note that the restriction of π_- to the subgroup $U \subset D$ coincides with the original Poisson structure π_U on U, i.e. (U, π_U) is a Poisson subgroup of (D, π_-).
For $\mathfrak{l} \in \mathfrak{L}(\mathfrak{d})$ the D-orbit through l is not only a Poisson manifold with respect to Π but a homogeneous Poisson space under the action of (D, π_-). Moreover, the U-orbit $U.\mathfrak{l}$ is a homogeneous (U, π_U)-space, since the Poisson tensor Π at $\mathfrak{l}$ turns out to be tangent to $U.\mathfrak{l}$. In fact, the tangent space at $\mathfrak{l} \in D.\mathfrak{l}$ can be identified with $\mathfrak{d}/n(\mathfrak{l})$, where $n(\mathfrak{l})$ is the normalizer subalgebra of $\mathfrak{l}$. In the case when $n(\mathfrak{l}) = \mathfrak{l}$, we identify the cotangent space with $\mathfrak{l}$ itself, and for $X, Y \in \mathfrak{l}$ one obtains:

$$\Pi(\mathfrak{l})(X, Y) = \langle pr_{\mathfrak{u}} X, Y \rangle, \quad \text{i.e.} \quad \Pi(\mathfrak{l})^\sharp(X) = pr_{\mathfrak{u}} X, \tag{2}$$

where $pr_{\mathfrak{u}} : \mathfrak{d} \to \mathfrak{u}$ denotes the projection along $\mathfrak{u}^*$.
Let U^* be the connected subgroup of D with Lie algebra $\mathfrak{u}^*$. What has been said about the Poisson Lie group U is also true for its dual group U^*, i.e. (U^*, π_{U^*}) is a Poisson Lie subgroup of $(D, -\pi_-)$ and the orbit $U^*.\mathfrak{l}$ is a homogeneous (U^*, π_{U^*})-space. It follows in particular that $(U.\mathfrak{l}) \cap (U^*.\mathfrak{l})$ contains the symplectic leaf through $\mathfrak{l}$.

We now want to apply this construction to our complex semisimple Lie algebra $\mathfrak{g}$. In the above notation we will have $\mathfrak{d} = \mathfrak{g}$, and the pairing $\langle , \rangle$ will be given by the imaginary part, $\Im\kappa$, of the Killing form κ on $\mathfrak{g}$. Note that $\mathfrak{k} \in$

$\mathfrak{L}(\mathfrak{d})$. Throughout the paper, we will identify the G-orbit through $\mathfrak{k}$ with the symmetric space G/K. In particular, orbits in $G.\mathfrak{k}$ are identified with those in G/K. Then we set $\mathfrak{u} = \mathfrak{h}$, and it remains to define $\mathfrak{u}^*$.

First we choose an appropriate Iwasawa decomposition of $\mathfrak{g}$. Recall the τ-stable Cartan decomposition $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$. We fix a maximal abelian subalgebra $\mathfrak{a}^{-\tau}$ in $\mathfrak{p} \cap \mathfrak{q}$. Then we can find an abelian subalgebra $\mathfrak{a}^{\tau}$ in $\mathfrak{p} \cap \mathfrak{h}$ such that $\mathfrak{a} = \mathfrak{a}^{-\tau} + \mathfrak{a}^{\tau}$ is maximal abelian in $\mathfrak{p}$. We choose a positive root system, $\Delta^+(\mathfrak{g}, \mathfrak{a})$ by the lexicographic ordering with respect to an ordering of a basis of $\mathfrak{a}$, which was constructed from a basis of $\mathfrak{a}^{-\tau}$ followed by a basis of $\mathfrak{a}^{\tau}$. This yields an Iwasawa decomposition $\mathfrak{g} = \mathfrak{n} + \mathfrak{a} + \mathfrak{k}$ which is compatible with the involution τ in the following sense.

Lemma 3.1. *For our choice of Iwasawa decomposition $\mathfrak{g} = \mathfrak{n} + \mathfrak{a} + \mathfrak{k}$, we have*

$$\mathfrak{h} \cap \mathfrak{n} = \{0\}.$$

Besides, the centralizer of $\mathfrak{a}^{-\tau}$ in $\mathfrak{g}$ is a Cartan subalgebra of $\mathfrak{g}$.

Proof. Consider the root space decomposition of $\mathfrak{g}$ with respect to $\mathfrak{a}$,

$$\mathfrak{g} = (\mathfrak{a} + i\mathfrak{a}) + \sum_{\alpha \in \Delta(\mathfrak{g}, \mathfrak{a})} \mathfrak{g}^{\alpha}.$$

It is well-known [7, Proposition 6.70] that there are no real roots for a maximally compact Cartan subalgebra $(i\mathfrak{a}^{-\tau} + \mathfrak{a}^{\tau})$ of $\mathfrak{h}$, and therefore there are no $\alpha \in \Delta(\mathfrak{g}, \mathfrak{a})$ such that $\alpha|_{\mathfrak{a}^{-\tau}} = 0$. By [5, Chapter VI, Lemma 3.3], this implies that $\tau(\mathfrak{g}^{\alpha}) \subset \bigoplus_{\alpha \in \Delta^+(\mathfrak{g}, \mathfrak{a})} \mathfrak{g}^{-\alpha}$ for all $\alpha \in \Delta^+(\mathfrak{g}, \mathfrak{a})$, and the claim $\mathfrak{h} \cap \mathfrak{n} = \{0\}$ follows immediately.

Since each $\alpha \in \Delta(\mathfrak{g}, \mathfrak{a})$ does not vanish outside a hyperplane of $\mathfrak{a}^{-\tau}$, it follows that $\mathfrak{a}^{-\tau}$ contains regular elements and its centralizer in $\mathfrak{g}$ is a Cartan subalgebra of $\mathfrak{g}$.

□

Consider the Cartan subalgebra $\mathfrak{c} = \mathfrak{z}(\mathfrak{a}^{-\tau})$ of $\mathfrak{g}$. Lemma 3.1 together with the properties of κ implies that $\mathfrak{g} = \mathfrak{h} \oplus (\mathfrak{c}^{-\tau} \oplus \mathfrak{n})$ is a Lagrangian splitting with respect to the bilinear form $\Im\kappa$. In other words, $(\mathfrak{g}, \mathfrak{h}, (\mathfrak{c}^{-\tau} + \mathfrak{n}))$ is a Manin triple.

We can now define the desired Poisson manifolds using the method of Evens and Lu outlined above. We set

$$\mathfrak{d} = \mathfrak{g},\ \mathfrak{u} = \mathfrak{h},\ \mathfrak{u}^* = \mathfrak{c}^{-\tau} + \mathfrak{n},\ \langle , \rangle = \Im\kappa.$$

Let C, $C^{-\tau}$, A and N denote the analytic subgroups of G with Lie algebras $\mathfrak{c}$, $\mathfrak{c}^{-\tau}$, $\mathfrak{a}$ and $\mathfrak{n}$, respectively. The group H now has the structure of a Poisson Lie group. Its dual group is $H^* = C^{-\tau}N$. Fix $a \in A^{-\tau}$ and consider the base point $a.K \in G/K$. The H-orbit $P_a = Ha.K \in G/K$ is a Poisson homogeneous manifold with respect to the action by (H, π_H). Also, the dual group orbit $H^*a.K$ is Poisson homogeneous with respect to π_{H^*}. For the symplectic leaf in P_a through a, denoted by M_a, we have $M_a \subseteq Ha.K \cap H^*a.K$.

LEMMA 3.2. *The Poisson manifold P_a is regular and equals the union of A^τ-translates of M_a, i.e. each $p \in P_a$ can be written $p = a'm$ with unique $a' \in A^\tau, m \in M_a$. Moreover, $M_a = Ha.K \cap H^*a.K$.*

Proof. Consider the map $M : A^\tau \times M_a \to P_a$.
First we will show that M is injective. The Poisson tensor $\pi_H = \pi_-$ as defined in (1) vanishes at each element $c \in C^\tau$, since $Ad(c)$ leaves both $\mathfrak{h}$ and $\mathfrak{h}^* = \mathfrak{c}^{-\tau} + \mathfrak{n}$ stable. Therefore $a' \in A^\tau$ acts on P_a by Poisson diffeomorphisms and maps the symplectic leaf M_a onto the symplectic leaf $M_{a'a}$. But $M_{a_1a} \neq M_{a_2a}$ for $a_1 \neq a_2 \in A^\tau$, following from the fact that M_{a_1a} lies in $H^*a_1a.K = C^{-\tau}Na_1a.K$ and the uniqueness of the Iwasawa decomposition.
At each point $p \in P_a$ one can explicitly calculate the codimension of the symplectic leaf through p in P_a, for instance by means of an infinitesimal version of Corollary 7.3 in [9] and Theorem 2.21 in [3]. It follows that the codimension of the leaf through the point $p = ha.K$ in the orbit P_a equals the dimension of the intersection of $Ad(a)\mathfrak{k}$ and $Ad(h^{-1})\mathfrak{h}^*$, which is easily seen to be independent from the point $p \in P_a$ and equal to the dimension of $\mathfrak{a}^\tau$. Here we used the fact that the dimension of $Ad(ha)\mathfrak{k} \cap \mathfrak{h}^*$ cannot exceed the dimension of $\mathfrak{a}^\tau$, since the Killing form is negative definite on $Ad(ha)\mathfrak{k}$ and a maximal negative definite subspace of $\mathfrak{h}^*$ is $i\mathfrak{a}^\tau$. This shows that P_a is a regular Poisson manifold, and that $A^\tau M_a$ is a full dimensional subset of P_a. Since A^τ acts freely on P_a and P_a is a regular Poisson manifold, it can be represented as the union of such open subsets. The connectedness of P_a then implies that $P_a = A^\tau M_a$.
Since A^τ is connected and the union of A^τ-translates of $Ha.K \cap H^*a.K$ equals $Ha.K$ and thus is also connected, it is easy to see that $Ha.K \cap H^*a.K$ is connected as well. Besides, from the transversality we see that

$$\dim(Ha.K \cap H^*a.K) = \dim(Ha.K) + \dim(H^*a.K) - \dim(G/K).$$

Note that the first part of the proof implies that $A^\tau a.K \cap H^*a.K = \{a.K\}$. Therefore, the codimension of $Ha.K \cap H^*a.K$ in $Ha.K$ is at least $\dim(\mathfrak{a}^\tau)$. But since M_a has codimension equal to $\dim(\mathfrak{a}^\tau)$, and $M_a \subseteq Ha.K \cap H^*a.K$, the last inclusion is actually an equality.

□

Consider the torus $T = \exp(i\mathfrak{a}^{-\tau}) \subset H$. It acts on M_a in a symplectic manner, since π_H vanishes at each $t \in T$. Moreover, the next lemma shows that this action is Hamiltonian with an associated moment map that is closely related to the middle projection $\mu : G = NAK \to A$ of the Iwasawa decomposition.

LEMMA 3.3. *The action of $T = \exp(i\mathfrak{a}^{-\tau})$ on M_a is Hamiltonian with a moment map $\Phi = pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu$. Here, $pr_{\mathfrak{a}^{-\tau}} : \mathfrak{a} \to \mathfrak{a}^{-\tau}$ denotes the projection along $\mathfrak{a}^\tau$, and $\mathfrak{t}^*$ is identified with $\mathfrak{a}^{-\tau}$ via $\Im\kappa$.*
Moreover, the moment map Φ is proper.

Proof. (1) $\Phi = pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu$ is a moment map.
Let $b : G = NAK \longrightarrow B = NA$ be the B-projection in the Iwasawa decomposition. We write $pr_{\mathfrak{a}} : \mathfrak{g} = \mathfrak{n} + \mathfrak{a} + \mathfrak{k} \to \mathfrak{a}$ for the middle

projection on the Lie algebra level. Let $Z \in \mathfrak{t} = i\mathfrak{a}^{-\tau}$, $h \in H$ and $X \in \mathfrak{h}$. We denote by Φ_Z the function obtained by evaluating Φ at Z, by $\tilde{X}_{ha}$ the tangent vector of the vector field generated by X at the point $ha.K \in M_a$ (for brevity we will write $h.K$ simply as h henceforth, without fear of confusion) and by $D\Phi_{b(ha)}$ the derivative of Φ at the point $b(ha)$. We have:

$$\begin{aligned}
d\Phi_Z(ha).\tilde{X}_{ha} &= \frac{d}{ds}\Big|_{s=0}\Phi_Z(\exp(sX)ha) = \langle \frac{d}{ds}\Big|_{s=0}\Phi(\exp(sX)ha), Z\rangle \\
&= \langle \frac{d}{ds}\Big|_{s=0}\Phi(b(ha)\exp(sAd(b(ha)^{-1})X)), Z\rangle \\
&= \langle D\Phi_{b(ha)}Ad(b(ha)^{-1})X, Z\rangle \\
&= \langle pr_{\mathfrak{a}^{-\tau}} \circ pr_{\mathfrak{a}} Ad(b(ha)^{-1})X, Z\rangle = \langle Ad(b(ha)^{-1})X, Z\rangle \\
&= \langle X, Ad(b(ha))Z\rangle
\end{aligned}$$

The second last step follows from the fact that $\mathfrak{t}$ and $\mathfrak{k} + \mathfrak{a}^\tau + \mathfrak{n}$ are orthogonal with respect to $\langle , \rangle$.

Note that $Ad(b(ha))Z \in Z + \mathfrak{n}$. With (2) this implies

$$\Pi(ha)^\sharp(d\Phi_Z(ha)) = pr_{\mathfrak{h}} Ad(b(ha))Z = Z.$$

(2) Φ is proper.

This follows from Lemma 3.3 in [14], which states the properness of the map

$$F_a : (H \cap L_0)\backslash H \to \mathfrak{a}^{-\tau}, \quad F_a(x) = \Phi(xa).$$

In our case $L_0 = \exp(i\mathfrak{a})A^\tau$ (since $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{a}^{-\tau}) = \mathfrak{c}$ by the argument in the proof of Lemma 3.1).
Properness of the map $F_a : TA^\tau\backslash H \to \mathfrak{a}^{-\tau}$ implies properness of the induced maps $F_a : A^\tau\backslash H \to \mathfrak{a}^{-\tau}$ and $F_a : A^\tau\backslash H/(H \cap aKa^{-1}) \to \mathfrak{a}^{-\tau}$. Since $A^\tau\backslash H/(H \cap aKa^{-1}) \cong M_a$ by Lemma 3.2, and since F_a becomes Φ under this identification, the claim follows.

□

Remark 3.4. *In case $\tau = \theta$ the Lu-Evens Poisson structure on $P_a = Ka.K$ coincides with the Lu-Weinstein symplectic structure, and Lemma 3.3 becomes Theorem 4.13 in* [10].

4. Symplectic convexity

Throughout this section we assume G to be complex and the involution τ to be complex antilinear. In this case we will interpret van den Ban's theorem in the symplectic framework developed in Section 3. More precisely, it can be viewed as a corollary of a symplectic convexity theorem for Hamiltonian torus actions.

Van den Ban's theorem describes the image of the group orbit Ha under the map $pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu$. Recall from Section 3 the symplectic manifold $M_a \subseteq$

$Ha.K \subseteq G/K$ on which the torus $T = \exp(i\mathfrak{a}^{-\tau})$ acts in a Hamiltonian fashion (Lemma 3.3). The associated moment map is $\Phi = pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu$. From Lemma 3.2 and from the A^τ-invariance of $pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu$ it follows that

$$(pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu)(Ha) = \Phi(M_a).$$

This means that van den Ban's theorem can be viewed as a description of the image of a symplectic manifold under an appropriate moment map.
The description of the image of the moment map is the content of a series of symplectic convexity theorems. Probably best known are the original theorems of Atiyah and Guillemin-Sternberg [1, 4]. The result needed here is a generalization of the AGS-theorems to a non-compact setting. Several versions can be found in the literature, e.g. [8, 13]. We will state the theorem as given in [6]. Recall that a subset C of a finite dimensional vector space V is called locally polyhedral iff for each $x \in C$ there is a neighborhood $U_x \subseteq V$ such that $C \cap U_x = (x + \Gamma_x) \cap U_x$ for some cone Γ_x. A cone Γ is called proper if it contains no lines, otherwise Γ is called improper.

theorem 4.1. [6, Theorem 4.1(i)] *Consider a Hamiltonian torus action of T on the connected symplectic manifold M. Suppose the associated moment map $\Phi : M \to \mathfrak{t}^*$ is proper, i.e. Φ is a closed mapping and $\Phi^{-1}(Z)$ is compact for every $Z \in \mathfrak{t}^*$. Then $\Phi(M)$ is a closed, locally polyhedral, convex set.*

Remark 4.2. *Theorem 4.1 in* [6] *contains more detailed information, in particular a description of the cones that span $\Phi(M)$ locally (part (v)). More precisely, for each $m \in M$ there is a neighborhood $U_{\Phi(m)} \subseteq \mathfrak{t}^*$ of $\Phi(m)$ such that $\Phi(M) \cap U_{\Phi(m)} = (\Phi(m) + \Gamma_{\Phi(m)}) \cap U_\Phi(m)$, where $\Gamma_{\Phi(m)} = \mathfrak{t}_m^\perp + C_m$. Here, $\mathfrak{t}_m$ denotes the Lie algebra of the stabilizer T_m of m, and $C_m \subseteq \mathfrak{t}_m^*$ denotes the cone which is spanned by the weights of the linearized action of T_m. The (nontrivial) fact that the cone $\Gamma_{\Phi(m)} = \mathfrak{t}_m^\perp + C_m$ is actually independent of the choice of a preimage point of $\Phi(m)$ is also shown in* [6].

Coming back to the symplectic manifold M_a, Lemma 3.3 shows that the moment map $\Phi = pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu$ on M_a is proper. Theorem 4.1 can therefore be applied and yields

$$\Phi(M_a) \quad \text{is a closed, locally polyhedral, convex set.}$$

We will now give a more detailed description of $\Phi(M_a)$. It turns out that the T-action on M_a has (finitely many) fixed points. At each fixed point we can calculate the cones that locally span $\Phi(M_a)$. From this description it will follow that the entire set $\Phi(M_a)$ lies in a proper cone and can therefore be described entirely by the local data at the fixed points.
We begin by determining the T-fixed points.

Proposition 4.3. *The T-fixed points in M_a are exactly those elements of the form $w(a).K \in G/K$ with $w \in \mathcal{W}_{K\cap H} = N_{K\cap H}(\mathfrak{a}^{-\tau})/Z_{K\cap H}(\mathfrak{a}^{-\tau})$.*

Proof. Recall that for $a \in A^{-\tau}$ we view the symplectic manifold M_a as a submanifold of the H-orbit in G/K through the base point $a.K \in G/K$. Clearly,

each element $w(a).K \in G/K$ with $w \in \mathcal{W}_{K\cap H}$ is T-fixed. To see that $w(a).K$ lies in M_a, note that $w(a).K \in H^*a.K$ since $w(a) \in A^{-\tau}$. On the other hand, there exists $k \in K\cap H$ such that $w(a) = kak^{-1}$, which implies $w(a).K \in Ha.K$. Therefore, $w(a).K \in Ha.K \cap H^*a.K = M_a$ by Lemma 3.2.
Conversely, assume that $cpa.K \in M_a$ with $c \in K^\tau, p \in \exp(\mathfrak{p}^\tau)$ is T-fixed. Since M_a lies in the orbit of the dual group $H^* = NC^{-\tau}$ there are elements $n \in N, b \in A^{-\tau}, k \in K$ such that $cpa = nbk$. Since $nb.K \in G/K$ is a T-fixed point,

$$tnt^{-1}b \in nbK \qquad \forall\ t \in T.$$

The Lie subalgebra $\mathfrak{n}$ is T-invariant, so by the uniqueness of the Iwasawa decomposition $tnt^{-1} = n$ for all $t \in T$. But since $\alpha|_{\mathfrak{a}^{-\tau}} \neq 0$ for all $\alpha \in \Delta(\mathfrak{g}, \mathfrak{a})$ this can happen only for $n = e$. This implies $cpa = bk$.
Symmetrizing the last equation yields

$$cpa\theta(cpa)^{-1} = cpa^2pc^{-1} = b^2. \tag{3}$$

Applying $\theta \circ \tau$ to (3) gives

$$cp^{-1}a^2p^{-1}c^{-1} = b^2. \tag{4}$$

We multiply (3) by (4) from the right and from the left and obtain

$$cpa^4p^{-1}c^{-1} = b^4 = cp^{-1}a^4pc^{-1}.$$

But then $pa^4p^{-1} = p^{-1}a^4p$, i.e. p^2 and a^4 commute (and are self-adjoint). Therefore, p and a^2 also commute, and we can combine equations (3) and (4) to

$$cp^2a^2c^{-1} = b^2 = cp^{-2}a^2c^{-1}.$$

This shows $p^2 = p^{-2}$ or $p = e$. But then (4) implies $cac^{-1} = b$. Since both a and b lie in $A^{-\tau}$ and since $c \in K^\tau = K \cap H$, there is some element $w \in \mathcal{W}_{K\cap H}$ such that $w(a) = b$ (Recall from Remark 2.1 that $\mathcal{W}_{K\cap H}$ is the Weyl group of the reductive Lie algebra $\mathfrak{g}^{\theta\tau} = (\mathfrak{k} \cap \mathfrak{h}) + (\mathfrak{p} \cap \mathfrak{q})$ of $\theta\tau$-fixed points of $\mathfrak{g}$).
The T-fixed point $cpa.K \in M_a$ can therefore be written as $cpa.K = b.K = w(a).K$ for some $w \in \mathcal{W}_{K\cap H}$. □

Recall our choice of base point $a = \exp(X)$ and the identification $\mathfrak{t}^* \cong \mathfrak{a}^{-\tau}$. We now describe the image of the moment map $\Phi(M_a) \in \mathfrak{a}^{-\tau}$ in the neighborhood of a fixed point image $\Phi(w(a).K) = w(X)$. From Theorem 4.1 (and Remark 4.2) we know that locally $\Phi(M_a)$ looks like $w(X)+\Gamma_{w(X)}$ for some cone $\Gamma_{w(X)} \in \mathfrak{a}^{-\tau}$. The next Lemma describes $\Gamma_{w(X)}$ in terms of the vectors H_β for (reduced) roots $\beta \in \Delta(\mathfrak{g}, \mathfrak{a}^{-\tau})$ defined in Section 2.

Lemma 4.4. *Let $a = \exp X$ with $X \in \mathfrak{a}^{-\tau}$ and $w \in \mathcal{W}_{K\cap H}$. The local cone $\Gamma_{\Phi(w(a).K)} = \Gamma_{w(X)} \subseteq \mathfrak{a}^{-\tau}$ is the cone spanned by the union of the following two sets.*

$$\{-\beta(w(X))H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_+ \neq 0\}$$
$$\text{and} \quad \{-H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_- \neq 0\}$$

Proof. We are adapting the argument from [6, page 155] to our setting. To determine the local cone $\Gamma_{w(X)}$ it is enough to consider the linearized action of T on the tangent space $V_{w(a).K} := T_{w(a).K}M_a$. Darboux's theorem guarantees the existence of a T-equivariant symplectomorphism of a neighborhood of $w(a).K \in M_a$ onto a neighborhood of $0 \in V_{w(a).K}$. This leads to a local normal form for the moment map.

$$\Phi_Z(Y) = \frac{1}{2}\Omega_{w(a).K}(Z.Y, Y) \quad \forall\, Y \in V_{w(a).K}, Z \in \mathfrak{t}.$$

Here, $\Omega_{w(a).K}$ denotes the symplectic form on the symplectic vector space $V_{w(a).K}$. Since T acts symplectically on $V_{w(a).K}$ the notation $Z.Y$ makes sense as the linear action of an element $Z \in \mathfrak{sp}(V_{w(a).K})$ on a vector $Y \in V_{w(a).K}$. In appropriate symplectic coordinates $q_1, p_1, \ldots, q_n, p_n$ we have $\Omega_{w(a).K} = \sum_i dq_i \wedge dp_i$ and the matrix representation for the linear map defined by $Z \in \mathfrak{t}$ is

$$Z.(q_1, p_1, \ldots, q_n, p_n) = \begin{pmatrix} 0 & \alpha_1(Z) & & & \\ -\alpha(Z) & 0 & & & \\ & & \ddots & & \\ & & & 0 & \alpha_n(Z) \\ & & & -\alpha_n(Z) & 0 \end{pmatrix} \begin{pmatrix} q_1 \\ p_1 \\ \vdots \\ q_n \\ p_n \end{pmatrix}.$$

The moment map takes the form

$$\Phi(q_1, p_1, \ldots, q_n, p_n) = \Phi(w(a).K) + \sum_{i=1}^{n} \alpha_i \frac{1}{2}(q_i^2 + p_i^2).$$

In terms of the symplectic coordinates on $V_{w(a).K}$ chosen above, the matrix representations for the symplectic form $\Omega_{w(a).K}$ and the corresponding Poisson tensor $\Pi_{w(a).K}$ just differ by a factor of (-1). The moment map can then be expressed in terms of the Poisson tensor.

$$\Phi_Z(\varphi) = -\Pi_{w(a).K}(Z.\varphi, \varphi) \qquad \forall\, \varphi \in V^*_{w(a).K}, Z \in \mathfrak{t}.$$

(Recall the bijection $\Pi^\sharp : V^*_{w(a).K} \to V_{w(a).K}$. Then $Z.\varphi = (\Pi^\sharp)^{-1}(Z.(\Pi^\sharp(\varphi)))$, where the dot on the right hand side has been explained above.)
The local cone $\Gamma_{w(X)}$ is just $\Phi(V^*_{w(a).K})$, i.e. it consists exactly of the weights

$$\{\ Z \mapsto -\Pi_{w(a).K}(Z.\varphi, \varphi)\ :\ \varphi \in V^*_{w(a).K}\ \} \tag{5}$$

Recall that we identify the cotangent space $T^*_{w(a).K}(G/K)$ with $Ad(w(a)).\mathfrak{k}$. The formula for the Poisson tensor at $w(a).K$ says that for $Y_1, Y_2 \in \mathfrak{k}$,

$$\Pi_{w(a).K}(Ad(w(a))Y_1, Ad(w(a))Y_2) = \langle pr_{\mathfrak{h}} Ad(w(a))Y_1, Ad(w(a))Y_2\rangle.$$

Note that $T^*_{w(a).K}(G/K) = T^*_{w(a).K}M_a \oplus (T_{w(a).K}M_a)^\perp$. Both $T^*_{w(a).K}M_a$ and $(T_{w(a).K}M_a)^\perp$ are stable under the action of T. Moreover, $T_{w(a).K}M_a = \Pi^\sharp_{w(a).K}(T^*_{w(a).K}(G/K))$ by the definition of the symplectic leaf M_a. Hence, for $\varphi \in T^*_{w(a).K} M_a, \psi \in (T_{a_w} M_{a_w})^\perp$ and $Z \in \mathfrak{t}$, one obtains

$$\begin{aligned}\Pi_{w(a).K}(Z.(\varphi+\psi),(\varphi+\psi)) &= (\varphi+\psi).\Pi^\sharp_{w(a).K}(Z.(\varphi+\psi))\\ &= \varphi.\Pi^\sharp_{w(a).K}(Z(\varphi+\psi))\\ &= \Pi_{w(a).K}(Z\varphi+Z\psi,\varphi)\\ &= -(Z\varphi+Z\psi).\Pi^\sharp_{w(a).K}(\varphi)\\ &= \Pi_{w(a).K}(Z\varphi,\varphi)\end{aligned}$$

In view of (5) and (2) (from Section 3) it follows that the local cone is given by

$$\Gamma_{w(X)} = \{\ Z \mapsto -\langle pr_{\mathfrak{h}}[Z, Ad(w(a))Y], Ad(w(a))Y\rangle \ :\ Y \in \mathfrak{k}\ \}. \tag{6}$$

In order to determine the weights in (6) we will construct a basis $\{v_1,\dots,v_r\}$ for $\mathfrak{k}$ with two main features.

(1) For each v_i we determine explicitly an element $H_i \in \mathfrak{a}^{-\tau}$ such that

$$\langle pr_{\mathfrak{h}}[Z, Ad(w(a))v_i], Ad(w(a))v_i\rangle = \Im\kappa(H_i, Z) \quad \forall\ Z \in \mathfrak{t}.$$

(2) $\langle pr_{\mathfrak{h}}[Z, Ad(w(a))v_i], Ad(w(a))v_j\rangle = 0$ for all $Z \in \mathfrak{t}$ whenever $i \neq j$.

Once such a basis is found each $Y \in \mathfrak{k}$ can be written as a linear combination $Y = \sum_{i=1}^N c_i v_i$. Then, for $Z \in \mathfrak{t}$,

$$\begin{aligned}&\langle pr_{\mathfrak{h}}[Z, Ad(w(a))Y], Ad(w(a))Y\rangle\\ &\qquad = \langle pr_{\mathfrak{h}}[Z, Ad(w(a))\sum_{i=1}^N c_i v_i], Ad(w(a))\sum_{i=1}^N c_i v_i\rangle\\ &\qquad = \sum_{i=1}^N c_i^2 \langle pr_{\mathfrak{h}}[Z, Ad(w(a))v_i], Ad(w(a))v_i\rangle\\ &\qquad = \sum_{i=1}^N c_i^2 \Im\kappa(H_i, Z)\end{aligned}$$

In view of (6) it then follows that $\Gamma_{w(X)}$ is the cone spanned by the vectors H_i. Recall the weight space decomposition of $\mathfrak{g}$ with respect to $\mathfrak{a}^{-\tau}$.

$$\mathfrak{g} = \mathfrak{a}^{-\tau} \oplus \mathfrak{a}^{\tau} \oplus i\mathfrak{a}^{-\tau} \oplus i\mathfrak{a}^{\tau} \oplus \sum_{\beta\in\Delta(\mathfrak{g},\mathfrak{a}^{-\tau})} \mathfrak{g}^\beta$$

Each $\mathfrak{g}^\beta$ is stable under the involution $\theta\tau$, hence decomposes into (+1)- and (−1)-eigenspaces $\mathfrak{g}^\beta = (\mathfrak{g}^\beta)_+ \oplus (\mathfrak{g}^\beta)_-$. We first consider certain bases for $\mathfrak{g}^\beta = (\mathfrak{g}^\beta)_+$ and $\mathfrak{g}^\beta = (\mathfrak{g}^\beta)_-$. Each $\mathfrak{g}^\beta$ is stable under the adjoint action of $\mathfrak{a}^\tau$. For the corresponding weight space decomposition we write

$$\mathfrak{g}^\beta = \sum_{\eta\in\Delta(\mathfrak{g}^\beta,\mathfrak{a}^\tau)} \mathfrak{g}^{\beta,\eta}$$

Note that $\mathfrak{g}^{\beta,\eta}$ is equal to the eigenspace $\mathfrak{g}^{\alpha} \subset \mathfrak{n}$ for $\alpha \in \Delta(\mathfrak{g},\mathfrak{a})$ if and only if $\alpha|_{\mathfrak{a}^{-\tau}} = \beta$ and $\alpha|_{\mathfrak{a}^{\tau}} = \eta$. Also, if $\mathfrak{g}^{\beta,\eta} = \mathfrak{g}^{\alpha}$, then $\beta \in \Delta^+(\mathfrak{g},\mathfrak{a}^{-\tau})$ if and only if $\alpha \in \Delta^+(\mathfrak{g},\mathfrak{a})$. The involutions τ and θ transform the eigenspaces as follows

$$\tau(\mathfrak{g}^{\beta,\eta}) = \mathfrak{g}^{-\beta,\eta}, \quad \theta(\mathfrak{g}^{\beta,\eta}) = \mathfrak{g}^{-\beta,-\eta}, \quad \theta\tau(\mathfrak{g}^{\beta,\eta}) = \mathfrak{g}^{\beta,-\eta}$$

For each eigenspace $\mathfrak{g}^{\beta,\eta}$ fix a vector $X_{\beta,\eta}$ that spans $\mathfrak{g}^{\beta,\eta}$ as a complex vector space. If $\eta \neq 0$ we define

$$A_{\beta,\eta} = X_{\beta,\eta} + \theta\tau X_{\beta,\eta}, \quad B_{\beta,\eta} = X_{\beta,\eta} - \theta\tau X_{\beta,\eta}.$$

We obtain the following (complex) basis for the reduced root space $\mathfrak{g}^{\beta}$

$$\{X_{\beta,0}\} \cup \{A_{\beta,\eta} : \eta \neq 0\} \cup \{B_{\beta,\eta} : \eta \neq 0\}$$

The important feature of this basis is that it consists of eigenvectors of the complex linear involution $\theta\tau$. Indeed, $\theta\tau A_{\beta,\eta} = A_{\beta,\eta}, \theta\tau B_{\beta,\eta} = -B_{\beta,\eta}$ and $X_{\beta,0}$ might be a $(+1)$- or a (-1)-eigenvector of $\theta\tau$. Therefore, a basis for $(\mathfrak{g}^{\beta})_+$ is given by the $A_{\beta,\eta}$'s and possibly $X_{\beta,0}$. A basis for $(\mathfrak{g}^{\beta})_-$ is given by the $B_{\beta,\eta}$'s and possibly $X_{\beta,0}$ (iff it is not contained in $\mathfrak{g}^{\beta} = (\mathfrak{g}^{\beta})_+$).
The desired (real) basis for $\mathfrak{k}$ now consists of a basis for $\mathfrak{z}_{\mathfrak{k}}(\mathfrak{a}) = \mathfrak{z}_{\mathfrak{k}}(\mathfrak{a}^{-\tau}) = i\mathfrak{a}^{-\tau} + i\mathfrak{a}^{\tau}$ and the following set.

$$\begin{aligned} \bigcup_{\beta \in \Delta^+(\mathfrak{g},\mathfrak{a}^{-\tau})} \Big(&\{X_{\beta,0} + \theta X_{\beta,0}\} \cup \{iX_{\beta,0} + \theta iX_{\beta,0}\} \\ &\cup \{A_{\beta,\eta} + \theta A_{\beta,\eta} : \eta \neq 0\} \cup \{iA_{\beta,\eta} + \theta iA_{\beta,\eta} : \eta \neq 0\} \\ &\cup \{B_{\beta,\eta} + \theta B_{\beta,\eta} : \eta \neq 0\} \cup \{iB_{\beta,\eta} + \theta iB_{\beta,\eta} : \eta \neq 0\} \Big) \end{aligned} \tag{7}$$

We can now calculate the weights appearing in (6) for each basis element. We fix $Z = iH \in \mathfrak{t} = i\mathfrak{a}_{-\tau}$. Recall that $a = \exp X$, therefore $w(a) = \exp(w(X))$. First we make two short auxiliary calculations. For a vector $C_{\beta} \in \mathfrak{g}^{\beta}$ which is also a $\theta\tau$-fixed point,

$$\begin{aligned} [Z, Ad(w(a)).(C_{\beta} + \theta C_{\beta})] &= i\beta(H)w(a)^{\beta}C_{\beta} - i\beta(H)w(a)^{-\beta}\theta C_{\beta} \\ &= \beta(H)w(a)^{-\beta}(iC_{\beta} + \theta iC_{\beta}) + \beta(H)(w(a)^{\beta} - w(a)^{-\beta})iC_{\beta} \end{aligned}$$

In the second line, the first summand lies in $\mathfrak{h}$ the second in $\mathfrak{c}^{-\tau} + \mathfrak{n}$. For $D_{\beta} \in \mathfrak{g}^{\beta}$ such that $\theta\tau D_{\beta} = -D_{\beta}$, the $\mathfrak{h} \oplus (\mathfrak{c}^{-\tau} + \mathfrak{n})$ decomposition is different:

$$\begin{aligned} [Z, Ad(w(a)).(D_{\beta} + \theta D_{\beta})] &= i\beta(H)w(a)^{\beta}D_{\beta} - i\beta(H)w(a)^{-\beta}\theta D_{\beta} \\ &= \beta(H)w(a)^{-\beta}(-iD_{\beta} + \theta iD_{\beta}) + \beta(H)(w(a)^{\beta} + w(a)^{-\beta})iD_{\beta} \end{aligned}$$

Now, for $A_{\beta,\eta}$, which lies in $\mathfrak{g}^\beta$ and satisfies $\theta\tau A_{\beta,\eta} = A_{\beta,\eta}$, we compute

$$\begin{aligned}
(8)\quad & \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(A_{\beta,\eta} + \theta A_{\beta,\eta})], Ad(w(a)).(A_{\beta,\eta} + \theta A_{\beta,\eta})\rangle \\
&= \langle \beta(H) w(a)^{-\beta}(iA_{\beta,\eta} + \theta i A_{\beta,\eta}), w(a)^{\beta} A_{\beta,\eta} + w(a)^{-\beta}\theta A_{\beta,\eta}\rangle \\
&= \beta(H) w(a)^{-2\beta}\langle iA_{\beta,\eta}, \theta A_{\beta,\eta}\rangle + \beta(H)\langle \theta i A_{\beta,\eta}, A_{\beta,\eta}\rangle \\
&= (w(a)^{-2\beta} - 1)\ \Re\kappa(A_{\beta,\eta}, \theta A_{\beta,\eta})\ \beta(H) \\
&= (w(a)^{-2\beta} - 1)\ \Re\kappa(A_{\beta,\eta}, \theta A_{\beta,\eta})\ \kappa(H_\beta, H) \\
&= (w(a)^{-2\beta} - 1)\ \Re\kappa(A_{\beta,\eta}, \theta A_{\beta,\eta})\ \Im\kappa(H_\beta, Z)
\end{aligned}$$

We can replace $A_{\beta,\eta}$ with $iA_{\beta,\eta}$ in the above calculation and obtain

$$\begin{aligned}
& \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(iA_{\beta,\eta} + \theta i A_{\beta,\eta})], Ad(w(a)).(iA_{\beta,\eta} + \theta i A_{\beta,\eta})\rangle \\
&\qquad = (w(a)^{-2\beta} - 1)\ \Re\kappa(iA_{\beta,\eta}, \theta i A_{\beta,\eta})\ \beta(H) \\
&\qquad = (w(a)^{-2\beta} - 1)\ \Re\kappa(A_{\beta,\eta}, \theta A_{\beta,\eta})\ \Im\kappa(H_\beta, Z)
\end{aligned}$$

Carrying out the calculation for $B_{\beta,\eta}$ (which are (-1)-eigenvectors of $\theta\tau$) we obtain a result of a different nature

$$\begin{aligned}
(9)\quad & \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(B_{\beta,\eta} + \theta B_{\beta,\eta})], Ad(w(a)).(B_{\beta,\eta} + \theta B_{\beta,\eta})\rangle \\
&\qquad = -(w(a)^{-2\beta} + 1)\ \Re\kappa(B_{\beta,\eta}, \theta B_{\beta,\eta})\ \Im\kappa(H_\beta, Z),
\end{aligned}$$

and

$$\begin{aligned}
& \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(iB_{\beta,\eta} + \theta i B_{\beta,\eta})], Ad(w(a)).(iB_{\beta,\eta} + \theta i B_{\beta,\eta})\rangle \\
&\qquad = -(w(a)^{-2\beta} + 1)\ \Re\kappa(B_{\beta,\eta}, \theta B_{\beta,\eta})\ \Im\kappa(H_\beta, Z).
\end{aligned}$$

If $X_{\beta,0}$ is fixed by $\theta\tau$, then

$$\begin{aligned}
(10)\quad & \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(X_{\beta,0} + \theta X_{\beta,0})], Ad(w(a)).(X_{\beta,0} + \theta X_{\beta,0})\rangle \\
&\qquad = (w(a)^{-2\beta} - 1)\ \Re\kappa(X_{\beta,0}, \theta X_{\beta,0})\ \Im\kappa(H_\beta, Z),
\end{aligned}$$

and

$$\begin{aligned}
& \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(iX_{\beta,0} + \theta i X_{\beta,0})], Ad(w(a)).(iX_{\beta,0} + \theta i X_{\beta,0})\rangle \\
&\qquad = (w(a)^{-2\beta} - 1)\ \Re\kappa(X_{\beta,0}, \theta X_{\beta,0})\ \Im\kappa(H_\beta, Z).
\end{aligned}$$

The case that $\theta\tau X_{\beta,0} = -X_{\beta,0}$ leads to

$$\begin{aligned}
(11)\quad & \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(X_{\beta,0} + \theta X_{\beta,0})], Ad(w(a)).(X_{\beta,0} + \theta X_{\beta,0})\rangle \\
&\qquad = -(w(a)^{-2\beta} + 1)\ \Re\kappa(X_{\beta,0}, \theta X_{\beta,0})\ \Im\kappa(H_\beta, Z),
\end{aligned}$$

and

$$\begin{aligned}
& \langle pr_{\mathfrak{h}}[Z, Ad(w(a)).(iX_{\beta,0} + \theta i X_{\beta,0})], Ad(w(a)).(iX_{\beta,0} + \theta i X_{\beta,0})\rangle \\
&\qquad = -(w(a)^{-2\beta}) + 1)\ \Re\kappa(X_{\beta,0}, \theta X_{\beta,0})\ \Im\kappa(H_\beta, Z).
\end{aligned}$$

Moreover, for $Y \in \mathfrak{z}_{\mathfrak{k}}(\mathfrak{a})$ one easily checks that

$$\langle pr_{\mathfrak{h}}[Z, Ad(w(a)).Y], Ad(w(a)).Y\rangle = 0.$$

Note that the coefficient of $\Im\kappa(H_\beta, Z)$ in (9) and (11) is always positive. Therefore, basis vectors of $\mathfrak{k}$ which are (-1)-eigenvectors of $\theta\tau$ contribute the set $\{-H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_- \neq 0\}$ to $\Gamma_{w(X)}$.
On the other hand, the coefficient of $\Im\kappa(H_\beta, Z)$ in (8) and (10) depends on the value of $\beta(w(X))$. If $\beta(w(X)) = 0$ this coefficient is zero. If $\beta(w(X)) > 0$ the coefficient is positive, and if $\beta(w(X)) < 0$ it is negative. Therefore, basis vectors of $\mathfrak{k}$ which are $(+1)$-eigenvectors of $\theta\tau$ contribute the set $\{-\beta(w(X))H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_+ \neq 0\}$ to $\Gamma_{w(X)}$.
The fact that $\langle pr_{\mathfrak{h}}[Z, Ad(w(a))v_i], Ad(w(a))v_j\rangle = 0$ holds for all $Z \in \mathfrak{t}$ whenever $i \neq j$ follows from general properties of the Killing form.
The conclusion is that the cone $\Gamma_{w(X)} = \Phi(V^*_{w(a).K})$ is generated by the weights

$$\{-\beta(w(X))H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_+ \neq 0\} \\ \cup \{-H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_- \neq 0\},$$

as asserted.

□

Corollary 4.5. *The image of the moment map $\Phi(M_a)$ is contained in the set $w'(X) + \Gamma_+$, where $w' \in \mathcal{W}_{K\cap H}$ is such that $\beta(w'(X)) \geq 0$ for all $\beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau})$ and Γ_+ is the proper cone $\Gamma_+ = \mathrm{cone}(-\mathrm{H}_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}))$.*

Proof. ¿From Theorem 4.1 and Remark 4.2 we know that there is a neighborhood $U_{w'(X)} \subseteq \mathfrak{a}^{-\tau}$ of $w'(X)$ such that $\Phi(M_a) \cap U_{w'(X)} = (w'(X) + \Gamma_{w'(X)}) \cap U_{w'(X)}$. Lemma 4.4 implies that $\Gamma_{w'(X)} \subseteq \Gamma_+$. Suppose there exists some $Z \in \Phi(M_a)$ such that $Z \notin w'(X) + \Gamma_+$. Since $\Phi(M_a)$ is convex the line segment $\overline{w'(X)Z}$ lies entirely in $\Phi(M_a)$. Fix some $Y \in \overline{w'(X)Z} \cap U_{w'(X)}$ with $Y \neq w'(X)$. Then $Y \in \Phi(M_a) \cap U_{w'(X)} \subseteq w'(X) + \Gamma_{w'(X)} \subseteq w'(X) + \Gamma_+$. But this implies $Z \in w'(X) + \Gamma_+$ since Γ_+ is a cone and $Y \neq w'(X)$, a contradiction. Therefore, $\Phi(M_a) \subseteq w'(X) + \Gamma_+$. The cone Γ_+ is proper since it is spanned by vectors $-H_\beta$ associated to positive roots β. □

The special property of $\Phi(M_a)$ stated in the corollary allows us to describe $\Phi(M_a)$ entirely in terms of the local cones $\Gamma_{w(X)}$ associated to the fixed points, as the following proposition shows.

Proposition 4.6. *Let C be a closed, convex, locally polyhedral set (in some finite dimensional vector space V). Denote by Γ_c the local cone at $c \in C$ (i.e. there is a neighborhood $U_c \subset V$ of c such that $C \cap U_c = (c + \Gamma_c) \cap U_c$). Suppose $C \subset x + \Gamma$ for some $x \in V$ and some proper cone $\Gamma \subset V$. Then*

$$C = \bigcap_{\Gamma_c \text{ proper}} (c + \Gamma_c),$$

i.e. C is completely determined by the local cones that are proper.

Proof. For any $c \in C$ we write d_c for the dimension of the maximal subspace contained in Γ_c. (In particular, $d_c = 0$ means that Γ_c is proper.) First we will show that if $d_c > 0$, then $c \in c' + \Gamma_{c'}$ for some c' with $d_{c'} < d_c$.
If $d_c > 0$, then Γ_c contains a line, say L. Since C lies in a proper cone, $(c+L)\cap C$ is semi-bounded. We pick an endpoint c' of $(c+L)\cap C$. Since C is closed $c' \in C$, and clearly $c \in c' + \Gamma_{c'}$. Convexity of C implies that if a line L' is contained in $\Gamma_{c'}$ then $L' \subset \Gamma_{\tilde{c}}$ for each inner point $\tilde{c}$ of $(c+L)\cap C$. In particular, $d_{c'} \leq d_c$. On the other hand, $\Gamma_{c'}$ does not contain the line $L \subset \Gamma_c$. Therefore, $d_{c'} < d_c$.
Now, the assumptions on C imply

$$C = \bigcap_{c \in C} (c + \Gamma_c)$$

If we set $n = \dim(\mathrm{V})$ the above arguments lead to

$$C = \bigcap_{d_c \leq n} (c + \Gamma_c) = \bigcap_{d_c \leq n-1} (c + \Gamma_c) = \cdots = \bigcap_{d_c = 0} (c + \Gamma_c)$$

□

We are now ready to give the desired description of $\Phi(M_a)$ which is the content of van den Ban's theorem.

THEOREM 4.7. *The set $\Phi(M_a) = (pr_{\mathfrak{a}^{-\tau}} \circ \log \circ \mu)(Ha)$ is the sum of a compact convex set and a closed (proper) cone Γ. More precisely, for $a = \exp X$,*

$$\Phi(M_a) = \mathrm{conv}(\mathcal{W}_{K\cap H}.X) + \Gamma,$$

with

$$\Gamma = \mathrm{cone}\{-H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_- \neq 0\}$$

Proof. The image $\Phi(M_a)$ is closed, convex and locally polyhedral. Moreover, by Corollary 4.5, it is contained in $w'(X) + \Gamma_+$ for some proper cone Γ_+. Proposition 4.6 implies that $\Phi(M_a)$ is determined by the local cones that are proper. According to Remark 4.2, a local cone $\Gamma_{\Phi(m)}$ can be proper only if $\mathfrak{t}_m = \mathfrak{t}$, i.e. if m is a T-fixed point. The T-fixed points have been characterized in Proposition 4.3, so Proposition 4.6 yields

$$\Phi(M_a) = \bigcap_{w \in \mathcal{W}_{K\cap H}} (w(X) + \Gamma_{w(X)}),$$

with $\Gamma_{w(X)}$ as in Lemma 4.4.
The sum $\mathrm{conv}(\mathcal{W}_{K\cap H}.X) + \Gamma$ is closed, convex and locally polyhedral as well. As a sum of a compact set and the proper cone Γ it is contained in $x+\Gamma$ for some $x \in \mathfrak{a}^{-\tau}$, hence Proposition 4.6 is applicable. First we want to see at which points in $\mathrm{conv}(\mathcal{W}_{K\cap H}.X)+\Gamma$ the local cone is proper. Let $c \in \mathrm{conv}(\mathcal{W}_{K\cap H}.X)$ and $\gamma \in \Gamma$. Clearly, the local cone at $c+\gamma$ is improper unless $\gamma = 0$. But then $c+\gamma = c$ is contained in a convex set with extremal points $\{w(X) : w \in \mathcal{W}_{K\cap H}\}$. The local cone can be proper only if $c+\gamma$ is one of those extremal points. Proposition 4.6 now gives

$$\mathrm{conv}(\mathcal{W}_{K\cap H}.X) + \Gamma = \bigcap_{w \in \mathcal{W}_{K\cap H}} (w(X) + \Gamma'_{w(X)}).$$

Here, $\Gamma'_{w(X)}$ denotes the local cone of $\mathrm{conv}(\mathcal{W}_{K\cap H}.X)+\Gamma$ at $w(X)$. To finish the proof it is sufficient to show that $\Gamma'_{w(X)} = \Gamma_{w(X)}$.

Clearly, $\Gamma'_{w(X)} = \Gamma''_{w(X)} + \Gamma$, where $\Gamma = \mathrm{cone}\{-H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_- \neq 0\}$ as before and $\Gamma''_{w(X)} = \mathrm{cone}\{w'(X) - w(X) : w' \in \mathcal{W}_{K\cap H}\}$. From Lemma 4.4 we know that $\Gamma_{w(X)}$ contains the cone Γ. Moreover, the set $\Phi(M_a)$ is convex and contains all points $w(X)$, and therefore contains $\mathrm{conv}(\mathcal{W}_{K\cap H}.X)$. This implies that its local cone at $w(X)$, i.e. $\Gamma_{w(X)}$, contains $\Gamma''_{w(X)}$ as well. Therefore, $\Gamma_{w(X)} \supseteq \Gamma''_{w(X)} + \Gamma = \Gamma'_{w(X)}$.

Each root $\beta \in \Delta(\mathfrak{g}, \mathfrak{a}^{-\tau})$ defines the isomorphism

$$s_\beta : \mathfrak{a}^{-\tau} \to \mathfrak{a}^{-\tau}, Z \mapsto Z - 2\frac{\beta Z}{\langle \beta, \beta\rangle} H_\beta.$$

In view of Remark 2.1 the Weyl group $\mathcal{W}' = \mathcal{W}_{K\cap H}$ consists exactly of those s_β for which $(\mathfrak{g}^\beta)_+ \neq 0$. In particular, $s_\beta(w(X)) \in \mathcal{W}_{K\cap H}$ for all $\beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau})$ for which $(\mathfrak{g}^\beta)_+ \neq 0$. The identity $s_\beta(w(X)) - w(X) = -2\frac{\beta(w(X))}{\langle\beta,\beta\rangle} H_\beta$ implies $\mathrm{cone}\{-\beta(w(X))H_\beta : \beta \in \Delta^+(\mathfrak{g}, \mathfrak{a}^{-\tau}), (\mathfrak{g}^\beta)_+ \neq 0\} \subseteq \Gamma''_X$. With Lemma 4.4 we obtain $\Gamma_{w(X)} \subseteq \Gamma''_{w(X)} + \Gamma = \Gamma'_{w(X)}$. □

References

1. Atiyah, M.F., *Convexity and commuting Hamiltonians*, Bull. London Math. Soc. 14 (1) (1982), 1-15.
2. Duistermaat, J.J., *Convexity and tightness for restrictions of Hamiltonian functions to fixed point sets of an antisymplectic involution*, Trans. Amer. Math. Soc. 275 (1) (1983), 417-429.
3. Evens, S., and Lu, J.-H., *On the variety of Lagrangian subalgebras, I*, Ann. Scient. Éc. Norm. Sup. 4 (34) (2001), 631-668.
4. Guillemin, V., and Sternberg, S., *Convexity properties of the moment mapping*, Invent. Math. 67 (3) (1982), 491-513.
5. Helgason, S., *Differential geometry, Lie groups, and symmetric spaces*, Pure and Applied Math. 80, Academic Press, New York-London, 1978.
6. Hilgert, J., and Neeb, K.-H., and Plank, W., *Symplectic Convexity Theorems and Coadjoint orbits*, Compositio Math. 94 (1994), 129-180.
7. Knapp, A., *Lie groups beyond an introduction*, Progress in Mathematics, 140. Birkhäuser Boston, 2002.
8. Lerman, E., Meinrenken, E., Tolman, S., Woodward, C., *Non-abelian convexity by symplectic cuts*, Topology 37 (2) (1998), 245–259.
9. Lu, J.-H., *Poisson homogeneous spaces and Lie algebroids associated to Poisson actions*, Duke Math. J. 86 (2) (1997), 261-303.
10. Lu, J.-H., and Ratiu, T., *On the nonlinear convexity theorem of Kostant*, J. Amer. Math. Soc. 4 (2) (1991), 349-363.
11. Lu, J.-H., and Weinstein, A., *Poisson Lie groups, dressing transformations and Bruhat decompositions*, J. Diff. Geom. 31 (1990), 501-526.
12. Otto, M., *Restriction of the moment map to certain non-Lagrangian submanifolds*, arXiv:math.SG/0609541.

13. Prato, E., *Convexity properties of the moment map for certain non-compact manifolds*, Comm. Anal. Geom. 2 (2) (1994), 267–278.
14. Van den Ban, E.P., *A convexity theorem for semisimple symmetric spaces*, Pacific J. Math. 124 (1) (1986), 21-55.

Philip Foth
Department of Mathematics
University of Arizona
Tucson, AZ 85721-0089
U.S.A.
foth@math.arizona.edu

Michael Otto
Department of Mathematics
University of Arizona
Tucson, AZ 85721-0089
U.S.A.
otto@math.arizona.edu

Volumes of Symmetric Spaces via Lattice Points

Henri Gillet and Daniel R. Grayson

Received: February 15, 2004
Revised: August 2, 2006

Communicated by Ulf Rehmann

Abstract. We show how to use elementary methods to compute the volume of $\mathrm{Sl}_k \mathbb{R}/ \mathrm{Sl}_k \mathbb{Z}$. We compute the volumes of certain unbounded regions in Euclidean space by counting lattice points and then appeal to the machinery of Dirichlet series to get estimates of the growth rate of the number of lattice points appearing in the region as the lattice spacing decreases. We also present a proof of the closely related result that the Tamagawa number is 1.

2000 Mathematics Subject Classification: 11F06, 11H06, 11M45.
Keywords and Phrases: special linear group, volume, lattice, Tauberian theorem, arithmetic group, Tamagawa number.

Introduction

In this paper we show how to use elementary methods to prove that the volume of $\mathrm{Sl}_k \mathbb{R}/ \mathrm{Sl}_k \mathbb{Z}$ is $\zeta(2)\zeta(3)\cdots\zeta(k)/k$; see Corollary 3.16. Using a version of reduction theory presented in this paper, we can compute the volumes of certain unbounded regions in Euclidean space by counting lattice points and then appeal to the machinery of Dirichlet series to get estimates of the growth rate of the number of lattice points appearing in the region as the lattice spacing decreases.

In section 4 we present a proof of the closely related result that the Tamagawa number of $\mathrm{Sl}_{k,\mathbb{Q}}$ is 1 that is somewhat simpler and more arithmetic than Weil's in [37]. His proof proceeds by induction on k and appeals to the Poisson summation formula, whereas the proof here brings to the forefront local versions (5) of the formula, one for each prime p, which help to illuminate the appearance of values of zeta functions in formulas for volumes.

The volume computation above is known; see, for example, [26] (with important corrections in [30]), formula (24) in [29], and Theorem 10.4 in [22]. The methods used in the computation of the volume of $\mathrm{Sl}_k \mathbb{R}/\mathrm{Sl}_k \mathbb{Z}$ in the book [31, Lecture XV] have a different flavor from ours and do not involve counting lattice points. One positive point about the proof there is that it proceeds by induction on k, making clear how the factor $\zeta(k)$ enters in at k-th stage. See also [36, §14.12, formula (2)]. The proof offered there seems to have a gap which consists of assuming that a certain region (denoted by T there) is bounded, thereby allowing the application of [36, §14.4, Theorem 3][1]. The region in Example 2.7 below shows that filling the gap is not easy, hence if we want to compute the volume by counting lattice points, something like our use of reduction theory in Section 3 is needed.

An almost equivalent result was proved by Minkowski in formula (85.) of [16], where he computed the volume of $SO(k)\backslash \mathrm{Sl}_k \mathbb{R}/\mathrm{Sl}_k \mathbb{Z}$. The relationship between the two volume computations is made clear in the proof of [36, §14.12, Theorem 2].

Some of the techniques we use were known to Siegel, who used similar methods in his investigation of representability of integers by quadratic forms in [24, 25, 27]. See especially [25, Hilfssatz 6, p. 242], which is analogous to our Lemma 2.5 and the reduction theory of Section 3, where we show how to compute the volume of certain unbounded domains in Euclidean space by counting lattice points; see also the computations in [24, §9], which have the same general flavor as ours. See also [28, p. 581] where Siegel omits the laborious study, using reduction theory, of points at infinity; it is those details that concern us here.

We thank Harold Diamond for useful information about Dirichlet series and Ulf Rehmann for useful suggestions, advice related to Tamagawa numbers, and clarifications of Siegel's work. We also thank the National Science Foundation for support provided by NSF grants DMS 01-00587 and 05-00762 (Gillet), and 99-70085 and 03-11378 (Grayson).

1 Counting with zeta functions

As in [8] we define the zeta function of a group G by summing over the subgroups H in G of finite index.

$$\zeta(G, s) = \sum_{H \subseteq G} [G : H]^{-s} \tag{1}$$

Evidently, $\zeta(\mathbb{Z}, s) = \zeta(s)$ and the series converges for $s > 1$. For good groups G the number of subgroups of index at most T grows slowly enough as a function of T that $\zeta(G, s)$ will converge for s sufficiently large.

Let's pick $k \geq 0$ and compute $\zeta(\mathbb{Z}^k, s)$. Any subgroup H of $\mathbb{Z}^k$ of finite index is isomorphic to $\mathbb{Z}^k$; choosing such an isomorphism amounts to finding a matrix $A : \mathbb{Z}^k \to \mathbb{Z}^k$ whose determinant is nonzero and whose image is H.

[1] called Dirichlet's Principle in [3, §5.1, Theorem 3]

Any two matrices A, A' with the same image H are related by an equation $A' = AS$ where $S \in \mathrm{Gl}_k \mathbb{Z}$.

Thus the terms in the sum defining $\zeta(\mathbb{Z}^k, s)$ correspond to the orbits for the action of $\mathrm{Gl}_k \mathbb{Z}$ via column operations on the set of $k \times k$-matrices with integer entries and nonzero determinant. A unique representative from each orbit is provided by the matrices A that are in *Hermite normal form* (see [4, p. 66] or [19, II.6]), i.e., those matrices A with $A_{ij} = 0$ for $i > j$, $A_{ii} > 0$ for all i, and $0 \le A_{ij} < A_{ii}$ for $i < j$.

Let HNF be the set of integer $k \times k$ matrices in Hermite normal form. Given positive integers $n_1, \dots, n_k$, consider the set of matrices A in HNF with $A_{ii} = n_i$ for all i. The number of matrices in it is $n_1^{k-1} n_2^{k-2} \cdots n_{k-1}^1 n_k^0$. Using that, we compute formally as follows.

$$\begin{aligned}
\zeta(\mathbb{Z}^k, s) &= \sum_{H \subseteq \mathbb{Z}^k} [\mathbb{Z}^k : H]^{-s} \\
&= \sum_{A \in \mathrm{HNF}} (\det A)^{-s} \\
&= \sum_{n_1 > 0, \dots, n_k > 0} (n_1^{k-1} n_2^{k-2} \cdots n_{k-1}^1 n_k^0)(n_1 \cdots n_k)^{-s} \\
&= \sum_{n_1 > 0, \dots, n_k > 0} n_1^{k-1-s} n_2^{k-2-s} \cdots n_{k-1}^{1-s} n_k^{-s} \\
&= \sum_{n_1 > 0} n_1^{k-1-s} \sum_{n_2 > 0} n_2^{k-2-s} \cdots \sum_{n_{k-1} > 0} n_{k-1}^{1-s} \sum_{n_k > 0} n_k^{-s} \\
&= \zeta(s-k+1)\zeta(s-k+2) \cdots \zeta(s-1)\zeta(s)
\end{aligned} \tag{2}$$

The result $\zeta(s-k+1)\zeta(s-k+2)\cdots\zeta(s-1)\zeta(s)$ is a product of Dirichlet series with positive coefficients that converge for $s > k$, and thus $\zeta(\mathbb{Z}^k, s)$ also converges for $s > k$. This computation is old, and appears in various guises. See, for example: proof 2 of Proposition 1.1 in [8]; Lemma 10 in [15]; formula (1.1) in [32]; page 64 in [23]; formula (5) and the lines following it in [26], where the counting argument is attributed to Eisenstein, and its generalization to number rings is attributed to Hurwitz; and pages 37–38 in [37].

Lemma 1.1. *$\#\{H \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : H] \le T\} \sim \zeta(2)\zeta(3)\cdots\zeta(k)T^k/k$ for $k \ge 1$.*

The right hand side is interpreted as T when $k = 1$. The notation $f(T) \sim g(T)$ means that $\lim_{T\to\infty} f(T)/g(T) = 1$.

Proof. We give two proofs.

The first one is more elementary, and was told to us by Harold Diamond. Writing $\zeta(s-k+1) = \sum n^{k-1} n^{-s}$ and letting $B(T) = \sum_{n \le T} n^{k-1}$ be the corresponding coefficient summatory function we see that $B(T) = T^k/k + O(T^{k-1})$. If $k \ge 3$ we may apply Theorem A.2 to show that the coefficient summatory function for the Dirichlet series $\zeta(s)\zeta(s-k+1)$ behaves as $\zeta(k)T^k/k + O(T^{k-1})$.

Applying it several more times shows that the coefficient summatory function for the Dirichlet series $\zeta(s)\zeta(s-1)\cdots\zeta(s-k+3)\zeta(s-k+1)$ behaves as $\zeta(k)\zeta(k-1)\cdots\zeta(3)T^k/k + O(T^{k-1})$. Applying it one more time we see that the coefficient summatory function for $\zeta(\mathbb{Z}^k, s) = \zeta(s)\cdots\zeta(s-k+1)$ behaves as $\zeta(k)\zeta(k-1)\cdots\zeta(2)T^k/k + O(T^{k-1}\log T)$, which in turn implies the result.

The second proof is less elementary, since it uses a Tauberian theorem. From (2) we know that the rightmost (simple) pole of $\zeta(\mathbb{Z}^k, s)$ occurs at $s = k$, that the residue there is the product $\zeta(2)\zeta(3)\cdots\zeta(k)$, and that Theorem A.4 can be applied to get the result. □

Now we point out a weaker version of lemma 1.1 whose proof is even more elementary.

Lemma 1.2. *If* $T > 0$ *then* $\#\{H \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : H] \le T\} \le T^k$.

Proof. As above, we obtain the following formula.

$$\begin{aligned}\#\{H \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : H] \le T\} &= \#\{A \in \mathrm{HNF} \mid \det A \le T\} \\ &= \sum_{\substack{n_1>0,\ldots,n_k>0 \\ n_1\cdot\cdots\cdot n_k \le T}} n_1^{k-1} n_2^{k-2}\cdots n_{k-1}^1 n_k^0\end{aligned}$$

We use it to prove the desired inequality by induction on k, the case $k = 0$ being clear.

$$\begin{aligned}\#\{H \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : H] \le T\} &= \sum_{n_1=1}^{\lfloor T\rfloor} n_1^{k-1} \sum_{\substack{n_2>0,\ldots,n_k>0 \\ n_2\cdots n_k \le T/n_1}} n_2^{k-2}\cdots n_{k-1}^1 n_k^0 \\ &= \sum_{n_1=1}^{\lfloor T\rfloor} n_1^{k-1}\cdot \#\{H \subseteq \mathbb{Z}^{k-1} \mid [\mathbb{Z}^{k-1} : H] \le T/n_1\} \\ &\le \sum_{n_1=1}^{\lfloor T\rfloor} n_1^{k-1}(T/n_1)^{k-1} \qquad \text{[by induction on } k\text{]} \\ &= \sum_{n_1=1}^{\lfloor T\rfloor} T^{k-1} = \lfloor T\rfloor \cdot T^{k-1} \le T^k\end{aligned}$$

□

2 Volumes

Recall that a bounded subset U of Euclidean space $\mathbb{R}^k$ is said to have *Jordan content* if its volume can be approximated arbitrarily well by unions of boxes contained in it or by unions of boxes containing it, or in other words, that the the characteristic function χ_U is Riemann integrable. Equivalently, the boundary ∂U of U has (Lebesgue) measure zero (see [21, Theorem 105.2, Lemma

105.2, and the discussion above it]). If U is a possibly unbounded subset of $\mathbb{R}^k$ whose boundary has measure zero, its intersection with any ball will have Jordan content.

Now let's consider the Lie group $G = \mathrm{Sl}_k \mathbb{R}$ as a subspace of the Euclidean space $M_k\mathbb{R}$ of $k \times k$ matrices. Siegel defines a Haar measure on G as follows (see page 341 of [29]). Let E be a subset of G. Letting $I = [0,1]$ be the unit interval and considering a number $T > 0$, we may consider the following cones.

$$I \cdot E = \{t \cdot B \mid B \in E, 0 \leq t \leq 1\}$$
$$T \cdot I \cdot E = \{t \cdot B \mid B \in E, 0 \leq t \leq T\}$$
$$\mathbb{R}^+ \cdot E = \{t \cdot B \mid B \in E, 0 \leq t\}$$

Observe that if $B \in T \cdot I \cdot E$, then $0 \leq \det B \leq T^k$.

Definition 2.1. *We say that E is measurable if $I \cdot E$ is, and in that case we define $\mu_\infty(E) = \mathrm{vol}(I \cdot E) \in [0, \infty]$.*

The Jacobian of left or right multiplication by a matrix γ on $M_k\mathbb{R}$ is $(\det B)^k$, so for $\gamma \in \mathrm{Sl}_k \mathbb{R}$ volume is preserved. Thus the measure is invariant under G, by multiplication on either side. According to Siegel, the introduction of such invariant measures on Lie groups goes back to Hurwitz (see [10, p. 546] or [9]).

Let $F \subseteq G$ be the fundamental domain for the action of $\Gamma = \mathrm{Sl}_k \mathbb{Z}$ on the right of G presented in [15, section 7]; it's an elementary construction of a fundamental domain which is a Borel set without resorting to Minkowski's reduction theory. In each orbit they choose the element which is closest to the identity matrix in the standard Euclidean norm on $M_k\mathbb{R} \cong \mathbb{R}^{k^2}$, and ties are broken by ordering $M_k\mathbb{R}$ lexicographically. This set F is the union of an open subset of G (consisting of those matrices with no ties) and a countable number of sets of measure zero.

The intersection of $T \cdot I \cdot F$ with a ball has Jordan content. To establish that, it is enough to show that the measure of the boundary ∂F in G is zero. Suppose $g \in \partial F$. Then it is a limit of points $g_i \notin F$, each of which has another point $g_i h_i$ in its orbit which is at least as close to 1. Here h_i is in $\mathrm{Sl}_k(\mathbb{Z})$ and is not 1. The sequence $i \mapsto g_i h_i$ is bounded, and thus so is the sequence h_i; since $\mathrm{Sl}_k(\mathbb{Z})$ is discrete, that implies that h_i takes only a finite number of values. So we may assume $h_i = h$ is independent of i, and is not 1. By continuity, gh is at least as close to 1 as g is. Now g is also a limit of points f_i in F, each of which has $f_i h$ not closer to 1 than f_i is. Hence gh is not closer to 1 than g is, by continuity. Combining, we see that gh and g are equidistant from 1. The locus of points g in $\mathrm{Sl}_k(\mathbb{R})$ such that gh and g are equidistant from 1 is given by the vanishing of a nonzero quadratic polynomial, hence has measure zero. The boundary ∂F is contained in a countable number of such sets, because $\mathrm{Sl}_k(\mathbb{Z})$ is countable, hence has measure zero, too.

We remark that HNF contains a unique representative for each orbit of the action of $\mathrm{Sl}_k \mathbb{Z}$ on $\{A \in M_k\mathbb{Z} \mid \det A > 0\}$. The same is true for $\mathbb{R}^+ \cdot F$.

Restricting our attention to matrices B with $\det B \le T^k$ we see that $\#(T \cdot I \cdot F \cap M_k\mathbb{Z}) = \#\{A \in \mathrm{HNF} \mid \det A \le T^k\}$.

Warning: HNF is not contained in $\mathbb{R}^+ \cdot F$. To convince yourself of this, consider the matrix $A = \begin{pmatrix} 5 & -8 \\ 3 & 5 \end{pmatrix}$ of determinant 49. Column operations with integer coefficients reduce it to $B = \begin{pmatrix} 49 & 18 \\ 0 & 1 \end{pmatrix}$, but $(1/7)A$ is closer to the identity matrix than $(1/7)B$ is, so $B \in HNF$, but $B \notin \mathbb{R}^+ \cdot F$.

We want to approximate the volume of $T \cdot I \cdot F$ by counting the lattice points it contains, i.e., by using the number $\#(T \cdot I \cdot F \cap M_k\mathbb{Z})$, at least when T is large. Alternatively, we may use $\#(I \cdot F \cap r \cdot M_k\mathbb{Z})$, when r is small.

DEFINITION 2.2. *Suppose U is a subset of $\mathbb{R}^n$. Let*

$$N_r(U) = r^n \cdot \#\{U \cap r \cdot \mathbb{Z}^n\}$$

and let

$$\mu_{\mathbb{Z}}(U) = \lim_{r \to 0} N_r(U),$$

if the limit exists, possibly equal to $+\infty$. An equation involving $\mu_{\mathbb{Z}}(U)$ is to be regarded as true only if the limit exists.

LEMMA 2.3. $\mu_{\mathbb{Z}}(I \cdot F) = \zeta(2)\zeta(3)\cdots\zeta(k)/k$

Proof. We replace r above with $1/T$:

$$\begin{aligned} \mu_{\mathbb{Z}}(I \cdot F) &= \lim_{T \to \infty} T^{-k^2} \cdot \#(T \cdot I \cdot F \cap M_k\mathbb{Z}) \\ &= \lim_{T \to \infty} T^{-k^2} \cdot \#\{A \in \mathrm{HNF} \mid \det A \le T^k\} \\ &= \lim_{T \to \infty} T^{-k^2} \cdot \#\{H \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : H] \le T^k\} \\ &= \zeta(2)\zeta(3)\cdots\zeta(k)/k \qquad \text{[using lemma 1.1]} \end{aligned}$$

□

LEMMA 2.4. *If U is a bounded subset of $\mathbb{R}^n$ with Jordan content, then $\mu_{\mathbb{Z}}(U) = \operatorname{vol} U$.*

Proof. Subdivide $\mathbb{R}^n$ into cubes of width r (and of volume r^n) centered at the points of $r\mathbb{Z}^n$. The number $\#\{U \cap r \cdot \mathbb{Z}^n\}$ lies between the number of cubes contained in U and the number of cubes meeting U, so $r^n \cdot \#\{U \cap r \cdot \mathbb{Z}^n\}$ is captured between the total volume of the cubes contained in U and the total volume of the cubes meeting U, hence approaches the same limit those two quantities do, namely $\operatorname{vol} U$. □

LEMMA 2.5. *Let B_R be the ball of radius $R > 0$ centered at the origin, and let U be a subset of $\mathbb{R}^n$ whose boundary has measure zero.*

1. *For all R, the quantity $\mu_{\mathbb{Z}}(U)$ exists if and only if $\mu_{\mathbb{Z}}(U - B_R)$ exists, and in that case, $\mu_{\mathbb{Z}}(U) = \mathrm{vol}(U \cap B_R) + \mu_{\mathbb{Z}}(U - B_R)$.*
2. *If $\mu_{\mathbb{Z}}(U)$ exists then $\mu_{\mathbb{Z}}(U) = \mathrm{vol}(U) + \lim_{R\to\infty} \mu_{\mathbb{Z}}(U - B_R)$.*
3. *If $\mathrm{vol}(U) = +\infty$, then $\mu_{\mathbb{Z}}(U) = +\infty$.*
4. *If $\lim_{R\to\infty} \limsup_{r\to 0} N_r(U - B_R) = 0$, then $\mu_{\mathbb{Z}}(U) = \mathrm{vol}(U)$.*

Proof. Writing $U = (U \cap B_R) \cup (U - B_R)$ we have

$$N_r(U) = N_r(U \cap B_R) + N_r(U - B_R).$$

For each $R > 0$, the set $U \cap B_R$ is a bounded set with Jordan content, and thus lemma 2.4 applies to it. We deduce that

$$\liminf_{r\to 0} N_r(U) = \mathrm{vol}(U \cap B_R) + \liminf_{r\to 0} N_r(U - B_R)$$

and

$$\limsup_{r\to 0} N_r(U) = \mathrm{vol}(U \cap B_R) + \limsup_{r\to 0} N_r(U - B_R),$$

from which we can deduce (1), because $\mathrm{vol}(U \cap B_R) < \infty$. We deduce (2) from (1) by taking limits. Letting $R \to \infty$ in the equalities above we see that

$$\liminf_{r\to 0} N_r(U) = \mathrm{vol}(U) + \lim_{R\to\infty} \liminf_{r\to 0} N_r(U - B_R)$$

and

$$\limsup_{r\to 0} N_r(U) = \mathrm{vol}(U) + \lim_{R\to\infty} \limsup_{r\to 0} N_r(U - B_R),$$

in which some of the terms might be $+\infty$. Now (3) follows from $\liminf_{r\to 0} N_r(U) \geq \mathrm{vol}(U)$, and (4) follows because if

$$\lim_{R\to\infty} \limsup_{r\to 0} N_r(U - B_R) = 0,$$

then

$$\lim_{R\to\infty} \liminf_{r\to 0} N_r(U - B_R) = 0$$

also. □

LEMMA 2.6. *If U is a subset of $\mathbb{R}^n$ whose boundary has measure zero, and $\mu_{\mathbb{Z}}(U) = \mathrm{vol}(U)$, then $\mathrm{vol}(T \cdot U) \sim \#(T \cdot U \cap \mathbb{Z}^n)$ as $T \to \infty$.*

Proof. The statement follows immediately from the definitions. □

Care is required in trying to compute the volume of $I \cdot F$ by counting lattice points in it, for it is not a bounded set (even for $k = 2$, because $\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \in F$).

Example 2.7. It's easy to construct an unbounded region where counting lattice points does not determine the volume, by concentrating infinitely many very thin spikes along rays of rational slope with small numerator and denominator. Consider, for example, a bounded region B in $\mathbb{R}^2$ with Jordan content and nonzero area $v = \operatorname{vol} B$, for which (by Lemma 2.4) $\mu_{\mathbb{Z}} B = \operatorname{vol} B$. Start by replacing B by its intersection B' with the lines through the origin of rational (or infinite) slope – this doesn't change the value of $\mu_{\mathbb{Z}}$, because every lattice point is contained in a line of rational slope, but now the boundary $\partial B'$ does not have measure zero. To repair that, we enumerate the lines $M_1, M_2, \dots$ through the origin of rational slope, and for each $i = 1, 2, 3, \dots$ we replace $R_i = B \cap M_i$ by a suitably scaled and rotated version L_i of it contained in the line N_i of slope i through the origin, with scaling factor chosen precisely so L_i intersects each $r \cdot \mathbb{Z}^2$ in the same number of points as does R_i, for every $r > 0$. The scaling factor is the ratio of the lengths of the shortest lattice points in the lines M_i and N_i. The union $L = \bigcup L_i$ has $\mu_{\mathbb{Z}} L = \mu_{\mathbb{Z}} B = v \neq 0$, but it and its boundary have measure zero.

3 Reduction Theory

In this section we apply reduction theory to show that the volume of $I \cdot F$ can be computed by counting lattice points.

We introduce a few basic notions about lattices. For a more leisurely introduction see [7].

Definition 3.1. *A lattice is a free abelian group L of finite rank equipped with an inner product on the vector space $L \otimes \mathbb{R}$.*

We will regard $\mathbb{Z}^k$ or one of its subgroups as a lattice by endowing it with the standard inner product on $\mathbb{R}^k$.

Definition 3.2. *If L is a lattice, then a sublattice $L' \subseteq L$ is a subgroup with the induced inner product. The quotient L/L', if it's torsion free, is made into a lattice by equipping it with the inner product on the orthogonal complement of L'.*

There's a way to handle lattices with torsion, but we won't need them.

Definition 3.3. *If L is a lattice, then* $\operatorname{covol} L$ *denotes the volume of a fundamental domain for L acting on $L \otimes \mathbb{R}$.*

The covolume can be computed as $|\det(\theta v_1, \cdots, \theta v_k)|$, where $\theta : L \otimes \mathbb{R} \to \mathbb{R}^k$ is an isometry, $\{v_1, \dots, v_k\}$ is a basis of L, and $(\theta v_1, \dots, \theta v_k)$ denotes the matrix whose i-th column is θv_i. We have the identity $\operatorname{covol}(L) = \operatorname{covol}(L') \cdot \operatorname{covol}(L/L')$ when L/L' is torsion free.

If L is a subgroup of $\mathbb{Z}^k$ of finite index, then $\operatorname{covol} L = [\mathbb{Z}^k : L]$.

Definition 3.4. *If L is a nonzero lattice, then* $\min L$ *denotes the smallest length of a nonzero vector in L.*

If L is a lattice of rank 1, then $\min L = \operatorname{covol} L$.

Proposition 3.5. *For any natural number $k > 0$, there is a constant c such that for any $S \geq 1$ and for any $T > 0$ the following inequality holds.*

$$cS^{-k}T^{k^2} \geq \#\{L \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : L] \leq T^k \text{ and } \min L \leq T/S\}.$$

Proof. For $k = 1$ we may take $c = 2$, so assume $k \geq 2$. Letting N be the number of these lattices L, we bound N by picking within each L a nonzero vector v of minimal length, and counting the pairs (v, L) instead. For each v occurring in such pair we write v in the form $v = n_1 v_1$ where $n_1 \in \mathbb{N}$ and v_1 is a primitive vector of $\mathbb{Z}^k$, and then we extend $\{v_1\}$ to a basis $B = \{v_1, \ldots, v_k\}$ of $\mathbb{Z}^k$. We count the lattices L occurring in such pairs with v by putting a basis C for L into Hermite normal form with respect to B, i.e., it will have the form $C = \{n_1 v_1, A_{12} v_1 + n_2 v_2, \ldots, A_{1k} v_1 + \cdots + A_{k-1,k} v_{k-1} + n_k v_k\}$, with $n_i > 0$ and $0 \leq A_{ij} < n_i$. Notice that n_1 has been determined in the previous step by the choice of v. The number of vectors $v \in \mathbb{Z}^k$ satisfying $\|v\| \leq T/S$ is bounded by a number of the form $c(T/S)^k$; for c we may take a large enough multiple of the volume of the unit ball. With notation as above, and counting the bases for C in Hermite normal form as before, we see that

$$\begin{aligned}
N &\leq \sum_{\|v\| \leq T/S} \sum_{\substack{n_2 > 0, \ldots, n_k > 0 \\ n_1 \cdots n_k \leq T^k}} n_1^{k-1} n_2^{k-2} \cdots n_{k-1}^1 n_k^0 \\
&= \sum_{\|v\| \leq T/S} n_1^{k-1} \sum_{\substack{n_2 > 0, \ldots, n_k > 0 \\ n_2 \cdots n_k \leq T^k/n_1}} n_2^{k-2} \cdots n_{k-1}^1 n_k^0 \\
&= \sum_{\|v\| \leq T/S} n_1^{k-1} \cdot \#\{H \subseteq \mathbb{Z}^{k-1} \mid [\mathbb{Z}^{k-1} : H] \leq T^k/n_1\} \\
&\leq \sum_{\|v\| \leq T/S} n_1^{k-1} (T^k/n_1)^{k-1} \qquad \text{[by Lemma 1.2]} \\
&= \sum_{\|v\| \leq T/S} T^{k(k-1)} \\
&\leq c(T/S)^k T^{k(k-1)} \\
&= cS^{-k} T^{k^2}.
\end{aligned}$$

□

Corollary 3.6. *The following equality holds.*

$$0 = \lim_{S \to \infty} \limsup_{T \to \infty} T^{-k^2} \cdot \#\{L \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : L] \leq T^k \text{ and } \min L \leq T/S\}$$

The following two lemmas are standard facts. Compare them, for example, with [2, 1.4 and 1.5].

Lemma 3.7. *Let L be a lattice and let $v \in L$ be a primitive vector. Let $\bar{L} = L/\mathbb{Z}v$, let $\bar{w} \in \bar{L}$ be any vector, and let $w \in L$ be a vector of minimal length among all those that project to $\bar{w}$. Then $\|w\|^2 \leq \|\bar{w}\|^2 + (1/4)\|v\|^2$.*

Proof. The vectors w and $w \pm v$ project to $\bar{w}$, so $\|w\|^2 \leq \|w \pm v\|^2 = \|w\|^2 + \|v\|^2 \pm 2\langle w, v\rangle$, and thus $|\langle w, v\rangle| \leq (1/2)\|v\|^2$. We see then that

$$\begin{aligned} \|\bar{w}\|^2 &= \|w - \frac{\langle w, v\rangle}{\|v\|^2} v\|^2 \\ &= \|w\|^2 - \frac{\langle w, v\rangle^2}{\|v\|^2} \\ &\geq \|w\|^2 - \frac{1}{4}\|v\|^2. \end{aligned}$$

□

Lemma 3.8. *Let L be a lattice of rank 2 with a nonzero vector $v \in L$ of minimal length. Let $L' = \mathbb{Z}v$ and $L'' = L/L'$. Then $\operatorname{covol} L'' \geq (\sqrt{3}/2) \operatorname{covol} L'$.*

Proof. Let $\bar{w} \in L''$ be a nonzero vector of minimal length, and lift it to a vector $w \in L$ of minimal length among possible liftings. By lemma 3.7 $\|w\|^2 \leq \|\bar{w}\|^2 + (1/4)\|v\|^2$. Combining that with $\|v\|^2 \leq \|w\|^2$ we deduce that $\operatorname{covol} L'' = \|\bar{w}\| \geq (\sqrt{3}/2)\|v\| = (\sqrt{3}/2) \operatorname{covol} L'$. □

Definition 3.9. *If L is a lattice, then* $\operatorname{minbasis} L$ *denotes the smallest value possible for $(\|v_1\|^2 + \cdots + \|v_k\|^2)^{1/2}$, where $\{v_1, \ldots, v_k\}$ is a basis of L.*

Proposition 3.10. *Given $k \in \mathbb{N}$ and $S \geq 1$, for all $R \gg 0$, for all $T > 0$, and for all lattices L of rank k with* $\operatorname{covol} L \leq T^k$, *if* $\operatorname{minbasis} L \geq RT$ *then* $\min L \leq T/S$.

Proof. We show instead the contrapositive: provided $\operatorname{covol} L \leq T^k$, if $\min L > T/S$ then $\operatorname{minbasis} L < RT$. There is an obvious procedure for producing an economical basis of a lattice L, namely: we let v_1 be a nonzero vector in L of minimal length; we let v_2 be a vector in L of minimal length among those projecting onto a nonzero vector in $L/(\mathbb{Z}v_1)$ of minimal length; we let v_3 be a vector in L of minimal length among those projecting onto a vector in $L/(\mathbb{Z}v_1)$ of minimal length among those projecting onto a nonzero vector in $L/(\mathbb{Z}v_1 + \mathbb{Z}v_2)$ of minimal length; and so on. A vector of minimal length is primitive, so one can show by induction that the quotient group $L/(\mathbb{Z}v_1 + \cdots + \mathbb{Z}v_i)$ is torsion free; the case where $i = k$ tells us that $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_k$. Let $L_i = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_i$, and let $\alpha_i = \operatorname{covol}(L_i/L_{i-1})$, so that $\alpha_1 = \|v_1\| = \min L > T/S$.

Applying Lemma 3.8 to the rank 2 lattice L_i/L_{i-2} shows that $\alpha_i \geq A\alpha_{i-1}$, where $A = \sqrt{3}/2$, and repeated application of Lemma 3.7 shows that $\|v_i\|^2 \leq$

$\alpha_i^2 + (1/4)(\alpha_{i-1}^2 + \cdots + \alpha_1^2)$, so of course $\|v_i\|^2 \leq (1/4)(\alpha_k^2 + \cdots + \alpha_{i+1}^2) + \alpha_i^2 + (1/4)(\alpha_{i-1}^2 + \cdots + \alpha_1^2)$. We deduce that

$$\operatorname{minbasis} L \leq (\sum_{i=1}^{k} \|v_i\|^2)^{1/2} \leq \left(\frac{k+3}{4} \sum \alpha_i^2\right)^{1/2}. \tag{3}$$

Going a bit further, we see that

$$\begin{aligned} T^k &\geq \operatorname{covol} L \\ &= \alpha_1 \cdots \alpha_k \\ &\geq A^{0+1+2+\cdots+(i-2)} \alpha_1^{i-1} \cdot A^{0+1+2+\cdots+(k-i)} \alpha_i^{k-i+1} \\ &> c_1 (T/S)^{i-1} \alpha_i^{k-i+1} \end{aligned}$$

where c_1 is some constant depending on S which we may take to be independent of i. Dividing through by T^{i-1} we get $T^{k-i+1} > c_2 \alpha_i^{k-i+1}$, from which we deduce that $T > c_3 \alpha_i$, where c_2 and c_3 are new constants (depending only on S). Combining these latter inequalities for each i, we find that $(((k+3)/4) \sum \alpha_i^2)^{1/2} < RT$, where R is a new constant (depending only on S); combining that with (3) yields the result. □

Corollary 3.11. *The following equality holds.*

$$0 = \lim_{R\to\infty} \limsup_{T\to\infty} T^{-k^2} \cdot \#\{L \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : L] \leq T^k \text{ and } \operatorname{minbasis} L \geq RT\}$$

Proof. Combine (3.6) and (3.10). □

If in the definition of our fundamental domain F we had taken the smallest element of each orbit, rather than the one nearest to 1, we would have been almost done now. The next lemma takes care of that discrepancy.

Definition 3.12. *If L is a (discrete) lattice of rank k in $\mathbb{R}^k$, then* $\operatorname{size} L$ *denotes the value of* $(\|w_1\|^2 + \cdots + \|w_k\|^2)^{1/2}$*, where* $\{w_1, \ldots, w_k\}$ *is the (unique) basis of L satisfying* $(w_1, \ldots, w_k) \in \mathbb{R}^+ \cdot F$.

Lemma 3.13. *For any (discrete) lattice $L \subseteq \mathbb{R}^k$ of rank k the inequalities*

$$\operatorname{minbasis} L \leq \operatorname{size} L \leq \operatorname{minbasis} L + 2\sqrt{k}(\operatorname{covol} L)^{1/k}$$

hold.

Proof. Let $\{v_1, \ldots, v_k\}$ be the basis envisaged in the definition of $\operatorname{minbasis} L$, let $\{w_1, \ldots, w_k\}$ be the basis of L envisaged the definition of $\operatorname{size} L$, and let $U = (\operatorname{covol} L)^{1/k} = (\det(v_1, \ldots, v_k))^{1/k} = (\det(w_1, \ldots, w_k))^{1/k}$. The following chain of inequalities gives the result.

$$\begin{aligned} \operatorname{minbasis} L &= \|(v_1, \ldots, v_k)\| \leq \operatorname{size} L \\ &= \|(w_1, \ldots, w_k)\| \leq \|(w_1, \ldots, w_k) - U \cdot 1_k\| + U\sqrt{k} \\ &\leq \|(v_1, \ldots, v_k) - U \cdot 1_k\| + U\sqrt{k} \\ &\leq \|(v_1, \ldots, v_k)\| + 2U\sqrt{k} = \operatorname{minbasis} L + 2U\sqrt{k} \end{aligned}$$

□

Corollary 3.14. *The following equality holds.*

$$0 = \lim_{Q\to\infty} \limsup_{T\to\infty} T^{-k^2} \cdot \#\{L \subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : L] \le T^k \text{ and } \operatorname{size} L \ge QT\}$$

Proof. It follows from (3.13) that given $R > 0$, for all $Q \gg 0$ (namely $Q \ge R + 2\sqrt{k}$) if $\operatorname{covol} L \le T^k$ and $\operatorname{size} L \ge QT$ then $\operatorname{minbasis} L \ge RT$. Now apply (3.11). □

Theorem 3.15. $\operatorname{vol}(I \cdot F) = \mu_{\mathbb{Z}}(I \cdot F)$.

Proof. Observe that $\#\{L \subseteq \mathbb{Z}^k \mid \operatorname{covol} L \le T^k \text{ and } \operatorname{size} L \ge QT\} = \#((T \cdot I \cdot F - B_{QT}) \cap M_k\mathbb{Z}) = \#((I \cdot F - B_Q) \cap T^{-1}M_k\mathbb{Z})$, so replacing $1/T$ by r, Corollary 3.14 implies that $\lim_{Q\to\infty} \limsup_{r\to 0} N_r(I \cdot F - B_Q) = 0$, which allows us to apply Lemma 2.5 (4). □

The theorem allows us to compute the volume of F arithmetically, simultaneously showing it's finite.

Corollary 3.16. $\mu_\infty(G/\Gamma) = \zeta(2)\zeta(3)\cdots\zeta(k)/k$

Proof. Combine the theorem with lemma 2.3 as follows.

$$\mu_\infty(G/\Gamma) = \mu_\infty(F) = \operatorname{vol}(I \cdot F) = \mu_{\mathbb{Z}}(I \cdot F) = \zeta(2)\zeta(3)\cdots\zeta(k)/k$$

□

Remark 3.17. *Theorem 10.4 in [22] states that the volume of G/Γ is $\zeta(2)\zeta(3)\cdots\zeta(k)\sqrt{k}$. The difference arises from a different choice of Haar measure on G. Theirs assigns volume $\sqrt{k}$ to $\mathfrak{sl}_k(\mathbb{R})/\,\mathfrak{sl}_k(\mathbb{Z})$, whereas ours assigns volume $1/k$ to it, as we see in formula (14) below. The ambiguity is unavoidable, because there is no canonical choice of Haar measure. (The Tamagawa number resolves that ambiguity.)*

4 p-adic volumes

In this section we reformulate the computation of the volume of G/Γ to yield a natural and informative computation of the Tamagawa number of Sl_k. We are interested in the form of the proof, not its length, so we incorporate the proofs of (3.16) and (2) rather than their statements. The standard source for information about p-adic measures and Tamagawa measures is Chapter II of [37], and the proof we simplify occurs there in sections 3.1 through 3.4. See also [11] and [20].

We let μ_p denote the standard translation invariant measure on $\mathbb{Q}_p$ normalized so that $\mu_p(\mathbb{Z}_p) = 1$. Let μ_p also denote the product measure on the ring of k by k matrices, $M_k(\mathbb{Q}_p)$. Observe that $\mu_p(M_k(\mathbb{Z}_p)) = 1$.

For $x \in \mathbb{Q}_p$, let $|x|_p$ denote the standard valuation normalized so that $|p|_p = 1/p$

If $A \in M_k(\mathbb{Q}_p)$ and $U \subseteq \mathbb{Q}_p^k$, then $\mu_p(A \cdot U) = |\det A|_p \cdot \mu_p(U)$. (To prove this, first diagonalize A using row and column operations, and then assume that U is a cube.) It follows that if $V \subseteq M_k(\mathbb{Q}_p)$, then $\mu_p(A \cdot V) = |\det A|_p^k \cdot \mu_p(V)$.

Consider $\mathrm{Gl}_k(\mathbb{Z}_p)$ as an open subset of $M_k(\mathbb{Z}_p)$. The following computation occurs on page 31 of [37].

$$\begin{aligned}\mu_p(\mathrm{Gl}_k(\mathbb{Z}_p)) &= \#(\mathrm{Gl}_k(\mathbb{F}_p))/p^{k^2} \\ &= (p^k-1)(p^k-p)\cdots(p^k-p^{k-1})/p^{k^2} \\ &= (1-p^{-k})(1-p^{-k+1})\cdots(1-p^{-1})\end{aligned} \tag{4}$$

Weil considers the open set $M_k(\mathbb{Z}_p)^* = \{A \in M_k(\mathbb{Z}_p) \mid \det A \neq 0\}$.

Lemma 4.1. $\mu_p(M_k(\mathbb{Z}_p)^*) = 1$

Proof. Let $Z = M_k(\mathbb{Z}_p) \setminus M_k(\mathbb{Z}_p)^*$ be the set of singular matrices. If $A \in Z$, then one of the columns of A is a linear combination of the others. (This depends on $\mathbb{Z}_p$ being a discrete valuation ring – take any linear dependency with coefficients in $\mathbb{Q}_p$ and multiply the coefficients by a suitable power of p to put all of them in $\mathbb{Z}_p$, with at least one of them being invertible.) For each $n \geq 0$ we can get an upper bound for the number of equivalence classes of elements of Z modulo p^n by enumerating the possibly dependent columns, the possible vectors in the other columns, and the possible coefficients in the linear combination: $\mu_p(Z) \leq \lim_{n\to\infty} k \cdot (p^{nk})^{k-1} \cdot (p^n)^{k-1}/(p^n)^{k^2} = \lim_{n\to\infty} k \cdot p^{-n} = 0$. □

We call rank k submodules J of $\mathbb{Z}_p^k$ *lattices*. To each $A \in M_k(\mathbb{Z}_p)^*$ we associate the lattice $J = A\mathbb{Z}_p^k \subseteq \mathbb{Z}_p^k$. This sets up a bijection between the lattices J and the orbits of $\mathrm{Gl}_k(\mathbb{Z}_p)$ acting on $M_k(\mathbb{Z}_p)^*$. The measure of the orbit corresponding to J is $\mu_p(A \cdot \mathrm{Gl}_k(\mathbb{Z}_p)) = |\det A|_p^k \cdot \mu_p(\mathrm{Gl}_k(\mathbb{Z}_p)) = [\mathbb{Z}_p^k : J]^{-k} \cdot \mu_p(\mathrm{Gl}_k(\mathbb{Z}_p))$. Now we sum over the orbits.

$$\begin{aligned}1 &= \mu_p(M_k(\mathbb{Z}_p)^*) \\ &= \sum_J \Big([\mathbb{Z}_p^k : J]^{-k} \cdot \mu_p(\mathrm{Gl}_k(\mathbb{Z}_p))\Big) \\ &= \Big(\sum_J [\mathbb{Z}_p^k : J]^{-k}\Big) \cdot \mu_p(\mathrm{Gl}_k(\mathbb{Z}_p))\end{aligned} \tag{5}$$

An alternative way to prove (5) would be to use the local analogue of (2), which holds and asserts that $\sum_J [\mathbb{Z}_p^k : J]^{-s} = (1-p^{k-1-s})^{-1}(1-p^{k-2-s})^{-1}\cdots(1-p^{-s})^{-1}$; we could substitute k for s and compare with the number in (4). The approach via lemma 4.1 and (5) is preferable because $M_k(\mathbb{Z}_p)^*$ provides natural glue that makes the computation seem more natural.

The product $\prod_p \mu_p(\mathrm{Gl}_k(\mathbb{Z}_p))$ doesn't converge because $\prod_p(1-p^{-1})$ doesn't converge, so consider the following formula instead.

$$1 = \Big((1-p^{-1})\sum_J [\mathbb{Z}_p^k : J]^{-k}\Big) \cdot \Big((1-p^{-1})^{-1}\mu_p(\mathrm{Gl}_k(\mathbb{Z}_p))\Big)$$

Now we can multiply these formulas together.

$$1 = \Big(\prod_p (1-p^{-1})\sum_J [\mathbb{Z}_p^k : J]^{-k}\Big) \cdot \prod_p \Big((1-p^{-1})^{-1}\mu_p(\mathrm{Gl}_k(\mathbb{Z}_p))\Big) \qquad (6)$$

We've parenthesized the formula above so it has one factor for each place of $\mathbb{Q}$, and now we connect each of them with a volume involving Sl_k at that place.

We use the Haar measure on $\mathrm{Sl}_k(\mathbb{Z}_p)$ normalized to have total volume

$$\#\,\mathrm{Sl}_k(\mathbb{F}_p)/p^{\dim \mathrm{Sl}_k}.$$

The normalization anticipates (13), which shows how a gauge form could be used to construct the measure, or alternatively, it ensures that the exact sequence $1 \to \mathrm{Sl}_k(\mathbb{Z}_p) \to \mathrm{Gl}_k(\mathbb{Z}_p) \to \mathbb{Z}_p^\times \to 1$ of groups leads to the desired assertion $\mu_p(\mathrm{Gl}_k(\mathbb{Z}_p)) = \mu_p(\mathbb{Z}_p^\times) \cdot \mu_p(\mathrm{Sl}_k(\mathbb{Z}_p))$ about multiplicativity of measures. We rewrite the factor of the right hand side of (6) corresponding to the prime p as follows.

$$\begin{aligned}(1-p^{-1})^{-1}\mu_p(\mathrm{Gl}_k(\mathbb{Z}_p)) &= \mu_p(\mathbb{Z}_p^\times)^{-1} \cdot \mu_p(\mathrm{Gl}_k(\mathbb{Z}_p)) \\ &= \mu_p(\mathrm{Sl}_k(\mathbb{Z}_p)).\end{aligned} \qquad (7)$$

To evaluate the left hand factor of the right hand side of (6), we insert the complex variable s. Because the ring $\mathbb{Z}$ is a principal ideal domain, any finitely generated sub-$\mathbb{Z}$-module $H \subseteq \mathbb{Z}^k$ is free. Hence a lattice $H \subseteq \mathbb{Z}^k$ is determined freely by its localizations $H_p = H \otimes_{\mathbb{Z}} \mathbb{Z}_p \subseteq \mathbb{Z}_p^k$ (where $H_p = \mathbb{Z}_p^k$ for all but finitely many p), and its index is given by the formula

$$[\mathbb{Z}^k : H] = \prod_p [\mathbb{Z}_p^k : H_p], \qquad (8)$$

in which only a finite number of terms are not equal to 1.

$$
\begin{aligned}
&\operatorname{res}_{s=k}\zeta(\mathbb{Z}^k, s)\\
&\qquad = \operatorname{res}_{s=k}\sum_H [\mathbb{Z}^k : H]^{-s} \qquad \text{[by (1)]}\\
&\qquad = \lim_{s\to k+} \zeta(s-k+1)^{-1}\cdot \sum_H [\mathbb{Z}^k : H]^{-s}\\
&\qquad = \lim_{s\to k+} \Big(\zeta(s-k+1)^{-1}\big(\sum_{H\subseteq \mathbb{Z}^k}\prod_p [\mathbb{Z}_p^k : H_p]^{-s}\big)\Big) \qquad \text{[by (8)]}\\
&\qquad = \lim_{s\to k+} \Big(\zeta(s-k+1)^{-1}\big(\prod_p \sum_{J\subseteq \mathbb{Z}_p^k} [\mathbb{Z}_p^k : J]^{-s}\big)\Big) \qquad \text{[positive terms]}\\
&\qquad = \lim_{s\to k+} \prod_p \big((1-p^{-s+k-1})\sum_J [\mathbb{Z}_p^k : J]^{-s}\big)\\
&\qquad = \prod_p (1-p^{-1})\sum_J [\mathbb{Z}_p^k : J]^{-k}
\end{aligned}
\tag{9}
$$

Starting again we get the following chain of equalities.

$$
\begin{aligned}
\operatorname{res}_{s=k}\zeta(\mathbb{Z}^k, s) &= \operatorname{res}_{s=k}\zeta(s-k+1)\zeta(s-k+2)\cdots\zeta(s-1)\zeta(s)\\
&= \zeta(2)\cdots\zeta(k-1)\zeta(k)\\
&= k\cdot \lim_{T\to\infty} T^{-k}\#\{H\subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : H]\le T\} \qquad \text{[by 1.1]}\\
&= k\cdot \lim_{T\to\infty} T^{-k^2}\#\{H\subseteq \mathbb{Z}^k \mid [\mathbb{Z}^k : H]\le T^k\}\\
&= k\cdot \lim_{T\to\infty} T^{-k^2}\#\{A\in \mathrm{HNF} \mid \det A\le T^k\}\\
&= k\cdot \mu_{\mathbb{Z}}(I\cdot F) \qquad \text{[by definition 2.2]}\\
&= k\cdot \mu_\infty(\mathrm{Sl}_k(\mathbb{R})/\,\mathrm{Sl}_k(\mathbb{Z})) \qquad \text{[by 3.15 and 2.1]}
\end{aligned}
\tag{10}
$$

Combining (9) and (10) we get the following equation.

$$
\prod_p (1-p^{-1})\sum_J [\mathbb{Z}_p^k : J]^{-k} = k\cdot \mu_\infty(\mathrm{Sl}_k(\mathbb{R})/\,\mathrm{Sl}_k(\mathbb{Z})) \tag{11}
$$

We combine (6), (7) and (11) to obtain the following equation.

$$
1 = k\cdot \mu_\infty(\mathrm{Sl}_k(\mathbb{R})/\,\mathrm{Sl}_k(\mathbb{Z}))\cdot \prod_p \mu_p(\mathrm{Sl}_k(\mathbb{Z}_p)) \tag{12}
$$

To relate this to the Tamagawa number we have to introduce a gauge form ω on the algebraic group Sl_k over $\mathbb{Q}$, invariant by left translations, as in sections 2.2.2 and 2.4 of [37]. We can even get gauge forms over $\mathbb{Z}$. Let X be a generic element of Gl_k. The entries of the matrix $X^{-1}dX$ provide a basis for the 1-forms invariant by left translation on Gl_k. On Sl_k we see that $\mathrm{tr}(X^{-1}dX) = d(\det X) = 0$, so omitting the element in the (n,n) spot will provide a basis of the invariant forms on Sl_k. We let ω be the exterior product of these forms. Just as in the proof of Theorem 2.2.5 in [37] we obtain the following equality.

$$\int_{\mathrm{Sl}_k(\mathbb{Z}_p)} \omega_p = \mu_p(\mathrm{Sl}_k(\mathbb{Z}_p)) \tag{13}$$

The measure ω_p is defined in [37, 2.2.1] in a neighborhood of a point P by writing $\omega = f\,dx_1 \wedge \cdots \wedge dx_n$ and setting $\omega_p = |f(P)|_p (dx_1)_p \ldots (dx_n)_p$, where $(dx_i)_p$ is the Haar measure on $\mathbb{Q}_p$ normalized so that $\int_{\mathbb{Z}_p} (dx_i)_p = 1$, and $|c|_p$ is the p-adic valuation normalized so that $d(cx)_p = |c|_p (dx)_p$.

Now we want to determine the constant that relates our original Haar measure μ_∞ on $\mathrm{Sl}_k(\mathbb{R})$ to the one determined by ω_∞. For this purpose, it will suffice to evaluate both measures on the infinitesimal parallelepiped B in $\mathrm{Sl}_k(\mathbb{R})$ centered at the identity matrix and spanned by the tangent vectors εe_{ij} for $i \neq j$ and $\varepsilon(e_{ii} - e_{kk})$ for $i < k$. Here ε is an infinitesimal number, and e_{ij} is the matrix with a 1 in position (i,j) and zeroes elsewhere. For the purpose of this computation, we may even take $\varepsilon = 1$. We remark that B is a fundamental domain for $\mathfrak{sl}_k(\mathbb{Z})$ acting on the Lie algebra $\mathfrak{sl}_k(\mathbb{R})$. We compute easily that $\int_B \omega_\infty = 1$ and

$$\begin{aligned}
\mu_\infty(B) &= \mathrm{vol}(I \cdot B) \\
&= (1/k^2) \cdot |\det(e_{11} - e_{kk}, \cdots, e_{k-1,k-1} - e_{kk}, \textstyle\sum e_{ii})| \\
&= (1/k^2) \cdot |\det(e_{11} - e_{kk}, \cdots, e_{k-1,k-1} - e_{kk}, k e_{kk})| \\
&= (1/k^2) \cdot |\det(e_{11}, \cdots, e_{k-1,k-1}, k e_{kk})| \\
&= 1/k
\end{aligned} \tag{14}$$

We obtain the following equation.

$$\mu_\infty(\mathrm{Sl}_k(\mathbb{R})/\,\mathrm{Sl}_k(\mathbb{Z})) = \frac{1}{k} \int_{\mathrm{Sl}_k(\mathbb{R})/\,\mathrm{Sl}_k(\mathbb{Z})} \omega_\infty \tag{15}$$

See [36, §14.12, (3)] for an essentially equivalent proof of this equation. We may now rewrite (12) as follows.

$$1 = \int_{\mathrm{Sl}_k(\mathbb{R})/\,\mathrm{Sl}_k(\mathbb{Z})} \omega_\infty \cdot \prod_p \int_{\mathrm{Sl}_k(\mathbb{Z}_p)} \omega_p \tag{16}$$

(If done earlier, this computation would have justified normalizing μ_∞ differently.)

The Tamagawa number $\tau(\mathrm{Sl}_{k,\mathbb{Q}}) = \int_{\mathrm{Sl}_k(\mathbb{A}_\mathbb{Q})/\,\mathrm{Sl}_k(\mathbb{Q})} \omega$ is the same as the right hand side of (16) because $F \times \prod_p \mathrm{Sl}_k(\mathbb{Z}_p)$ is a fundamental domain for the action of $\mathrm{Sl}_k(\mathbb{Q})$ on $\mathrm{Sl}_k(\mathbb{A}_{\mathbb{Q}})$. Thus $\tau(\mathrm{Sl}_{k,\mathbb{Q}}) = 1$. This was originally proved by Weil in Theorem 3.3.1 of [37]. See also [14], [12], and [36, §14.11, Corollary to Langlands' Theorem].

See also [33, §8] for an explanation that Siegel's measure formula amounts to the first determination that $\tau(SO) = 2$.

A Dirichlet series

Theorem A.1. *Suppose we are given a Dirichlet series $f(s) := \sum_{n=1}^{\infty} a_n n^{-s}$ with nonnegative coefficients. Let $A(T) := \sum_{n \leq T} a_n$. If $A(T) = O(T^k)$ as $T \to \infty$, then $\sum_{n=T}^{\infty} a_n n^{-s} = O(T^{k-s})$ as $T \to \infty$, and thus $f(s)$ converges for all complex numbers s with $\mathrm{Re}\, s > k$.*

Proof. Write $\sigma = \mathrm{Re}\, s$ and assume $\sigma > k$. We estimate the tail of the series as follows.

$$\begin{aligned}
\sum_{n=T}^{\infty} a_n n^{-s} &= \int_T^{\infty} x^{-s}\, dA(x) \\
&= x^{-s} A(x)\Big]_T^{\infty} - \int_T^{\infty} A(x)\, d(x^{-s}) \\
&= x^{-s} A(x)\Big]_T^{\infty} + s \int_T^{\infty} x^{-s-1} A(x)\, dx \\
&= O(x^{k-\sigma})\Big]_T^{\infty} + s \int_T^{\infty} x^{-s-1} O(x^k)\, dx \\
&= O(T^{k-\sigma}) + s \int_T^{\infty} O(x^{k-\sigma-1})\, dx \\
&= O(T^{k-\sigma})
\end{aligned}$$

□

Theorem A.2. *Suppose we are given two Dirichlet series*

$$f(s) := \sum_{n=1}^{\infty} a_n n^{-s} \qquad g(s) := \sum_{n=1}^{\infty} b_n n^{-s}$$

with nonnegative coefficients and corresponding coefficient summatory functions

$$A(T) := \sum_{n \leq T} a_n \qquad B(T) := \sum_{n \leq T} b_n$$

Assume that $A(T) = O(T^i)$ and $B(T) = cT^k + O(T^j)$, where $i \leq j < k$. Let $h(s) := f(s)g(s) = \sum_{n=1}^{\infty} c_n n^{-s}$, and let $C(T) := \sum_{n \leq T} c_n$. Then $C(T) = cf(k)T^k + O(T^j \log T)$ if $i = j$, and $C(T) = cf(k)T^k + O(T^j)$ if $i < j$.

Proof. The basic idea for this proof was told to us by Harold Diamond.

Observe that Theorem A.1 ensures that $f(k)$ converges. Let's fix the notation $\beta(T) = O(\gamma(T))$ to mean that there is a constant C so that $|\beta(T)| \leq C\gamma(T)$ for all $T \in [1,\infty)$, and simultaneously replace $O(T^j \log T)$ in the statement by $O(T^j(1+\log T))$ in order to avoid the zero of $\log T$ at $T=1$. We will use the notation in an infinite sum only with a uniform value of the implicit constant C.

We examine $C(T)$ as follows.

$$\begin{aligned}
C(T) &= \sum_{n\leq T} c_n = \sum_{n\leq T}\sum_{pq=n} a_p b_q = \sum_{pq\leq n} a_p b_q \\
&= \sum_{p\leq T} a_p \sum_{q\leq T/p} b_q = \sum_{p\leq T} a_p B(T/p) \\
&= \sum_{p\leq T} a_p\{c(T/p)^k + O((T/p)^j)\} \\
&= cT^k \sum_{p\leq T} a_p p^{-k} + O(T^j)\sum_{p\leq T} a_p p^{-j} \\
&= cT^k\{f(k) + O(T^{i-k})\} + O(T^j)\sum_{p\leq T} a_p p^{-j} \\
&= cf(k)T^k + O(T^i) + O(T^j)\sum_{p\leq T} a_p p^{-j}
\end{aligned}$$

If $i<j$ then $\sum_{p\leq T} a_p p^{-j} \leq f(j) = O(1)$. Alternatively, if $i=j$, then

$$\begin{aligned}
\sum_{p\leq T} a_p p^{-j} = \sum_{p\leq T} a_p p^{-i} &= \int_{1-}^{T} p^{-i}\, d(A(p)) \\
&= p^{-i}A(p)\big]_{1-}^{T} - \int_{1-}^{T} A(p)\, d(p^{-i}) \\
&= T^{-i}A(T) + i\int_{1-}^{T} A(p)p^{-i-1}\, dp \\
&= O(1) + O(\int_{1-}^{T} p^{-1}\, dp) = O(1+\log T)
\end{aligned}$$

In both cases the result follows. □

The proof of the following "Abelian" theorem for generalized Dirichlet series is elementary.

Theorem A.3. *Suppose we are given numbers R, $k \geq 1$, and $1 \leq \lambda_1 \leq \lambda_2 \leq \cdots \to \infty$. Suppose that*

$$N(T) := \sum_{\lambda_n\leq T} 1 = (R+o(1))\frac{T^k}{k} \qquad (T\to\infty)$$

for some number R. Then the generalized Dirichlet series $\psi(s) := \sum \lambda_n^{-s}$ *converges for all real numbers* $s > k$, *and* $\lim_{s\to k+}(s-k)\psi(s) = R$.

Proof. In the case $R \neq 0$, the proof can be obtained by adapting the argument in the last part of the proof of [3, Chapter 5, Section 1, Theorem 3]: roughly, one reduces to the case where $k = 1$ by a simple change of variables, shows $\lambda_n \sim n/R$, uses that to compare a tail of $\sum \lambda_n^{-s}$ to a tail of $\zeta(s) = \sum n^{-s}$, and then uses $\lim_{s\to 1+}(s-1)\zeta(s) = 1$.

Alternatively, one can refer to [34, Theorem 10, p. 114] for the statement about convergence, and then to [34, Theorem 2, p. 219] for the statement about the limit. Actually, those two theorems are concerned with Dirichlet series of the form $F(s) = \sum a_n n^{-s}$, but the first step there is to consider the growth rate of $\sum_{n\le x} a_n$ as $x \to \infty$. Essentially the same proof works for $F(s) = \psi(s)$ by considering the growth rate of $N(x)$ instead.

The result also follows from the following estimate, provided to us by Harold Diamond. Assume $s > k$.

$$\begin{aligned}
\psi(s) &:= \sum \lambda_n^{-s} \\
&= \int_{1-}^{\infty} x^{-s}\, dN(x) \\
&= x^{-s}N(x)\big]_{1-}^{\infty} + s\int_1^{\infty} x^{-s-1}N(x)\, dx \\
&= O(x^{k-s})\big]^{\infty} + s\int_1^{\infty} x^{-s-1}(R+o(1))\frac{x^k}{k}\, dx \qquad (x\to\infty) \\
&= \frac{s(R+o(1))}{k}\int_1^{\infty} x^{-s-1+k}\, dx \qquad (s\to k+) \\
&= \frac{s(R+o(1))}{k(s-k)} \qquad (s\to k+)
\end{aligned}$$

Notice the shift in the meaning of $o(1)$ from one line to the next, verified by writing $\int_1^\infty = \int_1^b + \int_b^\infty$ and letting b go to ∞; it turns out that for sufficiently small ϵ the major contribution to $\int_1^\infty x^{-1-\epsilon}\, dx$ comes from $\int_b^\infty x^{-1-\epsilon}\, dx$. □

The following Wiener-Ikehara "Tauberian" theorem is a converse to the previous theorem, but the proof is much harder.

Theorem A.4. *Suppose we are given numbers* $R > 0$, $k > 0$, $1 \le \lambda_1 \le \lambda_2 \le \cdots \to \infty$, *and nonnegative numbers* $a_1, a_2, \ldots$. *Suppose that the Dirichlet series* $\psi(s) = \sum a_n \lambda_n^{-s}$ *converges for all complex numbers with* $\operatorname{Re} s > k$, *and that the function* $\psi(s) - R/(s-k)$ *can be extended to a function defined and continuous for* $\operatorname{Re} s \ge k$. *Then*

$$\sum_{\lambda_n \le T} a_n \sim RT^k/k.$$

Proof. Replacing s by ks allows us to reduce to the case where $k = 1$, which can be deduced directly from the Landau-Ikehara Theorem in [1], from Theorem 2.2 on p. 93 of [35], from Theorem 1 on p. 464 of [17], or from Theorem 1 on p. 534 of [18]. See also Theorem 17 on p. 130 of [40] for the case where $\lambda_n = n$, which suffices for our purposes. A weaker prototype of this theorem was first proved by Landau in 1909 [13, §241]. Other relevant papers include [39], [6], and [5]. See also Bateman's discussion in [13, Appendix, page 931] and the good exposition of Abelian and Tauberian theorems in chapter 5 of [38]. □

References

[1] S. Bochner. Ein Satz von Landau und Ikehara. *Math. Z.*, 37:1–9, 1933.

[2] Armand Borel. *Introduction aux groupes arithmétiques.* Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris, 1969.

[3] A. I. Borevich and I. R. Shafarevich. *Number theory.* Academic Press, New York, 1966. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20.

[4] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[5] Hubert Delange. Sur le théorème taubérien de Ikéhara. *C. R. Acad. Sci. Paris*, 232:465–467, 1951.

[6] Hubert Delange. Généralisation du théorème de Ikehara. *Ann. Sci. Ecole Norm. Sup. (3)*, 71:213–242, 1954.

[7] Daniel R. Grayson. Reduction theory using semistability. *Comment. Math. Helv.*, 59:600–634, 1984.

[8] F. J. Grunewald, D. Segal, and G. C. Smith. Subgroups of finite index in nilpotent groups. *Invent. Math.*, 93:185–223, 1988.

[9] Adolf Hurwitz. Ueber die Erzeugung der Invarianten durch Integration. *Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse*, pages 71–90, 1897.

[10] Adolf Hurwitz. *Mathematische Werke. Bd. II: Zahlentheorie, Algebra und Geometrie.* Birkhäuser Verlag, Basel, 1963. Herausgegeben von der Abteilung für Mathematik und Physik der Eidgenössischen Technischen Hochschule in Zürich.

[11] M. Kneser. Semisimple algebraic groups. In *Algebraic Number. Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 250–265. Thompson, Washington, D.C., 1967.

[12] Robert E. Kottwitz. Tamagawa numbers. *Ann. of Math. (2)*, 127:629–646, 1988.

[13] Edmund Landau. *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*. Chelsea Publishing Co., New York, 1953. 2d ed, With an appendix by Paul T. Bateman.

[14] R. P. Langlands. The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 143–148. Amer. Math. Soc., Providence, R.I., 1966.

[15] A. M. Macbeath and C. A. Rogers. Siegel's mean value theorem in the geometry of numbers. *Proc. Cambridge Philos. Soc.*, 54:139–151, 1958.

[16] Hermann Minkowski. Diskontinuitätsbereich für arithmetische Äquivalenz. *J. Reine Angew. Math.*, 192:220–274, 1905.

[17] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. PWN—Polish Scientific Publishers, Warsaw, 1974. Monografie Matematyczne, Tom 57.

[18] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer-Verlag, Berlin, second edition, 1990.

[19] Morris Newman. *Integral matrices*. Academic Press, New York, 1972. Pure and Applied Mathematics, Vol. 45.

[20] Takashi Ono. On the relative theory of Tamagawa numbers. *Ann. of Math. (2)*, 82:88–111, 1965.

[21] Hans Sagan. *Advanced calculus of real-valued functions of a real variable and vector-valued functions of a vector variable*. Houghton Mifflin Co., Boston, Mass., 1974.

[22] Winfried Scharlau and Hans Opolka. *From Fermat to Minkowski*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1985. Lectures on the theory of numbers and its historical development, Translated from the German by Walter K. Bühler and Gary Cornell.

[23] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[24] Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen, I. *Ann. Math.*, 36:527–606, 1935.

[25] Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen, II. *Ann. Math.*, 37:230–263, 1936.

[26] Carl Ludwig Siegel. The volume of the fundamental domain for some infinite groups. *Trans. Amer. Math. Soc.*, 39:209–218, 1936.

[27] Carl Ludwig Siegel. Über die analytische Theorie der quadratischen Formen, III. *Ann. Math.*, 38:212–291, 1937.

[28] Carl Ludwig Siegel. On the theory of indefinite quadratic forms. *Ann. of Math. (2)*, 45:577–622, 1944.

[29] Carl Ludwig Siegel. A mean value theorem in the geometry of numbers. *Ann. Math.*, 46:340–347, 1945.

[30] Carl Ludwig Siegel. Zur Bestimmung des Volumens des Fundamentalbereichs der unimodularen Gruppe. *Math. Ann.*, 137:427–432, 1959.

[31] Carl Ludwig Siegel. *Lectures on the geometry of numbers.* Springer-Verlag, Berlin, 1989. Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan.

[32] Louis Solomon. Zeta functions and integral representation theory. *Advances in Math.*, 26:306–326, 1977.

[33] Tsuneo Tamagawa. Adèles. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 113–121. Amer. Math. Soc., Providence, R.I., 1966.

[34] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory.* Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.

[35] J. van de Lune. *An introduction to Tauberian theory: from Tauber to Wiener.* Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1986.

[36] V. E. Voskresenskiĭ. *Algebraic groups and their birational invariants.* American Mathematical Society, Providence, RI, 1998. Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ].

[37] André Weil. *Adeles and algebraic groups.* Birkhäuser, Boston, Mass., 1982. With appendices by M. Demazure and Takashi Ono.

[38] David Vernon Widder. *The Laplace Transform.* Princeton University Press, Princeton, N. J., 1941.

[39] N. Wiener. Tauberian theorems. *Ann. of Math.*, 33:1–100, 1932.

[40] Norbert Wiener. *The Fourier integral and certain of its applications.* Cambridge University Press, London, 1933.

Henri Gillet
University of Illinois at Chicago
http://www.math.uic.edu/~henri/
henri@math.uic.edu

Daniel R. Grayson
University of Illinois
at Urbana-Champaign
http://www.math.uiuc.edu/~dan/
dan@math.uiuc.edu

The Supersingular Loci and Mass Formulas on Siegel Modular Varieties

Chia-Fu Yu

Received: October 2, 2006
Revised: December 4, 2006

Communicated by Takeshi Saito

Abstract. We describe the supersingular locus of the Siegel 3-fold with a parahoric level structure. We also study its higher dimensional generalization. Using this correspondence and a deep result of Li and Oort, we evaluate the number of irreducible components of the supersingular locus of the Siegel moduli space $\mathcal{A}_{g,1,N}$ for arbitrary g.

2000 Mathematics Subject Classification: Primary 11G18; Secondary 14K12.
Keywords and Phrases: Siegel modular varieties, supersingular locus, superspecial locus, parahoric level structure, mass formula

1

1. Introduction

In this paper we discuss some extensions of works of Katsura and Oort [5], and of Li and Oort [8] on the supersingular locus of a mod p Siegel modular variety. Let p be a rational prime number, $N \geq 3$ a prime-to-p positive integer. We choose a primitive N-th root of unity ζ_N in $\overline{\mathbb{Q}} \subset \mathbb{C}$ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Let $\mathcal{A}_{g,1,N}$ be the moduli space over $\mathbb{Z}_{(p)}[\zeta_N]$ of g-dimensional principally polarized abelian varieties (A, λ, η) with a symplectic level-N structure (See Subsection 2.1).

Let $\mathcal{A}_{2,1,N,(p)}$ be the cover of $\mathcal{A}_{2,1,N}$ which parametrizes isomorphism classes of objects (A, λ, η, H), where (A, λ, η) is an object in $\mathcal{A}_{2,1,N}$ and $H \subset A[p]$ is a finite flat subgroup scheme of rank p. It is known that the moduli scheme $\mathcal{A}_{2,1,N,(p)}$ has semi-stable reduction and the reduction $\mathcal{A}_{2,1,N,(p)} \otimes \overline{\mathbb{F}}_p$ modulo p has two irreducible components. Let $\mathcal{S}_{2,1,N,(p)}$ (resp. $\mathcal{S}_{2,1,N}$) denote the supersingular locus of the moduli space $\mathcal{A}_{2,1,N,(p)} \otimes \overline{\mathbb{F}}_p$ (resp. $\mathcal{A}_{2,1,N} \otimes \overline{\mathbb{F}}_p$). Recall

The research is partially supported by NSC 95-2115-M-001-004.

that an abelian variety A in characteristic p is called *supersingular* if it is isogenous to a product of supersingular elliptic curves over an algebraically closed field k; it is called *superspecial* if it is isomorphic to a product of supersingular elliptic curves over k.

The supersingular locus $\mathcal{S}_{2,1,N}$ of the Siegel 3-fold is studied in Katsura and Oort [5]. We summarize the main results for $\mathcal{S}_{2,1,N}$ (the local results obtained earlier in Koblitz [7]):

THEOREM 1.1.
(1) *The scheme $\mathcal{S}_{2,1,N}$ is equi-dimensional and each irreducible component is isomorphic to $\mathbf{P}^1$.*
(2) *The scheme $\mathcal{S}_{2,1,N}$ has*

$$|\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})|\frac{(p^2-1)}{5760} \tag{1.1}$$

irreducible components.
(3) *The singular points of $\mathcal{S}_{2,1,N}$ are exactly the superspecial points and there are*

$$|\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})|\frac{(p-1)(p^2+1)}{5760} \tag{1.2}$$

of them. Moreover, at each singular point there are $p+1$ irreducible components passing through and intersecting transversely.

PROOF. See Koblitz [7, p.193] and Katsura-Oort [5, Section 2, Theorem 5.1, Theorem 5.3].

In this paper we extend their results to $\mathcal{S}_{2,1,N,(p)}$. We show

THEOREM 1.2.
(1) *The scheme $\mathcal{S}_{2,1,N,(p)}$ is equi-dimensional and each irreducible component is isomorphic to $\mathbf{P}^1$.*
(2) *The scheme $\mathcal{S}_{2,1,N,(p)}$ has*

$$|\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})|\cdot\frac{(-1)\zeta(-1)\zeta(-3)}{4}\left[(p^2-1)+(p-1)(p^2+1)\right] \tag{1.3}$$

irreducible components, where $\zeta(s)$ is the Riemann zeta function.
(3) *The scheme $\mathcal{S}_{2,1,N,(p)}$ has only ordinary double singular points and there are*

$$|\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})|\cdot\frac{(-1)\zeta(-1)\zeta(-3)}{4}(p-1)(p^2+1)(p+1) \tag{1.4}$$

of them.
(4) *The natural morphism $\mathcal{S}_{2,1,N,(p)}\to\mathcal{S}_{2,1,N}$ contracts*

$$|\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})|\cdot\frac{(-1)\zeta(-1)\zeta(-3)}{4}(p-1)(p^2+1) \tag{1.5}$$

projective lines onto the superspecial points of $\mathcal{S}_{2,1,N}$.

Remark 1.3. (1) By the basic fact that

$$\zeta(-1)=\frac{-1}{12} \quad \text{and} \quad \zeta(-3)=\frac{1}{120},$$

the number (1.5) (of the vertical components) equals the number (1.2) (of superspecial points), and the number (1.3) (sum of vertical and horizontal components) equals the sum of the numbers (1.1) (of irreducible components) and (1.2) (of superspecial points). Thus, the set of horizontal irreducible components of $\mathcal{S}_{2,1,N,(p)}$ is in bijection with the set of irreducible components of $\mathcal{S}_{2,1,N}$

(2) Theorem 1.2 (4) says that $\mathcal{S}_{2,1,N,(p)}$ is a "desingularization" or a "blow-up" of $\mathcal{S}_{2,1,N}$ at the singular points. Strictly speaking, the desingularization of $\mathcal{S}_{2,1,N}$ is its normalization, which is the (disjoint) union of horizontal components of $\mathcal{S}_{2,1,N,(p)}$. The vertical components of $\mathcal{S}_{2,1,N,(p)}$ should be the exceptional divisors of the blowing up of a suitable ambient surface of $\mathcal{S}_{2,1,N}$ at superspecial points.

In the proof of Theorem 1.2 (Section 4) we see that

- the set of certain superspecial points (the set Λ in Subsection 4.1) in $\mathcal{S}_{2,p,N}$ (classifying degree-p^2 polarized supersingular abelian surfaces) is in bijection with the set of irreducible components of $\mathcal{S}_{2,1,N}$, and
- the set of superspecial points in $\mathcal{S}_{2,1,N}$ is in bijection with the set of irreducible components of $\mathcal{S}_{2,p,N}$, furthermore
- the supersingular locus $\mathcal{S}_{2,1,N,(p)}$ provides the explicit link of this duality as a correspondence that performs simply through the "blowing-ups" and "blowing-downs".

In the second part of this paper we attempt to generalize a similar picture to higher (even) dimensions.

Let $g=2D$ be an even positive integer. Let $\mathcal{H}$ be the moduli space over $\mathbb{Z}_{(p)}[\zeta_N]$ which parametrizes equivalence classes of objects $(\varphi:\underline{A}_1\to\underline{A}_2)$, where

- $\underline{A}_1=(A_1,\lambda_1,\eta_1)$ is an object in $\mathcal{A}_{g,1,N}$,
- $\underline{A}_2=(A_2,\lambda_2,\eta_2)$ is an object in $\mathcal{A}_{g,p^D,N}$, and
- $\varphi:A_1\to A_2$ is an isogeny of degree p^D satisfying $\varphi^*\lambda_2=p\lambda_1$ and $\varphi_*\eta_1=\eta_2$.

The moduli space $\mathcal{H}$ with natural projections gives the following correspondence:

$$\begin{array}{ccc} & \mathcal{H} & \\ {\scriptstyle \mathrm{pr}_1}\swarrow & & \searrow{\scriptstyle \mathrm{pr}_2} \\ \mathcal{A}_{g,1,N} & & \mathcal{A}_{g,p^D,N}. \end{array}$$

Let $\mathcal{S}$ be the supersingular locus of $\mathcal{H}\otimes\overline{\mathbb{F}}_p$, which is the reduced closed subscheme consisting of supersingular points (either A_1 or A_2 is supersingular, or equivalently both are so).

In the special case where $g=2$, $\mathcal{H}$ is isomorphic to $\mathcal{A}_{2,1,N,(p)}$, and $\mathcal{S} \simeq \mathcal{S}_{2,1,N,(p)}$ under this isomorphism (See Subsection 4.5).

As the second main result of this paper, we obtain

Theorem 1.4. *Let C be the number of irreducible components of $\mathcal{S}_{g,1,N}$. Then*

$$C = |\operatorname{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \cdot \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{i=1}^{g} \zeta(1-2i) \right\} \cdot L_p \,,$$

where

$$L_p = \begin{cases} \prod_{i=1}^{g} \left\{ (p^i + (-1)^i \right\} & \text{if } g \text{ is odd;} \\ \prod_{i=1}^{D} (p^{4i-2} - 1) & \text{if } g = 2D \text{ is even.} \end{cases}$$

In the special case where $g=2$, Theorem 1.4 recovers Theorem 1.1 (2).

We give the idea of the proof. Let $\Lambda_{g,1,N}$ denote the set of superspecial (geometric) points in $\mathcal{A}_{g,1,N} \otimes \overline{\mathbb{F}}_p$. For $g=2D$ is even, let $\Lambda^*_{g,p^D,N}$ denote the set of superspecial (geometric) points (A,λ,η) in $\mathcal{A}_{g,p^D,N} \otimes \overline{\mathbb{F}}_p$ satisfying $\ker \lambda = A[F]$, where $F: A \to A^{(p)}$ is the relative Frobenius morphism on A. These are finite sets and each member is defined over $\overline{\mathbb{F}}_p$. By a result of Li and Oort [8] (also see Section 5), we know

$$C = \begin{cases} |\Lambda_{g,1,N}| & \text{if } g \text{ is odd;} \\ |\Lambda^*_{g,p^D,N}| & \text{if } g \text{ is even.} \end{cases}$$

One can use the geometric mass formula due to Ekedahl [2] and some others (see Section 3) to compute $|\Lambda_{g,1,N}|$. Therefore, it remains to compute $|\Lambda^*_{g,p^D,N}|$ when g is even. We restrict the correspondence $\mathcal{S}$ to the product $\Lambda_{g,1,N} \times \Lambda^*_{g,p^D,N}$ of superspecial points, and compute certain special points in $\mathcal{S}$. This gives us relation between $\Lambda^*_{g,p^D,N}$ and $\Lambda_{g,1,N}$. See Section 6 for details.

Theorem 1.4 tells us how the number $C = C(g,N,p)$ varies when p varies. For another application, one can use this result to compute the dimension of the space of Siegel cusp forms of certain level at p by the expected Jacquet-Langlands correspondence for symplectic groups. As far as the author knows, the latter for general g is not available yet in the literature.

The paper is organized as follows. In Section 2, we recall the basic definitions and properties of the Siegel moduli spaces and supersingular abelian varieties. In Section 3, we state the mass formula for superspecial principally polarized abelian varieties due to Ekedahl (and some others). The proof of Theorem 1.2 is given in Section 4. In Section 5, we describe the results of Li and Oort on irreducible components of the supersingular locus. In Section 6, we introduce a correspondence and use this to evaluate the number of irreducible components of the supersingular locus.

Acknowledgments. The author is grateful to Katsura, Li and Oort for their inspiring papers on which the present work relies heavily. He also thanks C.-L. Chai for his encouragements on this subject for years, and thanks T. Ibukiyama for his interest of the present work. He is indebted to the referee

for careful reading and helpful comments that improve the presentation of this paper.

2. Notation and preliminaries

2.1. Throughout this paper we fix a rational prime p and a prime-to-p positive integer $N \geq 3$. Let d be a positive integer with $(d,N)=1$. We choose a primitive N-th root of unity ζ_N in $\overline{\mathbb{Q}} \subset \mathbb{C}$ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. The element ζ_N gives rise to a trivialization $\mathbb{Z}/N\mathbb{Z} \simeq \mu_N$ over any $\mathbb{Z}_{(p)}[\zeta_N]$-scheme. For a polarized abelian variety (A,λ) of degree d^2, a full symplectic level-N structure with respect to the choice ζ_N is an isomorphism

$$\eta : (\mathbb{Z}/N\mathbb{Z})^{2g} \simeq A[N]$$

such that the following diagram commutes

$$\begin{array}{ccc}
(\mathbb{Z}/N\mathbb{Z})^{2g} \times (\mathbb{Z}/N\mathbb{Z})^{2g} & \xrightarrow{(\eta,\eta)} & A[N] \times A[N] \\
{\scriptstyle \langle\, , \rangle}\downarrow & & {\scriptstyle e_\lambda}\downarrow \\
\mathbb{Z}/N\mathbb{Z} & \xrightarrow{\zeta_N} & \mu_N,
\end{array}$$

where $\langle\, , \rangle$ is the standard non-degenerate alternating form on $(\mathbb{Z}/N\mathbb{Z})^{2g}$ and e_λ is the Weil pairing induced by the polarization λ.
Let $\mathcal{A}_{g,d,N}$ denote the moduli space over $\mathbb{Z}_{(p)}[\zeta_N]$ of g-dimensional polarized abelian varieties (A,λ,η) of degree d^2 with a full symplectic level N structure with respect to ζ_N. Let $\mathcal{S}_{g,d,N}$ denote the supersingular locus of the reduction $\mathcal{A}_{g,d,N} \otimes \overline{\mathbb{F}}_p$ modulo p, which is the closed reduced subscheme of $\mathcal{A}_{g,d,N} \otimes \overline{\mathbb{F}}_p$ consisting of supersingular points in $\mathcal{A}_{g,d,N} \otimes \overline{\mathbb{F}}_p$. Let $\Lambda_{g,d,N}$ denote the set of superspecial (geometric) points in $\mathcal{S}_{g,d,N}$; this is a finite set and every member is defined over $\overline{\mathbb{F}}_p$.

For a scheme X of finite type over a field K, we denote by $\Pi_0(X)$ the set of geometrically irreducible components of X.
Let k be an algebraically closed field of characteristic p.

2.2. Over a ground field K of characteristic p, denote by α_p the finite group scheme of rank p that is the kernel of the Frobenius endomorphism from the additive group $\mathbb{G}_{\mathrm{a}}$ to itself. One has

$$\alpha_p = \mathrm{Spec} K[X]/X^p, \quad m(X) = X \otimes 1 + 1 \otimes X,$$

where m is the group law.
By definition, an elliptic curve E over K is called *supersingular* if $E[p](\overline{K}) = 0$. An abelian variety A over K is called *supersingular* if it is isogenous to a product of supersingular elliptic curves over $\overline{K}$; A is called *superspecial* if it is isomorphic to a product of supersingular elliptic curves over $\overline{K}$.
For any abelian variety A over K where K is perfect, the *a-number* of A is defined by

$$a(A) := \dim_K \mathrm{Hom}(\alpha_p, A).$$

The following interesting results are well-known; see Subsection 1.6 of [8] for a detail discussion.

THEOREM 2.1 (Oort). *If $a(A)=g$, then A is superspecial.*

THEOREM 2.2 (Deligne, Ogus, Shioda). *For $g \geq 2$, there is only one g-dimensional superspecial abelian variety up to isomorphism over k.*

3. THE MASS FORMULA

Let Λ_g denote the set of isomorphism classes of g-dimensional principally polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$. Write

$$M_g := \sum_{(A,\lambda)\in\Lambda_g} \frac{1}{|\operatorname{Aut}(A,\lambda)|}$$

for the mass attached to Λ_g. The following mass formula is due to Ekedahl [2, p.159] and Hashimoto-Ibukiyama [3, Proposition 9].

THEOREM 3.1. *Notation as above. One has*

$$M_g = \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^{g} \zeta(1-2k) \right\} \cdot \prod_{k=1}^{g} \left\{ (p^k + (-1)^k \right\}. \tag{3.1}$$

Similarly, we set

$$M_{g,1.N} := \sum_{(A,\lambda,\eta)\in\Lambda_{g,1,N}} \frac{1}{|\operatorname{Aut}(A,\lambda,\eta)|}.$$

LEMMA 3.2. *We have $M_{g,1,N} = |\Lambda_{g,1,N}| = |\operatorname{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \cdot M_g$.*

PROOF. The first equality follows from a basic fact that (A,λ,η) has no non-trivial automorphism. The proof of the second equality is elementary; see Subsection 4.6 of [11].

COROLLARY 3.3. *One has*

$$|\Lambda_{2,1,N}| = |\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})| \cdot \frac{(-1)\zeta(-1)\zeta(-3)}{4}(p-1)(p^2+1).$$

4. PROOF OF THEOREM 1.2

4.1. In this section we consider the case where $g=2$. Let

$$\Lambda := \{(A,\lambda,\eta) \in \mathcal{S}_{2,p,N};\ \ker\lambda \simeq \alpha_p \times \alpha_p\}.$$

Note that every member $\underline{A}$ of Λ is superspecial (because $A \supset \alpha_p \times \alpha_p$), that is, $\Lambda \subset \Lambda_{2,p,N}$. For a point ξ in Λ, consider the space S_ξ which parametrizes the isogenies of degree p

$$\varphi : (A_\xi, \lambda_\xi, \eta_\xi) \to \underline{A} = (A,\lambda,\eta)$$

which preserve the polarizations and level structures. Let

$$\psi_\xi : S_\xi \to \mathcal{S}_{2,1,N}$$

be the morphism which sends $(\varphi : \xi \to \underline{A})$ to $\underline{A}$. Let $V_\xi \subset \mathcal{S}_{2,1,N}$ be the image of S_ξ under ψ_ξ.
The following theorem is due to Katsura and Oort [5, Theorem 2.1 and Theorem 5.1]:

Theorem 4.1 (Katsura-Oort). *Notation as above. The map $\xi \mapsto V_\xi$ gives rise to a bijection $\Lambda \simeq \Pi_0(\mathcal{S}_{2,1,N})$ and one has*

$$|\Lambda| = |\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})|(p^2-1)/5760.$$

We will give a different way of evaluating $|\Lambda|$ that is based on the geometric mass formula (see Corollary 4.6).

4.2. Dually we can consider the space S'_ξ for each $\xi \in \Lambda$ that parametrizes the isogenies of degree p

$$\varphi' : \underline{A} = (A, \lambda, \eta) \to \xi = (A_\xi, \lambda_\xi, \eta_\xi),$$

with $\underline{A} \in \mathcal{A}_{2,1,N} \otimes \overline{\mathbb{F}}_p$, such that $\varphi'_* \eta = \eta_\xi$ and $\varphi'^* \lambda_\xi = p\,\lambda$. Let

$$\psi'_\xi : S'_\xi \to \mathcal{S}_{2,1,N}$$

be the morphism which sends $(\varphi' : \underline{A} \to \xi)$ to $\underline{A}$. Let $V'_\xi \subset \mathcal{S}_{2,1,N}$ be the image of S'_ξ under ψ'_ξ.
For a degree p isogeny $(\varphi : \underline{A}_1 \to \underline{A}_2)$ with $\underline{A}_2$ in $\mathcal{A}_{2,1,N}$, $\varphi^* \lambda_2 = \lambda_1$ and $\varphi_* \eta_1 = \eta_2$, we define

$$(\varphi : \underline{A}_1 \to \underline{A}_2)^* = (\varphi' : \underline{A}'_2 \to \underline{A}'_1),$$

where $\varphi' = \varphi^t$ and

$$\underline{A}'_2 = (A_2^t, \lambda_2^{-1}, \lambda_2 \circ \eta_2),$$
$$\underline{A}'_1 = (A_1^t, p\,\lambda_1^{-1}, \lambda_1 \circ \eta_1).$$

Note that $\varphi'_* \eta'_2 = \eta'_1$ as we have the commutative diagram:

$$\begin{array}{ccccc} (\mathbb{Z}/N\mathbb{Z})^4 & \xrightarrow{\eta_2} & A_2[N] & \xrightarrow{\lambda_2} & A_2^t[N] \\ \big\downarrow{=} & & \big\uparrow{\varphi} & & \big\downarrow{\varphi^t} \\ (\mathbb{Z}/N\mathbb{Z})^4 & \xrightarrow{\eta_1} & A_1[N] & \xrightarrow{\lambda_1} & A_1^t[N]. \end{array}$$

If $\underline{A}_1 \in \Lambda$, then $\underline{A}'_1$ is also in Λ. Therefore, the map $\xi \mapsto V'_\xi$ also gives rise to a bijection $\Lambda \simeq \Pi_0(\mathcal{S}_{2,1,N})$.

4.3. We use the classical contravariant Dieudonné theory. We refer the reader to Demazure [1] for a basic account of this theory. Let K be a perfect field of characteristic p, $W := W(K)$ the ring of Witt vectors over K, $B(K)$ the fraction field of $W(K)$. Let σ be the Frobenius map on $B(K)$. A quasi-polarization on a Dieudonné module M here is a non-degenerate (meaning of non-zero discriminant) alternating pairing

$$\langle\, , \rangle : M \times M \to B(K),$$

such that $\langle Fx, y \rangle = \langle x, Vy \rangle^\sigma$ for $x, y \in M$ and $\langle M^t, M^t \rangle \subset W$. Here we regard the dual M^t of M as a Dieudonné submodule in $M \otimes B(K)$ using the pairing. A

quasi-polarization is called *separable* if $M^t = M$. Any polarized abelian variety (A, λ) over K naturally gives rise to a quasi-polarized Dieudonné module. The induced quasi-polarization is separable if and only if $(p, \deg \lambda) = 1$.
Recall (Subsection 2.1) that k denotes an algebraically closed field of characteristic p.

LEMMA 4.2.
(1) *Let M be a separably quasi-polarized superspecial Dieudonné module over k of rank 4. Then there exists a basis f_1, f_2, f_3, f_4 for M over $W := W(k)$ such that*

$$Ff_1 = f_3, Ff_3 = pf_1, \quad Ff_2 = f_4, Ff_4 = pf_2$$

and the non-zero pairings are

$$\langle f_1, f_3\rangle = -\langle f_3, f_1\rangle = \beta_1, \quad \langle f_2, f_4\rangle = -\langle f_4, f_2\rangle = \beta_1,$$

where $\beta_1 \in W(\mathbb{F}_{p^2})^\times$ with $\beta_1^\sigma = -\beta_1$.
(2) *Let ξ be a point in Λ, and let M_ξ be the Dieudonné module of ξ. Then there is a W-basis e_1, e_2, e_3, e_4 for M_ξ such that*

$$Fe_1 = e_3, \quad Fe_2 = e_4, \quad Fe_3 = pe_1, \quad Fe_4 = pe_2,$$

and the non-zero pairings are

$$\langle e_1, e_2\rangle = -\langle e_2, e_1\rangle = \frac{1}{p}, \quad \langle e_3, e_4\rangle = -\langle e_4, e_3\rangle = 1.$$

PROOF. (1) This is a special case of Proposition 6.1 of [8].
(2) By Proposition 6.1 of [8], $(M_\xi, \langle\, ,\rangle)$ either is indecomposable or decomposes into a product of two quasi-polarized supersingular Dieudonné modules of rank 2. In the indecomposable case, one can choose such a basis e_i for M_ξ. Hence it remains to show that $(M_\xi, \langle\, ,\rangle)$ is indecomposable. Let $(A_\xi[p^\infty], \lambda_\xi)$ be the associated polarized p-divisible group. Suppose it decomposes into $(H_1, \lambda_1) \times (H_2, \lambda_2)$. Then the kernel of λ is isomorphic to $E[p]$ for a supersingular elliptic curve E. Since $E[p]$ is a nontrivial extension of α_p by α_p, one gets contradiction. This completes the proof. ∎

4.4. Let (A_0, λ_0) be a superspecial principally polarized abelian surface and $(M_0, \langle\, ,\rangle_0)$ be the associated Dieudonné module. Let $\varphi' : (A_0, \lambda_0) \to (A, \lambda)$ be an isogeny of degree p with $\varphi'^*\lambda = p\,\lambda_0$. Write $(M, \langle\, ,\rangle)$ for the Dieudonné module of (A, λ). Choose a basis f_1, f_2, f_3, f_4 for M_0 as in Lemma 4.2. We have the inclusions

$$(F, V)M_0 \subset M \subset M_0.$$

Modulo $(F, V)M_0$, a module M corresponds a one-dimensional subspace $\overline{M}$ in $\overline{M}_0 := M_0/(F, V)M_0$. As $\overline{M}_0 = k < f_1, f_2 >$, $\overline{M}$ is of the form

$$\overline{M} = k < af_1 + bf_2 >, \quad [a : b] \in \mathbf{P}^1(k).$$

The following result is due to Moret-Bailly [9, p.138-9]. We include a proof for the reader's convenience.

LEMMA 4.3. *Notation as above,* $\ker\lambda \simeq \alpha_p\times\alpha_p$ *if and only if the corresponding point* $[a:b]$ *satisfies* $a^{p+1}+b^{p+1}=0$. *Consequently, there are* $p+1$ *isogenies* φ' *so that* $\ker\lambda\simeq\alpha_p\times\alpha_p$.

PROOF. As $\varphi'^*\lambda = p\lambda_0$, we have $\langle\,,\rangle = \frac{1}{p}\langle\,,\rangle_0$. The Dieudonné module $M(\ker\lambda)$ of the subgroup $\ker\lambda$ is equal to M/M^t. Hence the condition $\ker\lambda\simeq \alpha_p\times\alpha_p$ is equivalent to that F and V vanish on $M(\ker\lambda)=M/M^t$.
Since $\langle\,,\rangle$ is a perfect pairing on FM_0, that is, $(FM_0)^t = FM_0$, we have

$$pM_0\subset M^t\subset FM_0\subset M\subset M_0.$$

Changing the notation, put $\overline{M}_0 := M_0/pM_0$ and let

$$\langle\,,\rangle_0 : \overline{M}_0\times\overline{M}_0\to k.$$

be the induced perfect pairing. In $\overline{M}_0$, the subspace $\overline{M^t}$ is equal to $\overline{M}^\perp$. Indeed,

$$(4.1)\qquad \begin{aligned} M^t &= \{m\in M_0; \langle m,x\rangle_0\in pW\ \forall x\in M\},\\ \overline{M^t} &= \{m\in\overline{M}_0; \langle m,x\rangle_0 = 0\ \forall x\in\overline{M}\} = \overline{M}^\perp. \end{aligned}$$

From this we see that the condition $\ker\lambda\simeq\alpha_p\times\alpha_p$ is equivalent to $\langle\overline{M},F\overline{M}\rangle = \langle\overline{M},V\overline{M}\rangle = 0$. Since $\overline{FM_0} = k < f_3, f_4 >$, one has $\overline{M} = k < f_1', f_3, f_4 >$ where $f_1' = af_1+bf_2$. The condition $\langle\overline{M},F\overline{M}\rangle = \langle\overline{M},V\overline{M}\rangle = 0$, same as $\langle f_1', Ff_1'\rangle = \langle f_1', Vf_1'\rangle = 0$, gives the equation $a^{p+1}+b^{p+1}=0$. This completes the proof. ∎

Conversely, fix a polarized superspecial abelian surface (A,λ) such that $\ker\lambda\simeq\alpha_p\times\alpha_p$. Then there are p^2+1 degree-p isogenies $\varphi' : (A_0,\lambda_0)\to(A,\lambda)$ such that A_0 is superspecial and $\varphi'^*\lambda = p\,\lambda_0$. Indeed, each isogeny φ' always has the property $\varphi'^*\lambda = p\,\lambda_0$ for a principal polarization λ_0, and there are $|\mathbf{P}^1(\mathbb{F}_{p^2})|$ isogenies with A_0 superspecial.

4.5. We denote by $\mathcal{A}'_{2,1,N,(p)}$ the moduli space which parametrizes equivalence classes of isogenies $(\varphi' : \underline{A}_0\to\underline{A}_1)$ of degree p, where $\underline{A}_1$ is an object in $\mathcal{A}_{2,p,N}$ and $\underline{A}_0$ is an object in $\mathcal{A}_{2,1,N}$, such that $\varphi'^*\lambda_1 = p\,\lambda_0$ and $\varphi'_*\eta_0=\eta_1$.
There is a natural isomorphism from $\mathcal{A}_{2,1,N,(p)}$ to $\mathcal{A}'_{2,1,N,(p)}$. Given an object (A,λ,η,H) in $\mathcal{A}_{2,1,N,(p)}$, let $\underline{A}_0 := \underline{A}$, $A_1 := A/H$ and $\varphi' : A_0\to A_1$ be the natural projection. The polarization $p\,\lambda_0$ descends to one, denoted by λ_1, on A_1. Put $\eta_1 := \varphi'_*\eta_0$ and $\underline{A}_1 = (A_1,\lambda_1,\eta_1)$. Then $(\varphi' : \underline{A}_0\to\underline{A}_1)$ lies in $\mathcal{A}'_{2,1,N,(p)}$ and the morphism

$$q : \mathcal{A}_{2,1,N,(p)}\to\mathcal{A}'_{2,1,N,(p)},\quad (A,\lambda,\eta,H)\mapsto(\varphi' : \underline{A}_0\to\underline{A}_1)$$

is an isomorphism.
We denote by $\mathcal{S}'_{2,1,N,(p)}$ the supersingular locus of $\mathcal{A}'_{2,1,N,(p)}\otimes\overline{\mathbb{F}}_p$. Thus we have $\mathcal{S}'_{2,1,N,(p)}\simeq\mathcal{S}_{2,1,N,(p)}$. It is clear that $S'_\xi\subset\mathcal{S}'_{2,1,N,(p)}$ for each $\xi\in\Lambda$, and $S'_\xi\cap S'_{\xi'}=\emptyset$ if $\xi\neq\xi'$. For each $\gamma\in\Lambda_{2,1,N}$, let S''_γ be the subspace of $\mathcal{S}'_{2,1,N,(p)}$ that consists of objects $(\varphi' : \underline{A}_0\to\underline{A}_1)$ with $\underline{A}_0=\underline{A}_\gamma$. One also has $S''_\gamma\cap S''_{\gamma'}=\emptyset$ if $\gamma\neq\gamma'$.

LEMMA 4.4. (1) *Let* $(M_0, \langle\,,\rangle_0)$ *be a separably quasi-polarized supersingular Dieudonné module of rank* 4 *and suppose* $a(M_0) = 1$. *Let* $M_1 := (F, V)M_0$ *and* N *be the unique Dieudonné module containing* M_0 *with* $N/M_0 = k$. *Let* $\langle\,,\rangle_1 := \frac{1}{p}\langle\,,\rangle_0$ *be the quasi-polarization for* M_1. *Then one has* $a(N) = a(M_1) = 2$, $VN = M_1$, *and* $M_1/M_1^t \simeq k \oplus k$ *as Dieudonné modules.*
(2) *Let* $(M_1, \langle\,,\rangle_1)$ *be a quasi-polarized supersingular Dieudonné module of rank* 4. *Suppose that* M_1/M_1^t *is of length* 2, *that is, the quasi-polarization has degree* p^2.

- (i) *If* $a(M_1) = 1$, *then letting* $M_2 := (F, V)M_1$, *one has that* $a(M_2) = 2$ *and* $\langle\,,\rangle_1$ *is a separable quasi-polarization on* M_2.
- (ii) *Suppose* $(M_1, \langle\,,\rangle_1)$ *decomposes as the product of two quasi-polarized Dieudonné submodules of rank* 2. *Then there are a unique Dieudonné submodule* M_2 *of* M_1 *with* $M_1/M_2 = k$ *and a unique Dieudonné module* M_0 *containing* M_1 *with* $M_0/M_1 = k$ *so that* $\langle\,,\rangle_1$ *(resp.* $p\langle\,,\rangle_1$*) is a separable quasi-polarization on* M_2 *(resp.* M_0*).*
- (iii) *Suppose* $M_1/M_1^t \simeq k \oplus k$ *as Dieudonné modules. Let* $M_2 \subset M_1$ *be any Dieudonné submodule with* $M_1/M_2 = k$, *and* $M_0 \supset M_1$ *be any Dieudonné overmodule with* $M_0/M_1 = k$. *Then* $\langle\,,\rangle_1$ *(resp.* $p\langle\,,\rangle_1$*) is a separable quasi-polarization on* M_2 *(resp.* M_0*).*

This is well-known; the proof is elementary and omitted.

PROPOSITION 4.5. *Notation as above.*
(1) *One has*

$$\mathcal{S}'_{2,1,N,(p)} = \left(\coprod_{\xi\in\Lambda} S'_\xi\right) \cup \left(\coprod_{\gamma\in\Lambda_{2,1,N}} S''_\gamma\right).$$

(2) *The scheme* $\mathcal{S}'_{2,1,N,(p)}$ *has ordinary double singular points and*

$$(\mathcal{S}'_{2,1,N,(p)})^{\mathrm{sing}} = \left(\coprod_{\xi\in\Lambda} S'_\xi\right) \cap \left(\coprod_{\gamma\in\Lambda_{2,1,N}} S''_\gamma\right).$$

Moreover, one has

$$|(\mathcal{S}'_{2,1,N,(p)})^{\mathrm{sing}}| = |\Lambda_{2,1,N}|(p+1) = |\Lambda|(p^2+1).$$

PROOF. (1) Let $(\varphi' : \underline{A}_0 \to \underline{A}_1)$ be a point of $\mathcal{S}'_{2,1,N,(p)}$. If $a(A_0) = 1$, then $\ker\varphi'$ is the unique α-subgroup of $A_0[p]$ and thus $\underline{A}_1 \in \Lambda$. Hence this point lies in S'_ξ for some ξ. Suppose that $\underline{A}_1$ is not in Λ, then there is a unique lifting $(\varphi'_1 : \underline{A}'_0 \to \underline{A}_1)$ in $\mathcal{S}'_{2,1,N,(p)}$ and the source $\underline{A}'_0$ is superspecial. Hence $\underline{A}_0 = \underline{A}'_0$ is superspecial and the point $(\varphi' : \underline{A}_0 \to \underline{A}_1)$ lies in S''_γ for some γ.
(2) It is clear that the singularities only occur at the intersection of S'_ξ's and S''_γ's, as S'_ξ and S''_γ are smooth. Let $x = (\varphi' : \underline{A}_\gamma \to \underline{A}_\xi) \in S'_\xi \cap S''_\gamma$. We know that the projection $\mathrm{pr}_0 : \mathcal{S}'_{2,1,N,(p)} \to \mathcal{S}_{2,1,N}$ induces an isomorphism from S'_ξ to V'_ξ. Therefore, pr_0 maps the one-dimensional subspace $T_x(S'_\xi)$ of $T_x(\mathcal{A}'_{2,1,N,(p)} \otimes \overline{\mathbb{F}}_p)$ onto the one-dimensional subspace $T_{\mathrm{pr}_0(x)}(V'_\xi)$ of $T_{\mathrm{pr}_0(x)}(\mathcal{A}_{2,1,N} \otimes \overline{\mathbb{F}}_p)$, where

$T_x(X)$ denotes the tangent space of a variety X at a point x. On the other hand, pr_0 maps the subspace $T_x(S''_\gamma)$ to zero. This shows $T_x(S'_\xi) \neq T_x(S''_\gamma)$ in $T_x(\mathcal{A}'_{2,1,N,(p)} \otimes \overline{\mathbb{F}}_p)$; particularly $\mathcal{S}'_{2,1,N,(p)}$ has ordinary double singularity at x. Since every singular point lies in both S'_ξ and S''_γ for some ξ, γ, by Subsection 4.4 each S'_ξ has p^2+1 singular points and each S''_γ has $p+1$ singular points. We get

$$|(\mathcal{S}'_{2,1,N,(p)})^{\mathrm{sing}}| = |\Lambda_{2,1,N}|(p+1), \quad \text{and} \quad |(\mathcal{S}'_{2,1,N,(p)})^{\mathrm{sing}}| = |\Lambda|(p^2+1).$$

This completes the proof. ∎

COROLLARY 4.6. *We have*

$$|(\mathcal{S}'_{2,1,N,(p)})^{\mathrm{sing}}| = |\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})| \cdot \frac{(-1)\zeta(-1)\zeta(-3)}{4}(p-1)(p^2+1)(p+1)$$

and

$$|\Lambda| = |\operatorname{Sp}_4(\mathbb{Z}/N\mathbb{Z})| \cdot \frac{(-1)\zeta(-1)\zeta(-3)}{4}(p^2-1).$$

PROOF. This follows from Corollary 3.3 and (2) of Proposition 4.5. ∎

Note that the evaluation of $|\Lambda|$ here is different from that given in Katsura-Oort [5]. Their method does not rely on the mass formula but the computation is more complicated.

Since $\mathcal{S}_{2,1,N,(p)} \simeq \mathcal{S}'_{2,1,N,(p)}$ (Subsection 4.5), Theorem 1.2 follows from Proposition 4.5 and Corollary 4.6.

As a byproduct, we obtain the description of the supersingular locus $\mathcal{S}_{2,p,N}$.

THEOREM 4.7.
(1) *The scheme $\mathcal{S}_{2,p,N}$ is equi-dimensional and each irreducible component is isomorphic to $\mathbf{P}^1$.*
(2) *The scheme $\mathcal{S}_{2,p,N}$ has $|\Lambda_{2,1,N}|$ irreducible components.*
(3) *The singular locus of $\mathcal{S}_{2,p,N}$ consists of superspecial points (A, λ, η) with $\ker \lambda \simeq \alpha_p \times \alpha_p$, and thus $|\mathcal{S}^{\mathrm{sing}}_{2,p,N}| = |\Lambda|$. Moreover, at each singular point there are p^2+1 irreducible components passing through and intersecting transversely.*
(4) *The natural morphism $\mathrm{pr}_1 : \mathcal{S}_{2,1,N,(p)} \to \mathcal{S}_{2,p,N}$ contracts $|\Lambda|$ projective lines onto the singular locus of $\mathcal{S}_{2,p,N}$.*

5. THE CLASS NUMBERS $H_n(p,1)$ AND $H_n(1,p)$

In this section we describe the arithmetic part of the results in Li and Oort [8]. Our references are Ibukiyama-Katsura-Oort [4, Section 2] and Li-Oort [8, Section 4].

Let B be the definite quaternion algebra over $\mathbb{Q}$ with discriminant p, and $\mathcal{O}$ be a maximal order of B. Let $V = B^{\oplus n}$, regarded as a left B-module of row vectors, and let $\psi(x,y) = \sum_{i=1}^n x_i \bar{y}_i$ be the standard hermitian form on V, where $y_i \mapsto \bar{y}_i$ is the canonical involution on B. Let G be the group of ψ-similitudes over $\mathbb{Q}$; its group of $\mathbb{Q}$-points is

$$G(\mathbb{Q}) := \{ h \in M_n(B) \,|\, h\bar{h}^t = rI_n \text{ for some } r \in \mathbb{Q}^\times \}.$$

Two $\mathcal{O}$-lattices L and L' in $B^{\oplus n}$ are called *globally equivalent* (denoted by $L \sim L'$) if $L' = Lh$ for some $h \in G(\mathbb{Q})$. For a finite place v of $\mathbb{Q}$, we write $B_v := B \otimes \mathbb{Q}_v$, $\mathcal{O}_v := \mathcal{O} \otimes \mathbb{Z}_v$ and $L_v := L \otimes \mathbb{Z}_v$. Two $\mathcal{O}$-lattices L and L' in $B^{\oplus n}$ are called *locally equivalent at* v (denoted by $L_v \sim L'_v$) if $L'_v = L_v h_v$ for some $h_v \in G(\mathbb{Q}_v)$. A *genus* of $\mathcal{O}$-lattices is a set of (global) $\mathcal{O}$-lattices in $B^{\oplus n}$ which are equivalent to each other locally at every finite place v.
Let

$$N_p = \mathcal{O}_p^{\oplus n} \cdot \begin{pmatrix} I_r & 0 \\ 0 & \pi I_{n-r} \end{pmatrix} \cdot \xi \subset B_p^{\oplus n},$$

where r is the integer $[n/2]$, π is a uniformizer in $\mathcal{O}_p$, and ξ is an element in $\mathrm{GL}_n(B_p)$ such that

$$\xi \bar{\xi}^t = \text{anti-diag}(1, 1, \ldots, 1).$$

DEFINITION 5.1. (1) Let $\mathcal{L}_n(p, 1)$ denote the set of global equivalence classes of $\mathcal{O}$-lattices L in $B^{\oplus n}$ such that $L_v \sim \mathcal{O}_v^{\oplus n}$ at every finite place v. The genus $\mathcal{L}_n(p, 1)$ is called the *principal genus*, and let $H_n(p, 1) := |\mathcal{L}_n(p, 1)|$.
(2) Let $\mathcal{L}_n(1, p)$ denote the set of global equivalence classes of $\mathcal{O}$-lattices L in $B^{\oplus n}$ such that $L_p \sim N_p$ and $L_v \sim \mathcal{O}_v^{\oplus n}$ at every finite place $v \neq p$. The genus $\mathcal{L}_n(p, 1)$ is called the *non-principal genus*, and let $H_n(1, p) := |\mathcal{L}_n(1, p)|$.

Recall (Section 3) that Λ_g is the set of isomorphism classes of g-dimensional principally polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$. When $g = 2D > 0$ is even, we denote by Λ^*_{g,p^D} the set of isomorphism classes of g-dimensional polarized superspecial abelian varieties (A, λ) of degree p^{2D} over $\overline{\mathbb{F}}_p$ satisfying $\ker \lambda = A[F]$.
Let $\mathcal{A}_{g,1}$ be the *coarse moduli scheme* of g-dimensional principally polarized abelian varieties, and let $\mathcal{S}_{g,1}$ be the supersingular locus of $\mathcal{A}_{g,1} \otimes \overline{\mathbb{F}}_p$. Recall (Subsection 2.1) that $\Pi_0(\mathcal{S}_{g,1})$ denotes the set of irreducible components of $\mathcal{S}_{g,1}$.

THEOREM 5.2 (Li-Oort). *We have*

$$|\Pi_0(\mathcal{S}_{g,1})| = \begin{cases} |\Lambda_g| & \text{if } g \text{ is odd;} \\ |\Lambda^*_{g,p^D}| & \text{if } g = 2D \text{ is even.} \end{cases}$$

The arithmetic part for $\Pi_0(\mathcal{S}_{g,1})$ is given by the following

PROPOSITION 5.3.
(1) *For any positive integer g, one has $|\Lambda_g| = H_g(p, 1)$.*
(2) *For any even positive integer $g = 2D$, one has $|\Lambda^*_{g,p^D}| = H_g(1, p)$.*

PROOF. (1) See [4, Theorem 2.10]. (2) See [8, Proposition 4.7].

6. CORRESPONDENCE COMPUTATION

6.1. Let M_0 be a superspecial Dieudonné module over k of rank $2g$, and call

$$\tilde{M}_0 := \{x \in M_0; F^2 x = px\},$$

the skeleton of M_0 (cf. [8, 5.7]). We know that $\tilde{M}_0$ is a Dieudonné module over $\mathbb{F}_{p^2}$ and $\tilde{M}_0 \otimes_{W(\mathbb{F}_{p^2})} W(k) = M_0$. The vector space $\tilde{M}_0/V\tilde{M}_0$ defines an $\mathbb{F}_{p^2}$-structure of the k-vector space M_0/VM_0.
Let $\mathrm{Gr}(n,m)$ be the Grassmannian variety of n-dimensional subspaces in an m-dimensional vector space. Suppose M_1 is a Dieudonné submodule of M_0 such that

$$VM_0 \subset M_1 \subset M_0, \quad \dim_k M_1/VM_0 = r,$$

for some integer $0 \le r \le g$. As $\dim M_0/VM_0 = g$, the subspace $\overline{M}_1 := M_1/VM_0$ corresponds to a point in $\mathrm{Gr}(r,g)(k)$.

LEMMA 6.1. *Notation as above. Then M_1 is superspecial (i.e. $F^2M_1 = pM_1$) if and only if $\overline{M}_1 \in \mathrm{Gr}(r,g)(\mathbb{F}_{p^2})$.*

PROOF. If M_1 is generated by $V\tilde{M}_0$ and $x_1, x_2, \ldots, x_r$, $x_i \in \tilde{M}_0$ over W. Then $\tilde{M}_1$ generates M_1 and thus $F^2M_1 = pM_1$. Therefore, M_1 is superspecial. Conversely if M_1 is superspecial, then we have

$$V\tilde{M}_0 \ \subset\ \tilde{M}_1 \ \subset \tilde{M}_0.$$

Therefore, $\tilde{M}_1$ gives rise to an element in $\mathrm{Gr}(r,g)(\mathbb{F}_{p^2})$. ∎

6.2. Let $L(n,2n) \subset \mathrm{Gr}(n,2n)$ be the Lagrangian variety of maximal isotropic subspaces in a $2n$-dimensional vector space with a non-degenerate alternating form.
From now on $g = 2D$ is an even positive integer. Recall (in Introduction and Section 5) that $\Lambda^*_{g,p^D,N}$ denotes the set of superspecial (geometric) points (A,λ,η) in $\mathcal{A}_{g,p^D,N} \otimes \overline{\mathbb{F}}_p$ satisfying $\ker\lambda = A[F]$.

LEMMA 6.2. *Let $(A_2,\lambda_2,\eta_2) \in \Lambda^*_{g,p^D,N}$ and $(M_2, \langle\,,\rangle_2)$ be the associated Dieudonné module. There is a W-basis $e_1, \ldots, e_{2g}$ for M_2 such that for $1 \le i \le g$*

$$Fe_i = e_{g+i}, \quad Fe_{g+i} = pe_i,$$

and the non-zero pairings are

$$\langle e_i, e_{D+i}\rangle_2 = -\langle e_{D+i}, e_i\rangle_2 = \frac{1}{p},$$

$$\langle e_{g+i}, e_{g+D+i}\rangle_2 = -\langle e_{g+D+i}, e_{g+i}\rangle_2 = 1,$$

for $1 \le i \le D$.

PROOF. Use the same argument of Lemma 4.2 (2).

6.3. Let $\mathcal{H}$ be the moduli space over $\mathbb{Z}_{(p)}[\zeta_N]$ which parametrizes equivalence classes of objects $(\varphi : \underline{A}_1 \to \underline{A}_2)$, where

- $\underline{A}_1 = (A_1,\lambda_1,\eta_1)$ is an object in $\mathcal{A}_{g,1,N}$,
- $\underline{A}_2 = (A_2,\lambda_2,\eta_2)$ is an object in $\mathcal{A}_{g,p^D,N}$, and
- $\varphi : A_1 \to A_2$ is an isogeny of degree p^D satisfying $\varphi^*\lambda_2 = p\lambda_1$ and $\varphi_*\eta_1 = \eta_2$.

The moduli space $\mathcal{H}$ with two natural projections gives the following correspondence:

$$\begin{array}{ccc} & \mathcal{H} & \\ {}^{\mathrm{pr}_1}\swarrow & & \searrow^{\mathrm{pr}_2} \\ \mathcal{A}_{g,1,N} & & \mathcal{A}_{g,p^D,N}. \end{array}$$

Let $\mathcal{S}$ be the supersingular locus of $\mathcal{H}\otimes\overline{\mathbb{F}}_p$, which is the reduced closed subscheme consisting of supersingular points (either A_1 or A_2 is supersingular, or equivalently both are supersingular). Restricting the natural projections on $\mathcal{S}$, we have the following correspondence

$$\begin{array}{ccc} & \mathcal{S} & \\ {}^{\mathrm{pr}_1}\swarrow & & \searrow^{\mathrm{pr}_2} \\ \mathcal{S}_{g,1,N} & & \mathcal{S}_{g,p^D,N}. \end{array}$$

Suppose that $\underline{A}_2 \in \Lambda^*_{g,p^D,N}$. Let $(\varphi : \underline{A}_1 \to \underline{A}_2) \in \mathcal{S}(k)$ be a point in the pre-image $\mathrm{pr}_2^{-1}(\underline{A}_2)$, and let $(M_1, \langle\, ,\rangle_1)$ be the Dieudonné module associated to $\underline{A}_1$. We have

$$M_1 \subset M_2, \quad p\langle\, ,\rangle_2 = \langle\, ,\rangle_1, \quad FM_2 = M_2^t.$$

Since $\underline{A}_2$ is superspecial and $\langle\, ,\rangle_1$ is a perfect pairing on M_1, we get

$$FM_2 = VM_2 = M_2^t, \quad M_2^t \subset M_1^t = M_1.$$

Therefore, we have

$$FM_2 = VM_2 \subset M_1 \subset M_2, \quad \dim_k M_1/VM_2 = D.$$

Put $\langle\, ,\rangle := p\langle\, ,\rangle_2$. The pairing

$$\langle\, ,\rangle : M_2 \times M_2 \to W$$

induces a pairing

$$\langle\, ,\rangle : M_2/VM_2 \times M_2/VM_2 \to k$$

which is perfect (by Lemma 6.2). Furthermore, M_1/VM_2 is a maximal isotropic subspace for the pairing $\langle\, ,\rangle$. This is because $\langle\, ,\rangle_1$ is a perfect pairing on M_1 and $\dim M_1/VM_2 = D$ is the maximal dimension of isotropic subspaces. We conclude that the point $(\varphi : \underline{A}_1 \to \underline{A}_2)$ lies in $\mathrm{pr}_2^{-1}(\underline{A}_2)$ if and only if $VM_2 \subset M_1 \subset M_2$ and M_1/VM_2 is a maximal isotropic subspace of the symplectic space $(M_2/VM_2, \langle\, ,\rangle)$. By Lemma 6.1, we have proved

PROPOSITION 6.3. *Let $\underline{A}_2$ be a point in $\Lambda^*_{g,p^D,N}$.*
(1) *The pre-image $\mathrm{pr}_2^{-1}(\underline{A}_2)$ is naturally isomorphic to the projective variety $L(D,2D)$ over k.*
(2) *The set $\mathrm{pr}_1^{-1}(\Lambda_{g,1,N}) \cap \mathrm{pr}_2^{-1}(\underline{A}_2)$ is in bijection with $L(D,2D)(\mathbb{F}_{p^2})$, where the $W(\mathbb{F}_{p^2})$-structure of M_2 is given by the skeleton $\tilde{M}_2$.*

6.4. We compute $\mathrm{pr}_1^{-1}(\underline{A}_1)\cap \mathrm{pr}_2^{-1}(\Lambda^*_{g,p^D,N})$ for a point $\underline{A}_1$ in $\Lambda_{g,1,N}$. Let $\mathcal{T}$ be the closed subscheme of $\mathcal{S}$ consisting of the points $(\varphi:\underline{A}_1\to\underline{A}_2)$ such that $\ker\lambda_2=A_2[F]$. We compute the closed subvariety $\mathrm{pr}_1^{-1}(\underline{A}_1)\cap\mathcal{T}$ first.
Let $\underline{A}_1\in\Lambda_{g,1,N}$, and let $(\varphi:\underline{A}_1\to\underline{A}_2)\in\mathcal{S}(k)$ be a point in the pre-image $\mathrm{pr}_1^{-1}(\underline{A}_1)$. Let $(M_1,\langle\,,\rangle_1)$ and $(M_2,\langle\,,\rangle_2)$ be the Dieudonné modules associated to $\underline{A}_1$ and $\underline{A}_2$, respectively.
One has

$$M_1^t=M_1\supset M_2^t=FM_2,$$

and thus has

$$FM_2\subset M_1\subset M_2\subset p^{-1}VM_1.$$

Since M_1 is superspecial, $p^{-1}VM_1=p^{-1}FM_1$. Put $M_0:=p^{-1}VM_1$ and $\langle\,,\rangle:=p\langle\,,\rangle_2$. We have

$$pM_0\subset M_2^t=FM_2\subset M_1=VM_0\subset M_2\subset M_0$$

and that $\langle\,,\rangle$ is a perfect pairing on M_0. By Proposition 6.1 of [8] (cf. Lemma 4.2 (1)), there is a W-basis $f_1\dots,f_{2g}$ for M_0 such that for $1\le i\le g$

$$Ff_i=f_{g+i},\quad Ff_{g+i}=pf_i,$$

and the non-zero pairings are

$$\langle f_i,f_{g+i}\rangle=-\langle f_{g+i},f_i\rangle=\beta_1,\quad\forall\,1\le i\le g$$

where $\beta_1\in W(\mathbb{F}_{p^2})^\times$ with $\beta_1^\sigma=-\beta_1$. In the vector space $\overline{M}_0:=M_0/pM_0$, $\overline{M}_2$ is a vector subspace over k of dimension $g+D$ with

$$\overline{M}_2\supset\overline{VM}_0=k<f_{g+1},\dots,f_{2g}>\quad\text{and}\quad\langle\overline{M}_2,F\overline{M}_2\rangle=0.$$

We can write

$$\overline{M}_2=k<v_1,\dots,v_D>+\overline{VM}_0,\quad v_i=\sum_{r=1}^g a_{ir}f_r.$$

One computes

$$\langle v_i,Fv_j\rangle=\langle\sum_{r=1}^g a_{ir}f_r,F(\sum_{q=1}^g a_{jq}f_q)\rangle=\langle\sum_{r=1}^g a_{ir}f_r,\sum_{q=1}^g a_{jq}^pf_{g+q}\rangle=\beta_1\sum_{r=1}^g a_{ir}a_{jr}^p.$$

This computation leads us to the following definition.

6.5. Let $V:=\mathbb{F}_{p^2}^{2n}$. For any field $K\supset\mathbb{F}_{p^2}$, we put $V_K:=V\otimes_{\mathbb{F}_{p^2}}K$ and define a pairing on V_K

$$\langle\,,\rangle':V_K\times V_K\to K,\quad\langle(a_i),(b_i)\rangle':=\sum_{i=1}^{2n}a_i\,b_i^p.$$

Let $\mathbf{X}(n,2n)\subset\mathrm{Gr}(n,2n)$ be the subvariety over $\mathbb{F}_{p^2}$ which parametrizes n-dimensional (maximal) isotropic subspaces in V with respect to the pairing $\langle\,,\rangle'$.
With the computation in Subsection 6.4 and Lemma 6.1, we have proved

PROPOSITION 6.4. *Let $\underline{A}_1$ be a point in $\Lambda_{g,1,N}$ and $g = 2D$.*
(1) *The intersection $\mathrm{pr}_1^{-1}(\underline{A}_1) \cap \mathcal{T}$ is naturally isomorphic to the projective variety $\mathbf{X}(n, 2n)$ over k.*
(2) *The set $\mathrm{pr}_1^{-1}(\underline{A}_1) \cap \mathrm{pr}_2^{-1}(\Lambda^*_{g,p^D,N})$ is in bijection with $\mathbf{X}(D, 2D)(\mathbb{F}_{p^2})$.*

When $g = 2$, Proposition 6.4 (2) is a result of Moret-Bailly (Lemma 4.3).

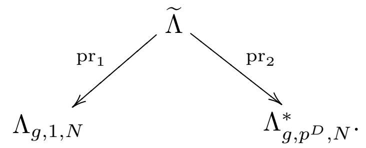
6.6. To compute $\mathbf{X}(n, 2n)(\mathbb{F}_{p^2})$, we show that it is the set of rational points of a homogeneous space under the quasi-split group $U(n, n)$.
Let $V = \mathbb{F}_{p^2}^{2n}$ and let $x \mapsto \bar{x}$ be the involution of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$. Let $\psi((x_i), (y_i)) = \sum_i x_i \bar{y}_i$ be the standard hermitian form on V. For any field $K \supset \mathbb{F}_p$, we put $V_K := V \otimes_{\mathbb{F}_p} K$ and extend ψ to a from

$$\psi : V_K \otimes V_K \to \mathbb{F}_{p^2} \otimes K$$

by K-linearity.
Let $U(n, n)$ be the group of automorphisms of V that preserve the hermitian form ψ. Let $LU(n, 2n)(K)$ be the space of n-dimensional (maximal) isotropic K-subspaces in V_K with respect to ψ. We know that $LU(n, 2n)$ is a projective scheme over $\mathbb{F}_p$ of finite type, and this is a homogeneous space under $U(n, n)$. It follows from the definition that

$$LU(n, 2n)(\mathbb{F}_p) = \mathbf{X}(n, 2n)(\mathbb{F}_{p^2}).$$

However, the space $LU(n, 2n)$ is not isomorphic to the space $\mathbf{X}(n, 2n)$ over k.
Let $\widetilde{\Lambda}$ be the subset of $\mathcal{S}$ consisting of elements $(\varphi : \underline{A}_1 \to \underline{A}_2)$ such that $\underline{A}_2 \in \Lambda^*_{g,p^D,N}$ and $\underline{A}_1 \in \Lambda_{g,1,N}$. We have natural projections



By Propositions 6.3 and 6.4, and Subsection 6.6, we have proved

PROPOSITION 6.5. *Notation as above, one has*

$$|\widetilde{\Lambda}| = |L(D, 2D)(\mathbb{F}_{p^2})| \cdot |\Lambda^*_{g,p^D,N}| = |LU(D, 2D)(\mathbb{F}_p)| \cdot |\Lambda_{g,1,N}|.$$

THEOREM 6.6. *We have*

$$|\Lambda^*_{g,p^D,N}| = |\operatorname{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \cdot \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{i=1}^{g} \zeta(1 - 2i) \right\} \cdot \prod_{i=1}^{D} (p^{4i-2} - 1).$$

PROOF. We compute in Section 7 that

$$|L(D, 2D)(\mathbb{F}_{p^2})| = \prod_{i=1}^{D} (p^{2i} + 1),$$

$$|LU(D, 2D)(\mathbb{F}_p)| = \prod_{i=1}^{D} (p^{2i-1} + 1).$$

Using Proposition 6.5, Theorem 3.1 and Lemma 3.2, we get the value of $|\Lambda^*_{g,p^D,N}|$. ∎

6.7. PROOF OF THEOREM 1.4. By a theorem of Li and Oort (Theorem 5.2), we know

$$|\Pi_0(\mathcal{S}_{g,1,N})| = \begin{cases} |\Lambda_{g,1,N}| & \text{if } g \text{ is odd;} \\ |\Lambda^*_{g,p^D,N}| & \text{if } g = 2D \text{ is even.} \end{cases}$$

Note that the result of Li and Oort is formulated for the coarse moduli space $\mathcal{S}_{g,1}$. However, it is clear that adding the level-N structure yields a modification as above. Theorem 1.4 then follows from Theorem 3.1, Lemma 3.2 and Theorem 6.6. ∎

7. $L(n,2n)(\mathbb{F}_q)$ AND $LU(n,2n)(\mathbb{F}_q)$

Let $L(n,2n)$ be the Lagrangian variety of maximal isotropic subspaces in a $2n$-dimensional vector space V_0 with a non-degenerate alternating form ψ_0.

LEMMA 7.1. $|L(n,2n)(\mathbb{F}_q)| = \prod_{i=1}^n (q^i+1)$.

PROOF. Let $e_1,\dots,e_{2n}$ be the standard symplectic basis for V_0. The group $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ acts transitively on the space $L(n,2n)(\mathbb{F}_q)$. For $h \in \mathrm{Sp}_{2n}(\mathbb{F}_q)$, the map $h \mapsto \{he_1, \dots he_{2n}\}$ induces a bijection between $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ and the set $\mathcal{B}(n)$ of ordered symplectic bases $\{v_1,\dots,v_{2n}\}$ for V_0. The first vector v_1 has $q^{2n}-1$ choices. The first companion vector v_{n+1} has $(q^{2n}-q^{2n-1})/(q-1)$ choices as it does not lie in the hyperplane $v_1^\perp$ and we require $\psi_0(v_1,v_{n+1})=1$. The remaining ordered symplectic basis can be chosen from the complement $\mathbb{F}_q < v_1, v_{n+1} >^\perp$. Therefore, we have proved the recursive formula

$$|\mathrm{Sp}_{2n}(\mathbb{F}_q)| = (q^{2n}-1)q^{2n-1}|\mathrm{Sp}_{2n-2}(\mathbb{F}_q)|.$$

From this, we get

$$|\mathrm{Sp}_{2n}(\mathbb{F}_q)| = q^{n^2}\prod_{i=1}^n (q^{2i}-1).$$

Let P be the stabilizer of the standard maximal isotropic subspace $\mathbb{F}_q < e_1,\dots,e_n >$. It is easy to see that

$$P = \left\{ \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}; AD^t = I_n,\ BA^t = AB^t \right\}.$$

The matrix BA^t is symmetric and the space of $n\times n$ symmetric matrices has dimension $(n^2+n)/2$. This yields

$$|P| = q^{\frac{n^2+n}{2}}\,|\mathrm{GL}_n(\mathbb{F}_q)| = q^{n^2}\prod_{i=1}^n (q^i-1)$$

as one has

$$|\mathrm{GL}_n(\mathbb{F}_q)| = q^{\frac{n^2-n}{2}}\prod_{i=1}^n (q^i-1).$$

Since $L(n,2n)(\mathbb{F}_q) \simeq \mathrm{Sp}_{2n}(\mathbb{F}_q)/P$, we get $|L(n,2n)(\mathbb{F}_q)| = \prod_{i=1}^n (q^i+1)$. ∎

7.1. Let $V=\mathbb{F}_{q^2}^{2n}$ and let $x\mapsto \bar x = x^q$ be the involution of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Let $\psi((x_i),(y_i))=\sum_i x_i\bar y_i$ be the standard hermitian form on V. For any field $K\supset \mathbb{F}_q$, we put $V_K:=V\otimes_{\mathbb{F}_p} K$ and extend ψ to a from

$$\psi : V_K\otimes V_K\to \mathbb{F}_{q^2}\otimes_{\mathbb{F}_q} K$$

by K-linearity.
Let $U(n,n)$ be the group of automorphisms of V that preserve the hermitian form ψ. Let $LU(n,2n)(K)$ be the set of n-dimensional (maximal) isotropic K-subspaces in V_K with respect to ψ. We know that $LU(n,2n)$ is a homogeneous space under $U(n,n)$. Let

$$I_m := \{\underline{a}=(a_1,\dots,a_m)\in \mathbb{F}_{q^2}^m\,;\ Q(\underline{a})=0\},$$

where $Q(\underline{a})=a_1^{q+1}+\cdots+a_m^{q+1}$.

LEMMA 7.2. *We have* $|I_m|=q^{2m-1}+(-1)^m q^m+(-1)^{m-1}q^{m-1}$.

PROOF. For $m>1$, consider the projection $p: I_m\to \mathbb{F}_{q^2}^{m-1}$ which sends $(a_1,\dots,a_m)$ to $(a_1,\dots,a_{m-1})$. Let I_{m-1}^c be the complement of I_{m-1} in $\mathbb{F}_{q^2}^{m-1}$. If $x\in I_{m-1}$, then the pre-image $p^{-1}(x)$ consists of one element. If $x\in I_{m-1}^c$, then the pre-image $p^{-1}(x)$ consists of solutions of the equation $a_m^{q+1}=-Q(x)\in \mathbb{F}_q^\times$ and thus $p^{-1}(x)$ has $q+1$ elements. Therefore, $|I_m|=|I_{m-1}|+(q+1)|I_{m-1}^c|$. From this we get the recursive formula

$$|I_m|=(q+1)q^{2(m-1)}-q|I_{m-1}|.$$

We show the lemma by induction. When $m=1$, $|I_m|=1$ and the statement holds. Suppose the statement holds for $m=k$, i.e. $|I_k|=q^{2k-1}+(-1)^k q^k+(-1)^{k-1}q^{k-1}$. When $m=k+1$,

$$\begin{aligned}|I_{k+1}| &= (q+1)q^{2k}-q[q^{2k-1}+(-1)^k q^k+(-1)^{k-1}q^{k-1}]\\ &= q^{2k+1}+(-1)^{k+1}q^{k+1}+(-1)^k q^k.\end{aligned}$$

This completes the proof. ∎

PROPOSITION 7.3. $|LU(n,2n)(\mathbb{F}_q)|=\prod_{i=1}^n (q^{2i-1}+1)$.

PROOF. We can choose a new basis $e_1,\dots,e_{2n}$ for V such that the non-zero pairings are

$$\psi(e_i,e_{n+i})=\psi(e_{n+i},e_i)=1,\quad \forall\, 1\le i\le n.$$

The representing matrix for ψ with respect to $\{e_1,\dots,e_{2n}\}$ is

$$J=\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}.$$

Let P be the stabilizer of the standard maximal isotropic subspace $\mathbb{F}_{q^2} < e_1,\dots,e_n >$. It is easy to see that

$$P=\left\{\begin{pmatrix}A & B\\ 0 & D\end{pmatrix}; AD^*=I_n,\ BA^*+AB^*=0\right\}.$$

The matrix BA^* is skew-symmetric hermitian. The space of $n \times n$ skew-symmetric hermitian matrices has dimension n^2 over $\mathbb{F}_q$. Indeed, the diagonal consists of entries in the kernel of the trace; this gives dimension n. The upper triangular has $(n^2-n)/2$ entries in $\mathbb{F}_{q^2}$; this gives dimension n^2-n. Hence,

$$|P| = q^{n^2}|\,\mathrm{GL}_n(\mathbb{F}_{q^2})| = q^{2n^2-n}\prod_{i=1}^{n}(q^{2i}-1).$$

We compute $|U(n,n)(\mathbb{F}_q)|$. For $h \in U(n,n)(\mathbb{F}_q)$, the map

$$h \mapsto \{he_1, \dots, he_{2n}\}$$

gives a bijection between $U(n,n)(\mathbb{F}_q)$ and the set $\mathcal{B}(n)$ of ordered bases $\{v_1,\dots,v_{2n}\}$ for which the representing matrix of ψ is J. The first vector v_1 has

$$|I_{2n}| - 1 = q^{4n-1} + q^{2n} - q^{2n-1} - 1 = (q^{2n}-1)(q^{2n-1}+1).$$

choices (Lemma 7.2). For the choices of the companion vector v_{n+1} with $\psi(v_{n+1}, v_{n+1}) = 0$ and $\psi(v_1, v_{n+1}) = 1$, consider the set

$$Y := \{v \in V; \psi(v_1, v) = 1\}.$$

Clearly, $|Y| = q^{4n-2}$. The additive group $\mathbb{F}_{q^2}$ acts on Y by $a \cdot v = v + av_1$ for $a \in \mathbb{F}_{q^2}$, $v \in Y$. It follows from

$$\psi(v+av_1, v+av_1) = \psi(v,v) + \bar{a} + a$$

that every orbit $O(v)$ contains an isotropic vector v_0 and any isotropic vector in $O(v)$ has the form $v_0 + av_1$ with $\bar{a} + a = 0$. Hence, the vector v_{n+1} has

$$\frac{|\,Y|\,q}{q^2} = q^{4n-3}$$

choices. In conclusion, we have proved the recursive formula

$$|U(n,n)(\mathbb{F}_q)| = (q^{2n}-1)(q^{2n-1}+1)q^{4n-3}|U(n-1,n-1)(\mathbb{F}_q)|.$$

It follows that

$$|U(n,n)(\mathbb{F}_q)| = q^{2n^2-n}\prod_{i=1}^{n}(q^{2i}-1)(q^{2i-1}+1).$$

Since $LU(n,2n)(\mathbb{F}_q) \simeq U(n,n)(\mathbb{F}_q)/P$, we get $|LU(n,2n)(\mathbb{F}_q)| = \prod_{i=1}^{n}(q^{2i-1}+1)$. ∎

References

[1] M. Demazure, *Lectures on p-divisible groups.* Lecture Notes in Math., vol. 302, Springer-Verlag, 1972.

[2] T. Ekedahl, On supersingular curves and supersingular abelian varieties. *Math. Scand.* 60 (1987), 151–178.

[3] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms, *J. Fac. Sci. Univ. Tokyo* 27 (1980), 549–601.

[4] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers. *Compositio Math.* 57 (1986), 127–152.

[5] T. Katsura and F. Oort, Families of supersingular abelian surfaces, *Compositio Math.* 62 (1987), 107–167.

[6] T. Katsura and F. Oort, Supersingular abelian varieties of dimension two or three and class numbers. *Adv. St. Pure Math.* (Algebraic Geometry, Sendai, 1985, Ed. T. Oda) (1987).

[7] N. Koblitz, p-adic variant of the zeta-function of families of varieties defined over finite fields. *Compositio Math.* 31 (1975), 119–218.

[8] K.-Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties.* Lecture Notes in Math., vol. 1680, Springer-Verlag, 1998.

[9] L. Moret-Bailly, Familles de courbes et de variétés abéliennes sur $\mathbf{P}^1$. Sém. sur les pinceaux de courbes de genre au moins deux (ed. L. Szpiro). *Astériques* 86 (1981), 109–140.

[10] D. Mumford, *Abelian Varieties.* Oxford University Press, 1974.

[11] C.-F. Yu, On the mass formula of supersingular abelian varieties with real multiplications. *J. Australian Math. Soc.* 78 (2005), 373–392.

Chia-Fu Yu
Institute of Mathematics
Academia Sinica
128 Academia Rd. Sec. 2
Nankang
Taipei
Taiwan
and NCTS (Taipei Office)
chiafu@math.sinica.edu.tw

Capacité Associeé a un Courant Positif Fermé

Dabbek Khalifa et Elkhadhra Fredj

Received: December 12, 2005
Revised: July 24, 2006

Communicated by Thomas Peternell

Abstract. Let Ω be an open set of $\mathbb{C}^n$ and T be a positive closed current of dimension $p \geq 1$ on Ω, we define a capacity associated to T by :

$$C_T(K,\Omega) = C_T(K) = \sup\left\{\int_K T \wedge (dd^c v)^p,\ v \in \mathrm{psh}(\Omega),\ 0 < v < 1\right\}$$

where K is a compact set of Ω.
We prove, in the same way as Bedford-Taylor, that a locally bounded plurisubharmonic function is quasi-continuous with respect to C_T. In the second part we define the convergence relatively to C_T and we prove that if (u_j) is a family of locally uniformly bounded plurisubharmonic functions and u is a locally bounded plurisubharmonic function such that $u_j \to u$ relatively to C_T then $T \wedge (dd^c u_j)^p \to T \wedge (dd^c u)^p$ in the current sense.

2000 Mathematics Subject Classification: 32C30 ; 31C10 ; 31A15 ; 32W20.
Keywords and Phrases: courant positif, plurisousharmonique , capacité, operateur de Monge Ampère.

1 Introduction

Soient Ω un ouvert de $\mathbb{C}^n$, K un compact de Ω et T un courant positif fermé de dimension $p \geq 1$ sur Ω. On note psh(Ω) l'ensemble de fonctions plurisousharmonique sur Ω et $L^\infty_{loc}(\Omega)$ l'ensemble de fonctions localement bornées. On définit la capacité de K (dans Ω) relativement à T par :

$$C_T(K,\Omega) = C_T(K) = \sup\left\{\int_K T \wedge (dd^c v)^p,\ v \in \mathrm{psh}(\Omega),\ 0 < v < 1\right\}$$

Dans la prémière partie on montre qu'une fonction plurisousharmonique localement bornée est continue en dehors d'un ouvert de capacité arbitrairement petite :

Théorème 1.1 *Soient Ω un ouvert borné de $\mathbb{C}^n$, $u \in \mathrm{psh}(\Omega) \cap \mathrm{L}^\infty_{\mathrm{loc}}(\Omega)$ et T un courant positif fermé sur Ω de dimension $p \geq 1$. Alors pour tout $\varepsilon > 0$, il existe un ouvert $\mathcal{O}$ de Ω tel que $C_T(\mathcal{O}, \Omega) < \varepsilon$ et u soit continue sur $\Omega \setminus \mathcal{O}$.*

Ce résultat est prouvé dans [Be-Ta] pour $T = 1$. L'intérêt de ce théorème est dû en partie au résultat suivant, qui constitue une généralisation d'un théorème de [Be-Ta].

Théorème 1.2 (théorème de Comparaison) *Soient Ω un ouvert borné de $\mathbb{C}^n$, T un courant positif fermé de dimension $p \geq 1$ sur Ω, u et $v \in \mathrm{psh}(\Omega) \cap \mathrm{L}^\infty(\Omega)$. Supposons que :*

$$\liminf_{\xi \to \partial\Omega} (u(\xi) - v(\xi)) \geq 0$$

Alors on a :

$$\int_{\{u<v\}} T \wedge (dd^c v)^p \leq \int_{\{u<v\}} T \wedge (dd^c u)^p$$

Dans la deuxième partie on définit la notion de convergence par rapport à C_T. On dit que u_j converge vers u par rapport à C_T sur E si pour tout $\delta > 0$, on a :

$$\lim_{j \to +\infty} C_T\Big(\big\{z \in E;\ \ |u_j(z) - u(z)| > \delta\big\}, \Omega\Big) = 0$$

On montre q'une suite de fonctions psh localement bornée décroissante vers une fonction psh est convergente par rapport à C_T :

Théorème 1.3 *Soient Ω un ouvert borné de $\mathbb{C}^n$, T un courant positif fermé sur Ω de dimension $p \geq 1$, u_j et u des fonctions psh, localement bornées sur Ω telles que $u_j = u$ sur un voisinage de $\partial\Omega$, (u_j) décroissante vers u, alors (u_j) converge vers u par rapport à C_T.*

Comme application nous généralisons des résultats de [Be-Ta] et de [Xi] sur l'opérateur de Monge-Ampère. Le théorème principale de cette partie est le suivant :

Théorème 1.4
Soient $(u_j)_j$ une suite de fonctions psh localement uniformément bornées et $u \in \mathrm{psh}(\Omega) \cap \mathrm{L}^\infty_{\mathrm{loc}}(\Omega)$, on a :
a) *Si u_j converge vers u par rapport à C_T sur chaque $E \subset\subset \Omega$, alors le courant $T \wedge (dd^c u_j)^p$ converge au sens des courants vers $T \wedge (dd^c u)^p$.*
b) *Supposons qu'il existe $E \subset\subset \Omega$ tel que $\forall j$, $u_j = u$ sur $\Omega \setminus E$ et que les suites $uT \wedge (dd^c u_j)^p$, $u_j T \wedge (dd^c u)^p$ et $u_j T \wedge (dd^c u_j)^p$ convergent au sens des courants vers $uT \wedge (dd^c u)^p$ alors u_j converge vers u par rapport à C_T sur E.*

2 Capacité associeé a un courant positif fermé

Définition 2.1

Soient Ω un ouvert de $\mathbb{C}^n$, K un compact de Ω et T un courant positif fermé de dimension $p \geq 1$ sur Ω, on définit la capacité de K (dans Ω) relativement à T par :

$$C_T(K,\Omega) = C_T(K) = \sup\left\{\int_K T \wedge (dd^c v)^p,\ v \in \mathrm{psh}(\Omega),\ 0 < v < 1\right\}$$

Pour tout $E \subset \Omega$, on pose :

$$C_T(E,\Omega) = \sup\{C_T(K),\ K \text{ compact},\ K \subset E\}$$

Proposition 2.2

1) Si E est un borélien, on a :

$$C_T(E,\Omega) = C_T(E) = \sup\left\{\int_E T \wedge (dd^c v)^p,\ v \in \mathrm{psh}(\Omega),\ 0 < v < 1\right\}$$

2) *Si $E_1 \subset E_2$, alors $C_T(E_1,\Omega) \leq C_T(E_2,\Omega)$.*

3) *Si $E \subset \Omega_1 \subset \Omega_2$, alors $C_T(E,\Omega_1) \geq C_T(E,\Omega_2)$.*

4) *Si $E_1, E_2 \ldots$ sont des ensembles boréliens dans Ω, on a :*

$$C_T\Big(\bigcup_{j\geq 1} E_j,\Omega\Big) \leq \sum_{j=1}^{+\infty} C_T(E_j,\Omega).$$

5) *Si $E_1 \subset E_2 \subset \cdots$ sont des ensembles boréliens dans Ω, alors :*

$$C_T\Big(\bigcup_{j\geq 1} E_j,\Omega\Big) = \lim_{j\to+\infty} C_T(E_j,\Omega).$$

6) *Si $f : \Omega_1 \mapsto \Omega_2$ est une fonction holomorphe, propre sur* SuppT *et $\mathcal{O}$ un ouvert de Ω_2, alors :*

$$C_{f_*T}(\mathcal{O},\Omega_2) \leq C_T(f^{-1}(\mathcal{O}),\Omega_1)$$

et l'égalité a lieu si f est un biholomorphisme.

Démonstration. Pour 1) → 5), on procède comme [Be-Ta] ; pour 6) on suppose que $0 \leq v \leq 1$ est psh, de classe $\mathcal{C}^\infty$ sur Ω_2, on a :

$$\begin{aligned}\int_{\mathcal{O}} f_*T \wedge (dd^c v)^p &= \int_{\Omega_2} f_*T \wedge (1\!\!1_{\mathcal{O}}(dd^c v)^p)\\ &= \int_{\Omega_1} T \wedge (1\!\!1_{\mathcal{O}} \circ f)(dd^c(v\circ f))^p\\ &= \int_{f^{-1}(\mathcal{O})} T \wedge (dd^c(v\circ f))^p \leq C_T(f^{-1}(\mathcal{O}),\Omega_1).\end{aligned}$$

Pour obtenir ces égalités il suffit de remplacer $1\!\!1_{\mathcal{O}}$ par une suite de fonctions de classe $\mathcal{C}^\infty$ $\varphi_k \uparrow 1\!\!1_{\mathcal{O}}$. Dans le cas général, on prend $v_\varepsilon \uparrow v$ une régularisation de v et en utilisant le fait que : $\displaystyle\int_{\mathcal{O}} f_*T \wedge (dd^c v)^p \leq \lim_{\varepsilon\to 0}\int_{\mathcal{O}} f_*T \wedge (dd^c v_\varepsilon)^p$. Si f est un biholomorphisme, on a de même

$$C_T(f^{-1}(\mathcal{O}),\Omega_1) = C_{f_*^{-1}(f_*T)}(f^{-1}(\mathcal{O}),\Omega_1) \leq C_{f_*T}(\mathcal{O},\Omega_2).$$

Dans 6), l'inégalité peut être stricte, en effet si f est l'éclatement de centre 0, $T = [E]$ le courant d'intégration sur l'ensemble exceptionnel $E = f^{-1}(0)$. $\square$

Problemes ouverts :

1) Si $\cdots \subset K_2 \subset K_1$ est une suite décroissante de compacts de Ω, alors d'après la proposition 2.2, $C_T(K_j)$ est décroissante. A-t-on $C_T(\cap K_j) = \lim_{j\to+\infty} C_T(K_j)$?

2) A-t-on l'égalité : $\tilde{C}_T \equiv C_T$?, où on a posé

$$\tilde{C}_T(K) = \sup\left\{\int_K T\wedge (dd^c v)^p,\ v \in \text{psh}(\Omega,[0,1]), v_{|K\cap \text{suppT}} \equiv 0\right\}$$

3) Soit K un compact de Ω, existe-t-il u dans $\text{psh}(\Omega,[0,1])$, telle que l'on ait $C_T(K) = \displaystyle\int_K T\wedge (dd^c u)^p$?

4) Définition : Un ensemble $A \subset \Omega$ est dit $T-$pluripolaire dans Ω si $C_T(A,\Omega) = 0$.
A est dit localement $T-$pluripolaire si, pour tout a dans A, il existe un voisinage ouvert V de a dans Ω tel que $A\cap V$ est $T-$pluripolaire dans V.
Un ensemble localement $T-$pluripolaire est-il $T-$pluripolaire dans Ω ?
Caractériser les ensembles $T-$pluripolaires dans Ω ?

Remarques.

(i) Si $T = [X]$ est le courant d'intégration sur un sous-ensemble analytique X de dimension pure p, $\mathcal{O}$ un ouvert de Ω et $\text{Reg}X$ l'ensemble des points réguliers de X. En utilisant l'égalité $\displaystyle\int_{\mathcal{O}} [X]\wedge(dd^c v)^p = \int_{\mathcal{O}\cap \text{Reg}X} (dd^c(i^*v))^p$ où $v \in \text{psh}(\Omega,[0,1])$, et $i : X \hookrightarrow \Omega$, est l'injection canonique, on a :

$\mathcal{O}$ *est localement* $[X]-$*pluripolaire* $\Longleftrightarrow$
$\text{Reg}X \cap \mathcal{O}$ *est localement pluripolaire dans* $\text{Reg}X$

On remarque que si T est un courant positif fermé de dimension $p \geq 1$ et $\nu_T(x) > 0$ $\forall x \in X$, alors un ouvert localement $T-$pluripolaire coupe $\text{Reg}X$ en un ouvert localement pluripolaire dans $\text{Reg}X$.

(ii) Si w est une fonction psh, bornée et A un borélien $T-$pluripolaire, alors A est $T\wedge(dd^c w)^k-$pluripolaire pour tout $0 \leq k \leq \text{dimT}$. En effet, il est facile de voir qu'il existe $\alpha > 0$ telle que

$$C_{T\wedge(dd^c w)^k}(A,\Omega) \leq \alpha C_T(A,\Omega).$$

En particulier si $T = 1$, on retrouve le fait que le courant $(dd^c w)^k$ ne charge pas les ensembles pluripolaires.

(iii) Soit $\varphi \in \mathrm{psh}(\Omega)$ et localement bornée sur $\Omega \setminus K$ où $K = \{\varphi = -\infty\}$. Alors

$$C_{T\wedge(dd^c\varphi)^k}(K) \geq C_T(K)\Big(C_{dd^c\varphi}(K)\Big)^k .$$

En effet, on peut supposer que $k = 1$ et soit $v \in \mathrm{psh}(\Omega, [0,1])$. Posons $\gamma = C_{dd^c\varphi}(K)$ et soit $\varphi_j = \max(\varphi, \gamma v - j)$. Alors $\varphi_j \downarrow \varphi$ et $\varphi_j = \gamma v - j$ sur $K_j = \{\varphi \leq -j\}$. De plus $K_j \downarrow K$. Soit j_0 fixé, alors

$$\begin{aligned}\int_{K_{j_0}} T\wedge dd^c\varphi\wedge(dd^c v)^{p-1} &\geq \limsup_{j\to+\infty}\int_{K_{j_0}} T\wedge dd^c\varphi_j\wedge(dd^c v)^{p-1}\\ &\geq \limsup_{j\to+\infty}\Big(\int_{K_j} T\wedge dd^c\varphi_j\wedge(dd^c v)^{p-1}\Big)\\ &= \gamma\limsup_{j\to+\infty}\int_{K_j} T\wedge(dd^c v)^p ,\end{aligned}$$

on fait tendre j_0 vers $+\infty$ puis on passe au sup sur tout les fonctions v psh telle que $0 \leq v \leq 1$.

(iv) Soient $\pi : \Delta^n \mapsto \Delta^k$ $(k < p)$ la projection canonique ; $v \in \mathrm{psh}(\Delta^k, [0,1])$ et $w \in (\mathrm{psh}\cap\mathcal{C}^\infty)(\Delta^n, [0,1])$. D'après [Bm-El], si $\mathcal{O} \subset\subset \Delta^n$, on a :

$$\begin{aligned}\int_{a\in\pi(\mathcal{O})}\Big\{\int_{\mathcal{O}}\langle T,\pi,a\rangle\wedge(dd^c w)^{p-k}\Big\}(dd^c v)^k &= \int_{\mathcal{O}} T\wedge(dd^c w)^{p-k}\wedge(dd^c\tilde{v})^k\\ &\leq \tfrac{2^p}{C_p^k}C_T(\mathcal{O},\Delta^n)\end{aligned}$$

où $\tilde{v} = v\circ\pi$. Par régularisation, l'inégalité reste vraie pour $w \in \mathrm{psh}(\Delta^{\mathrm{n}}, [0,1])$. Comme $\pi(\mathcal{O}) \subset\subset \Delta^k$, on a :

$$\int_{a\in\pi(\mathcal{O})} C_{\langle T,\pi,a\rangle}(\mathcal{O})(dd^c v)^k \leq \frac{2^p}{C_p^k}C_T(\mathcal{O},\Delta^n) ,$$

$$\begin{aligned}\mathcal{O}\ \textit{est}\ T-\textit{pluripolaire} &\Longrightarrow \forall v,\ \mathcal{O}\ \textit{est}\ \langle T,\pi,a\rangle-\textit{pluripolaire}\\ &\qquad (dd^c v)^k - p.p\\ &\Longrightarrow \exists N\ \textit{pluripolaire de}\ \pi(\mathcal{O})\ \textit{tel que}\ \forall a\notin N,\\ &\qquad \mathcal{O}\ \textit{est}\ \langle T,\pi,a\rangle-\textit{pluripolaire} .\end{aligned}$$

La réciproque est fausse, il suffit de prendre le courant $T = (dd^c|z'|^2)^p$.

Le résultat suivant est une conséquencce directe de l'inégalité de Cauchy-Schwarz qui sera utile dans la suite.

Proposition 2.3 *Soient* $u_1, u_2, v_1, v_2, w_1, \ldots, w_{p-1}$ *dans* $\mathrm{psh}(\Omega)\cap\mathrm{L}^\infty_{\mathrm{loc}}(\Omega)$ *et* T *un courant positif fermé sur* Ω *de dimension* $p \geq 1$. *Supposons que* $\{u_1 \neq u_2\} \subset\subset \Omega$ *et soit* $0 \leq \psi \in \mathcal{D}(\Omega)$, $\psi = 1$ *sur* $\{u_1 \neq u_2\}$. *Alors on a :*

$$\Big(\int_\Omega d(u_1-u_2)\wedge d^c(v_1-v_2)\wedge\chi\Big)^2 \leq \Big(\int_\Omega d(u_1-u_2)\wedge d^c(u_1-u_2)\wedge\chi\Big).$$
$$\Big(\int_\Omega \psi d(v_1-v_2)\wedge d^c(v_1-v_2)\wedge\chi\Big)$$

où $\chi = T \wedge dd^c w_1 \wedge \ldots \wedge dd^c w_{p-1}$

Démonstration. On remarque que l'application $(u,v) \mapsto \int_\Omega \psi du \wedge d^c v \wedge \chi$ est une forme bilinéaire symétrique et positive sur $\mathcal{C}^\infty(\Omega) \times \mathcal{C}^\infty(\Omega)$. La proposition 2.3 se justifie alors par application de l'inégalité de Cauchy-Schwarz au couple $(u_1 - u_2, v_1 - v_2)$ où $u_i, v_i \in \mathrm{psh}(\Omega) \cap \mathcal{C}^\infty(\Omega)$. Dans le cas général, on procède par régularisation. □

Théorème 2.4 *Soient* Ω *un ouvert borné de* $\mathbb{C}^n$, T *un courant positif fermé sur* Ω *de dimension* $p \geq 1$, u_j *et* u *des fonctions psh, localement bornées sur* Ω *telles que* $u_j = u$ *sur un voisinage de* $\partial\Omega$, (u_j) *décroissante vers* u, *alors* $\forall\ \delta > 0$ *on a :*

$$\lim_{j \to +\infty} C_T\Big(\{z \in \Omega,\ u_j(z) > u(z) + \delta\}\Big) = 0\ .$$

Démonstration. Sans perte de généralité, on peut supposer que $\delta = 1$. Posons $\Omega_j = \{z \in \Omega,\ u_j(z) > u(z) + 1\}$ et choisissons un ouvert $\mathcal{W}$ de sorte que $\{u_j \neq u\} \subset \mathcal{W} \subset\subset \Omega$. Soit $v \in \mathrm{psh}(\Omega, [0,1])$, on a :

$$\int_{\Omega_j} T \wedge (dd^c v)^p \leq \int_{\mathcal{W}} (u_j - u) T \wedge (dd^c v)^p = -\int_{\mathcal{W}} d(u_j - u) \wedge d^c v \wedge T \wedge (dd^c v)^{p-1}.$$

D'après la proposition 2.3, l'intégrale à droite est majorée par

$$C\Big(\int_{\mathcal{W}} d(u_j - u) \wedge d^c(u_j - u) \wedge T \wedge (dd^c v)^{p-1}\Big)^{\frac{1}{2}}\ ,$$

où $C = (\int_{\mathcal{W}} T \wedge dv \wedge d^c v \wedge (dd^c v)^{p-1})^{\frac{1}{2}} \leq M < \infty$ et M est une constante indépendante de v d'après l'inégalité de Chern.Levine.Nirenberg (cf.[C.L.N]). Appliquons encore une fois la formule de Stokes, on obtient

$$\begin{aligned}
& \int_{\mathcal{W}} d(u_j - u) \wedge d^c(u_j - u) \wedge T \wedge (dd^c v)^{p-1} \\
= \quad & -\int_{\mathcal{W}} (u_j - u) T \wedge dd^c(u_j - u) \wedge (dd^c v)^{p-1} \\
= \quad & \int_{\mathcal{W}} (u - u_j) T \wedge (dd^c u_j - dd^c u) \wedge (dd^c v)^{p-1} \\
\leq \quad & \int_{\mathcal{W}} (u_j - u) T \wedge dd^c u \wedge (dd^c v)^{p-1}
\end{aligned}$$

Il s'ensuit alors :

$$\int_{\Omega_j} T \wedge (dd^c v)^p \leq C\Big(\int_{\mathcal{W}} (u_j - u) T \wedge dd^c u \wedge (dd^c v)^{p-1}\Big)^{\frac{1}{2}}$$

La puissance de $dd^c v$ diminue de 1, on répéte ensuite le procédé $(p-1)$-fois, dans chaque étape en majorant $(u - u_j) dd^c(u_j - u)$ par $(u_j - u) dd^c u$ et en appliquant la proposition 2.3, on obtient finalement une majoration de $\int_{\Omega_j} T\wedge(dd^c v)^p$ par :

$$B\Big(\int_{\Omega}(u_j-u)T\wedge(dd^c u)^p\Big)^{\frac{1}{2^p}} ,$$

où B est une constante indépendante de j et de v.
Donc $\lim_{j\to+\infty} C_T(\Omega_j)=0.$ □

Comme conséquence du théorème 2.4, on montre qu'une fonction psh, localement bornée sur un ouvert borné Ω est continue si on retire de Ω un ouvert $\mathcal{O}$ de capacité C_T-arbitrairement petite. Plus précisement, on a

Théorème 2.5 *Soient Ω un ouvert borné de $\mathbb{C}^n$, $u\in \mathrm{psh}(\Omega)\cap \mathrm{L}^\infty_{\mathrm{loc}}(\Omega)$ et T un courant positif fermé sur Ω de dimension $p\geq 1$. Alors pour tout $\varepsilon>0$, il existe un ouvert $\mathcal{O}$ de Ω tel que $C_T(\mathcal{O},\Omega)<\varepsilon$ et u soit continue sur $\Omega\setminus\mathcal{O}$.*

Démonstration. D'après 3) et 4) de la proposition 2.2, on peut supposer que $\Omega=\{\rho<0\}$ est strictement pseudoconvexe et u bornée au voisinage de $\overline{\Omega}$. Soit (u_j) une suite de fonctions psh, de classe $\mathcal{C}^\infty$ qui décroit vers u dans un voisinage de $\overline{\Omega}$. Par rétrécissement de Ω et en remplaçant u_j par $max(u_j,A\rho+B)$ et u par $max(u,A\rho+B)$, on peut supposer que $u_j=u=A\rho+B$ au voisinage de $\partial\Omega$ pour A et $B>0$ convenablement choisis (pour plus de détails voir [Be-Ta]). D'après le théorème 2.4, pour tout $l\in\mathbb{N}^*$, il existe j_l tel que :

$$\mathcal{O}'_l=\{u_{j_l}>u+1/l\}\subset\Omega \ \ ; \ \ C_T(\mathcal{O}'_l)<2^{-l} .$$

Fixons un entier k tel que $2^{-k}<\varepsilon$ et posons : $G_k=\cup_{l\geq k}\mathcal{O}'_l$. La suite (u_{j_l}) est décroissante vers u uniformément sur $\Omega\setminus G_k$, donc u est continue sur $\Omega\setminus G_k$ et d'après 3) de la proposition 2.2, on obtient
$C_T(G_k,\Omega)\leq\sum_{l\geq k}C_T(\mathcal{O}'_l,\Omega)<2^{-k}<\varepsilon$ □

Remarques.

1) Si X est un sous-ensemble analytique, alors le théorème classique de [Be-Ta] ne donne aucune information sur la régularité de la fonction u sur X (i.e u peut être discontinue sur X tout entier). En appliquant 2.5 au courant $T=[X]$, nous obtenons un résultat plus précis : u est continue sur X privé de l'ensemble $\mathcal{O}\cap X$ qui est de volume arbitrairement petit dans X.

2) Le théorème 2.5 est faux si on enlève l'hypothèse $u\in L^\infty_{loc}(\Omega)$, et ce au vu du contre-exemple suivant :

$$\Omega=\Delta^2\subset\mathbb{C}^2; \quad T=[z_1=0]; \qquad u(z_1,z_2)=\log|z_1| .$$

3) Si l'on suppose de plus que T est assez régulier, c'est-à-dire pour tout u psh

$$\lim_{j\to+\infty} C_T\Big(\{u<-j\},\Omega\Big)=0 ,$$

comme c'est le cas des courants à coéfficients localement bornés, alors on peut généraliser 2.5 pour u seulement psh sur Ω.

L'intérêt du théorème 2.5 est dû en partie au résultat suivant, qui constitue une généralisation d'un théorème de [Be-Ta].

Théorème 2.6 (théorème de Comparaison) *Soient Ω un ouvert borné de $\mathbb{C}^n$, T un courant positif fermé de dimension $p \geq 1$ sur Ω, u et $v \in \mathrm{psh}(\Omega) \cap \mathrm{L}^\infty(\Omega)$. Supposons que :*

$$\liminf_{\xi \to \partial\Omega}(u(\xi) - v(\xi)) \geq 0$$

Alors on a :

$$\int_{\{u<v\}} T \wedge (dd^c v)^p \leq \int_{\{u<v\}} T \wedge (dd^c u)^p$$

Démonstration. On commence d'abord par l'étude du cas où u et v sont continues. Quitte à travailler sur l'ouvert $\{u < v\}$, on peut supposer que $\Omega = \{u < v\}$ et $u = v$ sur $\partial\Omega$. Soit $v_\varepsilon = \max(v - \varepsilon, u)$, $v_\varepsilon = u$ dans un voisinage de $\partial\Omega$.
D'après Stokes, on a :

$$\int_\Omega T \wedge (dd^c v_\varepsilon)^p = \int_\Omega T \wedge (dd^c u)^p$$

quand $\varepsilon \searrow 0$, v_ε converge uniformement vers v, donc $T \wedge (dd^c v_\varepsilon)^p$ converge faiblement vers $T \wedge (dd^c v)^p$. Soit $(\varphi_n)_{n\in\mathbb{N}}$ une suite dans $\mathcal{D}(\Omega)$ qui croit vert la fonction caracteristique de Ω, on trouve :

$$\int_\Omega \varphi_n T \wedge (dd^c v_\varepsilon)^p \leq \int_\Omega T \wedge (dd^c v_\varepsilon)^p = \int_\Omega T \wedge (dd^c u)^p$$

On finit la preuve en faisant $\varepsilon \to 0$ et $n \to +\infty$ dans cet ordre.
Nous étudions maintenant le cas général. Quitte à remplacer u par $u + 2\delta$ et faire tendre δ vers 0, on peut supposer que :

$$\liminf_{\xi \to \partial\Omega}(u(\xi) - v(\xi)) \geq 2\delta > 0$$

Dans ce cas, il existe un ouvert $\mathcal{O} \subset\subset \Omega$ tel que : $u(z) \geq v(z) + \delta$ pour tout $z \in \Omega \setminus \mathcal{O}$. Choisissons deux suites de fonctions u_k et v_j Psh, de classe $\mathcal{C}^\infty$ qui décroissent respectivement vers u et v dans un voisinage de $\overline{\mathcal{O}}$ et de sorte que pour tout $j \geq k$, on a $u_k \geq v_j$ sur $\partial\mathcal{O}$. D'après ce qui précède, on a :

$$\int_{\{u_k<v_j\}} T \wedge (dd^c v_j)^p \leq \int_{\{u_k<v_j\}} T \wedge (dd^c u_k)^p \qquad (2.6.1)$$

Soit $\varepsilon > 0$ et G un ouvert de Ω, tel que $C_T(G, \Omega) < \varepsilon$ et u, v sont continues sur $\Omega \setminus G$ (cf 2.5). On peut écrire $v = \varphi + \psi$ où φ est continue sur Ω et $\psi = 0$ sur

$\Omega \setminus G$.
Soit l'ouvert $U = \{u_k < \varphi\}$, on a :

$$\int_U T \wedge (dd^c v)^p \leq \lim_{j\to+\infty} \int_U T \wedge (dd^c v_j)^p \qquad (2.6.2)$$

Comme $U \cup G = \{u_k < v\} \cup G$, on a :

$$\begin{aligned}
\int_{\{u_k<v\}} T \wedge (dd^c v)^p &\leq \int_U T \wedge (dd^c v)^p + \int_G T \wedge (dd^c v)^p \\
&\leq \lim_{j\to+\infty} \int_U T \wedge (dd^c v_j)^p + \int_G T \wedge (dd^c v)^p \\
&\leq \lim_{j\to+\infty} \Big(\int_{\{u_k<v_j\}} T \wedge (dd^c v_j)^p + \int_G T \wedge (dd^c v_j)^p \Big) \\
&+ \int_G T \wedge (dd^c v)^p \\
&\leq \lim_{j\to+\infty} \int_{\{u_k<v_j\}} T \wedge (dd^c v_j)^p + 2M^p\varepsilon \\
&\leq \lim_{j\to+\infty} \int_{\{u_k<v_j\}} T \wedge (dd^c u_k)^p + 2M^p\varepsilon.
\end{aligned}$$

La $2^{ème}$ inégalité résulte de (2.6.2). Comme $U \subset \{u_k < v_j\} \cup G$, on obtient la $3^{ème}$ inégalité. La $4^{ème}$ résulte du fait que $C_T(G,\Omega) < \varepsilon$, tandis que la dernière inégalité se justifie par (2.6.1).
Comme $\{u_k < v_j\} \downarrow \{u_k \leq v\}$,$\{u_k < v\} \uparrow \{u < v\}$, on obtient :

$$\int_{\{u<v\}} T \wedge (dd^c v)^p \leq \lim_{k\to+\infty} \int_{\{u_k\leq v\}} T \wedge (dd^c u_k)^p + 2M^p\varepsilon \qquad (2.6.3)$$

Les fonctions u et v sont continues sur $\Omega \setminus G$, donc $\{u \leq v\} \setminus G$ est un fermé de Ω. Il s'ensuit alors : $\int_{\{u\leq v\}\setminus G} T \wedge (dd^c u)^p \geq \lim_{k\to+\infty} \int_{\{u\leq v\}\setminus G} T \wedge (dd^c u_k)^p$.
On a alors :

$$\begin{aligned}
\int_{\{u\leq v\}} T \wedge (dd^c u)^p &\geq \int_{\{u\leq v\}\setminus G} T \wedge (dd^c u)^p \\
&\geq \lim_{k\to+\infty} \int_{\{u\leq v\}\setminus G} T \wedge (dd^c u_k)^p \\
&\geq \lim_{k\to+\infty} \Big(\int_{\{u_k<v\}} T \wedge (dd^c u_k)^p - \int_G T \wedge (dd^c u_k)^p \Big) \\
&\geq \lim_{k\to+\infty} \int_{\{u_k<v\}} T \wedge (dd^c u_k)^p - M^p\varepsilon
\end{aligned}$$

La $3^{ème}$ inégalité se justifie par l'inclusion $\{u_k < v\} \setminus G \subset \{u < v\} \setminus G$.
D'après (2.6.3), on obtient :

$$\int_{\{u<v\}} T \wedge (dd^c v)^p \leq \int_{\{u\leq v\}} T \wedge (dd^c u)^p + 3M^p\varepsilon$$

Comme ε est arbitraire, on en déduit l'inégalité

$$\int_{\{u<v\}} T\wedge(dd^cv)^p \leq \int_{\{u\leq v\}} T\wedge(dd^cu)^p$$

Pour achever la preuve, il suffit de remplaçer u par $u+\eta$ et d'utiliser le fait que $\{u+\eta<v\}\uparrow\{u<v\}$ si $\eta\downarrow 0$ et que $\{u+\eta\leq v\}\uparrow\{u<v\}$ si $\eta\downarrow 0$. □

Remarque. Ce théorème reste vrai si on suppose que u et v sont dans $\mathrm{psh}(\Omega)\cap L^\infty(\Omega\setminus K)$ avec $K=\{v=-\infty\}\subset\{u=-\infty\}\subset\subset\Omega$. En effet : On suppose d'abord que u et v sont continues sur $\Omega\setminus\{v=-\infty\}$. Soient $u_s=\max(u,-s)$; $v_s=\max(v,-s)$, alors pour $s\gg$, $u_s=u,\ v_s=v$ au voisinage de $\partial\Omega$. D'après 2.6, on a

$$\int_{\{u_s<v_s\}} T\wedge(dd^cv_s)^p \leq \int_{\{u_s<v_s\}} T\wedge(dd^cu_s)^p$$

Comme $\{u_s<v_s\}=\{u<v\}\setminus\{v\leq -s\}\uparrow\{u<v\}\setminus K$, on a

$$\int_{\{u<v\}\setminus K} T\wedge(dd^cv)^p \leq \lim_{s\to+\infty}\int_{\{u_s<v_s\}} T\wedge(dd^cv_s)^p$$

D'autre part, l'ensemble $\{u_s<v_s\}\subset F_s=\{u\leq v\}\setminus\{v<-s\}$ est un fermé de Ω et vu que $F_s\uparrow\{u\leq v\}\setminus K$, on obtient

$$\lim_{s\to+\infty}\int_{\{u_s<v_s\}} T\wedge(dd^cu_s)^p \leq \lim_{s\to+\infty}\int_{F_s} T\wedge(dd^cu_s)^p \leq \int_{\{u\leq v\}\setminus K} T\wedge(dd^cu)^p$$

Le résultat se déduit aisément, en remplaçant u par $u+\eta$ et en faisant tendre η vers 0. Le cas général se traite par régularisation des fonctions u et v. □

Corollaire 2.7 (*principe de domination*) *Soient Ω un ouvert borné de $\mathbb{C}^n$, u et $v\in\mathrm{psh}(\Omega)\cap\mathrm{L}^\infty(\Omega)$. Supposons que :*
i) $\lim_{\xi\to\partial\Omega}\inf(u(\xi)-v(\xi))\geq 0$ *;*
ii) $T\wedge(dd^cu)^p\leq T\wedge(dd^cv)^p$ *;*
Alors $u\geq v$ en dehors d'un ensemble $\|T\|$−négligeable.

Démonstration. Sans perte de génératité, on peut supposer que $\Omega=\{\rho<0\}$ où ρ est une fonction C^∞, strictement psh qui définie Ω. Supposons que $\|T\|\big(\{u<v\}\big)>0$, alors il existe $\varepsilon>0$ tel que $\|T\|\big(\{u<v+\varepsilon\rho\}\big)>0$. D'après 2.6, on a :

$$\int_{\{u<v+\varepsilon\rho\}} T\wedge(dd^cv+\varepsilon\rho)^p \leq \int_{\{u<v+\varepsilon\rho\}} T\wedge(dd^cu)^p \leq \int_{\{u<v+\varepsilon\rho\}} T\wedge(dd^cv)^p$$

D'où :

$$\varepsilon^p\int_{\{u<v+\varepsilon\rho\}} T\wedge(dd^c\rho)^p + \int_{\{u<v+\varepsilon\rho\}} T\wedge(dd^cv)^p \leq \int_{\{u<v+\varepsilon\rho\}} T\wedge(dd^cv)^p$$

cela se contredit avec le fait que $\|T\|\big(\{u < v + \varepsilon\rho\}\big) > 0$. $\square$

Application. Dans plusieurs problèmes on est amené a contrôler la masse d'un produit de Monge-Ampere mixte ($\int_\Omega T \wedge (dd^c u)^j \wedge (dd^c v)^{p-j}$) par celles des produits homogènes ($\int_\Omega T \wedge (dd^c u)^p$ et $\int_\Omega T \wedge (dd^c v)^p$), en appliquant le théorème de comparaison on a réussit à faire ça dans certains cas (Proposition 2.9).

Soit φ une fonction continue, psh sur Ω et semi-exhaustive sur SuppT i.e il existe un nombre réel R tel que $B(R) \cap \mathrm{SuppT} \subset\subset \Omega$, où $B(R) = \{\varphi < R\}$. Pour $r \in]-\infty, R[$, on note :

$$B(r) = \{z \in \Omega; \varphi(z) < r\},\ S(r) = \{z \in \Omega; \varphi(z) = r\},\ \varphi_r = \max(\varphi, r)$$

L'application $r \mapsto T \wedge (dd^c\varphi_r)^p$, à valeurs dans l'espace des mesures sur Ω muni de la topologie faible, est continue sur $]-\infty, R[$. Comme la mesure $T \wedge (dd^c\varphi_r)^p$ est nulle sur $B(r)$ et coïncide avec $T \wedge (dd^c\varphi)^p$ sur $\Omega \setminus \overline{B}(r)$, on peut associer à T et φ une collection de mesure positives $\mu_{T,\varphi,r}$ portées par les ensembles $S(r)$ de la façon suivante :

$$\mu_{T,\varphi,r} = T \wedge (dd^c\varphi_r)^p - 1\!\!1_{\Omega\setminus B(r)} T \wedge (dd^c\varphi)^p$$

Si φ est de classe $\mathcal{C}^\infty$ et r une valeure régulière de φ, $\mu_{T,\varphi,r} = T \wedge (dd^c\varphi)^{p-1} \wedge d^c\varphi_{|S(r)}$. Pour $s > r$, on a : $\int_{B(s)} \Big(T \wedge (dd^c\varphi_r)^p - T \wedge (dd^c\varphi)^p\Big) = 0$. Donc la masse totale $\mu_{T,\varphi,r}(S(r)) = \mu_{T,\varphi,r}(B(s))$ coïncide avec la différence entre les masses de $T \wedge (dd^c\varphi)^p$ et $1\!\!1_{\Omega\setminus B(r)} T \wedge (dd^c\varphi)^p$ sur $B(s)$ i.e :

$$\mu_{T,\varphi,r}(S(r)) = \mu_{T,\varphi,r}(B(s)) = \int_{B(r)} T \wedge (dd^c\varphi)^p$$

On remarque que si $r \to r_0^-$ ($r_0 < R$), alors $1\!\!1_{\Omega\setminus B(r)}$ converge simplement vers $1\!\!1_{\Omega\setminus B(r_0)}$. Ceci veut dire que l'application $r \mapsto \mu_{T,\varphi,r}$ est continue faiblement à gauche.

Pour montrer la Proposition 2.9 on a besoin du lemme suivant

Lemme 2.8 *Soit ψ une fonction psh, négative et continue sur Ω, alors pour tout $s \geq 1$, $(-\psi)^s$ est $\mu_{T,\varphi,r}$−intégrable et on a :*

$$\begin{aligned} \mu_{T,\varphi,r}((-\psi)^s) &= \int_{B(r)} (-\psi)^s T \wedge (dd^c\varphi)^p \\ &+ \int_{B(r)} (r-\varphi) T \wedge dd^c(-\psi)^s \wedge (dd^c\varphi)^{p-1} \end{aligned} \tag{2.8.1}$$

Preuve. On procède comme Demailly (cf.[De]). On suppose d'abord que φ et ψ sont de classe $\mathcal{C}^\infty$, alors comme les deux membres de (2.8.1) sont continus à gauche, il suffit d'appliquer la formule de Stokes en utilisant l'égalité $\mu_{T,\varphi,r} = T\wedge(dd^c\varphi)^{p-1}\wedge d^c\varphi_{|S(r)}$ pour r une valeure régulière de φ. Si φ est continue et ψ de classe $\mathcal{C}^\infty$, on prend $\varphi_k\downarrow\varphi$ psh, de classe C^∞. Pour φ_k, on a :

$$\mu_{T,\varphi_k,r}((-\psi)^s)-\int_{\varphi_k<r}(-\psi)^sT\wedge(dd^c\varphi_k)^p=\int_{\varphi_k<r}(r-\varphi_k)T\wedge dd^c(-\psi)^s\wedge(dd^c\varphi_k)^{p-1}$$

On vérifie aisément que la suite $T\wedge dd^c(-\psi)^s\wedge(dd^c\varphi_k)^{p-1}$ converge faiblement vers $T\wedge dd^c(-\psi)^s\wedge(dd^c\varphi)^{p-1}$, et que $1\!\!1_{B(r)}(r-\varphi)$ est une fonction continue à support compact. Il en résulte que l'intégrale $\int_{\varphi_k<r}(r-\varphi_k)T\wedge dd^c(-\psi)^s\wedge(dd^c\varphi_k)^{p-1}$ converge vers $\int_{B(r)}(r-\varphi)T\wedge dd^c(-\psi)^s\wedge(dd^c\varphi)^{p-1}$. De plus, d'après la définition de $\mu_{T,\varphi_k,r}$, on a :

$$\mu_{T,\varphi_k,r}((-\psi)^s)-\int_{\varphi_k<r}(-\psi)^sT\wedge(dd^c\varphi_k)^p=\int_\Omega(-\psi)^s\Big(T\wedge(dd^c\varphi_{k,r})^p-T\wedge(dd^c\varphi_k)^p\Big)$$

où $\varphi_{k,r}=\max(\varphi_k,r)$. Comme $(T\wedge(dd^c\varphi_{k,r})^p-T\wedge(dd^c\varphi_k)^p)$ est à support dans le compact $\overline{B}(r)$, il s'ensuit que l'intégrale

$$\int_\Omega(-\psi)^s\big(T\wedge(dd^c\varphi_{k,r})^p-T\wedge(dd^c\varphi_k)^p\big)$$

converge vers

$$\int_\Omega(-\psi)^s\big(T\wedge(dd^c\varphi_r)^p-T\wedge(dd^c\varphi)^p\big)=\mu_{T,\varphi,r}((-\psi)^s)-\int_{B(r)}(-\psi)^sT\wedge(dd^c\varphi)^p.$$

Supposons maintenant que φ et ψ sont continues et choisissons $\psi_k\downarrow\psi$ psh, de classe $\mathcal{C}^\infty$, d'après ce qui précède, on a :

$$\mu_{T,\varphi,r}((-\psi_k)^s)-\int_{B(r)}(-\psi_k)^sT\wedge(dd^c\varphi)^p=\int_{B(r)}(r-\varphi)T\wedge dd^c(-\psi_k)^s\wedge(dd^c\varphi)^{p-1}$$

Le terme à gauche coïncide avec $\int_\Omega(-\psi_k)^s(T\wedge(dd^c\varphi_r)^p-T\wedge(dd^c\varphi)^p)$; cette intégrale converge vers $\int_\Omega(-\psi)^s(T\wedge(dd^c\varphi_r)^p-T\wedge(dd^c\varphi)^p)$ par application du théorème de la convergence monotone. D'autre part, puisque la fonction $1\!\!1_{B(r)}(r-\varphi)$ est continue à support compact et la suite $T\wedge dd^c(-\psi_k)^s\wedge(dd^c\varphi)^{p-1}$ converge faiblement vers $T\wedge dd^c(-\psi)^s\wedge(dd^c\varphi)^{p-1}$, on en déduit que l'intégrale $\int_{B(r)}(r-\varphi)T\wedge dd^c(-\psi_k)^s\wedge(dd^c\varphi)^{p-1}$ converge vers l'intégrale
$\int_{B(r)}(r-\varphi)T\wedge dd^c(-\psi)^s\wedge(dd^c\varphi)^{p-1}$. □

Proposition 2.9 *Soient* Ω *un ouvert borné de* $\mathbb{C}^n$, T *un courant positif fermé de dimension* $p \geq 1$, u *et* $v \in \mathrm{psh}(\Omega)$, *continues sur* Ω. *On suppose que :* $\lim\limits_{z\to\partial\Omega} u(z) = \lim\limits_{z\to\partial\Omega} v(z) = 0$ *et que* $\int_\Omega T \wedge \big((dd^c u)^p + (dd^c v)^p\big) < \infty$ *;*
Alors pour tout $s \geq 1, 0 \leq j \leq p$ *on a :*

$$\int_\Omega (-u)^s T \wedge (dd^c u)^j \wedge (dd^c v)^{p-j} \quad \leq D_{j,s}\Big(\int_\Omega (-u)^s T \wedge (dd^c u)^p\Big)^{\frac{s+j}{s+p}} \Big(\int_\Omega (-v)^s T \wedge (dd^c v)^p\Big)^{\frac{p-j}{s+p}}$$

Avec $D_{j,s} = s^{\frac{(s+j)(p-j)}{s-1}}$ *si* $s > 1$ *et* $D_{j,1} = exp\{(1+j)(p-j)\}$.

Démonstration. On reprend la démonstration de [Ce-Pe], on montre d'abord que : $\displaystyle\int_\Omega T \wedge (dd^c(u+v))^p < \infty$. En effet : soient $\mu = T \wedge (dd^c(u+v))^p$, avec $1 < \alpha < 2$ tels que $\mu\{u = \alpha v\} = 0$. D'après le théorème 2.6, on a :

$$\begin{aligned}
\mu(\Omega) &= \int_\Omega T \wedge (dd^c(u+v))^p \\
&= \int_{\{\frac{1+\alpha}{\alpha}u<u+v\}} T \wedge (dd^c(u+v))^p + \int_{\{(1+\alpha)v<u+v\}} T \wedge (dd^c(u+v))^p \\
&\leq (\tfrac{1+\alpha}{\alpha})^p \int_\Omega T \wedge (dd^c u)^p + (1+\alpha)^p \int_\Omega T \wedge (dd^c v)^p \\
&\leq 3^p \int_\Omega T \wedge \big((dd^c u)^p + (dd^c v)^p\big) < +\infty
\end{aligned}$$

En appliquant le lemme précédent au courant $R = T \wedge (dd^c v)^j$, on a :

$$\begin{aligned}
\mu_{R,u,-\varepsilon}((-v)^p) &= \int_{B(-\varepsilon)} (-v)^s R \wedge (dd^c u)^{p-j} \\
&+ \int_{B(-\varepsilon)} (-\varepsilon - u) R \wedge (dd^c(-v)^s) \wedge (dd^c u)^{p-j-1}
\end{aligned}$$

De plus, on a :

$$\begin{aligned}
0 \leq \mu_{R,u,-\varepsilon}((-v)^s) &\leq \sup_{\{u=-\varepsilon\}} \big\{(-v(z))^s\big\} \int_\Omega R \wedge (dd^c u)^{p-j} \\
&= \sup_{\{u=-\varepsilon\}} \big\{(-v(z))^s\big\} \int_\Omega T \wedge (dd^c u)^{p-j} \wedge (dd^c v)^j \\
&\leq \sup_{\{u=-\varepsilon\}} \big\{(-v(z))^s\big\} \int_\Omega T \wedge (dd^c(u+v))^p
\end{aligned}$$

D'après l'hypothèse sur u et v et le lemme, on en déduit alors,

$$\begin{aligned}
0 = \lim_{\varepsilon\to 0} \mu_{R,u,-\varepsilon}((-v)^p) &= \int_\Omega (-v)^s T \wedge (dd^c v)^j \wedge (dd^c u)^{p-j} \\
&+ \int_\Omega (-u) T \wedge (dd^c(-v)^s) \wedge (dd^c u)^{p-j-1} \wedge (dd^c v)^j
\end{aligned}$$

Par application de l'inégalité de Hölder, on obtient

$$\begin{aligned}
&\int_\Omega (-v)^s T\wedge (dd^cv)^j\wedge (dd^cu)^{p-j}\\
= &\int_\Omega udd^c(-v)^s\wedge T\wedge (dd^cv)^j\wedge (dd^cu)^{p-j-1}\\
= & s(s-1)\int_\Omega u(-v)^{s-2}T\wedge (dd^cv)^j\wedge (dd^cu)^{p-j-1}\wedge dv\wedge d^cv\\
+ & s\int_\Omega (-u)(-v)^{s-1}T\wedge (dd^cv)^{j+1}\wedge (dd^cu)^{p-j-1}\\
\leq & s\int_\Omega (-u)(-v)^{s-1}T\wedge (dd^cv)^{j+1}\wedge (dd^cu)^{p-j-1}\\
\leq & \Big(s\int_\Omega (-u)^s T\wedge (dd^cv)^{j+1}\wedge (dd^cu)^{p-j-1}\Big)^{\frac{1}{s}}\\
& \Big(s\int_\Omega (-v)^s T\wedge (dd^cv)^{j+1}\wedge (dd^cu)^{p-j-1}\Big)^{\frac{s-1}{s}}
\end{aligned}$$

En prenant le logarithme, on obtient :
$x_j\leq \frac{s-1}{s}x_{j+1}+\frac{1}{s}y_{p-j-1}+\log s$; $y_j\leq \frac{s-1}{s}y_{j+1}+\frac{1}{s}x_{p-j-1}+\log s$. où :

$$\begin{aligned}
x_j &= \log\int_\Omega (-u)^s T\wedge (dd^cu)^j\wedge (dd^cv)^{p-j}\\
y_j &= \log\int_\Omega (-v)^s T\wedge (dd^cv)^j\wedge (dd^cu)^{p-j}
\end{aligned}$$

Le reste de la démonstration est réduit à un problème de résolution d'un système linéaire (cf.[Ce-Pe]). □

3 Convergence par rapport à C_T et operateur de monge-ampère

Dans cette partie nous introduisons la notion de la convergence par rapport à la capacité C_T. Comme application nous généralisons des résultats de [Be-Ta] et de [Xi] sur l'opérateur de Monge-Ampère.

Définition 3.1 *Soient T un courant positif fermé de dimension $p\geq 1$ sur un ouvert Ω de $\mathbb{C}^n$ et $E\subset\Omega$. On dit que u_j converge vers u par rapport à C_T sur E si pour tout $\delta>0$, on a :*

$$\lim_{j\to+\infty} C_T\Big(\big\{z\in E;\quad |u_j(z)-u(z)|>\delta\big\},\Omega\Big)=0$$

Théorème 3.2
Soient $(u_j)_j$ une suite de fonctions psh localement uniformément bornées et $u\in \mathrm{psh}(\Omega)\cap \mathrm{L}^\infty_{\mathrm{loc}}(\Omega)$, on a :
a) *Si u_j converge vers u par rapport à C_T sur chaque $E\subset\subset\Omega$, alors le courant $T\wedge(dd^cu_j)^p$ converge au sens des courants vers $T\wedge (dd^cu)^p$.*
b) *Supposons qu'il existe $E\subset\subset\Omega$ tel que $\forall j,\ u_j=u$ sur $\Omega\setminus E$ et que les suites*

$uT\wedge(dd^cu_j)^p$, $u_jT\wedge(dd^cu)^p$ et $u_jT\wedge(dd^cu_j)^p$ convergent au sens des courants vers $uT\wedge(dd^cu)^p$ alors u_j converge vers u par rapport à C_T sur E.

Remarques.

1) Si $T=1$ ou $T=dd^c|z|^2$, on retrouve un résultat de Xing (cf.[Xi]).

2) a) constitue encore une généralisation d'un résultat de [Be-Ta], dans le cas où la suite $(u_j)_j$ est décroissante vers u. En effet on montre dans ce cas (cf théorème2.4) que u_j converge vers u par rapport à la capacité C_T.

3) Dans b), si on suppose de plus que $u\geq u_j$ $\forall j$ (en particulier si $u_j\uparrow u$), on peut conclure sans utiliser la convergence faible des suites $uT\wedge(dd^cu_j)^p$ et $u_jT\wedge(dd^cu_j)^p$. Dans la démonstration de b), on peut en effet utiliser l'inégalité $dd^c(u-u_j)\leq dd^cu$ à la place de $dd^c(u_j-u)\leq dd^c(u+u_j)$.

Démonstration. On procède comme dans [Xi].
a). On raisonne par récurrence sur l'entier p. Le cas $p=1$ se déduit si on montre que u_jT converge faiblement vers uT.
Soit $\varphi\in\mathcal{D}_{p,p}(\Omega)$, supp$\varphi\subset\Omega_1\subset\subset\Omega$, alors :

$$\begin{aligned}
\Big|\int_\Omega(u_jT-uT)\wedge\varphi\Big| &\leq C\int_{\Omega_1}|u_j-u|T\wedge\beta^p\\
&= C\int_{\{|u_j-u|\leq\delta\}\cap\Omega_1}|u_j-u|T\wedge\beta^p\\
&+ C\int_{\{|u_j-u|>\delta\}\cap\Omega_1}|u_j-u|T\wedge\beta^p\\
&\leq C\delta\|T\|_{\Omega_1}+C\|u_j-u\|_\infty\int_{\{|u_j-u|>\delta\}\cap\Omega_1}T\wedge\beta^p\\
&\leq C\delta\|T\|_{\Omega_1}+MC_T\big\{z\in\Omega_1;\ \ |u_j(z)-u(z)|>\delta\big\}
\end{aligned}$$

Comme δ est arbitraire, M est indépendante de j et u_j converge vers u par rapport à la capacité C_T sur Ω_1, on a donc le résultat pour $p=1$. On suppose que $T\wedge(dd^cu_j)^s$ converge faiblement vers $T\wedge(dd^cu)^s(s<p)$, et montrons que $u_jT\wedge(dd^cu_j)^s$ converge faiblement vers $uT\wedge(dd^cu)^s$.
Pour tout $\varepsilon>0$, il existe d'après le théorème2.5 un ouvert $\mathcal{O}$ tel que $C_T(\mathcal{O},\Omega)<\varepsilon$, $u=\phi+\psi$ où ϕ est continue sur Ω et $\psi=0$ sur $\Omega\setminus\mathcal{O}$.

$$\begin{aligned}
u_jT\wedge(dd^cu_j)^s-uT\wedge(dd^cu)^s &= (u_j-u)T\wedge(dd^cu_j)^s\\
&+ \psi\big(T\wedge(dd^cu_j)^s-T\wedge(dd^cu)^s\big)\\
&+ \phi\big(T\wedge(dd^cu_j)^s-T\wedge(dd^cu)^s\big)\\
&= (1)+(2)+(3)
\end{aligned}$$

(3) tend faiblement vers 0 par l'hypothèse de récurrence et le fait que ϕ est continue.

Pour (1), soit $\varphi \in \mathcal{D}_{p-s,p-s}(\Omega)$, supp$\varphi \subset \Omega_1 \subset\subset \Omega$, alors :

$$
\begin{aligned}
\Big| \int_\Omega (u_j - u) T \wedge (dd^c u_j)^s \wedge \varphi \Big| &\leq C \int_{\Omega_1} |u_j - u| T \wedge (dd^c u_j)^s \wedge (dd^c |z|^2)^{p-s} \\
&\leq C \int_{\Omega_1} |u_j - u| T \wedge \big(dd^c(u_j + |z|^2)\big)^p \\
&= C \int_{\{|u_j - u| > \delta\} \cap \Omega_1} u_j - u| T \wedge \big(dd^c(u_j + |z|^2)\big)^p \\
&\quad + C \int_{\{|u_j - u| \leq \delta\} \cap \Omega_1} u_j - u| T \wedge \big(dd^c(u_j + |z|^2)\big)^p \\
&\leq A \int_{\{|u_j - u| > \delta\} \cap \Omega_1} T \wedge \big(dd^c(u_j + |z|^2)\big)^p + \delta M \|T\|_{\Omega_1} \\
&\leq A_1 C_T \big\{ z \in \Omega_1 ; |u_j(z) - u(z)| > \delta \big\} + \delta M \|T\|_{\Omega_1}
\end{aligned}
$$

Comme u_j est une suite localement uniformément bornée, A_1 et M ne dépendent pas de j, on a (1) converge faiblement vers 0.
On raisonne de même pour (2), on a :

$$
\begin{aligned}
\int_{\Omega_1 \cap \mathcal{O}} \psi T \wedge (dd^c u_j)^s \wedge \beta^{p-s} &\leq B \int_{\Omega_1 \cap \mathcal{O}} T \wedge \big(dd^c(u_j + |z|^2)\big)^p \\
&\leq B_1 C_T(\mathcal{O}, \Omega) \leq \varepsilon B_1
\end{aligned}
$$

De même : $\displaystyle\int_{\Omega_1 \cap \mathcal{O}} \psi T \wedge (dd^c u)^s \wedge \beta^{p-s} \leq B_2 \varepsilon.$
b) Soient Ω' un ouvert tel que $E \subset\subset \Omega' \subset\subset \Omega$, $w \in \mathrm{psh}(\Omega, [0,1])$ et $\delta > 0$. D'après Stokes et l'inégalité de Cauchy-Shawrz, on obtient :

$$
\begin{aligned}
&\int_{\{|u_j - u| > \delta\}} T \wedge (dd^c w)^p \\
\leq\; & \tfrac{1}{\delta^2} \int_{\Omega'} (u_j - u)^2 T \wedge (dd^c w)^p \\
=\; & \tfrac{-1}{\delta^2} \int_{\Omega'} T \wedge d(u_j - u)^2 \wedge d^c w \wedge (dd^c w)^{p-1} \\
\leq\; & A_1 \Big(\int_{\Omega'} T \wedge d(u_j - u)^2 \wedge d^c (u_j - u)^2 \wedge (dd^c w)^{p-1} \Big)^{\frac{1}{2}} \\
\leq\; & 2 A_1 A_2 \Big(\int_{\Omega'} T \wedge d(u_j - u) \wedge d^c (u_j - u) \wedge (dd^c w)^{p-1} \Big)^{\frac{1}{2}}
\end{aligned}
$$

où l'on a posé $A_1 = \frac{1}{\delta^2} \int_{\Omega'} T \wedge dw \wedge d^c w \wedge (dd^c w)^{p-1} < \infty$ (cf.[C.L.N]) et $A_2 = \|u_j - u\|_\infty < \infty$.
En appliquant encore $(p-1)-$fois la formule de Stokes, l'inégalité de Cauchy-

Schwarz et en utilisant l'inégalité $dd^c(u_j - u) \leq dd^c(u_j + u)$, on trouve :

$$\begin{aligned}
&\int_{\Omega'} T \wedge d(u_j - u) \wedge d^c(u_j - u) \wedge (dd^c w)^{p-1} \\
= \quad & \int_{\Omega'} T \wedge d(u_j - u) \wedge d^c w \wedge dd^c(u_j - u) \wedge (dd^c w)^{p-2} \\
\leq \quad & B\Big(\int_{\Omega'} T \wedge d(u_j - u) \wedge d^c(u_j - u) \wedge dd^c(u_j + u) \wedge (dd^c w)^{p-2}\Big)^{\frac{1}{2}} \\
\leq \quad & B_1\Big(\int_{\Omega'} T \wedge d(u_j - u) \wedge d^c(u_j - u) \wedge \big(dd^c(u_j + u)\big)^{p-1}\Big)^{\frac{1}{2^p}} \\
\leq \quad & B_2\Big(\int_{\Omega'} T \wedge d(u_j - u) \wedge d^c(u_j - u) \wedge \sum_{k=0}^{p-1}(dd^c u_j)^{p-k-1} \wedge (dd^c u)^k\Big)^{\frac{1}{2^p}} \\
= \quad & B_2\Big(\int_{\Omega'} (u_j - u) T \wedge (dd^c u_j - dd^c u) \wedge \sum_{k=0}^{p-1}(dd^c u_j)^{p-k-1} \wedge (dd^c u)^k\Big)^{\frac{1}{2^p}} \\
= \quad & B_2\Big(\int_{\Omega'} (u_j - u)\big(T \wedge (dd^c u_j)^p - T \wedge (dd^c u)^p\big)\Big)^{\frac{1}{2^p}}
\end{aligned}$$

où la constante B_2 est indépendante de j et de w. Comme $u = u_j$ sur $\Omega' \setminus E$ et $uT \wedge (dd^c u_j)^p$, $u_j T \wedge (dd^c u)^p$, $u_j T \wedge (dd^c u_j)^p$ converge vers la même limite $uT \wedge (dd^c u)^p$, on obtient : $\lim_{j \to +\infty} \int_{\Omega'} (u_j - u)(T \wedge (dd^c u_j)^p - T \wedge (dd^c u)^p) = 0$

Il en résulte que : $C_T(|u_j - u| > \delta, \Omega) = 0$ □

Références

[Be-Ta] Bedford E. et Taylor B. A., A new capacity for Plurisubharmonic functions, *Acta Math*, 149 (1982), 1-40.

[Bm-El] H. Ben Messaoud et H. El Mir, Tranchage et prolongement des courants positifs fermés, *Math. Ann.* 307 (1997), 473-487.

[Ce] Cegrell. U, *Capacities in Complex Analysis*, Braunschwerg Wiesbaden Friedr. Vieweg et Sohn, 1988.

[Cee-Pe] Cegrell. U et Leif Person, An energy estimate for complex Monge-Ampère Operateur, *Annales Polimici Mathematici*, LXVII1 (1997) 95-102.

[C.L.N] Chern S.S., Levine H.I. et Nirenberg L. *Intrinsic norms on a complex manifold ; Global Analysis*, Papers in Honor of K.Kodaira, pp. 119-139, Univ. of Tokyo Press, Tokyo, 1969.

[De] Demailly J.P., *Monge-Ampère operator, Lelong numbers and intersection theory, in complex Analysis and Geometry*, (V. Ancona and A Silva, eds.), pp.15-193. Univ. Ser. Math., Plenum Press, New York, 1993.

[Xi] Xing Y., *Continuity of the complex Monge-Ampère*, Proc. Amer.Math. Soc. 124, 457-467 , (1996).

Dabbek Khalifa
Département de Math
Faculé de sciences de Gabès
6071 Gabès Tunisie
khalifa.dabbek@fsg.rnu.tn

Elkhadhra Fredj
Département de Math
Faculé de sciences Monastir
5000 Monastir Tunisie
fredj.elkhadhra@fsm.rnu.tn