Journal de Théorie des Nombres
de Bordeaux **12** (2000), 437–453

On lattice bases with special properties

par Ulrich HALBRITTER et Michael E. POHST

Dedicated to Jacques Martinet on his 60th birthday

Résumé. Nous introduisons ici des réseaux multiplicatifs de $(\mathbb{R}^{>0})^r$ et déterminons des réunions finies de simplexes convenables comme domaines fondamentaux de sous-réseaux d'indices finis. Nous définissons pour cela des bases cycliques positives de réseaux arbitraires. Nous utilisons ces bases pour calculer les cônes de Shintani dans des corps totalement réels de nombres algébriques. Nous nous intéressons plus particulièrement aux réseaux en dimensions deux et trois correspondants à des corps cubiques ou quartiques.

Abstract. In this paper we introduce multiplicative lattices in $(\mathbb{R}^{>0})^r$ and determine finite unions of suitable simplices as fundamental domains for sublattices of finite index. For this we define cyclic non-negative bases in arbitrary lattices. These bases are then used to calculate Shintani cones in totally real algebraic number fields. We mainly concentrate our considerations to lattices in two and three dimensions corresponding to cubic and quartic fields.

1. Introduction

Since the guiding principles for this article are adopted from algebraic number theory and since this is the topic, where our ideas mainly apply (see Section 4), we shortly introduce some notation for algebraic number fields.

Throughout this paper F denotes a totally real algebraic number field of degree n over the rational numbers $\mathbb{Q}$. We assume that it is generated by a root ρ of a monic irreducible polynomial

$$f(t) \; = \; t^n + a_1 t^{n-1} + ... + a_n \; \in \; \mathbb{Z}[t] \quad . \tag{1.1}$$

Manuscrit reçu le 3 mars 2000.

Over the real numbers $\mathbb{R}$ the polynomial $f(t)$ splits into a product of linear factors

$$f(t) \ = \ \prod_{j=1}^{n}(t-\rho^{(j)}) \ \ .$$

We assume $\rho = \rho^{(1)}$ for the *conjugates* $\rho^{(1)}, ..., \rho^{(n)}$ of ρ as usual. An element α of F is called *totally positive* if all its conjugates are positive real numbers.

Arithmetical problems usually require computations with *algebraic integers* contained in F, i.e., those elements of F whose minimal polynomials have coefficients in $\mathbb{Z}$. They form a ring o_F with a $\mathbb{Z}$-basis $\omega_1, ..., \omega_n$ (*integral basis* of F), the so-called *maximal order* of F. Then the *discriminant* d_F of F is given by

$$d_F \ = \ (\det(\ (\omega_i^{(j)})_{1\leq i,j\leq n}))^2 \ \ . \tag{1.2}$$

Two elements of o_F are called multiplicatively equivalent (*associated*), if their quotient is an invertible element (*unit*) of o_F. The units of o_F form a finitely generated abelian group U_F. For totally real fields it consists of a torsion part $TU_F = \pm 1$ and the direct product of $r = n-1$ infinite cyclic groups the generators of which, say $\varepsilon_1, ..., \varepsilon_r$, are called *fundamental units.* Equivalence is usually tested in logarithmic space. For this we consider the mapping:

$$L \ : \ F^{\times} \to \mathbb{R}^r \ : \ x \mapsto (\log \mid x^{(1)} \mid, ..., \log \mid x^{(r)} \mid) \ \ .$$

Clearly, $\Lambda := L(U_F)$ is a lattice in r-dimensional Euclidean space with basis $L(\varepsilon_1), ..., L(\varepsilon_r)$ and, consequently, two elements $x, y \in o_F \setminus \{0\}$ are associated if and only iff $L(x)$ and $L(y)$ differ by an element of Λ.

In this article we study the problem of choosing appropriate bases of lattices Λ in r-dimensional Euclidean space such that so-called Shintani cones which are of importance for ray class zeta functions become more easily accessible. We proceed as follows. In Section 2 we define "nice" bases of lattices (respectively, sublattices of finite index) and prove their existence. In Section 3 we define a generalized multiplicative equivalence for vectors with all coordinates positive in Euclidean r-space. We show how the bases of Section 2 can be used to obtain fundamental domains for that multiplicative equivalence for $r \leq 3$ and conjecture that this is true for arbitray r. Interpreting them as the intersection of a decomposition of $(\mathbb{R}^{>0})^n$ into Shintani cones with the hyperplane $x_n = 1$ these can then be used to calculate a Shintani decomposition of $(\mathbb{R}^{>0})^n$, where r denotes a natural number and (the field degree) n is $r+1$.

We illustrate our considerations by an example of a fundamental domain for a quartic field. The application of that decomposition to the calculation of the values of ray class zeta functions at non-negative integers will be done in a subsequent paper.

2. Lattice bases with special properties

In this section we consider full lattices Λ in r-dimensional Euclidean space $\mathbb{R}^r$ for $r \geq 1$. In later sections we shall need the existence of special lattice bases for Λ (or at least for a sublattice $\tilde{\Lambda}$ of Λ of finite index).

Definition 2.1. A set of r non-zero vectors $S = \{\mathbf{b}_1, ..., \mathbf{b}_r\}$ of Λ is called *cyclic non-negative*, if the coordinates of the i-th vector $\mathbf{b}_i = (b_{i1}, ..., b_{ir})$ satisfy the inequalities $b_{ii} \geq b_{i,i+1} \geq ... \geq b_{i,i+r-1} \geq 0 \quad (1 \leq i \leq r)$, where the second indices j are considered modulo r, i.e. j is to be replaced by $j - r$ for $j > r$.

We will show that every lattice Λ contains cyclic non-negative sets of independent vectors. In a first step we construct a cyclic non-negative set for Λ, where all inequalities between the coordinates of the vectors are strict.

Proposition 2.1. *A lattice Λ contains a cyclic non-negative set of vectors $\mathbf{b}_1, ..., \mathbf{b}_r$ the coordinates of which satisfy $b_{ii} > b_{i,i+1} > ... > b_{i,i+r-1} > 0 \quad (1 \leq i \leq r)$.*

Proof. Let $\mathbf{x}_1, ..., \mathbf{x}_r$ be any basis of Λ and K an upper bound for the absolute values of the coordinates of the basis vectors. Any $\mathbf{x} \in \mathbb{R}^r$ has a presentation $\mathbf{x} = \sum_{i=1}^r \lambda_i \mathbf{x}_i$ with coefficients $\lambda_i \in \mathbb{R}$. Let $m_i \in \mathbb{Z}$ subject to $\mid m_i - \lambda_i \mid \leq \frac{1}{2} \quad (1 \leq i \leq r)$ and put $\mathbf{y} := \sum_{i=1}^r m_i \mathbf{x}_i$. Then we have $\mathbf{y} = \mathbf{x} + \sum_{i=1}^r (m_i - \lambda_i)\mathbf{x}_i$ and therefore

$$y_{j+1} - y_j = x_{j+1} - x_j + \sum_{i=1}^r (m_i - \lambda_i)(x_{i,j+1} - x_{i,j}) \geq x_{j+1} - x_j - r\frac{1}{2}(2K).$$

Hence, an appropriate choice of $\mathbf{x}$ guarantees $y_{j+1} - y_j > 0$. □

Next we will show that the cyclic non-negative set obtained in the proposition is linearly independent.

Proposition 2.2. *Let $\mathbf{b}_1, ..., \mathbf{b}_r$ be a cyclic non-negative set of vectors of a lattice Λ and denote by $B := (b_{ij})$ the matrix with rows $\mathbf{b}_1, ..., \mathbf{b}_r$. Then the determinant of B is non-negative. If we have $b_{ii} > b_{i,i+1}$ for at least $r - 1$ of the vectors $\mathbf{b}_1, ..., \mathbf{b}_r$ the given cyclic non-negative set is linearly independent.*

Proof. Let $D_1 := \det(B)$ be the determinant of the matrix with rows $\mathbf{b}_1, ..., \mathbf{b}_r$. We will show $D_1 \geq 0$ by induction on r. This is trivial for $r = 1, 2$. Hence, we assume $r \geq 3$ in the sequel.

The determinant D_1 is a linear polynomial in each of the entries of the matrix B. Hence, it suffices to consider the value of D_1 on the boundaries of those entries. The coefficient of b_{11} is the determinant of the matrix with entries $b_{ij} \quad (2 \leq i, j \leq r)$, hence, it is non-negative according to our induction assumption. As a consequence, D_1 becomes at most smaller, when we replace b_{11} by b_{12} in the original matrix.

Again we proceed by induction on the number κ of equal entries in the first row of the given matrix starting from the left. Let C be the matrix with entries $c_{ij} = b_{ij}$ for $2 \le i$ or $i = 1$ and $j \ge \kappa$ whereas $c_{1j} = c_{1\kappa}$ for $1 \le j < \kappa$. We conclude from $\kappa - 1$ to κ.

The determinant of C is a linear polynomial in $c_{1\kappa}$. We subtract column 1 of C from columns $2, ..., \kappa$ and obtain for the coefficient of $c_{1\kappa}$ the determinant of the matrix E with entries

$$e_{ij} = \begin{cases} b_{i+1,j+1} - b_{i+1,1} & \text{for } 1 \le j < \kappa \\ b_{i+1,j+1} & \text{for } \kappa \le j < r \end{cases}$$

for $1 \le i < r$. We add the last column of E to columns $1, ..., \kappa - 1$. Then the rows of the new matrix F form a cyclic non-negative set, and we obtain $\det F \ge 0$ according to our induction assumption. This finishes the step from $\kappa - 1$ to κ.

Hence, the original determinant D_1 is bounded from below by the determinant of the matrix originating from B by replacing all entries in the first row by b_{1n}. Moving the first row to the last and the first column to the last and taking the common factor b_{1n} of the new last row, we obtain

$$D_1 \ \ge \ b_{1n} \begin{vmatrix} b_{22} & \dots & b_{2n} & b_{21} \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ b_{n2} & \dots & b_{nn} & b_{n1} \\ 1 & \dots & 1 & 1 \end{vmatrix} \quad .$$

Again, the rows of the last matrix form a cyclic non-negative set. Carrying out the same procedure again, we get

$$D_1 \ \ge \ b_{1n} b_{21} D_3 \ = \ 0 \quad ,$$

since D_3 is the determinant of a matrix with 2 equal rows with entries all one. Thus we have also shown the induction step from $r - 1$ to r.

If the additional premise $b_{ii} > b_{i,i+1}$ holds for at least $r-1$ of the vectors $\mathbf{b}_1, ..., \mathbf{b}_r$ we can rearrange the order of rows and columns such that this condition is satisfied for the first $r - 1$ rows. Then the proof above clearly yields $\det B > 0$. □

The preceding propositions show that we can compute cyclic non-negative sets in every lattice which generate sublattices of finite index. Of course, we are interested in generating sublattices of small index. For $r = 2$ we can prove the existence of cyclic non-negative lattice bases and that proof also provides an algorithm for calculating them.

Proposition 2.3. *For $r = 2$ any lattice Λ has a cyclic non-negative set $\{\mathbf{b}_1, \mathbf{b}_2\}$ as a basis.*

Proof. We apply a purely geometrical construction which is based on Minkowski's convex body theorem. We note that for calculating lattice points in practice the occuring rectangles will be covered by ellipses. For algorithmic details we refer the reader to [5].

We consider the closed first quadrant $(\mathbb{R}^{\geq 0})^2$. For the bisector $G_1 := \{(x, y) \in \mathbb{R}^2 \mid x = y\}$ we let G_2, G_3 be the parallel lines to G_1 with distance $\delta > 0$. That distance is chosen maximal subject to $\sqrt{2}\delta < M(\Lambda)$, where $M(\Lambda)$ denotes the minimum of the lattice, i.e., the norm of a shortest lattice vector. This guarantees that all lattice points between G_2 and G_3 lie in the first and third quadrant.

Then we choose the smallest $\mathbf{0}$–symmetric closed rectangle with two sides on G_2 and G_3 which contains at least one lattice point $\mathbf{c}$, necessarily on the boundary. We choose $\mathbf{c}$ in the first quadrant with maximal distance, say ε, to G_1. We need to discuss two cases depending on whether ε is zero or not.

To begin with let us assume $\varepsilon > 0$. We let G_4, G_5 be the parallel lines to G_1 with distance ε. Then we choose the smallest $\mathbf{0}$–symmetric closed rectangle with two sides on G_4 and G_5 which contains at least one lattice point $\mathbf{d}$ in the first quadrant which is different from $\mathbf{c}$. It is easy to see that $\mathbf{c}$ and $\mathbf{d}$ lie on different sides of G_1. Hence, putting them into the right order they form a linearly independent cyclic non-negative set. Also the closed triangle with vertices $\mathbf{0}, \mathbf{c}, \mathbf{d}$ contains exactly these vertices as lattice points. Therefore $\{\mathbf{c}, \mathbf{d}\}$ is a basis of Λ.

In the case $\varepsilon = 0$ we consider the parallel lines G_6, G_7 with distance $\gamma = d(\Lambda)/\|\mathbf{c}\|$, where $d(\Lambda)$ denotes the mesh of the lattice. Let $\mathbf{d}$ be a lattice point on G_6 or G_7 which lies in the first quadrant. Such a point must exist according to our assumptions. Ordering $\mathbf{c}, \mathbf{d}$ appropriately they form a cyclic non-negative set which is a lattice basis because of the volume of the parallelogram spanned by them. $\square$

We note that for $r = 3$ we can show the existence of a cyclic non-negative set generating a sublattice of index at most 24, independently of the lattice Λ. The proof is quite lengthy and therefore omitted. In practice we always obtained sublattices of much smaller index.

3. Multiplicative equivalence in $(\mathbb{R}^{>0})^r$

The concept of multiplicative equivalence for the integers of an algebraic number field F which we introduced in Section 1 needs to be generalized with respect to multiplicative equivalence in $(\mathbb{R}^{>0})^r$ and Shintani cones. For multiplicatively equivalent totally positive elements $\alpha, \beta \in o_F$ there exists a totally positive unit η with $\alpha = \beta\eta$. Somewhat weaker we now require

$$\exists\lambda \in \mathbb{R}^{>0} \ : \ (\alpha^{(1)},...,\alpha^{(n)}) \ = \ \lambda(\beta^{(1)}\eta^{(1)},...,\beta^{(n)}\eta^{(n)}) \ .$$

This is easily seen to be equivalent to

$$\left(\frac{\alpha^{(1)}}{\alpha^{(n)}},...,\frac{\alpha^{(n-1)}}{\alpha^{(n)}},1\right) \ = \ \left(\frac{\beta^{(1)}\eta^{(1)}}{\beta^{(n)}\eta^{(n)}},...,\frac{\beta^{(n-1)}\eta^{(n-1)}}{\beta^{(n)}\eta^{(n)}},1\right)$$

and therefore also to

$$\left(\frac{\alpha^{(1)}}{\alpha^{(n)}},...,\frac{\alpha^{(n-1)}}{\alpha^{(n)}}\right) \ = \ \left(\frac{\beta^{(1)}\eta^{(1)}}{\beta^{(n)}\eta^{(n)}},...,\frac{\beta^{(n-1)}\eta^{(n-1)}}{\beta^{(n)}\eta^{(n)}}\right) \ .$$

This yields the following general definition which is independent of number fields. (We note that $r = n-1$ throughout the paper.)

Definition 3.1. Let $E_i^{(j)}$ $(1 \le i,j \le r)$ be fixed positive constants. Vectors $\mathbf{x},\mathbf{y} \in (\mathbb{R}^{>0})^r$ are called (multiplicatively) *equivalent*, if there is a vector $\mathbf{m} = (m_1,...,m_r) \in \mathbb{Z}^r$ such that $y_j = x_j \prod_{i=1}^r (E_i^{(j)})^{m_i}$.

From the definition it is clear that this relation is an equivalence relation and we are interested in a "nice" fundamental domain. If we set $\mathbf{E}_i := (E_i^{(1)},...,E_i^{(r)})$ $(1 \le i \le r)$ the vectors $\mathbf{x},\mathbf{y}$ are equivalent, if and only if $L(\mathbf{y}) = L(\mathbf{x}) + \sum_{i=1}^r m_i L(\mathbf{E}_i)$ holds, where the map L is given by

$$L \ : \ (\mathbb{R}^{>0})^r \to \mathbb{R}^r \ : \ (x_1,...,x_r) \mapsto (\log x_1,...,\log x_r) \ .$$

It is obvious that the vectors $L(\mathbf{E}_i)$ should be linearly independent, we therefore stipulate this in the sequel.

Hence, $L(\mathbf{E}_1),...,L(\mathbf{E}_r)$ are basis vectors of a (logarithmic) lattice Λ in $\mathbb{R}^r$. It would be tempting to take as a fundamental domain for multiplicative equivalence the preimage of the fundamental domain of Λ, i.e. of the set

$$\prod \ := \ \{\sum_{i=1}^r x_i L(\mathbf{E}_i) \mid 0 \le x_i < 1 \ \ (1 \le i \le r)\} \ .$$

Even though the exponential function generally behaves quite nicely, such a choice does not yield an appropriate fundamental domain. Namely, its boundary is not contained in a finite number of hyperplanes which will be required at a later stage. Therefore the idea comes up to deform $\prod$ into a set $\tilde{\prod}$. This procedure must be carried out such that the integral translations of the new fundamental domain still form a disjoint cover of $\mathbb{R}^r$:

$$\mathbb{R}^r \ = \ \dot{\bigcup_{(m_1,...,m_r)\in\mathbb{Z}^r}} \left(\sum_{i=1}^r m_i L(\mathbf{E}_i)\right) + \tilde{\prod} \tag{3.3}$$

and that the boundary of $L^{-1}(\tilde{\prod})$ is contained in a finite number of hyperplanes. To achieve this in a straightforward manner would mean to connect the preimages of the vertices of $\prod$ by hyperplanes, and to consider the logarithmic image of that multiplicative "fundamental domain " as new fundamental domain $\tilde{\prod}$ for Λ applying 3.3 . In the sequel we will study this approach and the occuring difficulties in the simplest case $r = 2$. The ideas for new methods to overcome these difficulties will later form the guiding principles for higher dimensions.

Let us assume that $\mathbf{a} = (a_1, a_2)$ and $\mathbf{b} = (b_1, b_2)$ are linearly independent vectors in logarithmic space spanning a lattice Λ. In exponential space the images of the vertices of the fundamental domain $\prod$ of Λ are the points

$$\mathbf{1} = (1,1), \mathbf{E}_1 = (e^{a_1}, e^{a_2}), \mathbf{E}_2 = (e^{b_1}, e^{b_2}) \text{ and } \mathbf{E}_{12} = (e^{a_1}e^{b_1}, e^{a_2}e^{b_2}) \ .$$

We would be tempted to connect $\mathbf{1}$ with $\mathbf{E}_1, \mathbf{E}_2$ and those two with $\mathbf{E}_{12}$ by straight lines. The images of these lines in logarithmic space are congruent modulo 1, but this does not generally yield a fundamental domain as is demonstrated by the following example.

Example. We choose $\mathbf{E}_1 = (2,4)$, $\mathbf{E}_2 = (4,11)$. Then the preimage of $\prod$ has the vertices $(1,1)$, $(2,4)$, $(4,11)$, $(8,44)$, and the straight lines connecting $(1,1)$, $(4,11)$, respectively $(2,4)$, $(8,44)$, intersect in $(\frac{21}{10}, \frac{14}{3})$.

We therefore proceed as follows. In logarithmic space we assume that S_1 and T_1 are piecewise smooth double point free curves connecting the lattice points $\mathbf{0}$ with $L(\mathbf{E}_1), L(\mathbf{E}_2)$, respectively. We set $S_2 := S_1 + L(\mathbf{E}_2), T_2 := T_1 + L(\mathbf{E}_1)$ and get the following lemma.

Lemma 3.1. *Denote by J the set of points enclosed by $C := S_1 \cup T_2 \cup S_2^{-1} \cup T_1^{-1}$. If the closed curve C is double point free then the set $(J \cup C) \setminus (S_2 \cup T_2)$ is a fundamental domain for $\mathbb{R}^2/\Lambda$.*

We note that a fundamental domain for $\mathbb{R}^2/\Lambda$ yields a fundamental domain for multiplicative equivalence upon applying the exponential map.

Proof. The proof is carried out in several steps. We begin by simplifying the description. For simplicity's sake we assume that the lattice in logarithmic space is spanned by the unit vectors $(1,0), (0,1)$ and the fundamental domain is therefore $[0,1)^2$. This can be easily achieved by a linear transformation.

In a first step we introduce the piecewise smooth boundary curves. We assume that $\phi_1, \phi_2, \psi_1, \psi_2$ are continuously differentiable maps from $[0,1]$ into $\mathbb{R}$ satisfying $0 = \phi_1(0) = \phi_2(0) = \phi_2(1) = \psi_1(0) = \psi_1(1) = \psi_2(0)$ as well as $1 = \phi_1(1) = \psi_2(1)$ such that $C = C_1 \dot{\cup} C_2 \dot{\cup} C_3 \dot{\cup} C_4$ with

$$\begin{aligned} C_1 &= \{(\phi_1(t), \psi_1(t)) \mid t \in [0,1)\} \ , \\ C_2 &= \{(\phi_2(1-t), \psi_2(1-t)) \mid t \in [0,1)\} \ , \\ C_3 &= \{(\phi_1(1-t), \psi_1(1-t)+1) \mid t \in [0,1)\} \ , \\ C_4 &= \{(\phi_2(t)+1, \psi_2(t)) \mid t \in [0,1)\} \ , \end{aligned}$$

and C double point free. By $\bar{G}$ we denote the (closed) area surrounded by C. We will show that the union of the interior of $\bar{G}$ with C_1 and C_2 without the point $(0,1)$ is also a fundamental domain.

Since we will apply some Fourier theory and the theorem of Gauss we introduce several auxiliary formulae in the second step. By the theorem of Gauss an integral over G can be evaluated by a contour integral over the boundary C of G. Using the parametrization of the boundary of G from above we calculate Fourier coefficients:

$$\begin{aligned} (3.4) \quad & 2\pi i m \int_G \exp(2\pi i(mx+ny))d(x,y) \\ & = \int_C \exp(2\pi i(mx(t)+ny(t)))d(C(t)) = 0 \quad (m,n \in \mathbb{Z}, m \neq 0) \ , \end{aligned}$$

the same result also holds for $n \neq 0$; finally we find

$$(3.5) \qquad \int_G d(x,y) \ = \ \int_C d(C(t)) \ = \ 1 \ .$$

In the third step we show that all $x \in [0,1)^2$ are obtained modulo 1. Let us assume that there exists $\mathbf{x} \in [0,1)^2$ with $(m,n)+\mathbf{x}$ not in $\overline{G}$ for all $(m,n) \in \mathbb{Z}^2$. Then the set $\{\mathbf{x}+(m,n) \mid (m,n) \in \mathbb{Z}^2\}$ has a positive distance to $\overline{G}$ which is larger than a positive constant ε. Hence, if $\mathbf{y} \in [0,1]^2$ has distance smaller than ε from $\mathbf{x}$ then the intersection of $\{\mathbf{y}+(m,n) \mid (m,n) \in \mathbb{Z}^2\}$ with $\overline{G}$ is empty. Without loss of generality we can assume that $\mathbf{x} \in (0,1)^2$ and that the open $\varepsilon/2$-neighborhood of $\mathbf{x}$ is contained in $(0,1)^2$.

Consequently, there exists a function $h : [0,1]^2 \to \mathbb{R}$ with the properties:
(i) h is non-negative and $h(\mathbf{z}) > 0$ for all z in the open $\varepsilon/2$-neighborhood of $\mathbf{x}$;
(ii) $h(\mathbf{z}) = 0$ for all $\mathbf{z} \in [0,1]^2$ having a distance of at least ε from $\mathbf{x}$;
(iii) h is arbitrarily often differentiable.
The periodic continuation of h to all of $\mathbb{R}^2$ is denoted H. Also H is arbitrarily often differentiable and has therefore an absolutely convergent Fourier series, say $\sum_{(m,n)\in\mathbb{Z}^2} a_{mn} \exp(2\pi i(mx+ny))$ with $a_{00} \neq 0$. According to

our assumption on $\mathbf{x}$ the function H vanishes on G. Hence, we get a contradiction as follows:

$$\begin{aligned} 0 &= \int_G H(x,y)d(x,y) \\ &= \sum_{(m,n)\in\mathbb{Z}^2} a_{mn} \int_G \exp(2\pi i(mx+ny))d(x,y) \\ &= a_{00} \ . \end{aligned}$$

In the fourth and last step we show that no point $\mathbf{x}$ can occur several times modulo 1. We start to prove this for $\mathbf{x}$ in the interior of G. We assume that also $\mathbf{x} + (m,n) \in G$ for some non-zero $(m,n) \in \mathbb{Z}^2$. Let μ denote the Lebesgue measure. We obtain

$$\begin{aligned} 1 &= \mu([0,1]^2) \\ &= \mu\left(\bigcup_{(m,n)\in\mathbb{Z}^2} (G+(m,n)) \cap [0,1]^2 \right) \\ &\leq \sum_{(m,n)\in\mathbb{Z}^2} \mu((G+(m,n)) \cap [0,1]^2) \\ &= \sum_{(m,n)\in\mathbb{Z}^2} \mu(G \cap [m,m+1] \times [n,n+1]) \\ &= \mu(G) \\ &= 1 \ . \end{aligned}$$

Hence, we must have equality everywhere and translations of G by different integral vectors cannot have common interior points.

A slightly modified argument also shows that a boundary point of one translate of G cannot be an interior point of another one. Eventually, considering two boundary points in different translates, we argue by deforming the boundary curves. $\square$

Remark. The last lemma is proved in a much more general version than needed. Namely, in our case the curves S_1 and T_1 are just images of straight lines under L. But the latter does not lead to any considerable simplification of the proof for $r = 2$.
However, for $r > 2$ we indeed use the fact that the multiplicative fundamental domain in exponential space is a 2^r–gon. The application of Gauss' theorem in that situation becomes much easier since the outer normal is almost everywhere well defined on the boundary. The proof for $r = 2$ given above can therefore easily be adopted to $r > 2$ and so we omit it.

Clearly, the premises of the lemma are not satisfied in the example above if we choose the logarithmic images of the straight lines as curves. We will see, however, that the lemma becomes applicable, if $L(\mathbf{E}_1), L(\mathbf{E}_2)$ form a linearly independent cyclic non-negative set in logarithmic space.

Example (cont.). Clearly, the original vectors

$$\{(\log 2, \log 4),\ (\log 4, \log 11)\}$$

do not form a cyclic non-negative set. The reduction procedure developed in Section 2 for $r = 2$ yields as new (and cyclic non-negative) basis

$$\{(\log 2,\ \log \frac{121}{64})\ ,\ (0,\ \log \frac{16}{11})\}\ .$$

The quadrangle with vertices

$$(1,1),\ (2, \frac{121}{64}),\ (1, \frac{16}{11}),\ (2, \frac{11}{4})$$

is convex and the last lemma becomes applicable.

This phenomenon is explained by the next proposition.

Proposition 3.1. *Any cyclic non-negative basis of vectors* $\mathbf{b}_1, \mathbf{b}_2$ *of a 2–dimensional lattice* Λ *(in logarithmic space) yields a convex fundamental domain for multiplicative equivalence.*

Proof. Let $x_i = \exp(b_{i1}), y_i = \exp(b_{i2})$ for $i = 1, 2$. Hence, we have $1 \leq y_1 \leq x_1,\ 1 \leq x_2 \leq y_2$. We first show that the slope of the straight line through $(1,1)$ and (x_1x_2, y_1y_2) is larger than that through $(1,1)$ and (x_1, y_1) and smaller than that through $(1,1)$ and (x_2, y_2). From our assumptions we obtain successively

$$\begin{aligned}
(x_2 - 1)(x_1 - y_1) &\geq 0\ ,\\
x_2(y_1(x_1 - 1) + x_1(1 - y_1)) - (x_1 - y_1) &\geq 0\ ,\\
y_1y_2(x_1 - 1) + x_1x_2(1 - y_1) - (x_1 - 1) + y_1 - 1) &\geq 0\ ,\\
(y_1y_2 - 1)(x_1 - 1) - (x_1x_2 - 1)(y_1 - 1) &\geq 0\ ,
\end{aligned}$$

as well as

$$\begin{aligned}
(y_1 - 1)(y_2 - x_2) &\geq 0\ ,\\
y_1(x_2(y_2 - 1) + y_2(1 - x_2)) - (y_2 - x_2) &\geq 0\ ,\\
x_1x_2(y_2 - 1) + y_1y_2(1 - x_2) - (y_2 - 1) + (x_2 - 1) &\geq 0\ ,\\
(x_1x_2 - 1)(y_2 - 1) - (y_1y_2 - 1)(x_2 - 1) &\geq 0\ ,
\end{aligned}$$

hence, in case $x_i > 1\ \ (i = 1, 2)$,

$$\frac{y_1 - 1}{x_1 - 1} \leq \frac{y_1y_2 - 1}{x_1x_2 - 1} \leq \frac{y_2 - 1}{x_2 - 1}\quad .$$

If one of the x_i is one, however, the proof is obvious.

Finally, we need to show that the point (x_1x_2, y_1y_2) is not in the interior of the triangle with vertices $(1,1)$, (x_1,y_1), (x_2,y_2). This is again obvious from the size conditions.

$\square$

Although in principle the same ideas can be used in dimensions $r > 2$ the description of the fundamental domain in exponential space becomes much more complicated. The reason for this is that for vertices of a maximal bounding $r-1$–dimensional parallelotope of the fundamental domain of Λ the preimages of these vertices in exponential space will not necessarily lie in a hyperplane anymore. Hence, we need to decompose each of these surfaces in an appropriate way. This will be explained in the sequel.

The general procedure is roughly as follows. The original fundamental domain in logarithmic space is decomposed into a finite number of simplices. For each such simplex we consider the images of its vertices in exponential space. They form the vertices of a simplex there. What we then need to show is that the logarithmic image of the union of the exponential simplices becomes a fundamental domain for the lattice in logarithmic space.

We decompose the fundamental domain of the lattice Λ with basis $\mathbf{b}_1, ..., \mathbf{b}_r$:
For $\sigma \in \mathcal{S}_r$ we set

$$(3.6) \quad P(\sigma) := \{\sum_{i=1}^{r} x_i\mathbf{b}_i \mid 0 \le x_{\sigma(1)} \le x_{\sigma(2)} \le ... \le x_{\sigma(r)} < 1\}$$
$$= \{\sum_{j=1}^{r} x_j \left(\sum_{i=j}^{r} \mathbf{b}_{\sigma(i)}\right) \mid 0 \le x_j \;\; (1 \le j \le r),\; \sum_{j=1}^{r} x_j < 1\}$$

and consequently obtain (we put $x_{\sigma(0)} := 0 \;\forall \sigma \in \mathcal{S}_r$)

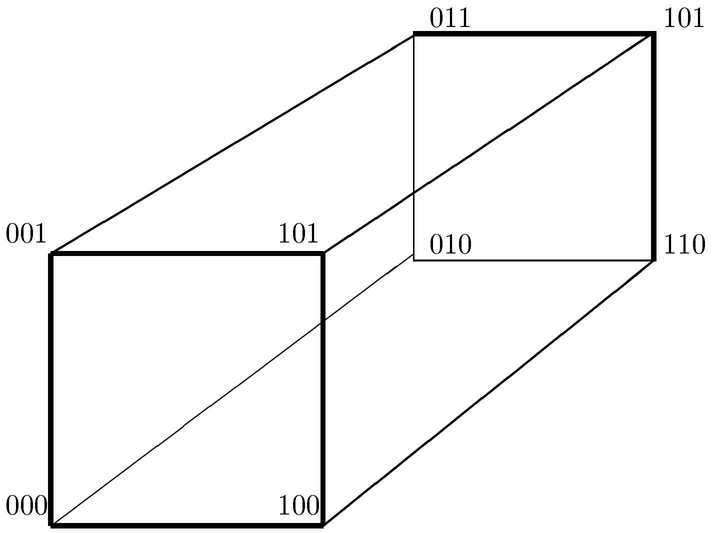
$$(3.7) \quad \prod := \left\{\sum_{i=1}^{r} x_i\mathbf{b}_i \mid 0 \le x_i < 1 \;\; (1 \le i \le r)\right\}$$
$$= \bigcup_{\sigma\in\mathcal{S}_r} P(\sigma)$$
$$= \{\mathbf{0}\} \cup \bigcup_{\kappa=1}^{r} \; \bigcup_{1\le i_1<i_2<...<i_\kappa\le r} \; \bigcup_{\sigma\in\mathcal{S}_r}{}' \left\{\sum_{i=1}^{r} x_i\mathbf{b}_i \mid x_{\sigma(i-1)} \begin{cases} < x_{\sigma(i)} \text{ for } i \in \{i_1, ..., i_\kappa\} \\ = x_{\sigma(i)} \text{ else} \end{cases} \text{and } x_{\sigma(r)} < 1 \right\}.$$

The accent at the last union indicates that sets occuring several times are considered only once. Then all sets of the fourfold union are disjoint and and all components are open simplices in their corresponding dimension.

(Without the accent we had a union over $2^r r!$ sets. With the accent this number decreases from 48 to 26 for $r = 3$.)

The vertices of every such simplex are mapped into exponential space and the images become the vertices of a corresponding simplex there. The simplex defined by $P(\sigma)$ in this way in exponential space will be denoted by $P_e(\sigma)$. We will show that for $\sigma, \tau \in \mathcal{S}_r$ the closures $\overline{P_e(\sigma)}, \overline{P_e(\tau)}$ intersect in the closed simplex which is spanned by the preimages of the vertices of $\overline{P(\sigma)} \cap \overline{P(\tau)}$ thus exactly mirroring the situation in logarithmic space. Because of the definition of $P_e(\sigma)$ it suffices to show that for $\sigma \neq \tau$ the sets $\overline{P_e(\sigma)}$ and $\overline{P_e(\tau)}$ are separated by a hyperplane in exponential space which contains the preimage of $\overline{P(\sigma)} \cap \overline{P(\tau)}$. Therefore we can glue the exponential simplices $P_e(\sigma)$ in the same manner as the fundamental domain of Λ is glued as indicated by the decomposition of $\prod$ into the simplices $P(\sigma)$. Thus we get a 2^r–gon (which is not necessarily convex) whose image in logarithmic space has boundary sets which are congruent modulo 1. Again we can apply Gauss' theorem to prove that we indeed have a fundamental domain. To avoid complications at first it should be assumed that the exponential simplices $P_e(\sigma)$ contain interior points. The other cases are then obtained by performing limits. We omit details since all important steps were already explained in the proof of Lemma 3.1 and the subsequent remark.

Of course, the practical problem remains to show that the union of exponential simplices constructed as above indeed satisfies the requirements of the preceding paragraph. We conjecture that this is in general the case when we choose a cyclic non-negative basis for Λ in the beginning. A rigorous proof is given only in the case $r = 3$ in the sequel.



For proving that different open exponential simplices $P_e(\sigma)$ do not have common points it suffices to show that their vertices are separated by a hyperplane. For a better understanding we enumerate the vertices of the exponential simplices from 0 to 7 in binary representation, e.g., $6 = (0,1,1)$ denotes the vertex whose coordinates are the exponential values of the coordinates of the vector $\mathbf{b}_2 + \mathbf{b}_3$.

In the sequel we only consider the six closed three-dimensional simplices. We order them as follows:

$$\begin{aligned}
&(1)\ x_1 \geq x_2 \geq x_3 \geq 0 \text{ with vertices } 0,1,3,7\ ,\\
&(2)\ x_2 \geq x_3 \geq x_1 \geq 0 \text{ with vertices } 0,2,6,7\ ,\\
&(3)\ x_3 \geq x_1 \geq x_2 \geq 0 \text{ with vertices } 0,4,5,7\ ,\\
&(4)\ x_2 \geq x_1 \geq x_3 \geq 0 \text{ with vertices } 0,2,3,7\ ,\\
&(5)\ x_1 \geq x_3 \geq x_2 \geq 0 \text{ with vertices } 0,1,5,7\ ,\\
&(6)\ x_3 \geq x_2 \geq x_1 \geq 0 \text{ with vertices } 0,4,6,7\ .
\end{aligned}$$

For example, concerning the intersection of simplices (1) and (2) we show that the point 1 is separated from points 2,6 by the plane determined by the three points 0,3,7 . We do this by considering the sign of the determinant whose first two rows are the vectors spanning the separating plane and the last row is the vector from 0 to the point under consideration, i.e., 1 or 2,6. In this way we need to discuss a total of 15 intersections. Because of occuring symmetries it suffices to consider 6 different determinants.

We recall that $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ is a cyclic non-negative basis. The coordinates of these vectors are denoted by $\mathbf{b}_i = (b_{i1}, b_{i2}, b_{i3})$ for $1 \leq i \leq 3$. In exponential space we write $B_{ij} := \exp(b_{ij})\ \ (1 \leq i,j \leq 3)$ for abbreviation. Then the plane through 0,3,7 is spanned by the vectors $(B_{11}B_{21}B_{31} - 1, B_{12}B_{22}B_{32} - 1, B_{13}B_{23}B_{33} - 1), (B_{11}B_{21} - 1, B_{12}B_{22} - 1, B_{13}B_{23} - 1)$ and for the point 1 we need to determine the sign of the determinant

$$\begin{vmatrix} B_{11}B_{21}B_{31} - 1 & B_{12}B_{22}B_{32} - 1 & B_{13}B_{23}B_{33} - 1 \\ B_{11}B_{21} - 1 & B_{12}B_{22} - 1 & B_{13}B_{23} - 1 \\ B_{11} - 1 & B_{12} - 1 & B_{13} - 1 \end{vmatrix} .$$

We do this similarly as in Section 2. We write the determinant as a polynomial $P(B_{11}, B_{12}, B_{13}, B_{21}, B_{22}, B_{23}, B_{31}, B_{32}, B_{33})$. This polynomial is linear in each of its 9 variables. Hence, we only need to discuss its sign on the boundary of each variable. Instead of just considering 2^9 cases we reduce the number of variables by 3, i.e., we discuss polynomials in 6 variables (not necessarily linear anymore) in 8 different cases. We recall that

(3.8)
$$B_{11} \geq B_{12} \geq B_{13} \geq 1\ ,\ B_{22} \geq B_{23} \geq B_{21} \geq 1\ ,\ B_{33} \geq B_{31} \geq B_{32} \geq 1\ .$$

We therefore start to consider the sign of the coefficient P_1 of B_{11} in P: $P = P_1 B_{11} + P_2$. Repeating this procedure we obtain successively:

$$P_1 = P_{11}B_{12} + P_{12}\ ,\ P_{11} = P_{111}B_{13} + P_{112}\ \ .$$

At this stage the coefficient polynomial P_{111} is a polynomial in only 6 variables B_{ij} $(1 \leq j \leq 3\ ,\ i = 2,3)$. Writing it as polynomial in B_{22}, then the coefficients as polynomials in B_{23} the sign of P_{111} (and similarly for any such polynomial in the same 6 variables) can be computed fairly easily. Next we set $B_{13} = 1$ in P_{11} and determine the sign of that polynomial. These two signs take care of the coefficient P_{11} of B_{12} (in the coefficient P_1 of B_{11} in P), i.e., they determine the sign of P_1 for B_{12} large. This is followed by a discussion of the case $B_{12} = B_{13}$. We need to consider a polynomial $\tilde{P}_1 = P_{11}B_{13} + P_{12}$ in the new main variable B_{13} which can be treated similarly.

We note that considering a coefficient of one variable or setting one variable to 1 yields a polynomial with one variable less, but the degrees in the other variables stay invariant. However, if we need to replace one variable by another one, say A by B, the degree of of B in the resulting polynomial can increase. Fortunately, only quadratic polynomials occur. For those we need to consider the coefficient of the quadratic term, the value at a potential extremal point (derivative vanishing), and the value obtained by replacing the variable by the next smaller one. For all quadratic polynomials it turned out that their extremal values were outside the considered interval of the main variable.

For discussing the different cases we wrote a small Maple program [2] which made these investigations a lot easier. As we conjectured it turned out that the signs for any of these parametrized determinants were the same for all potential values of the parameters and did indeed separate the considered simplices. We therefore proved the next theorem.

Theorem 3.1. *Let $r \leq 3$ and $\prod = \bigcup_{\sigma\in\mathcal{S}_r} P(\sigma)$ be the standard decomposition 3.7 of a fundamental domain given by a cyclic non-negative basis in logarithmic space. Let $\mathbf{0}, \mathbf{v}_2(\sigma), ..., \mathbf{v}_{r+1}(\sigma)$ be the $r+1$ vertices of $\overline{P(\sigma)}$ and $\mathbf{1}, \mathbf{E}(\mathbf{v}_j(\sigma))$ $(2 \leq j \leq r+1)$ be their preimages in exponential space. Let*

(3.9)

$$S(\sigma)\ :=\ \{\mathbf{1} + \sum_{j=2}^{r+1} x_j(\mathbf{E}(\mathbf{v}_j(\sigma)) - \mathbf{1})\ |\ 0 \leq x_j\ \ (2 \leq j \leq r+1),\ \sum_{j=2}^{r+1} x_j < 1\}$$

be the simplex spanned by $\mathbf{1}, \mathbf{E}(\mathbf{v}_j(\sigma))$ $(2 \leq j \leq r+1)$ and

$$\mathcal{F}\ =\ \bigcup_{\sigma\in\mathcal{S}_r} S(\sigma)\ \ . \tag{3.10}$$

Then $\mathcal{F}$ is a fundamental domain for multiplicative equivalence as introduced in Definition 3.1.

Remark. (i) If the cyclic non-negative basis in the theorem is denoted $\mathbf{b}_1, ..., \mathbf{b}_r$, then we have $\mathbf{E}_i = \exp(\mathbf{b}_i)$ $(1 \leq i \leq r)$ in Definition 3.1, where the exponential map is applied coordinatewise.
(ii) The amount of work for proving a similar theorem in higher dimensions grows exponentially, but the cases $r = 4, 5, 6$ are easily within the scope of these methods. Also we emphasize that for explicitly given lattices it is no problem to check numerically whether the corresponding simplices $P_e(\sigma)$ can be separated as demonstrated for $r = 3$.

4. Shintani decomposition

Let $\mathbf{f}$ be a module of the totally real algebraic number field F, i.e. $\mathbf{f}$ is an integral ideal of F combined with a subset of the infinite places. In the sequel, we only need the ideal part, which we also denote by $\mathbf{f}$. Let $\mathbf{b}$ be a (fractional) ideal coprime to $\mathbf{f}$, hence representing a narrow ray class $\mathbf{b}$ modulo $\mathbf{f}$. The corresponding ray class zeta function is defined by

$$\zeta(\mathbf{b}, \mathbf{f}, s) := \sum_{\mathbf{g}} N(\mathbf{g})^{-s} \quad ,$$

where the summation is over all integral ideals of $\mathbf{b}$ modulo $\mathbf{f}$. We recall Shintani's ideas [7] for evaluating that zeta function at non-positive integers.

Besides the full unit group U_F of F we need the subgroup of totally positive units U_F^+, respectively the subgroup $U_F^+(\mathbf{f})$ of totally positive ray class units. Both subgroups are of finite index in U_F. A full set of generators for them is easily obtained from fundamental units of U_F.

Example. For determining U_F^+ we just need to find representatives of those classes of U_F/U_F^2, which contain only totally positive units. This is straightforward from the signs of the conjugates of the fundamental units of U_F and requires only binary arithmetic.

The group U_F^+ (respectively $U_F^+(\mathbf{f})$) acts on $(\mathbb{R}^{>0})^n$ as described in the previous section. Shintani showed that there exists a finite number, say s, of open simplicial cones C_j $\quad (1 \leq j \leq s)$ such that

$$(\mathbb{R}^{>0})^n \; = \; \bigcup_{j=1}^{s} \; \bigcup_{\varepsilon \in U_F^+(\mathbf{f})} \varepsilon C_j \quad .$$

The union on the right-hand side is disjoint. The open simplicial cones are spanned by $g \in \{1, ..., n\}$ linearly independent vectors $\mathbf{v}_1, ..., \mathbf{v}_g$:

$$C_j(\mathbf{v}_1, ..., \mathbf{v}_g) := \{\sum_{i=1}^{g} \lambda_i \mathbf{v}_i \mid \lambda_i > 0\} \quad .$$

Following Shintani we set for $S \subset (\mathbb{R}^{>0})^n$:

$$R(j,S) := \{\sum_{i=1}^{g} \lambda_i \mathbf{v}_i \in S \mid \lambda_i \in]0,1] \cap \mathbb{Q}\}$$

and note, that $R(j,S)$ is finite, when S is a subset of a fractional ideal. In the sequel we use the notation $x \in S+1$ for $x-1 \in S$. For $m \in \mathbb{N}$ Shintani obtains:

$$\zeta(\mathbf{b},\mathbf{f},1-m) \;=\; m^{-n}N(\mathbf{b})^{m-1}\sum_{j=1}^{s}\sum_{x\in R(j,\mathbf{b}^{-1}\mathbf{f}+1)}(-1)^{s-j}B_m(A_j,x) \;\; ,$$

where the A_j are matrices the rows of which span one of the s simplicial cones and the B_m are generalized Bernoulli polynomials. Once the simplicial cones are known, all remaining calculations are quite straightforward. This will be demonstrated in a forthcoming paper by the authors. In the remainder of this section we show how to apply the general theory of multiplicative fundamental domains developed in Section 3 in this special situation.

It is of importance that we need multiplicative (in)dependence only for non-zero integers of F of the same norm. This is used to eliminate one dimension. Whereas Shintani [7] and Okazaki [4] do this by requiring the trace of the integers to be one, we rather follow Reidemeister's precedent [6] and normalize the last coordinate to one.

In the sequel we assume that $\varepsilon_1, ..., \varepsilon_r$ are a basis of the unit group under consideration (consisting only of totally positive units). Then the lattice Λ in logarithmic space has the basis

$$\mathbf{E}_i \;:=\; (\log(\varepsilon_i^{(1)}/\varepsilon_i^{(n)}), ..., \log(\varepsilon_i^{(r)}/\varepsilon_i^{(n)})) \quad (1 \le i \le r) \;\; .$$

From these vectors we determine a cyclic non-negative basis $\mathbf{b}_1, ..., \mathbf{b}_r$ which generates a lattice $\tilde{\Lambda}$ of finite index ι in Λ. We just have to keep in mind that the elements which need to be determined in the simplicial cones coming from $\tilde{\Lambda}$ will occur with multiplicity ι. As outlined in Section 3 the fundamental domain of $\tilde{\Lambda}$ with respect to $\mathbf{b}_1, ..., \mathbf{b}_r$ is decomposed in the standard way into $r!$ simplices and the corresponding simplices for the multiplicative fundamental domain are calculated.

Example. Let $F = \mathbb{Q}(\rho)$ for a root ρ of the polynomial $x^4+x^3-4x^2-4x+1$. The discriminant of F is 1125. (Up to isomorphy we could also put $F = \mathbb{Q}(\sqrt{15+6\sqrt{5}})$, but in that case the equation order would not be maximal.) The unit group U_F of F is generated by -1 and the three fundamental units $e_1 = 3\rho - \rho^3, e_2 = 1+\rho, e_3 = 3-\rho^2$. None of the fundamental units is totally positive, only the product of all 3. Hence, the index of U_F^+ in U_F is 4. Choosing the order of the conjugates of ρ appropriately, we obtain a cyclic non-negative basis of Λ from the totally positive units

$\varepsilon_1 := e_1e_2e_3 = 2+\rho,\ \varepsilon_2 = e_3^2 = 8+4\rho-2\rho^2-\rho^3,\ \varepsilon_3 = e_1^2 = 1-3\rho+\rho^3$.

This kind of calculations is very easy with a software package like KANT [1].

References

[1] M. Daberkow et al., *KANT V4*. J. Symb. Comp. **24** (1997), 267–283.

[2] D. Redfern, *The Maple handbook: Maple V release 3.* Springer Verlag, New York (1994).

[3] R. Okazaki, *On an effective determination of a Shintani's decomposition of the cone* $\mathbb{R}_+^n$. J. Math. Kyoto Univ. **33–4** (1993), 1057–1070.

[4] R. Okazaki, *An elementary proof for a theorem of Thomas and Vasquez.* J. Number Th. **55** (1995), 197–208.

[5] M. Pohst, H. Zassenhaus, *Algorithmic Algebraic Number Theory.* Cambridge University Press 1989.

[6] K. Reidemeister, *Über die Relativklassenzahl gewisser relativ–quadratischer Zahlkörper.* Abh. Math. Sem. Univ. Hamburg **1** (1922), 27–48.

[7] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers.* J. Fac. Sci. Univ. Tokyo IA **23** (1976),393–417.

Ulrich Halbritter
Mathematisches Institut
Universität zu Köln
Weyertal 86–90
50931 Köln
Germany
E-mail : `uhalb@math.uni-koeln.de`

Michael E. Pohst
Fachbereich 3 Mathematik, MA 8-1
Technische Universität Berlin
Straße des 17. Juni 136
10623 Berlin
Germany
E-mail : `pohst@math.tu-berlin.de`