Journal de Théorie des Nombres
de Bordeaux **15** (2003), 393–410

Sur la racine carrée de la codifférente

par Stéphane VINATIER

Résumé. On présente deux résultats nouveaux concernant la racine carrée de la codifférente d'une extension faiblement ramifiée de $\mathbb{Q}$. Le premier, relatif à sa structure galoisienne, s'inscrit dans la stratégie classique développée notamment par Fröhlich et Taylor. Le second, qui concerne le réseau entier unimodulaire associé, est prouvé à l'aide de calculs numériques portant sur des exemples intéressants.

Abstract. We present two new results about the square root of the inverse different of a weakly ramified extension of $\mathbb{Q}$. The first one deals with its Galois structure and fits in the classical strategy developed by Fröhlich and Taylor in particular. The second one deals with the associated integral unimodular lattice and is proved through numerical calculation on interesting examples.

1. Introduction

Soit N une extension galoisienne finie de $\mathbb{Q}$. On note $\mathcal{O}$ l'anneau d'entiers de N, $\mathcal{D}$ la différente de l'extension et G son groupe de Galois. On supposera tout au long de cet article que G est d'ordre impair. Sous cette condition, on sait par la formule de Hilbert pour la valuation de $\mathcal{D}$ en un idéal premier de $\mathcal{O}$ qu'il existe un unique idéal fractionnaire $\mathcal{A}$ vérifiant la relation :

$$\mathcal{A}^2 = \mathcal{D}^{-1} \ .$$

On appelle $\mathcal{A}$ la *racine carrée de la codifférente*. De par sa définition, l'idéal $\mathcal{A}$ a deux propriétés qui vont retenir notre attention. D'une part, il est stable pour l'action du groupe de Galois, ce qui en fait un $\mathbb{Z}[G]$-module. D'autre part, il est auto-dual pour la forme trace de l'extension, ce qui en fait un G-réseau entier unimodulaire. C'est cette deuxième propriété qui a d'abord motivé l'étude de $\mathcal{A}$ par Erez [11].

Deux questions se posent donc naturellement à propos de la racine carrée de la codifférente :

- admet-elle une base normale, c'est-à-dire l'idéal $\mathcal{A}$ est-il libre en tant que $\mathbb{Z}[G]$-module ?

Manuscrit reçu le 13 septembre 2001.

- le réseau associé à $\mathcal{A}$ est-il G-isométrique au G-réseau entier unimodulaire standard $\mathbb{Z}[G]$, obtenu en munissant $\mathbb{Z}[G]$ de la forme bilinéaire symétrique q_G qui rend orthonormale la base de $\mathbb{Z}[G]$ formée des éléments de G ?

Précisons que deux G-réseaux sont dits G-isométriques s'ils sont isométriques via une isométrie qui commute à l'action de G. On voit donc que la deuxième question contient la première, puisqu'une telle G-isométrie serait à fortiori un isomorphisme de $\mathbb{Z}[G]$-modules, entraînant la liberté de $\mathcal{A}$ en tant que $\mathbb{Z}[G]$-module.

Dans cet article, on donne à ces deux questions des réponses de natures différentes : réponses théoriques pour la question de structure galoisienne, réponses numériques pour celle du réseau associé.

On commence par traiter le problème le plus classique (et le moins fort), celui de la structure galoisienne de $\mathcal{A}$. On dispose alors des techniques mises au point notamment par Fröhlich [16] et Taylor [23] pour l'étude de la structure galoisienne de l'anneau d'entiers, ainsi que d'un critère local (l'analogue du théorème de Nœther), dû à Erez. Avant de l'énoncer, on a besoin de la définition suivante.

Définition 1.1. *$N/\mathbb{Q}$ est dite faiblement ramifiée si, pour tout idéal premier $\wp$ de $\mathcal{O}$, le deuxième groupe de ramification $G_2(\wp)$ est trivial.*

Il est implicite dans cette définition que l'extension considérée est galoisienne. Le critère local d'Erez [13, théorème 1] stipule que $\mathcal{A}$ est localement libre en tant que $\mathbb{Z}[G]$-module si et seulement si l'extension $N/\mathbb{Q}$ est faiblement ramifiée. La ramification faible est donc une condition nécessaire pour l'existence d'une base normale pour la racine carrée de la codifférente (à fortiori pour que le réseau associé soit G-isométrique au réseau standard). Nous nous plaçons désormais dans le cas où $N/\mathbb{Q}$ est faiblement ramifiée.

Rappelons que l'extension est modérément ramifiée quand, pour tout idéal premier $\wp$ de $\mathcal{O}$, le premier groupe de ramification $G_1(\wp)$ est trivial. Dans le cas de la ramification faible, on accepte un peu de ramification sauvage, que l'on contrôle en exigeant la nullité des groupes $G_2(\wp)$. Cette ramification sauvage n'en pose pas moins des problèmes nouveaux par rapport à ceux traités par Taylor dans [23], qui empêchent encore de résoudre complètement le problème de la structure galoisienne de $\mathcal{A}$ dans le cas de la ramification faible. Dans la partie 2, on rappelle les principaux résultats connus sur cette question et on montre :

Théorème 1. *Soient p un nombre premier impair et $N/\mathbb{Q}$ une p-extension finie, faiblement ramifiée, de groupe de Galois G. On note $(\mathcal{A})$ la classe de la racine carrée de la codifférente de l'extension dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres et e l'indice de ramification en p dans $N/\mathbb{Q}$. Alors $(\mathcal{A})^e = 1$.*

Dans notre cadre, la liberté de $\mathcal{A}$ en tant que $\mathbb{Z}[G]$-module équivaut à la trivialité de la classe $(\mathcal{A})$. La majoration de l'ordre de $(\mathcal{A})$ donnée par le résultat précédent n'est certainement pas optimale. Des calculs numériques menés sur un grand nombre d'exemples, ainsi que le théorème 2.1 ci-dessous, nous font croire à la conjecture suivante.

Conjecture. *Soit $N/\mathbb{Q}$ une extension faiblement ramifiée de degré impair, de groupe de Galois G. Alors $\mathcal{A}$ est un $\mathbb{Z}[G]$-module libre.*

On en vient ensuite au problème de la structure du G-réseau entier unimodulaire associé à $\mathcal{A}$. On fait le point sur les résultats théoriques connus. Là encore, la ramification faible et sauvage pose des problèmes non entièrement résolus (à part dans le cas des extensions abéliennes de $\mathbb{Q}$). Des calculs menés à l'aide du logiciel PARI [4] sur des exemples d'extensions faiblement ramifiées non abéliennes permettent de montrer le résultat suivant :

Théorème 2. *Il existe des extensions $N/\mathbb{Q}$ faiblement ramifiées de degré impair, pour lesquelles le réseau associé à $\mathcal{A}$ n'est pas isométrique au réseau standard $\mathbb{Z}[G]$, avec $G = \mathrm{Gal}(N/\mathbb{Q})$. Parmi celles-ci, il y a des extensions modérées, ainsi que des extensions sauvagement ramifiées pour lesquelles $\mathcal{A}$ est isomorphe à $\mathbb{Z}[G]$ en tant que $\mathbb{Z}[G]$-module.*

On donne le détail de ces calculs dans la partie 3, ainsi que des exemples d'extensions adéquats. Ces deux théorèmes complètent les résultats présentés dans [25] et [26].

Remerciements. L'auteur remercie le rapporteur de l'article pour sa lecture attentive et pour ses commentaires.

2. Structure galoisienne

En plus du critère local évoqué plus haut, Erez a obtenu des résultats globaux sur la structure galoisienne de $\mathcal{A}$: il a notamment montré que $\mathcal{A}$ est un $\mathbb{Z}[G]$-module libre quand l'extension est abélienne, absolue et faiblement ramifiée [11], ainsi que dans le cas où l'extension est modérément ramifiée [13, théorème 3] (ce résultat est valable pour une extension relative galoisienne de corps de nombres N/K, en considérant toujours $\mathcal{A}_{N/K}$ comme $\mathbb{Z}[G]$-module).

Lorsque l'extension n'est pas abélienne et que la ramification sauvage rentre en jeu, les outils dont on dispose sont moins performants. On montre cependant dans [25] :

Théorème 2.1. *Soit $N/\mathbb{Q}$ une extension faiblement ramifiée de groupe G d'ordre impair. On suppose que les groupes de décomposition aux places sauvages de $N/\mathbb{Q}$ sont abéliens. Alors $\mathcal{A}$ est un $\mathbb{Z}[G]$-module libre.*

L'hypothèse technique sur les groupes de décomposition aux places sauvages peut rappeller celle apparaissant dans un article récent de Cassou-Noguès et Taylor [7] sur la structure galoisienne de l'anneau d'entiers d'une extension sauvagement ramifiée de $\mathbb{Q}$. On la verra ressurgir comme une condition naturelle lorsqu'on présentera des résultats numériques sur le réseau associé à $\mathcal{A}$.

2.1. Stratégie de la preuve du théorème 2.1. Sans entrer dans le détail de la démonstration de ce théorème, donnée dans [25], on souhaite en présenter quelques étapes en rappelant notamment les notations et les résultats que nous utilisons pour démontrer le théorème 1 dans le paragraphe suivant. La stratégie d'attaque du problème est la même que celle utilisée par Taylor pour démontrer la conjecture de Fröhlich dans [23] et par bien d'autres auteurs depuis. Par contre, le traitement des places sauvages requiert de nouvelles méthodes et utilise l'hypothèse du théorème 2.1 sur les groupes de décomposition en ces places. Hormis ce dernier point, ce travail s'applique à la situation considérée dans le théorème 1.

Puisque $N/\mathbb{Q}$ est supposée faiblement ramifiée, on sait grâce au critère local d'Erez rappelé dans l'introduction que $\mathcal{A}$ est localement libre en tant que $\mathbb{Z}[G]$-module. On peut donc considérer sa classe $(\mathcal{A})$ dans le groupe des classes de $\mathbb{Z}[G]$-modules localement libres $\mathrm{Cl}(\mathbb{Z}[G])$. Le fait que G soit d'ordre impair apporte un avantage par rapport à la situation étudiée par Taylor, à savoir que $\mathcal{A}$ est libre en tant que $\mathbb{Z}[G]$-module si et seulement si $(\mathcal{A})$ est triviale (il y a simplification).

L'étude de $(\mathcal{A})$ se fait grâce à la Hom-description de Fröhlich de $\mathrm{Cl}(\mathbb{Z}[G])$, qui est l'isomorphisme de groupes suivant [16] :

$$\mathrm{Cl}(\mathbb{Z}[G]) \simeq \frac{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^*)\mathrm{Det}(\mathcal{U}(\mathbb{Z}[G]))} \tag{1}$$

où, ayant fixé une clôture algébrique $\mathbb{Q}^c$ de $\mathbb{Q}$, R_G est le groupe additif des caractères virtuels de G dans $\mathbb{Q}^c$, $E \subset \mathbb{Q}^c$ un corps de nombres "suffisamment gros" pour contenir les valeurs des fonctions de caractères considérées, $J(E)$ désigne le groupe des idèles de E, $\Omega_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ et $\mathcal{U}(\mathbb{Z}[G]) = \prod_p \mathbb{Z}_p[G]^*$. Pour plus de précisions, voir [16, I.2] ou [12, 2]. La stratégie consiste alors à trouver un représentant f de la classe $(\mathcal{A})$ dans $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))$ et à montrer qu'il appartient en fait au dénominateur de (1). On obtient le représentant de $(\mathcal{A})$ à l'aide de deux sortes d'ingrédients, les résolvantes (de nature algébrique) et les sommes de Gauss (de nature analytique, car issues de l'équation fonctionnelle des fonctions L d'Artin). Soit l un premier de $\mathbb{Q}$. Puisque $\mathcal{A}$ est localement libre en tant que $\mathbb{Z}[G]$-module, il existe une base a_l de $\mathcal{A}_l = \mathcal{A} \otimes_\mathbb{Z} \mathbb{Z}_l$ sur $\mathbb{Z}_l[G]$. Si χ est le caractère d'une représentation T de G, on définit la résolvante par :

$$(a_l \mid \chi) = \mathrm{Det}\Big(\sum_{g\in G} a_l{}^g T(g^{-1})\Big)$$

(on sait que cela ne dépend que de χ) et on désigne par $R_l(\chi)$ l'idèle de E dont la p-composante est donnée par :

$$R_l(\chi)_p = \begin{cases} 1 & \text{si } p \neq l, \\ (a_l \mid \chi) & \text{si } p = l. \end{cases}$$

On note τ_l la somme de Gauss locale en l [19, II4]. A l'instar d'Erez, on la "tord" à l'aide de la seconde opération d'Adams ψ. Il s'agit de l'endomorphisme de R_G défini pour $\chi \in R_G$ par $\psi(\chi)(g) = \chi(g^2)$ pour tout $g \in G$. On définit alors $\widetilde{T}_l(\chi) \in E^*$ par :

$$\widetilde{T}_l(\chi) = \begin{cases} 1 & \text{si } l = \infty, \\ \tau_l(\chi - \psi(\chi)) & \text{sinon.} \end{cases}$$

Soit S l'ensemble des diviseurs premiers de G et soit S_W l'ensemble des premiers de $\mathbb{Q}$ qui sont sauvagement ramifiés dans $N/\mathbb{Q}$ (bien sûr, $S_W \subset S$). Si $l \notin S_W$, on définit de même $\widetilde{T}_l^*$ à partir de la somme de Gauss modifiée τ_l^* [23, 3]. On obtient alors comme dans [25] :

Proposition 2.2. *Soit $f_{(l)}$ (resp. $f^*_{(l)}$) l'application $R_l\widetilde{T}_l^{-1}$ (resp. $R_l\widetilde{T}_l^{*-1}$) pour $l \in S_W$ (resp. $l \notin S_W$). Alors*

$$f = \prod_{l\in S_W} f_{(l)} \prod_{l\notin S_W} f^*_{(l)}$$

où le produit court sur toutes les places l de $\mathbb{Q}$, est un représentant de $(\mathcal{A})$ dans $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J(E))$.

Il faut maintenant étudier le représentant f. Pour cela, on considère, pour chaque p premier, la composante f_p de f dans $\mathrm{Hom}(R_G, J_p(E))$, où $J_p(E) = (E \otimes_{\mathbb{Q}} \mathbb{Q}_p)^*$. Le théorème 2 de [13] entraîne que, pour tout premier p, $f_p \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, \mathcal{U}_p(E))$, où $\mathcal{U}_p(E)$ est le groupe des unités de $J_p(E)$. Or on sait par la proposition 2.2 de [16, I] que, si $\mathcal{M}$ est un ordre maximal de $\mathbb{Q}[G]$, alors

$$\mathrm{Det}(\mathcal{M}_p{}^*) = \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, \mathcal{U}_p(E)) \tag{2}$$

où $\mathcal{M}_p = \mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Enfin, lorsque p est premier à $|G|$, $\mathbb{Z}_p[G]$ est un ordre maximal de $\mathbb{Q}_p[G]$ (donc $\mathbb{Z}_p[G] = \mathcal{M}_p$ pour un bon choix d'un ordre maximal $\mathcal{M}$ de $\mathbb{Q}[G]$). On en déduit :

Proposition 2.3. *Soit p un nombre premier avec $p \notin S$, alors $f_p \in \mathrm{Det}(\mathbb{Z}_p[G]^*)$.*

Soit maintenant p un premier divisant l'ordre de G. L'isomorphisme (3) ci-dessous montre qu'on peut travailler entièrement localement, bien que f_p soit à valeurs semi-locales ($J_p(E) \simeq \prod_{\mathfrak{p}\,|\,p} E_{\mathfrak{p}}^*$). On fixe pour tout premier p une clôture algébrique $\mathbb{Q}_p^c$ de $\mathbb{Q}_p$ ainsi qu'un plongement :

$$j_p \,:\, \mathbb{Q}^c \hookrightarrow \mathbb{Q}_p^c \ .$$

Pour tout corps de nombres F, on note F_p la fermeture de $j_p(F)$ dans $\mathbb{Q}_p^c$ et on note encore j_p l'homomorphisme d'algèbres induit : $F \otimes_{\mathbb{Q}} \mathbb{Q}_p \twoheadrightarrow F_p$. Soit $R_{G,p}$ l'anneau des caractères virtuels de G dans $\mathbb{Q}_p^c$, alors l'application $\chi \mapsto \chi^{j_p}$ est un isomorphisme d'anneaux de R_G sur $R_{G,p}$. On obtient ainsi un homomorphisme de groupes :

$$\begin{array}{rrcl} j_p^* \,:\, & \mathrm{Hom}(R_G, J_p(E)) & \longrightarrow & \mathrm{Hom}(R_{G,p}, E_p^*) \\ & f & \longmapsto & \big(\chi \mapsto f(\chi^{j_p^{-1}})^{j_p}\big) \end{array}$$

qui induit l'isomorphisme de groupes [16, II, lemma 2.1] :

$$j_p^* \,:\, \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J_p(E))}{\mathrm{Det}(\mathbb{Z}_p[G]^*)} \simeq \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G,p}, E_p^*)}{\mathrm{Det}(\mathbb{Z}_p[G]^*)} \tag{3}$$

où $\Omega_{\mathbb{Q}_p} = \mathrm{Gal}(\mathbb{Q}_p^c/\mathbb{Q}_p)$. On peut se reporter à [7] pour des détails. De plus, si on note $G(p)$ le groupe de décomposition en p dans $N/\mathbb{Q}$, on montre que, pour un bon choix de a_p, il existe une base α_p de $\mathcal{A}_{N_p/\mathbb{Q}_p}$ comme $\mathbb{Z}_p[G(p)]$-module telle que :

$$j_p^*(a_p \mid ..) = \mathrm{Ind}_{G(p)}^G(\alpha_p \mid ..)$$

modulo un élément de $\mathrm{Det}(\mathbb{Z}_p[G]^*)$ (que l'on omettra dorénavant). Pour $\chi \in R_G$ et l un nombre premier, notons χ_l la restriction de χ à $G(l)$. Soit $\theta \in R_{G,p}$, alors

$$j_p^*(\widetilde{T}_l)(\theta) = \widetilde{T}_l(\theta_l^{j_p^{-1}})^{j_p}.$$

On en déduit que $j_p^*(\widetilde{T}_l) \in \mathrm{Ind}_{G(l)}^G(\mathrm{Hom}(R_{G(l),p}, E_p^*))$; il en va de même pour $j_p^*(\widetilde{T}_l^*)$.

Il suffit maintenant pour montrer le théorème 2.1 de démontrer que $j_p^*(f_p) \in \mathrm{Det}(\mathbb{Z}_p[G]^*)$ pour tout nombre premier $p \in S$. On constate que $j_p^*(f_p)$ est un produit d'au plus trois types de facteurs choisis parmi les suivants :

$$j_p^*(f_{(p),p}) \text{ ou } j_p^*(f_{(p),p}^*), \quad j_p^*(f_{(l),p}^*),\ l \notin S_W, \quad j_p^*(f_{(l),p}),\ l \in S_W$$

où $l \neq p$ décrit l'ensemble des nombres premiers de $\mathbb{Q}$ correspondant à une place ramifiée dans $N/\mathbb{Q}$ (en effet, $f_{(l),p}^* = 1$ si l correspond à une place non ramifiée). On note que le premier facteur n'intervient que si $p \in S_W$, le deuxième seulement si $p \notin S_W$. Le comportement des facteurs "modérés" $j_p^*(f_{(p),p}^*)$, pour lequel $p \notin S_W$, et $j_p^*(f_{(l),p}^*)$, pour lequel $l \neq p$, $l \notin S_W$ (mais p peut indifféremment appartenir ou non à S_W) s'obtient essentiellement par adaptation de résultats existants. Ainsi, le traitement de $j_p^*(f_{(l),p}^*)$ se fait à l'aide du théorème 3 de [23], avec des aménagements rendus possibles par les inclusions (2-7) de [6]. On obtient [25, lemme 4.4] :

Lemme 2.4. *Pour tout premier l avec $l \notin S_W$ et $l \neq p$, il existe une extension galoisienne non ramifiée $F_l/\mathbb{Q}_p$ telle que*

$$j_p^*(f_{(l),p}^*) \in \mathrm{Ind}_{G(l)}^G \mathrm{Det}(\mathcal{O}_{F_l}[G(l)]^*) \ .$$

Ce résultat sera utile dans la suite. Précisons qu'il ne nécessite pas d'hypothèse sur les groupes de décomposition aux places sauvages, puisque l'on travaille au-dessus d'une place modérée. Le traitement des facteurs de la forme $j_p^*(f_{(p),p}^*)$ avec $p \notin S_W$ est basé sur la preuve du théorème 31 de [16], en utilisant le théorème 5.2 et l'égalité (6.3) de [13] (on reprend celle-ci plus bas dans le lemme 2.8).

Le comportement des facteurs "sauvages" $j_p^*(f_{(p),p})$ (pour lequel $p \in S_W$) et $j_p^*(f_{(l),p})$, pour lequel $l \neq p, l \in S_W$ (mais p peut indifféremment appartenir ou non à S_W) nécessite l'hypothèse faite dans le théorème sur les groupes de décomposition aux places sauvages. Notamment, le traitement du premier d'entre eux utilise la description exhaustive des extensions abéliennes faiblement et sauvagement ramifiées de $\mathbb{Q}_p$ [25, théorème 1.1], qui est obtenue grâce à la version locale de la théorie de Kronecker-Weber.

2.2. Preuve du théorème 1. On en vient maintenant à la preuve du théorème 1. Soit $N/\mathbb{Q}$ une p-extension finie galoisienne de groupe G, faiblement ramifiée. Si p n'est pas ramifié dans $N/\mathbb{Q}$, le résultat est une conséquence de [13, théorème 3]. On suppose donc que p est ramifié, on a alors $S = S_W = \{p\}$ et l'on sait que le groupe d'inertie Γ_0 de $N_p/\mathbb{Q}_p$ est abélien p-élémentaire (par exemple à l'aide des corollaires 1 et 3 de [20, IV]), d'ordre e. Par la proposition 2.3, on ne doit se préoccuper que de :

$$j_p^*(f_p) = j_p^*(f_{(p),p}) \prod_{l \neq p} j_p^*(f_{(l),p}^*) \ ,$$

où l décrit l'ensemble des diviseurs premiers du discriminant de l'extension qui sont distincts de p. Le lemme 2.4 traite les facteurs en l, ce qui nous ramène à étudier $j_p^*(f_{(p),p})$. C'est le produit d'une résolvante par une somme de Gauss et on a le résultat suivant pour la puissance p-ième de la somme de Gauss.

Proposition 2.5. *Sous les hypothèses du théorème 1, soit la fonction $m_p \in \mathrm{Hom}(R_G, E^*)$ définie par $m_p(\chi) = \tau_p(\chi - \psi(\chi))$ pour tout $\chi \in R_G$. Alors ${m_p}^p \in \mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, \mathcal{O}_E^*)$ et, pour tout nombre premier l distinct de p, on a $j_l^*({m_p}^p) \in \mathrm{Det}(\mathbb{Z}_l[G]^*)$.*

Preuve. Puisque G est un p-groupe, la deuxième assertion découle de la première, via le raisonnement tenu pour obtenir la proposition 2.3. Par définition des sommes de Gauss locales, on note que $m_p = \mathrm{Ind}_\Gamma^G n_p$, où Γ est le groupe de Galois de l'extension $N_p/\mathbb{Q}_p$ (identifié au groupe de décomposition en p) et, pour tout $\chi \in R_\Gamma$, $n_p(\chi) = \tau_p(\chi - \psi(\chi))$.

Il suffit de calculer n_p sur les caractères irréductibles de Γ. Or, bien que la suite exacte $1 \longrightarrow \Gamma_0 \longrightarrow \Gamma \longrightarrow \Gamma/\Gamma_0 \longrightarrow 1$ ne soit pas nécessairement scindée, on dispose d'un analogue du "lemme des petits groupes" [21, proposition 25]. Soient φ un caractère irréductible de Γ_0 et $\gamma \in \Gamma$, on définit le caractère φ^γ par :

$$\varphi^\gamma(x) = \varphi(\gamma^{-1}x\gamma) \ ,$$

pour $x \in \Gamma_0$, et on note $\Sigma = \{\gamma \in \Gamma,\ \varphi^\gamma = \varphi\}$ le stabilisateur de φ. On déduit alors de [9, 11.47] que φ s'étend en un caractère abélien de Σ. Le caractère de Γ induit par φ est irréductible et la proposition 5.1 de [15] montre que tout caractère irréductible χ de Γ est de cette forme :

$$\chi = \mathrm{Ind}_\Sigma^\Gamma \varphi \ .$$

Comme $[\Gamma : \Sigma]$ est premier à 2, la seconde opération d'Adams ψ commute à l'induction de Σ à Γ. Or $\varphi - \psi(\varphi) = \varphi - \varphi^2$ est un caractère de degré 0. Par la propriété d'induction en degré 0 de la somme de Gauss, on en déduit :

$$n_p(\chi) = \tau_p(\varphi - \varphi^2) \ . \tag{4}$$

On détermine maintenant le conducteur de φ. Comme φ est abélien, il est trivial sur le sous-groupe dérivé Σ' de Σ. Notons N' (resp. N_Σ) la sous-extension de N_p fixée par Σ' (resp. Σ). Alors $\mathrm{Gal}(N'/N_\Sigma) \simeq \Sigma/\Sigma'$ et on peut voir φ comme un caractère de ${N_\Sigma}^*$ via la théorie du corps de classes. Enfin $\Gamma_0 \subset \Sigma$, donc p est une uniformisante de N_Σ.

Lemme 2.6. *Le conducteur de φ et celui de φ^2 sont égaux et valent :*

$$f(\varphi) = f(\varphi^2) = \begin{cases} p^2\mathcal{O}_{N_\Sigma} & \textit{si } \varphi \textit{ est ramifié,} \\ \mathcal{O}_{N_\Sigma} & \textit{sinon.} \end{cases}$$

Preuve. On a $\varphi(1 + p^2\mathcal{O}_{N_\Sigma}) = \varphi\big((1 + p^2\mathcal{O}_{N_\Sigma}, N'/N_\Sigma)\big)$, où $(.., N'/N_\Sigma)$ est l'application d'Artin, et on sait par le théorème 2 de [20, XV] et le théorème de Herbrand [20, IV, proposition 14] que

$$(1 + p^2\mathcal{O}_{N_\Sigma}, N'/N_\Sigma) = (\Sigma/\Sigma')^2 = (\Sigma^2\Sigma')/\Sigma' \ .$$

Or $\Sigma^2 \subset \Sigma_2 = \Gamma_2 \cap \Sigma = \{1\}$, donc φ est trivial sur $1 + p^2\mathcal{O}_{N_\Sigma}$. Si de plus $\varphi(1 + p\,\mathcal{O}_{N_\Sigma}) = 1$, alors φ est trivial sur $(\Sigma/\Sigma')^1 = (\Sigma/\Sigma')_1 = (\Sigma/\Sigma')_0$, donc φ est non ramifié et son conducteur est $\mathcal{O}_{N_\Sigma}$. □

En utilisant le lien avec le "local root number" W [22, p. 94], on obtient :

$$\tau_p(\varphi - \varphi^2) = \frac{\tau_p(\varphi)}{\tau_p(\varphi^2)} = \frac{W(\overline{\varphi})}{W(\overline{\varphi}^2)}$$

(ici $\overline{\varphi} = \varphi^{-1}$). Vu le lemme précédent et à l'aide du corollaire 1 de [22, p. 96], on en déduit que $\tau_p(\varphi - \varphi^2)$ est une racine de l'unité. Il s'ensuit que n_p et m_p sont à valeurs dans $\mathcal{O}_E^*$.

Etudions maintenant l'action galoisienne sur n_p. Soit $\omega \in \Omega_{\mathbb{Q}}$, on déduit de (4) et du théorème 5.1 de [19, II] :

$$n_p(\chi^{\omega^{-1}})^{\omega} = \varphi(u_p(\omega))^{-1} n_p(\chi)$$

où $u_p(\omega)$ est l'unique élément de $\mathbb{Z}_p^*$ tel que $\eta^{\omega^{-1}} = \eta^{u_p(\omega)}$ pour tout η racine p^n-ième de l'unité de $\mathbb{Q}_p^c$ (n entier quelconque). Puisque $u_p(\omega)$ est une unité, son image dans $\mathrm{Gal}(N_p/N_\Sigma)$ par l'application d'Artin est un élément du groupe d'inertie Γ_0, donc son ordre est 1 ou p. Comme φ est un caractère abélien, on en tire que $\varphi(u_p(\omega))^p = 1$, c'est-à-dire que ${n_p}^p$ et donc ${m_p}^p$ commutent à l'action de $\Omega_{\mathbb{Q}}$. $\square$

On en déduit que $(\mathcal{A})^p$ est représenté dans $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J(E))$ par la fonction $g = (f{m_p}^{-1})^p$, ce qui ramène à étudier $j_p^*(f_{(p),p}{m_p}^{-1})^p = \mathrm{Ind}_\Gamma^G(h_p)^p$ où h_p est l'élément de $\mathrm{Hom}(R_{\Gamma,p}, \mathcal{O}_{E_p}^*)$ défini par :

$$h_p(\chi) = (\alpha_p \,|\, \chi)$$

α_p étant une base normale de la racine carrée de la codifférente locale $\mathcal{A}_{N_p/\mathbb{Q}_p}$. On note N_0 la sous-extension de N_p fixée par Γ_0 et $q = p^f$ le cardinal du corps résiduel de N_0. On a :

Proposition 2.7. $h_p^{(q-1)e} \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma]^*)$.

Preuve. On commence par se ramener au groupe d'inertie Γ_0 de l'extension. L'égalité (6.3) de [13], que l'on retranscrit dans le lemme suivant, donne le comportement de la résolvante par rapport à la restriction $\mathrm{Res} = \mathrm{Res}_{\Gamma_0}^{\Gamma}$ des caractères au groupe d'inertie. On note β_p une base de $\mathcal{A}_{N_p/\mathbb{Q}_p}$ comme $\mathcal{O}_{N_0}[\Gamma_0]$-module.

Lemme 2.8. *Il existe $\lambda \in \mathcal{O}_{N_0}[\Gamma]^*$ tel que, pour tout $\chi \in R_\Gamma$:*

$$(\alpha_p \,|\, \chi) = (\beta_p \,|\, \mathrm{Res}\,\chi)\mathrm{Det}_\chi(\lambda) \ .$$

Soit k_p l'élément de $\mathrm{Hom}(R_{\Gamma_0,p}, E_p^*)$ défini par $k_p(\theta) = (\beta_p \,|\, \theta)$ pour tout $\theta \in R_{\Gamma_0,p}$. On déduit du lemme précédent que, pour un $\lambda \in \mathcal{O}_{N_0}[\Gamma]^*$:

$$h_p = \mathrm{Ind}_{\Gamma_0}^{\Gamma}(k_p)\mathrm{Det}(\lambda) \ . \tag{5}$$

Voici un premier résultat concernant la fonction k_p :

Lemme 2.9. $(k_p)^p \in \mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0,p}, \mathcal{O}_{E_p}^*)$.

Preuve. Soit θ un caractère de Γ_0. La proposition 4.4 de [16, I] donne l'action de $\omega \in \Omega_{N_0}$ sur la résolvante :

$$(\beta_p \,|\, \theta^{\omega^{-1}})^{\omega} = (\beta_p \,|\, \theta)\mathrm{Det}_\theta(\omega) \ .$$

Comme Det_θ est un caractère de Γ_0 qui est d'exposant p, on en déduit que $(k_p)^p$ est Ω_{N_0}-équivariant, c'est-à-dire $(k_p)^p \in \mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0,p}, E_p^*)$.

Il faut maintenant montrer que $(\beta_p \,|\, \theta) \in \mathcal{O}_{E_p}^*$. On suit pour cela le cheminement de la preuve de [13, proposition 7.6]. Si ζ_p est une racine primitive p-ième de l'unité, les extensions N_0 et $\mathbb{Q}_p(\zeta_p)$ sont linéairement disjointes sur $\mathbb{Q}_p$, donc $H = \mathrm{Gal}(N_0(\zeta_p)/N_0)$ est isomorphe à $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$. On tire de la formule ci-dessus :

$$\prod_{\omega\in H} (\beta_p \,|\, \theta^\omega) = \prod_{\omega\in H} (\beta_p \,|\, \theta)^\omega \prod_{\omega\in H} \mathrm{Det}_\theta(\omega^{-1})^\omega \quad .$$

Or $\mathrm{Det}_\theta(\omega^{-1})$ est une racine p-ième de l'unité et la valuation de $(\beta_p \,|\, \theta)^\omega$ ne dépend pas de $\omega \in H$. On est donc ramené à prouver que $\prod_H (\beta_p \,|\, \theta^\omega) = (\beta_p \,|\, \sum_H \theta^\omega)$ appartient à $\mathcal{O}_{E_p}^*$. Tous les θ^ω ayant le même noyau $\ker(\theta)$, on note N_θ la sous-extension de N_p fixée par $\ker(\theta)$ et $\Gamma_\theta = \Gamma_0/\ker(\theta)$; alors, par [13, lemme 7.9] :

$$\sum_H \theta^\omega = \mathrm{Inf}_{\Gamma_\theta}^{\Gamma_0}\big(\mathrm{reg}_{\Gamma_\theta} - 1_{\Gamma_\theta}\big) \quad ,$$

où $\mathrm{Inf}_{\Gamma_\theta}^{\Gamma_0}$ est l'inflation des caractères de Γ_θ à Γ_0, $\mathrm{reg}_{\Gamma_\theta}$ et 1_{Γ_θ} désignent respectivement le caractère de la représentation régulière et le caractère trivial de Γ_θ. Posons $\beta_\theta = \mathrm{tr}_{N_p/N_\theta}(\beta_p)$, on a :

$$\big(\beta_p \,|\, \sum_H \theta^\omega\big) = \frac{(\beta_\theta \,|\, \mathrm{reg}_{\Gamma_\theta})}{(\beta_\theta \,|\, 1_{\Gamma_\theta})} \quad .$$

Soit $\mathcal{P}$ (resp. $\wp_\theta$, $\wp_0$) l'idéal premier de l'anneau d'entiers de N_p (resp. N_θ, N_0), alors $\mathcal{A}_{N_p/\mathbb{Q}_p} = \mathcal{P}^{1-e}$ par la formule de Hilbert pour la valuation de la différente et, par [20, III, proposition 7] :

$$\mathrm{tr}_{N_p/N_0}(\mathcal{A}_{N_p/\mathbb{Q}_p}) = \mathcal{O}_{N_0} \quad .$$

On en déduit $\mathcal{O}_{N_0} = \mathrm{tr}_{N_p/N_0}(\mathcal{O}_{N_0}[\Gamma_0]\beta_p) = \mathrm{tr}_{N_p/N_0}(\beta_p)\mathcal{O}_{N_0}$, puis

$$(\beta_\theta \,|\, 1_{\Gamma_\theta}) = \mathrm{tr}_{N_\theta/N_0}(\beta_\theta) = \mathrm{tr}_{N_p/N_0}(\beta_p) \in \mathcal{O}_{N_0}^*.$$

Si θ n'est pas le caractère trivial de Γ_0, alors $|\ker(\theta)| = e/p$ et on obtient de manière analogue :

$$\mathrm{tr}_{N_p/N_\theta}(\mathcal{A}_{N_p/\mathbb{Q}_p}) = {\wp_\theta}^{1-p} = \mathcal{A}_{N_\theta/N_0} \quad .$$

En particulier, $\beta_\theta = \mathrm{tr}_{N_p/N_\theta}(\beta_p) \in {\wp_\theta}^{1-p} \setminus {\wp_\theta}^{2-p}$, d'où $\beta_\theta\mathcal{O}_{N_\theta} = \mathcal{A}_{N_\theta/N_0}$. Sinon, $\ker(\theta) = \Gamma_0$, $N_\theta = N_0$, donc $\beta_\theta \in \mathcal{O}_{N_\theta}^*$ et on a encore $\mathcal{A}_{N_\theta/N_0} = \beta_\theta\mathcal{O}_{N_\theta}$. Dans les deux cas, β_θ engendre une base “normale” de $\mathcal{A}_{N_\theta/N_0}$ comme $\mathcal{O}_{N_\theta}$-module, sous l'action de $\mathrm{Gal}(N_\theta/N_\theta) = \{1\}$. On utilise alors la formule d'induction pour la résolvante [13, p.252], en notant que $\mathrm{reg}_{\Gamma_\theta} = \mathrm{Ind}_{\{1\}}^{\Gamma_\theta} 1_{\{1\}}$, et on obtient l'égalité suivante entre idéaux de $\mathcal{O}_{E_p}$:

$$((\beta_\theta \mid \mathrm{reg}_{\Gamma_\theta})) = \mathrm{N}_{N_\theta/N_0}(\beta_\theta)(d_{N_\theta/N_0})^{1/2}$$

où $\mathrm{N}_{N_\theta/N_0}$ désigne la norme de N_θ à N_0 et d_{N_θ/N_0} le discriminant de cette extension. Mais la norme de $\beta_\theta \mathcal{O}_{N_\theta} = \mathcal{A}_{N_\theta/N_0}$ vaut justement $(d_{N_\theta/N_0})^{-1/2}$, donc $(\beta_\theta \mid \mathrm{reg}_{\Gamma_\theta})$ est lui aussi une unité. $\square$

Soit $\mathcal{M}_0$ l'ordre maximal de $N_0[\Gamma_0]$. On déduit du lemme précédent et de l'analogue de (2) avec N_0 comme corps de base qu'il existe $u \in \mathcal{M}_0{}^*$ tel que $(k_p)^p = \mathrm{Det}(u)$. De plus, en notant $|\Gamma_0| = p^m$ ($m \geq 1$ d'après nos hypothèses) et $r = 1 + p + \cdots + p^{m-1}$, on a la décomposition :

$$\mathcal{M}_0 = \mathcal{O}_{N_0} \oplus \big(\underbrace{\mathcal{O}_{N_0(\zeta_p)} \oplus \cdots \oplus \mathcal{O}_{N_0(\zeta_p)}}_{r \text{ termes}}\big),$$

donc u s'écrit $(u_0, u_1, \ldots, u_r)$, avec $u_0 \in \mathcal{O}_{N_0}^* \simeq \mu_{q-1} \times (1 + p\mathcal{O}_{N_0})$ et $u_i \in \mathcal{O}_{N_0(\zeta_p)}^* \simeq \mu_{q-1} \times (1 + \pi\mathcal{O}_{N_0(\zeta_p)})$ pour $1 \leq i \leq r$, où π est une uniformisante de $N_0(\zeta_p)$.

Lemme 2.10. *On a* $u^{(q-1)p^{m-1}} \in \mathcal{O}_{N_0}[\Gamma_0]^*$.

Preuve. Le théorème de Jacobinski [9, 27.8] décrit le conducteur $\mathcal{F}$ de $\mathcal{M}_0$ dans $\mathcal{O}_{N_0}[\Gamma_0]$. Le calcul donne la décomposition :

$$\mathcal{F} = p^m \mathcal{O}_{N_0} \oplus \big(p^m \pi^{1-p} \mathcal{O}_{N_0(\zeta_p)} \oplus \cdots \oplus p^m \pi^{1-p} \mathcal{O}_{N_0(\zeta_p)}\big) \ .$$

Soit $x = (x_0, x_1, \ldots, x_r) = u^{q-1}$. Alors $x_0 = 1 + pa_0$ avec $a_0 \in \mathcal{O}_{N_0}$ et $x_i = 1 + \pi a_i$ avec $a_i \in \mathcal{O}_{N_0(\zeta_p)}$ pour $1 \leq i \leq r$. De plus,

$$x_0{}^{p^{m-1}} = 1 + \sum_{k=1}^{p^{m-1}} \binom{p^{m-1}}{k} (pa_0)^k \,, \qquad x_i{}^{p^{m-1}} = 1 + \sum_{k=1}^{p^{m-1}} \binom{p^{m-1}}{k} (\pi a_i)^k$$

et, en notant v_p la valuation p-adique :

$$v_p\left(\binom{p^{m-1}}{k}\right) = v_p\Big(\frac{p^{m-1}}{k}\Big) = m - 1 - v_p(k) \ ,$$

si bien que $x_0{}^{p^{m-1}} \equiv 1 \bmod p^m \mathcal{O}_{N_0}$ et $x_i{}^{p^{m-1}} \equiv 1 \bmod \pi^{(p-1)(m-1)} \mathcal{O}_{N_0(\zeta_p)}$, c'est-à-dire $x^{p^{m-1}} - 1 \in \mathcal{F}$. A fortiori, $x^{p^{m-1}} - 1$ et $x^{p^{m-1}} = u^{(q-1)p^{m-1}}$ appartiennent à $\mathcal{O}_{N_0}[\Gamma_0]$. Il ne reste qu'à noter que

$$\mathcal{M}_0{}^* \cap \mathcal{O}_{N_0}[\Gamma_0] = \mathcal{O}_{N_0}[\Gamma_0]^*$$

pour achever la démonstration du lemme. $\square$

Comme $k_p{}^p = \mathrm{Det}(u)$ et $e = p^m$, on déduit du lemme précédent que $k_p{}^{(q-1)e} \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma_0]^*)$. On termine la preuve de la proposition 2.7 grâce à (5). $\square$

On est maintenant en mesure de terminer la preuve du théorème 1. On déduit de la proposition 2.7 que
$$j_p^*(f_{(p),p}{m_p}^{-1})^{(q-1)e} \in \mathrm{Det}(\mathcal{O}_{N_0}[G]^*) \ .$$
On voit alors à l'aide du lemme 2.4 et de la proposition 2.5 qu'il existe une extension non ramifiée $B_p/\mathbb{Q}_p$ telle que $j_p^*(f_p{m_p}^{-1})^{(q-1)e} \in \mathrm{Det}(\mathcal{O}_{B_p}[G]^*)$. Le théorème des points fixes [23, théorème 6] entraîne :
$$j_p^*(f_p{m_p}^{-1})^{(q-1)e} \in \mathrm{Det}(\mathbb{Z}_p[G]^*)$$
c'est-à-dire $(\mathcal{A})^{(q-1)e} = 1$. Mais on sait par [13, théorème 2] que $(\mathcal{A})$ appartient au groupe noyau $D(\mathbb{Z}[G])$ et, comme G est un p-groupe, $D(\mathbb{Z}[G])$ en est un aussi [9, 50.18]. Il s'ensuit que $(\mathcal{A})^e = 1$, ce qui est le résultat annoncé.

2.3. Un commentaire. La preuve du théorème 1 laisse entrevoir la possibilité d'une amélioration du résultat. En effet, on montre (lemme 2.9) que la fonction de caractères à étudier vérifie :
$$(k_p)^p \in \mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0,p}, \mathcal{O}_{E_p}^*) \ .$$
On aimerait pouvoir en déduire que $(k_p)^p \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma_0]^*)$. On obtiendrait alors que l'ordre de $(\mathcal{A})$ est 1 ou p. Mais comme Γ_0 est un p-groupe, on ne peut pas appliquer le raisonnement tenu pour montrer la proposition 2.3 (il sert aussi pour montrer le théorème 31 de [16] évoqué plus haut). Dans la preuve du théorème 2.1, le même type de problème est réglé grâce à la description exhaustive des extensions abéliennes faiblement et sauvagement ramifiées de $\mathbb{Q}_p$ (à l'aide de la version locale de la théorie de Kronecker-Weber), qui permet de ramener le calcul de la résolvante à un cas où il est entièrement explicite.

On aimerait avoir une aussi bonne description des extensions abéliennes faiblement et sauvagement ramifiées de N_0, afin de rendre possible une estimation précise de la résolvante qui définit la fonction k_p. Une façon de l'obtenir pourrait être via les corps de division associés à des groupes formels de Lubin-Tate. Une partie du travail dans ce sens est faite par Byott dans [5], où il étudie la structure galoisienne de l'anneau d'entiers des extensions d'un corps p-adique K contenues dans le deuxième corps de division $K^{(2)}$, traitant en particulier le cas des extensions abéliennes totalement et faiblement ramifiées de K.

3. Le réseau associé

On se penche maintenant sur le deuxième problème évoqué dans l'introduction, celui de la structure du G-réseau entier unimodulaire obtenu en munissant la racine carrée de la codifférente de la forme trace. On commence par faire le point des principaux résultats connus ; puis on montre comment construire des exemples intéressants d'extensions qui ne vérifient pas leurs hypothèses ; enfin, on présente le calcul et les exemples qui prouvent le théorème 2, ainsi que de nouvelles pistes ouvertes par ces calculs.

3.1. Les résultats théoriques. Une présentation très complète des résultats concernant la racine carrée de la codifférente (au début des années 1990) peut être consultée dans [12]. Nous en extrayons ceux qui suivent. Dans sa thèse [11], Erez traite entièrement (du point de vue adopté dans cet article) le cas abélien absolu.

Théorème 3.1 (Erez). *Soit $N/\mathbb{Q}$ une extension galoisienne de groupe G d'ordre impair. Si $N/\mathbb{Q}$ est abélienne, les assertions suivantes sont équivalentes :*

(i) *$N/\mathbb{Q}$ est faiblement ramifiée,*

(ii) *$\mathcal{A}$ est isomorphe à $\mathbb{Z}[G]$,*

(iii) *le réseau associé à $\mathcal{A}$ est G-isométrique au réseau standard $\mathbb{Z}[G]$.*

Pour ce qui est du cas non faiblement ramifié, des résultats sur le réseau associé à $\mathcal{A}$ ont aussi été obtenus ([3] est l'aboutissement de travaux de Bachoc auxquels Erez a pris part).

On a rappelé au début de la partie 2 que Erez avait établi l'existence d'une base normale pour $\mathcal{A}$ dans le cas modéré. Le résultat suivant sur la structure du réseau associé dans le cas modéré est venu peu après.

Théorème 3.2 (Erez-Taylor). *Si $N/\mathbb{Q}$ est modérée, alors le réseau associé à $\mathcal{A}$ est stablement G-isométrique au réseau standard $\mathbb{Z}[G]$.*

Précisons que deux réseaux sont dits *stablement G-isométriques* s'ils deviennent G-isométriques après ajout à chacun d'un même réseau hyperbolique (on verra plus loin qu'il n'y a pas toujours simplification). Le résultat présenté dans [14] est valable pour une extension relative galoisienne de corps de nombres N/K : $\mathcal{A}_{N/K}$ et $\mathcal{O}_K[G]$, munis des formes hermitiennes adéquates (construites à partir de la trace de N à K pour $\mathcal{A}_{N/K}$ et à partir de l'inversion dans G pour $\mathcal{O}_K[G]$), définissent la même classe dans le groupe de Grothendieck de $\mathbb{Z}[G]$-modules hermitiens.

Ces deux théorèmes laissent place à l'expérimentation puisqu'ils ne traitent pas le cas non modéré, non abélien. La première étape est de construire des exemples intéressants d'extensions, c'est l'objet du prochain paragraphe.

3.2. Une famille infinie d'extensions faiblement ramifiées. On voudrait faire ici l'ébauche de la construction d'une famille infinie d'extensions de $\mathbb{Q}$ faiblement et sauvagement ramifiées, non abéliennes, de degré impair, qui est décrite en détail dans [26]. Le premier point est de construire des extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois donné. Il s'agit d'un problème de théorie de Galois inverse explicite et on utilise pour cela une méthode élémentaire mise au point par Eichenlaub [10]. On choisit arbitrairement de réaliser le produit semi-direct $C_9 \rtimes C_3$ (des considérations de faisabilité des calculs par ordinateur interviennent dans ce choix).

La construction d'Eichenlaub d'une famille infinie d'extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois $C_9 \rtimes C_3$ est décrite par le diagramme suivant :

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_9, \sqrt[9]{\alpha}) \arrow[dl, dash, "2"] \arrow[dd, dash, "9"] \\
N \arrow[ddd, dash, "27"'] & \\
& \mathbb{Q}(\zeta_9) \arrow[d, dash, "3"] \\
& \mathbb{Q}(j) \ni \alpha(t) \\
\mathbb{Q} \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

où ζ_9 est une racine primitive 9-ième de l'unité, $j = {\zeta_9}^3$, t est un paramètre et $\alpha = \alpha(t) \in \mathbb{Q}(j)[t]$ est choisi de sorte que, pour une infinité de spécialisations de t en des valeurs entières, l'extension $\mathbb{Q}(\zeta_9, \sqrt[9]{\alpha})/\mathbb{Q}$ soit galoisienne de groupe de Galois isomorphe à un produit semi-direct $C_9 \rtimes C_6$ ne contenant qu'un 2-Sylow. Celui-ci est alors distingué et la sous-extension $N/\mathbb{Q}$ qu'il fixe a les propriétés voulues.

On peut déterminer un polynôme paramétré dont N est le corps de décomposition (pour les bonnes valeurs de t). On pose $w = t^2 - t + 1$, il s'agit de :

$$\begin{aligned} P_t(x) = \ & x^9 - 9wx^7 + 27w^2x^5 - 30w^3x^3 + 9w^4x \\ & -(2t-1)(t^6 - 3t^5 - 12t^4 + 29t^3 - 3t^2 - 12t + 1)w \ . \end{aligned}$$

Le calcul de la ramification en 3 dans les extensions N pour un grand nombre de valeurs de t semble indiquer que $N/\mathbb{Q}$ est faiblement ramifiée quand t est congru à 5 modulo 9. Dans [26], on montre que cela est bien le cas. Le point essentiel est de pouvoir déterminer la ramification dans l'extension kummérienne $\mathbb{Q}(\zeta_9, \sqrt[9]{\alpha})/\mathbb{Q}(\zeta_9)$ en fonction de t (c'est-à-dire sans le spécialiser en des valeurs entières). Cela est possible grâce à des critères de ramification dans les extensions kummériennes dus à Hecke (extensions de degré premier, [18]) et à Greither (extensions de degré une puissance d'un premier, [17]). On obtient de plus des renseignements sur la décomposition de 3 dans l'extension en fonction de la congruence de t modulo 27 (en particulier, on trouve des exemples d'extensions vérifiant les hypothèses du théorème 2.1).

C'est le calcul du réseau associé à $\mathcal{A}$ sur ces exemples (ainsi que d'autres) qui permet de montrer le théorème 2.

3.3. Preuve du théorème 2. La preuve du théorème 2 est numérique et passe par un calcul sur ordinateur à l'aide du logiciel PARI [4] (dont les sources sont publiques). Voici un algorithme qui permet de calculer le minimum et le nombre de vecteurs minimaux du réseau entier unimodulaire associé à la racine carrée de la codifférente d'une extension galoisienne N de $\mathbb{Q}$, où N est donné comme corps de rupture d'un polynôme P. Il a été conçu avec l'aide de Bachoc et mis au format PARI avec l'aide d'Allombert. On peut se reporter à [8] pour les notions sous-jacentes aux fonctions utilisées. On donne ensuite des exemples de polynômes pour lesquels ce calcul valide les assertions du théorème 2.

```
N=nfinit(P);                                  (trouve une Z-base de O_N sur Z[θ], où θ est une racine de P)
diff=idealfactor(N,N.diff);                   (factorisation de la différente en idéaux premiers)
for(i=1,length(diff[,2]),diff[i,2]\=-2);      (calcul de la racine carrée A)
rcc=factorback(diff,N);                       (donne une Z-base de A sur la base de O_N trouvée plus haut)
gram=N[5][4];                                 (matrice de Gram pour la forme trace sur la base de O_N)
grcc=rcc~*gram*rcc;                           (le réseau associé à A)
matdet(grcc)                                  (pour vérifier que le réseau obtenu est unimodulaire !)
qfminim(grcc,0,0)                             (donne le minimum et le nombre de vecteurs minimaux du réseau)
```

Le réseau standard $\mathbb{Z}[G]$ a $|G|$ vecteurs de longueur égale à 1 puisque la forme bilinéaire symétrique q_G qui le définit vérifie $q_G(g,g) = 1$ pour tout $g \in G$, si bien que $\mathbb{Z}[G]$ est isométrique à $\mathbb{Z}^{|G|}$. Il suffit donc pour prouver le théorème 2 de trouver des polynômes P définissant des extensions de $\mathbb{Q}$ qui vérifient les propriétés requises dans le théorème et pour lesquels l'algorithme ci-dessus donne des vecteurs minimaux de longueur supérieure ou égale à 2 (la longueur d'un vecteur $x \in \mathcal{A}$ est donnée par $\mathrm{tr}_{N/\mathbb{Q}}(x^2)$). Si cela est réalisé, le réseau associé à $\mathcal{A}$ ne peut pas être isométrique à $\mathbb{Z}^{|G|}$, donc à fortiori il ne peut pas être G-isométrique à $\mathbb{Z}[G]$.

1er exemple : prenons $t = 5$ dans le polynôme P_t défini dans le paragraphe précédent et appliquons la fonction `polredabs` de PARI, on trouve le polynôme :

$$x^9 - 21x^7 - 7x^6 + 126x^5 + 105x^4 - 189x^3 - 252x^2 - 63x + 7$$

que l'on note `p5`. Soit N son corps de décomposition. La suite d'instructions :

```
nf5=nfinit(subst(p5,x,y)); nffactor(nf5,p5);
    rnfequation(nf5,%[5,1]); polredabs(%)
```

donne un polynôme P de degré 27 dont N est le corps de rupture. On vérifie que le groupe de Galois de $N/\mathbb{Q}$ est isomorphe à $C_9 \rtimes C_3$ (par exemple à l'aide de la fonction `galoisinit` de PARI) ; on sait alors par le théorème 2 de [26] que $N/\mathbb{Q}$ est faiblement ramifiée (de plus, la seule place sauvage 3 n'est pas décomposée dans N). On applique donc à P l'algorithme ci-dessus. On obtient que le réseau associé à $\mathcal{A}$ est unimodulaire (de dimension 27), de minimum 3 et contient 2664 vecteurs minimaux.

On retrouve ce réseau dans la classification de [2] : il s'agit de celui à 3317760 automorphismes. On peut d'ailleurs montrer [26, théorème 5.2] que celui-ci est le seul des 3 réseaux entiers unimodulaires de dimension 27 sans racines pouvant se réaliser comme réseau associé à la racine carrée de la codifférente d'une extension faiblement ramifiée de $\mathbb{Q}$ (les *racines* d'un réseau entier sont les vecteurs de longueur 1 ou 2).

2ème exemple : comme on l'a fait remarquer, on sait que 3 ne se décompose pas dans l'extension de l'exemple précédent, donc elle ne vérifie pas l'hypothèse du théorème 2.1 et la théorie ne dit pas si $\mathcal{A}$ est ou non isomorphe à $\mathbb{Z}[G]$ en tant que $\mathbb{Z}[G]$-module. L'objet du deuxième exemple est de fournir une extension vérifiant les hypothèses du théorème 2.1 et pour laquelle il n'y a pas isométrie avec le réseau standard. Il provient d'une famille régulière d'extensions de $\mathbb{Q}$ à groupe de Galois isomorphe à $C_9 \rtimes C_3$, qui a été fournie à l'auteur par Eichenlaub. On considère le polynôme :

$$x^9 - 2359x^7 - 14154x^6 + 1585248x^5 + 12946192x^4 - 336865200x^3 \\ -2851861152x^2 + 8004445568x - 1707840512 \ .$$

On vérifie comme ci-dessus que le groupe de Galois du corps de décomposition N de ce polynôme est isomorphe à $C_9 \rtimes C_3$, que $N/\mathbb{Q}$ est faiblement ramifiée, que 3 s'y décompose (donc le groupe de décomposition en 3, d'ordre 3 ou 9, est abélien) et que le réseau associé à $\mathcal{A}$ est de minimum 2, à 216 vecteurs minimaux (et 3960 vecteurs de norme 3).

On a ainsi un exemple d'extension pour laquelle il y a isomorphisme de $\mathbb{Z}[G]$-modules entre $\mathcal{A}$ et $\mathbb{Z}[G]$, mais pas isométrie entre les réseaux associés. Le théorème 3.1 assure que ce phénomène ne peut pas se produire dans le cas où l'extension est abélienne absolue.

3ème exemple : on veut maintenant un exemple d'extension modérée pour laquelle le réseau associé à la racine carrée de la codifférente ne soit pas isométrique au réseau standard. On présente dans [24] une méthode similaire à celle du paragraphe 3.2 pour construire une infinité d'extensions modérées de $\mathbb{Q}$ de groupe de Galois isomorphe à $C_7 \rtimes C_3$. On en extrait l'exemple suivant. Considérons le polynôme :

$$x^7 - 3x^6 - 327x^5 + 785x^4 + 7935x^3 - 12297x^2 - 21293x + 12411 \ .$$

On vérifie que le groupe de Galois du corps de décomposition N de ce polynôme est isomorphe à $C_7 \rtimes C_3$, que $N/\mathbb{Q}$ est modérément ramifié (de discriminant $2^{18}7^{14}193^{18}$) et que le réseau associé à $\mathcal{A}$ est le seul réseau unimodulaire de rang 21, de minimum 2, à 84 vecteurs minimaux.

Dans cette situation, on sait par le théorème 3.2 que le réseau associé à $\mathcal{A}$ est stablement G-isométrique au réseau standard et on voit qu'il n'y a pas simplification.

Cet exemple clôt la démonstration du théorème 2.

3.4. Nouvelles pistes. Contrairement à ce qu'on pourrait penser à la lecture du paragraphe précédent, les calculs numériques n'apportent pas que des réponses "négatives". Ils peuvent aussi conforter des présomptions, indiquer la piste à suivre et éventuellement ils font apparaître des phénomènes insoupçonnés.

Ainsi, dans tous les exemples testés pour lesquels $\mathcal{A}$ n'est pas isométrique à $\mathbb{Z}[G]$, on a pu appliquer un nouvel algorithme de calcul explicite des automorphismes du groupe de Galois d'un corps de nombres (présenté dans [1]), qui a toujours permis de trouver une base normale pour la racine carrée de la codifférente. Ces calculs motivent la conjecture présentée dans l'introduction et incitent à tenter d'améliorer les résultats théoriques existants.

Si on veut généraliser le théorème 3.2, on pourrait être tenté de rester dans le cas de la ramification modérée et de travailler pour ôter l'adverbe "stablement" de l'énoncé. Le troisième exemple du paragraphe précédent montre que cet espoir est vain et qu'il faut plutôt essayer d'élargir le résultat (avec l'adverbe "stablement") aux extensions faiblement ramifiées (du moins celles pour lesquelles on sait que $\mathcal{A}$ admet une base normale).

Enfin, les calculs sur un grand nombre d'extensions faiblement ramifiées de $\mathbb{Q}$ de groupe de Galois isomorphe à $C_9 \rtimes C_3$, notamment dans une nouvelle famille construite avec Allombert, font apparaître le lien suivant :

$$\begin{aligned} &3 \text{ non décomposé } \leftrightarrow (\text{minimum du réseau associé à } \mathcal{A}) = 3,\\ &3 \text{ décomposé } \leftrightarrow (\text{minimum du réseau associé à } \mathcal{A}) \in \{1, 2\}. \end{aligned}$$

Notons que les réseaux de minimum supérieur ou égal à 3 sont sans racines, tandis que ceux de minimum 1 ou 2 sont avec racines. De plus, dans les extensions considérées, 3 est la seule place sauvage et elle se décompose si et seulement si le groupe de décomposition en 3 est abélien. Faut-il en conclure qu'il y a un lien entre l'hypothèse technique du théorème 2.1 et le fait que le réseau associé à $\mathcal{A}$ ait des racines ?

Bibliographie

[1] B. Allombert, *An efficient algorithm for the computation of Galois automorphisms*, to appear in Math. Comp.

[2] R. Bacher, B. Venkov, *Réseaux entiers unimodulaires sans racines en dimensions 27 et 28*. Réseaux euclidiens, designs sphériques et formes modulaires, 212–267, Monogr. Enseign. Math., **37**, *Enseignement Math., Genève*, 2001.

[3] C. Bachoc, *Sur la structure hermitienne de la racine carrée de la codifférente*. Ann. Inst. Fourier (Grenoble) **43** (1993), *no. 3*, 619–654.

[4] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *Users's guide to PARI-GP*. Université Bordeaux 1, 2000 ;
téléchargeable `ftp ://megrez.math.u-bordeaux.fr/pub/pari`.

[5] N. P. Byott, *Integral Galois module structure of some Lubin-Tate extensions.* J. Number Theory, **77** (1999), *no. 2*, 252–273.

[6] Ph. Cassou-Noguès, M. J. Taylor, *Opérations d'Adams et groupes de classes d'algèbres de groupes. J. Algebra* **95** (1985), 125–152.

[7] ———, *Galois module structure for wild extensions*, in Algebraic number theory and diophantine analysis, Proc. Conf. Graz 1998, 69–91, ed. Halter-Koch F. and Tichy R.F., de Gruyter, New York, 2000.

[8] H. Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1993.

[9] C. W. Curtis, I. Reiner, *Methods of representation theory, Vol. I & II.* Wiley, New York, 1990.

[10] Y. Eichenlaub, *Problèmes effectifs de théorie de Galois en degrés 8 à 11.* Thèse de Doctorat, Université Bordeaux 1, 1996.

[11] B. Erez, *Structure galoisienne et forme trace dans les corps de nombres.* Thèse de Doctorat, Université de Genève, 1987.

[12] ———, *A survey of recent work on the square root of the inverse different.* Journées arithmétiques, Exp. Congr. Luminy (1989), *Astérisque*, **198-200**, 133–152.

[13] ———, *The Galois structure of the square root of the inverse different. Math. Z.* **208** (1991), 239–255.

[14] B. Erez, M. J. Taylor, *Hermitian modules in Galois extensions of number fields and Adams operations.* Ann. of Math. **135** (1992), 271–296.

[15] J.-M. Fontaine, *Sur la décomposition des algèbres de groupes.* Ann. Sc. E.N.S. (4) **4** (1971), 121–180.

[16] A. Fröhlich, *Galois module structure of algebraic integers.* Ergebnisse der Mathematik, 3. Folge, Bd. 1, Springer, Berlin, 1983.

[17] C. Greither, *Unramified Kummer extensions of prime power degree.* Manuscripta Math. **64** (1989), 261–290.

[18] E. Hecke, *Lectures on the theory of algebraic numbers.* Graduate texts in Math. **77**, Springer-Verlag, New York-Berlin, 1981.

[19] J. Martinet, *Character theory and Artin L-functions*, in Algebraic number fields (L-functions and Galois properties), ed. Fröhlich A., Acad. Press, London, 1977, 1–87.

[20] J.-P. Serre, *Corps locaux*, 3e édition. Hermann, Paris, 1968.

[21] ———, *Représentations linéaires des groupes finis*, 3e édition. Hermann, Paris, 1978.

[22] J. T. Tate, *Local constants*, in Algebraic number fields (L-functions and Galois properties), 89–131, ed. Fröhlich A., Acad. Press, London, 1977.

[23] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions.* Invent. Math. **63** (1981), 41–79.

[24] S. Vinatier, *Arithmétique des extensions faiblement ramifiées.* Thèse de Doctorat, Université Bordeaux 1, 2000. `http://www.math.u-bordeaux.fr/~vinatier`.

[25] ———, *Structure galoisienne dans les extensions faiblement ramifiées de $\mathbb{Q}$.* J. Number Theory **91** (2001), 126–152.

[26] ———, *Une famille infinie d'extensions faiblement ramifiées.* Math. Nachr. **243** (2002), 165–187.

Stéphane Vinatier
Laboratoire A2X
Université Bordeaux 1
351, cours de la Libération
F-33405 Talence cedex
France
E-mail : `vinatier@math.u-bordeaux.fr`