ANNALES DE L'INSTITUT FOURIER

CHRISTINE BACHOC

Sur la structure hermitienne de la racine carrée de la codifférente

Annales de l'institut Fourier, tome 43, n° 3 (1993), p. 619-654

<http://www.numdam.org/item?id=AIF_1993__43_3_619_0>

Ann. Inst. Fourier, Grenoble
43, 3 (1993), 619-654

SUR LA STRUCTURE HERMITIENNE DE LA RACINE CARRÉE DE LA CODIFFÉRENTE

par Christine BACHOC

Introduction.

Un corps de nombres K est naturellement muni d'une forme quadratique sur $\mathbb{Q}$ non dégénérée qui est la forme $x \mapsto \mathrm{Trace}_{K/\mathbb{Q}}(x^2)$. On sait qu'il existe au plus un idéal fractionnaire unimodulaire pour cette forme; s'il existe, il est noté $\mathcal{A}_K$ et est caractérisé par la relation : $\mathcal{A}_K^2 = \mathcal{D}_K^{-1}$. Celle-ci justifie son appellation de "racine carrée de la codifférente" (voir [E1], [E2], [BE]).

Lorsque K est galoisien sur $\mathbb{Q}$ et de degré impair, l'existence de cet idéal est assurée; de plus la relation précédente montre qu'il est stable sous l'action du groupe de Galois G du corps. Le couple formé par l'idéal $\mathcal{A}_K$ et la forme $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$ est alors un $\mathbb{Z}[G]$-module hermitien (le groupe G est un groupe d'automorphismes de la forme quadratique $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$). On dit que deux $\mathbb{Z}[G]$-modules hermitiens sont $\mathbb{Z}[G]$-isométriques s'il existe entre eux un isomorphisme de $\mathbb{Z}[G]$-modules qui soit aussi une isométrie des formes quadratiques.

Le but de cet article est de décrire un représentant de la classe de $\mathbb{Z}[G]$-isométrie de l'idéal $\mathcal{A}_K$, dans le cas où le groupe G est abélien et de degré impair. Dans ce cas, le corps K est totalement réel, donc la forme quadratique $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$ est définie positive. On parle alors de $\mathbb{Z}[G]$-réseau plutôt que de $\mathbb{Z}[G]$-module hermitien.

L'étude de cet idéal a débuté dans la thèse de Boas Erez ([E1]). Celui-ci a caractérisé les extensions abéliennes K de $\mathbb{Q}$ pour lesquelles

Mots-clés : Corps de nombres – Forme trace – Réseau.
Classification A.M.S. : 11R33.

$(\mathcal{A}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ est $\mathbb{Z}[G]$-isométrique à l'anneau de groupe $\mathbb{Z}[G]$ muni de la forme usuelle $\sum \lambda_g g \mapsto \sum \lambda_g^2$; ce sont les extensions peu ramifiées, c'est-à-dire pour lesquelles le deuxième groupe de ramification est nul en tout nombre premier.

Ensuite, dans [BE] et [B] des extensions avec ramification sauvage sont considérées. Plus précisément, ces deux articles couvrent le cas où, pour tout nombre premier p, le groupe d'inertie en p est soit d'ordre premier à p, soit un p-groupe. On y donne une description du $\mathbb{Z}[G]$-réseau $(\mathcal{A}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ et on montre en particulier que sa classe de $\mathbb{Z}[G]$-isométrie ne dépend que de la ramification dans K.

Un point commun à ces résultats est que, dans ces cas, l'idéal $\mathcal{A}_K$ est libre sur son ordre associé. Or, dans [Bu], David Burns montre que ce n'est pas un fait général, contrairement à l'anneau des entiers de K dont il est bien connu qu'il est libre sur son ordre associé (théorème de Leopoldt). Un calcul d'indices lui permet de donner explicitement la classe sur l'ordre maximal $\mathfrak{M}$ de l'algèbre $\mathbb{Q}[G]$ de $\mathfrak{M}\mathcal{A}_K$. Celle-ci n'est pas toujours triviale ; le plus petit corps K pour lequel cela arrive est de degré 39 sur $\mathbb{Q}$, en supposant le nombre premier 13 totalement ramifié dans K.

Expliquons pourquoi la situation où l'idéal $\mathcal{A}_K$ est libre sur son ordre associé est la plus simple : supposons que $\mathcal{A}_K = \Lambda.x = \{\lambda(x), \lambda \in \Lambda\}$. Alors, le lemme suivant montre qu'il suffit de connaître pour tout caractère χ de G la valeur de $(x|\chi)\overline{(x|\chi)}$ pour obtenir un représentant de la classe de $\mathbb{Z}[G]$-isométrie de $\mathcal{A}_K$:

LEMME 1.1. — *Soit K un corps de nombres galoisien sur $\mathbb{Q}$ de groupe de Galois G et soit x appartenant à K tel que $K = \mathbb{Q}[G].x$. Alors l'isomorphisme de $\mathbb{Q}[G]$-modules :*

$$\begin{aligned} \mathbb{Q}[G] &\to K \\ \lambda &\mapsto \lambda(x) \end{aligned}$$

est une isométrie lorsque K est muni de la forme $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$ *et $\mathbb{Q}[G]$ de la forme $T_1(s\lambda\overline{\lambda})$ avec*

$$s = \sum_{\chi \in \hat{G}} (x|\chi)\overline{(x|\chi)} e_\chi,$$

où

$$(t|\chi) = \sum_{g \in G} \chi(g^{-1}) g(t)$$

est la résolvante de t en χ et T_1 est la forme linéaire sur $\mathbb{Q}[G]$ définie par :

$$T_1\Big(\sum_{g\in G}\lambda_g g\Big) = \lambda_1.$$

Démonstration. — Il suffit de montrer, pour tout g, g' appartenant à G, l'égalité suivante : $\mathrm{Trace}_{K/\mathbb{Q}}(g(x)g'(x)) = T_1(sgg'^{-1})$. Or c'est une conséquence de :

$$s = \sum_{\chi\in\hat{G}}(x|\chi)\overline{(x|\chi)}e_\chi = \sum_{g\in G}\mathrm{Trace}_{K/\mathbb{Q}}(g(x)x)g$$

qui se vérifie aisément. □

Par ce lemme, on obtient alors la $\mathbb{Z}[G]$-isométrie :

$$(\mathcal{A}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2)) \sim_{\mathbb{Z}[G]} (\Lambda, T_1(s\lambda\overline{\lambda}))$$

avec

$$s = \sum_{\chi\in\hat{G}}(x|\chi)\overline{(x|\chi)}e_\chi.$$

C'est en fait la méthode adoptée dans [BE] et [B]. Ce lemme montre aussi que le théorème de Leopoldt contient assez d'informations pour déterminer la classe de $\mathbb{Z}[G]$-isométrie de l'anneau des entiers de K (voir le corollaire 1.4).

Dans le cas général, afin de contourner cette difficulté, nous procédons de la façon suivante : on définit d'abord un idéal I_K contenu dans $\mathcal{A}_K$, et assez "proche" de celui-ci (par exemple, si un seul nombre premier est "très sauvage" dans K, c'est-à-dire si un seul nombre premier n'est ni modéré, ni peu ramifié dans K, alors $\mathcal{I}_K$ est à peu de choses près le système de racines de $\mathcal{A}_K$; voir Exemples 1.9). L'objet du paragraphe 1 est de décrire le réseau $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$.

Le réseau dual $\mathcal{I}_K^* = \mathcal{I}_K^{-1}\mathcal{D}_K^{-1}$ a la propriété d'être, en tant que $\mathbb{Z}[G]$-module, libre sur son ordre associé Λ_K. La description de Λ_K, et la donnée d'un générateur explicite de $\mathcal{I}_K^*$ sur Λ_K suffit donc à déterminer sa classe de $\mathbb{Z}[G]$-isométrie (théorème 1.7). Celle-ci ne dépend que de la ramification dans K.

Pour cela, nous appliquons conjointement le théorème de Leopoldt ([L]) et le théorème 2 de [E2] à un idéal $\mathcal{J}_L$ d'une extension L de K, dont la trace sur K est égale à $\mathcal{I}_K^*$ (paragraphe 1.4).

Une fois déterminée la classe de $\mathbb{Z}[G]$-isométrie du sous-réseau $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ de la racine carrée de la codifférente, on procède de la façon suivante : parmi les réseaux L tels que $\mathcal{I}_K \subset L \subset \mathcal{I}_K^*$, $\mathcal{A}_K$ est déterminé par un "métaboliseur" M du quotient $T(\mathcal{I}_K) = \mathcal{I}_K^*/\mathcal{I}_K$ (c'est-à-dire un sous-groupe de $T(\mathcal{I}_K)$ égal à son orthogonal pour la forme induite, voir le paragraphe 2.1).

La classe de $\mathbb{Z}[G]$-isométrie de $\mathcal{A}_K$ modulo les $\mathbb{Z}[G]$-isométries stabilisant $\mathcal{I}_K$ ne dépend que de l'orbite de M sous l'action des $\mathbb{Z}[G]$-isométries de $\mathcal{I}_K$. Celle-ci est déterminée au théorème 4.1.

Le schéma de la démonstration est le suivant : le quotient $T(\mathcal{I}_K)$ est étudié au paragraphe 2.2. On se ramène à la situation locale. Si F est un localisé de K, un élément de l'orbite du métaboliseur correspondant à $\mathcal{A}_F$ sous le groupe des $\mathbb{Z}_p[D]$-isométries de $\mathcal{I}_F$ est déterminé au théorème 3.4. Dans la démonstration de ce théorème intervient de façon essentielle un calcul d'indices tout à fait analogue à celui de D. Burns dans [Bu]. Ensuite, on globalise les résultats locaux dans le paragraphe 4.

Le paragraphe 5 est consacré à la comparaison des $\mathbb{Z}[G]$-réseaux $(\mathcal{A}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ lorsque K décrit les extensions abéliennes de $\mathbb{Q}$ de degré impair.

Parmi les résultats antérieurs sur la structure de $\mathbb{Z}[G]$-réseau de la racine carrée de la codifférente, nous utilisons ici seulement le théorème 2 de [E2] relatif au cas d'une extension cyclique d'ordre p de $\mathbb{Q}$.

Les définitions suivantes seront utilisées dans toute la suite : soit R un anneau principal ou un corps (on aura $R = \mathbb{Z}, \mathbb{Q}, \mathbb{Z}_p, \mathbb{Q}_p, \mathbb{F}_p$) et soit k son corps des fractions. Soit G un groupe ; un $R[G]$-module hermitien V est un $R[G]$-module, tel que $k \otimes V$ soit muni d'une forme bilinéaire symétrique non dégénérée $b(x, y)$ telle que le groupe G laisse b invariante, c'est-à-dire : pour tout $x, y \in V$ et pour tout $g \in G$, $b(g(x), g(y)) = b(x, y)$. Par exemple, V peut être un sous-$R[G]$ module de $k[G]$. Les formes G-invariantes sur $k[G]$ sont du type $\lambda \to T_1(s\lambda\overline{\lambda})$ où T_1 est la forme linéaire $T_1(\sum \lambda_g g) = \lambda_1$, $\lambda \mapsto \overline{\lambda}$ l'application linéaire déduite de l'application de G dans G qui à un élément associe son inverse, et s un élément de $k[G]$ vérifiant $\overline{s} = s$. En particulier, $T_1(\lambda\overline{\lambda}) = \sum_{g \in G} \lambda_g^2$ est la forme usuelle sur $k[G]$.

On dit que deux $R[G]$-modules hermitiens sont $R[G]$-isométriques s'il existe entre eux un isomorphisme de $R[G]$-modules qui soit aussi une isométrie des formes bilinéaires (et on note $V \sim_{R[G]} V'$).

Enfin, si $R = \mathbb{Z}$ ou bien $\mathbb{Z}_p$, le dual du réseau V est $V^* = \{x \in k \otimes V | b(x, V) \subset R\}$; c'est encore un $R[G]$-réseau. On dit que V est entier si $V \subset V^*$, et dans ce cas, l'indice $[V^* : V]$ est le discriminant de V. On dit que V est unimodulaire si $V = V^*$.

Remerciements. — L'auteur remercie David Burns pour de profitables discussions avec lui. Les résultats de son article [Bu] m'ont été fort utiles pour l'établissement du théorème 3.1.

1. Le $\mathbb{Z}[G]$-réseau $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$.

Dans ce paragraphe, on définit l'idéal $\mathcal{I}_K$ contenu dans $\mathcal{A}_K$ et on détermine sa classe de $\mathbb{Z}[G]$-isométrie (théorème 1.7). En particulier, son réseau de racines, c'est-à-dire le sous-réseau engendré par ses éléments de longueur 1 et 2 (la longueur d'un élément est la valeur prise par la forme quadratique $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$ sur celui-ci), est déterminé à la proposition 1.8.

1.1. Notations et définition de $\mathcal{I}_K$.

Le corps K est toujours galoisien de groupe de Galois G sur $\mathbb{Q}$ et de degré impair. L'ensemble $\mathbb{P}$ des nombres premiers ramifiés dans K est la réunion disjointe des ensembles $\mathbb{P}_m$, $\mathbb{P}_{pr}$, $\mathbb{P}_s$ qui sont respectivement l'ensemble des nombres premiers modérés, peu ramifiés mais non modérés, et ramifiés mais non peu ramifiés dans K. Pour un nombre premier p, on note son degré de ramification $e_{K/\mathbb{Q}}(p) = r_p p^{m_p}$ avec r_p premier à p ; rappelons qu'alors r_p divise $p-1$, et que le groupe d'inertie en p est cyclique. On désigne par $\phi_K(p)$ le produit des idéaux de K au-dessus de p. On aura besoin de distinguer dans l'ensemble $\mathbb{P}_s$ les sous-ensembles $\mathbb{P}_{s,0}$ et $\mathbb{P}_{s,1}$ qui sont respectivement l'ensemble des nombres premiers p appartenant à $\mathbb{P}_s$ tels que m_p soit congru à 0 et 1 modulo 2. Soit f le conducteur de K. Alors $f = \prod_{p \in \mathbb{P}} p^{m_p+1}$ et l'extension $\mathbb{Q}(\zeta_f)/K$ est modérée.

DÉFINITION 1.2. — *On pose* $\mathcal{I}_K = \prod_{p \in \mathbb{P}_s} \phi_K(p)^{n_p} \mathcal{A}_K$ *avec*

$$2n_p = \begin{cases} \dfrac{p^{m_p}-1}{p-1} r_p + 1 & \text{si } m_p \equiv 1 \pmod 2 \\ \dfrac{p^{m_p}-1}{p-1} r_p & \text{si } m_p \equiv 0 \pmod 2. \end{cases}$$

Le réseau dual du réseau $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ est le réseau $(\mathcal{I}_K^*, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ avec $\mathcal{I}_K^* = \mathcal{I}_K^{-1}\mathcal{D}_K^{-1}$. Il est bien sûr équivalent de déterminer la classe de $\mathbb{Z}[G]$-isométrie de $\mathcal{I}_K$ ou celle de $\mathcal{I}_K^*$. Dans ce but, nous allons montrer que $\mathcal{I}_K^*$ est libre sur son ordre associé Λ_K et en donner un générateur (théorème 1.7). Comme, d'une part, la définition de Λ_K est analogue à celle de l'ordre associé à l'anneau des entiers donnée par Leopoldt, et que, d'autre part, le théorème de Leopoldt intervient de façon cruciale dans la démonstration du théorème 1.7, nous consacrons le paragraphe suivant à un rappel de ce théorème.

1.2. Le théorème de Leopoldt [L], [Le].

Soit k une extension abélienne de $\mathbb{Q}$, de groupe de Galois G. Leopoldt décrit l'ordre associé Ω_k de l'anneau des entiers $\mathcal{O}_k$, montre que $\mathcal{O}_k$ est libre sur son ordre associé et exhibe explicitement un générateur T_k de $\mathcal{O}_k$ sur Ω_k (on trouve dans [Le] un générateur simplifié par rapport à celui donné par Leopoldt dans [L] ; c'est celui que nous utiliserons). On a donc $\mathcal{O}_k = \Omega_k.T_k$.

Nous utilisons les notations de [Le].

Soit f le conducteur de k, et soit :

$$\mathcal{D}(f) = \Big\{ d \in \mathbb{N} \text{ tels que } \Big(\prod_{p \in \mathbb{P} - \{2\}} p \Big) / d,\ d/f,\ d \not\equiv 2(4) \Big\}$$

et pour tout $n \in \mathbb{N}$:

$$q(n) = \prod_{\substack{p \in \mathbb{P} \\ v_p(n) \geq 2}} p^{v_p(n)}.$$

La relation d'équivalence sur le groupe des caractères de G définie par :

$$\chi \sim \psi \Longleftrightarrow q(f_\chi) = q(f_\psi)$$

a pour classes d'équivalence les ensembles :

$$\Phi_d = \{\chi \in \hat{G} \text{ tels que } q(f_\chi) = q(d)\},\ d \in \mathcal{D}(f).$$

On définit encore :

$$G_d = \bigcap_{\chi \in \Phi_d} \ker(\chi) \quad ; \quad k_d = k^{G_d}.$$

Les idempotents $\epsilon_d = \sum_{\chi \in \Phi_d} e_\chi$ appartiennent à l'algèbre $\mathbb{Q}[G]$ et permettent de définir l'ordre suivant :

$$\Omega_k = \sum_{d \in \mathcal{D}(f)} \mathbb{Z}[G]\epsilon_d.$$

(Rappelons que $e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g) g^{-1}$). Soit finalement :

$$T_k = \sum_{d \in \mathcal{D}(f)} \mathrm{Trace}_{\mathbb{Q}(\zeta_d)/k_d}(\zeta_d)$$

où $(\zeta_k)_{k \in \mathbb{N}}$ est un système projectif de racines de l'unité.

THÉORÈME 1.3 [L], [Le]. — *Avec les notations ci-dessus, on a :*

$$\mathcal{O}_k = \Omega_k . T_k.$$

Il est intéressant de remarquer qu'en fait, le théorème de Leopoldt donne non seulement la structure de $\mathbb{Z}[G]$-module de l'anneau des entiers, mais également sa structure de $\mathbb{Z}[G]$-module hermitien :

COROLLAIRE 1.4.

$$(\mathcal{O}_k, \mathrm{Trace}_{k/\mathbb{Q}}(x^2)) \sim_{\mathbb{Z}[G]} (\Omega_k, T_1(s\lambda\overline{\lambda}))$$

avec

$$s = \sum_{d \in \mathcal{D}(f)} [k : k_d]^2 \sum_{\chi \in \Phi_d} f_\chi e_\chi.$$

Démonstration. — D'après (2), (5) et Théorème 1.b de [Le], on a :

$$(T_k|\chi) = [k : k_d] \mu\Big(\frac{d}{f_\chi}\Big) \overline{\chi}\Big(-\frac{d}{\chi}\Big) \overline{\tau(\chi)}$$

et comme

$$\tau(\chi)\overline{\tau(\chi)} = f_\chi,$$

il vient :

$$(T_k|\chi)\overline{(T_k|\chi)} = [k : k_d]^2 f_\chi. \tag{1}$$

Le lemme 1.1 permet de conclure. □

1.3. $\mathcal{I}_K^*$ est libre sur son ordre associé; théorème de structure pour le $\mathbb{Z}[G]$-réseau $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$.

Dans ce paragraphe, le degré de K sur $\mathbb{Q}$ n'est pas nécessairement impair, mais on suppose que le nombre premier 2 n'est pas ramifié dans K. On conserve les notations du paragraphe 1.1.

On définit des idempotents de l'algèbre de groupe $\mathbb{Q}[G]$ de la façon suivante : soit

$$d_0 = \prod_{p \in \mathbb{P}_{pr}} p^2 \prod_{p \in \mathbb{P}_m \cup \mathbb{P}_s} p$$

et

$$\mathcal{D}_s(f) = \{d \in \mathbb{N} \text{ tels que } d_0/d \text{ et } d/f\}.$$

Pour tout entier k, on pose

$$q_s(k) = \prod_{\substack{p \in \mathbb{P}_s \\ v_p(k) \geq 2}} p^{v_p(k)}.$$

Soit $\hat{G}$ le groupe des caractères de G; on dit que deux éléments χ et ψ de $\hat{G}$ de conducteurs f_χ, f_ψ sont équivalents si $q_s(f_\chi) = q_s(f_\psi)$. Les classes d'équivalence de cette relation d'équivalence sont les ensembles

$$\Psi_d = \{\chi \in \hat{G} \text{ tels que } q_s(f_\chi) = q_s(d)\}, d \in \mathcal{D}_s(f).$$

Si e_χ est l'idempotent de $\mathbb{C}[G]$ associé au caractère χ de G on définit : $e_{\Psi_d} = \sum_{\chi \in \Psi_d} e_\chi$. Ces idempotents sont dans $\mathbb{Q}[G]$.

On définit encore :

$$G_{\Psi_d} = \bigcap_{\chi \in \Psi_d} \ker(\chi); \qquad K_{\Psi_d} = K^{G_{\Psi_d}}$$

et l'ordre de l'algèbre $\mathbb{Q}[G]$:

$$\Lambda_K = \sum_{d \in \mathcal{D}_s(f)} \mathbb{Z}[G] e_{\Psi_d}.$$

Remarques 1.5.

1) Les ordres Ω_K et Λ_K sont construits de façon tout à fait semblable ; pour Λ_K, on "ignore" simplement les nombres premiers qui sont peu ramifiés dans K. Si 2 n'est pas ramifié dans K et si aucun nombre premier n'est pas ramifié dans K, ces deux ordres sont égaux.

2) Explicitons quelques cas particuliers. Si $\mathbb{P}_s = \varnothing$, alors $\Lambda_K = \mathbb{Z}[G]$.

Si $\mathbb{P}_s = \{p\}$, alors $\mathcal{D}_s(f) = \{d_0 p^k, 0 \leq k \leq m_p\}$. Soit, pour tout k, P_k le sous-groupe d'ordre p^k du groupe d'inertie en p de K. Si H est un sous-groupe de G, on pose $e_H = \dfrac{1}{|H|} \sum_{h \in H} h$. Alors, grâce au lemme 1.6 suivant, on voit facilement que : $e_{\Psi_{d_0}} = e_{P_{m_p}}$, et $e_{\Psi_{d_0 p^k}} = e_{P_{m_p - k}} - e_{P_{m_p - k + 1}}$ pour $1 \leq k \leq m_p$. Avec la convention $e_{P_k} = 0$ si $k \geq m_p + 1$, on trouve pour l'ordre Λ_K :

$$\Lambda_K = \sum_{0 \leq i \leq m_p} \mathbb{Z}[G](e_{P_i} - e_{P_{i+1}}).$$

Nous aurons besoin des propriétés suivantes :

LEMME 1.6. — *Soit $d \in \mathcal{D}_s(f)$. Alors :*

(1) Ψ_d est non vide.

(2) $K_{\Psi_d} = K \cap \mathbb{Q}(\zeta_d)$

(3) $[K : K_{\Psi_d}] = f/d$.

Démonstration. — On paraphrase la démonstration du lemme 1 de [Le]. Soit $X(n)$ le groupe des caractères de $(\mathbb{Z}/n\mathbb{Z})^*$. On identifie $X(n)$ au groupe des caractères du groupe de Galois de $\mathbb{Q}(\zeta_n)$. Le corps K correspond à un sous-groupe X de $X(f)$.

Pour tout nombre premier p et tout entier m, $X(p^{m+1})$ est le produit direct de $X(p)$ et d'un sous-groupe cyclique d'ordre p^m noté $Y(p^m)$. Le groupe $X(f)$, est lui produit direct des $X(p^{m_p+1})$.

Ceci permet de définir la projection π :

$$\pi : X(f) \to \prod_{p \in \mathbb{P}_s} Y(p^{m_p}).$$

L'expression du conducteur f_χ d'un caractère χ appartenant à $X(f)$ ([Le],(1)) montre que la restriction de π à X est surjective (f est le ppcm

des f_χ lorsque χ parcourt X), et que, pour tout χ, ψ appartenant à $X(f)$,

$$q_s(f_\chi) = q_s(f_\psi) \Leftrightarrow \pi(\chi) = \pi(\psi),$$

d'où (1). Il est équivalent de montrer (2) ou de montrer que le sous-groupe engendré par Ψ_d et noté $< \Psi_d >$ est égal à $X \cap X(d)$.

L'inclusion $< \Psi_d > \subset X \cap X(d)$ est évidente. Réciproquement, soit χ un caractère de K appartenant à $X(d)$. Alors son conducteur divise d. Soit χ' un élément de Ψ_d ; il est facile de voir que, comme $q_s(\chi)$ divise $q_s(\chi')$, $\pi(\chi)$ appartient au sous-groupe engendré par $\pi(\chi')$.

Alors, si $\pi(\chi) = \pi(\chi')^k$, $\pi(\chi {\chi'}^{1-k}) = \pi(\chi')$ et donc χ appartient à $< \Psi_d >$.

L'égalité (3) se déduit directement de (2). □

On suppose désormais que le degré de K sur $\mathbb{Q}$ est impair.

Avec les définitions de l'introduction et des paragraphes précédents, nous sommes en mesure d'énoncer le théorème de structure pour le $\mathbb{Z}[G]$-réseau $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$.

THÉORÈME 1.7. — *Soit K une extension abélienne de $\mathbb{Q}$ de degré impair.*

(1) *Il existe un élément explicite t_K de K tel que $\mathcal{I}_K^* = \Lambda_K.t_K$.*

(2) *L'application $\lambda \mapsto \lambda(t_K)$ induit la $\mathbb{Z}[G]$-isométrie :*

$$(\mathcal{I}_K^*, \mathrm{Trace}_{K/\mathbb{Q}}(x^2)) \sim_{\mathbb{Z}[G]} (\Lambda_K, T_1(s^{-1}\lambda\overline{\lambda}))$$

avec

$$s = \sum_{d \in \mathcal{D}_s(f)} d/f \sum_{\chi \in \Psi_d} \Big(\prod_{\substack{p \in \mathbb{P}_{s,1} \\ p \nmid f_\chi}} p \Big) e_\chi.$$

(3) *Par dualité on a :*

$$(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2)) \sim_{\mathbb{Z}[G]} \Big(\bigoplus_{d \in \mathcal{D}_s(f)} \mathbb{Z}[G]^{e_{\Psi_d}}, T_1(s\lambda\overline{\lambda}) \Big)$$

avec

$$\mathbb{Z}[G]^{e_{\Psi_d}} = \{\lambda \in \mathbb{Z}[G] \text{ tels que } \lambda e_{\Psi_d} = \lambda\}$$

(cette somme est une somme orthogonale de $\mathbb{Z}[G]$-réseaux).

La démonstration du théorème 1.7 est l'objet des paragraphes 1.4 et 1.5. En particulier, l'élément t_K est donné au paragraphe 1.5. On définit une extension L de K, abélienne sur $\mathbb{Q}$, et un idéal $\mathcal{J}_L$ de L tel que $\mathcal{I}_K^* = \mathrm{Trace}_{L/K}(\mathcal{J}_L)$. On applique ensuite les théorèmes de Leopoldt et de B. Erez pour montrer que cet idéal est libre sur son ordre associé et pour en donner un générateur.

Le système de racines d'un réseau entier est l'ensemble des vecteurs sur lesquels la forme quadratique prend la valeur 1 ou 2 (il est souvent confondu avec le réseau que ces vecteurs engendrent). La proposition suivante donne le système de racines de $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$. Les notations sont celles de [CS]. La somme orthogonale de k réseaux isométriques à R est notée R^k.

PROPOSITION 1.8.

1) *Pour d différent de d_0, $(\mathbb{Z}[G]^{e_{\Psi_d}}, T_1(s\lambda\overline{\lambda}))$ est pair et son rang est égal au cardinal de Ψ_d. Ce réseau a pour minimum 2 si et seulement si les deux conditions suivantes sont remplies :*

(i) *$q_s(d)$ est une puissance d'un seul nombre premier p*

(ii) *pour tout $q \in \mathbb{P}_{s,1}$ et pour tout $\chi \in \Psi_d$, q divise f_χ*

et dans ce cas, $(\mathbb{Z}[G]^{e_{\Psi_d}}, T_1(s\lambda\overline{\lambda})) \sim \mathbb{A}_{p-1}^{[G:G_{\Psi_{d/p}}]}$.

2) *Pour $d = d_0$, le réseau $(\mathbb{Z}[G]^{e_{\Psi_d}}, T_1(s\lambda\overline{\lambda}))$ est impair. Il représente 1 si et seulement si $\mathbb{P}_{s,1}$ est vide, et dans ce cas il est isométrique au réseau $\mathbb{Z}^{[K_{\Psi_d}:\mathbb{Q}]}$.*

Si $\mathbb{P}_{s,1}$ est non vide, son système de racines est $\mathbb{A}_{|J|-1}^{[H:J]}$, où $H = \mathrm{Gal}(K_{\Psi_d}/\mathbb{Q})$ et J est l'intersection des groupes d'inertie des nombres premiers appartenant à $\mathbb{P}_{s,1}$ de l'extension $K_{\Psi_d}/\mathbb{Q}$ (avec la convention : $\mathbb{A}_0 = \varnothing$).

La démonstration de la proposition 1.8 est l'objet du paragraphe 1.6.

Exemples 1.9.

1) Supposons que $\mathbb{P}_s = \varnothing$. Alors $\mathcal{I}_K = \mathcal{A}_K$, $\Lambda_K = \mathbb{Z}[G]$ et $s = 1$. On retrouve l'énoncé du résultat de B. Erez ([E1]) : si l'extension $K/\mathbb{Q}$ est peu ramifiée, alors on a la $\mathbb{Z}[G]$-isométrie : $(\mathcal{A}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2)) \sim_{\mathbb{Z}[G]} (\mathbb{Z}[G], T_1(\lambda\overline{\lambda}))$.

2) Supposons que $\mathbb{P}_s = \{p\}$. L'ordre Λ_K a été explicité au point 2) de la remarque 1.5.

La proposition 1.8 montre que

$$(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2)) \sim R_0 \oplus \mathbb{A}_{p-1}^k$$

où $k = |G| - [G : P_{m_p}]$ et R_0 est le terme correspondant à d_0 dans les notations du théorème 1.7(3). Si $m_p \equiv 0 \pmod 2$, $R_0 \sim \mathbb{Z}^{[G:P_{m_p}]}$ (c'est le point 2) de la proposition 1.8). Si $m_p \equiv 1 \pmod 2$, notons $G' = G/P_{m_p}$ et C le sous-groupe d'ordre r_p de G' qui est l'image du groupe d'inertie en p. Alors, on voit par le théorème 1.7 que

$$R_0 \sim_{\mathbb{Z}[G]} (\mathbb{Z}[G'], T_1(((p-1)e_C + 1)\lambda\overline{\lambda})).$$

En termes de réseaux, $R_0 = R_1^{[G':C]}$, où R_1 est un réseau de rang r_p, de discriminant p, dont une matrice de Gram est $(s_{i,j})$ avec $s_{i,j} = \dfrac{p-1}{r_p}$ si $i \neq j$ et $s_{i,j} = \dfrac{p-1}{r_p} + 1$ si $i = j$. Remarquons que R_1 est impair, de minimum 2 et contient la somme orthogonale $< pr_p > \oplus \mathbb{A}_{r_p-1}$, où $< pr_p >$ désigne le réseau de rang 1 et de discriminant pr_p.

Or, on peut vérifier facilement que, dans les deux cas, $R_0 = \mathcal{I}_K^{e_{P_m}} = \mathcal{A}_K^{e_{P_m}}$. C'est donc un invariant de la classe de $\mathbb{Z}[G]$-isométrie de $\mathcal{A}_K$. Quant au terme $\mathbb{A}_{p-1}^k$, c'est un système de racines contenu dans $\mathcal{A}_K^{1-e_{P_m}}$ et de même rang. Si $p \neq 3, 5$, $\mathbb{A}_{p-1}^k$ n'est contenu dans aucun autre système de racines de même rang, donc c'est le système de racines de $\mathcal{A}_K^{1-e_{P_m}}$ et c'est encore un invariant de la classe de $\mathbb{Z}[G]$-isométrie de $\mathcal{A}_K$. Si $p = 3$ ou 5, il peut être contenu dans une somme de $\mathbb{E}_6$ ou de $\mathbb{E}_8$. Mais, si $p = 3$ ou 5, alors $r_p = 1$, et l'extension $K/\mathbb{Q}$ est un cas particulier de celles qui sont étudiées dans [BE] et [B]. Comme on le montre dans ces articles, le système de racines de $\mathcal{A}_K$ est effectivement, lorsque $p = 3$, soit une somme de $\mathbb{E}_6$, soit une $\mathbb{E}_8$.

1.4. L'extension L de K et l'idéal $\mathcal{J}_L$.

Soit k_p l'unique sous-extension de degré p sur $\mathbb{Q}$ de $\mathbb{Q}(\zeta_{p^2})$. Soit $f' = f/\Big(\prod_{p \in \mathbb{P}_{pr}} p^2\Big)$. On pose

$$L = \mathbb{Q}(\zeta_{f'}) \prod_{p \in \mathbb{P}_{pr}} k_p.$$

Alors K est inclus dans L et L est le composé arithmétiquement disjoint des corps L_p avec $L_p = k_p$ pour $p \in \mathbb{P}_{pr}$ et $L_p = \mathbb{Q}(\zeta_{p^{m_p+1}})$ pour $p \in \mathbb{P}_m \cup \mathbb{P}_s$. Il est donc légitime d'identifier L et le produit tensoriel de ces corps. On pose :

$$\mathcal{J}_L = \prod_{p/f} \mathcal{J}(p)$$

avec

$$\mathcal{J}(p) = \begin{cases} p^{-\frac{m_p+1}{2}} \mathcal{O}_{L_p} & \text{si } p \in \mathbb{P}_{s,1} \\ p^{-1}\mathfrak{P} & \text{si } p \in \mathbb{P}_{pr} \\ p^{-\frac{m_p+2}{2}} \mathfrak{P}^{\frac{p^{m_p+1}-p^{m_p}}{2}} & \text{si } p \in \mathbb{P}_m \cup \mathbb{P}_{s,0} \end{cases}$$

où $\mathfrak{P}$ est l'unique idéal de L_p au-dessus de p.

LEMME 1.10.

$$\mathcal{I}_K^* = \mathrm{Trace}_{L/K}(\mathcal{J}_L).$$

Démonstration du lemme 1.10. — C'est un calcul facile. De la connaissance de la suite de ramification de $L/\mathbb{Q}$ et du fait que l'extension L/K est modérée, on déduit la valuation en $\phi_K(p)$ de l'idéal $\mathcal{A}_K$, et donc de $\mathcal{I}_K^* = \prod_{p \in \mathbb{P}_s} \phi_K(p)^{-n_p} \mathcal{A}_K$.

On trouve que la partie au-dessus de p de $\mathcal{I}_K^*$ est égale à : $p^{-\frac{m_p+1}{2}} \mathcal{O}_K$ si $p \in \mathbb{P}_{s,1}$, et à : $p^{-\frac{m_p+2}{2}} \phi_K(p)^{\frac{r_p p^{m_p}+1}{2}}$ si $p \in \mathbb{P}_{s,2}$.

On conclut ensuite en utilisant la formule : si $J = \prod_p \phi_L(p)^{s_p}$ est un idéal de L alors $\mathrm{Trace}_{L/K}(J) = \prod_p \phi_K(p)^{t_p}$ avec pour tout p, t_p est égal à la partie entière du quotient : $\dfrac{s_p + \delta_p}{e_p}$ où δ_p est la valuation en $\phi_L(p)$ de la différente relative de L/K et e_p est le degré de ramification de L/K ([U]). □

Soit G_L le groupe de Galois de L sur $\mathbb{Q}$. On a défini au paragraphe 1.3 l'ordre Λ_L de l'algèbre $\mathbb{Q}[G_L]$. Remarquons que l'ensemble $\mathcal{D}_s(f)$ relatif à L est le même que celui de K.

Soit π l'élément de $\mathbb{Q}(\zeta_p)$ vérifiant $\pi^2 = (-1)^{\frac{p-1}{2}} p$. On pose

$$t_L = \prod_{p \in \mathbb{P}} t_p$$

avec

$$t_p = \begin{cases} p^{-1}(1 + \mathrm{Trace}_{\mathbb{Q}(\zeta_{p^2})/k_p}(\zeta_{p^2})) & \text{si } p \in \mathbb{P}_{pr} \\ p^{-\frac{m_p+1}{2}} T_{L_p} & \text{si } p \in \mathbb{P}_{s,1} \\ p^{-\frac{m_p+2}{2}} \pi T_{L_p} & \text{si } p \in \mathbb{P}_{s,0} \end{cases}$$

avec les notations du paragraphe 1.2.

LEMME 1.11. — *Avec les notations précédentes,*

$$\mathcal{J}_L = \Lambda_L.t_L = \{\lambda(t_L), \lambda \in \Lambda_L\}$$

et, pour tout $\chi \in \hat{G_L}$, *si* $\chi \in \Psi_d$,

$$(t_L|\chi)\overline{(t_L|\chi)} = \left(\prod_{\substack{p \in \mathbb{P}_{s,1} \\ p \nmid f_\chi}} p \right)^{-1} \frac{f}{d}.$$

Démonstration. — Comme L est le produit arithmétiquement disjoint des L_p, le groupe G_L est le produit direct des groupes de Galois G_{L_p} ; le groupe des caractères $\hat{G_L}$ est le produit direct des groupes de caractères $\hat{G_{L_p}}$ et le conducteur f_χ d'un caractère χ de G_L est le produit des conducteurs f_{χ_p} des composantes $\chi_p \in \hat{G_{L_p}}$ de χ. L'ordre Λ_L s'identifie donc avec le produit des ordres Λ_{L_p} de $\mathbb{Q}[G_{L_p}]$.

De plus, si $t = \prod_{p \in \mathbb{P}} t_p$ avec $t_p \in L_p$, alors, pour tout caractère χ de G_L, $(t|\chi) = \prod_{p \in \mathbb{P}} (t_p|\chi_p)$. Il suffit donc de démontrer que, pour tout p appartenant à $\mathbb{P}$, $\mathcal{J}(p) = \Lambda_{L_p}.t_p$ avec, pour tout $\chi \in \hat{G_{L_p}}$, et si $\chi \in \Psi_d$,

$$(t_p|\chi)\overline{(t_p|\chi)} = \begin{cases} p^{-1}\frac{f_{L_p}}{d} & \text{si } p \in \mathbb{P}_{s,1} \text{ et } \chi = 1 \\ \frac{f_{L_p}}{d} & \text{si } p \in \mathbb{P}_{s,1} \text{ et } \chi \neq 1 \\ 1 & \text{si } p \in \mathbb{P}_{pr} \\ \frac{f_{L_p}}{d} & \text{si } p \in \mathbb{P}_m \cup \mathbb{P}_{s,0}. \end{cases}$$

1) Si $p \in \mathbb{P}_{pr}$ alors on vérifie facilement que $\mathcal{J}(p)$ est la racine carrée de la codifférente de L_p. D'après le lemme 2.e de [E2], $\mathcal{J}(p) = \mathbb{Z}[G_{L_p}].t_p$ avec, pour tout caractère χ de G_{L_p}, $(t_p|\chi)\overline{(t_p|\chi)} = 1$. Or $\Lambda_{L_p} = \mathbb{Z}[G_{L_p}]$.

2) Si $p \in \mathbb{P}_{s,1}$, alors on applique le théorème de Leopoldt. D'après la remarque 1.5, $\Omega_{L_p} = \Lambda_{L_p}$; donc $\mathcal{J}(p) = \Lambda_{L_p}.t_p$ avec $t_p = p^{-\frac{m_p+1}{2}} T_{L_p}$.

Si χ est un caractère de G_{L_p}, $(t_p|\chi)\overline{(t_p|\chi)} = p^{-(m_p+1)}(T_{L_p}|\chi)\overline{(T_{L_p}|\chi)}$.

Comme le conducteur de L_p est p^{m_p+1}, l'ensemble $\mathcal{D}_s(f_{L_p})$ est égal à $\{p, p^2, ..., p^{m_p+1}\}$. Donc, si $d \in \mathcal{D}_s(f_{L_p})$ et si $\chi \in \Psi_d$ n'est pas le caractère trivial, alors $f_\chi = d$ (par contre, si $\chi = 1$ alors $f_\chi = 1$ et $d = p$).

La formule (1), le lemme 1.6(3) et les remarques précédentes établissent la formule annoncée.

3) Supposons enfin que $p \in \mathbb{P}_m \cup \mathbb{P}_{s,0}$. L'idéal $\mathcal{J}(p)$ de $L_p = \mathbb{Q}(\zeta_{p^{m_p+1}})$ est engendré par $p^{-\frac{m_p+2}{2}}\pi$. Donc, d'après le théorème de Leopoldt et la remarque 1.5,

$$\mathcal{J}(p) = p^{-\frac{m_p+2}{2}} \pi \Lambda_{L_p}.T_{L_p} = \{p^{-\frac{m_p+2}{2}} \pi\lambda(T_{L_p}), \lambda \in \Lambda_{L_p}\}.$$

Nous allons montrer que

$$\mathcal{J}(p) = \Lambda_{L_p}.p^{-\frac{m_p+2}{2}} \pi T_{L_p} = \{\lambda(p^{-\frac{m_p+2}{2}} \pi T_{L_p}), \lambda \in \Lambda_{L_p}\}.$$

Soit, pour $1 \leq k \leq m_p$, P_k l'unique sous-groupe de $\mathrm{Gal}(L_p/\mathbb{Q})$ d'ordre p^k. D'après le point 2) de la remarque 1.5, les idempotents définissant Λ_{L_p} sont : $1 - e_{P_1}, e_{P_1} - e_{P_2}, ..., e_{P_{m_p-1}} - e_{P_{m_p}}, e_{P_{m_p}}$.

Ils appartiennent tous à l'algèbre $\mathbb{Q}[\mathrm{Gal}(L_p/\mathbb{Q}(\zeta_p))]$, donc vérifient : pour tout x appartenant à L_p, $e(\pi x) = \pi e(x)$. Si $g \in G_{L_p}$, alors $g(\pi) = \pm\pi$. Donc, si $\lambda \in \mathbb{Z}[G_{L_p}]$, alors pour tout x appartenant à L_p, il existe λ' appartenant à $\mathbb{Z}[G_{L_p}]$ tel que $\lambda(\pi x) = \pi\lambda'(x)$. Finalement, on a : $\Lambda_{L_p}.\pi T_{L_p} = \pi\Lambda_{L_p}.T_{L_p}$, d'où l'expression annoncée de $\mathcal{J}(p)$.

Il nous reste à calculer $(t_p|\chi)\overline{(t_p|\chi)}$.

$$(t_p|\chi)\overline{(t_p|\chi)} = p^{-(m_p+2)}(\pi T_{L_p}|\chi)\overline{(\pi T_{L_p}|\chi)}.$$

Soit χ_0 l'unique caractère d'ordre 2 de G_{L_p}. Alors on voit facilement que :

$$(\pi T_{L_p}|\chi) = \pi(T_{L_p}|\chi\chi_0).$$

De plus, les conducteurs de χ et de $\chi\chi_0$ sont égaux, sauf si $\chi = 1$ auquel cas $f_\chi = 1$ et $f_{\chi\chi_0} = p$. Les caractères χ et $\chi\chi_0$ appartiennent donc au même Ψ_d, et de plus : $f_{\chi\chi_0} = d$. Compte tenu du fait que $\pi\overline{\pi} = p$, on conclut comme au 2). □

1.5. Fin de la démonstration du théorème 1.7.

Soit H le groupe de Galois de l'extension L/K. On note toujours $e_H = 1/|H| \sum_{h \in H} h$.

Par le lemme 1.11, $\mathcal{J}_L = \Lambda_L.t_L$. Par le lemme 1.10, $\mathcal{I}_K^* = \mathrm{Trace}_{L/K}(\mathcal{J}_L)$. Donc :

$$\mathcal{I}_K^* = \mathrm{Trace}_{L/K}(\mathcal{J}_L) = |H| e_H(\mathcal{J}_L) = \Lambda_L e_H.\mathrm{Trace}_{L/K}(t_L).$$

Dans l'isomorphisme entre les algèbres $\mathbb{Q}[G_L]e_H$ et $\mathbb{Q}[G]$ donné par :

$$\begin{aligned} \mathbb{Q}[G_L]e_H &\to \mathbb{Q}[G] \\ ge_H &\mapsto g \text{ modulo } H \end{aligned}$$

l'ordre $\Lambda_L e_H$ est envoyé sur Λ_K. En posant

$$t_K = \mathrm{Trace}_{L/K}(t_L)$$

on a donc :

$$\mathcal{I}_K^* = \Lambda_K.t_K$$

avec, si χ est un caractère de G, c'est-à-dire un caractère de G_L dont le noyau contient H,

$$(t_K|\chi)\overline{(t_K|\chi)} = (t_L|\chi)\overline{(t_L|\chi)} = \left(\prod_{\substack{p \in \mathbb{P}_{s,1} \\ p \nmid f_\chi}} p \right)^{-1} \frac{f}{d}$$

cette dernière égalité provenant du lemme 1.11. On conclut ensuite avec le lemme 1.1. □

1.6. Démonstration de la proposition 1.8.

Posons $R_d = (\mathbb{Z}[G]^{e_{\Psi_d}}, T_1(s\lambda\overline{\lambda}))$.

1) $d \neq d_0$. Le réseau R_d est pair car Ψ_d ne contient pas le caractère trivial, ou encore parce que $R_d \subset \mathcal{A}_K \cap \{x \in K, \mathrm{Trace}_{K/\mathbb{Q}}(x) = 0\}$ (voir le lemme 10.2 de [E1]).

Supposons les conditions (i) et (ii) réalisées. Posons $q_s(d) = p^k$. D'après la définition de Ψ_d, $\chi \in \Psi_d \Leftrightarrow q_s(f_\chi) = p^k \Leftrightarrow f_\chi/d$ et $f_\chi \nmid d/p$; or

$\sum_{f_\chi/d} e_\chi = e_{G_{\Psi_d}}$ d'après le lemme 1.6(2), donc :

$$e_{\Psi_d} = e_{G_{\Psi_d}} - e_{G_{\Psi_{d/p}}}.$$

De plus, $se_{\Psi_d} = d/f \sum_{\chi\in\Psi_d} e_\chi = \frac{1}{|G_{\Psi_d}|} e_{\Psi_d}$, d'après la condition (ii) et le lemme 1.6(3). On a donc :

$$R_d \sim_{\mathbb{Z}[G]} (\mathbb{Z}[G]^{(e_{G_{\Psi_d}} - e_{G_{\Psi_{d/p}}})}, \frac{1}{|G_{\Psi_d}|} T_1(\lambda\overline{\lambda})).$$

Or ce dernier réseau est isométrique à $\mathbb{A}_{p-1}^{[G:G_{\Psi_{d/p}}]}$ grâce au lemme suivant, et grâce au fait que $[G_{\Psi_d} : G_{\Psi_{d/p}}] = p$ (lemme 1.6(3)) :

LEMME 1.12. — *Si H et H_1 sont deux sous-groupes de G tels que $H_1 \subset H$, alors*

$$\left(\mathbb{Z}[G]^{(e_{H_1} - e_H)}, \frac{1}{|H_1|} T_1(\lambda\overline{\lambda})\right) \sim_{\mathbb{Z}} \mathbb{A}_{[H:H_1]-1}^{[G:H]}$$

et les vecteurs minimaux sont les $(g - g')|H_1|e_{H_1}$ avec $gH_1 \neq g'H_1$ et $gH = g'H$.

Réciproquement, supposons que le minimum de R_d soit 2. Si le caractère χ appartient à Ψ_d, alors il est non trivial, et son conducteur divise d. Or

$$\sum_{\substack{f_\chi/d \\ \chi\neq 1}} e_\chi = e_{G_{\Psi_d}} - e_G,$$

donc

$$R_d \subset (\mathbb{Z}[G]^{(e_{G_{\Psi_d}} - e_G)}, T_1(s\lambda\overline{\lambda})).$$

Si s est un élément de $\mathbb{Q}[G]$ vérifiant $\overline{s} = s$, on montre facilement que la forme $T_1(s\lambda\overline{\lambda})$ est positive si et seulement si $\chi(s)$ est positif pour tout caractère χ de G, et que les éléments λ de $\mathbb{Q}[G]$ isotropes, c'est-à-dire tels que $T_1(s\lambda\overline{\lambda}) = 0$ sont ceux pour lesquels $\chi(\lambda) = 0$ dès que $\chi(s) = 0$. Cela montre en particulier que, pour le s du théorème 1.7, $T_1(s\lambda\overline{\lambda}) \geq \frac{1}{|G_{\Psi_d}|} T_1(e_{G_{\Psi_d}}\lambda\overline{\lambda})$. Or d'après le lemme 1.12, le minimum du réseau $(\mathbb{Z}[G]^{(e_{G_{\Psi_d}} - e_G)}, \frac{1}{|G_{\Psi_d}|} T_1(\lambda\overline{\lambda}))$ est 2, et est atteint sur les éléments

$(g-g')|G_{\Psi_d}|e_{G_{\Psi_d}}$ avec $gG_{\Psi_d} \neq g'G_{\Psi_d}$. Une condition nécessaire pour que R_d ait pour minimum 2 est donc que l'un au moins de ces éléments appartienne à $\mathbb{Z}[G]^{e_{\Psi_d}}$.

Posons $x = (g-g')|G_{\Psi_d}|e_{G_{\Psi_d}}$ avec $g'g^{-1} \notin G_{\Psi_d}$.

$$\begin{aligned} x \in \mathbb{Z}[G]^{e_{\Psi_d}} &\Leftrightarrow xe_{\Psi_d} = x \\ &\Leftrightarrow (g-g')e_\chi = 0 \text{ si } \chi \notin \Psi_d \text{ et } G_{\Psi_d} \subset \ker(\chi) \\ &\Leftrightarrow g'g^{-1} \in \bigcap_{\substack{\chi \notin \Psi_d \\ G_{\Psi_d} \subset \ker(\chi)}} \ker(\chi). \end{aligned}$$

Une condition nécessaire pour que R_d ait pour minimum 2 est donc que cette dernière intersection soit différente de G_{Ψ_d}. Montrons que cette condition n'est pas réalisée si $q_s(d)$ a deux diviseurs premiers. On a :

$$\bigcap_{\substack{\chi \notin \Psi_d \\ G_{\Psi_d} \subset \ker\chi}} \ker\chi = \bigcap_{\substack{\chi \in \Psi_{d'} \\ d'/d,\ d' \neq d}} \ker\chi = \bigcap_{\substack{d'/d \\ d' \neq d}} G_{\Psi_{d'}}$$

or, si d a deux diviseurs premiers distincts, on peut trouver dans $\mathcal{D}_s(f)$ deux entiers d' et d'' divisant d et tels que d/d' et d/d'' soient différents de 1 et premiers entre eux. Alors, grâce au point (3) du lemme 1.6, $G_{\Psi_{d'}} \cap G_{\Psi_{d''}} = G_{\Psi_d}$.

On a donc $q_s(d) = \{p\}$, et $e_{\Psi_d} = e_{G_{\Psi_d}} - e_{G_{\Psi_{d/p}}}$. Toujours d'après le lemme 1.12, pour que le minimum de R_d soit 2, il faut et il suffit que R_d contienne un élément de la forme $x = (g-g')|G_{\Psi_d}|e_{G_{\Psi_d}}$ avec $g'g^{-1} \notin G_{\Psi_d}$, $g'g^{-1} \in G_{\Psi_{d/p}}$, et x isotrope pour la forme $T_1\Big(\Big(s - \dfrac{1}{|G_{\Psi_d}|}e_{G_{\Psi_d}}\Big)\lambda\overline{\lambda}\Big)$. Cette dernière condition conduit à demander que $\chi(x) = 0$ pour tout χ appartenant à $E = \{\chi \in \Psi_d | \exists q \in \mathbb{P}_{s,1} | q \nmid f_\chi\}$, c'est-à-dire que $g'g^{-1} \in \cap_{\chi \in E}\ker(\chi)$.

Or, l'indice $[G_{\Psi_{d/p}} : G_{\Psi_d}]$ est égal à p d'après le lemme 1.6(3), donc G_{Ψ_d} et $g'g^{-1}$ engendrent $G_{\Psi_{d/p}}$. Si l'ensemble E est non vide, et si χ appartient à E, on aurait donc $G_{\Psi_{d/p}} \subset \ker(\chi)$, soit $\chi \in \Psi_{d/p}$, ce qui contredit le fait que $\chi \in \Psi_d$. L'ensemble E est donc vide, ce qui est la condition (ii).

2) $d = d_0$. Alors $\chi \in \Psi_{d_0}$ si et seulement si f_χ divise d_0, donc $e_{\Psi_{d_0}} = e_{G_{\Psi_{d_0}}}$ et

$$R_{d_0} = (\mathbb{Z}[G]^{e_{G_{\Psi_{d_0}}}}, T_1(s\lambda\overline{\lambda})).$$

En posant $G' = G/G_{\Psi_{d_0}}$, on voit facilement que

$$R_{d_0} \sim_{\mathbb{Z}[G]} (\mathbb{Z}[G'], T_1(s'\lambda\overline{\lambda}) \text{ avec } s' = \sum_{\chi \in \Psi_d} \Big(\prod_{\substack{p \in \mathbb{P}_{s,1} \\ p \nmid f_\chi}} p \Big) e_\chi.$$

Si $\mathbb{P}_{s,1} = \varnothing$, alors

$$R_{d_0} \sim_{\mathbb{Z}[G]} (\mathbb{Z}[G'], T_1(\lambda\overline{\lambda}) \sim \mathbb{Z}^{[G:G_{\Psi_{d_0}}]}.$$

Si $\mathbb{P}_{s,1} \neq \varnothing$, montrons que le minimum de R_{d_0} n'est pas égal à 1 : comme la forme $T_1((s'-1)\lambda\overline{\lambda})$ est positive, un élément de carré scalaire égal à 1 de R_{d_0} serait un élément g appartenant à G' et isotrope pour la forme $T_1((s'-1)\lambda\overline{\lambda})$, c'est-à-dire tel que $\chi(g) = 0$ dès que $\chi(s') \neq 1$. Or $\chi(g) = 0$ est impossible.

Le minimum de R_{d_0} est donc au moins 2. Un élément de carré scalaire égal à 2 est de la forme $g \pm g'$, avec $g \pm g'$ isotrope pour la forme $T_1((s'-1)\lambda\overline{\lambda})$, c'est-à-dire tel que $\chi(g \pm g') = 0$ dès que $\chi \in E$. Comme l'ordre de G est impair, il est impossible d'avoir $\chi(g+g') = 0$. Un élément de carré scalaire égal à 2 est donc de la forme $g - g'$, avec $g'g^{-1} \in \bigcap_{\substack{p \in \mathbb{P}_{s,1} \\ p \nmid f_\chi}} \ker(\chi)$. Cette dernière intersection est égale à l'intersection des groupes d'inertie en p de l'extension $K_{\Psi_{d_0}}/\mathbb{Q}$ lorsque p parcourt $\mathbb{P}_{s,1}$, et on voit facilement que ces éléments forment le système de racines annoncé. □

1.7. Compléments sur le groupe des $\mathbb{Z}[G]$-isométries de $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$.

Dans ce paragraphe, nous mettons en évidence un sous-groupe du groupe des $\mathbb{Z}[G]$-isométries de $(\mathcal{I}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ dont nous aurons besoin au paragraphe 4.

On a défini au paragraphe 1.4 une extension L de K, et un idéal $\mathcal{J}_L$ de L tel que : $\mathcal{J}_L = \prod_{p \in \mathbb{P}} \mathcal{J}(p)$. Supposons maintenant que p appartienne à $\mathbb{P}_s$. Au cours de la démonstration du lemme 1.11, on a vu que $\mathcal{J}(p) = \Lambda_{L_p}.t_p$. Le point 2) de l'exemple 1.5 montre que l'ordre Λ_{L_p} est égal à :

$$\Lambda_{L_p} = \sum_{0 \leq i \leq m_p} \mathbb{Z}[G_{L_p}](e_{P_i} - e_{P_{i+1}})$$

où P_i est le sous-groupe d'ordre p^i de G_{L_p}, ce qui conduit à la décomposition en somme directe orthogonale :

$$\mathcal{J}(p) = \bigoplus_{0 \leq i \leq m_p} \mathbb{Z}[G_{L_p}](e_{P_i} - e_{P_{i+1}}).t_p.$$

Pour tout $\epsilon = (\epsilon_0, \epsilon_1, ..., \epsilon_{m_p})$ appartenant à $\{\pm 1\}^{m_p+1}$, l'application $f_{p,\epsilon}$ définie dans cette décomposition par :

$$f_{p,\epsilon}\Big(\sum_{0 \leq i \leq m_p} x_i\Big) = \sum_{0 \leq i \leq m_p} \epsilon_i x_i$$

est une $\mathbb{Z}[G_{L_p}]$-isométrie de $(\mathcal{J}(p), \mathrm{Trace}_{L_p/\mathbb{Q}}(x^2))$. L'ensemble de ces $\mathbb{Z}[G_{L_p}]$-isométries forme un groupe isomorphe à $\{\pm 1\}^{m_p+1}$.

Comme le réseau $(\mathcal{J}_L, \mathrm{Trace}_{L/\mathbb{Q}}(x^2))$ est le produit tensoriel des $(\mathcal{J}(p), \mathrm{Trace}_{L_p/\mathbb{Q}}(x^2))$, on obtient un groupe de $\mathbb{Z}[G_L]$-isométries de $\mathcal{J}_L$ isomorphe à $\prod_{p \in \mathbb{P}_s} \{\pm 1\}^{m_p+1}$ en considérant l'ensemble des $f = \prod_{p \in \mathbb{P}_s} f_{p,\epsilon}$ lorsque les ϵ parcourent les $\{\pm 1\}^{m_p+1}$. Ce groupe sera noté Is.

Comme $\mathcal{I}_K^* = \mathrm{Trace}_{L/K}(\mathcal{J}_L)$, et que les éléments de Is sont des $\mathbb{Z}[G_L]$-isométries, ils stabilisent $\mathcal{I}_K^*$ et forment donc un sous-groupe du groupe des $\mathbb{Z}[G]$-isométries de $\mathcal{I}_K^*$ (et donc de $\mathcal{I}_K$).

2. Réseau et forme de torsion.

2.1. Généralités.

Soit R un $\mathbb{Z}$-module ou un $\mathbb{Z}_p$-module hermitien entier pour la forme bilinéaire symétrique $b(x, y)$. Le groupe fini $T(R) = R^*/R$ est muni de la forme bilinéaire symétrique induite par celle de R :

$$\begin{aligned} T(R) \times T(R) &\to \mathbb{Q}/\mathbb{Z} \text{ (ou } \mathbb{Q}_p/\mathbb{Z}_p) \\ (\overline{x}, \overline{y}) &\mapsto \overline{b}(\overline{x}, \overline{y}) = \overline{b(x, y)}. \end{aligned}$$

Elle est non dégénérée, c'est-à-dire qu'elle induit un isomorphisme entre $T(R)$ et $\mathrm{Hom}_{\mathbb{Z}}(T(R), \mathbb{Q}/\mathbb{Z})$ (ou $\mathrm{Hom}_{\mathbb{Z}_p}(T(R), \mathbb{Q}_p/\mathbb{Z}_p)$). Si U est un sous-groupe de $T(R)$, on note $U^{\perp} = \{x \in T(R) | \overline{b}(x, U) = 0\}$ l'orthogonal de U pour $\overline{b}$.

Soit s la surjection canonique $s : R^* \to T(R)$; il est bien connu que l'application $L \mapsto s(L)$ établit une bijection entre l'ensemble des réseaux

L tels que $R \subset L \subset R^*$ et l'ensemble des sous-groupes U de $T(R)$ avec les propriétés suivantes : L est entier si et seulement si $U \subset U^\perp$ et dans ce cas $[L^* : L] = [U^\perp : U]$ (cf [Ba]). En particulier, L est unimodulaire si et seulement si $U^\perp = U$. On dit alors que U est un métaboliseur de $T(R)$.

Si, de plus, R est un $\mathbb{Z}[G]$-réseau, alors le groupe G agit sur $T(R)$ et conserve la forme $\overline{b}$. Les $\mathbb{Z}[G]$-réseaux L vérifiant $R \subset L \subset R^*$ sont en bijection avec les sous-groupes U stables par G.

Une isométrie de R conserve nécessairement R^* ; d'où un homomorphisme du groupe des isométries de R dans celui des isométries de $(T(R), \overline{b})$. Deux réseaux L et L' intermédiaires entre R et R^* sont échangés par une isométrie f de R si et seulement si les sous-groupes U, U' de $T(R)$ correspondants sont échangés par l'isométrie de $T(R)$ induite par f. Il se peut par contre que L et L' soient isométriques sans qu'aucune isométrie entre eux ne stabilise R. Cette situation est évitée si, par exemple, R est un système de racines non plongeable dans aucun autre système de racines.

Exemple 1. — $R = R_1 \perp R_2$ avec $T(R_i) \simeq \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier impair. Alors la forme $\overline{b}$ est à valeurs dans $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$; on la remplace par $\overline{pb}$ qui est à valeurs dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi T(R) est un plan vectoriel sur le corps fini à p éléments muni d'une forme quadratique non dégénérée. Il y a alors soit aucun sous-espace isotrope non réduit à $\{0\}$, soit deux droites isotropes, échangées par l'image de l'isométrie de R donnée par : $x_1 + x_2 \mapsto x_1 - x_2$. Les deux réseaux unimodulaires définis par ces deux droites isotropes sont échangés par cette même isométrie.

Exemple 2. — Idéaux de $\mathbb{F}_p[G]$. Soit G un groupe cyclique d'ordre n impair. On pose $n = p^m r$ et on suppose que r divise $p - 1$. Nous aurons besoin d'une description des idéaux de $\mathbb{F}_p[G]$ totalement isotropes pour la forme $T_1(\lambda\overline{\lambda})$ (c'est-à-dire des idéaux sur lesquels la forme est nulle).

Posons $G = P \times C$ où P est d'ordre p^m et C est d'ordre r. On identifie l'algèbre $\mathbb{F}_p[G]$ avec le produit tensoriel sur $\mathbb{F}_p$ des algèbres $\mathbb{F}_p[P]$ et $\mathbb{F}_p[C]$.

Soit σ un générateur de P ; l'anneau $\mathbb{F}_p[P]$ est un anneau local, d'idéal maximal l'idéal d'augmentation

$$A = \left\{ \lambda = \sum_{g \in P} \lambda_g g \Big| \sum_{g \in P} \lambda_g = 0 \right\} = \mathbb{F}_p[P](1 - \sigma).$$

Les idéaux de $\mathbb{F}_p[P]$ sont les A^k pour $k = 0, 1, ..., p^m$. La dimension de A^k sur $\mathbb{F}_p$ est $m - k$.

Comme l'ordre de C est premier à p, l'anneau $\mathbb{F}_p[C]$ est semi-simple. Comme r divise $p-1$, les caractères de C sur une clôture algébrique de $\mathbb{F}_p$ sont à valeurs dans $\mathbb{F}_p$. On note $\hat{C}$ leur groupe. Alors

$$\mathbb{F}_p[C] = \bigoplus_{\theta \in \hat{C}} \mathbb{F}_p[C]e_\theta = \bigoplus_{\theta \in \hat{C}} \mathbb{F}_p e_\theta$$

et tout idéal de $\mathbb{F}_p[C]$ est la somme de certains $\mathbb{F}_p e_\theta$.

Le lemme suivant décrit les idéaux de $\mathbb{F}_p[G]$:

LEMME 2.1.

1) *Tout idéal de* $\mathbb{F}_p[G]$ *est de la forme :*

$$J = \bigoplus_{\theta \in \hat{C}} (A^{k_\theta} \otimes_{\mathbb{F}_p} \mathbb{F}_p e_\theta)$$

avec $k_\theta \in \{0, 1, ..., p^m\}$.

2) *L'idéal* J *est isotrope pour la forme standard* $T_1(\lambda\overline{\lambda})$ *si et seulement si :*

$$\begin{cases} k_1 & \geq \dfrac{p^m + 1}{2} \\ k_\theta + k_{\theta^{-1}} & \geq p^m \text{ pour tout } \theta \in \hat{C} - \{1\}. \end{cases}$$

3) *L'idéal* J *est isotrope et maximal pour l'inclusion si et seulement si les inégalités précédentes sont des égalités. Dans ce cas, sa dimension sur* $\mathbb{F}_p$ *est* $\dfrac{n-1}{2}$.

Démonstration. — Soit J un idéal de $\mathbb{F}_p[G]$. En tant que $\mathbb{F}_p[C]$-module, celui-ci est semi-simple. Donc $J = \bigoplus_{\theta \in \hat{C}} Je_\theta$. Fixons $\theta \in \hat{C}$; soit $p(J) = \{x \in \mathbb{F}_p[P] | x \otimes e_\theta \in J\}$. Alors $p(J)$ est un idéal de $\mathbb{F}_p[P]$ et $Je_\theta = p(J) \otimes \mathbb{F}_p e_\theta$. Comme $p(J)$ est une puissance de l'idéal d'augmentation A de $\mathbb{F}_p[P]$, on obtient l'expression de 1).

Comme le groupe G laisse la forme $T_1(\lambda\overline{\lambda})$ invariante, les sous-espaces Je_θ et $Je_{\theta'}$ sont orthogonaux si θ' est différent de θ^{-1}. Il est facile de voir que Je_θ et $Je_{\theta^{-1}}$ sont orthogonaux si et seulement si A^{k_θ} et $A^{k_{\theta^{-1}}}$ le sont,

et que l'orthogonal de A^k pour $T_1(\lambda\overline{\lambda})$ dans $\mathbb{F}_p[P]$ est A^{m-k}. On obtient alors les conditions de 2) et 3). □

2.2. Description de $T(\mathcal{I}_K)$; réduction à la situation locale.

Nous voulons décrire le $\mathbb{Z}[G]$-module de torsion $T(\mathcal{I}_K) = \mathcal{I}_K^*/\mathcal{I}_K$ muni de la forme induite par la forme $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$. Notons :

$$\mathcal{I}_K = \prod_{p\in\mathbb{P}} \Phi_K(p)^{t_p} \quad ; \quad \mathcal{A}_K = \prod_{p\in\mathbb{P}} \Phi_K(p)^{u_p} \quad ; \quad \mathcal{I}_K^* = \prod_{p\in\mathbb{P}} \Phi_K(p)^{s_p}$$

où $t_p = u_p + n_p$ avec les notations de la définition 1.2.

En tant que $\mathbb{Z}[G]$-module, $\mathcal{I}_K^*/\mathcal{I}_K \simeq \bigoplus_{p\in\mathbb{P}} (\Phi_K(p)^{s_p}/\Phi_K(p)^{t_p})$. Les termes de ce quotient correspondant à un nombre premier n'appartenant pas à $\mathbb{P}_s$ sont nuls. Chaque terme de cette somme directe est annulé par p : en effet, d'après la donnée de n_p, il est facile de vérifier que $p\Phi_K(p)^{s_p} \subset \Phi_K(p)^{t_p}$. De plus, cette somme est orthogonale pour la forme induite par la forme $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$, que nous noterons $\overline{T}(x,y)$: en effet, si p et q sont deux nombres premiers distincts de $\mathbb{P}$, on peut trouver une relation de Bezout $1 = pu + qv$. Alors, si x, y sont deux éléments de $T(\mathcal{I}_K)$ tels que $px = 0$ et $qy = 0$, on a : $\overline{T}(x,y) = (pu+qv)\overline{T}(x,y) = u\overline{T}(px,y) + v\overline{T}(x,qy) = 0$.

Comme le réseau $\mathcal{A}_K$ est unimodulaire, l'image de la racine carrée de la codifférente dans $T(\mathcal{I}_K)$ par la surjection canonique est un métaboliseur de $T(\mathcal{I}_K)$. On voit que celui-ci est la somme orthogonale de métaboliseurs des quotients $\Phi_K(p)^{s_p}/\Phi_K(p)^{t_p}$, qui sont les images de $\Phi_K(p)^{u_p}$.

Notations. — Pour tout nombre premier p appartenant à $\mathbb{P}_s$, on fixe un idéal $\mathfrak{P}$ de K au-dessus de p. Les notations $K_\mathfrak{P}$, $D_\mathfrak{P}$, $I_\mathfrak{P}$ désignent respectivement le complété de K en $\mathfrak{P}$, le groupe de décomposition et d'inertie en $\mathfrak{P}$. On définit de façon évidente les idéaux $\mathcal{A}_{K_\mathfrak{P}}$, $\mathcal{I}_{K_\mathfrak{P}}$ de $K_\mathfrak{P}$. Ce sont les complétés de $\mathcal{A}_K$, $\mathcal{I}_K$ en $\mathfrak{P}$. Ils sont naturellement munis d'une structure de $\mathbb{Z}_p[D_\mathfrak{P}]$-module hermitien pour la forme $\mathrm{Trace}_{K_\mathfrak{P}/\mathbb{Q}_p}(x^2)$. Le quotient $T(\mathcal{I}_{K_\mathfrak{P}}) = \mathcal{I}_{K_\mathfrak{P}}^*/\mathcal{I}_{K_\mathfrak{P}}$ est muni de la forme induite par la forme $\mathrm{Trace}_{K_\mathfrak{P}/\mathbb{Q}_p}(x^2)$ (à valeurs dans $\frac{1}{p}\mathbb{Z}_p/\mathbb{Z}_p = \frac{1}{p}\mathbb{Z}/\mathbb{Z}$).

Par ailleurs, soit k un corps, G un groupe et H un sous-groupe de G. Soit $(V, b(x,y))$ un $k[H]$-module hermitien. Soit $V' = V \underset{k[H]}{\otimes} k[G]$ le $k[G]$-module induit par V. Alors V' est muni d'une structure naturelle de

$k[G]$-module hermitien pour la forme $\tilde{b}(x,y)$ obtenue par linéarité à partir des formules suivantes : pour tout $g, g' \in G$ et pour tout $x, y \in V$

$$\tilde{b}(x \otimes g, y \otimes g') = \begin{cases} b(x, g'g^{-1}y) & \text{si } g'g^{-1} \in H \\ 0 & \text{si } g'g^{-1} \notin H. \end{cases}$$

Remarquons que, en tant qu'espace hermitien, $(V', \tilde{b})$ est la somme orthogonale de $[G : H]$ sous-espaces isométriques à V. Dans la suite, tout module induit d'un module hermitien est, sauf mention explicite d'une autre forme, muni de cette structure de $k[G]$-module hermitien. La forme $\tilde{b}$ est appelée forme induite de b.

PROPOSITION 2.2. — *Pour tout nombre premier p appartenant à $\mathbb{P}_s$, soit $\mathfrak{P}$ un idéal de K fixé au-dessus de p. Alors :*

$$T(\mathcal{I}_K) \sim_{\mathbb{Z}[G]} \bigoplus_{p \in \mathbb{P}_s} (T(\mathcal{I}_{K_\mathfrak{P}}) \otimes_{\mathbb{F}_p[D_\mathfrak{P}]} \mathbb{F}_p[G]).$$

Si s (respectivement s_p) est la surjection canonique $s : \mathcal{I}_K \to T(\mathcal{I}_K)$ (respectivement $s_p : \mathcal{I}_{K_\mathfrak{P}} \to T(\mathcal{I}_{K_\mathfrak{P}})$), alors par l'isomorphisme précédent :

$$s(\mathcal{A}_K) \sim_{\mathbb{Z}[G]} \bigoplus_{p \in \mathbb{P}_s} s_p(\mathcal{A}_{K_\mathfrak{P}}) \otimes_{\mathbb{F}_p[D_\mathfrak{P}]} \mathbb{F}_p[G].$$

Démonstration. — Fixons un nombre premier p appartenant à $\mathbb{P}_s$. On a une isométrie canoniquement définie de $\mathbb{Q}_p[G]$-modules hermitiens :

$$\alpha : K \otimes_\mathbb{Q} \mathbb{Q}_p \to K_\mathfrak{P} \otimes_{\mathbb{Q}_p[D]} \mathbb{Q}_p[G]$$

où $K \otimes \mathbb{Q}_p$ est muni de la forme $\mathbb{Q}_p$-linéaire déduite de $\mathrm{Trace}_{K/\mathbb{Q}}(x^2)$, et $K_\mathfrak{P} \otimes \mathbb{Q}_p[G]$ est muni de la forme $\tilde{\mathrm{Trace}}_{K_\mathfrak{P}/\mathbb{Q}_p}(x^2)$ décrite ci-dessus.

La restriction de α induit les $\mathbb{Z}_p[G]$-isométries de $\mathbb{Z}_p[G]$-modules hermitiens suivantes :

$$\begin{aligned} \alpha &: \mathcal{A}_K \otimes_\mathbb{Z} \mathbb{Z}_p \to \mathcal{A}_{K_\mathfrak{P}} \otimes_{\mathbb{Z}_p[D]} \mathbb{Z}_p[G] \\ \alpha &: \mathcal{I}_K^* \otimes_\mathbb{Z} \mathbb{Z}_p \to \mathcal{I}_{K_\mathfrak{P}}^* \otimes_{\mathbb{Z}_p[D]} \mathbb{Z}_p[G] \\ \alpha &: \mathcal{I}_K \otimes_\mathbb{Z} \mathbb{Z}_p \to \mathcal{I}_{K_\mathfrak{P}} \otimes_{\mathbb{Z}_p[D]} \mathbb{Z}_p[G]. \end{aligned}$$

Par passage au quotient on obtient :

$$\begin{aligned} \mathcal{I}_K^* \otimes_\mathbb{Z} \mathbb{Z}_p/\mathcal{I}_K \otimes_\mathbb{Z} \mathbb{Z}_p &\sim_{\mathbb{F}_p[G]} \mathcal{I}_{K_\mathfrak{P}}^*/\mathcal{I}_{K_\mathfrak{P}} \otimes_{\mathbb{F}_p[D]} \mathbb{F}_p[G] \\ \mathcal{A}_K \otimes_\mathbb{Z} \mathbb{Z}_p/\mathcal{I}_K \otimes_\mathbb{Z} \mathbb{Z}_p &\sim_{\mathbb{F}_p[G]} \mathcal{A}_{K_\mathfrak{P}}/\mathcal{I}_{K_\mathfrak{P}} \otimes_{\mathbb{F}_p[D]} \mathbb{F}_p[G] \end{aligned}$$

où les quotients sont munis des formes $\overline{T}$ correspondantes et les modules induits des formes induites. Cela termine la preuve. □

Remarque. — Par la proposition précédente, nous sommes ramenés à déterminer le métaboliseur de $T(\mathcal{I}_{K_\mathfrak{P}})$ correspondant à $\mathcal{A}_{K_\mathfrak{P}}$. C'est l'objet du paragraphe suivant.

3. Le métaboliseur de $T(\mathcal{I}_F)$ associé à la racine carrée de la codifférente dans le cas d'une extension F de $\mathbb{Q}_p$.

Dans ce paragraphe, F est une extension finie de $\mathbb{Q}_p$ galoisienne de groupe de Galois D et de degré impair. Le nombre premier p est impair (en effet on se restreint aux corps F qui sont des complétés de K aux places appartenant à $\mathbb{P}$, et même à $\mathbb{P}_s$). On note I le groupe d'inertie de l'extension. Celui-ci est d'ordre $e = p^m r$ avec r divisant $p-1$, et est cyclique. Soit, pour tout i tel que $0 \leq i \leq m$, P_i le sous-groupe de I d'ordre p^i et soit C le sous-groupe de I d'ordre r. Pour tout sous-groupe H de D, on pose $e_H = \dfrac{1}{|H|} \sum\limits_{h \in H} h$ avec la convention $e_{P_i} = 0$ si $i \geq m+1$.

L'idéal $\mathcal{A}_F$ est la racine carrée de la codifférente dans F ; l'idéal $\mathcal{I}_F$ est défini par : $\mathcal{I}_F = \mathfrak{P}^{n_p}\mathcal{A}_F$ où n_p est donné à la définition 1.2. Ce sont des $\mathbb{Z}_p[D]$-modules hermitiens pour la forme $\mathrm{Trace}_{F/\mathbb{Q}_p}(x^2)$. La forme induite par celle-ci sur le quotient $T(\mathcal{I}_F) = \mathcal{I}_F^*/\mathcal{I}_F$ est à valeurs dans $\dfrac{1}{p}\mathbb{Z}_p/\mathbb{Z}_p$ (on se restreint au cas où p appartient à $\mathbb{P}_s$; alors ce quotient est non nul et est annulé par p, voir paragraphe précédent) ; on obtient une forme à valeurs dans $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$ en la multipliant par p, que l'on note encore $\overline{T}$.

Le couple $(T(\mathcal{I}_F), \overline{T})$ est donc un $\mathbb{F}_p[D]$-module hermitien. Sa structure est décrite à la proposition 3.2.

3.1. Description de $(T(\mathcal{I}_F), \overline{T})$.

La localisation du résultat du théorème 1.7 montre que l'on a une $\mathbb{Z}_p[D]$-isométrie explicite :

$$(3) \qquad (\mathcal{I}_F^*, \mathrm{Trace}_{F/\mathbb{Q}_p}(x^2)) \sim_{\mathbb{Z}_p[D]} (\oplus_{0 \leq i \leq m} \mathbb{Z}_p[I](e_{P_i} - e_{P_{i+1}}), T_1(s\lambda\overline{\lambda})) \otimes_{\mathbb{Z}_p[I]} \mathbb{Z}_p[D]$$

$$\text{avec } s = \begin{cases} \displaystyle\sum_{0\le i\le m} p^i(e_{P_i} - e_{P_{i+1}}) & \text{si } m \equiv 0 \pmod 2 \\ \displaystyle\sum_{0\le i\le m-1} p^i(e_{P_i} - e_{P_{i+1}}) + p^m(e_{P_m} - e_I) + p^{m-1}e_I & \text{si } m \equiv 1 \pmod 2. \end{cases}$$

La proposition suivante décrit le $\mathbb{F}_p[D]$-module hermitien $(T(\mathcal{I}_F), \overline{T})$.

PROPOSITION 3.2.

$$(T(\mathcal{I}_F), \overline{T}) \sim_{\mathbb{F}_p[D]} \Big(\bigoplus_{1\le i\le m} (\mathbb{F}_p[I/P_i], -T_1(\lambda\overline{\lambda})) \oplus \Delta_p\Big) \otimes_{\mathbb{F}_p[I]} \mathbb{F}_p[D]$$

$$\text{avec } \Delta_p = \begin{cases} \{0\} & \text{si } m \equiv 0 \pmod 2 \\ (\mathbb{F}_p, x \mapsto -\dfrac{p-1}{r}x^2) & \text{si } m \equiv 1 \pmod 2. \end{cases}$$

Démonstration. — Pour tout sous-groupe H de I, notons s_H la surjection canonique : $s_H : I \to I/H$. Soit R un anneau quelconque, s_H s'étend par linéarité $s_H : R[I] \to R[I/H]$ et l'application suivante :

$$\begin{aligned} R[I]e_H &\to R[I/H] \\ \lambda e_H &\mapsto s_H(\lambda) \end{aligned} \tag{4}$$

est un isomorphisme de $R[I]$-modules, et même une isométrie si $R[I]$ est muni de $T_1(ae_H\lambda\overline{\lambda})$ et $R[I/H]$ de $\dfrac{1}{|H|}T_1(s_H(a)\lambda\overline{\lambda})$ (pour tout a appartenant à $Fr(R)[I]$).

Le terme Δ_p est la contribution du dernier terme de la somme orthogonale dans (3). Lorsque $m \equiv 0 \pmod 2$, celui-ci est $(\mathbb{Z}_p[I]e_{P_m}, T_1(e_{P_m}\lambda\overline{\lambda}))$ qui est par (4) $\mathbb{Z}_p[I]$-isométrique à $(\mathbb{Z}_p[I/P_m], T_1(\lambda\overline{\lambda}))$. Ce dernier réseau est unimodulaire, donc il donne $\{0\}$ dans $T(\mathcal{I}_F)$. Lorsque $m \equiv 1 \pmod 2$, ce dernier terme est $\mathbb{Z}_p[I]$-isométrique à

$$\Big(\mathbb{Z}_p[I/P_m], T_1\Big(\Big(\frac{1}{p}e_{I/P_m} + (1 - e_{I/P_m})\Big)\lambda\overline{\lambda}\Big)\Big).$$

Posons $J = I/P_m$; J est d'ordre r. Le dual de ce réseau est $((p-1)e_J+1)\mathbb{Z}_p[J]$. L'homomorphisme $\lambda \mapsto \sum_{g\in J} \lambda_g$ modulo p induit un isomorphisme :

$$\mathbb{Z}_p[J]/((p-1)e_J + 1)\mathbb{Z}_p[J] \to \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p.$$

De plus,

$$T_1\Big(\frac{1}{p}e_J + (1-e_J)\Big) = -\frac{p-1}{pr} + 1 = -\frac{p-1}{pr} \text{ modulo } \mathbb{Z}$$

donc la forme induite sur $\mathbb{F}_p$ (multipliée par p) est $x \mapsto -\dfrac{p-1}{r}x^2$ (rappelons que r divise $p-1$).

Il reste à examiner la contribution des termes $\mathbb{Z}_p[I](e_{P_i} - e_{P_{i+1}})$ pour $0 \leq i \leq m-1$. Grâce à (4), il suffit de considérer le cas $i = 0$, c'est-à-dire le $\mathbb{Z}_p[I]$-module hermitien $(\mathbb{Z}_p[I](1-e_{P_1}), T_1(\lambda\overline{\lambda}))$. Son dual est $\mathbb{Z}_p[I]^{(1-e_{P_1})}$. On vérifie que l'application :

$$\begin{aligned} \mathbb{Z}_p[I](1-e_{P_1}) &\to \mathbb{F}_p[I/P_1] \\ \lambda(1-e_{P_1}) &\mapsto \sum_{g\in I} s_p(\lambda_g)s_{P_1}(g) \end{aligned}$$

où s_p est la réduction modulo p, induit une $\mathbb{F}_p[I]$-isométrie du quotient

$$\mathbb{Z}_p[I](1-e_{P_1})/\mathbb{Z}_p[I]^{(1-e_{P_1})}$$

muni de la forme induite par $T_1(\lambda\overline{\lambda})$ (multipliée par p) sur $\mathbb{F}_p[I/P_1]$ muni de $-T_1(\lambda\overline{\lambda})$. □

Remarque. — Remarquons que la dimension de $T(\mathcal{I}_F)$ comme $\mathbb{F}_p$-espace vectoriel est paire. C'est une condition nécessaire pour l'existence d'un métaboliseur, qui est ici un sous-espace totalement isotrope maximal au sens de ([L], chapitre 1). Le sous-paragraphe suivant décrit celui qui est associé à $\mathcal{A}_F$.

3.2. L'image de $\mathcal{A}_F$ dans $T(\mathcal{I}_F)$.

On voit à la proposition 3.2 que la structure de $\mathbb{F}_p[D]$-module hermitien de $T(\mathcal{I}_F)$ ne dépend que de la ramification dans F. C'est aussi vrai plus généralement pour un corps global K.

Par contre, le métaboliseur de $T(\mathcal{I}_F)$ associé à $\mathcal{A}_F$ va dépendre de la nature du corps F, comme le montre le théorème 3.4, et ce pour les mêmes raisons qui faisaient que la structure de module sur l'ordre maximal de $\mathcal{A}_K$ ne dépendait pas uniquement de la ramification dans K ([Bu]).

Nous rappelons quelques notations de [Bu] : soit π une uniformisante de F. L'application :

$$C \to \overline{F}$$
$$g \mapsto g(\pi)/\pi$$

est un isomorphisme de C sur un sous-groupe de racines de l'unité du corps résiduel $\overline{F}$ de F, indépendant du choix de π ([S], chapitre IV). Soit $\hat{C}_{\text{loc}} = \text{Hom}(C, \overline{\mathbb{Q}}_p^*)$ le groupe des caractères locaux de C (en fait $\hat{C}_{\text{loc}} = \text{Hom}(C, \mathbb{Q}_p^*)$ car l'ordre de C divise $p-1$). Soit χ_F l'unique élément de $\hat{C}_{\text{loc}}$ induisant par passage au corps résiduel l'isomorphisme ci-dessus. Alors, pour tout caractère χ de $\hat{C}_{\text{loc}}$, il existe un entier u_χ défini modulo r tel que

$$\chi = \chi_F^{-u_\chi}.$$

Nous aurons besoin du lemme suivant :

LEMME 3.3.

(1) *Si i est pair et $0 \leq i \leq m$, alors le réseau $\mathcal{A}_F^{e_{P_i}}$ est unimodulaire. De façon équivalente, e_{P_i} appartient à l'ordre associé à $\mathcal{A}_F$.*

(2) *Si i est impair et $0 \leq i \leq m$, alors le réseau $\mathcal{A}_F^{e_{P_i}}$ est de discriminant p^f, où f est le degré résiduel de $F/\mathbb{Q}_p$.*

(3) *Pour tout caractère χ de $\hat{C}_{\text{loc}}$ et pour tout $1 \leq i \leq m$,*

$$[\mathcal{A}_F^{(e_{P_{i-1}} - e_{P_i})} e_\chi : \mathcal{I}_F^{(e_{P_{i-1}} - e_{P_i})} e_\chi] = \begin{cases} p^{f\frac{p^{m-i}+1}{2}} & \text{si } i \equiv 1 + \left[\frac{2u_\chi}{r}\right] \pmod 2 \\ p^{f\frac{p^{m-i}-1}{2}} & \text{si } i \equiv \left[\frac{2u_\chi}{r}\right] \pmod 2. \end{cases}$$

Démonstration. — Les points (1) et (2) s'établissent facilement : en effet, $\mathcal{A}_F^{e_{P_i}} = \mathcal{A}_F \cap F^{P_i}$ qui se calcule grâce à la formule de [U] rappelée dans la démonstration du lemme 1.10. Pour le point (3), on a :

$$[\mathcal{A}_F^{(e_{P_{i-1}} - e_{P_i})} e_\chi : \mathcal{I}_F^{(e_{P_{i-1}} - e_{P_i})} e_\chi] = \frac{[\mathcal{A}_F^{e_{P_{i-1}}} e_\chi : \mathcal{I}_F^{e_{P_{i-1}}} e_\chi]}{[\mathcal{A}_F^{e_{P_i}} e_\chi : \mathcal{I}_F^{e_{P_i}} e_\chi]}.$$

Ensuite, le calcul de $[\mathcal{A}_F^{e_{P_i}} e_\chi : \mathcal{I}_F^{e_{P_i}} e_\chi]$ est tout à fait analogue à celui du lemme 19 de [Bu]. Grâce aux expressions explicites de $\mathcal{A}_F$ et $\mathcal{I}_F$, on

calcule la valuation de $\mathcal{A}_F^{e_{P_i}} = \mathcal{A}_F \cap F^{P_i}$ et de $\mathcal{I}_F^{e_{P_i}} = \mathcal{I}_F \cap F^{P_i}$. Puis on utilise le lemme 15 de [Bu], exactement comme dans la démonstration du lemme 19. □

Nous sommes en mesure d'énoncer le théorème décrivant le métaboliseur de $T(\mathcal{I}_F)$ associé à $\mathcal{A}_F$.

THÉORÈME 3.4.

1) *L'image de $\mathcal{A}_F$ dans $(T(\mathcal{I}_F), \overline{T})$ par l'isomorphisme de la proposition 3.2 est de la forme $M \otimes_{\mathbb{F}_p[I]} \mathbb{F}_p[D]$, où M est un métaboliseur de $\bigoplus_{1\le i\le m} \mathbb{F}_p[I/P_i] \oplus \Delta_p$ stable par I, avec :*

(1) $M = \bigoplus_{1\le k\le\left[\frac{m+1}{2}\right]} M_{2k-1}$.

(2) *M_{2k-1} est un métaboliseur I-stable de $\mathbb{F}_p[I/P_{2k-1}] \oplus \mathbb{F}_p[I/P_{2k}]$ si $k < \dfrac{m+1}{2}$;*

M_m est un métaboliseur I-stable de $\mathbb{F}_p[I/P_m] \oplus \Delta_p$ si $m \equiv 1 \pmod 2$ et $k = \dfrac{m+1}{2}$.

(3) *M_{2k-1} est égal à l'un des deux métaboliseurs contenant la somme orthogonale $S_{2k-1} \oplus S_{2k}$, où, pour $m \equiv 1 \pmod 2$, $S_{m+1} = \{0\}$, et pour tout $i \le m$, S_i est l'idéal de $\mathbb{F}_p[I/P_i]$ totalement isotrope pour $-T_1(\lambda\overline{\lambda})$ donné par les formules suivantes :*

$$S_i = \bigoplus_{\overline{\theta}\in\hat{C}} (A_i^{k_{\overline{\theta},i}} \otimes_{\mathbb{F}_p} \mathbb{F}_p e_{\overline{\theta}})$$

avec

$$\begin{cases} k_{1,i} = \dfrac{p^{m-i}+1}{2} & \\ k_{\overline{\theta},i} = \dfrac{p^{m-i}+1}{2} & \text{si } i \equiv 1 + \left[\dfrac{2u_\theta}{r}\right] \pmod 2 \\ k_{\overline{\theta},i} = \dfrac{p^{m-i}-1}{2} & \text{si } i \equiv \left[\dfrac{2u_\theta}{r}\right] \pmod 2 \end{cases}$$

où les notations sont celles du lemme 2.1 ; A_i est l'idéal d'augmentation de $\mathbb{F}_p[P_m/P_i]$ et $\theta \mapsto \overline{\theta}$ est l'isomorphisme de $\hat{C}_{\text{loc}}$ sur $\hat{C}$ déduit du passage au corps résiduel.

2) *Le groupe des $\mathbb{Z}_p[D]$-isométries de $\mathcal{I}_F$ est transitif sur l'ensemble des métaboliseurs de $(T(\mathcal{I}_F), \overline{T})$ de la forme $M \otimes_{\mathbb{F}_p[I]} \mathbb{F}_p[D]$, et tels que M vérifie les propriétés (1), (2), (3).*

Démonstration. — On commence par établir le lemme suivant :

LEMME 3.5. — *Par la $\mathbb{Z}_p[D]$-isométrie (3), l'image de l'idéal $\mathcal{A}_F$ est de la forme*

$$R \underset{\mathbb{Z}_p[I]}{\otimes} \mathbb{Z}_p[D]$$

où R est un $\mathbb{Z}_p[I]$-module hermitien unimodulaire pour la forme $T_1(s\lambda\overline{\lambda})$.

Démonstration du lemme. — Reprenons la démonstration du théorème 1.7. On a défini un idéal $\mathcal{J}_L = \prod_{q \in \mathbb{P}} \mathcal{J}(q)$ de $L = \prod_{q \in \mathbb{P}} L_q$ tel que $\mathrm{Trace}_{L/K}(\mathcal{J}_L) = \mathcal{I}_K^*$. De même, on peut définir un idéal $\mathcal{B}_L = \prod_{q \in \mathbb{P}} \mathcal{B}(q)$ de L tel que $\mathrm{Trace}_{L/K}(\mathcal{B}_L) = \mathcal{A}_K$ avec $\mathcal{B}_L \subset \mathcal{J}_L$. Pour cela, on prend $\mathcal{B}(q) = \mathcal{J}(q)$ si $q \in \mathbb{P}_m \cup \mathbb{P}_{pr}$, et $\mathcal{B}(q) = \mathfrak{Q}^k$ avec $\left[\dfrac{k + v_{\mathfrak{Q}}(\mathcal{D}_{L/K})}{e_{L/K}(q)}\right] = v_{\mathfrak{Q} \cap K}(\mathcal{A}_K)$ ([U]), ce qui est toujours possible.

Soit $\mathfrak{P}$ l'idéal de K au-dessus de p tel que $F = K_{\mathfrak{P}}$. On choisit dans L un idéal $\mathfrak{p}$ au-dessus de $\mathfrak{P}$, et dans chaque L_q on considère $\mathfrak{p} \cap L_q$. La localisation respectivement en ces idéaux sera notée par des primes (donc $F = K'$). Alors on a : $\mathcal{J}'_L = \prod_{q \in \mathbb{P}} \mathcal{J}(q)'$ et $\mathcal{B}'_L = \prod_{q \in \mathbb{P}} \mathcal{B}(q)'$. Si $q \neq p$, alors L'_q est non ramifiée, et :

$$\mathcal{J}(q)' = \mathcal{B}(q)' = \mathbb{Z}_p[G_{L'_q}].t_q.$$

Si $q = p$, alors $\mathcal{J}(p)' = \Lambda.t_p$, avec :

$$\Lambda = \sum_{0 \leq i \leq m} \mathbb{Z}_p[G_{L'_p}](e_{P_i} - e_{P_{i+1}}),$$

et on peut poser $\mathcal{B}(p)' = M.t_p$ où M est un certain $\mathbb{Z}_p[G_{L'_p}]$-module inclus dans Λ.

Il vient alors :

$$\mathcal{J}'_L = \left(\sum_{0 \leq i \leq m} \mathbb{Z}_p[G_{L'_p}](e_{P_i} - e_{P_{i+1}}) \underset{\mathbb{Z}_p[G_{L'_p}]}{\otimes} \mathbb{Z}_p[G_{L'}] \right) .t_L$$

et

$$\mathcal{B}'_L = (M \underset{\mathbb{Z}_p[G_{L'_p}]}{\otimes} \mathbb{Z}_p[G_{L'}]).t_L.$$

En prenant la trace sur F, et compte tenu du fait que $G_{L'_p}$ est le groupe d'inertie de L', et donc que, si H est le groupe de Galois de L' sur F, alors $G_{L'_p}H/H = I$, on obtient :

$$\mathcal{I}_F^* = \left(\sum_{0 \leq i \leq m} \mathbb{Z}_p[I](e_{P_i} - e_{P_{i+1}}) \underset{\mathbb{Z}_p[I]}{\otimes} \mathbb{Z}_p[D] \right) .t_K$$

et

$$\mathcal{A}_F = (R \underset{\mathbb{Z}_p[I]}{\otimes} \mathbb{Z}_p[D]).t_K$$

pour un certain $\mathbb{Z}_p[I]$-module R. Par le lemme 1.1 (ou du moins sa version locale) on obtient le résultat. □

Démonstration du théorème. — Notons f la $\mathbb{Z}_p[D]$-isométrie (3). En posant $M = f(R)$, les lemmes 3.3 et 3.5 établissent le point (1) avec

$$M_{2k-1} \underset{\mathbb{F}_p[I]}{\otimes} \mathbb{F}_p[D] = f(\mathcal{A}_F^{e_{P_{2k-2}} - e_{P_{2k}}}).$$

En posant

$$S_i \underset{\mathbb{F}_p[I]}{\otimes} \mathbb{F}_p[D] = f(\mathcal{A}_F^{e_{P_{i-1}} - e_{P_i}}),$$

le point (2) du lemme 3.3 montre que S_i est un idéal de $\mathbb{F}_p[I/P_i]$ totalement isotrope pour $T_1(\lambda\overline{\lambda})$, et tel que $[S_i^\perp : S_i] = p$. Il est donc totalement isotrope et maximal pour l'inclusion; d'après le lemme 2.1, il existe des entiers $k_{\overline{\theta},i}$ tels que :

$$S_i = \underset{\overline{\theta} \in \hat{C}}{\oplus} (A_i^{k_{\overline{\theta},i}} \otimes_{\mathbb{F}_p} e_{\overline{\theta}}).$$

Supposons momentanément les entiers $k_{\overline{\theta},i}$ connus. Le quotient $S_{2k-1}^\perp \oplus S_{2k}^\perp / S_{2k-1} \oplus S_{2k}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, donc un métaboliseur M vérifiant

$$S_{2k-1} \oplus S_{2k} \subset M \subset S_{2k-1}^\perp \oplus S_{2k}^\perp$$

est de la forme : $M = S_{2k-1} \oplus S_{2k} + \mathbb{F}_p(x_{2k-1} + x_{2k})$, avec $x_i \in S_i^\perp$ et $T_1(x_{2k-1}\overline{x}_{2k-1}) + T_1(x_{2k}\overline{x}_{2k}) = 0$. On voit facilement que, si le couple

(x_{2k-1}, x_{2k}) est une solution, (et on sait qu'il y en a puisque M existe), alors toute autre solution conduit à $M = S_{2k-1} \oplus S_{2k} + \mathbb{F}_p(x_{2k-1} + x_{2k})$ ou à $M = S_{2k-1} \oplus S_{2k} + \mathbb{F}_p(x_{2k-1} - x_{2k})$.

Ces deux métaboliseurs sont échangés par toute $\mathbb{F}_p[D]$-isométrie de $T(\mathcal{I}_F)$ dont la restriction à $\mathbb{F}_p[I/P_{2k-1}] \oplus \mathbb{F}_p[I/P_{2k}]$ est : $x+y \mapsto x-y$ (ou $x+y \mapsto -x+y$).

Les $\mathbb{Z}_p[D]$-isométries de $\mathcal{I}_F^*$ définies par : $\sum_{0\le i\le m} x_i \mapsto \sum_{0\le i\le m} \epsilon_i x_i$ avec $\epsilon_i \in \{\pm 1\}$ dans la décomposition $\mathcal{I}_F^* \sim \bigoplus_{0\le i\le m} \mathbb{Z}_p[D](e_{P_i} - e_{P_{i+1}})$ forment un groupe isomorphe à $\{\pm 1\}^{m+1}$ et clairement transitif sur l'ensemble des métaboliseurs de $T(\mathcal{I}_F)$ de la forme $M = \bigoplus_{1\le k\le [\frac{m+1}{2}]} M_{2k-1}$ tels que M_{2k-1} vérifie la propriété énoncée en (3).

Pour terminer la démonstration du théorème 3.4, il suffit maintenant de calculer les entiers $k_{\overline{\theta},i}$. Remarquons que ceux-ci ne dépendent que de la structure de $\mathbb{F}_p[I]$-module de S_i. On a les isomorphismes de $\mathbb{F}_p[D]$-modules suivants :

$$\begin{aligned} S_i \otimes_{\mathbb{F}_p[I]} \mathbb{F}_p[D] &\simeq_{\mathbb{F}_p[D]} \mathcal{A}_F^{e_{P_{i-1}}-e_{P_i}}/\mathcal{I}_F^{e_{P_{i-1}}-e_{P_i}} \\ &\simeq_{\mathbb{F}_p[D]} \bigoplus_{\theta\in\hat{C}_{\mathrm{loc}}} \mathcal{A}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta / \bigoplus_{\theta\in\hat{C}_{\mathrm{loc}}} \mathcal{I}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta \\ &\simeq_{\mathbb{F}_p[D]} \bigoplus_{\overline{\theta}\in\hat{C}} (\mathcal{A}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta / \mathcal{I}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta) \end{aligned}$$

donc, pour tout $\overline{\theta} \in \hat{C}$,

$$S_i e_{\overline{\theta}} \underset{\mathbb{F}_p[I]}{\otimes} \mathbb{F}_p[D] \simeq_{\mathbb{F}_p[D]} \mathcal{A}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta / \mathcal{I}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta.$$

En particulier,

$$\mathrm{Card}(S_i e_{\overline{\theta}} \underset{\mathbb{F}_p[I]}{\otimes} \mathbb{F}_p[D]) = p^{f k_{\overline{\theta},i}} = [\mathcal{A}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta : \mathcal{I}_F^{e_{P_{i-1}}-e_{P_i}} e_\theta]$$

et cette dernière expression est donnée par le lemme 3.3. □

4. Le métaboliseur de $T(\mathcal{I}_K)$ associé à la racine carrée de la codifférente.

Dans ce paragraphe, nous déterminons le métaboliseur de $T(\mathcal{I}_K)$ associé à la racine carrée de la codifférente de K, aux $\mathbb{Z}[G]$-isométries de

$\mathcal{I}_K$ près. Nous utilisons les notations et les résultats des propositions 2.2 et 3.2 qui décrivent le couple $(T(\mathcal{I}_K), \overline{T})$.

THÉORÈME 4.1. — *Soit K une extension abélienne de degré impair de $\mathbb{Q}$. Pour tout nombre premier p, soit $\mathfrak{P}$ un idéal de K au-dessus de p; les notations $D_\mathfrak{P}$, $I_\mathfrak{P}$ désignent respectivement le groupe de décomposition et le groupe d'inertie en $\mathfrak{P}$.*

1) *Le métaboliseur $s(\mathcal{A}_K)$ appartient à l'ensemble des métaboliseurs de $(T(\mathcal{I}_K), \overline{T})$ de la forme :*

$$\bigoplus_{p\in\mathbb{P}_s} M(\mathfrak{P}) \underset{\mathbb{F}_p[I_\mathfrak{P}]}{\otimes} \mathbb{F}_p[G]$$

où $M(\mathfrak{P})$ est un métaboliseur de $\underset{1\le i\le m_p}{\oplus} \mathbb{F}_p[I_\mathfrak{P}/P_i] \oplus \Delta_p$ stable par $I_\mathfrak{P}$, et vérifiant les propriétés (1), (2), (3) du théorème 3.4 (appliqué à $F = K_\mathfrak{P}$).

2) *Le groupe des $\mathbb{Z}[G]$-isométries de $\mathcal{I}_K$ est transitif sur l'ensemble des métaboliseurs de $(T(\mathcal{I}_K), \overline{T})$ décrit en 1).*

Démonstration. — La première partie du théorème découle directement des propositions 2.2, 3.2, et du théorème 3.4. Il reste à montrer que le groupe des $\mathbb{Z}[G]$-isométries de $\mathcal{I}_K$ est transitif sur les métaboliseurs de $T(\mathcal{I}_K)$ ayant les propriétés (1), (2), (3). Soit

$$M = \bigoplus_{p\in\mathbb{P}_s} M(\mathfrak{P}) \underset{\mathbb{F}_p[I_\mathfrak{P}]}{\otimes} \mathbb{F}_p[G]$$

et

$$N = \bigoplus_{p\in\mathbb{P}_s} N(\mathfrak{P}) \underset{\mathbb{F}_p[I_\mathfrak{P}]}{\otimes} \mathbb{F}_p[G]$$

deux tels métaboliseurs. On a vu, dans la démonstration du théorème 3.4, que, pour tout p appartenant à $\mathbb{P}_s$, il existe $\epsilon_\mathfrak{P} \in \{\pm 1\}^{m_p+1}$ tel que l'isométrie $f_{\mathfrak{P},\epsilon_\mathfrak{P}}$ de $\mathcal{I}_{K_\mathfrak{P}}$ donnée par : $f_{\mathfrak{P},\epsilon_\mathfrak{P}}(\sum x_i) = \sum \epsilon_{\mathfrak{P},i} x_i$ dans la décomposition $\mathcal{I}_F^* \sim \underset{0\le i\le m}{\oplus} \mathbb{Z}_p[D_\mathfrak{P}](e_{P_i} - e_{P_{i+1}})$, échange $M(\mathfrak{P}) \underset{\mathbb{F}_p[I_\mathfrak{P}]}{\otimes} \mathbb{F}_p[D_\mathfrak{P}]$ et $N(\mathfrak{P}) \underset{\mathbb{F}_p[I_\mathfrak{P}]}{\otimes} \mathbb{F}_p[D_\mathfrak{P}]$.

Soit maintenant, avec les notations du paragraphe 1.7, l'élément f du sous-groupe Is des $\mathbb{Z}[G]$-isométries de $\mathcal{I}_K$ défini par $f = \prod_{p\in\mathbb{P}_s} f_{p,\epsilon_\mathfrak{P}}$. Nous allons montrer que, par localisation, f induit sur $\mathcal{I}_{K_\mathfrak{P}}$ une $\mathbb{Z}_p[D_\mathfrak{P}]$-isométrie de la forme : $x \mapsto u_\mathfrak{P} f_{\mathfrak{P},\epsilon_\mathfrak{P}}(x)$, où $u_\mathfrak{P}$ est une unité de $\mathbb{Z}_p[D_\mathfrak{P}]$.

Si cela est vrai, alors il est clair que, pour tout p, la localisation de f échange $M(\mathfrak{P}) \underset{\mathbb{F}_p[I_\mathfrak{P}]}{\otimes} \mathbb{F}_p[D_\mathfrak{P}]$ et $N(\mathfrak{P}) \underset{\mathbb{F}_p[I_\mathfrak{P}]}{\otimes} \mathbb{F}_p[D_\mathfrak{P}]$, et nous aurons terminé la démonstration.

Revenons donc à la construction de f du paragraphe 1.7. Cette $\mathbb{Z}[G]$-isométrie de $\mathcal{I}_K$ est en fait la restriction d'une $\mathbb{Z}[G_L]$-isométrie de $\mathcal{J}_L$, qui est le produit tensoriel de $\mathbb{Z}[G_{L_p}]$-isométries de $\mathcal{J}(p)$ (les $f_{p,\epsilon_\mathfrak{P}}$). Fixons un nombre premier p appartenant à $\mathbb{P}_s$, et localisons les extensions considérées au-dessus de p ; on note par des "primes" les localisés. Si q est différent de p, alors $\mathcal{J}(q)' \sim (\mathbb{Z}_p[G_{L'_q}], T_1(\lambda\overline{\lambda}))$ puisque L'_q est non ramifiée sur $\mathbb{Q}_p$, donc la localisation de f_{q,ϵ_Ω} ne peut être que de la forme $f_{q,\epsilon_\Omega}(x) = v_q x$, où v_q est une unité de $\mathbb{Z}_p[G_{L'_q}]$. Si $q = p$, alors $\mathcal{J}(p)' \sim \underset{0\leq i\leq m_p}{\oplus} \mathbb{Z}_p[G_{L'_p}](e_{P_i} - e_{P_{i+1}})$ et, dans cette décomposition, $f_{p,\epsilon_\mathfrak{P}}(\sum x_i) = \sum \epsilon_{\mathfrak{P},i} x_i$. Il est clair alors que la restriction de la localisation de f à $\mathcal{I}_{K_\mathfrak{B}}$ est bien de la forme annoncée. □

5. Questions de classes de $G_\mathbb{Q}$-isométries.

Dans ce paragraphe, on s'intéresse, lorsque K parcourt les extensions de $\mathbb{Q}$ abéliennes de degré impair, au problème de la comparaison des réseaux $(\mathcal{A}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$.

Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. On suppose les extensions de $\mathbb{Q}$ plongées dans $\overline{\mathbb{Q}}$. Soit $G_\mathbb{Q}$ le groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$. Alors, on peut considérer tout couple $(\mathcal{A}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x^2))$ comme un $\mathbb{Z}[G_\mathbb{Q}]$-réseau, et on se demande naturellement quand les racines carrées de la codifférente relatives à deux corps K et K' sont $\mathbb{Z}[G_\mathbb{Q}]$-isométriques. En fait, les résultats de cet article ne répondent à cette question que si l'on se restreint aux $\mathbb{Z}[G_\mathbb{Q}]$-isométries conservant les sous-réseaux $\mathcal{I}_K$, à moins que $\mathbb{P}_s(K)$ soit réduit à un seul nombre premier. Plus précisément :

THÉORÈME 5.1. — *Soit K et K' deux extensions abéliennes de degré impair de $\mathbb{Q}$ contenues dans $\overline{\mathbb{Q}}$, telles que* $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(K'/\mathbb{Q})$. *Il existe une $\mathbb{Z}[G_\mathbb{Q}]$-isométrie $f : \mathcal{A}_K \to \mathcal{A}_{K'}$, telle que $f(\mathcal{I}_K) = \mathcal{I}_{K'}$, si et seulement si :*

(1) $\mathbb{P}_s(K) = \mathbb{P}_s(K')$.

(2) *Pour tout nombre premier p appartenant à $\mathbb{P}_s$, $e_{K/\mathbb{Q}}(p) = e_{K'/\mathbb{Q}}(p)$.*

(3) *Pour tout nombre premier p appartenant à $\mathbb{P}_s$, tout idéal $\mathfrak{P}$ de K divisant p, et tout idéal $\mathfrak{P}'$ de K' divisant p, $\chi_{K_{\mathfrak{P}}} = \chi_{K'_{\mathfrak{P}'}}$ (notations du paragraphe 3.2).*

Si, de plus, $\mathbb{P}_s(K) = \{p\}$, et si p est différent de 3, alors toute $\mathbb{Z}[G_{\mathbb{Q}}]$-isométrie f de $\mathcal{A}_K$ sur $\mathcal{A}_{K'}$ est telle que $f(\mathcal{I}_K) = \mathcal{I}_{K'}$.

Démonstration. — Supposons que $\mathcal{A}_K$ et $\mathcal{A}_{K'}$ soient $\mathbb{Z}[G_{\mathbb{Q}}]$-isométriques, et que, par cette isométrie, l'image de $\mathcal{I}_K$ soit $\mathcal{I}_{K'}$. En particulier, $\mathcal{I}_K$ et $\mathcal{I}_{K'}$ sont isométriques, donc leurs discriminants sont égaux. En utilisant la proposition 1.2, on voit facilement que cela est équivalent aux conditions suivantes : $\mathbb{P}_s(K) = \mathbb{P}_s(K')$, $\mathbb{P}_{s,0}(K) = \mathbb{P}_{s,0}(K')$, $\mathbb{P}_{s,1}(K) = \mathbb{P}_{s,1}(K')$, et, si $e_{K/\mathbb{Q}}(p) = r_p(K)p^{m_p(K)}$, alors $e_{K/\mathbb{Q}}(p) = e_{K'/\mathbb{Q}}(p)$ si $p \in \mathbb{P}_{s,1}$ et $m_p(K) = m_p(K')$ si $p \in \mathbb{P}_{s,0}$.

De plus, pour tout $p \in \mathbb{P}_{s,0}$, et tout $0 \leq i \leq m_p$, les $\mathbb{Z}_p[G_{\mathbb{Q}}]$-réseaux $\mathbb{Z}_p \otimes \mathcal{A}_K^{e_{P_i}}$ et $\mathbb{Z}_p \otimes \mathcal{A}_{K'}^{e_{P_i}}$ sont isométriques. Le lemme 3.3(2) montre que cela implique $r_p(K) = r_p(K')$, ce qui complète les conditions (1) et (2) du théorème.

Réciproquement, si (1) et (2) sont réalisées, alors le théorème 1.7 décrivant la structure de $\mathcal{I}_K$ montre que $\mathcal{I}_K$ et $\mathcal{I}_{K'}$ sont $\mathbb{Z}[G_{\mathbb{Q}}]$-isométriques. Identifions ces deux réseaux via l'isométrie, en un même réseau $\mathcal{I}$. S'il existe une $\mathbb{Z}[G_{\mathbb{Q}}]$-isométrie de $\mathcal{I}$ transformant $\mathcal{A}_K$ en $\mathcal{A}_{K'}$, alors les images respectivement de $\mathcal{A}_K$ et $\mathcal{A}_{K'}$ dans $T(\mathcal{I})$ sont en particulier $\mathbb{F}_p[G_{\mathbb{Q}}]$-isomorphes. Ceci est équivalent à ce que les idéaux S_i du théorème 3.4 associés respectivement à K et K' soient $\mathbb{F}_p[G_{\mathbb{Q}}]$-isomorphes, ou encore à ce que les entiers $k_{\overline{\theta},i}$ respectifs soient égaux (en effet, ces entiers donnent les dimensions sur $\mathbb{F}_p$ de $S_i e_{\overline{\theta}}$, donc sont des invariants de la classe de $\mathbb{F}_p[G_{\mathbb{Q}}]$-isomorphisme des S_i). L'égalité de ces entiers est équivalente à la condition (3) du théorème (on peut remarquer que, comme r_p divise $p-1$, l'élément $\chi_{K_{\mathfrak{P}}}$ ne dépend pas du choix de l'idéal $\mathfrak{P}$ de K au-dessus de p).

Réciproquement, si (3) est réalisée, alors les S_i associés à K et K' sont égaux, et les réseaux $\mathcal{A}_K$ et $\mathcal{A}_{K'}$ sont $\mathbb{Z}[G_{\mathbb{Q}}]$-isométriques d'après le théorème 4.1.

Finalement, supposons que $\mathbb{P}_s(K) = \{p\}$, et soit f une $\mathbb{Z}[G_{\mathbb{Q}}]$-isométrie de $\mathcal{A}_K$ sur $\mathcal{A}_{K'}$. Alors, on a vu précédemment que $\mathbb{P}_s(K') = \{p\}$. Le point 2) de l'exemple 1.9 montre que, si p est différent de 3, alors $\mathcal{I}_K$ est égal à la somme orthogonale de $\mathcal{A}_K^{e_{P_{m_p}}}$ et du système de racines de $\mathcal{A}_K^{1-e_{P_{m_p}}}$. Comme f est une $\mathbb{Z}[G_{\mathbb{Q}}]$-isométrie, l'image par f de $\mathcal{A}_K^{e_{P_{m_p}}}$ est

$\mathcal{A}_{K'}^{e_{P_{m_p}}}$, et l'image par f du système de racines de $\mathcal{A}_K^{1-e_{P_{m_p}}}$ est égal au système de racines de $\mathcal{A}_{K'}^{1-e_{P_{m_p}}}$. L'image par f de $\mathcal{I}_K$ est donc $\mathcal{I}_{K'}$. □

BIBLIOGRAPHIE

[B] C. BACHOC, Sur les réseaux unimodulaires pour la forme Trace(x^2), Séminaire de Théorie des Nombres de Paris, 1988-1989.

[BE] C. BACHOC et B. EREZ, Forme Trace et ramification sauvage, Proc. London Math. Soc., (3) 61 (1990), 209-226.

[Ba] E. BAYER-FLUCKIGER, Réseaux unimodulaires, Séminaire de Théorie des Nombres de Bordeaux, 3 (1991), 189-196.

[Bu] D. BURNS, On the Galois structure of the square root of the codifférent, Séminaire de Théorie des Nombres, Bordeaux, 3 (1991), 73-92.

[CS] J.H. CONWAY, N.J.A. SLOANE, Sphere Packings, Lattices and Groups, Springer-Verlag, New-York Inc., 1988.

[E1] B. EREZ, Structure galoisienne et forme trace dans les corps de nombres, Thèse, Université de Genève (1987).

[E2] B. EREZ, The Galois structure of the trace form in extensions of odd prime degree, J. Algebra, 118 (1988), 438-446.

[La] T.Y. LAM, The Algebraic Theory of Quadratic Forms, The Benjamin/Cummings publishing company inc., 1973.

[L] H.-W. LEOPOLDT, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math., 201 (1959), 119-149.

[Le] G. LETTL, The ring of integers of an abelian number field, J. reine angew. Math., 404 (1990), 171-188.

[U] S. ULLOM, Normal bases in Galois extensions of number fields, Nagoya Math. J., 34 (1969), 153-167.

[S] J.-P. SERRE, Corps locaux, Hermann, Paris, 3e éd, 1980.

Manuscrit reçu le 22 janvier 1992,
révisé le 23 novembre 1992.

Christine BACHOC,
Laboratoire de Mathématiques de Bordeaux
351, cours de la Libération
F-33405 Talence.