ILLINOIS JOURNAL OF MATHEMATICS
Volume 43, Number 1, Spring 1999

CLASSES DE STEINITZ D'EXTENSIONS GALOISIENNES RELATIVES DE DEGRÉ UNE PUISSANCE DE 2 ET PROBLÈME DE PLONGEMENT

BOUCHAÏB SODAÏGUI

ABSTRACT. Soit k un corps de nombres. L'objectif de cet article est double. D'une part, on étudie l'ensemble des éléments du groupe des classes de k qui sont réalisables par les classes de Steinitz des extensions galoisiennes de k qui sont modérément ramifiées et dont le groupe de Galois est d'ordre 4 ou quaternionien d'ordre 8. D'autre part, on décrit l'ensemble des classes de Steinitz des extensions quadratiques (resp. biquadratiques) de k qui sont plongeables dans des extensions cycliques de degré 4 (resp. quaternioniennes de degré 8), sous l'hypothèse de la ramification modérée.

1. Introduction et énoncé des principaux résultats

Soient k un corps de nombres, O_k son anneau d'entiers, N/k une extension de degré n et O_N son anneau d'entiers. L'anneau O_N est un O_k-module sans torsion de rang n, donc il existe un idéal I de O_k tel que $O_N \simeq O_k^{n-1} \oplus I$ en tant que O_k-module. La classe de I dans le groupe $Cl(k)$ des classes de k est appelée la classe de Steinitz de l'extension N/k ou de l'anneau O_N, et on la note $Cl(O_N)$.

Soit Γ un groupe fini. On désigne par $\mathcal{R}(O_k)$ l'ensemble des éléments c de $Cl(k)$ tels qu'il existe une extension N/k galoisienne, modérement ramifiée, à groupe de Galois isomorphe à Γ avec $c = Cl(O_N)$; on dira que c est réalisable par la classe de Steinitz de N/k.

Lorsque Γ est cyclique d'ordre ℓ^r, ℓ premier impair et $r \geq 1$, Long ([L1], [L2]) a montré que $\mathcal{R}(O_k)$ est le sous-groupe de $Cl(k)$ égal à $W^{\frac{\ell-1}{2}} = \{c^{\frac{\ell-1}{2}} | c \in W\}$, où si ξ_ℓ est une racine primitive $\ell^{\text{ième}}$ de l'unité, W est la norme dans $k(\xi_\ell)/k$ du groupe de classes de $k(\xi_\ell)$. Signalons aussi un travail récent de Carter [Ca], où il montre que $\mathcal{R}(O_k)$ est un groupe dans le cas où Γ est un groupe non abélien d'ordre ℓ^3, ℓ premier impair, et k contient les racines $m^{\text{ième}}$ de l'unité, où m est l'exposant de Γ. Lorsque Γ est d'ordre 2, d'après [F1] ou ([So1], Th. 2.4), $\mathcal{R}(O_k) = Cl(k)$.

L'objectif de cet article est le suivant: d'une part, on étudie $\mathcal{R}(O_k)$ lorsque Γ est un 2-groupe dans les cas où Γ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ou $\mathbb{Z}/4\mathbb{Z}$, ou à H_8 le groupe quaternionien d'ordre 8; d'autre part, on décrit l'ensemble des classes de Steinitz des extensions quadratiques (resp. biquadratiques) de k qui sont plongeables dans des extensions cycliques de degré 4 (resp. quaternioniennes de degré 8), sous l'hypothèse de la ramification modérée.

Les principaux résultats sont les suivants.

Received May 20, 1997.
1991 Mathematics Subject Classification. Primary 11R33, 11R04.

THÉORÈME 1.1. *Soit k un corps de nombres. Alors:*

(*i*) *L'ensemble des classes de Steinitz des extensions biquadratiques de k (resp. cycliques de degré 4 avec le nombre de classes de k impair), modérément ramifiées, est égal au groupe $Cl(k)$.*
(*ii*) *Si le nombre de classes de k est impair alors l'ensemble des classes de Steinitz des extensions quaternioniennes de degré 8 sur k, modérément ramifiées, est égal au groupe $Cl(k)$.*

Remarque. Dans le cas biquadratique, le (i) est un cas particulier de [L3, Th. 3, p. 15]. Dans le cas cyclique on peut déduire (i) de [E, 2.6, p. 41]. Dans cet article la preuve est différente et plus courte.

THÉORÈME 1.2. *Soient k un corps de nombres et ξ_4 une racine primitive $4^{\text{ième}}$ de l'unité. Alors, l'ensemble des éléments de $Cl(k)$ réalisables par des classes de Steinitz d'extensions quadratiques (resp. biquadratiques avec $\xi_4 \in k$ ou $k(\xi_4)/k$ ramifiée) K de k, modérement ramifiées, et plongeables dans des extensions N/k cycliques de degré 4 (resp. quaternioniennes de degré 8), modérement ramifiées, est un groupe égal à $Cl(k)$.*

Soit $\mathcal{M}$ un ordre maximal de O_k dans l'algèbre semi-simple $k[\Gamma]$ tel que $O_k[\Gamma] \subset \mathcal{M}$. Si N/k est modérément ramifiée, à groupe de Galois isomorphe à Γ, alors par extension des scalaires on peut associer à O_N une classe dans $Cl(\mathcal{M})$ le groupe de classes de $\mathcal{M}$ (cf. [F3]), on désigne par $\mathcal{R}(\mathcal{M})$ le sous-ensemble de $Cl(\mathcal{M})$ formé par de telles classes. En utilisant le lien entre les classes de Steinitz et $\mathcal{R}(\mathcal{M})$ lorsque Γ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, on démontre:

THÉORÈME 1.3. *Si Γ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, alors $\mathcal{R}(\mathcal{M})$ est un groupe isomorphe au groupe produit $Cl(k) \times Cl(k) \times Cl(k)$.*

Remarque. L'une des motivations de cet article est l'étude de $\mathcal{R}(\mathcal{M})$ lorsque $\Gamma \simeq H_8$; ce qui justifie (en partie) l'hypothèse de la ramification modérée, l'intérêt particulier porté aux extensions quaternioniennes de degré 8, et aux extensions biquadratiques ou cycliques de degré 4, ces deux dernières pouvant être des sous-corps des premières. Pour le problème de l'étude de $\mathcal{R}(\mathcal{M})$ avec Γ quelconque, voir [Mc1], [Mc2], [So1], [So2]; on pourrait voir le Théorème 1.3 comme une illustration des méthodes utilisées pour l'aborder.

2. Préliminaires

Dans cette section, on donne les notations et quelques résultats qui seront utilisés pour la démonstration des théorèmes du paragraphe 1.

Pour tout corps de nombres F, on note O_F l'anneau d'entiers de F. Si $\mathfrak{p}$ est un idéal premier de O_F, $v_\mathfrak{p}$ désigne la valuation en $\mathfrak{p}$.

Pour tout idéal premier $\mathfrak{p}$ de O_F et $a \in F^\times$ tels que $v_\mathfrak{p}(a) = 0$, $(\frac{a}{\mathfrak{p}})$ désigne le symbole de Legendre généralisé.

Soient v une place de F, et $a, b \in F^\times$, $(a, b)_v$ et le symbole local (de Hilbert) (cf. [Se1], chap. XIV, cas n=2).

Soit C un cycle de k, $Cl(k, C)$ désigne le groupe de classes de rayon modulo C (cf. [N1], p. 98); lorsque $C = O_k$, on note simplement $Cl(k)$, c'est le groupe de classes de k; la classe d'un idéal fractionnaire I de O_k dans $Cl(k, C)$ est notée $Cl(I)$. Le cycle $\prod_{\sigma(k)\subset\mathbb{R}} \sigma$, où σ est un plongement de k, est noté C_∞. On rappelle la notation de la congruence mod* usuelle de la théorie du corps de classes: soient le cycle $C = C_0C_1$, où C_0 divise C_∞ et C_1 est un idéal entier de O_F, et $a \in F^\times$, alors $a \equiv 1 \bmod^*(C)$ si et seulement si, pour tout $\sigma|C_0$ on a $\sigma(a) > 0$ et pour tout $\mathfrak{p}|C_1$ on a $v_\mathfrak{p}(a-1) \geq v_\mathfrak{p}(C_1)$.

Soit G/F une extension de degré fini. On note $\Delta(G/F)$ (resp. $\mathcal{D}(G/F)$, resp. $N_{G/F}$, resp. $\mathrm{Tr}_{G/F}$) le discriminant relatif par rapport à la forme trace (resp. la différente, resp. la norme, resp. la trace) de G/F.

La classe de Steinitz de G/F est notée $Cl_F(O_G)$, ou, simplement $Cl(O_G)$ si aucune confusion n'est possible.

On rappelle que G/F est dite modérément ramifiée, ou, plus simplement, modérée, si et seulement si, pour tout idéal premier $\mathfrak{p}$ de O_G, l'indice de ramification de $\mathfrak{p}$ dans G/F est premier à la caractéristique du corps résiduel $O_G/\mathfrak{p}$; dans ce cas, si H est un sous-corps de G qui contient F, alors les extensions G/H et H/F sont modérées.

Dans les paragraphes suivants, on ne considérera que le cas où G/F est galoisienne et $\mathrm{Gal}(G/F)$ est un 2-groupe, donc G/F est modérée si et seulement si les idéaux premiers de O_F au dessus de 2 ne sont pas ramifiés dans G/F.

Soient G/F une extension galoisienne finie, χ un caractère de $\mathrm{Gal}(G/F)$, $f(\chi, G/F)$ désignera le conducteur d'Artin de χ. Rappelons que la décomposition d'Artin du discriminant en un produit de conducteurs est: $\Delta(G/F) = \prod f(\chi, G/F)^{\chi(1)}$, où χ parcourt l'ensemble des caractères irréductibles de $\mathrm{Gal}(G/F)$ (cf. [Se1], Chap. VI, Cor. 2, p. 112).

La notion de résolvante de Lagrange est fondamentale pour la démonstration du Théorème 1.3, en voici une définition dans le cas qui nous intéresse: soient G/F une extension galoisienne, χ un caractère de degré 1 de $\mathrm{Gal}(G/F)$ et $b \in G$; on appelle résolvante de Lagrange de b et de χ l'élément noté $\langle b, \chi\rangle$, ou $\langle b, \chi\rangle_{G/F}$ si l'on veut préciser l'extension G/F, défini par: $\langle b, \chi\rangle = \sum_{\sigma\in\mathrm{Gal}(G/F)} \chi(\sigma^{-1})\sigma(b)$.

Les deux propositions qui suivent seront souvent utilisées.

PROPOSITION 2.1. *Soient F, G, H des corps de nombres tels que $F \subset G \subset H$, et $[H : G]$ le degré de H/G. Alors*:

(*i*) $\Delta(H/F) = \Delta(G/F)^{[H:G]} N_{G/F}(\Delta(H/G))$.
(*ii*) $Cl_F(O_H) = Cl_F(O_G)^{[H:G]} N_{G/F}(Cl_G(O_H))$.

Démonstration. L'assertion (i) est bien connue, elle résulte de la transitivité de la différente (cf. [FT], Chap. III, Prop. 2.15, p. 126). L'assertion (ii) est le Théorème 4.1 de [F1].

On rappelle la proposition suivante (cf. [MS], Prop. 1.2 et [H], §39) dont la démonstration découle immédiatement de la théorie de Kummer, et la notion d'invariant relatif de deux réseaux (cf. [Se1], Chap. III, §1 et §2).

PROPOSITION 2.2. *Soient G/F une extension quadratique et $m \in F$ tel que $G = F(\sqrt{m})$.*

(*a*) *G/F est modérément ramifiée si et seulement si on peut choisir $m \equiv 1 \, mod^*$ $(4O_k)$.*

(*b*) *On suppose que G/F est modérément ramifiée. Alors*:

  (i) *On peut écrire d'une manière unique $mO_F = I(m)^2 J$, où $I(m)$ est un idéal fractionnaire de O_F, et J est un idéal entier de O_F sans facteur carré.*

  (ii) *On a $\Delta(G/F) = J$.*

  (iii) *La classe de Steinitz de O_G est égale à la classe de l'idéal $I(m)^{-1}$ dans le groupe de classes de F*:

$$Cl_F(O_G) = Cl(I(m)^{-1}).$$

3. Classes de Steinitz d'extensions biquadratiques

Dans cette section on suppose que Γ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Soient N/k une extension galoisienne modérée à groupe de Galois isomorphe à Γ, et k_i/k, $1 \leq i \leq 3$, ses trois sous-corps quadratiques.

Pour alléger les notations, on pose: $\Delta = \Delta(N/k)$, $\Delta_i = \Delta(k_i/k)$ pour tout i, $1 \leq i \leq 3$, et $(\Delta_1, \Delta_2) = PGCD(\Delta_1, \Delta_2)$; $Cl_k(O_N) = Cl(O_N)$ et $Cl_k(O_{k_i}) = Cl(O_{k_i})$.

La proposition suivante précise les discriminants des différentes sous-extensions de N.

PROPOSITION 3.1. *Sous les hypothèses et notations précédentes, on a*:

(1) $\Delta = \Delta_1\Delta_2\Delta_3$.
(2) $\Delta_3 = \Delta_1\Delta_2(\Delta_1, \Delta_2)^{-2}$.
(3) $\Delta(N/k_1) = \Delta_2(\Delta_1, \Delta_2)^{-1}O_{k_1}$, $\Delta(N/k_2) = \Delta_1(\Delta_1, \Delta_2)^{-1}O_{k_2}$, $\Delta(N/k_3) = (\Delta_1, \Delta_2)O_{k_3}$.

Démonstration. (1) Le groupe $\mathrm{Gal}(N/k)$ possède trois caractères irréductibles non triviaux χ_i, $1 \leq i \leq 3$, de degré 1 qui proviennent de caractères de $\mathrm{Gal}(N/k)/\mathrm{Gal}$

(N/k_i) qui est isomorphe à $\mathrm{Gal}(k_i/k)$. Donc, la décomposition d'Artin du discriminant $\Delta(N/k)$ est: $\Delta(N/k) = \prod_{i=1}^{3} f(\chi_i, N/k)$, et $f(\chi_i, N/k) = f(\chi_i, k_i/k)$ (cf. [Se1], Chap. VI, §3, Prop. 6 (c), p. 111) où l'on a considéré χ_i comme caractère de $\mathrm{Gal}(k_i/k)$. On a alors (1) car $\Delta_i = f(\chi_i, k_i/k)$.

(2) Soient m_i, $1 \leq i \leq 2$, des éléments de k tels que $k_i = k(\sqrt{m_i})$; il est clair que $k_3 = k(\sqrt{m_1 m_2})$, et les extensions k_i/k, $1 \leq i \leq 3$, sont modérées car N/k est modérée. Pour $i = 1, 2$, écrivons $m_i O_k = I(m_i)^2 \Delta_i$, alors $m_1 m_2 O_k = (I(m_1) I(m_2)(\Delta_1, \Delta_2))^2 \Delta_1 \Delta_2 (\Delta_1, \Delta_2)^{-2}$; d'où (2) par la Proposition 2.2 ((i) et (ii)) puisque $\Delta_1 \Delta_2 (\Delta_1, \Delta_2)^{-2}$ est un idéal entier de O_k sans facteur carré.

(3) D'après le (i) de la Proposition 2.1, $\Delta = \Delta_1^2 N_{k_1/k}(\Delta(N/k_1))$. En utilisant (1) et (2) on obtient

$$(\Delta_2(\Delta_1, \Delta_2)^{-1})^2 = N_{k_1/k}(\Delta(N/k_1)),$$

par conséquent $\Delta(N/k_1) = \Delta_2(\Delta_1, \Delta_2)^{-1} O_{k_1}$. De la même manière, on démontre les deux assertions qui restent.

PROPOSITION 3.2. *Avec les hypothèses et notations de la Proposition* 3.1, *on a*:

(1) $Cl(O_{k_3}) = Cl(O_{k_1}) Cl(O_{k_2}) Cl((\Delta_1, \Delta_2))^{-1}$.
(2) $Cl(O_N) = \prod_{i=1}^{3} Cl(O_{k_i}) = Cl(\Delta_1 \Delta_2 (\Delta_1, \Delta_2)^{-1})$.

Démonstration. (1) D'après la démonstration de (2) de la proposition précédente et le (iii) de la Proposition 2.2, $Cl(O_{k_3}) = Cl((I(m_1) I(m_2)(\Delta_1, \Delta_2)^{-1})$ et pour $i = 1, 2, Cl(I(m_i)^{-1}) = Cl(O_{k_i})$, d'où (1).

(2) On a $Cl(O_N) = Cl(O_{k_1})^2 N_{k_1/k}(Cl_{k_1}(O_N))$ par le (ii) de la Proposition 2.1. Il est clair que $N = k_1(\sqrt{m_2})$. Considérons la décomposition $m_2 O_k = I(m_2)^2 \Delta_2$ et posons $(\Delta_1, \Delta_2) O_{k_1} = I'^2$, d'où $m_2 O_{k_1} = (I(m_2) I')^2 \Delta_2 (\Delta_1, \Delta_2)^{-1} O_{k_1}$. Comme $\Delta(N/k_1) = \Delta_2(\Delta_1, \Delta_2)^{-1} O_{k_1}$ (Proposition 3.1 (3)), $Cl_{k_1}(O_N) = Cl((I(m_2) O_{k_1} I')^{-1})$ dans $Cl(k_1)$ (Proposition 2.2 (iii)). De $N_{k_1/k}(I') = (\Delta_1, \Delta_2)$ et $Cl(O_{k_2}) = Cl(I(m_2)^{-1})$ on déduit que $N_{k_1/k}(Cl_{k_1}(O_N)) = Cl(O_{k_2})^2 Cl((\Delta_1, \Delta_2)^{-1})$. Donc, $Cl(O_N) = Cl(O_{k_1})^2 Cl(O_{k_2})^2 Cl((\Delta_1, \Delta_2)^{-1})$, d'où la première égalité de (2) par (1), pour la seconde il suffit de remarquer que $Cl(O_{k_i})^2 = \Delta_i$.

THÉORÈME 3.3. *Soient k un corps de nombres*, $(c_1, c_2, c_3) \in Cl(k)^3$. *Alors, il existe trois extensions k_i/k*, $1 \leq i \leq 3$, *quadratiques modérées, telles que*:

(1) *Pour tout i*, $1 \leq i \leq 3$, $Cl(O_{k_i}) = c_i$.
(2) *La composée des extensions k_i*, $1 \leq i \leq 3$, *est une extension N/k biquadratique modérée.*

Démonstration. En vertu du théorème de densité généralisé de Dirichlet (cf. [N1], Th. 6.2, p. 131), on a les assertions suivantes.

Il existe un idéal premier $\mathfrak{p}$ de O_k ne divisant pas $2O_k$ tel que: $c_1c_2c_3^{-1} = Cl(\mathfrak{p})$ dans $Cl(k)$.

Pour un tel $\mathfrak{p}$, il existe un idéal premier $\mathfrak{p}'$ de O_k ne divisant pas $4O_k$ tel que

(a) $c_1^{-2}Cl(\mathfrak{p})Cl(\mathfrak{p}') = 1$ dans $Cl(k, 4O_k)$.

Pour de tels $\mathfrak{p}$ et $\mathfrak{p}'$, il existe un idéal premier $\mathfrak{p}''$ de O_k ne divisant pas $4\mathfrak{p}'$ tel que

(b) $c_2^{-2}Cl(\mathfrak{p})Cl(\mathfrak{p}'') = 1$ dans $Cl(k, 4\mathfrak{p}')$.

Les assertions (a) et (b) se traduisant de la façon suivante: il existe $m_1, m_2 \in k^\times$ et deux idéaux fractionnaires $I(m_1)$, $I(m_2)$ de O_k tels que

$$m_1O_k = I(m_1)^2\mathfrak{p}\mathfrak{p}',\ m_1 \equiv 1\ mod^*(4O_k), \text{et}\ Cl(I(m_1)^{-1}) = c_1,$$
$$m_2O_k = I(m_2)^2\mathfrak{p}\mathfrak{p}'',\ m_2 \equiv 1\ mod^*(4\mathfrak{p}'), \text{et}\ Cl(I(m_2)^{-1}) = c_2.$$

Les extensions $k_i = k(\sqrt{m_i})/k$, $1 \leq i \leq 2$, sont quadratiques, en effet, $v_\mathfrak{p}(m_i) \equiv 1$ mod(2), par suite les m_i ne peuvent être des carrés dans k. Grâce à la Proposition 2.2, on voit qu'elles sont modérées, de discriminants respectifs $\mathfrak{p}\mathfrak{p}'$ et $\mathfrak{p}\mathfrak{p}''$ d'où $k_1 \neq k_2$ car $\mathfrak{p}' \neq \mathfrak{p}''$, et de classes de Steinitz respectives c_1 et c_2. La composée $N = k_1k_2/k$ est donc une extension biquadratique modérée; soit k_3/k sa troisième sous-extension quadratique, le (1) de la Proposition 3.2 nous affirme que $Cl(O_{k_3}) = Cl(O_{k_1})Cl(O_{k_2})Cl(\mathfrak{p})^{-1}$, d'où $Cl(O_{k_3}) = c_1c_2Cl(\mathfrak{p})^{-1}$ égale à c_3. Ce qui achève la démonstration du théorème.

Démonstration de l'assertion (*i*) *du Théorème* 1.1 *dans le cas biquadratique.* Soit $c \in Cl(k)$. Sous les hypothèses et notations du Théorème 3.3 précédent, posons $c_1 = c$, $c_2 = c_3 = 1$; soit N/k l'extension biquadratique modérée obtenue à la fin de sa démonstration, alors $Cl(O_N) = c$ par le (2) de la Proposition 3.2; d'où le (i) du Théorème 1.1.

Démonstration du Théorème 1.3. On utilise les hypothèses et les notations du Théorème 1.3.

Le groupe Γ étant isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, la décomposition de l'algèbre semi-simple $k[\Gamma]$ en un produit d'algèbres simples est $k[\Gamma] \simeq k \times k \times k \times k$, par suite $Cl(\mathcal{M}) \simeq Cl(k) \times Cl(k) \times Cl(k) \times Cl(k)$.

D'après Fröhlich ([F3], Th. 4 et Chap. I, note [4], pp. 50–51), la classe de O_N dans $Cl(\mathcal{M})$ a pour composantes dans $Cl(k) \times Cl(k) \times Cl(k) \times Cl(k)$, les classes des idéaux fractionnaires $\langle O_N, \chi_i\rangle_{N/k}\langle a, \chi_i\rangle_{N/k}^{-1}$ de O_k, $0 \leq i \leq 3$, où χ_0 est le caractère trivial de $\mathrm{Gal}(N/k)$, les χ_i, $1 \leq i \leq 3$, sont les caractères non triviaux de degré 1 de $\mathrm{Gal}(N/k)$ cités dans la démonstration du (1) de la Proposition 3.1, et a est une base du $k[\Gamma]$-module N.

En utilisant simplement la définition des résolvantes de Lagrange (cf. §2), on obtient:

- Si $i = 0$, $\langle O_N, \chi_0\rangle_{N/k}\langle a, \chi_0\rangle_{N/k}^{-1} = (Tr_{N/k}(O_N))\langle a, \chi_0\rangle_{N/k}^{-1}$.
- Si $i = 1, 2$ ou 3,

$$\langle O_N, \chi_i\rangle_{N/k}\langle a, \chi_i\rangle_{N/k}^{-1} = \langle Tr_{N/k_i}(O_N), \chi_i\rangle_{k_i/k}\langle Tr_{N/k_i}(a), \chi_i\rangle_{k_i/k}^{-1}$$

où, dans le deuxième membre de cette égalité, χ_i est considéré comme caractère de $\mathrm{Gal}(k_i/k)$.

On a $(\mathrm{Tr}_{N/k}(O_N)) = O_k$ et $(\mathrm{Tr}_{N/k_i}(O_N)) = O_{k_i}$ car N/k et les N/k_i sont modérées (cf. [FT], Th. 26, p. 140). Il est clair que $\mathrm{Tr}_{N/k_i}(a) = a_i'$ est une base du $k[\mathrm{Gal}(k_i/k)]$-module k_i.

D'après [Sol] (Th. 2.2 et Th. 2.3, cas $l = 2$) et la Proposition 2.2, la classe de $\langle O_{k_i}, \chi_i\rangle_{k_i/k}\langle a_i', \chi_i\rangle_{k_i/k}^{-1}$ est la classe de Steinitz de l'extension k_i/k.

Le Théorème 1.3 est donc une conséquence du Théorème 3.3.

4. Classes de Steinitz d'extensions cycliques de degré 4

Dans ce paragraphe on suppose que Γ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

PROPOSITION 4.1. *Soient N/k une extension cyclique de degré 4, modérement ramifiée, K/k son unique sous-extension quadratique. Alors*

(1) $\Delta(N/k) = \Delta(K/k)^3 J^2$, *où J est un idéal entier de O_k sans facteur carré et est premier à $\Delta(K/k)$.*

Plus précisément, on a

(2) $\Delta(N/K) = \mathcal{D}(K/k) J O_K$.

Démonstration. (1) Le groupe $\mathrm{Gal}(N/k)$ possède deux classes de conjugaison de caractères irréductibles non triviaux, de degré 1, qui sont représentées par un caractère χ_1 (d'ordre 2) qui provient de $\mathrm{Gal}(N/k)/\mathrm{Gal}(N/K)$, et un caractère χ_2 (d'ordre 4). La décomposition d'Artin du discriminant de N/k est $\Delta(N/k) = f(\chi_1, N/k)f(\chi_2, N/k)^2$. Soient $\mathfrak{p}$ un idéal premier de O_k, $\mathfrak{P}$ un idéal premier de O_N au dessus de $\mathfrak{p}$, et $e(\mathfrak{P}/\mathfrak{p})$ l'indice de ramification de $\mathfrak{P}$ dans N/k; comme N/k et modérée, $v_{\mathfrak{P}}(\mathcal{D}(N/k)) = e(\mathfrak{P}/\mathfrak{p}) - 1$ (cf. [FT], Th. 26, p. 140), l'extension N/k étant galoisienne de degré 4, on en déduit que $v_{\mathfrak{p}}(\Delta(N/k)) = 0, 2$ ou 3. Supposons que $\mathfrak{p}$ soit ramifié dans N/k; si $\mathfrak{p}$ est ramifié dans K/k alors $v_{\mathfrak{p}}(\Delta(N/k)) = 1 + 2v_{\mathfrak{p}}(f(\chi_2, N/k))$, donc $v_{\mathfrak{p}}(\Delta(N/k)) = 3$ et $v_{\mathfrak{p}}(f(\chi_2, N/k)) = 1$; si $\mathfrak{p}$ n'est pas ramifié dans K/k, $v_{\mathfrak{p}}(\Delta(N/k)) = 2v_{\mathfrak{p}}(f(\chi_2, N/k))$, d'où $v_{\mathfrak{p}}(f(\chi_2, N/k)) = 1$. Donc on a (1).

(2) En vertu de (1) de la Proposition 2.1, $\Delta(N/k) = \Delta(K/k)^2 N_{K/k}(\Delta(N/K))$, d'où $\Delta(K/k)J^2 = N_{K/k}(\Delta(N/K))$ d'après (1). Donc $N_{K/k}(\mathcal{D}(K/k)J) = N_{K/k}(\Delta(N/K))$, par suite $\Delta(N/K) = \mathcal{D}(K/k)J$.

PROPOSITION 4.2. *Avec les hypothèses et les notations de la Proposition* 4.1, *on a* $Cl_k(O_N) = Cl_k(O_K)^3 Cl(J)$.

Démonstration. On a $Cl_k(O_N) = Cl_k(O_K)^2 N_{K/k}(Cl_K(O_N))$ par le (ii) de la Proposition 2.1. Montrons que $N_{K/k}(Cl_K(O_N)) = Cl(J)Cl_k(O_K)$, ce qui donne la proposition. Soient $M \in K$, $m \in k$ tels que $K = k(\sqrt{m})$ et $N = K(\sqrt{M})$. Il est facile de vérifier que N/k est cyclique de degré 4 si et seulement s'il existe $x \in k$ tel que $N_{K/k}(M) = mx^2$. En utilisant la Proposition 2.2 et le (2) de la proposition précédente, on peut poser

$$mO_k = I(m)^2\Delta(K/k) \text{ et } MO_K = I(M)^2\mathcal{D}(K/k)J.$$

On a alors

$$\begin{aligned} N_{K/k}(MO_K) &= (JN_{K/k}(I(M)))^2\Delta(K/k) \\ &= (x\, I(m))^2\Delta(K/k). \end{aligned}$$

Par conséquent $JN_{K/k}(I(M)) = xI(m)$, il en résulte ce qu'on veut montrer puisque $Cl(I(M)^{-1}) = Cl_K(O_N)$ et $Cl(I(m)^{-1}) = Cl_k(O_K)$.

Démonstration du Théorème 1.2 (*dans le cas des extensions quadratiques plongeables dans les cycliques de degré* 4). Soit $c \in Cl(k)$. On considère le cycle $C = C_\infty 4O_k$. Par le théorème de densité généralisé de Dirichlet (cf. [N1]), il existe $m \in k^\times$, $\mathfrak{p}$ un idéal premier de O_k ne divisant pas $2O_k$, et $I(m)$ un idéal fractionnaire de O_k tels que $mO_k = I(m)^2\mathfrak{p}$, $m \equiv 1 \bmod^*(C)$, et $c = Cl(I(m)^{-1})$.

Soit $K = k(\sqrt{m})$, il est clair que K/k est quadratique modérée. Il est bien connu que K/k est plongeable dans une extension cyclique de degré 4 sur k si et seulement si pour toute place v de k, $(-1, m)_v = 1$ (condition équivalente à m est somme de deux carrés dans k).

Dans la suite, on utilisera les propriétés des symboles locaux (cf. [Se1], Chap. XIV et p. 237) pour montrer que pour toute place v de k, $(-1, m)_v = 1$.

Soit v une place archimédienne de k; si v est complexe, $(-1, m)_v = 1$ par définition; si v est réelle, $(-1, m)_v = 1$ car m est totalement positif par la congruence qu'il vérifie.

Soit $c = \mathfrak{p}'$ une place non archimédienne de k; si $\mathfrak{p}'$ est au dessus de 2, et e son indice ramification absolu, la congruence que vérifie m entraîne $v_{\mathfrak{p}'}(m-1) \geq v_{\mathfrak{p}'}(4O_k) = 2e$, donc il existe $a \in \mathbb{Z}$ tel que $(-1, m)_{\mathfrak{p}'} = (-1)^{av_{\mathfrak{p}'}(-1)}$ (cf. [Se1], Prop. 6, p. 237) d'où $(-1, m)_{\mathfrak{p}'} = 1$; si $\mathfrak{p}'$ n'est pas au dessus de 2 et $\mathfrak{p}' \neq \mathfrak{p}$, $(-1, m)_{\mathfrak{p}'} = 1$ car $v_{\mathfrak{p}'}(m) \equiv 0 \bmod(2)$; pour la place $\mathfrak{p}$ on a $(-1, m)_{\mathfrak{p}} = 1$ par la formule du produit.

On conclut que K/k est plongeable dans une extension N/k cyclique de degré 4, que l'on peut choisir modérée par le Théorème 6.6 de [N2]. D'où le Théorème 1.2 puisque $c = \mathcal{C}l_k(O_K)$.

Démonstration de (*i*) *du théorème* 1.1 *dans le cas où* $\Gamma \simeq \mathbb{Z}/4\mathbb{Z}$. Soient k un corps de nombres, $c \in \mathcal{C}l(k)$. Le Théorème 1.2 nous affirme l'existence d'une extension K/k quadratique modérée, plongeable dans une extension cyclique N/k de degré 4, modérée et telle que $\mathcal{C}l_k(O_K) = c$. En vertu de la Proposition 4.1, $\Delta(N/k) = \Delta(K/k)^3 J^2$. On considére $c^2\mathcal{C}l(J)$; elle est un carré puisque le nombre de classes de k est impair. Choisissons un idéal I premier à $4O_k$ et tel que $I^2 \in C^2\mathcal{C}l(J)$. Grâce au théorème de densité de Dirichlet dans $\mathcal{C}l(k, 4O_k)$, il existe un idéal premier $\mathfrak{p}$ de O_k ne divisant pas $\Delta(N/k)$ et $m \in k^\times$ tels que

$$m'O_k = I^2\mathfrak{p}, m' \equiv 1 \bmod^*(4O_k).$$

Alors $\mathcal{C}l(\mathfrak{p}) = c^{-2}\mathcal{C}l(J)^{-1}$. Ecrivons $I(m') = I$.

L'extension $k(\sqrt{m'})/k$ est quadratique, modérée et est arithmétiquement disjointe de N/k. Soit $M \in K$ tel que $N = K(\sqrt{M})$. Par des considérations élémentaires de la théorie des groupes, la composée de N et $k(\sqrt{m'})$ contient une extension N'/k cyclique de degré 4 avec $N' = K(\sqrt{Mm'})$. Comme $MO_K = I(M)^2\mathcal{D}(K/k)J$, $Mm'O_K = (I(M)I(m'))^2\mathcal{D}(K/k)J\mathfrak{p}$. Mais N'/k est modérée (car $N(\sqrt{m'})/k$ est modérée), donc N'/K l'est aussi et par suite $\Delta(N'/K) = \mathcal{D}(K/k)J\mathfrak{p}$ par le (ii) de la Proposition 2.2. Le (1) de la Proposition 4.1 nous donne $\Delta(N'/k) = \Delta(K/k)^3(J\mathfrak{p})^2$, d'où $\mathcal{C}l_k(O_{N'}) = \mathcal{C}l_k(O_K)^3\mathcal{C}l(J)\mathcal{C}l(\mathfrak{p})$ en vertu de la Proposition 4.2. On en déduit que $\mathcal{C}l_k(O_{N'}) = c^3\mathcal{C}l(J)c^{-2}\mathcal{C}l(J)^{-1} = c$. Ce qui achève la démonstration.

5. Classes de Steinitz d'extensions quaternioniennes de degré 8

Dans cette section, il s'agit du cas où Γ est isomorphe au groupe quaternionien d'ordre 8.

PROPOSITION 5.1. *Soient N/k une extension galoisienne modérée dont le groupe de Galois est isomorphe au groupe quaternionien d'ordre* 8, *K/k sa sous-extension biquadratique. Alors*

(1) $\Delta(N/k) = \Delta(K/k)^3 J^4$, *où J est un idéal entier de O_k, sans facteur carré et premier à* $\Delta(K/k)$.

Plus précisement on a

(2) $\Delta(N/K) = \mathcal{D}(K/k)J\ O_K$.

Démonstration. (1) Soit $\mathfrak{p}$ un idéal premier de O_k qu'on suppose ramifié dans N. Soient k_i/k, $1 \leq i \leq 3$, les sous-extensions quadratiques de K. Si $\mathfrak{p}$ est ramifié dans K, il est non ramifié dans l'une des extensions k_i en vertu de la Proposition 3.1, supposons par exemple que c'est k_1; soit $\mathfrak{P}$ un idéal premier de O_{k_1} au dessus de $\mathfrak{p}$, comme $\mathfrak{P}$ est ramifié dans K/k_1 et N/k_1 est cyclique on a $v_{\mathfrak{P}}(\Delta(N/k_1)) = 3$ par la Proposition 4.1, par suite $v_{\mathfrak{p}}(\Delta(N/k)) = 6$ par le (i) de la Proposition 2.1. Si $\mathfrak{p}$ n'est pas ramifié dans K, alors il est ramifié seulement dans N/K, donc $v_{\mathfrak{P}}(\Delta(N/k_1)) = 2$ grâce à la Proposition 4.1, et comme ci-dessus $v_{\mathfrak{p}}(\Delta(N/k)) = 4$. On conclut qu'on a (1) puisque d'après le (1) et (2) de la Proposition 3.1, si $\mathfrak{p}$ est ramfié dans K/k alors $v_{\mathfrak{p}}(\Delta(K/k)) = 2$.

(2) En utilisant l'assertion (1) et le (i) de la Proposition 2.1 on obtient $\Delta(K/k)J^4 = N_{K/k}(\Delta(N/K))$. Comme $N_{K/k}(\mathcal{D}(K/k)J) = \Delta(K/k)J^4$, on a (2).

Remarque. On garde les mêmes hypothèses et notations que ci-dessus. Le groupe $\mathrm{Gal}(N/k)$ possède trois caractères irréductibles χ_i, $1 \leq i \leq 3$, de degré 1 non triviaux qui proviennent de $\mathrm{Gal}(N/k)/\mathrm{Gal}(N/k_i)$, et un caractère χ de degré 2 à valeurs réelles (qui est induit par un caractère de degré 1 d'ordre 4 d'un sous-groupe cyclique d'ordre 4 de $\mathrm{Gal}(N/k)$) (pour voir tout ceci, on utilise [Se2]). Donc $\Delta(N/k) = (\prod_{i=1}^{3} f(\chi_i, N/k)) f(\chi, N/k)^2$. D'autre part $\Delta(N/k) = \Delta(K/k)^3 J^4$, $f(\chi_i, N/k) = \Delta(k_i/k)$ et $\Delta(K/k) = \prod_{i=1}^{3} \Delta(k_i/k)$. On en déduit que

$$f(\chi, N/k) = (\Delta(K/k)J^2)^2,$$

d'où le Théorème 1 de [Se3] dans le cas modéré: $f(\chi, N/k)$ est le carré d'un idéal de O_k (dans les notations de [Se3], dans notre cas on vérifie que δ_χ est trivial).

PROPOSITION 5.2. *Sous les hypothèses et notations de la Proposition* 5.1, *on a* $Cl_k(O_N) = Cl_k(O_K)^3 Cl(J)^2$.

Démonstration. En vertu de la Proposition 2.2, $Cl_k(O_N) = Cl_k(O_K)^2 N_{K/k}(Cl_K(O_N))$; il suffit donc de montrer que $N_{K/k}(Cl_K(O_N)) = Cl_k(O_K) Cl(J)^2$ pour que l'on ait la proposition. Soient $M \in K$, $m_i \in k$, $1 \leq i \leq 3$, tels que $N = K(\sqrt{M})$ et $k_i = k(\sqrt{m_i})/k$ soient les trois sous-extensions quadratiques de K. Posons $MO_K = I(M)^2 \Delta(N/K)$, où l'on a $Cl_K(O_N) = Cl(I(M)^{-1})$, et $\Delta_i = \Delta(k_i/k)$. On a

$$N_{K/k}(M)O_k = (N_{K/k}(I(M))\,\Delta_1\Delta_2(\Delta_1, \Delta_2)^{-1} J^2)^2,$$

car $N_{K/k}(\Delta(N/K)) = \Delta(K/k)J^4$ (Prop. 5.1, (2)), et $\Delta(K/k) = (\Delta_1\Delta_2(\Delta_1, \Delta_2)^{-1})^2$ (Prop. 3.1, (1) et (2)). D'autre part, en utilisant le fait que N/k est galoisienne et les extensions N/k_i sont cycliques de degré 4, on obtient que il existe $x \in k_1$ tel que $N_{K/k_1}(M) = m_2 x^2$, d'où $N_{K/k}(M) = (m_2 N_{k_1/k}(x))^2$. Donc, $m_2 N_{k_1/k}(x) O_k = N_{K/k}(I(M))\Delta_1\Delta_2(\Delta_1, \Delta_2)^{-1} J^2$. Comme $Cl(\Delta_1\Delta_2(\Delta_1, \Delta_2)^{-1}) = Cl_k(O_K)$ (le (2) de la Prop. 3.2), $Cl(N_{K/k}(I(M)^{-1})) = Cl_k(O_K)Cl(J)^2 = N_{K/k}Cl_K(O_N)$.

THÉORÈME 5.3. *Soit k un corps de nombres. On suppose $\xi_4 \in k$ ou $k(\xi_4)/k$ ramifiée. Alors, pour tout $(c_1, c_2, c_3) \in Cl(k)^3$, il existe trois extensions k_i/k, $1 \leq i \leq 3$, quadratiques modérées, telles que pour tout i, $1 \leq i \leq 3$, $Cl_k(O_{k_i}) = c_i$, et la composée des k_i/k est une extension K/k biquadratique modérée, plongeable dans une extension N/k quaternionienne de degré 8 modérée.*

Démonstration. L'extension $k(\xi_4)/k$ est contenue dans le corps de classes de rayon modulo $C_\infty 4O_k$, donc $\mathrm{Gal}(k(\xi_4)/k) \simeq Cl(k, C_\infty 4O_k)/W^*$, où $W^* = N_{k(\xi_4)/k}(Cl(k(\xi_4), C_\infty 4O_{k(\xi_4)}))$. Comme $k(\xi_4)/k$ est ramifiée ou bien $\xi_4 \in k$, $N_{k(\xi_4)/k}(Cl(k(\xi_4))) = Cl(k)$ (cf. [Wa, Th. 10.1, p. 185]). D'où une surjection de W^* sur $Cl(k)$ d'après les surjections canoniques de $Cl(k, C_\infty 4O_k)$ sur $Cl(k)$ et W^* sur $N_{k(\xi_4)/k}(Cl(k(\xi_4)))$.

Soient $(c_1, c_2, c_3) \in Cl(k)^3$, $\mathfrak{p}$ un idéal premier de O_k tel que $Cl(\mathfrak{p}) \in W^*$ et $Cl(\mathfrak{p}) = c_1c_2c_3^{-1}$. Soit I_1 un idéal fractionnaire de O_k dans c_1^{-1} avec $Cl(I_1) \in Cl(k, C_\infty 4O_k)$, alors $Cl(I_1)^2 \in W^*$, par suite $Cl(I_1^2\mathfrak{p})^{-1} \in W^*$. Soit $\mathfrak{p}_1$ un idéal premier de O_k ne divisant pas $2\mathfrak{p}$ tel que $Cl(\mathfrak{p}_1) = Cl(I_1^2\mathfrak{p})^{-1}$ dans $Cl(k, C_\infty 4O_k)$. Alors, il existe $m_1 \in k^\times$ tel que $m_1O_k = I_1^2\mathfrak{p}\mathfrak{p}_1$, $m_1 \equiv 1 \bmod^*(C_\infty 4O_k)$. De plus $\left(\frac{-1}{\mathfrak{p}_1}\right) = 1$ car $\mathfrak{p}_1$ est décomposé dans $k(\xi_4)/k$ lorsque cette dernière est ramifiée puisque $Cl(\mathfrak{p}_1) \in W^*$, et c'est évident si $\xi_4 \in k$.

L'extension $k(\sqrt{-m_1})/k$ étant contenue dans le corps de classes de rayon modulo $C_\infty 4\mathfrak{p}\mathfrak{p}_1$, on a $\mathrm{Gal}(k(\sqrt{-m_1})/k) \simeq Cl(k, C_\infty 4\mathfrak{p}\mathfrak{p}_1)/W^{**}$, où $W^{**} = N_{k(\sqrt{-m_1})/k}(Cl(k(\sqrt{-m_1}), C_\infty 4\mathfrak{p}\mathfrak{p}_1))$. Elle est ramifiée en $\mathfrak{p}$, par suite elle n'est pas contenue dans le corps de classes de rayon modulo $C_\infty 4\mathfrak{p}_1$, d'où $N_{k(\sqrt{-m_1})/k}(Cl(k(\sqrt{-m_1}), C_\infty 4\mathfrak{p}_1)) = Cl(k, C_\infty 4\mathfrak{p}_1)$ par un argument similaire à celui de [Wa, Th. 10.1, p. 400]. On en déduit une surjection de W^{**} sur $Cl(k, C_\infty 4\mathfrak{p}_1)$ d'après les surjections canoniques de $Cl(k, C_\infty 4\mathfrak{p}\mathfrak{p}_1)$ sur $Cl(k, C_\infty 4\mathfrak{p}_1)$ et W^{**} sur $N_{k(\sqrt{-m_1})/k}(Cl(k(\sqrt{-m_1}), C_\infty 4\mathfrak{p}_1))$.

Choisissons un idéal premier $\mathfrak{q}$ de O_k tel que $Cl(\mathfrak{q}) \in W^{**}$ et $Cl(\mathfrak{p}) = Cl(\mathfrak{q})$ dans $Cl(k, C_\infty 4\mathfrak{p}_1)$. Soit $a \in k$ tel que $\mathfrak{p}\mathfrak{q}^{-1} = aO_k$, où $a \equiv 1 \bmod^*(C_\infty 4\mathfrak{p}_1)$. Soit I_2 un idéal fractionnaire de O_k premier à $4\mathfrak{p}\mathfrak{p}_1$ avec $Cl(I_2) = c_2^{-1}$, alors $Cl(I_2)^2 \in W^{**}$. Soit $\mathfrak{p}_2$ un idéal premier de O_k ne divisant pas m_1O_k et tel que $Cl(\mathfrak{p}_2) = Cl(I_2^2\mathfrak{q})^{-1}$ dans W^{**}, i.e., il existe $b \in k$ tel que $bO_k = I_2^2\mathfrak{q}\mathfrak{p}_2$ et $b \equiv 1 \bmod^*(C_\infty 4\mathfrak{p}\mathfrak{p}_1)$. Posons $m_2 = ab$, alors $m_2O_k = I_2^2\mathfrak{p}\mathfrak{p}_2$ et $m_2 \equiv 1 \bmod^*(C_\infty 4\mathfrak{p}_1)$. De plus $\left(\frac{-m_1}{\mathfrak{p}_2}\right) = 1$ puisque $Cl(\mathfrak{p}_2) \in W^{**}$.

On considère $K = k(\sqrt{m_1}, \sqrt{m_2})$. On vérifie sans peine que l'extension K/k est biquadratique modérée. Montrons que K/k est plongeable dans une extension quaternionienne de degré 8 sur k, ce qui équivaut par [Wi] à: pour toute place v de k,

$$(*) \qquad (-1, m_1)_v(-1, m_2)_v(m_1, m_2)_v = 1$$

Pour les places archimédiennes et celles au dessus de 2, la même méthode que celle de la démonstration du Théorème 1.2 au §4 montre que $(*)$ est bien vérifiée.

Si $\mathfrak{p}'$ est un idéal premier de O_k qui n'est pas au dessus de 2 et est différent de $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2$, alors on a $(*)$ car $v_{\mathfrak{p}'}(m_1)$ et $v_{\mathfrak{p}'}(m_2)$ sont paires.

Si $\mathfrak{p}' = \mathfrak{p}_1$ alors, $(-1, m)_{\mathfrak{p}'} = 1$ car $(\frac{-1}{\mathfrak{p}_1}) = 1$, $(-1, m_2)_{\mathfrak{p}'} = 1$ car $v_{\mathfrak{p}_1}(m_2) = 0$, et $(m_1, m_2)_{\mathfrak{p}'} = 1$ car par la congruence que vérifie m_2 on a $v_{\mathfrak{p}_1}(m_2) = 0$ et la classe de m_2 dans le corps résiduel est égal à 1. Donc on a $(*)$.

Supposons $\mathfrak{p}' = \mathfrak{p}_2$. Alors, $(-1, m_1)_{\mathfrak{p}'} = 1$ car $v_{\mathfrak{p}_2}(m_1) = 0$, $(-1, m_2)_{\mathfrak{p}'} = (-1)^{(N_{k/\mathbb{Q}}(\mathfrak{p}_2)-1)/2}$ car $v_{\mathfrak{p}_2}(m_2)$ est impaire, $(m_1, m_2)_{\mathfrak{p}'} = \overline{m_1}^{(N_{k/\mathbb{Q}}(\mathfrak{p}_2)-1)/2}$ car $v_{\mathfrak{p}_2}(m_1) = 0$ et où $\overline{m_1}$ est la classe de m_1 dans le corps résiduel. Donc $(*)$ est vérifiée si et seulement si $\overline{-m_1}^{(N_{k/\mathbb{Q}}(\mathfrak{p}_2)-1)/2} = 1$, or cette égalité est équivalente à l'assertion $(\frac{-m_1}{\mathfrak{p}_2}) = 1$ par définition du symbole de Legendre généralisé, mais cette dernière est vérifiée par le choix fait au début, donc on a $(*)$.

Pour la place $\mathfrak{p}$, $(*)$ est vraie par la formule du produit. On conclut que K/k est plongeable dans une extension N/k quaternionienne de degré 8, que l'on peut choisir modérée par le Théorème 6.6 de [N2].

Une conséquence immédiate du Théorème 5.3 est le corollaire suivant.

COROLLAIRE 5.4. *Sous l'hypothèse du Théorème* 5.3, *l'ensemble des éléments de* $Cl(k)$ *réalisables par des classes de Steinitz d'extensions quadratiques de* k, *modérées, et plongeables dans des extensions quaternioniennes de degré* 8 *sur* k, *modérées, est égal au groupe* $Cl(k)$.

Remarque. Pour la preuve du Corollaire 5.4 sans l'hypothèse du Théorème 5.3 voir le Théorème 1.1 de [MS].

Démonstration du Théorème 1.2 (*dans le cas des extensions biquadratiques plongeables dans des extensions quaternioniennes de degré* 8) Soit $c \in Cl(k)$. Dans les notations du Théorème 5.3, posons $c_1 = c, c_2 = c_3 = 1$, alors $Cl_k(O_K) = c_1c_2c_3 = c$, par le (2) de la Proposition 3.2. Comme K/k est biquadratique, modérée, plongeable dans une extension quaternionienne modérée de degré 8 sur k, on a terminé la preuve du Théorème 1.2.

Démonstration de (*ii*) *du Théorème* 1.1. Soient k un corps de nombres dont le nombre de classes est impair (donc l'hypothèse du Théorème 5.3 est vérifiée), $c \in Cl(k)$. Sous les notations du Théorème 5.3 et d'après la démonstration du Théorème 1.2 ci-dessus, on a que il existe N/k quaternionienne modérée contenant K, et $Cl_k(O_K) = c$. Par la Proposition 5.1, $\Delta(N/k) = \Delta(K/k)^3 J^4$. La classe $(cCl(J))^{-1}$ est un carré donc (comme dans la preuve de (i) du Théoréme 1.1 dans le cas où $\Gamma \simeq \mathbb{Z}/4\mathbb{Z}$) peut être considérée comme la classe du discriminant d'une extension $k(\sqrt{m})/k$ quadratique modérée, qu'on peut supposer en plus arithmétiquement disjointe de N. Soit $M \in K$ tel que $N = K(\sqrt{M})$. Par des considérations élémentaires de la théorie des groupes, la composeé de N et $k(\sqrt{m})$ contient une extension N'/k, quaternionienne de degré 8, et telle que $N' = K(\sqrt{Mm})$. Il est clair que N'/k est modérée. Si $MO_K =$

$I(M)^2\mathcal{D}(K/k)J$ et $mO_k = I(m)^2\Delta(k(\sqrt{m})/k)$, alors $mMO_K = (I(M)I(m))^2 \mathcal{D}(K/k)J\Delta(k(\sqrt{m})/k)$, où $\mathcal{D}(K/k)J\Delta(k(\sqrt{m})/k)$ est sans facteur carré donc égal à $\Delta(N'/K)$ car N'/K est modérée (Proposition 2.2). Par suite

$$\begin{aligned}\Delta(N'/k) &= \Delta(K/k)^3(J\Delta(k(\sqrt{m})/k))^4 \quad \text{(Proposition 5.1) et}\\ \mathcal{C}l_k(O_{N'}) &= \mathcal{C}l_k(O_K)^3(\mathcal{C}l(J)\mathcal{C}l(\Delta(k(\sqrt{m})/k))^2 \quad \text{(Proposition 5.2)}\\ &= c^3(\mathcal{C}l(J)(c\mathcal{C}l(J))^{-1})^2 = c.\end{aligned}$$

Donc on a le (ii) du Théorème 1.1.

Remerciements. Je remercie le referee pour ses remarques et la réparation de la preuve du Théorème 5.3.

Dans le plat pays qui n'est pas le mien, la bibliothèque et le jeune séminaire d'arithmétique de l'université de Lille1 etaient des ailes pour m'envoler au dessus d'un ciel si bas.

RÉFÉRENCES

[Ca] J. E. Carter, *Steinitz classes of nonabelien extensions of degree p^3*, Acta Arith. **78** (1997), 297–303.

[Cr] T. Crespo, *Embedding problems with ramification conditions*, Arch. Math. **53** (1989), 270–276.

[E] L. P. Endo, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, Thesis, University of Illinois at Urbana-Champaign, 1975.

[F1] A. Fröhlich, *The discriminants of relative extensions and the existence of integral bases*, Mathematika **7** (1960), 15–22.

[F2] ———, *Artin-root numbers and normal integral bases for quaternion fields*, Invent. Math. **17** (1972), 143–166.

[F3] ———, *Galois module structure of algebraic integers*, Springer-Verlag, Berlin, 1983.

[FT] A. Fröhlich et M. J. Taylor, *Algebraic number theory*, Cambridge University Press, 1991.

[H] E. Hecke, *Lectures on the theory of algebraic numbers*, Springer-Verlag, Berlin, 1981.

[L1] R. Long, *Steinitz classes of cyclic extensions of prime degree*, J. Reine Angew. Math. **250** (1971), 87–98.

[L2] ———, *Steinitz classes of cyclic extensions of degree l^r*, Proc. Amer. Math. Soc. **49** (1975), 297–304.

[L3] ———, *Steinitz classes of relative Galois extensions*, Thesis, University of Illinois at Urbana-Champaign, 1970.

[Mc1] L. R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987), 259–306.

[Mc2] ———, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), 102–134.

[MS] R. Massy et B. Sodaïgui, *Classes de Steinitz et extensions quaternioniennes*, Proyecciones **16**, July 1997, no. 1, 01–13.

[N1] J. Neukirch, *Class field theory*, Springer-Verlag, Berlin, 1986. 1986

[N2] ———, *Über das einbettungsproblem der algebraischen zahlen-theorie*, Invent. Math. **21** (1973), 59–116.

[Se1] J.-P. Serre, *Corps locaux*, 3ème ed, Hermann, Paris, 1980.

[Se2] ———, *Représentation linéaire des groupes finis*, 2ème ed, Hermann, Paris, 1977.

[Se3] ———, *Conducteurs d'Artin des caractères réels*, Invent. Math. **14** (1971), 173–183.

[So1] B. Sodaïgui, *Structure galoisienne relative des anneaux d'entiers*, J. Number Theory **28** (1988), 189–204.

[So2] ———, *Classes réalisables par des extensions métacylciques non abéliennes et éléments de Stickelberger*, J. Number Theory **65** (1997), 87–95.

[Wa] L. C. Washington, *Introduction to cyclotomic fields*, 2nd edition, Springer-Verlag, Berlin, 1996.

[Wi] E. Witt, *Konstruktion von galoisschen körpern der charakteristik p zu vorgegebener gruppe der ordnung* p^f, J. Crelle **174** (1936), 237–245.

Département de Mathématiques, Université de Valenciennes, Le Mont Houy, B.P. 311, F - 59304 Valenciennes cedex, France
sodaigui@univ-valenciennes.fr