ACTA ARITHMETICA
LXXVIII.3 (1997)

Classes logarithmiques ambiges des corps quadratiques

par

FLORENCE SORIANO (Talence)

0. Introduction. La notion de corps logarithmiquement principal (relativement à un nombre premier p) a été introduite par J.-F. Jaulent à l'occasion de l'étude de certaines pro-p-extensions canoniques des corps de nombres en liaison avec la K-théorie : l'arithmétique des classes logarithmiques, qui se révèle semblable (quoique plus complexe) à celle des classes de diviseurs au sens habituel donne, en effet, des informations directes sur celle des noyaux modéré et sauvage des corps considérés : plus précisément, si K désigne un corps de nombres qui contient les racines $2l$-ièmes de l'unité, le l-groupe des classes logarithmiques s'interprête par la théorie d'Iwasawa comme le quotient des genres

$$\widetilde{Cl}_K = {}^{\Gamma}\mathcal{C}$$

du groupe de Galois $\mathcal{C} = \mathrm{Gal}(\overline{K}^{\mathrm{c}}/K^{\mathrm{c}})$ attaché à la pro-l-extension abélienne complètement décomposée partout maximale $\overline{K}^{\mathrm{c}}$ du corps cyclotomique $K^{\mathrm{c}} = K[\zeta_{l^\infty}]$ relativement au groupe procyclique $\Gamma = \mathrm{Gal}(K^{\mathrm{c}}/K)$ (cf. [J$_1$]), tandis que la cohomologie galoisienne permet de montrer que la l-partie ${}_{l^\infty}H_2(K)$ du noyau des symboles de Hilbert dans $K_2(K)$ est donnée, elle, par l'identité (cf. [Sc], th. 7.3)

$${}_{l^\infty}H_2(K) = {}^{\Gamma}(\mathbb{T}_l \otimes_{\mathbb{Z}_l} \mathcal{C}),$$

où $\mathbb{T}_l = \varprojlim \mu_{l^n}$ désigne le module de Tate.

Il résulte de cela (cf., par exemple, [J$_2$], mais on peut aussi le montrer directement), que pour $l = 2$ et en présence des racines 4-ièmes de l'unité, il existe un isomorphisme canonique

$$\{\pm 1\} \otimes_{\mathbb{Z}} \widetilde{Cl}_K = {}^{2}H_2(K)$$

entre les quotients d'exposant 2 respectifs du 2-groupe des classes logarithmiques et du noyau hilbertien de sorte en particulier que $\widetilde{Cl}_K$ et ${}_{2^\infty}H_2(K)$ sont alors simultanément triviaux.

Les résultats de J. Browkin et A. Schinzel (cf. [BS]) permettant de dresser la liste des extensions quadratiques $\mathbb{Q}(\sqrt{\pm d})$ de $\mathbb{Q}$ pour lesquelles le 2-groupe ${}_{2^\infty}H_2(K)$ est trivial, il était tentant de regarder si la condition de trivialité ${}_{2^\infty}H_2(K) = 1$ était encore corrélée ou non avec la condition logarithmique analogue alors même que l'hypothèse $\mu_4 \subset K$ n'était plus satisfaite. Nous nous proposons donc dans cet article de déterminer la liste des corps quadratiques $K = \mathbb{Q}(\sqrt{\pm d})$ du corps des rationnels dont le 2-groupe des classes logarithmiques (au sens de [J_3]) $\widetilde{Cl}_{\mathbb{Q}(\sqrt{\pm d})}$ est trivial et de comparer la classification obtenue à celle, tirée de [BS], des mêmes corps K, pour lesquelles c'est ${}_{2^\infty}H_2(K)$ qui est trivial.

1. Notations et position du problème. Nous utilisons dans ce travail les notations de [J_3]. En particulier nous posons :

1.1. Définition. Le corps de nombres K est dit 2-*logarithmiquement principal* si et seulement si son 2-groupe des classes logarithmiques $\widetilde{Cl}_K$ est trivial.

Exemples. 1. Comme nous le verrons au paragraphe 5, l'exemple le plus simple est le corps des nombres rationnels $K = \mathbb{Q}$.

2. Si i désigne une racine primitive quatrième de l'unité dans $\mathbb{C}$, le corps de nombres $K = \mathbb{Q}(i)$ étant 2-régulier (cf. par exemple, [GJ], Th. 2.1.iv.a.), son 2-noyau hilbertien $H_2(K)$ est en particulier trivial. Et ainsi, l'isomorphisme $\{\pm 1\} \otimes_{\mathbb{Z}} \widetilde{Cl}_K = {}_2H_2(K)$ montre que $K = \mathbb{Q}(i)$ est effectivement un corps de nombres 2-logarithmiquement principal .

Remarque. Le lien étroit entre la notion de groupe des classes logarithmiques avec celle du 2-Sylow du noyau hilbertien, nous suggère de citer certains auteurs dont les travaux concernent la trivialité du 2-noyau hilbertien des extensions quadratiques de $\mathbb{Q}$.

1. En 1972, les calculs de J. Tate (cf. [BT], appendice) montrent que le noyau hilbertien est trivial pour les corps quadratiques imaginaires dont le discriminant Δ de valeur absolue strictement inférieure à 35 n'est pas congru à 1 modulo 8.

2. En 1982, J. Browkin et A. Schinzel publient dans [BS] les calculs du 2-rang du noyau hilbertien des extensions quadratiques de $\mathbb{Q}$.

3. En 1993, H. Qin (cf. [Qi]) prouve la trivialité du noyau hilbertien de $\mathbb{Q}(\sqrt{-6})$ par une méthode basée sur les travaux de Tate et transposable dans l'étude d'autres exemples de corps quadratiques imaginaires.

4. Un article récent de M. Skałba (cf. [Sk]) étudie les cas particuliers des extensions quadratiques imaginaires $\mathbb{Q}(\sqrt{-5})$ et $\mathbb{Q}(\sqrt{-19})$, comme application d'une généralisation du théorème de Thue.

5. Enfin H. Thomas par des méthodes algorithmiques dresse dans [Th] la liste complète des extensions quadratiques de $\mathbb{Q}$ et de $\mathbb{Q}(i)$ dont le 2-noyau hilbertien est trivial.

Notre principal outil dans l'étude de la condition $\widetilde{Cl}_K = 0$ est l'inégalité des classes logarithmiques ambiges (cf. [J$_3$], Th. 4.5) qui établit en particulier qu'une extension quadratique F du corps $\mathbb{Q}$ des nombres rationnels, de groupe de Galois G, est 2-logarithmiquement principale si et seulement si les deux conditions suivantes sont satisfaites :

(i) on a

$$\prod_{\mathfrak{p}\mid\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q}) = [F : F \cap \mathbb{Q}^{\mathrm{c}}] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})$$

où $d_{\mathfrak{p}}(F/\mathbb{Q})$ désigne le degré local en $\mathfrak{p}$ de l'extension $F/\mathbb{Q}$, $\widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})$ le degré de ramification logarithmique, $\mathbb{Q}^{\mathrm{c}}$ la $\mathbb{Z}_l$-extension cyclotomique, $\widetilde{\mathcal{E}}_{\mathbb{Q}}$ le groupe des unités logarithmiques de $\mathbb{Q}$ et $\mathcal{N}_{L/K}$ le $\mathbb{Z}_l$-tensorisé des normes dans l'extension $F/\mathbb{Q}$;

(ii) le morphisme φ du premier groupe de cohomologie $H^1(G, \widetilde{Pl}_F)$ des diviseurs principaux dans celui $H^1(G, \widetilde{Dl}_F)$ des diviseurs logarithmiques de degré nul de F, déduit de la suite exacte

$$1 \to \widetilde{Pl}_F \to \widetilde{Dl}_F \to \widetilde{Cl}_F \to 1,$$

est surjectif.

Lors de l'étude de la surjectivité du morphisme φ, les lemmes 4.1 et 4.2 de [J$_3$] nous conduisent à introduire la définition suivante :

1.2. Définition. Une 2-extension L/K de corps de nombres est dite (*CM*)-*primitivement ramifiée* (au sens logarithmique) si l'une au moins des conditions suivantes est vérifiée :

• l'extension L/K est primitivement ramifiée, c'est-à-dire les diviseurs logarithmiques de L sont sommes de diviseurs ambiges et de diviseurs de degré nul,

• le quotient $\widetilde{\mathcal{E}}_K \cap \mathcal{N}_{L/K}/N_{L/K}(\widetilde{\mathcal{E}}_L)$ est engendré par des éléments totalement positifs (on parle alors d'extension (*CM*)-primitivement ramifiée *au sens non trivial*).

Remarque. Comme $\mathbb{Q}$ ne possède qu'une place paire, le groupe $\widetilde{\mathcal{E}}_{\mathbb{Q}}$ des unités logarithmiques de $\mathbb{Q}$ coïncide avec le tensorisé du groupe des 2-unités logarithmiques de $\mathbb{Q}$, et est en particulier engendré par -1 et 2. Les 2-extensions (*CM*)-primitivement ramifiées de $\mathbb{Q}$ comprennent en particulier les extensions quadratiques imaginaires de $\mathbb{Q}$, et les extensions quadratiques réelles dont les unités -1 et -2 ne sont pas normes.

Sous l'hypothèse de (CM)-primitivité, les deux paragraphes suivants établissent qu'en fait le morphisme φ est surjectif si et seulement si ni le radical $\pm d$, ni sa moitié $\pm d/2$ ne sont congrus à 9 modulo 16. Autrement dit, l'ordre du 2-groupe des classes logarithmiques ambiges de l'extension quadratique $F = \mathbb{Q}(\sqrt{\pm d})$ de $\mathbb{Q}$ est donné dans chacun des cas suivants par la formule :

1$^{\text{er}}$ cas : pour $\pm d \equiv 1 \pmod{16}$ ou $\pm d \equiv 2 \pmod{32}$, on a

$$|\widetilde{Cl}_F^G| = \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})} |H^1(G, \widetilde{Dl}_F)|,$$

2$^{\text{nd}}$ cas : pour $\pm d \not\equiv 1 \pmod{16}$ et $\pm d \not\equiv 2 \pmod{32}$, on a

$$|\widetilde{Cl}_F^G| = \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})}.$$

La liste des extensions quadratiques 2-logarithmiquement principales F de $\mathbb{Q}$ est alors dans ce cas facilement déterminée, et fait l'objet du paragraphe 6.

2. Classes logarithmiques ambiges des extensions quadratiques de $\mathbb{Q}$

2.1. *Présentation du problème.* Comme nous l'avons dit, nous souhaitons calculer l'ordre du groupe des classes logarithmiques ambiges d'une extension quadratique F quelconque de $K = \mathbb{Q}$. La formule des classes logarithmiques ambiges permettant de conclure dans le cas primitif (i.e. lorsque $H^1(G, \widetilde{Dl}_F) = 1$ (cf. §3)), le problème est dans le cas contraire ramené à l'étude de la surjectivité du morphisme $\varphi : H^1(G, \widetilde{Pl}_F) \to H^1(G, \widetilde{Dl}_F)$, déduit de la suite exacte

$$1 \to \widetilde{Pl}_F \to \widetilde{Dl}_F \to \widetilde{Cl}_F \to 1.$$

D'après [J$_3$], §4, le nombre de classes logarithmiques ambiges est donné, en effet, par la formule

$$|\widetilde{Cl}_F^G| = |\widetilde{Cl}_{\mathbb{Q}}| \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})} |\mathrm{Coker}\, \varphi|.$$

La difficulté majeure de manipulation de cette formule réside donc en l'étude de la surjectivité du morphisme de groupes cohomologiques φ. Cette étude est bien entendu plus facile lorsque le premier groupe cohomologique $H^1(G, \widetilde{Pl}_F)$ est trivial, puisque le nombre de classes logarithmiques ambiges de F est donné alors par la relation

$$|\widetilde{Cl}_F^G| = |\widetilde{Cl}_{\mathbb{Q}}| \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})} |H^1(G, \widetilde{Dl}_F)|.$$

Pour ces raisons, au moins dans le cas imprimitif, l'étude de la surjectivité de φ est ramenée à celle de la trivialité de l'image d'une classe génératrice du groupe $H^1(G, \widetilde{Pl}_F)$ (d'ordre 1 ou 2). D'où la nécessité dans un premier temps, de revenir sur la définition de φ :

2.2. *Etude du morphisme φ.* Le diagramme commutatif suivant (où tous les groupes sont d'ordre 1 ou 2) :

$$\begin{array}{ccc} H^1(G, \widetilde{Pl}_F) & \xrightarrow{\ \varphi\ } & H^1(G, \widetilde{Dl}_F) \\ \wr\downarrow & & \wr\downarrow \\ \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}}/N_{F/\mathbb{Q}}(\widetilde{\mathcal{E}}_F) & \xrightarrow{\ \bar{\varphi}\ } & \deg_F Dl_F / \deg_F Dl_F^G \end{array}$$

déduit des isomorphismes donnés par les lemmes 4.1 et 4.2 dans [J$_3$], montre que les morphismes φ et $\overline{\varphi}$ sont équivalents. Plus précisément :

2.2.1. Proposition. *Soient $\mathbb{Q}$ le corps des nombres rationnels et F une extension quadratique de $\mathbb{Q}$, dont le groupe de Galois G est engendré par un $\mathbb{Q}$-automorphisme σ. Le morphisme φ du premier groupe de cohomologie $H^1(G, \widetilde{Pl}_F)$ des diviseurs principaux de F dans le premier groupe de cohomologie $H^1(G, \widetilde{Dl}_F)$ des diviseurs de degré nul de F induit un morphisme $\overline{\varphi}$ qui à toute classe dans $\widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}}/N_{F/\mathbb{Q}}(\widetilde{\mathcal{E}}_F)$ d'une unité logarithmique $N_{F/\mathbb{Q}}(\alpha)$, norme de l'extension $F/\mathbb{Q}$, associe la classe dans le groupe quotient $\deg_F Dl_F / \deg_F Dl_F^G$, du degré d'un diviseur $\mathfrak{A}$ tel que $\mathfrak{A}^\sigma - \mathfrak{A} = \widetilde{\mathrm{div}}_F(\alpha)$.*

Preuve. Si $N_{F/\mathbb{Q}}(\alpha)$ désigne une unité logarithmique du corps $\mathbb{Q}$ des nombres rationnels, norme de l'extension $F/\mathbb{Q}$, il est toujours possible de déterminer un diviseur $\mathfrak{A}$ de F tel que $\mathfrak{A}^\sigma - \mathfrak{A} = \widetilde{\mathrm{div}}_F(\alpha)$. En effet, la condition normique $N_{F/\mathbb{Q}}(\alpha) \in \widetilde{\mathcal{E}}_{\mathbb{Q}}$, qui s'écrit encore $\widetilde{\mathrm{div}}_{\mathbb{Q}} N_{F/\mathbb{Q}}(\alpha) = 0$, nous donne les conditions

$$\widetilde{v}_{\mathfrak{p}}(\alpha) + \widetilde{v}_{\mathfrak{p}}^{\sigma}(\alpha) = 0, \quad \forall \mathfrak{p} \in Pl_F^\circ \text{ (ensemble des places finies de } F).$$

Faisons donc choix d'un système de représentants $Pl_{F/\mathbb{Q}}^\circ$ de Pl_F° pour l'action du groupe de Galois $G = \mathrm{Gal}(F/\mathbb{Q})$ (autrement dit, pour chaque premier p de $\mathbb{Q}$ décomposé dans $F/\mathbb{Q}$, faisons choix de l'un des premiers $\mathfrak{p}$ de F au-dessus de p), et considérons le diviseur logarithmique

$$\mathfrak{A} = -\sum_{\mathfrak{p} \in Pl_{F/\mathbb{Q}}^\circ} \widetilde{v}_{\mathfrak{p}}(\alpha)\mathfrak{p}.$$

Nous obtenons immédiatement

$$\mathfrak{A}^\sigma - \mathfrak{A} = \sum_{\mathfrak{p} \in Pl_{F/\mathbb{Q}}^\circ} \widetilde{v}_{\mathfrak{p}}(\alpha)(\mathfrak{p} - \mathfrak{p}^\sigma),$$

$$\begin{aligned}\mathfrak{A}^\sigma - \mathfrak{A} &= \sum_{\mathfrak{p}\in Pl^\circ_{F/\mathbb{Q}}} (\widetilde{v}_\mathfrak{p}(\alpha)\mathfrak{p} - \widetilde{v}_\mathfrak{p}(\alpha)\mathfrak{p}^\sigma) = \sum_{\mathfrak{p}\in Pl^\circ_{F/\mathbb{Q}}} (\widetilde{v}_\mathfrak{p}(\alpha)\mathfrak{p} + \widetilde{v}^\sigma_\mathfrak{p}(\alpha)\mathfrak{p}^\sigma)\\ &= \widetilde{\operatorname{div}}_F(\alpha),\end{aligned}$$

comme attendu.

Deux étapes s'imposent alors :

(i) montrer que l'image $\deg\mathfrak{A} \pmod{Dl_F^G}$ de $\mathfrak{A}$ par $\overline{\varphi}$ ne dépend en fait que de l'unité logarithmique de départ $N_{F/\mathbb{Q}}(\alpha)$,

(ii) montrer que cette image est nulle dès que α est une unité logarithmique de F.

Ainsi, dans un premier temps, nous considérons $\mathfrak{A}$ et $\mathfrak{B}$, deux diviseurs tels que $\mathfrak{A}^\sigma - \mathfrak{A} = \mathfrak{B}^\sigma - \mathfrak{B} = \widetilde{\operatorname{div}}_F(\alpha)$. L'écriture du diviseur $\mathfrak{A}^\sigma - \mathfrak{B}^\sigma$ sous la forme

$$\begin{aligned}\mathfrak{A}^\sigma - \mathfrak{B}^\sigma &= (\mathfrak{A} - \mathfrak{B}) + (\mathfrak{A}^\sigma - \mathfrak{A}) + (\mathfrak{B} - \mathfrak{B}^\sigma)\\ &= (\mathfrak{A} - \mathfrak{B}) + \widetilde{\operatorname{div}}_F(\alpha) - \widetilde{\operatorname{div}}_F(\alpha) = \mathfrak{A} - \mathfrak{B}\end{aligned}$$

montre que $\mathfrak{A} - \mathfrak{B}$ est un diviseur ambige et donc que les degrés de $\mathfrak{A}$ et $\mathfrak{B}$ ont même image dans le premier groupe de cohomologie $H^1(G, \widetilde{Dl}_F) \simeq \deg_F Dl_F / \deg_F Dl_F^G$. Enfin, soit $\mathfrak{A}$ un diviseur logarithmique provenant, par la construction précédente, de la norme d'une unité logarithmique de F; alors, conservant les notations, nous obtenons banalement $\mathfrak{A} = 0$ donc trivialement $\deg_F \mathfrak{A} = 0$.

Tous les outils de manipulation enfin présentés, commençons par examiner le cas le plus simple correspondant aux extensions primitivement ramifiées.

3. Application au cas primitif. Ce chapitre vise à caractériser les extensions quadratiques $F = \mathbb{Q}(\sqrt{\pm d})$ primitivement ramifiées (i.e. telles que $H^1(G, \widetilde{Dl}_F) = 1$). Plus précisément, il établit le résultat suivant :

3.1. LEMME. *L'entier naturel d étant supposé sans facteur carré, l'extension quadratique $\mathbb{Q}(\sqrt{\pm d})/\mathbb{Q}$ est primitivement ramifiée si et seulement si $\pm d$ n'est congru ni à 1 modulo 8, ni à 2 modulo 16, ou encore si d est divisible par un premier impair p congru à ± 3 modulo 8, ou enfin si $\pm d = 2$.*

Preuve. Si $\pm d = 2$, les corps de nombres F et $F \cap \mathbb{Q}^c$ coïncident, si bien que l'extension est trivialement primitivement ramifiée.

Sinon, il s'agit de vérifier l'existence d'un diviseur premier p ramifié au sens logarithmique dans l'extension $F/F\cap\mathbb{Q}^c$, et dont le degré est générateur du $\mathbb{Z}_2$-module $\deg_\mathbb{Q} Dl_\mathbb{Q} = 4\mathbb{Z}_2$. Dans le cas de ramification logarithmique en 2, c'est-à-dire $\pm d \not\equiv 1 \pmod 8$ et $\pm d \not\equiv 2 \pmod{16}$, l'extension $F/\mathbb{Q}$ est primitivement ramifiée (puisque le degré $\deg_F \mathcal{L}$ d'une place sauvage $\mathcal{L}$ de F est égal à 4).

Dans le cas $\pm d \equiv 1 \pmod 8$ ou $\pm d \equiv 2 \pmod{16}$, l'extension $F/\mathbb{Q}$ ne peut être primitivement ramifiée qu'en un diviseur premier p de $\mathbb{Q}$, divisant l'entier d. De plus, un diviseur premier impair p de $\mathbb{Q}$ est primitif si et seulement si $\log p$ est une $\mathbb{Z}_2$-base de $\deg_{\mathbb{Q}} Dl_{\mathbb{Q}}$, soit $p \equiv \pm 3 \pmod 8$.

R e m a r q u e. Dans cette situation, le conoyau de φ est clairement trivial, si bien que la formule des classes logarithmiques ambiges est aisément applicable.

4. Application au cas (CM)**-primitif.** Nous notons F une extension quadratique de $\mathbb{Q}$, que nous supposons dans ce paragraphe (CM)-primitivement ramifiée (au sens non trivial), si bien que F est une extension non primitivement ramifiée et de la forme $\mathbb{Q}(\sqrt{\pm d})$, où d est un entier sans facteur carré et strictement supérieur à 2.

Ce chapitre se restreignant au cas imprimitif (sinon cf. §3), nous avons les congruences

$$\pm d \equiv 1 \pmod 8 \quad \text{ou} \quad \pm\, d \equiv 2 \pmod{16}.$$

L'une des conséquences immédiates de cette hypothèse de (CM)-primitivité au sens non trivial est, comme nous allons le voir, l'existence d'un élément α de norme 2 dans l'extension $F/\mathbb{Q}$.

4.1. LEMME. *Si $F/\mathbb{Q}$ désigne une extension quadratique de $\mathbb{Q}$, que nous supposons (CM)-primitivement ramifiée au sens non trivial, alors l'unité logarithmique 2 est norme dans l'extension $F/\mathbb{Q}$.*

P r e u v e. Soit d l'entier positif, supposé sans facteur carré, tel que $F = \mathbb{Q}(\sqrt{\pm d})$. Dire que 2 est norme dans l'extension $F/\mathbb{Q}$, c'est dire que les symboles quadratiques de Hilbert $[2, \pm d]_p$ attachés aux places p de $\mathbb{Q}$ valent tous $+1$. Lorsque p est infini ou étranger à d, le symbole $[2, \pm d]_p$ est naturellement trivial. Enfin, lorsque p désigne un diviseur premier impair de d, p est congru à ± 1 modulo 8 (puisque l'extension $F/\mathbb{Q}$ n'est pas primitivement ramifiée), si bien que

$$[2, \pm d]_p = \left(\frac{2}{p}\right) = 1.$$

La formule du produit $\prod_{p \in P} [2, \pm d]_p = 1$, où P désigne l'ensemble des places de $\mathbb{Q}$, établit la trivialité de l'expression $[2, \pm d]_2$. Par conséquent, 2 est norme locale partout dans l'extension $\mathbb{Q}(\sqrt{\pm d})/\mathbb{Q}$ et donc, par le principe de Hasse, norme globale.

Enfin, en notant que le groupe $\widetilde{\mathcal{E}}_{\mathbb{Q}}$ des unités logarithmiques de $\mathbb{Q}$ est engendré par les entiers -1 et 2, et en nous plaçant sous la condition de

(CM)-primitivité au sens logarithmique, nous pouvons convenir que 2 est un représentant d'une classe génératrice du groupe (éventuellement trivial) $H^1(G, \widetilde{Pl}_F)$. Toutes les hypothèses restrictives ayant été faites, nous allons chercher à déterminer l'image par φ de la classe de 2 dans $H^1(G, \widetilde{Pl}_F)$.

Dire que 2 est norme dans l'extension quadratique $\mathbb{Q}(\sqrt{\pm d})/\mathbb{Q}$ revient évidemment à affirmer que $\pm d$ est norme dans l'extension quadratique $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, c'est-à-dire, puisque l'anneau $\mathbb{Z}[\sqrt{2}]$ est principal, qu'il existe deux entiers relatifs u et v tels que l'on ait $u^2 - 2v^2 = \pm d$. En effet, si $\pm d$ est la norme de l'élément α dans l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, alors α s'écrit sous la forme $q \times \prod_{p \in I} \pi_p^{n_p} \overline{\pi}_p^{n'_p}$ où q est un rationnel ne faisant intervenir que les premiers p non décomposés dans l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et I désigne l'ensemble des premiers p se décomposant en deux irréductibles notés π_p et $\overline{\pi}_p$. L'identité $N_{L/K}(\pi_p/\overline{\pi}_p) = 1$ nous permet de supposer que les entiers n_p et n'_p sont de même signe. Cela étant, le radical $\pm d$ étant supposé sans facteur carré, le passage à la norme

$$\pm d = N_{L/K}(\alpha) = q^2 \times \prod_{p \in I} p^{n_p + n'_p}$$

nous donne alors $q = \pm 1$ et $n_p + n'_p = 0$ ou 1, si bien que α est alors un entier de $\mathbb{Z}[\sqrt{2}]$.

Introduisons maintenant les nouvelles notations suivantes :

- $\alpha = (u + \sqrt{\pm d})/v$ et $\beta = u + \sqrt{\pm d}$,
- $\overline{\alpha}$ et $\overline{\beta}$ les conjugués respectifs de α et β.

Nous avons par construction (en abrégeant $N_{F/\mathbb{Q}}$ par N)

$$N(\beta) = \beta\overline{\beta} = (u + \sqrt{\pm d})(u - \sqrt{\pm d}) = u^2 \mp d = 2v^2,$$

et par suite,

$$N(\alpha) = N\left(\frac{\beta}{v}\right) = \frac{N(\beta)}{v^2} = 2,$$

comme attendu. L'étude de la surjectivité de $\overline{\varphi}$ nous suggère l'étude de la parité des $\mathfrak{p}$-valuations logarithmiques de β.

4.2. Lemme. *En conservant les hypothèses et notations précédentes, les $\mathfrak{p}$-valuations logarithmiques de $\beta = u + \sqrt{\pm d}$ sont paires en toute place finie modérée (i.e. impaire) $\mathfrak{p}$ de F.*

Preuve. Nous avons le système suivant :

$$\beta\overline{\beta} = 2v^2, \tag{1}$$

$$\beta + \overline{\beta} = 2u, \tag{2}$$

$$\beta - \overline{\beta} = 2\sqrt{\pm d}, \tag{3}$$

$$2v^2 = u^2 \mp d. \tag{4}$$

Plaçons nous dans le cas où $\mathfrak{p}$ désigne une place de F, au-dessus d'un nombre premier impair p, et raisonnons par l'absurde, en supposant que la $\mathfrak{p}$-valuation de β est impaire. Sous ces hypothèses, $\mathfrak{p}$ divise β. Or, les $\mathfrak{p}$-valuations de β et $\overline{\beta}$ ayant même parité (d'après (1)), $\mathfrak{p}$ divise aussi $\overline{\beta}$, donc u et $\sqrt{\pm d}$ (avec (2) et (3)), et enfin v (avec (4)). Ainsi p divise u et v, ce qui implique d'après (4) que le carré p^2 divise l'entier d, supposé sans facteur carré.

Lorsque $\mathfrak{p}$ désigne une place sauvage $\mathcal{L}$, deux cas interviennent :

4.3. *Le cas décomposé* $\pm d \equiv 1 \pmod 8$. Dans le cas $\pm d \equiv 1 \pmod 8$ (où l'extension locale $F_{\mathcal{L}}/\mathbb{Q}_2$ est triviale), nous imposons, pour des raisons techniques, quelques conditions supplémentaires aux entiers u et v.

4.3.1. LEMME. *Soient F une extension quadratique de $\mathbb{Q}$ (CM)-primitivement ramifiée* (*au sens non trivial*) *et d l'entier naturel*, *supposé sans facteur carré*, *tel que $F = \mathbb{Q}(\sqrt{\pm d})$. En conservant les notations précédemment précisées*, *il est toujours possible*, *lorsque l'entier $\pm d$ est congru à* 1 *modulo* 8, *de choisir les entiers u et v satisfaisant les deux propriétés suivantes* :

$$\begin{cases} u^2 - 2v^2 = \pm d, \\ 2u \mp d + 3 \in 32\mathbb{Z}. \end{cases}$$

Preuve. Ecrivons $\pm d = u^2 - 2v^2$ pour deux entiers u et v. De la congruence $\pm d \equiv 1 \pmod 8$, nous concluons que u est impair, ce qui nous donne $u^2 \equiv 1 \pmod 8$; il suit que v est pair, autrement dit $v \equiv 0 \pmod 4$ ou $v \equiv 2 \pmod 4$.

• 1er cas : pour $v \equiv 0 \pmod 4$, nous pouvons, quitte à changer u en $-u$, supposer $u \equiv -1 \pmod 4$.

• 2ième cas : pour $v \equiv 2 \pmod 4$, choisissons $u \equiv 1 \pmod 4$, et considérons le couple (u', v') défini par

$$u' + v'\sqrt{2} = (u + v\sqrt{2})(1 + \sqrt{2})^2.$$

Nous avons encore $\pm d = {u'}^2 - 2{v'}^2$ avec, maintenant

$$\begin{cases} u' = 3u + 4v \equiv -1 \pmod 4, \\ v' = 2u + 3v \equiv 0 \pmod 4 \end{cases}$$

et le remplacement du couple (u, v) par le couple (u', v') nous ramène au cas précédent.

Cela acquis, écrivons donc $\pm d = u^2 - 2v^2$ avec $u \equiv -1 \pmod 4$, disons $u = -1 + 4a$, et $v \equiv 0 \pmod 4$, disons $v = 4b$. Nous obtenons, comme annoncé,

$$2u \mp d + 3 = 2u - u^2 + 2v^2 + 3 = -2 + 8a - 1 + 8a - 16a^2 + 32b^2 + 3,$$
$$2u \mp d + 3 = -16a(a-1) + 32b^2 \equiv 0 \pmod{32}.$$

L'intérêt de la construction d'un tel élément α provient du lemme suivant :

4.3.2. LEMME. *Sous l'hypothèse de* (CM)*-primitivité au sens non trivial, il existe un diviseur logarithmique* $\mathfrak{B}$ *de degré nul tel que*

$$\widetilde{\operatorname{div}}_F(\beta) = 2\mathfrak{B} + \varrho(\mathcal{L} - \mathcal{L}^\sigma)$$

où ϱ *est l'entier* 0 (*resp.* 1) *si* $\pm d \equiv 1 \pmod{16}$ (*resp.* $\pm d \equiv 9 \pmod{16}$).

Preuve. Compte tenu du lemme 4.2, il s'agit ici d'examiner la $\mathcal{L}$-valuation logarithmique de β :

• Si $\pm d \equiv 1 \pmod{16}$, les complétés en 2 des corps de nombres F et $\mathbb{Q}$ coïncident. Nous sommes alors amenés à faire choix d'une racine de $\pm d$, que nous noterons δ et prendrons congrue à -1 modulo 8. Par suite, il vient successivement :

$$\begin{aligned}(\delta+1)^2 &\equiv 1 + 2\delta + \delta^2 \equiv 0 \pmod{64},\\ \delta &\equiv -\frac{\pm d + 1}{2} \pmod{32},\\ \delta + u &\equiv \frac{2u \mp d - 1}{2} \pmod{32}.\end{aligned}$$

C'est ici qu'intervient la troisième propriété de d, puisqu'elle nous permet d'écrire $2u \mp d - 1 \equiv -4 \pmod{32}$, et donc d'établir la parité de la $\mathcal{L}$-valuation logarithmique de β.

• Si $\pm d \equiv 9 \pmod{16}$, nous faisons alors choix d'une racine de $\pm d$, que nous noterons encore δ et prendrons congrue à 3 modulo 8. Par suite, $\delta + u \equiv (6u \pm d + 9)/6 \pmod{32}$.

Comme $6u \pm d + 9 = 3(2u \mp d + 3) + 4d$, nous avons $6u \pm d + 9 \equiv 4 \pmod{32}$, soit

$$6u \pm d + 9 \ \in 2^{\mathbb{Z}} \times (\pm 1 + 8\mathbb{Z}_2),$$

et enfin, $\delta + u \ \in 2^{\mathbb{Z}} \times (\pm 3 + 8\mathbb{Z}_2)$. Ceci prouve que la $\mathcal{L}$-valuation logarithmique de β est effectivement impaire. Dans les deux cas, $\mathfrak{B} = \frac{1}{2}(\widetilde{\operatorname{div}}_F(\beta) - \varrho(\mathcal{L} - \mathcal{L}^\sigma))$ est effectivement un diviseur logarithmique de degré nul.

Nous concluons alors par le résultat suivant :

4.3.3. PROPOSITION. *Soient* F *une extension quadratique de* $\mathbb{Q}$ (CM)*-primitivement ramifiée et* d *l'entier naturel, supposé sans facteur carré, tel que* $F = \mathbb{Q}(\sqrt{\pm d})$ *sous la contrainte* $\pm d \equiv 1 \pmod 8$. *En désignant par* G *le groupe de Galois de l'extension* $F/\mathbb{Q}$, *on trouve le nombre de classes logarithmiques ambiges de* F *donné selon le cas par la formule correspondante* :

- *ou bien* $\pm d \equiv 1 \pmod{16}$, *auquel cas*

$$|\widetilde{Cl}_F^G| = |\widetilde{Cl}_{\mathbb{Q}}| \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})} |H^1(G, \widetilde{Dl}_F)|;$$

- *ou bien* $\pm d \equiv 9 \pmod{16}$, *auquel cas*

$$|\widetilde{Cl}_F^G| = |\widetilde{Cl}_{\mathbb{Q}}| \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})}.$$

P r e u v e. Avec les notations du lemme 4.3.2, nous obtenons

$$2(\mathfrak{B} + \mathfrak{B}^\sigma) = \widetilde{\operatorname{div}}_F(N\beta) = \widetilde{\operatorname{div}}_F(v^2) = 2\widetilde{\operatorname{div}}_F(v),$$

si bien que

$$\mathfrak{B} + \mathfrak{B}^\sigma = \widetilde{\operatorname{div}}_F(v),$$

puis

$$\begin{aligned} \widetilde{\operatorname{div}}_F(\alpha) &= \widetilde{\operatorname{div}}_F(\beta/v) = \widetilde{\operatorname{div}}_F(\beta) - \widetilde{\operatorname{div}}_F(v) \\ &= 2\mathfrak{B} + \varrho(\mathcal{L} - \mathcal{L}^\sigma) - (\mathfrak{B} + \mathfrak{B}^\sigma) = \mathfrak{B} - \mathfrak{B}^\sigma + \varrho(\mathcal{L} - \mathcal{L}^\sigma); \end{aligned}$$

ce qui nous invite à poser $\mathfrak{A} = \mathfrak{B}^\sigma + \varrho\mathcal{L}^\sigma$. Il vient ainsi $\widetilde{\operatorname{div}}_F(\alpha) = \mathfrak{A}^\sigma - \mathfrak{A}$ avec $\deg_F \mathfrak{A} = \varrho \deg_F \mathcal{L}^\sigma = \varrho \deg_F \mathcal{L}$, soit selon le reste modulo 16 de $\pm d$,

$$\deg_F \mathfrak{A} = \begin{cases} 0 & \text{si } \pm d \equiv 1 \pmod{16}, \\ \deg_F \mathcal{L} & \text{si } \pm d \equiv 9 \pmod{16}. \end{cases}$$

Dans le premier cas, le morphisme φ est nul, si bien qu'il ne peut être surjectif. Dans le second cas, le $\mathbb{Z}_2$-module des degrés des diviseurs logarithmiques de F coïncidant avec le $\mathbb{Z}_2$-module $4[F \cap \mathbb{Q}^c : \mathbb{Q}]\mathbb{Z}_2 = 4\mathbb{Z}_2$, le $\mathbb{Z}_2$-module des degrés des diviseurs ambiges est en fait le $\mathbb{Z}_2$-module $8\mathbb{Z}_2$ puisque l'extension $F/\mathbb{Q}$ est par hypothèse non primitivement ramifiée. Comme le degré de la place sauvage $\mathcal{L}$ est égale à 4, le degré de $\mathcal{L}$ est générateur du $\mathbb{Z}_2$-module $\deg_F Dl_F$ si bien que l'image par φ de l'unité logarithmique 2 n'est pas nulle. Le morphisme φ est donc ici surjectif.

4.4. *Le cas non décomposé* $d \equiv 2 \pmod{16}$. Le cas non décomposé se traite de façon analogue; nous en donnons cependant les différentes étapes.

4.4.1. Lemme. *Sous l'hypothèse de* (CM)*-primitivité au sens non trivial, il existe un diviseur logarithmique* $\mathfrak{B}$ *de degré nul tel que*

$$\widetilde{\operatorname{div}}_F(\beta) = 2\mathfrak{B} + \varrho\mathcal{L}$$

où ϱ *est l'entier égal à* 0 (*resp.* 1) *si* $\pm d \equiv 2 \pmod{32}$ (*resp.* $\pm d \equiv 18 \pmod{32}$).

P r e u v e. Comme pour le lemme 4.3.2, nous examinons la $\mathcal{L}$-valuation logarithmique du nombre β, qui par définition, est paire si et seulement si la norme $2v^2$ de $\beta = u + v\sqrt{\pm d}$ appartient à $\{\pm 1\} \times 2^{\mathbb{Z}} \times (1 + 16\mathbb{Z}_2)$. La relation $u^2 - 2v^2 = \pm d$ nous impose les congruences

$$u^2 \equiv 4 \pmod{32}, \qquad v^2 \equiv \begin{cases} 1 \pmod{16} & \text{si } \pm d \equiv 2 \pmod{32}, \\ 9 \pmod{16} & \text{si } \pm d \equiv 18 \pmod{32}; \end{cases}$$

ce qui achève la démonstration.

Nous concluons là aussi par le résultat analogue :

4.4.2. Proposition. *Soient F une extension quadratique de $\mathbb{Q}$ (CM)-primitivement ramifiée et d l'entier naturel, supposé sans facteur carré, tel que $F = \mathbb{Q}(\sqrt{\pm d})$ sous la contrainte $\pm d \equiv 2 \pmod{16}$. En désignant par G le groupe de Galois de l'extension $F/\mathbb{Q}$, on trouve le nombre de classes logarithmiques ambiges de F donné selon le cas par la formule correspondante :*

- *ou bien $\pm d \equiv 2 \pmod{32}$, auquel cas*
$$|\widetilde{Cl}_F^G| = |\widetilde{Cl}_{\mathbb{Q}}| \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})} |H^1(G, \widetilde{Dl}_F)|;$$
- *ou bien $\pm d \equiv 18 \pmod{32}$, auquel cas*
$$|\widetilde{Cl}_F^G| = |\widetilde{Cl}_{\mathbb{Q}}| \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F \cap \mathbb{Q}^c] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})}.$$

Preuve. Avec les notations du lemme 4.3.2, nous obtenons

$$2(\mathfrak{B} + \mathfrak{B}^\sigma) = \widetilde{\operatorname{div}}_F(N\beta) - 2\varrho\mathcal{L} = 2\widetilde{\operatorname{div}}_F(v) - 2\varrho\mathcal{L},$$

si bien que

$$\mathfrak{B} + \mathfrak{B}^\sigma = \widetilde{\operatorname{div}}_F(v) - \varrho\mathcal{L},$$

puis

$$\widetilde{\operatorname{div}}_F(\alpha) = \widetilde{\operatorname{div}}_F(\beta) - \widetilde{\operatorname{div}}_F(v) = 2\mathfrak{B} + \varrho\mathcal{L} - (\mathfrak{B} + \mathfrak{B}^\sigma) - \varrho\mathcal{L} = \mathfrak{B} - \mathfrak{B}^\sigma;$$

ce qui invite à poser $\mathfrak{A} = \mathfrak{B}^\sigma$. Il vient ainsi $\widetilde{\operatorname{div}}_F(\alpha) = \mathfrak{A}^\sigma - \mathfrak{A}$ avec $\deg_F \mathfrak{A} = -(\varrho/2)\deg_F \mathcal{L}$, soit selon le reste modulo 32 de $\pm d$,

$$\deg_F \mathfrak{A} = \begin{cases} 0 & \text{si } \pm d \equiv 2 \pmod{32}, \\ -\frac{1}{2}\deg_F \mathcal{L} & \text{si } \pm d \equiv 18 \pmod{32}. \end{cases}$$

Dans le premier cas, le morphisme φ est nul, si bien qu'il ne peut être surjectif. Dans le second cas, le degré de la place sauvage $\mathcal{L}$ est égale à 8 si bien que l'entier 2-adique $-\frac{1}{2}\deg_F \mathcal{L}$ est générateur du $\mathbb{Z}_2$-module $\deg_F Dl_F$ et que l'image par φ de l'unité logarithmique 2 n'est pas nulle. Le morphisme φ est donc ici surjectif.

Le paragraphe suivant récapitule enfin ces résultats :

5. Expression de la formule des classes logarithmiques ambiges sur $\mathbb{Q}$. Les propositions 4.3.3 et 4.4.2 nous suggèrent l'examen préalable du 2-groupe des classes logarithmiques du corps $\mathbb{Q}$ des nombres rationnels.

5.1. PROPOSITION. *Le corps $\mathbb{Q}$ des nombres rationnels est 2-logarithmiquement principal.*

P r e u v e. D'après [J$_3$], th. 2.3, le 2-groupe $\widetilde{Cl}_{\mathbb{Q}}$ des classes logarithmiques de $\mathbb{Q}$ s'identifie au groupe de Galois $\mathrm{Gal}(\mathbb{Q}^{\mathrm{lc}}/\mathbb{Q}^{\mathrm{c}})$, où $\mathbb{Q}^{\mathrm{c}}$ est la $\mathbb{Z}_2$-extension cyclotomique de $\mathbb{Q}$ et $\mathbb{Q}^{\mathrm{lc}}$ la pro-2-extension abélienne maximale de $\mathbb{Q}$ qui est localement cyclotomique (i.e. complètement décomposée sur $\mathbb{Q}^{\mathrm{c}}$ en chacune de ses places). Et comme $\mathbb{Q}^{\mathrm{lc}}$ est contenue dans la pro-2-extension abélienne 2-ramifiée maximale de $\mathbb{Q}$ qui n'est autre ici que $\mathbb{Q}^{\mathrm{c}}$ puisque $\mathbb{Q}$ est 2-rationnel au sens de [GJ] ou de [MN], il suit que $\mathbb{Q}^{\mathrm{lc}} = \mathbb{Q}^{\mathrm{c}}$, i.e. $\widetilde{Cl}_{\mathbb{Q}} = 0$.

5.2. THÉORÈME. *Soient F une extension quadratique (CM)-primitivement ramifiée de $\mathbb{Q}$ et d l'entier naturel, supposé sans facteur carré, tel que $F = \mathbb{Q}(\sqrt{\pm d})$. En désignant par G le groupe de Galois de l'extension $F/\mathbb{Q}$, on trouve le nombre de classes logarithmiques ambiges de F donné selon le cas par la formule suivante :*

- 1^{er} *cas : pour* $\pm d \equiv 1 \pmod{16}$ *ou* $\pm d \equiv 2 \pmod{32}$, *il vient*

$$|\widetilde{Cl}_F^G| = \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F\cap\mathbb{Q}^{\mathrm{c}}]\cdot(\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})}|H^1(G, \widetilde{Dl}_F)|;$$

- 2^{nd} *cas : pour* $\pm d \not\equiv 1 \pmod{16}$ *et* $\pm d \not\equiv 2 \pmod{32}$, *il vient*

$$|\widetilde{Cl}_F^G| = \frac{\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q})}{[F : F\cap\mathbb{Q}^{\mathrm{c}}]\cdot(\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})}.$$

R e m a r q u e s. 1. Nous rappelons que dans le cas primitif ou imaginaire, l'extension $F/\mathbb{Q}$ est (CM)-primitivement ramifiée, si bien que les hypothèses du théorème 5.2 s'avèrent considérablement allégées.

2. Lorsque 2 est norme de l'extension $F/\mathbb{Q}$, où l'entier d satisfait, cette fois-ci, l'une des congruences

$$\pm d \not\equiv 9 \pmod{16} \quad \text{ou} \quad \pm\, d \not\equiv 18 \pmod{32},$$

sa classe engendre le premier groupe de cohomologie $H^1(G, \widetilde{Pl}_F) \simeq \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}}/N_{F/\mathbb{Q}}(\widetilde{\mathcal{E}}_F)$, puisque son image par φ n'est pas nulle. L'extension est donc là aussi (CM)-primitivement ramifiée.

3. Malheureusement, en l'absence de l'hypothèse de (CM)-primitivité, aucune conclusion ne peut être établie dans le cas général, comme le témoignent ultérieurement certains calculs numériques.

6. Application aux extensions quadratiques 2-logarithmiquement principales de $\mathbb{Q}$

6.1. *Les extensions quadratiques réelles de* $\mathbb{Q}$. Les hypothèses sur l'entier d étant conservées, nous considérons dans un premier temps les extensions quadratiques réelles $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, et nous donnons une autre formulation de la condition

$$\text{(i)} \qquad \prod_{\mathfrak{p}\mid\infty} d_{\mathfrak{p}}(F/\mathbb{Q}) \cdot \prod_{\mathfrak{p}\nmid\infty} \widetilde{e}_{\mathfrak{p}}(F/\mathbb{Q}) = [F : F \cap \mathbb{Q}^{\mathrm{c}}] \cdot (\widetilde{\mathcal{E}}_{\mathbb{Q}} : \widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}})$$

précisée en introduction. Cette condition nous conduit à introduire les deux notations suivantes :

- t désigne le nombre de diviseurs premiers impairs de $\mathbb{Q}$, ramifiés dans l'extension $F/\mathbb{Q}$,
- 2^s est l'indice dans le groupe $\widetilde{\mathcal{E}}_{\mathbb{Q}}$ du sous-groupe $\widetilde{\mathcal{E}}_{\mathbb{Q}} \cap \mathcal{N}_{F/\mathbb{Q}}$ des unités logarithmiques normes dans l'extension $F/\mathbb{Q}$.

Cela posé, la condition (i) devient

$$\text{(i)}' \qquad \begin{cases} \widetilde{e}_2(F/\mathbb{Q}) = 1 & \text{si } d = 2, \\ 2^t \times \widetilde{e}_2(F/\mathbb{Q}) = 2 \times 2^s & \text{sinon.} \end{cases}$$

6.1.1. LEMME. *La condition* (i) *est vérifiée lorsque* $d = 2$ *et s'écrit sinon sous la forme*

$$t - s = \begin{cases} 1 & \textit{si } d \equiv 1 \pmod 8 \textit{ ou } d \equiv 2 \pmod{16}, \\ 0 & \textit{si } d \not\equiv 1 \pmod 8 \textit{ et } d \not\equiv 2 \pmod{16}. \end{cases}$$

Preuve. Par définition de l'indice de ramification logarithmique en 2, il vient en effet

$$\begin{aligned} \widetilde{e}_2(F/\mathbb{Q}) &= [\mathbb{Q}_2(\sqrt{d}) : \mathbb{Q}_2(\sqrt{d}) \cap \mathbb{Q}_2^{\mathrm{c}}] \\ &= \begin{cases} 1 & \text{si } d \equiv 1 \pmod 8 \text{ ou } d \equiv 2 \pmod{16}, \\ 2 & \text{si } d \not\equiv 1 \pmod 8 \text{ et } d \not\equiv 2 \pmod{16} \end{cases} \end{aligned}$$

et le lemme 6.1.1 est ainsi établi.

Ces derniers résultats adjoints au lemme 3.1, nous pouvons à présent dresser la liste des extensions quadratiques réelles 2-logarithmiquement principales de $\mathbb{Q}$. Notant que l'extension $\mathbb{Q}(\sqrt{2})$ est bien 2-logarithmiquement principale; supposons donc désormais $(t \geq 1)$, et distinguons deux cas :

1$^{\text{er}}$ cas : $d \neq 2$ et ($d \equiv 1 \pmod 8$ ou $d \equiv 2 \pmod{16}$). La condition $t - s = 1$ nous conduit à envisager trois possibilités.

- Le cas $t = 1$ et $s = 0$, auquel cas les extensions obtenues sont

$$\mathbb{Q}(\sqrt{p}) \ \text{ ou } \ \mathbb{Q}(\sqrt{2p}) \quad \text{avec } p \equiv 9 \pmod{16} \quad \text{(cf. §5, rq 2)},$$

ainsi que certaines des extensions

$$\mathbb{Q}(\sqrt{p}) \quad \text{ou} \quad \mathbb{Q}(\sqrt{2p}) \qquad \text{avec } p \equiv 1 \pmod{16}.$$

• Le cas $t = 2$ et $s = 1$, qui nous donne les extensions

$$\mathbb{Q}(\sqrt{pq}) \quad \text{ou} \quad \mathbb{Q}(\sqrt{2pq}) \qquad \text{avec } p \equiv \pm 3 \pmod 8 \text{ et } q \equiv \pm 3 \pmod 8;$$
$$\mathbb{Q}(\sqrt{pq}) \quad \text{ou} \quad \mathbb{Q}(\sqrt{2pq}) \qquad \text{avec } p \equiv -1 \pmod 8 \text{ et } q \equiv -1 \pmod 8.$$

Dans la dernière situation, en effet, ni -1, ni -2 ne sont normes, si bien que la condition de (CM)-primitivité est vérifiée. Ainsi, placés sous les hypothèses du théorème 5.2, nous en déduisons les congruences nécessaires : $p \equiv -1 \pmod{16}$ et $q \equiv -9 \pmod{16}$.

• Le cas $t = 3$ et $s = 2$ enfin, qui nous donne les extensions

$$\mathbb{Q}(\sqrt{pqr}) \quad \text{ou} \quad \mathbb{Q}(\sqrt{2pqr}) \qquad \text{avec } p \equiv 3 \pmod 8,\ q \equiv 5 \pmod 8 \text{ et } r \equiv -1 \pmod 8.$$

2$^{\text{ième}}$ cas : $d \not\equiv 1 \pmod 8$ et $d \not\equiv 2 \pmod{16}$. La condition $t - s = 0$ ouvre ici deux possibilités seulement :

• ou bien $t = s = 1$, auquel cas les extensions obtenues sont

$$\mathbb{Q}(\sqrt{p}) \quad \text{ou} \quad \mathbb{Q}(\sqrt{2p}) \qquad \text{avec } p \equiv -1 \pmod 8 \text{ ou } p \equiv \pm 3 \pmod 8,$$

• ou bien $t = s = 2$, auquel cas les extensions obtenues sont

$$\mathbb{Q}(\sqrt{pq}) \text{ ou } \mathbb{Q}(\sqrt{2pq}) \qquad \text{avec } \begin{cases} p \equiv 3 \pmod 8 \text{ et } q \equiv 5 \pmod 8, \text{ ou} \\ p \equiv \pm 3 \pmod 8 \text{ et } q \equiv -1 \pmod 8. \end{cases}$$

6.1.2. Théorème. *Les extensions quadratiques réelles* 2*-logarithmiquement de* $\mathbb{Q}$ *sont les extensions suivantes* (*où* p, q, r *désignent trois premiers impairs distincts arbitraires de* $\mathbb{N}$) :

• $\mathbb{Q}(\sqrt{2})$,

• $\mathbb{Q}(\sqrt{p})$ *ou* $\mathbb{Q}(\sqrt{2p})$ *avec* $p \equiv -1 \pmod 8$, $p \equiv 9 \pmod{16}$ *ou* $p \equiv \pm 3 \pmod 8$,

• $\mathbb{Q}(\sqrt{pq})$ *ou* $\mathbb{Q}(\sqrt{2pq})$ *avec* $\begin{cases} p \equiv -1 \pmod{16} \textit{ et } q \equiv -9 \pmod{16}, \textit{ ou} \\ p \equiv \pm 3 \pmod 8 \textit{ et } q \not\equiv 1 \pmod 8, \end{cases}$

• $\mathbb{Q}(\sqrt{pqr})$ *ou* $\mathbb{Q}(\sqrt{2pqr})$ *avec* $p \equiv 3 \pmod 8$, $q \equiv 5 \pmod 8$ *et* $r \equiv -1 \pmod 8$

et les extensions de la forme

• $\mathbb{Q}(\sqrt{d})$ *avec* $d = p$ *ou* $d = 2p$ *et* $p \equiv 1 \pmod{16}$ *lorsqu'on peut écrire*

$$-1 = N\left(\frac{u' + \sqrt{d}}{v'}\right) \qquad \textit{avec} \begin{cases} u' \equiv \pm 7 \pmod{16} \textit{ pour } d \equiv 1 \pmod{32}, \\ u' \equiv \pm 1 \pmod{16} \textit{ pour } d \equiv 17 \pmod{32}, \\ u' \equiv \pm 3 \pmod 8 \textit{ pour } d \equiv 2 \pmod{32}. \end{cases}$$

P r e u v e. Examinons le cas des extensions F de la forme $\mathbb{Q}(\sqrt{p})$ ou $\mathbb{Q}(\sqrt{2p})$ (avec $p \equiv 1 \pmod{16}$). Conformément à la preuve du lemme 4.3.2, il est possible d'écrire 2 sous la forme $2 = N((u+\sqrt{d})/v)$ avec $\widetilde{v}_{\mathcal{L}}(u+\sqrt{d})$ paire. L'analogue de la preuve du lemme 4.1 montre que -1 est norme dans l'extension $F/\mathbb{Q}$ si et seulement si $(-1/p) = 1$, i.e. $p \equiv 1 \pmod 4$. Par conséquent, nous pouvons affirmer que dans cette situation d est effectivement norme dans l'extension quadratique $\mathbb{Q}(i)/\mathbb{Q}$, c'est-à-dire puisque l'anneau $\mathbb{Z}[i]$ est principal, qu'il existe deux entiers relatifs u' et v' tels que l'on ait $\beta' = {u'}^2 + {v'}^2 = d$. L'analogue du lemme 4.2 prouve alors que toutes les $\mathfrak{p}$-valuations logarithmiques de $u'+\sqrt{d}$ sont paires en toute place finie modérée $\mathfrak{p}$ de F, si bien que le corps quadratique $F = \mathbb{Q}(\sqrt{d})$ est 2-logarithmiquement si et seulement si $\widetilde{v}_{\mathcal{L}}(u'+\sqrt{d})$ est impaire. Bien entendu, les entiers u' et v' ayant des rôles symétriques, nous pouvons supposer u' impair. Trois cas se distinguent alors :

• Lorsque $d = p$ et $p \equiv 1 \pmod{32}$, il est possible de choisir la racine carrée de p congrue à -1 modulo 16. Notons alors les deux situations suivantes :

— ou bien u' peut être choisi congru à -1 modulo 16, si bien que $\beta' \equiv -2 \pmod{16}$ et F n'est pas 2-logarithmiquement principal,

— ou bien u' peut être choisi congru à 7 modulo 16, si bien que $\beta' \equiv 6 \pmod{16}$ et F est 2-logarithmiquement principal.

• Lorsque $d = p$ et $p \equiv 17 \pmod{32}$, il est possible de choisir la racine carrée de p congrue à 7 modulo 16. Notons alors les deux situations suivantes :

— ou bien u' peut être choisi congru à -1 modulo 16, si bien que $\beta' \equiv 6 \pmod{16}$ et F est 2-logarithmiquement principal,

— ou bien u' peut être choisi congru à 7 modulo 16, si bien que $\beta' \equiv -2 \pmod{16}$ et F n'est pas 2-logarithmiquement principal.

• Lorsque $d = 2p$ et $p \equiv 1 \pmod{16}$, u' et v' ayant des rôles symétriques, les $\mathcal{L}$-valuations logarithmiques attachées à la place sauvage $\mathcal{L}$ de F des nombres $\beta = u' + \sqrt{d}$ et $v' + \sqrt{d}$ sont de même parité. En particulier, $\widetilde{v}_{\mathcal{L}}(\beta)$ est impaire si et seulement si $u' \equiv \pm 3 \pmod 8$.

Le reste est alors immédiat.

R e m a r q u e s. 1. Dans la dernière situation, la condition nécessaire et suffisante obtenue porte uniquement sur les congruences puisque nous sommes assurés de l'existence de $u+\sqrt{d}$ et $u'+\sqrt{d}$. Elle est donc tout à fait explicite et caractérise parfaitement les corps de nombres 2-logarithmiquement principaux de la forme $\mathbb{Q}(\sqrt{p})$ ou $\mathbb{Q}(\sqrt{2p})$ avec $p \equiv 1 \pmod{16}$.

2. Une sous-extension d'un corps de nombres 2-logarithmiquement principal n'est pas forcément 2-logarithmiquement principale. En effet, posons

$K = \mathbb{Q}(\sqrt{p})$ et $L = \mathbb{Q}(i, \sqrt{p})$, où p est un nombre premier congru à 3 modulo 8. Alors l'extension L est 2-logarithmiquement principale (cf. [Th]), bien que le corps de nombres K ne le soit pas.

3. Selon Browkin et Schinzel (cf. [BS], th. 2), les extensions quadratiques dont le 2-Sylow du noyau hilbertien est trivial sont celles de la forme :

- $\mathbb{Q}(\sqrt{2})$,
- $\mathbb{Q}(\sqrt{p})$ ou $\mathbb{Q}(\sqrt{2p})$ avec $p \equiv 3 \pmod 8$ ou $p \equiv 5 \pmod 8$,
- $\mathbb{Q}(\sqrt{p})$ avec $p \equiv 1 \pmod 8$, p ne pouvant pas s'écrire sous la forme $u^2 - 2v^2$ avec $u > 0$, $u \equiv 1 \pmod 4$ et $v \equiv 0 \pmod 4$,
- $\mathbb{Q}(\sqrt{pq})$ avec $p \equiv 3 \pmod 8$ et $q \equiv 3 \pmod 8$.

Cela nous conduit à la proposition suivante :

6.1.3. Scolie. *Les extensions quadratiques réelles dont le* 2*-Sylow du noyau hilbertien est trivial sont* 2*-logarithmiquement principales.*

Preuve. Examinons le seul cas douteux des extensions quadratiques réelles de la forme $F = \mathbb{Q}(\sqrt{p})$ où $p \equiv 1 \pmod{16}$ et dont le 2-Sylow du noyau hilbertien est trivial. D'après les résultats de H. Thomas (cf. [Th], p. 472, Prop. 1, cas 1), le 2-groupe des classes logarithmiques de l'extension biquadratique $K = \mathbb{Q}(i, \sqrt{p})$ est alors cyclique d'ordre 2. En particulier, si Δ désigne le groupe de Galois de l'extension K/F, il coïncide avec son 2-groupe ambige $\widetilde{Cl}_K^{\Delta}$. La formule des classes logarithmiques ambiges nous donne donc la minoration suivante :

$$|\widetilde{Cl}_F| \geq \frac{(\widetilde{\mathcal{E}}_F : \widetilde{\mathcal{E}}_F \cap \mathcal{N}_{K/F})}{2},$$

puisque le conoyau du morphisme $[H^1(\Delta, \widetilde{Pl}_K) \to H^1(\Delta, \widetilde{Dl}_K)]$ déduit de la suite exacte

$$1 \to \widetilde{Pl}_K \to \widetilde{Dl}_K \to \widetilde{Cl}_K \to 1$$

est au plus d'ordre 2. Si ε désigne une unité fondamentale de F, -1 et ε sont deux générateurs du 2-groupe des unités logarithmiques de F. Comme K est totalement imaginaire, -1 ne peut être norme dans l'extension K/F. Supposons en revanche que ε le soit, auquel cas son conjugué $\bar{\varepsilon}$ et leur produit $\varepsilon\bar{\varepsilon} = -1$ sont tous deux normes dans l'extension K/F; ce qui ne peut être. Une vérification analogue montre plus précisément que les classes de -1 et ε sont distinctes modulo $\widetilde{\mathcal{E}}_F \cap \mathcal{N}_{K/F}$. L'indice $(\widetilde{\mathcal{E}}_F : \widetilde{\mathcal{E}}_F \cap \mathcal{N}_{K/F})$ est ainsi égal à 4 et le corps quadratique F n'est pas 2-logarithmiquement principal.

Remarque. En revanche, aucune réciproque n'est envisageable. En effet, l'extension quadratique $\mathbb{Q}(\sqrt{pq})$ où p et q désignent deux nombres premiers distincts congrus à 5 modulo 8 est primitivement ramifiée et 2-logarithmiquement principale, bien que la 2-partie de son noyau hilbertien ne soit pas triviale.

6.1.4. *Exemples numériques.* Dans ces exemples, nous illustrons la situation des corps de nombres

$$\mathbb{Q}(\sqrt{p}) \text{ et } \mathbb{Q}(\sqrt{2p}) \quad \text{avec } p \equiv 1 \pmod{16}.$$

Exemple 1. Lorsque $F = \mathbb{Q}(\sqrt{17})$, nous considérons $\beta' = -1 + \sqrt{17}$ un élément de norme -4^2. Comme $u' = -1$, F est 2-logarithmiquement principal.

Exemple 2. Lorsque $F = \mathbb{Q}(\sqrt{113})$, nous considérons le nombre $\beta' = 7 + \sqrt{113}$ de norme -8^2. Comme $u' \equiv \pm 7 \pmod{16}$, F n'est pas 2-logarithmiquement principal.

Exemple 3. Lorsque $F = \mathbb{Q}(\sqrt{34})$, l'unité logarithmique -1 est norme de l'élément $\alpha' = (5 + \sqrt{34})/3$. Comme $u' \equiv \pm 3 \pmod 8$, l'extension F est ici 2-logarithmiquement principale.

Exemple 4. Lorsque $F = \mathbb{Q}(\sqrt{226})$, l'unité logarithmique -1 est norme de l'élément $\beta' = 15 + \sqrt{226}$. Comme $u' \equiv \pm 1 \pmod 8$, $F = \mathbb{Q}(\sqrt{226})$ n'est pas 2-logarithmiquement principal.

6.2. *Les extensions quadratiques imaginaires.* Les hypothèses sur l'entier d étant conservées, nous considérons à présent les extensions quadratiques imaginaires $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$. De façon analogue, nous démontrons successivement les résultats suivants :

6.2.1. Lemme. *La condition* (i) *est vérifiée lorsque* $d = 2$ *et s'écrit sinon sous la forme*

$$\text{(i)}'' \qquad t - s = \begin{cases} 0 & \textit{si } d \equiv -1 \pmod 8 \textit{ ou } d \equiv -2 \pmod{16}, \\ 1 & \textit{si } d \not\equiv -1 \pmod 8 \textit{ et } d \not\equiv -2 \pmod{16}, \end{cases}$$

où s *peut être l'entier* 1 *ou* 2.

6.2.2. Théorème. *Les extensions quadratiques imaginaires* 2*-logarithmiquement de* $\mathbb{Q}$ *sont les extensions suivantes* (*où* p *et* q *désignent deux nombres premiers impairs distincts arbitraires de* $\mathbb{N}$) :

- $\mathbb{Q}(\sqrt{-2})$,
- $\mathbb{Q}(i)$,
- $\mathbb{Q}(\sqrt{-p})$ *ou* $\mathbb{Q}(\sqrt{-2p})$ *avec* $p \equiv \pm 3 \pmod 8$ *ou* $p \equiv -9 \pmod{16}$,
- $\mathbb{Q}(\sqrt{-pq})$ *ou* $\mathbb{Q}(\sqrt{-2pq})$ *avec* $p \equiv 3 \pmod 8$ *et* $q \equiv 5 \pmod 8$.

Remarque. Selon Browkin et Schinzel (cf. [BS], th. 4), les extensions quadratiques imaginaires dont le 2-Sylow du noyau hilbertien est trivial sont celles de la forme :

- $\mathbb{Q}(\sqrt{-2})$ ou $\mathbb{Q}(i)$,
- $\mathbb{Q}(\sqrt{-p})$ ou $\mathbb{Q}(\sqrt{-2p})$ avec $p \equiv \pm 3 \pmod 8$,

- $\mathbb{Q}(\sqrt{-p})$ avec $p \equiv -1 \pmod 8$,
- $\mathbb{Q}(\sqrt{-pq})$ avec $p \equiv 3 \pmod 8$ et $q \equiv 5 \pmod 8$.

Nous constatons alors :

— que toute extension quadratique imaginaire dont le 2-Sylow du noyau hilbertien est trivial, est 2-logaritmiquement principale, dès qu'elle est 2-primitivement ramifiée sur $\mathbb{Q}$,

— qu'un corps de nombres imaginaire dont la 2-partie du noyau hilbertien est trivial, n'est pas nécessairement 2-logarithmiquement principal (comme l'illustre l'exemple $F = \mathbb{Q}(\sqrt{-31})$).

Références

[BT] H. Bass and J. Tate, *The Milnor ring of a global field*, dans: Algebraic K-Theory II, Lecture Notes in Math. 342, Springer, 1973, 349–428.

[BS] J. Browkin and A. Schinzel, *On Sylow 2-subgroups of $K_2(\mathcal{O}_F)$ for quadratic number fields F*, J. Reine Angew. Math. 331 (1982), 104–113.

[GJ] G. Gras et J.-F. Jaulent, *Sur les corps de nombres réguliers*, Math. Z. 202 (1989), 343–365.

[J$_1$] J.-F. Jaulent, *La théorie de Kummer et le K_2 des corps de nombres*, Sém. Théor. Nombres Bordeaux 2 (1990), 377–411.

[J$_2$] —, *Sur le noyau sauvage des corps de nombres*, Acta Arith. 67 (1994), 335–348.

[J$_3$] —, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux 6 (1994), 301–325.

[JN] J.-F. Jaulent and T. Nguyen Quang Do, *Corps p-rationnels*, *corps p-réguliers*, *et ramification restreinte*, ibid. 5 (1994), 343–363.

[MN] A. Movahhedi and T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, dans: Séminaire de Théorie des Nombres, Paris 1987/1988, Progr. in Math. 81, Birkhäuser, 1990, 155–200.

[Qi] H. Qin, *Computation of $K_2\mathbb{Z}[\sqrt{-6}]$*, J. Pure Appl. Algebra 96 (1994), 133–146.

[Sc] P. Schneider, *Über gewisse Galoiscohomologiegruppen*, Math. Z. 168 (1979), 181–205.

[Sk] M. Skałba, *Generalization of Thue's theorem and computation of the group $K_2\mathcal{O}_F$*, J. Number Theory 46 (1994), 303–322.

[Th] H. Thomas, *Trivialité du 2-rang du noyau hilbertien*, J. Théor. Nombres Bordeaux 6 (1994), 459–483.

Laboratoire de Mathématiques Pures
Université de Bordeaux I
351, cours de la Libération
33405 Talence Cedex, France
E-mail: soriano@math.u-bordeaux.fr

Reçu le 16.5.1995
et révisé le 18.4.1996 (2794)