J. Math. Soc. Japan
Vol. 30, No. 2, 1978

Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $Q(\sqrt{2p})$ et $Q(\sqrt{-2p})$.

Par Bernard ORIAT

(Reçu le 6 juil., 1976)

Introduction.

Soit p un nombre premier congru à 1 modulo 8. Notons $h(d)$ le nombre de classes d'idéaux au sens restreint du corps quadratique $Q(\sqrt{d})$. Nous démontrons ci-après les implications :

A : Si $h(2p)\equiv 0\ (8)$, alors $h(-2p)\equiv 0\ (8)$;

B : Si $h(2p)\equiv 0\ (16)$, alors $h(-2p)\equiv 0\ (16)$.

L'implication A a été énoncée et démontrée à l'aide de formes quadratiques par P. Kaplan ; [3]. Celui-ci a montré d'ailleurs le résultat plus précis :

$h(2p)\equiv 0\ (8)$ si et seulement si $h(-p)\equiv 0\ (8)$ et $h(-2p)\equiv 0\ (8)$.

Le paragraphe I est consacré à la démonstration de l'implication A. Elle est obtenue comme conséquence des résultats exposés dans [6]. Le paragraphe II contient la démonstration de B. Celle-ci n'est pas conséquence de [6], mais la plupart des principes appliqués dans [6] (et en particulier la "Spiegelungsrelation" de Leopoldt [5]) seront encore utilisés. On donne dans le paragraphe III quelques contre-exemples à des implications du même type que celles énoncées ci-dessus.

RAPPELS. Si p est un nombre premier (impair) le 2-groupe des classes d'idéaux (au sens restreint) de $Q(\sqrt{2p})$ est cyclique. Si p n'est pas congru à 1 modulo 8, il est exactement d'ordre 2. Si p est congru à 1 modulo 8, il est d'ordre au moins égal à 4.

De la même façon, le 2-groupe des classes d'idéaux de $Q(\sqrt{-2p})$ est cyclique. Si p n'est pas congru ± 1 modulo 8, il est exactement d'ordre 2. Si p est congru à ± 1 modulo 8, il est d'ordre au moins égal à 4.

NOTATIONS. Dans toute la suite, on supposera que p est premier congru à 1 modulo 8. Il ne sera question que de classes d'idéaux au sens restreint.

Le 2-groupe des classes d'idéaux du corps de nombres L sera noté $\mathfrak{H}_L$.

I. Démonstration de l'implication A.

Rappelons que nous avons démontré dans [6] le résultat suivant :

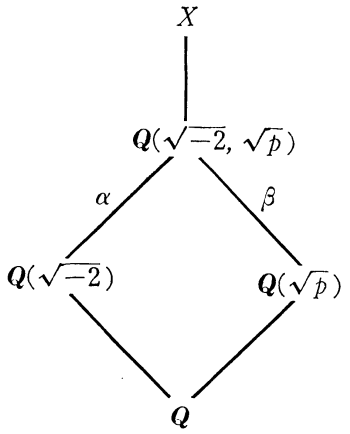
PROPOSITION I. *Soit k un corps de nombres 2-principal et totalement réel. Soit d un élément de k. On suppose qu'aucune des quantités $\sqrt{d}$, $\sqrt{-d}$, $\sqrt{-1}$ n'appartient à k. Soient $K=k(\sqrt{d})$ et $\bar{K}=k(\sqrt{-d})$. Soient $E_{\bar{K}}$ et E_k les groupes d'unités de $\bar{K}$ et k. Soit m une puissance de 2, supérieure à 4 et telle que k contienne $\boldsymbol{Q}_0^{(m)}$, sous-corps réel maximal du m^{eme} corps cyclotomique. Alors la différence des m-rangs des groupes des classes $\mathfrak{H}_K$ et $\mathfrak{H}_{\bar{K}}$ vérifie l'inégalité :*

$$\dim_m \mathfrak{H}_K - \dim_m \mathfrak{H}_{\bar{K}} \leqq \dim_Z E_{\bar{K}} - \dim_Z E_k.$$

Si nous appliquons ce résultat à $k=\boldsymbol{Q}(\sqrt{p})$ et $d=2$, nous obtenons :

$$\dim_4 \mathfrak{H}_{\boldsymbol{Q}(\sqrt{2},\sqrt{p})} \leqq \dim_4 \mathfrak{H}_{\boldsymbol{Q}(\sqrt{-2},\sqrt{p})}.$$

Supposons $h(2p)\equiv 0$ (8). Le corps quadratique $\boldsymbol{Q}(\sqrt{2p})$ possède une extension non ramifiée cyclique de degré 8 et son corps des genres est $\boldsymbol{Q}(\sqrt{2}, \sqrt{p})$. Il s'en suit : $\dim_4 \mathfrak{H}_{\boldsymbol{Q}(\sqrt{2},\sqrt{p})} \neq 0$. D'après l'inégalité ci-dessus, on aura donc : $\dim_4 \mathfrak{H}_{\boldsymbol{Q}(\sqrt{-2},\sqrt{p})} \neq 0$. Soit X la 2-extension abélienne non ramifiée maximale de $\boldsymbol{Q}(\sqrt{-2}, \sqrt{p})$. Soit α (resp. β) l'automorphisme de $\boldsymbol{Q}(\sqrt{-2}, \sqrt{p})/\boldsymbol{Q}(\sqrt{-2})$ (resp. $\boldsymbol{Q}(\sqrt{-2}, \sqrt{p})/\boldsymbol{Q}(\sqrt{p})$) différent de 1 et soit a (resp. b) un prolongement de α (resp. β) à X. Puisque $\boldsymbol{Q}(\sqrt{-2})$ est principal, on a pour tout x de



$\mathrm{Gal}(X/\boldsymbol{Q}(\sqrt{-2}, \sqrt{p}))$: $a^{-1}xa=x^{-1}$. De même $b^{-1}xb=x^{-1}$. D'où $abx=xab$ et l'extension $X/\boldsymbol{Q}(\sqrt{-2p})$ est abélienne. Il s'en suit que X est aussi la 2-extension abélienne non ramifiée maximale de $\boldsymbol{Q}(\sqrt{-2p})$. Nous aurons donc $h(-2p)\equiv 0$ (8). (On aurait pu aussi employer à la place de ce dernier argument, la formule

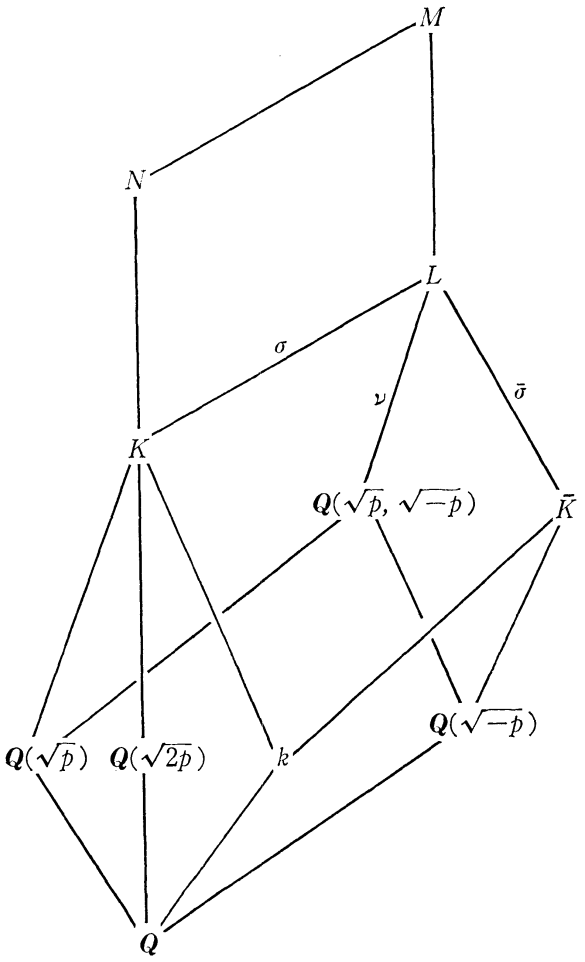
analytique liant le nombre de classes de $\boldsymbol{Q}(\sqrt{-2}, \sqrt{p})$ aux nombres de classes de $\boldsymbol{Q}(\sqrt{-2}, \sqrt{p})$ aux nombres de classes de ses sous-corps quadratiques; [2] § 26; ou bien, la formule des classes ambiges ([1] Théorème IV 1), appliquée à $\boldsymbol{Q}(\sqrt{-2}, \sqrt{p})/\boldsymbol{Q}(\sqrt{-2p})$).

II. Démonstration de l'implication B.

Cette démonstration sera réalisée en deux étapes. Démontrons d'abord la

PROPOSITION II a: *Si* $h(2p)\equiv 0$ (16), *alors il existe une classe d'idéaux de* $\boldsymbol{Q}(\sqrt{2}, \sqrt{-p})$ *d'ordre* 8 *exactement, dont le carré est une classe ambige dans l'extension* $\boldsymbol{Q}(\sqrt{2}, \sqrt{-p})/\boldsymbol{Q}(\sqrt{-2p})$.

DÉMONSTRATION. Posons $k=\boldsymbol{Q}(\sqrt{2})$, $K=\boldsymbol{Q}(\sqrt{2}, \sqrt{p})$, $\bar{K}=\boldsymbol{Q}(\sqrt{2}, \sqrt{-p})$. Supposons donc $h(2p)\equiv 0$ (16). Le corps quadratique $\boldsymbol{Q}(\sqrt{2p})$ possède une ex-



tension non ramifiée cyclique de degré 16 que l'on notera N. Comme le corps des genres de $\boldsymbol{Q}(\sqrt{2p})$ est K, on en déduit que K est inclus dans N et que l'extension N/K est non ramifiée cyclique de degré 8. (On peut alors déduire de la proposition I rappelée ci-dessus, l'existence d'un élément d'ordre 8 dans $\mathfrak{H}_{\bar{K}}$. Mais ce résultat ne suffit pas pour conclure).

Soit $L=\boldsymbol{Q}(\sqrt{2}, \sqrt{p}, \sqrt{-1})$ et soit σ (resp. $\bar{\sigma}$; ν) l'élément de $\mathrm{Gal}(L/\boldsymbol{Q})$ invariant K (resp. $\bar{K}$; $\boldsymbol{Q}(\sqrt{p}, \sqrt{-p})$). Posons $M=NL$. L'extension M/L est une extension de Kummer de degré 8 exactement et on note W son radical, c'est-à-dire :

$$W=\{w\,;\, w\in M,\ w^8\in L^*\}.$$

Si τ appartient à $\mathrm{Gal}(L/\boldsymbol{Q})$, soit t un prolongement de τ à M. Le groupe W/L^* est muni de la structure de $\mathrm{Gal}(L/\boldsymbol{Q})$-module définie par $(wL^*)^\tau=w^tL^*$. Précisons cette structure :

Soit s (resp. $\bar{s}$; v) un prolongement de σ (resp. $\bar{\sigma}$, ν) à M et soit x un élément de $\mathrm{Gal}(M/L)$. On a alors : $s^{-1}xs=x$; $\bar{s}^{-1}x\bar{s}=x^{-1}$ et $v^{-1}xv=x^{-1}$. D'autre part, si ζ désigne une racine 8^{eme} de 1, nous avons : $\zeta^\sigma=\zeta^{-1}$; $\zeta^{\bar{\sigma}}=\zeta^{-1}$ et $\zeta^\nu=\zeta^5$. On déduit alors de la "Spiegelungsrelation" ([5] ou [7]) : $(wL^*)^\sigma=(wL^*)^{-1}$; $(wL^*)^{\bar{\sigma}}=wL^*$ et $(wL^*)^\nu=(wL^*)^3$.

Nous allons montrer que les deux premières égalités peuvent être précisées : L'extension N/K est décomposée sur k. Il en est de même de M/L sur $\bar{K}$. Si $\bar{s}$ est un prolongement d'ordre 2 de $\bar{\sigma}$ à M, on désigne par W' l'ensemble des éléments de W invariants pas $\bar{s}$.

Considérons l'injection canonique de W' dans W. Elle induit un homomorphisme injectif de $W'/\bar{K}^*$ dans W/L^*. Montrons qu'il s'agit d'un isomorphisme : Si w appartient à W, $w^{\bar{s}-1}$ appartient à L^* et vérifie $(w^{\bar{s}-1})^{\bar{\sigma}+1}=1$. Il existe donc un élément α de L^* tel que $\alpha^{\bar{\sigma}-1}=w^{\bar{s}-1}$. On en déduit que $w\alpha^{-1}$ appartient à W' et que $W'/\bar{K}^*$ est isomorphe à W/L^*.

Montrons aussi que si w appartient à W', alors $w^{8(\sigma+1)}$ appartient à k^8. Nous pouvons supposer que s a pour ordre 2. Nous aurons alors $s^2=1$ et $s\bar{s}=\bar{s}s$. Comme w^{s+1} appartient à L^*, on en déduit que w^{s+1} appartient à k, c'est-à-dire que $w^{8(\sigma+1)}$ appartient à k^8. (Ces résultats étaient déjà énoncés dans [6] ; Proposition II b).

Nous pouvons construire maintenant un homomorphisme θ de $W'/\bar{K}^*$ dans $\mathfrak{H}_{\bar{K}}$ de la façon suivante : Si w appartient à W', w^8 appartient à $\bar{K}$ et engendre dans L un idéal qui est une puissance 8^{eme} d'un idéal de L. Cet idéal est invariant par $\bar{\sigma}$ et l'extension $L/\bar{K}$ est non ramifiée. Cet idéal est donc l'étendu d'un idéal $\mathfrak{a}$ de $\bar{K}$ et nous avons : ($A_{\bar{K}}$ étant l'anneau des entiers de $\bar{K}$)

$$w^8A_{\bar{K}}=\mathfrak{a}^8.$$

En associant à $w\bar{K}^*$ la classe de $\mathfrak{a}$, on définit un homomorphisme θ de $W'/\bar{K}^*$ dans $\mathfrak{H}_{\bar{K}}$.

Montrons que cet homomorphisme θ est injectif. Supposons que $\theta(w\bar{K}^*)=cl(\mathfrak{a})$ soit d'ordre 4 au plus. Alors il existe b dans $\bar{K}$ tel que $w^8A_{\bar{K}}=b^2A_{\bar{K}}$, avec $bA_{\bar{K}}=\mathfrak{a}^4$. Il existe une unité ε de $\bar{K}$ telle que $w^8=b^2\varepsilon$. Or le groupe des unités de $\bar{K}$ coïncide avec le groupe des unités de k ([2] Satz 25) et d'autre part, $b^{\sigma+1}A_{\bar{K}}$ est la puissance 4^{eme} d'un idéal de k. On a donc $b^{\sigma+1}=c^4\varepsilon'$, avec c dans k et ε' unité de k. Cette unité est totalement positive. C'est donc un carré dans k et $b^{\sigma+1}$ est un carré dans k. De la relation $w^{8(\sigma+1)}=b^{2(\sigma+1)}\varepsilon^{\sigma+1}=b^{2(\sigma+1)}\varepsilon^2$ on déduit que ε^2 appartient à k^4, c'est-à-dire que ε appartient à L^2 et w^4 appartient à $\bar{K}$. L'élément $w\bar{K}^*$ est donc d'ordre 4 au plus. Comme $W'/\bar{K}^*$ est cyclique d'ordre 8, nous avons montré que θ est injectif.

Utilisons maintenant l'égalité $(wL^*)^\nu=(wL^*)^3$. Si w appartient à W', $w^{8(\nu-3)}$ appartient donc à $L^8\cap\bar{K}$. On en déduit que $w^{8(\nu+1)}$ appartient à $L^4\cap\bar{K}$. Un calcul élémentaire prouve que cette intersection est égale à $\bar{K}^4\cup-\bar{K}^4$. Nous avons donc $w^{8(\nu+1)}=\pm b^4$ avec b dans $\bar{K}$. L'image de w par θ est définie par:

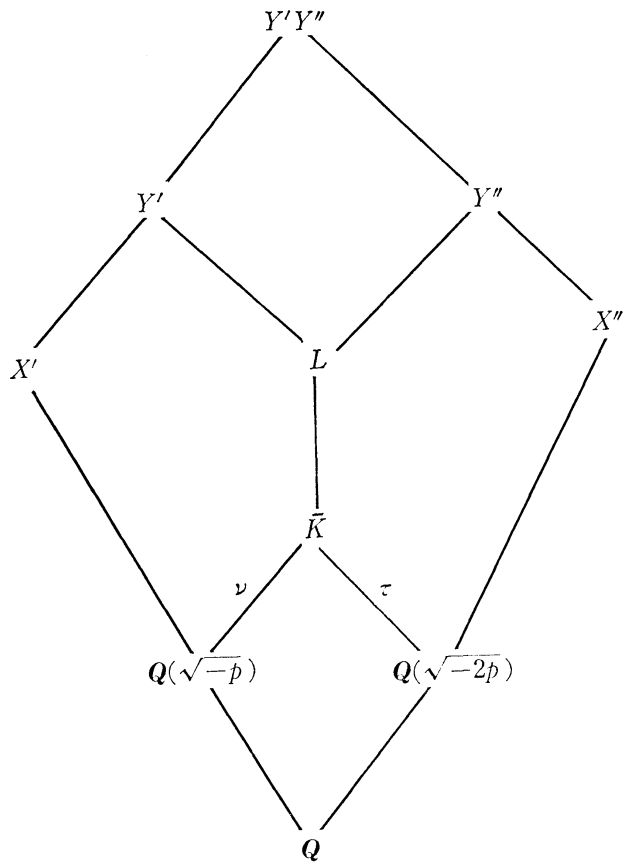
$$w^8A_{\bar{K}}=\mathfrak{a}^8$$

et nous aurons donc $\mathfrak{a}^{2(\nu+1)}=bA_{\bar{K}}$. Ceci montre que $cl(\mathfrak{a})^{2(\nu+1)}$ est principale; c'est-à-dire que $cl(\mathfrak{a})^2$ est ambige dans $\bar{K}/\boldsymbol{Q}(\sqrt{-2p})$.

PROPOSITION II b. *Si* $\boldsymbol{Q}(\sqrt{2},\sqrt{-p})$ *possède une classe d'idéaux d'ordre* 8 *exactement dont le carré est ambige dans* $\boldsymbol{Q}(\sqrt{2},\sqrt{-p})/\boldsymbol{Q}(\sqrt{-2p})$ *et si* $h(-p)\equiv0$ (8), *alors* $h(-2p)\equiv0$ (16).

DÉMONSTRATION. Notons encore $\bar{K}$ le corps $\boldsymbol{Q}(\sqrt{2},\sqrt{-p})$. Désignons par X' (resp. X'') la 2-extension abélienne maximale non ramifiée de $\boldsymbol{Q}(\sqrt{-p})$ (resp. $\boldsymbol{Q}(\sqrt{-2p})$). On posera $Y'=X'\bar{K}$, $Y''=X''\bar{K}$, $G'=\mathrm{Gal}(Y'/\bar{K})$ et $G''=\mathrm{Gal}(Y''/\bar{K})$. Les extensions $\bar{K}/\boldsymbol{Q}(\sqrt{-p})$ et $\bar{K}/\boldsymbol{Q}(\sqrt{-2p})$ sont ramifiées. Les groupes G' et G'' sont donc isomorphes aux 2-groupes des classes d'idéaux de $\boldsymbol{Q}(\sqrt{-p})$ et $\boldsymbol{Q}(\sqrt{-2p})$. Nous désignerons par ν et τ les automorphismes de $\bar{K}$ invariants par $\boldsymbol{Q}(\sqrt{-p})$ et $\boldsymbol{Q}(\sqrt{-2p})$.

Désignons encore par L le corps $\boldsymbol{Q}(\sqrt{2},\sqrt{-1},\sqrt{p})$. Montrons que $L=Y'\cap Y''$. L'inclusion $L\subset Y'\cap Y''$ provient de ce que $\boldsymbol{Q}(\sqrt{-1},\sqrt{p})$ (resp. $\boldsymbol{Q}(\sqrt{-2},\sqrt{p})$) est le corps des genres de $\boldsymbol{Q}(\sqrt{-p})$ (resp. $\boldsymbol{Q}(\sqrt{-2p})$). Réciproquement, désignons par v un prolongement de ν à $Y'\cap Y''$. Si x est un élément de $\mathrm{Gal}(Y'\cap Y''/\bar{K})$, on aura: $v^{-1}xv=x$. D'autre part, en vertu de l'isomorphisme de réciprocité liant $\mathfrak{H}_{\boldsymbol{Q}(\sqrt{-2p})}$ et $\mathrm{Gal}(X''/\boldsymbol{Q}(\sqrt{-2p})$, on aura aussi $v^{-1}xv=x^{-1}$. Il s'en suit que $\mathrm{Gal}(Y'\cap Y''/\bar{K})$ est d'exposant 2. Comme G' est cyclique, on a donc $[Y'\cap Y'':\bar{K}]=2$ ce qui démontre l'égalité $L=Y'\cap Y''$.



Le degré $[Y'Y'':\bar{K}]$ est égal au demi-produit des 2-nombres de classes de $\boldsymbol{Q}(\sqrt{-p})$ et $\boldsymbol{Q}(\sqrt{-2p})$. Or d'après la formule analytique de [2] §26, ce nombre est égal au 2-nombre de classes de $\bar{K}$. La 2-extension abélienne non ramifiée maximale de $\bar{K}$ est donc $Y'Y''$. D'après l'isomorphisme de réciprocité, $\mathrm{Gal}(Y'Y''/\bar{K})$ est isomorphe à $\mathfrak{H}_{\bar{K}}$.

D'autre part le groupe de Galois $\mathrm{Gal}(Y'Y''/\bar{K})$ s'identifie canoniquement au sous-groupe $G'\overset{\circ}{\times}G''$ de $G'\times G''$ formé des couples (x', x'') tels que les restrictions de x' et x'' à L soient égales. Soit t un prolongement de τ à $Y'Y''$. Notons encore t les restricitions de t à Y' et Y''. Nous avons:

$$t^{-1}(x', x'')t=(t^{-1}x't, t^{-1}x''t)=(x'^{-1}, x'').$$

Un élément (x', x'') de $G'\overset{\circ}{\times}G''$ correspond donc à une classe d'idéaux de $\bar{K}$, ambige dans $\bar{K}/\boldsymbol{Q}(\sqrt{-2p})$, si et seulement si $x'^2=1$.

Supposons donc que $\mathfrak{H}_{\bar{K}}$ possède un élément d'ordre 8, dont le carré est ambige dans $\bar{K}/\boldsymbol{Q}(\sqrt{-2p})$. Il existe donc dans $G'\overset{\circ}{\times}G''$ un élément (x', x'') d'ordre 8 tel que $x'^4=1$. L'ordre de x'' est exactement 8. Si $h(-p)\equiv 0$ (8), le

groupe G' est d'ordre multiple de 8 et puisqu'il est cyclique, la restriction de x' à L est égale à 1. Il en sera de même de x''. Puisque G'' est aussi cyclique, x'' est un carré et G'' est d'ordre divisible par 16. Nous avons donc montré que $h(-2p)\equiv 0$ (16).

L'implication B résulte des deux propositions énoncées ci-dessus et de l'implication : $h(2p)\equiv 0$ (8) $\Rightarrow h(-p)\equiv 0$ (8) ([3]).

III. Conjecture et contre-exemples.

Les trois implications suivantes sont fausses. On a écrit à la suite de chacune d'elles le plus petit p qui les contredit :

$$h(2p)\equiv 0 \ (16) \Rightarrow h(-p)\equiv 0 \ (16); \qquad (2593)$$

$$h(-p)\equiv 0 \ (16) \text{ et } h(-2p)\equiv 0 \ (16) \Rightarrow h(2p)\equiv 0 \ (16); \qquad (257)$$

$$h(2p)\equiv 0 \ (32) \Rightarrow h(-2p)\equiv 0 \ (32); \qquad (12641)$$

P. Kaplan a suggéré de préciser l'implication B par la conjecture suivante : Si $h(2p)\equiv 0$ (8), alors : $h(-2p)\equiv 0$ (16) si et seulement si $h(2p)\equiv 0$ (16) ou l'équation $x^2-2py^2=-2$ a des solutions entières.

Bibliographie

[1] G. Gras, Sur les l-classs d'idéaux dans les extensions cycliques relatives de degré premier l, Ann. Inst. Fourier, **23** (1973).

[2] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, Berlin, 1952.

[3] P. Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique et réciprocité biquadratique, J. Math. Soc. Japan, **25** (1973), 596-608.

[4] P. Kaplan et C. Sanchez, Table des 2-groupes des classes d'idéaux au sens restreint et des facteurs principaux des corps quadratiques réels $\mathbf{Q}(\sqrt{2p})$, $p<2\cdot 10^6$, Université de Nancy I (1974).

[5] H. W. Leopoldt, Zur Struktur der l-Klassengruppe galoischer Zahlkörper, J. Reine Angew. Math., **199** (1958) 165-175.

[6] B. Oriat, Relations entre les 2-groupes des classes d'idéaux des extensions quadratiques $k(\sqrt{d})$ et $k(\sqrt{-d})$, Ann. Inst. Fourier, **27** (1977) (à paraître).

[7] B. Oriat, Spiegelungssatz, Publications mathématiques de la Faculté de Besançon, 1975.

Bernard ORIAT
Faculté des Sciences
Mathématiques
Université de Besançon
25030 Besançon Cedex
France