TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 353, Number 7, Pages 2741–2752
S 0002-9947(01)02753-2
Article electronically published on February 7, 2001

SUR LE RANG DU 2-GROUPE DE CLASSES DE $Q(\sqrt{m},\sqrt{d})$ OÙ $m=2$ OU UN PREMIER $p\equiv 1\,(mod\,4)$

ABDELMALEK AZIZI AND ALI MOUHIB

ABSTRACT. **On the rank of the 2-class group of $Q(\sqrt{m},\sqrt{d})$.** Let d be a square-free positive integer and p be a prime such that $p\equiv 1\,(mod\,4)$. We set $K=Q(\sqrt{m},\sqrt{d})$, where $m=2$ or $m=p$. In this paper, we determine the rank of the 2-class group of K.

RÉSUMÉ. Soit $K=Q(\sqrt{m},\sqrt{d})$, un corps biquadratique où $m=2$ ou bien un premier $p\equiv 1\,(mod\,4)$ et d étant un entier positif sans facteurs carrés. Dans ce papier, on détermine le rang du 2-groupe de classes de K.

1. INTRODUCTION

Soit k un corps de nombres. Si k est un corps quadratique, on sait d'après la théorie des genres, déterminer le rang du 2-groupe de classes de k; mais ceci n'est pas simple pour un corps de nombres quelconque. Si k est un corps biquadratique, plusieurs mathématiciens se sont intéressés à ce type de problèmes; en particulier on note les travaux suivants: Dans [Az-93], A. Azizi avait structuré le 2-groupe de classes de tous les corps biquadratiques imaginaires de la forme $Q(\sqrt{-1},\sqrt{d})$ où d est un entier naturel sans facteurs carrés, ayant une 2-partie de nombre de classes égale à 4. De même dans [Be-97], I. Benhamza avait étudiée le même problème pour les corps biquadratiques de la forme $Q(\sqrt{-2},\sqrt{d})$ où d est un entier naturel sans facteurs carrés. De plus dans [Mc-Pa-Ra-95], T. M. McCall, C. J. Parry et R. R. Ranalli avaient déterminé tous les corps biquadratiques imaginaires dont le 2-groupe de classes est cyclique. D'autre part, dans [Si-95], P. J. Sime avait considéré des corps biquadratiques réels K, qui possèdent des sous-corps quadratiques, ayant des 2-groupes de classes élémentaires. Sous ces conditions, il avait donné des éstimations sur le 4-rang du 2-groupe de classes de K.

De notre part, on s'est intéressé aux corps biquadratiques réels $K=Q(\sqrt{m},\sqrt{d})$, tel que $m=2$ ou bien m est un nombre premier avec $m\equiv 1\,(mod\,4)$ et d un entier naturel sans facteurs carrés, et on démontre les résultats suivants, sur le rang du 2-groupe de classes de K:

On note par H le 2-groupe de classes de K, r le nombre des premiers de $Q(\sqrt{m})$ qui se ramifient dans K et e un entier naturel défini par $2^e=[E:\mathcal{N}(K^*)\cap E]$ où E désigne le groupe des unités de $Q(\sqrt{m})$ et $\mathcal{N}$ l'application norme, alors le rang de H $(rangH)$ est égal à $r-1-e$ et de plus on démontre les deux théorèmes suivants:

Théorème 1. *Soient $k=Q(\sqrt{m})$ où $m=2$ ou bien m est un premier $p\equiv 1\,(mod\,4)$, $K=k(\sqrt{d})$ où d est un entier naturel sans facteurs carrés et $S=$*

Received by the editors October 13, 1999 and, in revised form, July 8, 2000.
2000 *Mathematics Subject Classification.* Primary 11R16, 11R29, 11R37.

$\{q_1|d$ *tel que* $(\frac{m}{q_1})=1$ *et* q_1 *premier impair de* $Q\}$. *S'il existe un premier impair* q, *tel que* $q\equiv 3\,(mod\,4)$ *et* $q|d$, *alors* $e=1$ *ou* $e=2$. *Plus précisément on a:*

1) Si $m=2$, *ou* $m=p\equiv 5\,(mod\,8)$, *alors* $rangH=r-2$ *si et seulement si* $\forall q_1\in S$, $(\frac{-1}{q_1})=1$.

2) Si $m=p\equiv 1\,(mod\,8)$, *alors* $rangH=r-2$ *si et seulement si* $\forall q_1\in S$, $(\frac{-1}{q_1})=1$ *et* $\{\ [\ d=2c$ *avec* $(\frac{-1}{c})=1\ ]$ *ou bien* $d\equiv 1\,(mod\,4)\ \}$.

Théorème 2. *Soient* $k=Q(\sqrt{m})$, *tel que* $m=2$ *ou bien* m *est un premier* $p\equiv 1\,(mod\,4)$ *et* $K=k(\sqrt{d})$ *où* d *est un entier naturel sans facteurs carrés, qui n'est pas divisible par les premiers* $q\equiv -1\,(mod\,4)$. *Alors* $e=0$ *ou* $e=1$; *plus précisément on a:*

1) Si $m=p\equiv 1\,(mod\,4)$, *alors* $rangH=r-1$ *si et seulement si* $\forall q|d$ *tel que* $(\frac{q}{p})=1$ *on a* $(\frac{q}{p})_4=(\frac{p}{q})_4$ *et* $[\ (\frac{2}{p})_4=(-1)^{\frac{p-1}{8}}$ *si* $p\equiv 1\,(mod\,8)$ *et* $d=2c\ ]$.

2) Si $m=2$, *alors* $rangH=r-1$ *si et seulement si* $\forall q|d$ *tel que* $q\equiv 1\,(mod\,8)$ *on a* $(\frac{2}{q})_4=(-1)^{\frac{q-1}{8}}$.

A la fin de cet article, on applique nos résultats sur des cas particuliers pour démontrer que le 2-groupe de classes de K est cyclique ou encore qu'il est de type $(2,2)$.

2. Définition et propriétés du symbole du reste normique

Soient k un corps de nombres algébrique et K une extension abélienne de conducteur f. Pour chaque idéal premier $\mathcal{P}$ de k, on désigne par $f_{\mathcal{P}}$ la plus grande puissance de $\mathcal{P}$ qui divise f ($\mathcal{P}$ fini ou infini).

Soient $b\in k^*$ et $\mathcal{P}$ un idéal premier fini ou infini de k. A l'aide du théorème d'approximation, il existe un nombre auxiliaire b_0 vérifiant:

$$b_0\equiv b \bmod f_{\mathcal{P}} \quad \text{et} \quad b_0\equiv 1 \bmod \frac{f}{f_{\mathcal{P}}}.$$

Alors si $(b_0)=\mathcal{P}^nI$ avec $n\in\mathbb{Z}$ et $(I,\mathcal{P})=1$ ($n=0$ si $\mathcal{P}$ est infini), on pose $(\frac{b,K}{\mathcal{P}})=(\frac{K}{I})$ où $(\frac{K}{I})$ désigne l'application d'Artin dans l'extension K/k appliquée à l'idéal I.

Soit m un entier naturel. On suppose que k contient les racines m- ièmes de l'unité et que K est de la forme $K=k(\sqrt[m]{a})$ où $a\in k^*$. Pour $b\in k^*$, on définit le symbole du reste normique par:

$$(\frac{b,a}{\mathcal{P}})_m=\frac{(\frac{b,\,k(\sqrt[m]{a})}{\mathcal{P}})(\sqrt[m]{a})}{\sqrt[m]{a}}$$

où $\mathcal{P}$ est un idéal premier de k.

Si $\mathcal{P}$ ne divise pas le conducteur de $k(\sqrt[m]{a})/k$, on pose:

$$(\frac{a}{\mathcal{P}})_m=\frac{(\frac{k(\sqrt[m]{a})}{\mathcal{P}})(\sqrt[m]{a})}{\sqrt[m]{a}}.$$

Propriétés du symbole du reste normique:

1) $(\frac{b_1b_2,\,a}{\mathcal{P}})_m=(\frac{b_1,\,a}{\mathcal{P}})_m(\frac{b_2,\,a}{\mathcal{P}})_m$,

2) Si $\mathcal{P}$ ne divise pas le conducteur f de l'extension $k(\sqrt[m]{a})/k$ et apparait dans (b) à l'exposant e, alors $(\frac{b,\,a}{\mathcal{P}})=(\frac{a}{\mathcal{P}})_m^{-e}$ où $v_{\mathcal{P}}(b)=e$,

3) $(\frac{b,\,a}{\mathcal{P}})_m=1$, si $\mathcal{P}$ n'apparait ni dans f ni dans (b),

4) $\prod_{\mathcal{P}}(\frac{b,\,a}{\mathcal{P}})_m=1$,

5) $(\frac{b,\,a_1a_2}{\mathcal{P}})_m = (\frac{b,\,a_1}{\mathcal{P}})_m(\frac{b,\,a_2}{\mathcal{P}})_m$,
6) $(\frac{b,\,a}{\mathcal{P}})_m = (\frac{a,\,b}{\mathcal{P}})_m^{-1}$,
7) $(\frac{-x,\,x}{\mathcal{P}})_m = 1\ \forall x \in k$.

3. Rang du 2-groupe de classes de certains corps biquadratiques

Notations:
K: Corps biquadratique réel.
k: Sous-corps quadratique de K de nombre de classes impair.
$(\frac{a,\,d}{\mathcal{P}})$: C'est le symbole du reste normique d'indice 2 qu'on note $(\frac{a,\,d}{\mathcal{P}})_2$.
E: Le groupe des unités de k.
$\mathcal{N}$: L'application norme.
r: Le nombre des premiers de k qui se ramifient dans K.
e: Entier naturel défini par $2^e = [E : E \cap \mathcal{N}(K^*)]$.
ϵ: L'unité fondamentale de k.
H: Le 2-groupe de classes de K.

On sait d'après [Gr-73] que le nombre des 2-classes ambigues de K/k est égal à $2^{r-1-e} = \frac{2^{r-1}}{[E:E\cap\mathcal{N}(K^*)]}$.

Lemme 1. *On garde les mêmes notations que précédemment. Alors le rang de H est égal à $r-1-e$.*

Preuve. Soit f l'homomorphisme de groupes défini de H dans H^2 par:

$[I] \overset{f}{\longmapsto} [I]^2$ où H^2 désigne le sous groupe de H formé par les carrés de H.

L'homomophisme f est surjectif, de plus on a: $Kerf = \{[I] \in H/[I]^2 = 1\}$.

Si $[I] \in Kerf$, alors $[I]^2 = 1$. Or $\mathcal{N}_{K/k}(I) = I^{1+\sigma}$ est un idéal de k et sa classe est d'ordre un diviseur de 2. Comme le nombre de classes de k est impair, alors $[I]^{1+\sigma} = 1$. Ainsi $[I]^\sigma = [I]^{-1} = [I]$, par suite $Kerf$ n'est rien autre que le groupe des 2-classes ambigues de K. D'où $|Kerf| = 2^{r-1-e}$.

Ainsi on a $|H/H^2| = 2^{r-1-e}$ et le rang de H est égal à $r-1-e$. ■

Remarque 1. L'entier e est égal à 0, 1 ou 2.

En effet: On sait que le groupe des unités de H est engendré par -1 et ϵ. Par suite on a:

1) $e = 0$ si et seulement si -1 et ϵ sont des normes dans l'extension K/k.

2) $e = 1$ si et seulement si -1 est une norme et ϵ ne l'est pas, ou bien -1 n'est pas une norme et ϵ ou $-\epsilon$ est une norme dans l'extension K/k.

3) $e = 2$ si et seulement si -1, ϵ et $-\epsilon$ ne sont pas des normes dans l'extension K/k. ■

Lemme 2. *Soient d un entier naturel sans facteurs carrés, $K = k(\sqrt{d})$ et $u \in k^*$ tel que l'idéal (u), engendré par u dans k, est norme d'un idéal de K. Alors u est une norme dans K/k si et seulement si $(\frac{u,\,d}{\mathcal{P}}) = 1$ pour tout premier $\mathcal{P}$ de k qui se ramifie dans K.*

Preuve. Soient $f = \mathcal{P}_1^{u_1}...\mathcal{P}_n^{u_n}$ le conducteur de l'extension K/k et $\mathcal{P}$ un diviseur quelconque de f.

On suppose que u est une norme dans l'extension K/k. Alors il existe $x \in K$, tel que $\mathcal{N}_{K/k}(x) = u$, par suite $\mathcal{N}_{K/k}(x) \equiv u\,(mod\,\mathcal{P}^m)$ où $\mathcal{P}^m$ est la plus grande puissance de $\mathcal{P}$ qui divise le conducteur f de K/k. Ainsi $(\frac{u,\,d}{\mathcal{P}}) = 1$ pour tout premier $\mathcal{P}$ de k qui se ramifie dans K.

Inversement: Si $(\frac{u,\,d}{\mathcal{P}})=1$, pour tout $\mathcal{P}$ premier de k qui se ramifie dans K, alors il existe des $b_i\in K$ tels que: $u\equiv\mathcal{N}_{K/k}(b_i)\,(mod\,\mathcal{P}_i^{u_i})$ où $\mathcal{P}_i^{u_i}$ est la plus grande puissance de $\mathcal{P}_i$ qui apparait dans f. De plus on a:

Soit O_K l'anneau des entiers de K, on a $\mathcal{P}_iO_K=Y_i^2$ où Y_i est un idéal premier de K. D'après le théorème d'approximation on a:

Il existe $b\in K$, tel que $b\equiv b_i\,(mod\,Y_i^{2u_i})$ pour tout $i\in\{1,2,\ldots,n\}$.

Pour $\sigma\in Gal(K/k)$ on a $\sigma(b)\equiv\sigma(b_i)\,(mod\,Y_i^{2u_i})$, par suite

$$\mathcal{N}(b)\equiv\mathcal{N}(b_i)\,(mod\,Y_i^{2u_i}).$$

Puisque $\mathcal{N}(b)$ et $\mathcal{N}(b_i)\in k$, alors $\mathcal{N}(b)\equiv\mathcal{N}(b_i)\,(mod\,\mathcal{P}_i^{u_i})$, d'où $u\equiv\mathcal{N}(b)\,(mod\,\mathcal{P}_i^{u_i})$. Ainsi $u(\mathcal{N}(b))^{-1}\in k_{f,1}$ où $k_{f,1}=\{x\in k^*/\ ((x),f)=1$ et $x\equiv 1\,(mod\,f)\}$.

L'idéal (u) est norme d'un idéal de K, donc $u(\mathcal{N}_{K/k}(b))^{-1}\in k_{f,1}\cap i^{-1}(\mathcal{N}_{K/k}(I_K^f))$ où I_K désigne le groupe des idéaux fractionnaires de K, $I_K^f=\{J$ idéal de $K/(J,f)=1\}$ et i est l'application de K^* dans I_K, défini par $x\overset{i}{\longmapsto}(x)$.

D'après [Ja-73] page 156 on a $k_{f,1}\cap i^{-1}(\mathcal{N}(I_K^f))=k_{f,1}\cap\mathcal{N}(K^*)$, par suite u est une norme dans l'extension K/k. ■

Remarque 2. Si (u) n'est pas norme d'un idéal de K, alors l'implication $\Longleftarrow$ n'est pas toujours vérifiée.

Preuve. Soient $k=Q$, $K=k(\sqrt{p})$ où p est un premier de Q tel que $p\equiv 1\,(mod\,4)$ et $u=p_1q_1$ où p_1 et q_1 sont des premiers de Q qui vérifient $(\frac{p}{p_1})=(\frac{p}{q_1})=-1$. Le nombre p est le seul premier de k qui se ramifie dans K. De plus on a:

$$(\frac{u,p}{p})=(\frac{p_1q_1,p}{p})=(\frac{p,p_1q_1}{p})=(\frac{p_1q_1}{p})^{-v_p(p)}=(\frac{p_1q_1}{p}).$$

Ceci implique que $(\frac{u,\,p}{p})=(\frac{p_1}{p})(\frac{q_1}{p})=1$. D'autre part l'idéal (u) n'est pas norme dans K/k. En effet:

L'idéal (p_1) reste inerte dans K, d'où (p_1) ne peut être norme d'un idéal de K. Ainsi (u) ne peut être norme d'un idéal de K. Par conséquent l'élément u n'est pas une norme dans l'extension K/k. ■

Lemme 3. *Soient d un entier naturel sans facteurs carrés et $K=k(\sqrt{d})$. Si l'idéal (u) de k engendré par u est norme dans l'extension K/k, alors $\prod_{\mathcal{P}|f}(\frac{u,\,d}{\mathcal{P}})=1$ où le produit est pris sur les premiers divisant le conducteur f de l'extension K/k.*

Preuve. On sait que $\prod_{\mathcal{P}}(\frac{u,\,d}{\mathcal{P}})=1$.

On suppose que $\mathcal{P}$ ne se ramifie pas dans K, alors on a $(\frac{u,\,d}{\mathcal{P}})=(\frac{d}{\mathcal{P}})^{-m}$ où $m=v_{\mathcal{P}}(u)$. Puisque l'idéal (u) est norme, alors les premiers divisant (u) qui restent inerte dans K doivent apparaitre dans (u) avec des puissances paires. Ainsi si m est impair, alors $\mathcal{P}$ se décompose complétement dans K et par suite $(\frac{d}{\mathcal{P}})=1$. Ainsi on a $\prod_{\mathcal{P}|f}(\frac{u,\,d}{\mathcal{P}})=1$. ■

Remarque 3. Si l'idéal (u) n'est pas norme dans K, alors le résultat précédent n'est pas toujours vrais.

Preuve. Soient $k=Q$, $K=Q(\sqrt{p})$ où p est un premier de Q qui vérifie $p\equiv 1\,(mod\,4)$ et $u=q$ tel que $(\frac{p}{q})=-1$. Le nombre p est le seul premier de Q qui se ramifie dans K. Par suite on a:

$$\prod_{\mathcal{P}|f}(\frac{u,p}{\mathcal{P}})=(\frac{q,p}{p})=(\frac{p,q}{p})=(\frac{q}{p})^{-v_p(p)}=(\frac{q}{p})=-1.\qquad ■$$

Lemme 4. *Soient p un nombre premier impair de Q qui reste inerte dans k/Q, $\mathcal{P}$ l'idéal premier de k au dessus de p engendré par p, d un entier naturel sans facteurs carrés et $K = k(\sqrt{d})$. On suppose que $\mathcal{P}$ est ramifié dans K/k, alors on a:*

$$\forall u \in \mathbb{Z} \quad (\frac{u,d}{\mathcal{P}}) = 1.$$

Preuve. Si $u = u'b^2$ où u' et b sont deux entiers, alors $(\frac{u,d}{\mathcal{P}}) = (\frac{u',d}{\mathcal{P}})$. On se ramène ainsi au cas où u est sans facteurs carrés.

a) On suppose que $\mathcal{P}$ ne se ramifie pas dans $k(\sqrt{u})/k$.

On a $(\frac{u,\,d}{\mathcal{P}}) = (\frac{d,\,u}{\mathcal{P}}) = (\frac{u}{\mathcal{P}})^{-v_{\mathcal{P}}(d)}$ où $(\frac{u}{\mathcal{P}})$ désigne l'application d'Artin dans l'extension $k(\sqrt{u})/k$ appliquée à l'idéal premier $\mathcal{P}$. Comme p est inerte dans k, alors $\mathcal{P}$ se décompose dans $k(\sqrt{u})/k$. Par conséquent $(\frac{u,\,d}{\mathcal{P}}) = (\frac{u}{\mathcal{P}}) = 1$.

b) On suppose que $\mathcal{P}$ se ramifie dans $k(\sqrt{u})$.

Le fait que l'idéal $\mathcal{P}$ se ramifie dans $k(\sqrt{u})$ implique que $p|u$ (car p est impair). Par suite $(\frac{u,\,d}{\mathcal{P}}) = (\frac{u,\,p}{\mathcal{P}})(\frac{u,\,d'}{\mathcal{P}})$ où $d = d'p$.

On a $(\frac{u,\,d'}{\mathcal{P}}) = (\frac{d'}{\mathcal{P}})^{-1} = (\frac{d'}{\mathcal{P}}) = 1$ (on se ramène au cas a)). Par suite on a $(\frac{u,\,d}{\mathcal{P}}) = (\frac{u,\,p}{\mathcal{P}}) = (\frac{p,\,p}{\mathcal{P}})(\frac{u',\,p}{\mathcal{P}})$ où $u' = \frac{u}{p}$. De plus on a $(\frac{u',\,p}{\mathcal{P}}) = (\frac{p,\,u'}{\mathcal{P}}) = 1$ (même démonstration que dans a)).

Comme $(\frac{p,\,p}{\mathcal{P}}) = (\frac{-1,\,p}{\mathcal{P}})(\frac{-p,\,p}{\mathcal{P}})$, $(\frac{-p,\,p}{\mathcal{P}}) = 1$, et $(\frac{-1,\,p}{\mathcal{P}}) = (\frac{p,\,-1}{\mathcal{P}}) = (\frac{-1}{\mathcal{P}}) = 1$, alors on a:

$$\forall u \in \mathbb{Z} \quad (\frac{u,d}{\mathcal{P}}) = 1. \qquad \blacksquare$$

4. Preuves des théorèmes

On s'intéresse à déterminer le rang du 2-groupe de classes de $K = Q(\sqrt{m},\sqrt{d})$ où $m = 2$ ou bien $m = p \equiv 1\,(mod\,4)$. Dans toute la suite on va supposer que $k = Q(\sqrt{m})$ où $m = p \equiv 1\,(mod\,4)$ ou bien $m = 2$. On commence par rappeler quelques résultats utiles dans la suite.

Soit q un premier impair, on pose $q^* = (-1)^{\frac{q-1}{2}}q$.

Proposition 1. *Soit $F = Q(\sqrt{d_1},\sqrt{d_2})$ où d_1 et d_2 sont deux entiers relatifs sans facteurs carrés. Soient $p_1,\ldots,p_s$ les diviseurs premiers impairs du discriminant D_F de F. Alors le corps de genres au sens restreint de F est donné par la formule suivante:*

$$F_{(*)} = F(\sqrt{p_1^*},...,\sqrt{p_s^*}).$$

Preuve. Voir par exemple [Be-97]. $\blacksquare$

Proposition 2. *Soient $F = Q(\sqrt{d_1},\sqrt{d_2})$ où d_1 et d_2 sont deux entiers relatifs sans facteurs carrés et $F^{(*)}$ le corps de genres au sens large de F. On désigne par $p_1,p_2,...,p_s$ les différents premiers ramifiés dans F/Q et par $e_1,e_2,...,e_s$ leurs indices de ramifications. Alors on a*

$$[F^{(*)}:Q] = \begin{cases} \frac{1}{2}\prod_{i=1}^{i=s} e_i & \text{si } F \text{ est réel et } -1 \text{ n'est pas un reste normique} \\ & \text{modulo un premier } p, \\ \prod_{i=1}^{i=s} e_i & \text{dans le cas contraire.} \end{cases}$$

Preuve. Voir [Kub-56]. $\blacksquare$

Preuve du théorème 1. On suppose qu'il existe un premier q impair, tel que $q \equiv 3\,(mod\,4)$ et $q|d$. On sait que le corps de genres au sens large de K est le sous corps réel maximal du corps de genres au sens restreint du corps K. Ainsi, d'après la proposition 1, on trouve que $[K^{(*)} : Q] = \frac{1}{2}\prod_{i=1}^{i=s} e_i$.

D'après la proposition 2, il existe un premier p' tel que -1 n'est pas un reste normique modulo p'. Par conséquent, ϵ et $-\epsilon$ ne sont pas des normes dans l'extension K/k car sinon on aura:

Il existe $x \in K$ tel que $N_{K/k}(x) = \pm\epsilon$. Puisque $N_{k/Q}(\pm\epsilon) = -1$ on a $N_{K/Q}(x) = -1$. Par suite, -1 est un reste normique dans l'extension K/k modulo chaque premier p. Ce qui est absurde. Ainsi ϵ et $-\epsilon$ ne sont pas des normes dans l'extension K/k. D'où $e = 1$ ou $e = 2$ suivant que -1 est une norme ou non dans K/k.

1) Soit $m = 2$ ou $m = p \equiv 5\,(mod\,8)$.

Soit $\mathcal{P}$ un idéal premier de k, qui se ramifie dans K. Si $\mathcal{P}$ est au dessus de q_1 où q_1 est un premier impair tel que $(\frac{m}{q_1}) = -1$, alors d'après le lemme 4 on a $(\frac{-1,d}{\mathcal{P}}) = 1$.

Si $\mathcal{P}$ est au dessus de q_1 où $q_1 \in S$, alors on a $(\frac{-1,d}{\mathcal{P}}) = (\frac{d,-1}{\mathcal{P}}) = (\frac{-1}{\mathcal{P}})^{v_{\mathcal{P}}(d)} = (\frac{-1}{q_1})$.

Si $\mathcal{P}$ est au dessus de 2, alors le symbole $(\frac{-1,\,d}{\mathcal{P}})$ se calcule à partir de la formule $\prod_{\mathcal{P}|f}(\frac{-1,\,d}{\mathcal{P}}) = 1$ (voir lemme 3). Ainsi -1 est une norme dans l'extension K/k si et seulement si $\forall q_1 \in S \quad (\frac{-1}{q_1}) = 1$. Par suite $rangH = r - 1 - e = r - 2$ si et seulement si $\forall q_1 \in S \quad (\frac{-1}{q_1}) = 1$.

2) Soit $m = p \equiv 1\,(mod\,8)$.

Soit $\mathcal{P}$ un premier de k qui se ramifie dans K. Si $\mathcal{P}$ est au dessus de q_1 où q_1 est tel que $(\frac{m}{q_1}) = -1$, alors d'après le lemme 4 on a $(\frac{-1,\,d}{\mathcal{P}}) = 1$.

Si $\mathcal{P}$ est au dessus de q_1 où $q_1 \in S$, alors on trouve que: $(\frac{-1,d}{\mathcal{P}}) = (\frac{d,-1}{\mathcal{P}}) = (\frac{-1}{\mathcal{P}}) = (\frac{-1}{q_1})$. Si $\mathcal{P}$ est au dessus de 2 et comme $p \equiv 1\,(mod\,8)$, alors il existe deux premiers $\mathcal{P}_1$ et $\mathcal{P}_2$ tels que $2O_k = \mathcal{P}_1\mathcal{P}_2$. Calculons $(\frac{-1,\,d}{\mathcal{P}_i})$ pour $i = 1, 2$. Comme $(\frac{-1,\,d}{\mathcal{P}_1}) = (\frac{-1,\,d}{\mathcal{P}_2})$ (propriétés du symbole du reste normique), on ne s'intéresse qu'au cas $i = 1$.

a) Soit $d \equiv 3\,(mod\,4)$.

On pose $d = qd'$ où $d' \equiv 1\,(mod\,4)$. On a $(\frac{-1,d}{\mathcal{P}_1}) = (\frac{-1,d'}{\mathcal{P}_1})(\frac{-1,q}{\mathcal{P}_1})$ et $(\frac{-1,\,d'}{\mathcal{P}_1}) = (\frac{d'}{\mathcal{P}_1})^0 = 1$ (car $d' \equiv 1\,(mod\,4)$ et $\mathcal{P}_1$ ne se ramifie pas dans $k(\sqrt{d'})$). Ainsi $(\frac{-1,\,d}{\mathcal{P}_1}) = (\frac{-1,\,q}{\mathcal{P}_1})$. Donc on se ramène à calculer $(\frac{-1,\,q}{\mathcal{P}_1})$.

*) On suppose que $(\frac{p}{q}) = 1$.

Si $\mathcal{P}$ est un premier de k au dessus de q, alors $(\frac{-1,\,d}{\mathcal{P}}) = (\frac{-1,\,q}{\mathcal{P}})(\frac{-1,\,d'}{\mathcal{P}})$. Comme $(\frac{-1,\,d'}{\mathcal{P}}) = 1$ (car $d' \equiv 1\,(mod\,4)$), alors $(\frac{-1,\,d}{\mathcal{P}}) = (\frac{-1,\,q}{\mathcal{P}}) = (\frac{-1}{q}) = -1$. Ainsi -1 n'est pas norme dans l'extension K/k.

*) On suppose que $(\frac{p}{q}) = -1$.

On note par H' le 2-groupe de classes de $K' = Q(\sqrt{p}, \sqrt{q})$, r_1 (resp. r_2) le nombre des premiers de $Q(\sqrt{p})$, (resp. $Q(\sqrt{q})$), qui se ramifient dans K' et e_1 (resp. e_2) l'entier défini dans les notations correspondant à l'extension $K'/Q(\sqrt{p})$ (resp. $K'/Q(\sqrt{q})$). On a $r_1 = 3$ et $r_2 = 1$. Or $rangH' = r_1 - 1 - e_1 = r_2 - 1 - e_2$, donc $rangH' = 2 - e_1 = 0 - e_2$. Ceci implique que $e_1 = 2$ et $e_2 = 0$. Ainsi -1 et ϵ ne sont pas des normes dans l'extension $K'/Q(\sqrt{p})$.

Comme $(\frac{p}{q}) = -1$, alors $qO_k = \mathcal{P}'$ est un premier et $(\frac{-1,q}{\mathcal{P}'}) = 1$ (voir lemme 4)

or $e_1 = 2$, par conséquent $(\frac{-1,q}{\mathcal{P}_1}) = (\frac{-1,q}{\mathcal{P}_2}) = -1$. Ainsi si $d \equiv 3\,(mod\,4)$ on a:

$$(\frac{-1,d}{\mathcal{P}_1}) = (\frac{-1,d}{\mathcal{P}_2}) = -1.$$

b) Soit $d = 2c$.

On pose $2O_k = \mathcal{P}_1\mathcal{P}_2$ dans k. On a $(\frac{-1,\,d}{\mathcal{P}_1}) = (\frac{-1,\,2}{\mathcal{P}_1})(\frac{-1,\,c}{\mathcal{P}_1})$. D'autre part on a $(\frac{-1,\,d}{\mathcal{P}_1}) = (\frac{-1,\,d}{\mathcal{P}_2})$ et $(\frac{-1,\,2}{\mathcal{P}_1}) = 1$ (car $-1 = N_{k(\sqrt{2})/k}(1+\sqrt{2})$). Calculons $(\frac{-1,c}{\mathcal{P}_1})$. Si $c \equiv 1\,(mod\,4)$, alors $(\frac{-1,\,c}{\mathcal{P}_1}) = (\frac{c}{\mathcal{P}_1})^0 = 1$ (car $\mathcal{P}_1$ ne se ramifie pas dans $k(\sqrt{c})$). Si $c \equiv 3\,(mod\,4)$, alors comme dans le cas où $d \equiv 3\,(mod\,4)$, on trouve que $(\frac{-1,\,c}{\mathcal{P}_1}) = -1$.

Ainsi -1 est une norme dans l'extension $k(\sqrt{d})/k$ si et seulement si $\forall q_1 \in S$, $(\frac{-1}{q_1}) = 1$ et $\{[d = 2c$ avec $(\frac{-1}{c}) = 1]$ ou $d \equiv 1\,(mod\,4)\}$. Ce qui est équivalent à $rang H = r - 2$. Ainsi le théorème 1 est démontré. ■

Dans la suite on suppose que $k = Q(\sqrt{m})$ où $m = 2$ ou bien $m = p \equiv 1\,(mod\,4)$ et $K = k(\sqrt{d})$ est tel qu' il n'existe aucun premier $q \equiv 3\,(mod\,4)$ divisant d. Pour la suite on aura besoin des deux propositions suivantes:

Proposition 3. *Soient p et q deux premiers différents, tels que $p \equiv q \equiv 1\,(mod\,4)$ et h est le nombre de classes de $Q(\sqrt{p},\sqrt{q})$. Si $(\frac{p}{q}) = 1$, alors h est impair si et seulement si $(\frac{p}{q})_4 \neq (\frac{q}{p})_4$.*

Preuve. Voir [Kuc-95]. ■

Proposition 4. *Soient p un premier, tel que $p \equiv 1\,(mod\,4)$ et h le nombre de classes de $Q(\sqrt{p},\sqrt{2})$. Si $(\frac{2}{p}) = 1$, alors h est impair si et seulement si $(\frac{2}{p})_4 \neq (-1)^{\frac{p-1}{8}}$.*

Preuve. Voir [Kuc-95]. ■

Preuve du théorème 2.

*) Cas où $m = 2$.

Soit $\mathcal{P}$ un premier de k qui se ramifie dans $k(\sqrt{d})$. Par suite $\mathcal{P}$ est au dessus d'un premier impair.

-1 est norme dans l'extension $k(\sqrt{d})/k$, en effet:

Si $\mathcal{P}$ est au dessus d'un premier q, alors: $(\frac{-1,d}{\mathcal{P}}) = (\frac{-1,q}{\mathcal{P}}) = (\frac{q,-1}{\mathcal{P}}) = (\frac{-1}{\mathcal{P}})^{-1} = (\frac{-1}{q}) = 1$, car $q \equiv 1\,(mod\,4)$. Par suite -1 est norme dans l'extension $k(\sqrt{d})/k$. Ainsi on a $e = 0$ ou $e = 1$.

Soit ϵ l'unité fondamentale de $Q(\sqrt{2})$. Calculons $(\frac{\epsilon,\,d}{\mathcal{P}})$.

Si $\mathcal{P}$ est au dessus de q où q est un nombre premier; alors $d = qd'$ où d' est un entier naturel premier avec q. Puisque $\mathcal{P}$ est non ramifié dans $k(\sqrt{d'})$, alors $(\frac{\epsilon,\,d'}{\mathcal{P}}) = 1$. Comme $(\frac{\epsilon,\,d}{\mathcal{P}}) = (\frac{\epsilon,\,q}{\mathcal{P}})(\frac{\epsilon,\,d'}{\mathcal{P}})$, alors le calcul de $(\frac{\epsilon,\,d}{\mathcal{P}})$ revient au calcul de $(\frac{\epsilon,\,q}{\mathcal{P}})$.

-) Si q est un premier vérifiant $(\frac{2}{q}) = -1$, alors le seul premier de k qui se ramifie dans $Q(\sqrt{2},\sqrt{q})$ est $\mathcal{P}$. Ainsi, en utilisant le lemme 3, on trouve que $(\frac{\epsilon,\,q}{\mathcal{P}}) = 1$.

-) Si q est un premier vérifiant $(\frac{2}{q}) = 1$, alors on pose $qO_k = \mathcal{P}_1\mathcal{P}_2$ où $\mathcal{P}_1$ et $\mathcal{P}_2$ sont des premiers de k ramifiés dans $Q(\sqrt{2},\sqrt{q})$. On calcule $(\frac{\epsilon,\,q}{\mathcal{P}_i})$.

Soit H' le 2-groupe de classes de $Q(\sqrt{2},\sqrt{q})$. Soient r et e les entiers définis dans les notations correspondant à l'extension $Q(\sqrt{2},\sqrt{q})/Q(\sqrt{2})$. Comme $(\frac{2}{q}) = 1$, alors

$r = 2$ et par suite $rang H' = 1 - e$. D'après la proposition 4, le nombre de classes de $Q(\sqrt{2}, \sqrt{q})$ est impair si et seulement si $(\frac{2}{q})_4 \neq (-1)^{\frac{q-1}{8}}$. Ce qui est équivalent à $e = 1$.

On a -1 est norme dans l'extension $Q(\sqrt{2}, \sqrt{q})/Q(\sqrt{2})$, ainsi $e = 1$ si et seulement si ϵ n'est pas norme dans l'extension $Q(\sqrt{2}, \sqrt{q})/Q(\sqrt{2})$. Par suite $e = 1$ si et seulement si $\exists i \in \{1, 2\}$ tels que $(\frac{\epsilon, q}{\mathcal{P}_i}) = -1$ (voir lemme 2). D'après le lemme 3 on a $(\frac{\epsilon, q}{\mathcal{P}_1})(\frac{\epsilon, q}{\mathcal{P}_2}) = 1$, d'où $(\frac{\epsilon, q}{\mathcal{P}_1}) = (\frac{\epsilon, q}{\mathcal{P}_2})$. Ainsi

$$(\frac{\epsilon, q}{\mathcal{P}_1}) = (\frac{\epsilon, q}{\mathcal{P}_2}) = -1 \Longleftrightarrow (\frac{2}{q})_4 \neq (-1)^{\frac{q-1}{8}}.$$

Par conséquent si $(\frac{2}{q}) = 1$, alors

$$(\frac{\epsilon, q}{\mathcal{P}_1}) = (\frac{\epsilon, q}{\mathcal{P}_2}) = (\frac{2}{q})_4 (-1)^{\frac{q-1}{8}}.$$

D'où ϵ est norme dans $k(\sqrt{d})/k$ si et seulement si $\forall q | d$, tel que $q \equiv 1 \,(mod\, 8)$ on a $(\frac{2}{q})_4 = (-1)^{\frac{q-1}{8}}$.

*) Cas où $m = p \equiv 1 \,(mod\, 4)$.

Soit $\mathcal{P}$ un premier de k qui se ramifie dans l'extension $k(\sqrt{d})/k$. Si $\mathcal{P}$ est au dessus de q où q est un premier impair, alors comme dans le cas $m = 2$, $(\frac{-1,d}{\mathcal{P}}) = 1$.

Si $\mathcal{P}$ est au dessus de 2, alors $(\frac{-1,d}{\mathcal{P}}) = (\frac{-1,2c}{\mathcal{P}}) = (\frac{-1,2}{\mathcal{P}})(\frac{-1,c}{\mathcal{P}})$ où $d = 2c$ et c un entier naturel impair. D'autre part on a $(\frac{-1,\, c}{\mathcal{P}}) = (\frac{c}{\mathcal{P}}) = 1$ car $c \equiv 1 \,(mod\, 4)$ et $(\frac{-1,\, 2}{\mathcal{P}}) = 1$ car $-1 = \mathcal{N}_{k(\sqrt{2})/k}(1 + \sqrt{2})$. Ainsi -1 est norme dans l'extension $k(\sqrt{d})/k$.

Soit ϵ l'unité fondamentale de $Q(\sqrt{p})$, calculons $(\frac{\epsilon,\, d}{\mathcal{P}})$:

Si $\mathcal{P}$ est au dessus de q où q est un nombre premier y compris le premier 2; alors $d = qd'$ où d' est un entier naturel premier avec q. Comme dans le cas $m = 2$, on trouve que $(\frac{\epsilon,\, d'}{\mathcal{P}}) = 1$. Ainsi le calcul de $(\frac{\epsilon,\, d}{\mathcal{P}})$ revient au calcul de $(\frac{\epsilon,\, q}{\mathcal{P}})$.

-) Si q est un premier vérifiant $(\frac{q}{p}) = -1$, alors le seul premier de k qui se ramifie dans $Q(\sqrt{p}, \sqrt{q})$ est $\mathcal{P}$. En utilisant le lemme 3, on trouve que $(\frac{\epsilon,\, q}{\mathcal{P}}) = 1$.

-) Si q est un premier impair vérifiant $(\frac{p}{q}) = 1$, alors $qO_k = \mathcal{P}_1\mathcal{P}_2$ dans $k = Q(\sqrt{p})$. On refait le même raisonnement que dans le cas où $m = 2$ et en utilisant la proposition 3, on trouve que

$$(\frac{\epsilon,\ q}{\mathcal{P}_1}) = (\frac{\epsilon,\ q}{\mathcal{P}_2}) = (\frac{p}{q})_4 (\frac{q}{p})_4.$$

-) Si $q = 2$ et $(\frac{2}{p}) = 1$, alors $2O_k = \mathcal{P}_1\mathcal{P}_2$ dans k. Avec le même raisonnement que précédemment et en utilisant la proposition 4, on trouve que

$$(\frac{\epsilon, 2}{\mathcal{P}_1}) = (\frac{\epsilon, 2}{\mathcal{P}_2}) = (\frac{2}{p})_4 (-1)^{\frac{p-1}{8}}.$$

En fin ϵ est norme dans $k(\sqrt{d})/k$ si et seulement si $\forall q | d$ tel que $(\frac{p}{q}) = 1$ on a $(\frac{p}{q})_4 = (\frac{q}{p})_4$ et si $p \equiv 1 \,(mod\, 8)$ et $2|d$ alors $(\frac{2}{p})_4 = (-1)^{\frac{p-1}{8}}$. Ainsi le théorème 2 est démontré. ■

5. Applications

Soit K un corps de nombres. On note par $h(K)$ le 2-nombre de classes de K et par $h(m)$ le 2-nombre de classes du corps quadratique $Q(\sqrt{m})$. Dans toute la suite p, q, p_1, q_1, q_2 désignent des nombres premiers.

I-Première application. Soient p un nombre premier tel que $p \equiv 1\,(mod\,4)$, d un entier naturel sans facteurs carrés et $K = Q(\sqrt{p},\sqrt{d})$. Comme au paravant, on désigne par $K^{(*)}$ le corps de genres de K. On suppose que $K^{(*)} = K$; alors les formes possibles de d sont:

1) $d = p_1$ où $p_1 \equiv 1\,(mod\,4)$;
2) $d = q$ où $q \equiv -1\,(mod\,4)$;
3) $d = 2$;
4) $d = 2q$ où $q \equiv -1\,(mod\,4)$;
5) $d = q_1q_2$ où $q_1 \equiv q_2 \equiv -1\,(mod\,4)$.

Théorème 3. *Soient $K = Q(\sqrt{p},\sqrt{d})$ un corps biquadratique et $K^{(*)}$ le corps de genres de K. Si $K^{(*)} = K$ alors le 2-groupe de classes de K est trivial ou cyclique. De plus on a $h(K) = \frac{1}{2}h(pd)$.*

Avant de donner la preuve du théorème 3, on a besoin de la proposition suivante:

Proposition 5. *Soient F un corps de nombres et p un nombre premier. On note par $F_p^{(1)}$ le p-corps de classes de Hilbert de F et par $F_p^{(2)}$ le p-corps de classes de Hilbert de $F_p^{(1)}$. Alors on a:*

Si $F_p^{(1)}/F$ est cyclique alors $F_p^{(1)} = F_p^{(2)}$.

Preuve. Voir [Ta-37]. ■

Preuve du théorème 3. Pour les cas 1 et 3, le théorème 2 implique que le 2-groupe de classes de K est trivial ou cyclique. Les cas 2, 4 et 5 découlent du théorème 1. La théorie des genres montre que le 2-groupe de classes du corps quadratique $Q(\sqrt{pd})$ est cyclique. Puisque $K/Q(\sqrt{pd})$ est une extension abélienne non ramifiée, alors, d'après la proposition 5, les 2-corps de classes de Hilbert de K et de $Q(\sqrt{pd})$ sont identiques. Par suite on a $h(K) = \frac{1}{2}h(pd)$. ■

II-Deuxième application. Soient p un premier tel que $p \equiv 1\,(mod\,4)$, $d = p_1q_1q_2$ avec $q_1 \equiv q_2 \equiv -p_1 \equiv -1\,(mod\,4)$ et $K = Q(\sqrt{p},\sqrt{p_1q_1q_2})$.

Théorème 4. *Soit $K = Q(\sqrt{p},\sqrt{p_1q_1q_2})$ tel que $p \equiv p_1 \equiv -q_1 \equiv -q_2 \equiv 1\,(mod\,4)$. Alors le 2-groupe de classes de K est cyclique si et seulement si l'une des conditions suivantes est vérifiée:*

1) $(\frac{p}{p_1}) = (\frac{p}{q_1}) = (\frac{p}{q_2}) = -1$,
2) $(\frac{p}{p_1}) = -1$ et $(\frac{p}{q_1})(\frac{p}{q_2}) = -1$.

Preuve. Voir théorème 1. ■

On note par H, le 2-groupe de classes de K. Par application du théorème 1, on trouve que $rang H \in \{1,2,3\}$ et $rang H = 3$ si et seulement si $(\frac{p}{p_1}) = (\frac{p}{q_1}) = (\frac{p}{q_2}) = 1$. Dans ce qui suit on s'intéresse à déterminer tous les entiers d pour lesquels le 2-groupe de classes de K est de type $(2,2)$.

Soit E (resp. E_i) le groupe des unités du corps K (resp. $Q(\sqrt{m_i})$) où $m_1 = p$, $m_2 = p_1q_1q_2$ et $m_3 = pp_1q_1q_2$.

On note par $Q'=[E:\prod E_i]$ l'indice des unités de K. Alors d'après [Wa-66] on a la formule suivante

$$(*)\qquad h(K)=\frac{Q'h(p)h(d)h(pd)}{4}.$$

Soient $\epsilon_1,\ \epsilon_2$ et ϵ_3 les unités fondamentales réspectives de $Q(\sqrt{p}),\ Q(\sqrt{p_1q_1q_2})$ et $Q(\sqrt{pp_1q_1q_2})$. Comme $\mathcal{N}_{Q(\sqrt{p})/Q}(\epsilon_1)=-1$, alors on montre que l'indice des unités Q' de K est tel que $Q'=1$ ou $Q'=2$.

Pour déterminer le 2-nombre de classes de $Q(\sqrt{p_1q_1q_2})$ et celui de $Q(\sqrt{pp_1q_1q_2})$, on utilise les résultats de [Ka-76] et [Be-Le-Sn-96].

a) On suppose que deux éléments de $\{(\frac{p}{p_1}),(\frac{p}{q_1}),(\frac{p}{q_2})\}$ valent -1.

a_1) Si $(\frac{p}{p_1})=1$ et $(\frac{p}{q_1})=(\frac{p}{q_2})=-1$, alors $rangH=2$ (voir théorème 1). On distingue les cas suivants:

*) Si $(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=1$, alors $4|h(p_1q_1q_2)$. Or $8|h(pp_1q_1q_2)$ donc $8|h(K)$. Par suite ce cas est à rejeter.

*) Si $(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=-1$, alors $h(p_1q_1q_2)\equiv 2\,(mod\,4)$. Comme $8|h(pp_1q_1q_2)$, par un calcul d'indice on montre que $Q'=2$. Ainsi $8|h(K)$. D'où ce cas est à rejeter.

*) Si $(\frac{p_1}{q_1})(\frac{p_1}{q_2})=-1$, alors $h(p_1q_1q_2)\equiv 2\,(mod\,4)$. Comme $h(pp_1q_1q_2)\equiv 4\,(mod\,8)$, $rangH=2$ et $Q'=1$ ou $Q'=2$, alors de la formule (*) on trouve que $Q'=2$ et $h(K)\equiv 4\,(mod\,8)$.

Conclusion 1. *Soit $K=Q(\sqrt{p},\sqrt{p_1q_1q_2})$ tel que $(\frac{p}{p_1})=-(\frac{p}{q_1})=-(\frac{p}{q_2})=1$. Alors le 2-groupe de classes de K est de type $(2,2)$ si et seulement si $(\frac{p_1}{q_1})(\frac{p_1}{q_2})=-1$.*

b) On suppose qu'un seul élément de $\{(\frac{p}{p_1}),(\frac{p}{q_1}),(\frac{p}{q_2})\}$ est égal à -1.

b_1) Si $(\frac{p}{p_1})=-1$ et $(\frac{p}{q_1})=(\frac{p}{q_2})=1$, alors $rangH=2$ (voir théorème 1). On distingue les cas suivants:

*) Si $(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=1$, alors $4|h(p_1q_1q_2)$. Or $8|h(pp_1q_1q_2)$, donc $8|h(K)$. Ainsi ce cas est à rejeter.

*) Si $(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=-1$, alors $h(p_1q_1q_2)\equiv 2\,(mod\,4)$. Comme $h(pp_1q_1q_2)\equiv 4\,(mod\,8)$, $rangH=2$ et $Q'=1$ ou bien $Q'=2$, alors d'après la formule (*) on trouve que $Q'=2$ et $h(K)\equiv 4\,(mod\,8)$.

*) Si $(\frac{p_1}{q_1})(\frac{p_1}{q_2})=-1$, alors $h(p_1q_1q_2)\equiv 2\,(mod\,4)$. Comme $h(pp_1q_1q_2)\equiv 4\,(mod\,8)$ et $rangH=2$, alors on trouve que $Q'=2$ et $h(K)\equiv 4\,(mod\,8)$.

b_2) Si $(\frac{p}{p_1})=1$ et $(\frac{p}{q_1})(\frac{p}{q_2})=-1$, alors $rangH=2$ (voir théorème 1). On distingue les cas suivants:

*) Si $(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=-1$, alors $h(p_1q_1q_2)\equiv 2\,(mod\,4)$. Comme $h(pp_1q_1q_2)\equiv 4\,(mod\,8)$ et $rangH=2$, alors, comme dans b_1), on trouve que $Q'=2$ et $h(K)\equiv 4\,(mod\,8)$.

*) Si $(\frac{p_1}{q_1})(\frac{p_1}{q_2})=-1$, alors $h(p_1q_1q_2)\equiv 2\,(mod\,4)$. Comme $h(pp_1q_1q_2)\equiv 4\,(mod\,8)$ et $rangH=2$, alors on trouve que $Q'=2$ et $h(K)\equiv 4\,(mod\,8)$.

*) Si $(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=1$, alors $4|h(p_1q_1q_2)$. Or $8|h(pp_1q_1q_2)$ donc $8|h(K)$. Ainsi ce cas est à rejeter.

Conclusion 2. *Soit $K=Q(\sqrt{p},\sqrt{p_1q_1q_2})$ tel que $p\equiv p_1\equiv -q_1\equiv -q_2\equiv 1\,(mod\,4)$ et un seul élément de $\{(\frac{p}{p_1}),(\frac{p}{q_1}),(\frac{p}{q_2})\}$ est égal à -1. Alors pour que le 2-groupe de classes de K soit de type $(2,2)$ il faut et il suffit que l'une des conditions suivantes soit vérifiée:*

1) $(\frac{p}{q_1})=(\frac{p}{q_2})=-(\frac{p}{p_1})=1$ *et* $[(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=-1$ *ou* $(\frac{p_1}{q_1})(\frac{p_1}{q_2})=-1]$,

2) $(\frac{p}{p_1})=1$, $(\frac{p}{q_1})(\frac{p}{q_2})=-1$ *et* $[(\frac{p_1}{q_1})=(\frac{p_1}{q_2})=-1$ *ou* $(\frac{p_1}{q_1})(\frac{p_1}{q_2})=-1]$.

On énonce ainsi le théorème suivant:

Théorème 5. *Soit* $K=Q(\sqrt{p},\sqrt{p_1q_1q_2})$ *tel que* $p\equiv p_1\equiv -q_1\equiv -q_2\equiv 1\,(mod\,4)$. *Alors le 2-groupe de classes de* K *est de type* $(2,2)$ *si et seulement si l'une des conditions suivantes est vérifiée:*

1) $(\frac{p}{p_1})=-(\frac{p}{q_1})=-(\frac{p}{q_2})=1$ *et* $(\frac{p_1}{q_1})(\frac{p_1}{q_2})=-1$,

2) $[\ (\frac{p_1}{q_1})=-1$ *ou* $(\frac{p_1}{q_2})=-1\ ]$ *et* $[\ (\frac{p}{q_1})=(\frac{p}{q_2})=-(\frac{p}{p_1})=1$ *ou* $\{(\frac{p}{p_1})=1$ *et* $(\frac{p}{q_1})(\frac{p}{q_2})=-1\}\ ]$.

Exemples numériques.

I- Première application.

*) On prend $p=133$ et $d=3$.

On a $h(pd)=8$. Alors, d'après le théorème 3, $h(K)\equiv 4\,(mod\,8)$ et le 2-groupe de classes de K est cyclique.

*) On prend $p=113$ et $d=2$.

On a $h(pd)=8$. Alors, d'après le théorème 5, $h(K)\equiv 4\,(mod\,8)$ et le 2-groupe de classes de K est cyclique.

*) On prend $p=13$, $q_1=3$ et $q_2=7$.

On a le 2-groupe de classes de K est trivial.

*) On prend $p=41$ et $d=2$.

On a $h(pd)=4$ et le 2-groupe de classes de K est cyclique d'ordre 2.

*) On prend $p=5$ et $d=219$.

On a $h(pd)=2$ et le 2-groupe de classes de K est trivial.

II- Deuxième application.

*) On prend $p=5$, $p_1=13$, $q_1=11$ et $q_2=19$.

On a $(\frac{p}{p_1})=-1$, $(\frac{p}{q_1})=(\frac{p}{q_2})=1$ et $(\frac{p_1}{q_1})=-1$. Alors, d'après le théorème 5, le 2-groupe de classes de K est de type $(2,2)$.

*) On prend $p=5$, $p_1=29$, $q_1=3$ et $q_2=11$.

On a $(\frac{p}{p_1})=1$, $(\frac{p}{q_2})=-(\frac{p}{q_1})=1$ et $(\frac{p_1}{q_1})=-1$. Alors, d'après le théorème 5, le 2-groupe de classes de K est de type $(2,2)$.

*) On prend $p=5$, $p_1=29$, $q_1=3$ et $q_2=7$.

On a $(\frac{p}{p_1})=1$, $(\frac{p}{q_2})=(\frac{p}{q_1})=-1$ et $(\frac{p_1}{q_2})=-(\frac{p_1}{q_1})=1$. Alors, d'après le théorème 5, le 2-groupe de classes de K est de type $(2,2)$.

*) On prend $p=5$, $p_1=13$, $q_1=3$ et q_2 quelconque.

On a $(\frac{p}{p_1})=-1$ et $(\frac{p}{q_1})=-1$. Alors, d'après le théorème 4, le 2-groupe de classes de K est cyclique.

References

[Az-93] A. Azizi, *Capitulation des 2-classes d'idéaux de* $Q(\sqrt{d};i)$. Thèse. Univ. Laval. Québec. (1993).

[Be-Le-Sn-96] E. Benjamin, F. Lemmermeyer, C. Snyder, *Real quadratic fields with abelien 2-class field tower.* Research institute of mathematics, Orono, January, 1996.

[Be-97] I. Benhamza, *Unités des corps* $Q(\sqrt{d_1},\sqrt{d_2},\sqrt{-d})$ *et application au problème de capitulation sur le corps* $Q(\sqrt{d},\sqrt{-2})$. Thèse. Université Mohamed I. Oujda. (1997).

[Gr-73] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l.* Ann. Inst. Fourier, Grenoble, tome 23, (1973). MR **50:**12967

[Ja-73] G. J. Janusz, *Algebraic number fields.* Academic press, New York-London. (1973). MR **51:**3110

[Ka-73] P. Kaplan, *Divisibilité par 8 du nombre de classes des corps quadratiques dont le 2-groupe des classes est cyclique et réciprocité biquadratique.* J. Math. Soc. Japan. vol 25, No 4. (1973). MR **48:**2113

[Ka-76] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques.* J. Reine. Angew. Math. 283/284. (1976). 313-363. MR **53:**2896

[Ki-76] H. Kisilevsky, *Number fields with class number congruent to 4 modulo 8 and Hilbert's theorem 94*. J. Number Theory 8, (1976). 271-279. MR **54:**5188

[Kub-56] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper.* Nagoya Math. J, 10 (1956), 65-85. MR **18:**643e

[Kuc-95] R. Kucera, *On the parity of the class number of a biquadratic field.* J. Number Theory 52.43-52 (1995). MR **96e:**11139

[Kur-43] S. Kuroda, *Über den Dirichletschen Zahlkörper* J. Fac. Sc. Imp. Univ. Tokyo Sect. I, 4 (1943). 383-406.

[Mc-Pa-Ra-95] T. M. McCall, C. J. Parry, R. R. Ranalli, *On imaginary bicyclic biquadratic fields with cyclic* 2*-class group.* J. Number Theory 53, 88-99 (1995). MR **96e:**11131

[Si-95] P. J. Sime, *On the ideal class group of real biquadratic fields.* Trans. Amer. Math. Soc. 347, 4855-4876 (1995). MR **96c:**11130

[Ta-37] O. Taussky, *A remark on the class field tower.* J. London Math. Soc. 12 (1937). 82-85.

[Wa-66] H. Wada, *On the class number and the unit group of certain algebraic number fields.* J. Fac. Sci. Univ. Tokyo Sect. I 13 (1966), 201-209. MR **35:**5414

Département de Mathématiques, Faculté des Sciences, Université Mohammed 1, Oujda, Maroc

E-mail address: azizi@sciences.univ-oujda.ac.ma

Département de Mathématiques, Faculté des Sciences, Université Mohammed 1, Oujda, Maroc