Canad. Math. Bull. Vol. **54** (2), 2011 pp. 330–337
doi:10.4153/CMB-2011-006-9


# Sur la borne inférieure du rang du 2-groupe de classes de certains corps multiquadratiques

A. Mouhib

*Résumé.* Soient $p_1, p_2, p_3$ et $q$ des nombres premiers distincts tels que $p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4$, $k = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{q})$ et $\mathrm{Cl}_2(k)$ le 2-groupe de classes de $k$. A. Fröhlich a démontré que $\mathrm{Cl}_2(k)$ n'est jamais trivial. Dans cet article, nous donnons une extension de ce résultat, en démontrant que le rang de $\mathrm{Cl}_2(k)$ est toujours supérieur ou égal à 2. Nous démontrons aussi, que la valeur 2 est optimale pour une famille infinie de corps $k$.

*Abstract.* Let $p_1, p_2, p_3$ and $q$ be distinct prime numbers such that $p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4$, $k = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{q})$ and $\mathrm{Cl}_2(k)$ the 2-class group of $k$. A. Fröhlich has shown that $\mathrm{Cl}_2(k)$ can never be trivial. In this article, we give an extension of this result by proving that the rank of $\mathrm{Cl}_2(k)$ is greater or equal to 2. Moreover, we prove that there exist infinitely many fields $k$ in which the rank of $\mathrm{Cl}_2(k)$ is equal to 2.

## 1 Introduction

Dans [F], A. Fröhlich a étudié la parité du nombre de classes des corps multiquadratiques réels. Utilisant les extensions centrales, il a donné une méthode permettant de déterminer les corps multiquadratiques réels dont le 2-groupe de classes est trivial. Particulièrement, il a sélectionné certains corps biquadratiques et triquadratiques dont le discriminant est divisible par au plus trois nombres premiers et le 2-groupe de classes est trivial [F, Theorem 5.1 and addenda I and II to Theorem 5.6]. D'autres travaux, se basant sur la théorie des unités circulaires ont été consacré à l'étude du problème de la trivialité du 2-groupe de classes des corps multiquadratiques réels retrouvant, ainsi les résultats de [F]. Notamment dans [Ku], R. Kučera a étudié la parité du nombre de classes des corps biquadratiques $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$ où $p_1$ et $p_2$ sont des nombres premiers non congrus à $-1$ modulo 4. Dans [B-1] et [B-2], M. Bulant a étudié la parité du nombre de classes des corps de la forme $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ et $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4}, \sqrt{p_5})$ où $p_1, \dots, p_5$ sont des nombres premiers non congrus à $-1$ modulo 4.

Dans cet article, on va étudier le rang du 2-groupe de classes de certains corps multiquadratiques de degré $2^4$ sur $\mathbf{Q}$. Précisément, soient $p_1, p_2, p_3$ et $q$ des nombres premiers distincts tels que

$$p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4 \quad \text{et} \quad k = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{q}).$$

Reçu par la rédaction le 10 avril, 2008.
Publié electronique au 26 janvier, 2011.
Classification (AMS) par sujet: **11R29**, 11R11.
Mots clés: class group, units, multiquadratic number fields.

D'après [F, Theorem 5.6], le 2-groupe de classes de $k$ est toujours pair. Notre premier objectif est donc d'améliorer ce résultat, en démontrant que le rang du 2-groupe de classes du corps multiquadratique $k$ est supérieur ou égal à 2. Pour le deuxième objectif, nous déterminons une famille infinie de corps $k$ dont le rang du 2-groupe de classes est exactement égal à 2. Notons que dans [M-M], nous avons démontré les mêmes résultats pour les corps multiquadratiques $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$ où $p_1, p_2, p_3$ et $p_4$ sont des nombres premiers non congrus à $-1$ modulo 4.

## 2 Préliminaires

Soit $G$ un $p$-groupe abélien. On désigne par $\operatorname{rang}(G)$, la dimension de $G/G^p$ vu comme un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel.

Soient $K/k$ une $p$-extension galoisienne de corps de nombres à groupe de Galois $G$. On définit le corps de genres de $K/k$, qu'on note par $G(K/k)$, comme l'extension maximale non ramifiée sur $K$ pour tous les premiers finis et infinis et qui est le composé de $K$ par une extension abélienne sur $k$. Soit de plus, $L$ une extension galoisienne sur $k$ contenant $K$. On suppose que le groupe $\operatorname{Gal}(L/K)$ est contenu dans le centre du groupe $\operatorname{Gal}(L/k)$, alors on dit que $L$ est une extension centrale de $K/k$. Sous cette hypothèse, il est clair que $L/K$ est abélienne. Notons par $K_p^{(1)}$ le $p$-corps de classes de Hilbert de $K$. L'extension centrale maximale de $K/k$ contenue dans $K_p^{(1)}$, notée $Z(K,k)$ est appelé corps de classes central de $K/k$.

Notons par $\mathcal{M}(G) = H^2(G, \mathbf{Q}/\mathbf{Z})$ le multiplicateur de Schur de $G$ et $E_k$ le groupe des unités de $k$. Supposons que $K/k$ est non ramifiée. Les résultats standards de la théorie du corps de classes donnent la suite exacte suivante de groupes abéliens (voir par exemple [B-L-S]) :

$$1 \longrightarrow E_k/E_k \cap N_{K/k}(K^*) \longrightarrow \mathcal{M}(\hat{G}) \longrightarrow \operatorname{Gal}\big(Z(K,k)/G(K/k)\big) \longrightarrow 1$$

où $\mathcal{M}(\hat{G})$ désigne le dual de $\mathcal{M}(G)$ et $K^*$ le groupe multiplicatif de $K$. Ce qui permet d'obtenir l'isomorphisme non canonique de groupes suivant :

$$(*) \qquad \operatorname{Gal}\big(Z(K,k)/G(K/k)\big) \simeq \mathcal{M}(\hat{G})/\big(E_k/E_k \cap N_{K/k}(K^*)\big).$$

Supposons que $K/k$ est une extension quadratique et que le nombre de classes de $k$ est impair, en utilisant la formule des classes ambiges, on trouve que (voir par exemple [A-M-1]) :

$$\operatorname{rang}\big(\mathrm{Cl}_2(K)\big) = \operatorname{Ram}(K/k) - \operatorname{rang}\big(E_k/E_k \cap N_{K/k}(K^{(*)})\big) - 1,$$

où $\operatorname{Ram}(K/k)$ désigne le nombre des premiers de $k$ ramifiés dans $K$.

## 3 Résultats

Nous aurons besoin de certains résultats sur les unités des corps quadratiques. Nous donnons, ainsi des informations sur l'indice des unités dans certaines extensions à groupe de Galois isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Pour tout entier naturel $n$, notons $\varepsilon_n$ l'unité fondamentale du corps quadratique $\mathbf{Q}(\sqrt{n})$.

https://doi.org/10.4153/CMB-2011-006-9 Published online by Cambridge University Press

***Lemme 3.1*** *Soient $n$ un entier naturel, $K = \mathbf{Q}(\sqrt{n})$ un corps quadratique de discriminant $D$. Supposons que $N_{K/\mathbf{Q}}(\varepsilon_n) = 1$, alors il existe un entier naturel $m$ sans facteur carré divisant $D$ tel que $m\varepsilon_n$ est un carré dans $K$.*

**Preuve** (1) Supposons que $n \equiv 1 \pmod 4$ (ici $D = n$), notons $\varepsilon_n = \frac{x}{2} + \frac{y}{2}\sqrt{n}$ où $x$ et $y$ sont deux entiers. D'après les hypothèses, on a $N_{K/\mathbf{Q}}(\varepsilon_n) = 1$, alors $(x-2)(x+2) = ny^2$. On a $(x-2, x+2)$ divise 4. S'il existe deux entiers $y_1$ et $y_2$ vérifiant les deux équations suivantes :

$$(x \pm 2) = 2n' y_1^2, \quad 2y_1y_2 = y,$$
$$(x \mp 2) = 2n'' y_2^2, \quad n'n'' = n,$$

alors $2 = y_2^2 n'' - y_1^2 n'$. Comme $y_2^2 n'' - y_1^2 n'$ est pair et $n = n'n''$ est impair, nous trouvons que si l'un des entiers $y_1$ et $y_2$ est pair, alors les deux sont pairs. D'autre part, si $y_1$ et $y_2$ sont impairs, alors $y_2^2 n'' - y_1^2 n' \equiv n'' - n' \pmod 4$ et comme $n \equiv 1 \pmod 4$, alors $y_2^2 n'' - y_1^2 n' \equiv 0 \pmod 4$, ce qui est absurde. Supposons qu'il existe deux entiers $y_1$ et $y_2$ tels que $y_1 y_2 = y$ vérifiant les deux équations suivantes :

$$(x \pm 2) = n y_1^2,$$
$$(x \mp 2) = y_2^2.$$

Si on pose $w = \sqrt{n}y_1 + y_2$, alors $w^2 = 4\varepsilon_n$, il s'ensuit que $\sqrt{\varepsilon_n} = \frac{w}{2} \in \mathbf{Q}(\sqrt{n})$. Ce qui contredit le fait que $\varepsilon_n$ est l'unité fondamentale de $\mathbf{Q}(\sqrt{n})$. Ainsi l'unique possibilité est l'existence de quatre entiers $y_1, y_2, n'$ et $n''$ tels que $y_1 y_2 = y$ et $n'n'' = n$ $(n', n'' \neq 1)$ vérifiant les deux équations suivantes :

$$(x \pm 2) = n' y_1^2,$$
$$(x \mp 2) = n'' y_2^2,$$

Notons $Z = y_1\sqrt{n'} + y_2\sqrt{n''}$, alors $Z^2 = 4\varepsilon_n$, donc

$$\sqrt{\varepsilon_n} = \frac{y_1}{2}\sqrt{n'} + \frac{y_2}{2}\sqrt{n''}.$$

Ce qui montre que $n'\varepsilon_n$ est un carré dans $K$.

(2) Supposons que $n \not\equiv 1 \pmod 4$ (ici $D = 4n$), alors $\varepsilon_n = x + y\sqrt{n}$, où $x$ et $y$ sont deux entiers. On a $N_{K/\mathbf{Q}}(\varepsilon_n) = 1$, alors $(x-1)(x+1) = ny^2$. Utilisant les mêmes techniques que dans le premier cas, nous démontrons qu'il existe quatre entiers $n'$, $n''$, $y_1$ et $y_2$ vérifiant les équations suivantes :

$$(x \pm 1) = 2^i n' y_1^2,$$
$$(x \mp 1) = 2^i n'' y_2^2,$$
$$2^i y_1 y_2 = y \quad \text{et} \quad i \in \{0, 1\},$$
$$n'n'' = n.$$

Soit $Z = y_1\sqrt{2^i n'} + y_2\sqrt{2^i n''}$, alors $Z^2 = 2\varepsilon_n$, par suite

$$\sqrt{\varepsilon_n} = y_1\sqrt{2^{i-1}n'} + y_2\sqrt{2^{i-1}n''}.$$

Ce qui montre que $n'\varepsilon_n$ ou $2n'\varepsilon_n$ est un carré dans $K$. Le lemme est donc démontré. ∎

***Remarque*** Il n'est pas difficile de voir que l'entier naturel $m$ du lemme doit être différent de $n$, car sinon, $n\varepsilon_n$ serait un carré dans $K$. Ce qui contredit le fait que $\varepsilon_n$ est l'unité fondamentale de $K$.

Dans tout ce qui suit, on désigne par $p_1, p_2, p_3$ et $q$ des nombres premiers distincts tels que

$$p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4,\ d = p_1p_2p_3q \text{ et } k = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{q}).$$

Introduisons le corps quadratique $F = \mathbf{Q}(\sqrt{d})$.

***Proposition 3.2*** *Supposons qu'il existe $i, j \in \{1, 2, 3, 4\}$ distincts tels que $(\frac{p_i}{p_j}) = -1$, alors l'indice des unités $(E_F : E_F \cap N_{k/F}(k^*))$ est au plus égal à 2.*

**Preuve** Pour fixer les idées, supposons que $(\frac{p_1}{p_2}) = -1$. Il est clair que $E_F$ est engendré par les unités $-1$ et $\varepsilon_d$. Montrons que $-1$ est norme d'un élément dans l'extension $k/F$. Introduisons le corps triquadratique contenu dans

$$k : M = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{d}).$$

On a l'unité

$$u = \sqrt{\varepsilon_{p_1}\varepsilon_{p_2}\varepsilon_{p_1p_2}} \in \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$$

[Kur]. Par suite, comme $N_{\mathbf{Q}(\sqrt{p_1})/\mathbf{Q}}(\varepsilon_{p_1}) = -1$, alors on a :

$$N_{M/F}(u) = N_{\mathbf{Q}(\sqrt{p_1},\sqrt{d})/F}\big(N_{M/\mathbf{Q}(\sqrt{p_1},\sqrt{d})}(u)\big) = N_{\mathbf{Q}(\sqrt{p_1})/\mathbf{Q}}(\varepsilon_{p_1}) = -1.$$

Ainsi, $-1$ est norme d'une unité dans l'extension $M/F$. Comme $k/M$ est une extension quadratique non ramifiée, alors $-1$ est norme d'un élément dans l'extension $k/F$. Dans ce qui suit, nous allons démontrer que $\varepsilon_d^2$ est norme d'un élément dans l'extension $k/F$.

D'après le lemme 3.1, il existe un entier naturel $m$ sans facteur carré divisant $2d$ tel que $m\varepsilon_d$ est un carré dans $F$. Ce qui entraîne que $\sqrt{\varepsilon_d} \in \mathbf{Q}(\sqrt{m}, \sqrt{d})$. Supposons que $m$ est impair, alors pour toute sous-extension propre $K$ de $k/\mathbf{Q}(\sqrt{m}, \sqrt{d})$, on a

$$N_{K/F}(\sqrt{\varepsilon_d}) = N_{\mathbf{Q}(\sqrt{m},\sqrt{d})/F}\big(N_{K/\mathbf{Q}(\sqrt{m},\sqrt{d})}(\sqrt{\varepsilon_d})\big) = \varepsilon_d^2.$$

Ainsi $\varepsilon_d^2$ est norme d'une unité dans $K/F$. D'autre part, il est clair que l'extension $k/\mathbf{Q}(\sqrt{m}, \sqrt{d})$ est non ramifiée, il en est de même pour toute extension propre $k/K$ de $k/\mathbf{Q}(\sqrt{m}, \sqrt{d})$. Alors $\varepsilon_d^2$ est norme d'un élément dans $k/F$. Supposons que $m$ est

https://doi.org/10.4153/CMB-2011-006-9 Published online by Cambridge University Press

pair, donc $\varepsilon_d$ n'est pas un carré dans $k$. On sait que $2\varepsilon_q$ est un carré dans $\mathbf{Q}(\sqrt{q})$ (on peut utiliser le lemme 3.1). Alors, puisque $m\varepsilon_d$ est un carré dans $F$, l'unité $\varepsilon_d\varepsilon_q$ doit être un carré dans le corps triquadratique $K = \mathbf{Q}(\sqrt{2m}, \sqrt{d}, \sqrt{q})$. Ainsi, on a

$$N_{K/F}(\sqrt{\varepsilon_q\varepsilon_d}) = N_{\mathbf{Q}(\sqrt{q},\sqrt{d})/F}\big(N_{K/\mathbf{Q}(\sqrt{q},\sqrt{d})}(\sqrt{\varepsilon_d\varepsilon_q})\big) = \varepsilon_d^2.$$

Par conséquent, $\varepsilon_d^2$ est norme d'une unité dans $K/F$. De plus, il n'est pas difficile de voir que l'extension $k/K$ est non ramifiée, il s'ensuit que l'unité $\varepsilon_d^2$ est norme d'un élément dans $k/F$. Ainsi, dans tous les cas, $-1$ et $\varepsilon_d^2$ sont des normes dans l'extension $k/F$, par suite, le groupe $E_F/E_F \cap N_{k/F}(k^*)$ est d'ordre au plus égal à 2. ■

***Théorème 3.3*** *Soient $p_1, p_2, p_3$ et $q$ des nombres premiers tels que $p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4$ et $k = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{q})$. Alors, le rang du 2-groupe de classes de $k$ : $\operatorname{rang}\big(\mathrm{Cl}_2(k)\big)$ est supérieur ou égal à 2.*

**Preuve** Il est clair que l'extension $k/F$ est abélienne non ramifiée à groupe de Galois $G \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On suppose que $(\frac{p_1}{p_2}) = (\frac{p_1}{p_3}) = (\frac{p_2}{p_3}) = 1$, alors d'après [F, Addendum II to Theorem 5.6], le 2-groupe de classes de $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ n'est pas trivial et en combinant avec [M-M, théorème 5.8], on trouve que $\operatorname{rang}(\mathrm{Cl}_2(\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}))) \geq 2$. Or $k/\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ est une extension quadratique ramifiée, alors

$$\operatorname{rang}\big(\mathrm{Cl}_2(k)\big) \geq 2.$$

On suppose qu'on n'a pas $(\frac{p_1}{p_2}) = (\frac{p_1}{p_3}) = (\frac{p_2}{p_3}) = 1$, alors d'après la proposition 3.2, l'indice normique $\big(E_F : E_F \cap N_{k/F}(k^*)\big)$ est au plus égal à 2. D'autre part, on a la structure du multiplicateur de Schur de $G$ : $\mathcal{M}(G) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et en combinant avec la formule $(*)$ de la section 2, on tire que $\operatorname{Gal}\big(Z(k, F)/G(k/F)\big)$ contient un sous-groupe de 2-rang supérieur ou égal à 2. D'où $\operatorname{rang}\big(\mathrm{Cl}_2(k)\big) \geq 2$ et on a le théorème. ■

Dans ce qui suit, nous démontrons que la valeur 2 est atteinte par le rang du 2-groupe de classes d'une famille infinie de corps multiquadratiques $k$ : Supposons dans ce qui suit que $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$ et $(\frac{q}{p_1}) = -(\frac{q}{p_2}) = -(\frac{p_1}{p_2}) = 1$. Sous ces conditions, on a le lemme suivant :

***Lemme 3.4*** *Le 2-groupe de classes du corps triquadratique $M = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q})$ est trivial.*

**Preuve** Introduisons le corps $K = \mathbf{Q}(\sqrt{p_1p_2}, \sqrt{q})$ qui est un sous corps de $M$. La 2-partie du nombre de classes de $K$ est $h_2(K) = (Q_K h_2(p_1p_2)h_2(q)h_2(p_1p_2q))/4$ où $Q_K$ désigne l'indice des unités du corps $K$ et $h_2(m)$ la 2-partie du nombre de classes du corps quadratique $\mathbf{Q}(\sqrt{m})$ (voir par exemple [W]). Sous les conditions du lemme, on a $h_2(p_1p_2q) = 4$ (voir par exemple [B-S]). De plus, $h_2(p_1p_2) = 2$ et $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = -1$ (voir par exemple [K]). D'autre part, $2p_1\varepsilon_{p_1p_2q}$ est un carré dans $F = \mathbf{Q}(\sqrt{p_1p_2q})$ [A-M-2, preuve du lemme 5], et puisque $2\varepsilon_q$ est un carré dans $\mathbf{Q}(\sqrt{q})$ et $N_{\mathbf{Q}(\sqrt{p_1p_2})/\mathbf{Q}}(\varepsilon_{p_1p_2}) = -1$, alors les unités $\varepsilon_q, \varepsilon_{p_1p_2q}$ et $\varepsilon_q\varepsilon_{p_1p_2q}$ ne sont pas des carrés dans $K$. Il s'ensuit, d'après les systèmes fondamentales d'unités possibles de $K$ donnés dans [Kur], $\{\varepsilon_q, \varepsilon_{p_1p_2}, \varepsilon_{p_1p_2q}\}$ est un système fondamental d'unités de $K$. Ainsi, $Q_K = 1$ et donc $h_2(K) = 2$ et comme $M/K$ est une extension quadratique non ramifiée, alors le 2-groupe de classes de $M$ est trivial. ■

***Théorème 3.5*** *Soient $p_1, p_2, p_3$ et $q$ des nombres premiers tels que $p_1 \equiv p_2 \equiv p_3 \equiv -q \equiv 1 \pmod 4$ et $k = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{q})$. Supposons que $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$, $(\frac{q}{p_1}) = -(\frac{q}{p_2}) = -(\frac{p_1}{p_2}) = 1$ et que $(\frac{q}{p_3}) = -(\frac{p_1}{p_3}) = -(\frac{p_2}{p_3}) = 1$. Alors on a* $\operatorname{rang}\bigl(\mathrm{Cl}_2(k)\bigr) = 2$.

**Preuve** D'après le lemme 3.4, le 2-groupe de classes de $M = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q})$ est trivial. On peut appliquer les résultats de la section 2, à l'extension $k/M$ :

$$\operatorname{rang}\bigl(\mathrm{Cl}_2(k)\bigr) = \operatorname{Ram}(k/M) - \operatorname{rang}\bigl(E_M/E_M \cap N_{k/M}(k^{(*)})\bigr) - 1,$$

où $\operatorname{Ram}(k/M)$ est le nombre des premiers ramifiés dans l'extension $k/M$. Les premiers de $M$ ramifiés dans $k$ sont les premiers au dessus de $p_3$. Comme $(\frac{p_1}{p_3}) = -1$, alors il est clair que $\operatorname{Ram}(k/M) = 4$ et par suite $\operatorname{rang}\bigl(\mathrm{Cl}_2(k)\bigr) = 3 - \operatorname{rang}\bigl(E_M/E_M \cap N_{k/M}(k^{(*)})\bigr)$. D'après le théorème 3.3, on a $\operatorname{rang}\bigl(\mathrm{Cl}_2(k)\bigr) \geq 2$, ainsi démontrer le théorème 3.5 revient à démontrer que $\operatorname{rang}\bigl(E_M/E_M \cap N_{k/M}(k^{(*)})\bigr) = 1$. Ce qui se traduit par la détermination d'une unité de $M$ qui n'est pas norme dans l'extension $k/M$. Soit le corps biquadratique $K = \mathbf{Q}(\sqrt{p_1p_2}, \sqrt{q})$ introduit dans la preuve du lemme précédent. On a $h_2(K) = 2$ et par suite $M$ est le 2-corps de classe de Hilbert de $K$. Ainsi chaque unité de $K$ est norme d'une unité de $M$. Notons $u$ une unité de $M$ telle que

$$N_{M/K}(u) = \begin{cases} \varepsilon_{p_1p_2q} & \text{si } (\frac{2}{p_3}) = 1, \\ \varepsilon_q & \text{si } (\frac{2}{p_3}) = -1 \end{cases}$$

et montrons que $u$ n'est pas norme dans l'extension $k/M$. Soit $\mathcal{P}$ un idéal premier de $M$ ramifié dans $k$. Sous les conditions $(\frac{q}{p_3}) = -(\frac{p_1}{p_3}) = -(\frac{p_2}{p_3}) = 1$, il est clair que $\mathcal{P}$ est inerte dans l'extension $M/K$. Par suite

$$\Bigl(\frac{u, p_3}{\mathcal{P}}\Bigr) = \Bigl(\frac{N_{M/K}(u), p_3}{N_{M/K}(\mathcal{P})}\Bigr) = \begin{cases} (\frac{\varepsilon_{p_1p_2q}, p_3}{N_{M/K}(\mathcal{P})}) & \text{si } (\frac{2}{p_3}) = 1, \\ (\frac{\varepsilon_q, p_3}{N_{M/K}(\mathcal{P})}) & \text{si } (\frac{2}{p_3}) = -1, \end{cases}$$

où $(\frac{\cdot,\cdot}{\cdot})$ désigne le symbole du reste normique (voir [H]).

Supposons que $(\frac{2}{p_3}) = 1$, on a donc

$$\Bigl(\frac{u, p_3}{\mathcal{P}}\Bigr) = \Bigl(\frac{\varepsilon_{p_1p_2q}, p_3}{N_{M/K}(\mathcal{P})}\Bigr).$$

Comme $2p_1\varepsilon_{p_1p_2q}$ est un carré dans $\mathbf{Q}(\sqrt{p_1p_2q})$ [A-M-2, preuve du lemme 5], alors

$$\Bigl(\frac{u, p_3}{\mathcal{P}}\Bigr) = \Bigl(\frac{2p_1, p_3}{p_3}\Bigr) = \Bigl(\frac{2p_1}{p_3}\Bigr) = -1.$$

https://doi.org/10.4153/CMB-2011-006-9 Published online by Cambridge University Press

Supposons que $(\frac{2}{p_3}) = -1$, on a donc

$$\left(\frac{u, p_3}{\mathcal{P}}\right) = \left(\frac{\varepsilon_q, p_3}{N_{M/K}(\mathcal{P})}\right).$$

Comme $2\varepsilon_q$ est un carré dans $\mathbf{Q}(\sqrt{q})$, alors

$$\left(\frac{u, p_3}{\mathcal{P}}\right) = \left(\frac{2, p_3}{p_3}\right) = \left(\frac{2}{p_3}\right) = -1.$$

Ainsi, dans tous les cas, l'unité $u$ n'est pas norme dans l'extension $k/M$ et par conséquent $\operatorname{rang}(\mathrm{Cl}_2(k)) = 2$. ■

***Exemple*** Posons $p_1 = 5$, $p_2 = 13$ et $p_3 = 37$. On peut vérifier que $(\frac{2}{p_1}) = (\frac{2}{p_2}) = -1$ et que pour tout $i$, $j$ distincts dans $\{1, 2, 3\}$, on a $(\frac{p_i}{p_j}) = -1$. Il reste à déterminer $q$ tel que $q \equiv -1 \pmod 4$ et

$$\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_3}\right) = -\left(\frac{q}{p_2}\right) = 1. \tag{1}$$

On va prendre $q \equiv -1 \pmod{4 \cdot 5 \cdot 37}$ et remarquer que le premier terme de cette progression est $739 \equiv -2 \pmod{13}$ et que $-2$ n'est pas un résidu quadratique modulo 13. Il s'ensuit que les premiers $q$ tels que $q \equiv 739 \pmod{4 \cdot 5 \cdot 13 \cdot 37}$ vérifient bien les équations (1). On a donc le corollaire suivant :

***Corollaire 3.6*** *On sait qu'il existe une infinité de nombre premiers dans une progression arithmétique. Alors il est clair d'après l'exemple précédent qu'il existe une infinité de corps multiquadratiques $k$ vérifiant les conditions du théorème et donc tels que :* $\operatorname{rang}\big(\mathrm{Cl}_2(k)\big) = 2$.

## Références


[A-M-1] A. Azizi et A. Mouhib, *Sur le rang du 2-groupe de classes de $\mathbf{Q}(\sqrt{m}, \sqrt{d})$ où $m = 2$ ou un premier $p \equiv 1 \pmod 4$*. Trans. Amer. Math. Soc. **353**(2001), 2741–2752. doi:10.1090/S0002-9947-01-02753-2

[A-M-2] ———, *Capitulation des 2-classes d'idéaux de $\mathbf{Q}(\sqrt{2}, \sqrt{d})$ où $d$ est un entier naturel sans facteurs carrés.* Acta Arith. **109**(2003), 27–73. doi:10.4064/aa109-1-2

[B-1] M. Bulant, *On the Parity of the Class Number of the Fields $\mathbf{Q}(\sqrt{p}, \sqrt{p}, \sqrt{r})$*. J. Number Theory **68**(1998), 72–86. doi:10.1006/jnth.1997.2190

[B-2] ———, *Class Number Parity of a Compositum of Five Quadratic Fields.* Acta Math. Inform. Univ. Ostraviensis **10**(2002) 25–34.

[B-L-S] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields with cyclic* $\mathrm{cl}_2(k^1)$. J. Number Theory **67**(1997), 229–245. doi:10.1006/jnth.1997.2174

[B-S] E. Benjamin and C. Snyder, *Real quadratic number fields with 2-class group of type* $(2, 2)$. Math. Scand. **76**(1995), 161–178.

[F] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields.* Contemp. Math. **24**, Amer. Math. Soc., Providence, 1983.

[H] H. Hasse, *Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols.* J. Reine Angew. Math. **162**(1930), 143–144.

[K] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques.* J. Reine Angew. Math. **283/284**(1976), 313–363.

[Ku] R. Kučera, *On the parity of the class number of a biquadratic field.* J. Number Theory **52**(1995), 43–52. doi:10.1006/jnth.1995.1054

[Kur] S. Kuroda, *Uber die Dirichletschen Körper.* J. Fac. Sci. Imp. Univ. Tokyo **4**(1943), 382–406.

[M-M] A. Mouhib et A. Movahhedi, *Sur le 2-groupe de classes des corps multiquadratiques réels.* J. Théor. Nombres Bordeaux **17**(2005), 619–641.

[W] 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.

*Univ. Mohammed Ben Abdellah, Faculté polydisciplinaire, Laboratoire d'Informatique, Mathématiques, Automatique et Optoélectronique, B/P 1223, Taza-Gare, Maroc*
*courriel*: mouhibali@yahoo.fr

https://doi.org/10.4153/CMB-2011-006-9 Published online by Cambridge University Press