

Sur le 2-groupe de classes des corps multiquadratiques réels

par ALI MOUHIB et ABBAS MOVAHHEDI

À Georges Gras, pour son 60-ième anniversaire

RÉSUMÉ. Soient p_1, p_2, \dots, p_n des nombres premiers distincts $\not\equiv -1 \pmod{4}$, $d := p_1 p_2 \cdots p_n$ et $k_n = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$. On peut approcher le 2-rang du groupe de classes des corps k_n en étudiant celui du corps $k_m(\sqrt{d})$ pour un entier $m < n$. Dans cet article, on traite le cas où $m = 2$ ou 3 . Comme application, on déduit que le rang du 2-groupe de classes de k_4 est au moins égal à deux (on savait déjà grâce à un résultat de Fröhlich que le groupe de classes de k_4 est toujours d'ordre pair). On en déduit également la liste de tous les corps multiquadratiques k_n ayant un 2-groupe de classes cyclique non trivial.

ABSTRACT. Let p_1, p_2, \dots, p_n be distinct rational prime numbers $\not\equiv -1 \pmod{4}$, $d := p_1 p_2 \cdots p_n$ and $k_n = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$. The 2-rank of the class group of k_n can be approached by studying that of the field $k_m(\sqrt{d})$, for an integer $m < n$. In this article, we treat the case where $m = 2$ or 3 . As an application, we deduce that the rank of the 2-class group of k_4 is at least two (according to a result of Fröhlich, we already knew that the class group of k_4 is always of even order). We also draw the list of all multiquadratic fields k_n whose 2-class group is cyclic non-trivial.

1. Introduction

Soient p_1, p_2, \dots, p_n des nombres premiers distincts non congrus à -1 modulo 4, $d := p_1 p_2 \cdots p_n$, $k_n = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ et $Cl_2(k_n)$ le 2-groupe de classes de k_n . En utilisant les extensions centrales, A. Fröhlich a étudié la parité du nombre de classes des 2-extensions abéliennes réelles K du corps \mathbf{Q} des nombres rationnels [F]. Il a démontré que si K coïncide avec son corps de genres au sens restreint, alors le nombre de classes de K est pair dès que le nombre des places de \mathbf{Q} ramifiées dans K est supérieur ou égal à 4. Notons qu'avec l'hypothèse de Fröhlich, les premiers impairs divisant le discriminant de K sont congrus à 1 modulo 4. En particulier,

si $n \geq 4$, alors le nombre de classes de k_n est toujours pair. Dans le cas où $n = 2$, il a déterminé tous les corps k_2 dont le groupe de classes est d'ordre pair. On trouve également dans le livre [C-H], une caractérisation de tous les corps biquadratiques dont le nombre de classes est pair. Dans le cas où $n = 3$, Fröhlich a donné les conditions nécessaires et suffisantes pour que le corps triquadratique k_3 ait un nombre de classes pair [F]. Pour une approche par les unités circulaires de ces résultats voir [K] pour $n = 2$ et [B] pour $n = 3$.

En général, les résultats de A. Fröhlich n'apportent pas d'informations sur le rang de $Cl_2(k_n)$. Dans ce travail, on se propose d'étudier le rang du 2-groupe de classes des corps k_n à l'aide de la théorie des genres et moyennant des résultats sur les unités des corps biquadratiques et triquadratiques. La stratégie consiste à calculer le 2-rang du groupe de classes des corps $k(\sqrt{d})$ où $k = k_2$ ou bien $k = k_3$. Comme application on démontre que $\text{rang}(Cl_2(k_4)) \geq 2$ (voir théorème 5.3) et on donne un exemple d'une famille infinie de corps k_4 tels que $\text{rang}(Cl_2(k_4)) = 2$. Ceci, à son tour, permet de généraliser le résultat de Fröhlich : $\text{rang}(Cl_2(K)) \geq 2$ dès qu'il y a au moins 4 premiers non congrus à -1 modulo 4 ramifiés dans la 2-extension abélienne réelle K (voir théorème 5.5). Soit $K := \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ un corps multiquadratique où les d_i sont des entiers naturels sans facteurs carrés non-divisibles par des premiers congrus à -1 modulo 4. Pour qu'un tel corps K ait un 2-groupe de classes cyclique, il est nécessaire que $[K : \mathbf{Q}] \leq 8$ (voir théorème 5.5). On détermine parmi ces corps multiquadratiques ceux dont le 2-groupe de classes est cyclique non trivial (théorème 5.8).

Avant d'aller plus loin, nous introduisons les notations suivantes :

n :	entier naturel
$p_i, i = 1, 2, \dots, n$:	nombre premier $\not\equiv -1 \pmod{4}$
d :	$= p_1 p_2 \dots p_n$
k_n :	le corps multiquadratique $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$
$Cl_2(F)$:	le 2-groupe de classes du corps F
$\text{rang}(Cl_2(F))$:	la dimension du $\mathbf{Z}/2\mathbf{Z}$ -espace vectoriel $Cl_2(F)/Cl_2(F)^2$
F :	un corps multiquadratique
E_F :	le groupe des unités de F
Q_F :	l'indice des unités de F
O_F :	l'anneau des entiers de F
$h(F)$:	le nombre de classes de F
$h_2(F)$:	la 2-partie du nombre de classes de F
ε_n :	l'unité fondamentale de $\mathbf{Q}(\sqrt{n})$
$h(n)$:	le nombre de classes de $\mathbf{Q}(\sqrt{n})$
$h_2(n)$:	la 2-partie du nombre de classes de $\mathbf{Q}(\sqrt{n})$

$N_{K/k}$: la norme relative à l'extension K/k
 $\rho := \rho(K/k)$ le nombre des premiers de k ramifiés dans K .
 $e := e(K/k)$ le 2-rang de $E_k/E_k \cap N_{K/k}(K^*)$ dans une 2-extension K/k .

2. p -groupe de classes dans une extension cyclique

Dans ce paragraphe, K/k désigne une extension cyclique de groupe de Galois G d'ordre un premier p , $D_{K/k}$ le discriminant relatif de l'extension K/k , $e_q(K/k)$ l'indice de ramification du premier q , E_k (resp. E_K) le groupe des unités de k (resp. de K), $h(k)$ le nombre de classes de k , $N_{K/k}$ l'application norme par rapport à l'extension K/k et $\rho(K/k)$ le nombre des premiers finis et infinis ramifiés dans l'extension K/k . Soit $Cl(K)$ (resp. $Cl(k)$) le groupe de classes de K (resp. de k). La formule des classes ambiges s'écrit comme suit :

$$|Cl(K)^G| = \frac{h(k) \prod_{q|D_{K/k}} e_q(K/k)}{[K : k][E_k : E_k \cap N_{K/k}(K^*)]}.$$

On définit le groupe des classes relatives par

$$Cl(K/k) = \text{Ker}(N_{K/k} : Cl(K) \rightarrow Cl(k)).$$

Soit H un groupe abélien et H_p le p -groupe de Sylow de H , on note par $\text{rang}(H_p)$ la dimension de H/H^p considéré comme espace vectoriel sur le corps $\mathbf{Z}/p\mathbf{Z}$. Dans [J], W. Jehne a donné une minoration du p -rang du groupe de classes relatives de K/k :

$$\text{rang}(Cl_p(K/k)) \geq \rho(K/k) - \text{rang}(E_k/E_k \cap N_{K/k}(K^*)) - 1.$$

Soit $Cl_p(K)$ le p -groupe de classes de K . Comme $Cl_p(K/k)$ est un sous-groupe de $Cl_p(K)$, alors on a toujours

$$\text{rang}(Cl_p(K)) \geq \rho(K/k) - \text{rang}(E_k/E_k \cap N_{K/k}(K^*)) - 1.$$

Dans le cas où $h(k)$ est impair et $p = 2$, alors $Cl_2(K/k) = Cl_2(K)$. En utilisant la formule des classes ambiges ci-dessus, on a le résultat suivant :

$$\text{rang}(Cl_2(K)) = \rho(K/k) - \text{rang}(E_k/E_k \cap N_{K/k}(K^*)) - 1.$$

Dans le cas où k est un composé de n corps quadratiques linéairement disjoints et K/k est une extension quadratique, alors on a

$$e(K/k) = \text{rang}(E_k/E_k \cap N_{K/k}(K^*)) \leq 2^n.$$

3. Les unités des corps biquadratiques et triquadratiques

Soient d_1, d_2, \dots, d_n des entiers relatifs distincts tels que le corps multiquadratique $k := \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_n})$ est une extension de degré 2^n de \mathbf{Q} . On sait qu'il existe $t = 2^n - 1$ corps quadratiques k'_i distincts contenus dans k . Soit E_k (resp. $E_{k'_i}$) le groupe des unités de k (resp. de k'_i). D'après [W], on a

$$h(k) = \frac{1}{2^v} Q_k \prod_{i=1}^{i=t} h(k'_i),$$

où $Q_k = [E_k : \prod_{i=1}^{i=t} E_{k'_i}]$ est l'indice des unités de k et

$$v = \begin{cases} n(2^{n-1} - 1) & \text{si } k \text{ est réel,} \\ (n-1)(2^{n-2} - 1) + 2^{n-1} - 1 & \text{si } k \text{ est imaginaire.} \end{cases}$$

Dans toute la suite, on s'intéresse aux corps multiquadratiques réels.

3.1. Les unités de certains corps biquadratiques. Soient m et n deux entiers naturels distincts sans facteurs carrés, $\varepsilon_m, \varepsilon_n$ et ε_{mn} les unités fondamentales respectives de $\mathbf{Q}(\sqrt{m}), \mathbf{Q}(\sqrt{n})$ et $\mathbf{Q}(\sqrt{mn})$ et $k = \mathbf{Q}(\sqrt{m}, \sqrt{n})$. On suppose que $N_{\mathbf{Q}(\sqrt{m})/\mathbf{Q}}(\varepsilon_m) = N_{\mathbf{Q}(\sqrt{n})/\mathbf{Q}}(\varepsilon_n) = -1$. S. Kuroda a démontré qu'un système fondamental d'unités de k prend l'une des trois formes suivantes ([Ku]) :

- (1) $\{\varepsilon_m, \varepsilon_n, \varepsilon_{mn}\}$.
- (2) $\{\varepsilon_m, \varepsilon_n, \sqrt{\varepsilon_{mn}}\}$ (dans ce cas, on a forcément $N_{\mathbf{Q}(\sqrt{mn})/\mathbf{Q}}(\varepsilon_{mn}) = 1$).
- (3) $\{\varepsilon_m, \varepsilon_n, \sqrt{\varepsilon_m \varepsilon_n \varepsilon_{mn}}\}$ (dans ce cas, on a forcément $N_{\mathbf{Q}(\sqrt{mn})/\mathbf{Q}}(\varepsilon_{mn}) = -1$).

Définition 3.1. Soient m et n deux entiers naturels distincts sans facteurs carrés et $k = \mathbf{Q}(\sqrt{m}, \sqrt{n})$. On dit que k est un **corps de Kuroda**, si on a les deux conditions suivantes :

- (i) $N_{\mathbf{Q}(\sqrt{m})/\mathbf{Q}}(\varepsilon_m) = N_{\mathbf{Q}(\sqrt{n})/\mathbf{Q}}(\varepsilon_n) = N_{\mathbf{Q}(\sqrt{mn})/\mathbf{Q}}(\varepsilon_{mn}) = -1$.
- (ii) $\sqrt{\varepsilon_m \varepsilon_n \varepsilon_{mn}} \in k$.

On dit aussi que $\sqrt{\varepsilon_m \varepsilon_n \varepsilon_{mn}}$ est une **unité de Kuroda**.

Lemme 3.2. ([S]) Soient p_1 et p_2 deux nombres premiers non congrus à -1 modulo 4 et $k_2 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$. Alors on a :

- (i) $\{\varepsilon_{p_1}, \varepsilon_{p_2}, \sqrt{\varepsilon_{p_1 p_2}}\}$ est un système fondamental d'unités de k_2 , dès que $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$.
- (ii) $\{\varepsilon_{p_1}, \varepsilon_{p_2}, \sqrt{\varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}}\}$ est un système fondamental d'unités de k_2 , dès que $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$.

Lemme 3.3. *On garde les notations du lemme 3.2 et soit $F = \mathbf{Q}(\sqrt{m})$ un sous-corps quadratique de k_2 . Alors on a :*

(i) $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$ entraîne que

$$N_{k_2/F}(\sqrt{\varepsilon_{p_1 p_2}}) = \begin{cases} \pm 1 & \text{si } F \neq \mathbf{Q}(\sqrt{p_1 p_2}), \\ \pm \varepsilon_{p_1 p_2} & \text{sinon.} \end{cases}$$

(ii) $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$ entraîne que $N_{k_2/F}(\sqrt{\varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}}) = \pm \varepsilon_m$.

Démonstration. Il suffit de voir que

$$N_{k_2/F}(\varepsilon_{p_1 p_2}) = \begin{cases} 1 & \text{si } F \neq \mathbf{Q}(\sqrt{p_1 p_2}), \\ \varepsilon_{p_1 p_2}^2 & \text{sinon} \end{cases}$$

et que $N_{k_2/F}(\varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}) = \varepsilon_m^2$ où $m \in \{p_1, p_2, p_1 p_2\}$ et $F = \mathbf{Q}(\sqrt{m})$. \square

3.2. Les unités de certains corps triquadratiques. Soit $k_3 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ avec $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$. Nous allons expliciter un système fondamental d'unités de k_3 , suivant que $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ est un corps de Kuroda ou non. Notons que :

(i)

$$\begin{aligned} N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) &= N_{\mathbf{Q}(\sqrt{p_1 p_3})/\mathbf{Q}}(\varepsilon_{p_1 p_3}) \\ &= N_{\mathbf{Q}(\sqrt{p_1 p_2 p_3})/\mathbf{Q}}(\varepsilon_{p_1 p_2 p_3}) \\ &= -1. \end{aligned}$$

(ii) Si $\left(\frac{p_2}{p_3}\right) = 1$ et les symboles biquadratiques $\left(\frac{p_2}{p_3}\right)_4 \neq \left(\frac{p_3}{p_2}\right)_4$, on a :

$$N_{\mathbf{Q}(\sqrt{p_2 p_3})/\mathbf{Q}}(\varepsilon_{p_2 p_3}) = 1.$$

Ainsi une condition nécessaire pour que $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ soit un corps de Kuroda est que

$$\left(\frac{p_2}{p_3}\right) = -1 \text{ ou } \left[\left(\frac{p_2}{p_3}\right) = 1 \text{ et } \left(\frac{p_2}{p_3}\right)_4 = \left(\frac{p_3}{p_2}\right)_4\right].$$

Pour deux entiers naturels distincts m et n divisant $p_1 p_2 p_3$ tels que

$$N_{\mathbf{Q}(\sqrt{m})/\mathbf{Q}}(\varepsilon_m) = N_{\mathbf{Q}(\sqrt{n})/\mathbf{Q}}(\varepsilon_n) = -1,$$

on note

$$\eta(m, n) = \begin{cases} \sqrt{\varepsilon_m \varepsilon_n \varepsilon_{mn}} & \text{si } N_{\mathbf{Q}(\sqrt{mn})/\mathbf{Q}}(\varepsilon_{mn}) = -1, \\ \sqrt{\varepsilon_{mn}} & \text{si } N_{\mathbf{Q}(\sqrt{mn})/\mathbf{Q}}(\varepsilon_{mn}) = 1. \end{cases}$$

Lorsque m et n sont premiers, le symbole $\eta(m, n) \in \mathbf{Q}(\sqrt{m}, \sqrt{n})$.

Rappelons que d'après [C], on a :

(1) Lorsque $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ n'est pas un corps de Kuroda

$$\{\varepsilon_{p_1}, \varepsilon_{p_2}, \varepsilon_{p_3}, \eta(p_1, p_2), \eta(p_1, p_3), \eta(p_2, p_3), \eta(p_2, p_1 p_3)\}$$

est un système fondamental d'unités de k_3 .

(2) Lorsque k est un corps de Kuroda, il existe $a_i, b_i, c_i \in \{0, 1\}$ avec $i = 1, 2, 3$ tels que si on pose :

$$\begin{aligned}\varepsilon(p_1, p_2) &= \varepsilon_{p_1}^{a_1} \varepsilon_{p_2}^{a_2} \varepsilon_{p_1 p_2}^{a_3} \eta(p_1, p_2) \\ \varepsilon(p_1, p_3) &= \varepsilon_{p_1}^{b_1} \varepsilon_{p_3}^{b_2} \varepsilon_{p_1 p_3}^{b_3} \eta(p_1, p_3) \\ \varepsilon(p_1, p_2 p_3) &= \varepsilon_{p_1}^{c_1} \varepsilon_{p_2 p_3}^{c_2} \varepsilon_{p_1 p_2 p_3}^{c_3} \eta(p_1, p_2 p_3),\end{aligned}$$

alors

$$\xi = (\varepsilon(p_1, p_2) \varepsilon(p_1, p_3) \varepsilon(p_1, p_2 p_3))^{\frac{1}{2}} \in k_3.$$

De plus,

$$\{\varepsilon_{p_1}, \varepsilon_{p_2}, \varepsilon_{p_3}, \eta(p_1, p_2), \eta(p_1, p_3), \eta(p_2, p_3), \xi\}$$

est un système fondamental d'unités de k_3 .

Notons que l'hypothèse $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$ entraîne que si $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ est un corps de Kuroda, alors il en est de même de $\mathbf{Q}(\sqrt{p_2}, \sqrt{p_1 p_3})$ et $\mathbf{Q}(\sqrt{p_3}, \sqrt{p_1 p_2})$.

4. Rang du 2-groupe de classes des corps multiquadratiques

Notre objectif est d'étudier le rang du 2-groupe de classes des corps $K = k(\sqrt{d})$ où $k = k_2$ ou bien $k = k_3$ afin d'obtenir une meilleure minoration de rang $(Cl_2(K))$. On sait que $\text{rang}(Cl_2(K)) \geq \rho - e - 1$ avec égalité lorsque $Cl_2(k)$ est trivial. De plus, si k est un corps biquadratique, alors $0 \leq e \leq 4$ et si k est un corps triquadratique, alors $0 \leq e \leq 8$. La détermination de l'entier naturel e revient à chercher les unités fondamentales u de k qui sont des normes dans l'extension K/k . Ce qui revient à calculer le symbole du reste normique $\left(\frac{u, d}{\mathfrak{p}}\right)$ pour tout premier \mathfrak{p} de k qui se ramifie dans K .

Lemme 4.1. *Soient m et n deux entiers naturels tels que $m < n$ et r le nombre des premiers p_i , $i = 1, 2, \dots, n$ qui se décomposent totalement dans k_m . Alors le nombre $\rho := \rho(k_n/k_m)$ des idéaux premiers de k_m ramifiés dans k_n est donné par :*

$$\rho = 2^m r + 2^{m-1} (n - m - r).$$

Démonstration. Il suffit de noter qu'un premier qui ne se ramifie pas dans k_m est soit totalement décomposé dans k_m , soit produit de 2^{m-1} idéaux premiers distincts de k_m . \square

Le résultat suivant est un lemme clé qui jouera un rôle important dans la suite.

Lemme 4.2. *Plaçons-nous dans $k_n = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ et fixons $i \geq 4$. Notons E le corps de décomposition de p_i dans k_3 . Soit $F := \mathbf{Q}(\sqrt{m})$ un sous-corps quadratique de E . Alors*

(i) *lorsque $m = p_1$, l'unité ε_m est norme dans l'extension $E(\sqrt{p_i})/E$ (resp. $F(\sqrt{p_i})/F$) si et seulement si on a l'égalité des symboles biquadratiques*

$$\left(\frac{p_1}{p_i}\right)_4 = \left(\frac{p_i}{p_1}\right)_4.$$

(ii) *lorsque $m = p_1 p_2$, l'unité ε_m est norme dans l'extension $E(\sqrt{p_i})/E$ (resp. $F(\sqrt{p_i})/F$) si et seulement si l'une des trois conditions suivantes est satisfaite :*

(a) $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$, et $\left(\frac{p_2}{p_i}\right) = \left(\frac{p_1}{p_i}\right) = 1$;

(b) $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$, $\left(\frac{p_2}{p_i}\right) = \left(\frac{p_1}{p_i}\right) = 1$ et $\left(\frac{p_1 p_2}{p_i}\right)_4 = \left(\frac{p_i}{p_1 p_2}\right)_4$;

(c) $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$, $\left(\frac{p_2}{p_i}\right) = \left(\frac{p_1}{p_i}\right) = -1$ et $Q_{F(\sqrt{p_i})} = 2$.

(iii) *lorsque $m = p_1 p_2 p_3$, $E = F(\sqrt{p_1})$ et que*

$$N_{\mathbf{Q}(\sqrt{p_2 p_3})/\mathbf{Q}}(\varepsilon_{p_2 p_3}) = N_{\mathbf{Q}(\sqrt{p_1 p_2 p_3})/\mathbf{Q}}(\varepsilon_{p_1 p_2 p_3}) = -1,$$

l'unité ε_m est norme dans l'extension $E(\sqrt{p_i})/E$ (resp. $F(\sqrt{p_i})/F$) si et seulement si l'une des deux conditions suivantes est satisfaite :

(d) $\sqrt{\varepsilon_{p_1} \varepsilon_{p_2 p_3} \varepsilon_{p_1 p_2 p_3}} \in E$ et $(-1)^{Q_{\mathbf{Q}(\sqrt{p_2 p_3}, \sqrt{p_i})}} = \left(\frac{p_1}{p_i}\right)_4 \left(\frac{p_i}{p_1}\right)_4$;

(e) $\sqrt{\varepsilon_{p_1} \varepsilon_{p_2 p_3} \varepsilon_{p_1 p_2 p_3}} \notin E$ et $(-1)^{Q_{\mathbf{Q}(\sqrt{p_2 p_3}, \sqrt{p_i})}} = -\left(\frac{p_1}{p_i}\right)_4 \left(\frac{p_i}{p_1}\right)_4$.

Démonstration. Soit \mathfrak{p} un idéal premier de E au dessus de p_i . L'idéal \mathfrak{p} se ramifie dans $E(\sqrt{p_i})$. Par hypothèse, p_i se décompose totalement dans E et donc dans F : $\left(\frac{m}{p_i}\right) = 1$. On a

$$\left(\frac{\varepsilon_m, p_i}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_m, p_i}{\mathfrak{p}'}\right)$$

où \mathfrak{p}' est l'idéal premier de F en dessous de \mathfrak{p} . Ainsi, ε_m est norme dans l'extension $E(\sqrt{p_i})/E$ précisément lorsque ε_m est norme dans l'extension $F(\sqrt{p_i})/F$. On distingue plusieurs cas :

(i) lorsque $m = p_1$, alors d'après ([A-M-1], preuve du théorème 2), on a

$$\left(\frac{\varepsilon_m, p_i}{\mathfrak{p}'}\right) = \left(\frac{p_1}{p_i}\right)_4 \left(\frac{p_i}{p_1}\right)_4.$$

Ainsi ε_{p_1} est norme dans l'extension $F(\sqrt{p_i})/F$ si et seulement si

$$\left(\frac{p_1}{p_i}\right)_4 = \left(\frac{p_i}{p_1}\right)_4.$$

(ii) Lorsque $m = p_1 p_2$, on va raisonner suivant la valeur de $N_{F/\mathbf{Q}}(\varepsilon_m)$.

Supposons d'abord que $N_{F/\mathbf{Q}}(\varepsilon_m) = 1$. D'après ([A-M-2], preuve du lemme 1), il existe deux nombres rationnels x et y tels que $\sqrt{\varepsilon_m} = x\sqrt{p_1} + y\sqrt{p_2}$. Par suite, ε_m/p_1 est un carré de F de sorte que :

$$\left(\frac{\varepsilon_m, p_1}{\mathfrak{p}'}\right) = \left(\frac{p_1, p_1}{\mathfrak{p}'}\right) = \left(\frac{p_1}{p_1}\right).$$

Autrement dit, ε_m est norme dans $F(\sqrt{p_i})/F$ si et seulement si $\left(\frac{p_1}{p_i}\right) = 1$.

Supposons maintenant que $N_{F/\mathbf{Q}}(\varepsilon_m) = -1$. D'après le lemme 3.2, on a $\eta(p_1, p_2) = \sqrt{\varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}} \in E$ et donc $N_{E(\sqrt{p_i})/E}(\eta(p_1, p_2)) = \varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}$. Par suite, l'unité ε_m est norme dans $E(\sqrt{p_i})/E$ si et seulement si $\varepsilon_{p_1} \varepsilon_{p_2}$ est norme dans $E(\sqrt{p_i})/E$. Si $\left(\frac{p_1}{p_i}\right) = 1$, alors on a $\left(\frac{p_2}{p_i}\right) = 1$ et en se servant du cas (i), on trouve que ε_m est norme dans $E(\sqrt{p_i})/E$ si et seulement si

$$\left(\frac{m}{p_i}\right)_4 = \left(\frac{p_i}{m}\right)_4.$$

Si, au contraire, $\left(\frac{p_1}{p_i}\right) = -1$, alors, de même $\left(\frac{p_2}{p_i}\right) = -1$. Dans ce cas, il est bien connu que $N_{\mathbf{Q}(\sqrt{p_i m})/\mathbf{Q}}(\varepsilon_{p_i m}) = -1$ et $h_2(p_i m) = 4$ (voir par exemple [Ré-Re]). De plus lorsque ε_m est norme dans $F(\sqrt{p_i})/F$, alors le nombre des 2-classes ambiges de $F(\sqrt{p_i})/F$ est égal à $2h_2(m)$. D'où en utilisant la formule rappelée dans la section 3 :

$$h(F(\sqrt{p_i})) = \frac{1}{4} Q_{F(\sqrt{p_i})} h(\mathbf{Q}(\sqrt{p_i})) h(F) h(\mathbf{Q}(\sqrt{m p_i})), \quad (*)$$

on voit que l'indice des unités $Q_{F(\sqrt{p_i})} = 2$ (rappelons, en effet, que d'après la section 3.1, $Q_{F(\sqrt{p_i})} = 1$ ou 2). Cette dernière égalité montre, toujours d'après la section 3.1, que $\eta(p_i, m) = \sqrt{\varepsilon_m \varepsilon_{p_i} \varepsilon_{p_i m}} \in F(\sqrt{p_i})$. Ainsi, $\varepsilon_m = \pm N_{F(\sqrt{p_i})/F}(\eta(p_i, m))$ est norme dans $F(\sqrt{p_i})/F$ précisément lorsque $Q_{F(\sqrt{p_i})} = 2$.

(iii) Lorsque $m = p_1 p_2 p_3$ et $E = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$. Dans ce cas $\eta(p_1, p_2 p_3) = \sqrt{\varepsilon_{p_1} \varepsilon_{p_2 p_3} \varepsilon_m}$ est bien défini (section 3.2) et on va raisonner suivant que $\eta(p_1, p_2 p_3) \in E$ ou non.

Supposons d'abord que $\eta(p_1, p_2 p_3) = \sqrt{\varepsilon_{p_1} \varepsilon_{p_2 p_3} \varepsilon_m} \in E$, alors on a $N_{E(\sqrt{p_i})/E}(\eta(p_1, p_2 p_3)) = \varepsilon_{p_1} \varepsilon_{p_2 p_3} \varepsilon_m$, et donc ε_m est norme dans l'extension $E(\sqrt{p_i})/E$ si et seulement si $\varepsilon_{p_1} \varepsilon_{p_2 p_3}$ est norme dans $E(\sqrt{p_i})/E$ et, d'après (i) et (ii-c), cette dernière unité est à son tour norme dans $E(\sqrt{p_i})/E$ si et seulement si

$$(-1)^{Q_{\mathbf{Q}(\sqrt{p_2 p_3}, \sqrt{p_i})}} = \left(\frac{p_1}{p_i}\right)_4 \left(\frac{p_i}{p_1}\right)_4.$$

Supposons maintenant que $\eta(p_1, p_2 p_3) \notin E$. D'après [W], on a $\eta(p_1, p_2 p_3) \in k_3$ de sorte que \mathfrak{p} reste inerte dans $E(\eta(p_1, p_2 p_3)) = k_3$ et

$$\left(\frac{p_i, \eta(p_1, p_2 p_3)^2}{\mathfrak{p}}\right) = \left(\frac{\eta(p_1, p_2 p_3)^2}{\mathfrak{p}}\right) = -1.$$

D'où, puisque $\eta(p_1, p_2 p_3)^2 = \varepsilon_{p_1} \varepsilon_{p_2 p_3} \varepsilon_m$:

$$\left(\frac{p_i, \varepsilon_m}{\mathfrak{p}}\right) = - \left(\frac{p_i, \varepsilon_{p_1}}{\mathfrak{p}}\right) \left(\frac{p_i, \varepsilon_{p_2 p_3}}{\mathfrak{p}}\right).$$

Donc, en utilisant (i) et (ii-c), on trouve :

$$\left(\frac{p_i, \varepsilon_m}{\mathfrak{p}}\right) = -(-1)^{Q_{\mathbf{Q}(\sqrt{p_2 p_3}, \sqrt{p_i})}} \left(\frac{p_1}{p_i}\right)_4 \left(\frac{p_i}{p_1}\right)_4.$$

Ce qui démontre le lemme. □

Remarque. Plaçons-nous dans le cas (ii-c) du lemme précédent. Supposons que $\left(\frac{p_1}{p_2}\right) = -1$, alors d'après [Ré-Re], $h(p_1 p_2) = 2$, de plus le 2-groupe de classes du corps quadratique $\mathbf{Q}(\sqrt{p_1 p_2 p_i})$ est de type $(2, 2)$. D'autre part, d'après [B-L-S-1, théorème 1], la tour des 2-corps de classes de Hilbert de $\mathbf{Q}(\sqrt{p_1 p_2 p_i})$ s'arrête en $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_i})$ si et seulement si $\left(\frac{p_1 p_2}{p_i}\right)_4 \left(\frac{p_1 p_i}{p_2}\right)_4 \left(\frac{p_2 p_i}{p_1}\right)_4 = 1$. Ce qui équivaut à dire que le 2-groupe de classes du corps biquadratique $F(\sqrt{p_i})$ est d'ordre égal à 2. Ce qui est équivalent à son tour, d'après la relation (*) de la preuve du lemme 4.2, à ce que $Q_{F(\sqrt{p_i})} = 1$. Ainsi l'égalité $Q_{F(\sqrt{p_i})} = 2$ dans le cas (ii-c) peut s'écrire sous la forme :

$$\left(\frac{p_1 p_2}{p_i}\right)_4 \left(\frac{p_1 p_i}{p_2}\right)_4 \left(\frac{p_2 p_i}{p_1}\right)_4 = -1.$$

4.1. Rang du 2-groupe de classes des corps $k_2(\sqrt{d})$. On sait d'après le lemme 3.2 qu'un système fondamental d'unités de $k_2 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$ est donné par : $\{\varepsilon_{p_1}, \varepsilon_{p_2}, \eta(p_1, p_2)\}$ où

$$\eta(p_1, p_2) = \begin{cases} \sqrt{\varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}} & \text{si } N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1, \\ \sqrt{\varepsilon_{p_1 p_2}} & \text{si } N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1 \end{cases}$$

On pose $K = k_2(\sqrt{d})$ où d est un entier naturel somme de deux carrés (ie, les premiers impairs divisant d sont congrus à 1 modulo 4). Soit r le nombre des premiers divisant d et qui se décomposent totalement dans k_2 . D'après l'inégalité $\text{rang}(Cl_2(K/k_2)) \geq \rho(K/k_2) - \text{rang}(E_{k_2}/E_{k_2} \cap N_{K/k_2}(K^*)) - 1$ (voir section 2) et le lemme 4.1

$$\text{rang}(Cl_2(K)) \geq 2^2 r + 2(n - 2 - r) - e - 1,$$

où $2^e = [E_{k_2} : E_{k_2} \cap N_{K/k_2}(K^*)]$. L'entier naturel e est déterminé suivant que ε_{p_1} , ε_{p_2} et $\eta(p_1, p_2)$ sont des normes ou non dans l'extension K/k_2 . Dans le théorème qui suit, on suppose que $r = 0$ et on étudie le rang du 2-groupe de classes de K , ce qui revient à calculer l'entier e . Pour $i \geq 3$, on note $E_i = \mathbf{Q}(\sqrt{p_1 p_2}, \sqrt{p_i})$.

Théorème 4.3. *Supposons qu'aucun des nombres premiers p_3, p_4, \dots, p_n ne se décompose totalement dans $k_2 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$. Soit $K = k_2(\sqrt{d})$ avec $d = p_1 p_2 \cdots p_n$. Alors, $e(K/k_2) \leq 1$. De plus :*

- (i) *lorsque $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$, $e(K/k_2) = 0$ si et seulement si $\left(\frac{p_1 p_2}{p_i}\right) = -1$ pour tout $i \geq 3$.*
- (ii) *lorsque $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$, $e(K/k_2) = 0$ si et seulement si l'une des deux conditions suivantes est satisfaite :*
 - (a) *pour tout $i \geq 3$, $\left(\frac{p_1}{p_i}\right) = \left(\frac{p_2}{p_i}\right) = -1$ et $Q_{E_i} = 2$;*
 - (b) *pour tout $i \geq 3$, on a (quitte à échanger p_1 et p_2) $\left(\frac{p_1}{p_i}\right) = -\left(\frac{p_2}{p_i}\right) = 1$ et $\left(\frac{p_1}{p_i}\right)_4 = \left(\frac{p_i}{p_1}\right)_4$.*

Remarque. Supposons que $\left(\frac{p_1}{p_2}\right) = -1$, alors comme dans la remarque précédente, l'égalité $Q_{E_i} = 2$ dans le cas (ii-a) du théorème précédent peut s'écrire sous la forme :

$$\left(\frac{p_1 p_2}{p_i}\right)_4 \left(\frac{p_1 p_i}{p_2}\right)_4 \left(\frac{p_2 p_i}{p_1}\right)_4 = -1.$$

Démonstration du théorème 4.3. Comme d est somme de deux carrés, -1 est norme dans l'extension K/k_2 et donc $e(K/k_2) \leq 3$. Soit \mathfrak{p} un idéal premier de k_2 ramifié dans K , alors \mathfrak{p} est au dessus d'un premier p_i $i \geq 3$. On note par F le corps de décomposition de p_i dans k_2 .

Soit $\mathfrak{q} := \mathfrak{p} \cap F$ l'idéal premier de F en dessous de \mathfrak{p} . Alors, on a l'égalité des symboles du reste normique

$$\left(\frac{\varepsilon_{p_1}, d}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_{p_1}, p_i}{\mathfrak{p}}\right) = \left(\frac{N_{k_2/F}(\varepsilon_{p_1}), p_i}{\mathfrak{q}}\right).$$

Le dernier symbole vaut 1 puisque $N_{k_2/F}(\varepsilon_{p_1}) = -1$ ou $\varepsilon_{p_1}^2$. Ainsi, ε_{p_1} (et de même ε_{p_2}) est norme dans l'extension K/k_2 . Il nous reste à étudier la valeur du symbole

$$\left(\frac{\eta(p_1, p_2), p_i}{\mathfrak{p}}\right) = \left(\frac{N_{k_2/F}(\eta(p_1, p_2)), p_i}{\mathfrak{q}}\right).$$

Dans le cas où $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$, on a, d'après la section 3.1, $\eta(p_1, p_2) = \sqrt{\varepsilon_{p_1 p_2}}$. Il existe donc un nombre rationnel u tel que $\varepsilon_{p_1 p_2} = p_1 u^2$ (démonstration du lemme 4.2). Par suite, en utilisant le lemme 3.3,

on trouve que

$$\left(\frac{\eta(p_1, p_2), p_i}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{si } \left(\frac{p_1}{p_i}\right) \neq \left(\frac{p_2}{p_i}\right), \\ -1 & \text{si } \left(\frac{p_1}{p_i}\right) = \left(\frac{p_2}{p_i}\right) = -1. \end{cases}$$

Notons que par hypothèse p_i ne se décompose pas totalement dans k_2 , de sorte que les deux symboles $\left(\frac{p_1}{p_i}\right)$ et $\left(\frac{p_2}{p_i}\right)$ ne prennent pas simultanément la valeur 1. Ainsi, dans ce cas, $\eta(p_1, p_2)$ est norme dans K/k_2 précisément lorsque $\left(\frac{p_1}{p_i}\right) \neq \left(\frac{p_2}{p_i}\right)$ pour tout $i \geq 3$.

Dans le cas où $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$, on a, d'après la section 3.1, $\eta(p_1, p_2) = \sqrt{\varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}}$. Par suite, d'après le lemme 3.3 (ii) :

$$\left(\frac{\eta(p_1, p_2), p_i}{\mathfrak{p}}\right) = \left(\frac{N_{k_2/F}(\eta(p_1, p_2)), p_i}{\mathfrak{q}}\right) = \left(\frac{\pm \varepsilon_m, p_i}{\mathfrak{q}}\right),$$

où $m \in \{p_1, p_2, p_1 p_2\}$ et $F = \mathbf{Q}(\sqrt{m})$. En utilisant le lemme 4.2, on trouve que:

$$\left(\frac{\eta(p_1, p_2), p_i}{\mathfrak{p}}\right) = \begin{cases} \left(\frac{p_i}{p_\ell}\right)_4 \left(\frac{p_\ell}{p_i}\right)_4 & \text{si } m = p_\ell, \ell = 1, 2 \\ (-1)^{Q_{E_i}} & \text{si } m = p_1 p_2. \end{cases}$$

Ainsi dans le cas où $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$, l'unité $\eta(p_1, p_2)$ est norme dans K/k_2 si et seulement si pour tout $i \geq 3$, on se trouve dans la situation (a) ou (b) de l'énoncé du théorème. \square

Nous allons tirer deux conséquences de ce théorème concernant le rang du 2-groupe de classes des corps $k_2(\sqrt{d})$ et k_n . Le premier corollaire est une conséquence immédiate de la section 2 :

Corollaire 4.4. *On garde les hypothèses du théorème 4.3. Si de plus le nombre de classes du corps k_2 est impair, alors on a*

$$\text{rang}(Cl_2(K)) = 2(n - 2) - e - 1,$$

où $e = e(K/k_2) = 0$ ou 1 comme dans l'énoncé du théorème 4.3.

Corollaire 4.5. *Sous les hypothèses du théorème 4.3, on a*

$$\text{rang}(Cl_2(k_n)) \geq n - 2 - e(K/k_2),$$

où $e = e(K/k_2) = 0$ ou 1 comme dans l'énoncé du théorème 4.3. En particulier, on a :

$$\text{rang}(Cl_2(k_n)) \geq n - 3.$$

Démonstration. On sait que $k_n/k_2(\sqrt{d})$ est une extension abélienne non ramifiée de degré 2^{n-3} . \square

Comme cas particulier du théorème précédent, on retrouve également le résultat de Fröhlich sur la parité du nombre de classes des corps k_3 . Pour une approche alternative voir [B].

Corollaire 4.6. ([F, page 78]) *Le nombre de classes de k_3 est impair si et seulement si, quitte à échanger les p_i , l'une des conditions suivantes est satisfaite :*

- (i) $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = -1$ et $\left(\frac{p_1 p_2}{p_3}\right)_4 \left(\frac{p_1 p_3}{p_2}\right)_4 \left(\frac{p_2 p_3}{p_1}\right)_4 = 1$.
(ii) $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -\left(\frac{p_2}{p_3}\right) = -1$ et $\left(\frac{p_2}{p_3}\right)_4 \neq \left(\frac{p_3}{p_2}\right)_4$.

Démonstration. Supposons qu'au moins deux des trois symboles $\left(\frac{p_1}{p_2}\right)$, $\left(\frac{p_1}{p_3}\right)$, $\left(\frac{p_2}{p_3}\right)$ valent 1, disons $\left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = 1$. Alors le nombre des premiers de k_2 ramifiés dans k_3 est $\rho = 4$. D'autre part, pour toute place de k_2 divisant p_3 nous avons, d'après la preuve du lemme 4.2 (i),

$$\left(\frac{\varepsilon_{p_1}, p_3}{\mathfrak{p}'}\right) = \left(\frac{p_1}{p_3}\right)_4 \left(\frac{p_3}{p_1}\right)_4.$$

De même

$$\left(\frac{\varepsilon_{p_2}, p_3}{\mathfrak{p}'}\right) = \left(\frac{p_2}{p_3}\right)_4 \left(\frac{p_3}{p_2}\right)_4,$$

de sorte qu'au moins l'une des unités ε_{p_1} , ε_{p_2} ou $\varepsilon_{p_1} \varepsilon_{p_2}$ est norme dans l'extension k_3/k_2 . En particulier, $e(k_3/k_2) \leq 2$ et on a, d'après la section 4.1, $\text{rang}(Cl_2(k_3)) \geq \rho - 1 - e(k_3/k_2) \geq 1$.

On peut donc supposer qu'au moins deux des trois symboles $\left(\frac{p_1}{p_2}\right)$, $\left(\frac{p_1}{p_3}\right)$, $\left(\frac{p_2}{p_3}\right)$ valent -1 , disons $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$. Dans ce cas, d'une part, le nombre de classes de $k_2 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$ est impair (voir par exemple [F, page 78]) et d'autre part p_3 ne se décompose pas totalement dans k_2 . On obtient donc, d'après le corollaire 4.4, que

$$\text{rang}(Cl_2(k_3)) = 2(3 - 2) - e - 1 = 1 - e,$$

avec $e = 1$ précisément lorsque l'une des conditions (i) et (ii) du corollaire est satisfaite. \square

Dans la section 5, nous donnerons les conditions nécessaires et suffisantes pour que le 2-groupe de classes de k_3 soit cyclique non trivial.

4.2. Rang du 2-groupe de classes des corps $k_3(\sqrt{d})$. On conserve les notations précédentes et on s'intéresse, dans cette section à l'étude du rang du 2-groupe de classes des corps $K = k_3(\sqrt{d})$. On a d'après le lemme 4.1 :

$$\text{rang}(Cl_2(K)) \geq \rho(K/k_3) - e(K/k_3) - 1 = 8r + 4(n - 3 - r) - e - 1,$$

où r est le nombre de premiers divisant d et décomposés dans k_3 .

Théorème 4.7. Soient $p_1, p_2, \dots, p_n, n \geq 4$ des nombres premiers distincts $\not\equiv -1 \pmod{4}$. Supposons qu'aucun des nombres premiers p_4, p_5, \dots, p_n ne se décompose totalement dans $k_3 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$. Soient $E = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ et $K = k_3(\sqrt{d})$ avec $d = p_1 p_2 \cdots p_n$. On suppose que $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$. Alors $e(K/k_3) \leq 4$ et de plus :

- (i) lorsque E n'est pas un corps de Kuroda, alors $e(K/k_3) \leq n - 3$.
- (ii) lorsque E est un corps de Kuroda, alors $e(K/k_3) \leq n - 2$.

Démonstration. Puisque $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$, un système fondamental d'unités de k_3 est de la forme suivante (section 3.2) :

$$\{\varepsilon_{p_1}, \varepsilon_{p_2}, \varepsilon_{p_3}, \eta(p_1, p_2), \eta(p_1, p_3), \eta(p_2, p_3), u\}$$

où

$$u = \begin{cases} \xi & \text{si } \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3}) \text{ est un corps de Kuroda,} \\ \eta(p_2, p_1 p_3) & \text{si } \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3}) \text{ n'est pas un corps de Kuroda.} \end{cases}$$

Comme -1 est norme dans l'extension K/k_3 (car d est somme de deux carrés), alors $0 \leq e(K/k_3) \leq 7$. Soit \mathfrak{p} un idéal premier de k_3 ramifié dans K , alors \mathfrak{p} est au dessus d'un premier $p_i, i \geq 4$. Soit E_i le corps de décomposition de p_i dans k_3 . L'extension k_3/E_i est quadratique puisque, par hypothèse, p_i ne se décompose pas totalement dans k_3 . Comme dans la preuve du théorème 4.3, on démontre que pour tout $j = 1, 2, 3$, on a

$$\left(\frac{\varepsilon_{p_j}, d}{\mathfrak{p}}\right) = 1,$$

autrement dit, $\varepsilon_{p_j}, j = 1, 2, 3$ est toujours une norme dans l'extension K/k_3 . En particulier, on a dans tous les cas : $e(K/k_3) \leq 4$.

Soit maintenant $\mathfrak{q} := \mathfrak{p} \cap E_i$ l'idéal premier de E_i en dessous de \mathfrak{p} . Étant donné $m \mid p_1 p_2 p_3$, on vérifie sans difficulté que $N_{k_3/E_i}(\varepsilon_m) = \pm 1$ ou ε_m^2 . Par suite, il existe $i_1, i_2, i_3, j_1, j_2, j_3 = 0, 1$ tels que

$$\begin{aligned} \left(\frac{\eta(p_j, p_k), p_i}{\mathfrak{p}}\right) &= \left(\frac{N_{k_3/E_i}(\eta(p_j, p_k)), p_i}{\mathfrak{q}}\right) \\ &= \left(\frac{\pm \varepsilon_{p_j}^{i_1} \varepsilon_{p_k}^{i_2} \varepsilon_{p_j p_k}^{i_3}, p_i}{\mathfrak{q}}\right) \end{aligned} \tag{1}$$

et

$$\begin{aligned} \left(\frac{\eta(p_2, p_1 p_3), p_i}{\mathfrak{p}}\right) &= \left(\frac{N_{k_3/E_i}(\eta(p_2, p_1 p_3)), p_i}{\mathfrak{q}}\right) \\ &= \left(\frac{\pm \varepsilon_{p_2}^{j_1} \varepsilon_{p_1 p_3}^{j_2} \varepsilon_{p_1 p_2 p_3}^{j_3}, p_i}{\mathfrak{q}}\right) \end{aligned} \tag{2}$$

quels que soient $j, k = 1, 2, 3$ distincts.

En redescendant ces derniers symboles à une sous extension quadratique de E_i , on voit qu'ils ne dépendent pas du choix des places \mathfrak{q} au dessus de p_i . Le fait que les symboles $\left(\frac{\eta(p_j, p_k), p_i}{\mathfrak{p}}\right)$ et $\left(\frac{\eta(p_2, p_1 p_3), p_i}{\mathfrak{p}}\right)$ ne dépendent pas du choix des idéaux premiers \mathfrak{p} au dessus de $p_i, i \geq 4$, nous donne les inégalités suivantes :

(i) $[E_{k_3} : E_{k_3} \cap N_{k_3(\sqrt{p_i})/k_3}(k_3(\sqrt{p_i}))] \leq 2$ lorsque E n'est pas un corps de Kuroda et

(ii) $[E_{k_3} : E_{k_3} \cap N_{k_3(\sqrt{p_i})/k_3}(k_3(\sqrt{p_i}))] \leq 4$ lorsque E est un corps de Kuroda.

L'inégalité du cas (i) de l'énoncé s'en déduit immédiatement grâce à l'injection

$$E_{k_3}/E_{k_3} \cap N_{K/k_3}(K^*) \longrightarrow \prod_{i \geq 4} E_{k_3}/E_{k_3} \cap N_{k_3(\sqrt{p_i})/k_3}(k_3(\sqrt{p_i})).$$

Désormais on suppose que E est un corps de Kuroda, il faut noter que le symbole $\left(\frac{\xi, p_i}{\mathfrak{p}}\right)$ peut alors dépendre du choix des premiers de k_3 au-dessus de p_i . Le morphisme injectif précédent permet de conclure dans ce cas pour $n = 4$. Il nous reste donc à traiter le cas où $n = 5$. Puisque $\left(\frac{\eta(p_j, p_k), p_i}{\mathfrak{p}}\right)$ ne dépend pas du choix des idéaux premiers $\mathfrak{p} \mid p_i (i = 4, 5)$, on voit que les classes des trois unités $\eta(p_1, p_2), \eta(p_1, p_3), \eta(p_2, p_3)$ vont engendrer un sous-espace de dimension au plus 2 dans $E_{k_3}/E_{k_3} \cap N_{K/k_3}(K^*)$; ce qui montre bien que $e(K/k_3) \leq 3$. \square

Définition 4.8. Soient $p_1, p_2, \dots, p_n, n \geq 4$ des nombres premiers distincts $\not\equiv -1 \pmod{4}$. On suppose que $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$. On dit que p_1, p_2, \dots, p_n satisfont l'hypothèse \mathcal{H} si les trois conditions suivantes sont satisfaites :

(\mathcal{H}_a) $\forall i \in \{1, 2, 3\}$ et $\forall \ell \geq 4$ tels que $\left(\frac{p_i}{p_\ell}\right) = 1$, on a

$$\left(\frac{p_i}{p_\ell}\right)_4 = \left(\frac{p_\ell}{p_i}\right)_4.$$

(\mathcal{H}_b) $\forall i, j \in \{1, 2, 3\}$ et $\forall \ell \geq 4$ tels que $\left(\frac{p_\ell}{p_i}\right) = \left(\frac{p_\ell}{p_j}\right) = -1$, on a

$$Q_{\mathbb{Q}(\sqrt{p_\ell}, \sqrt{p_i p_j})} = 2$$

(\mathcal{H}_c) $\forall i, j, k \in \{1, 2, 3\}$ et $\forall \ell \geq 4$ tels que $\left(\frac{p_\ell}{p_i}\right) = -\left(\frac{p_\ell}{p_j}\right) = -\left(\frac{p_\ell}{p_k}\right) = 1$, on a

$$Q_{\mathbb{Q}(\sqrt{p_i}, \sqrt{p_j p_k})} = 2.$$

On se place sous les hypothèses du théorème 4.7. Moyennant les deux égalités (1) et (2) de la preuve du théorème 4.7 et le lemme 4.2, on peut montrer que les unités $\eta(p_1, p_2), \eta(p_1, p_3), \eta(p_2, p_3)$ et $\eta(p_2, p_1 p_3)$ sont des normes dans l'extension K/k_3 si et seulement si p_1, p_2, \dots, p_n satisfont l'hypothèse \mathcal{H} . Ce qui permet d'obtenir le corollaire suivant :

Corollaire 4.9. *Supposons qu'aucun des nombres premiers p_4, p_5, \dots, p_n ne se décompose totalement dans k_3 et que $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$.*

- (i) *Lorsque le corps $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ n'est pas de Kuroda, alors $e(K/k_3) = 0$ si et seulement si p_1, p_2, \dots, p_n satisfont l'hypothèse \mathcal{H} .*
- (ii) *Lorsque le corps $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ est de Kuroda, alors $e(K/k_3) = 0$ ou 1 dès que p_1, p_2, \dots, p_n satisfont l'hypothèse \mathcal{H} .*

Plaçons-nous sous les hypothèses du corollaire précédent avec $n = 4$: p_1, p_2 et p_3 sont des nombres premiers distincts $\not\equiv -1 \pmod{4}$ tels que $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$ et $p_4 \not\equiv -1 \pmod{4}$ est un nombre premier qui ne se décompose pas totalement dans k_3 . Alors

$$\text{rang}(Cl_2(k_4)) \geq \rho(k_4/k_3) - e(K/k_3) - 1 = 3 - e(K/k_3) = 3 \text{ ou } 2.$$

Si le nombre de classes de k_3 est impair, alors l'inégalité précédente devient une égalité : $\text{rang}(Cl_2(k_4)) = 3$ ou 2. Plus précisément, $\text{rang}(Cl_2(k_4)) = 3$ si et seulement si les premiers p_1, p_2, p_3 et p_4 satisfont à l'hypothèse \mathcal{H} . Numériquement, on peut prendre par exemple $p_1 = 41, p_2 = 137, p_3 = 13$ et $p_4 = 2$.

Corollaire 4.10. *Sous les hypothèses et notations du théorème 4.7, on a :*

$$\text{rang}(Cl_2(k_n)) \geq 3(n - 3) - e(K/k_3) \geq 3n - 13.$$

En particulier, si $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ n'est pas de Kuroda et les p_i satisfont à l'hypothèse \mathcal{H} , alors on a :

$$\text{rang}(Cl_2(k_n)) \geq 3(n - 3).$$

Démonstration. Il suffit de remarquer que $k_n/k_3(\sqrt{d})$ est une extension abélienne non ramifiée de degré 2^{n-4} . □

5. Applications

Nous allons appliquer les résultats obtenus aux cas particuliers où $n = 3$ ou $n = 4$.

En supposant que K/\mathbf{Q} est une 2-extension abélienne réelle qui est son propre corps de genres au sens restreint (notons que ceci entraîne que les nombres premiers impairs ramifiés dans K sont congrus à 1 modulo 4), A. Fröhlich a démontré que $\text{rang}(Cl_2(K)) \geq 1$ dès que le discriminant de K est divisible par au moins 4 premiers [F, théorème 5.6].

Dans ce qui suit, on démontre dans un premier temps que $\text{rang}(Cl_2(k_4)) \geq 2$ (théorème 5.3). On détermine aussi une famille infinie de corps k_4 tels que $\text{rang}(Cl_2(k_4)) = 2$. Ensuite, on en déduit que $\text{rang}(Cl_2(K)) \geq 2$ pour toute 2-extension abélienne réelle K dont les premiers impairs ramifiés sont congrus à 1 modulo 4 (théorème 5.5). Ce qui améliore le résultat de Fröhlich. Signalons de plus que le corps de genres de tels corps K au sens restreint peut contenir strictement son corps de genres au sens large.

Comme application des sections précédentes, on détermine également parmi les corps multiquadratiques dont le discriminant n'est divisible par aucun nombre premier $\equiv -1 \pmod{4}$, ceux dont le 2-groupe de classes est cyclique non trivial.

On reprend les notations de la section 4.

Proposition 5.1. *Soient p_1, p_2, p_3 et p_4 des nombres premiers distincts $\not\equiv -1 \pmod{4}$. On suppose que pour tout $i = 1, 2, 3, 4$, il existe au plus un $j \in \{1, \dots, 4\}$, tel que $\left(\frac{p_i}{p_j}\right) = 1$. Alors, il existe un sous-corps M de k_4 tel que k_4/M est une extension quadratique ramifiée et $e(k_4/M) \leq 1$. En particulier, $\text{rang}(Cl_2(k_4)) \geq 2$.*

Démonstration. L'assertion sur le rang de $Cl_2(k_4)$ est une conséquence de l'inégalité $e(k_4/M) \leq 1$ et de la formule

$$\text{rang}(Cl_2(k_4)) \geq \rho(k_4/M) - 1 - e(k_4/M)$$

de la section 2, puisque, sous les hypothèses de l'énoncé, on a $\rho(k_4/M) = 4$.

D'après le point (i) du théorème 4.7, on peut supposer que quels que soient i, j, k tels que $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_i}{p_k}\right) = -1$, le corps $\mathbf{Q}(\sqrt{p_i}, \sqrt{p_j p_k})$ est de Kuroda.

Deux des trois symboles $\left(\frac{p_1}{p_2}\right), \left(\frac{p_1}{p_3}\right), \left(\frac{p_1}{p_4}\right)$ valent -1 , disons $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$. Comme $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$ est un corps de Kuroda, un système fondamental d'unités de k_3 est de la forme $\{\varepsilon_{p_1}, \varepsilon_{p_2}, \varepsilon_{p_3}, \eta(p_1, p_2), \eta(p_1, p_3), \eta(p_2, p_3), \xi\}$. D'après la preuve du théorème 4.7, les unités $\varepsilon_{p_1}, \varepsilon_{p_2}$ et ε_{p_3} sont des normes dans k_4/k_3 . Montrons que les unités $\eta(p_1, p_2), \eta(p_1, p_3), \eta(p_2, p_3)$ sont aussi des normes dans l'extension k_4/k_3 .

Soit E le corps de décomposition de p_4 dans k_3 . Soit \mathfrak{q} un idéal premier de E au-dessus de p_4 et \mathfrak{p} l'idéal premier de k_3 au-dessus de \mathfrak{q} . Comme dans la preuve du théorème 4.7, pour tout $i, j = 1, 2, 3$ distincts, il existe $i_1, i_2, i_3 = 0, 1$ tels que :

$$\left(\frac{\eta(p_i, p_j), p_4}{\mathfrak{p}}\right) = \left(\frac{\pm \varepsilon_{p_i}^{i_1} \varepsilon_{p_j}^{i_2} \varepsilon_{p_i p_j}^{i_3}, p_4}{\mathfrak{q}}\right).$$

Le corps biquadratique E prend l'une des deux formes suivantes :

(i) $E = \mathbf{Q}(\sqrt{p_1 p_2}, \sqrt{p_1 p_3})$.

Comme ε_{p_i} et ε_{p_j} ne sont pas dans E , dans l'égalité précédente sur les symboles du reste normique on a forcément $i_1 = i_2 = 0$.

De plus, puisque dans ce cas $\left(\frac{p_i}{p_4}\right) = \left(\frac{p_j}{p_4}\right) = -1$ où $i, j = 1, 2, 3$, le corps $\mathbf{Q}(\sqrt{p_4}, \sqrt{p_i p_j})$ est de Kuroda. Ainsi, par définition, l'indice $Q_{\mathbf{Q}(\sqrt{p_4}, \sqrt{p_i p_j})} = 2$ et d'après le lemme 4.2 (ii-c), $\varepsilon_{p_i p_j}$ est norme dans $E(\sqrt{p_4})/E$. Par conséquent $\eta(p_i, p_j)$ est norme dans k_4/k_3 .

(ii) E est l'un des trois corps $\mathbf{Q}(\sqrt{p_1}, \sqrt{p_2 p_3})$, $\mathbf{Q}(\sqrt{p_2}, \sqrt{p_1 p_3})$ et $\mathbf{Q}(\sqrt{p_3}, \sqrt{p_1 p_2})$.

Comme dans le cas (i), on voit que $\varepsilon_{p_i p_j}$ est norme dans $E(\sqrt{p_4})/E$. L'exposant i_1 (resp. i_2) est nul si E ne contient pas $\sqrt{p_i}$ (resp. $\sqrt{p_j}$). Quitte à échanger i_1 et i_2 , on peut supposer $i_1 = 1$ et $i_2 = 0$. Il nous reste donc à justifier que ε_{p_i} est norme dans $E(\sqrt{p_4})/E$. On a nécessairement $\left(\frac{p_4}{p_i}\right) = 1$. Il existe $s \leq 4$ tel que $\left(\frac{p_s}{p_i}\right) = \left(\frac{p_s}{p_4}\right) = -1$. En particulier $\mathbf{Q}(\sqrt{p_s}, \sqrt{p_i p_4})$ est un corps de Kuroda. Or, comme $\left(\frac{p_4}{p_i}\right) = 1$, on a, d'après la section 3.2, $\left(\frac{p_i}{p_4}\right)_4 = \left(\frac{p_4}{p_i}\right)_4$. En utilisant le lemme 4.2(i), ε_{p_i} est norme dans l'extension $E(\sqrt{p_4})/E$. D'où finalement $\eta(p_i, p_j)$ est norme dans k_4/k_3 . □

Proposition 5.2. *Soient p_1, p_2, p_3 et p_4 des nombres premiers distincts $\not\equiv -1 \pmod{4}$. On suppose que p_3 se décompose totalement dans $k_2 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$.*

(i) *Si p_4 ne se décompose pas totalement dans k_2 , alors $e(k_2(\sqrt{p_3 p_4})/k_2) \leq 2$. En particulier $\text{rang}(Cl_2(k_4)) \geq 2$.*

(ii) *Si p_4 se décompose totalement dans k_2 , alors $\text{rang}(Cl_2(k_4)) \geq 3$.*

Démonstration. On sait que :

$$\begin{aligned} \text{rang}(Cl_2(k_4)) &\geq \text{rang}(Cl_2(k_2(\sqrt{p_3 p_4}))) - 1 \\ &\geq \rho(k_2(\sqrt{p_3 p_4})/k_2) - 2 - e(k_2(\sqrt{p_3 p_4})/k_2), \end{aligned}$$

où évidemment $e(k_2(\sqrt{p_3 p_4})/k_2) \leq 3$.

Comme p_3 se décompose totalement dans k_2 , on a $\rho(k_2(\sqrt{p_3 p_4})/k_2) = 8$ ou 6 suivant que p_4 se décompose totalement ou non dans k_2 . Par conséquent, dès que p_4 se décompose totalement dans k_2 , on a bien $\text{rang}(Cl_2(k_4)) \geq 3$.

Si, au contraire, p_4 ne se décompose pas totalement dans k_2 , on a

$$\text{rang}(Cl_2(k_4)) \geq 4 - e(k_2(\sqrt{p_3 p_4})/k_2)$$

et il reste à démontrer que $e(k_2(\sqrt{p_3 p_4})/k_2) \leq 2$.

D'après la preuve du théorème 4.3, ε_{p_1} et ε_{p_2} sont des normes dans l'extension $k_2(\sqrt{p_4})/k_2$ et d'après la preuve du lemme 4.2(i), l'une des unités ε_{p_1} , ε_{p_2} ou $\varepsilon_{p_1} \varepsilon_{p_2}$ est une norme dans l'extension $k_2(\sqrt{p_3})/k_2$. Ainsi, l'une de

ces trois unités est norme dans $k_2(\sqrt{p_3p_4})/k_2$ de sorte que $e(k_2(\sqrt{p_3p_4})/k_2) \leq 2$. □

En combinant les deux propositions précédentes, on obtient :

Théorème 5.3. *Soient p_1, p_2, p_3, p_4 des nombres premiers distincts $\not\equiv -1 \pmod{4}$. Alors le 2-groupe de classes de $k_4 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$ est de rang ≥ 2 .*

Une démonstration alternative de ce dernier théorème devrait pouvoir se faire de la façon suivante. Notons $k = \mathbf{Q}(\sqrt{p_1p_2p_3p_4})$. L'extension k_4/k est abélienne non ramifiée de groupe de Galois G . Soient K_{cen} et K_{gen} respectivement l'extension centrale et le corps de genres de k_4/k , et soit $M(G)$ le multiplicateur de Schur de G . Les résultats standard de la théorie du corps de classes (voir par exemple [B-L-S-2]) montrent que :

$$\text{rang}(Gal(K_{cen}/K_{Gen})) \geq \text{rang}(M(G)) - \text{rang}(E_k/E_k \cap N(k_4^*)).$$

Comme G est un 2-groupe élémentaire d'ordre 8, alors il en est de même de $M(G)$. D'autre part, puisque les quatre premiers p_i sont $\not\equiv -1 \pmod{4}$, on devrait pouvoir démontrer que -1 est une norme dans l'extension k_4/k de sorte que $\text{rang}(E_k/E_k \cap N(k_4^*)) \leq 1$. On en déduirait immédiatement que $\text{rang}(Gal(K_{cen}/K_{Gen})) \geq 2$.

L'exemple suivant montre que la borne inférieure 2 est optimale :

Exemple 5.4. Il existe une infinité de corps k_4 tels que $\text{rang}(Cl_2(k_4)) = 2$. En effet, soient p_1, p_2 et p_3 des nombres premiers tels que le nombre de classes de k_3 soit impair. Quitte à renuméroter les p_i on a d'après le corollaire 4.6 : $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -1$. Par ailleurs, d'après [M-U, théorème 7], il existe une infinité de nombres premiers $p_4 \equiv 1 \pmod{4}$ satisfaisant aux deux propriétés suivantes :

(i) $\left(\frac{p_4}{p_1}\right) = \left(\frac{p_4}{p_2}\right) = -1$;

(ii) le corps $\mathbf{Q}(\sqrt{p_1p_2}, \sqrt{p_1p_4})$ est d'indice d'unités égal à 1.

Pour $i, j = 1, 2, 4$, on a $h_2(p_i p_j) = 2$ et $h_2(p_1 p_2 p_4) = 4$ [Ré-Re]. Par suite en appliquant la formule du nombre de classes d'un corps multiquadratique (section 3) au corps $\mathbf{Q}(\sqrt{p_1p_2}, \sqrt{p_1p_4})$, puis au corps $\mathbf{Q}(\sqrt{p_4}, \sqrt{p_1p_2})$ on voit que l'indice des unités de ce dernier corps est égal à 1. Donc d'après le lemme 4.2(c), l'unité $\varepsilon_{p_1p_2}$ n'est pas norme dans l'extension $E(\sqrt{p_4})/E$. Comme $N_{k_3/E}(\eta(p_1, p_2)) = \pm \varepsilon_{p_1p_2}$, alors l'unité $\eta(p_1, p_2)$ n'est pas norme dans k_4/k_3 . Ainsi $e(k_4/k_3) \geq 1$. Or, comme le nombre de classes de k_3 est impair, on a :

$$\text{rang}(Cl_2(k_4)) = \rho(k_4/k_3) - e(k_4/k_3) - 1 = 3 - e(k_4/k_3).$$

Il suffit maintenant d'appliquer le théorème 5.3.

À partir du théorème 5.3, il n'est pas difficile de montrer :

Théorème 5.5. *Soit K/\mathbf{Q} une 2-extension abélienne réelle dans laquelle au moins quatre premiers $\not\equiv -1 \pmod{4}$ se ramifient. Alors, on a*

$$\text{rang}(Cl_2(K)) \geq 2.$$

Démonstration. Notons par $K^{(*)}$ le corps de genres de K au sens large et par $K_{(*)}$ le corps de genres de K au sens restreint. Il est bien connu que $K^{(*)}$ est le sous-corps réel maximal de $K_{(*)}$. D'après la théorie des genres, $Gal(K_{(*)}/\mathbf{Q})$ est de rang supérieur ou égal à 4 puisqu'au moins quatre premiers $p_1, p_2, p_3, p_4 \not\equiv -1 \pmod{4}$ sont ramifiés dans K . Il s'ensuit que $K_{(*)}$ contient k_4 et puisque k_4 est totalement réel, il en est de même de $K^{(*)}$.

Notons par H le 2-corps de classes de Hilbert de k_4 . Comme $k_4 = k_4^{(*)}$ est son propre corps de genres au sens large, alors $K^{(*)} \cap H = k_4$. Ainsi, en appliquant le théorème 5.3, le rang du 2-groupe de classes de $K^{(*)}$ est supérieur ou égal à 2. Par conséquent, on a $\text{rang}(Cl_2(K)) \geq 2$. \square

Exemple 5.6. Soit m un entier naturel et $K := \mathbf{Q}(\zeta_m)$. Lorsque m est divisible par au moins quatre nombres premiers congrus à 1 modulo 4, G. Cornell et L. Washington ont démontré que le nombre de classes de K est pair [C-W]. Dans [L], F. Lemmermeyer a démontré que lorsque m est divisible seulement par trois nombres premiers non congrus à -1 modulo 4, alors le nombre de classes de K est pair. Soit $m := p_1 p_2 p_3 p_4$ le produit de quatre nombres premiers non congrus à -1 modulo 4. Alors pour toute 2-sous-extension K du corps cyclotomique $\mathbf{Q}(\zeta_m)$ où les quatre premiers p_i sont ramifiés, on a $\text{rang}(Cl_2(K)) \geq 2$. Lorsque $K := \mathbf{Q}(\zeta_m)^+$ est le sous-corps réel maximal de $\mathbf{Q}(\zeta_m)$, il n'est pas difficile de voir que $K_{(*)} \neq K^{(*)}$.

Dans la suite, nous allons déterminer tous les corps multiquadratiques réels dont les premiers impairs ramifiés sont congrus à 1 modulo 4 et dont le 2-groupe de classes est cyclique non trivial.

Au préalable, nous avons besoin d'analyser la situation où le nombre premier p_3 se décompose totalement dans $k_2 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2})$. Au cours de la démonstration du corollaire 4.6, on a vu l'inégalité $e(k_3/k_2) \leq 2$. Le résultat suivant précise la valeur de $e(k_3/k_2)$.

Lemme 5.7. *On suppose que $\left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = 1$, alors $e(k_3/k_2) \leq 2$. De plus :*

- (i) *lorsque $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$, alors $e(k_3/k_2) \leq 1$.*
- (ii) *lorsque $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$, alors $e(k_3/k_2) = 2$ si et seulement si $\left(\frac{p_1}{p_3}\right)_4 \neq \left(\frac{p_3}{p_1}\right)_4$ ou $\left(\frac{p_2}{p_3}\right)_4 \neq \left(\frac{p_3}{p_2}\right)_4$.*

Démonstration. Par hypothèse, k_2 est le corps de décomposition de p_3 dans k_3 . Donc, d'après le lemme 4.2 (i), l'unité ε_{p_1} (resp. ε_{p_2}) est norme dans

k_3/k_2 si et seulement si $(\frac{p_1}{p_3})_4 = (\frac{p_3}{p_1})_4$ (resp. $(\frac{p_2}{p_3})_4 = (\frac{p_3}{p_2})_4$).

(i) lorsque $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = 1$, alors $\{\varepsilon_{p_1}, \varepsilon_{p_2}, \sqrt{\varepsilon_{p_1 p_2}}\}$ est un système fondamental d'unités de k_2 (lemme 3.2(i)).

Soient \mathfrak{p} et \mathfrak{p}' deux idéaux premiers de k_2 au dessus de p_3 , on a

$$\left(\frac{\sqrt{\varepsilon_{p_1 p_2}}, p_3}{\mathfrak{p}}\right) \left(\frac{\sqrt{\varepsilon_{p_1 p_2}}, p_3}{\mathfrak{p}'}\right) = \left(\frac{N_{k_2/F}(\sqrt{\varepsilon_{p_1 p_2}}), p_3}{\mathfrak{q}}\right),$$

où \mathfrak{q} est un idéal premier d'un sous-corps quadratique F de k_2 . Or d'après le lemme 3.3 (i), on a

$$N_{k_2/F}(\sqrt{\varepsilon_{p_1 p_2}}) = \begin{cases} \pm 1 & \text{si } F \neq \mathbf{Q}(\sqrt{p_1 p_2}), \\ \pm \varepsilon_{p_1 p_2} & \text{sinon.} \end{cases}$$

Ce qui montre directement que ce dernier symbole vaut 1 lorsque $F \neq \mathbf{Q}(\sqrt{p_1 p_2})$. Dans le cas où $F = \mathbf{Q}(\sqrt{p_1 p_2})$, comme on l'a remarqué au cours de la démonstration du lemme 4.2(ii), $\varepsilon_{p_1 p_2}/p_1$ est un carré de F , de sorte que

$$\left(\frac{N_{k_2/F}(\sqrt{\varepsilon_{p_1 p_2}}), p_3}{\mathfrak{q}}\right) = \left(\frac{p_1}{p_3}\right) = 1.$$

Ainsi, le symbole $\left(\frac{\sqrt{\varepsilon_{p_1 p_2}}, p_3}{\mathfrak{p}}\right)$ ne dépend pas du choix des premiers \mathfrak{p} de k_2 au dessus de p_3 . On en tire aussitôt que $e(k_3/k_2) \leq 1$.

(ii) lorsque $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$, alors $\{\varepsilon_{p_1}, \varepsilon_{p_2}, \eta(p_1, p_2)\}$ est un système fondamental d'unités de k_2 où $\eta(p_1, p_2) = \sqrt{\varepsilon_{p_1} \varepsilon_{p_2} \varepsilon_{p_1 p_2}}$. Si nous avons simultanément $(\frac{p_1}{p_3})_4 = (\frac{p_3}{p_1})_4$ et $(\frac{p_2}{p_3})_4 = (\frac{p_3}{p_2})_4$, alors ε_{p_1} et ε_{p_2} sont des normes dans k_3/k_2 et trivialement $e(k_3/k_2) \leq 1$.

Réciproquement supposons qu'il existe $i \in \{1, 2\}$ tel que $(\frac{p_i}{p_3})_4 \neq (\frac{p_3}{p_i})_4$, alors ε_{p_i} n'est pas norme dans k_3/k_2 . De plus, contrairement au cas (i), le symbole $\left(\frac{\eta(p_1, p_2), p_3}{\mathfrak{p}}\right)$ dépend du choix des premiers \mathfrak{p} de k_2 au dessus de p_3 . En effet,

$$\begin{aligned} \left(\frac{\eta(p_1, p_2), p_3}{\mathfrak{p}}\right) \left(\frac{\eta(p_1, p_2), p_3}{\mathfrak{p}'}\right) &= \left(\frac{N_{k_2/\mathbf{Q}(\sqrt{p_i})}(\eta(p_1, p_2)), p_3}{\mathfrak{q}}\right) \\ &= \left(\frac{\pm \varepsilon_{p_i} p_3}{\mathfrak{q}}\right) && \text{(lemme 3.3(ii))} \\ &= \left(\frac{p_i}{p_3}\right)_4 \left(\frac{p_3}{p_i}\right)_4 && \text{(lemme 4.2(i))} \\ &= -1 && \text{(par hypothèse)} \end{aligned}$$

Ainsi les unités ε_{p_i} , $\eta(p_1, p_2)$ et $\varepsilon_{p_i} \eta(p_1, p_2)$ ne sont pas des normes dans k_3/k_2 . Donc $e(k_3/k_2) = 2$. □

Soient d_1, d_2, \dots, d_r des entiers naturels sans facteurs carrés non divisibles par un premier $\equiv -1 \pmod{4}$ et $K := \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_r})$. Notons p_1, p_2, \dots, p_n tous les nombres premiers divisant le discriminant de K de sorte que $k_n = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ est le corps de genres de K . Supposons que le 2-groupe de classes du corps multiquadratique K est cyclique non trivial. Alors $\text{rang}(Cl_2(k_n)) \leq 1$ et forcément $n \leq 3$ d'après le théorème 5.3. Lorsque $n \leq 2$, il est bien connu que le 2-groupe de classes de K est cyclique (avec possibilité qu'il soit trivial). Pour $n = 3$, K pourrait prendre l'une des quatre formes suivantes :

- (i) $K := \mathbf{Q}(\sqrt{p_1 p_2 p_3})$;
- (ii) $K := \mathbf{Q}(\sqrt{p_1 p_2}, \sqrt{p_3})$;
- (iii) $K := \mathbf{Q}(\sqrt{p_1 p_2}, \sqrt{p_1 p_3})$;
- (iv) $K := k_3 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$.

Le cas (i) est évidemment exclu car $\text{rang}(Cl_2(\mathbf{Q}(\sqrt{p_1 p_2 p_3}))) = 2$. Les cas (ii) et (iii) sont essentiellement connus. Le théorème suivant donne les conditions nécessaires et suffisantes pour que le 2-groupe de classes de $k_3 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ soit cyclique non trivial :

Théorème 5.8. *Soient p_1, p_2 et p_3 trois nombres premiers $\not\equiv -1 \pmod{4}$. Alors le 2-groupe de classes de $k_3 = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3})$ est cyclique non trivial précisément lorsque, quitte à échanger les p_i , l'une des trois conditions suivantes est satisfaite :*

- (i) $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = -1$ et $\left(\frac{p_1 p_2}{p_3}\right)_4 \left(\frac{p_1 p_3}{p_2}\right)_4 \left(\frac{p_2 p_3}{p_1}\right)_4 = -1$;
- (ii) $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = -\left(\frac{p_2}{p_3}\right) = -1$ et $\left(\frac{p_2}{p_3}\right)_4 = \left(\frac{p_3}{p_2}\right)_4$;
- (iii) $\left(\frac{p_1}{p_2}\right) = -\left(\frac{p_1}{p_3}\right) = -\left(\frac{p_2}{p_3}\right) = -1$ et $\left[\left(\frac{p_1}{p_3}\right)_4 \neq \left(\frac{p_3}{p_1}\right)_4 \text{ ou } \left(\frac{p_2}{p_3}\right)_4 \neq \left(\frac{p_3}{p_2}\right)_4\right]$.

Démonstration. Si k_3/E est une extension quadratique ramifiée, on a

$$\text{rang}(Cl_2(k_3)) \geq \rho(k_3/E) - 1 - e(k_3/E)$$

avec égalité dès que le nombre de classes de E est impair.

Supposons d'abord que $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = 1$. Alors en vertu du lemme 5.7, pour que $\text{rang}(Cl_2(k_3)) \leq 1$ il est nécessaire que

$$N_{\mathbf{Q}(\sqrt{p_i p_j})/\mathbf{Q}}(\varepsilon_{p_i p_j}) = -1$$

quels que soient i et j . Or puisque cette dernière condition entraîne que $\left(\frac{p_i}{p_j}\right)_4 = \left(\frac{p_j}{p_i}\right)_4$ quels que soient i et j (voir section 3.2), on voit, toujours d'après le lemme 5.7, que $\text{rang}(Cl_2(k_3)) \geq 2$. Ainsi pour que le 2-groupe de classes de k_3 soit cyclique non trivial, il est nécessaire que l'un des trois symboles $\left(\frac{p_1}{p_2}\right)$, $\left(\frac{p_1}{p_3}\right)$, $\left(\frac{p_2}{p_3}\right)$ soit égal à -1 . Disons $\left(\frac{p_1}{p_2}\right) = -1$. Alors on

a $N_{\mathbf{Q}(\sqrt{p_1 p_2})/\mathbf{Q}}(\varepsilon_{p_1 p_2}) = -1$ (section 3.2). De plus, d'après [F, théorème 5.7], le nombre de classes de k_2 est impair de sorte que $\text{rang}(Cl_2(k_3)) = \rho(k_3/k_2) - e(k_3/k_2) - 1$. Deux cas se présentent :

$\rho(k_3/k_2) = 2$, autrement dit l'un des deux symboles $\left(\frac{p_1}{p_3}\right)$ ou $\left(\frac{p_2}{p_3}\right)$ vaut -1. Il suffit alors d'appliquer le théorème 4.3 (ii) correspondant aux cas (i) et (ii) de l'énoncé.

$\rho(k_3/k_2) = 4$, autrement dit les deux symboles $\left(\frac{p_1}{p_3}\right)$ et $\left(\frac{p_2}{p_3}\right)$ valent 1. Il suffit alors d'appliquer le lemme 5.7 (ii) correspondant au cas (iii) de l'énoncé. \square

Remerciements. Le premier auteur tient à remercier le conseil régional du Limousin et le LACO (UMR 6090 CNRS) qui l'ont financé pendant son séjour post-doctoral à Limoges.

Bibliographie

- [A-M-1] A. AZIZI, 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**, no 7 (2001), 2741–2752.
- [A-M-2] A. AZIZI, A. MOUHIB, *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**, no 1 (2003), 27–73.
- [B] M. BULANT, *On the Parity of the Class Number of the Fields $\mathbf{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$* . Journal of Number Theory **68** (1998), 72–86.
- [B-L-S-1] E. BENJAMIN, F. LEMMERMEYER, C. SNYDER, *Real quadratic fields with abelian 2-class field tower*. J. Number Theory **73**, no. 2 (1998), 182–194.
- [B-L-S-2] E. BENJAMIN, F. LEMMERMEYER, C. SNYDER, *Imaginary quadratic fields k with cyclic $Cl_2(k^1)$* . J. Number Theory **67**, no. 2 (1997), 229–245.
- [C] H. COHN, *A Numerical Study of units in Composite Real Quartic and Octic fields*. Proceedings of the sciences Research Council Atlas Symposium No. 2 held at Oxford, from 18-23 August, 1969
- [C-W] G. CORNELL, L. WASHINGTON, *Class numbers of cyclotomic fields*. J. Number Theory **21** (1985), 260–274.
- [C-H] P. E. CONNER, J. HURRELBRINK, *Class Number Parity*. Series in pure Mathematics, Vol. **8**, World Sciences, Singapore, 1988.
- [F] A. FRÖHLICH, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*. Contemp. Math. **24**, Amer. Math. Soc., Providence, 1983.
- [G] G. GRAS, *Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier l* . Ann. Institut. Fourier **23**, fasc. 3 (1973), 1–48.
- [H] H. HASSE, *Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols*. J. Reine Angew. Math. **162** (1930), 143–144.
- [J] W. JEHNÉ, *On knots in algebraic number theory*. J. Reine Angew. Math. **311/312** (1979), 215–254.
- [K] R. KUČERA, *On the parity of the class number of a biquadratic field*. J. Number theory **52** (1995), 43–52.
- [Ku] S. KURODA, *Über den Dirichletschen Körper*. J. Fac. Sci. Univ. Tokyo, Sect. I **4** (1943), 383–406.
- [L] F. LEMMERMEYER, *On class groups of cyclotomic number fields II*. Acta Arith. **84** (1998), 59–70.
- [M-U] M. MAZUR, S. V. ULLOM, *Galois module structure of units in real biquadratic number fields*. Acta Arith. **111**, no 2 (2004), 105–124.

- [Ré-Re] L. RÉDEI, H. REICHARDT, *Die Anzahl der durch 4 teilbaren Invarianten der Klassen-
gruppe eines beliebigen quadratischen Zahlkörpers*. J. Reine Angew. Math. **170** (1933),
69–74.
- [S] A. SCHOLZ, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$* . Math. Zeitschrift **39**
(1934), 93–111.
- [W] H. WADA, *On the class number and the unit group of certain algebraic number fields*.
Tokyo U., Fac. of sc. J., Serie I, **13** (1966), 201–209.

Ali MOUHIB
Université Mohammed Ben Abdellah
Faculté polydisciplinaire de Taza
Maroc

Abbas MOVAHHEDI
LACO, UMR 6090 CNRS
Université de Limoges
123, Avenue A. Thomas
87060 Limoges, France