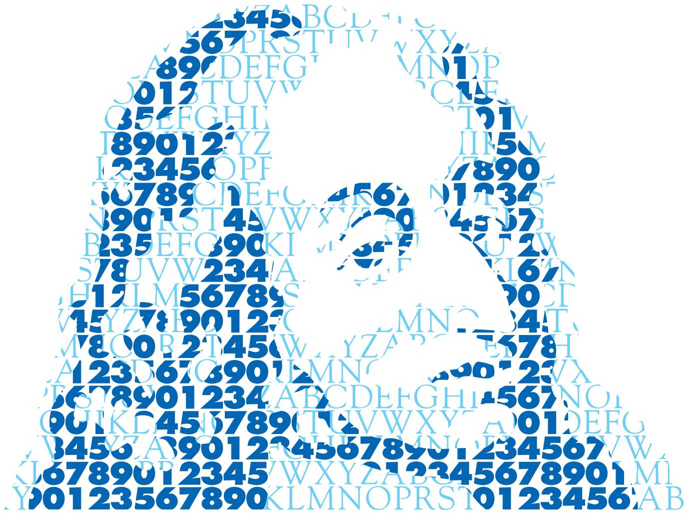
ANNALES MATHÉMATIQUES



BLAISE PASCAL

Abdelmalek Azizi et Mohammed Taous

Condition nécessaire et suffisante pour que certain groupe de Galois soit métacyclique

Volume 16, n° 1 (2009), p. 83-92.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_83_0>

Publication éditée par le laboratoire de mathématiques
de l'université Blaise-Pascal, UMR 6620 du CNRS
Clermont-Ferrand — France

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Annales mathématiques Blaise Pascal **16**, 83-92 (2009)

Condition nécessaire et suffisante pour que certain groupe de Galois soit métacyclique

Abdelmalek Azizi
Mohammed Taous

Résumé

Soient d est un entier sans facteurs carrés, $\mathbf{K} = \mathbf{Q}(\sqrt{d}, i)$, $i = \sqrt{-1}$, $\mathbf{K}_2^{(1)}$ le 2-corps de classes de Hilbert de $\mathbf{K}$, $\mathbf{K}_2^{(2)}$ le 2-corps de classes de Hilbert de $\mathbf{K}_2^{(1)}$ et $G = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$ le groupe de Galois de $\mathbf{K}_2^{(2)}/\mathbf{K}$. Notre but est de montrer qu'il existe une forme de d tel que le 2-groupe G est non métacyclique et de donner une condition nécessaire et suffisante pour que le groupe G soit métacyclique dans le cas où $d = 2p$ avec p un nombre premier tel que $p \equiv 1 \pmod 4$.

Necessary condition and sufficient for certain Galois group to be metacyclic

Abstract

Let d be positive square-free integers, $\mathbf{K} = \mathbf{Q}(\sqrt{d}, i)$ and $i = \sqrt{-1}$. Let $\mathbf{K}_1^{(2)}$ be the Hilbert 2-class field of $\mathbf{K}$, $\mathbf{K}_2^{(2)}$ be the Hilbert 2-class field of $\mathbf{K}_1^{(2)}$ and $G = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$ be the Galois group of $\mathbf{K}_2^{(2)}/\mathbf{K}$. Our goal is to show that there is some form of d such G is a nonmetacyclic 2-group and give the necessary condition and sufficient for the group G to be metacyclic in case $d = 2p$ with p a prime number such that $p \equiv 1 \pmod 4$.

1. Introduction

Soient G un 2-groupe, G' le groupe des commutateurs de G, $\mathbf{K}$ un corps de nombres, $\mathbf{K}^*$ le corps de genres de $\mathbf{K}$, $\mathbf{K}_2^{(1)}$ le 2-corps de classes de Hilbert de $\mathbf{K}$ et $\mathbf{K}_2^{(2)}$ le 2-corps de classes de Hilbert de $\mathbf{K}_2^{(1)}$. On dit que le 2-groupe G est *métacyclique*, s'il existe un sous-groupe cyclique

Mots-clés : groupe des unités, système fondamentale d'unités, capitulation, corps de classes de Hilbert, 2-groupe métacyclique.
Classification math. : 11R27, 11R29, 11R37.

normal H, tel que le groupe quotient G/H est cyclique. On sait que si $G/G^{'}$ est de type (2, 2), alors d'après [12] et [15], le groupe G est métacyclique (exactement abélien de type (2, 2), quaternionique, diédral ou semi-diédral). Mais, si $G/G^{'}$ est de type $(2, 2^n)$ avec $n \geq 2$, alors d'après [8], le groupe G peut être métacyclique ou non métacyclique ; le problème qu'on veut aborder dans cet article est le suivant : Pour $\mathbf{K} = \mathbf{Q}(\sqrt{d}, i)$ où d est un entier sans facteurs carrés et $\mathbf{K}^*$ est une extension quadratique de $\mathbf{K}$, existe-t-il une forme de d tel que le 2-groupe $G = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$ est non métacyclique et quelles sont les conditions nécessaires et suffisantes pour que le groupe G soit métacyclique dans le cas où $d = 2p$ avec p un nombre premier tel que $p \equiv 1 \pmod 4$?

2. Le rang du 2-groupe de classes de K où $[\mathbf{K}^* : \mathbf{K}] = 2$

Soit p un diviseur premier du discriminant $D_{\mathbf{K}}$ de $\mathbf{K}$, on désigne par $e(p)$ l'indice de ramification de p dans $\mathbf{K}/\mathbf{Q}$. On sait, d'après [13] que

$$\prod_{p/D_{\mathbf{K}}} e(p) = [\mathbf{K}^* : \mathbf{Q}] = [\mathbf{K}^* : \mathbf{K}] \cdot [\mathbf{K} : \mathbf{Q}] = 4 \cdot [\mathbf{K}^* : \mathbf{K}].$$

Dans le cas où $\mathbf{K}^*$ est une extension quadratique de $\mathbf{K}$, on a $\prod_{p/D_{\mathbf{K}}} e(p) = 2^3 = 8$, alors si 2 est totalement ramifié dans $\mathbf{Q}(\sqrt{d})$, 2 figure dans la décomposition en facteurs premiers de d, par suite, d est le produit d'un nombre premier et 2. Si 2 n'est pas totalement ramifié, 2 ne divise pas d, dans ce cas d est le produit de deux nombres premiers impairs. Alors les formes possibles pour d sont :

(i) $d = p_1 p_2$ où $p_1 \equiv p_2 \equiv 1 \pmod 4$;

(ii) $d = 2p$ où $p \equiv 1 \pmod 4$;

(iii) $d = pq$ où $p \equiv -q \equiv 1 \pmod 4$;

(iv) $d = 2q$ où $q \equiv -1 \pmod 4$;

(v) $d = q_1 q_2$ où $q_1 \equiv q_2 \equiv -1 \pmod 4$.

Dans la suite de cette section, on va étudier le rang du 2-groupe de classes de $\mathbf{K} = \mathbf{Q}(\sqrt{d}, i)$ avec d prenant les formes précédentes. Pour cela nous allons rappeler le résultat suivant :

Lemme 2.1 ([14])**.** *Le rang du 2-groupe de classes de* $\mathbf{K}$ *est :*

$$\begin{cases} s+s_0 & \text{si } d \text{ est pair et } p\equiv 1 \pmod 8 \text{ pour tout } p\in S_0.\\ s+s_0-1 & \text{si } d \text{ est pair et il existe } p\in S_0 \text{ tel que } p\equiv 5 \pmod 8\\ & \text{ou } d \text{ est impair et } p\equiv 1 \pmod 8 \text{ pour tout } p\in S_0.\\ s+s_0-2 & \text{si } d \text{ est impair et il existe } p\in S_0 \text{ tel que } p\equiv 5 \pmod 8.\end{cases}$$

(1) $s=|S|$ *et* S *est l'ensemble des premiers impairs ramifiés dans* $\mathbf{Q}(\sqrt{d})$ *;*

(2) $s_0=|S_0|$ *où* S_0 *est le sous-ensemble de* S *contenant tous les premiers congrues à* 1 *modulo* 4.

Théorème 2.2. *Soient* $\mathbf{K}=\mathbf{Q}(\sqrt{d},\,i)$ *un corps biquadratique avec* d *est un entier sans facteurs carrés,* $\mathbf{K}^*$ *le corps de genres de* $\mathbf{K}$ *et* r *le rang du* 2*-groupe de classes de* $\mathbf{K}$*. Si* $\mathbf{K}^*$ *est une extension quadratique de* $\mathbf{K}$*, alors*

(1) $r=1$*, si* d *prend les formes suivantes :*

- (1.i) $d=2p$ *où* $p\equiv 5 \pmod 8$ *;*
- (1.ii) $d=pq$ *où* $p\equiv 5 \pmod 8$ *et* $-q\equiv 1 \pmod 4$ *;*
- (1.iii) $d=2q$ *où* $q\equiv -1 \pmod 4$ *;*
- (1.iv) $d=q_1q_2$ *où* $q_1\equiv q_2\equiv -1 \pmod 4$ *;*

(2) $r=2$*, si* d *prend les formes suivantes :*

- (2.i) $d=p_1p_2$ *où* $p_1\equiv 5 \pmod 8$ *ou* $p_2\equiv 5 \pmod 8$ *;*
- (2.ii) $d=2p$ *où* $p\equiv 1 \pmod 8$ *;*
- (2.iii) $d=pq$ *où* $p\equiv 1 \pmod 8$ *et* $-q\equiv 1 \pmod 4$ *;*

(3) $r=3$*, si* d *prend la forme suivante :*

- (3.i) $d=p_1p_2$ *où* $p_1\equiv p_2\equiv 1 \pmod 8$.

Démonstration. Il suffit de calculer s et s_0 et appliquer le lemme précédent. □

3. Structure de G dans le cas où $d=2p$

Soient $\mathbf{K}=\mathbf{Q}(\sqrt{d},\,i)$ un corps biquadratique avec d est un entier sans facteurs carrés, $\mathbf{K}^*$ le corps de genres de $\mathbf{K}$ et $G=\mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$ le groupe de Galois du deuxième 2-corps de classes de Hilbert par rapport à $\mathbf{K}$. Il est très important de savoir que G est métacyclique ou non, car dans le cas métacyclique, G est connu explicitement, ainsi ses sous-groupes, ce qui permet de calculer le nombre des 2-classes d'idéaux de $\mathbf{K}$ qui capitulent dans les sous-extensions de $\mathbf{K}_2^{(1)}/\mathbf{K}$. A. Azizi a montré dans [1] et [2] que G peut être métacyclique si d prend les formes (2.i) et (2.iii) (notation du Théorème 2.2) avec des conditions supplémentaires, qui sont équivalentes de dire que G/G' est de type (2, 2). Dans ce cas d'après un résultat de la théorie des groupes de Taussky ([15]), G est métacyclique (exactement abélien de type (2, 2), quaternionique, diédral ou semi-diédral). Mais si d prend la forme (2.ii), le 2-groupe de classes de $\mathbf{K}$ (et G/G') ne peut pas être de type (2, 2), alors la question naturelle qui se pose est : quelles sont les conditions nécessaires et suffisantes pour que G soit métacyclique ? Dans cette section, on va répondre à cette question.

Dans ce qui va suivre, on adoptera les notations et les conventions suivantes : p un nombre premier, si $p \equiv 1 \pmod 8$, rappelons que le symbole $(\frac{2}{p})_4$ (biquadratique rationnel) est égal à 1 ou -1, suivant que $2^{\frac{p-1}{4}} \equiv \pm 1 \pmod p$. Le symbole $(\frac{p}{2})_4$ est égal à $(-1)^{\frac{p-1}{8}}$. Un 2-groupe est un groupe fini dont l'ordre est une puissance de 2. Pour tout 2-groupe H, le rang $d(H)$ de H est le nombre minimal de générateurs de H. Pour tout corps de nombres L, $h(L)$ désigne le 2-nombre de classes de L.

Lemme 3.1. *Soient $\mathcal{G}$ un groupe métacyclique et H un sous-groupe de $\mathcal{G}$. Alors H est aussi un groupe métacyclique. En particulier $1 \leq d(H) \leq 2$*

Démonstration. Comme $\mathcal{G}$ est un groupe métacyclique, alors il existe un sous-groupe cyclique normal N de $\mathcal{G}$ tel que le groupe quotient $\mathcal{G}/N$ est cyclique. Soit H un sous-groupe de G, d'après le 2-ème théorème d'isomorphisme on a $HN/N \simeq H/H{\cap}N$. Il est claire que HN/N est un sous-groupe de $\mathcal{G}/N$, ce qui prouve que $H/H \cap N$ est un groupe cyclique. Autrement dit, H est un groupe métacyclique, en particulier $1 \leq d(H) \leq 2$. □

Corollaire 3.2. *Soient $\mathbf{K} = \mathbf{Q}(\sqrt{d}, i)$ un corps biquadratique avec d est un entier sans facteurs carrés, $\mathbf{K}^*$ le corps de genres de $\mathbf{K}$, $\mathbf{K}_2^{(1)}$ le 2-corps de classes de Hilbert de $\mathbf{K}$, $\mathbf{K}_2^{(2)}$ le 2-corps de classes de Hilbert de $\mathbf{K}_2^{(1)}$ et $G = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$. Si $\mathbf{K}^*$ est une extension quadratique de $\mathbf{K}$, alors*

(1) *Si d prend les formes* (1.i), (1.ii), (1.iii) *et* (1.iv), *alors G est cyclique ;*

(2) *Si d prend la forme* (3.i), *alors G est non métacyclique.*

Démonstration. Notons $\Phi(G)$ le sous-groupe de Frattini de G, intersection de ses sous-groupes maximaux et $r = d(G)$. Il est bien connu que $\Phi(G)$ est le plus petit sous-groupe de G tel que $G/\Phi(G) \simeq (\mathbf{Z}/2\mathbf{Z})^r$. Puisque $G' \subseteq \Phi(G) = G^2$, le groupe quotient $G/\Phi(G)$ est vu comme un sous-groupe de G/G', alors $d(G) = d(G/G')$. Si d prend les formes (1.i), (1.ii), (1.iii) ou (1.iv), alors le 2-groupe de classes de $\mathbf{K}$ est cyclique, ainsi $d(G/G') = d(G) = 1$, enfin G est cyclique. Si d prend la forme (3.i), alors le 2-groupe de classes est égal à 3, le lemme précédent donne que G est non métacyclique, car $d(G) = d(G/G') = 3$. $\square$

Théorème 3.3. *Soient $\mathbf{K} = \mathbf{Q}(\sqrt{2p},\, i)$ avec p un nombre premier tel que $p \equiv 1 \pmod 8$, $\mathbf{K}^* = \mathbf{Q}(\sqrt{2},\, \sqrt{p},\, i)$ le corps de genres de $\mathbf{K}$ et $C_{\mathbf{K}^*,2}$ le 2-groupe de classes de $\mathbf{K}^*$. Alors le rang de $C_{\mathbf{K}^*,2} = 2$ ou 3. De plus le rang de $C_{\mathbf{K}^*,2} = 3$ si et seulement si $(\frac{2}{p})_4 = (\frac{p}{2})_4 = 1$.*

Démonstration. Notons F le corps $\mathbf{Q}(\sqrt{2},\, i) = \mathbf{Q}(\zeta_8)$, r le rang de $C_{\mathbf{K}^*,2}$, $Am(\mathbf{K}^*/F)$ le groupe de classes ambiguës dans $\mathbf{K}^*/F$, E_F est le groupe des unités de F et $\mathcal{N}_{\mathbf{K}^*/F}$ l'application norme de $\mathbf{K}^*/F$. On sait que le groupe des unités de F est engendré par $\varepsilon_0 = 1+\sqrt{2}$, l'unité fondamentale de $\mathbf{Q}(\sqrt{2})$ et ζ_8 la racine 8-ème de l'unité. De plus le nombre de classes de F est égal à 1. Alors la formule de genres donne le nombre des classes ambiguës dans $\mathbf{K}^*/F$:

$$|Am(\mathbf{K}^*/F)| = \frac{2^3}{[E_F : E_F \cap \mathcal{N}_{\mathbf{K}^*/F}(\mathbf{K}^*)]} = 2^r,$$

car il existe quatre idéaux premiers de F qui se ramifient dans $\mathbf{K}^*$, ces idéaux sont au-dessus de p. Comme F est imaginaire, $\mathbf{K}^* = F(\sqrt{p})$ et grâce à la formule de produit pour le symbole de Hilbert $(\ ,\ )_\beta$; le théorème de Hasse entraîne qu'une unité ε de F est une norme si et seulement si $(p,\, \varepsilon)_\beta = 1$ pour tout idéal premier de F qui n'est pas au-dessus de 2. En utilisant les propriétés du symbole de Hilbert on trouve que

$$(p,\, \varepsilon)_\beta = \begin{cases} 1 & \text{si} \quad \beta \text{ n'est pas au-dessus de } p, \\ (\frac{p}{2})_4 & \text{si} \quad \beta \text{ au-dessus de } p \text{ et } \varepsilon = \zeta_8, \\ (\frac{p}{2})_4(\frac{2}{p})_4 & \text{si} \quad \beta \text{ au-dessus de } p \text{ et } \varepsilon = \varepsilon_0, \\ (\frac{2}{p})_4 & \text{si} \quad \beta \text{ au-dessus de } p \text{ et } \varepsilon = \varepsilon_0\zeta_8. \end{cases}$$

En particulier

$$E_F \cap \mathcal{N}_{\mathbf{K}^*/F}(\mathbf{K}^*) = \begin{cases} \langle \zeta_8,\ \varepsilon_0 \rangle & \text{si} \quad (\frac{2}{p})_4 = (\frac{p}{2})_4 = 1, \\ \langle i,\ \varepsilon_0 \rangle & \text{si} \quad (\frac{2}{p})_4 = (\frac{p}{2})_4 = -1, \\ \langle \zeta_8,\ \varepsilon_0^2 \rangle & \text{si} \quad (\frac{2}{p})_4 = -(\frac{p}{2})_4 = -1, \\ \langle i,\ \varepsilon_0\zeta_8 \rangle & \text{si} \quad (\frac{2}{p})_4 = -(\frac{p}{2})_4 = 1. \end{cases}$$

Enfin

$$|Am(\mathbf{K}^*/F)| = \begin{cases} 2^3 & \text{si} \qquad (\frac{2}{p})_4 = (\frac{p}{2})_4 = 1, \\ 2^2 & \text{sinon.} \end{cases}$$

D'où le résultat. □

Théorème 3.4 ([3]). *Soient $\mathbf{K} = \mathbf{Q}(\sqrt{2p},\ i)$ avec p un nombre premier tel que $p \equiv 1 \pmod 8$, $\mathbf{K}_2^{(1)}$ le 2-corps de classes de Hilbert de $\mathbf{K}$, $\mathbf{K}_2^{(2)}$ le 2-corps de classes de Hilbert de $\mathbf{K}_2^{(1)}$ et $h(-p)$ le 2-nombre de classes de $\mathbf{Q}(\sqrt{-p})$. Alors on a*

$$\mathbf{K}_2^{(1)} \neq \mathbf{K}_2^{(2)} \Leftrightarrow h(-p) \geq 8 \Leftrightarrow (\tfrac{2}{p})_4 = (\tfrac{p}{2})_4$$

Lemme 3.5. *Soient $\mathbf{K} = \mathbf{Q}(\sqrt{2p},\ i)$ un corps biquadratique avec p est un nombre premier tel que $p \equiv 1 \pmod 8$, $(\frac{2}{p})_4 = (\frac{p}{2})_4 = -1$, $\mathbf{K}_2^{(1)}$ le 2-corps de classes de Hilbert de $\mathbf{K}$, $\mathbf{K}_2^{(2)}$ le 2-corps de classes de Hilbert de $\mathbf{K}_2^{(1)}$, $G = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$, H et K les deux sous-groupes maximaux de G tels que H/G' et K/G' sont cycliques d'ordre 4. Alors $[G' : H'] = [G' : K']$.*

Démonstration. Comme $p \equiv 1 \pmod 8$, alors il existe deux entiers x et y tels que $p = x^2 + 16y^2$. On pose $\pi_1 = x + 4yi$, $\pi_2 = x - 4yi$, $K_1 = \mathbf{K}(\sqrt{\pi_1})$ et $K_2 = \mathbf{K}(\sqrt{\pi_2})$. Puisque les deux premiers π_1 et π_2 sont ramifiés dans $\mathbf{K}/\mathbf{Q}(i)$, les idéaux engendrés par π_1 et π_2 sont des carrés d'idéaux de $\mathbf{K}$. Observons que x est un nombre impair, donc $x \equiv \pm 1 \equiv i^2 \pmod 4$, alors les deux équations $\pi_i \equiv \xi^2$ sont résolubles, ce qui implique que les deux extensions $\mathbf{K}(\sqrt{\pi_1})$ et $\mathbf{K}(\sqrt{\pi_2})$ sont des extensions non ramifiées de $\mathbf{K}$. Supposons que $\mathbf{K}(\sqrt{\pi}_1) = \mathbf{K}(\sqrt{\pi}_2)$, alors il existe un élément $t \in \mathbf{K}$ tel que $\pi_1 = t^2\pi_2$, ce qui montre que $p = t^2\pi_2^2$, et ce n'est pas le cas, car $\sqrt{p} \notin \mathbf{K}$. Comme l'extension $\mathbf{K}^*/\mathbf{Q}$ est normale et $\mathbf{K}(\pi_i)/\mathbf{Q}$ $(i = 1, 2)$ n'est pas normale, donc $\mathbf{K}(\pi_i) \neq \mathbf{K}^*$. Ce qui prouve que K_1, K_2 et $\mathbf{K}^*$ sont des extensions différentes non ramifiées de $\mathbf{K}$. Or, la condition $(\frac{2}{p})_4 = (\frac{p}{2})_4 = -1$ donne que le 2-groupe de classes de $\mathbf{K}$ est de type $(2, 4)$, alors

K_1, K_2 et $\mathbf{K}^*$ sont exactement les 3 extensions quadratiques non ramifiées de $\mathbf{K}$. Observons que K_1 et K_2 sont deux corps conjugués, alors le groupe de Galois de $\mathbf{K}_2^{(1)}/K_1$ et de $\mathbf{K}_2^{(1)}/K_2$ ont la même structure qui doit être qu'un groupe cyclique d'ordre 4, alors on pose $H = \mathrm{Gal}(\mathbf{K}_2^{(2)}/K_1)$ et $K = \mathrm{Gal}(\mathbf{K}_2^{(2)}/K_2)$, ce qui entraîne que les groupes $H/G^{'}$ et $K/G^{'}$ sont cycliques d'ordre 4 et $[H : H'] = h(K_1) = [H : G'][G' : H'] = h(K_2) = [K : G'][G' : K']$. Enfin $[G' : H'] = [G' : K']$. $\square$

Soit $\mathcal{G}$ un 2-groupe. On désigne par $\gamma_i(\mathcal{G})$ *le i-ème terme de série centrale descendante* de $\mathcal{G}$ définie par $\gamma_1(\mathcal{G}) = \mathcal{G}$ et $\gamma_{i+1}(\mathcal{G}) = [\gamma_i(\mathcal{G}), \mathcal{G}]$. Si $\gamma_1(\mathcal{G})/\gamma_2(\mathcal{G})$ est de type (2, 4), la situation est schématisée par le diagramme suivant :

$$\begin{tikzcd}
 & \gamma_3(\mathcal{G}) \arrow[d] & \\
 & \mathcal{G}' \arrow[dl] \arrow[d] \arrow[dr] & \\
N_1 \arrow[dr] & N_3 \arrow[dl] \arrow[d] \arrow[dr] & N_2 \arrow[dl] \\
H \arrow[dr] & M \arrow[d] & N \arrow[dl] \\
 & \mathcal{G} &
\end{tikzcd}$$

N. Blackburn a montré dans [10] que $\gamma_2(\mathcal{G})/\gamma_3(\mathcal{G})$ est un groupe cyclique d'ordre ≤ 2 et que l'exposant du groupe quotient $\gamma_i(\mathcal{G})/\gamma_{i+1}(\mathcal{G})$ est ≤ 2 $(i \geq 2)$. Soit c le plus petit entier tel que $\gamma_{c+1}(\mathcal{G}) = 1$, on appel *coclasse* de $\mathcal{G}$ l'entier $n - c$ avec 2^n est l'ordre de $\mathcal{G}$, il est à noter que la coclasse de $\mathcal{G}$ est égal à 2 si et seulement si le groupe quotient $\gamma_i(\mathcal{G})/\gamma_{i+1}(\mathcal{G})$ est d'ordre 2 $(2 \leq i \leq c)$. Dans [11] et [4], on trouvera la classification complète de tous les groupes dont la coclasse est 2.

Lemme 3.6. *Soit $\mathcal{G}$ un 2-groupe tel que $\mathcal{G}/\mathcal{G}' \simeq (2, 4)$. Soient H et M deux sous-groupes maximaux de $\mathcal{G}$ tels que $H/\mathcal{G}'$ est un groupe cyclique d'ordre 4 et $M/\mathcal{G}' \simeq (2, 2)$. Alors*

(i) *Si* $\mathcal{G}' \simeq (2, 2)$*, alors* $[\mathcal{G}' : H'] = 2$.

(ii) *Si la coclasse de* $\mathcal{G}$ *est égal à* 2 *et* $d(\mathcal{G}') = 2$*, alors* $d(M) \geq 3$. *En particulier* $\mathcal{G}$ *est non métacyclique.*

Démonstration. (i) Puisque $\mathcal{G}/\mathcal{G}' \simeq (2, 4)$, alors il existe deux éléments a et b tels que $a^2 \equiv b^4 \equiv 1 \mod \mathcal{G}'$ et $H = \langle b, \mathcal{G}' \rangle$. On pose $c_2 = [a, b]$ et $c_{j+1} = [b, c_j]$ ($[x, y]$ le commutateur de x et y). Alors $\mathcal{G}' = \langle c_2, c_3, ... \rangle$, $H' = \langle c_3, c_4, ... \rangle$ et le groupe quotient $\mathcal{G}'/H'$ est engendré par la classe de c_2 modulo H', ainsi la condition $\mathcal{G}' \simeq (2, 2)$ entraîne que $[\mathcal{G}' : H'] = 2$.
(ii) Dans [4], on trouve que $\mathcal{G} = \langle x_1, x_2, y \rangle$ et $\mathcal{G}' = \langle x_1^2, x_2 \rangle$ avec $y^4 \in \mathcal{G}'$. Comme $\mathcal{G}/\mathcal{G}' \simeq (2, 4)$, alors $M = \langle x_1, y^2, \mathcal{G}' >= \langle x_1, x_2, y^2 \rangle$ et $\mathcal{G}$ admet 3 sous-groupes normaux N_1, N_2 et N_3 (voir le diagramme précédent) tels que $N_1 = \langle x_1, \mathcal{G}' \rangle = \langle x_1, x_2 \rangle$, $N_2 = \langle y^2, \mathcal{G}' \rangle = \langle x_1^2, x_2, y^2 \rangle$ et $N_3 = \langle y^2 x_1, \mathcal{G}' \rangle = \langle y^2 x_1, x_1^2, x_2 \rangle$. Supposons que $d(M) = 2$, alors M admet exactement 3 sous-groupes d'indice 2, qui sont les N_i $(1 \leq i \leq 3)$. Le groupe $N_4 = \langle x_1, x_2^2, y^2 \rangle$ est sous-groupe d'indice 2 de M tel que $N_4 \neq N_i$ $(1 \leq i \leq 3)$, ce qui montre que $d(M) \geq 3$. □

Théorème 3.7. *Soient* $\mathbf{K} = \mathbf{Q}(\sqrt{2p}, i)$ *un corps biquadratique avec* p *est un nombre premier tel que* $p \equiv 1 \pmod 4$*,* $\mathbf{K}^*$ *le corps de genres de* $\mathbf{K}$*,* $\mathbf{K}_2^{(1)}$ *le* 2*-corps de classes de Hilbert de* $\mathbf{K}$*,* $\mathbf{K}_2^{(2)}$ *le* 2*-corps de classes de Hilbert de* $\mathbf{K}_2^{(1)}$ *et* $G = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$. *Si* $\mathbf{K}^*$ *est une extension quadratique de* $\mathbf{K}$. *Alors* G *est métacyclique non abélien si et seulement si* $p \equiv 1 \pmod 8$ *et* $(\frac{2}{p})_4 = (\frac{p}{2})_4 = -1$.

Démonstration. Supposons que $(\frac{2}{p})_4 = (\frac{p}{2})_4 = -1$, alors G est un groupe non abélien et le 2-groupe de classes de $\mathbf{K}$ est de type $(2, 4)$ et $h(\mathbf{K}^*) = 2h(-p)$ où $h(-p)$ est le 2-nombre de classes de $\mathbf{Q}(\sqrt{-p})$ ([3]). Soit $\gamma_i(G)$ le i-ème terme de série centrale descendante de $G = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K})$. Dans ce cas $\gamma_1(G)/\gamma_2(G)$ est de type $(2, 4)$. Puisque $\mathbf{K}^*$ est la plus grande extension abélienne non ramifiée de $\mathbf{K}$ telle que l'extension $\mathbf{K}/\mathbf{Q}$ est abélienne et si on pose $\mathcal{P} = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{Q})$, alors $M = \mathcal{P}' = \mathrm{Gal}(\mathbf{K}_2^{(2)}/\mathbf{K}^*)$, ainsi $\mathcal{P}'/\mathcal{P}''$ est isomorphe à $C_{\mathbf{K}^*,2}$ le 2-groupe de classes de $\mathbf{K}^*$, d'après le théorème précédent le rang de $\mathcal{P}'/\mathcal{P}''$ est égal à 2. N. Blackburn a montré dans [9] que dans cette situation $\mathcal{P}'$ est un groupe métacyclique. Comme G' est un sous-groupe normal de $\mathcal{P}'$, alors le lemme 3.1 entraîne que $1 \leq d(G') \leq 2$.

Commençons par étudier le cas où $[G' : H'] > 2$. Soit N_1 l'un des deux sous-groupes normaux cycliques d'indice 4 sur G. Soit L_1 le sous-corps de

$\mathbf{K}_2^{(2)}/\mathbf{K}$ laissé fixe par N_1. Suivant [7] on a :

$$[N_1 : N_1^{'}] = h(L_1) = \begin{cases} 4 & \text{si} \quad d(G^{'}) = 1; \\ 8 & \text{si} \quad d(G^{'}) = 2. \end{cases}$$

Comme L_1 est une extension non ramifiée de $\mathbf{K}^*$, alors $h(L_1) \geq h(\mathbf{K}^*)/2 = h(-p) \geq 8$, par suite $h(L_1) = h(\mathbf{K}^*)/2 = 8$ et $d(G^{'}) = 2$, la proposition 7 de [6] donne que $\mathcal{P}^{'}$ est abélien, alors il est de type (2, 8) ou (4, 4), puisque $G^{'}$ est un sous-groupe de $\mathcal{P}^{'}$ tel que $\mathcal{P}^{'}/G^{'}$ est de type (2, 2) et $d(G') = 2$, alors $G^{'}$ est de type (2, 2). Le (i) du lemme précédent montre que $[G^{'} : H^{'}] = 2$, ce qui affirme que le cas où $[G^{'} : H^{'}] > 2$ est impossible.

Nous avons montré que si $(\frac{2}{p})_4 = (\frac{p}{2})_4 = -1$, alors $[G^{'} : H^{'}] = 2$ et $1 \leq d(G^{'}) \leq 2$. E. Benjamin, F. Lemmermeyer et C. Snyder ont montré dans [5] que $\gamma_i(G)/\gamma_{i+1}(G)$ est d'ordre ≤ 2 et que si G est non métacyclique, alors $d(G^{'}) = 1$ si et seulement si $[G^{'} : H^{'}] = 2$ et $[G^{'} : K^{'}] > 2$. Pour notre cas le lemme 3.5 donne que $[G' : H'] = [G' : K']$. Cela signifie que la coclasse de G est égal à 2 avec G soit un groupe métacyclique, soit un groupe (non métacyclique) dont la coclasse est 2 et $d(G^{'}) = 2$. (ii) du lemme précédent affirme que ce deuxième cas est impossible, alors G est métacyclique non abélien.

Réciproquement, supposons que G est métacyclique non abélien, alors le théorème précédent nous donnera que $(\frac{2}{p})_4 = (\frac{p}{2})_4 = \pm 1$. Si $(\frac{2}{p})_4 = (\frac{p}{2})_4 = 1$, alors le 2-groupe de classes de $\mathbf{K}^*$ est égal à 3, ainsi $d(M) = 3$ et ce n'est pas le cas car M est sous-groupe d'un groupe métacyclique. $\square$

Références

[1] A. Azizi – « Capitulation of the 2-ideal classes of $\mathbb{Q}(\sqrt{p_1 p_2}, i)$ where p_1 and p_2 are primes such that $p_1 \equiv 1 \pmod 8$, $p_2 \equiv 5 \pmod 8$ and $(\frac{p_1}{p_2}) = -1$ », *Lecture notes in pure and applied mathematics* **208** (1999), p. 13–19.

[2] ———, « Sur une question de capitulation », *Proc. Amer. Math. Soc* **130** (2002), p. 2197–2202.

[3] A. Azizi et M. Taous – « Capitulation of 2-ideal classes of $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ in the genus field of $\mathbf{k}$ where p is prime such that $p \equiv 1 \pmod 8$ », *IJPAM* **35** (2007), no. 2, p. 481–487.

[4] C. BAGINSKI et A. KONOVALOV – « On 2-groups of almost maximal class », *Publ. Math* **65** (2004), no. 1-2, p. 97–131.

[5] E. BENJAMIN, F. LEMMERMEYER et C. SNYDER – « Imaginary Quadratic fields k with Cyclic $cl_2(k^1)$ », *J. Number Theory* **67** (1997), p. 229–245.

[6] ______, « Real quadratic fields with abelian 2-class field tower », *J. Number Theory* **73** (1998), p. 182–194.

[7] ______, « Imaginary quadratic fields with $cl_2(k) = (2, 2^m)$ and rank $cl_2(k^1) = 2$ », *Pac. J. Math* **198** (2001), p. 15–31.

[8] E. BENJAMIN et C. SNYDER – « Number Fields with 2-class Number Isomorphic to (2, 2^m) », preprint, 1994.

[9] N. BLACKBURN – « On Prime Power Groups in which the Derived Group has Two Generators », *Proc. Cambridge Phil. Soc* **53** (1957), p. 19–27.

[10] N. BLACKBURN – « On a special class of p-groups », *Acta Math* **100** (1958), p. 45–92.

[11] R. JAMES – « 2-groups of Almost Maximal Class », *J. Austral. Math. Soc. Ser. A* **19** (1975), p. 343–357.

[12] H. KISILEVSKY – « Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94 », *J. Number Theory* **8** (1976), no. 3, p. 271–279.

[13] T. KUBOTA – « Über die Beziehung der Klassenzahlen der Unterkörper des bizyklischen Zahlkörpers », *Nagoya Math. J* **6** (1953), p. 119–127.

[14] T. MCCALL, C. PARRY et R. RANALLI – « On imaginary bicyclic biquadratic fields with cyclic 2-class group », *J. Number Theory* **53** (1995), p. 88–99.

[15] O. TAUSSKY – « A remark on the class field tower », *J. Number Theory* **12** (1937), p. 82–85.

ABDELMALEK AZIZI
Département de Mathématiques
Faculté des Sciences
Université Mohammed 1
Oujda
Maroc
abdelmalekazizi@yahoo.fr

MOHAMMED TAOUS
Département de Mathématiques
Faculté des Sciences
Université Mohammed 1
Oujda
Maroc
taousm@hotmail.com