ACTA ARITHMETICA
131.2 (2008)

# Capitulation des 2-classes d'idéaux de $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$

par

Abdelmalek Azizi et Mohammed Taous (Oujda)

**1. Introduction.** Soient $k$ un corps de nombres de degré fini sur $\mathbb{Q}$, $p$ un nombre premier, $C_k$ le groupe de classes de $k$ et $C_{k,p}$ le $p$-groupe de classes de $k$. On note $k_p^{(1)}$ le $p$-corps de classes de Hilbert de $k$ au sens large. Soit $k_p^{(n)}$ (pour $n$ un entier naturel) la suite de $p$-corps de classes de Hilbert définie par $k_p^{(0)} = k$ et $k_p^{(n+1)} = (k_p^{(n)})_p^{(1)}$. Alors on a

$$k_p^{(0)} \subseteq k_p^{(1)} \subseteq \cdots \subseteq k_p^{(n)} \subseteq \cdots .$$

Cette suite est appelée la *tour des p-corps de classes de Hilbert* de $k$ ; on sait qu'elle est finie si et seulement s'il existe une $p$-extension finie $E$ de $k$ telle que le *p-nombre de classes* (la $p$-partie du nombre de classes) de $E$ est égal à 1. Mais cette caractérisation ne permet pas d'obtenir une procédure pour dire que cette suite s'arrête ou non ; cependant, il est connu par un résultat de Taussky ([Ta-37]) que si $C_{k_p^{(1)},p}$ est cyclique alors $C_{k_p^{(2)},p}$ est trivial, ce qui implique que $k_p^{(2)} = k_p^{(3)}$. Or, si $p = 2$ et $C_{k,p}$ est de type $(2, 4)$, alors d'après un résultat de Blackburn ([Bl-58]), le rang de $C_{k_p^{(1)},p}$ est $\leq 3$.

L'objet de ce travail est l'étude du problème de la tour pour le corps $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$, dont le 2-groupe de classes est de type $(2, 4)$. Nous déterminons aussi les 2-classes de $C_{\mathbf{k}}$ qui capitulent dans les sous-extensions propres de $\mathbf{k}_2^{(1)}/\mathbf{k}$, ce qui nous permet de trouver une représentation de $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$, le groupe de Galois de $\mathbf{k}_2^{(2)}/\mathbf{k}$, lorsque $\mathbf{k}_2^{(1)} \neq \mathbf{k}_2^{(2)}$. Notre théorème principal est le suivant :

Théorème principal. *Soit* $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ *avec* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 8$ *et* $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$. *Alors il existe* $e, f \in \mathbb{N}$ *tels que*

2000 *Mathematics Subject Classification*: 11R27, 11R29, 11R37.

*Key words and phrases*: unit group, fundamental system of units, capitulation, Hilbert class field, metacyclic 2-group.

Recherche de A. Azizi soutenue par l'Académie Hassan II des Sciences et Techniques, Maroc.

 

$p = e^2 + 16f^2$. *Soient* $\pi_1 = e + 4fi$, $\pi_2 = e - 4fi$, $2^n$ *le* 2*-nombre de classes de* $\mathbb{Q}(\sqrt{-p})$, *et* $\mathcal{H}_1$, $\mathcal{H}_2$ *et* $\mathcal{H}$ *les idéaux premiers au-dessus de* $\pi_1$, $\pi_2$ *et* $1+i$ *dans* $\mathbf{k}$. *Alors*

(1) *Les idéaux* $\mathcal{H}$, $\mathcal{H}_1$ *et* $\mathcal{H}_2$ *représentent la même classe dans* $\mathbf{k}$.
(2) $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k}) = \langle a, b\rangle$ *est un groupe métacyclique non modulaire où* $a^{2^n} = b^4 = 1$ *et* $b^{-1}ab = a^{-1+k2^{n-1}}$ *avec* $k$ *un nombre impair.*
(3) *Seules la classe de* $\mathcal{H}$ *et son carré capitulent dans chacune des trois extensions quadratiques non ramifiées de* $\mathbf{k}$.
(4) *Les huit classes de* $C_{\mathbf{k},2}$ *capitulent dans les trois extensions abéliennes non ramifiées de degré* 4 *de* $\mathbf{k}$.

Dans ce qui suit, on adoptera les notations et les conventions suivantes : $p$ est un nombre premier ; si $p \equiv 1 \bmod 8$, le symbole $\left(\frac{2}{p}\right)_4$ (biquadratique rationnel) est égal à 1 ou $-1$, suivant que $2^{(p-1)/4} \equiv \pm 1 \bmod p$. Le symbole $\left(\frac{p}{2}\right)_4$ est égal à $(-1)^{(p-1)/8}$. On désigne par $h(F)$ le 2-nombre de classes d'un corps de nombres $F$. Rappelons aussi que $D_3$ (resp. $Q_3$) est le groupe diédral (resp. des quaternions) d'ordre $2^3$.

**2. Résultats préliminaires.** Ce paragraphe est réservé à certains résultats utiles dans le reste de l'article. Les deux premiers résultats concernent des cas particuliers des extensions non ramifiées.

Théorème 1 ([Hi]). *Soient* $K/k$ *une extension quadratique et* $\mu$ *un nombre de* $k$ *premier à* 2 *tel que* $K = k(\sqrt{\mu})$. *L'extension de* $K/k$ *est non ramifiée aux premiers finis de* $k$ *si et seulement si* $\mu$ *vérifie les propriétés suivantes* :

- *L'idéal principal engendré par* $\mu$ *est le carré d'un idéal (fractionnaire) de* $k$.
- *Il existe un nombre non nul* $\xi \in k$ *vérifiant* $\mu \equiv \xi^2 \bmod 4$ (*il s'agit d'une congruence (multiplicative) dans* $k$, *modulo le sous-groupe des nombres de la forme* $1 + 4r/s$ *avec* $r$ *et* $s$ *entiers de* $k$ *tel que* $s$ *soit premier à* 2).

Proposition 1 ([R-R-33]). *Soit* $K/F$ *une extension quadratique telle que le nombre de classes de* $F$ *est impair. Si* $K$ *admet une extension non ramifiée cyclique* $R$ *d'ordre* 4, *alors* $R/F$ *est normale et* $\mathrm{Gal}(R/F) \simeq D_3$.

On aura besoin aussi de certains résultats sur les symboles quadratiques bien connus, notamment ceux de Hilbert $\left(\frac{a,b}{\mathcal{P}}\right)$ et les symboles des restes quadratiques $\left[\frac{a}{\mathcal{P}}\right]$ (pour plus de détails, voir [Gr-73] et [Za-99]). Explicitement, la valeur du symbole de Hilbert est donné dans un cas particulier par :

PROPOSITION 2 ([Se-70]). *Soient $K$ un corps de nombres de degré $n$ tel que son anneau des entiers est principal, $a = l^{v_l(a)}u$ et $b = l^{v_l(b)}v$ deux éléments de $K$ où $(l)$ est un idéal premier de $K$ au-dessus d'un nombre premier $p$ tel que $p - 1 \geq n$ et $v_l$ est la valuation $l$-adique. Alors*

$$\left(\frac{a,b}{(l)}\right) = \left[\frac{-1}{(l)}\right]^{v_l(a)v_l(b)} \left[\frac{u}{(l)}\right]^{v_l(b)} \left[\frac{v}{(l)}\right]^{v_l(a)}.$$

Le résultat suivant est la formule de Kuroda.

PROPOSITION 3 ([Lm-94]). *Soient $K/k$ une extension normale dont le groupe de Galois est de type $(2,2)$, et $k_j$ $(j = 1,2,3)$ ses trois sous-extensions quadratiques. Alors*

$$h(K) = 2^{d-\kappa-2-v} q(K) h(k_1) h(k_2) h(k_3) / h(k)^2,$$

*où $q(K) = (E_K : E_{k_1}E_{k_2}E_{k_3})$ est l'indice des unités de $K/k$, $d$ le nombre des premiers infinis de $k$ qui sont ramifiés dans $K$, $\kappa$ est le $\mathbb{Z}$-rang du groupe des unités $E_k$ de $k$ et $v = 1$ ou $0$ suivant que $K \subseteq k(\sqrt{E_k})$ ou non.*

Maintenant on va rappeler des résultats concernant la théorie des groupes qui se révélerons très utiles dans la suite de ce travail.

DÉFINITION 1. On dit qu'un groupe fini $G$ est *métacyclique* s'il possède un sous-groupe cyclique normal $H$ tel que le quotient $G/H$ est cyclique.

THÉORÈME 2 ([Hu-67]). *Soit $p$ un nombre premier. Tout $p$-groupe métacyclique d'ordre $p^N$ peut être représenté par*

$$G = \langle a, b : a^{p^n} = 1,\ b^{p^m} = a^i,\ b^{-1}ab = a^q \rangle$$

*avec les conditions suivantes* :

(i) $n + m = N$,
(ii) $q^{p^m} \equiv 1 \bmod p^n$,
(iii) $i(q-1) \equiv 0 \bmod p^n$.

Remarquons que les groupes métacycliques abéliens sont les groupes cycliques ou les groupes abéliens de rang 2, donc on suppose dans toute la suite qu'un groupe métacyclique est non abélien.

REMARQUE 1. *Soit $G$ un groupe métacyclique. Alors le groupe des commutateurs $G'$ est cyclique.*

*Démonstration.* Comme $G$ est métacyclique, il existe un sous-groupe normal $H$ de $G$ tel que $G/H$ est cyclique, donc abélien ; par suite $G' \subset N$, ce qui montre que $G'$ est cyclique. ∎

DÉFINITION 2. Le *groupe modulaire* est un groupe $G$ d'ordre $2^n$ $(n > 3)$ métacyclique tel que $G/G' \simeq (2, 2^{n-2})$. En particulier $G'$ est d'ordre deux.

PROPOSITION 4 ([Be-Sn-94]). *Soient $G$ un 2-groupe métacyclique non modulaire et $G'$ le groupe des commutateurs de $G$. Si le groupe $G/G'$ est de type $(2,2^m)$ avec $m>1$ et $G=\langle a,b\rangle$ avec $a^2\equiv b^{2^m} \bmod G'$, alors $G'=\langle a^2\rangle$ et $G$ est de l'un des types suivants* :

- Type 1 : $a^{2^\alpha}=1$, $b^{2^m}=1$, $b^{-1}ab=a^{-1}$, $\alpha>1$ ;
- Type 2 : $a^{2^\alpha}=1$, $b^{2^m}=a^{2^{\alpha-1}}$, $b^{-1}ab=a^{-1}$, $\alpha>1$ ;
- Type 3 : $a^{2^\alpha}=1$, $b^{2^m}=1$, $b^{-1}ab=a^{-1+k2^s}$, $1<s<\alpha$, $k$ *impair*;
- Type 4 : $a^{2^\alpha}=1$, $b^{2^m}=a^{2^{\alpha-1}}$, $b^{-1}ab=a^{-1+k2^s}$, $1<s<\alpha$, $k$ *impair.*

Soient $k$ un corps de nombres dont le 2-groupe de classes est de type $(2,4)$ et $G=\mathrm{Gal}(k_2^{(2)}/k)$. Alors $G/G'$ est de type $(2,4)$, donc $G=\langle a,b\rangle$ avec $a^2\equiv b^4\equiv 1 \bmod G'$ (théorème de la base de Burnside) et $C_{k,2}=\langle\tau,\sigma\rangle\simeq\langle aG',bG'\rangle$ où $(\tau,k_2^{(2)}/k)=aG'$ et $(\sigma,k_2^{(2)}/k)=bG'$ avec $(\cdot,k_2^{(2)}/k)$ le symbole d'Artin dans $k_2^{(2)}/k$. Par suite, il existe trois sous-groupes de $G$ d'indice 2 : $H_{1,2}$, $H_{2,2}$ et $H_{3,2}$ tels que

$$H_{1,2}=\langle b,G'\rangle,\qquad H_{2,2}=\langle ab,G'\rangle,\qquad H_{3,2}=\langle a,b^2,G'\rangle.$$

Il existe aussi trois sous-groupes de $G$ d'indice 4 : $H_{1,4}$, $H_{2,4}$ et $H_{3,4}$ tels que

$$H_{1,4}=\langle a,G'\rangle,\qquad H_{2,4}=\langle ab^2,G'\rangle,\qquad H_{3,4}=\langle b^2,G'\rangle.$$

Soient $H$ un sous-groupe de $G$ d'indice 2 ou 4, $K$ un sous-corps de $k_2^{(2)}/k$ laissé fixe par $H$ et $j=j_{k\to K}$ l'application de $C_{k,2}$ vers $C_{K,2}$, qui fait correspondre à la classe d'un idéal $I$ de $k$ la classe de l'idéal engendré par $I$ dans $K$. Artin a prouvé :

PROPOSITION 5 ([Mi-89]). *Il existe un homomorphisme de groupes $V_{G\to H}$ de $G/G'$ vers $H/H'$ appelé le transfer de $G$ vers $H$ tel que le diagramme suivant est commutatif* :

$$\begin{array}{ccc} C_{k,2} & \xrightarrow{\ j\ } & C_{K,2} \\ {\scriptstyle(\cdot,k_2^{(2)}/k)}\big\downarrow & & \big\downarrow{\scriptstyle(\cdot,K_2^{(2)}/K)} \\ G/G' & \xrightarrow{V_{G\to H}} & H/H' \end{array}$$

*où les flèches verticales sont des isomorphismes donnés par la loi de réciprocité d'Artin et $(\cdot,k_2^{(2)}/k)$ (resp. $(\cdot,K_2^{(2)}/K)$) est le symbole d'Artin dans $k_2^{(2)}/k$ (resp. $K_2^{(2)}/K$).*

Comme les $H_{r,s}$ sont des sous-groupes normaux de $G=\mathrm{Gal}(k_2^{(2)}/k)$, nous utilisons la proposition suivante ([Mi-89]) pour trouver les classes de $k$ qui capitulent dans les extensions $K_{r,s}$ ($K_{r,s}$ est le sous-corps de $k_2^{(2)}$ laissé fixe par $H_{r,s}$).

PROPOSITION 6. *Soit $H$ un sous-groupe normal d'un groupe $G$. Pour $g \in G$, on pose $f = [\langle g \rangle H : H]$ et soit $\{x_1, \ldots, x_t\}$ un ensemble de représentants de $G/\langle g \rangle H$. Alors*

$$V_{G \to H}(gG') = \prod_{i=1}^{t} x_i^{-1} g^f x_i H'.$$

On finit par un résultat concernant le 2-groupe de classes des corps de nombres de type $(2^n, 2^m)$ où $n$ et $m$ sont deux entiers strictement positifs.

PROPOSITION 7 ([Be-Le-Sn-98]). *Soient $k$ un corps de nombres dont le 2-groupe de classes est de type $(2^n, 2^m)$ où $n$ et $m$ sont deux entiers strictement positifs, et $k_2^{(1)}$ le 2-corps de classes de Hilbert de $k$. S'il existe une extension quadratique non ramifiée de $k$ dont le 2-nombre de classes est égale à $2^{n+m-1}$, alors le 2-nombre de classes des trois extensions quadratiques non ramifiées de $k$ est égale à $2^{n+m-1}$ et la suite des 2-corps de classes de Hilbert s'arrête en $k_2^{(1)}$.*

**3. Capitulation dans le corps de genres de k.** Soient $p$ un nombre premier tel que $p \equiv 1 \bmod 8$, $\mathbf{k}^*$ le corps de genres de $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$, $h(m)$ le 2-nombre de classes de $\mathbb{Q}(\sqrt{m})$ et $h(F)$ le 2-nombre de classes d'un corps de nombres $F$. Si $F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ est un corps biquadratique, $Q_F$ désigne l'indice du groupe engendré par les groupes des unités de $\mathbb{Q}(\sqrt{d_1})$, $\mathbb{Q}(\sqrt{d_2})$ et $\mathbb{Q}(\sqrt{d_1 d_2})$ dans le groupe des unités de $F$. Si $d_1 = d \neq 2, 3$ et $d_2 = i$, alors $Q_F$ est l'indice de Hasse de $K$ (voir p. 114). On sait d'après [H-S-82] que le nombre de classes qui capitulent dans une extension cyclique non ramifiée $M/N$ est égal à $[M : N][E_N : \mathcal{N}_{M/N}(E_M)]$, où $E_N$ (resp. $E_M$) est le groupe des unités de $N$ (resp. $M$). Alors pour calculer le nombre de classes qui capitulent dans $\mathbf{k}^*/\mathbf{k}$ il faut chercher un système fondamental d'unités (SFU) de $\mathbf{k}^*$. Comme $\mathbf{k}^* = \mathbb{Q}(\sqrt{p}, \sqrt{2}, i)$, on va chercher un SFU de $\mathbf{F} = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ afin de trouver un SFU de $\mathbf{k}^*$ (pour plus de détails sur cette méthode voir [Az-99]).

LEMME 1. *Soient $p$, $p'$, $q_1$, $q_2$ et $q$ des nombres premiers différents tels que $p \equiv p' \equiv -q_1 \equiv -q_2 \equiv -q \equiv 1 \bmod 4$, $\pi \in \{2, p', q, 2q, q_1 q_2\}$ et $\mathbf{F} = \mathbb{Q}(\sqrt{p}, \sqrt{\pi})$. Alors l'indice d'unités $Q_{\mathbf{F}}$ est égal à 2.*

*Démonstration.* D'après [Wa-66], on a $h(\mathbf{F}) = Q_{\mathbf{F}} h(p) h(\pi) h(p\pi)/4$. Or dans tous les cas de $\pi$, on a $h(\pi) = 1$ et aussi $h(p) = 1$, donc $h(\mathbf{F}) = Q_{\mathbf{F}} h(p\pi)/4$. On trouve dans [Az-Mo-01] que $h(\mathbf{F}) = h(p\pi)/2$, ce qui prouve que $Q_{\mathbf{F}} = 2$. ∎

THÉORÈME 3. *Soient $p$ un nombre premier tel que $p \equiv 1 \bmod 8$, $\mathbf{F} = \mathbb{Q}(\sqrt{p}, \sqrt{2})$, $\mathbf{k}^* = \mathbf{F}(\sqrt{-1})$ et $\varepsilon_1$ (resp. $\varepsilon_2$, $\varepsilon_3$) l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2p})$). Alors*

(i) $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ *est un SFU de* $\mathbf{F}$ *si et seulement si* $\varepsilon_3$ *est de norme* $-1$.

(ii) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ *est un SFU de* $\mathbf{F}$ *si et seulement si* $\varepsilon_3$ *est de norme* 1.

*Dans les deux cas tout SFU de* $\mathbf{F}$ *est un SFU de* $\mathbf{k}^*$.

*Démonstration.* Comme l'indice des unités de $\mathbf{F}$ est égal à 2 et les deux unités $\varepsilon_1$ et $\varepsilon_2$ sont de norme $-1$, le système $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ ou $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ est un SFU de $\mathbf{F}$ suivant que $\varepsilon_3$ est de norme $-1$ ou 1 ([Kub-56]). Si $\varepsilon_3$ est de norme $-1$, alors d'après [Az-99] $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ est un SFU de $\mathbf{k}^*$ si et seulement si il n'existe pas d'entiers $\alpha, \beta, \gamma \in \{0, 1\}$ non tous nuls tels que $(2+\sqrt{2})\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}^{\alpha}\varepsilon_2^{\beta}\varepsilon_3^{\gamma}$ est un carré dans $\mathbf{F}$. Supposons que l'on a $(2+\sqrt{2})\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}^{\alpha}\varepsilon_2^{\beta}\varepsilon_3^{\gamma} = X^2$ avec $X \in \mathbf{F}$ et les conditions précédentes. Soit $\varrho$ le $\mathbb{Q}$-automorphisme défini par $\sqrt{2} \mapsto -\sqrt{2}$ et $\sqrt{p} \mapsto \sqrt{p}$. Alors $(X\varrho(X))^2 = 2\varepsilon_1^{\alpha}(-1)^{\beta}(-1)^{\gamma} = 2\varepsilon_1^{\alpha}(-1)^{\beta+\gamma} = \pm 2\varepsilon_1^{\alpha}$, ce qui implique que 2 est un carré dans $\mathbb{Q}(\sqrt{p})$ ou bien $2\varepsilon_1$ est un carré dans $\mathbb{Q}(\sqrt{p})$, et ce n'est pas le cas. Si $\varepsilon_3$ est de norme 1 on reprend la même démonstration, et on trouve des contradictions. ∎

Remarque 2. *Soient* $p$ *un nombre premier impair,* $Q_{\mathbf{k}}$ *l'indice des unités de* $\mathbf{k}$ *et* $\varepsilon$ *l'unité fondamentale de* $\mathbb{Q}(\sqrt{2p})$. *Alors* $\varepsilon$ *est un carré dans* $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ *si et seulement si* $Q_{\mathbf{k}} = 2$ *si et seulement si* $\varepsilon$ *est de norme* 1.

*Démonstration.* On trouve dans [Az-99] que $Q_{\mathbf{k}} = 2$ si et seulement si $\varepsilon$ est de norme 1, et d'après [Az-00], on a $Q_{\mathbf{k}} = 2$ si et seulement si $2\varepsilon$ est un carré dans $\mathbf{k}$. Alors pour obtenir la remarque il suffit d'observer que $\varepsilon$ est un carré dans $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ si et seulement si $2\varepsilon$ est un carré dans $\mathbf{k}$. ∎

Théorème 4. *Soient* $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ *avec* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 8$, $\mathbf{k}^* = \mathbb{Q}(\sqrt{p}, \sqrt{2}, i)$ *le corps de genres de* $\mathbf{k}$, $C_{\mathbf{k},2}$ *le 2-groupe de classes de* $\mathbf{k}$ *au sens large et* $\varepsilon$ *l'unité fondamentale de* $\mathbb{Q}(\sqrt{2p})$. *Alors* $C_{\mathbf{k},2} \simeq (2^n, 2^m)$ $(n > 0$ *et* $m > 1)$ *et deux ou quatre classes de* $C_{\mathbf{k},2}$ *capitulent dans* $\mathbf{k}^*$, *suivant que* $\varepsilon$ *est de norme* $-1$ *ou* 1.

*Démonstration.* Comme $p \equiv 1 \bmod 8$, le 2-rang$(C_{\mathbf{k},2})$ est égal à 2 d'après [Mc-Pa-Ra-95], donc $C_{\mathbf{k},2}$ est de type $(2^n, 2^m)$. On peut conclure facilement que $n \geq 1$ et $m \geq 2$ (en utilisant la formule de Wada [Wa-66] et les résultats de Kaplan [Ka-73]). Soit $\varepsilon_1$ (resp. $\varepsilon_2$, $\varepsilon_3$) l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2p})$) et $\mathbf{F} = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. D'après le théorème 3 et [Az-99], on a les propriétés suivantes :

- Si $\varepsilon$ est de norme $-1$, alors $E_{\mathbf{k}^*} = \langle \zeta_8, \sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3 \rangle$, ainsi $\mathcal{N}_{\mathbf{k}^*/\mathbf{k}}(E_{\mathbf{k}^*}) = \langle i, \varepsilon_3 \rangle = E_{\mathbf{k}}$.
- Si $\varepsilon$ est de norme 1, alors $E_{\mathbf{k}^*} = \langle \zeta_8, \varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3} \rangle$, ainsi $\mathcal{N}_{\mathbf{k}^*/\mathbf{k}}(E_{\mathbf{k}^*}) = \langle i, \varepsilon_3 \rangle$, mais $E_{\mathbf{k}} = \langle i, \sqrt{i\varepsilon_3} \rangle$.

Puisque le nombre de classes qui capitulent dans $\mathbf{k}^*/\mathbf{k}$ est égal à $2[E_{\mathbf{k}} : \mathcal{N}_{\mathbf{k}^*/\mathbf{k}}(E_{\mathbf{k}^*})]$, on a le résultat du théorème. ∎

**4. Commutativité de $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$.** Le théorème suivant donne deux conditions nécessaires et suffisantes pour que la tour des 2-corps de classes de Hilbert de $\mathbf{k}$ ne s'arrête pas en premier terme. Ces conditions caractérisent la commutativité de $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$.

THÉORÈME 5. *Soient* $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ *avec* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 8$, $\mathbf{k}_2^{(1)}$ *le 2-corps de classes de Hilbert de* $\mathbf{k}$ *et* $\mathbf{k}_2^{(2)}$ *le 2-corps de classes de Hilbert de* $\mathbf{k}_2^{(1)}$. *Alors*

$$\mathbf{k}_2^{(1)} \neq \mathbf{k}_2^{(2)} \;\Leftrightarrow\; p = x^2 + 32y^2 \;\Leftrightarrow\; \left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4.$$

*Démonstration.* Comme $\mathbf{k}^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, i)$ est une extension de type $(2,2,2)$ sur $\mathbb{Q}$, d'après [Wa-66] on a

$$h(\mathbf{k}^*) = \frac{q(\mathbf{k}^*/\mathbb{Q})}{2^5}\, h(2)h(p)h(-1)h(-2)h(-p)h(2p)h(-2p).$$

De plus, $h(2) = h(p) = h(-1) = h(-2) = 1$ et $h(\mathbf{k}) = h(2p)h(-2p)/2Q_{\mathbf{k}}$, ce qui implique que $h(\mathbf{k}^*) = q(\mathbf{k}^*/\mathbb{Q})h(-p)h(\mathbf{k})/2^4 Q_{\mathbf{k}}$, où $q(\mathbf{k}^*/\mathbb{Q}) = [E_{\mathbf{k}^*} : \langle i, \varepsilon_1, \varepsilon_2, \varepsilon_3\rangle]$, avec $\varepsilon_1$ (resp. $\varepsilon_2$, $\varepsilon_3$) l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2p})$). Dans les deux cas de la norme de $\varepsilon_3$, il est facile de voir que $q(\mathbf{k}^*/\mathbb{Q}) = 4$. Par suite, puisque $\mathbf{k}^*$ est une extension non ramifiée de $\mathbf{k}$ et le rang du 2-groupe de classes de $\mathbf{k}$ est 2, on a $\mathbf{k}_2^{(1)} = \mathbf{k}_2^{(2)} \Leftrightarrow h(\mathbf{k}^*) = h(\mathbf{k})/2 \Leftrightarrow h(-p) = 2Q_{\mathbf{k}}$, ce qui équivalent à $h(-p) = 4$ et $Q_{\mathbf{k}} = 2$ ou $h(-p) = 2$ et $Q_{\mathbf{k}} = 1$. Or si $h(-p) = 4$ on a $Q_{\mathbf{k}} = 2$ ([Sc-34]). D'autre part P. Barrucand et H. Cohn [B-C-69] ont montré que $h(-p) = 4$ si et seulement si $p \neq x^2 + 32y^2$. On en déduit que $\mathbf{k}_2^{(1)} \neq \mathbf{k}_2^{(2)}$ si et seulement si $p = x^2 + 32y^2$. Pour compléter la preuve du théorème, on utilise lemme ci-dessous. ∎

LEMME 2. *Soit* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 8$. *Alors*

$$p = x^2 + 32y^2 \;\Leftrightarrow\; \left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4.$$

*Démonstration.* Comme $p \equiv 1 \bmod 8$, on a $p = x^2 + 2b^2$. D'après [Ka-76], $\left(\frac{2}{p}\right)_4 \left(\frac{p}{2}\right)_4 = (-1)^{b/2}$, par suite $p = x^2 + 32y \Leftrightarrow b = 4y \Leftrightarrow \left(\frac{2}{p}\right)_4 \left(\frac{p}{2}\right)_4 = 1$. ∎

COROLLAIRE 1. *Soient* $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ *avec* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 8$ *et* $C_{\mathbf{k},2}$ *le 2-groupe de classes au sens large de* $\mathbf{k}$. *Si* $C_{\mathbf{k},2}$ *est de type* $(2,4)$, *alors*

$$\mathbf{k}_2^{(1)} \neq \mathbf{k}_2^{(2)} \;\Leftrightarrow\; \left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1.$$

*Démonstration.* Comme $C_{\mathbf{k},2}$ est de type $(2,4)$, d'après [Wa-66] le 2-nombre de classes $h(\mathbf{k})$ de $\mathbf{k}$ est donné par

$$h(\mathbf{k}) = \frac{1}{2}\, Qh(2p)h(-2p)$$

où $Q = Q_{\mathbf{k}}$ désigne l'indice des unités de $\mathbf{k}$. Selon [Ka-73], $4 \,|\, h(2p)$ et $4 \,|\, h(-2p)$ ou $2 \,|\, h(2p)$ et $4 \,|\, h(-2p)$, donc $h(\mathbf{k}) = 8$ si et seulement si $h(2p) = h(-2p) = 4$ et $Q = 1$ ou $h(-2p) = 2h(2p) = 4$ et $Q = 2$. A. Scholz a montré dans [Sc-34] que les derniers conditions sont équivalentes à $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$ ou bien $\left(\frac{2}{p}\right)_4 = -\left(\frac{p}{2}\right)_4 = -1$. Alors d'après le théorème précédent, dans le premier cas on a $\mathbf{k}_2^{(1)} \neq \mathbf{k}_2^{(2)}$ et dans le deuxième on a $\mathbf{k}_2^{(1)} = \mathbf{k}_2^{(2)}$. ∎

**5. Les sous-extensions de $\mathbf{k}_2^{(1)}/\mathbf{k}$.** Dans toute cette section on suppose que $p$ est un nombre premier tel que $p \equiv 1 \bmod 8$ et $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$. Alors $C_{\mathbf{k},2} = \langle \sigma, \tau \rangle$ où $\sigma^4 = \tau^2$ et $\sigma\tau = \tau\sigma$, car $C_{\mathbf{k},2}$ est de type $(2,4)$. Il est clair que $C_{\mathbf{k},2}$ admet trois sous-groupes d'indice 2 et trois sous-groupes d'indice 4. Par la théorie des corps de classes, on sait que chaque sous-groupe $H$ de $C_{\mathbf{k},2}$ correspond à une extension non ramifiée $K$ de $\mathbf{k}_2^{(2)}$ telle que $C_{\mathbf{k},2}/H \simeq \mathrm{Gal}(K/\mathbf{k})$ et $H = \mathcal{N}_{K/\mathbf{k}}(C_{\mathbf{K},2})$. La situation est schématisée par le diagramme suivant :

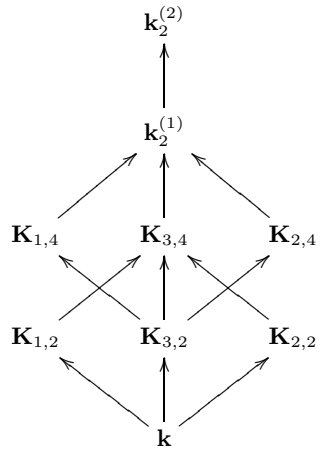


Diagramme 1

Dans cette section on va essayer de construire les corps $\mathbf{K}_{1,2}$, $\mathbf{K}_{2,2}$, $\mathbf{K}_{3,2}$, $\mathbf{K}_{1,4}$, $\mathbf{K}_{2,4}$, $\mathbf{K}_{3,4}$, et $\mathbf{k}_2^{(1)}$. Pour cela on aura besoin des deux résultats suivants :

Remarque 3. *Si on garde les notations précédentes, alors*

$$\mathrm{Gal}(\mathbf{K}_{1,4}/\mathbb{Q}(i)) \simeq \mathrm{Gal}(\mathbf{K}_{2,4}/\mathbb{Q}(i)) \simeq D_3.$$

*Démonstration.* Si on pose $F = \mathbb{Q}(i)$ et $K$ le corps $\mathbf{K}_{1,4}$ ou $\mathbf{K}_{2,4}$, la proposition 1 implique que $\mathrm{Gal}(\mathbf{K}_{1,4}/\mathbb{Q}(i)) \simeq \mathrm{Gal}(\mathbf{K}_{2,4}/\mathbb{Q}(i)) \simeq D_3$. ∎

LEMME 3 ([Lm-94]). *Soit $K/F$ une extension biquadratique telle que $\mathrm{Gal}(K/F) = \langle \varrho, \varphi \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et soit $R = K(\sqrt{\mu})$. Alors $R/F$ est normale si et seulement si $\mu^{1-\varrho}$ est un carré dans $K$ pour tout $\varrho \in \mathrm{Gal}(K/F)$. Dans ce cas écrivons $\mu^{1-\varrho} = \alpha_\varrho^2$, $\mu^{1-\tau} = \alpha_\varphi^2$ et $\mu^{1-\varrho\varphi} = \alpha_{\varrho\varphi}^2$. Il est facile de voir que $\alpha_\varrho^{1+\varrho} = \pm 1$ pour tout $\varrho \in \mathrm{Gal}(K/F)$; on définit $S(\mu, K/F) = (\alpha_\varrho^{1+\varrho}, \alpha_\varphi^{1+\varphi}, \alpha_{\varrho\varphi}^{1+\varrho\varphi})$. Alors à une permutation près on a :*

$$\mathrm{Gal}(R/F) \simeq \begin{cases} (2,2,2) & \Leftrightarrow \quad S(\mu, K/F) = (+1,+1,+1), \\ (2,4) & \Leftrightarrow \quad S(\mu, K/F) = (-1,-1,+1), \\ D_3 & \Leftrightarrow \quad S(\mu, K/F) = (-1,+1,+1), \\ Q_3 & \Leftrightarrow \quad S(\mu, K/F) = (-1,-1,-1). \end{cases}$$

*De plus $R$ est cyclique sur le corps fixé par $\langle \varrho \rangle$ si et seulement si $\alpha_\varrho^{1+\varrho} = -1$, et est de type $(2,2)$ dans le cas contraire.*

THÉORÈME 6. *Soient $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ avec $p$ un nombre premier tel que $p \equiv 1 \bmod 8$, $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$, $\mathbf{k}^* = \mathbb{Q}(\sqrt{p}, \sqrt{2}, i)$ le corps de genres de $\mathbf{k}$ et $\mathbf{K}_{1,2}$, $\mathbf{K}_{2,2}$, $\mathbf{K}_{3,2}$, $\mathbf{K}_{1,4}$, $\mathbf{K}_{2,4}$, $\mathbf{K}_{3,4}$ les sous-extensions du diagramme 1. Si on pose $p = e^2 + 16f^2 = x^2 + 32y^2 = c^2 - 32d^2$, $\pi_1 = e + 4fi$, $\pi_2 = e - 4fi$, $\pi_3 = x + 4y\sqrt{-2}$ et $\pi_4 = c + 4d\sqrt{2}$ ($c$ et $d > 0$), alors*

- $\mathbf{K}_{1,2} = \mathbf{k}(\sqrt{\pi_1})$, $\mathbf{K}_{3,2} = \mathbf{k}^*$, $\mathbf{K}_{2,2} = \mathbf{k}(\sqrt{\pi_2})$,
- $\mathbf{K}_{1,4} = \mathbf{k}^*(\sqrt{\pi_3})$, $\mathbf{K}_{3,4} = \mathbf{k}^*(\sqrt{\pi_1})$, $\mathbf{K}_{2,4} = \mathbf{k}^*(\sqrt{\pi_4})$,
- $\mathbf{k}_2^{(1)} = \mathbf{k}^*(\sqrt{\pi_3}, \sqrt{\pi_4})$.

*Démonstration.* Comme les premiers $\pi_1$ et $\pi_2$ (resp. $\pi_3$, $\pi_4$) sont ramifiées dans $\mathbf{k}/\mathbb{Q}(i)$ (resp. dans $\mathbf{k}^*/\mathbb{Q}(\sqrt{2}, i)$, $\mathbf{k}/\mathbb{Q}(\sqrt{2})$) et l'extension $\mathbf{k}^*/\mathbf{k}$ est non ramifiée, les idéaux engendrés par $\pi_1$ et $\pi_2$ (resp. $\pi_3$ et $\pi_4$) sont des carrés d'idéaux de $\mathbf{k}$ (resp. $\mathbf{k}^*$). Observons que $e$, $x$ et $c$ sont des nombres impairs, donc $e \equiv x \equiv c \equiv \pm 1 \equiv i^2 \bmod 4$, alors les équations $\pi_i \equiv \xi^2$ sont résolubles. Le théorème 1 implique que les extensions $\mathbf{k}(\sqrt{\pi_1})$, $\mathbf{k}(\sqrt{\pi_2})$, $\mathbf{k}^*(\sqrt{\pi_3})$ et $\mathbf{k}^*(\sqrt{\pi_4})$ sont des extensions différentes non ramifiées de $\mathbf{k}$. Supposons que $\mathbf{k}(\sqrt{\pi_1}) = \mathbf{k}^*(\sqrt{\pi_2})$. Alors il existe un élément $t$ tel que $\pi_1 = t^2\pi_2$, ce qui implique que $p = t^2\pi_2^2$, et ce n'est pas le cas, car $\sqrt{p} \notin \mathbf{k}$. Comme l'extension $\mathbf{k}^*/\mathbb{Q}$ est normale et $\mathbf{k}(\pi_i)/\mathbb{Q}$ ($i = 1, 2$) n'est pas normale, on a $\mathbf{k}(\pi_i) \neq \mathbf{k}^*$. De la même façon on montre que $\mathbf{k}^*(\sqrt{\pi_i}) \neq \mathbf{k}^*(\sqrt{\pi_1})$ ($i = 3, 4$). Puisque $\pi_4 > 0$, le corps réel maximal de $\mathbf{k}^*(\sqrt{\pi_4})$ est $\mathbb{Q}(\sqrt{2}, \sqrt{\pi_4}, \sqrt{p})$ et pour $\mathbf{k}^*(\sqrt{\pi_3})$ c'est $\mathbb{Q}(\sqrt{2}, \sqrt{p})$, ainsi $\mathbf{k}^*(\sqrt{\pi_3}) \neq \mathbf{k}^*(\sqrt{\pi_4})$. Or il est facile de vérifier que $S(\pi_3, \mathbf{k}^*)/\mathbb{Q}(i) = S(\pi_4, \mathbf{k}^*)/\mathbb{Q}(i) = (-1, +1, +1)$. Le lemme précédent donne alors $\mathrm{Gal}(\mathbf{k}^*(\sqrt{\pi_3})/\mathbb{Q}(i)) \simeq \mathrm{Gal}(\mathbf{k}^*(\sqrt{\pi_4})/\mathbb{Q}(i)) \simeq D_3$, ce qui achève la preuve. ∎

REMARQUE 4. *On garde les notations précédentes. Alors les deux corps* $\mathbf{K}_{1,2}$ *et* $\mathbf{K}_{2,2}$ *sont conjugués, en particulier* $h(\mathbf{K}_{1,2}) = h(\mathbf{K}_{2,2})$.

**6. Le 2-nombre de classes de** $\mathbb{Q}(\sqrt{2}, \sqrt{\pi}, \sqrt{p}, i)$**.** Soit $p$ un nombre premier tel que $p \equiv 1 \bmod 8$. Alors il existe des entiers $c$ et $d$ tels que $p = c^2 - 32d^2$. Soient $\pi = c + 4d\sqrt{2}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{\pi}, \sqrt{p}, i)$ et $h$ le 2-nombre de classes de $\mathbb{Q}(\sqrt{2}, \sqrt{-\pi}) = \mathbb{Q}(\sqrt{-\pi})$. Dans cette section, on va calculer $h(L)$, le 2-nombre de classes de $L$ et $h$. Soit $E/F$ une extension de corps de nombres tel que les anneaux des entiers de $E$ et $F$ sont principaux. Notons $[\text{-}]$ (resp. $(\text{-})$) le symbole de reste quadratique de $E$ (resp. $F$), $\mathcal{N}_{E/F}$ l'application norme de $E/F$, et $l$ (resp. $\mathfrak{p}$) un nombre premier de $E$ (resp. $F$) dont la norme absolue est impaire, $v_l$ la valuation $l$-adique et $\mathcal{N}_{E/F}((l)) = (\mathfrak{p})^f$. Nous avons alors :

PROPOSITION 8. *Pour tout élément* $a$ *de* $F$ *tel que* $v_l(a) = 0$, *on a*

$$\left[\frac{a}{(l)}\right] = \left(\frac{a}{(\mathfrak{p})}\right)^f.$$

*Démonstration.* Rappelons que le symbole de Hilbert sur $E$ a la propriété suivante :

$$\left(\frac{x, y}{\beta}\right) = \left(\frac{x, \mathcal{N}_{E/F}(y)}{P}\right)$$

pour $x \in F$, $y \in E$ et $P$ un idéal premier de $F$ au-dessus de l'idéal premier $\beta$ de $E$. Comme $v_l(a) = 0$ et d'après la proposition 2, on a

$$\left[\frac{a}{(l)}\right] = \left(\frac{a, l}{(l)}\right) = \left(\frac{a, \mathcal{N}_{E/F}((l))}{(\mathfrak{p})}\right) = \left(\frac{a, \mathfrak{p}^f}{(\mathfrak{p})}\right) = \left(\frac{a, \mathfrak{p}}{(\mathfrak{p})}\right)^f = \left(\frac{a}{(\mathfrak{p})}\right)^f. \ \blacksquare$$

Avant de démontrer le lemme suivant, rappelons que $\mathbb{Q}(\sqrt{2})$ admet deux premiers infinis, $\mathcal{P}_\infty$ et $\mathcal{P}'_\infty$. Si $u$ est un élément de $\mathbb{Q}(\sqrt{2})$ nous notons $u'$ son conjugué et $s(u) = uu'|uu'|^{-1}$.

LEMME 4. *On garde les notations précédentes. Alors*

(i) $\left(\dfrac{-\pi, \varepsilon_0}{(l)}\right) = \left(\dfrac{-\pi, \sqrt{2}}{(l)}\right) = 1$ *pour tout nombre premier* $l$ *de* $\mathbb{Q}(\sqrt{2})$ *différent de* $\pi$ *et de* $\sqrt{2}$.

(ii) $\left(\dfrac{-\pi, u}{\mathcal{P}_\infty}\right) = s(u)\left(\dfrac{-\pi, u}{\mathcal{P}'_\infty}\right)$.

(iii) $\left(\dfrac{-\pi, \varepsilon_0}{(\pi)}\right) = -\left(\dfrac{-\pi, \varepsilon_0}{(\sqrt{2})}\right) = \left(\dfrac{2}{p}\right)_4 \left(\dfrac{p}{2}\right)_4$.

(iv) $\left(\dfrac{-\pi, 2+\sqrt{2}}{(\pi)}\right) = \left(\dfrac{-\pi, 2+\sqrt{2}}{(\sqrt{2})}\right) = \left(\dfrac{p}{2}\right)_4$.

*Démonstration.* (i) évident, car $v_l(-\pi) = v_l(\varepsilon_0) = v_l(\sqrt{2}) = 0$.

(ii) Soit $i_1 : \sqrt{2} \mapsto \sqrt{2}$ (resp. $i_2 : \sqrt{2} \mapsto -\sqrt{2}$) le $\mathbb{Q}$-plongement de $\mathbb{Q}(\sqrt{2})$ dans le $\mathbb{Q}(\sqrt{2})_{\mathcal{P}_\infty} = \mathbb{R}$ (resp. $\mathbb{Q}(\sqrt{2})_{\mathcal{P}'_\infty} = \mathbb{R}$) le complété de $\mathbb{Q}(\sqrt{2})$ pour la valeur absolue associée à $\mathcal{P}_\infty$ (resp. $\mathcal{P}'_\infty$). Alors d'après [Gr-03], on a

$$\left(\frac{-\pi, u}{\mathcal{P}_\infty}\right) = \begin{cases} i_1^{-1}((-\pi, u)_{\mathcal{P}_\infty}) = i_1^{-1}(1) = 1 & \text{si } u > 0, \\ i_1^{-1}((-\pi, u)_{\mathcal{P}_\infty}) = i_1^{-1}(-1) = -1 & \text{si } u < 0, \end{cases}$$

$$\left(\frac{-\pi, u}{\mathcal{P}'_\infty}\right) = \begin{cases} i_2^{-1}((-\pi', u')_{\mathcal{P}'_\infty}) = i_2^{-1}(1) = 1 & \text{si } u' > 0, \\ i_2^{-1}((-\pi', u')_{\mathcal{P}'_\infty}) = i_2^{-1}(-1) = -1 & \text{si } u' < 0 \end{cases}$$

(car $(v, u)_{\mathbb{R}} = -1$ si et seulement si les deux nombres $u$ et $v$ sont négatifs) où $(-\pi, u)_{\mathcal{P}_\infty}$ (resp. $(-\pi, u)_{\mathcal{P}'_\infty}$) est le symbole local de Hilbert définit sur $\mathbb{Q}(\sqrt{2})_{\mathcal{P}_\infty} \times \mathbb{Q}(\sqrt{2})_{\mathcal{P}_\infty}$ (resp. $\mathbb{Q}(\sqrt{2})_{\mathcal{P}'_\infty} \times \mathbb{Q}(\sqrt{2})_{\mathcal{P}'_\infty}$). D'où le résultat.

(iii) Comme $v_l(-\pi) = 1$ et $v_l(\varepsilon) = 0$ et d'après la proposition 2, on a

$$\left(\frac{-\pi, \varepsilon_0}{(l)}\right) = \left[\frac{\varepsilon_0}{(\pi)}\right],$$

où [-] est le symbole de reste quadratique sur $\mathbb{Q}(\sqrt{2})$. Or $\varepsilon_0 = 1 + \sqrt{2}$ et $\pi = c + 4d\sqrt{2}$, alors

$$\left[\frac{\varepsilon_0}{(\pi)}\right] = \left[\frac{4d}{(\pi)}\right]\left[\frac{4d + 4\sqrt{2}\,d}{(\pi)}\right] = \left[\frac{4d}{(\pi)}\right]\left[\frac{4d - c + \pi}{(\pi)}\right] = \left[\frac{d}{(\pi)}\right]\left[\frac{4d - c}{(\pi)}\right].$$

D'après [Ka-76, théorème 2, p. 324] et la proposition précédente on a

$$\left[\frac{\varepsilon_0}{(\pi)}\right] = \left[\frac{d}{(p)}\right]\left[\frac{4d - c}{(p)}\right] = \left(\frac{2}{p}\right)_4 \left(\frac{p}{2}\right)_4.$$

Notons $S$ l'ensemble des nombres premiers $l$ de $\mathbb{Q}(\sqrt{2})$ différents de $\pi$, de $\sqrt{2}$, et de $\mathcal{P}_\infty$ et $\mathcal{P}'_\infty$, les deux premiers infinis de $\mathbb{Q}(\sqrt{2})$. Alors d'après la formule du produit pour le symbole de Hilbert, on a

$$\prod_{l \in S}\left(\frac{-\pi, \varepsilon_0}{(l)}\right)\left(\frac{-\pi, \varepsilon_0}{\mathcal{P}_\infty}\right)\left(\frac{-\pi, \varepsilon_0}{\mathcal{P}'_\infty}\right)\left(\frac{-\pi, \varepsilon_0}{(\pi)}\right)\left(\frac{-\pi, \varepsilon_0}{(\sqrt{2})}\right) = 1.$$

Puisque $s(\varepsilon_0) = -1$, alors $\left(\frac{-\pi, \varepsilon_0}{\mathcal{P}_\infty}\right) = -\left(\frac{-\pi, \varepsilon_0}{\mathcal{P}'_\infty}\right)$. Il résulte de (i) que

$$\left(\frac{-\pi, \varepsilon_0}{(\pi)}\right) = -\left(\frac{-\pi, \varepsilon_0}{(\sqrt{2})}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{p}{2}\right)_4.$$

(iv) De la même façon que dans (iii), on trouve le résultat annoncé. ∎

THÉORÈME 7. *On garde les notations et hypothèses précédentes. Alors le 2-groupe de classes de* $\mathbb{Q}(\sqrt{-\pi})$ *est cyclique. De plus, on a*

$$h = \begin{cases} 1 & si\ \left(\frac{2}{p}\right)_4 = -\left(\frac{p}{2}\right)_4, \\ 2 & si\ \left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1, \\ \geq 4 & si\ \left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = 1. \end{cases}$$

*Démonstration.* On a $\mathbb{Q}(\sqrt{-\pi}) = \mathbb{Q}(\sqrt{2})(\sqrt{-\pi})$. Le nombre de classes de $\mathbb{Q}(\sqrt{2})$ est égal à 1, donc d'après [Gr-73], le 2-rang du 2-groupe de classes de $\mathbb{Q}(\sqrt{-\pi})$ est $r_2 = t-1-e$, où $t$ est le nombre des premiers de $\mathbb{Q}(\sqrt{2})$ qui sont ramifiés dans $\mathbb{Q}(\sqrt{-\pi})$ et $e$ est l'entier naturel tel que $2^e$ est l'indice du groupe engendré par les unités de $\mathbb{Q}(\sqrt{2})$ qui sont des normes dans $\mathbb{Q}(\sqrt{-\pi})$ dans le groupe des unité de $\mathbb{Q}(\sqrt{2})$. Observons que $c$ est un nombre impair tel que $-(c+4d\sqrt{2}) = -\pi \equiv -\left(\frac{-1}{c}\right) \equiv -\left(\frac{2}{p}\right)_4\left(\frac{p}{2}\right)_4 \bmod 4$ (voir [Ka-76, théorème 2, p. 324] ; donc d'après la proposition 1.2 de [Gr-73, p. 11], $\mathbb{Q}(\sqrt{-\pi})/\mathbb{Q}(\sqrt{2})$ est non ramifié en $\sqrt{2}$ si et seulement si $\left(\frac{2}{p}\right)_4 = -\left(\frac{p}{2}\right)_4$. De plus, $\mathbb{Q}(\sqrt{2})$ admet deux premiers infinis, $\mathcal{P}_\infty$ et $\mathcal{P}'_\infty$, se ramifiant dans $\mathbb{Q}(\sqrt{-\pi})/\mathbb{Q}(\sqrt{2})$. Comme $-\pi$ et $-1$ sont deux nombres négatifs et $s(\varepsilon_0) = -1$, le (ii) du lemme précédent donne que

$$\left(\frac{-\pi,-1}{\mathcal{P}_\infty}\right) = -1 \quad \text{et} \quad \left(\frac{-\pi,\varepsilon_0}{\mathcal{P}_\infty}\right) = -\left(\frac{-\pi,\varepsilon_0}{\mathcal{P}'_\infty}\right).$$

Nous avons toujours $e = 2$, car $-1$ et $\varepsilon_0$ ne sont pas des normes dans l'extension $\mathbb{Q}(\sqrt{-\pi})/\mathbb{Q}(\sqrt{2})$ (un élément $u$ de $\mathbb{Q}(\sqrt{2})$ est norme dans cette extension si et seulement si la valeur du symbole de Hilbert $\left(\frac{-\pi,u}{(l)}\right)$ est égale à 1 pour tout idéal premier $(l)$ de $\mathbb{Q}(\sqrt{2})$). Si $\left(\frac{2}{p}\right)_4 = -\left(\frac{p}{2}\right)_4$, alors $e = 2$ et $t = 3$, par suite $h = 1$. Supposons dans toute la suite que $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4$. On vérifie facilement que $t = 4$ et nous avons $e = 2$, ce qui prouve que $r_2 = 1$ et le 2-groupe de classes de $\mathbb{Q}(\sqrt{-\pi})$ est cyclique.

Soient $r_4$ le 4-rang du 2-groupe de classes de $\mathbb{Q}(\sqrt{-\pi})$ et $\mathfrak{a}$ l'idéal premier de $\mathbb{Q}(\sqrt{-\pi})$ tel que $(\sqrt{2}) = \mathfrak{a}^2$. Il est facile de voir que la classe de $\mathfrak{a}$ dans $\mathbb{Q}(\sqrt{-\pi})$ est une classe ambiguë non triviale et l'idéal de $\mathbb{Q}(\sqrt{2})$ engendré par $\sqrt{2}$ est engendré aussi par $2+\sqrt{2}$ car $-\sqrt{2} = (2+\sqrt{2})(1-\sqrt{2}) = (2+\sqrt{2})\varepsilon_0^{-1}$. D'après la théorie des genres, $r_4 \geq 1$ si $2+\sqrt{2}$ est norme dans l'extension $\mathbb{Q}(\sqrt{-\pi})/\mathbb{Q}(\sqrt{2})$. Ainsi le (iv) du lemme précédent entraîne que $r_4 \geq 1$ si et seulement si $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = 1$. D'où le résultat énoncé. ∎

Rappelons qu'une *extension CM* est une extension quadratique totalement imaginaire d'un corps de nombres totalement réel. Soit $K/k$ une extension CM. Alors l'*indice des unités de Hasse* est défini par $Q_K = [E_K : W_K E_k]$ où $W_K$ est le groupe des racines de l'unité contenues dans $K$, et $E_K$ (resp. $E_k$) le groupe des unités de $K$ (resp. $k$). On note par $\omega_K$ le cardinal de $W_K$. Il est à noter que $Q_K = 1$ ou 2 (voir [Ha-85]).

Dans le lemme suivant on va calculer l'indice des unités de Hasse de $M = \mathbb{Q}(\sqrt{2}, \sqrt{-\pi}, \sqrt{p})$, $L = M(i)$ et $\mathbf{k}^*$, le corps de genres de $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$.

LEMME 5. *On garde les notations et hypothèses précédentes. Alors*

$$Q_M = Q_{\mathbf{k}^*} = Q_L = 1.$$

*Démonstration.* Soient $p$ un nombre premier tel que $p \equiv 1 \bmod 8$, $\mathbf{F} = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ et $\varepsilon_1$ (resp. $\varepsilon_2$, $\varepsilon_3$) l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2p})$). Alors $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ ou $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ est un SFU de $\mathbf{F}$ suivant que $\varepsilon_3$ est de norme $-1$ ou 1. Si $\varepsilon_3$ est de norme $-1$, alors d'après [Az-99], $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ est un SFU de $M$ si et seulement s'il n'existe pas d'entiers $\alpha, \beta, \gamma \in \{0, 1\}$ non tous nuls et tels que $\pi\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}^{\alpha}\varepsilon_2^{\beta}\varepsilon_3^{\gamma}$ est un carré dans $\mathbf{F}$. Supposons que $\pi\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}^{\alpha}\varepsilon_2^{\beta}\varepsilon_3^{\gamma}$ est un carré dans $\mathbf{F}$. Comme $\pi$ (resp. $\varepsilon_1, \varepsilon_2$) est de norme $p$ (resp. $-1$) dans $\mathbf{F}/\mathbb{Q}(\sqrt{2p})$, $p\varepsilon_3^{\alpha}(-1)^{\beta}\varepsilon_3^{2\gamma}$ est un carré dans $\mathbb{Q}(\sqrt{2p})$, ce qui implique que $p$ est un carré dans $\mathbb{Q}(\sqrt{2p})$ ou bien $p\varepsilon_3$ est un carré dans $\mathbb{Q}(\sqrt{2p})$, et ce n'est pas le cas. Si $\varepsilon_3$ est de norme 1 on reprend la même démonstration, et on trouve des contradictions. Il reste de prouver que $Q_{\mathbf{k}^*} = Q_L = 1$. Le théorème 3 implique que $Q_{\mathbf{k}^*} = 1$. On en déduit, avec le lemme 25 de [Ok-01], que $Q_L = 1$. ∎

THÉORÈME 8. *Soient* $L = \mathbb{Q}(\sqrt{2}, \sqrt{\pi}, \sqrt{p}, i)$ *avec* $p = c^2 - 32d^2$ *un nombre premier tel que* $p \equiv 1 \bmod 8$, $\pi = c + 4d\sqrt{2}$ $(c, d > 0)$ *et* $h$ *le* 2*-nombre de classes de* $\mathbb{Q}(\sqrt{-\pi})$. *Alors*

$$h(L) = \begin{cases} \left(\dfrac{h}{2}\right)^2 \cdot \dfrac{h(\mathbf{k}^*)}{2} & \text{si } \left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = 1, \\ \dfrac{h(\mathbf{k}^*)}{2} & \text{sinon.} \end{cases}$$

*Démonstration.* Notons que $L/\mathbf{F}$ est une extension normale de type $(2, 2)$ qui vérifie les hypothèses de la proposition 2 de [Lm-95]. Il en résulte que

$$h(L) = \frac{Q_L}{Q_M Q_{\mathbf{k}^*}} \frac{\omega_L}{\omega_M \omega_{\mathbf{k}^*}} \frac{h(M)h(\mathbf{k}^*)h(N)}{h(\mathbf{F})^2}$$

avec $M = \mathbb{Q}(\sqrt{p}, \sqrt{-\pi})$, $N = \mathbb{Q}(\sqrt{p}, \sqrt{\pi})$, $\mathbf{k}^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, i)$ le corps de genres de $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ et $\mathbf{F} = \mathbb{Q}(\sqrt{2}, \sqrt{p})$. Lorsque $\left(\frac{2}{p}\right)_4 = -\left(\frac{p}{2}\right)_4$, on a vu aux sections 4 et 5 que la suite des 2-corps de classes de $\mathbf{k}$ de Hilbert s'arrête en $\mathbf{k}_2^{(1)}$ et $L$ est une extension quadratique non ramifiée de $\mathbf{k}^*$ ; par suite,

$$h(L) = h(\mathbf{k}^*)/2.$$

Si $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4$, alors $\left(\frac{2}{p}\right)_4\left(\frac{p}{2}\right)_4 = \left(\frac{-1}{c}\right) = 1$ (voir [Ka-76]). Dans ce cas, $c \equiv 1 \bmod 4$, ainsi $\pi \equiv 1 \bmod 4$. Sous ces conditions, le théorème 1 implique que $N = \mathbf{F}(\sqrt{\pi})$ est une extension quadratique non ramifiée, et donc puisque le groupe de classes de $\mathbf{F}$ est cyclique (voir [Az-Mo-01]) on a

$$h(N) = h(\mathbf{F})/2. \tag{6.1}$$

Maintenant, remarquons que $M/\mathbb{Q}(\sqrt{2})$ est une extension normale de type $(2,2)$ ; nous pouvons alors appliquer la formule de Kuroda (proposition 3) et on a

$$h(M) = \frac{qhh'h(\mathbf{F})}{2h(\mathbb{Q}(\sqrt{2}))^2}$$

avec $q = [E_M : EE'E_{\mathbf{F}}]$, $h$ (resp. $h'$) le 2-nombre de classes de $\mathbb{Q}(\sqrt{-\pi})$ (resp. $\mathbb{Q}(\sqrt{-\pi'})$), $\pi' = c - 4d\sqrt{2}$ et $E$ (resp. $E'$) le groupe des unités de $\mathbb{Q}(\sqrt{-\pi})$ (resp. $\mathbb{Q}(\sqrt{-\pi'})$). Comme $\mathbb{Q}(\sqrt{-\pi})$ et $\mathbb{Q}(\sqrt{-\pi'})$ sont deux corps de nombres conjugués, on a $h = h'$ et le lemme précédent implique que

$$[E_M : E_{\mathbf{F}}] = 1.$$

Il est clair que $\mathbb{Q}(\sqrt{-\pi})$ et $\mathbb{Q}(\sqrt{-\pi'})$ sont des extensions CM dont les indices des unités sont égaux à 1 (il suffit de remarquer que $-\pi\varepsilon_0$ n'est jamais un carré dans $\mathbb{Q}(\sqrt{2})$ où $\varepsilon_0$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{2})$). Par suite, $E$ et $E'$ sont engendrés par $-1$ et $\varepsilon_0$ et inclus dans $E_{\mathbf{F}}$, c'est-à-dire $q = [E_M : EE'E_{\mathbf{F}}] = [E_M : E_{\mathbf{F}}] = 1$. Ainsi

$$h(M) = \frac{1}{2}\, h^2 h(\mathbf{F}). \tag{6.2}$$

Compte tenu du lemme précédent on a

$$\frac{Q_L}{Q_M Q_{\mathbf{k}^*}} \frac{\omega_L}{\omega_M \omega_{\mathbf{k}^*}} = \frac{1}{1\cdot 1} \frac{8}{2\cdot 8} = \frac{1}{2}. \tag{6.3}$$

Les résultats (6.1)–(6.3) impliquent que $h(L) = (h/2)^2 \cdot h(\mathbf{k}^*)/2$. Les résultats du théorème 7 achèvent la preuve. ∎

## 7. Structure de $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ et de $C_{2,\mathbf{k}}$

THÉORÈME 9. *Soient* $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ *avec* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 8$, $\mathbf{k}^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, i)$ *le corps de genres de* $\mathbf{k}$ *et* $C_{\mathbf{k}^*,2}$ *le 2-groupe de classes de* $\mathbf{k}^*$. *Alors le rang de* $C_{\mathbf{k}^*,2}$ *est* 2 *ou* 3. *De plus, le rang de* $C_{\mathbf{k}^*,2}$ *est* 3 *si et seulement si* $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = 1$.

*Démonstration.* Notons $F$ le corps $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$, $\mathrm{Am}(\mathbf{k}^*/F)$ le groupe de classes ambiguës dans $\mathbf{k}^*/F$ et $r$ le rang de $C_{\mathbf{k}^*,2}$. Il est bien connu que le groupe des unités de $F$ est engendré par $\varepsilon_0 = 1 + \sqrt{2}$, l'unité fondamentale de $\mathbb{Q}(\sqrt{2})$, et $\zeta_8$, la racine 8-ième 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 $\mathbf{k}^*/F$ :

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

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 $\left(\frac{\cdot,\cdot}{\beta}\right)$, le théorème de Hasse entraîne qu'une unité $\varepsilon$ 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 et le même raisonnement que dans le lemme 4 on trouve que

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

En particulier,

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

Enfin

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

D'où le résultat. ∎

Remarque 5. *Soient $p$ un nombre premier tel que $p \equiv 1 \bmod 8$ et $\mathbf{k}^*$ le corps de genres de $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$. Alors on a les décompositions suivantes* :

- $(p) = (\pi\pi')$ *dans* $\mathbb{Q}(\sqrt{2})$,
- $(\pi) = (\pi_1\pi_2)$ *et* $(\pi') = (\pi_3\pi_4)$ *dans* $\mathbb{Q}(\zeta_8)$,
- $(\pi_i) = \mathcal{G}_i^2$ *dans* $\mathbf{k}^*$,
- $(p) = \beta^2$ *dans* $\mathbb{Q}(\sqrt{2p})$,
- $\beta = \mathcal{P}_1\mathcal{P}_2$ *dans* $\mathbb{Q}(\sqrt{2}, \sqrt{p})$,
- $\mathcal{P}_1 = \mathcal{G}_1\mathcal{G}_2$ *dans* $\mathbf{k}^*$,
- $(\pi) = \mathcal{P}_1^2$ *dans* $\mathbb{Q}(\sqrt{2}, \sqrt{p})$.

Théorème 10. *Soient $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ avec $p$ un nombre premier tel que $p \equiv 1 \bmod 8$, $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$, $\mathbf{k}^* = \mathbb{Q}(\sqrt{2}, \sqrt{p}, i)$ le corps de genres de $\mathbf{k}$ et $C_{\mathbf{k}^*,2}$ le 2-groupe de classes de $\mathbf{k}^*$. Alors le 4-rang de $C_{\mathbf{k}^*,2}$ est 1.*

*Démonstration.* D'après le théorème précédent, la condition $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$ entraîne que le rang de $C_{\mathbf{k}^*,2}$ est égal à 2 ou encore il y a exactement quatre classes ambiguës dans $\mathbf{k}^*/\mathbb{Q}(\zeta_8)$.

Il est à noter que, si $E/F$ est une extension quadratique de corps de nombres telle que le nombre de classes de $F$ est impair et il existe exactement $2^r$ classes ambiguës qui sont des carrés, alors le 4-rang de $C_E$ est égal à $r$. Comme le 2-nombre de classes de $\mathbf{k}^*$ est égal à $2h(-p)$ et est divisible par 16, le 4-rang de $C_{\mathbf{k}^*,2}$ est 1 ou 2. Il reste de trouver la classe ambiguë non triviale de $C_{\mathbf{k}^*,2}$ qui n'est pas un carré.

Nous reprenons les notations de la remarque précédente. Alors l'idéal $\beta$ est non principal car sinon $p\varepsilon$ est un carré dans $\mathbb{Q}(\sqrt{2p})$ où $\varepsilon$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{2p})$, ce qui implique que $\varepsilon$ est un carré dans $\mathbb{Q}(\sqrt{2},\sqrt{p})$, c'est-à-dire que $\varepsilon$ est de norme 1 (voir remarque 2). Mais puisque $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$, $\varepsilon$ est de norme $-1$, et on obtient une contradiction. Or la relation $\mathcal{N}_{\mathbb{Q}(\sqrt{2},\sqrt{p})/\mathbb{Q}(\sqrt{2p})}(\mathcal{P}_1) = \beta$ implique que $\mathcal{P}_1$ est non principal, et par suite la classe de $\mathcal{P}_1$ est d'ordre 2. De même $\mathcal{N}_{\mathbf{k}^*/\mathbb{Q}(\sqrt{2},\sqrt{p})}(\mathcal{G}_1) = \mathcal{P}_1$ et $\mathcal{G}_1$ est non principal dans $\mathbf{k}^*$, donc la classe $[\mathcal{G}_1]$ est ambiguë non triviale dans $\mathbf{k}^*/\mathbb{Q}(\zeta_8)$ car $(\pi_1) = \mathcal{G}_1^2$. Rappelons que puisque $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$, le nombre de classes de $\mathbb{Q}(\sqrt{2},\sqrt{p})$ est égal à 2, ce qui prouve que la classe $[\mathcal{P}_1] = \mathcal{N}_{\mathbf{k}^*/\mathbb{Q}(\sqrt{2},\sqrt{p})}([\mathcal{G}_1])$ engendre le groupe de classes de $\mathbb{Q}(\sqrt{2},\sqrt{p})$ ; ainsi la classe $[\mathcal{G}_1]$ n'est pas un carré dans $C_{\mathbf{k}^*,2}$. D'où le résultat énoncé. ∎

Lemme 6. *Soit $L/k$ une extension quadratique non ramifiée telle que la suite des 2-corps de Hilbert de $k$ s'arrête en $k_2^{(1)}$. Alors $\mathcal{N}_{L/k}(C_{L,2}) \simeq C_{L,2}$.*

*Démonstration.* Montrons que l'homomorphisme suivant est injectif :

$$C_{L,2} \to C_{k,2}, \qquad c \mapsto \mathcal{N}_{L/k}(c).$$

Comme $L$ est une extension non ramifiée de $k$, d'après la théorie des corps de classes on a

$$[C_{k,2} : \mathcal{N}_{L/k}(C_{L,2})] = [L : k] = 2,$$

ce qui implique que

$$|\mathcal{N}_{L/k}(C_{L,2})| = h(k)/2.$$

Puisque la suite des 2-corps de Hilbert de $k$ s'arrête en $k_2^{(1)}$ et que $L$ est une extension quadratique non ramifiée de $k$, on a

$$h(L) = h(k)/2.$$

Ceci prouve que $h(L) = |\mathcal{N}_{L/k}(C_{L,2})|$, par suite $\mathcal{N}_{L/k}$ est injectif et

$$\mathcal{N}_{L/k}(C_{L,2}) \simeq C_{L,2}. \ ∎$$

Théorème 11. *Soient $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ avec $p = c^2 - 32d^2$ un nombre premier tel que $p \equiv 1 \bmod 8$, $\pi = c + 4d\sqrt{2} > 0$, $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$, $\mathbf{k}_2^{(1)}$ le 2-corps de classes de Hilbert de $\mathbf{k}$, $\mathbf{k}_2^{(2)}$ le 2-corps de classes de Hilbert de $\mathbf{k}_2^{(1)}$ et $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$. Alors $G$ est métacyclique non modulaire et la*

*suite des* 2*-corps de classes de Hilbert de* $\mathbf{k}$ (*resp.* $\mathbf{k}^*$) *s'arrête en* $\mathbf{k}_2^{(2)}$ (*resp.* $\mathbf{k}_2^{*(1)} = \mathbf{k}_2^{(2)}$).

*Démonstration.* Compte tenu des théorèmes 9 et 10, on peut conclure que le 2-groupe de classes de $\mathbf{k}^*$ est de type $(2, 2^m)$. Alors $\mathbf{k}^*$ admet trois extensions quadratiques non ramifiées. Le diagramme 1 et le théorème 6 montrent que ces trois extensions sont $\mathbf{K}_{1,4}$, $\mathbf{K}_{2,4}$ et $\mathbf{K}_{3,4}$ et donc, d'après le théorème 8, $h(\mathbf{K}_{2,4}) = h(\mathbf{k}^*)/2 = h(-p)$. Dans ce cas, la proposition 7 implique que la suite des 2-corps de classes de Hilbert de $\mathbf{k}^*$ s'arrête en $\mathbf{k}_2^{*(1)}$. Par ailleurs, il découle du lemme précédent que $\mathcal{N}_{M_i/\mathbf{k}}(C_{M_i,2}) \simeq C_{M_i,2}$, où $M_i = \mathbf{K}_{i,4}$. La théorie des corps de classes nous donne que $\mathcal{N}_{M_i/\mathbf{k}}(C_{M_i,2})$ est cyclique pour deux indices $i$. On en déduit que $M_i$ et $\mathbf{k}_2^{(1)}$ ont le même 2-corps de classes de Hilbert $\mathbf{k}_2^{(2)}$, donc $G'$ est d'ordre $h(-p)/2 \geq 4$. Par suite, $\mathbf{k}_2^{*(1)} = \mathbf{k}_2^{(2)}$ et $G$ est non modulaire. Soit $i$ tel que $M_i/\mathbf{k}$ est cyclique ; alors $H = \mathrm{Gal}(\mathbf{k}_2^{(2)}/M_i)$ est un sous-groupe cyclique normal de $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ tel que $G/H \simeq \mathrm{Gal}(M_i/\mathbf{k})$. Donc $G$ est un groupe métacyclique non modulaire, ce qui entraîne que $G'$ est cyclique, et par conséquent $\mathbf{k}_2^{(2)} = \mathbf{k}_2^{(3)}$. ∎

Lemme 7. *Soit* $L/k$ *une extension quadratique ramifiée. Alors l'homomorphisme suivant est surjectif* :

$$C_{L,2} \to C_{k,2}, \qquad c \mapsto \mathcal{N}_{L/k}(c).$$

*Démonstration.* Comme $L/k$ est ramifiée, la théorie des corps de classes implique que

$$[C_{k,2} : \mathcal{N}_{L/k}(C_{L,2})] < [L : k] = 2.$$

Autrement dit, $\mathcal{N}_{L/k}$ est surjectif. ∎

Proposition 9. *Soient* $d$ *un entier naturel sans facteurs carrés,* $k = \mathbb{Q}(\sqrt{2d}, i)$, $\varepsilon$ *l'unité fondamentale de* $k$ *et* $\mathcal{H}$ *l'idéal premier au-dessus de* $1 + i$ *dans* $k$. *Si l'indice des unités de* $k$ *est égal à* 1, *alors la classe de* $\mathcal{H}$ *dans* $k$ *est d'ordre* 2. *De plus, la classe* $\mathcal{H}$ *capitule dans* $k(\sqrt{2})$.

*Démonstration.* Même démonstration que dans [Az-00]. ∎

Théorème 12. *Soient* $\mathbf{k} = \mathbb{Q}(\sqrt{2p}, i)$ *avec* $p$ *un nombre premier tel que* $p \equiv 1 \bmod 8$, $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$, $C_{\mathbf{k},2}$ *le* 2*-groupe de classes de* $\mathbf{k}$ *et* $\mathcal{H}$ *l'idéal premier au-dessus de* $1 + i$ *dans* $\mathbf{k}$. *Alors* $C_{\mathbf{k},2} = \langle \sigma, \tau \rangle$ *avec* $\sigma^2 = [\mathcal{H}]$ (*la classe de* $\mathcal{H}$ *dans* $\mathbf{k}$) *et* $\mathcal{N}_{\mathbf{k}/\mathbb{Q}(\sqrt{2p})}(\tau) = 1$.

*Démonstration.* Comme $\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = -1$, le 2-groupe de classes de $\mathbb{Q}(\sqrt{2p})$ est cyclique d'ordre 4, engendré par une classe $c$ et

$$C_{\mathbf{k},2} = \langle \sigma, \tau \rangle \quad \text{avec} \quad \sigma^4 = \tau^2 = 1 \text{ et } \sigma\tau = \tau\sigma. \tag{7.1}$$

On note $\kappa$ le noyau de l'homomorphisme $\mathcal{N}_{\mathbf{k}/\mathbb{Q}(\sqrt{2p})}$ ; d'après le lemme précédent,

$$C_{\mathbf{k},2}/\kappa \simeq \langle c\rangle \simeq \mathbb{Z}/4\mathbb{Z}. \tag{7.2}$$

Soit $\beta$ l'idéal premier de $\mathbb{Q}(\sqrt{2p})$ au-dessus de 2. Alors

$$2=\beta^2 \text{ dans } \mathbb{Q}(\sqrt{2p}),\quad \beta=\mathcal{H}^2 \text{ dans } \mathbf{k},\quad \mathcal{N}_{\mathbf{k}/\mathbb{Q}(\sqrt{2p})}([\mathcal{H}])=[\beta].$$

Par suite, la classe de $\beta$ est d'ordre 2 dans $\mathbb{Q}(\sqrt{2p})$ (car l'unité fondamentale de $\mathbb{Q}(\sqrt{2p})$ est de norme $-1$). Ceci implique que $[\beta]=c^2$, en particulier

$$\mathcal{N}_{\mathbf{k}/\mathbb{Q}(\sqrt{2p})}([\mathcal{H}])=c^2. \tag{7.3}$$

Les résultats (7.1)–(7.3) donnent le théorème énoncé. ∎

**8. Preuve du théorème principal.** Reprenons la situation et les notations de la section 5. Alors le groupe $G=\mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ est métacyclique et non modulaire. Donnons maintenant une démonstration du théorème principal ; pour cela nous avons besoin du lemme suivant :

LEMME 8. *Soit* $\mathbf{k}=\mathbb{Q}(\sqrt{2p},i)$ *avec* $p$ *un nombre premier tel que* $\left(\frac{2}{p}\right)_4=\left(\frac{p}{2}\right)_4=-1$. *Si on suppose que* $G=\langle a,b\rangle=\mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k})$ *avec* $a^2\equiv b^4\equiv 1 \bmod G'$, *alors* $ab^2=b^2a$.

*Démonstration.* Nous avons vu que la suite des 2-corps de classes de $\mathbf{k}^*$ s'arrête en $\mathbf{k}_2^{*(1)}=\mathbf{k}_2^{(2)}$ ; alors le groupe $\mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k}^*)=H_{3,2}=\langle a,b^2,G'\rangle$ est abélien, ce qui implique que $ab^2=b^2a$. ∎

*Preuve du théorème principal.* Montrons que la classe $[\mathcal{H}_i]$ de $\mathcal{H}_i$ est d'ordre 2. Comme $\pi_i$ se ramifie dans $\mathbf{k}/\mathbb{Q}(i)$ et $p$ se ramifie dans $\mathbb{Q}(\sqrt{2p})$, il existe un idéal $\mathcal{H}_i$ de $\mathbf{k}$ tel que $\mathcal{H}_i^2=(\pi_i)$ et un idéal $\beta$ de $\mathbb{Q}(\sqrt{2p})$ tel que $\beta^2=(p)$. On suppose que $\mathcal{H}_i=(y)$ pour un certain $y$ de $\mathbf{k}$. On a donc, en prenant la norme, $\mathcal{N}_{\mathbf{k}/\mathbb{Q}(\sqrt{2p})}(\mathcal{H}_i)=(x)$ pour un certain $x$ de $\mathbb{Q}(\sqrt{2p})$ et $\beta^2=(x^2)=(p)$. Cela est équivalent à l'existence d'une unité $\varepsilon$ de $\mathbb{Q}(\sqrt{2p})$ telle que $p\varepsilon=x^2$ ; alors $\varepsilon$ est égal à $\pm\varepsilon_{2p}$ où $\varepsilon_{2p}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{2p})$ ou bien $\pm1$, ce qui montre que la norme de $\varepsilon_{2p}$ est positive ou bien $p$ est un carré dans $\mathbb{Q}(\sqrt{2p})$. Cela mène à une contradiction, puisque la norme de $\varepsilon_{2p}$ vaut $-1$ et $\sqrt{p}\notin\mathbb{Q}(\sqrt{2p})$. Il s'ensuit que la classe de $\mathcal{H}_i$ est d'ordre 2.

Montrons que $\mathcal{H}_i$ et $\mathcal{H}$ représentent la même classe dans $\mathbf{k}$. Rappelons que si $L/M$ est une extension cyclique, on désigne par $\mathrm{Am}(L/M)$ le groupe de classes ambiguës et par $\mathrm{Am_f}(L/M)$ celui des classes fortement ambiguës. Alors on a

$$|\mathrm{Am}(L/M)|=|\mathrm{Am_f}(L/M)|[E_M\cap\mathcal{N}_{L/M}(L^\times):\mathcal{N}_{L/M}(E_L)],$$

où $E_L$ (resp. $E_M$) est le groupe des unités de $L$ (resp. $M$). Dans le notre cas le 2-groupe de classes de $\mathbf{k}$ est de type $(2,4)$, donc $|\mathrm{Am}(\mathbf{k}/\mathbb{Q}(i))|=4$.

De plus, $E_{\mathbf{k}}$ est engendré par $\varepsilon_{2p}$ et $i$ ; or $i$ est norme dans $\mathbf{k}/\mathbb{Q}(i)$, par suite $|\mathrm{Am_f}(\mathbf{k}/\mathbb{Q}(i))| = 2$, c'est-à-dire qu'il existe une seule classe de $\mathbf{k}$ d'ordre 2, fortement ambiguë. Comme $(\pi_i) = \mathcal{H}_i^2$ et $(1+i) = \mathcal{H}^2$, les classes de $\mathcal{H}_i$ et $\mathcal{H}$ sont fortement ambiguës. Finalement, on a $[\mathcal{H}_1] = [\mathcal{H}_2] = [\mathcal{H}]$.

Montrons que $G = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k}) = \langle a, b\rangle$ est un groupe métacyclique non modulaire où $a^{2^n} = b^4 = 1$ et $b^{-1}ab = a^{-1+k2^s}$ avec $1 < s < \alpha$ et $k$ un nombre impair. On sait d'après la proposition 9 que la classe de $\mathcal{H}$ est d'ordre 2 et capitule dans $\mathbf{k}^* = \mathbf{K}_{3,2}$. Or, on a vu (théorème 4) qu'il y a exactement deux classes qui capitulent dans $\mathbf{k}^*$, donc $\ker j_{\mathbf{k}\to\mathbf{k}^*} = [\mathcal{H}] = \sigma^2$. Par la loi de réciprocité d'Artin, on trouve que $\ker V_{G\to H_{3,2}} = b^2G'$. D'après la proposition 6 et le lemme précédent, on a $V_{G\to H_{3,2}}(b^2G') = b^{-1}b^2bb^2H'_{3,2} = b^4 = 1$, ce qui se produit seulement si $G$ est un groupe métacyclique non modulaire de type 1 ou 3 (voir proposition 4). Supposons que $G$ est de type 1, donc $b^{-1}ab = a^{-1}$. D'après la proposition 6, $V_{G\to H_{3,2}}(aG') = b^{-1}aba = a^{-1}a = 1$, ce qui implique qu'il y a exactement quatre classes qui capitulent dans $\mathbf{k}^*$, ce qui n'est pas le cas. Donc $G$ est de type 3, c'est-à-dire $G = \langle a, b\rangle$ où $a^{2^\alpha} = 1$, $b^4 = 1$, $b^{-1}ab = a^{-1+k2^s}$ avec $1 < s < \alpha$, $k$ un nombre impair, et $G$ est d'ordre $2^{\alpha+2}$. Or, on sait d'après le théorème 11 que la suite des 2-corps de classes de $\mathbf{k}^*$ s'arrête en $\mathbf{k}_2^{*(1)} = \mathbf{k}_2^{(2)}$. Alors $\mathrm{Gal}(\mathbf{k}_2^{*(1)}/\mathbf{k}^*) = \mathrm{Gal}(\mathbf{k}_2^{(2)}/\mathbf{k}^*)$. De plus, $h(\mathbf{k}^*) = 2h(-p) = 2\cdot 2^n$, par conséquent l'ordre de $G$ est égal à $2^{n+2}$ et $\alpha = n$.

Montrons que seules la classe de $\mathcal{H}$ et son carré capitulent dans chacune des trois extensions quadratiques non ramifiées de $\mathbf{k}$. On a vu que la classe de $\mathcal{H}$ et son carré capitulent dans $\mathbf{k}^*$. Calculons $V_{G\to H_{1,2}}(aG')$, $V_{G\to H_{1,2}}(b^2G')$, $V_{G\to H_{2,2}}(aG')$ et $V_{G\to H_{2,2}}(b^2G')$. Remarquons d'abord que $H_{1,2} = \langle b, G'\rangle = \langle b, a^2\rangle$, donc le groupe des commutateurs $H'_{1,2}$ est $\langle a^{-2}b^{-1}a^2b\rangle$. Comme $b^{-1}ab = a^{-1+k2^s}$, on a

$$H'_{1,2} = \langle a^{-2}a^{-2+k2^{s+1}}\rangle = \langle a^{-2+k2^s}\rangle^2 = \langle a^{-1}b^{-1}ab\rangle^2 = G'^2 = \langle a^4\rangle.$$

De la même façon, on trouve que $H'_{2,2} = \langle a^4\rangle$. Les résultats de la proposition 6 et le lemme précédent montrent que

$$V_{G\to H_{1,2}}(b^2G') = a^{-1}b^2ab^2H'_{1,2} = a^{-1}ab^2b^2H'_{1,2} = b^4H'_{1,2} = H'_{1,2} = 1.$$

Avec le même raisonnement, on montre les résultats suivants :

$$V_{G\to H_{1,2}}(aG') = a^2H'_{1,2} = V_{G\to H_{2,2}}(aG') \quad \text{et} \quad V_{G\to H_{2,2}}(b^2G') = H'_{2,2} = 1.$$

Puisque $a^2 \notin H'_{1,2}, H'_{2,2}$, par la loi de réciprocité d'Artin, seules la classe de $\mathcal{H}$ et son carré capitulent dans $\mathbf{K}_{1,2}/\mathbf{k}$ et dans $\mathbf{K}_{2,2}/\mathbf{k}$.

Montrons que les huit classes de $C_{\mathbf{k},2}$ capitulent dans les trois extensions abéliennes non ramifiées de degré 4 de $\mathbf{k}$. On peut comme précédemment montrer que $V_{G\to H_{1,4}}(aG') = V_{G\to H_{2,4}}(aG') = V_{G\to H_{3,4}}(aG') = a^{k2^{s+1}}$ et $V_{G\to H_{1,4}}(bG') = V_{G\to H_{2,4}}(bG') = V_{G\to H_{3,4}}(bG') = b^4$. Soient $F$ le corps de

genres de $\mathbf{k}/\mathbb{Q}(i)$ et $\mathrm{Am}(\mathbf{k}/\mathbb{Q}(i))$ le sous-groupe des classes ambiguës dans $\mathbf{k}/\mathbb{Q}(i)$ de $C_{\mathbf{k},2}$. Comme le nombre de classes de $\mathbb{Q}(i)$ est égal à 1, d'après la théorie des genres on a

$$\mathrm{Am}(\mathbf{k}/\mathbb{Q}(i)) \simeq \mathrm{Gal}(F/\mathbf{k}) \simeq C_{\mathbf{k},2}/(C_{\mathbf{k},2})^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

en particulier $\mathrm{Am}(\mathbf{k}/\mathbb{Q}(i)) = \langle \sigma^2, \tau \rangle$ et $F = \mathbf{K}_{3,4}$ (car $\mathbf{K}_{3,4}$ est la seule extension abélienne non ramifiée de type $(2,2)$ sur $\mathbf{k}$). Comme $\langle \sigma^2, \tau \rangle \simeq \langle b^2G', aG' \rangle$, d'après F. Terada toutes les classes ambiguës de $\mathbf{k}$ relativement à $\mathbb{Q}(i)$ capitulent dans $\mathbf{K}_{3,4}$ (voir par exemple [Su-91]). Par suite on a $\langle b^2G', aG' \rangle \subset \ker V_{G \to H_{3,4}}$. Les résultats précédents impliquent que $a^{k2^{s+1}} = 1$, par conséquent $2^n$ divise $k2^{s+1}$. Puisque $k$ est un nombre impair et $a$ d'ordre $2^n$, on trouve que $2^n$ divise $2^{s+1}$ et $n \leq s+1$ ; or on a $s \leq n-1$, ce qui prouve que $s = n-1$ et $a^{k2^{s+1}} = a^{k2^n} = b^4 = 1$, ainsi

$$V_{G \to H_{1,4}}(G/G') = V_{G \to H_{2,4}}(G/G') = V_{G \to H_{3,4}}(G/G') = 1.$$

Ceci achève la preuve du théorème principal. ∎

## Références


[Az-99] A. Azizi, *Unités de certains corps de nombres imaginaires et abéliens sur* $\mathbb{Q}$, Ann. Sci. Math. Québec 23 (1999), 87–93.

[Az-00] —, *Sur la capitulation des 2-classes d'idéaux de* $\mathbb{k} = \mathbb{Q}(\sqrt{2pq}, i)$, Acta Arith. 94 (2000), 383–399.

[Az-Mo-01] A. Azizi et A. Mouhib, *Sur le rang du 2-groupe de classes de* $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ *où* $m = 2$ *ou bien un premier* $p \equiv 1 \pmod 4$, Trans. Amer. Math. Soc. 353 (2001), 2741–2752.

[B-C-69] P. Barrucand and H. Cohn, *Note on primes of type* $x^2 + 32y^2$, *class number and residuacity*, J. Reine Angew. Math. 238 (1969), 67–70.

[Be-Le-Sn-98] E. Benjamin, F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian 2-class field tower*, J. Number Theory 73 (1998), 182–194.

[Be-Sn-94] E. Benjamin and C. Snyder, *Number fields with 2-class number isomorphic to* $(2, 2^m)$, preprint, 1994.

[Bl-58] N. Blackburn, *On prime power groups with two generators*, ibid. 54 (1958), 327–337.

[Gr-73] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier (Grenoble) 23, no. 3 (1973), 1–48.

[Gr-03] —, *Class Field Theory, from Theory to Practice*, Springer, 2003.

[Ha-85] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1985, reprint of the 1952 edition.

[H-S-82] F. P. Heider und B. Schmithals, *Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen*, J. Reine Angew. Math. 336 (1982), 1–25.

[Hi] D. Hilbert, *Über die Theorie des relativquadratischen Zahlkörper*, Math. Ann. 51 (1899), 1–127.

[Hu-67] B. Huppert, *Endliche Gruppen I*, Springer, 1967.

[Ka-73] P. Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan 25 (1973), 506–608.

[Ka-76] —, *Sur le 2-groupe de classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1976), 313–363.

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

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

[Lm-94] F. Lemmermeyer, *Kuroda's class number formula*, Acta Arith. 66 (1994), 245–260.

[Lm-95] —, *Ideal class groups of cyclotomic number fields I*, ibid. 72 (1995), 347–359.

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

[Mi-89] K. Miyake, *Algebraic investigations on Hilbert's theorem 94, the principal ideal theorem and capitulation problem*, Expo. Math. 7 (1989), 289–346.

[Ok-01] R. Okazaki, *On parities of relative class numbers of certain CM-extensions*, in: Class Field Theory—Its Centenary and Prospect (Tokyo, 1998), Adv. Stud. Pure Math. 30, Math. Soc. Japan, 2001, 419–444.

[R-R-33] L. Rédei und H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), 69–74.

[Sc-34] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. 39 (1934), 95–111.

[Se-70] J.-P. Serre, *Cours d'arithmétique*, Presses Univ. France, 1970.

[Su-91] H. Suzuki, *A generalization of Hilbert's Theorem 94*, Nagoya Math. J. 121 (1991), 161–169.

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

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

[Za-99] M. Zahidi, *Symboles des restes quadratiques et discriminants*, thèse, Univ. Limoges, France, 1999.

Département de Mathématiques
Faculté des Sciences
Université Mohammed 1
Oujda, Maroc
E-mail: abdelmalekazizi@yahoo.fr
taousm@hotmail.com

*Reçu le 8.6.2006*
*et révisé le 26.9.2007* (5216)