Rend. Istit. Mat. Univ. Trieste
Vol. XXXI, 1–24 (1999)

Les Corps $\mathbb{Q}\left(\sqrt{-p_o}, \sqrt{d}\right)$ dont les 2-groupes de Classes sont de Klein, avec $p_o \equiv 1 \mod(4)$, Premier

A. Azizi and R. Lamjoun (*)

Summary. - *Dans ce papier on donne les corps biquadratiques* $\mathbf{k}\left(\sqrt{-p_o}, \sqrt{d}\right)$, *avec* $p_0 \equiv 1 \mod(4)$ *un nombre premier et* d *un entier naturel sans facteurs carrés, dont les* 2*-groupes de classes sont isomorphes à* $\mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$.

1. Notations et Théorème Principal (P)

$\mathbb{Q}$	:	corps des nombres rationnels;
$\mathbb{Z}$	:	anneau des entiers relatifs;
p_0	:	nombre premier qui vérifie $p_0 \equiv 1 \mod(4)$;
d	:	entier naturel sans facteurs carrés;
m	:	entier relatifs sans facteurs carrés;
$\mathbf{k}$	:	corps biquadratique $\mathbb{Q}\left(\sqrt{-p_0}, \sqrt{d}\right)$;
E	:	groupe des unités de $\mathbf{k}$;
$\mathbf{k}^{(*)}$	:	corps de genre de $\mathbf{k}$;
$\mathbf{k}_2^{(1)}$	:	2-corps de classes de Hilbert de $\mathbf{k}$;
$\mathbf{k_1}$	:	corps quadratique $\mathbb{Q}(\sqrt{-p_0})$;
$\mathbf{k_2}$	:	corps quadratique $\mathbb{Q}(\sqrt{d})$;
$\mathbf{k_3}$	:	corps quadratique $\mathbb{Q}(\sqrt{-p_0 d})$;

(*) Authors' addresses: A. Azizi, Département de Mathématiques, Faculté des Sciences, Université Mohammed Premier, Oujda, Maroc.
R. Lamjoun, Département de Mathématiques, faculté des Sciences, Université Mohammed Premier, Oujda, Maroc.

$\mathcal{N}_i$	:	la norme de $\mathbf{k}$ sur $\mathbf{k}_i$ pour $i = 1, 2, 3$;
E_i	:	groupe des unités de $\mathbf{k}_i$ pour $i = 1, 2, 3$;
Q	:	l'indice $[E : E_1E_2E_3]$ du sous groupe engendré par les E_i dans le groupe E;
C	:	groupe de classes de $\mathbf{k}$;
C_2	:	2-groupe de classes de $\mathbf{k}$;
h	:	nombre de classes de $\mathbf{k}$;
h_2	:	2-nombre de classes de $\mathbf{k}$;
$C(m)$	:	groupe de classes de $\mathbb{Q}(\sqrt{m})$;
$C_2(m)$	:	2-groupe de classes de $\mathbb{Q}(\sqrt{m})$;
$h(m)$	:	nombre de classes de $\mathbb{Q}(\sqrt{m})$;
$h_2(m)$	:	2-nombre de classes de $\mathbb{Q}(\sqrt{m})$;
$\left(\frac{a}{b}\right)$	:	symbole de Legendre;
$\left(\frac{a}{b}\right)_4$	:	symbole biquadratique;
$(\alpha, \beta)_{\mathcal{P}}$	:	symbole de Hilbert en l'idéal $\mathcal{P}$;
$\Delta_{\mathbf{k}}$	:	discriminant de $\mathbf{k}$;
$e(p)$	:	indice de ramification de l'entier premier p;
ϵ_0	:	unité fondamentale de $\mathbf{k_2}$.

On va montrer le théorème principal (P) suivant:

THÉORÈME 1.1. *On suppose que* $p_0 \equiv 5 \bmod(8)$. *Alors, le groupe* C_2 *est de type* $(2, 2)$, *si et seulement si, l'une des conditions suivantes est vérifiée*

i) $d = 2$;

ii) $d = 2p$, $p \equiv -1 \bmod(4)$ *et* $-1 \in \left\{\left(\frac{p_o}{p}\right), \left(\frac{2}{p}\right)\right\}$;

iii) $d = 2p_0p$, $p \equiv 3 \bmod(8)$ *et* $\left(\frac{p}{p_o}\right) = 1$;

iv) $d = p_0p$, $p \equiv -1 \bmod(4)$ *et* $\left(\frac{p}{p_o}\right) = 1$;

v) $d = p_0p$, $p \equiv 5 \bmod(8)$ *et* $\left(\frac{p}{p_o}\right) = 1$ *et* $\left(\frac{p}{p_o}\right)_4 . \left(\frac{p_o}{p}\right)_4 = -1$.

Dans les cas i), iv) et v) on a $[\mathbf{k}_2^{(1)} : \mathbf{k}^{(*)}] = [\mathbf{k}^{(*)} : \mathbf{k}] = 2$, *par contre dans les autres cas les corps* $\mathbf{k}_2^{(1)}$ *et* $\mathbf{k}^{(*)}$ *coincident. Lorsque* $p_0 \equiv 1 \bmod(8)$ *alors le groupe* C_2 *est de type* $(2, 2)$, *si et seulement*

si, $d = p_0 p$, $p \equiv 7 \bmod(8)$ *avec* $\left(\frac{p}{p_o}\right) = -1$ *et* p_0 *ne se décompose pas en* $x^2 + 32y^2$. *Dans ces conditions* $[\mathbf{k}_2^{(1)} : \mathbf{k}^{(*)}] = [\mathbf{k}^{(*)} : \mathbf{k}] = 2$.

Le nombre p *désigne toujours un premier différent de* p_0.

2. Corps $\mathbb{Q}\left(\sqrt{-p_o}, \sqrt{d}\right)$ dont le 2-nombre de classes est égal à 4

Le corps $\mathbf{k}^{(*)}$ est l'extention maximale de $\mathbf{k}$ qui soit non ramifiée sur $\mathbf{k}$ et abélienne sur $\mathbb{Q}$, elle est contenue dans $\mathbf{k}_2^{(1)}$ l'extension maximal de $\mathbf{k}$ qui soit non ramifiée et abélienne sur $\mathbf{k}$ de degré une puissance de 2. Alors, le degré $[\mathbf{k}^{(*)} : \mathbb{Q}]$ est inférieur à celui de l'extension $\mathbf{k}_2^{(1)}/\mathbb{Q}$. De plus, le degré $[\mathbf{k}_2^{(1)} : \mathbf{k}]$ de $\mathbf{k}_2^{(1)}/\mathbf{k}$ n'est autre que l'ordre du groupe C_2. Lorsque l'ordre de C_2 est 4, alors

$$[\mathbf{k}^{(*)} : \mathbb{Q}] = [\mathbf{k}^{(*)} : \mathbf{k}].[\mathbf{k} : \mathbb{Q}] = 4.[\mathbf{k}^{(*)} : \mathbf{k}] \leq 4.[\mathbf{k}_2^{(1)} : \mathbf{k}] = 16 \qquad (1)$$

Il faut notrer que si $p_0 \equiv 5 \bmod(8)$ alors $h_2(-p_0) \equiv 2 \bmod(4)$, mais lorsque $p_0 \equiv 1 \bmod(8)$ alors $h_2(-p_0) \equiv 0 \bmod(4)$, de plus $h_2(-p_0) \equiv 0 \bmod(8)$ si et seulement si p_0 se décompose dans $\mathbb{Z}$ sous la forme $p_0 = x^2 + 32y^2$, et pour plus de détails il faut voir [2]. Donc d'après [16] voir aussi [19] on a

$$h = 1/2 Q h(-p_0) h(d) h(-p_0 d) = a Q h(d) h(-p_0 d) \quad \text{avec } a \in \mathbb{N}. \qquad (2)$$

Lorsque $p_0 \equiv 5 \bmod(8)$ alors $a = 1$.

Si $p_0 \equiv 1 \bmod(8)$ alors

$$h = 2\, a'\, Q\, h(d)\, h(-p_0 d) \quad \text{avec } a' \in \mathbb{N}. \qquad (3)$$

Si p_0 ne se décompose pas en $x^2 + 32y^2$ alors $a' = 1$. Mais lorsque p_0 se décompose sous la forme $p_0 = x^2 + 32y^2$ alors

$$h = 4\, a\text{"}\, Q\, h(d)\, h(-p_0 d) \quad \text{avec } a\text{"} \in \mathbb{N}. \qquad (4)$$

LEMME 2.1 (GAUSS). *Soit* m *un entier naturel sans facteurs carrés. Si on note par* r_m *(resp.* r_{-m}*) le nombre des premiers ramifiés dans* $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ *(resp.* $\mathbb{Q}(\sqrt{-m})/\mathbb{Q}$*) alors* $2^{r_m - 2}/h(m)$ *et* $2^{r_m - 1}/h(-m)$. *De plus* $C_2(m)$ *(resp.* $C_2(-m)$*) est le produit de* $r_m - 1$ *(resp.* $r_{-m} - 1$*) groupes cycliques.*

PROPOSITION 2.2. 1) *On suppose que* $p_0 \equiv 5 \mod(8)$, *pour que le* 2*-nombre de classes* h_2 *de* $\mathbf{k}/\mathbb{Q}$ *soit égal à* 4, *il faut que* d *ait l'une des formes:*

i) $d = p$;

ii) $d = 2p$;

iii) $d = p_0p$;

iv) $d = 2p_0p$;

v) $d \in \{2, p_0, 2p_0\}$.

2) *On suppose que* $p_0 \equiv 1 \mod(8)$ *et* p_0 *n'est pas de la forme* $p_0 = x^2 + 32y^2$, *pour que* h_2 *soit* 4, *il faut que* d *ait l'une des formes:*

i) $d = p$, *avec* $p \equiv -1 \mod(4)$;

ii) $d = p_0p$;

iii) $d \in \{2, p_0, 2p_0\}$.

3) *On suppose que* $p_0 \equiv 1 \mod(8)$ *et* p_0 *est de la forme* $p_0 = x^2 + 32y^2$, *pour que* h_2 *soit* 4, *il faut que* d *ait l'une des formes:*

i) $d = p_0p$ *avec* $p \equiv -1 \mod(4)$;

ii) $d \in \{p_0, 2p_0\}$;

où p *est un nombre premier différent de* 2 *et* p_0.

Preuve. Dans toute la preuve, p et q désignent deux nombres premiers différents de 2 et p_0. Le but est de chercher des conditions nécessaires sur d pour que $h_2 = 4$. On sait d'après [14] que

$$\prod_{p/\Delta_{\mathbf{k}}} e(p) = [\mathbf{k}^{(*)} : \mathbb{Q}]. \tag{5}$$

Donc, d'après (1), on a $\prod_{p/\Delta_{\mathbf{k}}} e(p) \leq 16$. Or l'indice de ramification $e(p)$ du nombre premier p divisant $\Delta_{\mathbf{k}}$ est égal à 2 si p est impair et $e(2)$ est égal à 2 ou à 4. Donc le nombre des premiers ramifiés dans $\mathbf{k}/\mathbb{Q}$ est inférieur ou égal à 4. Il en suit que $d = p$ ou $d =$

pq lorsque ni 2 ni p_0 ne divise d. On va montrer que le deuxième cas n'est pas valide. Supposons que $p \equiv 1 \equiv -q \bmod(4)$, donc les nombres ramifiés dans $\mathbf{k_2}/\mathbb{Q}$ (resp. $\mathbf{k_3}/\mathbb{Q}$) sont 2, p et q (resp. p_0, p et q). Alors d'après le Lemme 2.1, le nombre 2 divise $h_2(d)$ et 4 divise $h_2(-p_0 d)$ ce qui n'est pas possible d'après (2). Si maintenant $p \equiv q \equiv 1 \bmod(4)$ (de même si $p \equiv q \equiv -1 \bmod(4)$), alors les nombres ramifiés dans $\mathbf{k_3}/\mathbb{Q}$ sont 2, p_0, p et q. Donc le Lemme 2.1 permet de dire que 8 divise $h_2(-p_0 d)$ ce qui n'est pas possible d'après (2). On utilisera les mêmes méthodes pour vérifier les assertions qui restent. Lorsque p_0 divise d et d est impair alors d ne peut être que p_0 ou $p_0 p$ ou $p_0 pq$. On va montrer que le troisième cas n'est pas réalisé. Supposons que $d = p_0 pq$ alors si $p \equiv q \equiv 1 \bmod(4)$ (de même si $p \equiv q \equiv -1 \bmod(4)$) alors les nombres ramifiés dans $\mathbf{k_2}/\mathbb{Q}$ (resp. $\mathbf{k_3}/\mathbb{Q}$) sont p_0, p et q (resp. 2, p et q) donc 2 divise $h_2(d)$ et 4 divise $h_2(-p_0 d)$, ce qui n'est pas possible en tenant compte de (2). Si $p \equiv -q \equiv 1 \bmod(4)$ alors les nombres ramifiés dans $\mathbf{k_2}/\mathbb{Q}$ (resp. $\mathbf{k_3}/\mathbb{Q}$) sont 2, p_0, p et q (resp. p et q) donc 4 divise $h_2(d)$ et 2 divise $h_2(-p_0 d)$ ce qui est impossible d'après (2). Maintenant si p_0 divise d et d est pair alors $d = 2p_0$ ou $2p_0 p$ ou $2p_0 pq$. Suposons que $d = 2p_0 pq$, en étudiant les nombres ramifiés dans $\mathbf{k_2}/\mathbb{Q}$ et $\mathbf{k_3}/\mathbb{Q}$, on montre comme avant que 4 divise à la fois $h_2(d)$ et $h_2(-p_0 d)$, ce qui est impossible d'après (2). Lorsque p_0 ne divise pas d et 2 divise d alors $d = 2$ ou $d = 2p$ ou $d = 2pq$. Comme ce qui précède, on montre que lorsque $d = 2pq$ alors 2 divise $h_2(d)$ et 4 divise $h_2(-p_0 d)$ ce qui n'est pas possible. On va étudier en particulier le cas $p_0 \equiv 1 \bmod(8)$. Si $d = 2p$ (resp. $d = 2p_0 p$) alors 4 divise $h_2(-p_0 d)$ (resp. 2 divise à la fois $h_2(d)$ et $h_2(-p_0 d)$). On conclut par (3) que h_2 ne peut être 4. Si $d = p$ avec $p \equiv 1 \bmod(4)$ alors 4 divise $h(-p_0 p)$ et h_2 ne peut être 4 d'après (3). Etudiant maintenant le cas particulier $p_0 \equiv 1 \bmod(8)$ et p_0 de la forme $p_0 = x^2 + 32y^2$. Si $d = 2$ (resp. $d = p$) alors 2 divise $h_2(-p_0 d)$ et par suite h_2 ne peut être 4. Si $d = p_0 p$ avec $p \equiv 1 \bmod(4)$ alors 2 divise $h_2(-p_0 d)$ et h_2 ne peut être 4. □

REMARQUE 2.3. Si $h_2 = 4$ alors

$$[\mathbf{k}_2^{(1)} : \mathbf{k}] = 4 \geq [\mathbf{k}^{(*)} : \mathbf{k}].$$

Ainsi, par la suite on détermine les conditions nécessaires et suff-

isantes pour que h_2 soit 4, en étudiant les cas suivants:

$$\mathbf{k}^{(*)} = \mathbf{k}_2^{(1)}, \quad [\mathbf{k}^{(*)} : \mathbf{k}] = 2 \quad \text{et} \quad \mathbf{k}^{(*)} = \mathbf{k}.$$

Il faut noter que le cas $\mathbf{k}^{(*)} = \mathbf{k}$ ne peut avoir lieu que si $d = p_0$. En effet si $\mathbf{k}^{(*)} = \mathbf{k}$ alors d'après (5) on a

$$\prod_{p/\Delta_{\mathbf{k}}} e(p) \; = \; [\mathbf{k}^{(*)} : \mathbb{Q}] \; = \; 4.$$

Donc le nombre des premiers ramifiés dans $\mathbf{k}/\mathbb{Q}$ est inférieur ou égal à 2. En tenant compte de la Proposition 2.2, d est nécessairement un élément de $\{2, p_0, 2p_0\}$. Mais lorsque $d = 2$ ou $d = 2p_0$ alors $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$ puisque le nombre 2 est totalement ramifié dans $\mathbf{k}/\mathbb{Q}$. Si $d = p_0$ i.e. $\mathbf{k} = \mathbb{Q}(i, \sqrt{p_0})$ ($i^2 = -1$) alors $\mathbf{k}^{(*)} = \mathbf{k}$ et d'après [1, Théorème 2.5], le 2-nombre de classes de $\mathbf{k}$ est 4 si et seulement si $p_0 \equiv 1 \bmod(8)$ de la forme $p_0 = x^2 + 32y^2$ et $h_2(-p_0) \not\equiv 0 \bmod(16)$. D'autre part, en tenant compte de la Proposition 2.2, l'égalité $\mathbf{k}^{(*)} = \mathbf{k}_2^{(1)}$ n'est réalisable que lorsque $p_0 \equiv 5 \bmod(8)$.

1°) Cas où $\mathbf{k}^{(*)} = \mathbf{k}_2^{(1)}$

On cherchera les d pour que $h_2 = 4$ et $\mathbf{k}^{(*)} = \mathbf{k}_2^{(1)}$. D'après la Remarque 2.3, on supposera alors que $p_0 \equiv 5 \bmod(8)$. En tenant compte de la Proposition 2.2, il suffit d'étudier les formes de d suivantes:

i) $d = 2p_0p$;

ii) $d = 2p$;

où p est un nombre premier différent de 2 et p_0.

En fait se sont les seuls cas où les nombres premiers 2, p_0 et p sont ramifiés dans $\mathbf{k}/\mathbb{Q}$, avec l'indice de ramification $e(2)$ de 2 égal à 4. Donc d'après (1) et (5), si la 2-partie h_2 du nombre de classes de $\mathbf{k}/\mathbb{Q}$ est 4 alors $\mathbf{k}^{(*)} = \mathbf{k}_2^{(1)}$. Le problème est alors de chercher les p de telle sorte que $h_2 = 4$.

2.1. Cas où $d = 2p_0p$

Cas où $p \equiv -1$ mod(4)
Si $p \equiv -1$ mod(8) alors le groupe $C_2(-p_0d) = C_2(-2p)$ est cyclique d'ordre au moins 4 (voir [12]). Donc 4 divise $h(-2p)$. D'autre part, le Lemme 2.1 permet de dire que 2 divise $h_2(d)$. En tenant compte de (2) on ne peut avoir $h_2 = 4$.

Si $p \equiv 3$ mod(8) alors $h(-2p) \equiv 2$ mod(4) et $h_2(-2p) = 2$ (voir [13]). Le groupe $C_2(d)$ est isomorphe à $\mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$ et donc $h_2(d) = 2$. Donc d'après (2), pour que h_2 soit égal à 4 il faut et il suffit que Q soit égal à 1.

Cas où $p \equiv 1$ mod(4)

Il est bien connu en théorie des genres des corps quadratiques que si on écrit $m = p_0p$, alors puisque m possède $r = 2$ diviseurs premiers congru à 1 modulo 4, alors le 2-rang du groupe de classes du corps $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{2m})$ est r et $2^r = 4$ divise $h(2m) = h(d)$. Donc 4 divise $h_2(d)$. D'autre part, le Lemme 2.1 permet de dire que 2 divise $h_2(-2p)$. Ainsi, en tenant compte de (2), on ne peut avoir $h_2 = 4$.

Remarque 2.4. Si $p \equiv 1$ mod(8) alors d'après [2] le nombre premier p s'écrit de la forme $a^2 + 16b^2$. Il suit que $h(-2p) \equiv 0$ mod(4) (voir [12]) et que $h(-2p) \equiv 0$ mod(8) si et seulement si $b \equiv 0$ mod(2). Donc 4 divise $h_2(-2p)$. La référence précédente montre aussi que $C_2(2p)$ est cyclique d'ordre au moins 4, et par suite 2 divise $h_2(2p)$. Si $p \equiv 5$ mod(8) alors $h(2p) = h(-2p) \equiv 2$ mod(4) et $h_2(2p) = h_2(-2p) = 2$ (voir [12]).

2.2. Cas où $d = 2p$

Tout d'abord le Lemme 2.1 permet de dire que 4 divise $h(-2p_0p)$. Si $p \equiv 1$ mod(4) alors 2 divise $h(2p)$ (Remarque 2.4). En tenant compte de (2), on ne peut avoir $h_2 = 4$.

Si $p \equiv -1$ mod(4) alors $h(2p)$ est impair (voir [4]). D'autre part d'après [13], le groupe $C_2(-p_0d)$ est isomorphe à $\mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$ et $h_2(-p_0d) = 4$ lorsque au moins un de $\left(\frac{p_o}{p}\right)$ et $\left(\frac{2}{p}\right)$ est -1 (où $\left(\frac{p'}{q'}\right)$ désigne le symbole de Legendre si p' et q' sont impairs et le symbole de Kronecker si $p' = 2$ et q' est impair). Dans le cas contraire

$C_2(-p_0d)$ est produit de deux groupes cycliques dont au moins un est d'ordre 4 et par suite 8 divise $C_2(-p_0d)$ et h_2 ne peut être égal à 4. Ainsi d'après (2), $h_2 = 4$ si et seulement si au moins un de $\left(\frac{p_o}{p}\right)$ et $\left(\frac{2}{p}\right)$ est -1 et $Q = 1$.

Ainsi on a la proposition suivante:

PROPOSITION 2.5. *Pour que* $h_2 = 4$ *et* $\mathbf{k}_2^{(1)} = \mathbf{k}^{(*)}$ *il faut que* $p_0 \equiv 5 \mod(8)$. *De plus si* $p_0 \equiv 5 \mod(8)$ *alors,* $h_2 = 4$ *et* $\mathbf{k}_2^{(1)} = \mathbf{k}^{(*)}$ *si et seulement si l'une des deux conditions suivantes est vérifée*

i) $d = 2p_0p,\ p \equiv 3 \mod(8)$ *et* $Q = 1$*;*

ii) $d = 2p,\ p \equiv -1 \mod(4),\ -1 \in \left\{\left(\frac{p_o}{p}\right), \left(\frac{2}{p}\right)\right\}$ *et* $Q = 1$.

Dans les deux conditions p *désigne un nombre premier différent de* 2 *et* p_0.

2°) Cas où $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$

On cherchera les d pour que $h_2 = 4$ et l'indice $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$. D'après la Proposition 2.2 et la Remarque 2.3, il suffit d'étudier les formes de d suivantes:

i) $d = p$,

ii) $d = p_0p$,

iii) $d \in \{2, 2p_0\}$,

avec p désignant un nombre premier différent de p_0.

Dans les deux premiers cas les nombres premiers 2, p_0 et p sont ramifiés dans $\mathbf{k}/\mathbb{Q}$ avec un même indice de ramification qui est 2. Donc si la 2-partie h_2 du nombres de classes de $\mathbf{k}/\mathbb{Q}$ est 4, alors $[\mathbf{k}_2^{(1)} : \mathbf{k}^{(*)}] = [\mathbf{k}^{(*)} : \mathbf{k}] = 2$. Le problème est alors de chercher les p de telle sorte que $h_2 = 4$. Il faut noter que le iii) sera traité plus tard (Remarque 3.6).

2.3. Cas où $d = p$ avec $p \equiv 1 \mod(4)$

Tout d'abord $h(d)$ est impair et d'après la Proposition 2.2 pour que h_2 soit 4, il faut que $p_0 \equiv 5 \mod(8)$. Dans la suite de ce cas, on supposera que $p_0 \equiv 5 \mod(8)$.

Cas où $\left(\frac{p_o}{p}\right) = 1$
D'après [13], le groupe $C_2(-p_0 d)$ est produit de deux groupes cycliques dont un est au moins d'ordre 4. Donc, 8 divise $h(-p_0 d)$ et en tenant compte de (2), on ne peut avoir $h_2 = 4$.

Cas où $\left(\frac{p_o}{p}\right) = -1$
Si $p \equiv 5 \mod(8)$ alors d'après [13], le groupe $C_2(-p_0 d)$ est également un produit de deux groupes cycliques dont un est au moins d'ordre 4. Donc le nombre 8 divise $h(-p_0 d)$ et en tenant compte de (2), on ne peut avoir $h_2 = 4$.

Si $p \equiv 1 \mod(8)$ alors d'après [3], on a $h_2(-p_0 d) = 4$. En tenant compte de (2), on conclut que pour avoir $h_2 = 4$ il faut et il suffit que $Q = 1$.

2.4. Cas où $d = p$ avec $p \equiv -1 \mod(4)$

On note tout d'abord que $h(d) = h(p)$ est impair et que 2 divise $h(-p_0 p)$ (voir Lemme 2.1). On sait (voir [12] et [5]) d'une part que 4 divise $h(-p_0 p)$ si et seulement si $\left(\frac{p}{p_o}\right) = 1$ et d'autre part lorsque $\left(\frac{p}{p_o}\right) = 1$, 8 divise $h(-p_0 p)$ si et seulement si $\left(\frac{-p}{p_o}\right)_4 = 1$. Il en suit que, si $\left(\frac{p}{p_o}\right) = 1$ alors pour que h_2 soit 4 il faut que $p_0 \equiv 5 \mod(8)$ et $h_2 = 4$ si et seulement si $Q = 1$ et $\left(\frac{-p}{p_o}\right)_4 = -1$. On suppose maintenant que $\left(\frac{p}{p_o}\right) = -1$ alors, on conclut par (2) que si $p_0 \equiv 5 \mod(8)$ alors $h_2 = 4$ si et seulement si $Q = 2$. Si $p_0 \equiv 1 \mod(8)$ et p_0 n'est pas de la forme $p_0 = x^2 + 32y^2$ alors $h_2 = 4$ si et seulement si $Q = 1$. Si $p_0 \equiv 1 \mod(8)$ et $p_0 = x^2 + 32y^2$ alors h_2 n'est pas 4.

2.5. Cas où $d = p_0p$ avec $p \equiv +1 \mod(4)$

D'après [4], puisque $p \equiv 1 \mod(4)$ alors 2 divise $h(p_0p)$. D'autre part on sait que $h(-p) \equiv 0 \mod(2)$, et que $h(-p) \equiv 0 \mod(4)$ si et seulement si $p \equiv 1 \mod(8)$. Donc, si $p \equiv 1 \mod(8)$ alors 4 divise $h_2(-p)$. En tenant compte de (2), on ne peut avoir $h_2 = 4$.

Si $p \equiv 5 \mod(8)$ alors $h_2(-p) = 2$.

Si $\left(\frac{p}{p_0}\right) = -1$ alors, d'après ([12] et [5]) $h(p_0p) \equiv 2 \mod(4)$. Donc $h_2(p_0p) = 2$.

Si $\left(\frac{p}{p_o}\right) = 1$ alors d'après ([12] et [5]) on a $h(p_op) \equiv 2 \mod(4)$ si et seulement si $\left(\frac{p}{p_o}\right)_4.\left(\frac{p_o}{p}\right)_4 = -1$.

D'où si $\left(\frac{p}{p_o}\right)_4.\left(\frac{p_o}{p}\right)_4 \neq -1$ alors le nombre 4 divise $h(p_0p)$ et par suite h_2 ne peut être 4.

En tenant compte de la Proposition 2.2, on conclut que lorsque $d = p_0p$ avec $p \equiv 1 \mod(4)$ que, si $p_0 \equiv 5 \mod(8)$ alors $h_2 = 4$ si et seulement si

$$\begin{cases} p \equiv 5 \mod(8),\ \left(\dfrac{p}{p_o}\right) = -1 \text{ et } Q = 1 & (R_1) \\ \text{ ou} \\ p \equiv 5 \mod(8),\ \left(\dfrac{p}{p_o}\right) = 1,\ \left(\dfrac{p}{p_o}\right)_4.\left(\dfrac{p_o}{p}\right)_4 = -1 \text{ et } Q = 1. & (R_2) \end{cases}$$

Si $p_0 \equiv 1 \mod(8)$ alors on ne peut avoir $h_2 = 4$.

REMARQUE 2.6. Dans les deux cas (R_1) et (R_2) l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$ est de norme -1. Pour le premier cas, ceci résulte de [18]. Par contre pour le deuxième cas ceci résulte de [11].

2.6. Cas où $d = p_0p$ avec $p \equiv -1 \mod(4)$

Il faut noter tout d'abord que $h(-p_0d) = h(-p)$ est impair. On rappelle le résultat suivant dû à Kaplan (voir [13]), que si $d' = p'q'$ où p' et q' sont deux nombres tels que $p' \equiv -q' \equiv 1 \mod(4)$, alors 4 divise $h(d')$ si et seulement si $p' \equiv 1 \mod(8)$ et $\left(\frac{p'}{q'}\right) = 1$. Dans le cas contraire $h_2(d') = 2$. Il en suit que, si $p_0 \equiv 5 \mod(8)$ alors $h_2(d) = h_2(p_0p) = 2$ et (2) permet d'affirmer que $h_2 = 4$ si et seulement si l'indice $Q = 2$.

On suppose maintenant que $p_0 \equiv 1 \mod(8)$ et que p_0 ne se décompose pas sous la forme $p_0 = x^2 + 32y^2$. Si $\left(\frac{p_o}{p}\right) = -1$ alors $h_2(d) = h_2(p_0 p) = 2$ et (3) permet d'affirmer que $h_2 = 4$ si et seulement si l'indice $Q = 1$. Si $\left(\frac{p_o}{p}\right) = 1$ alors 4 divise $h_2(d)$ et d'après (3), h_2 ne peut être 4. Lorsque $p_0 \equiv 1 \mod(8)$ et $p_0 = x^2 + 32y^2$ alors d'après (4), h_2 ne peut être 4.

On résume les résultats trouvés dans la proposition suivante:

PROPOSITION 2.7. *On suppose que d est différent de 2 et $2p_0$. Si $p_0 \equiv 5 \mod(8)$ alors, $h_2 = 4$ et $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$ si et seulement si l'une des conditions suivantes est vérifée:*

i) $d = p,\ p \equiv 1 \mod(8),\ \left(\frac{p_o}{p}\right) = -1$ *et* $Q = 1$;

ii) $d = p,\ p \equiv -1 \mod(4),\ \left(\frac{p}{p_o}\right) = 1,\ \left(\frac{-p}{p_o}\right)_4 = -1$ *et* $Q = 1$;

iii) $d = p,\ p \equiv -1 \mod(4),\ \left(\frac{p}{p_o}\right) = -1$ *et* $Q = 2$;

iv) $d = p_0 p,\ p \equiv 5 \mod(8),\ \left(\frac{p}{p_o}\right) = -1$ *et* $Q = 1$;

v) $d = p_0 p,\ p \equiv 5 \mod(8),\ \left(\frac{p}{p_o}\right) = 1,\ \left(\frac{p}{p_o}\right)_4 . \left(\frac{p_o}{p}\right)_4 = -1$ *et* $Q = 1$;

vi) $d = p_0 p,\ p \equiv -1 \mod(4)$ *et* $Q = 2$,

où p désigne un nombre premier différent de p_0.

Si $p_0 \equiv 1 \mod(8)$ avec p_0 ne se décompose pas sous la forme $p_0 = x^2 + 32y^2$ alors $h_2 = 4$ et $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$ si et seulement si l'une des deux conditions suivantes est vérifée:

i) $d = p,\ p \equiv -1 \mod(4),\ \left(\frac{p}{p_o}\right) = -1$ *et* $Q = 1$;

ii) $d = p_0 p,\ p \equiv -1 \mod(4),\ \left(\frac{p}{p_o}\right) = -1$ *et* $Q = 1$.

Si $p_0 \equiv 1 \mod(8)$ avec la décomposition $p_0 = x^2 + 32y^2$ alors h_2 ne peut être 4.

3. Indice du groupe des unités

Le but de ce paragraphe est de déterminer l'indice Q pour les différents cas de d des Propositions 2.5 et 2.7. On commence par donner un rappel sur le lien entre le nombre de classes des corps quadratiques sur $\mathbb{Q}$ et les formes quadratiques binaires.

Rappel (voir [6], [7],[9] et [8])

Soit $\mathbf{F}$ un corps quadratique sur $\mathbb{Q}$ de discriminant d. On associe à $\mathbf{F}$ des formes quadratiques binaires de déterminant d. Une forme quadratique binaire $AX^2 + BXY + CY^2$ sera notée $[A, B, C]$ son déterminant est $B^2 - 4AC$. On ne considère que des formes "Proprement Primitives" i.e. le P.G.C.D de A, B et C est 1. Deux formes f et f' sont équivalentes (noté: $f \approx f'$) si l'on passe de l'une à l'autre par une substitution linéaire de déterminant $+1$. Les classes d'équivalences des formes de même déterminant d, positives si $d < 0$, forment un groupe (C) pour la composition (Composition Gaussienne): Deux classes $[f]$ et $[f']$ étant données, il existe des formes $\varphi = [A, B, A'C]$ et $\varphi' = [A', B, AC]$ telles que φ appartient à $[f]$ et φ' appartient à $[f']$; la classe de $\psi = [AA', B, C]$ qui est déterminée par $[f]$ et $[f']$ est dite composée ou produit de $[f]$ et $[f']$ et est notée $[f].[f']$. On note par I la classe unité de (C), qui est la classe de la forme binaire $[1, 0, -d]$. Le groupe $C(d)$ des classes d'idéaux au sens restreint de $\mathbf{F}$ est isomorphe au groupe (C) ou au quotient de (C) par un sous-groupe à trois éléments, donc leurs 2-composantes (C_2) et $C_2(d)$ sont isomorphes. Le groupe (C_2) est cyclique non trivial quand il existe, outre la classe unité, exactement une autre classe dont le carré est I. Toute classe dont le carré est I est appelée classe ambiguë.

Une forme $[A, B, C]$ est appelée forme ambiguë simple si $B = 0$ ou $B = A$ et dont le premier coefficient est positif. Il est connu (voir [9]) que lorsque d est positif, chaque classe ambiguë contient exactement deux formes ambiguë simples.

Par ailleurs puisque d est le discriminant d'un corps quadratique alors d est fondamental i.e. il n'existe pas un carré $s^2 > 1$ tel que $d/s^2 \equiv 0$ ou $1 \bmod(4)$. Donc le nombre de genre g de d est égal à $2^{\gamma-\theta-1}$ où γ est le nombre de facteurs premiers impairs de d et $\theta = 0$

ou 1 suivant que $d \equiv 1 \bmod(4)$ ou $\equiv 8, 12 \bmod(16)$. Gauss montre que g est aussi le nombre de classes ambiguë de (C), c'est aussi l'indice du genre principal (C^+) de (C). On rappelle que (C^+) est le sous groupe de (C) formé des classes qui sont des carrés. Une classe d'une forme f est dans le genre principal si les caractères génériques associés à f sont tous égals à 1.

Une forme quadratique binaire f représente un entier m de $\mathbb{Z}$ s'il existe deux entiers $x, y \in \mathbb{Z}$ tel que $f(x, y) = 1$. On dit qu'on a une représentation primitive si x et y sont premiers entre eux. On montre qu'une forme représente primitivement m si et seulement si elle est équivalente à une autre forme binaire de la forme $[m, m_1, m_2]$.

LEMME 3.1. *Soient p et q deux nombres premiers tels que $p \equiv 5 \bmod(8)$ et $q \equiv -1 \bmod(4)$. Il est clair que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ et $\left(\frac{-1}{p}\right) = 1$, de plus on a les assertions suivantes:*

i) $\left(\frac{2}{p}\right) = -1$;

ii) l'équation $px^2 - qy^2 = 1$ (equ1) *est résoluble dans* $\mathbb{Z}^2$ *si et seulement si* $\left(\frac{p}{q}\right) = 1$;

iii) l'équation $2qx^2 - py^2 = 1$ (equ2) *est résoluble dans* $\mathbb{Z}^2$ *si et seulement si* $\left(\frac{p}{q}\right) = -1$.

Preuve. On a $p^2 - 1 = (p-5)(p+5) + 24$. Puisque $p \equiv 5 \bmod(8)$ et $p+5$ est pair alors $p^2 - 1 = 16k + 24$ où $k \in \mathbb{Z}$. Donc $\left(\frac{2}{p}\right) = -1$ d'où le i). Pour montrer, dans le ii), que la condition est nécessaire il suffit de voir l'équation (equ1) dans le corps $\mathbb{Z}/q\mathbb{Z}$. Dans la suite de cette preuve les résultats rappelés sont dûs à E. Brown dans [4]. On prend $d = 4pq$ (voir le rappel donné plus haut) et on suppose que $\left(\frac{p}{q}\right) = 1$ alors, il y a quatre classes ambiguës. En étudiant les caractères génériques, qui sont $\left(\frac{m}{p}\right)$, $\left(\frac{m}{q}\right)$ et $\left(\frac{-1}{m}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{q}\right)$, des huit formes ambiguës simples f_i (voir [4]), on trouve que les classes des formes $f_1 = [1, 0, -pq]$ et $f_p = [p, 0, -q]$ sont les seules parmis celles associées aux f_i qui sont dans le genre principal. Puisque d est positif alors $f_1 \approx f_p$ et par suite f_p represente 1. Donc, il existe deux entiers relatifs x et y tels que $px^2 - qy^2 = 1$ d'où le ii). Pour montrer, dans le iii), que la condition est nécessaire il suffit de voir l'equation (equ2)

dans le corps $\mathbb{Z}/p\mathbb{Z}$. Pour vérifier la réciproque on prend $d = 8pq$ et on suppose que $\left(\frac{p}{q}\right) = -1$. On a quatre classes ambiguës. Comme plus haut, on étudie les caractères génériques des classes associées aux formes ambiguës simples g_i (voir [4]). On trouve que seulement les classes associées à $g_1 = [1, 0, -2pq]$ et $g_{-p} = [2q, 0, -p]$ qui sont dans le genre principal et par suite $g_1 \approx g_{-p}$ puisque d est positif. Donc, g_{-p} représente 1 et il existe $x, y \in \mathbb{Z}$ tels que $2qx^2 - py^2 = 1$ d'où le iii). □

LEMME 3.2 (PRO. 1.3, [1]). *Soient $\mathbf{F}_0$ un corps de nombres réels, $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\}$ un SFU (système fondamental d'unités de $\mathbf{F}_0$) formé d'éléments positifs et $\mathbf{F} = \mathbf{F}_0(\sqrt{-\alpha})$ une extension quadratique de $\mathbf{F}_0$, où α désigne un nombre positif de $\mathbf{F}_0$ sans facteurs carrés. Alors,*

i) s'il existe une une unité de la forme $\epsilon = \epsilon_1^{j_1}\epsilon_2^{j_2}\ldots\epsilon_{r-1}^{j_{r-1}}\epsilon_r$ (à une permutation près), avec les $j_i \in \{0, 1\}$, telle que $\alpha\epsilon$ est un carré dans $\mathbf{F}_0$ alors $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_{r-1}, \sqrt{-\epsilon}\}$ est un SFU de $\mathbf{F}$. Dans le cas contraire

ii) l'ensemble $\{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\}$ est un SFU de $\mathbf{F}$.

LEMME 3.3 (REM. 1.3 APP., [1]). *Soient $\mathbf{F} := \mathbb{Q}\left(\sqrt{d}, \sqrt{-d_0}\right)$ un corps biquadratique tel que d et d_0 sont des entiers naturels distincts non nuls avec en plus d sans facteurs carrés. Soit $\epsilon = s + t\sqrt{d}$ l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$. Si ϵ est de norme -1 alors $\{\epsilon\}$ est un SFU de $\mathbf{F}$. Si ϵ est de norme 1 alors, lorsque $d_0 = 1$ on a $\{\sqrt{i\epsilon}\}$ ($i^2 = -1$) est un SFU de $\mathbf{F}$ si et seulement si $s + 1$ ou $s - 1$ est un carré dans $\mathbb{N}$, et dans le cas contraire $\{\epsilon\}$ est un SFU de $\mathbf{F}$. Mais lorsque d_0 est différent de 1 alors, $\{\sqrt{-\epsilon}\}$ est un SFU de $\mathbf{F}$ si et seulement si $2d(s + 1)$ ou $2d(s - 1)$ est un carré dans $\mathbb{N}$, et dans le cas contraire $\{\epsilon\}$ est un SFU de $\mathbf{F}$.*

REMARQUE 3.4. Le Lemme 3.3 permet d'affirmer que l'indice $Q \leq 2$.

LEMME 3.5. *On suppose que $\mathcal{N}_2(\epsilon_0) = 1$ (ϵ_0 l'unité fondamentale de $\mathbf{k_2}$). Alors, l'indice $Q = 2$ si et seulement si il existe une unité ϵ de $\mathbf{k_2}$ telle que $p_0\epsilon$ est un carré dans $\mathbf{k_2}$.*

Preuve. Il faut remarquer tout d'abord que si ϵ est une unité de $\mathbf{k_2}$, alors $p_0\epsilon$ est un carré dans $\mathbf{k_2}$, si et seulement si, $p_0\epsilon^{-1}$ est un carré dans $\mathbf{k_2}$.

Il est clair, par le Lemme 3.2, que la condition est nécessaire. Réciproquement, soit $j \in \mathbb{Z}^*$ tel que $p_0\epsilon_0^j$ est un carré dans $\mathbf{k_2}$. On peut supposer que j est positif. Si j est pair, alors p_0 devient un carré dans $\mathbf{k_2}$ ce qui n'est pas possible. Donc j est impair et par suite $p_0\epsilon_0$ est un carré dans $\mathbf{k_2}$. □

On va chercher l'indice Q pour les différents cas de d des Propositions 2.5 et 2.7.

3.1. Cas où $d = p_0p$

D'après la Remarque 2.6, dans les deux cas:

i) $p_0 \equiv p \equiv 5 \mod(8)$ et $\left(\frac{p}{p_o}\right) = -1$;

ii) $p_0 \equiv p \equiv 5 \mod(8)$, $\left(\frac{p}{p_o}\right) = 1$ et $\left(\frac{p}{p_o}\right)_4.\left(\frac{p_o}{p}\right)_4 = -1$,

on a $\mathcal{N}_2(\epsilon_0) = -1$. On conclut donc, par le Lemme 3.3, que l'indice $Q = 1$.

On suppose maintenant que $p \equiv -1 \mod(4)$, donc $\mathcal{N}_2(\epsilon_0) = 1$. Si $p_0\epsilon_0$ est un carré dans $\mathbf{k_2}$, alors il existe $c, d \in \mathbb{Z}$ tels que $p_0\epsilon_0 = X^2$ avec $X = c + d\sqrt{p_0p}$. Donc, $\mathcal{N}_2(p_0\epsilon_0) = \mathcal{N}_2(X^2)$ donne $p_0^2 = (c^2 - p_0pd^2)^2$ et $c^2 - p_0pd^2 = \pm p_0$. Alors, le nombre p_0 divise c et $p_0c'^2 - pd^2 = \pm 1$ avec $c = p_0c'$. Donc $pd^2 \equiv \pm 1 \mod(p_0)$ et $\left(\frac{p}{p_o}\right) = \left(\frac{p_o}{p}\right) = 1$. Réciproquement, supposons que $\left(\frac{p}{p_o}\right) = 1$, si $p_0 \equiv 5 \mod(8)$ alors, d'après le Lemme 3.1, il existe $c_1, d_1 \in \mathbb{Z}$ tels que $p_0c_1^2 - pd_1^2 = 1$. Posons $\epsilon = (p_0c_1^2 + pd_1^2) + 2c_1d_1\sqrt{p_0p}$, on a $p_0\epsilon = X^2$ avec $X = p_0c_1 + d_1\sqrt{p_0p}$. Or $\mathcal{N}_2(X) = p_0$, donc $\mathcal{N}_2(\epsilon) = 1$ et par suite ϵ est une unité de $\mathbf{k_2}$. D'après le Lemme 3.3, on conclut que $Q = 2$. D'où, lorsque $p_0 \equiv 5 \mod(8)$ alors l'indice $Q = 2$ si et seulement si $\left(\frac{p}{p_o}\right) = 1$. Mais si $p_0 \equiv 1 \mod(8)$, ne se décompose pas en $x^2 + 32y^2$ avec $\left(\frac{p}{p_o}\right) = -1$ alors $Q = 1$.

3.2. Cas où $d = p$

Lorsque $p \equiv 1 \mod(8)$, alors $\mathcal{N}_2(\epsilon_0) = -1$. Donc, d'après le Lemme 3.3, l'indice $Q = 1$.

On suppose maintenant que $p \equiv -1 \mod(4)$, donc $\mathcal{N}_2(\epsilon_0) = 1$. Si $p_0\epsilon_0$ est un carré dans $\mathbf{k_2}$, alors il existe $c, d \in \mathbb{Z}$ tels que $p_0\epsilon_0 = (c + d\sqrt{p})^2$. Cette égalité avec $\mathcal{N}_2(p_0\epsilon_0) = \mathcal{N}_2((c + d\sqrt{p})^2)$ donne le système suivant

$$\begin{cases} p_0 a = c^2 + pd^2, \\ p_0 b = 2cd, \\ c^2 - pd^2 = \pm p_0, \end{cases} \qquad \text{avec } \epsilon_0 = a + b\sqrt{p}, \tag{6}$$

On voit que p_0 divise à la fois c et d. Mais la troisième équation du système (6) implique que p_0^2 divise p_0, ce qui est absurde. Donc, $p_0\epsilon_0$ n'est pas un carré dans $\mathbf{k_2}$ et par suite l'indice $Q = 1$.

3.3. Cas où $d = 2p_0p$

On suppose que $p_0 \equiv 5 \mod(8)$ et que $p \equiv 3 \mod(8)$, donc $\mathcal{N}_2(\epsilon_0) = 1$. Si $p_0\epsilon_0$ est un carré dans $\mathbf{k_2}$, alors il existe $c, d \in \mathbb{Z}$ tels que $p_0\epsilon_0 = X^2$ avec $X = c + d\sqrt{2p_0p}$. Donc $\mathcal{N}_2(p_0\epsilon_0) = \mathcal{N}_2(X^2)$ donne $p_0^2 = (c^2 - 2p_0pd^2)^2$ et $c^2 - 2p_0pd^2 = \pm p_0$. Alors, p_0 divise c et $p_0c'^2 - 2pd^2 = \pm 1$ avec $c = p_0c'$. Donc, $2pd^2 = \pm 1 \mod(p_0)$ et $\left(\frac{p_o}{p}\right) = \left(\frac{p}{p_o}\right) = -1$. Réciproquement si $\left(\frac{p}{p_o}\right) = -1$ alors, d'après le Lemme 3.1, il existe $c_1, d_1 \in \mathbb{Z}$ tels que $2pd_1^2 - p_0c_1^2 = 1$. Posons $\epsilon = (p_0c_1^2 + 2pd_1^2) + 2c_1d_1\sqrt{2p_0p}$, on a $p_0\epsilon = X^2$ avec $X = p_0c_1 + d_1\sqrt{2p_0p}$. Or $\mathcal{N}_2(X) = -p_0$, donc $\mathcal{N}_2(\epsilon) = 1$ et par suite ϵ est une unité de $\mathbf{k_2}$. D'après le Lemme 3.3, on conclut que $Q = 2$. D'où l'indice $Q = 2$ si et seulement si $\left(\frac{p}{p_o}\right) = -1$.

3.4. Cas où $d = 2p$

On suppose que $p \equiv -1 \mod(4)$, donc $\mathcal{N}_2(\epsilon_0) = 1$. Si $p_0\epsilon_0$ est un carré dans $\mathbf{k_2}$, alors il existe $c, d \in \mathbb{Z}$ tels que $p_0\epsilon_0 = (c + d\sqrt{2p})^2$. Cette égalité avec $\mathcal{N}_2(p_0\epsilon_0) = \mathcal{N}_2((c + d\sqrt{2p})^2)$ donne le système suivant

$$\begin{cases} p_0 a = c^2 + 2pd^2, \\ p_0 b = 2cd, \\ c^2 - 2pd^2 = \pm p_0, \end{cases} \qquad \text{avec } \epsilon_0 = a + b\sqrt{2p}, \tag{7}$$

On voit que p_0 divise à la fois c et d. Mais, la troisième équation du système (7) implique que p_0^2 divise p_0, ce qui est absurde. Donc, $p_0\epsilon_0$ n'est pas un carré dans $\mathbf{k_2}$ et par suite l'indice $Q = 1$.

REMARQUE 3.6. i) On suppose que $d = 2$. Alors d'après (2), le 2-nombre h_2 de $\mathbf{k}$ est

$$1/2Qh(-2p_0)h(2)h(-p_0) = 1/2Qh(-2p_0)h(-p_0).$$

L'unité fondamentale de $\mathbf{k_2}$ est $s + t\sqrt{2}$ avec $s = t = 1$. Donc $2d(s-1) = 0$ est un carré dans $\mathbb{N}$, donc d'après le Lemme 3.3, $Q = 2$. Par ailleurs, 2 divise à la fois $h(-2p_0)$ et $h(-p_0)$. Si $p_0 \equiv 1 \bmod(8)$ alors 4 divise $h(-p_0)$ et par suite h_2 ne peut être 4. Lorsque $p_0 \equiv 5 \bmod(8)$ on sait d'après [12] que $h_2(-2p_0) = 2$, il en suit que $h_2 = 4$ puisque $h_2(-p_0) = 2$. De plus $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$.

ii) On suppose que $d = 2p_0$, alors d'après (2), le 2-nombre h_2 de $\mathbf{k}$ est

$$1/2Qh(-2)h(2p_0)h(-p_0) = 1/2Qh(2p_0)h(-p_0).$$

On suppose que $p_0 \equiv 5 \bmod(8)$, alors l'unité fondamentale de $\mathbf{k_2}$ est de norme -1. Donc d'après le Lemme 3.3, l'indice $Q = 1$. D'autre part on sait que $h_2(2p_0) = 2$ (voir [12]) et donc $h_2 = 2$. Si $p_0 \equiv 1 \bmod(8)$, alors 4 divise $h(-p_0)$. Si l'unité fondamentale de $\mathbf{k_2}$ est de norme -1, alors d'après [12], 4 divise $h(2p_0)$ et par suite h_2 ne peut être 4.

LEMME 3.7. *Si l'unité fondamentale de* $\mathbf{k_2}$ *est de norme* 1 *alors l'indice* $Q = 2$.

Preuve. Supposons que $Q = 1$, alors d'après le Lemme 3.3, si $\epsilon = x+y\sqrt{2p_0}$ est l'unité fondamentale de $\mathbf{k_2}$, alors ni $p_0(n+1)$ ni $p_0(n-1)$ n'est un carré dans $\mathbb{N}$. Puisque la norme de ϵ est 1, alors $(x-1)(x+1) = 2p_0y^2$. Donc $p_0(x-1)\,p_0(x+1) = 2p_0y'^2$ avec $y' = p_0y$. Il en suit que

$$\begin{cases} p_0(x+1) = 2y_1^2, \\ p_0(x-1) = p_0y_2^2, \\ y' = y_1y_2, \end{cases} \quad ou \quad \begin{cases} p_0(x+1) = p_0y_2^2, \\ p_0(x-1) = 2y_1^2, \\ y' = y_1y_2. \end{cases} \tag{8}$$

Alors, en posant $X = y_1 + 1/2y_2\sqrt{2p_0}$ on a $p_0\epsilon = X^2$, ce qui est impossible d'après le Lemme 3.5. On conclut donc que $Q = 2$. □

On suppose que la norme de l'unité fondamentale de $\mathbf{k_2}$ est 1, donc $Q = 2$. Or 4 divise $h(-p_0)$ et puisque le groupe $C_2(2p_0)$ est cyclique d'ordre au moins 4 (voir [12]) alors 2 divise $h(2p_0)$. Donc h_2 ne peut être 4.

On conclut alors, en tenant compte des Propositions 2.5 et 2.7, les théorèmes suivants:

THÉORÈME 3.8. *Pour que* $h_2 = 4$ *et* $\mathbf{k}_2^{(1)} = \mathbf{k}^{(*)}$ *il faut que* $p_0 \equiv 5 \mod(8)$. *De plus, lorsque cette condition est vérifiée alors* $h_2 = 4$ *et* $\mathbf{k}_2^{(1)} = \mathbf{k}^{(*)}$, *si et seulement si, l'une des deux conditions suivantes est vérifiée:*

i) $d = 2p_0p$, $p \equiv 3 \mod(8)$ *et* $\left(\frac{p}{p_o}\right) = 1$;

ii) $d = 2p$, $p \equiv -1 \mod(4)$ *et* $-1 \in \left\{\left(\frac{p_o}{p}\right), \left(\frac{2}{p}\right)\right\}$;

où p *désigne un nombre premier différent de* p_0.

THÉORÈME 3.9. *Si* $p_0 \equiv 5 \mod(8)$ *alors,* $h_2 = 4$ *et* $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$, *si et seulement si, l'une des conditions suivantes est vérifiée:*

i) $d = 2$;

ii) $d = p$, $p \equiv 1 \mod(8)$ *et* $\left(\frac{p}{p_o}\right) = -1$;

iii) $d = p$, $p \equiv -1 \mod(4)$, $\left(\frac{p}{p_o}\right) = 1$ *et* $\left(\frac{-p}{p_o}\right)_4 = -1$;

iv) $d = p_0p$, $p \equiv -1 \mod(4)$ *et* $\left(\frac{p}{p_o}\right) = 1$;

v) $d = p_0p$, $p \equiv 5 \mod(8)$ *et* $\left(\frac{p}{p_o}\right) = -1$;

vi) $d = p_0p$, $p \equiv 5 \mod(8)$ *et* $\left(\frac{p}{p_o}\right) = 1$ *et* $\left(\frac{p}{p_o}\right)_4 . \left(\frac{p_o}{p}\right)_4 = -1$;

où p *désigne un nombre premier différent de* 2 *et* p_0.

Si $p_0 \equiv 1 \mod(8)$ *et* p_0 *ne se décompose pas en* $x^2 + 32y^2$ *alors* $h_2 = 4$ *et* $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$, *si et seulement si, l'une des deux conditions suivantes est vérifiée:*

i) $d = p$ *avec* $p \equiv -1 \mod(4)$ *et* $\left(\frac{p}{p_o}\right) = -1$;

ii) $d = p_0 p$ *avec* $p \equiv -1 \bmod(4)$ *et* $\left(\frac{p}{p_o}\right) = -1$.

Lorsque $p_0 \equiv 1 \bmod(8)$ *et* p_0 *se décompose sous la forme* $p_0 = x^2 + 32y^2$ *alors* h_2 *n'est* 4 *que lorsque* $d = p_0$ *et* $h_2(-p_0) \not\equiv 0 \bmod(16)$, *et dans ce cas* $\mathbf{k}^{(*)} = \mathbf{k}$.

4. Corps $\mathbb{Q}\left(\sqrt{-p_o}, \sqrt{d}\right)$ dont le 2-groupe de classes est de type (2,2)

Le but de ce paragraphe est de vérifier le Théorème principal (P). Soit d un entier naturel sans facteurs carrés telque $C_2 \simeq \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$. Puisque l'ordre $\mid C_2 \mid$ de C_2 est 4, alors $[\mathbf{k}^{(*)} : \mathbf{k}] \leq 4$. D'après la Remarque 2.3, le degré $[\mathbf{k}^{(*)} : \mathbf{k}]$ ne prend la valeur 1 que si $\mathbf{k} = \mathbb{Q}(i, \sqrt{p_0})$ et dans ce cas l'ordre de C_2 est 4 si et seulement si $p_0 \equiv 1 \bmod(8)$ et p_0 de la forme $p_0 = x^2 + 32y^2$ et $h_2(-p_0) \not\equiv 0 \bmod(16)$, de plus C_2 est cyclique (voir Remarque 2.2 de [1]). Donc, pour que C_2 soit du type $(2,2)$ il faut que $\mathbf{k}^{(*)} = \mathbf{k}_2^{(1)}$ ou $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$. D'après [15], on peut affirmer que lorsque $\mathbf{k}^{(*)} = \mathbf{k}_2^{(1)}$, le groupe C_2 est isomorphe à $\mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$ si et seulement si $\mid C_2 \mid = 4$. Les Théorèmes 3.8 et 3.9 donnent les d de telle sorte que la 2-partie C_2 du groupe de classes de $\mathbf{k} = \mathbb{Q}\left(\sqrt{-p_0}, \sqrt{d}\right)$ soit d'ordre 4. Ainsi, le problème qui reste est de chercher les d pour que $[\mathbf{k}^{(*)} : \mathbf{k}] = 2$ et $C_2 \simeq \mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$. L'entier d vérifie nécessairement une condition parmi celles du Théorème 3.9. Par la suite, on étudie le groupe C_2 pour chacune de ces conditions.

On énonce maintenant un théorème qui nous donne l'ordre du groupe des classes invariantes;

THÉORÈME 4.1 (PAR. 13, SATZ 13, [10]). *Soient* $\mathbf{L}/\mathbf{F}$ *une extension de corps de nombres et* $C_\mathbf{F}$ *(resp.* $C_\mathbf{L}$*) le groupe de classes de* $\mathbf{F}$ *(resp.* $\mathbf{L}$*). Soient* $E_\mathbf{F}$ *le groupe des unités de* $\mathbf{F}$, $V_\mathbf{F}$ *le sous groupe de* $E_\mathbf{F}$ *formé des éléments qui sont normes d'éléments de* $\mathbf{L}$ *et* $C'_\mathbf{L}$ *le sous groupe de* $C_\mathbf{L}$ *formé des classes qui sont stables par les éléments du groupe de Galois de* $\mathbf{L}/\mathbf{F}$. *Si on note par* r *le rang de la partie abélienne libre de* $E_\mathbf{F}$ *et* t *le nombre des idéaux premiers ramifiés dans* $\mathbf{L}/\mathbf{F}$, *alors l'ordre de* $C'_\mathbf{L}$ *est égal à* $\mid C_\mathbf{F} \mid [V_\mathbf{F} : E_\mathbf{F}^2]\, 2^{t-(r+2)}$.

LEMME 4.2. *Soient* $\mathbf{k}$ *une extension biquadratique de* $\mathbb{Q}$ *telle que le* 2*-groupe de classes* C_2 *de* $\mathbf{k}$ *est d'ordre* 4 *et* $\mathbf{F}$ *une sous-extension de* $\mathbf{k}$ *telle que l'indice* $[\mathbf{k}:\mathbf{F}]$ *est* 2. *On note par* C_2' *le sous groupe de* C_2 *formé des classes qui sont invariantes par les éléments du groupe de Galois de* $\mathbf{k}/\mathbf{F}$.

1) *Si le groupe* C_2 *est cyclique alors l'ordre* $\mid C_2' \mid$ *de* C_2' *est supérieur ou égal à* 2.

2) *Si le groupe de classes* $C_{\mathbf{F}}$ *de* $\mathbf{F}$ *est d'ordre impair alors l'ordre* $\mid \mathcal{N}_{\mathbf{k}/\mathbf{F}}(C_2) \mid$ *est* 1.

Preuve. On note par σ le générateur du groupe de Galois $\mathbf{k}/\mathbf{F}$. On suppose que C_2 est cyclique et soit $cl(\mathcal{A})$ un générateur de C_2. Si la classe $cl(\mathcal{A})$ n'est pas invariante par σ alors $cl(\mathcal{A})^\sigma = cl(\mathcal{A})^3$ et $(cl(\mathcal{A})^2)^\sigma = cl(\mathcal{A})^6 = cl(\mathcal{A})^2$. Donc $cl(\mathcal{A})^2$ est un élément de C_2' d'où le 1). On vérifie maintenant le 2); soit $cl(\mathcal{A})$ un élément de C_2. L'ordre de la classe $cl(\mathcal{A})$ est une puissance de 2, il en est de même de l'ordre de $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(cl(\mathcal{A}))$. Puisque l'ordre de $C_{\mathbf{F}}$ est impair alors $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(cl(\mathcal{A})) = \mathcal{I}$ où $\mathcal{I}$ est la classe unité. □

LEMME 4.3. *On garde les hypothèses du Lemme* 4.2. *On a les deux assertions suivantes:*

i) Si $C_2 = C_2'$ *alors, le groupe* C_2 *est de type* $(2,2)$ *si et seulement si* $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(C_2) = \{\mathcal{I}\}$*; où* $\mathcal{I}$ *est la classe unité.*

ii) Si C_2' *est contenu strictement dans* C_2 *alors, le groupe* C_2 *est de type* $(2,2)$ *si et seulement si* $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(C_2) \neq \{\mathcal{I}\}$.

Preuve. On suppose que $C_2 = C_2'$. Soit $cl(\mathcal{A})$ un élément de C_2, on a $cl(\mathcal{A})^\sigma = cl(\mathcal{A})$. De plus $cl(\mathcal{A})$ est d'ordre 2 si et seulement si $\mathcal{N}(cl(\mathcal{A})) = cl(\mathcal{A})^{\sigma+1} = cl(\mathcal{A})^\sigma cl(\mathcal{A}) = cl(\mathcal{A})^2 = \mathcal{I}$. Donc C_2 est isomorphe à $\mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$ si et seulement si $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(C_2) = \{\mathcal{I}\}$.

On suppose maintenant que $C_2 \neq C_2'$. Si C_2 est cyclique et $cl(\mathcal{A})$ un générateur de C_2 alors, $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(cl(\mathcal{A})) = cl(\mathcal{A})^3\, cl(\mathcal{A}) = \mathcal{I}$ puisque $C_2 \neq C_2'$. Donc $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(C_2) = \{\mathcal{I}\}$. Si C_2 est isomorphe à $\mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$ alors $C_2 = \{\mathcal{I}, cl(\mathcal{A}), cl(\mathcal{B}), cl(\mathcal{C})\}$, où les classes $cl(\mathcal{A})$, $cl(\mathcal{B})$ et $cl(\mathcal{C})$ sont toutes d'ordre deux. Comme $C_2 \neq C_2'$ on peut supposer que $cl(\mathcal{A})^\sigma = cl(\mathcal{B})$. Donc

$$\mathcal{N}_{\mathbf{k}/\mathbf{F}}(cl(\mathcal{A})) = cl(\mathcal{A})^{\sigma+1} = cl(\mathcal{B})\, cl(\mathcal{A}) = cl(\mathcal{C}),$$

et par suite $\mathcal{N}_{\mathbf{k}/\mathbf{F}}(C_2) \neq \{\mathcal{I}\}$. □

PROPOSITION 4.4. *On suppose que $d = p$ est un nombre premier différent de p_0. La 2-partie C_2 du groupe de classes de $\mathbf{k} = \mathbb{Q}(\sqrt{-p_0}, \sqrt{d})$ est isomorphe à $\mathbb{Z}/4.\mathbb{Z}$ dans les cas suivants:*

i) $p_0 \equiv 5 \mod(8)$ *et* $p \equiv 1 \mod(8)$ *avec* $\left(\frac{p}{p_o}\right) = -1$;

ii) $p_0 \equiv 5 \mod(8)$ *et* $p \equiv -1 \mod(4)$ *avec* $\left(\frac{p}{p_o}\right) = -\left(\frac{-p}{p_o}\right)_4 = 1$;

iii) $p_0 \equiv 1 \mod(8)$ *ne se décompose pas en* $x^2 + 32y^2$ *et* $p \equiv -1 \mod(4)$ *avec* $\left(\frac{p}{p_o}\right) = -1$.

Preuve. Tout d'abord il faut noter, pour les trois cas, que l'ordre de C_2 est 4 (voir Théorème 3.9). On désigne par C_2' le sous groupe de C_2 constitué des classes stables par le générateur σ du groupe de Galois de $\mathbf{k}/\mathbf{k_2}$. Comme le nombre de classes $h(p)$ de $\mathbf{k_2}/\mathbb{Q}$ est impair alors l'ordre de C_2' est $[\mathcal{N}_2(\mathbf{k}) \cap E_2 : E_2^2]\, 2^{t-3}$ (Théorème 4.1) où t est le nombre des idéaux ramifiés dans $\mathbf{k}/\mathbf{k_2}$. Si $p_0 \equiv 5 \mod(8)$ et $p \equiv 1 \mod(8)$ avec $\left(\frac{p}{p_o}\right) = -1$ alors les idéaux ramifiés dans $\mathbf{k}/\mathbf{k_2}$ sont l'idéal engendré par p_0, les idéaux π_1 et π_2 où π_1 et π_2 sont les idéaux premiers de $\mathbf{k_2}$ au dessus de 2. Donc $t = 3$ et l'ordre $\mid C_2' \mid = [\mathcal{N}_2(\mathbf{k}) \cap E_2 : E_2^2] \leq [E_2 : E_2^2] = 2$. Il en suit que $C_2' \neq C_2$. D'autre part, le Lemme 4.2 montre que $\mathcal{N}_2(C_2) = \{\mathcal{I}\}$ puisque $h(p)$ est impair. On conclut alors, par le Lemme 4.3, que le groupe C_2 est isomorphe à $\mathbb{Z}/4.\mathbb{Z}$. Supposons maintenant que $p_0 \equiv 5 \mod(8)$ et $p \equiv -1 \mod(4)$ avec $\left(\frac{p}{p_o}\right) = -\left(\frac{-p}{p_o}\right)_4 = 1$ alors les idéaux ramifiés dans $\mathbf{k}/\mathbf{k_2}$ sont l'idéal engendré par 2, les idéaux π_1 et π_2 de $\mathbf{k_2}$ au dessus de p_0. Donc $t = 3$ et comme pour le cas précédent on montre que le groupe C_2 est cyclique. Lorsque $p_0 \equiv 1 \mod(8)$ ne se décompose pas en $x^2 + 32y^2$ et $p \equiv -1 \mod(4)$ avec $\left(\frac{p}{p_o}\right) = -1$ alors $t = 2$ et comme dans les deux cas précédents on vérifie que C_2 est également cyclique. □

PROPOSITION 4.5. *On suppose que $p_0 \equiv 5 \mod(8)$. Soient $d = p_0 p$, avec p un nombre premier qui vérifie $p \equiv -1 \mod(4)$ et $\left(\frac{p}{p_o}\right) = 1$. Alors, le 2-groupe de classes C_2 de $\mathbf{k} = \mathbb{Q}\left(\sqrt{-p_0}, \sqrt{d}\right)$ est isomorphe à $\mathbb{Z}/2.\mathbb{Z} \times \mathbb{Z}/2.\mathbb{Z}$.*

Preuve. Tout d'abord il faut noter que le nombre de classes $h(-p)$ de $\mathbf{k_3} = \mathbb{Q}(\sqrt{-p_0 d}) = \mathbb{Q}(\sqrt{-p})$ est impair. Donc, d'après le Lemme 4.2, $\mid \mathcal{N}_3(C_2) \mid = 1$. D'autre part, le nombre t d'idéaux ramifiés dans $\mathbf{k}/\mathbf{k_3}$ dépend de p. Si $p \equiv 7 \bmod(8)$ alors $t = 4$, et si $p \equiv 3 \bmod(8)$ alors $t = 3$. Dans le premier cas, en tenant compte du Théorème 4.1, il est clair que $\mid C_2'(\mathbf{k_3}) \mid = 4$, où $C_2'(\mathbf{k_3})$ est le sous groupe de C_2 formé des classes qui sont stables par les éléments du groupe de Galois de $\mathbf{k}/\mathbf{k_3}$. Or l'ordre de C_2 est 4 (voir Théorème 3.9) donc $C_2 = C_2'(\mathbf{k_3})$. On conclut, par le Lemme 4.3, que lorsque $p \equiv 7 \bmod(8)$ le groupe C_2 est de type $(2,2)$. On suppose maintenant que $p \equiv 3 \bmod(8)$. Le Thérorème 4.1 permet d'écrire $\mid C_2'(\mathbf{k_3}) \mid = 2[V_{\mathbf{k_3}} : E_3^2]$, où $V_{\mathbf{k_3}}$ est le groupe formé des unités de $\mathbf{k_3}$ qui sont normes d'éléments de $\mathbf{k}$. Pour connaitre l'indice $[V_{\mathbf{k_3}} : E_3^2]$ On calcule le symbole de Hilbert $(-p_0, -1)_{\mathcal{P}}$ pour tout idéal premier $\mathcal{P}$ de $\mathbf{k_3}$. Soit π l'idéal premier de $\mathbf{k_3}$ au dessus de 2. Il est clair que pour tout idéal premier $\mathcal{P}$ de $\mathbf{k_3}$, différent de π, le symbole de Hilbert $(-p_0, -1)_{\mathcal{P}} = 1$. D'autre part, on a $(-p_0, -1)_{\pi}(-1, -p_0)_{\pi} = 1$ et $(-1, -p_0)_{\pi} = 1$, donc $(-p_0, -1)_{\pi} = 1$. D'où $-1 \in V_{\mathbf{k_3}}$ et $[V_{\mathbf{k_3}} : E_3^2] = 2$. On conclut que $C_2 = C_2'(\mathbf{k_3})$ et le Lemme 4.3 permet d'affirmer que le groupe C_2 est également de type $(2,2)$. □

PROPOSITION 4.6. *On suppose que* $p_0 \equiv 5 \bmod(8)$. *Soient* $d = p_0 p$ *où* p *est un nombre premier tel que* $p \equiv 5 \bmod(8)$. *Alors, on a les deux assertions suivantes.*

1) *Si* $\left(\frac{p}{p_o}\right) = -1$ *alors* C_2 *est cyclique.*

2) *Si* $\left(\frac{p}{p_o}\right) = 1$ *et* $\left(\frac{p}{p_o}\right)_4 . \left(\frac{p_o}{p}\right)_4 = -1$ *alors* C_2 *est de type* $(2,2)$.

Preuve. Dans les deux cas 1) et 2), il faut noter que l'ordre de C_2 est 4. Comme dans la preuve de la Proposition 4.5 on a $\mid \mathcal{N}_3(C_2) \mid = 1$. Soit t le nombre d'idéaux ramifiés dans $\mathbf{k}/\mathbf{k_3}$. Si $\left(\frac{p}{p_o}\right) = -1$ alors $t = 2$ et $\mid C_2'(\mathbf{k_3}) \mid = \mid \mathbf{V_{k_3}} \mid$ où $C_2'(\mathbf{k_3})$ (resp. $V_{\mathbf{k_3}}$) est le sous groupe de C_2 formé des classes qui sont stables par les éléments du groupe de Galois de $\mathbf{k}/\mathbf{k_3}$ (resp. le groupe des unités de $\mathbf{k_3}$ qui sont normes d'éléments de $\mathbf{k}$). Donc $\mid C_2'(\mathbf{k_3}) \mid \leq 2$ et le Lemme 4.3 permet d'affirmer que C_2 est cyclique. Si maintenant $\left(\frac{p}{p_o}\right) = 1$ et $\left(\frac{p}{p_o}\right)_4 . \left(\frac{p_o}{p}\right)_4 = -1$ alors $t = 3$. On montre, comme dans la preuve

de la Proposition 4.5, que $\mid C_2'(\mathbf{k_3}) \mid = 2 \mid V_{\mathbf{k_3}} \mid$ et que $-1 \in V_{\mathbf{k_3}}$. Donc $C_2'(\mathbf{k_3}) = C_2$ et d'après le Lemme 4.3, on conclut que C_2 est de type $(2,2)$. □

REMARQUE 4.7. En tenant compte des Théorèmes 3.8 et 3.9 d'une part et des Propositions 4.4, 4.5 et 4.6 d'autre part, alors pour finir la vérification du Théorème principal (P) il reste à traiter les deux cas suivants:

(i) $d = 2$ et $p_0 \equiv 5 \bmod(8)$;

(ii) $d = p_0 p$ où $p_0 \equiv 1 \bmod(8)$, ne se décompose pas en $x^2 + 32y^2$ et $p \equiv -1 \bmod(4)$ avec $\left(\frac{p}{p_o}\right) = -1$.

Supposons qu'on est dans les conditions du (i). On sait que le nombre de classes de $\mathbf{k} = \mathbb{Q}(\sqrt{-p_0}, \sqrt{2})$ est 4 (voir le Théorème 3.9) et que le nombre de classes de $\mathbf{k_2} = \mathbb{Q}(\sqrt{2})$ est $h(2) = 1$, donc d'après le Lemme 4.2, l'ordre $\mid \mathcal{N}_2(C_2) \mid$ est 1. D'autre part le nombre d'idéaux ramifés dans $\mathbf{k}/\mathbf{k_2}$ est 2. Il en suit que l'ordre de $C_2'(\mathbf{k_2})$, sous groupe de C_2 formé des classes qui sont stables par les éléments du groupe de Galois de $\mathbf{k}/\mathbf{k_2}$, est $2[V_{\mathbf{k_2}} : E_2^2]$ avec $V_{\mathbf{k_2}}$ désignant le sous groupe de E_2 formé des éléments qui sont normes d'éléments de $\mathbf{k}$. On vérifie que pour tout idéal premier $\mathcal{P}$ de $\mathbf{k_2}$, le symbole de Hilbert $(-p_0, -1)_{\mathcal{P}} = 1$. Donc, $-1 \in V_{\mathbf{k_2}}$ et par suite $C_2'(\mathbf{k_2}) = \mathbf{C_2}$. D'où le groupe C_2 est de type $(2,2)$ (voir Lemme 4.3).

Supposons maintenant qu'on est dans les conditions du (ii), alors le nombre de classes $h(-p)$ de $\mathbf{k_3}$ est impair. Si $p \equiv 3 \bmod(8)$ alors le nombre d'idéaux ramifés dans $\mathbf{k}/\mathbf{k_3}$ est $t = 2$. Donc, d'après le Théorème 4.1, l'ordre du sous groupe $C_2'(\mathbf{k_3})$, de C_2 formé des classes qui sont stables par les éléments du groupe de Galois de $\mathbf{k}/\mathbf{k_3}$, n'est pas 4. On conclut, par le Lemme 4.3, que le groupe C_2 est cyclique. Si $p \equiv 7 \bmod(8)$ alors $t = 3$ et $\mid C_2'(\mathbf{k_3}) \mid = 2 \mid V_{\mathbf{k_3}} \mid$. En calculant le symbole de Hilbert $(-p_0, -1)_{\mathcal{P}}$ pour tout idéal premier $\mathcal{P}$ de $\mathbf{k_3}$, on trouve que $-1 \in V_{\mathbf{k_3}}$ et $\mid C_2'(\mathbf{k_3}) \mid = 4$. Donc $C_2'(\mathbf{k_3}) = C_2$ et on conclut, par le Lemme 4.3, que le groupe C_2 est de type $(2,2)$.

Remerciements. Nous remercions vivement l'institut de Recherche en Mathématiques I.R.M.A.R de l'Université de Rennes1 d'avoir mis à notre disposition tous les moyens pour la réalisation de cet article.

References

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

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

[3] Brown E., *The Power of* 2 *dividing the class number of a binary quadratic discriminant*, J. Number Theory **5** (1973), 413–419.

[4] Brown E., *Class number of real quadratic number fields*, Trans. Amer. Math. Soc. **190** (1974), 99–107.

[5] Brown E., *The class number of* $\mathbb{Q}(\sqrt{-pq})$, *for* $p \equiv q \equiv 1 \bmod(4)$ *primes*, Houston J. Math. **7** (1981), 497–505.

[6] Burton W. Jones, *The arithmetic forms*, The Math. Assoc. of Am., Buffalo, Carus Monograph Series, N. 10, New York, 1950.

[7] Dirichlet P.G.L., "Werke I".

[8] Dirichlet P.G.L. and Dedekind R., "Vorlesungenüber Zahlentheorie".

[9] Gordon P., *Discriminantal divisors of binary quadratic forms*, J. Number Theory **1** (1969), 525–533.

[10] Hasse H., "Zahlbericht 3 auflage", Physica-Verlag, Würzburg-Wien, 1970.

[11] Hurrelbrink J., *On the norm of fundamental unit*, At Baton Rouge, Preprint, 1992.

[12] Kaplan P., *Divisibilité par* 8 *du nombre de classes des corps quadratiques dont le* 2*-groupe des classes est cyclique et réciprocité biquadratique*, J. Math. Soc. Japan **25** (1973), 596–607.

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

[14] Kubota T., *Über die beziehungder klassenzahlen der unterkoper des bizyklischen zahlkörpers*, Nagoya Math. J. **6** (1953), 119–127.

[15] Kubota T., *Über din bizyklischen biquadratischen zahlkörper*, Nagoya Math. J. **10** (1956), 65–85.

[16] Kuroda S., *Über die Klassenzahlen algebraischer zahlkörper*, Nagoya Math. J. **1** (1950), 1–10.

[17] Oriat B., *Relation entre les* 2*-groupes des classes d'idéaux de* $\boldsymbol{k}(\sqrt{d})$ *et* $\boldsymbol{k}(\sqrt{-d})$, Soc. Math. France, Asteérisque **41/42** (1977), 247–249.

[18] Taya H. and Terai N., *Determination of certain real quadratic fields with class number two*, Proc. Jap. Acad. A **67** (1991), 139–144.

[19] Wada H., *On the class number and the unit group of certain algebraic number fields*, Tokyo U. Fac. of Sc. J. I **13** (1966), 201–209.

Received December 6, 1997.