

## SUR UNE QUESTION DE CAPITULATION

ABDELMALEK AZIZI

(Communicated by David E. Rohrlich)

ABSTRACT. Let  $p$  and  $q$  be prime numbers such that  $p \equiv 1 \pmod{8}$ ,  $q \equiv -1 \pmod{4}$  and  $\left(\frac{p}{q}\right) = -1$ . Let  $d = pq$ ,  $\mathbf{k} = \mathbf{Q}(\sqrt{d}, i)$ , and let  $\mathbf{k}_2^{(1)}$  be the 2-Hilbert class field of  $\mathbf{k}$ ,  $\mathbf{k}_2^{(2)}$  the 2-Hilbert class field of  $\mathbf{k}_2^{(1)}$  and  $G_2$  the Galois group of  $\mathbf{k}_2^{(2)}/\mathbf{k}$ . The 2-part  $C_{\mathbf{k},2}$  of the class group of  $\mathbf{k}$  is of type  $(2, 2)$ , so  $\mathbf{k}_2^{(1)}$  contains three extensions  $\mathbf{K}_i/\mathbf{k}$ ,  $i = 1, 2, 3$ . Our goal is to study the problem of capitulation of the 2-classes of  $\mathbf{k}$  in  $\mathbf{K}_i$ ,  $i = 1, 2, 3$ , and to determine the structure of  $G_2$ .

RÉSUMÉ. Soient  $p$  et  $q$  deux nombres premiers tels que  $p \equiv 1 \pmod{8}$ ,  $q \equiv -1 \pmod{4}$  et  $\left(\frac{p}{q}\right) = -1$ ,  $d = pq$ ,  $i = \sqrt{-1}$ ,  $\mathbf{k} = \mathbf{Q}(\sqrt{d}, i)$ ,  $\mathbf{k}_2^{(1)}$  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  $G_2$  le groupe de Galois de  $\mathbf{k}_2^{(2)}/\mathbf{k}$ . La 2-partie  $C_{\mathbf{k},2}$  du groupe de classes de  $\mathbf{k}$  est de type  $(2, 2)$ , par suite  $\mathbf{k}_2^{(1)}$  contient trois extensions  $\mathbf{K}_i/\mathbf{k}$ ,  $i = 1, 2, 3$ . On s'intéresse au problème de capitulation des 2-classes de  $\mathbf{k}$  dans  $\mathbf{K}_i$ ,  $i = 1, 2, 3$ , et à déterminer la structure de  $G_2$ .

### 1. INTRODUCTION

Soient  $\mathbf{k}$  un corps de nombres de degré fini sur  $\mathbf{Q}$ ,  $\mathbf{F}$  une extension non ramifiée de  $\mathbf{k}$  et  $p$  un nombre premier. L'extension  $\mathbf{k}^{(1)}$  de  $\mathbf{k}$ , abélienne maximale et non-ramifiée pour tous les idéaux premiers, finis et infinis, est dite *corps de classes de Hilbert* de  $\mathbf{k}$ . De même l'extension  $\mathbf{k}_p^{(1)}$  de  $\mathbf{k}$  dont le degré est une puissance de  $p$ , abélienne maximale et non-ramifiée pour tous les idéaux premiers, finis et infinis, est dite  *$p$ -corps de classes de Hilbert* de  $\mathbf{k}$ .

La recherche des idéaux de  $\mathbf{k}$  qui capitulent dans  $\mathbf{F}$  (deviennent principaux dans  $\mathbf{F}$ ), a été l'objet d'étude d'un grand nombre de mathématiciens. En effet, Kronecker était parmi les premiers à avoir abordé des problèmes de capitulation dans le cas des corps quadratiques imaginaires. Dans le cas où  $\mathbf{F}$  est égal au corps de classes de Hilbert  $\mathbf{k}^{(1)}$  de  $\mathbf{k}$ , D. Hilbert avait conjecturé que toutes les classes de  $\mathbf{k}$  capitulent dans  $\mathbf{k}^{(1)}$  (théorème de l'idéal principal). La preuve de ce dernier théorème a été réduite par E. Artin à un problème de la théorie des groupes, et c'est Ph. Furtwängler qui l'avait achevée. Le théorème de l'idéal principal a été généralisé de la façon suivante: Soient  $\mathbf{k}_0$  un corps de nombres et  $\mathbf{k}/\mathbf{k}_0$  une

---

Received by the editors February 23, 2001.

2000 *Mathematics Subject Classification*. Primary 11R37.

*Key words and phrases*. Groupe des unités, système fondamental d'unités, capitulation, corps de classes de Hilbert.

extension cyclique finie. Alors toutes les classes ambiges (les classes stables par le groupe de Galois de  $\mathbf{k}/\mathbf{k}_0$ ) de  $\mathbf{k}$ , relativement à  $\mathbf{k}/\mathbf{k}_0$ , capitulent dans le corps des genres  $(\mathbf{k}/\mathbf{k}_0)^{(*)}$  de  $\mathbf{k}$  (c'est l'extension maximale non ramifiée pour tous les idéaux premiers, finis et infinis, et qui est abélienne sur  $\mathbf{k}_0$ ). Ce théorème a été conjecturé par T. Tannaka et démontré par F. Terada (voir [14]).

Le cas où  $\mathbf{F}/\mathbf{k}$  est une extension cyclique et  $[\mathbf{F} : \mathbf{k}] = p$ , un nombre premier, a été traité par Hilbert. Sa réponse est le sujet du théorème 94 qui affirme qu'il y a au moins une classe non triviale dans  $\mathbf{k}$  qui capitule dans  $\mathbf{F}$ . De plus, Hilbert avait trouvé le résultat suivant: Soient  $\sigma$  un générateur du groupe de Galois de  $\mathbf{F}/\mathbf{k}$ ,  $N$  la norme de  $\mathbf{F}/\mathbf{k}$ ,  $\mathbf{U}_0$  le groupe des unités de  $\mathbf{k}$ ,  $\mathbf{U}$  le groupe des unités de  $\mathbf{F}$  et  $\mathbf{U}^*$  le sous-groupe des unités de  $\mathbf{U}$  dont la norme, relative à l'extension  $\mathbf{F}/\mathbf{k}$ , est égale à 1. Alors le groupe des classes de  $\mathbf{k}$  qui capitulent dans  $\mathbf{F}$  est isomorphe au groupe quotient  $\mathbf{U}^*/\mathbf{U}^{1-\sigma} = \mathbf{H}^1(\mathbf{U})$ , le groupe cohomologique de  $\mathbf{U}$  de dimension 1.

A l'aide de ce théorème et de plusieurs résultats sur les groupes cohomologiques des unités, on montre le théorème suivant:

**Théorème 1.** *Soit  $\mathbf{F}/\mathbf{k}$  une extension cyclique de degré un nombre premier, alors le nombre des classes qui capitulent dans  $\mathbf{F}/\mathbf{k}$  est égal à*

$$[\mathbf{F} : \mathbf{k}][\mathbf{U}_0 : N(\mathbf{U})].$$

On trouve une preuve de ce théorème dans [9].

Dans le cas général où  $\mathbf{F}/\mathbf{k}$  est une extension abélienne  $K$ . Miyake avait conjecturé que le nombre des classes qui capitulent dans  $\mathbf{F}/\mathbf{k}$  est un multiple de  $[\mathbf{F} : \mathbf{k}]$  (voir [12]). Ceci a été démontré par H. Suzuki (voir [13]).

Plusieurs résultats ont été établis; en particulier on a: Soit  $\mathbf{k}$  tel que  $C_{\mathbf{k},2}$ , la 2-partie du groupe des classes  $C_{\mathbf{k}}$  de  $\mathbf{k}$ , est isomorphe à  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ ,  $\mathbf{k}_2^{(2)}$  le 2-corps de classes de Hilbert de  $\mathbf{k}_2^{(1)}$  et  $G_2$  le groupe de Galois de  $\mathbf{k}_2^{(2)}/\mathbf{k}$ . On sait par la théorie des corps de classes que  $Gal(\mathbf{k}_2^{(1)}/\mathbf{k}) \simeq C_{\mathbf{k},2}$ , par suite  $Gal(\mathbf{k}_2^{(1)}/\mathbf{k}) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . Alors  $\mathbf{k}_2^{(1)}$  contient trois extensions quadratiques de  $\mathbf{k}$  dénotées par  $\mathbf{K}_1$ ,  $\mathbf{K}_2$  et  $\mathbf{K}_3$ . D'après [10] on a:

**Théorème 2.** *Soient  $\mathbf{k}$  tel que  $C_{\mathbf{k},2} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  et  $G_2$  le groupe de Galois de  $\mathbf{k}_2^{(2)}/\mathbf{k}$ ; alors on a trois types de capitulation:*

*type 1: Les quatre classes de  $C_{\mathbf{k},2}$  capitulent dans chacune des extensions  $\mathbf{K}_i/\mathbf{k}$ ,  $i = 1, 2, 3$ . Ceci est possible si et seulement si  $\mathbf{k}_2^{(2)} = \mathbf{k}_2^{(1)}$ .*

*type 2: Les quatre classes de  $C_{\mathbf{k},2}$  capitulent toutes seulement dans une extension parmi les trois extensions  $\mathbf{K}_i/\mathbf{k}$ ,  $i = 1, 2, 3$ . Dans ce cas le groupe  $G_2$  est diédral.*

*type 3: Seulement deux classes capitulent dans chacune des extensions  $\mathbf{K}_i/\mathbf{k}$ ,  $i = 1, 2, 3$ . Dans ce cas le groupe  $G_2$  est semidiédral ou quaternionique.*

Dans toute la suite on désigne par  $p$  et  $q$  deux nombres premiers tels que  $p \equiv 1 \pmod{8}$ ,  $q \equiv -1 \pmod{4}$  et  $(\frac{p}{q}) = -1$ ,  $d = pq$ ,  $\mathbf{k} = \mathbf{Q}(\sqrt{d}, i)$ ,  $\mathbf{k}_2^{(1)}$  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  $G_2$  le groupe de Galois de  $\mathbf{k}_2^{(2)}/\mathbf{k}$ . On montre que l'indice  $Q$  des unités de  $\mathbf{k}$  est égal à 2; par suite, d'après [2], on a  $C_{\mathbf{k},2} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . Donc  $\mathbf{k}_2^{(1)}$  contient trois extensions quadratiques de  $\mathbf{k}$ ,  $\mathbf{K}_1$ ,  $\mathbf{K}_2$  et  $\mathbf{K}_3$ . Notre but est l'étude de la capitulation dans les trois extensions  $\mathbf{K}_i/\mathbf{k}$ ,  $i = 1, 2, 3$ .

2. UNITÉS DE CERTAINS CORPS DE NOMBRES DE DEGRÉ 8 SUR  $\mathbf{Q}$

Soient  $d_1$  et  $d_2$  deux entiers naturels sans facteurs carrés et premiers entre eux,  $d_3 = d_1d_2$ ,  $\epsilon_1$  (resp.  $\epsilon_2, \epsilon_3$ ) l'unité fondamentale de  $\mathbf{k}_1 = \mathbf{Q}(\sqrt{d_1})$  (resp.  $\mathbf{k}_2 = \mathbf{Q}(\sqrt{d_2})$ ,  $\mathbf{k}_3 = \mathbf{Q}(\sqrt{d_3})$ ),  $\mathbf{k} = \mathbf{k}_3(i)$ ,  $Q$  l'indice des unités de  $\mathbf{k}$ ,  $\mathbf{K}_0 = \mathbf{k}_1\mathbf{k}_2$ ,  $\mathbf{K} = \mathbf{K}_0(i)$ ,  $N_1$  (resp.  $N_2, N_3$ ) la norme de  $\mathbf{K}_0/\mathbf{k}_1$  (resp.  $\mathbf{K}_0/\mathbf{k}_2, \mathbf{K}_0/\mathbf{k}_3$ ) et  $\mathbf{E}_{\mathbf{k}}$  (resp.  $\mathbf{E}_{\mathbf{K}_0}, \mathbf{E}_{\mathbf{K}}$ ) le groupe des unités de  $\mathbf{k}$  (resp.  $\mathbf{K}_0, \mathbf{K}$ ).

On sait d'après [11] qu'un système fondamental d'unités (SFU) de  $\mathbf{K}_0$  est (à une permutation près) l'un des systèmes suivants:

- i)  $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ ;
- ii)  $\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_3}\}$  ( $N_2(\epsilon_3) = 1$ );
- iii)  $\{\sqrt{\epsilon_1\epsilon_2}, \epsilon_2, \epsilon_3\}$  ( $N_3(\epsilon_1) = N_3(\epsilon_2) = 1$ );
- iv)  $\{\sqrt{\epsilon_1\epsilon_2}, \sqrt{\epsilon_3}, \epsilon_2\}$  ( $N_2(\epsilon_1) = N_3(\epsilon_2) = N_2(\epsilon_3) = 1$ );
- v)  $\{\sqrt{\epsilon_1}, \sqrt{\epsilon_2}, \epsilon_3\}$  ( $N_3(\epsilon_1) = N_3(\epsilon_2) = 1$ );
- vi)  $\{\sqrt{\epsilon_1\epsilon_2}, \sqrt{\epsilon_2\epsilon_3}, \sqrt{\epsilon_1\epsilon_3}\}$  ( $N_2(\epsilon_3) = N_3(\epsilon_j) = 1, j = 1, 2$ );
- vii)  $\{\sqrt{\epsilon_1\epsilon_2\epsilon_3}, \epsilon_2, \epsilon_3\}$  ( $N_3(\epsilon_1) = N_3(\epsilon_2) = N_2(\epsilon_3) = \pm 1$ ).

D'autre part, d'après [3], on a les résultats suivants:

**R1: SFU de  $\mathbf{k} = \mathbf{Q}(\sqrt{d}, i)$  où  $d$  est un entier naturel différent de 2 et sans facteurs carrés.**

Soit  $\epsilon_0 = s + t\sqrt{d}$  l'unité fondamentale de  $\mathbf{Q}(\sqrt{d})$ .

- i) Si  $\epsilon_0$  est de norme  $-1$ , alors  $\{\epsilon_0\}$  est un SFU de  $\mathbf{Q}(\sqrt{d}, i)$  ( $Q = 1$ ).
  - ii) Si  $\epsilon_0$  est de norme 1, alors  $\{\sqrt{i\epsilon_0}\}$  est un SFU de  $\mathbf{k}$  ( $Q = 2$ ) si et seulement si  $s \pm 1$  est un carré dans  $\mathbf{N}$  (i.e. si et seulement si  $2\epsilon_0$  est un carré dans  $\mathbf{Q}(\sqrt{d})$ ).
- Dans le cas contraire,  $\{\epsilon_0\}$  est un SFU de  $\mathbf{k}$  ( $Q = 1$ ).

**R2: SFU de  $\mathbf{K}$ .**

Soient  $n$  un entier supérieur ou égal à 2 et  $\xi_n$  une racine primitive  $2^n$ -ième de l'unité. Alors

$$\xi_n = \frac{1}{2}(\mu_n + \lambda_n i),$$

où

$$\mu_n = \sqrt{2 + \mu_{n-1}}, \lambda_n = \sqrt{2 - \mu_{n-1}}, \mu_2 = 0, \lambda_2 = 2 \text{ et } \mu_3 = \lambda_3 = \sqrt{2}.$$

De plus, on a: Soient  $n_0$  le plus grand entier tel que  $\xi_{n_0}$  appartient à  $\mathbf{K}$ ,  $\{\epsilon'_1, \epsilon'_2, \epsilon'_3\}$  un SFU de  $\mathbf{K}_0$  et  $\epsilon$  une unité de  $\mathbf{K}_0$  telle que  $(2 + \mu_{n_0})\epsilon$  est un carré dans  $\mathbf{K}_0$  (si elle existe). Alors un SFU de  $\mathbf{K}$  est l'un des systèmes suivants:

- a)  $\{\epsilon'_1, \epsilon'_2, \epsilon'_3\}$  si  $\epsilon$  n'existe pas;
- b)  $\{\epsilon'_1, \epsilon'_2, \sqrt{\xi_{n_0}\epsilon}\}$  si  $\epsilon$  existe; dans ce cas on a  $\epsilon = \epsilon'_1{}^{i_1}\epsilon'_2{}^{i_2}\epsilon'_3$ , où  $i_1, i_2 \in \{0, 1\}$  (à une permutation près).

**Lemme 3.** Soient  $q$  un nombre premier impair congru à  $-1$  modulo 4 et  $\epsilon = x + y\sqrt{q}$  l'unité fondamentale de  $\mathbf{Q}(\sqrt{q})$ . Alors  $x$  est un entier naturel pair,  $x \pm 1$  est un carré dans  $\mathbf{N}$  et  $2\epsilon$  est un carré dans  $\mathbf{Q}(\sqrt{q})$ .

*Preuve.* Comme  $q \equiv -1 \pmod{4}$ , alors  $\epsilon = x + y\sqrt{q}$  est tel que  $(x, y) \in \mathbf{Z}^2$  et  $x^2 - qy^2 = 1$ . D'où  $(x+1)(x-1) = qy^2$ . Du fait que  $(x+1) - (x-1) = 2$ , le plus grand commun diviseur de  $x+1$  et  $x-1$  est un diviseur de 2. Par suite il existe  $(y_1, y_2) \in \mathbf{Z}^2$  tel que

$$\begin{cases} x-1 &= q^i 2^j y_1^2, \\ x+1 &= q^{i'} 2^j y_2^2, \end{cases} \text{ où } i, i', j \in \{0, 1\}, i + i' = 1 \text{ et } 2^j y_1 y_2 = y,$$

$$(1) \quad (y_1\sqrt{q^i 2^j} + y_2\sqrt{q^{i'} 2^j})^2 = 2\epsilon \quad \text{et} \quad \sqrt{2\epsilon} = \pm(y_1\sqrt{q^i 2^j} + y_2\sqrt{q^{i'} 2^j}).$$

Si  $x - 1$  est pair, alors  $j = 1$ . En multipliant (1) par  $\sqrt{2}$  on trouve que  $\sqrt{\epsilon} = \pm(y_1\sqrt{q^i} + y_2\sqrt{q^{i'}}) \in \mathbf{Q}(\sqrt{q})$ , puisque  $i + i' = 1$ . Comme  $\epsilon$  est l'unité fondamentale de  $\mathbf{Q}(\sqrt{q})$ , alors  $\sqrt{\epsilon} \notin \mathbf{Q}(\sqrt{q})$ , donc on a une contradiction. Par conséquent,  $x$  est pair et  $x \pm 1$  est un carré dans  $\mathbf{N}$ . De plus, comme  $x - 1$  est impair, alors  $j = 0$  et  $2\epsilon$  est un carré dans  $\mathbf{Q}(\sqrt{q})$ .  $\square$

**Théorème 4.** Soient  $p$  et  $q$  deux nombres premiers impairs tels que  $p \equiv -q \equiv 1 \pmod{4}$ ,  $\mathbf{K}_0 = \mathbf{Q}(\sqrt{p}, \sqrt{q})$ ,  $\mathbf{K} = \mathbf{K}_0(i)$  et  $\epsilon_1$  (resp.  $\epsilon_2, \epsilon_3$ ) l'unité fondamentale de  $\mathbf{Q}(\sqrt{p})$  (resp.  $\mathbf{Q}(\sqrt{q}), \mathbf{Q}(\sqrt{pq})$ ). On suppose que  $2\epsilon_3$  est un carré dans  $\mathbf{Q}(\sqrt{pq})$ . Alors un SFU de  $\mathbf{K}_0$  est  $\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_2\epsilon_3}\}$  et un SFU de  $\mathbf{K}$  est  $\{\epsilon_1, \sqrt{i\epsilon_2}, \sqrt{\epsilon_2\epsilon_3}\}$ .

*Preuve.* On sait, d'après le lemme 3, que  $2\epsilon_2$  est un carré dans  $\mathbf{Q}(\sqrt{q})$ . Comme  $2\epsilon_3$  est un carré dans  $\mathbf{Q}(\sqrt{pq})$ , alors  $\sqrt{\epsilon_2\epsilon_3}$  appartient à  $\mathbf{K}_0$ . De plus  $\sqrt{\epsilon_2} \notin \mathbf{K}_0$  et  $\sqrt{\epsilon_3} \notin \mathbf{K}_0$ . D'où un SFU de  $\mathbf{K}_0$  est  $\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_2\epsilon_3}\}$ . D'autre part  $\sqrt{2\epsilon_2} \in \mathbf{K}_0 \Leftrightarrow \sqrt{i\epsilon_2} \in \mathbf{K}$ . Par suite, d'après le résultat R2,  $\{\epsilon_1, \sqrt{i\epsilon_2}, \sqrt{\epsilon_2\epsilon_3}\}$  est un SFU de  $\mathbf{K}$ .  $\square$

*Remarque 5.* Soient  $p$  et  $q$  deux nombres premiers impairs tels que  $p \equiv 1 \pmod{8}$ ,  $q \equiv -1 \pmod{4}$  et  $\left(\frac{p}{q}\right) = -1$ , et  $\epsilon_3$  l'unité fondamentale de  $\mathbf{Q}(\sqrt{pq})$ . Alors  $2\epsilon_3$  est un carré dans  $\mathbf{Q}(\sqrt{pq})$  (c.a.d.  $Q = 2$ ).

*Preuve.* Soit  $\epsilon_3 = x + y\sqrt{pq}$ . Comme  $\epsilon_3$  est de norme 1, alors on a  $(x - 1)(x + 1) = pqy^2$ .

- a) Si  $2pq(x - 1)$  ou  $2(x - 1)$  est un carré dans  $\mathbf{N}$ , alors on a:
- Si  $2pq(x - 1)$  est un carré dans  $\mathbf{N}$ , alors il existe  $(y_1, y_2) \in \mathbf{Z}^2$  tel que

$$\begin{cases} x - 1 = 2pqy_1^2, \\ x + 1 = 2y_2^2, \end{cases} \quad \text{et} \quad \sqrt{\epsilon_3} = y_1\sqrt{pq} + y_2 \in \mathbf{k}_3.$$

Comme  $\epsilon_3$  est l'unité fondamentale de  $\mathbf{k}_3$ , alors  $\sqrt{\epsilon_3} \notin \mathbf{k}_3$ . Donc ce cas est impossible.

- Il en est de même pour le cas où  $2(x - 1)$  est un carré dans  $\mathbf{N}$ .
- b) Si  $p(x - 1)$  ou  $2p(x - 1)$  est un carré dans  $\mathbf{N}$ , alors on a:
- Si  $p(x - 1)$  est un carré dans  $\mathbf{N}$ , alors il existe  $(y_1, y_2) \in \mathbf{Z}^2$  tel que

$$\begin{cases} x - 1 = py_1^2, \\ x + 1 = qy_2^2. \end{cases}$$

Donc on a  $-2 = py_1^2 - qy_2^2$ . Ce qui implique que  $\left(\frac{p}{q}\right) = \left(\frac{-2}{p}\right) = 1$ . Ce qui n'est pas possible.

- Si  $2p(x - 1)$  est un carré dans  $\mathbf{N}$ , on obtient la même contradiction.
- c) Si  $q(x - 1)$  ou  $2q(x - 1)$  est un carré dans  $\mathbf{N}$ , alors on a:
- Si  $2q(x - 1)$  est un carré dans  $\mathbf{N}$ , alors il existe  $(y_1, y_2) \in \mathbf{Z}^2$  tel que

$$\begin{cases} x - 1 = 2qy_1^2, \\ x + 1 = 2py_2^2. \end{cases}$$

Donc on a  $1 = py_2^2 - qy_1^2$ . Ce qui implique que  $\left(\frac{p}{q}\right) = 1$ . Ce qui n'est pas possible.

- Si  $q(x - 1)$  est un carré dans  $\mathbf{N}$ , on obtient la même contradiction.

Ainsi donc  $pq(x - 1)$  ou  $(x - 1)$  est un carré dans  $\mathbf{N}$ ; ce qui est équivalent à dire que  $2\epsilon_3$  est un carré dans  $\mathbf{Q}(\sqrt{pq})$  (c.a.d.  $Q = 2$ ).  $\square$

3. CAPITULATION DANS CERTAINES EXTENSIONS QUADRATIQUES DE  $\mathbf{k}$

Soient  $p$  et  $q$  deux nombres premiers,  $d = pq$ ,  $\mathbf{k} = \mathbf{Q}(\sqrt{d}, i)$  et  $Q$  l'indice des unités de  $\mathbf{k}$ . Dans toute la suite on supposera que  $p \equiv 1 \pmod{8}$ ,  $q \equiv -1 \pmod{4}$  et  $(\frac{p}{q}) = -1$ . Comme  $Q = 2$ , alors d'après [2], la 2-partie  $\mathbf{C}_{\mathbf{k},2}$  du groupe de classes de  $\mathbf{k}$  est isomorphe à  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . Soient  $\mathbf{k}_2^{(1)}$  le 2-corps de classes de  $\mathbf{k}$  et  $\mathbf{k}^{(*)}$  le corps des genres de  $\mathbf{k}$  (c'est l'extension maximale non ramifiée pour tous les idéaux premiers, finis et infinis, et qui est abélienne sur  $\mathbf{Q}$ ). On va déduire de la section précédente quelques résultats concernant le problème de la capitulation.

Le corps des genres de  $\mathbf{k}$  est  $\mathbf{k}^{(*)} = \mathbf{Q}(\sqrt{p}, \sqrt{q}, i)$ . Soient  $\epsilon_1$  (resp.  $\epsilon_2, \epsilon_3$ ) l'unité fondamentale de  $\mathbf{Q}(\sqrt{p})$  (resp.  $\mathbf{Q}(\sqrt{q}), \mathbf{Q}(\sqrt{pq})$ ) et  $\mathbf{k}_0^{(*)}$  le sous-corps réel maximal de  $\mathbf{k}^{(*)}$ . D'après le théorème 4, on a les propriétés suivantes:

- Un SFU de  $\mathbf{k}_0^{(*)}$  est  $\{\epsilon_1, \epsilon_2, \sqrt{\epsilon_2\epsilon_3}\}$ .
- Un SFU de  $\mathbf{k}^{(*)}$  est  $\{\epsilon_1, \sqrt{i\epsilon_2}, \sqrt{\epsilon_2\epsilon_3}\}$  et un SFU de  $\mathbf{Q}(\sqrt{pq}, i)$  est  $\{\sqrt{i\epsilon_3}\}$ .

Par suite  $N(\mathbf{E}_{\mathbf{k}^{(*)}})$  est engendré par  $\{i, \epsilon_3\}$  et  $\mathbf{E}_{\mathbf{k}}$  est engendré par  $\{i, \sqrt{i\epsilon_3}\}$ . Donc  $N(\mathbf{E}_{\mathbf{k}^{(*)}}) \neq \mathbf{E}_{\mathbf{k}}$ . Il vient donc que toutes les classes de  $\mathbf{C}_{\mathbf{k},2}$  capitulent dans  $\mathbf{k}^{(*)}$ . En résumé nous avons:

**Théorème 6.** Soient  $\mathbf{k} = \mathbf{Q}(\sqrt{pq}, i)$  avec  $p$  et  $q$  deux nombres premiers tels que  $q \equiv -1 \pmod{4}, p \equiv 1 \pmod{8}, (\frac{p}{q}) = -1, \mathbf{k}^{(*)} = \mathbf{Q}(\sqrt{p}, \sqrt{q}, i)$  le corps des genres de  $\mathbf{k}$  et  $\mathbf{C}_{\mathbf{k},2}$  la 2-partie du groupe des classes au sens large de  $\mathbf{k}$ . Alors toutes les classes de  $\mathbf{C}_{\mathbf{k},2}$  capitulent dans  $\mathbf{k}^{(*)}$ .

**Théorème 7.** Soient  $\mathbf{k} = \mathbf{Q}(\sqrt{pq}, i)$  avec  $p$  et  $q$  deux premiers tels que  $p \equiv 1 \pmod{8}, q \equiv -1 \pmod{4}$  et  $(\frac{p}{q}) = -1, \mathbf{k}^{(*)} = \mathbf{Q}(\sqrt{p}, \sqrt{q}, i) = \mathbf{k}(\sqrt{p})$  le corps des genres de  $\mathbf{k}$ ,  $\mathbf{k}_2^{(1)}$  le 2-corps de classes de Hilbert de  $\mathbf{k}$  et  $\mathbf{k}_2^{(2)}$  le 2-corps de classes de Hilbert de  $\mathbf{k}_2^{(1)}$ . Alors on a

$$\mathbf{k}_2^{(2)} \neq \mathbf{k}_2^{(1)} \Leftrightarrow 4|h(\mathbf{k}^{(*)}) \Leftrightarrow p = x^2 + 32y^2.$$

*Preuve.* D'après le théorème 2,  $\mathbf{k}_2^{(2)} = \mathbf{k}_2^{(1)}$  entraîne que toutes les classes de  $\mathbf{C}_{\mathbf{k},2}$  capitulent dans toute sous-extension quadratique  $\mathbf{L}/\mathbf{k}$  de  $\mathbf{k}_2^{(1)}/\mathbf{k}$ , et  $\mathbf{k}_2^{(2)} \neq \mathbf{k}_2^{(1)}$  entraîne que toutes les classes de  $\mathbf{C}_{\mathbf{k},2}$  capitulent dans au plus une sous-extension  $\mathbf{L}/\mathbf{k}$  de  $\mathbf{k}_2^{(1)}/\mathbf{k}$ . Par suite, si dans une sous-extension  $\mathbf{L}/\mathbf{k}$  exactement deux classes de  $\mathbf{C}_{\mathbf{k},2}$  capitulent, alors  $\mathbf{k}_2^{(2)} \neq \mathbf{k}_2^{(1)}$  et il existe une extension quadratique  $\mathbf{F}$  de  $\mathbf{k}_2^{(1)}$  telle que  $\mathbf{k}_2^{(1)} \subset \mathbf{F} \subset \mathbf{k}_2^{(2)}$ . Ainsi, comme  $\mathbf{k}^{(*)} \neq \mathbf{k}_2^{(1)}, \mathbf{k}_2^{(2)} \neq \mathbf{k}_2^{(1)} \Leftrightarrow 4|h(\mathbf{k}^{(*)})$  où  $h(\mathbf{k}^{(*)})$  est le nombre de classes de  $\mathbf{k}^{(*)}$ .

On désigne par  $h(c)$  le nombre de classes au sens large de  $\mathbf{Q}(\sqrt{c})$  et par  $\mathbf{E}_c$  le groupe des unités de  $\mathbf{Q}(\sqrt{c})$ . Soient  $\mathbf{E}_{\mathbf{k}^{(*)}}$  (resp.  $\mathbf{E}_{\mathbf{k}_0^{(*)}}$ ) le groupe des unités de  $\mathbf{k}^{(*)}$  (resp.  $\mathbf{k}_0^{(*)} = \mathbf{Q}(\sqrt{p}, \sqrt{q})$ ),  $h(\mathbf{L})$  le nombre de classes d'un corps de nombres  $\mathbf{L}$ ,  $Q = [\mathbf{E}_{\mathbf{k}} : \mathbf{E}_{-1}\mathbf{E}_{pq}\mathbf{E}_{-pq}]$ ,  $Q' = [\mathbf{E}_{\mathbf{k}^{(*)}} : \mathbf{E}_{-1}\mathbf{E}_p\mathbf{E}_{-p}\mathbf{E}_q\mathbf{E}_{-q}\mathbf{E}_{pq}\mathbf{E}_{-pq}]$  et  $\epsilon_1$  (resp.  $\epsilon_2, \epsilon_3$ ) l'unité fondamentale de  $\mathbf{Q}(\sqrt{p})$  (resp.  $\mathbf{Q}(\sqrt{q}), \mathbf{Q}(\sqrt{pq})$ ). Alors d'après [15] on a

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

$$h(\mathbf{k}) = \frac{1}{2} Q h(pq)h(-pq).$$

Comme la 2-partie de  $h(\mathbf{k})$  est égale à 4 et  $Q = 2$ , alors la 2-partie de  $h(pq)h(-pq)$  est égale à 4. D'autre part, comme  $p \equiv 1 \pmod{8}$ , alors la 2-partie de  $h(-p)$  est au moins divisible par 4. Les nombres de classes  $h(p)$ ,  $h(q)$  et  $h(-q)$  sont impairs. Par suite, on a :

$$4|h(\mathbf{k}^{(*)}) \Leftrightarrow 2^5|h(-p)Q'.$$

On sait que  $\{\epsilon_1, \sqrt{i\epsilon_2}, \sqrt{\epsilon_2\epsilon_3}\}$  est un SFU de  $\mathbf{k}^{(*)}$ . Les groupes des unités  $\mathbf{E}_{-p}$ ,  $\mathbf{E}_{-q}$  et  $\mathbf{E}_{-pq}$  sont réduits à  $\{-1, 1\}$ . Donc  $Q'$  est l'indice du sous-groupe engendré par  $\{i, \epsilon_1, \epsilon_2, \epsilon_3\}$  dans  $\mathbf{E}_{\mathbf{k}^{(*)}}$ . Ainsi on a  $Q' = 4$  et  $4|h(\mathbf{k}^{(*)}) \Leftrightarrow 8|h(-p)$ . Or, d'après [6], on a  $8|h(-p) \Leftrightarrow p = x^2 + 32y^2$ . Par suite  $4|h(\mathbf{k}^{(*)}) \Leftrightarrow p = x^2 + 32y^2$ .  $\square$

**Corollaire 8.** *On garde les hypothèses du théorème précédent. Soit  $G_2$  le groupe de Galois de  $\mathbf{k}_2^{(2)}/\mathbf{k}$ . Alors le groupe  $G_2$  est de type (2, 2) ou bien diédral d'ordre  $2^m$ ,  $m > 2$ . De plus,  $G_2$  est diédral si et seulement si  $p = n^2 + 32m^2$  avec  $n$  et  $m$  deux entiers naturels; et dans ces conditions  $\mathbf{k}^{(*)}$  est l'unique extension quadratique de  $\mathbf{k}$ , contenue dans  $\mathbf{k}_2^{(1)}$ , où toutes les classes de  $\mathbf{C}_{\mathbf{k},2}$  capitulent.*

*Preuve.* C'est une conséquence des théorèmes 2 et 7.  $\square$

**Exemples numériques.** - Si  $d = 17 \times 7$ , alors le groupe  $G_2$  est de type (2, 2).

- Si  $d = 41 \times 7$ , alors le groupe  $G_2$  est diédral.

#### REFERENCES

- [1] A. Azizi, *Sur la capitulation des 2-classes d'idéaux de  $\mathbf{Q}(\sqrt{d}, i)$* . C. R. Acad. Sci. Paris, t. 325, Série I, p. 127-130, (1997). MR **98d**:11131
- [2] A. Azizi, *Sur le 2-groupe de classes d'idéaux de  $\mathbf{Q}(\sqrt{d}, i)$* . Rendiconti del circolo matematico di Palermo (2) 48 (1999), 71-92. MR **2000d**:11131
- [3] A. Azizi, *Unités de certains corps de nombres imaginaires et abéliens sur  $\mathbf{Q}$* . Annales des Sciences Mathématiques du Québec 23( 1999), no. 1, 15-21. MR **2000k**:11120
- [4] A. Azizi, *Capitulation of the 2-ideal classes of  $\mathbf{Q}(\sqrt{p_1}, \sqrt{-p_2})$* . Lecture notes in pure and applied mathematics, vol. 208, p. 13-19, 1999. MR **2000h**:11118
- [5] A. Azizi, *Capitulation des 2-classes d'idéaux de  $\mathbf{Q}(\sqrt{2pq}, i)$* . Acta Arithmetica 94 (2000), p 383 - 399. MR **2001k**:11221
- [6] P. Barruccand et H. Cohn, *Note on primes of type  $x^2 + 32y^2$ , class number, and residuacity*. J. reine angew. Math. 238 (1969), 67-70. MR **40**:2641
- [7] S. M. Chang and R. Foote, *Capitulation in Class Field Extensions of Type (p,p)*. Can. J. Math. vol 32, No.5, (1980), 1229-1243. MR **82i**:12013
- [8] H. Cohn, *The Explicit Hilbert 2-Cyclic Class Fields of  $\mathbf{Q}(\sqrt{-p})$* . J. reine angew. Math. 321 (1981), 64-77. MR **82e**:12011
- [9] F. P. Heider und B. Schmithals, *Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen*. J. reine angew. Math. 336 (1982), 1-25. MR **84g**:12002
- [10] H. Kisilevsky, *Number Fields with Class Number Congruent to 4 mod 8 and Hilbert's Theorem 94*. J. Number Theory 8, (1976), 271-279. MR **54**:5188
- [11] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*. Nagoya Math. J, 10 (1956), 65-85. MR **18**:643e
- [12] K. Miyake, *Algebraic Investigations of Hilbert's Theorem 94, the Principal Ideal Theorem and Capitulation Problem*. Expos. Math. 7 (1989), 289-346. MR **90k**:11144
- [13] H. Suzuki, *A Generalisation of Hilbert's Theorem 94*. Nagoya Math. J., vol 121 (1991). MR **92h**:11098
- [14] F. Terada, *A Principal Ideal Theorem in the Genus Fields*. Tôhoku Math. J. Second Series, vol. 23, 1971, pp. 697-718. MR **46**:5285
- [15] H. Wada, *On the Class Number and the Unit Group of Certain Algebraic Number Fields*. Tokyo U., Fac. of Sc. J., Serie I, 13 (1966), 201-209. MR **35**:5414

DÉPARTEMENT DE MATHÉMATIQUES, FACULTÉ DES SCIENCES, UNIVERSITÉ MOHAMMED I, Oujda, MAROC

*E-mail address:* azizi@sciences.univ-oujda.ac.ma