ACTA ARITHMETICA
XCIV.4 (2000)

Sur la capitulation des 2-classes d'idéaux de $\mathbb{k} = \mathbb{Q}(\sqrt{2pq}, i)$ où $p \equiv -q \equiv 1 \bmod 4$

par

Abdelmalek Azizi (Oujda)

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

La recherche des idéaux de $\mathbb{k}$ qui capitulent dans $\mathbb{F}$ (deviennent principaux dans $\mathbb{F}$) 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 $\mathbb{F}$ est égal au corps de classes de Hilbert $\mathbb{k}^{(1)}$ de $\mathbb{k}$, D. Hilbert avait conjecturé que toutes les classes de $\mathbb{k}$ capitulent dans $\mathbb{k}^{(1)}$ (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 cas où $\mathbb{F}/\mathbb{k}$ est une extension cyclique de degré un nombre premier p 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 $\mathbb{k}$ qui capitule dans $\mathbb{F}$. De plus, Hilbert avait trouvé le résultat suivant :

Soient σ un générateur du groupe de Galois de $\mathbb{F}/\mathbb{k}$, N la norme de $\mathbb{F}/\mathbb{k}$, $\mathbf{U}_0$ le groupe des unités de $\mathbb{k}$, $\mathbf{U}$ le groupe des unités de $\mathbb{F}$ et $\mathbf{U}^*$ le sous-groupe des unités de $\mathbf{U}$ dont la norme, relative à l'extension $\mathbb{F}/\mathbb{k}$, est égale à 1. Alors le groupe des classes de $\mathbb{k}$ qui capitulent dans $\mathbb{F}$ 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.

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

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

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

Théorème 1. *Soit* $\mathbb{F}/\Bbbk$ *une extension cyclique de degré un nombre premier*, *alors le nombre des classes qui capitulent dans* $\mathbb{F}/\Bbbk$ *est égal à* $[\mathbb{F}:\Bbbk][\mathbf{U}_0 : N(\mathbf{U})]$.

Soient $\Bbbk$ un corps de nombres, $\mathbf{C}_\Bbbk$ le groupe de classes de $\Bbbk$, $\mathbf{C}_2$ la 2-composante du groupe de classes de $\Bbbk$, $\Bbbk_2^{(1)}$ le 2-corps de classes de Hilbert de $\Bbbk$, $\Bbbk_2^{(2)}$ le 2-corps de classes de Hilbert de $\Bbbk_2^{(1)}$ et G_2 le groupe de Galois de $\Bbbk_2^{(2)}/\Bbbk$.

Définition 2. Soient $\mathbb{M}$ une extension cyclique non ramifiée de $\Bbbk$, $\mathbf{C}_\mathbb{M}$ le groupe de classes de $\mathbb{M}$ et $\mathbf{C}_{\Bbbk,\mathbb{M}}$ le sous-groupe de $\mathbf{C}_\Bbbk$ associé à $\mathbb{M}$ par la théorie du corps de classes. On dit que $\mathbb{M}$ est

- *de type* (A) si un élément de $\mathbf{C}_{\Bbbk,\mathbb{M}}$ capitule dans $\mathbb{M}$,
- *de type* (B) si aucun élément de $\mathbf{C}_{\Bbbk,\mathbb{M}}$ ne capitule dans $\mathbb{M}$.

Soient j l'application de $\mathbf{C}_\Bbbk$ vers $\mathbf{C}_\mathbb{M}$ qui fait correspondre à la classe d'un idéal $\mathcal{A}$ de $\Bbbk$ l'idéal engendré par $\mathcal{A}$ dans $\mathbb{M}$ et N la norme de $\mathbb{M}/\Bbbk$; alors on a :

$$\mathbb{M} \text{ est de type (A)} \Leftrightarrow |\mathrm{Ker}(j) \cap N(\mathbf{C}_\mathbb{M})| > 1,$$
$$\mathbb{M} \text{ est de type (B)} \Leftrightarrow |\mathrm{Ker}(j) \cap N(\mathbf{C}_\mathbb{M})| = 1.$$

Définition 3. Soient Q_m *le groupe des quaternions*, D_m *le groupe diédral* et S_m *le groupe semi-diédral* d'ordre 2^m. Ces groupes sont définis comme suit : chaque groupe est engendré par deux éléments x et y tels que :

$$\begin{aligned} Q_m &= \langle x, y\rangle \quad \text{où } x^{2^{m-2}} = y^2 = a,\ a^2 = 1,\ y^{-1}xy = x^{-1}, \\ D_m &= \langle x, y\rangle \quad \text{où } x^{2^{m-1}} = y^2 = 1,\ y^{-1}xy = x^{-1}, \\ S_m &= \langle x, y\rangle \quad \text{où } x^{2^{m-1}} = y^2 = 1,\ y^{-1}xy = x^{2^{m-2}-1}. \end{aligned}$$

On sait que si G_2 est d'ordre $2^m, m > 1$ et $G_2/G_2' \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, alors G_2 est isomorphe à Q_m, D_m ou S_m. Dans tous ces cas, on a $G_2' = \langle x^2\rangle$ et les trois sous-groupes d'indice 2 de G_2 sont : $H_1 = \langle x\rangle$, $H_2 = \langle x^2, y\rangle$ et $H_3 = \langle x^2, xy\rangle$. Soient $\mathbb{F}_i$ le sous-corps de $\Bbbk_2$ laissé fixe par H_i et j_i l'application j définie pour $\mathbb{M} = \mathbb{F}_i$. Si $G_2' \neq 1$, alors il existe un sous-groupe $\langle x^4\rangle$ de G_2' d'indice 2 engendré par x^4. Soit $\mathbb{L}$ le sous-corps de $\Bbbk_2$ laissé fixe par $\langle x^4\rangle$.

Théorème 4. *On suppose que* $G_2/G_2' \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Alors on a* :

(i) *Si* $\Bbbk_2 = \Bbbk_1$, *alors les corps* $\mathbb{F}_i$ *sont de type* (A), $|\mathrm{Ker}(j_i)| = 4$ *pour* $i = 1, 2, 3$ *et* $G_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(ii) *Si* $\mathrm{Gal}(\mathbb{L}/\Bbbk) \simeq Q_3$, *alors* $\mathbb{F}_i$ *est de type* (A), $|\mathrm{Ker}(j_i)| = 2$ *pour* $i = 1, 2, 3$ *et* $G_2 \simeq Q_3$.

(iii) *Si* $\mathrm{Gal}(\mathbb{L}/\Bbbk) \simeq D_3$, *alors* $\mathbb{F}_2$ *et* $\mathbb{F}_3$ *sont de type* (B) *et* $|\mathrm{Ker}(j_2)| = |\mathrm{Ker}(j_3)| = 2$. *De plus, si* $\mathbb{F}_1$ *est de type* (B) *alors* $|\mathrm{Ker}(j_1)| = 2$ *et* $G_2 \simeq S_m$. *Si* $\mathbb{F}_1$ *est de type* (A) *et* $|\mathrm{Ker}(j_1)| = 2$, *alors* $G_2 \simeq Q_m$. *Enfin si* $\mathbb{F}_1$ *est de type* (A) *et* $|\mathrm{Ker}(j_1)| = 4$, *alors* $G_2 \simeq D_m$.

On trouve plus d'informations sur ce dernier théorème dans [Ki-76]. On trouve d'autres résultats sur le problème de capitulation dans [Te-71], [Ki-76], [Mi-89], [Su-91] et [Az-97].

On désigne par p un nombre premier congru à 1 modulo 4, q un nombre premier congru à -1 modulo 4, $\Bbbk = \mathbb{Q}(\sqrt{2pq}, i)$, $\Bbbk_2^{(1)}$ le 2-corps de classes de Hilbert de $\Bbbk$, $\Bbbk_2^{(2)}$ le 2-corps de classes de Hilbert de $\Bbbk_2^{(1)}$ et G_2 le groupe de Galois de $\Bbbk_2^{(2)}/\Bbbk$. D'après [Az-93] ou [Az-99:1], on a : $\mathbf{C}_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si et seulement si au moins deux éléments de $\left\{ \left(\frac{2}{p}\right), \left(\frac{2}{q}\right), \left(\frac{p}{q}\right) \right\}$ valent -1 et l'indice Q des unités de $\mathbb{Q}(\sqrt{2pq})$ dans $\Bbbk$ est égal à 1. Dans toute la suite on va donner un ensemble de résultats pour démontrer le théorème principal suivant :

Théorème principal. *Soient* $\Bbbk = \mathbb{Q}(\sqrt{2pq}, i)$ *et* $\mathbf{C}_2$ *la* 2*-partie du groupe de classes de* $\Bbbk$. *On suppose que* $\mathbf{C}_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; *alors* $\Bbbk_2^{(1)}$ *contient trois extensions quadratiques de* $\Bbbk$, $\mathbb{K}_1$, $\mathbb{K}_2$ *et* $\mathbb{K}_3$ *où seulement deux classes de* $\mathbf{C}_2$ *capitulent et de plus* $G_2 \simeq Q_m$.

2. Unités de certains corps de nombres de degré 8 sur $\mathbb{Q}$

2.1. *Préliminaires.* Soient d_1 et d_2 deux entiers naturels sans facteurs carrés et premiers entre eux, $d_3 = d_1 d_2$, ε_1 (resp. $\varepsilon_2, \varepsilon_3$) l'unité fondamentale de $\Bbbk_1 = \mathbb{Q}(\sqrt{d_1})$ (resp. $\Bbbk_2 = \mathbb{Q}(\sqrt{d_2})$, $\Bbbk_3 = \mathbb{Q}(\sqrt{d_3})$), $\Bbbk = \Bbbk_3(i)$, $\mathbb{K}_0 = \Bbbk_1\Bbbk_2$, $\mathbb{K} = \mathbb{K}_0(i)$, N_1 (resp. N_2, N_3) la norme de $\mathbb{K}_0/\Bbbk_1$ (resp. $\mathbb{K}_0/\Bbbk_2$, $\mathbb{K}_0/\Bbbk_3$) et $\mathbf{E}_{\Bbbk}$ (resp. $\mathbf{E}_{\mathbb{K}_0}$, $\mathbf{E}_{\mathbb{K}}$) le groupe des unités de $\Bbbk$ (resp. $\mathbb{K}_0$, $\mathbb{K}$).

On sait d'après [Kur-43] qu'un système fondamental d'unités (SFU) de $\mathbb{K}_0$ est, à une permutation près des indices, l'un des systèmes suivants :

(i) $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$;
(ii) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ $(N_2(\varepsilon_3) = 1)$;
(iii) $\{\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_2, \varepsilon_3\}$ $(N_3(\varepsilon_1) = N_3(\varepsilon_2) = 1)$;
(iv) $\{\varepsilon_1, \sqrt{\varepsilon_2}, \sqrt{\varepsilon_3}\}$ $(N_1(\varepsilon_2) = N_1(\varepsilon_3) = 1)$;
(v) $\{\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}, \sqrt{\varepsilon_1\varepsilon_3}\}$ $(N_2(\varepsilon_3) = N_3(\varepsilon_j) = 1,\ j = 1, 2)$;
(vi) $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ $(N_3(\varepsilon_1) = N_3(\varepsilon_2) = N_2(\varepsilon_3) = \pm 1)$.

D'autre part, d'après [Az-93] ou [Az-99:2], on a les résultats suivants :

R1: *SFU de* $\Bbbk = \mathbb{Q}(\sqrt{d}, i)$ *où* d *est un entier naturel différent de* 2 *et sans facteurs carrés.* Soit $\varepsilon_0 = s + t\sqrt{d}$ l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$.

(i) Si ε_0 est de norme -1, alors $\{\varepsilon_0\}$ est un SFU de $\mathbb{Q}(\sqrt{d}, i)$.

(ii) Si ε_0 est de norme 1, alors $\{\sqrt{i\varepsilon_0}\}$ est un SFU de $\Bbbk$ si et seulement si $s \pm 1$ est un carré dans $\mathbb{N}$ (i.e. si et seulement si $2\varepsilon_0$ est un carré dans $\mathbb{Q}(\sqrt{d})$). Dans le cas contraire, $\{\varepsilon_0\}$ est un SFU de $\Bbbk$ (ce résultat se trouve aussi dans [Kub-56]).

R2: *SFU de* $\mathbb{K}$. Soient n un entier supérieur ou égal à 2 et ξ_n une racine primitive 2^n-ième de l'unité. Alors

$$\xi_n = \frac{1}{2}(\mu_n + \lambda_n i), \quad \text{où} \quad \mu_n = \sqrt{2 + \mu_{n-1}},\ \lambda_n = \sqrt{2 - \mu_{n-1}},$$
$$\mu_2 = 0,\ \lambda_2 = 2 \quad \text{et} \quad \mu_3 = \lambda_3 = \sqrt{2}.$$

De plus, soient n_0 le plus grand entier tel que ξ_{n_0} appartient à $\mathbb{K}$, $\{\varepsilon'_1, \varepsilon'_2, \varepsilon'_3\}$ un SFU de $\mathbb{K}_0$ et ε une unité de $\mathbb{K}_0$ telle que $(2 + \mu_{n_0})\varepsilon$ est un carré dans $\mathbb{K}_0$ (si elle existe). Alors, d'après [Az-93], l'un des systèmes suivants est un SFU de $\mathbb{K}$:

(a) $\{\varepsilon'_1, \varepsilon'_2, \varepsilon'_3\}$ si ε n'existe pas,

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

2.2. *SFU de certains corps de nombres de degré* 4 *ou* 8

LEMME 5. *Soient d un entier relatif sans facteur carré et $\varepsilon = x + y\sqrt{d}$ l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$ où x et y sont des entiers ou bien des demi-entiers. On suppose que ε est de norme* 1. *Alors* $2(x \pm 1)$ *et* $2d(x \pm 1)$ *ne sont pas des carrés dans* $\mathbb{Q}$.

Preuve. Comme
$$\sqrt{\varepsilon} = \frac{1}{2}(\sqrt{2(x+1)} + \sqrt{2(x-1)}) \quad \text{et} \quad \sqrt{2(x+1)}\sqrt{2(x-1)} = 2y\sqrt{d},$$
alors $\sqrt{2(x-1)}$ et $\sqrt{2(x+1)}$ ne sont pas des carrés dans $\mathbb{Q}$. Si $2d(x \pm 1) = s^2$, alors $\sqrt{2(x \pm 1)} = (s/d)\sqrt{d}$ appartient à $\mathbb{Q}(\sqrt{d})$ et $\sqrt{2(x \mp 1)} = 2yd/s$ appartient à $\mathbb{Q}$. Par suite $\sqrt{\varepsilon} \in \mathbb{Q}(\sqrt{d})$, donc on a une contradiction. ∎

LEMME 6. *Soient q un nombre premier impair congru à -1 modulo 4 et $\varepsilon = x + y\sqrt{q}$ l'unité fondamentale de $\mathbb{Q}(\sqrt{q})$. Alors x est un entier naturel pair, $x \pm 1$ est un carré dans $\mathbb{N}$ et 2ε est un carré dans $\mathbb{Q}(\sqrt{q})$.*

Preuve. Comme $q \equiv -1 \bmod 4$, alors $\varepsilon = x + y\sqrt{q}$ est tel que $(x, y) \in \mathbb{Z}^2$ 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 $(y_1, y_2) \in \mathbb{Z}^2$ tel que
$$\begin{cases} x - 1 = q^i 2^j y_1^2, \\ x + 1 = q^{i'} 2^j y_2^2, \end{cases}$$
où $i, i', j \in \{0, 1\}$, $i + i' = 1$ et $2^j y_1 y_2 = y$.

Si $x-1$ est pair, alors $j=1$ et $\sqrt{2(x\mp 1)}$ est un carré dans $\mathbb{N}$. D'après le lemme 5, ceci est impossible. Par conséquent, x est pair et $x\pm 1$ est un carré dans $\mathbb{N}$. De plus, comme $x-1$ est impair, alors $j=0$ et 2ε est un carré dans $\mathbb{Q}(\sqrt{q})$. ∎

Lemme 7. *Soient p un nombre premier impair et $\varepsilon = x + y\sqrt{2p}$ l'unité fondamentale de $\mathbb{Q}(\sqrt{2p})$. On suppose que ε est de norme 1. Alors $x\pm 1$ est un carré dans $\mathbb{N}$ et 2ε est un carré dans $\mathbb{Q}(\sqrt{2p})$.*

Preuve. On suppose que $x\pm 1$ n'est pas un carré dans $\mathbb{N}$. Comme $\varepsilon = x+y\sqrt{2p}$ est de norme 1, alors $(x+1)(x-1)=2py^2$. Les entiers $x+1$ et $x-1$ ont pour diviseurs communs les diviseurs de 2. Par suite on a :

$$\begin{cases} x+1 = 2y_1^2, \\ x-1 = py_2^2, \\ \quad y = y_1y_2, \end{cases} \qquad \text{ou} \qquad \begin{cases} x-1 = 2y_1^2, \\ x+1 = py_2^2, \\ \quad y = y_1y_2. \end{cases}$$

Donc $\sqrt{2(x\mp 1)}$ est un carré dans $\mathbb{N}$. D'après le lemme 5, ceci est impossible. Il vient donc que $x\pm 1$ est un carré dans $\mathbb{N}$. De plus, d'après le résultat R1, $x\pm 1$ est un carré dans $\mathbb{N}$ si et seulement si 2ε est un carré dans $\mathbb{Q}(\sqrt{2p})$. Ceci termine la preuve. ∎

Lemme 8. *Soient p et q nombres premiers impairs, $\mathbb{K}_0 = \mathbb{Q}(\sqrt{q}, \sqrt{2p})$, ε_1 (resp. ε_2, ε_3) l'unité fondamentale de $\Bbbk_1 = \mathbb{Q}(\sqrt{q})$ (resp. $\Bbbk_2 = \mathbb{Q}(\sqrt{2p})$, $\Bbbk_3 = \mathbb{Q}(\sqrt{2pq})$). On suppose que toutes les unités ε_i sont de norme 1 et que $2\varepsilon_3$ n'est pas un carré dans $\Bbbk_3$. On pose $\varepsilon_3 = x + y\sqrt{2pq}$. Alors on a :*

(i) *Si $2p(x\pm 1)$ est un carré dans $\mathbb{N}$, alors $2\varepsilon_3$ est un carré dans $\mathbb{K}_0$ et $\{\sqrt{\varepsilon_1\varepsilon_3}, \sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$.*

(ii) *Si $2q(x\pm 1)$ est un carré dans $\mathbb{N}$, alors ε_3 est un carré dans $\mathbb{K}_0$ et $\{\varepsilon_1, \sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$.*

Preuve. Soit $\varepsilon_3 = x + y\sqrt{2pq}$ tel que $(x-1)(x+1) = 2pqy^2$. On sait que $2\varepsilon_3$ est un carré dans $\Bbbk_3$ si et seulement si $x\pm 1$ est un carré dans $\mathbb{N}$ (voir résultat R1).

D'après le lemme 5, $2(x\pm 1)$ et $pq(x\pm 1)$ ne sont pas des carrés dans $\mathbb{N}$. Ainsi on a :

• Si $2p(x\pm 1)$ est un carré dans $\mathbb{N}$, alors $q(x\mp 1)$ est un carré dans $\mathbb{N}$ et il existe $(y_1, y_2)\in\mathbb{Z}^2$ tel que

$$\begin{cases} x\pm 1 = 2py_1^2, \\ x\mp 1 = qy_2^2, \end{cases} \qquad \begin{cases} \sqrt{2\varepsilon_3} = y_1\sqrt{2p} + y_2\sqrt{q}, \\ \sqrt{\varepsilon_3} = \frac{1}{2}(2y_1\sqrt{p} + y_2\sqrt{2q}). \end{cases}$$

• Si $2q(x\pm 1)$ est un carré dans $\mathbb{N}$, alors $p(x\mp 1)$ est un carré dans $\mathbb{N}$ et il existe $(y_1, y_2)\in\mathbb{Z}^2$ tel que

$$\begin{cases} x\pm 1 = 2qy_1^2, \\ x\mp 1 = py_2^2, \end{cases} \qquad \begin{cases} \sqrt{2\varepsilon_3} = y_1\sqrt{2q} + y_2\sqrt{p}, \\ \sqrt{\varepsilon_3} = \frac{1}{2}(2y_1\sqrt{q} + y_2\sqrt{2p}). \end{cases}$$

Par conséquent, si $2p(x \pm 1)$ est un carré dans $\mathbb{N}$, alors $2\varepsilon_3$ est un carré dans $\mathbb{K}_0$ et si $2q(x \pm 1)$ est un carré dans $\mathbb{N}$, alors ε_3 est un carré dans $\mathbb{K}_0$. D'autre part, d'après les lemmes 6 et 7, $2\varepsilon_1$ et $2\varepsilon_2$ sont des carrés dans $\mathbb{K}_0$. D'où $\varepsilon_1\varepsilon_2$ est un carré dans $\mathbb{K}_0$. De même, si $2\varepsilon_3$ est un carré dans $\mathbb{K}_0$, alors $\varepsilon_1\varepsilon_3$ et $\varepsilon_2\varepsilon_3$ sont des carrés dans $\mathbb{K}_0$ et donc $\{\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_1\varepsilon_3}, \sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$. Dans le cas où ε_3 est un carré dans $\mathbb{K}_0$, l'unité $\varepsilon_1\varepsilon_2\varepsilon_3$ est un carré dans $\mathbb{K}_0$ et d'après les résultats de [Kur-43], rappelés au début de ce paragraphe, $\{\varepsilon_1, \sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$. ∎

THÉORÈME 9. *On se place dans les conditions du lemme* 8. *Soit* $\mathbb{K} = \mathbb{K}_0(i)$. *Alors on a* :

(i) *Si* $2p(x \pm 1)$ *est un carré dans* $\mathbb{N}$, *alors* $\{\sqrt{i\varepsilon_1}, \sqrt{i\varepsilon_2}, \sqrt{i\varepsilon_3}\}$ *est un SFU de* $\mathbb{K}$.

(ii) *Si* $2q(x \pm 1)$ *est un carré dans* $\mathbb{N}$, *alors* $\{\sqrt{i\varepsilon_1}, \sqrt{\varepsilon_3}, \sqrt{i\varepsilon_2}\}$ *est un SFU de* $\mathbb{K}$.

Preuve. Les unités ε_1 et ε_2 jouent un rôle symétrique.

(i) Soit $\varepsilon = \sqrt{\varepsilon_1\varepsilon_2}\sqrt{\varepsilon_1\varepsilon_3}\sqrt{\varepsilon_2\varepsilon_3} = \varepsilon_1(\sqrt{\varepsilon_2\varepsilon_3})^2$. On sait que $\sqrt{i\varepsilon} \in \mathbb{K}$ si et seulement si $\sqrt{2\varepsilon} \in \mathbb{K}_0$ (car $\sqrt{i} = (1+i)/\sqrt{2}$). Comme $2\varepsilon_1$ est un carré dans $\mathbb{K}_0$, alors 2ε est un carré dans $\mathbb{K}_0$. Un SFU de $\mathbb{K}_0$ est donné par le lemme précédent. D'où, d'après le résultat R2, $\{\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_1\varepsilon_3}, \sqrt{i\varepsilon_1\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}$. Comme $2\varepsilon_i$ est un carré dans $\mathbb{K}_0$ pour $i = 1, 2, 3$, alors $\{\sqrt{i\varepsilon_1}, \sqrt{i\varepsilon_2}, \sqrt{i\varepsilon_3}\}$ est aussi un SFU de $\mathbb{K}$.

(ii) Soit $\varepsilon = \varepsilon_2$. On sait d'après le lemme 7 que $2\varepsilon_2$ est un carré dans $\mathbb{K}_0$ et le lemme 8 nous donne un SFU de $\mathbb{K}_0$. Donc en utilisant le résultat R2, on trouve que $\{\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_3}, \sqrt{i\varepsilon_2}\}$ est un SFU de $\mathbb{K}$. Puisque $2\varepsilon_i$ est un carré dans $\mathbb{K}_0$ pour $i = 1, 2$, alors $\{\sqrt{i\varepsilon_1}, \sqrt{\varepsilon_3}, \sqrt{i\varepsilon_2}\}$ est aussi un SFU de $\mathbb{K}$. ∎

THÉORÈME 10. *Soient* p *et* q *deux nombres premiers impairs tels que* $p \equiv -q \equiv 1 \bmod 4$, $\mathbb{K}_0 = \mathbb{Q}(\sqrt{p}, \sqrt{2q})$ *et* ε_1 (*resp.* ε_2, ε_3) *l'unité fondamentale de* $\mathbb{k}_1 = \mathbb{Q}(\sqrt{p})$ (*resp.* $\mathbb{k}_2 = \mathbb{Q}(\sqrt{2q})$, $\mathbb{k}_3 = \mathbb{Q}(\sqrt{2pq})$). *On pose* $\varepsilon_3 = x + y\sqrt{2pq}$ *et on suppose que* $2\varepsilon_3$ *n'est pas un carré dans* $\mathbb{k}_3$. *Alors on a* :

(i) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ *est un SFU de* $\mathbb{K}_0 \Leftrightarrow 2p(x \pm 1)$ *est un carré dans* $\mathbb{N}$. *Dans ce cas* $\{\varepsilon_1, \sqrt{\varepsilon_3}, \sqrt{i\varepsilon_2}\}$ *est un SFU de* $\mathbb{K} = \mathbb{K}_0(i)$.

(ii) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}\}$ *est un SFU de* $\mathbb{K}_0 \Leftrightarrow 2q(x \pm 1)$ *est un carré dans* $\mathbb{N}$. *Dans ce cas* $\{\varepsilon_1, \sqrt{\varepsilon_2\varepsilon_3}, \sqrt{i\varepsilon_2}\}$ *est un SFU de* $\mathbb{K} = \mathbb{K}_0(i)$.

Preuve. Les unités ε_1 et ε_2 ne jouent pas un rôle symétrique dans ce théorème. On a que ε_1 est de norme -1, ε_2 et ε_3 sont de norme 1. D'après le lemme 7, $2\varepsilon_2$ est un carré dans $\mathbb{k}_2$. D'où ε_2 n'est pas un carré dans $\mathbb{K}$, car sinon $\sqrt{2} \in \mathbb{K}_0$. Soit $\varepsilon_3 = x + y\sqrt{2pq}$. Par hypothèse $2\varepsilon_3$ n'est pas un carré dans $\mathbb{k}_3$, ce qui est équivalent au fait que $x \pm 1$ n'est pas un carré dans $\mathbb{N}$ (le résultat R1). De la même façon que dans le lemme 8, comme $(x+1)(x-1) = 2pqy^2$, alors $2p(x \pm 1)$ ou $2q(x \pm 1)$ est un carré dans $\mathbb{N}$.

(a) On suppose que $2p(x \pm 1)$ est un carré dans $\mathbb{N}$. Si $2p(x-1)$ est un carré dans $\mathbb{N}$, alors il existe $(y_1, y_2) \in \mathbb{Z}^2$ tel que

$$\begin{cases} x-1 = 2py_1^2, \\ x+1 = qy_2^2, \end{cases} \qquad \begin{cases} \sqrt{2\varepsilon_3} = y_1\sqrt{2p} + y_2\sqrt{q}, \\ \sqrt{\varepsilon_3} = \frac{1}{2}(2y_1\sqrt{p} + y_2\sqrt{2q}). \end{cases}$$

Il en est de même si $2p(x+1)$ est un carré dans $\mathbb{N}$. Il vient donc que si $2p(x \pm 1)$ est un carré dans $\mathbb{N}$, alors $\sqrt{\varepsilon_3} \in \mathbb{K}_0$ et $\sqrt{2\varepsilon_3} \notin \mathbb{K}_0$.

(b) On fait la même chose si $2q(x \pm 1)$ est un carré dans $\mathbb{N}$ et on trouve que $\sqrt{\varepsilon_3} \notin \mathbb{K}_0$ et $\sqrt{2\varepsilon_3} \in \mathbb{K}_0$. Si $\sqrt{2\varepsilon_3} \in \mathbb{K}$, alors $\sqrt{\varepsilon_2\varepsilon_3} \in \mathbb{K}_0$, puisque $\sqrt{2\varepsilon_2} \in \mathbb{K}$. Ainsi on a :

(i) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$ si et seulement si $2p(x \pm 1)$ est un carré dans $\mathbb{N}$.

(ii) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$ si et seulement si $2q(x \pm 1)$ est un carré dans $\mathbb{N}$.

D'autre part, $2\varepsilon_2$ est un carré dans $\mathbb{k}_2$ entraîne que $\sqrt{i\varepsilon_2} \in \mathbb{k}_2(i)$. En utilisant le résultat R2, on trouve qu'un SFU de $\mathbb{K} = \mathbb{K}_0(i)$ est :

(i′) $\{\varepsilon_1, \sqrt{i\varepsilon_2}, \sqrt{\varepsilon_3}\}$ si $2p(x \pm 1)$ est un carré dans $\mathbb{N}$.

(ii′) $\{\varepsilon_1, \sqrt{i\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}\}$ si $2q(x \pm 1)$ est un carré dans $\mathbb{N}$. ∎

THÉORÈME 11. *Soient* $\mathbb{K}_0 = \mathbb{Q}(\sqrt{q}, \sqrt{2p})$, $\mathbb{K} = \mathbb{K}_0(i)$, $\mathbb{k}_1 = \mathbb{Q}(\sqrt{q})$, $\mathbb{k}_2 = \mathbb{Q}(\sqrt{2p})$ *et* $\mathbb{k}_3 = \mathbb{Q}(\sqrt{2pq})$. *On garde les autres notations du théorème précédent. On suppose que* ε_2 *est de norme* -1 *et* $2\varepsilon_3$ *n'est pas un carré dans* $\mathbb{k}_3$. *Alors si* $\varepsilon_3 = x + y\sqrt{2pq}$ *on a :*

(i) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ *est un SFU de* $\mathbb{K}_0$ *si et seulement si* $2q(x \pm 1)$ *est un carré dans* $\mathbb{N}$. *Dans ce cas un SFU de* $\mathbb{K}$ *est* $\{\varepsilon_2, \sqrt{i\varepsilon_1}, \sqrt{\varepsilon_3}\}$.

(ii) $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_1\varepsilon_3}\}$ *est un SFU de* $\mathbb{K}_0$ *si et seulement si* $2p(x \pm 1)$ *est un carré dans* $\mathbb{N}$. *Dans ce cas, un SFU de* $\mathbb{K}$ *est* $\{\varepsilon_2, \sqrt{i\varepsilon_1}, \sqrt{\varepsilon_1\varepsilon_3}\}$.

Preuve. Il suffit de remarquer que $2\varepsilon_1$ est un carré dans $\mathbb{k}_1$, ε_1 n'est pas un carré dans $\mathbb{K}_0$ et si $\varepsilon_3 = x + y\sqrt{2pq}$, alors on a :

(i) $2q(x \pm 1)$ est un carré dans $\mathbb{N} \Leftrightarrow \sqrt{\varepsilon_3} \in \mathbb{K}_0$ et $\sqrt{2\varepsilon_3} \notin \mathbb{K}_0$.

(ii) $2p(x \pm 1)$ est un carré dans $\mathbb{N} \Leftrightarrow \sqrt{2\varepsilon_3} \in \mathbb{K}_0$ et $\sqrt{\varepsilon_3} \notin \mathbb{K}_0$.

Avec le même raisonnement que dans le théorème précédent, on arrive aux résultats voulus. ∎

THÉORÈME 12. *Soient* p *et* q *deux nombres premiers impairs tels que* $q \equiv -1 \bmod 4$, $\mathbb{K}_0 = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$, $\mathbb{K} = \mathbb{K}_0(i)$ *et* ε_1 *(resp.* ε_2, ε_3*) l'unité fondamentale de* $\mathbb{k}_1 = \mathbb{Q}(\sqrt{2})$ *(resp.* $\mathbb{k}_2 = \mathbb{Q}(\sqrt{pq})$, $\mathbb{k}_3 = \mathbb{Q}(\sqrt{2pq})$*). On suppose que* $2\varepsilon_3$ *n'est pas un carré dans* $\mathbb{k}_3$.

1. *Si* $\varepsilon_2 = x + y\sqrt{pq}$ *avec* $(x, y) \in \mathbb{Z}^2$. *Alors on a :*

(i) *Si* $x \pm 1$ *est un carré dans* $\mathbb{N}$, *alors* $\{\varepsilon_1, \sqrt{\varepsilon_2}, \varepsilon_3\}$ *est un SFU de* $\mathbb{K}_0$ *et de* $\mathbb{K}$.

(ii) *Sinon*, $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}\}$ *est un SFU de* $\mathbb{K}_0$ *et de* $\mathbb{K}$.

2. *Si* $\varepsilon_2 = x/2 + (y/2)\sqrt{pq}$ *avec* x *et* y *deux entiers impairs. Alors les deux corps* $\mathbb{K}_0$ *et* $\mathbb{K}$ *ont le même SFU* $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}\}$.

Preuve. 1. On a que ε_1 est de norme -1, ε_2 et ε_3 sont de norme 1 et $(x-1)(x+1) = pqy^2$. D'après le lemme 5, $2pq(x \pm 1)$ n'est pas un carré dans $\mathbb{N}$. Ainsi on a :

(a) Soit $pq(x \pm 1)$ un carré dans $\mathbb{N}$. Si $pq(x-1)$ est un carré dans $\mathbb{N}$, alors il existe $(y_1, y_2) \in \mathbb{Z}^2$ tel que

$$\begin{cases} x - 1 = pqy_1^2, \\ x + 1 = y_2^2, \end{cases} \qquad \sqrt{\varepsilon_2} = (y_1\sqrt{2pq} + y_2\sqrt{2})/2 \in \mathbb{K}_0.$$

Il en est de même si $pq(x+1)$ est un carré dans $\mathbb{N}$.

(b) Soit $p(x \pm 1)$ ou $2p(x \pm 1)$ un carré dans $\mathbb{N}$. Si $p(x-1)$ est un carré dans $\mathbb{N}$, alors il existe $(y_1, y_2) \in \mathbb{Z}^2$ tel que

$$\begin{cases} x - 1 = py_1^2, \\ x + 1 = qy_2^2, \end{cases} \qquad \sqrt{\varepsilon_2} = (y_1\sqrt{2p} + y_2\sqrt{2q})/2 \notin \mathbb{K}_0, \ \sqrt{p\varepsilon_2} \text{ et } \sqrt{q\varepsilon_2} \in \mathbb{K}_0.$$

Dans les trois cas qui restent on a que $\sqrt{\varepsilon_2} \notin \mathbb{K}_0$, $\sqrt{p\varepsilon_2}$ et $\sqrt{q\varepsilon_2} \in \mathbb{K}_0$.

Soit $\varepsilon_3 = s + t\sqrt{2pq}$. On a $(s-1)(s+1) = 2pqt^2$. Comme $2\varepsilon_3$ n'est pas un carré dans $\mathbb{k}_3$, alors $s \pm 1$ n'est pas un carré dans $\mathbb{N}$. Avec un raisonnement semblable à celui fait pour ε_2, on trouve que les seuls cas possibles sont :

- $2q(s \pm 1)$ est un carré dans $\mathbb{N}$;
- $2p(s \pm 1)$ est un carré dans $\mathbb{N}$.

Dans ces deux cas, $\sqrt{\varepsilon_3} \notin \mathbb{K}_0$ et $\sqrt{p\varepsilon_3}$, $\sqrt{q\varepsilon_3}$ appartiennent à $\mathbb{K}_0$. Si $\sqrt{p\varepsilon_2} \in \mathbb{K}_0$ et $\sqrt{p\varepsilon_3} \in \mathbb{K}_0$, alors $\sqrt{\varepsilon_2\varepsilon_3} \in \mathbb{K}_0$.

Enfin, avec toutes ces données et les résultats de [Kur-43] rappelés au début de ce paragraphe on conclut que :

(i) Si $x \pm 1$ est un carré dans $\mathbb{N}$, alors $\{\varepsilon_1, \sqrt{\varepsilon_2}, \varepsilon_3\}$ est un SFU de $\mathbb{K}_0$.

(ii) Sinon, $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$.

D'autre part, d'après le théorème 2(ii) sur les unités de $\mathbb{Q}(\sqrt{d}, \sqrt{2}, i)$ de [H-Y-90] une condition suffisante pour qu'un SFU de $\mathbb{K}_0$ soit aussi un SFU de $\mathbb{K}$, est que $s \pm 1$ ou $x \pm 1$ n'est pas un carré dans $\mathbb{N}$. Or, dans notre cas, on suppose que $2\varepsilon_3$ n'est pas un carré dans $\mathbb{k}_3$, ce qui est équivalent au fait que $s \pm 1$ n'est pas un carré dans $\mathbb{N}$. D'où $\mathbb{K}_0$ et $\mathbb{K}$ ont un même SFU.

2. Soit $\varepsilon_2 = x/2 + (y/2)\sqrt{pq}$. Comme ε_2 est de norme 1, alors on a $(x-2)(x+2) = pqy^2$, $(x+2) - (x-2) = 4$, $x-2$ et $x+2$ sont impairs. Par suite $x+2$ et $x-2$ sont premiers entre eux.

(a) Soit $pq(x\pm 2)$ un carré dans $\mathbb{N}$. Si $pq(x-2)$ est un carré dans $\mathbb{N}$, alors il existe $(y_1,y_2)\in\mathbb{Z}^2$ tel que

$$\begin{cases} x-2=pqy_1^2,\\ x+2=y_2^2,\end{cases}\qquad \sqrt{\varepsilon_2}=(y_1\sqrt{pq}+y_2)/2\in\Bbbk_3.$$

Ceci est absurde puisque ε_2 est l'unité fondamentale de $\Bbbk_2=\mathbb{Q}(\sqrt{pq})$. Il en est de même si $pq(x+2)$ est un carré dans $\mathbb{N}$. Donc ces deux cas ne se présentent pas.

(b) Soit $p(x\pm 2)$ un carré dans $\mathbb{N}$. Si $p(x-2)$ est un carré dans $\mathbb{N}$, alors il existe $(y_1,y_2)\in\mathbb{Z}^2$ tel que

$$\begin{cases} x-2=py_1^2,\\ x+2=qy_2^2,\end{cases}\qquad \sqrt{\varepsilon_2}=(y_1\sqrt{p}+y_2\sqrt{q})/2\notin\mathbb{K}_0,\ \sqrt{p\varepsilon_2}\ \text{et}\ \sqrt{q\varepsilon_2}\in\mathbb{K}_0.$$

Les résultats du cas précédent concernant ε_3 restent valables ici, c'est-à-dire $\sqrt{\varepsilon_3}\notin\mathbb{K}_0$, $\sqrt{p\varepsilon_3}$ et $\sqrt{q\varepsilon_3}\in\mathbb{K}_0$. Par conséquent, $\sqrt{\varepsilon_2\varepsilon_3}\in\mathbb{K}_0$. De la même façon que dans le premier cas on conclut que $\{\varepsilon_1,\varepsilon_2,\sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$ et $\mathbb{K}$. ∎

Remarque 13. On garde les notations précédentes. Soient $d=pq$, ε_1 l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$, ε_2 l'unité fondamentale de $\mathbb{Q}(\sqrt{2d})$ et Δ_i la partie sans carré de $N(\varepsilon_i+1)$. On trouve dans [H-Y-90] que si $Q=2$ alors $\Delta_1=\Delta_2=2$ ou bien $\Delta_1=2d$ et $\Delta_2=d$. Or si $\varepsilon_1=x+y\sqrt{d}$ et $\varepsilon_2=s+t\sqrt{2d}$, alors

$$(x-1)(x+1)=dy^2\quad\text{et}\quad N(\varepsilon_1+1)=2(x+1)\,;$$
$$(s-1)(s+1)=2dt^2\quad\text{et}\quad N(\varepsilon_2+1)=2(s+1)\,;$$

et

$\Delta_1=2\ \Leftrightarrow (x+1)$ est un carré dans $\mathbb{N}$ $\Leftrightarrow d(x-1)$ est un carré dans $\mathbb{N}$.

$\Delta_1=2d \Leftrightarrow d(x+1)$ est un carré dans $\mathbb{N}$ $\Leftrightarrow (x-1)$ est un carré dans $\mathbb{N}$.

$\Delta_2=2\ \Leftrightarrow (s+1)$ est un carré dans $\mathbb{N}$ $\Leftrightarrow 2d(s-1)$ est un carré dans $\mathbb{N}$.

$\Delta_2=d\ \Leftrightarrow 2d(s+1)$ est un carré dans $\mathbb{N}$ $\Leftrightarrow (s-1)$ est un carré dans $\mathbb{N}$.

Par suite si $x\pm1$ ou $s\pm1$ n'est pas un carré dans $\mathbb{N}$ alors $Q=1$.

Théorème 14. *Soient p et q deux nombres premiers impairs tels que $p\equiv -q\equiv 1 \bmod 4$, $\mathbb{K}_0=\mathbb{Q}(\sqrt{p},\sqrt{q})$, $\mathbb{K}=\mathbb{K}_0(i)$ et ε_1 (resp. $\varepsilon_2,\varepsilon_3$) l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{q}),\mathbb{Q}(\sqrt{pq})$). On suppose que $2\varepsilon_3$ est un carré dans $\mathbb{Q}(\sqrt{pq})$. Alors $\{\varepsilon_1,\varepsilon_2,\sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$ et $\{\varepsilon_1,\sqrt{i\varepsilon_2},\sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}$.*

Preuve. On sait, d'après le lemme 6, que $2\varepsilon_2$ est un carré dans $\mathbb{Q}(\sqrt{q})$. Comme $2\varepsilon_3$ est un carré dans $\mathbb{Q}(\sqrt{pq})$, alors $\sqrt{\varepsilon_2\varepsilon_3}$ appartient à $\mathbb{K}_0$. De plus $\sqrt{\varepsilon_2}\notin\mathbb{K}_0$ et $\sqrt{\varepsilon_3}\notin\mathbb{K}_0$. D'où $\{\varepsilon_1,\varepsilon_2,\sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_0$. D'autre part

$\sqrt{2\varepsilon_2} \in \mathbb{K}_0 \Leftrightarrow \sqrt{i\varepsilon_2} \in \mathbb{K}$. Par suite, d'après le résultat R2, $\{\varepsilon_1, \sqrt{i\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}$. ∎

Remarque 15. Soient p et q deux nombres premiers impairs tels que $p \equiv 1 \bmod 8$, $-q \equiv 1 \bmod 4$ et $\left(\frac{p}{q}\right) = -1$. Soit ε_3 l'unité fondamentale de $\mathbb{Q}(\sqrt{pq})$. Alors $2\varepsilon_3$ est un carré dans $\mathbb{Q}(\sqrt{pq})$ (c.a.d. $Q = 2$).

Preuve. Soit $\varepsilon_3 = x + y\sqrt{pq}$. Comme ε_3 est de norme 1, alors on a $(x-1)(x+1) = pqy^2$. D'après le lemme 5, $2(x \pm 1)$ et $2pq(x \pm 1)$ ne sont pas des carrés dans $\mathbb{N}$. Ainsi on a deux cas :

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

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

Donc $-2 = py_1^2 - qy_2^2$. Ceci 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 $\mathbb{N}$, on obtient la même contradiction.

(b) $q(x-1)$ ou $2q(x-1)$ est un carré dans $\mathbb{N}$. Si $2q(x-1)$ est un carré dans $\mathbb{N}$, alors il existe $(y_1, y_2) \in \mathbb{Z}^2$ tel que

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

Donc $1 = py_2^2 - qy_1^2$. Ceci implique que $\left(\frac{p}{q}\right) = 1$, ce qui n'est pas possible. Si $q(x-1)$ est un carré dans $\mathbb{N}$, on obtient la même contradiction.

Ainsi donc $pq(x-1)$ ou $(x-1)$ est un carré dans $\mathbb{N}$; ce qui est équivalent à dire que $2\varepsilon_3$ est un carré dans $\mathbb{Q}(\sqrt{pq})$ (c.a.d. $Q = 2$).

3. Nombre de classes capitulant dans certaines extensions qudratiques de $\Bbbk$. Soient p un nombre premier congru à 1 modulo 4 et q un nombre premier congru à -1 modulo 4, $\Bbbk = \mathbb{Q}(\sqrt{2pq}, i)$ tel que au moins deux éléments de $\left\{\left(\frac{2}{p}\right), \left(\frac{2}{q}\right), \left(\frac{p}{q}\right)\right\}$ valent -1 et l'indice Q des unités de $\mathbb{Q}(\sqrt{2pq})$ dans $\Bbbk$ est égal à 1, et $\Bbbk_2^{(1)}$ le 2-corps de classes de $\Bbbk$. D'après [Az-93], la 2-partie du groupe de classes $\mathbf{C}_2$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans notre cas $\Bbbk_2^{(1)} = \mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{2}, i)$ et les sous-extensions quadratiques de $\Bbbk_2^{(1)}/\Bbbk$ sont : $\mathbb{K}_1 = \mathbb{Q}(\sqrt{p}, \sqrt{2q}, i)$, $\mathbb{K}_2 = \mathbb{Q}(\sqrt{q}, \sqrt{2p}, i)$ et $\mathbb{K}_3 = \mathbb{Q}(\sqrt{2}, \sqrt{pq}, i)$.

On va faire une étude du problème de la capitulation dans les différentes sous-extensions quadratiques $\mathbb{K}/\Bbbk$ de $\Bbbk_2^{(1)}/\Bbbk$.

$$\begin{tikzcd}
 & \Bbbk_2^{(2)} \arrow[d, dash] & \\
 & \Bbbk_2^{(1)} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{K}_1 \arrow[dr, dash] & \mathbb{K}_2 \arrow[d, dash] & \mathbb{K}_3 \arrow[dl, dash] \\
 & \Bbbk \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Diagramme 1

(a) *Capitulation dans* $\mathbb{K}_1/\Bbbk$. Soit ε_1 (resp. ε_2, ε_3) l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{2q})$, $\mathbb{Q}(\sqrt{2pq})$). On pose $\varepsilon_3 = s + t\sqrt{2pq}$. D'après le théorème 10, un SFU de $\mathbb{K}_1$ est donné de la façon suivante :

(i) Si $2p(s \pm 1)$ est un carré dans $\mathbb{N}$, alors $\{\varepsilon_1, \sqrt{\varepsilon_3}, \sqrt{i\varepsilon_2}\}$ est un SFU de $\mathbb{K}_1$.

(ii) Si $2q(s \pm 1)$ est un carré dans $\mathbb{N}$, alors $\{\varepsilon_1, \sqrt{i\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_1$.

Dans les deux cas on a $N(\mathbf{E}_{\mathbb{K}_1}) = \mathbf{E}_{\Bbbk}$. D'où, d'après le théorème 1, exactement deux classes de $\mathbf{C}_2$ capitulent dans $\mathbb{K}_1$.

(b) *Capitulation dans* $\mathbb{K}_2/\Bbbk$. Soit ε_1 (resp. ε_2, ε_3) l'unité fondamentale de $\mathbb{Q}(\sqrt{q})$ (resp. $\mathbb{Q}(\sqrt{2p})$, $\mathbb{Q}(\sqrt{2pq})$). On pose $\varepsilon_3 = s + t\sqrt{2pq}$. Distinguons les deux cas suivants :

(i) On suppose que ε_2 est de norme -1 (théorème 11). Dans ce cas :

- si $2q(s \pm 1)$ est un carré dans $\mathbb{N}$, alors $\{\sqrt{i\varepsilon_1}, \varepsilon_2, \sqrt{\varepsilon_3}\}$ est un SFU de $\mathbb{K}_2$;
- si $2p(s \pm 1)$ est un carré dans $\mathbb{N}$, alors $\{\sqrt{i\varepsilon_1}, \varepsilon_2, \sqrt{\varepsilon_1\varepsilon_3}\}$ est un SFU de $\mathbb{K}_2$.

(ii) On suppose que ε_2 est de norme 1 (lemme 8, théorème 9). Dans ce cas :

- si $2p(s \pm 1)$ est un carré dans $\mathbb{N}$, alors $\{\sqrt{i\varepsilon_1}, \sqrt{i\varepsilon_2}, \sqrt{i\varepsilon_3}\}$ est un SFU de $\mathbb{K}_2$;
- si $2q(s \pm 1)$ est un carré dans $\mathbb{N}$, alors $\{\sqrt{i\varepsilon_1}, \sqrt{i\varepsilon_2}, \sqrt{\varepsilon_3}\}$ est un SFU de $\mathbb{K}_2$.

Dans tous ces cas on a que $N(\mathbf{E}_{\mathbb{K}_2}) = \mathbf{E}_{\Bbbk}$. Par suite, d'après le théorème 1, exactement deux classes de $\mathbf{C}_2$ capitulent dans $\mathbb{K}_2$.

(c) *Capitulation dans* $\mathbb{K}_3$. Soit ε_1 (resp. $\varepsilon_2, \varepsilon_3$) l'unité fondamentale de $\mathbb{Q}(\sqrt{2})$ (resp. $\mathbb{Q}(\sqrt{pq}), \mathbb{Q}(\sqrt{2pq})$). On pose $\varepsilon_2 = x + y\sqrt{pq}$. D'après le théorème 12, un SFU de $\mathbb{K}_3$ est donné de la façon suivante :

(i) Si $x \pm 1$ est un carré dans $\mathbb{N}$, alors $\{\varepsilon_1, \sqrt{\varepsilon_2}, \varepsilon_3\}$ est un SFU de $\mathbb{K}_3$.

(ii) Sinon, $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_2\varepsilon_3}\}$ est un SFU de $\mathbb{K}_3$.

Donc, si $x \pm 1$ est un carré dans $\mathbb{N}$, alors $[\mathbf{E}_{\Bbbk} : N(\mathbf{E}_{\mathbb{K}_3})] = 2$; sinon, $N(\mathbf{E}_{\mathbb{K}_3}) = \mathbf{E}_{\Bbbk}$. Il vient, d'après le théorème 1, que toutes les classes de $\mathbf{C}_2$ capitulent dans $\mathbb{K}_3$ si et seulement si $x \pm 1$ est un carré dans $\mathbb{N}$.

On obtient alors le théorème suivant :

THÉORÈME 16. *Soient* $\Bbbk = \mathbb{Q}(\sqrt{2pq}, i)$ *avec au moins deux éléments de* $\{(\frac{2}{p}), (\frac{2}{q}), (\frac{p}{q})\}$ *valant* -1 *et l'indice* Q *des unités de* $\mathbb{Q}(\sqrt{2pq})$ *dans* $\Bbbk$ *est égal à* 1, $\mathbb{K}_1 = \mathbb{Q}(\sqrt{p}, \sqrt{2q}, i)$, $\mathbb{K}_2 = \mathbb{Q}(\sqrt{q}, \sqrt{2p}, i)$ *et* $\mathbb{K}_3 = \mathbb{Q}(\sqrt{2}, \sqrt{pq}, i)$. *Alors dans chaque extension* $\mathbb{K}_i$, $i \in \{1, 2, 3\}$, *il existe exactement deux classes de* $\mathbf{C}_2$ *qui capitulent.*

Preuve. Soit $\varepsilon_2 = x + y\sqrt{pq}$ (resp. $\varepsilon_3 = s + t\sqrt{2pq}$) l'unité fondamentale de $\mathbb{Q}(\sqrt{pq})$ (resp. $\mathbb{Q}(\sqrt{2pq})$). On rappelle que $p \equiv -q \equiv 1 \bmod 4$. On désigne par $\left(\frac{m}{p}\right)$ le symbole de Legendre pour un entier naturel m. On sait que deux classes seulement capitulent dans $\mathbb{K}_1$, que deux classes seulement capitulent dans $\mathbb{K}_2$ et que les 4 classes de $\mathbf{C}_2$ capitulent dans $\mathbb{K}_3$ si et seulement si $x \pm 1$ est un carré dans $\mathbb{N}$. On se propose de montrer que $x \pm 1$ n'est jamais un carré de $\mathbb{N}$.

Montrons que si $x \pm 1$ est un carré dans $\mathbb{N}$, alors $\left(\frac{2}{p}\right) = 1$. En effet, $(x-1)(x+1) = pqy^2$. Si $x \pm 1$ est un carré dans $\mathbb{N}$, alors il existe $(y_1, y_2) \in \mathbb{N}^2$ tel que l'une des deux situations suivantes est satisfaite :

$$\begin{cases} x - 1 = pqy_1^2, \\ x + 1 = y_2^2, \end{cases} \quad 1 = \left(\frac{y_2^2}{p}\right) = \left(\frac{x+1}{p}\right) = \left(\frac{x-1+2}{p}\right) = \left(\frac{2}{p}\right);$$

$$\begin{cases} x + 1 = pqy_1^2, \\ x - 1 = y_2^2, \end{cases} \quad 1 = \left(\frac{y_2^2}{p}\right) = \left(\frac{x-1}{p}\right) = \left(\frac{x+1-2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right).$$

Ainsi, cette propriété est démontrée.

Montrons que si $2\varepsilon_3$ n'est pas un carré dans $\mathbb{Q}(\sqrt{2pq})$, alors $\left(\frac{q}{p}\right) = 1$ ou bien $\left(\frac{2}{p}\right) = \left(\frac{q}{p}\right)$. En effet, $(s-1)(s+1) = 2pqt^2$. Si de plus $2\varepsilon_3$ n'est pas un carré dans $\mathbb{Q}(\sqrt{2pq})$, alors $s \pm 1$ n'est pas un carré dans $\mathbb{N}$ et il existe $(t_1, t_2) \in \mathbb{N}^2$ tel qu'on a l'une des situations suivantes :

$$\begin{cases} s \pm 1 = 2pt_1^2, \\ s \mp 1 = qt_2^2, \end{cases} \quad \left(\frac{q}{p}\right) = \left(\frac{s \mp 1}{p}\right) = \left(\frac{s \pm 1 \mp 2}{p}\right) = \left(\frac{2}{p}\right).$$

$$\begin{cases} s \pm 1 = pt_1^2, \\ s \mp 1 = 2qt_2^2, \end{cases} \quad \left(\frac{2q}{p}\right) = \left(\frac{s \mp 1}{p}\right) = \left(\frac{s \pm 1 \mp 2}{p}\right) = \left(\frac{2}{p}\right) \Rightarrow \left(\frac{q}{p}\right) = 1.$$

Ceci termine la démonstration de cette propriété.

Conclusion : Si $x\pm1$ est un carré dans $\mathbb{N}$, alors, d'après les deux propriétés précédentes, $\left(\frac{q}{p}\right) = \left(\frac{2}{p}\right) = 1$. Par conséquent, nos hypothèses ne seront pas vérifiées. Il en résulte que $x \pm 1$ ne peut pas être un carré dans $\mathbb{N}$. ∎

4. Structure de G_2 et 2-groupe de classes de $\mathbb{k}$. Soient p un nombre premier congru à 1 modulo 4 et q un nombre premier congru à -1 modulo 4, $\mathbb{k} = \mathbb{Q}(\sqrt{2pq}, i)$ tel que au moins deux éléments de $\left\{\left(\frac{2}{p}\right), \left(\frac{2}{q}\right), \left(\frac{p}{q}\right)\right\}$ valent -1 et l'indice Q des unités de $\mathbb{Q}(\sqrt{2pq})$ dans $\mathbb{k}$ est égal à 1, $\mathbf{C}_2$ le 2-groupe des classes de $\mathbb{k}$, $\mathbf{E}_{\mathbb{k}}$ le groupe des unités de $\mathbb{k}$, $\mathbb{k}_2^{(1)}$ le 2-corps de classes de Hilbert de $\mathbb{k}$ et G_2 le groupe de Galois de $\mathbb{k}_2^{(2)}/\mathbb{k}$.

Nous étudions la capitulation de certains idéaux de $\mathbb{k}$ et par la suite nous déterminons la structure de G_2 en nous basant sur le théorème 2.

PROPOSITION 17. *Soient $\mathbb{k} = \mathbb{Q}(\sqrt{2pq}, i)$ et $\mathcal{H}_0$ l'idéal premier au dessus de $1 + i$ dans $\mathbb{k}$. Alors la classe de $\mathcal{H}_0$ dans $\mathbb{k}$ est d'ordre 2. De plus $\mathcal{H}_0$ capitule dans $\mathbb{k}(\sqrt{2})$.*

P r e u v e. Montrons que la classe de $\mathcal{H}_0$ est d'ordre 2. Comme 2 est totalement ramifié dans $\mathbb{k}/\mathbb{Q}$, alors il existe un idéal $\mathcal{H}_0$ de $\mathbb{k}$ tel que $\mathcal{H}_0^2 = (1 + i)$. On suppose que $\mathcal{H}_0 = (\alpha)$ pour un certain α dans $\mathbb{k}$, ce qui est équivalent à $(\alpha^2) = (1+i)$. Il existe une unité ε de $\mathbb{k}$ telle que $(1+i)\varepsilon = \alpha^2$. Comme l'indice des unités Q est égal à 1, alors ε est un nombre réel ou bien un nombre purement imaginaire. Les deux cas se traitent de la même façon. Supposons que ε est réel. Soit $\alpha = \alpha_1 + i\alpha_2$ avec α_1 et α_2 deux nombres réels de $\mathbb{k}$. On a

$$\begin{cases} \varepsilon = \alpha_1^2 - \alpha_2^2, \\ \varepsilon = 2\alpha_1\alpha_2, \end{cases} \quad \alpha_1^2 - \alpha_2^2 - 2\alpha_1\alpha_2 = 0 \text{ et } \alpha_1 - \alpha_2 = \pm\alpha_2\sqrt{2}.$$

Comme $\sqrt{2} \notin \mathbb{k}$, alors on a une contradiction. Il s'ensuit que la classe de $\mathcal{H}_0$ est d'ordre 2.

Montrons que $\mathcal{H}_0$ capitule dans $\mathbb{k}(\sqrt{2})$. Comme dans le cas précédent, le problème est de chercher un élément α de $\mathbb{k}(\sqrt{2})$ tel que $(\alpha^2) = (1+i)$. Ceci est équivalent à $(1 + i)\varepsilon = \alpha^2$ pour une certaine unité ε de $\mathbb{k}(\sqrt{2})$. Si ε est réel et $\alpha = \alpha_1 + i\alpha_2$, on trouve que

$$\begin{cases} \varepsilon = \alpha_1^2 - \alpha_2^2, \\ \varepsilon = 2\alpha_1\alpha_2, \end{cases} \quad \text{ce qui est équivalent à} \quad \begin{cases} \alpha_1 = \sqrt{\varepsilon(1 \pm \sqrt{2})/2}, \\ \alpha_2 = \varepsilon/(2\alpha_1). \end{cases}$$

Il est clair que si $\varepsilon = 1 \pm \sqrt{2}$, alors α_1 et α_2 appartiennent à $\Bbbk(\sqrt{2})$ et par conséquent $(\mathcal{H}_0) = (\alpha)$ dans $\Bbbk(\sqrt{2})$. D'où le résultat. ∎

Proposition 18. *Soient* $\Bbbk = \mathbb{Q}(\sqrt{2pq}, i)$, *$b$ et c deux entiers tels que $p = b^2 + c^2$ et $\mathcal{P}$ l'idéal premier de $\Bbbk$ au-dessus de $b + ci$. Alors la classe de $\mathcal{P}$ est d'ordre 2 dans $\Bbbk$. De plus, l'idéal $\mathcal{P}$ devient principal dans $\Bbbk(\sqrt{p})$.*

Preuve. Comme p est ramifié dans $\Bbbk/\mathbb{Q}(i)$, alors il existe un idéal $\mathcal{P}$, premier dans $\Bbbk$ et tel que $(b + ci) = \mathcal{P}^2$. Si $\mathcal{P}$ est principal dans $\Bbbk$, alors il existe α dans $\Bbbk$ et ε une unité de $\Bbbk$ tels que $(b+ci)\varepsilon = \alpha^2$. Comme l'indice des unités Q est égal à 1, alors ε est une unité réelle ou bien une unité purement imaginaire. Les deux cas se traitent de la même façon. On suppose que ε est une unité réelle. Si $\alpha = \alpha_1 + i\alpha_2$ avec α_1 et α_2 deux nombres réels de $\Bbbk$, alors

$$\begin{cases} b\varepsilon = \alpha_1^2 - \alpha_2^2, \\ c\varepsilon = 2\alpha_1\alpha_2, \end{cases} \qquad c\alpha_1^2 - c\alpha_2^2 - 2b\alpha_1\alpha_2 = 0 \text{ et } \alpha_1 = \frac{2\alpha_2(b \pm \sqrt{p})}{2c}.$$

Or ceci implique que $\sqrt{p} \in \Bbbk$. Donc on a une contradiction. Par suite la classe de $\mathcal{P}$ est d'ordre 2. Montrons que l'idéal $\mathcal{P}$ devient principal dans $\Bbbk(\sqrt{p})$.

Soit ε_1 l'unité fondamentale de $\mathbb{Q}(\sqrt{p})$. Deux situations se présentent.

1) Cas où $\varepsilon_1 = x + y\sqrt{p}$ avec x et y dans $\mathbb{Z}$. Dans ce cas $(x-i)(x+i) = py^2$ et le plus grand commun diviseur de $x - i$ et $x + i$ est un diviseur de 2. Par suite,

$$\begin{cases} x - i = \pi y_1^2, \\ x + i = \pi' y_2^2, \end{cases}$$

avec $\pi = b + ci$ ou $i(b + ci)$, où π' est le conjugué de π et $y = y_1y_2$.

Vu que c et b jouent un rôle symétrique, on suppose que $\pi = b + ci$. Dans ces conditions, $\sqrt{\varepsilon_1} = \frac{1}{2}(y_1\sqrt{2\pi} + y_2\sqrt{2\pi'})$. D'autre part, $\mathcal{P}$ devient principal dans $\Bbbk(\sqrt{p})$ si et seulement s'il existe α dans $\Bbbk(\sqrt{p})$ et ε' une unité de $\Bbbk(\sqrt{p})$ tels que $\pi\varepsilon' = \alpha^2$. Si $\alpha = \alpha_1 + \alpha_2 i$ et $\varepsilon' = \varepsilon i$ avec ε une unité réelle, alors on trouve que $\alpha_1 = \sqrt{\varepsilon(-c \pm \sqrt{p})/2}$ et $\alpha_2 = b\varepsilon/(2\alpha_1)$. De plus, $\sqrt{-c + \sqrt{p}} = \frac{1}{1+i}(\sqrt{-\pi} + \sqrt{\pi'})$. Si on prend $\varepsilon = \varepsilon_1$, alors α_1 et α_2 appartiennent à $\Bbbk(\sqrt{p})$. D'où l'idéal engendré par $\mathcal{P}$ dans $\Bbbk(\sqrt{p})$ est principal.

2) Cas où $\varepsilon_1 = \frac{1}{2}(x + y\sqrt{p})$. De la même façon que précédemment, on trouve que

$$\begin{cases} x - 2i = \pi y_1^2, \\ x + 2i = \pi' y_2^2, \end{cases}$$

avec $\pi = b + ci$ ou $i(b + ci)$, où π' est le conjugué de π et $y = y_1y_2$.

On suppose que $\pi = b + ci$. Alors $\sqrt{\varepsilon_1} = \frac{1}{2}(y_1\sqrt{\pi} + y_2\sqrt{\pi'})$. De même, $\mathcal{P}$ devient principal dans $\Bbbk(\sqrt{p})$ si et seulement si l'équation en α, $\pi\varepsilon = \alpha^2$ où

ε est une unité de $\mathbb{k}(\sqrt{p})$, est résoluble dans $\mathbb{k}(\sqrt{p})$. Si $\alpha = \alpha_1 + \alpha_2 i$ et ε est une unité réelle, alors on trouve que $\alpha_1 = \sqrt{\varepsilon(b \pm \sqrt{p})/2}$ et $\alpha_2 = c\varepsilon/(2\alpha_1)$. Comme $\sqrt{b+\sqrt{p}} = \sqrt{\pi/2} + \sqrt{\pi'/2}$ et pour $\varepsilon = \varepsilon_1$, les nombres α_1 et α_2 appartiennent à $\mathbb{k}(\sqrt{p})$, alors $\mathcal{P}$ devient principal dans $\mathbb{k}(\sqrt{p})$. ■

PROPOSITION 19. *Soient $\mathbb{k} = \mathbb{Q}(\sqrt{2pq}, i)$, $\mathcal{H}_0$ l'idéal premier de $\mathbb{k}$ au-dessus de $1+i$ et $\mathcal{P}$ l'idéal premier de $\mathbb{k}$ au-dessus de $b+ci$ où b et c sont deux entiers tels que $b^2+c^2=p$. Alors la classe de $\mathcal{H}_0\mathcal{P}$ est d'ordre 2 dans $\mathbb{k}$ et la 2-partie du groupe des classes de $\mathbb{k}$ est engendrée par les classes de $\mathcal{H}_0$ et $\mathcal{P}$.*

Preuve. On pose $b' = b-c$ et $c' = b+c$. Alors $b'^2 + c'^2 = 2p$. L'idéal $\mathcal{H}_0\mathcal{P} = (\alpha)$ où α appartient à $\mathbb{k}$ si et seulement s'il existe une unité ε dans $\mathbb{k}$ telle que $(1+i)(b+ci)\varepsilon = \alpha^2$. Comme l'indice des unités Q est égal à 1, alors ε est une unité réelle ou bien une unité purement imaginaire. Les deux cas se traitent de la même façon. Par suite, on suppose que ε est une unité réelle. Si $\alpha = \alpha_1 + i\alpha_2$ avec α_1 et α_2 deux nombres réels de $\mathbb{k}$, alors

$$\begin{cases} b'\varepsilon = \alpha_1^2 - \alpha_2^2, \\ c'\varepsilon = 2\alpha_1\alpha_2, \end{cases} \qquad c'\alpha_1^2 - c'\alpha_2^2 - 2b'\alpha_1\alpha_2 = 0,$$

donc $\alpha_1 = \alpha_2(b' \pm \sqrt{2p})/c'$. Or ceci implique que $\sqrt{2p} \in \mathbb{k}$. Donc on a une contradiction. Par conséquent, la classe de $\mathcal{H}_0\mathcal{P}$ est d'ordre deux dans $\mathbb{k}$ et la 2-partie du groupe des classes de $\mathbb{k}$ est engendrée par les classes de $\mathcal{H}_0$ et de $\mathcal{P}$. ■

PROPOSITION 20. *On garde les notations et les hypothèses des propositions précédentes et on suppose de plus que $\left(\frac{2}{p}\right) = -1$. Alors l'idéal $\mathcal{H}_0\mathcal{P}$ capitule dans $\mathbb{k}(\sqrt{2p})$.*

Preuve. Dans ce cas l'unité fondamentale de $\mathbb{Q}(\sqrt{2p})$, $\varepsilon_2 = x + y\sqrt{2p}$, est de norme -1. D'où

$$\begin{cases} x - i = (1+i)\pi y_1^2, \\ x + i = (1-i)\pi' y_2^2, \end{cases}$$

avec $\pi = b+ci$ ou $i(b+ci)$, où π' est le conjugué de π et $y = y_1y_2$. Comme b et c jouent un rôle symétrique, on suppose que $\pi = b+ci$. Alors on a que $\sqrt{\varepsilon_2} = \frac{1}{2}(y_1\sqrt{(1+i)\pi} + y_2\sqrt{(1-i)\pi'})$. D'autre part, l'idéal $\mathcal{H}_0\mathcal{P}$ devient principal dans $\mathbb{k}(\sqrt{2p})$ si et seulement si l'équation en α, $(1+i)\pi\varepsilon = \alpha^2$ où ε est une unité de $\mathbb{k}(\sqrt{2p})$, est résoluble dans $\mathbb{k}(\sqrt{2p})$. Si $\alpha = \alpha_1 + \alpha_2 i$ avec α_1 et α_2 deux nombres réels et ε est une unité réelle, alors

$$\alpha_1 = \sqrt{\frac{\varepsilon(b' \pm \sqrt{2p})}{2}} \quad \text{et} \quad \alpha_2 = \frac{c'\varepsilon}{2\alpha_1} \quad \text{avec } b' = b-c \text{ et } c' = b+c.$$

De plus,

$$\sqrt{b' + \sqrt{2p}} = \sqrt{\frac{(1+i)\pi}{2}} + \sqrt{\frac{(1-i)\pi'}{2}}.$$

Il est clair que si $\varepsilon = \varepsilon_2$, alors α_1 et α_2 appartiennent à $\Bbbk(\sqrt{2p})$. Par suite, l'idéal $\mathcal{H}_0\mathcal{P}$ devient principal dans $\Bbbk(\sqrt{2p})$. ■

Théorème 21. *Soient* $\Bbbk = \mathbb{Q}(\sqrt{2pq}, i)$, $\Bbbk_2^{(1)}$ *le* 2-*corps de classes de Hilbert de* $\Bbbk$, $\Bbbk_2^{(2)}$ *le* 2-*corps des classes de Hilbert de* $\Bbbk_2^{(1)}$ *et* G_2 *le groupe de Galois de* $\Bbbk_2^{(2)}/\Bbbk$. *Suivant trois cas*, *le type des sous-corps de* $\Bbbk_2^{(1)}$, *quadratique sur* $\Bbbk$, *est donné dans le tableau ci-dessous* :

	$\Bbbk(\sqrt{2})$	$\Bbbk(\sqrt{p})$	$\Bbbk(\sqrt{2p})$
$\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = \left(\frac{p}{q}\right) = -1$	A	A	A
$\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = -1,\ \left(\frac{p}{q}\right) = 1$	A	B	B
$\left(\frac{2}{p}\right) = \left(\frac{p}{q}\right) = -1,\ \left(\frac{2}{q}\right) = 1$	B	A	B

En particulier, *si* $\mathbb{F} = \Bbbk(\sqrt{2p})$ *et* $\mathbf{C}_{\Bbbk,\mathbb{F}}$ *est le sous-groupe de* $\mathbf{C}_{\Bbbk}$ *associé à* $\mathbb{F}$ *par la théorie des corps de classes*, *alors dans le premier cas*, $\mathbf{C}_{\Bbbk,\mathbb{F}}$ *ne contient ni* $\mathcal{H}_0$ *ni* $\mathcal{P}$, *tandis que dans les deux autres cas il contient exactement l'un d'eux. De plus*, *le groupe* G_2 *est isomorphe au groupe des quaternions* Q_3 *dans le premier cas*, *tandis que dans les deux autres cas il est isomorphe à* Q_m *où* $4 \le m$.

Preuve. Soient b et c deux entiers tels que $p = b^2 + c^2$, $\mathcal{H}_0$ l'idéal premier de $\Bbbk$ au-dessus de $(1+i)$ et $\mathcal{P}$ l'idéal premier de $\Bbbk$ au-dessus de $(b+ci)$. On remarque les faits suivants.

L'idéal $\mathcal{H}_0$ capitule dans $\Bbbk(\sqrt{2})$ et il se décompose complètement dans $\Bbbk(\sqrt{2})/\Bbbk$ si et seulement $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = -1$. Dans ce cas, le corps $\Bbbk(\sqrt{2})$ est de type (A). Dans le cas contraire, $\Bbbk(\sqrt{2})$ est de type (B).

De plus, si $\left(\frac{2q}{p}\right) = 1$, alors $\mathcal{P}$ capitule dans $\Bbbk(\sqrt{p}) = \mathbb{Q}(\sqrt{p}, \sqrt{2q}, i)$ et se décompose complètement dans $\Bbbk(\sqrt{p})/\Bbbk$. D'où $\mathcal{P}$ est norme dans $\Bbbk(\sqrt{p})/\Bbbk$. Donc le corps $\Bbbk(\sqrt{p})$ est de type (A). Dans le cas contraire, $\Bbbk(\sqrt{p})$ est de type (B).

Si $\left(\frac{2q}{p}\right) = -1$, on a :

1) Soit $p \equiv 1 \bmod 8$ et $\left(\frac{q}{p}\right) = -1$. Alors, d'après la preuve du théorème 16, la condition $Q = 1$ entraîne que $\left(\frac{q}{p}\right) = 1$ ou bien $\left(\frac{2}{p}\right) = \left(\frac{q}{p}\right)$. Par suite ce cas est impossible.

2) Soit $p \equiv 5 \bmod 8$ et $\left(\frac{q}{p}\right) = 1$. Alors $\mathcal{H}_0\mathcal{P}$ capitule dans $\mathbb{k}(\sqrt{2p})$. Comme $\mathcal{H}_0$ est inerte dans $\mathbb{k}(\sqrt{2p})/\mathbb{k}$, alors $\mathcal{H}_0\mathcal{P}$ n'est pas norme dans $\mathbb{k}(\sqrt{2p})/\mathbb{k}$. Par suite, $\mathbb{k}(\sqrt{2p})$ est de type (B). De plus, dans ce cas $\mathbb{k}(\sqrt{2})$ est de type (A).

En utilisant le théorème 4 le résultat s'ensuit.

Remerciement. Je remercie vivement le rapporteur de mon article pour ses precieuses remarques.

Bibliographie

[Az-93] A. Azizi, *Capitulation des 2-classes d'idéaux de* $\mathbb{Q}(\sqrt{d}, i)$, thèse, Université Laval-Québec-Canada, 1993.

[Az-97] —, *Sur la capitulation des 2-classes d'idéaux de* $\mathbb{Q}(\sqrt{d}, i)$, C. R. Acad. Sci. Paris Sér. I 325 (1997), 127–130.

[Az-99:1] —, *Sur le groupe de classes d'idéaux de* $\mathbb{Q}(\sqrt{d}, i)$, Rend. Circ. Mat. Palermo (2) 48 (1999), 71–92.

[Az-99:2] —, *Unités de certains corps de nombres imaginaires et abéliens sur* $\mathbb{Q}$, Ann. Sci. Math. Québec 23 (1999), 87–93.

[H-Y-90] M. Hirabayashi and K. I. Yoshino, *Unit indices of imaginary abelian number fields of type* $(2, 2, 2)$, J. Number Theory 34 (1990), 346–361.

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

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

[Kur-43] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sec. I 4 (1943), 383–406.

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

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

[Te-71] F. Terada, *A principal ideal theorem in the genus fields*, Tôhoku Math. J. (2) 23 (1971), 697–718.

Département de Mathématiques
Faculté des Sciences
Université Mohammed 1
Oujda, Maroc
E-mail: azizi@sciences.univ-oujda.ac.ma

Reçu le 11.5.1999
et révisé le 28.1.2000 (3600)