THEORIE DES NOMBRES
BESANÇON

Années 1979-1980
et 1980-1981

$\mathbb{Z}$-BASES D'ENTIERS 1, ϑ, ϑ^2, ϑ^3 DANS LES EXTENSIONS CYCLIQUES DE DEGRE 4 DE $\mathbb{Q}$

Marie-Nicole GRAS

$\mathbb{Z}$-bases d'entiers $1, \vartheta, \vartheta^2, \vartheta^3$ dans les extensions cycliques de degré 4 de $\mathbb{Q}$

par Marie-Nicole GRAS

Introduction :

Soit $K/\mathbb{Q}$ une extension cyclique de degré 4 de $\mathbb{Q}$; soit A l'anneau des entiers de K ; A est dit est monogène s'il admet une $\mathbb{Z}$-base d'entiers de la forme $1, \vartheta, \vartheta^2, \vartheta^3$. Nous donnons des conditions nécessaires et suffisantes pour que A soit monogène ; nous montrons qu'il n'y a que deux tels corps imaginaires monogènes et nous déterminons tous les corps K réels monogènes de conducteur $f \leq 4000$ (il y en a 12 sur 1536, soit 0,78 %) ; nous étudions la monogénéité des corps K dont le sous-corps quadratique est $\mathbb{Q}(\sqrt{5})$. La monogénéité des corps cycliques de degré 4 a été étudiée indépendamment par T. Nakahara ([3] et [4]) et nous retrouvons certains de ses résultats.

1 - Rappels et notations :

Soit $K/\mathbb{Q}$ une extension cyclique de degré 4, soit $G = \langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$, et soit k le sous-corps quadratique de K. Soient f le conducteur de K, m celui de k ; alors f est de la forme mg, $g \in \mathbb{N}^*$, et le discriminant de K est égal à $m f^2$. On rappelle que si m est impair, alors g est soit impair, soit égal à $4g'$ ou $8g'$, g' impair, et que si m est pair, alors $m = 8m'$ et $g = 2g'$, m' et g' impairs.

Soit χ l'un des deux caractères de Dirichlet associés à K (caractère de $\mathrm{Gal}\left(\mathbb{Q}^{(f)}/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/f\mathbb{Z}\right)^*$, dont le noyau est $\mathrm{Gal}\left(\mathbb{Q}^{(f)}/K\right)$) ; on a $\chi(-1) = \pm 1$ et le corps K est réel si et seulement si $\chi(-1) = +1$.

D'après les résultats de [2], rappelés dans [1], p. 2 et 3 dans le cas réel, K est caractérisé par la donnée du triplet $(f, |a|, |b|)$, où $m = a^2 + b^2$, $b \equiv 0 (2)$; on a alors $K = \mathbb{Q}(\psi)$, où $\psi = \sqrt{\chi(-1)\, g\sqrt{m}\, \frac{\sqrt{m}+a}{2}}$.

Tout élément ϑ de K s'écrit de manière unique :

$\vartheta = \dfrac{t+z\sqrt{m}+2x\psi+2y\psi^{\sigma}}{4}$, où t, z, x, y $\in \mathbb{Q}$, et $\vartheta \in A$ si et seulement si t, z, x, y $\in \mathbb{Z}$ et vérifient les conditions supplémentaires suivantes :

$$(0)\quad \begin{cases} \text{(i) si } m \text{ est impair : } t \equiv z(2)\ ,\ \dfrac{t+z}{2} \equiv gx\,(2) \text{ et } \dfrac{t-z}{2} \equiv gy\,(2)\,, \\ \text{(ii) si } m \text{ est pair : } t \equiv 0(4) \text{ et } z \equiv 0(2). \end{cases}$$

2 - Conditions nécessaires et suffisantes de monogénéité :

Théorème 1 : Soit $K/\mathbb{Q}$ une extension cyclique de degré 4, de conducteur $f = mg$, où $m = a^2 + b^2$, $b \equiv 0(2)$, est le conducteur du sous-corps quadratique de K. L'anneau A des entiers de K admet une $\mathbb{Z}$-base 1, ϑ, ϑ^2, ϑ^3 si et seulement s'il existe x, y, z $\in \mathbb{Z}$ tels que :

$$(1)\qquad \begin{cases} b\left(x^2 - y^2\right) + 2\,a\,x\,y = \pm 2 \\ m\left[z^2 - \chi(-1)\,g\,(x^2+y^2)\right]^2 - 4\,g^2 = \pm 16. \end{cases}$$

Démonstration :

Soit ϑ un entier de K tel que 1, ϑ, ϑ^2, ϑ^3 soit une $\mathbb{Z}$-base d'entiers de K ; alors nécessairement $\Delta(\vartheta) = m\,f^2 = m^3\,g^2$.

Soit $\vartheta = \dfrac{t+z\sqrt{m}+2x\psi+2y\psi^{\sigma}}{4}$; en appliquant les formules de H. Hasse (voir [1] p. 4, pour le cas réel), on obtient :

$\left(\vartheta-\vartheta^{\sigma^2}\right)\left(\vartheta^{\sigma}-\vartheta^{\sigma^3}\right) = -\dfrac{b(x^2-y^2)+2axy}{2}\,\chi(-1)\,g\sqrt{m}$ que nous notons $\alpha\,g\sqrt{m}$,

$$\text{et } N_{K/\mathbb{Q}}\left(\vartheta-\vartheta^{\sigma}\right) = \frac{\left[m z^2 - \chi(-1)\,f\,(x^2+y^2)\right]^2 - m g^2\left[b(x^2-y^2) + 2axy\right]^2}{16}$$

$$= m\,\frac{m\left[z^2-\chi(-1)\,g(x^2+y^2)\right]^2 - g^2\left[b(x^2-y^2)+2axy\right]^2}{16},$$

noté $m\beta$.

Donc $\Delta(\vartheta)^{\frac{1}{2}} = \alpha\beta\,g\,m\sqrt{m}$; il est donc nécessaire d'avoir $\alpha\beta = \pm 1$; mais on vérifie facilement que l'hypothèse ϑ entier de K entraine $\alpha, \beta \in \mathbb{Z}$; donc $\alpha = \pm 1$ et $\beta = \pm 1$, d'où les relations (1).

Réciproquement, s'il existe x, y, z solutions de (1), alors pour tout $t \in \mathbb{Z}$, $\vartheta = \dfrac{t + z\sqrt{m} + 2x\psi + 2y\psi^{\sigma}}{4}$ vérifie $\Delta(\vartheta) = mf^2$; il est facile de vérifier, en utilisant les conditions (0), que l'on peut choisir $t \in \mathbb{Z}$ de telle sorte que ϑ soit un entier de K.

Remarque 1 : Pour certaines familles de f impairs, en exprimant les entiers de K sur la base $1, \theta, \theta^{\sigma}, \theta^{\sigma^2}$, où $\theta = Tr_{\mathbb{Q}^{(f)}/K}(\zeta_f)$, T. Nakahara obtient dans [4] des conditions analogues à celles du Théorème 1.

Proposition 1 : Une condition nécessaire pour que K admette une $\mathbb{Z}$-base d'entiers $1, \vartheta, \vartheta^2, \vartheta^3$ est qu'il existe $c \in \mathbb{Z}$ tel que :

(2) $$g^2 \pm 4 = mc^2.$$

Démonstration :

D'après (1), m divise $4(g^2 \pm 4)$; si m est impair, m divise $g^2 \pm 4$; si m est pair, alors on a $g = 2g'$, g' impair, donc $g^2 \pm 4 \equiv 0\ (8)$ et $m(=8m')$ divise $g^2 \pm 4$. Il résulte de (1) qu'il existe $c \in \mathbb{Z}$ tel que $g^2 \pm 4 = mc^2$.

Conséquence : Si g est fixé, il n'existe q'un nombre fini de corps K qui admettent une base d'entiers $1, \vartheta, \vartheta^2, \vartheta^3$. En particulier :

(i) Si $g = 1$, c'est-à-dire si $f = m$, K n'admet pas de base $1, \vartheta, \vartheta^2, \vartheta^3$ sauf si $f = m = 5$ (si $g = 1$, $g^2 \pm 4 = 5$ ou -3, et si $f = m = 5$, $K = \mathbb{Q}^{(5)}$ est monogène).

(ii) Si $g = 2$, c'est-à-dire si $f = 2m$, K n'admet pas de base $1, \vartheta, \vartheta^2, \vartheta^3$ sauf si $m = 8$, $f = 16$ (et dans ce dernier cas, le corps imaginaire et le corps réel correspondants admettent effectivement une base).

Remarque 2 : Dans [4], T. Nakahara démontre (i) dans le cas où $f = m = p$, nombre premier.

Il résulte du théorème 1 et de la proposition 1 :

Théorème 1' : Avec les notations du théorème 1, A est monogène si et seulement s'il existe $c, x, y, z \in \mathbb{Z}$ tels que :

(2) $$g^2 \pm 4 = m\,c^2$$

et

$$(3) \qquad \begin{cases} b(x^2 - y^2) + 2axy = \pm 2 \\ z^2 - \chi(-1)g(x^2+y^2) = \pm 2c . \end{cases}$$

Remarque 3 : A l'aide du théorème 1', nous retrouvons les familles suivantes de corps monogènes trouvées par T. Nakahara dans [4] : soit d un entier impair ; soit $g = d^2 \pm 2$, $a = g$, $b = 2$ et $m = a^2 + b^2$; si g et m sont sans facteur carré, alors il existe un corps cyclique de degré 4 sur $\mathbb{Q}$ défini par g et $m = a^2 + b^2$; ce corps est réel et monogène.

En effet, avec les hypothèses énoncées, on a $g \equiv 3(4)$, $m \equiv 1(4)$, $m \not\equiv 1(8)$ et $(g,m) = 1$. Il résulte des conditions énoncées dans [1], I, 1) qu'il existe un corps $K/\mathbb{Q}$ cyclique de degré 4 défini par g et $m = g^2+4$ et que ce corps est réel. Le corps obtenu est monogène car la condition nécessaire (2) est vérifiée avec $c = 1$ et alors le système (3) admet la solution $x = 1$, $y = 0$ et $z = d$.

Remarque 4 : Nous ne savons pas si ces deux familles de corps sont infinies ; nous conjecturons qu'elles le sont.

3 - Cas des corps imaginaires :

Lorsque $K/\mathbb{Q}$ est imaginaire, $\chi(-1) = -1$ et d'après le théorème 1', A est monogène si et seulement s'il existe $c, x, y, z \in \mathbb{Z}$ tels que :

$$(2) \qquad g^2 \pm 4 = mc^2$$

$$(3') \qquad \begin{cases} b(x^2 - y^2) + 2axy = \pm 2 \\ z^2 + g(x^2+y^2) = \pm 2c \qquad (g > 0). \end{cases}$$

On a alors le résultat suivant :

Proposition 2 : Il n'existe que deux corps cycliques imaginaires de degré 4 sur $\mathbb{Q}$, admettant une $\mathbb{Z}$-base d'entiers $1, \vartheta, \vartheta^2, \vartheta^3$; ce sont $K_1 = \mathbb{Q}^{(5)}$ et $K_2 = \mathbb{Q}\left(\zeta - \zeta^{-1}\right)$, où ζ est une racine $16^{\text{ème}}$ de l'unité.

Démonstration :

Les valeurs possibles pour m sont : $m = 5$, $m = 8$ et $m \geq 13$.

1er cas : Si $m \geq 13$, alors $\dfrac{g^2}{c^2} = m \pm \dfrac{4}{c^2} \geq m - 4 \geq 9$, donc $g \geq 3c$ et alors $z^2 + g(x^2+y^2) \geq 3c$ et (3') est impossible.

2ème cas : Si $m = 8$, on doit avoir $g^2 - 8c^2 = \pm 4$; si $g = 2$ et $c = 1$, alors (3') admet la solution $x = 1$, $y = 0$, $z = 0$ et le corps K_2 est monogène. Si $c \geq 2$, alors $\frac{g}{c} > 2\sqrt{2}\sqrt{1 - \frac{1}{2c^2}} > 2.6$, et (3') est impossible.

3ème cas : Si $m = 5$, on doit avoir $g^2 - 5c^2 = \pm 4$; si $g = 1$ et $c = 1$, alors le corps est imaginaire, (3') admet la solution $x = 1$, $y = 0$, $z = 1$, et le corps K_1 est monogène. Si $c \geq 2$, pour que le corps K soit imaginaire, il est nécessaire d'avoir $c \geq 13$ (voir le § 6) ; alors $\frac{g}{c} > \sqrt{5}\sqrt{1 - \frac{4}{5c^2}} > 2.2$, et (3') est impossible.

4 - Conditions nécessaires de monogénéité :

Dans ce paragraphe, on suppose que K est réel et que la condition nécessaire (2) est vérifiée, c'est-à-dire qu'il existe $c \in \mathbb{Z}$ tel que $g^2 \pm 4 = mc^2$. On a alors :

Proposition 3 : Si l'une au moins des conditions suivantes est vérifiée, alors $K/\mathbb{Q}$ n'est pas monogène :

(i) $\pm 2b$ n'est pas reste quadratique modulo m (ou modulo un de ses diviseurs) ;

(ii) $\pm 2c$ n'est pas reste quadratique modulo g (ou modulo un de ses diviseurs) ;

(iii) l'unité fondamentale ε_0 de $\mathbb{Q}(\sqrt{m})$ est de norme $+1$;

(iv) $m \equiv 1\,(8)$;

(v) $m \equiv 0\,(8)$ et $c \equiv 0\,(2)$;

(vi) $a \equiv 0\,(3)$, $c \equiv 0\,(3)$ et $g \equiv 2\,(3)$;

(vi') $b \equiv 0\,(3)$, $c \equiv 0\,(3)$ et $g \equiv 1\,(3)$.

Démonstration :

(i) l'égalité $b(x^2 - y^2) + 2axy = \pm 2$ s'écrit $(bx + ay)^2 - my^2 = \pm 2b$;

(ii) résulte immédiatement de l'égalité $z^2 - g(x^2+y^2) = \pm 2c$;

(iii) on a l'identité $m(x^2+y^2)^2 = [a(x^2 - y^2) - 2bxy]^2 + [b(x^2-y^2) + 2axy]^2$;

si A est monogène, on a donc $m\left(x^2+y^2\right)^2 = [a(x^2-y^2)-2bxy]^2 + 4$,

et $\dfrac{a(x^2-y^2)-2bxy+(x^2+y^2)\sqrt{m}}{2}$ est une unité de norme -1 de $\mathbb{Q}(\sqrt{m})$;

(iv), (v), (vi) et (vi') se montrent en vérifiant que les conditions (2), (3) sont impossibles modulo une puissance de 2 ou 3 convenable.

D'après la proposition ci-dessus (iii) et (3), pour que A soit monogène, il est nécessaire qu'il existe $x, y \in \mathbb{Z}$ tels que $\dfrac{a(x^2-y^2)-2bxy+(x^2+y^2)\sqrt{m}}{2}$ soit une unité de norme -1 de $\mathbb{Q}(\sqrt{m})$ et $g(x^2+y^2) \mp 2c \in \mathbb{Z}^2$. Il est donc nécessaire qu'il existe $\alpha, \beta \in \mathbb{Z}$, $\beta > 0$ tels que $\dfrac{\alpha+\beta\sqrt{m}}{2}$ soit une unité de norme -1 de $\mathbb{Q}(\sqrt{m})$ et $g\beta \mp 2c \in \mathbb{Z}^2$.

D'où :

<u>Proposition 4</u> : Soit $\varepsilon_o = \dfrac{\alpha_1+\beta_1\sqrt{m}}{2}$, $\beta_1 > 0$, l'unité fondamentale de $\mathbb{Q}(\sqrt{m})$, supposée de norme -1 ; soit $\left(\beta_{2n+1}\right)_{n\geq 0}$ la suite définie par $\beta_{-1} = \beta_1$ et la relation de récurrence

$$\beta_{2n+3} = \left(\alpha_1^2+2\right)\beta_{2n+1} - \beta_{2n-1}. \tag{4}$$

Une condition nécessaire pour que A soit monogène est qu'il existe $n \geq 0$ tel que $g\beta_{2n+1} \mp 2c \in \mathbb{Z}^2$.

<u>Conséquence</u> : Soit p un nombre premier ; on étudie la relation de récurrence (4) modulo p^k, $k \in \mathbb{N}^*$. Les solutions sont périodiques, de période n_o ; si pour les n_o valeurs $\beta_1, \ldots, \beta_{2n_o-1}$, $g\beta_i \mp 2c$ n'est pas un carré modulo p^k, alors A n'est pas monogène.

5 - <u>Résultats numériques concernant les corps réels de conducteur $f \leq 4000$:</u>

Il y a 1536 corps réels cycliques de degré 4 sur $\mathbb{Q}$, de conducteur $f \leq 4000$ ([1]) ; parmi eux, il y en a 32 qui vérifient la condition nécessaire (2) : $g^2 \pm 4 = m\,c^2$. Parmi ces 32 corps, 12 admettent une base $1, \vartheta, \vartheta^2, \vartheta^3$. Les conditions nécessaires établies aux propositions 3 et 4 permettent de montrer que les autres corps n'admettent pas de base. La liste de ces 32 corps, ainsi que le résultat pour chacun d'eux, est donnée dans la table 1.

<u>Remarque 5</u> : Pour deux corps de conducteur $f \leq 4000$, seule la méthode de la proposition 4 a permis de conclure ; il s'agit des cas suivants :

(i) Soit K le corps défini par $f = 2379$, $m = 61$, $a = 5$, $b = 6$, $g = 39$; on a $c = 5$; on cherche à résoudre :

$$\begin{cases} 3(x^2 - y^2) + 5xy = \pm 1 \\ z^2 - 39(x^2 + y^2) = 10 \end{cases} \qquad (-10 \text{ est impossible modulo } 3).$$

L'unité fondamentale de $\mathbb{Q}(\sqrt{61})$ est $\varepsilon_o = \dfrac{39 + 5\sqrt{61}}{2}$; on considère la suite $(\beta_{2n-1})_{n \geq 0}$ définie par $\beta_{-1} = \beta_1 = 5$ et $\beta_{2n+3} = 1523\,\beta_{2n+1} - \beta_{2n-1}$; soit $z_n = 39\beta_{2n-1} + 10$; on constate que :

$$\left(\frac{z_n}{11}\right) = -1 \Leftrightarrow n \not\equiv 2, 4, 5, 8, 9, 11 \bmod 12 ;$$

$$\left(\frac{z_n}{23}\right) = -1 \Leftrightarrow n \not\equiv 2, 3, 6, 7, 10, 11 \bmod 12 ;$$

$$\left(\frac{z_n}{59}\right) = -1 \Leftrightarrow n \not\equiv 0, 1, 4, 5, 6, 7, 8, 9 \bmod 12 ;$$

d'où $z_n \notin \mathbb{Z}^2$, pour tout n.

(ii) De même, soit K le corps défini par $f = 3824$, $m = 8$, $a = 2$, $b = 2$, $g = 478$, $c = 169$ (-169 est impossible mod. 239). On vérifie avec des notations analogues que z_n n'est pas un carré modulo 16, 9 ou 5.

6 - <u>Corps réels au-dessus de $\mathbb{Q}(\sqrt{5})$:</u>

On suppose ici que le sous-corps quadratique de K est $\mathbb{Q}(\sqrt{5})$. On a alors $f = 5g$, et la condition nécessaire (2) s'écrit $g^2 \pm 4 = 5c^2$, donc $\dfrac{g + c\sqrt{5}}{2}$ est une unité de $\mathbb{Q}(\sqrt{5})$; on a donc ,

pour $j \geq 1$, $g = v_j$ (nombres de Lucas),

$c = u_j$ (nombres de Fibonnaci),

où u_j et v_j sont définis par :

$$u_o = 1 \qquad u_1 = 1 \qquad u_{j+2} = u_{j+1} + u_j ,$$

$$v_o = 2 \qquad v_1 = 1 \qquad v_{j+2} = v_{j+1} + v_j .$$

On a alors :

Lemme : Une condition nécessaire et suffisante pour que le corps K soit réel est que $j \equiv 2, 3, 4, 5, 8, 10, 11$ (12).

Démonstration :

On étudie $g = v_j$ modulo 16 et on applique le I), 1), (ii) de [1]. Il en résulte que :

si $j \equiv 1, 7, 9$ (12) le corps est imaginaire,

si $j \equiv 0$ (6), il n'y a pas de corps,

sinon, le corps est réel.

Proposition 5 : Une condition nécessaire et suffisante pour que le corps K de conducteur $f = 5\, v_j$ soit monogène est qu'il existe $n \geq 1$ et $s = \pm 1$ tels que $v_j\, u_{2n-1} + 2\,s\,u_j \in \mathbb{Z}^2$.

Démonstration :

La condition nécessaire résulte de la proposition 5.

La condition est suffisante : il est facile de vérifier que pour tout $n \geq 1$, on a $u_{2n-1} = u_n^2 + u_{n-1}^2$

et $u_n^2 - u_{n-1}^2 - u_n\, u_{n-1} = (-1)^{n-1}$.

Il en résulte que $x = u_n$, $y = -u_{n-1}$ et z tel que $v_j\, u_{2n-1} + 2\,s\,u_j = z^2$ vérifient (3).

Conséquence : On étudie si la double suite $v_j\, u_{2n-1} + 2\,s\,u_j$ est un carré modulo une puissance d'un nombre premier ; elle est doublement périodique, de périodes n_o et j_o. Par exemple, si l'on considère les modules suivants, dont la période n_o divise 240 (alors j_o divise 480) : 2^4, 3^2, 5, 7, 11, 23, 31, 41, 47, 61, 241, 1103, 1601, 2161, 2521, 3041 et 20641, on trouve (en ne considérant que les corps réels) qu'il est nécessaire d'avoir $j \equiv 2, 3, 4, 5, 8, 11, 15, 80, 160, 161, 164, 171, 238, 239, 242, 243, 316, 317, 320, 400, 411, 472, 476, 478$ ou 479 modulo 480.

Remarque 6 : Pour les 7 premières valeurs de j, les corps correspondants admettent effectivement une $\mathbb{Z}$-base $1, \vartheta, \vartheta^2, \vartheta^3$ (cf table 2). Pour les valeurs de j restantes comprises entre 80 et 316, on vérifie que la suite $\left(v_j\, u_{2n-1} + 2s\, u_j\right)_n$ n'est pas un carré (modulo d'autres nombres premiers). Il en résulte que A n'est pas monogène si son conducteur $f = 5g$ est tel que

$$6820 < f < 8.10^{66} .$$

Nous ne savons pas s'il existe ou non une infinité de corps K de sous-corps quadratique $\mathbb{Q}(\sqrt{5})$ qui soient monogènes.

7 - Tables numériques :

Table 1 :

Cette table donne la liste des 32 corps K de conducteur $f = mg$, $f < 4000$ vérifiant la condition nécessaire (2) : $g^2 \pm 4 = mc^2$. Pour chaque corps, on donne la valeur de f, m, a, b, g, c, les conditions (3) et le résultat :

oui et des valeurs de x, y, z, si le corps est monogène,

non et une raison, si le corps n'est pas monogène.

f	m	a	b	g	c	conditions (3)	résultat
15	5	1	2	3	1	$x^2 - y^2 + xy = \pm 1$ $z^2 - 3(x^2+y^2) = \pm 2$	oui $x = 1$ $y = 0$ $z = 1$
16	8	2	2	2	1	$x^2 - y^2 + 2xy = \pm 1$ $z^2 - 2(x^2+y^2) = \pm 2$	oui $x = 1$ $y = 0$ $z = 0$
20	5	1	2	4	2	$x^2 - y^2 + xy = \pm 1$ $z^2 - 4(x^2+y^2) = \pm 4$	oui $x = 1$ $y = 0$ $z = 0$
35	5	1	2	7	3	$x^2 - y^2 + xy = \pm 1$ $z^2 - 7(x^2+y^2) = \pm 6$	oui $x = 1$ $y = 0$ $z = 1$
39	13	3	2	3	1	$x^2 - y^2 + 3xy = \pm 1$ $z^2 - 3(x^2+y^2) = \pm 2$	oui $x = 1$ $y = 0$ $z = 1$
48	8	2	2	6	2	$x^2 - y^2 + 2xy = \pm 1$ $z^2 - 6(x^2+y^2) = \pm 4$	non $m \equiv 0 (8)$ et $c \equiv 0 (2)$
55	5	1	2	11	5	$x^2 - y^2 + xy = \pm 1$ $z^2 - 11(x^2+y^2) = \pm 10$	oui $x = 1$ $y = 0$ $z = 1$
112	8	2	2	14	5	$x^2 - y^2 + 2xy = \pm 1$ $z^2 - 14(x^2+y^2) = \pm 10$	oui $x = 1$ $y = 0$ $z = 2$
136	17	1	4	8	2	$2(x^2 - y^2) + xy = \pm 1$ $z^2 - 8(x^2+y^2) = \pm 4$	non $m \equiv 1 (8)$
143	13	3	2	11	3	$x^2 - y^2 + 3xy = \pm 1$ $z^2 - 11(x^2+y^2) = \pm 6$	non $a \equiv c \equiv 0 (3)$, $g \equiv 2 (3)$
235	5	1	2	47	21	$x^2 - y^2 + xy = \pm 1$ $z^2 - 47(x^2+y^2) = \pm 42$	oui $x = 8$ $y = -5$ $z = 65$
240	40	6	2	6	1	$x^2 - y^2 + 6xy = \pm 1$ $z^2 - 6(x^2+y^2) = \pm 2$	oui $x = 1$ $y = 0$ $z = 2$

f	m	a	b	g	c	conditions (3)	résultat
240	40	2	6	6	1	$3(x^2-y^2)+2xy=\pm 1$ $z^2-6(x^2+y^2)=\pm 2$	non $\left(\frac{\pm 3}{5}\right)=-1$
272	8	2	2	34	12	$x^2-y^2+2xy=\pm 1$ $z^2-34(x^2+y^2)=\pm 24$	non $m\equiv 0(8)$ et $c\equiv 0(2)$
371	53	7	2	7	1	$x^2-y^2+7xy=\pm 1$ $z^2-7(x^2+y^2)=\pm 2$	oui $x=1$ $y=0$ $z=3$
615	5	1	2	123	55	$x^2-y^2+xy=\pm 1$ $z^2-123(x^2+y^2)=\pm 110$	non $\left(\frac{\pm 110}{41}\right)=-1$
656	8	2	2	82	29	$x^2-y^2+2xy=\pm 1$ $z^2-82(x^2+y^2)=\pm 58$	non $\left(\frac{\pm 58}{41}\right)=-1$
995	5	1	2	199	89	$x^2-y^2+xy=\pm 1$ $z^2-199((x^2+y^2)=\pm 178$	oui $x=1$ $y=-1$ $z=24$
1040	104	10	2	10	1	$x^2-y^2+10xy=\pm 1$ $z^2-10(x^2+y^2)=\pm 2$	non $\left(\frac{\pm 2}{5}\right)=-1$
1040	104	2	10	10	1	$5(x^2-y^2)+2xy=\pm 1$ $z^2-10(x^2+y^2)=\pm 2$	non $\left(\frac{\pm 2}{5}\right)=-1$
1520	40	6	2	38	6	$x^2-y^2+6xy=\pm 1$ $z^2-38(x^2+y^2)=\pm 12$	non $m\equiv 0(8)$ et $c\equiv 0(2)$
1520	40	2	6	38	6	$3(x^2-y^2)+2xy=\pm 1$ $z^2-38(x^2+y^2)=\pm 12$	non $m\equiv 0(8)$ et $c\equiv 0(2)$
1547	13	3	2	119	33	$x^2-y^2+3xy=\pm 1$ $z^2-119(x^2+y^2)=\pm 66$	non $a\equiv c\equiv 0(3)$; $g\equiv 2(3)$
2020	101	1	10	20	2	$5(x^2-y^2)+xy=\pm 1$ $z^2-20(x^2+y^2)=\pm 4$	oui $x=1$ $y=1$ $z=6$

f	m	a	b	g	c	conditions (3)		résultat
2379	61	5	6	39	5	$3(x^2-y^2)+5xy=\pm 1$ $z^2-39(x^2+y^2)=\pm 10$	non	rmq 5
2703	53	7	2	51	7	$x^2-y^2+7xy=\pm 1$ $z^2-51(x^2+y^2)=\pm 14$	non	$\left(\frac{\pm 14}{17}\right)=-1$
3315	221	11	10	15	1	$5(x^2-y^2)+11xy=\pm 1$ $z^2-15(x^2+y^2)=\pm 2$	non	$N(\varepsilon_o)=+1$
3315	221	5	14	15	1	$7(x^2-y^2)+5xy=\pm 1$ $z^2-15(x^2+y^2)=\pm 2$	non	$N(\varepsilon_o)=+1$
3435	229	15	2	15	1	$x^2-y^2+15xy=\pm 1$ $z^2-15(x^2+y^2)=\pm 2$	non	$\left(\frac{\pm 2}{5}\right)=-1$
3480	145	9	8	24	2	$4(x^2-y^2)+9xy=\pm 1$ $z^2-24(x^2+y^2)=\pm 4$	non	$m\equiv 1\ (8)$
3480	145	1	12	24	2	$6(x^2-y^2)+xy=\pm 1$ $z^2-24(x^2+y^2)=\pm 4$	non	$m\equiv 1\ (8)$
3824	8	2	2	478	169	$x^2-y^2+2xy=\pm 1$ $z^2-478(x^2+y^2)=\pm 338$	non	rmq 5

Table 2 :

Cette table donne, pour j variant de 1 à 24, la liste des v_j(=g) et u_j(=c), la "nature" du corps correspondant obtenu (imaginaire, réel, pas de corps), et lorsque ce dernier est réel le résultat :

oui et des valeurs de s, x, y, z si le corps est monogène,

non s'il n'est pas monogène (la raison en est donné par la conséquence de la proposition 5).

j	v_j	u_j	corps	résultat	s	x	y	z
1	1	1	imaginaire					
2	3	1	réel	oui	-1	1	0	1
3	4	2	réel	oui	-1	1	0	0
4	7	3	réel	oui	-1	1	0	1
5	11	5	réel	oui	-1	1	0	1
6	18	8	pas de corps					
7	29	13	imaginaire					
8	47	21	réel	oui	+1	8	-5	65
9	76	34	imaginaire					
10	123	55	réel	non				
11	199	89	réel	oui	+1	1	-1	24
12	322	144	pas de corps					
13	521	233	imaginaire					
14	843	377	réel	non				
15	1364	610	réel	oui	-1	1	0	12
16	2207	987	réel	non				
17	3571	1597	réel	non				
18	5778	2584	pas de corps					
19	9349	4181	imaginaire					
20	15127	6765	réel	non				
21	24476	10946	imaginaire					
22	39603	17711	réel	non				
23	64079	28657	réel	non				
24	103682	46368	pas de corps					

BIBLIOGRAPHIE

[1] GRAS M.N.
Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$.
Publ. Math. Univ. de Besançon, fasc. 2, 1977-78.

[2] HASSE H.
Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern.
Abh. Deutsch. Akad. Wiss. Berlin, Math. (1948), n°2, p. 1-95.

[3] NAKAHARA T.
On a power basis of the integer ring in an abelian biquadratic field (en japonais).
Surikaisekikenkyusho Kokyuroku, n°371, p. 31-46, (1979).

[4] NAKAHARA T.
On cyclic biquadratic fields related to a problem of Hasse, preprint.

Marie-Nicole GRAS
Laboratoire de Mathématiques
E.R.A. - C.N.R.S. n° 070654
Faculté des Sciences
25030 BESANÇON CEDEX