COURS DE L'INSTITUT FOURIER

J. J. PAYAN

Chapitre I Sur le groupe des classes d'un corps quadratique

Cours de l'institut Fourier, tome 7 (1972), p. 2-30

<http://www.numdam.org/item?id=CIF_1972__7__2_0>

CHAPITRE I

SUR LE GROUPE DES CLASSES D'UN CORPS QUADRATIQUE

Dans ce chapitre, on se propose de donner des méthodes tant théoriques qu'algorithmiques permettant de déterminer l'ordre et la structure du groupe des classes d'idéaux d'un corps quadratique.

1. RAPPELS SUR LES CORPS QUADRATIQUES.

Soit k un corps quadratique, c'est-à-dire une extension de degré 2 du corps $\mathbb{Q}$ des nombres rationnels. Soit O_k l'anneau des entiers de k et soient respectivement I_k et P_k le groupe des idéaux fractionnaires et le groupe des idéaux fractionnaires principaux de k. Le groupe $H_k = I_k/P_k$, appelé groupe des classes d'idéaux de k est un groupe fini.

Le corps k étant fixé, on sait qu'il existe un entier rationnel sans facteur carré m tel que $k = \mathbb{Q}(\sqrt{m})$. On sait aussi que O_k est un $\mathbb{Z}$-module libre de rang 2 dont une $\mathbb{Z}$-base est $\{1, \theta\}$ avec :

$\theta = \frac{1}{2}(1+\sqrt{m})$ si m est congru à 1 modulo 4

$\theta = \sqrt{m}$ sinon:

On appelle polynôme fondamental de k le polynôme $X^2 - SX + P = F(X)$ dont les coefficients sont définis comme suit :

$(S,P) = (1,\frac{1}{4}(1-m))$ si m est congru à 1 modulo 4

$(S,P) = (0,-m)$ sinon.

Il est clair, dans ces conditions que k est le corps de décomposition de $X^2 - SX + P$ ou encore que $X^2 - SX + P = \mathrm{Irr}(\theta,\mathbb{Q},X)$.

Remarquons encore avant d'entrer dans le vif du sujet que si M_1 et M_2 sont deux sous-$\mathbb{Z}$-modules de O_k , libres de rang 2 et tels que $M_1 \subset M_2$, les discriminants Δ_1 et Δ_2 de M_1 et de M_2 sont liés par une égalité

$$\Delta_1 = \Lambda^2 . \Delta_2 \quad \text{avec} \quad \Lambda \in \mathbb{Z}\setminus\{0\} .$$

De plus, on a $M_1 = M_2$ si et seulement si $\Lambda^2 = 1$.

2. IDEAUX SANS FACTEUR RATIONNEL.

Si on veut déterminer la structure du groupe des classes d'idéaux de k , il faut pouvoir caractériser un système de représentants aussi maniables que possible. Remarquons en premier lieu que ces représentants peuvent être choisis entiers.

Lemme 2.1.

Soit $\mathfrak{a}$ un idéal entier de k et soit $J(\mathfrak{a})$ l'ensemble

$$J(\mathfrak{a}) = \{x\in\mathbb{Q} \ ; \ x\mathfrak{a} \subset O_k\} .$$

Il existe $q \in \mathbb{Z}\setminus\{0\}$ tel que $J(\mathfrak{a}) = (q^{-1})\mathbb{Z}$.

Démonstration : L'idéal $\mathfrak{a}$ est un sous $\mathbb{Z}$-module libre de rang 2 de O_k . Soit $\{a_1,a_2\}$ une $\mathbb{Z}$-base de $\mathfrak{a}$ et soient $\alpha_1,\alpha_2,\beta_1,\beta_2$ les entiers rationnels tel que $a_1 = \alpha_1 + \beta_1\theta$, $a_2 = \alpha_2 + \beta_2\theta$. Puisque $\mathfrak{a}$ est un idéal entier on a $\mathbb{Z} \subset J(\mathfrak{a})$. Il suffit donc de déterminer l'ensemble $\{p\in\mathbb{Z}\setminus\{0\} \mid \frac{1}{p}\mathfrak{a} \subset O_k\}$. Cet ensemble est l'ensemble des diviseurs du P.G.C.D. de $(\alpha_1,\alpha_2,\beta_1,\beta_2)$ soit δ . On a donc

$$J(\delta) = \frac{1}{\delta}.\mathbb{Z} .$$

On vérifiera sans peine que δ ne dépend pas de la $\mathbb{Z}$-base choisie pour $\mathfrak{a}$.

Notations et définition 2.2.

Soit $\mathfrak{a}$ un idéal entier de k . On pose :

$$J_e(\mathfrak{a}) = J(\mathfrak{a}).O_k$$

et

$$\mathfrak{a}_1 = J_e(\mathfrak{a}).\mathfrak{a} \ .$$

Il est clair que l'idéal $\mathfrak{a}_1$ est entier et que $\mathfrak{a} = (q).\mathfrak{a}_1$. L'idéal entier $\mathfrak{a}$ est dit sans facteur rationnel si $q \in \{-1,+1\}$.

Remarque : Toute classe d'idéaux de k contient un idéal entier sans facteur rationnel. En effet, si $\mathfrak{a} = (q)\mathfrak{a}_1$, on a $Cl(\mathfrak{a}) = Cl(\mathfrak{a}_1)$ et l'idéal $\mathfrak{a}_1$ est sans facteur rationnel.

Proposition 2.3.

Soit $\mathfrak{a} = \prod_{i=1}^{\ell} \mathfrak{p}_i^{n_i}$ un idéal entier de k donné par sa décomposition en facteurs premiers. Les deux propriétés suivantes sont équivalentes :

A - L'idéal $\mathfrak{a}$ est sans facteur rationnel.

B - Soit $\mathfrak{p}$ un idéal premier de k .

si $\mathfrak{p}$ divise $\mathfrak{a}$, il est de degré 1 .

si $\mathfrak{p}$ est ramifié et divise $\mathfrak{a}$, $\mathfrak{p}^2$ ne divise pas $\mathfrak{a}$.

si $\mathfrak{p}$ est décomposé et divise $\mathfrak{a}$ son conjugué $\bar{\mathfrak{p}}$ ne divise pas $\mathfrak{a}$.

Démonstration : A implique B . Soit $\mathfrak{p}$ un idéal premier qui divise $\mathfrak{a}$. L'idéal $\mathfrak{p}$ ne peut être inerte, sinon $\mathfrak{p} = pO_k$ est principal et le nombre p^{-1} appartient à $J(\mathfrak{a})$. Si $\mathfrak{p}$ est ramifié on a $\mathfrak{p}^2 = pO_k$ si $\mathfrak{p}|p$. Donc l'exposant de $\mathfrak{p}$ dans $\mathfrak{a}$ est au plus égal à 1 . Enfin, si $\mathfrak{p}$ est décomposé de norme p on a $\mathfrak{p}.\bar{\mathfrak{p}} = pO_k$. Par conséquent si $\mathfrak{p}$ divise $\mathfrak{a}$, $\bar{\mathfrak{p}}$ ne divise pas $\mathfrak{a}$.

B implique A . Même type de raisonnement.

3. BASES D'IDEAUX SANS FACTEUR RATIONNEL.

Proposition 3.1.

Soit $\mathfrak{a}$ un idéal entier de k. Les deux assertions suivantes sont équivalentes :

1) L'idéal $\mathfrak{a}$ est sans facteur rationnel.

2) Les anneaux quotients $O_k/\mathfrak{a}$ et $\mathbb{Z}/N(\mathfrak{a})$ sont isomorphes.

Démonstration : L'homorphisme canonique d'anneaux $Z \to O_k/\mathfrak{a}$ a pour noyau $\mathfrak{a} \cap \mathbb{Z}$. On a donc un homomorphisme injectif $\varphi : \mathbb{Z}/\mathfrak{a}\cap\mathbb{Z} \to O_k/\mathfrak{a}$. Un tel homomorphisme est un isomorphisme si et seulement si les deux anneaux ont même cardinal. On est donc amené à montrer que $\mathfrak{a}$ est sans facteur rationnel si et seulement si $\mathfrak{a}\cap\mathbb{Z} = N(\mathfrak{a})\mathbb{Z}$. On peut écrire la décomposition de $\mathfrak{a}$ en facteurs premiers sous la forme

$$\mathfrak{a} = (\prod p_j^{n_j} O_k)(\prod q_\ell^{n_\ell} O_k)(\prod \mathfrak{q}_\ell^{m_\ell})(\prod r_m^{n_m} O_k) \prod \mathfrak{r}_m^{\epsilon_m}$$

où les p_j sont des nombres premiers inertes, les q_ℓ des nombres premiers décomposés, les r_m des nombres premiers ramifiés, les $\mathfrak{q}_\ell$ des idéaux premiers décomposés non conjugués deux à deux, les $\mathfrak{r}_m$ des idéaux ramifiés avec $\epsilon_m \in \{0,1\}$. Dans ces conditions on a :

$$\mathfrak{a} \cap \mathbb{Z} = (\prod p_j^{n_j} \prod q_\ell^{n_\ell+m_\ell} \prod r_m^{n_m+\epsilon_m})\mathbb{Z}$$

$$(N\mathfrak{a})\mathbb{Z} = \prod p_j^{2n_j} \prod q_\ell^{2n_\ell+m_\ell} \prod r_m^{2n_m+\epsilon_m}\,\mathbb{Z} .$$

On en conclut que $\mathfrak{a} \cap \mathbb{Z} = N(\mathfrak{a})\mathbb{Z}$ si et seulement si les exposants des idéaux premiers figurant dans la décomposition de $\mathfrak{a}$ satisfont aux conditions B de la proposition 2.3. La proposition est donc démontrée.

Corollaire 3.2.

Soit $\mathfrak{a}$ un idéal entier de k. Les deux assertions suivantes sont équivalentes :

1) L'idéal $\mathfrak{a}$ est sans facteur rationnel.

2) Il existe $c \in \mathbb{Z}$ tel que $\theta - c \in \mathfrak{a}$.

Il est évident que 2) implique 1). Réciproquement si $\mathfrak{a}$ est sans facteur rationnel, l'homomorphisme canonique $\mathbb{Z} \to O_k/\mathfrak{a}$ est surjectif et on conclut qu'il existe $c \in \mathbb{Z}$ tel que θ soit congru à c modulo $\mathfrak{a}$.

Définition 3.3.

L'ensemble $\{c \mid \theta - c \in \mathfrak{a}\}$ est appelé ensemble des racines de $\mathfrak{a}$.

Remarques 3.4 : 1) L'ensemble des racines de $\mathfrak{a}$ forme une progression arithmétique de raison $N\mathfrak{a}$.

2) Si c est une racine de $\mathfrak{a}$ et si $\bar{\mathfrak{a}}$ est l'idéal conjugué de $\mathfrak{a}$, alors S-c est une racine de $\bar{\mathfrak{a}}$. En effet, on a $\theta - c \in \mathfrak{a}$, donc $\bar{\theta} - c = S - c + \theta \in \bar{\mathfrak{a}}$ et $\theta - (S-c) \in \bar{\mathfrak{a}}$.

3) Dans l'intervalle $[\frac{S}{2} - \frac{1}{2}N(\mathfrak{a}), \frac{S}{2} + \frac{1}{2}N\mathfrak{a}]$, il existe au moins une et au plus 2 racines de $\mathfrak{a}$. S'il en existe une seule, on l'appelle la racine minimum et on la note $c_{\mathfrak{a}}$. S'il en existe deux on note $c_{\mathfrak{a}}$ celle des deux qui est positive.

Théorème 3.5.

Soit $\mathfrak{a}$ un idéal entier sans facteur rationnel de k . Si c est une racine de $\mathfrak{a}$, la famille $\{N(\mathfrak{a}), \theta - c\}$ est une $\mathbb{Z}$-base de $\mathfrak{a}$.

Démonstration : D'une part, le discriminant de $\mathfrak{a}$ est

$$\Delta(\mathfrak{a}) = (N(\mathfrak{a}))^2 \Delta_{k/\mathbb{Q}} \ ;$$

d'autre part, le discriminant du sous Z-module de $\mathfrak{a}$ engendré par $N(\mathfrak{a})$ et $\theta - c$ est :

$$\Delta\{N(\mathfrak{a}), \theta - c\} = \begin{vmatrix} N(\mathfrak{a}) & \theta - c \\ N(\mathfrak{a}) & \bar{\theta} - c \end{vmatrix}^2 = (N(\mathfrak{a}))^2 \begin{vmatrix} 1 & \theta \\ 1 & \bar{\theta} \end{vmatrix} = \Delta(\mathfrak{a}) \ .$$

En vertu des derniers rappels du §1, $\mathfrak{a}$ est engendré par $N(\mathfrak{a})$ et $\theta - c$.

Proposition 3.6.

Soit $\mathfrak{a}$ un idéal entier sans facteur rationnel et soit F(X) le polynôme fondamental de k . Si c est une racine de $\mathfrak{a}$, alors $N\mathfrak{a}$ divise F(c) .

Démonstration : On a $F(c) = (\theta-c)(\bar{\theta}-c) \in \mathfrak{a} \cap \mathbb{Z} = (N\mathfrak{a}).\mathbb{Z}$.

Proposition 3.7.

Soit a un entier naturel non nul. S'il existe $c \in \mathbb{Z}$ tel que a divise $F(c)$, alors le sous Z-module de O_k engendré par a et par $\theta-c$ est un idéal entier sans facteur rationnel de k .

Démonstration : Il suffit de montrer que $a\mathbb{Z} + (\theta-c)\mathbb{Z}$ est un idéal de O_k . Il est clair que $\{1, \bar{\theta}-c\}$ est une $\mathbb{Z}$-base de O_k . Tout $b \in O_k$ peut donc s'écrire $b = u + v(\bar{\theta}-c)$ avec $u,v \in \mathbb{Z}$ et pour tout $m,n \in \mathbb{Z}$ on a $(am+(\theta-c)n)b = aum + vnF(c) + amv(S-2c) + (\theta-c)(nu-amv)$. Il en résulte que $(am+(\theta-c)n)b \in a\mathbb{Z} + (\theta-c)\mathbb{Z}$.

Exemple : Soit $k = \mathbb{Q}(\sqrt{-3})$ et soit $c = +14$. On a $F(X) = X^2-X+1$ et $F(c) = 3.61$. Les idéaux suivants de O_k sont sans facteur rationnel : $\mathfrak{a}_1 = (3.61, \theta-14)$; $\mathfrak{a}_2 = (3, \theta-14)$; $\mathfrak{a}_3 = (61, \theta-14)$; $\mathfrak{a}_4 = (1, \theta-14) = O_k$.

4. NOTIONS SUR LES IDEAUX REDUITS.

Dans ce paragraphe, on se propose de caractériser une nouvelle famille d'idéaux de k qui permettra de déterminer les classes d'idéaux de k . Pour cela on a besoin d'une norme sur $\mathbb{R}^2$.

4.1. Définition d'une norme sur $\mathbb{R}^2$.

Puisque l'extension $k/\mathbb{Q}$ est de degré 2 , on sait qu'il existe un plongement canonique de k dans $\mathbb{R}^2$. Si k est un corps réel, le plongement canonique est $\alpha \to (\alpha, \bar{\alpha})$. Si le corps k est imaginaire, le plongement canonique est $\alpha \to (\text{Re } \alpha , \text{Im } \alpha)$. La norme $\varphi : \mathbb{R}^2 \to \mathbb{R}^+$ que l'on choisit est alors la norme du maximum si k est réel et la norme euclidienne sinon. Ainsi on aura $\varphi(\alpha) = \text{Max}\{|\alpha|, |\bar{\alpha}|\}$ si k est réel et $\varphi(\alpha) = \|\alpha\|$ si k est imaginaire. Remarquons au passage que k est dense dans $\mathbb{R}^2$ pour la métrique définie par cette norme.

Si Γ est un réseau de $\mathbb{R}^2$, par exemple un idéal fractionnaire de k, soit $\Gamma^* = \Gamma \setminus \{0\}$. Alors $\varphi|_{\Gamma^*}$ admet un minimum car Γ est un sous-groupe discret de $\mathbb{R}^2$.

Définition 4.2.

Soit $\mathfrak{a}$ un idéal entier de k. Cet idéal est dit réduit si le minimum de $\varphi|_{\mathfrak{a}^*}$ est atteint en un point $\alpha \in \mathfrak{a} \cap \mathbb{Z}$.

Remarques 4.3 : 1) Si $\mathfrak{a}$ est un idéal réduit, il en est de même de son conjugué $\bar{\mathfrak{a}}$ car l'application φ est invariante par conjugaison.

2) Soit $r \in \mathbb{Q}^*$ et soit $\mathfrak{a}$ un idéal de k. Si $\mathfrak{a}$ et $r\mathfrak{a}$ sont entiers, ils sont simultanément réduits. En particulier, un idéal est réduit si et seulement si sa partie sans facteur rationnel est un idéal réduit.

Lemme 4.4.

Soit $\mathfrak{a}$ un idéal entier sans facteur rationnel. Cet idéal est réduit si et seulement si $\varphi(\alpha) \geq N\mathfrak{a}$ pour tout $\alpha \in \mathfrak{a}^*$.

Démonstration : Si $\mathfrak{a}$ est un idéal sans facteur rationnel on a $\mathfrak{a} \cap \mathbb{Z} = (N(\mathfrak{a}))$. Dans ces conditions, $\mathfrak{a}$ est réduit si et seulement si $\min \varphi|_{\mathfrak{a}^*} = N\mathfrak{a}$.

Théorème 4.5.

Toute classe d'idéaux de k contient un idéal réduit sans facteur rationnel.

Démonstration : Soit $\mathfrak{a}$ un idéal entier de k. Soit $\alpha_o \in \mathfrak{a}^*$ un point réalisant le minimum de $\varphi|_{\mathfrak{a}^*}$. Si l'idéal $\bar{\alpha}_o \cdot \mathfrak{a}$ est réduit, la partie sans facteur rationnel de cet idéal est un idéal réduit, sans facteur rationnel et équivalent à l'idéal $\mathfrak{a}$. On montrera donc que $\bar{\alpha}_o \mathfrak{a}$ est réduit. Pour tout $\alpha \in \mathfrak{a}^*$ on a $\varphi(\bar{\alpha}_o \alpha_o \frac{1}{\bar{\alpha}_o}) \leq \varphi(\bar{\alpha}_o \alpha \frac{1}{\bar{\alpha}_o})$. Distinguons alors le cas réel et le cas imaginaire :

1) Si k est réel, la relation ci-dessus s'écrit comme suit :

$$\mathrm{Max}\{N(\alpha_o)\,|\frac{1}{\bar{\alpha}_o}|, N(\alpha_o)\,|\frac{1}{\alpha_o}|\} \leq \mathrm{Max}\{|\frac{1}{\bar{\alpha}_o}|\,|\alpha\bar{\alpha}_o|\ ,\ |\frac{1}{\alpha_o}|\,|\bar{\alpha}\alpha_o|\}\ .$$

Le premier membre de cette inégalité est égal à $N(\alpha_o)\ \mathrm{Max}\{|\frac{1}{\alpha_o}|, |\frac{1}{\bar{\alpha}_o}|\}$.

Si on pose $c = \mathrm{Max}\{|\frac{1}{\alpha_o}|, |\frac{1}{\bar{\alpha}_o}|\}$ on obtient

$$N(\alpha_o) \leq \mathrm{Max}\{\frac{1}{|\bar{\alpha}_o|c}\,|\alpha\bar{\alpha}_o|\ ,\ \frac{1}{|\alpha_o|c}\,|\bar{\alpha}\alpha_o|\} \leq \mathrm{Max}\{|\alpha\bar{\alpha}_o|, |\bar{\alpha}\alpha_o|\}$$

c'est-à-dire

$$N(\alpha_o) = \varphi(\alpha_o\bar{\alpha}_o) \leq \varphi(\alpha\bar{\alpha}_o)\ .$$

Il est clair alors que $\bar{\alpha}_o\mathfrak{a}$ est un idéal réduit car $\alpha_o\bar{\alpha}_o$ appartient à $\bar{\alpha}_o\mathfrak{a} \cap \mathbb{Z}$.

2) Si k est imaginaire, l'application $\varphi : k \to \mathbb{R}^+$ est multiplicative ; on a donc pour tout $\alpha \in \mathfrak{a}^*$

$$\varphi(\bar{\alpha}_o\alpha) = \varphi(\bar{\alpha}_o)\ \varphi(\alpha) \geq \varphi(\bar{\alpha}_o)\ \varphi(\alpha_o) = \varphi(\alpha_o\bar{\alpha}_o) = N(\alpha_o)\ .$$

L'idéal $\bar{\alpha}_o\mathfrak{a}$ est donc réduit.

5. GROUPE DES CLASSES D'UN CORPS QUADRATIQUE IMAGINAIRE.

Lemme 5.1.

Soit k un corps quadratique imaginaire. Soit $F(X)$ son polynôme fondamental et soit $\mathfrak{a}$ un idéal entier sans facteur rationnel de k . Les deux assertions suivantes sont équivalentes :

1) L'idéal $\mathfrak{a}$ est réduit.

2) Si $c_{\mathfrak{a}}$ est la racine minimum de $\mathfrak{a}$ on a : $(N(\mathfrak{a}))^2 \leq F(c_{\mathfrak{a}})$.

Démonstration : 1) implique 2) : une $\mathbb{Z}$-base de $\mathfrak{a}$ est $\{N\mathfrak{a}, \theta - c_{\mathfrak{a}}\}$. On a donc $N\mathfrak{a} \leq \varphi(\theta - c)$ et par suite puisque φ est multiplicative et invariante par conjugaison :

$$(N\mathfrak{a})^2 \leq \varphi(\theta - c_{\mathfrak{a}})\,\varphi(\bar{\theta} - c_{\mathfrak{a}}) = \varphi(F(c_{\mathfrak{a}})) = F(c_{\mathfrak{a}}) .$$

2) implique 1) : supposons donc $(N\mathfrak{a})^2 \leq F(c_{\mathfrak{a}})$ et soit $\alpha = uN\mathfrak{a} + v(\theta - c_{\mathfrak{a}}) \in \mathfrak{a}^*$ ($u \in \mathbb{Z}$, $v \in \mathbb{Z}$, u et v non tous deux nuls). On a $(\varphi(\alpha))^2 = \varphi(\alpha).\varphi(\bar{\alpha}) = N\alpha = (uN\mathfrak{a} - vc_{\mathfrak{a}} + v\theta)(uN\mathfrak{a} - vc_{\mathfrak{a}} + v\bar{\theta})$.

Si $v = 0$ on a $\varphi(\alpha)^2 = u^2(N\mathfrak{a})^2$

Si $v \neq 0$ on a $(\varphi(\alpha))^2 = v^2 F\{c_{\mathfrak{a}} - \frac{u}{v} N(\mathfrak{a})\}$.

D'après la formule de Taylor on obtient

$$(\varphi(\alpha))^2 = v^2 F(c_{\mathfrak{a}}) + uvN\mathfrak{a}(2c_{\mathfrak{a}} - S) + u^2(N\mathfrak{a})^2 .$$

Or $|2c_{\mathfrak{a}} - S| \leq N\mathfrak{a}$, d'après la remarque 3.4.3). On a donc

$$(\varphi(\alpha))^2 \geq v^2 F(c_{\mathfrak{a}}) + u^2(N\mathfrak{a})^2 - uv(N\mathfrak{a})^2 \geq (u^2 + v^2 - uv)(N\mathfrak{a})^2 \geq (N\mathfrak{a})^2 .$$

Dans ces conditions, on conclut que $\varphi(\alpha) \geq N\mathfrak{a}$ et que l'idéal $\mathfrak{a}$ est réduit.

Lemme 5.2.

Soit $\mathfrak{a} = (N\mathfrak{a}, \theta - c_{\mathfrak{a}})$ un idéal réduit sans facteur rationnel de k . On a l'inégalité

$$3(N\mathfrak{a})^2 \leq 4P - S^2 .$$

Démonstration : Par définition de la racine minimum de $\mathfrak{a}$ on a

$$|2c_{\mathfrak{a}} - S| \leq N\mathfrak{a} .$$

D'après le lemme 5.1 on a $F(c_{\mathfrak{a}}) \geq (N\mathfrak{a})^2$. On peut donc écrire

$$F(c_{\mathfrak{a}}) = \frac{1}{4}[(2c_{\mathfrak{a}} - S)^2 + 4P - S^2] \geq (N\mathfrak{a})^2 ;$$

et subséquemment :

$$3(N\mathfrak{a})^2 \leq 4P - S^2 .$$

Corollaire 5.3.

L'ensemble des idéaux réduits sans facteur rationnels d'un corps quadratique imaginaire est fini.

Théorème 5.4.

Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux entiers réduits, sans facteur rationnel et distincts d'un corps quadratique imaginaire k. Les deux assertions suivantes sont équivalentes :

1) Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont équivalents.
2) Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont conjugués et $\mathfrak{a}^2 = (\theta - c_{\mathfrak{a}})$.

Démonstration : 1) implique 2) : si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux équivalents il existe trois entiers rationnels premiers entre eux dans leur ensemble u , v , n , tels que :

$$\mathfrak{a} = \left(\frac{u+v\theta}{n}\right).\mathfrak{b} \quad . \tag{1}$$

Puisque l'idéal $\mathfrak{a}$ est sans facteur rationnel, les entiers u et v sont premiers entre eux. En particulier v n'est pas nul. De l'égalité (1) on déduit

$$n\mathfrak{a}\bar{\mathfrak{b}} = ((u+v\theta)N\mathfrak{b}) \quad . \tag{2}$$

Pour simplifier l'écriture, posons $N\mathfrak{a} = a$ et $N\mathfrak{b} = b$. Puisque $u+v\theta$ est sans facteur rationnel, n divise b et on a :

$$ab = N(u+v\theta)\left(\frac{b}{n}\right)^2 \tag{3}$$

ou encore

$$4ab = \left(\frac{b}{n}\right)^2[(2u+Sv)^2 + v^2(4P-S^2)] \geq \left(\frac{b}{n}\right)^2 v^2(4P-S^2) \quad .$$

Or il résulte du lemme 5.2 que $3a^2 \leq 4P-S^2$. Par conséquent, on a

$$4(4P-S^2) \geq 12ab \geq 3\left(\frac{b}{n}\right)^2 v^2(4P-S^2) \quad .$$

On en conclut puisque v n'est pas nul que $v^2 = 1$ et $n = b$. Quitte à changer le signe de u on peut supposer que v est égal à -1 et on déduit de l'égalité (2) que $\mathfrak{a} = (u-\theta)\bar{\mathfrak{b}}$. Ce dernier résultat indique que l'idéal $\mathfrak{a}\bar{\mathfrak{b}}$ est sans facteur rationnel. De plus les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont réduits. On a donc d'après (2) :

$$\text{Min } \varphi|(\mathfrak{a}\bar{\mathfrak{b}})^* = N\mathfrak{a}.N\mathfrak{b} = N\mathfrak{b}.\sqrt{N(\theta-u)} \quad .$$

On en conclut que $(N\mathfrak{a})^2 = F(u)$, c'est-à-dire que u est une racine de

l'idéal $\mathfrak{a}$. L'idéal engendré par $(N\mathfrak{a})^2$ et par $\theta-u$ est égal à l'idéal principal $(\theta-u)$, donc à l'idéal $\mathfrak{a}\bar{\mathfrak{b}}$, ce qui montre que $N\mathfrak{a} = N\mathfrak{b}$.

Enfin, puisque les idéaux $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}\bar{\mathfrak{b}}$ sont sans facteur rationnel les seuls idéaux qui interviennent dans la décomposition de $\mathfrak{a}\bar{\mathfrak{b}}$ en facteurs premiers sont des idéaux premiers décomposés non conjugués deux à deux. De plus, si $\mathfrak{a}$ et $\mathfrak{b}$ ont même norme, les décompositions de $\mathfrak{a}$ et de $\bar{\mathfrak{b}}$ sont les mêmes, c'est-à-dire que $\mathfrak{a} = \bar{\mathfrak{b}}$. En particulier, on a $\mathfrak{a}^2 = (\theta-u)$ et l'égalité $|\theta-u| = N\mathfrak{a}$ montre que u est la racine minimum de l'idéal $\mathfrak{a}$.

2) implique 1) : remarquons que $\mathfrak{a}$ est nécessairement distinct de son conjugué $\bar{\mathfrak{a}}$ car les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont différents. Ceci posé, si $\mathfrak{a}^2 = (\theta-c_{\mathfrak{a}})$ on a l'égalité :

$$\mathfrak{a}.N\mathfrak{a} = (\theta-c_{\mathfrak{a}})\bar{\mathfrak{a}} \quad .$$

Par conséquent, $\mathfrak{a}$ et $\bar{\mathfrak{a}}$ sont équivalents ; les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont équivalents. Le théorème est démontré.

Remarque : Il se peut qu'un idéal $\mathfrak{a}$ soit entier, réduit, sans facteur rationnel, égal à son conjugué et tel que $\mathfrak{a}^2 = (\theta-c_{\mathfrak{a}})$. Mais dans ce cas, on a $(N\mathfrak{a}) = \mathfrak{a}^2 = (\theta-c_{\mathfrak{a}})$. Puisque $(\theta-c_{\mathfrak{a}})$ est sans facteur rationnel, on a nécessairement $N\mathfrak{a} = 1$. Alors l'idéal $\mathfrak{a}$ est O_k tout entier, et $\theta-c_{\mathfrak{a}}$ est une unité de O_k qui n'est pas rationnelle. Cela implique $k = \mathbb{Q}(i)$ ou $k = \mathbb{Q}(j)$! .

Exemple : Considérons le corps $k = \mathbb{Q}(\sqrt{-21})$ et l'idéal entier $\mathfrak{a} = (5, \theta-2)$; il est clair que $\mathfrak{a}$ est réduit, sans facteur rationnel. On vérifie facilement que $\mathfrak{a}$ n'est pas principal et que $\mathfrak{a}^2 = (\theta-2)$. On peut conclure de cette propriété que le nombre de classes de $\mathbb{Q}(\sqrt{-21})$ est divisible par 2 .

Pour terminer ce paragraphe, nous donnerons quelques exemples de recherche du groupe des classes d'un corps quadratique et nous indiquerons sommairement la méthode générale.

Proposition 5.5.

Les corps quadratiques $\mathbb{Q}(\sqrt{-m})$ avec

$$m \in \{1,2,3,7,11,19,43,67,163\}$$

sont principaux.

Démonstration : Pour $m \leq 3$, il suffit d'utiliser l'inégalité de Minkowski.

Pour les autres valeurs de m , on utilise le théorème 5.4 et les résultats qui le précèdent, à savoir que si $\mathfrak{a}$ est un idéal réduit sans facteur rationnel on a

1) $N\mathfrak{a} \leq \sqrt{\frac{1}{3}(4P-S^2)} = \sqrt{\frac{m}{3}}$ si $m \equiv 3 \pmod 4$

2) $|2c_{\mathfrak{a}}-1| \leq N\mathfrak{a}$

3) $F_{-m}(c_{\mathfrak{a}}) \equiv 0 \pmod{N(\mathfrak{a})}$.

Ceci étant, le tableau suivant montre que les corps considérés sont principaux.

m	$N(\mathfrak{a})$	$c_{\mathfrak{a}}$	$F_{-m}(c_{\mathfrak{a}})$	Id. réduit ss. fact. rat.
7	1	1	2	O_k
11	1	1	3	O_k
19	1	1	5	O_k
	2	1	7	—
43	1	1	11	O_k
	2	1	11	—
	3	1;2	11;13	—
67	1	1	17	O_k
	2	1	17	—
	3	1;2	17;19	—
	4	1;2	17;19	O_k
163	1	1	41	O_k
	2	1	41	—
	3	1;2	41;43	—
	4	1;2	41;43	—
	5	1;2;3	41;43;47	—
	6	1;2;3	41;43;47	—
	7	1;2;3;4	41;43;47;53	—

Remarque : Stark a montré en 1966 qu'il n'y a pas d'autre corps imaginaire principal.

Exemple 5.6 : Groupe des classes du corps quadratique $\mathbb{Q}(\sqrt{-199})$.

Le polynôme fondamental de ce corps est $F(X) = X^2-X+50$. Les entiers susceptibles d'être la norme d'un idéal réduit sans facteur rationnel sont donc : 1,2,3,4,5,6,7,8 . On construit donc le tableau suivant :

$a = N_\alpha$	c_α	$F(c_\alpha)$	Idéaux réduits sans facteur rationnel	Motif de l'exclusion de l'idéal $(a, \theta-c_\alpha)$
1	1	50	O_k	
2	1	50	$(2,\theta-1),(2,\bar{\theta}-1)=(2,\theta-2)$	
3	1	50	Néant	$F(c_\alpha) \not\equiv 0 \pmod 3$
	2	52	Néant	$F(c_\alpha) \not\equiv 0 \pmod 3$
4	1	50	Néant	$F(c_\alpha) \not\equiv 0 \pmod 4$
	2	52	$(4,\theta-2),(4,\theta-3)=(4,\bar{\theta}-2)$	
5	1	50	$(5,\theta-1),(5,\theta-2)$	
	2	52	Néant	$F(c_\alpha) \not\equiv 0 \pmod 5$
	3	56	Néant	$F(c_\alpha) \not\equiv 0 \pmod 5$
6	1	50	Néant	$F(c_\alpha) \not\equiv 0 \pmod 6$
	2	52	Néant	
	3	56	Néant	
7	1	50	Néant	$F(c_\alpha) \not\equiv 0 \pmod 7$
	2	52	Néant	Idem
	3	56	$(7,\theta-3),(7,\bar{\theta}-3)$	
	4	62	Néant	Idem
8	1	50	Néant	$(N_\alpha)^2 > F(c_\alpha)$
	2	52	Néant	
	3	56	Néant	
	4	62	Néant	

Une fois ce tableau dressé, on vérifie qu'aucun des idéaux réduits trouvés n'est équivalent à son conjugué (sauf O_k, évidemment). On en déduit que $h_k = 9$. Le groupe des classes de $\mathbb{Q}(\sqrt{-199})$ est soit cyclique d'ordre 9 soit isomorphe à $(\mathbb{Z}/(3)) \times (\mathbb{Z}/(3))$. On vérifie alors sans peine que $(2,\theta-1)^3 = (8,\theta-3)$, lequel est équivalent à $(7,\bar{\theta}-3)$ qui n'est pas principal. On en conclut que le groupe des classes de $\mathbb{Q}(\sqrt{-199})$ est cyclique d'ordre 9 et engendré par $Cl(2,\theta-1)$.

5.7. Aperçu sur la méthode générale.

1) Etant donné k, on commence par dresser le tableau des idéaux entiers réduits sans facteur rationnel de k.

2) On recherche parmi ces idéaux ceux qui sont équivalents à leur conjugué, c'est-à-dire tels que $\mathfrak{a}^2 = (\theta-c_{\mathfrak{a}})$. Ceci fait, après avoir éliminé les conjugués en question, on obtient le nombre de classes par application du théorème 5.4.

3) On construit la table du groupe. Dans ce but, si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux réduits sans facteur rationnel, ou bien $\mathfrak{a}.\mathfrak{b}$ est réduit sans facteur rationnel, ou bien il ne l'est pas. S'il l'est, $Cl(\mathfrak{a}\mathfrak{b})$ est déterminée. Sinon on peut écrire $\mathfrak{a}.\mathfrak{b} = (q_o)\mathfrak{a}_o$ avec $\mathfrak{a}_o$ sans facteur rationnel. Soit c_o la racine minimum de $\mathfrak{a}_o$ et a_o la norme de $\mathfrak{a}_o$. On a alors $F(c_o) = a_o a_1$.

. Si $a_1 \geq a_o$, l'idéal $\mathfrak{a}_o$ est réduit sans facteur rationnel et $Cl(\mathfrak{a}\mathfrak{b})=Cl(\mathfrak{a}_o)$.

. Si $a_1 < a_o$, on peut écrire

$$(\theta-c_o) = \mathfrak{a}_o\mathfrak{a}_1$$

où $\mathfrak{a}_1$ est sans facteur rationnel et de norme a_1. Les idéaux $\mathfrak{a}_o$ et $\bar{\mathfrak{a}}_1$ sont équivalents car $\mathfrak{a}_o\mathfrak{a}_1\bar{\mathfrak{a}}_1 = \mathfrak{a}_o(a_1) = (\theta-c_o)\bar{\mathfrak{a}}_1$. Si $\bar{\mathfrak{a}}_1$ est réduit $cl(\mathfrak{a}\mathfrak{b}) = Cl(\bar{\mathfrak{a}}_1)$. Sinon on recommence l'opération qu'on vient d'effectuer avec $\mathfrak{a}_o$. On obtient une suite strictement décroissante de normes d'idéaux sans facteur rationnel : $a_o,\ldots,a_n$. Au bout d'un nombre fini d'opérations on obtient un idéal $\mathfrak{a}_n$ entier, réduit, sans facteur rationnel et équivalent à l'idéal $\mathfrak{a}.\mathfrak{b}$.

6. GROUPE DES CLASSES D'UN CORPS QUADRATIQUE REEL.

L'étude du cas des corps quadratiques réels est plus délicate que celle du cas imaginaire. Quelques remarques préliminaires permettront de simplifier cette étude :

Remarques 6.1.A. Soit $\mathfrak{a}$ un idéal entier réduit d'un corps quadratique réel k. Cet idéal possède une racine dans l'intervalle $]\bar{\theta}, \theta[$. En effet, si c est la plus grande racine de $\mathfrak{a}$ qui soit inférieure à $\bar{\theta}$, on a : $\varphi(\theta-c) = \max\{|\theta-c|, |\bar{\theta}-c|\} = \theta-c \geq N\mathfrak{a}$. Dans ces conditions, on a $\bar{\theta} < c+N\mathfrak{a} \leq \theta$. Puisque θ n'est pas rationnel, on a bien $\bar{\theta} < c+N\mathfrak{a} < \theta$.

6.1.B. Soit $\mathfrak{a}$ un idéal entier sans facteur rationnel et soit $c_{\mathfrak{a}}$ la racine minimum de $\mathfrak{a}$. Si $|F(c_{\mathfrak{a}})| \geq (N\mathfrak{a})^2$ l'idéal $\mathfrak{a}$ est réduit. En effet, il est clair d'après 6.1.A que $F(c_{\mathfrak{a}})$ est négatif. De plus, on a :

$$(N\mathfrak{a})^2 \leq \frac{1}{4}(S^2-4P) - (c_{\mathfrak{a}}-\frac{S}{2})^2 \leq \frac{S^2-4P}{4} = (\frac{\theta-\bar{\theta}}{2})^2 .$$

Soit maintenant $\alpha \in \mathfrak{a}$ tel que $\varphi(\alpha) < N\mathfrak{a}$. Si $\alpha = (N\mathfrak{a})u + v(\theta-c_{\mathfrak{a}})$ on a :

$$N\mathfrak{a} > \max\{|\alpha|, |\bar{\alpha}|\} \quad \text{et} \quad v = \frac{\alpha-\bar{\alpha}}{\theta-\bar{\theta}} \quad \text{avec} \quad |v| < \frac{2N\mathfrak{a}}{\theta-\bar{\theta}} \leq 1 .$$

Par suite, $v = 0$ et $u = 0$. Le minimum de $\varphi|_{\mathfrak{a}^*}$ est donc atteint au point $N\mathfrak{a}$, c'est-à-dire que l'idéal $\mathfrak{a}$ est réduit.

La réciproque de cette propriété est fausse, comme le montre l'exemple suivant :

Soit $k = \mathbb{Q}(\sqrt{7})$ le corps dont le polynôme fondamental est X^2-7 et soit $\mathfrak{a}$ l'idéal $(3, \sqrt{7}-1)$. Puisque $|F(1)| = 6$ l'idéal $\mathfrak{a}$ est sans facteur rationnel et satisfait à $F(1) < (N\mathfrak{a})^2$. Soit $\alpha \in \mathfrak{a}$ tel que $\varphi(\alpha) < N\mathfrak{a}$. Si $\alpha = 3u + v(\sqrt{7}-1)$, $(u,v \in \mathbb{Z})$ on a nécessairement $v = u = 0$, c'est-à-dire que l'idéal $\mathfrak{a}$ est réduit.

Cet exemple montre qu'il faut trouver une nouvelle caractérisation des idéaux réduits d'un corps quadratique réel.

Proposition 6.2.

Soit $\mathfrak{a}$ un idéal entier et sans facteur rationnel d'un corps quadratique réel k . Les deux assertions suivantes sont équivalentes :

1) L'idéal $\mathfrak{a}$ est réduit ;

2) L'idéal $\mathfrak{a}$ possède deux racines dans l'intervalle $]\bar{\theta},\theta[$;

Démonstration : 1) implique 2) . On sait d'après la remarque 6.1.A que $\mathfrak{a}$ possède une racine dans l'intervalle $]\bar{\theta},\theta[$. Si c est la plus grande racine de $\mathfrak{a}$ inférieure à $\bar{\theta}$, il résulte de 6.1.B que $c+N\mathfrak{a}$ et $c+2N\mathfrak{a}$ appartiennent à $]\bar{\theta},\theta[$.

2) implique 1) . Si $\mathfrak{a}$ possède deux racines dans l'intervalle $]\bar{\theta},\theta[$, soit c la plus grande des racines de $\mathfrak{a}$ appartenant à $]\bar{\theta},\theta[$. On a alors les inégalités : $0 < \theta-c < N\mathfrak{a}$ et $-N\mathfrak{a} > \bar{\theta}-c$. Soit alors $\alpha = uN\mathfrak{a} + v(\theta-c) \in \mathfrak{a}$ tel que $\varphi(\alpha) < N\mathfrak{a}$. Dans ces conditions, on a $|uN\mathfrak{a} + v(\theta-c)| < N\mathfrak{a}$ et $|uN\mathfrak{a} + v(\bar{\theta}-c)| < N\mathfrak{a}$. On en déduit $|v|(\theta-\bar{\theta}) < 2N\mathfrak{a}$. Si $\theta-\bar{\theta} > 2N\mathfrak{a}$ on a $v = u = 0$ et l'idéal $\mathfrak{a}$ est réduit. Si $\theta-\bar{\theta} \in]N\mathfrak{a},2N\mathfrak{a}[$, on peut supposer en changeant le signe de α que $v \in \{0,1\}$. L'hypothèse $v = 1$ conduit aux inégalités :

$$0 < -1 - \frac{\bar{\theta}-c}{N\mathfrak{a}} < u < 1 - \frac{\theta-c}{N\mathfrak{a}} < 1 .$$

Par conséquent, $v = u = 0$ et on conclut que l'idéal $\mathfrak{a}$ est réduit.

Définition 6.3.

Soit $\mathfrak{a}$ un idéal entier réduit et sans facteur rationnel d'un corps quadratique réel k . On appelle racine finale de $\mathfrak{a}$ la plus grande racine c de $\mathfrak{a}$ inférieure à θ . (On a alors $c \in]\frac{S}{2},\theta[$) .

Proposition 6.4.

Soit c un entier naturel appartenant à $]\frac{S}{2},\theta[$ et soit $F(c) = -ab$. Les deux assertions suivantes sont équivalentes :

1) L'idéal $\mathfrak{a} = (a,\theta-c)$ est réduit sans facteur rationnel et admet c comme racine finale ;

2) On a l'inégalité $(a+b)^2 < S^2-4P$.

Démonstration : Il est évident que $\mathfrak{a}$ est sans facteur rationnel. L'assertion 1) équivaut à la propriété $(F(c+a) > 0$ et $F(c-a) < 0)$: la formule de Taylor donne alors

$$F(c+a) = F(c) + aF'(c) + a^2 = -ab + a^2 + a(2c-S)$$
$$F(c-a) = F(c) - aF'(c) + a^2 = -ab + a^2 - a(2c-S) .$$

L'assertion 1) est donc équivalente à la propriété $2c-S > |a-b|$. Puisque $2c-S > 0$ par hypothèse, cette dernière inégalité équivaut à

$$S^2 - 4P = 4c^2 - 4Sc + S^2 + 4ab > (a+b)^2 .$$

Nota : Dorénavant, on dira qu'un idéal entier $\mathfrak{a}$ est réduit s'il est réduit sans facteur rationnel.

Définition 6.5.

Soit $\mathfrak{a}_o$ un idéal réduit de k . On pose $a = N\mathfrak{a}_o$. Soit $c_{\mathfrak{a}_o}$ (resp. $c_{\bar{\mathfrak{a}}_o}$) la racine finale de $\mathfrak{a}_o$ (resp. $\bar{\mathfrak{a}}_o$) . Si $F(c_{\mathfrak{a}_o}) = -ab$ et $F(c_{\bar{\mathfrak{a}}_o}) = -ab'$ on appelle respectivement :

- successeur de $\mathfrak{a}_o$ l'idéal $\mathfrak{a}_1 = (b, \theta-(S-c_{\mathfrak{a}_o}))$
- prédécesseur de $\mathfrak{a}_o$ l'idéal $\mathfrak{a}_{-1} = (b', \theta-c_{\bar{\mathfrak{a}}_o})$.

Exercices : A - Déduire de la proposition 6.4 que l'ensemble des idéaux réduits d'un corps quadratique réel est fini.

B - Montrer que si $\mathfrak{a}_o$ est réduit, alors $\mathfrak{a}_1$ et $\mathfrak{a}_{-1}$ sont réduits et que le successeur du prédécesseur de $\mathfrak{a}_o$ est $\mathfrak{a}_o$, de même que le prédécesseur du successeur de $\mathfrak{a}_o$.

Lemme 6.6.

Dans l'ensemble fini des idéaux réduits d'un corps quadratique réel k , la relation "il existe une chaîne de $\mathfrak{a}$ vers $\mathfrak{b}$, $\mathfrak{a} = \mathfrak{a}_o, \mathfrak{a}_1, \cdots \mathfrak{a}_n = \mathfrak{b}$ ou une chaîne $\mathfrak{b} = \mathfrak{b}_o, \ldots, \mathfrak{b}_n = \mathfrak{a}$ de $\mathfrak{b}$ vers $\mathfrak{a}$ telle que pour tout $i \leq n-1$, $\mathfrak{a}_{i+1}$ soit le successeur de $\mathfrak{a}_i$ (resp. telle que $\mathfrak{b}_{i+1}$ soit le successeur de $\mathfrak{b}_i$) " est une relation d'équivalence que l'on note $\mathfrak{a} \sim \mathfrak{b}$.

Définition 6.7.

On appelle cycle d'idéaux réduits de k toute classe d'équivalence pour la relation "$\mathfrak{a} \sim \mathfrak{b}$" .

Théorème 6.8.

Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux réduits d'un corps quadratique réel k . Les deux assertions suivantes sont équivalentes :

1) Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ appartiennent à un même cycle.

2) Les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont équivalents.

Ce théorème fondamental va permettre, grâce à la proposition 6.4 de déterminer l'ensemble des classes d'idéaux de k .

Démonstration du théorème 6.8 : Tout d'abord, il est clair que 1) implique 2) . Démontrons la réciproque.

Soit $\mathfrak{a}_o$ un idéal réduit et soit $\{\mathfrak{a}_n\}_{n\geq 0}$ la suite des successeurs itérés de $\mathfrak{a}_o$. Pour tout $n \geq 1$, on pose $a_n = N\mathfrak{a}_n$ et on définit $\rho_{n+1} \in k$ par la relation de récurrence $[\rho_o = 1 \ , \ a_{n+1}\rho_{n+1} = -\rho_n.(c_{\mathfrak{a}_n} - \theta)]$. Cette définition, donne lieu aux formules suivantes valables pour tout $n \geq 1$;

$$\rho_n = \prod_{j=1}^{n} (a_j)^{-1}(\theta - c_{\mathfrak{a}_{j-1}}) \qquad (1)$$

$$\rho_n \mathfrak{a}_n = \rho_o \mathfrak{a}_o = \mathfrak{a}_o \quad . \qquad (2)$$

La première formule est une conséquence immédiate de la définition de ρ_n . Pour démontrer la seconde, remarquons que $\mathfrak{a}_{n+1}$ est le successeur de $\mathfrak{a}_n$ et qu'on a : $\mathfrak{a}_{n+1}\bar{\mathfrak{a}}_{n+1} = (a_{n+1})$. On en déduit l'égalité

$$\rho_n(\theta - c_{\mathfrak{a}_n}).\mathfrak{a}_{n+1} = \rho_n a_{n+1}\mathfrak{a}_n = \rho_{n+1}a_{n+1}\mathfrak{a}_{n+1}$$

c'est-à-dire $\rho_{n+1}\mathfrak{a}_{n+1} = \rho_n\mathfrak{a}_n = \rho_o\mathfrak{a}_o = \mathfrak{a}_o$.

Ceci dit, puisque les $\mathfrak{a}_n$ forment un cycle, si la longueur de ce cycle est ℓ on a pour tout entier $n = q\ell + r$ l'égalité

$$\rho_n = \rho_\ell^q \cdot \rho_r \quad . \qquad (3)$$

On peut également étendre la famille des $\mathfrak{a}_n$ et des ρ_n aux entiers rationnels grâce à la relation (3) . On obtient alors le lemme :

Lemme 6.8.1.

Pour tout $n \in \mathbb{Z}$, soit $\alpha_n = \rho_n a_n$; La famille $\{\alpha_n, \alpha_{n+1}\}$ est une $\mathbb{Z}$-base de $\mathfrak{a}_o$.

Démonstration : On sait que $\rho_n \mathfrak{a}_n = \mathfrak{a}_o$ et que $\{a_n, \theta - c_{\mathfrak{a}_n}\}$ est une $\mathbb{Z}$-base de $\mathfrak{a}_n$. Par conséquent, la famille $\{\rho_n a_n = \alpha_n, \rho_n(\theta - c_{\mathfrak{a}_n}) = \alpha_{n+1}\}$ est une $\mathbb{Z}$-base de $\mathfrak{a}_o$.

Remarque 6.8.2.

Pour tout $n \in \mathbb{Z}$ on a $\dfrac{\alpha_n}{\alpha_{n+1}} = \dfrac{a_n}{\theta - c_{\mathfrak{a}_n}}$; du fait que $c_{\mathfrak{a}_n}$ est la racine finale de l'idéal réduit $\mathfrak{a}_n$, on a les relations $\alpha_n > \alpha_{n+1}$ et $\overline{\dfrac{\alpha_n}{\alpha_{n+1}}} \in]-1,0[$. En particulier, puisque le rapport $\dfrac{\alpha_n}{\alpha_{n+1}}$ ne prend qu'un nombre fini de valeurs lorsque n parcourt $\mathbb{Z}$ on a : $\lim\limits_{n \to +\infty} \alpha_n = +\infty$ et $\lim\limits_{n \to +\infty} \alpha_n = 0$.

Cette remarque nous amène à énoncer le lemme :

Lemme 6.8.2.

Soit $\{\beta, \gamma\}$ une $\mathbb{Z}$-base de $\mathfrak{a}_o$ dont les éléments satisfont aux propriétés suivantes :

$$\beta > \gamma > 0 \quad \text{et} \quad -1 < \overline{\left(\frac{\beta}{\gamma}\right)} < 0 \ ;$$

il existe alors $n \in \mathbb{Z}$ tel que $\beta = \alpha_n$ et $\gamma = \alpha_{n+1}$.

Démonstration : La suite $\{\alpha_n\}_{n \in \mathbb{Z}}$ est strictement croissante de 0 à l'infini. Il existe donc $n \in \mathbb{Z}$ tel que $\alpha_n \leq \beta < \alpha_{n+1}$. Raisonnons par l'absurde et supposons que $\beta \neq \alpha_n$. On peut écrire :

$\beta = u\alpha_n + v\alpha_{n+1}$ avec $u, v \in \mathbb{Z}$ car $\{\alpha_n, \alpha_{n+1}\}$ est une base de $\mathfrak{a}_o$.

Il résulte de l'encadrement de β que $uv < 0$ et par conséquent que

$$|\bar{\beta}| = |u\bar{\alpha}_n| + |v\bar{\alpha}_{n+1}| > |\bar{\alpha}_{n+1}| ;$$

par ailleurs on a $\alpha_{n+1} = \beta x + \gamma y$ $(x,y \in \mathbb{Z})$. Si $x = 0$ on a $y = \pm 1$ car la transformation $\{\beta,\gamma\} \to \{\alpha_n,\alpha_{n+1}\}$ est unimodulaire. On en déduit $|\overline{\alpha_{n+1}}| = |\bar{\gamma}|$ et $|\bar{\beta}||\bar{\gamma}^{-1}| > 1$. Contradiction. Si $x \neq 0$, alors $xy < 0$ et $|\bar{\alpha}_{n+1}| = |\bar{\beta}x| + |\bar{\gamma}y| > |\bar{\beta}|$. Contradiction. Dans ces conditions on a nécessairement $\beta = \alpha_n$. Reste à montrer que $\gamma = \alpha_{n+1}$. Si $\alpha_{n+1} = \alpha_n{}^{x+\gamma y} = \beta x+\gamma y$ on a $y = \pm 1$, $x > 0$. Si $y = -1$ on obtient $\alpha_{n+1} = \alpha_n{}^{x-y}$ et $\bar{\alpha}_n \cdot \bar{\alpha}_{n+1} = \bar{\alpha}_n{}^{z}x - \bar{\rho}\bar{\gamma} > 0$. Contradiction. Si $y = +1$ on a $x = 0$. Le lemme est démontré.

Achevons maintenant la démonstration du théorème. Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux réduits de k qui sont équivalents modulo les idéaux principaux. Il existe $\rho \in k^*$ tel que $\mathfrak{a} = \rho\mathfrak{b}$. La famille $\{\rho N\mathfrak{b}, \rho(\theta-c_{\mathfrak{b}})\}$ est alors une $\mathbb{Z}$-base de $\mathfrak{a}$. Posons $\beta = \rho N\mathfrak{b}$ et $\gamma = \rho(\theta-c_{\mathfrak{b}})$. On obtient $\beta > \gamma > 0$ et

$$\bar{\gamma}\bar{\beta}^{-1} = (\bar{\theta}-c_{\mathfrak{b}})(N\mathfrak{b})^{-1} < -1 .$$

On applique le lemme 6.8.2 et on montre ainsi que $\mathfrak{a}$ et $\mathfrak{b}$ appartiennent au même cycle.

Nous pouvons encore, grâce à la démonstration du théorème 6.8, obtenir une unité fondamentale de k :

Théorème 6.9.

On reprend les notations de la démonstration du théorème 6.8. L'élément ρ_ℓ est une unité fondamentale de k .

Démonstration : Soit $\epsilon > 0$ une unité de k et soit $\mathfrak{a}_o$ un idéal semi-réduit. On sait que $\epsilon\mathfrak{a}_o = \mathfrak{a}_o$ et que $\{\epsilon N\mathfrak{a}_o, \epsilon(\theta-c_{\mathfrak{a}_o})\}$ est une $\mathbb{Z}$-base de $\mathfrak{a}_o$ qui satisfait aux hypothèses du lemme 6.8.3. On en conclut qu'il existe $n = q\ell$ tel que $\epsilon = \rho_n = \rho_\ell^q$.

Pour conclure cette étude, nous donnerons deux exemples de recherche

du groupe des classes d'un corps quadratique réel.

Exemple 1.

On considère $k = \mathbb{Q}(\sqrt{11317})$; le polynôme fondamental de ce corps est $F(X) = X^2 - X - 2829$. On a de plus $[\theta] = 53$ et $[(S^2-4P)^{1/2}] = 106$. Le tableau suivant donne la recherche des idéaux réduits dont la méthode est suggérée par la proposition 6.4. On a numérotée les idéaux réduits dans l'ordre de leur découverte, ce qui permet une étude simple des cycles.

c	-F(c)	Id. réduits	N°	c	-F(c)	Id. réduits	N°
1	3x23x41	-		34	3x569	-	
2	11x257	-		35	11x149	-	
3	3x941	-		36	3x523	-	
4	9x11x29	-		37	3x499	-	
5	53x53	(53,θ-5)	1	38	1423	-	
6	9x311	-		39	3x449	-	
7	3x929	-		40	3^3x47	(27,θ-40)	8
8	47x59	(47,θ-8)	2			(47,θ-40)	9
		(59,θ-8)	3	41	29x41	(29,θ-41)	10
9	3x919	-				(41,θ-41)	11
10	3x11x83	-		42	3^3x41	(27,θ-42)	12
11	2719	-				(41,θ-42)	13
12	3x29x31	-		43	3x11x31	(11,θ-43)	14
13	3^5x11	-				(93,θ-43)	15
14	2647	-				(31,θ-43)	16
15	3^3x97	-				(33,θ-43)	17
16	3x863	-		44	937	-	
17	2557	-		45	3x283	-	
18	3x29^2	-		46	3x11x23	(11,θ-46)	18
19	3x829	-				(69,θ-46)	19
20	31x79	-				(23,θ-46)	20
21	3x11x73	(33,θ-21)	4			(33,θ-46)	21
		(73,θ-21)	5	47	29x23	(23,θ-47)	22
22	3^2x269	-				(29,θ-47)	23
23	23x101	-		48	3x191	-	
24	9x11x23	(33,θ-24)	6	49	9x53	(9,θ-49)	24
		(69,θ-24)	7			(53,θ-49)	25
25	3x743	-		50	379	-	
26	2179	-		51	3^2x31	(3,θ-51)	26
27	3x709	-				(93,θ-51)	27
28	3x691	-				(9,θ-51)	28
29	2017	-				(31,θ-51)	29
30	3x653	-		52	3.59	(3,θ-52)	30
31	3^2x211	-				(59,θ-52)	31
32	11x167	-		53	73	(1,θ-53)	32
33	3^2x197	-				(73,θ-53)	33

Lorsqu'on construit "les" cycles on obtient le résultat suivant :

(1) → (25) → (28) → (16) → (6) → (19) → (14) → (27) → (30) → (3) → (9)
(22) ← (21) ← (5) ← (32) ← (33) ← (4) ← (20) ← (23) ← (11) ← (12) ↵
↳ (10) → (13) → (8) → (2) → 31) → (26) → (15) → (18) → (7) → (17)
(1) ← (24) ← (29) ↵

Conclusion : le corps $\mathbb{Q}(\sqrt{11317})$ est principal !

Exemple 2 .

On considère $k = \mathbb{Q}(\sqrt{130})$; le polynôme fondamental de ce corps est $F(X) = X^2-130$ et on a $[\theta] = 11$.

Les cycles d'idéaux réduits sont alors les suivants :

$(11,\theta-3) \to (11,\theta-8) \to (6,\theta-10) \to (5,\theta-10) \to (6,\theta-8) \to (11,\theta-3)$

$(7,\theta-5) \to (15,\theta-10) \to (2,\theta-10) \to (15,\theta-5) \to (7,\theta-9) \to (7,\theta-5)$

$(9,\theta-7) \to (9,\theta-11) \to (1,\theta-11) \to (9,\theta-7)$

$(3,\theta-10) \to (10,\theta-10) \to (3,\theta-11) \to (3,\theta-10)$.

Le groupe des classes de $\mathbb{Q}(\sqrt{130})$ est d'ordre 4. Remarquons alors que $(2,\theta)^2 = (2)$, que $(10,\theta)^2 = (10)$ et $(5,\theta)^2 = (5)$. Le groupe des classes de $\mathbb{Q}(\sqrt{130})$ est par conséquent isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. L'utilisation du dernier cycle permet de calculer une unité fondamentale de $\mathbb{Q}(\sqrt{130})$ à savoir :

$$\varepsilon = \rho_3 = \frac{\theta-10}{3} \times \frac{\theta-11}{10} \times \frac{\theta-10}{3} = -57 + 5\theta \ .$$

L'unité fondamentale de $\mathbb{Q}(\sqrt{130})$ est donc $\varepsilon_1 = -\bar{\varepsilon} = 57 + 5\theta$.

Remarque 6.10.

Si $\{(a_i,\theta-c_{a_i})\}_{i=0,\ldots,\ell-1}$ est la suite des idéaux d'un cycle, l'unité fondamentale de k est

$$\rho_\ell = \prod_0^{\ell-1} \frac{\theta-c_{a_i}}{a_i} \ .$$

On a donc $N_{K/\mathbb{Q}}\rho_\ell = \prod_0^{\ell-1} \frac{N(\theta-c_{a_i})}{a_i^2}$.

Il en résulte que la norme de l'unité fondamentale est +1 ou -1 selon que ℓ est pair ou impair. En particulier la parité du nombre d'idéaux d'un cycle ne dépend pas de celui-ci.

APPENDICE

Majoration du nombre des classes d'un corps quadratique, solution de B. MORFIN

Proposition.

Soient $K = \mathbb{Q}(\sqrt{m})$, où m est un entier sans facteurs carrés, et Δ le discriminant de K . Le nombre des classes h de K vérifie :

$$h < \frac{|\Delta|}{6} + \sqrt{\frac{|\Delta|}{12}} \quad .$$

Démonstration : Puisque chaque classes contient au moins un idéal réduit sans facteur rationnel, il suffit de majorer le nombre de ces idéaux pour majorer h .

La norme a d'un idéal réduit sans facteur rationnel vérifie : $a^2 \leq N$ avec $N = [\frac{|\Delta|}{3}]$.

Les racines d'un idéal réduit $\mathfrak{a} = (a, \theta - i)$ sont définies modulo a . Il y a donc au plus a idéaux réduits sans facteurs rationnels de norme a . D'après les trois remarques précédentes, on a :

$$h \leq \sum_{i=1}^{N} i = \frac{N(N+1)}{2} < \frac{|\Delta|}{6} + \sqrt{\frac{|\Delta|}{12}} \quad .$$

Corollaire.

Soit p un nombre premier. Le nombre de classes de $\mathbb{Q}(\sqrt{\pm p})$ est premier à p .

Démonstration : On va montrer en fait que : $h < p$. En majorant $|\Delta|$ par $4p$, on obtient d'après la proposition précédente :

$$h < \frac{2p}{3} + \sqrt{\frac{p}{3}} \quad .$$

Si $p \geq 3$, $\sqrt{\frac{p}{3}} \leq \frac{p}{3}$ donc $h < p$.

Si $p = 1$ ou 2 , on sait que $h = 1$.

Calcul pratique du nombre de classes des corps quadratiques réels (rédaction de B. MORFIN).

(On trouve dans [1], chap. 2, Sec.7.3 un algorithme, fondé sur un développement en fraction continue, donnant l'unité fondamentale d'un corps

quadratique réel. On met, ci-après, en évidence, le parallélisme de ce développement avec la répartition en cycle des idéaux réduits en s'appuyant sur des notes manuscrites de G. GRAS).

Notations.

On se place dans un corps quadratique $K = \mathbb{Q}(\sqrt{m})$, où m est un entier positif sans facteurs carrés.

Comme d'habitude, on pose :

$$F(X) = X^2 - m \qquad \text{si} \quad m \equiv 2,3(4)$$
$$\theta = \sqrt{m}$$

et

$$F(X) = X^2 - X + \frac{1-m}{4} \qquad \text{si} \quad m \equiv 1(4)$$
$$\theta = \frac{\sqrt{m}+1}{4}$$

On pose aussi : $\theta' = -\bar{\theta}$, où $\bar{\theta}$ est le conjugué de θ . On a donc : $\theta' = \theta - S$ avec $S = \theta + \bar{\theta}$

$$\theta' = \sqrt{m} \qquad \text{si} \quad m \equiv 2,\ 3(4)$$

et

$$\theta' = \frac{\sqrt{m}-1}{2} \qquad \text{si} \quad m \equiv 1(4) \ .$$

On rappelle que le successeur d'un idéal réduit $\mathfrak{a} = (a, \theta - c_{\mathfrak{a}})$, où $c_{\mathfrak{a}}$ désigne la racine finale, est l'idéal réduit :

$$\mathfrak{a}_1 = (a_1, \theta - (S - c_{\mathfrak{a}})) = (a_1, \theta' + c_{\mathfrak{a}_o})$$

avec $F((c_{\mathfrak{a}}) = -aa_1$.

On note $\mathfrak{a}_i$ le successeur de $\mathfrak{a}_{i-1}$. Le symbole $[\alpha]$ désigne la partie entière du nombre réel α . A tout idéal réduit $\mathfrak{a} = (a, \theta - c_{\mathfrak{a}})$, on associe le nombre $\dfrac{\theta' + c_{\mathfrak{a}}}{a}$.

Nous allons montrer que le calcul du cycle engendré par un idéal réduit $\mathfrak{a}$ peut se faire en effectuant le développement en fraction continue de $\dfrac{\theta' + c_{\mathfrak{a}}}{a}$.

Remarque : Le développement en fraction continue de $\frac{\theta'+c_{\mathfrak{a}}}{a}$ est périodique. En effet, $\frac{\theta'+c_{\mathfrak{a}}}{a}$ est quadratique ; il suffit d'appliquer le théorème de Legendre.

Proposition.

Soient $\mathfrak{a}_o$ un idéal réduit et $\mathfrak{a}_1$ son successeur. Notons a_o et a_1 leurs normes et $c_{\mathfrak{a}_o}, c_{\mathfrak{a}_1}$ leurs racines finales respectives. Alors

$$\frac{\theta'+c_{\mathfrak{a}_1}}{a_1} = \left[\frac{\theta'+c_{\mathfrak{a}_1}}{a_1}\right] + \frac{a_o}{\theta'+c_{a_o}}$$

et le deuxième membre est le développement en fraction continue à l'ordre 1 de $\frac{\theta'+c_{\mathfrak{a}_1}}{a_1}$.

On en déduit alors grâce à l'unicité du développement en fraction continue :

Corollaire.

Ecrire le cycle des idéaux semi-réduits équivalents à $\mathfrak{a}_o$ revient à écrire le développement en fraction continue de $\frac{\theta'+c_{\mathfrak{a}_o}}{a_o}$.

Démonstration de la proposition : Il faut montrer que :

1) $\frac{\theta'+c_{\mathfrak{a}_1}}{a_1} - \frac{a_o}{\theta'+c_{\mathfrak{a}_o}}$ est un entier.

2) $0 < \frac{a_o}{\theta'+c_{\mathfrak{a}_o}} < 1$.

On sait que $c_{\mathfrak{a}_1} = S - c_{\mathfrak{a}_o} + na_1$, $n \in Z$. Le calcul devient alors :

$$\frac{\theta'+c_{\mathfrak{a}_1}}{a_1} - \frac{a_o}{\theta'+c_{\mathfrak{a}_o}} = \frac{\theta'+S-c_{\mathfrak{a}_o}+na_1}{a_1} - \frac{a_o}{\theta'+c_{\mathfrak{a}_o}} = n + \frac{(\theta'+S-c_{\mathfrak{a}_o})(\theta'+c_{\mathfrak{a}_o}) - a_o a_1}{a_1(\theta'+c_{\mathfrak{a}_o})}$$

$$= n + \frac{(\theta-c_{\mathfrak{a}_o})(-\bar{\theta}+c_{\mathfrak{a}_o}) - a_o a_1}{a_1(\theta'+c_{\mathfrak{a}_o})} = n .$$

Montrons maintenant que : $0 < \frac{a_o}{\theta'+c_{\mathfrak{a}_o}} < 1$. L'idéal $\mathfrak{a}_o$ est réduit donc :

$$\bar{\theta} < c_{\mathfrak{a}_1} - a_o$$

et

$$0 < a_o < c_{\mathfrak{a}_o} - \bar{\theta} = c_{\mathfrak{a}_o} + \theta' \ .$$

Remarque : Dans le développement en fraction continue à l'ordre 1 de $\frac{\theta'+c_{\mathfrak{a}_o}}{a_o}$, ce n'est pas le successeur mais le prédécesseur de $\mathfrak{a}_o$ qui intervient. Dans la pratique, on obtient donc le cycle en commençant par le dernier idéal, comme le montrent les exemples.

Exemple 1. $m = 115$, $h = 2$,

$m \equiv 3\ (4)$ $\qquad [\theta] = 10$ $\qquad [\sqrt{\Delta}] = 21$

		Idéaux réduits	
$-F(1) = 114$	$= 2.3.19$		
$-F(2) = 111$	$= 3.37$		
$-F(3) = 106$	$= 2.53$		
$-F(4) = 99$	$= 3^2.11$	$(11, \theta-4)$	$(9, \theta-4)$
$-F(5) = 90$	$= 2.3^2.5$	$(10, \theta-5)$	$(9, \theta-5)$
		$(15, \theta-5)$	$(6, \theta-5)$
$-F(6) = 79$			
$-F(7) = 66$	$= 2.3.11$	$(11, \theta-7)$	$(6, \theta-7)$
$-F(8) = 51$	$= 3.17$	$(17, \theta-8)$	$(3, \theta-8)$
$-F(9) = 34$	$= 2.17$	$(17, \theta-9)$	$(2, \theta-9)$
$-F(10) = 15$	$= 3.5$	$(3, \theta-10)$	$(5, \theta-10)$
		$(15, \theta-10)$	$(1, \theta-10)$

Calcul des cycles.

par la méthode du chapitre I :

1er cycle :

$a_o = (11, \theta-4)$

$a_1 = (9, \theta-5)$

$a_2 = (10, \theta-5)$

$a_3 = (9, \theta-4)$

$a_4 = (11, \theta-7)$

$a_5 = (6, \theta-10)$

$a_6 = (15, \theta-10)$

$a_7 = (1, \theta-10)$

$a_8 = (15, \theta-5)$

$a_9 = (6, \theta-7)$

2e cycle :

$a_o = (17, \theta-8)$

$a_1 = (3, \theta-10)$

$a_3 = (5, \theta-10)$

$a_4 = (3, \theta-8)$

$a_5 = (17, \theta-9)$

$a_6 = (2, \theta-9)$

par la méthode des fractions continues :

$$\frac{\theta+4}{11} = 1 + \frac{6}{\theta+7}$$

$$\frac{\theta+7}{6} = 2 + \frac{15}{\theta+5}$$

$$\frac{\theta+5}{15} = 1 + \frac{1}{\theta+10}$$

$$\theta+10 = 20 + \frac{15}{\theta+10}$$

$$\frac{\theta+10}{15} = 1 + \frac{6}{\theta+5}$$

$$\frac{\theta+5}{6} = 2 + \frac{11}{\theta+7}$$

$$\frac{\theta+7}{11} = 1 + \frac{9}{\theta+4}$$

$$\frac{\theta+4}{9} = 1 + \frac{10}{\theta+5}$$

$$\frac{\theta+5}{10} = 1 + \frac{9}{\theta+5}$$

$$\frac{\theta+5}{9} = 1 + \frac{11}{\theta+4}$$

$$\frac{\theta+8}{17} = 1 + \frac{2}{\theta+19}$$

$$\frac{\theta+9}{2} = 9 + \frac{17}{\theta+9}$$

$$\frac{\theta+9}{17} = 1 + \frac{3}{\theta+8}$$

$$\frac{\theta+8}{3} = 6 + \frac{5}{\theta+10}$$

$$\frac{\theta+10}{5} = 4 + \frac{3}{\theta+10}$$

$$\frac{\theta+10}{3} = 6 + \frac{17}{\theta+8}$$

Exemple 2. $m = 105$, $h = 2$.

$m \equiv 1\ (4)$ $\quad [\theta] = 5$ $\quad [\sqrt{\Delta}] = 10$

	Idéaux réduits	
$-F(1) = 26 = 2\times13$		
$-F(2) = 24 = 2^3\times3$	$(6,\theta-2)$	$(4,\theta-2)$
$-F(3) = 20 = 2^2\times5$	$(4,\theta-3)$	$(5,\theta-3)$
$-F(4) = 14 = 2\times7$	$(7,\theta-4)$	$(2,\theta-4)$
$-F(5) = 6 = 2\times3$	$(2,\theta-5)$	$(3,\theta-5)$
	$(1,\theta-5)$	$(6,\theta-5)$

Calcul des cycles.

par la méthode du chapitre I : par la méthode des fractions continues

Idéal associé à $\dfrac{a}{\sqrt{m}+c_a}$

1er cycle :

$a_o = (7,\theta-4)$	$\dfrac{\sqrt{m}+17}{14} = 1 + \dfrac{4}{\sqrt{m}+7}$		$(2,\theta-4)$
$a_1 = (2,\theta-5)$	$\dfrac{\sqrt{m}+7}{4} = 4 + \dfrac{6}{\sqrt{m}+9}$		$(3,\theta-5)$
$a_2 = (3,\theta-5)$	$\dfrac{\sqrt{m}+9}{6} = 3 + \dfrac{4}{\sqrt{m}+9}$		$(2,\theta-5)$
$a_3 = (2,\theta-4)$	$\dfrac{\sqrt{m}+9}{4} = 4 + \dfrac{14}{\sqrt{m}+17}$		$(7,\theta-4)$

2e cycle :

$a_o = (6,\theta-2)$	$\dfrac{\sqrt{m}+3}{12} = 1 + \dfrac{2}{\sqrt{m}+9}$		$(1,\theta-5)$
$a_1 = (4,\theta-3)$	$\dfrac{\sqrt{m}+9}{2} = 9 + \dfrac{12}{\sqrt{m}+9}$		$(6,\theta-5)$
$a_2 = (5,\theta-3)$	$\dfrac{\sqrt{m}+9}{12} = 1 + \dfrac{8}{\sqrt{m}+3}$		$(4,\theta-2)$
$a_3 = (4,\theta-2)$	$\dfrac{\sqrt{m}+3}{8} = 1 + \dfrac{\sqrt{m}+5}{10}$		$(5,\theta-3)$
$a_4 = (6,\theta-5)$	$\dfrac{\sqrt{m}+5}{10} = 1 + \dfrac{8}{\sqrt{m}+5}$		$(4,\theta-3)$
$a_5 = (1,\theta-5)$	$\dfrac{\sqrt{m}+5}{8} = 1 + \dfrac{12}{\sqrt{m}+3}$		$(6,\theta-2)$

BIBLIOGRAPHIE

[1] - BOREVICH and SCHAFAREVICH - "Number Theory". Academic Press.

[2] - A. CHATELET - "L'arithmétique des corps quadratiques". Monographie de l'Enseignement Mathématique n°9 - Genève.

[3] - E.L. INCE - "Cycles of reduced ideals in quadratic fields".
Maths Tables Vol. IV Brit. Ass. Adv. Science London 1934.

[4] - O. ZINK - "Construction du groupe des classes d'idéaux d'un corps quadratique réel".
Journées Arithmétiques de Besançon (1965).