PACIFIC JOURNAL OF MATHEMATICS
Vol. 96, No. 1, 1981

GROUPE DES CLASSES ET UNITE FONDAMENTALE DES EXTENSIONS QUADRATIQUES RELATIVES A UN CORPS QUADRATIQUE IMAGINAIRE PRINCIPAL

HÉDI AMARA

On établit un algorithme qui permet de calculer le nombre des classes et l'unité fondamentale des extensions quadratiques, non galoisienne sur Q, d'un corps quadratique imaginaire principal. La méthode consiste à mettre en évidence des représentants des classes d'idéaux, les idéaux réduits, qui s'introduisent au moyen des bases. Le regroupement de ces idéaux en classes, qui constitue l'essentiel de ce travail, donne le nombre des classes et l'unité fondamentale.

I. Notations. Idéaux réduits. Soit k l'un des 9 corps quadratique imaginaires principaux, O_k son anneau des entiers, α un entier de k sans facteurs carrés, K le corps $k(\sqrt{\alpha})$ et O_K son anneau des entiers, $\{1, \theta\}$ une O_k base des O_K et enfin τ (respectivement σ) le k-automorphisme non trivial de K (respectivement la conjugaison complexe).

Comme dans le cas des corps quadratiques [2], chaque classe d'idéaux fractionnaires de K contient un idéal entier admettant le couple $(a, \theta - c)$ comme O_k base où a et c sont deux entiers de k, appelés norme et racine, reliés par la relation $F(c) \equiv 0 \bmod a$, avec:

$$F(X) = X^2 - (\theta + \theta^\tau)X + \theta\theta^\tau .$$

DÉFINITION I. 1: un idéal entier $I = (a, \theta - c)$ est dit réduit si et seulement si il vérifie la propriété suivante: pour tout $\xi \in I$, $\xi \neq 0$ on a:

$$|a| \leqq \sup(|\xi|, |\xi^\tau|) .$$

Conséquences. (1) I est réduit si et seulement I^τ le soit aussi et ils ont la même norme.

(2) Il existe un nombre fini d'idéaux réduits.

Plus précisement: pour que $(a, \theta - c)$ soit réduit il faut que $|a|^2 \leqq (4/\Pi^2)\sqrt{D_{K/Q}}$ où $D_{K/Q}$ désigne le discriminant positif de K/Q.

(3) chaque classe d'idéaux fractionnaires de K contient au moins un idéal réduit.

PROPOSITION I.2. *Soient $I = (a, \theta - c_1)$ et $J = (b, \theta - c_2)$ deux idéaux réduits. Pour que JI^{-1} soit principal il faut et il suffit il existe dans I un élément h_0 tel que $|h_0| < |a|$ et vérifiant:*

(i) $J = (h_0^{\tau}/a)I$ *et* $N(h_0) = \varepsilon ab$ *où* N *désigne la norme de* K/k *et* ε *une unité de* k.

(ii) *pour tout* $h \in I^*$, $|h| < |h_0|$ *on a* $|h_0^{\tau}| \leqq |h^{\tau}|$.

Cette dernière condition est appelée condition de réduction et tout élément $h \in I^*$, $|h| < |a|$ *et vérifiant* (ii) *est appelé élément réduit dans* I.

Démonstration. Si JI^{-1} est principal, il existe $\gamma \in K^*$ tel que $J = \gamma I$; comme $b \in J$ il existe $\xi_0 \in I^*$ tel que $b = \gamma\xi_0$, si $|\xi_0| < a$ prenons $h_0 = \xi_0$ et en prenant la norme des deux membres dans l'égalité $J = \gamma I$ on obtient $b = N(J) = \varepsilon N(\gamma)$ a, avec ε unité de k.

On en déduit que: $b = \gamma h_0 = \varepsilon\gamma\gamma^{\tau}a$ donc que $h_0^{\tau}/a = \varepsilon^{\tau}\gamma$ et ainsi $J = \gamma I = h_0^{\tau}I/a$ et on obtient facilement $N(h_0) = \varepsilon ab$. Si $|\xi_0| > |a|$ on choisit u unité de K telle que $|u\xi_0| < |a|$ et on prend $h_0 = u\xi_0$ et on obtient facilement la même chose.

D'autre part comme J réduit on a pour tout $\eta \in J^*$, $|b| \leqq \sup(|\eta|, |\eta^{\tau}|)$ mais en tenant compte du fait que $J = (h_0^{\tau}/a)I$ ceci revient à dire que pour tout $\xi \in I^*$ on a:

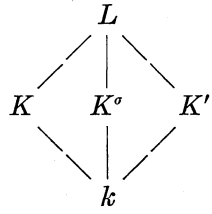
$$\frac{|h_0^{\tau}|\,|h_0|}{|a|} \leqq \sup\left(\frac{|h_0^{\tau}|\,|\xi|}{|a|}, \frac{|h_0|\,|\xi^{\tau}|}{|a|}\right)$$

en divisant par $|h_0^{\tau}|/|a|$ ceci reste équivalent à: pour tout $\xi \in I^*$ $|h_0| \leqq \sup(|\xi|, (|h_0|\,|\xi^{\tau}|/|h_0^{\tau}|))$. Cette dernière inégalité étant trivialement vérifiée pour les $\xi \in I^*$ tels que $|\xi| \geqq |h_0|$ elle devient donc équivalente à: pout tout $\xi \in I^*$, $|\xi| < |h_0|$ on a $|h_0| \leqq |h_0|\,|\xi^{\tau}|/|h_0^{\tau}|$ et c'est bien (ii).

Pour regrouper les idéaux réduits en classes, on est donc amené à étudier pour un idéal I l'ensemble de ses éléments réduits noté R_I. Le lemme suivant vérifié dans le cas K/Q non galoisien (i.e., $\alpha\alpha^{\tau} \notin k^{*2}$) simplifie cette étude.

LEMME I.3. *Soit* $I = (a, \theta - c)$ *un idéal réduit et soient* ξ *et* η *deux éléments de* R_I. *Pour que* $|\xi| = |\eta|$ *il faut et il suffit que* $\xi = \varepsilon\eta$ *avec* ε *unité de* k. *Plus précisemment les éléments de même module dans* R_I *diffère d'une unité de* k.

Démonstration. Si L désigne la cloture galoisienne de K et K' l'extension bicyclique $k(\sqrt{\alpha\alpha^{\tau}})$ on a la figure suivante:



Soit $\dot{J} = (\eta^\tau/a)I$, $\dot{J}$ est un idéal réduit de norme $b = \varepsilon_1(\eta\eta^\tau/a)$ avec ε_1 unité de k. L'élément $t = (\eta^\tau/a)\xi$ appartient à $\dot{J}$ et il est tel que $|t| = |b|$. Ecrivons $|t|^2 = tt^\sigma = bb^\sigma = |b|^2 \in \boldsymbol{Z}$ si bien que $t^\sigma = (|b|^2/t)$ appartient à K. On en déduit que $t \in K \cap K^\sigma = k$, comme $t \in \dot{J}$ on a $t \in \dot{J} \cap k = \dot{J} \cap O_k = bO_k$ et ainsi $t = b\varepsilon_2$ avec $\varepsilon_2 \in O_k$, $|\varepsilon_2| = 1$.

Cette dernière égalité s'écrit en remplaçant t et b par leur valeur $(\eta^\tau/a)\xi = \varepsilon_1\varepsilon_2(\eta\eta^\tau/a)$ et ainsi $\xi = \varepsilon\eta$ avec $\varepsilon = \varepsilon_1\varepsilon_2$ unité de k.

II Etude de R_I. Pour un idéal $I = (a, \theta - c)$ on va étudier R_I modulo les unités de k. Considérons l'application φ:

$$IN \longrightarrow |R_I| \cup \{|a|\}$$

définie par récurrence par:

$$\varphi(0) = |a| = |h_0|$$

$\varphi(n) = |h_n|$ où h_n est l'élément de I^* vérifiant:

(i) $|h_n| < |h_{n-1}|$

(ii) pour tout $h \in I^*$ et $|h| < |h_{n-1}|$ on a $|h_n^\tau| \leqq |h^\tau|$.

La condition (ii) est plus forte que la condition de réduction assure que $h_n \in R_I$ et l'existence des h_n n'étant pas difficile à voir si bien que φ est bien définie en vertu du Lemme I.3.

LEMME II.1. *La suite $\varphi(n) = |h_n|$ est décroissante et tend vers zéro.*

Démonstration. $|h_n|$ est décroissante par construction. Supposons que $|h_n|$ ne tend pas vers zéro. Il existe $t > 0$ tel que pour tout $n \in N$, $|h_n| \geqq t$. Soit $\xi \in I^*$ avec $|\xi| < t$, d'après la définition des h_n on doit avoir pour tout entier n, $|h_n^\tau| \leqq |\xi^\tau|$ ce qui donne les inégalités suivantes:

$$t \leqq |h_n| \leqq |a|$$
$$|a| \leqq |h_n^\tau| \leqq |\xi^\tau| .$$

Ceci exprimé au moyen du plongement habituel de la géométrie des nombres de K dans C^2 définie par: $s(\beta) = (\beta, \beta^\tau)$ pour tout $\beta \in K$ et pour lequel $s(I)$ est un réseau de C^2 donne $s(R_I) \subset s(I) \cap D$ où D est le compact de C^2 définie par:

$$D = \left\{(x, y) \in C^2 \;\middle\backslash\; \begin{matrix} t \leqq |x| \leqq |a| \\ |a| \leqq |y| \leqq |\xi^\tau| \end{matrix}\right\}$$

mais ceci entraine que R_I est fini ce qui est absurde.

LEMME II.2. *φ est une bijection de IN dans $|R_I| \cup \{|a|\}$.*

Démonstration. φ est injective par construction. Démontrons la surjectivité: soit $h \in R_I$: comme $|h| < |a|$ et que $\{|h_n|\}$ tend vers zéro en décroissant, il existe un entier m tel que $|h_{m+1}| \leqq |h| < |h_m|$ supposons que $|h_{m+1}| < |h|$, h étant un élément réduit de I cela entraine que $|h^{\tau}_{m+1}| \geqq |h^{\tau}|$. Par ailleurs d'après la définition de h_{m+1} et du fait que $|h| < |h_m|$ on a: $|h^{\tau}_{m+1}| \leqq |h^{\tau}|$ d'où l'égalité $|h^{\tau}| = |h^{\tau}_{m+1}|$ et par un raisonnement analogue à celui du Lemme I.3 on déduit que $h^{\tau} = \varepsilon h^{\tau}_{m+1}$ avec ε unité de k si bien que $h = \varepsilon^{\tau} h_{m+1}$ et φ est surjective.

LEMME II.3. *Soit u une unité de K*
(i) *Si $|u| \leqq 1$ alors pour tout h de R_I, $uh \in R_I$*
(ii) *Si $|u| < 1$ alors $ua \in R_I$.*

Démonstration. (i) Si $h \in R_I$, montrons que uh vérifie la condition de réduction soit $h_1 \in I^*$ et $|h_1| < |uh|$, ceci entraine: $|h_1 u^{-1}| < |h|$ donc h étant réduit:

$$|h_1^{\tau}(u^{-1})^{\tau}| \geqq |h^{\tau}| \quad \text{d'où} \quad |h_1^{\tau}| \geqq |(uh)^{\tau}|$$

(ii) Se démontre de la même manière.

III. Cycles d'idéaux réduits. Soit $I = (a, \theta - c)$ un idéal réduit et R_I l'ensemble de ses éléments réduits. $R_I = \{h_n\}_{n \in N^*}$. Notons Θ_I l'ensemble des idéaux réduits équivalents à I et considérons l'application $\Psi: R_I \to \Theta_I$ qui:

$$h_i \longrightarrow \frac{h_i^{\tau}}{a} I = I_i$$

pour tout $i \in N^*$. On appelle I_i le i-ème successeur de I.

LEMMA III.1. (i) *Ψ est surjective*
(ii) *$\Psi(i) = \Psi(j)$ si et seulement si il existe u unitè de K telle que $h_i = uh_j$.*

Démonstration. (i) Est une conséquence de la Proposition I.2.

Pour (ii) dire que $\Psi(i) = \Psi(j)$ c'est dire que $I_i = (h_i^{\tau}/a)I = I_j = (h_j^{\tau}/a)I$ donc qu'il existe u unité de K tel que $h_i = uh_j$.

LEMME III.2. *Pour tout $n \in N^*$, R_{I_n} est formé par les éléments $(h_n^{\tau}/a)h_i$ avec $i \geqq n + 1$.*

Démonstration. Pour montrer le lemme il suffit de montrer

que $|(h_n^\tau/a)h_i| < |NI_n|$ et les $(h_n^\tau/a)h_i$ vérifie la condition de réduction pour $i \geqq n+1$. En effet $|NI_n| = (|h_n^\tau|/|a|)|h_n|$ et on voit bien que $|(h_n^\tau/a)h_i| < (|h_n^\tau|h_n|/|a|)$ si et seulement si $|h_i| < |h_n|$ donc que $i \geqq n+1$.

D'autre part soit $\eta_i \in I_n^*$ avec $|\eta_i| < |h_n^\tau h_i|/|a|$, il existe alors $h \in I^*$ tel que $\eta_i = (h_n^\tau/a)h$ avec $|h| < |h_i|$; comme h_i est réduit dans I on a $|h_i^\tau| \leqq |h^\tau|$ si bien que $|\eta_i^\tau| = |(h_n h^\tau/a)| \geqq (|h_n h_i^\tau|/|a|)$ et ainsi $(h_n^\tau/a)h_i$ vérifie la condition de réduction dans I_n.

LEMME III.3. *Pour tout* $(n, p) \in N^{*2}$ *on a*: $(I_n)_p = I_{n+p}$.

Démonstration. D'aprés la définition du p iéme successeur d'un idéal réduit et le lemme précédent on a:

$$(I_n)_p = \left(\frac{h_n^\tau}{a} h_{n+p}\right)^\tau \frac{I_n}{a_n} = \frac{h_n}{a}\frac{h_{n+p}^\tau}{a_n} I_n$$

avec $a_n = NI_n = (h_n h_n^\tau/a)$ à l'unité prés dans k

$$\text{donc que } (I_n)_p = \frac{h_n}{h_n}\frac{h_{n+p}^\tau I_n}{h_n^\tau} = \frac{h_{n+p}^\tau}{h_n^\tau}\frac{h_n^\tau}{h} I$$

$$= \frac{h_{n+p}^\tau I}{a} = I_{n+p}\,.$$

DÉFINITION III.4. On appelle cycle de I l'ensemble des idéaux réduits de la forme I_n avec $n \in N^*$.

THÈORÈME III.5. *Soient* $I = (a, \theta - c)$ *un idéal réduit,* $R_I = \{h_n\}_{n \in N^*}$ *l'ensemble de ses élements réduits définis au produit près par une unité de* k. *et* $I_n = (h_n^\tau/a)I$. *Les assertions suivantes sont vérifiées*:

(i) *Les idéaux réduits équivalents à* I *sont ceux du cycle de* I.

(ii) *soit* d *le plus petit entier naturel non nul tel que* $I_d = I$ *alors,* h_d/a *est une unité fondamentale de* K.

(iii) *pour tout* $n \in N^*$ *faisons la division euclidienne de* n *par* d: $n = dq + r$ *avec* $0 \leqq r < d$ *alors*: $h_n = (h_d/a)^q h_r$.

(iv) *l'ensemble des idéaux réduits du cycle de* I *est égal à*: $\{I, (h_1^\tau/a)I, \cdots, (h_{d-1}^\tau/a)I\}$.

Démonstration. (i) est une conséquence du Lemme III.1 (surjectivité de Ψ). L'existence de d est assuré par la finitude des idéaux réduits, d'autre part comme $I_d = (h_d^\tau/a)I = I$ il en résulte que h_d^τ/a est une unité de K de même que h_d/a, notons u_0 une unité fondamentale de K vérifiant $|u_0| < 1$. Donc il existe $n \in Z$ tel que $h_d/a = u_0^n$, d'après le Lemme II. 3, $u_0 a \in R_I$ et il est tel que $|u_0 a| \geqq |h_d|$,

d'après la définition de d on a: $h_d = u_0 a$ et ainsi $h_d/a = u_0$ l'égalité étant à l'unité près dans k.

Pour démontrer (iii) remarquons que $I_d = I$ entraine d'aprés le Lemme III.3 que pour tout $q \in N^*$, $I_{qd} = I$ et ainsi on aura $I_m = I_{qd+r} = I_r$, ce qui signifie qu'il existe u unité de K tel que $h_m = uh_r$. Plus précisemment et en tenant compte de (ii) qu'il existe $x \in Z$ tel que $h_m = (h_d/a)^x h_r$, montrons que $x = q$. D'après le Lemme III.2 R_{I_d} est formé par les $(h_d^\tau/a)h_i$ avec $i \geqq d+1$. Comme $I_d = I$ ceci entraine $R_{I_d} = R_I$, on en déduit que: $h_1 = (h_d^\tau/a)h_{d+1}, \cdots, h_m = (h_d^\tau/a)h_{d+m}, \cdots$ et en particulier on a: $h_{m-d} = (h_d^\tau/a)h_m$ pour tout $m \in N^*$ et $m - d > 0$, soit encore $h_{m-d}h_d = (h_d h_d^\tau/a)h_m$ qu'on peut écrire $h_m = h_{m-d}(h_d/a)$ grâce à $N(h_d) = a^2$ égalité modulo les unités de k. En intérant cette égalité suffisamment de fois:

$$h_m = h_{m-d}\frac{h_d}{a}$$

$$h_{m-d} = h_{m-2d}\frac{h_d}{a}$$

$$\vdots$$

$$h_{m-(q-1)d} = h_{m-qd}\frac{h_d}{a}$$

d'où $h_m = (h_d/a)^q h_r$.

(iv) est une conséquence de (iii).

IV. Description de l'algorithme. Pour la partie pratique on va en plus supposer que O_k est euclidien pour la norme (i.e., $m = 1, 2, 3, 7, 11$).

On aura besoin des définitions et des lemmes suivants:

LEMME IV. *Soit $I = (a, \theta - c)$ un idéal entier avec $|\theta - c| < |a|$. Pour que I soit réduitil faut et il suffit que pour tout $\xi = \lambda a + \mu(\theta - c)$ dans I avec $(\lambda, \mu) \in O_k^{*2}$ et vérifiant:*

$$|\mu| < \frac{2|a|}{|\theta - \theta^\tau|}, \quad |\lambda| < 1 + |\mu|$$

on a:

$$|a| \leqq \sup(|\xi|, |\xi^\tau|) .$$

Démonstration. Si I est non réduit il existe $\xi \in I^*$ tel que: $|\xi| < |a|$, $|\xi^\tau| < |a|$. Ecrivons $\xi = \lambda a + \mu(\theta - c)$ avec $(\lambda, \mu) \in O_k^{*2}$ on a: $|\xi - \xi^\tau| = |\mu(\theta - \theta^\tau)| \leqq |\xi| + |\xi^\tau|$ donc que $|\mu|\,|\theta - \theta^\tau| < 2|a|$ donc que $|\mu| < (2|a|/|\theta - \theta^\tau|)$. D'autre part on a:

$$||\lambda|\,|a| - |\mu|\,|\theta - c|\,| \leqq |\xi| < |a|$$

d'où:

$$\begin{aligned} |\lambda|\,|a| &< |a| + |\mu|\,|\theta - c| \\ &< |a| + |\mu|\,|a| \end{aligned}$$

et ainsi

$$|\lambda| < 1 + |\mu| .$$

LEMME IV.2. *Soit* $I = (a, \theta - c)$ *un idéal réduit,* M_I *l'ensemble de ses racines* (i.e., *les entiers de* k *vérifiant* $F(c) \equiv 0 \bmod a$). *Il existe dans* M_I *un élément unique* c_I *appelé racine minimum vérifiant:*

(i) $|\theta - c_I| < |a|$

(ii) *pour tout* $c \in M_I$ *avec* $|\theta - c| < |a|$ *on a* $|\theta^\tau - c_I| \leqq |\theta^\tau - c|$.

Démonstration. L'existence des $c \in M_I$ vérifiant $|\theta - c| < |a|$ est une conséquence de la structure de M_I et de la division euclidienne. En effet soit $c \in M_I$ il existe λ et c_r dans O_k avec $|c_r| < |a|$ et $c = \lambda a + c_r$, or $c_r = c - \lambda a$ est une racine de I car $F(c_r) = (\theta - c_r)(\theta^\tau - c_r) = (\theta - c + \lambda a)(\theta^\tau - c + \lambda a) = F(c) + \lambda a(S - 2c) + \lambda^2 a^2$ avec $S = \theta + \theta^\tau$ dans O_k, et on voit bien que $F(c_r) \equiv F(c) \equiv 0 \bmod a$ et comme il y a un nombre fini de c_r il n'y a qu'à prendre pour c_I celui qui est minimum parmi les $|\theta^\tau - c_r|$. Pour l'unicité supposons qu'il existe deux racines minimum c_1 et c_2. La condition (ii) entraine que $|\theta^\tau - c_1| = |\theta^\tau - c_2|$ qui entraine d'après le Lemme I.3 que $\theta^\tau - c_1 = \varepsilon(\theta^\tau - c_2)$ avec ε une unité de k. On en déduit que $\varepsilon = 1$ et $c_1 = c_2$ du fait que $\{1, \theta^\tau\}$ est aussi une O_k base de O_K.

LEMMA IV.3. *Soient* $I = (a, \theta - c_I)$ *un idéal réduit,* c_I *sa racine minimum et* $R_I = \{h_i\}_{i \in N^*}$. *Ecrivons* $h_1 = \lambda_0 a + \mu_0(\theta - c_I)$ *alors*

$$|\mu_0| < \frac{|a| + |\theta^\tau - c_I|}{|\theta - \theta^\tau|} , \quad |\lambda_0| < 1 + |\mu_0| .$$

Démonstration. D'après la définition de h_1 on doit avoir $|h_1| < |a|$ et $|h_1^\tau| \leqq |\theta^\tau - c_I|$ ceci donne:

$$|h_1 - h_1^\tau| = |\mu_0(\theta - \theta^\tau)| \leqq |h_1| + |h_1^\tau| < |a| + |\theta^\tau - c_I|$$

d'où la première inégalité. La deuxième s'établit comme dans le Lemme III.1. Les $(\lambda_0, \mu_0) \in O_k^{*2}$ vérifiant les inégalités précédentes sont en nombre fini, h_1 sera alors celui qui réalise le minimum, parmi les $h = \lambda_0 a + \mu_0(\theta - c_I)$, par $|h^\tau|$.

DÉFINITION IV.4. On appelle comme dans [6] h_1 élément de

conversion de I. La recherche sur ordinateur des idéaux réduits se ramène donc aux opérations suivantes:

(1) Dresser le tableau T des entiers de k vérifant $|a|^2 \leqq 4/\Pi^2\sqrt{D_{K/Q}}$.

(2) Chercher pour chaque entier $a \in T$ les entiers c de k à l'intérieur du disque de rayon $|a|$ et vérifiant $F(c) \equiv 0 \bmod a$.

(3) Identifier les idéaux entiers pour lesquels la différence de deux valeurs de c est multiple de a.

(4) Eliminer grâce au Lemme III.1 les idéaux non réduits.

(5) Calculer pour chaque idéal réduit sa racine minimum et son élément de conversion.

Ceci étant fait, on peut alors pour chaque idéal réduit I calculer à la main son premier succeur I_1 et engendrer ainsi tous les cycles du groupe des classes et l'unité fondamentale et ceci grâce aux deux remarques suivantes:

REMARQUE IV.5. Soit $I = (a, \theta - c_I)$ un idéal réduit, c_I sa racine minimum et h_1 son élément de conversion. Ecrivons $h_1 = \lambda_0 a + \mu_0(\theta - c_I)$ avec $(\lambda_0, \mu_0) \in O_k^2$. Si $\lambda_0\mu_0 = 0$ alors $h_1 = \theta - c_I$, $I_1 = (b, \theta - c)$ avec $b = (F(c_I)/a)$ et $c = S - c_I$, où $S = \theta + \theta^\tau$.

Si non, λ_0 et μ_0 sont premiers entre eux et on a: $I_1 = (b, \theta - c)$ avec: $b = (N(h_1)/a)$, $c = -[\lambda_0\lambda_1 a - \lambda_0\mu_1 c_I + \lambda_1\mu_0(S - c_I) + \mu_0\mu_1(F(c_I)/a]$ où λ_1 et μ_1 sont deux entiers de k tels que

$$\lambda_0\mu_1 - \mu_0\lambda_1 = 1 .$$

Démonstration. Si $\lambda_0\mu_0 = 0$ alors nécéssairement $\lambda_0 = 0$ car $|h_1| < |a|$ et $h_1 = (\theta - c_I)$ car $|h_1^\tau| \leqq |\theta^\tau - c_I|$ (définition de h_1) donc $I_1 = (h_1^\tau/a) = ((\theta^\tau - c_I)/a)I$ d'où:

$$I_1 = \frac{\theta^\tau - c_I}{a}(a, \theta - c_I) = \left(\theta^\tau - c_I, \frac{F(c_I)}{a}\right)$$

$$= \left(\frac{F(c_I)}{a}, S - \theta - c_I\right) = \left(\frac{F(c_I)}{a}, \theta - S + c_I\right) .$$

Si $\lambda_0\mu_0 \neq 0$, soit $d = PGCD(\lambda_0, \mu_0)$ alors $h_1 = dh_1'$ avec $h_1' = (\lambda_0/d)a + (\mu_0/d)(\theta - c_I)$ si d n'est pas une unité de k, l'élément h_1' de I^* vérifierait $|h_1'| < |h_1|$ et $|h_1'^\tau| < |h_1^\tau|$ ce qui est absurde vu la définition de h_1. Soit donc λ_1 et μ_1 deux entiers de k tels que: $\lambda_0\mu_1 - \mu_0\lambda_1 = 1$ (identité de Bezout dans O_k), comme $I_1 = (h_1^\tau/a)$ alors $N(I_1) = (N(h_1)/a)$ et $(h_1^\tau/a)[\lambda_1 a + \mu_1(\theta - c_I)] \in I_1$, calculons donc:

$$\frac{h_1^\tau}{a}[\lambda_1 a + \mu_1(\theta - c_I)] = \left[\lambda_0 + \mu_0\frac{(\theta^\tau - c_I)}{a}\right][\lambda_1 a + \mu_1(\theta - c_I)]$$

$$= \left[\lambda_0\lambda_1 a + \lambda_0\mu_1(\theta - c_I) + \mu_0\lambda_1(\theta^\tau - c_I) + \mu_0\mu_1\frac{F(c_I)}{a} \right]$$

$$= \left[\lambda_0\lambda_1 a + \lambda_0\mu_1\theta - \lambda_0\mu_1 c_I + \mu_0\lambda_1(S - \theta) - \mu_0\lambda_1 c_I + \mu_0\mu_1\frac{F(c_I)}{a} \right]$$

$$= (\lambda_0\mu_1 - \mu_0\lambda_1)\theta + \lambda_0\lambda_1 a - \lambda_0\mu_1 c_I + \mu_0\lambda_1(S - c_I) + \mu_0\mu_1\frac{F(c_I)}{a}$$

$$= \theta - c$$

avec pour c la valeur annoncée; si bien que c est une racine de I_1 et $I_1 = (b, \theta - c)$.

REMARQUE IV.6. Soient $I = (a, \theta - c_I)$ un idéal réduit et h_1 son élément de conversion. Soient $I_1, \cdots, I_{n-1}$ les successeurs de I jusqu'à l'ordre $n-1$, $a_1, \cdots, a_{n-1}$ leurs normes respectifs et $h_{1,1}, \cdots, h_{1,n-1}$ leurs éléments de conversion respectifs. Alors:

$$\frac{h_n^\tau}{a} = \frac{h_1^\tau}{a} \cdot \frac{h_{1\,1}^\tau}{a_1} \cdots \frac{h_{1\,n-1}^\tau}{a_{n-1}} .$$

Plus précisemment une unité fondamentale de K se calcule sur un cycle quelquonque d'idéaux réduits en faisant le produit de h_1/a par le produit des $(h_{1,j}/a_j)$, $j \in [1, \cdots, d-1]$ où d est le plus petit entier tel que $I_d = I$.

Démonstration. On démontre par récurrence sur n. Si $n = 2$ comme $I_1 = (h_1^\tau/a)I$ et $h_{1,1} = (h_1^\tau/a)h_2$ (Lemme III.2) alors

$$\frac{h_1^\tau}{a}\frac{h_{1,1}^\tau}{a_1} = \frac{h_1^\tau}{a}\frac{h_1}{a}\frac{h_2^\tau}{a_1} = \frac{h_1 h_1^\tau}{a a_1}\frac{h_2^\tau}{a} = \frac{h_2^\tau}{a}$$

car $a_1 = N(h_1)/a$. Supposons mainteonnt que:

$$\frac{h_{n-1}^\tau}{a} = \frac{h_1^\tau}{a_1}\frac{h_{1\,1}^\tau}{a_1} \cdots \frac{h_{1\,n-2}^\tau}{a_{n-2}} .$$

Comme $I_{n-1} = (h_{n-1}^\tau/a)\ I$ et $h_{1,n-1} = (h_{n-1}^\tau/a)h_n$ (Lemme III.2), on a alors:

$$\frac{h_{n-1}^\tau}{a}\frac{h_{1\,n-1}^\tau}{a_{n-1}} = \frac{h_{n-1}^\tau}{a}\frac{h_{n-1}}{a}\frac{h_n^\tau}{a_{n-1}}$$

$$= \frac{h_{n-1}h_{n-1}^\tau}{a a_{n-1}}\frac{h_n^\tau}{a} = \frac{h_n^\tau}{a} \quad \text{car} \quad a_{n-1} = \frac{N(h_{n-1})}{a} .$$

La seconde partie est immédiate d'après le Thèorème III.5.

V. **Exemples numériques.** Dans les deux exemples qui suivent,

les tableaux donnés constitue la liste des idéaux réduits fournie à l'aide de l'ordinateur. On lit dans la colonne "idéaux réduits" l'idéal donné sous la forme (a, c_I) ou a désigne sa norme c_I sa racine minimum. Dans la colonne "éléments de conversion" on lit l'élément de conversion de l'idéal correspondant, donné sous la forme $\lambda_0 a + \mu_0(\theta - c_I)$ avec λ_0, μ_0 dans O_k.

EXEMPLE I. $k = Q(\sqrt{-1})$ et $\alpha = 29 + 37i$ avec $i = \sqrt{-1}$.

Le décomposition en facteurs premiers de α est la suivante:

$$\alpha = -i(1 + i)(2 + i)(2 + 3i)(4 + i) .$$

O_K admet comme O_k base $\{1, \theta\}$ où θ est une racine carrée de $29 + 37i$ et on aura:

$$F(X) = X^2 - 29 - 37i$$
$$D_{K/k} = 4(29 + 37i)$$
$$D_{K/Q} = 2^9 \times 5 \times 13 \times 17 .$$

Le tableau des idéaux réduits est le suivant:

Idéal réduit	Elément de conversion	Idéal réduit	Elément de conversion
$I_{(0)} = (1, 6 + 3i)$	$\theta - 6 - 3i$	$I_{(14)} = (3 + 10i, -2 + 7i)$	$\theta + 2 - 7i$
$I_{(1)} = (1 + i, 5 + 3i)$	$\theta - 5 - 3i$	$I_{(15)} = (3 + 10i, 5 + 3i)$	$\theta - 5 - 3i$
$I_{(2)} = (1 + 3i, 4 + 2i)$	$\theta - 4 - 2i$	$I_{(16)} = (4 + i, 4 + i)$	$\theta - 4 - i$
$I_{(3)} = (1 + 10i, 4 - 5i)$	$\theta - 4 + 5i$	$I_{(17)} = (5 + i, 5 + i)$	$\theta - 5 - i$
$I_{(4)} = (1 + 10i, 5 - 6i)$	$-i(1 + 10i) + (1 + i)(\theta - 5 + 6i)$	$I_{(18)} = (5 + 2i, 2 + 2i)$	$\theta - 2 - 2i$
$I_{(5)} = (2 + i, 6 + 3i)$	$\theta - 6 - 3i$	$I_{(19)} = (5 + 2i, 3)$	$\theta - 3$
$I_{(6)} = (2 + 3i, 5 + i)$	$\theta - 5 - i$	$I_{(20)} = (5 + 6i, 1 + 5i)$	$\theta - 1 - 5i$
$I_{(7)} = (2 + 5i, 2 + 2i)$	$\theta - 2 - 2i$	$I_{(21)} = (5 + 6i, 4 + i)$	$\theta - 4 - i$
$I_{(8)} = (2 + 5i, 5 + i)$	$\theta - 5 - i$	$I_{(22)} = (5 + 8i, -2 + 7i)$	$\theta + 2 - 7i$
$I_{(9)} = (3 + 5i, 3 + 5i)$	$\theta - 3 - 5i$	$I_{(23)} = (5 + 8i, -1 + 6i)$	$i(5 + 8i) + (1 + i)(\theta + 1 - 6i)$
$I_{(10)} = (3 + 7i, 1 + 5i)$	$\theta - 1 - 5i$	$I_{(24)} = (6 + 5i, 3)$	$\theta - 3$
$I_{(11)} = (3 + 7i, 2 + 2i)$	$\theta - 2 - 2i$	$I_{(25)} = (6 + 5i, 3 + 5i)$	$\theta - 3 - 5i$
$I_{(12)} = (3 + 8i, 4 - 5i)$	$\theta - 4 + 5i$	$I_{(26)} = (7 + 3i, 2 + 2i)$	$\theta - 2 - 2i$
$I_{(13)} = (3 + 8i, 4 + 2i)$	$\theta - 4 - 2i$	$I_{(27)} = (7 + 3i, 5 + i)$	$\theta - 5 - i$

Le groupe de classes admet quatre cycles d'idéaux réduits qui sont les suivants:

(1) $I_{(0)} \longrightarrow I_{(5)}$

(2) $I_{(1)} \longrightarrow I_{(14)} \longrightarrow I_{(23)} \longrightarrow I_{(3)} \longrightarrow I_{(13)} \longrightarrow I_{(2)} \longrightarrow I_{(12)}$
$\longrightarrow I_{(4)} \longrightarrow I_{(22)} \longrightarrow I_{(15)}$

$$(3)\quad I_{(6)} \longrightarrow I_{(26)} \longrightarrow I_{(19)} \longrightarrow I_{(25)} \longrightarrow I_{(9)} \longrightarrow I_{(24)} \longrightarrow I_{(18)} \longrightarrow I_{(27)}$$
$$(4)\quad I_{(10)} \longrightarrow I_{(21)} \longrightarrow I_{(16)} \longrightarrow I_{(20)} \longrightarrow I_{(11)} \longrightarrow I_{(8)} \longrightarrow I_{(11)} \longrightarrow I_{(7)}\ .$$

Ceci donne pour K un nombre des classes $h_K = 4$, un groupe des classes isomorphes à $\boldsymbol{Z}/_{2Z} \times \boldsymbol{Z}/_{2Z}$ car chaque cycle contient un idéal réduit et son conjugué donc il est d'ordre 2 et comme unité fondamentale:

$$u_K = \frac{(\theta - 6 - 3i)^2}{2 + i} = \frac{-2(6 + 3i)\theta + 56 + 73i}{2 + i}$$
$$= -6\theta + 37 + 18i\ .$$

EXEMPLE II. $k = Q(\sqrt{-3})$, $\alpha = 10 + 8j$, j la racine cubique de 1 $j = -(1/2) + (\sqrt{3}/2)i$. Une O_k base de O_K est formée par 1 et une racine carrée de α. On a donc:

$$F(X) = X^2 - 10 - 8j$$
$$D_{K/k} = 4(10 + 8j)$$
$$D_{K/Q} = 2^6 \times 3^3 \times 7$$

La liste des idéaux réduits est la suivante:

Idéal réduit	Elémént de conversion
$I_{(0)} = (1, 3 + 2j)$	$\theta - 3 - 2j$
$I_{(1)} = (2 + j, 2 + j)$	$\theta - 2 - j$
$I_{(2)} = (2, 2 + 2j)$	$\theta - 2 - 2j$
$I_{(3)} = (3 + j, 2 + 3j)$	$\theta - 2 - 3j$
$I_{(4)} = (4 + j, 2 + j)$	$\theta - 2 - j$
$I_{(5)} = (4 + j, 1 + 3j)$	$\theta - 1 - 3j$
$I_{(6)} = (5 + 2j, 2 + 2j)$	$\theta - 2 - 2j$
$I_{(7)} = (5 + 2j, 1 + 3j)$	$\theta - 1 - 3j$
$I_{(8)} = (5, 3 + 2j)$	$\theta - 3 - 2j$
$I_{(9)} = (5, 2 + 3j)$	$\theta - 2 - 3j$

Ceci donne les deux cycles d'idéaux réduits suivants

$$(1)\quad I_{(0)} \longrightarrow I_{(9)} \longrightarrow I_{(3)} \longrightarrow I_{(8)}$$
$$(2)\quad I_{(2)} \longrightarrow I_{(7)} \longrightarrow I_{(4)} \longrightarrow I_{(1)} \longrightarrow I_{(5)} \longrightarrow I_{(6)}\ .$$

Ceci donne pour K un groupe des classes d'ordre $h_K = 2$ et une unité fondamentale:

$$u_K = \frac{(\theta - 3 - 2j)^2(\theta - 2 - 3j)^2}{25(3 + j)}$$
$$= \frac{[-2(3 + 2j)\theta + 15 + 16j][-2(2 + 3j)\theta + 5 + 11j]}{25(3 + j)}$$

$$= \frac{-2(2j-1)\theta - 13 + 5j}{3+j} = \frac{-2j(3+j)\theta + j(3+j)(7+3j)}{(3+j)}$$

$$= j(-2\theta + 7 + 3j) .$$

REFERENCES

1. H. Amara, *Détermination de la structure du groupe des classes et de l'unité fondamentale des extensions quadratiques relatives d'un corps quadratique imaginaire principal*, Thèse 3e cycle, Grenoble (1977).
2. A. Chatelet, *Les corps quadratiques*, Monographie de l'enseignement mathématiques, Genève (1962).
3. E. L. Ince, *Cycles of reduced ideals in quadratic fields*, British Association Tables, vol. **4**, London (1934).
4. R. B. Lakein, *Computation of the ideal class group of certain complex quartic fields*, Math of computation, **28** (1974).
5. ———, *Computation of the ideal class group of certain complex quartic fields* II, Math of computation, **29** (1975).
6. R. Smadja, *Sur le groupe des classes des corps de nombres*, C. R. A. S., **276** (1973).

Received January 21, 1978 and in revised form October 9, 1978.

UNIVERSITE DE TUNIS
TUNISIA