ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Projet de semestre

Été 2003

Fractions continues et unités dans les corps quadratiques

Julien HOURIET

-MA- 4ème année

Responsables :

Prof. Eva BAYER FLUCKIGER

Leonardo ZAPPONI

Table des matières

Chapitre 1

Corps quadratiques et unités

1.1 Introdution

Ce premier paragraphe consiste essentiellement en un rappel de notions de théorie algébrique des nombres. Pour de plus amples informations à ce sujet, on peut se référer, par exemple, au livre de Samuel [2].

Définition 1.1.1 (Corps de nombres)
Un corps de nombres est une extension finie de $\mathbb{Q}$.
Les éléments des corps de nombres, c'est-à dire les racines d'équations polynomiales, sont appelés les **nombres algébriques**.

Un corps quadratique est un cas particulier de corps de nombres:

Définition 1.1.2 (Corps quadratiques)
Un corps quadratique est une extension de degré 2 de $\mathbb{Q}$.

Remarques:
- On peut montrer que tout corps quadratique est de la forme $\mathbb{Q}(\sqrt{d})$, où d est un entier sans facteur carré.
- Soit $d \in \mathbb{Z}$ sans facteur carré, alors tout élément de $\mathbb{Q}(\sqrt{d})$ a une écriture unique sous la forme:
$$\alpha = x + y\sqrt{d}, \quad x, y \in \mathbb{Q}$$
Par conséquent: $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$

Convention: par la suite, sauf mention du contraire, d sera toujours supposé sans facteur carré.

Définition 1.1.3 (Conjugué, trace et norme)
Soit $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, alors:
- le conjugué de α, noté α', est le nombre $\alpha' = x - y\sqrt{d}$
- la trace de α est définie comme étant: $Tr(\alpha) = \alpha + \alpha'$

– la trace de α est définie comme étant: $N(\alpha) = \alpha\alpha'$

Remarques:
Soit $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, alors:
– $Tr(\alpha) = 2x$, donc $Tr(\alpha) \in \mathbb{Q}$
– $N(\alpha) = x^2 - dy^2$, donc $N(\alpha) \in \mathbb{Q}$
– le polynôme minimal de α s'écrit donc

$$(X - \alpha)(X - \alpha') = X^2 - Tr(\alpha)X + N(\alpha)$$

– l'application $\alpha \mapsto \alpha'$ est un automorphisme de $\mathbb{Q}(\sqrt{d})$. En effet, on a par simple application de la définition:

$$(\alpha_1 + \alpha_2)' = \alpha_1' + \alpha_2'$$

$$(\alpha_1\alpha_2)' = \alpha_1'\alpha_2'$$

1.2 Anneau des entiers des corps quadratiques

Définition 1.2.1 (Anneau des entiers)
L'anneau des entiers d'un corps de nombres K est la fermeture intégrale de $\mathbb{Z}$ dans K. Il est noté $\mathcal{O}_K$.
Les éléments de $\mathcal{O}_K$ sont appelés **entiers algébriques** de K.

Donc α est un entier algébrique si α est racine d'un polynôme unitaire à coefficients entiers. La remarque ci-dessus a comme conséquence immédiate la proposition:

Proposition 1.2.1 (Entiers de $\mathbb{Q}(\sqrt{d})$)
Soit $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, alors α est un entier algébrique si et seulement si $Tr(\alpha)$ et $N(\alpha)$ sont des entiers.

On peut relativement bien caractériser les entiers des corps quadrtiques grâce au théorème suivant:

Théorème 1.2.2 (Caractérisation des entiers de $\mathbb{Q}(\sqrt{d})$)
Un élément de $\mathbb{Q}(\sqrt{d})$ est un entier algébrique si et seulement s'il peut être écrit:

$$\alpha = \frac{u + v\sqrt{d}}{2}$$

avec u et $v \in \mathbb{Z}$ et les conditions suivantes sont vérifées:

$$(\clubsuit) \begin{cases} u \equiv v \mod 2 & \text{si } d \equiv 1 \mod 4 \\ u \equiv v \equiv 0 \mod 2 & \text{si } d \equiv 2,3 \mod 4 \end{cases}$$

Démonstration

Montrons que si $\alpha \in \mathbb{Q}(\sqrt{d})$ est entier, alors on a bien les conditions souhaitées.

$\alpha = \frac{u+v\sqrt{d}}{2}$ implique $Tr(\alpha) = u$ et $N(\alpha) = \frac{u^2-dv^2}{4}$.

Donc

$$u \in \mathbb{Z} \quad \text{car} \quad Tr(\alpha) \in \mathbb{Z}$$

De plus

$$-dv^2 = 4N(\alpha) - u^2 \in \mathbb{Z}$$

Ainsi $v \in \mathbb{Z}$ car, sinon, $v = \frac{a}{b} \notin \mathbb{Z}$ et $\frac{da^2}{b^2} \in \mathbb{Z}$ impliqueraient $b^2|d$, ce qui est impossible par l'hypothèse faite sur d.

Ensuite

$$u^2 - dv^2 = 4N(\alpha) \quad \text{donc} \quad u^2 - dv^2 \equiv 0 \mod 4$$

Supposons que v soit pair, alors $v^2 \equiv 0 \mod 4$, et donc u est pair.
Supposons maintenant que $v = 2k + 1$ avec k entier, alors

$$v^2 = 4(k^2 + k) + 1 \equiv 1 \mod 4$$

Or $u^2 \equiv 0$ ou $1 \mod 4$. De plus d sans facteur carré, donc $d \equiv 1, 2$ ou $3 \mod 4$.
Par conséquent, la seule possibilié pour u et d est:

$$u \equiv 1 \mod 2 \quad \text{et} \quad d \equiv 1 \mod 4$$

On a donc bien les relations souhaitées.

Inversément, soit $\alpha = \frac{u+v\sqrt{d}}{2}$ avec u et v entiers satisfaisant les conditions (♣).
On vérifie alors trivialement que $Tr(\alpha)$ et $N(\alpha)$ sont entières. Donc α est bien un entier algébrique.

□

COROLLAIRE 1.2.3
Soit $\alpha \in \mathbb{Q}(\sqrt{d})$. Alors α est entier si et seulement si α peut être écrit sous la forme:

$$\alpha = x + y\theta \qquad x, y \in \mathbb{Z}$$

où $\begin{cases} \theta := \frac{1+\sqrt{d}}{2} & \text{si} \quad d \equiv 1 \mod 4 \\ \theta := \sqrt{d} & \text{si} \quad d \equiv 2, 3 \mod 4 \end{cases}$

Démonstration: découle directement du théorème 1.2.2.

□

Remarque
$\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ est bien un anneau. En effet, à partir du corollaire, il suffit de vérifier que θ^2 peut s'écrire sous la forme $x + y\theta$, avec $x, y \in \mathbb{Z}$.
Le cas $d \equiv 2, 3 \mod 4$ est évident.
D'autre part, si $d \equiv 1 \mod 4$, alors:

$$\theta^2 = \left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1+2\sqrt{d}+d}{2} = \frac{d-1}{2} + \theta$$

Donc θ^2 est bien un entier algébrique, car $d-1$ est pair.

1.3 Unités des corps quadratiques

Définition 1.3.1 (Unité d'un anneau)
Soit A un anneau (commutatif) unitaire.
Un élément $a \in A$ est une unité s'il existe $b \in A$ tel que $ab = 1_A$.

Dans le cas particulier de l'anneau des entiers d'un corps quadratique, on a donc

Définition 1.3.2 (Unité de $\mathbb{Q}(\sqrt{d})$)
Soit $\alpha \in \mathbb{Q}(\sqrt{d})$ un entier algébrique. Alors α est une unité si α^{-1} est aussi un entier algébrique.

Remarque
- Soit ω une unité de $\mathbb{Q}(\sqrt{d})$, alors $N(\omega) = \pm 1$.
  En effet
  $$1 = N(\omega\omega^{-1}) = N(\omega)N(\omega^{-1})$$
  De plus $N(\omega)$ et $N(\omega^{-1})$ sont entières, donc égaux à ± 1.
- Inversément, soit $\omega \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ tel que $N(\omega) = \pm 1$
  Si $N(\omega) = 1$, alors $\omega\omega' = 1 \quad \Rightarrow \quad \omega^{-1} = \omega' \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$
  Si $N(\omega) = -1$, alors $\omega(-\omega') = 1 \quad \Rightarrow \quad \omega^{-1} = -\omega' \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

Par conséquent, un élément d'un corps quadratique est une unité si et seulement si sa norme vaut ± 1.

Notation: on notera U l'ensemble des unités de $\mathbb{Q}(\sqrt{d})$. C'est-à-dire:

$$U = \{\omega \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} | N(\omega) = \pm 1\}$$

On observe que U est un groupe multiplicatif, car

$$N(\omega_1\omega_2) = N(\omega_1)N(\omega_2)$$

Conséquences
Par les remarques ci-dessus et le théorème 1.2.2, on a:

$\omega \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ peut s'écrire $\omega = \frac{u+v\sqrt{d}}{2}$, $\quad u, v \in \mathbb{Z}$ satisfaisant la condition (♣).

$\Rightarrow\ N(\omega) = \frac{u^2-dv^2}{4}$

$\Rightarrow\ \omega \in U \quad \Leftrightarrow \quad \frac{u^2-dv^2}{4} = \pm 1$

$\Rightarrow$ Déterminer le groupe des unités de $\mathbb{Q}(\sqrt{d})$ revient à trouver les couples d'entiers satisfaisant

$$u^2 - dv^2 = \pm 4$$

De plus, si $d \equiv 2,3 \mod 4$, alors u et v doivent être pairs. Par conséquent, chercher les unités de $\mathbb{Q}(\sqrt{d})$ est équivalent à résoudre en variables entières l'équation:

$$x^2 - dy^2 = \pm 1$$

Ces équation sont appelées **équations de Pell-Fermat**.

1.4 Unités des corps quadratiques imaginaires

Soit d un entier positif, sans facteur carré. On considère le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-d})$.
Notre objectif est de déterminer U, le groupe des unités de $\mathbb{Q}(\sqrt{-d})$. Selon ce qui a été dit dans la section précédente, cela revient à:

Trouver $\omega = \frac{u+v\sqrt{-d}}{2}$ tel que $N(\omega) = \pm 1$ parmi $u, v \in \mathbb{Z}$ satisfaisant les conditions (♣).

1) $-d \equiv 2,3 \mod 4$, chercher $u, v \in 2\mathbb{Z}$ tels que $u^2 + dv^2 = \pm 4$, i.e. chercher $x, y \in \mathbb{Z}$ tels que $x^2 + dy^2 = \pm 1$

Si $d = 1$, alors $x^2 + y^2 = \pm 1$, $x, y \in \mathbb{Z}$ a seulement quatre solutions, à savoir $x = \pm 1$, $y = 0$ et $x = 0$, $y = \pm 1$.
Donc

$$U = \{1, -1, i, -i\}$$

Si $d \neq 1$, comme on a supposé $d > 0$, $d \equiv 2,3 \mod 4$

$\Rightarrow\ d \geq 2$

$\Rightarrow\ dy^2 \geq 2$ si $y \in \mathbb{Z} - \{0\}$

$\Rightarrow\ y = 0$

$\Rightarrow\ x^2 = \pm 1$

$\Rightarrow\ x = \pm 1$ car $x \in \mathbb{Z}$

$\Rightarrow\ U = \{1, -1\}$

2) $-d \equiv 1 \mod 4$, chercher $u, v \in \mathbb{Z}$, de même parité, tels que $u^2 + dv^2 = \pm 4$

Si $d = 3$ alors $u^2 + 3v^2 = \pm 4$ a six solutions, à savoir $x = \pm 2,\ y = 0$ et $x = \pm 1,\ y = \pm 1$.
Donc

$$U = \{1, -1, \frac{1+\sqrt{3}i}{2}, \frac{-1+\sqrt{3}i}{2}, \frac{1-\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}\}$$

Si $d \geq 7$, alors $dv^2 > 4$ si $v \in \mathbb{Z} - \{0\}$.
Donc $v = 0$ et $u = \pm 2$
Par conséquent

$$U = \{1, -1\}$$

Comme on le voit il est très facile de déterminer explicitement le groupe des unités des corps quadratiques imaginaires, car on se ramène à des équations bornées, donc ayant un nombre fini de solutions. On va voir par la suite que le cas réel n'est pas du tout trivial.

1.5 Unités des corps quadratiques réels

Toute la suite de ce travail consistera à développer une méthode générale permettant de déterminer le groupe des unités de $\mathbb{Q}(\sqrt{d})$ dans le cas ou $d > 0$. Dans un premier temps, nous allons montrer que si ce groupe possède un élément différent de $\{1, -1\}$, alors il est cyclique infini, modulo $\{1, -1\}$. Pour ce faire, énonçons ce résultat sous forme de théorème:

THÉORÈME 1.5.1
Soit $d > 0$, entier, sans facteur carré.
Modulo $\{1, -1\}$, le groupe des unités U de $\mathbb{Q}(\sqrt{d})$ est cyclique infini. De plus, il existe une unique unité $\omega_1 > 1$ qui engendre ce groupe.
On appelera ω_1 **l'unité fondamentale** de $\mathbb{Q}(\sqrt{d})$.

Démonstration:

Considérons l'application

$$\begin{array}{rccc} L: & U & \longrightarrow & \mathbb{R}^2 \\ & \omega & \longmapsto & (\log|\omega|, \log|\omega'|) \end{array}$$

Alors $Im(L) \subseteq D = \{(x, -x) \mid x \in \mathbb{R}\}$

En effet, si $\omega \in U$, alors $\omega' = \pm\omega^{-1}$. Donc $|\omega'| = \frac{1}{|\omega|}$

$$\Rightarrow \quad \log|\omega'| = -\log|\omega|$$

De plus, $L: U \longrightarrow D$ est un homomorphisme.

En effet:

$$\begin{aligned} L(\omega_1\omega_2) &= (\log|\omega_1\omega_2|, \log|(\omega_1\omega_2)'|) \\ &= (\log|\omega_1\omega_2|, \log|\omega_1'\omega_2'|) \\ &= (\log(|\omega_1||\omega_2|), \log(|\omega_1'||\omega_2'|) \\ &= (\log|\omega_1| + \log|\omega_2|, \log(\omega_1'| + \log|\omega_2'|) \\ &= (\log|\omega_1|, \log|\omega_1'| + (\log|\omega_2|, \log|\omega_2'|) \\ &= L(\omega_1) + L(\omega_2) \end{aligned}$$

Donc L est bien un homomorphisme.

Déterminons maintenant le noyau de L:

$$\begin{aligned} \omega \in ker(L) &\Leftrightarrow |\omega| = |\omega'| = 1 \\ &\Rightarrow |N(\omega)| = |\omega\omega'| = |\omega||\omega'| = 1 \text{ et } |Tr(\omega)| \leq |\omega| + |\omega'| = 2 \\ &\Rightarrow \text{Le polynôme minimal de } \omega \text{ est borné} \\ &\Rightarrow |ker(L)| < \infty \\ &\Rightarrow ker(L) \text{ est un groupe fini de racines de l'unité dans } \mathbb{R} \\ &\Rightarrow ker(L) = \{1, -1\} \end{aligned}$$

De plus, il n'y a qu'un nombre fini d'éléments de l'image de L dans toute région bornée de $\mathbb{R}^2$. En effet, toute région bornée de $\mathbb{R}^2$ est contenue dans une boule. On peut donc supposer qu'il existe $B > 0$ tel que $\log|\omega| \leq B$ et $\log|\omega'| \leq B$. Alors, comme ci-dessus:

$$|N(\omega)| \leq e^{2B} \text{ et } |Tr(\omega)| \leq 2e^B$$

Ainsi le polynôme minimal de ω a des coefficients entiers bornés et on a le résultat souhaité.

Par conséquent, l'image de U par L est un sous-ensemble discret de D.

Pour terminer la démonstration, on a besoin de la proposition suivante:

PROPOSITION 1.5.2
Soit ω_1 une unité, $\omega_1 \neq \pm 1$, telle que $L(\omega_1)$ est un vecteur de plus petite longueur dans l'image de L.
Alors tout élément de l'image de L est un multiple entier de $L(\omega_1)$.

Démonstration

Soit $W_1 = L(\omega_1)$ et soit $W \in Im(L)$.
Alors, puisque $Im(L)$ est sur une droite, il existe $t \in \mathbb{R}$ tel que $W = tW_1$.
Soit $m \in \mathbb{Z}$ tel que $m \leq t < m + 1$ (i.e. $0 \leq t - m < 1$).
Alors

$$long(W - mW_1) = long((t - m)W_1) < long(W_1)$$

avec *long* l'application longueur de W.

De plus, comme L est un homomorphisme,

$$W - mW_1 = L(\omega) - mL(\omega_1) = L(\omega\omega_1^{-m})$$

et $\omega\omega_1^{-m} \in U$ car U est un groupe multiplicatif.
Donc $W - mW_1 \in Im(L)$ et sa longueur est plus courte que celle de W_1. Par minimalité de W_1, on a $t - m = 0$ et donc $W = mW_1$ avec $m \in \mathbb{Z}$. Ce qui conclut la démonstration de la proposition.

Par cette proposition et le fait que L est un homomorphisme, alors ω_1 engendre le groupe U, modulo ± 1.
Il reste à voir que ω_1 est unique si on l'exige > 1.

Or, on observe que $\omega_1, -\omega_1, \omega_1^{-1}, -\omega_1^{-1}$ ont tous une image de longueur $L(\omega_1)$, mais que parmi ces quatre unités, une seule est plus grande que 1. On choisit donc celle-ci et cela nous permet de conclure la démonstration.

□

Conséquence

Selon le résultat du théorème 1.5.1, si l'on est capable de déterminer une seule unité de $\mathbb{Q}(\sqrt{d})$, pour $d > 0$, on pourra alors obtenir toutes les autres, qui ne seront que des multiples de cette unité fondamentale, à multiplication par ± 1 près. Tout le travail consiste donc maintenant à exhiber cette unité fondamentale. La méthode utilisée fera appel aux fractions continues.

Chapitre 2

Fractions continues

2.1 Fraction continue d'un nombre rationnel

Soit un nombre rationnel $\frac{p}{q}$. Alors, si on effectue la division euclidienne, on obtient:

$$p = qa_0 + r_0 \quad \text{et ainsi} \quad \frac{p}{q} = a_0 + \frac{r_0}{q} = a_0 + \frac{1}{\frac{q}{r_0}}$$

avec $a_0 = \left\lfloor \frac{p}{q} \right\rfloor$ et $0 \leq r_0 < q$.

On peut poursuivre la division:

$$q = r_0 a_1 + r_1 \quad \Rightarrow \quad \frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_0}{r_1}}}$$

Et ainsi de suite, avec à chaque étape:

$$a_m = \left\lfloor \frac{r_{m-2}}{r_{m-1}} \right\rfloor \quad \text{et} \quad 1 \leq r_{m-1} < r_{m-2}$$

Par conséquent r_n est une suite strictement décroissante d'entiers positifs. Donc il existe $N \in \mathbb{N}$ tel que $r_N = 1$, si l'on suppose la fraction $\frac{p}{q}$ réduite. Par conséquent le processus s'arrête après un nombre fini ($< q$) d'itérations. On a donc obtenu ce que l'on nomme la **fraction continue de** $\frac{p}{q}$, à savoir:

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}}$$

Notation: on note la fraction continue ci-dessus:

$$\frac{p}{q} = [a_0, a_1, a_2, \ldots, a_n]$$

Remarque

Par construction de la fraction continue on observe que l'on a deux choix pour terminer la fraction. Soit on impose $a_n > 1$, comme ci-dessus, soit on termine avec une valeur de 1. En effet, on peut facilement vérifier que:

$$\frac{p}{q} = [a_0, a_1, a_2, \ldots, a_n] = [a_0, a_1, a_2, \ldots, a_n - 1, 1]$$

En temps utile, on pourra donc imposer la parité de la longueur d'une fraction continue.

2.2 Fraction continue d'un nombre irrationnel

Soit un nombre irrationnel $\alpha \in \mathbb{R}$. Alors en s'inspirant de ce qu'on a fait dans la section précédente, on peut écrire:

$$\alpha = a_0 + \frac{1}{\alpha_1}$$

avec $a_0 := \lfloor \alpha \rfloor$ et $\alpha_1 > 1$ un nombre réel irrationnel.

En effet, supposons que $\alpha_1 \in \mathbb{Q}$. Alors $\alpha = a_0 + \frac{1}{\alpha_1} \in \mathbb{Q}$ qui est une contradiction avec l'hypothèse d'irrationnalité de α.
On peut donc définir récursivement:

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n} \quad \text{avec} \quad a_n = \lfloor \alpha_{n-1} \rfloor \quad \text{et} \quad \alpha_n > 1 \quad \forall n \geq 1$$

Par récurrenc α_n est irrationnel pour tout $n \geq 1$. On a donc une suite infinie $\{\alpha_n\}$. Par conséquent, contrairement aux rationnels, on ne peut pas écrire α sous forme de fraction continue finie, car, si cela était possible, alors α serait rationnel. Selon la notation ci-dessus, on peut écrire:

$$\alpha = [a_0, a_1, a_2, \ldots, a_{n-1}, \alpha_n] = [a_0, a_1, a_2, \ldots]$$

2.3 Convergents principaux

Afin de pouvoir manipuler relativement aisément les fractions continues, on va maintenant définir un formalisme général les concernant.

On définit tout d'abord $p_n = p_n(a_0, a_1, a_2, \ldots, a_n)$ et $q_n = q_n(a_0, a_1, a_2, \ldots, a_n)$ deux nombres entiers tels que

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$$

par récurrence, on a:

$$p_0 = a_0, \quad q_0 = 1$$

$$p_n = a_0 p'_{n-1} + q'_{n-1}, \quad q_n = p'_{n-1}$$

avec $p'_k = p_k(a_1, a_2, \ldots, a_n)$, et $q'_k = q_k(a_1, a_2, \ldots, a_n)$

En effet, avec cette définition, on a bien:

$$\frac{p_n}{q_n} = \frac{a_0 p'_{n-1} + q'_{n-1}}{p'_{n-1}} = a_0 + \frac{1}{\frac{p'_{n-1}}{q'_{n-1}}} = a_0 + \frac{1}{[a_1, a_2, \ldots, a_n]}$$

qui est ce que l'on souhaitait.

DÉFINITION 2.3.1 (CONVERGENT PRINCIPAL)
Pour un nombre réel irrationnel α, on appelle n-ième convergent principal de α la fraction $\frac{p_n}{q_n}$ définie ci-dessus.

Il s'agit maintenant d'établir les propriétés et relations principales de ces convergents, avant de pouvoir les relier aux nombres algébriques et parvenir à notre objectif: trouver l'unité fondamentale des corps quadratiques réels.

2.4 Propriétés des convergents principaux

Cette section consiste essentiellement en une énumération des relations entre les convergents principaux, en utilisant uniquement les définitions récursives de p_n et q_n, pour des nombres réels quelconques a_i. Le premier sera très utile par la suite, et il interviendra très souvent dans les démonstrations à venir.

THÉORÈME 2.4.1
Avec les définitions précédentes, et avec $p_{-1} := 1$ et $q_{-1} := 0$, on a, pour $n \geq 2$

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_n = a_n q_{n-1} + q_{n-2}$$

Démonstration

La démonstration est effectuer par récurrence.
Calculons tout d'abord, les valeurs de p_n et q_n pour $n = 1$:

$$p_1 = a_0 p'_0 + q'_0 = a_0 p_0(a_1) + q_0(a_1) = a_0 a_1 + 1 \quad \text{et} \quad q_1 = p'_0 = a_1$$

Alors, pour $n = 2$:
$$\begin{aligned} p_2 &= a_0 p'_1 + q'_1 \\ &= a_0 p_1(a_1, a_2) + q_1(a_1, a_2) \\ &= a_0(a_1 a_2 + 1) + a_2 \\ &= a_2(a_0 a_1 + 1) + a_0 \\ &= a_2 p_1 + p_0 \end{aligned}$$

$$\begin{aligned} \text{et } q_2 &= p'_1 \\ &= p_1(a_1, a_2) \\ &= a_1 a_2 + 1 \\ &= a_2 q_1 + q_0 \end{aligned}$$

Par conséquent le premier pas est vérifié.
Supposons maintenant les relations vérifiées pour tout $2 \leq m \leq n-1$ et montrons qu'elles le sont aussi pour n.

$$\begin{aligned} p_n &= a_0 p'_{n-1} + q'_{n-1} \\ &= a_0 p_{n-1}(a_1, a_2, \ldots, a_n) + q_{n-1}(a_1, a_2, \ldots, a_n) \\ &= a_0(a_n p_{n-2}(a_1, \ldots, a_n) + p_{n-3}(a_1, \ldots, a_n)) + a_n q_{n-2}(\ldots) + q_{n-3}(\ldots) \\ &= a_n(a_0 p_{n-2}(a_1, \ldots, a_n) + q_{n-2}(a_1, \ldots, a_n)) + a_0 p_{n-3}(\ldots) + q_{n-3}(\ldots) \\ &= a_n(a_0 p'_{n-2} + q'_{n-2}) + a_0 p'_{n-3} + q'_{n-3} \\ &= a_n p_{n-1} + p_{n-2} \end{aligned}$$

et

$$\begin{aligned} q_n &= p'_{n-1} \\ &= p_{n-1}(a_1, a_2, \ldots, a_n) \\ &= a_n p_{n-2}(a_1, a_2, \ldots, a_n) + p_{n-3}(a_1, a_2, \ldots, a_n) \\ &= a_n q_{n-1}(a_0, a_1, \ldots, a_n) + q_{n-2}(a_0, a_1, \ldots, a_n) \\ &= a_n q_{n-1} + q_{n-2} \end{aligned}$$

On peut donc conclure.

□

COROLLAIRE 2.4.2
Soient $a_i > 0$ des nombres réels, pour $1 \leq i \leq n$.
Pour $1 \leq i \leq n$, soit $r_k := [a_k, \ldots, a_n]$.
Alors

$$[a_1, \ldots, a_n] = [a_1, \ldots, a_{k-1}, r_k] = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}}$$

Démonstration

Par construction, la première égalité est évidente et la deuxième est une conséquence directe du théorème 2.4.1.

□

COROLLAIRE 2.4.3
Soient $a_0, a_1, \ldots, a_n$ et $b_0, b_1, \ldots, b_n$ des nombres réels tels que
$a_i \geq 0$ et $b_i \geq 0$, $\forall i \geq 1$.
Supposons que a_j et b_j sont entiers pour $0 < j \leq n-1$.

Si $[a_0, \ldots, a_n] = [b_0, \ldots, b_n]$, alors $a_i = b_i$ pour tout $i \geq 0$.

Démonstration

Soit $r_1 = [a_1, \ldots, a_n]$ et soit $s_1 = [b_1, \ldots, b_n]$.

Alors $\quad r_1 = a_1 + \frac{1}{[a_1,\ldots,a_n]} \geq a_1 \geq 1.$

De même $\quad s_1 \geq 1.$

Par hypothèse : $a_0 + \frac{1}{r_1} = b_0 + \frac{1}{s_1}$.

Si $r_1 = 1$, alors

$$a_0 + \frac{1}{r_1} \quad \in \mathbb{Z} \quad \Rightarrow \quad b_0 + \frac{1}{s_1} \quad \in \mathbb{Z} \quad \Rightarrow \quad s_1 = 1$$

Ainsi, on a bien $a_0 = b_0$ et $r_1 = s_1$.

Si $r_1 > 1$,

$$a_0 + \frac{1}{r_1} \quad \notin \mathbb{Z} \quad \Rightarrow \quad b_0 + \frac{1}{s_1} \quad \notin \mathbb{Z} \quad \Rightarrow \quad s_1 > 1$$

Soit $x \in \mathbb{Z}$ tel que $x \leq [a_0, a_1, \ldots, a_n]$ maximal avec cette propriété.
Alors $a_0 = x = b_0$.
Par conséquent $a_0 = b_0$ et $r_1 = s_1$.

Par récurrence on vérifie de même que $a_i = b_i \quad \forall i \geq 0$.

□

THÉORÈME 2.4.4
Pour $n \geq 0$, on a

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n$$

Démonstration

La démonstration est encore une fois effectuée par récurrence.
Premièrement, si $n = 1$:

$$q_0 p_{-1} - p_0 q_{-1} = 1 \cdot 1 - a_0 \cdot 0 = 1 = (-1)^0$$

On suppose maintenant le théorème vrai pour tout $m \leq n-1$, et on démontre qu'il l'est aussi pour n.
Par le théorème 2.4.1:

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{cases}$$

En multipliant la première égalité par $-q_{n-1}$ et la deuxième par p_{n-1} et en les additionnant, on obtient:

$$\begin{aligned} q_n p_{n-1} - p_n q_{n-1} &= a_n(p_{n-1}q_{n-1} + q_{n-1}p_{n-1} - p_{n-2}q_{n-1} + q_{n-2}p_{n-1} \\ &= -(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) \\ &= -(-1)^{n-1} = (-1)^n \end{aligned}$$

La dernière égalité étant déduite par hypothèse de récurrence.

□

COROLLAIRE 2.4.5
Pour $n \geq 1$, on a

$$\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n-1}}$$

Démonstration: simple réécriture du théorème 2.4.4.

COROLLAIRE 2.4.6
Si $a_1, a_2, \ldots$ sont des entiers positifs, alors p_n et q_n sont premiers entre eux et $\{q_i\}$ forme une suite d'entiers strictement croissante, c'est-à-dire:

$$0 < q_1 < q_2 < \ldots$$

Démonstration

Par le théorème, il est clair que p_n et q_n sont premiers entre eux.
D'autre part, par récurrence: $q_1 = a_1 > 0$.
et $q_n = a_n q_{n-1} + q_{n-2} > a_n q_{n-1} \geq q_{n-1}$, car $a_n \geq 1$.

□

COROLLAIRE 2.4.7
On pose $\alpha = [a_0, \ldots, a_{n+2}]$. Alors

$$q_{n+1}\alpha - p_{n+1} = \frac{(-1)^{n+1}}{a_{n+2}q_{n+1} + q_n}$$

Démonstration:
Par définition de α, on a $\alpha = \frac{p_{n+2}}{q_{n+2}}$. Par conséquent:

$$\begin{aligned} q_{n+1}\alpha - p_{n+1} &= q_{n+1}\tfrac{p_{n+2}}{q_{n+2}} - p_{n+1} \\ &= q_{n+1}\left(\tfrac{p_{n+2}}{q_{n+2}} - \tfrac{p_{n+1}}{q_{n+1}}\right) \\ &= q_{n+1}\left(\tfrac{(-1)^{n+1}}{q_{n+2}q_{n+1}}\right) \\ &= \tfrac{(-1)^{n+1}}{a_{n+2}q_{n+1}+q_n} \end{aligned}$$

□

THÉORÈME 2.4.8
Pour $n \geq 1$, on a

$$q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n$$

Démonstration:

Semblable à la démonstration du théorème 2.4.4, en multipliant les égalités du théorème 2.4.1 par $-q_{n-2}$ et p_{n-2}, respectivement.

□

Les trois corollaires suivants sont des conséquences immédiates de ce théorème.

COROLLAIRE 2.4.9
Pour $n \geq 2$, on a

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}$$

COROLLAIRE 2.4.10
Si $a_1, a_2, \ldots$ sont des entiers positifs, alors la suite $\{\frac{p_n}{q_n}\}$ est
– strictement croissante pour les n pairs.
– strictement décroissante pour les n impairs.

COROLLAIRE 2.4.11
On pose $\alpha = [a_0, \ldots, a_{n+2}]$. Alors

$$q_n \alpha - p_n = \frac{(-1)^n a_{n+2}}{a_{n+2} q_{n+1} + q_n}$$

Enonçons à présent un théorème qui est plus esthétique qu'utile, mais qui permet de "s'amuser" un peu avec les fractions continues.

THÉORÈME 2.4.12
Pour $n \geq 1$, on a

$$\frac{q_n}{q_{n-1}} = [a_n, a_{n-1}, \ldots, a_1]$$

Démonstration

Encore une fois, par récurrence:, si $n = 1$, alors $\frac{q_1}{q_0} = \frac{a_1}{1} = a_1 = [a_1]$.
Supposons maintenant le théorème vérifié pour tout $m < n - 1$. En particulier, on a

$$\frac{q_{n-1}}{q_{n-2}} = [a_{n-1}, a_{n-2}, \ldots, a_1]$$

Alors:

$$\begin{aligned} \frac{q_n}{q_{n-1}} &= \frac{a_n q_{n-1} + q_{n-2}}{q_{n-1}} \\ &= a_n + \frac{1}{[a_{n-1}, a_{n-2}, \ldots, a_1]} \\ &= [a_n, a_{n-1}, \ldots, a_1] \end{aligned}$$

□

On peut maintenant appliquer toutes ces propriétés au cas particulier de la fraction continue d'un nombre réel irrationnel. Avec les notations de la section précédente, on a notamment, pour un nombre irrationnel $\alpha \in \mathbb{R}$, les deux relations suivantes:

$$\boxed{q_{n+1}\alpha - p_{n+1} = \frac{(-1)^{n+1}}{\alpha_{n+2}q_{n+1} + q_n}} \qquad (1)$$

$$\boxed{q_n\alpha - p_n = \frac{(-1)^n\alpha_{n+2}}{\alpha_{n+2}q_{n+1} + q_n}} \qquad (2)$$

Avec, par construction, $a_n < \alpha_n < a_n + 1$ et $a_n \geq 1 \; \forall \, n \geq 1$

Dans ce cas, les dénominateurs q_n sont des entiers positifs, et ils forment une suite croissante, par le corollaire 2.4.6.
A l'aide des propriétés des fractions continues, on peut démontrer d'autres propriétés relatives au cas particulier des nombres irrationnels.

THÉORÈME 2.4.13

i) Pour n pair, les n-ièmes convergents principaux de α forment une suite strictement croissante, convergeant vers α.

ii) Pour n impair, les n-ièmes convergents principaux de α forment une suite strictement décroissante, convergeant vers α.

iii) De plus, on a

$$\frac{1}{2q_{n+1}} < \frac{1}{q_{n+1} + q_n} < |q_n\alpha - p_n| < \frac{1}{q_{n+1}}$$

Démonstration

i) La croissance découle du corollaire 2.4.10.

ii) idem pour la décroissance, et la convergence des deux suites découle de la croissance de la suite $\{q_n\}$ et de la relation

$$\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n-1}}$$

iii) La première inégalité est une conséquence de la croissance des q_n. La deuxième se démontre comme suit:

$$\begin{aligned} |\alpha - \tfrac{p_n}{q_n}| &> |\tfrac{p_{n+2}}{q_{n+2}} - \tfrac{p_n}{q_n}| \\ &= \tfrac{a_{n+2}}{q_{n+2}q_n} \\ &= \tfrac{a_{n+2}}{(a_{n+2}q_{n+1}+q_n)q_n} \\ &= \tfrac{1}{(q_{n+1}+\frac{q_n}{a_{n+2}})q_n} \\ &\geq \tfrac{1}{(q_{n+1}+q_n)q_n} \end{aligned}$$

car $a_{n+2} \geq 1$.
Par conséquent $\frac{1}{q_{n+1}+q_n} < |q_n\alpha - p_n|$.

D'autre part

$$|\alpha - \frac{p_n}{q_n}| < |\frac{\frac{p_n}{q_n} - p_{n+1}}{q_{n+1}}|$$

Et donc $|q_n\alpha - p_n| < \frac{1}{q_{n+1}}$.

Ce qui conclut la démonstration.

□

2.5 Nombres équivalents

On définit $G := \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \quad a,b,c,d \in \mathbb{Z} \quad \text{et} \quad |det\sigma| = 1 \right\}$
Alors on vérifie facilement que G est un groupe.
Définissons maintenant l'action de G sur les nombres réel irrationnels par:

$$\sigma\alpha = \frac{a\alpha + b}{c\alpha + d}$$

Ceci est une action car $\sigma\alpha$ est un nombre réel irrationnel pour tout $\sigma \in G$ et tout α réel irrationnel.
En effet, si $\sigma\alpha \in \mathbb{Q}$, alors $\sigma'(\sigma\alpha) \in \mathbb{Q}$ pour tout $\sigma' \in G$, par définition de l'action.
Mais $\sigma^{-1}(\sigma\alpha) = \alpha \notin \mathbb{Q}$.
Il y a donc une contradiction, et ainsi on a bien $\sigma\alpha \notin \mathbb{Q}$.
De plus si $\sigma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, alors

$$\begin{aligned}
\sigma(\sigma'\alpha) &= \sigma\left(\tfrac{a'\alpha+b'}{c'\alpha+d'}\right) \\
&= \frac{\frac{aa'\alpha+ab'}{c'\alpha+d'}+b}{\frac{ca'\alpha+cb'}{c'\alpha+d'}+d} \\
&= \frac{(aa'+bc')\alpha+ab'+bd'}{(ca'+dc')\alpha+cb'+bd'} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \\
&= (\sigma\sigma')\alpha
\end{aligned}$$

et

$$I\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\alpha = \frac{\alpha+0}{0+1} = \alpha$$

Et, par conséquent, on a bien une action.

DÉFINITION 2.5.1 (NOMBRES ÉQUIVALENTS)
Deux nombres réels irrationnels α et β sont dits équivalents s'il existe $\sigma \in G$ telle que

$$\sigma\alpha = \beta$$

On notera $\alpha \sim \beta$.

Remarque

La relation définie ci-dessus est une relation d'équivalence, du fait qu'elle est définie à partir de l'action d'un groupe.

2.5.1 Lien avec les convergents principaux

On a vu qu'un nombre réel irrationnel α peut s'écrire comme:

$$\alpha = [a_0, \ldots, a_{n-1}, \alpha_n]$$

Alors, pour $n \geq 1$, par le corollaire 2.4.2 on a,

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$$

De plus, par le théorème 2.4.4, on a $|p_{n-1}q_{n-2} - p_{n-2}q_{n-1}| = 1$. Donc

$$\sigma_{n-1} := \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \in G$$

On appelle σ_{n-1} la **(n-1)-ième transformation continue de** α.

On obtient donc $\alpha = \sigma_{n-1}\alpha_n$ et par conséquent:

$$\alpha \sim \alpha_n \quad \forall\, n \geq 1 \qquad (\star)$$

De plus, $\sim$ étant un relation d'équivalence, tous les α_n $(n = 1, 2, \ldots)$ sont équivalents.
D'autre part, on observe que, par la relation du théorème 2.4.1, on obtient:

$$\sigma_n = \sigma_{n-1} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

avec $A_n := \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \in G$.
Donc on peut écrire, pour tout $n \geq 0$,

$$\sigma_n = A_0 A_1 \cdots A_n$$

Enonçons à présent un théorème qui sera très utile par la suite.

THÉORÈME 2.5.1
Soient α, β deux nombres réels irrationnels, et soit $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, tels que $\alpha = \sigma\beta = \frac{a\beta+b}{c\beta+d}$.
On suppose $\beta > 1$ et $c > d > 0$.

Alors $\frac{b}{d}$ et $\frac{a}{c}$ sont deux convergents principaux successifs de α.
De plus, si

$$\frac{b}{d} = \frac{p_{n-2}}{q_{n-2}} \text{ et } \frac{a}{c} = \frac{p_{n-1}}{q_{n-1}}$$

alors $\beta = \alpha_n$.

Démonstration
On observe premièrement que a et c sont premiers entre eux, de même que b et d, car $ad - bc = \pm 1$. Donc par la construction de la fraction continue d'un rationnel, on peut écrire:

$$\frac{a}{c} = [a_0, a_1, \ldots, a_{n-1}] = \frac{p_{n-1}}{q_{n-1}}$$

Et ainsi $a = p_{n-1}$ et $c = q_{n-1}$.

Par la remarque de la page 14, on peut choisir la parité de n de telle sorte que:

$$p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = \epsilon = ad - bc$$

On obtient alors

$$p_{n-1}(d - q_{n-2}) = q_{n-1}(b - p_{n-2})$$

Comme p_{n-1} et q_{n-1} sont premiers entre eux, q_{n-1} divise $(d - q_{n-2})$.
Mais $q_{n-2} < q_{n-1}$ et, par hypothèse $d < c = q_{n-1}$, donc $|d - q_{n-2}| < q_{n-1}$.
Par conséquent, $d - q_{n-2} = 0$ et donc $d = q_{n-2}$. De même $b = p_{n-2}$.
Avec ces égalités, on a

$$\alpha = \frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}$$

Par construction, ceci signifie:

$$\alpha = [a_0, \ldots, a_{n-1}, \beta]$$

Comme on a supposé $\beta > 1$, il s'ensuit que l'expression de α est l'expansion en fraction continue de α, et on a donc $\beta = \alpha_n$.

□

THÉORÈME 2.5.2 (SERRET)
Soit α, β deux nombres réels irrationnels, alors:

α, β sont équivalents $\Leftrightarrow$ $\alpha_n = \beta_m$ pour une paire d'entiers $n, m \geq 1$
$\Leftrightarrow$ dans leur fraction continue, $\alpha = [a_0, a_1, \ldots]$ et $\beta = [b_0, b_1, \ldots]$, il existe $l \in \mathbb{Z}$ tel que $a_n = b_{n+l}$ pour n suffisamment grand.

Démonstration

$\boxed{\Leftarrow}$
Supposons qu'il existe $k, l \geq 1$ tels que $\alpha_k = \beta_l$.
Par la relation $(\star)$, on a $\alpha \sim \alpha_k = \beta_l \sim \beta$. Ainsi, on a bien $\alpha \sim \beta$

$\boxed{\Rightarrow}$
Supposons $\alpha \sim \beta$, c'est-à-dire $\beta = \frac{a\alpha+b}{c\alpha+d}$, avec $ad - bc = \pm 1$.
Sans perte de généralité, on peut supposer que $c\alpha + d > 0$ (si ce n'est pas le cas il suffit de remplacer a, b, c, d par leurs opposés).

Soit σ_{n-1} comme on l'a défini précédemment, i.e. $\alpha = \sigma_{n-1}\alpha_n$.

Alors $\beta = \sigma\sigma_{n-1}\alpha_n$ et

$$\begin{aligned} \sigma\sigma_{n-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \\ &= \begin{pmatrix} ap_{n-1} + bq_{n-1} & ap_{n-2} + bq_{n-2} \\ cp_{n-1} + dq_{n-1} & cp_{n-2} + dq_{n-2} \end{pmatrix} \end{aligned}$$

Notons

$$\begin{aligned} c' &= cp_{n-1} + dq_{n-1} = q_{n-1}(c\tfrac{p_{n-1}}{q_{n-1}} + d) \\ d' &= cp_{n-2} + dq_{n-2} = q_{n-2}(c\tfrac{p_{n-2}}{q_{n-2}} + d) \end{aligned}$$

Pour n suffisamment grand, $\frac{p_{n-1}}{q_{n-1}}$ et $\frac{p_{n-2}}{q_{n-2}}$ sont proches de α, de sorte que c' et d' sont strictement positifs. De plus $\alpha_n > 1$.

D'autre part $c' > d'$.

En effet, si $c > 0$, alors on choisit n tel que $\frac{p_{n-2}}{q_{n-2}} < \alpha < \frac{p_{n-1}}{q_{n-1}}$. Donc, par la croissance et la positivité des q_k, on a:

$$c\frac{p_{n-2}}{q_{n-2}} + d < c\alpha + d < c\frac{p_{n-1}}{q_{n-1}} + d < \frac{q_{n-1}}{q_{n-2}}\left(c\frac{p_{n-1}}{q_{n-1}} + d\right)$$

Et donc $c' > d'$.

Si $c < 0$, alors on choisit n tel que $\frac{p_{n-1}}{q_{n-1}} < \alpha < \frac{p_{n-2}}{q_{n-2}}$. Donc

$$c\frac{p_{n-1}}{q_{n-1}} + d > c\alpha + d > c\frac{p_{n-2}}{q_{n-2}} + d > \frac{q_{n-2}}{q_{n-1}}\left(c\frac{p_{n-2}}{q_{n-2}} + d\right)$$

Et donc $c' > d'$.

Ainsi, on a toutes les hypothèses du théorème 2.5.1, et on peut conclure que $\alpha_n = \beta_m$ pour un certain m.

□

Chapitre 3

Fractions continues et nombres quadratiques

Dans ce chapitre nous allons établir des liens entre fractions continues et nombres quadratiques.

3.1 Discriminant et nombres réduits

On suppose toujours que d est un entier positif sans facteur carré.
Soit $\alpha = x + y\sqrt{d}$ un nombre quadratique. Alors on a vu que le polynôme unitaire sur $\mathbb{Q}$ ayant α pour racine peut s'écrire:

$$X^2 - Tr(\alpha)X + N(\alpha) = X^2 - (2x)X + (x^2 - dy^2)$$

On définit alors deux fraction $\frac{c}{a} = x^2 - dy^2$ et $\frac{b}{a} = -2x$, avec $a, b, c \in \mathbb{Z}$, sans diviseur commun et $a > 0$. Alors α sera racine du polynôme à coefficients entiers suivant:

$$aX^2 + bX + c$$

Remarque

a, b, c sont uniquement déterminés par le fait que α est racine de $aX^2+bX+c = 0$ et que $a, b, c \in \mathbb{Z}$ sont premiers entre eux et $a > 0$.

On peut alors définir:

Définition 3.1.1 (Discriminant)
Soit α un nombre quadratique et soit aX^2+bX+c son polynôme entier minimal avec $a > 0$, alors le discriminant de α est:

$$D(\alpha) = b^2 - 4ac$$

Remarque

Dans la définition ci-dessus, si $\alpha = x + y\sqrt{d}$, alors on observe que:

$$D(\alpha) = 4a^2dy^2$$

Par conséquent, si d est positif, $D(\alpha) > 0$. Ceci est cohérent avec le fait que α est un nombre quadratique réel.

DÉFINITION 3.1.2 (NOMBRES RÉDUITS)
Soit α un nombre quadratique. Alors α est réduit si $\alpha > 1$ et $-1 < \alpha' < 0$.

THÉORÈME 3.1.1
Pour un entier positif D donné, il n'y a qu'un nombre fini d'éléments réduits de $\mathbb{Q}(\sqrt{d})$ dont le discriminant est D.

Démonstration

Soit α un nombre algébrique réduit, et soient $a, b, c \in \mathbb{Z}$, sans diviseur commun, avec $a > 0$, tels que

$$a\alpha^2 + b\alpha + c = 0$$

Alors, $\alpha = \frac{-b+\epsilon\sqrt{d}}{2a} > 1$ et $-1 < \alpha' = \frac{-b-\epsilon\sqrt{d}}{2a} < 0$, avec $\epsilon = \pm 1$.

Si $\epsilon = -1$, alors $-b - \sqrt{D} > 2a > 0$
$-b + \sqrt{D} < -2a < 0$
Ceci n'est pas possible, car cela impliquerait $b < 0$ et $b > 0$. Donc $\epsilon = 1$.

Alors $-b + \sqrt{D} > 2a$
$-b - \sqrt{D} < -2a$

Ainsi $-b + \sqrt{D} > 2a > b + \sqrt{D} \quad (\star)$
et donc $-b > b$ ou $b < 0$.

De plus $\frac{-b-\sqrt{D}}{2a} < 0 \quad \Rightarrow \quad -b < \sqrt{D}$

Par conséquent $0 < -b < \sqrt{D}$ et donc $|b|$ est borné.

Par la relation $(\star)$, on a de plus $|a|$ borné. Comme $b^2 - 4ac = D$ on a encore $|c|$ borné.

Finalement, il y a donc un nombre fini d'équations quadratiques entières ayant D comme discriminant. Chaque polynôme ayant au plus deux racines, on peut donc conclure la démonstration.

□

THÉORÈME 3.1.2
Soit α un nombre réel irrationnel quadratique. Alors

(i) Dans la fraction continue $\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$, le nombre α_n a le même discriminant que α, pour tout $n \geq 1$.

(ii) Si α est réduit, alors α_n est réduit, pour tout $n \geq 1$.

(iii) Pour α non nécessairement réduit, il existe N tel que α_n est réduit pour tout $n \geq N$.

Afin de démontrer ce théorème, on a besoin du lemme suivant:

LEMME 3.1.3
Si α a un discriminant $D > 0$ et β est équivalent à α, alors β a le même discriminant D.

Démonstration du lemme
Soit $\alpha = x + y\sqrt{d}$. Alors β équivalent à α s'écrit

$$\beta = \frac{a\alpha + b}{c\alpha + d} = \frac{(ax+b)(cx+e) - acy^2 d}{(cx+e)^2 - c^2y^2d} + \frac{(a(cx+e) - c(ax+b))y}{(cx+e)^2 - c^2y^2d}\sqrt{d}$$

où $a, b, c, d \in \mathbb{Z}$ tels que $ae - bc = \pm 1$.
Alors on peut calculer la norme et la trace de β. On obtient :

$$N(\beta) = \frac{(ax+b)^2 - a^2y^2d}{(cx+e)^2 - c^2y^2d}$$

$$Tr(\beta) = 2\frac{(ax+b)(cx+e) - acy^2d}{(cx+e)^2 - c^2y^2d}$$

Alors le polynôme à coefficients entiers dont β est racine s'écrit :

$$AX^2 + BX + C$$

avec, selon les définitions usuelles:

$$A = p\left((cx+e)^2 - c^2y^2d\right)$$

$$B = p\left(2((ax+b)(cx+e) - acy^2d)\right)$$

$$C = p\left((ax+b)^2 - a^2y^2d\right)$$

où p est l'entier de plus petite valeur absolue tel que $A > 0$ et $p(2x)$, $p(x^2)$ et $p(dy^2)$ sont entiers. (Ceci suffit bien afin que A, B, C soient entiers, et minimaux avec les propriétés requises.)
Alors

$$D(\beta) = B^2 - 4AC = 4p^2y^2d\left(a(cx+e) - c(ax+b)\right)^2$$

or, $a(cx+e) - c(ax+b) = ae - bc = \pm 1$.
Donc

$$D(\beta) = 4p^2y^2d$$

On peut encore remarquer que la définition de p implique $D(\alpha) = 4p^2y^2d$.
Donc on obtient bien

$$D(\beta) = D(\alpha)$$

□

Démonstration du théorème

(i) par le lemme 3.1.3, il suffit de montrer que $\alpha_n \sim \alpha$. Or, ceci est vrai par les résultats du chapitre précédent ($\alpha = \sigma_{n-1}\alpha_n$).

(ii) Par récurrence, supposons que α_{n-1} est réduit ($\alpha_0 = \alpha$).

Alors, par construction, $\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$, avec $a_{n-1} \geq 1$ entier et $\alpha_n > 1$. Il suffit donc de vérifier que $-1 < \alpha'_n < 0$ ou de manière équivalente,

$$-\frac{1}{\alpha'_n} > 1$$

Or,

$$-\frac{1}{\alpha'_n} = (a_{n-1} - \alpha_{n-1})' = a_{n-1} - \alpha'_{n-1}$$

et $-1 < \alpha'_{n-1} < 0$ et $a_{n-1} \geq 1$, donc $a_{n-1} - \alpha'_{n-1} > 1$.

Donc α_n est réduit.

(iii) Comme pour (ii) on sait déjà que $\alpha_n > 1$, il suffit donc de montrer que $-1 < \alpha'_n < 0$.
Par la construction faite à la section 2.5.1, on a

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$$

Alors on peut développer:

$$\alpha_n(q_{n-1}\alpha - p_{n-1}) = -(q_{n-2}\alpha - p_{n-2})$$

$$\alpha'_n(q_{n-1}\alpha' - p_{n-1}) = -(q_{n-2}\alpha' - p_{n-2})$$

$$\alpha'_n = -\frac{q_{n-2}\alpha' - p_{n-2}}{q_{n-1}\alpha' - p_{n-1}}$$

$$\alpha'_n = -\frac{q_{n-2}}{q_{n-1}}\left(\frac{\alpha' - \frac{p_{n-2}}{q_{n-2}}}{\alpha' - \frac{p_{n-1}}{q_{n-1}}}\right)$$

Pour N suffisamment grand, $\frac{p_{n-2}}{q_{n-2}}$ et $\frac{p_{n-1}}{q_{n-1}}$ sont suffisamment proches de α pour que l'on ait $\alpha' - \frac{p_{n-2}}{q_{n-2}}$ de même signe que $\alpha' - \frac{p_{n-1}}{q_{n-1}}$. Par conséquent, on a

$$\alpha'_n < 0$$

D'autre part, par le résultat encadré (1) de la section 2.4, on sait que

$$q_{n-1}\alpha - p_{n-1} = \frac{(-1)^{n-1}}{\alpha_n q_{n-1} + q_{n-2}}$$

Ainsi, on obtient

$$\alpha'_n = \frac{1}{q_{n-1}} \left(\frac{(-1)^{n-1}}{q_{n-1}\alpha' - p_{n-1}} - q_{n-2} \right)$$

Ce qui implique

$$1 + \alpha'_n = \frac{1}{q_{n-1}} \left(q_{n-1} - q_{n-2} - \frac{(-1)^n}{q_{n-1}(\alpha' - \frac{p_{n-1}}{q_{n-1}})} \right)$$

Par le fait que la suite $\{q_n\}$ est croissante $q_{n-1} - q_{n-2} > 0$, et pour n suffisamment grand

$$\left| \frac{(-1)^n}{q_{n-1}(\alpha' - \frac{p_{n-1}}{q_{n-1}})} \right| \ll 1$$

car $\alpha' - \frac{p_{n-1}}{q_{n-1}} \neq 0$ pour α non rationnel.

Par conséquent $1 + \alpha'_n > 0$ et donc $-1 < \alpha'_n < 0$.

Donc α_n est réduit, pour n suffisamment grand, ce qui conclut la démonstration.

□

3.2 Périodicité

Nous allons maintenant introduire une nouvelle notion concernant les fractions continues.

DÉFINITION 3.2.1 (FRACTIONS CONTINUES PÉRIODIQUES)
Soit α un nombre réel irrationnel. On dit que sa fraction continue est périodique s'il existe k tel que pour tout n suffisamment grand, on ait $a_{n+k} = a_n$.
On dit que α est purement périodique si $a_{n+k} = a_n$ pour tout n.

On appelle k la **période primitive de** α si k est le plus petit entier avec cette propriété.

Notation
On emploiera la notation standard suivante pour une fraction continue périodique, de période k:

$$[a_0, a_1, \ldots, a_r, \overline{a_{r+1}, \ldots, a_{r+k}}]$$

comme abréviation de $[a_0, a_1, \ldots, a_r, a_{r+1}, \ldots, a_{r+k}, a_{r+1}, \ldots, a_{r+k}, \ldots]$

Donc, avec cette notation, une fraction continue est purement périodique si et seulement si on peut l'écrire comme $[\overline{a_1, \ldots, a_k}]$.

Voici un lemme qui sera utile plus tard.

LEMME 3.2.1
Soit $\alpha \in \mathbb{R}$ un nombre quadratique irrationnel réduit, et soit $a \in \mathbb{Z}$, tel que

$$\alpha = a + \frac{1}{\alpha_1}$$

Alors α_1 est réduit si et seulement si $a < \alpha < a+1$, i.e. $a = \lfloor \alpha \rfloor$.

Démonstration

$\boxed{\Rightarrow}$
Si $\alpha < a$, alors

$$\frac{1}{\alpha_1} = \alpha - a < 0 \quad \Rightarrow \quad \alpha_1 < 0 \quad \Rightarrow \quad \alpha_1 \text{ non réduit.}$$

Si $\alpha > a+1$, alors

$$\frac{1}{\alpha_1} = \alpha - a > 1 \quad \Rightarrow \quad \alpha_1 > 1 \quad \Rightarrow \quad \alpha_1 \text{ non réduit.}$$

Par conséquent, on a bien $a < \alpha < a+1$.

$\boxed{\Leftarrow}$
Si $a < \alpha < a+1$, alors $0 < \frac{1}{\alpha_1} = \alpha - a < 1$ et donc $\alpha_1 > 1$.
De plus, α réduit implique $a \geq 1$ et $\alpha' - a < -1$. Donc

$$-1 < \alpha_1 = \frac{1}{\alpha' - a} < 0$$

Ainsi, α_1 est réduit.

□

Remarque

Par ce lemme, il y a une bijection entre les deux nombres réduits α et α_1. En effet,

$$\alpha_1 = \frac{1}{\alpha - \lfloor \alpha \rfloor}$$

et, d'autre part, $-\frac{1}{\alpha_1'} = a + \frac{1}{-\frac{1}{\alpha'}}$ et $-\frac{1}{\alpha_1'}$ est réduit. Donc $a = \lfloor -\frac{1}{\alpha_1'} \rfloor$. Ainsi

$$-\frac{1}{\alpha'} = \frac{1}{-\frac{1}{\alpha_1'} - \lfloor -\frac{1}{\alpha_1'} \rfloor}$$

THÉORÈME 3.2.2 (EULER-LAGRANGE)
Soit α un nombre réel irrationnel.
La fraction continue de α est périodique si et seulement si α est quadratique.
De plus, si c'est le cas, α est réduit si et seulement si sa fraction continue est purement périodique.

Démonstration

$\boxed{\Leftarrow}$
Supposons $\alpha \in \mathbb{R}$ irrationnel quadratique.
Par le théorème 3.1.2, α_n est réduit pour tout n suffisamment grand.
Par le lemme 3.1.3, α_n a le même discriminant que α.
Par le théorème 3.1.1, il n'y a qu'un nombre fini de valeurs possibles pour un tel α_n.
Par conséquent, il existe $n, k \in \mathbb{N}$, $k > 1$ tel que $\alpha_n = \alpha_{n+k}$.
Ainsi la fraction continue est périodique.

Si α est réduit, alors, par le théorème 3.1.2, tous les α_n sont également réduits et supposons $\alpha_m = \alpha_{m+k}$.

Par le lemme 3.2.1 et la remarque ci-dessus, pour tout α_n réduit il existe un unique α_{n-1} réduit tel que

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}$$

Appliqué à notre cas, on obtient $\alpha_{m-1} = \alpha_{m+k-1}$ et $a_{m-1} = a_{m+k-1}$.

Par récurrence on obtient donc $\alpha_n = \alpha_{n+k}$ et $a_n = a_{n+k}$ pour tout n.

Par conséquent, la fraction continue de α est purement périodique.

$\boxed{\Rightarrow}$
Supposons la fraction continue de α purement périodique. Alors

$$\alpha = [\overline{a_0, a_1, \ldots, a_m}] = [a_0, a_1, \ldots, a_m, \alpha]$$

Par conséquent

$$\alpha = \sigma_m \alpha = \frac{a\alpha + b}{c\alpha + d}$$

Alors

$$c\alpha^2 + (d - a)\alpha - b = 0 \qquad \text{avec } a, b, c, d \in \mathbb{Z}$$

Ainsi, α est quadratique.

De plus, $\alpha = \alpha_n$ pour n arbitrairement grand. Or pour n suffisamment grand, α_n est réduit. Donc α est réduit.

Si la fraction est simplement périodique, alors

$$\alpha = [a_0, a_1, \ldots, a_r, \overline{a_{r+1}, \ldots, a_{r+k}}]$$

Donc

$$\alpha_{r+1} = [\overline{a_{r+1}, \ldots, a_{r+k}}]$$

Par la démonstration ci-dessus, α_{r+1} est quadratique. Par équivalence avec α_{r+1}, α est quadratique.

□

Exemple

On a déjà vu: α quadratique est réduit si et seulement si $\left(-\frac{1}{\alpha'}\right)$ l'est. Dans cette exemple nous allons préciser la relation entre les fractions continues de ces deux nombres. Soit α un nombre quadratique réduit, avec

$$\alpha = [\overline{a_0, a_1, \ldots, a_k}]$$

Alors on va montrer que

$$-\frac{1}{\alpha'} = [\overline{a_k, \ldots, a_1, a_1}]$$

On a

$$\alpha = a_0 + \frac{1}{[\overline{a_1, \ldots, a_k, a_0}]}$$

Donc

$$[\overline{a_1, \ldots, a_k, a_0}] = \frac{1}{\alpha - a_0} = a_1 + \frac{1}{[\overline{a_2, \ldots, a_k, a_0, a_1}]}$$

Et

$$[\overline{a_2, \ldots, a_k, a_0, a_1}] = \frac{1}{\frac{1}{\alpha - a_0} - a_1}$$

En répétant ce processus, on obtient finalement, après une période

$$\frac{1}{\alpha} = \frac{1}{[\overline{a_0, a_1, \ldots, a_k}]} = \cfrac{1}{\cfrac{1}{\vdots \cfrac{1}{\frac{1}{\alpha - a_0} - a_1} - a_2} - a_{k-1}} - a_k$$

Alors

$$-\frac{1}{\alpha'} = a_k + \cfrac{1}{a_{k-1} + \cfrac{1}{a_{k-2} + \cfrac{1}{\ddots + \cfrac{1}{a_0 + \cfrac{1}{-\frac{1}{\alpha'}}}}}}$$

Et par conséquent

$$-\frac{1}{\alpha'} = [a_k, \ldots, a_1, a_0, -\frac{1}{\alpha'}] = [\overline{a_k, \ldots, a_1, a_0}]$$

Chapitre 4

Fractions continues et unités

Commençons par résumer ce que nous avons obtenu jusqu'à présent.
Soit un corps quadratique réel $\mathbb{Q}(\sqrt{d})$, avec d entier, positif, sans facteur carré, alors:

(i) $\alpha \in \mathbb{Q}(\sqrt{d})$ est un entier si et seulement si on peut écrire

$$\alpha = \frac{u + v\sqrt{d}}{2} \quad \text{avec } u, v \in \mathbb{Z} \quad \text{satisfaisant } (\clubsuit)$$

(ii) $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ est une unité si et seulement si $\frac{u^2 - dv^2}{4} = \pm 1$

(iii) le groupe des unités de $\mathbb{Q}(\sqrt{d})$, modulo $\{1, -1\}$, est cyclique infini, engendré par une unique unité fondamentale > 1.

Nous allons maintenant développer une méthode qui permet d'exhiber cette unité fondamentale.

DÉFINITION 4.0.2
Le discriminant du corps $\mathbb{Q}(\sqrt{d})$ est le discriminant du nombre θ défini précédemment. On le notera D.

Avec les notations définies plus haut, on peut facilement observer que

$$D = \begin{cases} d & \text{si} \quad d \equiv 1 \mod 4 \\ 4d & \text{si} \quad d \equiv 2, 3 \mod 4 \end{cases}$$

On a alors le théorème suivant.

THÉORÈME 4.0.3
Un élément $\alpha \in \mathbb{Q}(\sqrt{d})$ est un entier algébrique si et seulement s'il peut être écrit sous la forme

$$\alpha = \frac{u + v\sqrt{D}}{2} \quad \text{avec } u, v \in \mathbb{Z} \quad \text{tels que } u \equiv Dv \mod 2$$

De plus α est une unité si et seulement si on a

$$\frac{u^2 - Dv^2}{4} = \pm 1$$

Démonstration

C'est une conséquence directe du théorème 1.2.2.

□

THÉORÈME 4.0.4
Soit $\alpha \in \mathbb{Q}(\sqrt{d})$ réduit, ayant D, le disciminant de $\mathbb{Q}(\sqrt{d})$, comme discriminant. Soit k une période de sa fraction continue. Soient v le plus grand commun diviseur de $(q_{k-1}, p_{k-1} - q_{k-2}, p_{k-2})$, et $u = p_{k-1} + q_{k-2}$.
Alors

$$\omega = \frac{u + v\sqrt{D}}{2}$$

est une unité > 1.
De plus, chaque unité > 1 est de ce type.
D'autre part $N(\omega) = (-1)^k$.

Démonstration

$\boxed{\Rightarrow}$
Par la construction de la section 2.5.1, $\alpha = \sigma_{k-1}\alpha = \frac{p_{k-1}\alpha + p_{k-2}}{q_{k-1}\alpha + q_{k-2}}$. Par conséquent

$$q_{k-1}\alpha^2 + (q_{k-2} - p_{k-1})\alpha - p_{k-2} = 0$$

D'autre part, soit $a\alpha^2 + b\alpha + c = 0$ l'équation minimale de α à coefficients entiers avec $a > 0$.

On peut donc écrire

$$q_{k-1} = av, \qquad q_{k-2} - p_{k-1} = bv, \qquad -p_{k-2} = cv$$

par définition de v. De plus $u = p_{k-1} + q_{k-2}$, donc on peut écrire

$$\begin{array}{lll} p_{k-1} = \frac{u-bv}{2} & \text{et} & q_{k-1} = av \\ p_{k-2} = -cv & \text{et} & q_{k-2} = \frac{u+bv}{2} \end{array}$$

Par le théorème 2.4.4, on a:

$$q_{k-1}p_{k-2} - p_{k-1}q_{k-2} = (-1)^{k-1}$$

En appliquant cette formule aux valeurs ci-dessus, on obtient

$$av(-cv) - \frac{u - bv}{2}\frac{u + bv}{2} = (-1)^{k-1}$$

$$-acv^2 - \frac{u^2 - b^2v^2}{4} = (-1)^{k-1}$$

$$\frac{u^2 + v^2(4ac - b^2)}{4} = (-1)^k$$

$$N(\omega) = \frac{u^2 + Dv^2}{4} = (-1)^k$$

De plus $Tr(\omega) = 2u \in \mathbb{Z}$. Donc ω est un entier algébrique avec $N(\omega) = (-1)^k$.
Par conséquent ω est bien une unité de $\mathbb{Q}(\sqrt{d})$.
D'autre part v et u sont positifs par construction, car $\alpha > 1$, donc $\omega > 1$.

$\boxed{\Leftarrow}$
Soit $\omega = \frac{u+v\sqrt{D}}{2} > 1$ une unité, avec $u, v \in \mathbb{Z}$.
Alors $u, v \geq 1$, car parmi les quatres valeurs $\pm\frac{u\pm v\sqrt{D}}{2} > 1$ une seule est >1.

Soit $\frac{p}{q}$ et $\frac{p'}{q'}$ deux fractions définies comme suit, à partir du polynôme entier minimal usuel de α ($a\alpha^2 + b\alpha + c = 0$).

$$\begin{array}{lll} p = \frac{u-bv}{2} & \text{et} & q = av \\ p' = -cv & \text{et} & q' = \frac{u+bv}{2} \end{array}$$

Alors, comme $b \equiv D \mod 2$, car $b^2 - 4ac = D$, et $u \equiv Dv \mod 2$ par le théorème précédent, on a

$$u \equiv bv \mod 2$$

Ce qui implique $p, q' \in \mathbb{Z}$, de même que p' et q.
Par définition de a, b, c, on a

$$a\alpha^2 + b\alpha + c = 0$$

Et donc

$$av\alpha^2 + bv\alpha + cv = 0$$

$$q\alpha^2 + (q' - p)\alpha + p' = 0$$

$$\alpha = \frac{p\alpha + p'}{q\alpha + q'}$$

De plus

$$pq' - qp' = \frac{u^2 - b^2v^2}{4} + acv^2 = \frac{u^2 - Dv^2}{4} = N(\omega) = \pm 1$$

Par hypothèse $\alpha \in \mathbb{Q}(\sqrt{d})$ est réduit avec discriminant D.
Alors on a vu dans la démonstration du théorème 3.1.1 que $0 < -b < \sqrt{D}$, on obtient alors:

$$q' = \frac{u + bv}{2} > \frac{u - v\sqrt{D}}{2} = \omega' = \frac{N(\omega)}{\omega} > \begin{cases} 0 & \text{si} \quad N(\omega) = 1 \\ -1 & \text{si} \quad N(\omega) = -1 \end{cases}$$

D'autre part, dans la même démonstration, on a vu que $2a - b > \sqrt{D}$. On obtient alors

$$q - q' = \frac{(2a-b)v - u}{2} > \frac{v\sqrt{D} - u}{2} = -\omega' = -\frac{N(\omega)}{\omega} > \begin{cases} -1 & \text{si} \quad N(\omega) = 1 \\ -0 & \text{si} \quad N(\omega) = -1 \end{cases}$$

On a alors deux cas à examiner:

Cas 1: $N(\omega) = -1$

Alors $q > q' \geq 0$ car ce sont des entiers.

Si $q' = 0$, alors $-p'q = -1$, donc $q > 0 \quad \Rightarrow \quad q = 1$ et $p' = 1$. Par conséquent

$$\alpha = \frac{p\alpha + 1}{\alpha} = p + \frac{1}{\alpha} \quad \Rightarrow \quad \alpha = [p, \alpha]$$

Ainsi la fraction continue de α a une période de $k = 1$.

On a bien la même situation que dans la première partie de la démonstration, avec

$$\begin{array}{lll} p_{k-1} = p_0 = p & \text{et} & q_{k-1} = q_0 = 1 = q \\ p_{k-2} = p_{-1} = 1 = p' & \text{et} & q_{k-2} = q_{-1} = 0 = q' \end{array}$$

Si $q' > 0$, on a toutes les hypothèses du théorème 2.5.1, donc $\frac{p'}{q'}$ et $\frac{p}{q}$ sont deux convergents principaux de α, disons $\frac{p_{k-2}}{q_{k-2}}$ et $\frac{p_{k-1}}{q_{k-1}}$ et $\alpha = \alpha_k$. On est donc bien dans la situation souhaitée.

Cas 2: $N(\omega) = -1$

On a alors $q' > 0$ et $q \geq q'$.

Si $q = q'$, alors $pq' - p'q = 1 \quad \Rightarrow \quad q = q' = 1$ et $p = p' + 1$. Ainsi

$$\alpha = \frac{(p'+1)\alpha + p'}{\alpha + 1} = p' + \frac{\alpha}{\alpha + 1} = p' + \frac{1}{1 + \frac{1}{\alpha}} = [p', 1, \alpha]$$

Par conséquent α est de période $k = 2$, et comme dans le cas $q' = 0$ ci-dessus, on vérifie facilement qu'on est bien dans la situation voulue.

Si $q > q'$, on applique de nouveau le théorème 2.5.1, et on peut conclure.

□

A l'aide de ce théorème, on peut maintenant déterminer l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$, à condition que l'on trouve un élément réduit dans ce corps quadratique. Le théorème suivant répond à cette attente.

THÉORÈME 4.0.5
Soit $d \neq 1$ un entier positif sans facteur carré.
Soit $\theta = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{si} \quad d \equiv 1 \mod 4 \\ \sqrt{d} & \text{si} \quad d \equiv 2,3 \mod 4 \end{cases}$

Alors $\tilde{\theta} = \frac{1}{\theta - \lfloor \theta \rfloor}$ est un élément réduit de $\mathbb{Q}(\sqrt{d})$.

Démonstration

Clairement, $\tilde{\theta} > 1$. On va montrer $-1 < \tilde{\theta}' = \frac{1}{\theta' - \lfloor \theta \rfloor} < 0$

Si $d \equiv 2,3 \mod 4$, alors $\theta = \sqrt{d}$, donc $\theta' = -\sqrt{d}$. Par conséquent

$$\theta' - \lfloor \theta \rfloor < 0$$

De plus, $\theta > 1$, donc

$$\theta' - \lfloor \theta \rfloor < -1$$

Ainsi

$$-1 < \tilde{\theta}' < 0$$

Si $d \equiv 1 \mod 4$, alors $\theta = \frac{1+\sqrt{d}}{2}$, avec $d \geq 5$. Alors

$$\theta' = \frac{1-\sqrt{d}}{2} \leq \frac{1-\sqrt{5}}{2} < -\frac{1}{2}$$

De plus

$$\lfloor \theta \rfloor \geq \lfloor \frac{1+\sqrt{5}}{2} \rfloor \geq 1$$

Alors on a bien

$$-1 < \tilde{\theta}' < 0$$

□

On peut maintenant résumer tout le travail effectué pour obtenir l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$ dans un algorithme.

4.1 Algorithme

Soit $d > 1$ un entier sans facteur carré.

Si $d \equiv 1 \mod 4$

$$\theta = \frac{1+\sqrt{d}}{2} \quad \text{et} \quad D = d$$

Sinon

$$\theta = \sqrt{d} \quad \text{et} \quad D = 4d$$

Calcul d'un élément réduit de $\mathbb{Q}(\sqrt{d})$

$$\alpha = \frac{1}{\theta - \lfloor \theta \rfloor}$$

Initialisation:

$$p_{-1} = 1 \quad q_{-1} = 0$$

$$a_0 = \lfloor \alpha \rfloor \quad \text{et} \quad \alpha_1 = \frac{1}{\alpha - a}$$

$$p_0 = a_0 \quad \text{et} \quad q_0 = 1$$

$$i = 1$$

Développement de la fraction continue jusqu'à obtenir un cycle

Tant que $\alpha_i \neq \alpha$

$$a_i = \lfloor \alpha_i \rfloor \quad \text{et} \quad \alpha_{i+1} = \frac{1}{\alpha_i - a_i}$$

$$p_i = a_i p_{i-1} + p_{i-2} \quad \text{et} \quad q_i = a_i q_{i-1} + q_{i-2}$$

$$i = i + 1$$

Calcul de l'unité fondamentale

$$v = pgcd(q_{i-1}, p_{i-1} - q_{i-2}, p_{i-2}) \quad \text{et} \quad u = p_{i-1} + q_{i-2}$$

$$\omega_1 := \frac{u + v\sqrt{D}}{2} \quad (L'unité fondamentale)$$

4.2 Equations de Pell-Fermat

L'équation dite de Pell-Fermat est l'équation:

$$x^2 - dy^2 = \pm 1$$

à résoudre en nombres entiers, pour un d positif donné. La méthode ci-dessus, valable lorsque d est sans facteur carré, donne des solutions entières si

$$d \equiv 2, 3 \mod 4$$

.
Si $d \equiv 1 \mod 4$, alors la solution peut également ne pas être entière, si

$$u \equiv v \equiv 1 \mod 2.$$

Dans ce cas, on peut toutefois vérifier que:

$$\left(\frac{u + v\sqrt{d}}{2}\right)^{3i} = x_i + y_i\sqrt{d} \quad \text{avec} \quad x_i, y_i \in \mathbb{Z} \quad \forall i$$

Par conséquent l'équation de Pell-Fermat a toujours une infinité de solutions. Par contre, il n'existe pas toujours de solution telle que

$$x^2 - dy^2 = -1$$

En effet, si l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$ est de norme positive, alors toutes les unité le seront, car

$$N(\omega^n) = (N(\omega))^n$$

Le sujet de ce travail n'étant pas l'analyse de cette équation précise, nous signalerons ici uniquement qu'il existe des cas où cette équation a une infinité de solutions, et d'autres où elle n'en a aucune. Dans le chapitre suivant nous donnerons donc la norme de l'unité fondamentale de chacun des exemples traités.

Chapitre 5

Exemples

Dans certains cas, principalement lorsque d est proche d'un carré, il est relativement facile d'obtenir explicitement l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$.

5.1 Exemple 1

Soit a un nombre impair. Alors $a^2 \equiv 1 \mod 4$, car

$$a^2 - 1 = (a+1)(a-1) \equiv 0 \mod 4.$$

Alors, soit $d = a^2 + 1 \equiv 2 \mod 4$.
On va calculer, à l'aide de l'algorithme, l'unité fondamentale de $\mathbb{Q}(\sqrt{a^2+1})$.
Comme $a^2 + 1 \equiv 2 \mod 4$, on a $\theta = \sqrt{a^2+1}$. Alors,

$$\alpha = \frac{1}{\theta - \lfloor \theta \rfloor} = \frac{1}{\sqrt{a^2+1} - a} = a + \sqrt{a^2+1}$$

On observe ainsi que:

$$\alpha = 2a + (-a + \sqrt{a^2+1}) = 2a + \frac{1}{\alpha}$$

Donc

$$\alpha = [\overline{2a}]$$

La période de la fraction continue de α est 1 et donc $v = 1$ et $u = 2a$. Ainsi

$$\boxed{\omega_1 = a + \sqrt{a^2+1}}$$

On a

$$\omega_1 \omega_1' = a^2 - (a^2+1) = -1$$

Donc, dans ce cas, l'équation $x^2 - (a^2+1)y^2 = -1$ a des solutions.

On peut appliquer cette formule à:

$$d = 2 \quad \Rightarrow \quad \omega_1 = 1 + \sqrt{2}$$

$$d = 10 \quad \Rightarrow \quad \omega_1 = 3 + \sqrt{10}$$

$$d = 26 \quad \Rightarrow \quad \omega_1 = 5 + \sqrt{26}$$

$$d = 82 \quad \Rightarrow \quad \omega_1 = 9 + \sqrt{82}$$

5.2 Exemple 2

Soit a un nombre impair. Alors, soit $d = a^2 + 2 \equiv 3 \mod 4$.
Les calculs sont semblables aux précédents, avec simplement un étage de plus dans la fraction continue. On trouve alors:

$$\alpha = [\overline{a, 2a}]$$

Par conséquent, $k = 2$ et $p_0 = a$, $q_0 = 1$, $p_1 = 2a^2 + 1$ et $q_1 = 2a$.
Alors, $v = a$ et $u = 2a^2 + 2$. Ainsi

$$\boxed{\omega_1 = (a^2 + 1) + a\sqrt{a^2 + 1}}$$

On a

$$\omega_1 \omega_1' = a^4 + 2a^2 + 1 - (a^4 + 2a^2) = 1$$

Donc, l'équation $x^2 - (a^2 + 2)y^2 = -1$ n'a pas de solution.

On peut appliquer cette formule à:

$$d = 3 \quad \Rightarrow \quad \omega_1 = 2 + \sqrt{3}$$

$$d = 11 \quad \Rightarrow \quad \omega_1 = 10 + 3\sqrt{11}$$

$$d = 51 \quad \Rightarrow \quad \omega_1 = 50 + 7\sqrt{51}$$

$$d = 83 \quad \Rightarrow \quad \omega_1 = 82 + 9\sqrt{83}$$

5.3 Exemple 3

Soit $a > 1$ un nombre impair. Alors, soit $d = a^2 + 4 \equiv 1 \mod 4$.
Comme $a^2 + 1 \equiv 1 \mod 4$, on a $\theta = \frac{1+\sqrt{a^2+4}}{2}$. Alors, on a

$$\lfloor \theta \rfloor = \frac{a + 1}{2}$$

et donc

$$\alpha = \frac{2}{-a + \sqrt{a^2+4}} = \frac{a + \sqrt{a^2+4}}{2}$$

On observe ainsi que:

$$\alpha = a + \frac{-a + \sqrt{a^2+4}}{2} = a + \frac{1}{\alpha}$$

Donc

$$\alpha = [\overline{a}]$$

La période de la fraction continue de α est 1 et donc $v = 1$ et $u = a$. Ainsi

$$\boxed{\omega_1 = \frac{a + \sqrt{a^2+4}}{2}}$$

La première solution entière de l'équation est alors

$$\omega_1^3 = \frac{1}{2}((a^3 + 3a) + (a^2+1)\sqrt{a^2+4})$$

On a

$$(\omega_1 \omega_1')^3 = (-1)^3 = -1$$

Donc, l'équation $x^2 - (a^2+4)y^2 = -1$ a des solutions.

On peut appliquer cette formule à:

$$d = 13 \quad \Rightarrow \quad \omega_1 = \tfrac{3+\sqrt{13}}{2} \quad \text{et} \quad \omega_1^3 = 18 + 5\sqrt{13}$$

$$d = 29 \quad \Rightarrow \quad \omega_1 = \tfrac{5+\sqrt{29}}{2} \quad \text{et} \quad \omega_1^3 = 70 + 13\sqrt{29}$$

$$d = 53 \quad \Rightarrow \quad \omega_1 = \tfrac{7+\sqrt{53}}{2} \quad \text{et} \quad \omega_1^3 = 182 + 25\sqrt{53}$$

5.4 Exemple 4

Soit $k \geq 1$ un nombre entier. Alors, soit $d = (2k)^2 + 1 \equiv 1 \mod 4$.
Comme $(2k)^2 + 1 \equiv 1 \mod 4$, on a $\theta = \frac{1+\sqrt{(2k)^2+1}}{2}$. Alors, on a

$$\lfloor \theta \rfloor = k$$

et donc

$$\alpha = \frac{2}{-(2k-1) + \sqrt{(2k)^2+1}} = \frac{(2k-1) + \sqrt{(2k)^2+1}}{2k}$$

On observe ainsi que:

$$\alpha = 1 + \frac{-1 + \sqrt{(2k)^2+1}}{2k} = 1 + \frac{1}{\frac{1+\sqrt{(2k)^2+1}}{2k}} = \frac{1}{\alpha_1}$$

Et on poursuit, si $k \neq 1$, alors $\alpha_1 \neq \alpha$.
(Dans le cas contraire, si $d = 5$, alors $\alpha = [\overline{1}]$.)

$$\alpha_1 = 1 + \frac{-(2k-1) + \sqrt{(2k)^2+1}}{2k} = 1 + \frac{1}{\frac{(2k-1)+\sqrt{(2k)^2+1}}{2}} = \frac{1}{\alpha_2}$$

Ensuite

$$\alpha_2 = (2k-1) + \frac{-(2k-1) + \sqrt{(2k)^2+1}}{2} = (2k-1) + \frac{1}{\alpha}$$

Donc

$$\alpha = [\overline{1, 1, 2k-1}]$$

La période de la fraction continue de α est 3 et donc on peut voir que $v = 2$ et $u = 4k$. Ainsi

$$\boxed{\omega_1 = 2k + \sqrt{(2k)^2+1}}$$

On a donc directement une solution entière, si $k \neq 1$. De plus

$$\omega_1 \omega_1' = -1$$

Donc, l'équation $x^2 - ((2k)^2+1)y^2 = -1$ a des solutions.
Si $d = 5$, alors

$$\boxed{\omega_1 = \frac{1+\sqrt{5}}{2}} \quad \text{(le nombre d'or)}$$

$$\omega_1^3 = 2 + \sqrt{5}$$

$$(\omega_1 \omega_1')^3 = (-1)^3 = -1$$

Donc, l'équation $x^2 - 5y^2 = -1$ a des solutions.

On peut appliquer cette formule à:

$$d = 17 \quad \Rightarrow \quad \omega_1 = 4 + \sqrt{17}$$

$$d = 37 \quad \Rightarrow \quad \omega_1 = 6 + \sqrt{37}$$

$$d = 65 \quad \Rightarrow \quad \omega_1 = 8 + \sqrt{65}$$

$$d = 101 \quad \Rightarrow \quad \omega_1 = 10 + \sqrt{101}$$

5.5 Exemple 5

Soit $k \geq 1$ un nombre entier. Alors, soit $d = (2k)^2 - 1 \equiv 3 \mod 4$.
Les calculs sont semblables aux précédents. On trouve alors:

$$\alpha = [\overline{1, 2(2k-1)}]$$

Par conséquent, $k = 2$ et $p_0 = 1$, $q_0 = 1$, $p_1 = 2(2k) - 1 + 1$ et $q_1 = 2(2k - 1)$. Alors, $v = 1$ et $u = 2(2k)$. Ainsi

$$\boxed{\omega_1 = 2k + \sqrt{(2k)^2 + 1}}$$

On a

$$\omega_1 \omega_1' = 1$$

Donc, l'équation $x^2 - (a^2 + 2)y^2 = -1$ n'a pas de solution.

On peut appliquer cette formule à:

$$d = 3 \quad \Rightarrow \quad \omega_1 = 2 + \sqrt{3}$$

$$d = 15 \quad \Rightarrow \quad \omega_1 = 4 + \sqrt{15}$$

$$d = 35 \quad \Rightarrow \quad \omega_1 = 6 + 7\sqrt{35}$$

$$d = 143 \quad \Rightarrow \quad \omega_1 = 12 + \sqrt{143}$$

On remarque que le cas $d = 3$ est cohérent avec celui de l'exemple 2.

5.6 Conclusion

Par ces exemples, on se rend compte que la méthode employée est très efficace, même pour des valeurs relativement élevées. Evidemment, on ne peut pas trouver si facilement des solutions explicites aussi générales pour tous les nombres sans facteur carré. Toutefois il est relativement aisé d'implémenter l'algorithme décrit dans la section précédente, qui est très efficace.

Bibliographie

[1] Serge Lang, *Introduction to Diophantine approximations*, Addison-Wesley, 1966.

[2] Pierre Samuel, *Théorie algébrique des nombres*, Paris Hermann ,1967.