RÉSOLUTION DE L'ÉQUATION DIOPHANTINNE DU SECOND DEGRÉ

Présentation par Jean-Pierre FRIEDELMEYER

Dans l'article qui suit, Éric KERN nous propose un algorithme original de résolution de l'équation dite de Pell-Fermat :

$$(x, y) \in \mathbb{Z}^2 \quad ; \quad x^2 - Dy^2 = \mp 1 \quad (D \in \mathbb{N}^*, \text{ non carré}),$$

et plus généralement de l'équation diophantienne du second degré :

$$Ax^2 + Bxy + Cy^2 = R \quad ; \quad A, B, C, R, \text{ entiers.}$$

Cet algorithme reprend en fait un article déjà ancien, publié en 1852 par Scheffler dans le journal de Crelle (*), mais il est considérablement perfectionné et modernisé.

L'attribution de l'équation $x^2 - Dy^2 = +1$ à John Pell (1611-1685) est erronée. Elle est probablement la conséquence d'une confusion due à Euler. C'est Fermat qui le premier a indiqué (en 1657) qu'une telle équation avait une infinité de solutions et affirmé être en possession d'une démonstration par descente infinie, soumettant le problème aux anglais Lord Brounker et Wallis. Mais son origine est beaucoup plus ancienne; il faut la chercher dans la détermination d'approximations rationnelles de $\sqrt{D}$ lorsque D n'est pas un carré parfait. Par exemple Boudhâyana, l'auteur hindou du plus vieux Sulba-Sutra (**), connu donne $\frac{17}{12}$ et $\frac{577}{408}$ comme approximations de $\sqrt{2}$, fractions dont les termes vérifient $17^2 - 2 \times 12^2 = 1$ et $577^2 - 2 \times 408^2 = 1$.

De façon plus générale, la recherche de x et y vérifiant $x^2 - Dy^2 = 1$ équivaut à la recherche d'un rationnel qui approxime $\sqrt{D}$ car alors on a : $\left(\frac{x}{y}\right)^2 = D + \frac{1}{y^2}$, de sorte que plus y est grand mieux $\sqrt{D}$ est approché par $\frac{x}{y}$.

Fermat et ses successeurs avaient compris qu'il y avait un lien entre le développement en fraction continue de $\sqrt{D}$ et les solutions de l'équation de Pell-Fermat.

Rappelons que si $(a_i)_{i \in \mathbb{N}}$ est une suite d'entiers naturels non nuls, la notation

---

© L'OUVERT 89 (1997)

(*) Methodus nova aequationem indeterminatam secundi gradus ... Journal de Crelle Tome XLV cahier 4, p. 349 à 369.

(**) Sulba-Sutra : textes sacrés décrivant les règles de constructions des temples et des autels. Ils sont datés environ de l'époque de Pythagore

$[a_0, a_1, a_2, \dots, a_n]$ désigne la fraction

$$r_n = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_{n-2} + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}}}$$

et avec la convention :

$$\begin{aligned} p_{(-1)} &= 1 & ; & & q_{(-1)} &= 0; \\ p_0 &= a_0 & ; & & q_0 &= 1 \end{aligned}$$

on a :

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

et alors la fraction $r_n = \frac{p_n}{q_n}$ est irréductible; $r_{n+1} - r_n = \frac{(-1)^n}{q_n q_{n+1}}$ et la suite $(r_n)_{n \in \mathbb{N}}$ converge vers un irrationnel positif.

Réciproquement, pour tout $x \in \mathbb{R} - \mathbb{Q}$ il existe une suite unique $(a_i)_{i \in \mathbb{N}}$ d'entiers naturels non nuls a_i telle que $r_n = [a_0, a_1, \dots, a_n]$ converge vers x . La fraction r_n s'appelle la réduite d'ordre n de x et a_n le $n^{\text{ième}}$ quotient partiel. Ce vocabulaire s'explique par le fait que a_n et r_n sont obtenus de la manière suivante. On décompose x en

$$x = [x] + \frac{1}{\partial x} \text{ où } \partial x = \frac{1}{x - [x]}$$

et on itère l'opération ∂x qui donne à chaque fois un nombre supérieur à 1, dont la partie entière n'est jamais nulle.

Exemple : $x = \sqrt{41}$; $\partial x = \frac{1}{\sqrt{41}-6} = \frac{1}{5}(\sqrt{41}+6) = 2 + \frac{\sqrt{41}-4}{5} = x_1$ donc $x = [x] + \frac{1}{x_1}$ avec $[x_1] = 2$. Soit $x_2 = \partial x_1 = \frac{5}{\sqrt{41}-4} = \frac{\sqrt{41}+4}{5} = 2 + \frac{\sqrt{41}-6}{5}$ donc

$$x = [x] + \frac{1}{[x_1] + \frac{1}{[x_2] + \frac{\sqrt{41}-6}{5}}}$$

Soit $x_3 = \partial x_2 = \frac{5}{\sqrt{41}-6} = \sqrt{41} + 6 = 12 + (\sqrt{41} - 6)$ et l'on constate que l'on est revenu au point de départ puisque

$$\partial x_3 = \frac{1}{x_3 - [x_3]} = \frac{1}{\sqrt{41} - 6} = x_1$$

Ainsi, dans ce cas particulier le développement est périodique et on écrit $\sqrt{41} = [6, 2, 2, 12, 2, 2, 12, \dots]$ ou plus simplement $[6, \overline{2, 2, 12}]$.

Lagrange fournira les premiers résultats précis et démontrés (*) sur le développement en fraction continue de $\sqrt{D}$, en relation avec l'équation $x^2 - Dy^2 = 1$.

Ces résultats peuvent se résumer ainsi :

1) Le développement en fraction continue d'un réel est périodique si et seulement si ce réel est quadratique, c'est à dire de la forme $a + b\sqrt{r}$ (a, b, r rationnels, $\sqrt{r}$ non rationnel).

2) Soit s la période du développement en fraction continue de $\sqrt{D}$ et $r_n = \frac{p_n}{q_n}$ ($n \geq 1$) les réduites; alors les solutions de $x^2 - Dy^2 = 1$ sont

$$\begin{cases} x = p_{ns-1}; y = q_{ns-1}, n \geq 1 & \text{si } s \text{ est pair} \\ x = p_{2ns-1}; y = q_{2ns-1}, n \geq 1 & \text{si } s \text{ est impair} \end{cases}$$

Par exemple : pour $x^2 - 41y^2 = 1$, $s = 3$. Et la "plus petite solution" est $x_0 = p_5$; $y_0 = q_5$ avec $\frac{p_5}{q_5} = [6, 2, 2, 12, 2, 2] = \frac{2049}{320}$ soit $x_0 = 2049$, $y_0 = 320$.

Dès que l'on connaît "la plus petite solution" (x_0, y_0) , les autres sont obtenues par les formules de récurrence

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_0 & Dy_0 \\ y_0 & x_0 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = T \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

Le déterminant de T vaut 1, d'où l'importance du groupe unimodulaire $GL(2, \mathbb{Z})$, des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = \mp 1$, $(a, b, c, d) \in \mathbb{Z}^4$) dans le traitement de ce problème.

Aujourd'hui la résolution de l'équation diophantienne du second degré est traitée au moyen de la théorie des modules ce qui représente un investissement assez lourd (**). L'avantage de l'article d'Eric Kern ci-dessous est qu'il ne nécessite que peu de connaissances théoriques, et se programme aisément avec un logiciel du type MAPLE.

Dans une première partie il met en place les éléments théoriques utilisés et classe les irrationnels au moyen d'une relation d'équivalence traduisant le fait que leur développement en fraction continue est identique à partir d'un certain rang, dans le cas réel. Une relation similaire est définie dans le cas des irrationnels complexes. Dans le prochain numéro il donnera les principes de résolution des équations $Ax^2 + Bxy + Cy^2 = R$ dans le cas d'un discriminant négatif, et dans une troisième partie le cas du discriminant positif.

(*) Lagrange : Solution d'un problème d'arithmétique, "Miscellanea Taurinensia 1766-1769. Oeuvres, tome I, Gauthier-Villars 1867 pp. 671-718

(**) Cf. par exemple Alain Faisant : L'équation diophantienne du second degré, Hermann Paris 1991

I. GÉNÉRALITÉ SUR LES NOMBRES QUADRATIQUES

Éric KERN

A. Nombres quadratiques

Rappelons que $z \in \mathbb{C} - \mathbb{Q}$ est appelé **nombre quadratique** si z est racine d'un (unique) polynôme unitaire du second degré à coefficients rationnels.

Il existe alors aussi un polynôme $P(t)$ à coefficients entiers tel que $P(z) = 0$. Ce polynôme n'étant pas unique, nous allons introduire un certain nombre de notions qui permettront d'établir une bijection (canonique) entre les nombres quadratiques et certains de ces polynômes.

Si D est un réel négatif, on posera

$$\sqrt{D} = i\sqrt{|D|}.$$

Soit $P(t) = At^2 + Bt + C$ un polynôme de degré 2 à coefficients dans $\mathbb{Z}$. Si $D = B^2 - 4AC$ est le discriminant de $P(t)$ alors

$$\frac{-B + \sqrt{D}}{2A} \quad \text{et} \quad \frac{-B - \sqrt{D}}{2A}$$

s'appellent respectivement la **première** et la **deuxième** racine de $P(t)$.

Ces deux racines (éventuellement confondues si $D = 0$) sont des nombres quadratiques si et seulement si $\sqrt{D} \notin \mathbb{N}$, et on dira alors que $P(t)$ est **irréductible**.

On dira que $P(t)$ est **primitif** si $\text{pgcd}(A, B, C) = 1$.

Il est facile de vérifier que pour tout nombre quadratique ρ , il existe un unique polynôme primitif irréductible $P(t) = At^2 + Bt + C$ à coefficients entiers tel que ρ soit la première racine de $P(t)$.

Ceci fournit la bijection annoncée entre nombres quadratiques et polynômes du second degré à coefficients entiers, irréductibles et primitifs.

On dira simplement que le nombre quadratique ρ et le polynôme $P(t)$ sont associés. Ceci permet bien sûr de parler du discriminant d'un nombre quadratique.

I. GÉNÉRALITÉ SUR LES NOMBRES QUADRATIQUES

Par exemple, $\rho = (3 - \sqrt{5})/7$ est un nombre quadratique (réel) de polynôme associé $P(t) = -49t^2 + 42t + 4$ et de discriminant $D = 980 = 4 \cdot 7^2 \cdot 5$.

Il est immédiat que, sans aucune restriction sur le polynôme à coefficients entiers $P(t) = At^2 + Bt + C$, le discriminant $D = B^2 - 4AC$ vérifie :

$$\begin{aligned} D &= 0 \pmod{4} \text{ si } B \text{ est pair,} \\ D &= 1 \pmod{4} \text{ si } B \text{ est impair.} \end{aligned}$$

Si $\rho = \alpha + \beta\sqrt{\gamma}$, avec $\alpha, \beta, \gamma \in \mathbb{Q}$, est un nombre quadratique, on désignera par $\rho^\sigma = \alpha - \beta\sqrt{\gamma}$ le conjugué de ρ .

On remarquera d'ailleurs que si $P(t)$ est le polynôme associé à ρ , alors $-P(t)$ est le polynôme associé à ρ^σ .

Ceci est en rupture avec les conventions habituelles qui imposent la condition $A > 0$ et qui du coup donnent un même polynôme pour ρ et pour ρ^σ , ce qui fait perdre la bijection entre nombres quadratiques et polynômes!

Pour la suite, une bonne partie de notre exposé reposant sur les propriétés du groupe unimodulaire

$$\text{GL}(2, \mathbb{Z}) = \{T \in M_2(\mathbb{Z}) \mid \det(T) = \pm 1\},$$

précisons en la structure.

B. Structure du groupe unimodulaire

On rappelle que :

$$\begin{aligned} \text{GL}(2, \mathbb{Z}) &= \{T \in M_2(\mathbb{Z}) \mid \det(T) = \pm 1\}, \\ \text{SL}(2, \mathbb{Z}) &= \{T \in M_2(\mathbb{Z}) \mid \det(T) = 1\}. \end{aligned}$$

Si $a \in \mathbb{Z}$, on pose:

$$T(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \in \text{GL}(2, \mathbb{Z}) \text{ et } \Delta(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$$

On a:

$$\begin{aligned} \Delta(a)\Delta(b) &= \Delta(a+b); & \Delta(a) &= T(a)T(0); & T(0)T(0) &= I \\ T(a)^{-1} &= T(0)T(-a)T(0) = T(0)\Delta(-a) \\ \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} &= T(-1)T(1)T(-1); & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} &= T(1)T(-1)T(1); \\ \begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\Delta(a); & \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\Delta(-a) \end{aligned}$$

$$-I = (T(-1)T(1))^3 = (T(1)T(-1))^3$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} T(a) = \begin{pmatrix} a\alpha + \beta & \alpha \\ a\gamma + \delta & \gamma \end{pmatrix}; \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \Delta(a) = \begin{pmatrix} \alpha & a\alpha + \beta \\ \gamma & a\gamma + \delta \end{pmatrix}$$

En particulier, si on pose :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix}, \quad \text{on a } T(a_0) \cdots T(a_n) = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

avec

$$p_k = a_k p_{k-1} + p_{k-2}, \quad q_k = a_k q_{k-1} + q_{k-2} \quad 0 \leq k \leq n$$

On reconnaît ici les formules classiques qui donnent les réduites p_n/q_n des fractions continues, généralisées ici au cas où les a_k peuvent être négatifs ou nuls.

Pour simplifier les notations, on posera aussi :

$$T(a_0) \cdots T(a_n) = T(a_0, \dots, a_n).$$

Remarque : (technique de calcul). On se sert des relations utiles suivantes :

$$T(a_0, a_1, \dots, a_r) T(b_0, b_1, \dots, b_s) = T(a_0, a_1, \dots, a_r, b_0, b_1, \dots, b_s)$$

$$T(a_0, a_1, \dots, a_r)^{-1} = T(0, -a_r, \dots, -a_1, -a_0, 0)$$

Ceci évite en général de multiplier entre eux deux grands nombres!

A titre d'exercice on pourra par exemple calculer

$$G = T(11, 12, 11, 13) T(13, 15, 11, 12, 11)^{-1}$$

Quel est (sans calculs) son déterminant ?

Réponse :

$$G = \begin{pmatrix} -5938883 & 77599038 \\ -535868 & 7001795 \end{pmatrix}$$

Théorème de structure :

Tout $T \in \text{GL}(2, \mathbb{Z})$ est produit d'un nombre fini (non nul) d'éléments de la forme $T(a)$ avec $a \in \mathbb{Z}$. En outre si $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\gamma \neq 0$, T s'écrit de façon unique sous la forme

$$(*) \quad T = \epsilon \cdot T(a_0, \dots, a_n) \Delta(a)$$

avec $\epsilon = \pm 1, a \in \mathbb{Z}, a_k \in \mathbb{Z}, a_k \geq 1$ si $1 \leq k \leq n$.

I. GÉNÉRALITÉ SUR LES NOMBRES QUADRATIQUES

Si $\gamma = 0$, on a $\alpha\delta = \pm 1, \delta = \pm 1$ et on a donc soit $T = \epsilon \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \epsilon\Delta(a)$, soit $T = \epsilon \begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}$ avec $\epsilon = \pm 1$. Les relations ci-dessus montrent que T est produit d'un nombre fini non nul d'éléments de la forme $T(a)$ avec $a \in \mathbb{Z}$.

Supposons désormais $\gamma \neq 0$. Si T vérifie (*), on a $\epsilon = \text{sgn}(\gamma)$ d'où l'unicité de ϵ . Quitte à multiplier T par $\epsilon = \text{sgn}(\gamma)$, on peut désormais supposer $\gamma > 0$.

Supposons d'abord que T vérifie (*) avec $\epsilon = 1$. Posons $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = T(a_0, \dots, a_n)$.

On a donc $T = \begin{pmatrix} p_n & ap_n + p_{n-1} \\ q_n & aq_n + q_{n-1} \end{pmatrix}$ et par suite

$$\alpha = p_n, \gamma = q_n \text{ et on a } \alpha/\gamma = p_n/q_n = [a_0, \dots, a_n].$$

Or on sait que l'on peut écrire de façon unique (fractions continues)

$$\alpha/\gamma = [b_0, \dots, b_m] \text{ avec } b_k \in \mathbb{Z}, b_k \geq 1 \text{ si } 1 \leq k < m, b_m \geq 2 \text{ si } m \geq 1.$$

On a donc

$$(a_0, \dots, a_n) = (b_0, \dots, b_m) \text{ si } (-1)^{m+1} = \det(T) = (-1)^{n+1}$$

et

$$(a_0, \dots, a_n) = (b_0, \dots, b_m - 1, 1) \text{ si } (-1)^{m+1} = -\det(T)$$

d'où l'unicité des $a_0, \dots, a_n$, donc aussi de (*).

Réciproquement, si on définit les $a_0, \dots, a_n$ de la manière ci-dessus et si on pose $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = T(a_0, \dots, a_n)$, on a $\alpha = p_n, \gamma = q_n$ et $\begin{vmatrix} \alpha & p_{n-1} \\ \gamma & q_{n-1} \end{vmatrix} = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$ et donc aussi $\begin{vmatrix} \alpha & \beta - p_{n-1} \\ \gamma & \delta - q_{n-1} \end{vmatrix} = 0$; par suite, il existe $\lambda \in \mathbb{Q}$ tel que

$$\beta - p_{n-1} = \lambda\alpha, \delta - q_{n-1} = \lambda\gamma.$$

Posons $\lambda = a/s$ avec $s \geq 1$ et $\text{pgcd}(a, s) = 1$. On a $a\alpha/s \in \mathbb{Z}, a\gamma/s \in \mathbb{Z}$ donc $s \mid \alpha$ et $s \mid \gamma$ et par suite $s = 1$ puisque $\text{pgcd}(\alpha, \gamma) = 1$. On a donc bien ici $T = T(a_0, \dots, a_n)\Delta(a)$. $\square$

C. Sur l'équivalence des irrationnels

Le groupe $\text{GL}(2, \mathbb{Z})$ opère à gauche sur $\mathbb{C} - \mathbb{Q}$ par :

$$G \cdot z = \frac{\alpha z + \beta}{\gamma z + \delta} \quad \text{si } G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{GL}(2, \mathbb{Z})$$

En particulier on a :

$$T(a) \cdot z = a + \frac{1}{z}, \quad \Delta(a) \cdot z = a + z$$

Cette opération ainsi que la restriction de l'opération à $SL(2, \mathbb{Z})$ définissent donc de façon naturelle deux relations d'équivalences sur $\mathbb{C} - \mathbb{Q}$, les classes d'équivalences (pour chacune des opérations) étant les orbites.

Lorsqu'on considèrera l'opération avec $SL(2, \mathbb{Z})$ on parlera d'**équivalence stricte**.

Quand un groupe opère sur un ensemble, une des notions importantes est l'étude du stabilisateur d'un élément. Ceci est l'objet du résultat :

Théorème : Soient $\rho \in \mathbb{C} - \mathbb{Q}$ et $G \in GL(2, \mathbb{Z})$. Alors :

- 1) Si ρ n'est pas un nombre quadratique on a $G \cdot \rho = \rho$ si et seulement si $G = \pm I$.
- 2) Si ρ est un nombre quadratique, $P(t) = At^2 + Bt + C$ le polynôme associé, $D = B^2 - 4AC$ son discriminant, alors pour que $G \cdot \rho = \rho$, il faut et il suffit que G soit de la forme

$$G = G(t, u) = \begin{pmatrix} \frac{1}{2}(t - Bu) & -Cu \\ Au & \frac{1}{2}(t + Bu) \end{pmatrix}$$

où $t, u \in \mathbb{Z}$ vérifient l'équation de Pell-Fermat :

$$t^2 - Du^2 = 4\epsilon$$

avec $\epsilon = \pm 1$. On a d'ailleurs $\epsilon = \det(G)$.

On remarquera enfin que, en posant $\alpha = \frac{1}{2}(t - Bu)$, $\gamma = Au$, on a $\alpha - \gamma\rho^\sigma = \frac{1}{2}(t + u\sqrt{D})$, de sorte que l'équation $t^2 - Du^2 = 4\epsilon$ s'écrit aussi :

$$N(\alpha - \gamma\rho^\sigma) = (\alpha - \gamma\rho)(\alpha - \gamma\rho^\sigma) = \epsilon$$

Posons $G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. L'équation $G \cdot \rho = \rho$ s'écrit aussi $\gamma\rho^2 + (\delta - \alpha)\rho - \beta = 0$, donc si ρ n'est pas un nombre quadratique ceci signifie que l'on a $\gamma = \delta - \alpha = \beta = 0$ et $\det(G) = \epsilon$ s'écrit alors $\alpha^2 = \epsilon$ i.e. $\alpha = \pm 1$ (on a $\alpha \in \mathbb{Z}$), autrement dit $G = \pm I$. Si ρ est un nombre quadratique cette équation signifie qu'il existe un $u \in \mathbb{Z}$ t.q.

$$\gamma = Au, \quad \delta - \alpha = Bu, \quad -\beta = Cu$$

Si on pose $t = \alpha + \delta \in \mathbb{Z}$ on a bien : $\alpha = \frac{1}{2}(t - Bu)$, $\beta = -Cu$, $\gamma = Au$, $\delta = \frac{1}{2}(t + Bu)$ et en écrivant que $\det(G) = \epsilon = \pm 1$ on obtient $t^2 - Du^2 = 4\epsilon$.

Réciproquement, si $t^2 - Du^2 = 4\epsilon$, on vérifie aisément en distinguant deux cas suivant la parité de D i.e. la parité de B , que $\frac{1}{2}(t - Bu) \in \mathbb{Z}$ et $\frac{1}{2}(t + Bu) \in \mathbb{Z}$ et en posant $G = \begin{pmatrix} \frac{1}{2}(t - Bu) & -Cu \\ Au & \frac{1}{2}(t + Bu) \end{pmatrix}$ il est alors trivial de vérifier que

I. GÉNÉRALITÉ SUR LES NOMBRES QUADRATIQUES

$G \in \text{GL}(2, \mathbb{Z})$ et que $G \cdot \rho = \rho$.

Enfin à partir de $\rho = \frac{-B+\sqrt{D}}{2A}$, un calcul simple montre que si $t, u \in \mathbb{Z}$ et si on pose $\alpha = \frac{1}{2}(t - Bu)$, $\gamma = Au$, alors $\alpha - \gamma\rho^\sigma = \frac{1}{2}(t + u\sqrt{D})$, de sorte que l'équation $t^2 - Du^2 = 4\epsilon$ s'écrit aussi $N(\alpha - \gamma\rho^\sigma) = (\alpha - \gamma\rho)(\alpha - \gamma\rho^\sigma) = \epsilon$. $\square$

Remarque : On vérifiera également que :

$$G(t_1, u_1)G(t_2, u_2) = G(t_3, u_3) \text{ avec } \frac{1}{2}(t_1 + u_1\sqrt{D})\frac{1}{2}(t_2 + u_2\sqrt{D}) = \frac{1}{2}(t_3 + u_3\sqrt{D})$$

soit :

$$t_3 = \frac{1}{2}(t_1t_2 + u_1u_2D), \quad u_3 = \frac{1}{2}(t_1u_2 + t_2u_1)$$

En particulier, si $G = G(t, u)$ et $n \in \mathbb{Z}$, on a $G^n = G(t_n, u_n)$, avec

$$\frac{1}{2}(t_n + u_n\sqrt{D}) = \left(\frac{1}{2}(t + u\sqrt{D})\right)^n$$

Enfin si $G = G(t, u) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ et si $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = G \begin{pmatrix} x \\ y \end{pmatrix}$ on a :

$$x_1 - y_1\rho = (x - y\rho)(\alpha - \gamma\rho) = (x - y\rho)\frac{1}{2}(t - u\sqrt{D})$$

Exercice : Étudions en détail le cas le plus simple, celui des nombres quadratiques imaginaires, c'est à dire le cas $D < 0$. Soit $\mathcal{G}$ le groupe des $G \in \text{GL}(2, \mathbb{Z})$ tels que $G \cdot \rho = \rho$.

On est donc amené à résoudre $t^2 + u^2|D| = 4\epsilon$, de sorte que l'on a $\epsilon = 1$, autrement dit on a $\mathcal{G} \subset \text{SL}(2, \mathbb{Z})$.

• Si $D < -4$, les uniques solutions sont : $(t, u) = \pm(2, 0)$, ce qui correspond à $G = \pm I$.

Sinon, comme D est un discriminant, on ne peut avoir que $D = -4$ ou $D = -3$.

• Si $D = B^2 - 4AC = -4$, les uniques solutions sont : $(t, u) = \pm(2, 0)$ et $(t, u) = \pm(0, 1)$, ce qui donne $\frac{1}{2}(t + u\sqrt{D}) = \pm 1$ et $\frac{1}{2}(t + u\sqrt{D}) = \pm i$, de sorte que $\mathcal{G}$ est un groupe à 4 éléments engendré par $G = G(0, 1) = \begin{pmatrix} -B/2 & -C \\ A & B/2 \end{pmatrix}$.

• Si $D = B^2 - 4AC = -3$, les uniques solutions sont : $(t, u) = \pm(2, 0)$, $(t, u) = \pm(1, 1)$ et $(t, u) = \pm(-1, 1)$, ce qui donne $\frac{1}{2}(t + u\sqrt{D}) = \pm 1$, $\frac{1}{2}(t + u\sqrt{D}) = \pm \frac{1}{2}(1 + i\sqrt{3})$ et $\frac{1}{2}(t + u\sqrt{D}) = \pm \frac{1}{2}(-1 + i\sqrt{3})$, de sorte que $\mathcal{G}$ est un groupe à 6 éléments engendré par $G = G(1, 1) = \begin{pmatrix} (1-B)/2 & -C \\ A & (1+B)/2 \end{pmatrix}$.

D. Équivalence des complexes non réels.

On pose $\Pi_+ = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ et $\Pi_- = \{z \in \mathbb{C} \mid \Im(z) < 0\}$. On a donc $\mathbb{C} - \mathbb{R} = \Pi_+ \cup \Pi_-$ et un petit calcul montre que si $G \in \text{SL}(2, \mathbb{Z})$ et si $z \in \Pi_+$ (resp. $z \in \Pi_-$) alors on a aussi $G \cdot z \in \Pi_+$ (resp. $G \cdot z \in \Pi_-$).

Pour simplifier les définitions on posera : $\mathcal{B} = \{z \in \mathbb{C} \mid -\frac{1}{2} < \Re(z) \leq \frac{1}{2}\}$, ainsi que $\mathcal{B}_+ = \mathcal{B} \cap \Pi_+$ et $\mathcal{B}_- = \mathcal{B} \cap \Pi_-$.

On appellera domaine fondamental la partie $\mathcal{F}$ de Π_+ définie par $z \in \mathcal{F}$ ssi $\Im(z) > 0$, $|z| \geq 1$, $-1/2 < \Re(z) \leq 1/2$, avec en outre $\Re(z) \geq 0$ si $|z| = 1$. On dira qu'un $z \in \mathbb{C} - \mathbb{R}$ est **réduit** si $z \in \mathcal{F}$ ou si $\bar{z} \in \mathcal{F}$.

On définit $\partial : \mathbb{C} - \mathbb{R} \longrightarrow \mathbb{C} - \mathbb{R}$ de la manière suivante :

Si z est réduit on pose $\partial z = z$. Sinon il existe un unique $a \in \mathbb{Z}$ tel que $a - 1/z \in \mathcal{B}$ et on pose alors

$$\partial z = a - \frac{1}{z} \in \mathcal{B}$$

autrement dit on a $\partial z = G \cdot z$ avec $G = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$.

On remarquera que $\partial \bar{z} = \overline{\partial z}$.

Lemme 1:

Soit $z \in \mathcal{B}_+$ alors :

Si $\Im(z) < 1/2$ on a $\Im(\partial z) > 2\Im(z)$ et si $\Im(z) \geq 1/2$ on a $\partial z \in \mathcal{F}$.

Supposons d'abord $z \in \mathcal{B}_+$, $\Im(z) < 1/2$ et montrons que $\Im(\partial z) > 2\Im(z)$. En posant $z = x + iy$, on a $\Im(\partial z) = y/(x^2 + y^2)$. La condition $\Im(\partial z) > 2\Im(z)$ s'écrit donc aussi $y/(x^2 + y^2) > 2y$, soit $(x^2 + y^2) < 1/2$, vérifiée car $|x| \leq 1/2$ et $|y| < 1/2$.

Supposons maintenant que $z = x + iy \in \mathcal{B}_+$, $\Im(z) = y \geq 1/2$ et $z \notin \mathcal{F}$. Nous allons montrer que $\partial z \in \mathcal{F}$. Comme $z \notin \mathcal{F}$ on a $|z| \leq 1$. Si $|z| = 1$ on a $x < 0$ et $-1/z = -x + iy \in \mathcal{B}$ donc $\partial z = -x + iy$, et comme $-x > 0$, on a bien $\partial z \in \mathcal{F}$ dans ce cas. On peut donc supposer que $|z| < 1$. On a $-1/z = (-x + iy)/(x^2 + y^2)$, donc aussi $|\Re(-1/z)| = |x|/(x^2 + y^2) \leq 4|x|/(4x^2 + 1) \leq 1$ car $(2|x| - 1)^2 \geq 0$. On a donc $\partial z = a - 1/z$ avec $a = 0, 1, -1$. Si $a = 0$ on a $|\partial z| = 1/|z| > 1$ donc $\partial z \in \mathcal{F}$.

Il suffit donc de considérer le cas $a = \epsilon = \pm 1$, de sorte que $\partial z = \frac{(\epsilon x - 1) - iy}{x + iy}$. La condition $|\partial z| \geq 1$ s'écrit simplement $-2\epsilon x + 1 \geq 0$ soit $\epsilon x \leq 1/2$. Comme $z \in \mathcal{B}$ on a $\epsilon x < 1/2$, donc $|\partial z| > 1$, donc $z \in \mathcal{F}$, sauf si $\epsilon = 1$ et $x = 1/2$. Dans ce dernier cas on a $|\partial z| = 1$ et $\Re(\partial z) = (-1/4 + y^2)/(1/4 + y^2) \geq 0$, car $y \geq 1/2$, donc $\partial z \in \mathcal{F}$. $\square$

Lemme 2:

Soient z, z' deux réduits de $\mathbb{C} - \mathbb{R}$. S'il existe un $G \in \text{SL}(2, \mathbb{Z})$ tel que $z' = G \cdot z$,

I. GÉNÉRALITÉ SUR LES NOMBRES QUADRATIQUES

on a $z = z'$. Deux réduits distincts de $\mathbb{C} - \mathbb{R}$ ne peuvent donc être strictement équivalents.

Posons $G = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$ et $z = x + iy$. On peut supposer que $z, z' \in \mathcal{F}$.

Quitte à échanger z et z' on peut supposer $\Im(z') \geq \Im(z) = y \geq \sqrt{3}/2$ donc, puisque $\Im(z') = \Im(z)/|cz + d|^2$ on a $|cz + d|^2 = (cx + d)^2 + c^2y^2 \leq 1$, donc aussi $\frac{3}{4}c^2 \leq 1$ et ceci n'est possible que si $c = 0, 1, -1$.

Si $c = 0$ on a $ad = 1$ donc $a = d = \pm 1$ et quitte à remplacer G par $-G$, on peut supposer $a = d = 1$. On a alors $z' = z + b$, donc $b = 0$ et par suite $z = z'$.

Si $c = 1$ on a $(x + d)^2 + y^2 \leq 1$ donc aussi $|x + d| \leq 1/2$ (car $y^2 \geq 3/4$) et ceci n'est possible que si $d = 0, 1, -1$ (car $-1/2 < x \leq 1/2$).

- On ne peut avoir $d = 1$ car alors $x + d = x + 1 > 1/2$.
- Si $d = -1$ on a $x + d = x - 1 \leq -1/2$ de sorte que l'on a nécessairement $x = 1/2$ et on a alors aussi $y = \sqrt{3}/2$, donc $z = j + 1$ et comme $-a - b = 1$, on a aussi :

$$z' = \frac{(-b-1)(j+1)+b}{(j+1)-1} = \frac{(b+1)j^2+b}{j} = j + b(j+j^2) = j - b$$

et par suite $b = -1$ et $z' = z$.

- Si $d = 0$ on a $b = -1$ et par suite $z' = a - 1/z$. En outre on a $x^2 + y^2 \leq 1$ donc $|z| = 1$ et $x \geq 0$. On a donc aussi

$$z' = a - 1/z = a - \bar{z} = (a - x) + iy \in \mathcal{F}$$

Comme $1/2 < x \leq 1/2$ et que $-1/2 < a - x \leq 1/2$, ceci n'est possible que si $a = 0, 1$.

Si $a = 0$ on a $z' = -x + iy$ donc $|z'| = |z| = 1$ et alors $x \geq 0$ et $-x \geq 0$, donc $z = iy$ et par suite $y = 1$, donc $z = z' = i$.

Si $a = 1$, on a $x = 1/2$ donc $z' = z$ car :

$$z = 1/2 + i\sqrt{3}/2 = j + 1 = -j^2 \text{ et } z' = 1 - 1/z = 1 + 1/j^2 = 1 + j = z.$$

Si $c = -1$ on se ramène à $c = 1$ en remplaçant G par $-G$. $\square$

Théorème :

Si $z \in \mathbb{C} - \mathbb{R}$, il existe un entier $n \geq 0$ tel que $z_n = \partial^n z$ soit réduit. En outre z_n est alors l'unique réduit de $\mathbb{C} - \mathbb{R}$ strictement équivalent à z .

Le lemme 1 montre qu'il existe un entier $n \geq 0$ tel que $z_n = \partial^n z$ soit un réduit, qui est donc strictement équivalent à z . Le reste est une conséquence du lemme 2. $\square$

Remarque : le lemme 1 montre en particulier que l'algorithme donne assez rapidement un z_n réduit.

Exemple : Si

$$z = z_0 = \frac{609 + i\sqrt{3}}{62}, \quad z \notin \mathcal{B}_+$$

Éric KERN

$$z_1 = 0 - \frac{1}{z_0} = \frac{-609 + i\sqrt{3}}{5982}, |z_1| < 1$$

$$z_2 = -10 - \frac{1}{z_1} = \frac{-11 + i\sqrt{3}}{62}, |z_2| < 1$$

$$z_3 = -5 - \frac{1}{z_2} = \frac{1 + i\sqrt{3}}{2}, |z_3| = 1$$

et z_3 est réduit.

E. Équivalence des irrationnels réels.

On définit maintenant $\partial : \mathbb{R} - \mathbb{Q} \longrightarrow \mathbb{R} - \mathbb{Q}$ par $\partial x = \frac{1}{x - [x]}$, ce qui s'écrit aussi $x = [x] + 1/\partial x$, i.e. $x = T([x]) \cdot (\partial x)$ ou encore $\partial x = T([x])^{-1} \cdot x$. En outre on a $\partial x > 1$.

Si on pose $x_n = \partial^n x$, $a_n = [x_n]$, alors $x = [a_0, a_1, \dots]$ est le développement en fraction continue de x et on a $x_n = [a_n, a_{n+1}, \dots]$ et $x = T(a_0, \dots, a_{n-1}) \cdot x_n$.

Il est clair que $\partial x = \partial y$ si et seulement si $y = x + a$ avec $a \in \mathbb{Z}$.

Nous allons maintenant donner une autre caractérisation de l'équivalence des irrationnels réels, d'une importance capitale par la suite.

Définition : (Condition de Scheffler)

Soient $x, y \in \mathbb{R} - \mathbb{Q}$. Nous dirons que x et y vérifient la condition S (resp. S_- , resp. S_+) s'il existe $r \in \mathbb{N}$ et $s \in \mathbb{N}$ tels que : $\partial^r x = \partial^s y$ (resp. $\partial^r x = \partial^s y$ et $r + s$ impair, resp. $\partial^r x = \partial^s y$ et $r + s$ pair). Si $x = [a_0, a_1, \dots]$ et $y = [b_0, b_1, \dots]$ sont les développements en fractions continues de x et de y , la condition $\partial^r x = \partial^s y$ signifie que l'on a $a_{r+p} = b_{s+p}$ pour tout $p \geq 0$. On peut d'ailleurs remarquer que l'on a alors aussi $\partial^{r+t} x = \partial^{s+t} y$ pour tout entier $t \geq 0$.

On vérifie aisément que S et S_+ sont des relations d'équivalence sur $\mathbb{R} - \mathbb{Q}$. En outre si x et y vérifient S_- alors, si y et z vérifient S_- (resp. S_+), alors x et z vérifient S_+ (resp. S_-).

Lemme :

Soient $x \in \mathbb{R} - \mathbb{Q}$ et $a \in \mathbb{Z}$. Alors :

1) x et $a + x$ vérifient S_+	2) x et $-x$ vérifient S_-
3) x et $1/x$ vérifient S_-	4) x et $a + 1/x$ vérifient S_-

La condition 1) est triviale car $a + x = [a + a_0, a_1, \dots]$ et on peut prendre $s = r = 1$.

D'autre part on a :

$$-x = [-(a_0 + 1), 1, a_1 - 1, a_2, \dots] \text{ si } a_1 \neq 1, \text{ donc ici } \partial^3(-x) = \partial^2 x$$

$$-x = [-(a_0 + 1), a_2 + 1, a_3, \dots] \text{ si } a_1 = 1, \text{ donc ici } \partial^2(-x) = \partial^3 x$$

et 2) est donc vérifié. Vérifions 3). Supposons d'abord $x > 0$. On a alors :

I. GÉNÉRALITÉ SUR LES NOMBRES QUADRATIQUES

$1/x = [0, a_0, a_1, \dots]$ si $a_0 > 0$, donc ici $\partial^2(1/x) = \partial x$

$1/x = [a_1, a_2, \dots]$ si $a_0 = 0$, donc ici $\partial(1/x) = \partial^2 x$

ce qui vérifie 3) lorsque $x > 0$. Lorsque $x < 0$ la conclusion résulte de ce qui précède et de $1/x = -1/(-x)$. Enfin 4) est alors une conséquence de 1) et de 3).

Théorème : Soient $x, y \in \mathbb{R} - \mathbb{Q}$ pour que x et y vérifient la condition S (resp. S_- , resp. S_+) il faut et il suffit qu'il existe $G \in \text{GL}(2, \mathbb{Z})$ (resp. $G \in \text{GL}(2, \mathbb{Z})$ et $\det(G) = -1$, resp. $G \in \text{SL}(2, \mathbb{Z})$) tel que $y = G \cdot x$.

Tout d'abord remarquons que si $x_r = \partial^r x = \partial^s y = y_s$, on a $x = T(a_0, \dots, a_{r-1}) \cdot x_r$ et $y = T(b_0, \dots, b_{s-1}) \cdot y_s$ et par suite aussi $y = T(b_0, \dots, b_{s-1})T(a_0, \dots, a_{r-1})^{-1} \cdot x = G \cdot x$ et $\det(G) = (-1)^{(r+s)}$, la condition est donc nécessaire.

Réciproquement soit $G \in \text{GL}(2, \mathbb{Z})$ (resp. $G \in \text{GL}(2, \mathbb{Z})$ avec $\det(G) = -1$, resp. $G \in \text{SL}(2, \mathbb{Z})$ avec $y = G \cdot x$ et montrons que x et y vérifient la condition S (resp. S_- , resp. S_+).

Comme tout élément de $\text{GL}(2, \mathbb{Z})$ est produit d'éléments de la forme $T(a)$ avec $a \in \mathbb{Z}$, la réciproque est alors une conclusion immédiate de 4) du lemme précédent.

□

Remarque : nous verrons comment cette condition d'équivalence, facile à tester pour les nombres quadratiques réels, ainsi que la façon qui permet de construire des stabilisateurs non triviaux peut être considérée comme un des piliers dans le succès de la résolution de l'équation de Pell-Fermat.

Corollaire :

Soit $x \in \mathbb{R} - \mathbb{Q}$. Pour qu'il existe un $G \in \text{GL}(2, \mathbb{Z})$ avec $\det(G) = -1$ tel que $G \cdot x = x$ il faut et il suffit que le développement en fraction continue de x soit périodique à partir d'un certain rang, avec une période impaire.

En effet d'après ce qui précède la condition demandée sur x signifie qu'il existe $n \geq 0$ et $p \geq 1$ impair tel que $a_m = a_{m+p}$ si $m \geq n$ ce qui démontre le résultat.