L'équation de Pell-Fermat

Justin Carel

Last updated December 1, 2022

Dans ce document, nous étudieront l'équation de Pell-Fermat $x^2 - dy^2 = 1$, et rechercherons ses solutions entières. Nous obtiendrons tout d'abord une paramétrisation de ses solutions rationnelles grâce à une étude géométrique, puis verront une seconde paramétrisation se comportant mieux vis-à-vis de ses solutions entières, qui permettra de motiver l'introduction de l'anneau $\mathbb{Z}[\sqrt{d}]$. Les propriétés de ce dernier nous permettront de mieux comprendre l'équation de Pell-Fermat d'un point de vue plus conceptuel, puis nous nous attellerons à la résolution en tant que tel.

1 Point de vue géométrique

L'équation définit une conique, et une hyperbole en particulier. Nous allons donc étudier les coniques et donner une méthode pour en construire des paramétrisations rationnelles dans le cas où elles sont irréductibles.

Si $f(x, y) = 0$ est l'équation d'une conique $\mathcal{C}$, on cherche des applications $\phi, \psi \in k(t)$ envoyant t sur un point de $\mathcal{C}$ et étant surjective à un nombre fini de points près. Autrement dit, on veut $f(\phi, \psi) = 0$ identiquement ainsi que pour tout $(x, y) \in \mathcal{C}$ à l'exception d'un nombre fini d'entre eux on puisse trouver $t \in k$ tel que $x = \phi(t)$ et $y = \psi(t)$.

Le prochain théorème va nous donner une manière de construire des paramétrisations rationnelles de n'importe quelle conique, et en particulier de celle qui correspond à l'équation de Pell-Fermat. Cette paramétrisation aura l'avantage d'être compatible avec les sous corps (dans un sens qui sera précisé par la preuve), permettant d'obtenir les solutions rationnelles de l'équation en faisant varier t sur $\mathbb{Q}$ au lieu de $\mathbb{R}$.

Théorème 1.1. *Soit $\mathcal{C}$ une conique non-vide, irréductible sur $\bar{k}$, définie par $f(x, y) = 0$. Alors $\mathcal{C}$ est une courbe rationnelle, c'est à dire qu'elle est birationnellement équivalente à la droite affine $\mathbb{A}^1$.*

Preuve. Soit $O = (x_0, y_0)$ un point de $\mathcal{C}$, ie tel que $f(x_0, y_0) = 0$. On considère la droite de pente t passant par O: son équation est $y - y_0 = t(x - x_0)$. Tout point (x, y) dans l'intersection de cette droite et de la conique vérifie

$$g(x) := f(x, t(x - x_0) + y_0) = 0.$$

Comme $g \in k(t)[x]$ est un polynôme de degré 2 en x admettant x_0 pour racine, il possède une autre racine $\phi \in k(t)$, qui n'est pas constante par irréductibilité de f. On pose

$$\psi = t(\phi - x_0) + y_0 \in k(t).$$

Par construction, on a bien $f(\phi, \psi) = g(\phi) = 0$. De plus, (ϕ, ψ) est bien inversible: l'inverse est donné par

$$\tau = \frac{y - y_0}{x - x_0} \in k(x, y). \qquad \square$$

Si le point O est à coordonnées dans un sous corps K de $\bar{k}$ et que $f \in K[x, y]$, alors les fonctions rationnelles ϕ et ψ sont aussi dans $K[x, y]$. Il suffit donc de faire varier t sur K pour obtenir les points de la conique à coordonnées dans le sous-corps, à l'exception d'un nombre fini d'entre eux.

Pour bien saisir la puissance de cette construction, étudions deux exemples:

Exemple 1.1. Nous allons trouver tous les triplets pythagoriciens, ie toutes les solutions entières à l'équation $x^2 + y^2 = z^2$. Pour cela, le changement de variables $X = x/z$ et $Y = y/z$ associe une solution non triviale (x, y, z) à un point rationnel du cercle:

$$x^2 + y^2 = z^2 \iff \left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \iff X^2 + Y^2 = 1.$$

Ce dernier possède le point évident $(1,0)$, et la droite de pente t passant par ce point est d'équation $Y = t(X-1)$. On réécrit alors l'équation du cercle

$$0 = X^2 + Y^2 - 1 = X^2 - 1 + t^2(X-1)^2 = (1+t^2)(X-1)\left(X + \frac{1-t^2}{1+t^2}\right).$$

La paramétrisation rationnelle est donc donnée par

$$\begin{cases} X = \dfrac{t^2-1}{t^2+1} \\ Y = t(X-1) = \dfrac{2t}{t^2+1} \end{cases}$$

Si on écrit $t = u/v$ avec $\gcd(u,v) \in \mathbb{Z}$, alors

$$\begin{cases} X = \dfrac{u^2-v^2}{u^2+v^2} \\ Y = \dfrac{2uv}{u^2+v^2} \end{cases} \quad \text{d'où} \quad \begin{cases} x = k(u^2-v^2) \\ y = k(2uv) \\ z = k(u^2+v^2) \end{cases}$$

Le seul point non atteint par la paramétrisation rationnelle est $(1,0)$, qui correspond aux solutions triviales $x = z$. On remarque cependant qu'on peut obtenir ces dernières dans la formule finale en posant $v = 0$, ce qui correspond intuitivement à $t = \infty$. Il est possible de formaliser cette intuition, mais ce ne sera pas important pour l'exposé.

Exemple 1.2. Regardons à tout hasard ce que ça donne pour l'équation de Pell-Fermat: $x^2 - dy^2 = 1$. Il y a une solution particulière $(x_0, y_0) = (1,0)$. Posons $y = t(x-1)$. On obtient alors

$$0 = x^2 - dy^2 - 1 = x^2 - dt^2(x-1)^2 - 1 = (1-dt^2)(x-1)\left(x + \frac{1+dt^2}{1-dt^2}\right).$$

La paramétrisation recherchée est donc donnée par les équations suivantes:

$$\begin{cases} x = \dfrac{dt^2+1}{dt^2-1} \\ y = t(x-1) = \dfrac{2t}{dt^2-1} \end{cases}$$

On peut faire varier t sur $\mathbb{Q}$ pour obtenir les points rationnels — à l'exception de $(1,0)$ — de la conique.

Malheureusement, cette paramétrisation est relativement moche et l'utiliser risque de ne pas beaucoup simplifier la recherche de solutions *entières*. On va donc chercher une paramétrisation plus jolie en se ramenant à l'hyperbole canonique $\mathcal{H}$. Le changement de variables $X = x + y\sqrt{d}$ et $Y = x - y\sqrt{d}$ donne

$$x^2 - dy^2 = 1 \iff (x + y\sqrt{d})(x - y\sqrt{d}) = 1 \iff XY = 1.$$

On peut évidemment paramétriser $\mathcal{H}$ par $X = t$ et $Y = 1/t$, ce que l'on traduit pour $\mathcal{C}$ en

$$x = \frac{X+Y}{2} = \frac{1}{2}\left(t + \frac{1}{t}\right) \text{ et } y = \frac{X-Y}{2\sqrt{d}} = \frac{1}{2\sqrt{d}}\left(t - \frac{1}{t}\right).$$

On remarque que $\mathcal{H}$ est naturellement munie d'une structure de groupe abélien, donnée par la multiplication terme-à-terme; on peut là encore transporter cette loi sur $\mathcal{C}$. Dans $(x_3, y_3) = (x_1, y_1) * (x_2, y_2)$, on a:

$$x_3 + y_3\sqrt{d} = X_3 = X_1X_2 = \left(x_1 + y_1\sqrt{d}\right)\left(x_2 + y_2\sqrt{d}\right) = (x_1x_2 + dy_1y_2) + (y_1x_2 + x_1y_2)\sqrt{d},$$

soit $x_3 = x_1x_2 + dy_1y_2$ et $y_3 = y_1x_2 + x_1y_2$. Cette loi se comporte très bien par rapport aux solutions entières de l'équation; en effet, si (x_1, y_1) et (x_2, y_2) sont à coefficients entiers alors (x_3, y_3) l'est aussi.

2 Point de vue algébrique

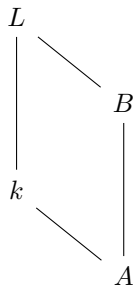
La loi de groupe introduite précédemment n'est autre que la multiplication de deux éléments de la forme $x + y\sqrt{d}$. On va donc introduire l'anneau $\mathbb{Z}[\sqrt{d}]$ qui nous permettra de parler de tels éléments, et la norme $\mathcal{N}$ sur cet anneau dont le noyau correspondra aux solutions de l'équation de Pell-Fermat.

2.1 Norme d'un élément

Définition 2.1. Pour un non-carré $d \in \mathbb{Z}$, on appelle $\mathbb{Z}[\sqrt{d}]$ l'anneau formé des polynômes en $\sqrt{d}$, ie l'anneau

$$\mathbb{Z}[\sqrt{d}] = \left\{ x + y\sqrt{d} \mid x, y \in \mathbb{Z} \right\} = \left\{ P(\sqrt{d}) \mid P \in \mathbb{Z}[X] \right\} \simeq \mathbb{Z}[X]/(X^2 - d).$$

Cette construction est analogue à celle de l'adjonction d'un élément à un corps, et ce n'est pas une surprise: en effet, $\mathbb{Z}[\sqrt{d}]$ est le sous-anneau de $\mathbb{Q}(\sqrt{d})$ constitué des éléments $x + y\sqrt{d}$ avec $x, y \in \mathbb{Z}$. Afin de bien voir la situation, il sera utile de garder en tête le schéma suivant pour la suite:



Ici A est un anneau intègre; $k = \operatorname{Frac} A$ est le corps des fractions de A; L/k est une extension finie de corps; B est entier sur A et tel que $L = \operatorname{Frac} B$. Pour se fixer les idées (et se simplifier la vie au passage), le lecteur pourra supposer que $A = \mathbb{Z}$, $k = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$, et $B = \mathbb{Z}[\sqrt{d}]$.

Définition 2.2. Pour $z \in L$, on définit la norme de z par $\mathcal{N}(z) = \det[z]$, où $[z] : L \to L$ est l'application k-linéaire induite par la multiplication par z.

Si $z = x + y\sqrt{d}$, sa matrice dans la base canonique $\mathcal{B} = (1, \sqrt{d})$ est

$$[z]_{\mathcal{B}} = \begin{bmatrix} x & dy \\ y & x \end{bmatrix},$$

d'où $\mathcal{N}(z) = x^2 - dy^2$. Comme $\mathcal{N}$ est multiplicative, on retrouve la structure de groupe évoquée géométriquement plus haut: les solutions entières de l'équation de Pell-Fermat sont données par

$$\left\{ z \in \mathbb{Z}[\sqrt{d}] \mid \mathcal{N}(z) = 1 \right\} = \ker \mathcal{N}_{\mathbb{Z}[\sqrt{d}]}.$$

Remarque 2.1. La norme est une généralisation de la notion de module d'un complexe: si $z \in \mathbb{C}$, $|z|^2 = z\bar{z} = \det[z]$, où $[z]$ est l'homothétie induite par z. Nous allons voir que l'égalité $\det[z] = z\bar{z}$ se généralise très bien à $\mathbb{Q}(\sqrt{d})$, ce qui permettra de montrer que $\ker \mathcal{N}_{\mathbb{Z}[\sqrt{d}]}$ est un sous-groupe de $\mathbb{Z}[\sqrt{d}]^\times$.

Remarque 2.2. Le théorème 90 de Hilbert — qui ne sera pas démontré — dit que si L/k est une extension Galoisienne (ie L est le corps de décomposition d'un polynôme à racines simples de $k[X]$) et que $\operatorname{Aut}(L/k)$ est cyclique de générateur σ, alors $\ker \mathcal{N} = \{\sigma(v)/v \mid v \in L\}$. Cela donne une autre manière de trouver une paramétrisation des solutions rationnelles de l'équation de Pell-Fermat. Si on effectue le calcul, on se rend compte qu'il s'agit en fait de la même paramétrisation que celle obtenue géométriquement.

Proposition 2.1 (Propriété universelle de la localisation)**.** Si $f : A \to C$ est un morphisme d'anneau envoyant tous les éléments non-nuls de A dans $C^\times$, il existe un unique morphisme $g : k \to C$ étendant f. De plus, g vérifie $g(a/b) = f(a)/f(b)$.

Preuve. Il suffit de montrer l'existence, car la formule pour g donnera automatiquement l'unicité. D'ailleurs, définissons g par $g(a/b) = f(a)/f(b)$ pour tout a, b de A. Cette fonction est bien définie: si $a/b = x/y$, alors

$$f(a)f(y) = f(ay) = f(bx) = f(b)f(x),$$

soit $g(a/b) = g(x/y)$. Il s'agit bien d'un morphisme d'anneaux:

$$g\left(\frac{a}{b} + \frac{x}{y}\right) = g\left(\frac{ay + bx}{by}\right) = \frac{f(a)f(y) + f(b)f(x)}{f(b)f(y)} = \frac{f(a)}{f(b)} + \frac{f(x)}{f(y)} = g\left(\frac{a}{b}\right) + g\left(\frac{x}{y}\right).$$

Enfin, g étend bien f. □

Corollaire 2.1. Tout automorphisme de B fixant A s'étend de manière unique en un automorphisme de L fixant k.

Preuve. Soit $\sigma : A \to A$. On peut le voir comme un morphisme de A dans k, dans lequel tous les éléments non-nuls sont inversibles. Il existe donc un unique $\tilde{\sigma} : k \to k$ étendant σ. Comme $\sigma(x)/\sigma(y) = 0$ implique $\sigma(x) = 0$, l'injectivité de σ donne celle de $\tilde{\sigma}$. La surjectivité étant aussi donnée par celle de σ, on a bien que $\tilde{\sigma}$ est un automorphisme de L fixant k. □

Exemple 2.1. Un résultat de théorie de Galois élémentaire nous dit que $\operatorname{Aut} \mathbb{Q}(\sqrt{d})$, le groupe des automorphismes de $\mathbb{Q}(\sqrt{d})$, est égal à $\{1, \tilde{\sigma}\}$ avec $\tilde{\sigma}(\sqrt{d}) = -\sqrt{d}$. Ainsi, $\mathbb{Z}[\sqrt{d}]$ possède au plus deux automorphismes. Comme de plus $\tilde{\sigma}$ envoie les éléments de $\mathbb{Z}[\sqrt{d}]$ dans $\mathbb{Z}[\sqrt{d}]$, on a

$$\operatorname{Aut} \mathbb{Z}[\sqrt{d}] = \{1, \sigma\}$$

où σ est donné par la restriction à $\mathbb{Z}[\sqrt{d}]$ de $\tilde{\sigma}$. Nous noterons désormais $\bar{z} = \sigma(z)$ pour tout z de $\mathbb{Q}(\sqrt{d})$.

Proposition 2.2. Pour tout $z \in \mathbb{Q}(\sqrt{d})$, $\mathcal{N}(z) = z\bar{z}$.

Preuve. Un simple calcul: $\mathcal{N}(x + y\sqrt{d}) = x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$. □

Remarque 2.3. Il s'agit là d'un avatar d'une propriété beaucoup plus générale, qui dit que si L/k est une extension séparable et $G = \hom_k(L, \bar{k})$ est l'ensemble des injections de L dans $\bar{k}$ fixant k, alors

$$\mathcal{N}(z) = \prod_{\sigma \in G} \sigma z, \quad \operatorname{Tr} z = \sum_{\sigma \in G} \sigma z, \quad \psi_z = \prod_{\sigma \in G} (X - \sigma z).$$

Ici $\operatorname{Tr} z$ et ψ_z représentent respectivement la trace et le polynôme caractéristique de z. Voir [Neu99, p.9] pour une preuve.

Corollaire 2.2. Soit $z \in \mathbb{Z}[\sqrt{d}]$. z est inversible (dans $\mathbb{Z}[\sqrt{d}]$) si et seulement si sa norme l'est (dans $\mathbb{Z}$).

Preuve. Si z est inversible, alors $\mathcal{N}(z)\mathcal{N}(z^{-1}) = \mathcal{N}(zz^{-1}) = 1$. Si u est l'inverse de $\mathcal{N}(z)$, alors $z\bar{z}u = \mathcal{N}(z)u = 1$. □

Remarque 2.4. Là encore, il y a une généralisation: quand L est séparable et A est algébriquement clos, un élément $a \in L$ entier sur A possède un inverse entier si et seulement si sa norme $\mathcal{N}(a)$ est inversible.

Corollaire 2.3. Les solutions entières à l'équation de Pell-Fermat forment un sous-groupe de $\mathbb{Z}[\sqrt{d}]^\times$, d'index 2 si et seulement s'il existe un élément de norme -1.

Preuve. Si $\mathcal{N}(z) = 1$ alors $z \in \mathbb{Z}[\sqrt{d}]^\times$. Ainsi, la norme définit un morphisme de groupe

$$0 \longrightarrow \ker \mathcal{N}_{\mathbb{Z}[\sqrt{d}]} \longrightarrow \mathbb{Z}[\sqrt{d}]^\times \xrightarrow{\mathcal{N}} \{\pm 1\},$$

qui est surjectif si et seulement s'il existe un élément de norme -1. Le premier théorème d'isomorphisme conclut. □

2.2 Existence d'une solution non-triviale

On en déduit qu'étudier la structure du groupe des inversibles de $\mathbb{Z}[\sqrt{d}]$ pourra révéler des informations sur celle du sous-groupe des solutions entières à l'équation de Pell-Fermat. Nous allons montrer que ce dernier possède des éléments non-triviaux, et enfin déterminer complètement sa structure. Notre stratégie pour l'existence se basera sur le principe des tiroirs, qui donnera deux éléments distincts engendrant le même idéal.

Lemme 2.1. Il existe une infinité d'éléments $\alpha \in \mathbb{Z}[\sqrt{d}]$ tels que $\alpha > 2\sqrt{d} - 1$ et $|\mathcal{N}(\alpha)| < 2\sqrt{d} + 1$.

Preuve. D'après le théorème d'approximation de Dirichlet, il existe une infinité de $p/q \in \mathbb{Q}$ vérifiant $\gcd(p, q) = 1$, $q > 0$, et

$$|q\sqrt{d} - p| < \frac{1}{q}.$$

On en déduit en particulier

$$p > q\sqrt{d} - \frac{1}{q} \geq q\sqrt{d} - q \text{ et } p < q\sqrt{d} + \frac{1}{q}.$$

On pose $\alpha = p + q\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, qui vérifie les horribles inégalités suivantes:

$$2\sqrt{d} - 1 \leq 2q\sqrt{d} - q < q\sqrt{d} + p = \alpha < 2q\sqrt{d} + \frac{1}{q} \leq 2q\sqrt{d} + q.$$

Maintenant,

$$|\mathcal{N}(\alpha)| = \left|p + q\sqrt{d}\right| \left|p - q\sqrt{d}\right| < (2q\sqrt{d} + q) \cdot \frac{1}{q} = 2\sqrt{d} + 1.$$ □

Lemme 2.2. Pour tout $0 \neq n \in \mathbb{Z}$, $\mathbb{Z}[\sqrt{d}]/(n)$ est fini de cardinal n^2.

Preuve. On a les isomorphismes de groupes abéliens suivants:

$$\frac{\mathbb{Z}[\sqrt{d}]}{n\mathbb{Z}[\sqrt{d}]} \cong \frac{\mathbb{Z} \oplus \mathbb{Z}}{n(\mathbb{Z} \oplus \mathbb{Z})} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}.$$ □

Théorème 2.1. *Pour tout $d \in \mathbb{N}$ qui n'est pas un carré, il existe une solution entière non-triviale à l'équation de Pell-Fermat $x^2 - dy^2 = 1$.*

Preuve. Soit $n \geq 2\sqrt{d} + 1$ un entier. Il existe une infinité de $\alpha \in \mathbb{Z}[\sqrt{d}]$ vérifiant $\alpha > 0$ $\mathcal{N}(\alpha) \leq n$, soit

$$\alpha \mid \alpha\bar{\alpha} = \mathcal{N}(\alpha) \mid n!.$$

En particulier, $(n!) \subseteq (\alpha)$. Mais $\mathbb{Z}[\sqrt{d}]/(n!)$ est fini, et d'après le théorème de correspondance il n'existe qu'un nombre fini d'idéaux contenant $(n!)$. On trouve donc deux éléments distincts $\alpha, \beta > 0$ pour lesquels $(\alpha) = (\beta)$, ie $\alpha = u\beta$ pour un certain inversible u. On a $\mathcal{N}(u^2) = \mathcal{N}(u)^2 = 1$. Maintenant $u^2 \neq 1$ car sinon $\alpha = \pm\beta$, et $u^2 \neq -1$. Ainsi, u^2 est une solution entière non-triviale à l'équation de Pell-Fermat. □

2.3 Structure du groupe des solutions entières

Afin de comprendre la structure de $\ker \mathcal{N}_{\mathbb{Z}[\sqrt{d}]}$, nous allons montrer qu'il existe une solution ζ minimale en un certain sens. Ce ζ engendrera la moitié des solutions, l'autre étant donnée en changeant le signe.

Lemme 2.3. Soit $\alpha = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. x et y sont strictement positifs si et seulement si $\alpha > \sqrt{|\mathcal{N}(\alpha)|}$, ie si $\alpha > |\bar{\alpha}|$.

Preuve. Soit $n = |\mathcal{N}(\alpha)| = |\alpha\bar{\alpha}|$.

$\Rightarrow$) Comme $x, y > 0$, on a $-\alpha < \bar{\alpha} < \alpha$ d'où $|\bar{\alpha}| < \alpha$ et $n = |\alpha\bar{\alpha}| < \alpha^2$.

$\Leftarrow$) Soit $\beta = |x| + |y|\sqrt{d}$. Si $\alpha \neq \beta$, alors comme $\alpha > |\bar{\alpha}| > 0$ on obtient $\bar{\alpha} = \pm\beta$ soit $\alpha > \beta$: absurde. D'où $\alpha = \beta$, et $x, y > 0$. □

Lemme 2.4. Soient $\alpha = x + y\sqrt{d}$ et $\beta = u + v\sqrt{d}$ des éléments de $\mathbb{Z}[\sqrt{d}]$ avec $x, y, u, v \geq 0$. Si $\mathcal{N}(\alpha) = \mathcal{N}(\beta)$, alors on a les équivalences suivantes:

1. $x < u$
2. $y < v$
3. $\alpha < \beta$

Preuve. On a $x^2 - dy^2 = u^2 - dv^2$, d'où $(x-u)(x+u) = d(y-v)(y+v)$.

$1 \Leftrightarrow 2$) Si $x < u$, alors $x - u < 0$ soit $y - v < 0$ d'où $y < v$. L'autre sens est donné de la même manière.

$1 \Leftrightarrow 3$) Si $x < u$ et $y < v$, alors $\alpha = x + y\sqrt{d} < u + v\sqrt{d} = \beta$. Réciproquement, si $\alpha < \beta$ on a nécessairement $x < y$ ou $u < v$, sinon $\alpha \geq \beta$. □

Théorème 2.2. *Il existe un plus petit élément supérieur strictement à 1 dans $\ker \mathcal{N}_{\mathbb{Z}[\sqrt{d}]}$, qu'on appelle solution minimale ζ de l'équation de Pell-Fermat.*

Preuve. L'ensemble des solutions strictement supérieures à 1 est non-vide. Posons donc ζ la solution ayant la plus petite coordonnée x: les deux lemmes précédent garantissent sa minimalité. □

Théorème 2.3. $\ker \mathcal{N}_{\mathbb{Z}[\sqrt{d}]} = \langle\zeta\rangle \oplus \{\pm 1\} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Preuve. Comme $\zeta > 1$, pour tout $n \geq 0$ on a $\zeta^n > 1$. En particulier, $\zeta^n = \pm 1$ est équivalent à $n = 0$. Ainsi, $\langle\zeta\rangle \cap \{\pm 1\} = 1$. Pour le caractère générateur, considérons $\alpha = x + y\sqrt{d} \in \ker \mathcal{N}_{\mathbb{Z}[\sqrt{d}]}$ et $\beta = |x| + |y|\sqrt{d}$. Comme $\zeta^n \longrightarrow +\infty$ on trouve n tel que

$$\zeta^n \leq \beta < \zeta^{n+1}, \text{ soit } 1 \leq \zeta^{-n}\beta < \zeta.$$

Par minimalité de ζ, on obtient $\zeta^{-n}\beta = 1$ d'où $\beta \in \langle\zeta\rangle$. Finalement, l'égalité $\alpha = \pm\beta^{\pm 1}$ donne $\alpha \in \langle\zeta\rangle \oplus \{\pm 1\}$. □

3 Annexe: Factorialité de $\mathbb{Z}[\sqrt{d}]$

Notre résolution de l'équation de Pell-Fermat s'est établie grâce à une étude de la structure de $\mathbb{Z}[\sqrt{d}]$. Plus généralement, la structure de l'anneau des entiers algébriques d'un corps de nombres se révèle souvent utile lors de la recherche des points entiers d'une courbe. Il est connu que l'anneau des entiers d'un corps de nombre (de degré fini) est toujours de Dedekind [Neu99]. Ces anneaux possèdent de nombreuses propriétés intéressantes; en particulier, ils sont factoriels si et seulement si ils sont principaux. Ainsi, il est important de pouvoir déterminer la factorialité des anneaux d'entiers. Nous allons montrer dans cette annexe que si d possède un facteur carré, alors $\mathbb{Z}[\sqrt{d}]$ n'est pas factoriel.

On rappelle que $a \in L$ est entier sur A s'il existe un polynôme unitaire $f \in A[X]$ ayant a pour racine.

Lemme 3.1. Soit $a \in L$. a est entier sur A si et seulement s'il existe un A-module finiment généré $M \subset L$ tel que $aM \subseteq M$.

Preuve.

$\Rightarrow$) Soit $f \in A[X]$ un polynôme unitaire annulant a. Alors $A[a] = \{g(a) \mid g \in A[X]\}$ est généré par les a^i pour $0 \leq i \leq \deg f$, et $aA[a] \subseteq A[a]$.

$\Leftarrow$ Soit M un tel module, de générateurs $(m_i)_{1 \leq i \leq n}$. Alors $[a] : m \to am$ est un endomorphisme de M, et d'après le théorème de Cayley-Hamilton on a $\psi([a]) = 0$ soit $\psi(a) = 0$, où ψ_a est le polynôme caractéristique d'une matrice associée à $[a]$. □

Théorème 3.1. *L'ensemble $\bar{A} \subset L$ des entiers sur A est un anneau, que l'on appelle la clôture intégrale de A.*

Preuve. Soit $a, b \in L$ entiers sur A. Il existe des modules finiment généré $M, N \subseteq L$ tels que $aM \subseteq M$ et $bN \subseteq N$. Alors le module $MN = \{\sum_i m_i n_i \mid \forall i, m_i \in M \wedge n_i \in N\}$ est finiment généré, et de plus $(a+b)MN \subseteq MN$ et $(ab)MN \subseteq MN$. □

Définition 3.1. On dit que A est intégralement clos dans L si $A = \bar{A}$. Si A est intégralement clos dans $k = \operatorname{Frac} A$, on dit qu'il est intégralement clos tout court.

Lemme 3.2. Soit B la clôture intégrale de A dans L. B est intégralement clos.

Preuve. Soit $b \in L$ un entier sur B, et soit $f \in B[X]$ le polynôme l'annulant. Si on appelle (a_i) les coefficients de f, b est évidemment entier sur $A[a_i]$, donc $A[a_i][b]$ est finiment généré en tant que $A[a_i]$-module. De plus les a_i sont entiers sur A, donc $A[a_i]$ est finiment généré en tant que A-module. Ainsi, $M = A[a_i, b]$ est un A-module finiment généré vérifiant $bM \subseteq M$, d'où b est entier sur A. □

Proposition 3.1. Si A est factoriel, alors il est intégralement clos.

Preuve. Soit $p/q \in k$ avec $\gcd(p, q) = 1$, et soit $f \in A[X]$ annulant p/q. Alors si on appelle (a_i) les coefficients de f, on a

$$a_0 + a_1 \frac{p}{q} + \ldots + \frac{p^n}{q^n} = 0.$$

En multipliant par q^n on obtient

$$a_0 q^n + a_1 p q^{n-1} + \ldots + p^i = 0,$$

d'où tout facteur premier de q est un facteur premier de p. On en déduit que $q \in A^\times$, soit $p/q \in A$. Ainsi $\bar{A} = A$. □

Théorème 3.2. *Si $d \in \mathbb{Z}$ possède un facteur carré, alors $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos. En particulier, il n'est pas factoriel.*

Preuve. Soit $d = n^2 d'$ avec $n, d \in \mathbb{Z}$. Alors $a = n^2 + \sqrt{d'} \notin \mathbb{Z}[\sqrt{d}]$, mais a est entier sur $\mathbb{Z}[\sqrt{d}]$. En effet,

$$a^2 = n^4 + n^2\sqrt{d'} + d' = n^4 + d' + \sqrt{d} \in \mathbb{Z}[\sqrt{d}].$$

Ainsi, le polynôme unitaire $X^2 - n^4 - d'$ annule $n^2 + a$.

References

[Neu99] Jürgen Neukirch. *Algebraic number theory. Transl. from the German by Norbert Schappacher*. English. Vol. 322. Grundlehren Math. Wiss. Berlin: Springer, 1999. ISBN: 3-540-65399-6.

[Sha94] Igor R. Shafarevich. *Basic Algebraic Geometry 1*. en. Berlin, Heidelberg: Springer, 1994. ISBN: 9783642579080. DOI: 10.1007/978-3-642-57908-0_1.

[Zap] Leonardo Zapponi. *4M033: Théorie des nombres 1*. URL: https://webusers.imj-prg.fr/~leonardo.zapponi/Web2/4M033.html (visited on 12/01/2022).