# Arithmétique des coniques

Notes (inachevées) pour le séminaire Jouve-Pazuki

Bruno Winckler

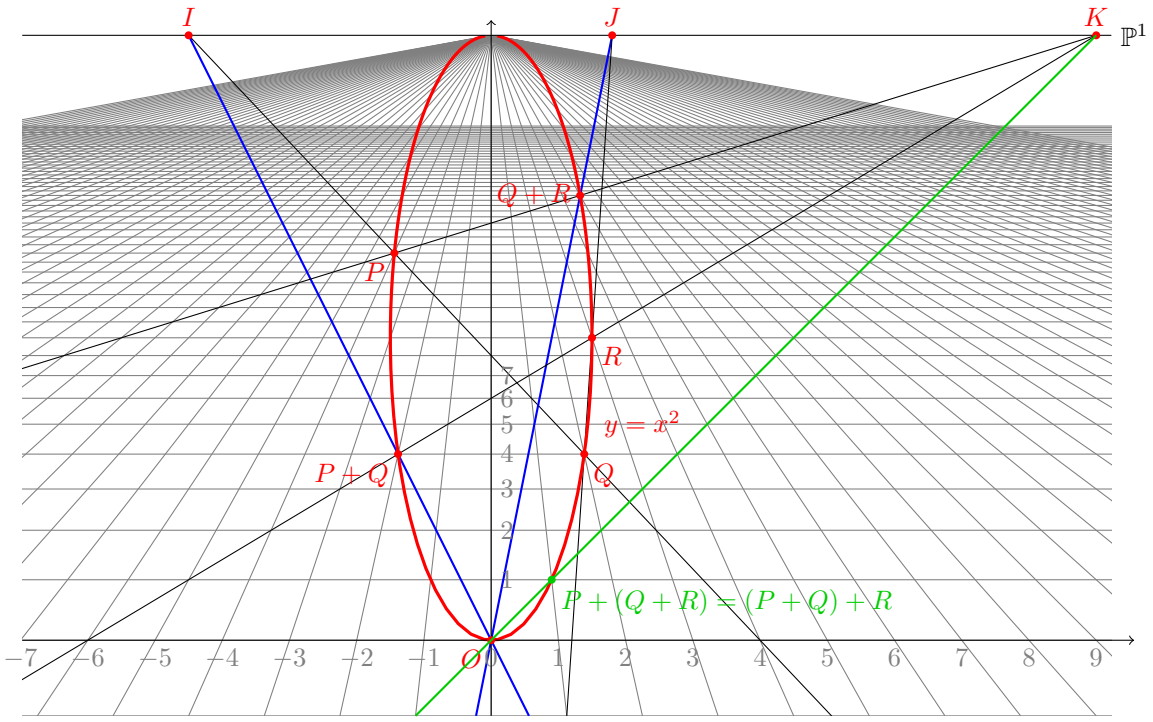



FIGURE 1. Loi de groupe sur une conique (vue d'artiste).

**Table des matières**

## Introduction

### 1. Rappels succincts de géométrie projective

**1.1. Définitions grossières.** — Les prérequis de géométrie projective nécessaires ici sont extrêment restreints, je me contenterai de définir la droite et le plan projectifs informellement, puisqu'ils sont un bon cadre pour formuler les théorèmes de géométrie dont j'ai besoin. Pour résumer, de façon simplifiée pour les besoins de cet exposé, on définit :

$$\mathbb{P}^1 = \{\text{droites vectorielles de } \mathbb{R}^2\} = \mathbb{R}^{*2}/\mathbb{R}^* = \mathbb{R} \sqcup \{\infty\}.$$

La première égalité revient à dire que $\mathbb{P}^1$ paramètre l'ensemble des droites vectorielles du plan. La seconde est la façon rigoureuse de le dire : $\mathbb{R}^*$ agit sur $\mathbb{R}^{*2}$ par multiplication scalaire ; comme une droite vectorielle est définie par son vecteur directeur à une constante non nulle près, cela correspond à la description que j'ai donnée. La dernière égalité revient à dire que $\mathbb{P}^1$ est une droite à laquelle on rajoute un point « à l'infini ». Cette interprétation se voit grâce à la bijection entre $\mathbb{P}^1$ et $\mathbb{R} \cup \{\infty\}$, donnée par l'application *classe de* $(a, b) \mapsto a/b$ si $b \neq 0$, $\infty$ si $b = 0$. Un moyen mnémotechnique rigolo se présente ainsi : on a

$$\mathbb{R}^{*2}/\mathbb{R}^* = \frac{\mathbb{R}^2 - \{\star\}}{\mathbb{R} - \{\star\}} = \mathbb{R} + \{\star\},$$

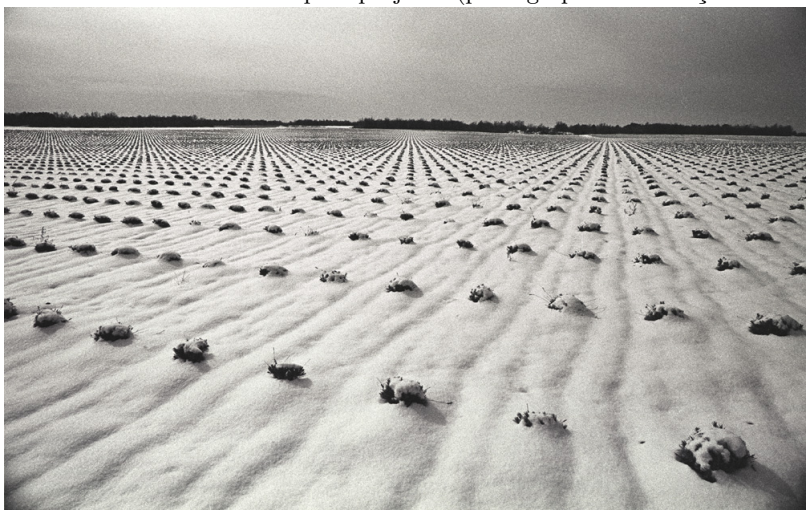
par analogie avec la formule $\frac{x^2-1}{x-1} = x + 1$. Ce moyen mnémotechnique vaut en fait pour tous les espaces projectifs $\mathbb{P}^n$, que je ne définirai pas. Enfin, on peut se dire intuitivement que $\mathbb{P}^1$ est « comme un cercle », puisqu'en adjoignant un point à la droite réelle, on lui permet de « joindre de les deux bouts » pour obtenir un cercle. Effectivement, $\mathbb{P}^1$ est en bijection avec un cercle. Je généraliserai cette idée plus tard.

Je définis également le plan projectif, le théâtre de cet exposé. Seule une interprétation de ce plan m'importera :

$$\mathbb{P}^2 = \mathbb{R}^{*3}/\mathbb{R}^* = \mathbb{R}^2 \sqcup \mathbb{P}^1 = \text{ un plan affine } \sqcup \text{ une droite « à l'infini ».}$$

Les points de $\mathbb{P}^2$ sont de la forme *classe de* $(x, y, z)$, et ceux à l'infini sont ceux définis par l'équation $z = 0$ : c'est l'équation d'une droite, qu'on choisit comme étant « la droite à l'infini ». Chaque point de cette droite à l'infini, décrite par un paramètre $t \in \mathbb{R} \sqcup \{\infty\}$ d'après notre définition d'une droite projective, est le point de concours de toutes les droites de pente $t$. Ainsi, même les droites parallèles ont un point d'intersection dans le plan projectif (ce que tous les amateurs de peinture savent bien, grâce aux points de fuite), qu'on peut observer sur la figure 2, où la ligne d'horizon joue le rôle de la « droite à l'infini » où les droites parallèles se rencontrent.

FIGURE 2. Le plan projectif (photographie de François Rouvière).



Dans ce contexte, une conique (affine) est le lieu d'annulation d'un polynôme réel du second degré en deux indéterminées [*].

Pour tout objet géométrique $C$ apparaissant dans cet exposé et pour tout corps $K$, je noterai $C(K)$ l'ensemble des points à coordonnées dans $K$, tels qu'ils vérifient l'équation définissant $C$.

**1.2. Théorie de l'intersection.** — Le plan projectif est un bon espace dès lors qu'on veut parler d'intersection entre des courbes. En effet, ce plan est une structure d'incidence vérifiant les axiomes de la géométrie projective, le plus important ici étant : *Deux droites distinctes se coupent en un et un seul point*, une droite du plan projectif étant une droite affine munie d'un point à l'infini qui « code » la pente de la droite, comme je l'ai brièvement décrit dans la section précédente. Si $D$ et $D'$ sont deux droites, on note $D \cap D'$ leur unique point d'intersection.

On peut aussi décrire l'intersection d'une droite et d'une conique assez simplement.

***Proposition 1.1.*** — *Une conique irréductible (*i.e. *qui est définie par un polynôme irréductible) et une droite ont au plus deux points d'intersection.*

Cette proposition sera la base de la loi de groupe sur les coniques qui fera son apparition dans la prochaine section. Dans le plan projectif, il y a exactement deux points d'intersection, modulo quelques hypothèses supplémentaires.

*Démonstration.* — Soit $f(x, y) = 0$ l'équation définissant notre conique, et $ax + by + c = 0$ celle définissant notre droite. L'un des coefficients est non nul, on peut supposer que c'est par exemple $a$. L'équation des points d'intersection s'écrit donc $x = -\frac{b}{a}y - \frac{c}{a}$ et $f\left(-\frac{b}{a}y - \frac{c}{a}, y\right) = 0$, qui a au plus deux racines, puisqu'il s'agit d'un polynôme au plus du second degré. □

Si on considère une conique projective, le polynôme est même exactement du second degré, donc admet exactement deux racines (éventuellement avec multiplicité) dans une clôture algébrique.

On note de plus que si l'intersection d'une conique et d'une droite contient un point qui est, disons, à coordonnées dans $K$, alors soit la droite est précisément la tangente en ce point (qui est le seul point d'intersection de cette droite avec la conique), soit la droite coupe la conique en un deuxième point qui est aussi à coordonnées dans $K$ (à cause des relations coefficients-racines).

Un autre théorème de géométrie projective, un poil pénible à démontrer et qui peut se déduire du fameux théorème de Bézout (non énoncé ici), est le théorème de Pascal :

***Théorème 1.2* (Théorème de Pascal).** — *On considère six points $P_1, \ldots, P_6$ sur une conique irréductible. Alors, les points $I = (P_1P_2) \cap (P_4P_5)$, $J = (P_2P_3) \cap (P_5P_6)$ et $K = (P_3P_4) \cap (P_6P_1)$ sont alignés.*

En outre, ce théorème permet de démontrer que par cinq points du plan dont quatre points ne sont jamais alignés, il passe toujours une unique conique, et on peut la construire explicitement.

***Remarque 1.3.*** — En particulier, si $I$ et $J$ sont à l'infini, alors $K$ aussi.

## 2. Loi de groupe sur une conique

Revenons au problème abordé dans l'introduction, et soit $\mathcal{C}$ une conique ; dorénavant on ne précisera plus si elles sont projectives ou affines, puisque de toute façon le passage de l'affine au projectif est aisé.

J'ai déjà esquissé une façon de décrire explicitement tous les points rationnels d'une conique, revenons là-dessus : si $\mathcal{C}(\mathbb{Q})$ est non vide, on fixe un point $P$ à coordonnées rationnelles. Alors, toute droite $\mathcal{D}$ passant par $P$ coupe $\mathcal{C}$ en un second point $P_{\mathcal{D}}$ (si la droite est tangente à $P$, on note $P_{\mathcal{D}} = P$), lui aussi à coordonnées rationnelles si la pente de la droite $\mathcal{D}$ l'est. L'application $\phi : \begin{cases} \mathbb{P}^1(\mathbb{Q}) & \to & \mathcal{C}(\mathbb{Q}) \\ \mathcal{D} & \mapsto & P_{\mathcal{D}} \end{cases}$ est bien définie et est une bijection : l'injectivité est claire car par deux points ne passe qu'une seule droite, et c'est une surjection parce que la droite $(PP_{\mathcal{D}})$ a une pente s'écrivant à l'aide des coordonnées de $P$ et $P_{\mathcal{D}}$, donc est rationnelle. Bref,

***Proposition 2.1.*** — *Soit $\mathcal{C}$ une conique projective irréductible, telle que $\mathcal{C}(\mathbb{Q}) \neq \emptyset$. On a une bijection entre $\mathcal{C}(\mathbb{Q})$ et $\mathbb{P}^1(\mathbb{Q})$.*

---

∗. Ici, je ne me tracasserai pas avec le problème des coniques vides, de la non unicité éventuelle de l'équation définissant la conique, *etc.*

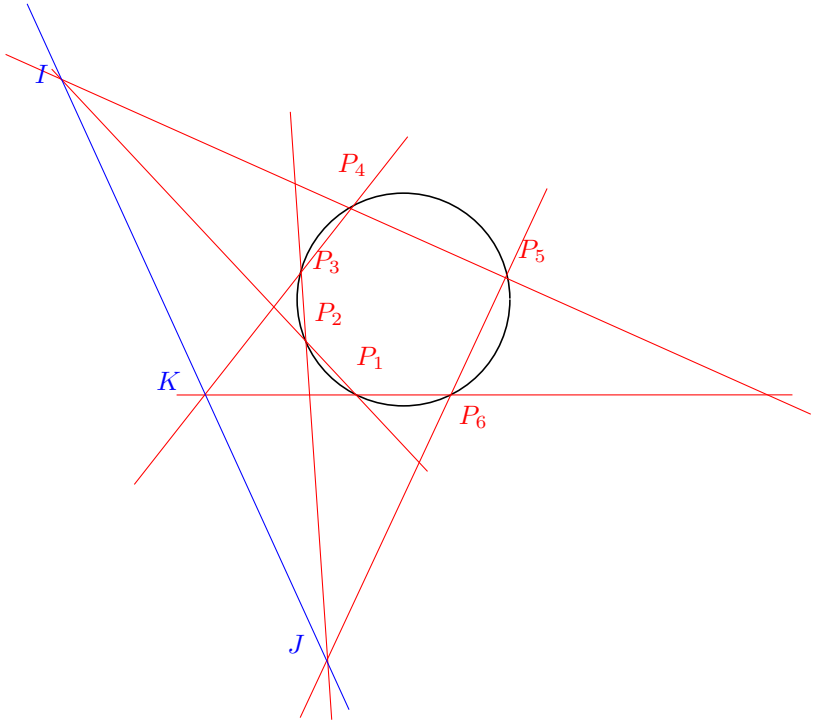
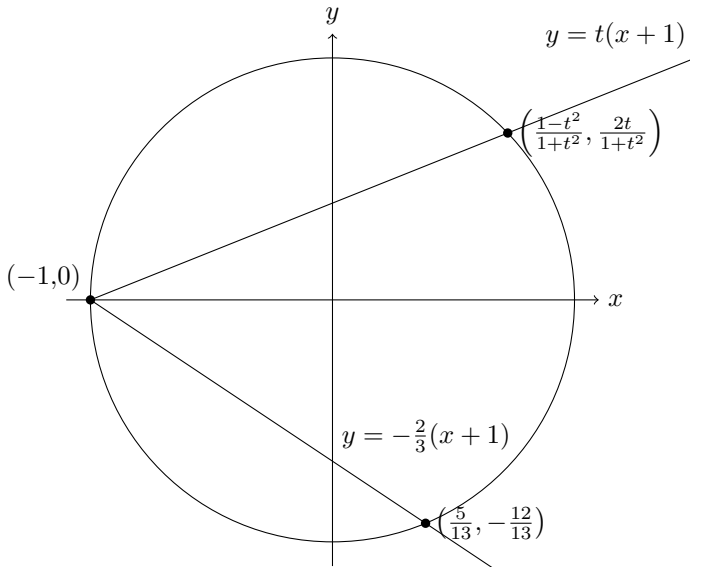



FIGURE 3. Illustration du théorème de Pascal pour un cercle

Ceci vaut bien sûr en remplaçant $\mathbb{Q}$ par n'importe quel corps. Comme on peut paramétrer l'ensemble $\mathbb{P}^1(\mathbb{Q})$ à l'aide d'un paramètre $t \in \mathbb{Q} \cup \{\infty\}$ (qui donne la pente des droites vectorielles), on peut de même paramétrer toute conique irréductible ainsi.

***Exemple 1.*** — L'ensemble des points du cercle unité, privé toutefois de $(-1,0)$, peut se décrire comme l'ensemble $\left\{ \left( \frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) ; t \in \mathbb{Q} \cup \{\infty\} \right\}$. La paramétrisation est illustrée en figure 2.2.1.

FIGURE 4. Paramétrisation du cercle grâce à $\mathbb{P}^1$.




Cette méthode permet de résoudre assez simplement la question de la recherche des points rationnels, mais n'est pas forcément d'un grand recours pour trouver les points entiers, où la

situation peut être très différente : alors que dans le cas des points rationnels, il y a zéro ou une infinité de points, il peut très bien y avoir très peu de points entiers (comme dans le cas du cercle ci-dessus) ou une infinité (comme dans le cas de la conique d'équation $x^2 - 2y^2 = 1$, qu'on traitera plus généralement plus loin). Il faudrait donc étudier plus minutieusement cette façon d'engendrer des points à partir d'intersections de droites, si on veut des informations plus précises sur les points entiers.

**2.1. Construction.** — Une solution est proposée à l'aide de la structure de groupe suivante : supposons que l'ensemble des points rationnels de notre conique affine $\mathcal{C}$ soit non vide ; on fixe alors une bonne fois pour toute un point $O \in \mathcal{C}(\mathbb{Q})$. Pour $P$ et $Q$ sur $\mathcal{C}$, on considère $P + Q$ le point d'intersection de la droite parallèle à $(PQ)$ passant par $O$ avec $\mathcal{C}$, avec éventuellement $P + Q = O$ si cette droite est tangente à $\mathcal{C}$ en $O$ (le point $O$ est en effet point double de cette intersection). Il est facile d'y retrouver tous les axiomes d'une loi de groupe, sauf l'associativité.

Pour montrer que cette loi est associative, étant donnés trois points $A$, $B$ et $C$ sur la conique, il faut vérifier que $(A + B) + C = A + (B + C)$, et le procédé de construction montre que ça revient à dire que les droites $((A + B)C)$ et $(A(B + C))$ sont parallèles, ou encore qu'elles se coupent à l'infini. Posons $P_1 = A$, $P_2 = B$, $P_3 = C$, $P_4 = A + B$, $P_5 = O$ et $P_6 = B + C$. On a choisi les points de sorte que $I$ (resp. $J$) soit le point d'intersection des droites $(O(A + B))$ et $(AB)$ (resp. $(O(B + C))$ et $(BC)$), qui se trouve à l'infini. Par le théorème de Pascal, les points $I$, $J$ et $K = ((A + B)C) \cap (A(B + C))$ sont alignés, donc $K$ est à l'infini, et c'est ce qu'on veut.

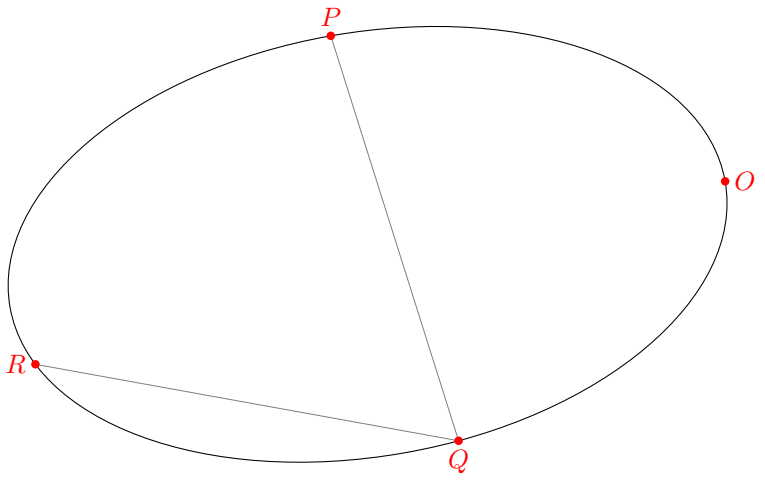



FIGURE 5. Associativité de la loi de groupe (à compléter)

On pose

$$[n]M = \begin{cases} \underbrace{M + \cdots + M}_{n \text{ fois}} & \text{si } n > 0, \\ [-n](-M) & \text{sinon.} \end{cases}$$

Les multiplications ainsi définies sont des endomorphismes. On définit $\mathcal{C}(K)[n]$ comme étant le noyau de $[n] : \mathcal{C}(K) \to \mathcal{C}(K)$ ; si le corps n'est pas précisé, on considère implicitement $\mathcal{C}(\bar{K})$, où $K$ est le corps engendré par les coefficients de $\mathcal{C}$.

***Exercice 1.*** — Est-ce que, de manière générale, ce sont les seuls endomorphismes ?
***Remarque 2.2.*** — Le choix de l'élément neutre n'a aucune importance : deux choix différents induisent des groupes isomorphes, l'isomorphisme étant fourni par une translation envoyant le premier choix sur le second.

**2.2. Exemples.** —

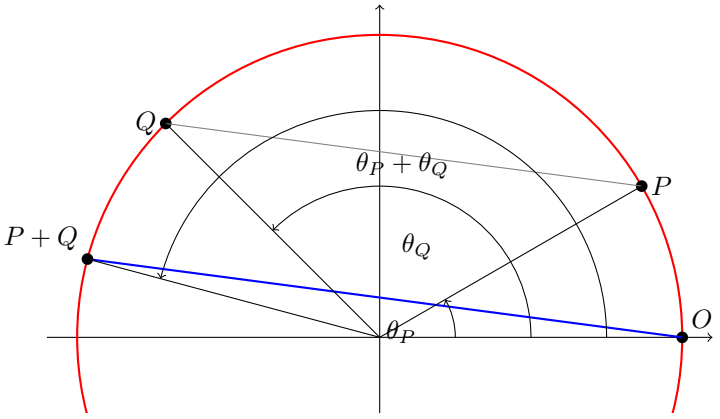
**2.2.1.** *Cercle unité.* — Reprenons, pour commencer, l'exemple du cercle unité d'équation affine $x^2+y^2=1$. Les points entiers sont vite trouvés, il s'agit de $\mathcal{C}(\mathbb{Z})=\{(\pm1,0),(0,\pm1)\}$. Munissons $\mathcal{C}(\mathbb{Q})$ d'une structure de groupe grâce au procédé décrit précédemment, en fixant (1,0) comme élément neutre. On peut alors vérifier que $\mathcal{C}(\mathbb{Q})$ s'injecte dans le groupe des nombres complexes de module 1 pour le produit usuel (c'est-à-dire : $(x+iy)\times(x'+iy')=(xx'-yy')+i(xy'+x'y)$), que je note $(\mathbb{U},\times)$. Autrement dit, si $P(x,y)$ et $Q(x',y')$ sont deux points rationnels de cette conique, on a

$$P(x,y)+Q(x',y')=(xx'-yy',xy'+x'y).$$

Cette formule rend claire l'assertion suivante :

***Proposition 2.3.*** — *$\mathcal{C}(\mathbb{Z})$ est un sous-groupe de $(\mathcal{C}(\mathbb{Q}),+)$.*

FIGURE 6. Loi de groupe pour $x^2+y^2=1$.




*Démonstration.* — J'ai juste à démontrer que $P+Q$ a les coordonnées indiquées ci-dessus. Alors, la stabilité des opérations de groupe pour $\mathcal{C}(\mathbb{Z})$ sera évidente. Écrivons plutôt les coordonnées de $P$ et $Q$ sous la forme $(\cos(\theta_P),\sin(\theta_P))$ et $(\cos(\theta_Q),\sin(\theta_Q))$ ; on doit alors montrer que $P+Q$ a pour coordonnées $(\cos(\theta_P+\theta_Q),\sin(\theta_P+\theta_Q))$ (qui sont bien les coordonnées correspondant au produit usuel des nombres complexes du cercle unité d'arguments $\theta_P$ et $\theta_Q$). La droite passant par $O(1,0)$ et parallèle à $(PQ)$ a pour équation affine

$$(\sin(\theta_Q)-\sin(\theta_P))(x-1)-(\cos(\theta_Q)-\cos(\theta_P))y=0. \tag{1}$$

Elle coupe le cercle en un point $(x,y)=(\cos(\theta),\sin(\theta))$ vérifiant (après réaménagement de (1))

$$\sin(\theta_Q-\theta)+\sin(\theta-\theta_P)=\sin(\theta_Q)-\sin(\theta_P).$$

Heureusement, on connait nos formules de trigonométrie, et on obtient l'équation équivalente

$$2\sin\left(\frac{\theta_Q-\theta_P}{2}\right)\cos\left(\frac{\theta_Q+\theta_P}{2}-\theta\right)=2\sin\left(\frac{\theta_Q-\theta_P}{2}\right)\cos\left(\frac{\theta_Q+\theta_P}{2}\right),$$

puis $\cos\left(\frac{\theta_Q+\theta_P}{2}-\theta\right)=\cos\left(\frac{\theta_Q+\theta_P}{2}\right)$, ce qui donne comme solutions $\theta=0 \bmod 2\pi$ (donc la solution $O$, qu'on connaissait déjà) ou $\theta=\theta_P+\theta_Q \bmod 2\pi$ ; c'est ce qu'on attendait. □

Ceci étant dit, comme $\mathcal{C}(\mathbb{Z})$ est un sous-groupe de $(\mathbb{U},\times)$, et donc un sous-groupe du groupe multiplicatif du corps $\mathbb{C}$, il est cyclique, et isomorphe à $\mathbb{Z}/4\mathbb{Z}$. La construction géométrique permet immédiatement de constater que $(\pm1,0)$ sont les générateurs de ce groupe. Plus généralement, si $K$ est un corps de nombres avec $r_1$ plongements réels et $2r_2$ plongements complexes, dont l'anneau des entiers est $\mathscr{O}_K$, alors :

***Proposition 2.4*** **([Sha01]).** — *Le groupe $\mathcal{C}(\mathscr{O}_K)$ est de type fini, et on a $\mathcal{C}(\mathscr{O}_K)\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}^{r_2-1}$ si $i\in K$, tandis que $\mathcal{C}(\mathscr{O}_K)\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}^{r_2}$ sinon.*

Le groupe $\mathcal{C}(\mathbb{Q})$, en revanche, est loin d'être cyclique, il n'est même pas de type fini.

***Proposition 2.5*** **([Tan96]).** — *Le groupe $\mathcal{C}(\mathbb{Q})$ est le produit d'une infinité de groupes cycliques, indexée par l'ensemble des nombres premiers congrus à 1 modulo 4.*

*Démonstration.* — On a vu comment paramétrer l'ensemble des points du cercle (privé de $(-1,0)$). On peut réécrire l'application $\rho : \mathbb{Q} \to \mathcal{C}(\mathbb{Q}) \setminus \{(-1,0)\}$ ainsi : $\rho\left(\frac{n}{m}\right) = \left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right)$. Si $(m,n)$ est un point du cercle, on reconnait ici $[2](m,n)$. À présent, pour tout élément $m+ni \in \mathbb{Z}+\mathbb{Z}i = \mathbb{Z}[i]$ non nul, je pose $f(m+ni) = \rho\left(\frac{n}{m}\right)$ (si $m=0$, alors $f(ni) = (-1,0)$). La fonction $f : \mathbb{Z}[i] \setminus \{0\} \to \mathcal{C}(\mathbb{Q})$ est surjective parce que $\rho$ l'est, est constante sur les droites de pente rationnelle, et est multiplicative : si $m+ni$ a pour argument $\theta$, alors $f(m+ni)$ a pour argument $2\theta$. Enfin, on vérifie facilement les identités suivantes :

$$f(m+ni) + f(m-ni) = (1,0), \tag{2}$$

$$f(m+ni) = (1,0) \Leftrightarrow n = 0, \tag{3}$$

$$f(m+ni) = (-1,0) \Leftrightarrow m = 0. \tag{4}$$

Ce presque-morphisme surjectif va nous aider à étudier la structure de $\mathcal{C}(\mathbb{Q})$, grâce aux propriétés bien connues de $\mathbb{Z}[i]$ que je ne démontrerai pas ici.

Pour commencer, les éléments $f(m+ni) \in \mathcal{C}(\mathbb{Q})$ avec $m+ni$ irréductible dans $\mathbb{Z}[i]$ suffisent à engendrer $\mathcal{C}(\mathbb{Q})$ : notons $\mathcal{C}(\mathbb{Q}) \ni (a_k, b_k) = f(m_k + n_k i)$. Alors, $(a_1,b_1) = (a_2,b_2) + (a_3,b_3)$ si, et seulement s'il existe des entiers non nuls $\ell$ et $\ell'$ tels que $(m_1+n_1 i)\ell = (m_2+n_2 i)(m_3+n_3 i)\ell'$. Les irréductibles de $\mathbb{Z}[i]$ sont :

- les nombres premiers $p$ congrus à 3 modulo 4, et on a $f(p) = (1,0)$ ;
- les diviseurs des nombres premiers congrus à 1 modulo 4 (forcément réductible dans $\mathbb{Z}[i]$). Pour chacun de ces nombres premiers $p$, notons $m_p \pm n_p i$ ses diviseurs ;
- $1 \pm i$ (diviseurs de 2), et on a $f(1 \pm i) = (0, \pm 1)$, des points d'ordre 4 dans $\mathcal{C}(\mathbb{Q})$.

D'après ce qu'on vient de dire, l'ensemble

$$\left\{ \left( \frac{m_p^2 - n_p^2}{m_p^2 + n_p^2}, \frac{2m_p n_p}{m_p^2 + n_p^2} \right) \mid p \equiv 1 \bmod 4 \right\} \bigcup \{(0,1)\}$$

est un système complet de générateurs pour $\mathcal{C}(\mathbb{Q})$. Il s'agit de démontrer qu'ils sont indépendants.

***Lemme 2.6.*** — *Il n'y a pas de relation non triviale entre les éléments de* $\left(\frac{m_p^2-n_p^2}{m_p^2+n_p^2}, \frac{2m_p n_p}{m_p^2+n_p^2}\right)_{p \equiv 1 \bmod 4}$.

*Démonstration du lemme..* — Une relation de dépendance entre ces éléments entraînerait, dans $\mathbb{Z}[i]$, une relation de la forme $\prod_k (m_{p_k} + n_{p_k} i)^{a_k} = \prod_k q_k$, où chaque élément du produit de gauche est irréductible dans $\mathbb{Z}[i]$, et ceux du produit de droite sont premiers dans $\mathbb{Z}$. Comme il y a unicité d'une factorisation en facteurs irréductibles, chaque $q_i$ est produit de deux facteurs du membre de gauche, qui doivent être conjugués l'un de l'autre. Deux éléments conjugués ont des images par $f$ inverses l'une de l'autre, par la relation (2). C'est impossible à moins d'avoir $a_k = 0$ pour tout $k$, puisque tous les $m_p$ et $n_p$ sont non nuls. □

Pour inclure (0,1) au lemme, il suffit de remarquer qu'une relation de dépendance pour notre système de générateurs se ramène, après multiplication par [4], au lemme. Comme il y a une infinité de nombres premiers $p \equiv 1 \bmod 4$, on en déduit le théorème 2.5. Plus précisément, $\mathcal{C}(\mathbb{Q})$ est isomorphe à $\langle (0,1) \rangle \times \prod_{p \equiv 1 \bmod 4} \left\langle \left( \frac{m_p^2-n_p^2}{m_p^2+n_p^2}, \frac{2m_p n_p}{m_p^2+n_p^2} \right) \right\rangle$ ; les groupes du produit sont monogènes infinis : si un élément $f(m_p + i n_p) \in \mathcal{C}(\mathbb{Q})$ était d'ordre fini $k$, alors on aurait $(m_p + i n_p)^k \in \mathbb{Q}$. Comme il s'agit d'un entier algébrique, on aurait même $(m_p + i n_p)^k \in \mathbb{Z}$, et considérer la norme de cet élément montre que ce serait une puissance de $p$. Pourtant, l'égalité

$$(m_p + i n_p)^k = p^\ell = (m_p + i n_p)^\ell (m_p - i n_p)^\ell$$

entraine $k = \ell = 0$ par unicité de la décomposition en facteurs irréductibles dans $\mathbb{Z}[i]$, ce qui est absurde. □

Citons un corollaire intéressant résultant de cette structure.

***Corollaire 2.7.*** — *Si $\alpha \in \mathbb{R}$, on note $P_\alpha$ le point du cercle d'argument $\alpha \bmod 2\pi$. Soient $\alpha$ et $\beta$ deux réels de commune mesure, tels que $P_\alpha$ et $P_\beta$ soient dans $\mathcal{C}(\mathbb{Q})$. Il existe alors $r, s$ deux entiers, $P_\gamma$ dans $\mathcal{C}(\mathbb{Q})$, et $c_\alpha, c_\beta \in \langle (0,1) \rangle$, tels que*

$$P_\alpha = [r]P_\gamma + c_\alpha, P_\beta = [s]P_\gamma + c_\beta.$$

*En particulier, si $P_\alpha \in \mathcal{C}(\mathbb{Q})$ avec $\alpha$ de commune mesure à $\pi$, alors $P_\alpha \in \langle (0,1) \rangle$.*

*Démonstration.* — Posons $\frac{\alpha}{\beta} = \frac{r}{s}$, où $r$ et $s$ sont premiers entre eux. Alors, $[s]P_\alpha = [r]P_\beta$, car la multiplication par $[n]$ revient à multiplier l'argument du point par $n$. Pour avoir le corollaire, il suffit alors de comparer les composantes dans $C_p := \left\langle \left( \frac{m_p^2 - n_p^2}{m_p^2 + n_p^2}, \frac{2m_p n_p}{m_p^2 + n_p^2} \right) \right\rangle$ de $P_\alpha$ et $P_\beta$ : chaque composante dans $C_p$ de $P_\alpha$ est « divisible » par $r$, et de même avec $P_\beta$ pour $s$. Pour définir $P_\gamma$, il suffit de prendre, pour chaque composante dans $C_p$, $\frac{1}{r}$ fois la composante de $P_\alpha$ dans $C_p$. La deuxième affirmation du corollaire s'obtient en prenant $\beta = \pi$. □

C'est un résultat intéressant : on en déduit en particulier que les $\cos\left(\frac{2\pi a}{b}\right)$ et $\sin\left(\frac{2\pi a}{b}\right)$ à être simultanément rationnels sont ceux que l'on connaît depuis l'enfance. Avec un peu plus de réflexion, on peut en déduire quels sont les seuls rationnels de la forme $\cos\left(\frac{2\pi a}{b}\right)$.

***Exercice 2.*** — Reproduire ces propositions pour l'hyperbole d'équation $x^2 - y^2 = 1$ ; on doit remplacer $\mathbb{Z}[i]$ par $\mathbb{Z}[X]/(X^2 - 1)$, ce qui a le défaut de ne pas être un anneau intègre et appelle à la vigilance.

**2.2.2.** *Conique de Pell-Fermat.* — Considérons un exemple qui va nous suivre tout au long de cet exposé : soit $d$ un entier qui n'est pas un carré parfait, et l'hyperbole $\mathcal{H}$ d'équation $x^2 - dy^2 = 1$. On munit cette hyperbole d'une structure de groupe en prenant pour élément neutre $O(1,0)$. Ces hyperboles sont appelées coniques de Pell-Fermat ; l'allusion à l'équation de Pell-Fermat va de soi, puisque la recherche des solutions entières de cette équation est un classique diophantien. On s'y attelle. Encore une fois, $\mathcal{H}(\mathbb{Q})$ n'est pas de type fini, admettant un système de générateur indexé par l'ensemble des nombres premiers. On peut décrire ses points rationnels autrement, grâce à la bijection entre $\mathcal{H}(\mathbb{Q})$ et $\mathbb{P}^1(\mathbb{Q})$, qui sont de la forme $\left( \frac{dt^2+1}{dt^2-1}, \frac{2dt}{dt^2-1} \right)$. Cette fois, ce sont les points entiers qui nous intéresseront le plus. Si $d$ est négatif, on a vite fait de déterminer $\mathcal{H}(\mathbb{Z})$. Supposons donc $d > 0$.

**Aspect géométrique de la conique de Pell-Fermat.** Avec ce choix d'élément neutre, l'inverse de $M(x,y)$ est $-M(x,-y)$. En effet, l'équation de la tangente en $O$ est $x = 1$, qui est parallèle à la droite passant par $(x,y)$ et $(x,-y)$.

Soit $M_1(x_1, y_1) \in \mathcal{H}$ le point minimal de la courbe, c'est-à-dire le point dont les coordonnées sont la solution minimale de l'équation de Pell-Fermat associée à $\mathcal{H}$, d'ordonnée strictement positive.

On définit une application $\varphi : \mathcal{H} \to \mathcal{H}$ en posant : $\forall M \in \mathcal{H}$, $\varphi(M) = M + M_1$.

***Proposition 2.8.*** — *Si $M$ a pour coordonnées $(x,y)$ dans le repère $R$, les coordonnées de $\varphi(M)$ dans le repère $R$ sont $(xx_1 + dyy_1, xy_1 + yx_1)$.*

*Démonstration.* — Dans un repère $R'$ tel que l'équation de $\mathcal{H}$ est $xy = 1$, en faisant le changement de base $x \mapsto x - \sqrt{d}y$, $y \mapsto x + \sqrt{d}y$ (on garde la même origine), il est nettement plus facile de calculer les coordonnées de $\varphi(M)$ : l'abscisse (ou l'ordonnée) de $M + M_1$ est le produit de celles de $M$ et $M_1$. Il n'y a plus qu'à multiplier le vecteur coordonnées par la bonne matrice de passage pour obtenir le même résultat.

Plus précisément, soit $\mathcal{B}$ la base canonique, et soit $f : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (x - \sqrt{d}y, x + \sqrt{d}y) \end{cases}$ l'application linéaire de changement de repère ; on note $\mathcal{B}'$ l'image réciproque de $\mathcal{B}$ par $f$.

On pose $P = \begin{pmatrix} 1 & -\sqrt{d} \\ 1 & \sqrt{d} \end{pmatrix}$ la matrice de changement de base ; on a $P^{-1} = \frac{1}{2\sqrt{d}} \begin{pmatrix} \sqrt{d} & \sqrt{d} \\ -1 & 1 \end{pmatrix}$ ; ce sont les matrices de passage qui nous permettront de passer d'un repère à l'autre. Alors, le repère $R'$ est plus précisément $(\Omega, \frac{1}{2}\left(\vec{e_1} - \frac{1}{\sqrt{d}}\vec{e_2}\right), \frac{1}{2}\left(\vec{e_1} + \frac{1}{\sqrt{d}}\vec{e_2}\right))$.

Dans ce repère $R'$, l'élément neutre $O$ a pour coordonnées (1,1). Supposons d'abord que $M = M_1$. Alors, la droite $\mathcal{D}$ parallèle à la tangente en $M_1$ de coordonnées $(x_1', y_1')$ dans $R'$, et passant par $O$, a pour équation $x_1'(y-1) + y_1'(x-1) = 0$.

La droite $\mathcal{D}$ coupe $\mathcal{H}$ en un point de coordonnées $(x,y)$ dans $R'$ vérifiant le système d'équations :

$$\left\{ \begin{array}{rcl} x_1'(y-1) + y_1'(x-1) & = & 0 \\ xy & = & 1 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} x_1'\left(\frac{1}{x} - 1\right) + y_1'(x-1) & = & 0 \\ y & = & \frac{1}{x} \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} x & \in & \{\frac{x_1'}{y_1'}(= x_1'^2), 1\} \\ y & = & \frac{1}{x} \end{array} \right.$$

Bref, $\varphi(M_1)$ a pour coordonnées $(x_1^2, y_1^2)$ dans $R'$. À présent, supposons que $M \neq M_1$ est de coordonnées $(x', y')$ dans $R'$. La droite $\mathcal{D}$ parallèle à $(MM_1)$ passant par $O$ a pour équation

$$\mathcal{D} : (x_1' - x')(y-1) + (y' - y_1')(x-1) = 0 \Leftrightarrow x_1'(y-1) + y'(x-1) = 0.$$

La ressemblance avec l'équation de la droite dans le cas $M = M_1$ doit nous convaincre que déterminer $\mathcal{D} \cap \mathcal{H}$ conduit aux mêmes calculs, et qu'alors $\varphi(M)$ a pour coordonnées $(x'x_1', y'y_1')$ dans $R'$ (un argument de continuité permet également d'y parvenir). Pour trouver les coordonnées dans $R$, on calcule $P^{-1}\begin{pmatrix} x'x_1' \\ y'y_1' \end{pmatrix}$, en se rappelant que $x' = x - \sqrt{d}y$ et $y' = x + \sqrt{d}y$. C'est lourd mais sans mystère :

$$P^{-1}\begin{pmatrix} x'x_1' \\ y'y_1' \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -\frac{1}{\sqrt{d}} & \frac{1}{\sqrt{d}} \end{pmatrix}\begin{pmatrix} (x-\sqrt{d}y)(x_1 - \sqrt{d}y_1) \\ (x+\sqrt{d}y)(x_1+\sqrt{d}y_1) \end{pmatrix} = \cdots = \begin{pmatrix} xx_1 + dyy_1 \\ xx_1 + yy_1 \end{pmatrix},$$

et on trouve finalement les coordonnées annoncées dans la proposition. □

***Remarque 2.9.*** — L'expression de $\mathcal{H}$ dans le repère $R'$ permet de voir l'isomorphisme de groupes entre $(\mathcal{H}(\mathbb{R}), +)$ et $(\mathbb{R}^*, \cdot)$, *via* $\left(x, \frac{1}{x}\right)_{R'} \mapsto x$.

**Aspects algébriques de la conique de Pell-Fermat.** Je rappelle que le corps quadratique $\mathbb{Q}(\sqrt{d})$ est une extension de degré 2 sur $\mathbb{Q}$, galoisienne, de groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z}$ : soit $\sigma$ son automorphisme non trivial (on a $\sigma^2 = \mathrm{id}_{\mathbb{Q}(\sqrt{d})}$). Le morphisme $\sigma$ est $\mathbb{Q}$-linéaire, et est une involution, donc admet 1 et $-1$ comme valeurs propres, et des espaces propres de dimension 1 chacun. Les éléments de $\ker(\sigma - \mathrm{id})$ sont les rationnels, et ceux de $\ker(\sigma + \mathrm{id})$ les irrationnels ; ce dernier est engendré par $\sqrt{d}$, et on appelle alors $\frac{\sigma(x)}{\sqrt{d}} \in \mathbb{Q}$ la partie irrationnelle de $x \in \ker(\sigma + \mathrm{id})$. Comme $\mathbb{Q}(\sqrt{d})$ est une somme directe de ces deux noyaux, chaque élément de ce corps s'écrit comme somme d'une partie rationnelle et d'une partie irrationnelle. Alors :

***Définition 2.10.*** — Tout $x \in \mathbb{Q}(\sqrt{d})$ a une partie rationnelle et irrationnelle, avec unicité. On note $\mathcal{R}(x)$ sa partie rationnelle, et $\mathcal{I}(x)$ sa partie irrationnelle. On a

$$x = \mathcal{R}(x) + \sqrt{d}\mathcal{I}(x) = \frac{x + \sigma(x)}{2} + \sqrt{d}\frac{x - \sigma(x)}{2\sqrt{d}}.$$

On peut vérifier, en effet, que les fractions écrites ci-dessus sont vecteurs propres de $\sigma$ pour 1 et $-1$ respectivement.

On munit $\mathbb{Q}(\sqrt{d})$ de la norme N définie par $\mathrm{N}(x) = x\sigma(x)$ pour tout $x \in \mathbb{Q}(\sqrt{d})$ ; cette norme est clairement multiplicative, et à valeurs dans $\mathbb{Q}$ car stable par le groupe de Galois.

On remarque que $x^2 - dy^2 = 1$ si, et seulement si $\mathrm{N}(x + \sqrt{d}y) = 1$. On a en effet $\mathrm{N}(x + \sqrt{d}y) = (x + \sqrt{d}y)\sigma(x + \sqrt{d}y) = (x + \sqrt{d}y)(x - \sqrt{d}y) = x^2 - dy^2$.

Pour $n \geqslant 1$, soit $(x_n, y_n)$ le couple d'entiers formé des parties rationnelle et irrationnelle de $(x_1 + \sqrt{d}y_1)^n$, où $(x_1, y_1)$ est une solution minimale de l'équation de Pell-Fermat. Alors, $(x_n, y_n)$ est également une solution de l'équation de Pell-Fermat, car $\mathrm{N}(x_n + \sqrt{d}y_n) = \mathrm{N}(x_1 + \sqrt{d}y_1)^n = 1$. On va démontrer qu'on tient là les seules solutions possibles, sans utiliser le théorème des unités de Dirichlet.

On retrouve notre application $\varphi : \mathcal{H} \to \mathcal{H}$ définie par $\varphi(M) = M_1 + M$, où $M_1$ est de coordonnées $(x_1, y_1)$. On a vu que si $M$ est de coordonnées $(x, y)$, alors $\varphi(M)$ est de coordonnées

$$(xx_1 + dyy_1, xy_1 + x_1y) = (\mathcal{R}(zz_1), \mathcal{I}(zz_1))$$

où $z = x + \sqrt{d}y$ et $z_1 = x_1 + \sqrt{d}y_1$ (un calcul direct le prouve). Ceci motive la notion d'affixe, comme dans le plan complexe :

***Définition 2.11* (Affixe dans $\mathbb{Q}(\sqrt{d})$).** — On appelle affixe d'un élément point $M$ de coordonnées $(x, y)$, l'élément $x + \sqrt{d}y \in \mathbb{Q}(\sqrt{d})$.

***Remarque 2.12.*** — Le paragraphe précédent montre que si $M$ est d'affixe $z$, et $M_1$ d'affixe $z_1$, alors l'affixe de $\varphi(M)$ est $zz_1$.

***Proposition 2.13.*** — *Si $M$ est d'affixe $z \in \mathbb{Q}(\sqrt{d})$, alors $-M$ est d'affixe $\sigma(z)$.*

*Démonstration.* — Immédiat, puisqu'on a vu que pour passer de $M$ à $-M$, il suffit de changer l'ordonnée en son opposé. □

***Proposition 2.14.*** — *Soit $M$ un point à coordonnées entières strictement positives $(x, y)$, et soit $M' = (-M_1) + M$ de coordonnées $(x', y')$. On a alors :*

$$0 \leqslant x' < x \text{ et } 0 \leqslant y' < y.$$

*Démonstration.* — Les mêmes réflexions que dans la remarque précédente montrent que $M'$ a pour affixe $\sigma(z_1)z$, où $z = x + \sqrt{d}y$. Alors,

$$x' = \mathcal{R}(\sigma(z_1)z) = \frac{1}{2}\left(\sigma(z_1)z + z_1\sigma(z)\right).$$

Comme $x^2 - dy^2 = 1$, $z$ et $\sigma(z)$ sont de même signe. Comme $x$ et $y$ sont positifs, $z > 0$, et donc $\sigma(z) > 0$. Pour la même raison, il en est de même pour $z_1$ et $\sigma(z_1)$. Ceci prouve que $x' > 0$. De plus, le point $M_1 + M' = M$ est d'ordonnée supérieure à celle de $M'$ : **(à écrire)**.

Comme la fonction $y \mapsto \sqrt{1 + dy^2}$ est strictement croissante, on a

$$x' = \sqrt{1 + dy'^2} < \sqrt{1 + dy^2} = x,$$

car $y' < y$. Il nous manque l'inégalité $y' \geqslant 0$.

On a :

$$y' = \mathcal{I}(\sigma(z_1)z) = \frac{1}{2\sqrt{d}}\left(\sigma(z_1)z - z_1\sigma(z)\right),$$

et on doit donc démontrer que $\sigma(z_1)z \geqslant z_1\sigma(z)$. Ceci équivaut à

$$\frac{z}{\sigma(z)} \geqslant \frac{z_1}{\sigma(z_1)} \Leftrightarrow \frac{z^2}{N(z)} \geqslant \frac{z_1^2}{N(z_1)} \Leftrightarrow z^2 \geqslant z_1^2,$$

en se rappelant que $z$ et $z_1$ sont les affixes de solutions de l'équation de Pell-Fermat (donc sont de norme 1) ; cette inégalité est vraie, parce que par hypothèse $M_1$ est solution minimale de l'équation de Pell-Fermat. □

En voyant la proposition précédente, vous avez raison de penser qu'on va résoudre l'équation de Pell-Fermat avec un argument ressemblant à sa fameuse méthode de descente infinie.

***Théorème 2.15* (Résolution de Pell-Fermat).** — *Soit $(x, y) \in \mathbb{N}^{*2}$. Si $(x, y)$ est solution de l'équation de Pell-Fermat, alors il existe un entier $n$ tel que $(x, y) = (x_n, y_n)$.*

*Démonstration.* — Soit $M \in \mathcal{H}$ de coordonnées $(x, y)$, comme dans l'énoncé. On définit la suite $(M'_n)_{n\geqslant 0}$ en posant $M'_0 = M$, et si $M'_0$, …, $M'_n$ sont bien définis, avec $x_{M'_n}, y_{M'_n} > 0$, on pose $M'_{n+1} = (-M_1) + M'_n$. Si on tombe sur $y_{M'_n} = 0$, la suite est finie.

On va démontrer que cette suite atteint nécessairement le cas $y_{M'_n} = 0$ : d'après le lemme précédent, on a $0 \leqslant y_{M'_{n+1}} < y_{M'_n}$. La suite $(y_{M'_n})_{n\geqslant 0}$ est une suite d'entiers naturels strictement décroissante, donc le cas $y_{M'_n} = 0$ finit par poindre le bout de son nez ; soit $n$ un entier tel qu'on y arrive. On a alors $x_{M'_n} = 1$ nécessairement, et $M'_n = O$. On vient de démontrer qu'il existe un entier $n$ tel que $[-n]M_1 + M = O$, donc $M = [n]M_1$. Or, l'affixe de $[n]M_1$ est $z_1^n = (x_1 + \sqrt{d}y_1)^n$, comme promis. □

***Corollaire 2.16.*** — *On a $\mathcal{H}(\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

Une conique peut donc avoir une infinité de points entiers, comme l'exemple du cercle ne le laissait pas présager du tout.

***Remarque 2.17.*** — Il existe un isomorphisme presque trivial entre $\mathcal{H}(\mathbb{Z})$ et $\mathcal{O}_K^*$, où $K$ est le corps quadratique $\mathbb{Q}(\sqrt{d})$. On s'est donc contenté de redémontrer le théorème des unités de Dirichlet dans ce cas particulier.

**2.2.3.** *Parabole.* — Cet exemple un peu idiot n'est là que pour éviter une discrimination envers les paraboles. On munit la parabole d'équation $\mathcal{P} : y = x^2$ d'une loi de groupe en choisissant comme élément neutre $O(0,0)$. Ses points entiers, tout comme ses points rationnels, sont connus : on a $\mathcal{P}(\mathbb{Z}) = \{(n, n^2); n \in \mathbb{Z}\} \simeq \mathbb{Z}$ (exercice trivial) et $\mathcal{P}(\mathbb{Q}) = \{(r, r^2); r \in \mathbb{Q}\} \simeq \mathbb{Q}$ (de même) qui n'est pas de type fini.

***Exercice 3.*** — Soit $\mathcal{C}$ une conique à coefficients réels. Montrer que $\mathcal{C}(\mathbb{R})$ est isomorphe à $(\mathbb{U}, \times)$, $(\mathbb{R}, +)$ ou $(\mathbb{R}^*, \times)$. Cette classification correspond exactement à la classification en ellipses, paraboles et hyperboles.

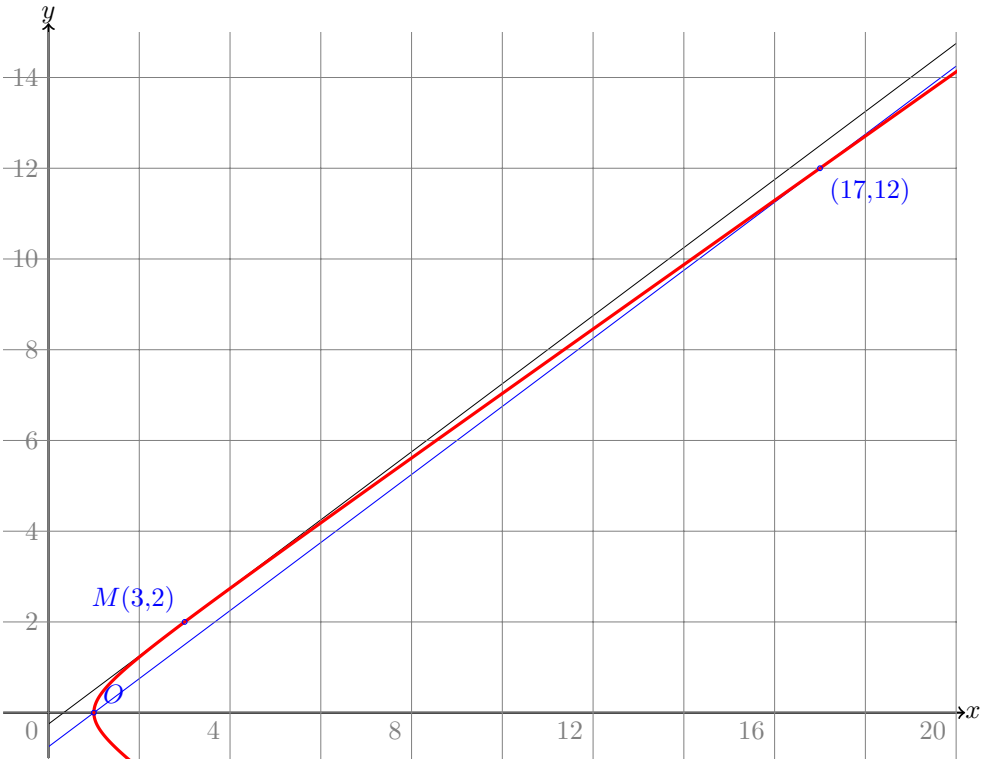



FIGURE 7. Points entiers de $x^2 - 2y^2 = 1$.

### 2.3. Applications. —

**2.3.1.** *Application à la réciprocité quadratique.* — il est également possible de démontrer la loi de réciprocité quadratique sans difficulté, avec cette loi de groupe sur les coniques. Cette fois, on s'intéresse à la conique d'équation $x^2 - \Delta y^2 = 4$, avec $\Delta = 8$. On utilisera cette loi de groupe pour démontrer que si $\left(\frac{p}{q}\right)$ est le fameux symbole de Legendre, alors il existe des polynômes unitaires $F_p$ et $F_q$, à coefficients entiers et de degrés respectifs $\frac{p-1}{2}$ et $\frac{q-1}{2}$, tels que

$$\left(\frac{p}{q}\right) = \prod_{\substack{a\in\mathbb{C}\\ F_p(a)=0}} F_q(a).$$

Le produit est donc indexé par tous les zéros de $F_a$, comptés avec multiplicité. La loi de réciprocité quadratique découlera alors du lemme suivant, familier des habitués du résultant :

***Lemme 2.18.*** — *Si $P$ et $Q$ sont deux polynômes unitaires, alors*

$$\prod_{\substack{a\in\mathbb{C}\\ P(a)=0}} Q(a) = (-1)^{\deg(P)\deg(Q)} \prod_{\substack{a\in\mathbb{C}\\ Q(a)=0}} P(a).$$

*Démonstration du lemme.* — On écrit $P = \prod_a (X-a) = (-1)^{\deg(P)} \prod_a (a-X)$, où le produit est indexé par ses zéros $a$. Alors :

$$\begin{aligned}\prod_{\substack{b\\ Q(b)=0}} P(b) &= \prod_{\substack{b\\ Q(b)=0}} (-1)^{\deg(P)} \prod_{\substack{a\\ P(a)=0}} (a-b)\\ &= (-1)^{\deg(P)\deg(Q)} \prod_{\substack{b\\ Q(b)=0}} \prod_{\substack{a\\ P(a)=0}} (a-b)\\ &= (-1)^{\deg(P)\deg(Q)} \prod_{\substack{a\\ P(a)=0}} Q(a).\end{aligned}$$

□

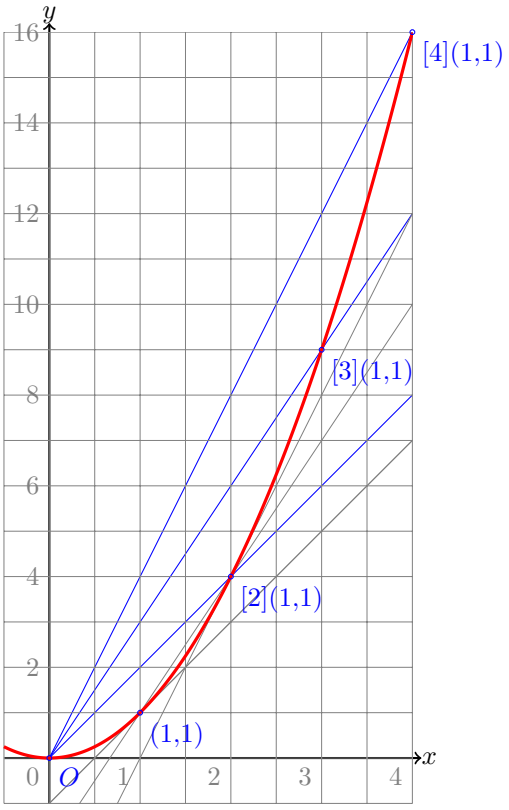



FIGURE 8. Points entiers de $y = x^2$.

Je vous laisse vérifier que le paragraphe précédent et ce lemme impliquent la loi de réciprocité quadratique. Il est important de noter que cette démonstration marche peu importe le corps dans lequel sont les coefficients de $P$ et $Q$, pourvu qu'on considère les racines dans une extension suffisamment grande de ce corps ; n'ayons pas peur de dire : dans un corps algébriquement clos.

Soit $\mathcal{H}$ la conique d'équation affine $x^2 - \Delta y^2 = 4$, et $O = (2,0) \in \mathcal{H}$. Avec le procédé de construction décrit dans ce papier, $(\mathcal{H}(\mathbb{Q}), +)$ est un groupe abélien d'élément neutre $O$. Mieux encore, on peut vérifier que dans le repère canonique du plan, si $M(x,y)$ et $M'(x',y')$ sont deux points de la conique, alors $M+M'$ a pour coordonnées $\left(\frac{1}{2}\left(xx' + \Delta yy'\right), \frac{1}{2}\left(xy' + yx'\right)\right)$. Ceci prouve :

***Proposition 2.19.*** — *$(\mathcal{H}(\mathbb{Z}), +)$ est un sous-groupe de $(\mathcal{H}(\mathbb{Q}), +)$.*

*Preuve.* Il suffit de démontrer la stabilité par somme et inverse. L'inverse n'est pas ce qui va nous poser problème. Si $M(x,y) \in \mathcal{H}(\mathbb{Z})$, alors $x^2 - \Delta y^2 \equiv 0 \bmod 2$, ou encore : $x \equiv \Delta y \bmod 2$. Alors, si $M(x,y)$ et $M'(x',y')$ sont des points de $\mathcal{H}(\mathbb{Z})$ :

$$xx' + \Delta yy' \equiv \Delta^2 yy' + \Delta yy' \equiv 2\Delta yy' \equiv 0 \bmod 2,$$

donc l'abscisse de $M+M'$ est entière. On montre le résultat de la même manière pour l'ordonnée. □

***Remarque 2.20.*** — Connaître les coordonnées de la somme de deux points permet de démontrer que les points de torsion $(x,y)$ de $\mathcal{H}(\mathbb{Z})$ vérifient $x \leqslant 2$ : comme $[n](x,y) = O$ implique $[n](x,-y) = O$, on peut supposer $y > 0$. Soient $P(x,y)$ et $Q(x',y')$ deux points sur $\mathcal{H}(\mathbb{Z})$ tels que $x, x' > 2$. Il est clair que l'ordonnée $y(P+Q)$ de $P+Q$ est strictement positive. Si $x = x'$, alors $y = y'$, et alors l'abscisse $x(P+Q)$ de $P+Q$ égale $x^2 - 2 > 2$. Sinon, comme $4(x-x')^2 > 0$, on a $(xx' - 4)^2 > (x^2 - 4)(x'^2 - 4) = (\Delta yy')^2$, et on a encore $x(P+Q) > 2$. Donc, dans tous les cas, si $x(P) > 2$, on ne peut pas avoir $x([n]P) = 2$ (et donc $[n]P = O$) pour $n \geqslant 2$.

On a donné les coordonnées de la somme de deux points de la courbe. On peut aussi calculer les coordonnées de $[n]M$. Si $(x_n, y_n)$ représente les coordonnées de $[n]M$ pour tout $n$, alors :

$$\left\{ \begin{array}{rcl} x_{n+1} & = & \frac{1}{2}\left(x_n x + \Delta y_n y\right) \\ y_{n+1} & = & \frac{1}{2}\left(x_n y + y_n x\right) \end{array} \right.$$

En fait, comme $\Delta y^2 = x^2 - 4$ pour $(x, y) \in \mathcal{H}$, on peut presque écrire les coordonnées à l'aide exclusive de deux polynômes en $x$ ; par exemple, $[2]M$ a pour coordonnées

$$\left(\frac{1}{2}\left(x^2 + \Delta y^2\right), \frac{1}{2}\left(2xy\right)\right) = (x^2 - 2, xy).$$

À cet effet, posons $f_0 = 2$, $f_1 = X$, $g_0 = 0$, $g_1 = 1$, et pour tout $n \geqslant 2$, on définit les suites $(f_n)_{n\geqslant 0}$ et $(g_n)_{n\geqslant 0}$ par les relations

$$\left\{ \begin{array}{rcl} f_{n+1} & = & Xf_n - f_{n-1}, \\ g_{n+1} & = & Xg_n - g_{n-1}. \end{array} \right.$$

Le choix de $f_0$ et $g_0$ est motivé par $[0]M = O$ qui est de coordonnées (2,0). On remarque que les $f_n$ et $g_n$ sont des polynômes unitaires à coefficients entiers, de degrés respectifs $n$ et $n-1$, et ne dépendent pas de $\Delta$. Ces polynômes décrivent la multiplication par $n$ sur le groupe $\mathcal{H}$ :

***Proposition 2.21.*** — *Soit $M(x, y) \in \mathcal{H}$. Alors, $[n]M$ est de coordonnées $(f_n(x), yg_n(x))$.*

*Démonstration.* — On raisonne par récurrence. Les « petits » cas sont déjà traités. Supposons donc que le résultat est vrai jusqu'à un certain rang $n \geqslant 1$. Toujours par récurrence, il est aisé de vérifier que pour tout $n \geqslant 1$, on a

$$(X^2 - 4)g_n = Xf_n - 2f_{n-1}, \text{ et } 2g_{n+1} = f_n + Xg_n.$$

Je laisse le lecteur s'en charger. Alors, les coordonnées de $[n]M$ sont :

$$\left\{ \begin{array}{rcl} x_{n+1} & = & \frac{1}{2}\left(x_n x + \Delta y_n y\right) = \frac{1}{2}\left(xf_n(x) + (x^2-4)g_n(x)\right) = xf_n(x) - f_{n-1}(x) = f_{n+1}(x) \\ y_{n+1} & = & \frac{1}{2}\left(f_n(x)y + g_n(x)x\right) = \frac{1}{2}\left((2g_{n+1}(x) - xg_n(x))y + g_n(x)x\right) = yg_{n+1}(x) \end{array} \right.$$

et ceci achève la récurrence. □

Ceci permet de déterminer la torsion du groupe. Comme les $f_n$ et $g_n$ sont des polynômes non nuls, ils ont un nombre fini de racines, et l'équation $(f_n(x), yg_n(x)) = (2,0)$ a un nombre fini de solutions, il y a donc un nombre fini de points de $n$-torsion pour tout $n$. Pour être de torsion, on doit avoir $f_n(x) = 2$. Par exemple, pour $n = 2$, on doit avoir $x^2 - 4 = 0$, donc $x = \pm 2$, et on trouve que $\mathcal{T}(-2,0)$ est l'unique point d'ordre 2 de $\mathcal{H}$.

***Remarque 2.22.*** — Comme $f_n$ est, pour tout $n \geqslant 1$, un polynôme unitaire à coefficients entiers, on en déduit que les points de torsion sont entiers.

***Remarque 2.23.*** — On a $\mathcal{H}(\bar{\mathbb{Q}})[n] \simeq \mathbb{Z}/n\mathbb{Z}$ : il y a bien $n$ éléments car $f_n$ est de degré $n$, et l'étude de l'exemple précédent montre que $\mathcal{H}(\mathbb{Q})[n] \simeq \mathcal{H}_0(\bar{\mathbb{Q}})[n] \hookrightarrow \mathcal{H}_0(\bar{\mathbb{Q}}) \simeq \bar{\mathbb{Q}}^*$, où $\mathcal{H}_0$ est l'hyperbole d'équation $xy = 1$. Comme $\bar{\mathbb{Q}}^*$ est le groupe multiplicatif d'un corps, ses sous-groupes finis sont cycliques.

***Remarque 2.24.*** — On aura besoin de calculer $f_n'(2)$ pour la suite des évènements. De $f_{n+1} = Xf_n - f_{n-1}$, on tire $f_{n+1}' = f_n + Xf_n' - f_{n-1}'$. Une récurrence permet alors de démontrer que $f_n'(2) = n^2$. On a besoin pour cela de l'égalité $f_n(2) = 2$, que je justifie très bientôt. On peut aussi s'amuser à démontrer que $f_n''(2) = \frac{1}{6}n^2(n^2-1)$, ce qui ne servira pas pour démontrer la loi de réciprocité quadratique, mais peut servir pour déterminer $\left(\frac{2}{p}\right)$.

Comme $[n]M$ appartient à $\mathcal{H}$, on a $\Delta(yg_n(x))^2 = f_n(x)^2 - 4$, si et seulement si

$$(x^2-4)g_n(x)^2 = (f_n(x)-2)(f_n(x)+2) \Leftrightarrow (x-2)(x+2)g_n(x)^2 = (f_n(x)-2)(f_n(x)+2).$$

Ceci vaut pour une infinité de $x \in \mathbb{R}$, donc l'égalité est en fait polynomiale. Faisons un peu d'arithmétique dans $\mathbb{Z}[X]$, qui est factoriel. Les deux facteurs de droite sont premiers entre eux : si un diviseur premier divise ces deux facteurs, alors il divise 4, donc égale 2 ; or, 2 ne divise pas ces deux facteurs, puisqu'alors il diviserait $f_n$, qui est unitaire. De plus, $X - 2$ divise $f_n - 2$, car $f_n(2) - 2 = 0$ : ceci découle du fait que $[n]O = O$. À présent, prenons $n$ *impair*. Alors, comme $[n]\mathcal{T} = \mathcal{T} \neq O$, $X + 2$ ne divise pas $f_n - 2$, donc divise $f_n + 2$. Bref, on a :

$$g_n^2 = \frac{f_n - 2}{X - 2} \cdot \frac{f_n + 2}{X + 2},$$

qui est une égalité dans l'anneau factoriel $\mathbb{Z}[X]$, où les deux facteurs de droite sont premiers entre eux, et celui de gauche est un carré. Donc les facteurs de droite sont aussi des carrés, et on peut écrire

$$f_n - 2 = (X - 2)R_n^2,$$

toujours pour $n$ impair, où $R_n$ est un polynôme de degré $\frac{n-1}{2}$. Posons également, pour se simplifier la vie, $R_2 = X$. Les choses sérieuses commencent :

***Proposition 2.25.*** — *Soient $p$ et $q$ deux nombres premiers distincts, avec $p$ impair. Alors*

$$\left(\frac{p}{q}\right) = \prod_{R_p(a)=0} R_q(a).$$

Encore une fois, les racines sont à compter avec multiplicités, dans un corps de décomposition de $R_p$.

*Démonstration.* — Posons $L_{q,p} = \prod_{R_p(a)=0} R_q(a)$. Si $p$ ne divise pas $\Delta$ (ce qui est le cas si $\Delta = 8$ et $p \neq 2$), soit $\mathbb{F}_{p^k}$ « le » corps de décomposition de $\bar{R}_p$ sur $\mathbb{F}_p$ ($\bar{R}_p$ désigne la réduction modulo $p$ de $R_p$). Comme pour $f_p$, les racines de $\bar{R}_p$ représentent les abscisses des points de $p$-torsion de $\mathcal{H}(\mathbb{F}_{p^k})$. Or :

***Lemme 2.26.*** — *Le groupe $\mathcal{H}(\mathbb{F}_{p^k})$ a $p^k \pm 1$ éléments.*

*Démonstration du lemme.* — On considère l'application bijective de $\mathcal{H}$ dans $\mathcal{H}_0$ (défini par $xy = \Delta$), donnée par $M(x,y) \mapsto \left(\frac{x-2}{y}, \frac{x+2}{y}\right)$ si $M \neq O, \mathcal{T}$, de réciproque $N(u,v) \mapsto \left(\frac{2(v+u)}{v-u}, \frac{4}{v-u}\right)$ si $v \neq u$. Les éléments de $\mathcal{H}_0$ sont les couples $(x, \Delta x^{-1})$ où $x$ parcourt $\mathbb{F}_{p^k}^*$. Ceci fournit $p^k - 1$ éléments distincts de $\mathcal{H}_0$, donc $p^k - 1$ ou $p^k - 3$ éléments distincts de $\mathcal{H}$ *via* l'application birationnelle, selon que le cas de figure $x = \Delta x^{-1}$ se produise ou non ; il se produit si, et seulement si $\Delta$ est un carré dans $\mathbb{F}_{p^k}$, et dans ce cas il y a deux $x$ qui conviennent. En rajoutant $O$ et $\mathcal{T}$, on obtient $p^k \pm 1$ éléments. □

Revenons à la démonstration de la proposition : ce qui importe est de savoir que ce groupe ne peut pas avoir d'élément d'ordre $p$, donc l'unique racine de $\bar{R}_p$ dans $\mathbb{F}_{p^k}$ est 2, puis $\bar{R}_p = (X-2)^{(p-1)/2}$. Alors :

$$L_{q,p} = \prod_{\bar{R}_p(a)=0} \bar{R}_q(a) = \bar{R}_q(2)^{(p-1)/2} \equiv \left(\frac{\bar{R}_q(2)}{p}\right) \bmod p.$$

Il ne reste plus qu'à vérifier que $\bar{R}_q(2) = q$. Si $q = 2$, on sait déjà que $R_2(2) = 2$. Sinon, le développement en série de Taylor de $f_n$ en 2 est

$$f_n = 2 + n^2(X-2) + \frac{1}{12}n^2(n^2-1)(X-2)^2 + etc.,$$

donc celui de $R_n$ en 2, pour $n$ impair, est

$$\pm R_n = n + \frac{n(n^2-1)}{24}(X-2) + etc.,$$

et on trouve $R_n(2) = \pm n$ (le développement de $f_n$ à l'ordre 1 suffirait, l'ordre 2 nous sera utile pour la remarque en conclusion). Mais $R_n(2) \neq -n$, sinon $R_n$ aurait une racine réelle plus grande que 2 par le théorème des valeurs intermédiaires ($R_n(x) \to \infty$ quand $x \to \infty$), ce qui contredirait le fait que les points de torsion de $\mathcal{H}(\mathbb{Z})$ vérifient $x \leqslant 2$. Donc $R_n(2) = n$, et dans tous les cas on trouve $R_q(2) = q$. Ce qui prouve que $L_{q,p} \equiv \left(\frac{q}{p}\right) \bmod p$.

Pour finir la démonstration de la proposition (et donc de la loi de réciprocité quadratique), il ne reste plus qu'à démontrer que $L_{q,p} = \pm 1$. La multiplication par $[q]$ sur $\mathcal{H}(\mathbb{Z})$ est un automorphisme du groupe des points de $p$-torsion car $p$ et $q$ sont premiers entre eux, donc $f_q$ permute les racines de $R_p$. Alors,

$$\prod_{R_p(a)=0} (a-2) = \prod_{R_p(a)=0} (f_q(a)-2) = \prod_{R_p(a)=0} (a-2)R_q(a)^2.$$

En simplifiant par les facteurs $(a-2)$ (qui sont non nuls, car $R_p(2) = p \neq 0$), on obtient bien que $L_{q,p}^2 = 1$. □

***Remarque 2.27.*** — On a donc prouvé la loi de réciprocité quadratique. Si $q = 2$, alors le lemme 2.18 donne

$$\left(\frac{2}{p}\right) = L_{2,p} = (-1)^{(p-1)/2} R_p(0).$$

Pour déterminer le signe de $R_p(0)$, il suffit de déterminer $R_p(0)$ mod 4 (pour le lecteur : pourquoi ?). Or, le développement en série de Taylor à l'ordre 1 de $\pm R_p$ en 2, où on pose $X = 0$, fournit

$$R_p(0) = \begin{cases} +1 & \text{si } p \equiv 1{,}3 \bmod 8, \\ -1 & \text{si } p \equiv -1, -3 \bmod 8. \end{cases}$$

La valeur de $\left(\frac{2}{p}\right)$ en découle.

**2.3.2.** *Application cryptographique.* — Ce paragraphe part de l'heuristique suivante : quitte à s'autoriser quelques racines carrées, une conique de Pell-Fermat est isomorphe à l'hyperbole d'équation $xy = 1$ dont l'élément neutre est (1,1), elle-même isomorphe à $(A^*, \times)$ (si on considère ses points à coordonnées dans un anneau $A$) grâce à l'application $\left(x, \frac{1}{x}\right) \leftrightarrow x$. Ainsi, on est en droit de penser que les algorithmes de théorie des nombres fonctionnant, par exemple, dans le groupe multiplicatif de $\mathbb{Z}/p\mathbb{Z}$, auront un analogue avec les coniques. C'est effectivement le cas :

***Proposition 2.28.*** — *Soit $n \geqslant 5$ un entier naturel impair, et $\mathcal{C}$ la conique de Pell-Fermat d'équation $x^2 - \Delta y^2 = 4$, d'élément neutre $O(2{,}0)$, où on suppose que $\left(\frac{\Delta}{n}\right) = -1$ (symbole de Jacobi). L'entier $n$ est un nombre premier si, et seulement s'il existe un point $P \in \mathcal{C}(\mathbb{Z}/n\mathbb{Z})$ tel que*

— $[n+1]P = O$ ;

— $\left[\frac{n+1}{r}\right] P \neq O$ *pour tout diviseur premier $r$ de $n+1$.*

C'est un pendant géométrique du test de primalité de Lucas, qui serait le même énoncé en remplaçant $\mathcal{C}(\mathbb{Z}/n\mathbb{Z})$ par $\mathcal{H}(\mathbb{Z}/n\mathbb{Z})$ (et donc $(\mathbb{Z}/n\mathbb{Z})^*$ d'après la remarque préliminaire). Je reviendrai sur cette application lors de la comparaison avec les courbes elliptiques.

## 3. Un théorème à la Mordell-Weil

Dans toute cette section, $\mathcal{C}$ désigne une conique de Pell-Fermat d'équation affine $x^2 - \Delta y^2 = 4$, où $\Delta$ n'est pas un carré parfait.

Les énoncés et démonstrations qui suivent sont valables en remplaçant $\mathbb{Q}$ par un corps de nombres $K$, et $\mathbb{Z}$ par un anneau de $S$-entiers $\mathcal{O}_{K,S}$, mais pour fixer les idées et éviter d'introduire la théorie des hauteurs sur un corps de nombres quelconque, je reste sur $\mathbb{Z}$ et $\mathbb{Q}$ (quitte à ce que l'artillerie invoquée paraisse inutilement lourde, d'autant plus qu'on a déjà eu des résultats plus forts en procédant plus directement).

***Théorème 3.1*** **(Théorème de Mordell-Weil faible pour les coniques)**

*Le groupe $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z})$ est fini.*

***Corollaire 3.2*** **(Théorème de Mordell-Weil pour les coniques)**

*Le groupe $\mathcal{C}(\mathbb{Z})$ est de type fini : on a $\mathcal{C}(\mathbb{Z}) \simeq \mathbb{Z}^r \times \mathcal{C}(\mathbb{Z})_{\text{tors}}$ pour un certain entier $r \geqslant 0$.*

**3.1. Réduction du théorème de Mordell-Weil à sa forme faible.** — Pour montrer le corollaire à l'aide du théorème, on a besoin d'un lemme abstrait de théorie des groupes :

***Lemme 3.3.*** — *Soit $G$ un groupe abélien tel que $G/2G$ est fini. Supposons l'existence d'une fonction $h : G \to \mathbb{R}_+$ vérifiant :*

— *pour tout $c > 0$, l'ensemble $\{g \in G; h(g) < c\}$ est fini ;*

— *pour tout $g \in G$, on a $h(2g) = 2h(g)$ ;*

— *pour tous $g, g' \in G$, on a $h(g-g')^2 + h(g+g')^2 = 2(h(g)^2 + h(g')^2)$.*

*Alors $G$ est de type fini.*

*Démonstration du lemme.* — Soit $\Gamma$ un système de représentants de $G/2G$ ; par hypothèse, $\Gamma$ est fini. Tout $g \in G$ peut s'écrire $g - \gamma = 2g'$ pour un certain $\gamma \in \Gamma$ et pour $g' \in G$. Posons $c = \max_{\gamma \in \Gamma} h(\gamma)$.

Soit $\Omega$ le sous-groupe de $G$ engendré par tous les éléments de $\Gamma$ et par les éléments $g \in G$ vérifiant $h(g) \leqslant c$. On va montrer que $G = \Omega$ : si ce n'était pas le cas, on pourrait choisir $g \in G \setminus \Omega$, et le

supposer de hauteur minimale tant qu'à faire. En particulier, $h(g) > c$. En écrivant $g - \gamma = 2g'$ comme ci-dessus, on voit que $g'$ est de hauteur strictement plus petite :

$$4h(g')^2 = h(g-\gamma)^2 = 2(h(g)^2 + h(\gamma)^2) - h(g+\gamma)^2 \leqslant 2h(g)^2 + 2c^2 < 4h(g)^2.$$

La minimalité de $g$ impose $g' \in \Omega$, mais alors on aurait $g = 2g' + \gamma \in \Omega$ : absurde ! □

Une conique possède une telle fonction $h$ : pour un rationnel $r = \frac{m}{n}$ dont on a ici écrit la fraction irréductible, posons $H(r) = \ln(\max(|m|, |n|))$ et $H(0) = 0$. Pour un point $P(x, y) \in \mathcal{C}(\mathbb{Q})$, on pose $H(P) = H(x)$. Cette fonction $H$ vérifie presque les propriétés désirées par le lemme, à des constantes additives près. Pour s'en débarasser, il suffit de prendre à la place :

$$\hat{h}(P) = \lim_{n\to\infty} \frac{H([2^n]P)}{2^n}.$$

Cette fonction, qu'on appelle une *hauteur canonique*, vérifie toutes les propriétés désirées. On peut même la calculer explicitement : si $P(x, y) \in \mathcal{C}(\mathbb{Q})$, et qu'on écrit les coordonnées de $P$ sous la forme $x = \frac{r}{n}$ et $y = \frac{s}{n}$ avec $r$ et $s$ premiers entre eux (exercice : pourquoi est-ce possible quand $y \neq 0$ ?), alors :

$$\hat{h}(P) = \begin{cases} \ln(|n|) & \text{si } \Delta < 0, \\ \ln\left(\frac{|r|+|s|\sqrt{\Delta}}{2}\right) & \text{si } \Delta > 0. \end{cases}$$

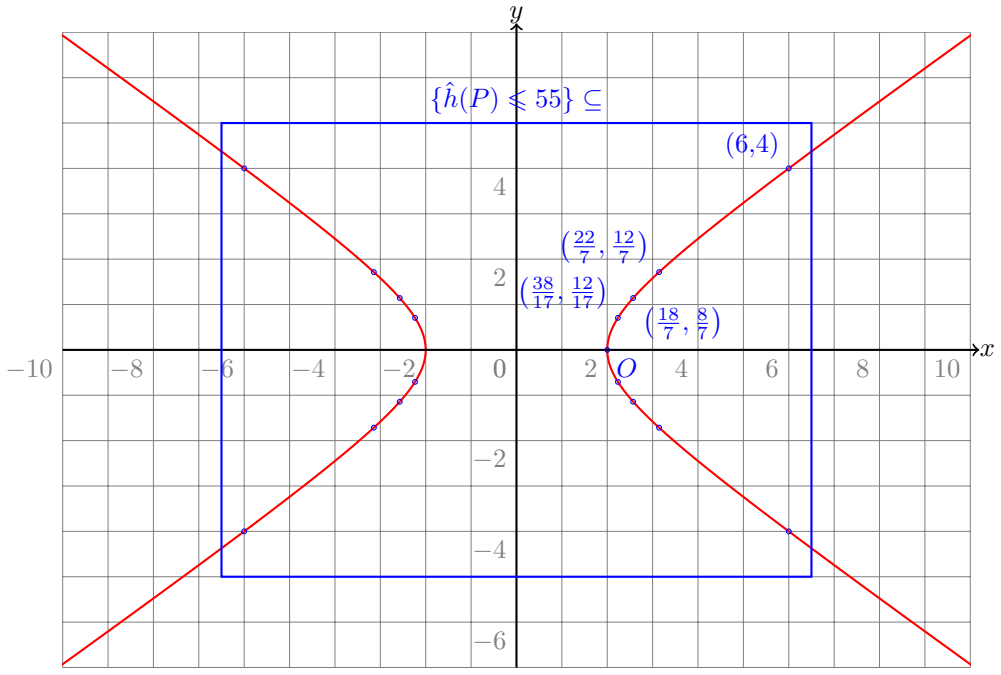



FIGURE 9. Points de hauteur inférieure à 55 sur la conique d'équation $x^2 - 2y^2 = 4$.

Pour plus de détails sur les propriétés mirifiques des hauteurs, il va falloir regarder du côté de [**Lem03**], voire de [**HS00**] pour un exposé plus systématique. On peut donc, théoriquement, trouver un algorithme trouvant tous les points de $\mathcal{C}(\mathbb{Z})$ de hauteur inférieure à une certaine quantité donnée. Ce qui pose problème est de trouver un système de générateurs pour $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z})$. Mais avant de se demander pourquoi c'est difficile, montrons sa finitude.

**3.2. Introduction sans douleur à la cohomologie galoisienne.** — Pour comprendre le groupe $\mathcal{C}(\mathbb{Q})$ (et plus tard $\mathcal{C}(\mathbb{Z})$, en vue de la démonstration du théorème ci-dessus), on s'intéresse d'abord aux points de la conique définis sur $\bar{\mathbb{Q}}$, où tout est particulièrement simple : on a la suite exacte suivante qui résume la situation,

$$1 \longrightarrow \mathcal{C}(\bar{\mathbb{Q}})[2] \longrightarrow \mathcal{C}(\bar{\mathbb{Q}}) \xrightarrow{[2]} \mathcal{C}(\bar{\mathbb{Q}}) \longrightarrow 1, \tag{5}$$

et en plus, on a vu que $\mathcal{C}(\bar{\mathbb{Q}})[2] = \{(\pm 2{,}0)\} = \mathcal{C}(\mathbb{Q})[2]$ ; la multiplication par [2] dans $\mathcal{C}(\bar{\mathbb{Q}})$ est surjective et $\mathcal{C}(\bar{\mathbb{Q}})/2\mathcal{C}(\bar{\mathbb{Q}})$ est trivial. En effet, il suffit de montrer que pour tout $Q(r,s) \in \mathcal{C}(\bar{\mathbb{Q}})$, l'équation $[2](x,y) = (r,s)$ a une solution $(x,y) \in \mathcal{C}(\bar{\mathbb{Q}})$. Comme $[2](x,y) = (x^2-2, xy)$, l'équation donne $x^2 = r+2$ et $s = xy$. Si $r \neq -2$, on obtient $(x,y) = \left(\pm\sqrt{r+2}, \pm\frac{s}{\sqrt{r+2}}\right)$, dont on vérifie l'appartenance à $\mathcal{C}(\bar{\mathbb{Q}})$.

Connaissant la situation sur $\bar{\mathbb{Q}}$, on souhaite la « descendre » à $\mathbb{Q}$, en mesurant ce qu'on perd ou gagne *via* ce procédé (en particulier, [2] n'est plus surjective, mais il faut voir « à quel point »). Passer de $\bar{\mathbb{Q}}$ à $\mathbb{Q}$ revient à considérer les points fixes de l'action du groupe de Galois absolu de $\mathbb{Q}$ sur $\mathcal{C}$, et mesurer la différence ainsi produite est typiquement un problème de cohomologie galoisienne, dont je vais parler aussi brièvement que possible.

Je ne compte pas trop parler de cohomologie des groupes pour le moment. Informellement, étant donnée une suite exacte de $G$-modules :

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1, \tag{6}$$

rien ne permet d'assurer qu'après avoir fait subir une transformation aux groupes $A$, $B$, $C$ (ici, on veut « passer » de $A$ au $G$-module $A^G$ des points fixes de $A$ sous l'action de $G$, *idem* pour $B$ et $C$), la suite restera exacte. Les groupes de cohomologie sont là pour pallier le défaut d'exactitude. Ainsi, si $G$ est un groupe, on pose

$\mathrm{H}^1(G, \bigstar) =$ le groupe mesurant l'obstruction des suites à rester exactes quand on remplace $\bigstar$ par $\bigstar^G$.

Plus rigoureusement (si j'ose me permettre...), il faudrait dire « la *première* obstruction », parce qu'il existe autant de groupes de cohomologie $\mathrm{H}^i(G,\cdot)$ qu'il y a d'entiers naturels $i$. La suite exacte ci-dessus deviendrait alors :

$$1 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} \mathrm{H}^1(G,A) \longrightarrow \mathrm{H}^1(G,B) \longrightarrow \mathrm{H}^1(G,C), \tag{7}$$

qui pourrait en fait se poursuivre à l'aide des $\mathrm{H}^2$, $\mathrm{H}^3$, *etc.* Le « morphisme de connexion » $\delta$ gagne souvent à être explicité, on le fera dans notre situation. Le théorème à connaître quand on parle de cohomologie galoisienne est le suivant :

***Théorème 3.4*** **(Théorème 90 de Hilbert).** — *Soit $G$ le groupe de Galois d'une extension galoisienne (éventuellement infinie) $L/K$. Ce groupe agit sur $L^*$ et il est donc légitime de considérer $\mathrm{H}^1(G, L^*)$. Ce groupe est trivial.*

Pour plus d'informations sur la cohomologie galoisienne, voir [**Sil09**] pour une référence simple d'accès et adaptée à notre étude, ou [**Ser94**] pour une référence plus complète et costaude.

**Démonstration du théorème de Mordell-Weil faible.** Revenons à notre théorème de Mordell-Weil faible. Si on applique la transformation « points fixes sous l'action de $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ » à la suite exacte (5), on obtient, en ne préservant que la séquence qui nous intéresse et en se souvenant que $\mathcal{C}(\bar{\mathbb{Q}})[2] \simeq \{\pm 1\}$ (même en tant que $G$-modules),

$$\mathcal{C}(\mathbb{Q}) \xrightarrow{[2]} \mathcal{C}(\mathbb{Q}) \longrightarrow \mathrm{H}^1(G, \{\pm 1\}) \longrightarrow \mathrm{H}^1(G, \mathcal{C}(\bar{\mathbb{Q}})) \xrightarrow{[2]} \mathrm{H}^1(G, \mathcal{C}(\bar{\mathbb{Q}})). \tag{8}$$

La détermination du groupe $\mathrm{H}^1(G, \{\pm 1\})$ est assez standard : on part de la suite exacte de Kummer

$$1 \longrightarrow \{\pm 1\} \longrightarrow \bar{\mathbb{Q}}^* \xrightarrow{[2]} \bar{\mathbb{Q}}^* \longrightarrow 1,$$

et on applique encore la transformation « points fixes sous l'action de $G$ ». Comme $\mathrm{H}^1(G, \bar{\mathbb{Q}}^*) = 1$ grâce au théorème de 90 de Hilbert, on résume la situation avec

$$\mathbb{Q}^* \xrightarrow{[2]} \mathbb{Q}^* \longrightarrow \mathrm{H}^1(G, \{\pm 1\}) \longrightarrow 1.$$

Comme $[2]\mathbb{Q}^* = \mathbb{Q}^{*2}$ (l'ensemble des carrés de rationnels), on obtient l'isomorphisme $\mathrm{H}^1(G, \{\pm 1\}) \simeq \mathbb{Q}^*/\mathbb{Q}^{*2}$. On a donc, à partir de la suite exacte (8), une application $\alpha : \mathcal{C}(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$. Il reste à expliciter l'image de ce morphisme de groupes, dans l'espoir d'en déduire la finitude de $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z})$.

**3.3. Détermination du noyau et de l'image du morphisme $\alpha$.** — En fait, il existe des théorèmes généraux de cohomologie pour expliciter les « morphismes de connexion » $C^G \to \mathrm{H}^1(G, A)$ dans une suite exacte (7) : pour $c \in C^G$, soit $b \in B$ un antécédent de $c$ par le morphisme $f : B \to C$ de la suite exacte ($f$ est surjective, donc $b$ existe), et posons $x(\sigma) = \sigma(b) - b \in A$ pour tout $\sigma \in G$. L'image de $c$ dans $\mathrm{H}^1(G, A)$ est alors $x$ (ou, plus précisément, une classe d'équivalence de $x$ pour une certaine relation, mais je n'ai pas défini rigoureusement $\mathrm{H}^1$).

On utilise d'abord cette méthode pour expliciter l'isomorphisme $\mathbb{Q}^*/\mathbb{Q}^{*2} \simeq \mathrm{H}^1(G, \{\pm 1\})$ issu de la suite de Kummer : la classe d'équivalence $a\mathbb{Q}^{*2}$ est envoyée sur l'application $x : G \to \{\pm 1\}$ définie par $x(\sigma) = \frac{\sigma(\sqrt{a})}{\sqrt{a}}$. Maintenant, pour définir le morphisme $\alpha : \mathcal{C}(\mathbb{Q}) \to \mathbb{Q}/\mathbb{Q}^*$, il faut réussir à déterminer le fameux antécédent $b$ pour $c$ du paragraphe précédent dans la suite exacte (8). Autrement dit, étant donné $P(r, s) \in \mathcal{C}(\mathbb{Q})$, je dois trouver $Q(x, y) \in \mathcal{C}(\bar{\mathbb{Q}})$ tel que $[2]Q = P$. Ce calcul a déjà été fait au début du paragraphe sur la cohomologie galoisienne, et on en déduit, en comparant sereinement les différents isomorphismes, que le morphisme $\alpha$ est défini par

$$\alpha(P(r, s)) = \begin{cases} (r+2)\mathbb{Q}^{*2} & \text{si } r \neq 2, \\ -\Delta\mathbb{Q}^{*2} & \text{si } r = -2. \end{cases}$$

Bien malin, celui qui aurait pu percevoir qu'il s'agit d'un morphisme de groupes immédiatement ! Le début de la suite exacte (8) montre que le noyau de $\alpha$ est $2\mathcal{C}(\mathbb{Q})$, et le noyau de la restriction de $\alpha$ à $\mathcal{C}(\mathbb{Z})$ est bien évidemment $2\mathcal{C}(\mathbb{Z})$. On a $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z}) \hookrightarrow \mathrm{im}(\alpha)$, et il ne reste plus qu'à montrer que l'image de $\alpha$ restreint à $\mathcal{C}(\mathbb{Z})$ est finie, on aura alors démontré la version faible du théorème de Mordell-Weil.

***Proposition 3.5.*** — *L'image de $\alpha_{|\mathcal{C}(\mathbb{Z})}$ est l'ensemble des classes $a\mathbb{Q}^{*2}$ telles que $ab = \Delta$, où l'équation $ar^2 - bs^2 = 4$ a une solution entière.*

Une fois cette proposition démontrée, il est évident que l'image est finie, et le théorème est démontré.

*Démonstration de la proposition.* — Si $ab = \Delta$ et $ar^2 - bs^2 = 4$ a une solution entière $(r, s)$, alors

$$(ar^2 - 2)^2 - \Delta(rs)^2 = (ar^2)^2 - 4ar^2 + 4 - ab(rs)^2 = ar^2(ar^2 - bs^2) - 4ar^2 + 4 = 4,$$

donc $P(ar^2 - 2, rs)$ est une solution de Pell-Fermat, et $\alpha(P) = a\mathbb{Q}^{*2}$. Inversement, si $a\mathbb{Q}^{*2} \in \mathrm{im}(\alpha_{|\mathcal{C}(\mathbb{Z})})$, alors il existe $P(x, y) \in \mathcal{C}(\mathbb{Z})$ tel que $\alpha(P) = a\mathbb{Q}^{*2}$. Montrons que $a$ divise $\Delta$, et que $ar^2 - bs^2 = 4$ admet une solution, où $b = \frac{\Delta}{a}$. On peut toujours supposer $a$ entier et sans facteur carré (en choisissant la partie *quadratfrei* de $x + 2$).

Comme $x^2 - \Delta y^2 = 4$, on peut aussi écrire $\Delta y^2 = (x-2)(x+2)$. Comme le plus grand diviseur commun de $x + 2$ et $x - 2$ divise 4, il y a trois possibilités :

- soit $x \equiv 1 \bmod 2$, donc $\Delta \equiv 5 \bmod 8$, $\mathrm{pgcd}(x-2, x+2) = 1$, donc $x+2 = ar^2$ et $x-2 = bs^2$, où $ab = \Delta$ et $r$, $s$ sont des entiers ; le $a$ est bien celui de $\alpha(P)$, par définition de $\alpha$. On a bien $ar^2 - bs^2 = 4$ ;
- soit $x \equiv 2 \bmod 4$, et dans ce cas $\mathrm{pgcd}(x-2, x+2) = 4$. On peut encore écrire $x + 2 = ar^2$ et $x - 2 = bs^2$ (avec $r$ et $s$ pairs), et encore une fois $ar^2 - bs^2 = 4$ ;
- soit $x \equiv 0 \bmod 4$ ; alors $\Delta = 4d$ avec $d \equiv 3 \bmod 4$, et $\mathrm{pgcd}(x-2, x+2) = 2$, et alors $x + 2 = 2Ar^2$, $x - 2 = 2Bs^2$ avec $AB = d$. En déduit que $ar^2 - bs^2 = 4$, avec $a = 2A$, $b = 2B$ et $ab = \Delta$.

Dans tous les cas, on a produit une solution entière à l'équation $ar^2 - bs^2 = 4$. □

Tout ceci, on l'a vu, suffit à démontrer le théorème de Mordell-Weil faible, puis le théorème de Mordell-Weil. De plus, l'image de $\alpha$ est finie dans $\mathbb{Q}^*/\mathbb{Q}^{*2} \simeq \prod_{r \in \mathbb{Q}} (\mathbb{Z}/2\mathbb{Z})$, donc son cardinal est de la forme $2^n$. Il est simple de constater que le rang de $\mathcal{C}(\mathbb{Z})$ est exactement $n - 1$. Cette observation est sans intérêt dans la recherche des points entiers (où $n = 2$, on l'a vu), mais le rang n'est pas connu en toute généralité si l'on remplace $\mathbb{Z}$ par l'anneau des entiers d'un corps de nombres plus grand que $\mathbb{Q}$.

**3.4. Recherche de générateurs.** — Le problème est, à présent, de trouver des générateurs de $\mathcal{C}(\mathbb{Z})$. Ceci revient à déterminer un système de représentants pour $\mathcal{C}(\mathbb{Z})/2\mathcal{C}(\mathbb{Z})$, d'après la section précédente. L'isomorphisme fourni par $\alpha$ montre que cela revient à trouver une solution à l'équation de Legendre $ar^2 - bs^2 = 4$, pour $a$ et $b$ des entiers vérifiant $ab = \Delta$. Il est donc important de bien

comprendre ces courbes ; notons-les $\mathcal{T}_a(\mathcal{C})$. On les appelle les courbes descendantes de la conique $\mathcal{C}$.

***Exemple 2.*** — Soit $\mathcal{C}(\mathbb{Z})$ la conique de Pell-Fermat définie par $x^2-205y^2=4$. Je vous laisse vous convaincre que trouver des solutions entières, hormis celle triviale (2,0) (qui correspond à un point entier sur $\mathcal{T}_a(\mathcal{C})$ également), n'est pas évident. Si on considère $T_5(\mathcal{C})$, d'équation $5r^2-41s^2=4$, on trouve après quelques essais la solution (3,1), qui induit la solution $(5r^2-2,rs)=(43,3)$ sur la conique de Pell-Fermat.

La recherche de points entiers sur $T_{41}(\mathcal{C})$ et $T_{205}(\mathcal{C})$ est plus délicate, et nécessiterait peut-être d'encore réduire la question à la recherche de points entiers sur d'autres courbes. Heureusement, la théorie des coniques de Pell-Fermat nous informe d'ores et déjà que $\mathcal{C}(\mathbb{Z})$ est de rang 1, donc $T_{41}(\mathcal{C})$ et $T_{205}(\mathcal{C})$ n'ont pas de point entier. Si on voulait trouver des générateurs pour les points entiers d'un corps de nombres, on ne pourrait pas s'affranchir d'une recherche approfondie sur ces courbes.

Maintenant, puisqu'on a trouvé un point entier (43,3), dont la théorie nous dit que c'est même un générateur libre de $\mathcal{C}(\mathbb{Z})$, on peut tous les produire :

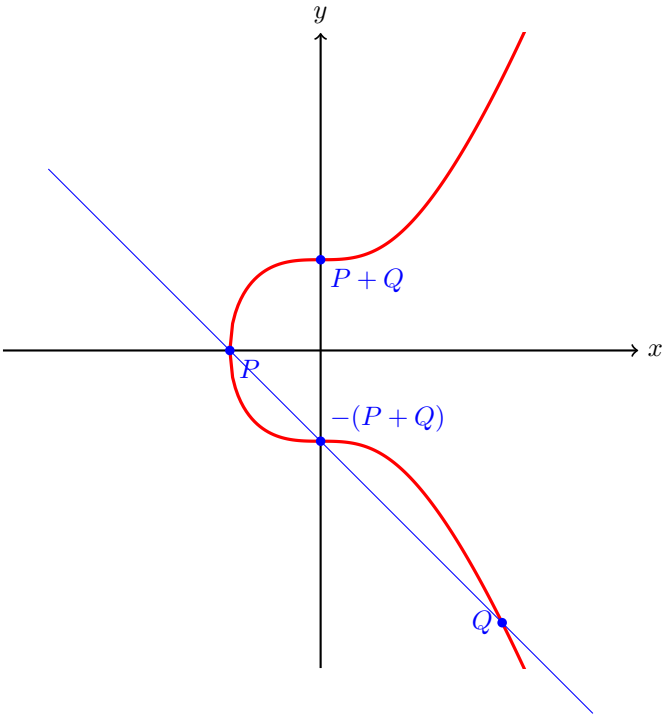
$$\mathcal{C}(\mathbb{Z})/\mathcal{C}(\mathbb{Z})_{\text{tors}} \simeq \langle(43,3)\rangle = \{(2,0),(43,\pm3),(1847,\pm129),(79378,\pm5544),(3411407,\pm238263),\dots\}$$

Plus généralement, savoir combien de courbes $\mathcal{T}_a(\mathcal{C})$ ont un point entier donne le cardinal de l'image de $\alpha$, donc le nombre de générateurs du groupe.

## 4. Analogies avec les courbes elliptiques

Pour simplifier, ici je définis une courbe elliptique $E$ par une équation affine de la forme $y^2=x^3+ax+b$, où $X^3+aX+b$ est un polynôme sans racine double. On définit une loi de groupe sur $E$ en demandant que $A+B+C=0$ si, et seulement si $A$, $B$ et $C$ sont alignés. On a besoin d'un point « à l'infini » pour considérer le cas des droites verticales (qui ne coupent $E$ qu'en deux points), on demande donc à voir $E$ comme une courbe projective. L'associativité n'est pas triviale, et dépend d'une forme simple du théorème de Bézout (comme c'était déjà le cas pour les coniques).

FIGURE 10. Une belle courbe elliptique et sa loi de groupe.



**4.1. Théorème de Mordell-Weil.** — Un théorème important sur les courbes elliptiques est le théorème de Mordell-Weil, qui se déduit lui aussi d'une version faible du théorème de Mordell-Weil :

***Théorème 4.1.*** — *Le groupe $E(\mathbb{Q})/2E(\mathbb{Q})$ est fini.*

***Théorème 4.2.*** — *Le groupe $E(\mathbb{Q})$ est de type fini : on a $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\mathrm{tors}}$ pour un certain entier $r \geqslant 0$.*

Ces deux résultats restent valables en remplaçant $\mathbb{Q}$ par un corps de nombres. En revanche, un théorème de Siegel montre que sur $\mathbb{Z}$, la situation n'a rien à voir avec celle des coniques, puisqu'il y a toujours un nombre fini de points entiers sur une courbe elliptique.

Il existe aussi une fonction de hauteur sur les courbes elliptiques, définie de la même manière essentiellement, mais je ne compte pas en parler ici. La démonstration du théorème de Mordell-Weil débute de la même manière : on suppose d'abord que l'ensemble des points de 2-torsion appartiennent à $\mathbb{Q}$ ; je ne le démontrerai pas, mais on peut toujours s'y ramener (dans le cas des coniques de Pell-Fermat, on n'avait pas à le supposer, la 2-torsion étant particulièrement simple et toujours définie sur $\mathbb{Q}$). On aboutit, semblablement, à la suite exacte :

$$E(\mathbb{Q}) \xrightarrow{[2]} E(\mathbb{Q}) \longrightarrow \mathrm{H}^1(G, E[2]) \longrightarrow \mathrm{H}^1(G, E(\bar{\mathbb{Q}})) \xrightarrow{[2]} \mathrm{H}^1(G, E(\bar{\mathbb{Q}})). \tag{9}$$

Comme $E[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$ sur $\mathbb{Q}$, ce n'est plus aussi simple de travailler avec $\mathrm{H}^1(G, E[2])$ : l'action de $G$ sur $E[2]$ est triviale, et on peut alors démontrer (avec une définition rigoureuse des $\mathrm{H}^1$...) que $\mathrm{H}^1(G, E[2])$ est l'ensemble des homomorphismes de $G$ dans $E[2]$. On déduit de la suite exacte et de cette description du $\mathrm{H}^1$ une injection $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathrm{Hom}(G, E[2])$. Malheureusement, ce dernier groupe est infini, et il est ardu de savoir quels sont ses éléments qui ont un antécédent dans $E(\mathbb{Q})/2E(\mathbb{Q})$. Pour remédier à ce problème, on travaille dans $\mathbb{Q}_p$, dont l'arithmétique est nettement plus simple que celle de $\mathbb{Q}$. Ceci nous mène à définir

$$\mathrm{Sel}_2(E) = \{x \in \mathrm{H}^1(G, E[2]) \ ; \ \beta(x) \in \mathrm{im}(\alpha)\},$$

où les morphismes $\alpha$ et $\beta$ sont définis ci-dessous :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & \mathrm{H}^1(G, E[2]) & \longrightarrow & \mathrm{H}^1(G, E)[2] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \beta} & & \downarrow & & \\
0 & \longrightarrow & \prod_{p \leqslant \infty} E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{\alpha} & \prod_{p \leqslant \infty} \mathrm{H}^1(\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p), E[2]) & \longrightarrow & \prod_{p \leqslant \infty} \mathrm{H}^1(\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p), E)[2] & \longrightarrow & 0
\end{array}$$

Ce diagramme montre que $E(\mathbb{Q})/2E(\mathbb{Q})$ est inclus dans $\mathrm{Sel}_2(E)$. En fait, si on définit le groupe de Tate-Shafarevich

$$Ш(E/\mathbb{Q}) = \ker\left(\mathrm{H}^1(G, E) \to \prod_{p \leqslant \infty} \mathrm{H}^1(\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p), E)\right),$$

alors on a la suite exacte suivante,

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathrm{Sel}_2(E) \longrightarrow Ш(E/\mathbb{Q})[2] \longrightarrow 0,$$

et il s'avère que le 2-groupe de Selmer est fini et calculable, donc $E(\mathbb{Q})/2E(\mathbb{Q})$ également. Par contre, $Ш(E/\mathbb{Q})$ est très mal connu en dehors de quelques cas particuliers, donc déterminer $E(\mathbb{Q})/2E(\mathbb{Q})$ explicitement est délicat.

**(à développer)**

**4.2. Fonctions L.** — Pour toute courbe sur $\mathbb{Q}$, donc en particulier les coniques et les courbes elliptiques, on peut définir des fonctions zdêta (ceci n'est pas une faute de frappe). Soit $C$ une conique ou une courbe elliptique, définie sur le corps fini $\mathbb{F}_p$. On appelle fonction zdêta de $C$ sur $\mathbb{F}_p$ la série formelle

$$\mathrm{Z}_p(T) = \exp\left(\sum_{r=1}^{\infty} \mathrm{card}(C(\mathbb{F}_{p^r}))\frac{T^r}{r}\right).$$

En posant $T = p^{-s}$, on obtient $\zeta_p(s)$. Le produit de ces fonctions $\zeta_p$ donne, en général, une fonction L aux propriétés intéressantes.

***Exemple 3* (Parabole).** — Reconsidérons la parabole d'équation $\mathcal{P} : y = x^2$, et $p$ un nombre premier impair (pour $p = 2$, nous n'avons plus une conique). Il est immédiat que $\mathcal{P}(\mathbb{F}_q) \simeq \mathbb{F}_q$, donc $\mathrm{card}(\mathcal{P}(\mathbb{F}_{p^r})) = p^r$, et un calcul très simple fournit $\mathrm{Z}_p(T) = \frac{1}{1-pT}$, $\zeta_p(s) = \frac{1}{1-p^{1-s}}$ et

$$\mathrm{L}(s, \mathcal{P}) = \prod_{p>2} \frac{1}{1-p^{1-s}} = \zeta(s-1)(1-2^{1-s}),$$

qui diffère très peu de la fonction zdêta de Riemann. Cette fonction L se prolonge où vous savez, et on a les valeurs spéciales $\mathrm{L}(1, \mathcal{P}) = 0$, ou encore $\mathrm{L}(0, \mathcal{P}) = \frac{1}{12}$. C'était très intéressant, merci. On va explorer un exemple plus éclairant.

***Exemple 4* (Courbe elliptique).** — Pour une courbe elliptique, un résultat profond permet d'obtenir

$$\mathrm{Z}_p(T) = \frac{P(T)}{(1-T)(1-pT)},$$

où $P(T) = qT^2 - a_pT + 1$, et $a_p = (p+1) - \mathrm{card}(E(\mathbb{F}_p))$, pour $p$ ne divisant pas le discriminant de $E$. Posons $\mathrm{L}_p(s) = \frac{1}{(1-p^{-s})(1-p^{1-s})}$, et $\mathrm{L}(s, E) = \prod_p \mathrm{L}_p(s)$. Le théorème de Taniyama-Shimura-Wiles assure que L peut être étendu analytiquement à tout le plan complexe, et vérifie une équation fonctionnelle ; ceci fait appel à la théorie des formes modulaires :

*Toute courbe elliptique (rationnelle) est encodée par une fonction L de forme modulaire (primitive).*

L'énoncé est, en vérité, plus précis que cela, mais ce n'est pas l'objet de cette étude. On a vu que dans le cas des coniques de Pell-Fermat, l'ordre d'annulation de $L$ en $s = 0$ donnait le rang du groupe sur la conique. De manière analogue, une conjecture de Birch et Swinnerton-Dyer, qui fait partie des problèmes du millénaire, prédit que l'ordre d'annulation de $\mathrm{L}(s, E)$ en $s = 1$ donne le rang du groupe $E(\mathbb{Q})$. Plus précisément, on pense que

$$\lim_{s\to 1} (s-1)^{-r} \mathrm{L}(s, E) = \frac{\Omega \cdot \mathrm{card}(Ш(E/\mathbb{Q})) \cdot R(E/\mathbb{Q}) \cdot \prod_p c_p}{(\mathrm{card}(E(\mathbb{Q})_{\mathrm{tors}}))^2},$$

où $r$ est le rang du groupe $E(\mathbb{Q})$, puis $\Omega$, $R(E/\mathbb{Q})$ et $c_p$ des quantités que je ne veux pas définir et $Ш(E/\mathbb{Q})$ le groupe de Tate-Shafarevich.

***Exemple 5* (Conique de Pell-Fermat).** — Reprenons l'exemple fil-rouge des coniques de Pell-Fermat. Pour la conique d'équation $x^2 - \Delta y^2 = 4$, le calcul du nombre de points dans $\mathbb{F}_q$ a été fait dans la démonstration du lemme 2.26, et une analyse plus approfondie de la démonstration montre que c'est plus précisément $q - \left(\frac{\Delta}{p}\right)^{\dim(\mathbb{F}_q/\mathbb{F}_p)}$. Si $q = p$, c'est clair d'après la définition du symbole de Legendre, et sinon, il suffit de remarquer que si $\Delta$ n'est pas un carré dans $\mathbb{F}_p$, alors $\Delta$ et un carré dans $\mathbb{F}_q$ si, et seulement si $\mathbb{F}_{p^2} \simeq \mathbb{F}_p(\sqrt{\Delta}) \subseteq \mathbb{F}_q$, ce qui impose que la dimension de $\mathbb{F}_q$ sur $\mathbb{F}_p$ soit paire [†]. Un petit calcul donne donc :

$$\mathrm{Z}_p(T) = \exp\left(\sum_{r=1}^{\infty} \left(p^r \frac{T^r}{r} - \left(\frac{\Delta}{p}\right)^r \frac{T^r}{r}\right)\right) = \exp(-\ln(1-pT) + \ln(1-\chi(p)T)) = \frac{1-\chi(p)T}{1-pT},$$

où $\chi$ est le caractère de Dirichlet défini par $\chi(p) = \left(\frac{\Delta}{p}\right)$ [‡].

Votre serviteur calcule aussi la fonction L associée par analogie avec la fonction L des courbes elliptiques, pour obtenir

$$\mathrm{L}(s, \chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}},$$

†. Si on ose utiliser la géométrie projective, on pourrait aussi, simplement, utiliser le fait que la conique projective associée est en bijection avec $\mathbb{P}^1(\mathbb{F}_q)$, donc a $q+1$ points. Pour obtenir la conique affine, on n'a qu'à compter les points à l'infini à retirer, et ces points à l'infini sont $(\pm\sqrt{\Delta},1)$.

‡. Ce résultat ne contredit pas le théorème de Weil sur les fonctions $\mathrm{Z}_p$, qui énonce que pour une courbe projective lisse de genre $g$, alors $\mathrm{Z}_p(T) = \frac{P(T)}{(1-T)(1-pT)}$ où $P(T)$ est de degré $2g$. En effet, on travaille ici avec une conique *affine* ; en ajoutant les points à l'infini, on obtient bien le résultat énoncé ici en note de pied de page.

qui est la fonction L de Dirichlet associée au caractère quadratique $\chi = \left(\frac{\Delta}{\cdot}\right)$. On vient de voir :

*Toute conique de Pell-Fermat est encodée par une fonction* L *de Dirichlet.*

Précisons cette affirmation. Un résultat de toute beauté est la valeur (non nulle) de cette fonction L en $s = 1$ :

$$\mathrm{L}(1,\chi) = \begin{cases} h \cdot \frac{2\pi}{w\sqrt{|\Delta|}} & \text{si } \Delta < 0, \\ h \cdot \frac{2\ln(\varepsilon)}{\sqrt{|\Delta|}} & \text{si } \Delta > 0, \end{cases}$$

où $w$, $h$ et $\varepsilon > 1$ sont respectivement le nombre de racines de l'unité, le nombre de classes et l'unité fondamentale de $\mathbb{Q}(\sqrt{\Delta})$. On tient encore là un des miracles de la théorie des nombres : si $\Delta > 0$, on a un générateur du groupe $\mathcal{C}(\mathbb{Z})$ qu'on a vu être de rang 1 ; à l'aide d'informations locales (le nombre de points sur $\mathcal{C}$ après réduction modulo $p$), on a construit un objet un objet global (une fonction entière) dont une valeur spéciale donne un générateur de $\mathcal{C}(\mathbb{Z})$, à une puissance $h$ près. Grâce à l'équation fonctionnelle vérifiée par L, on peut réécrire cette égalité ainsi :

$$\lim_{s\to 0} s^{-r}\mathrm{L}(s,\chi) = \frac{2hR}{w},$$

où $r = 0$ et $R = 1$ pour $\Delta < 0$, et $r = 1$ et $R = \ln(\varepsilon)$ si $\Delta > 0$. On remarque que l'ordre d'annulation de L en 0 donne le rang de la conique.

**4.3. Tests de primalité.** — Pour une conique de Pell-Fermat, nous avons vu dans la proposition 2.28 un test de primalité basé sur leur arithmétique modulo $n$. Si on prend le cas particulier $n = 2^p - 1$ ($n$ est un nombre de Mersenne), alors $n \equiv 7 \bmod 12$ pour $p \geqslant 3$, et alors $\left(\frac{3}{n}\right) = -1$. Pour un choix de conique d'équation affine $x^2 - 12y^2 = 4$ et $P(4,1)$, alors ce test n'est rien d'autre que le test de Lucas-Lehmer :

***Proposition 4.3* (Test de Lucas-Lehmer).** — *Définissons une suite $(s_i)_{i\geqslant 0}$ définie par $s_0 = 4$ et $s_i = s_{i-1}^2 - 2$. Alors $n = 2^p - 1$ est premier si, et seulement si $s_{p-2} \equiv 0 \bmod n$.*

Gross a également élaboré un test de primalité pour les nombres de Mersenne, cette fois-ci basé sur les courbes elliptiques :

***Proposition 4.4* ([Gro05]).** — *Définissons une suite $(s_i)_{i\geqslant 0}$ définie par $s_0 = -2$ et*

$$s_i = \frac{(s_{i-1}^2 + 12)^2}{4s_{i-1}(s_{i-1}^2 - 12)}.$$

*Alors $n = 2^p - 1$ est premier si, et seulement si $s_k(s_k^2 - 12)$ est premier à $n$ pour tout $k$ entre 0 et $p - 2$, et* $\mathrm{pgcd}(s_{p-1}, n) > 1$.

**(à développer)**

## Références


[Gro05] B. H. Gross – « An elliptic curve test for Mersenne primes », *J. Number Theory* **110** (2005), no. 1, p. 114–119.

[HS00] M. Hindry & J. H. Silverman – *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction.

[Lem03] F. Lemmermeyer – « Conics – a poor man's elliptic curves », 2003.

[Ser94] J.-P. Serre – *Cohomologie galoisienne*, fifth éd., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994.

[Sha01] P. Shastri – « Integral points on the unit circle », *J. Number Theory* **91** (2001), no. 1, p. 67–70.

[Sil09] J. H. Silverman – *The arithmetic of elliptic curves*, second éd., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Tan96] L. Tan – « The group of rational points on the unit circle », *Math. Mag.* **69** (1996), no. 3, p. 163–171.


**(la bibliographie est incomplète ; bien référencer tous les papiers de Lemmermeyer *etc.*)**

Bruno Winckler