Algorithmique des courbes elliptiques

Master de Mathématiques et Applications

Fabien NARBONNE et Reynald LERCIER

Février 2024

Université de Rennes

Table des matières

I Courbes elliptiques

Introduction

Comme leur nom l'indique, les courbes elliptiques sont des objets issus de la géométrie. Une spécificité remarquable de ces courbes est qu'elles peuvent être munies d'une structure de groupe compatible avec leur structure géométrique. Ce sont en fait les seules courbes (projectives) ayant cette propriété. On peut donc appliquer à ces objets un vaste éventail d'outils issus de différentes théories (géométrie algébrique, théorie des groupes, théorie des nombres, *etc.*). Les courbes elliptiques interviennent dans de nombreux problèmes : factorisation rapide d'entiers, empilement de sphères de dimension n, nombres congruents, cryptographie, *etc.*. L'utilisation moderne la plus spectaculaire des courbes elliptiques est probablement la démonstration du grand théorème de Fermat en 1994 par Andrew Wiles (l'idée clé de sa démonstration était la démonstration d'une partie de la conjecture de Shimura-Taniyama-Weil qui porte sur les courbes elliptiques).

Cette partie comporte 3 chapitres. Le chapitre 1 sert à développer les outils nécessaires à la manipulation des courbes elliptiques (courbes planes, géométrie projective, morphismes, diviseurs). Beaucoup de texte d'initiation aux courbes elliptiques n'abordent pas la théorie des diviseurs. On a fait le choix de le faire ici car, étant donnée une courbe C, le groupe $\mathrm{Pic}^0(C)$ peut être considéré comme une généralisation du groupe $(E,+)$ pour des courbes de genre différent de 1 (lorsque $C = E$, $\mathrm{Pic}^0(E) \simeq E$) et on peut donc faire de la cryptographie dessus lorsque C est définie sur un corps fini (voir [Kob89] par exemple).

Dans le chapitre 2, on introduit les courbes elliptiques et on développe les outils de base nécessaires à leur étude sur un corps quelconque (structure de groupe, discriminant, j-invariant, torsion, isogénies).

Dans le chapitre 3, on s'intéresse spécifiquement à l'étude des courbes elliptiques définies sur un corps fini. L'étude du morphisme de Frobenius d'une telle courbe fournit des résultats puissants sur son nombre de points rationnels.

Dans l'appendice A, on propose des rappels très généraux sur les corps finis.

Il s'agit de notes de cours et il existe bien entendu des références plus complètes. Pour ceux ou celles qui souhaitent en savoir plus sur les courbes elliptiques ou qui veulent lire des preuves complètes des résultats énoncés, on recommande les références ci-dessous.

- Un cours d'introduction aux courbes elliptiques donné au Massachusetts Institute of Technology [Sut17].
- La seconde édition [Mil06] des notes de cours de James Milne de 2006 (disponibles sur son site).
- Le célèbre texte de Silverman [Sil09], moins accessible mais très clair et complet.

1. Géométrie projective et affine

Dans ce chapitre, nous allons voir deux types de géométrie. Une géométrie très classique et intuitive qui consiste à travailler dans l'*espace affine* $\mathbb{A}^n(k) = k^n$ où k est un corps. Malheureusement, travailler en affine pose de nombreux problèmes. Par exemple, deux droites parallèles ne se coupent pas ou, si $k = \mathbb{R}$ ou $\mathbb{C}$, alors k^n n'est pas compact [1]. Nous introduisons donc un nouvel espace, noté $\mathbb{P}^n(k)$, qui est k^n à qui on rajoute des points « à l'infini ». À l'instar de $\mathbb{A}^n$, l'*espace projectif* $\mathbb{P}^n$ est de dimension n mais deux droites quelconques se coupent toujours, et $\mathbb{P}^n(\mathbb{R})$ et $\mathbb{P}^n(\mathbb{C})$ sont compacts.

Les objets qui nous intéressent sont les courbes elliptiques. Comme nous le verrons au chapitre 2, ce sont des courbes dans $\mathbb{P}^2$. Nous concentrons donc nos efforts sur $n = 2$, ce qui simplifie légèrement la tâche. Cependant, la majorité de ce que nous définissons dans la section 1.1 est vrai pour n quelconque.

1.1 Géométrie affine

1.1.1 Courbes planes

Soit k un corps et $\bar{k}$ une clôture algébrique de k. On rappelle que l'anneau des polynômes à n indéterminées $k[X_1, \dots, X_n]$ est *factoriel*, c'est-à-dire que tout élément $f \in k[X_1, \dots, X_n]$ se factorise toujours en un produit d'irréductibles

$$f = f_1^{m_1} \cdots f_r^{m_r}, \tag{1.1}$$

où $f_i \neq \lambda f_j$ pour tout $\lambda \in k^* = k \setminus \{0\}$ et $i \neq j$. Cette factorisation est unique à une permutation près des f_i et à une multiplication près par une constante non nulle des f_i. Lorsque la factorisation de f dans $\bar{k}[X, Y]$ est sans facteur carré, *i.e.* $m_i \leq 1$ pour tout i, on dit que f est *géométriquement réduit* [2].

Définition 1.1 L'*espace affine* de dimension n sur k est $\mathbb{A}^n(k) = k^n$. Le *plan affine* sur k est $\mathbb{A}^2(k) = k^2$.

Soit $f \in k[X, Y]$ un polynôme géométriquement réduit. La *courbe affine plane* C_f sur k est l'ensemble des solutions dans $\bar{k}$ de l'équation $f(x, y) = 0$. Pour toute extension de corps $k \to K$, on pose $C_f(K) = \{(x, y) \in K^2,\ f(x, y) = 0\}$, et on appelle cet ensemble les points *K-rationnels* de C_f. On parle souvent des points rationnels pour désigner les points k-rationnels. On appelle degré de C_f le degré de f.

1. On précise $k = \mathbb{R}$ ou $\mathbb{C}$ car ça n'a pas de sens, *a priori*, de parler de compacité pour un corps k général.
2. En géométrie algébrique, « géométriquement » signifie souvent « sur $\bar{k}$ ».

Rq Il est important de bien comprendre pourquoi on définit la courbe sur k comme l'ensemble des points $\bar{k}-$rationnels. Prenons par exemple les polynômes $f(X,Y)=X^2+Y^2+1$ et $g(X,Y)=X^4+Y^4+1$ dans $\mathbb{R}[X,Y]$. Les deux courbes correspondantes n'ont aucun point rationnel, *i.e.* $C_f(\mathbb{R})=C_g(\mathbb{R})=\emptyset$; leur points rationnels ne permettent pas de les distinguer pourtant leur géométrie sur $\mathbb{C}$ est très différente.

Rq Il peut-être déstabilisant qu'on utilise une notation aussi compliquée que $\mathbb{A}^n(k)$ pour désigner un objet aussi simple que k^n . La raison est qu'il faut considérer $\mathbb{A}^n$ comme un objet géométrique au même titre qu'une courbe et $\mathbb{A}^n(K)$ est simplement les points K-rationnels de $\mathbb{A}^n$. L'avantage est de pouvoir écrire des choses comme $C\longrightarrow\mathbb{A}^1$ qui signifie que pour tout corps K on a une application $C(K)\longrightarrow\mathbb{A}^1(K)=K$. Il en est de même pour les espaces projectifs que nous voyons ensuite.

Lorsque f est irréductible dans $k[X,Y]$, *i.e.* $r=1$ dans l'équation (1.1), on dit que C_f est *irréductible*. Lorsque f est irréductible dans $\bar{k}[X,Y]$ on dit que C_f est *géométriquement irréductible*. Si $f=f_1\cdots f_r$ on voit que pour tout $k\subseteq K$ on a

$$C_f(K)=C_{f_1}(K)\cup\cdots\cup C_{f_r}(K).$$

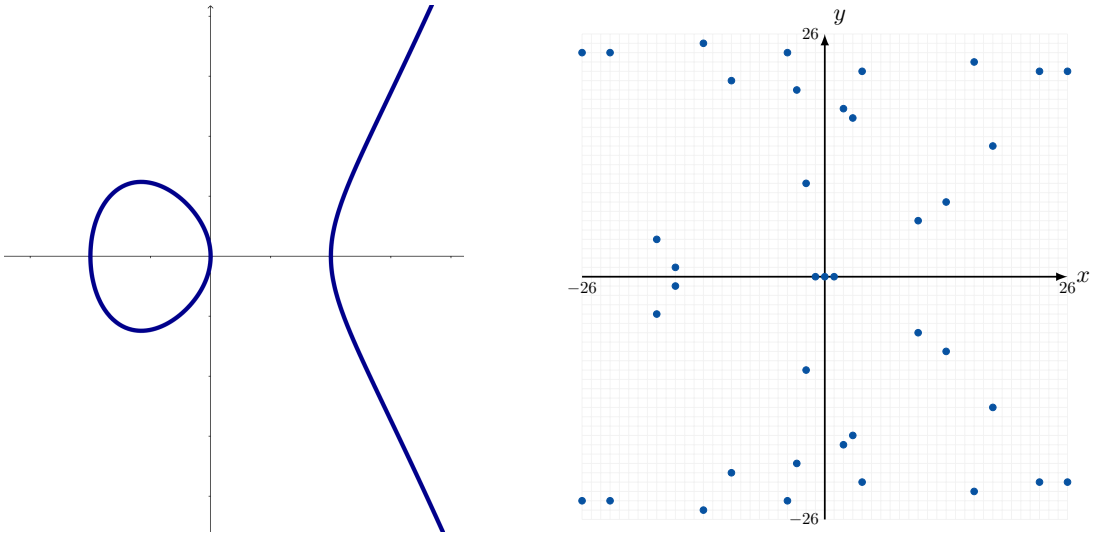
En d'autres termes une courbe quelconque C_f est toujours une union finie de courbes irréductibles appelées les composantes irréductibles de C_f .

■ **Exemple 1.2 — Droites.** Si on considère f de degré 1, *i.e.* $f(X,Y)=aX+bY+c$ où a ou b est non nul on a une équation de droite. Les droites sont donc des courbes affines planes. ■

■ **Exemple 1.3 — Conique.** Si on considère f de degré 2, *i.e.* $f(X,Y)=aX^2+bY^2+cXY+eX+fY+d$ avec a,b ou c non nul ça donne l'équation d'une conique (sur $k=\mathbb{R}$ on les appelle ellipse, parabole ou hyperbole).

Considérons $f(X,Y)=X^2+Y^2$ sur $\mathbb{R}$, c'est un polynôme irréductible sur $\mathbb{R}$ donc C_f est irréductible en revanche $f(X,Y)=(X+iY)(X-iY)\in\mathbb{C}[X,Y]$, donc C_f n'est pas géométriquement irréductible. ■

■ **Exemple 1.4 — Cubique.** Lorsque f est de degré 3, une courbe C_f est appelée une *cubique*. ■



(a) Sur $\mathbb{R}$ (b) Sur $\mathbb{F}_{53}$

FIGURE 1.1 – Points rationnels de la courbe $y^2=x^3-x$

■ **Exemple 1.5 — Courbes de Fermat-Wiles.** Considérons $n \geq 3$ et $f(X,Y) = X^n + Y^n - 1$ sur $\mathbb{Q}$. Une solution rationnelle $(\alpha/\alpha', \beta/\beta')$ avec $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}$ donne $(\alpha/\alpha')^n + (\beta/\beta')^n = 1$, c'est-à-dire

$$a^n + b^n = c^n \text{ avec } a = \alpha\beta',\ b = \beta\alpha',\ c = \alpha'\beta'.$$

Réciproquement, on voit facilement qu'une solution entière de $a^n + b^n = c^n$ donne un point $\mathbb{Q}$-rationnel de C_f.

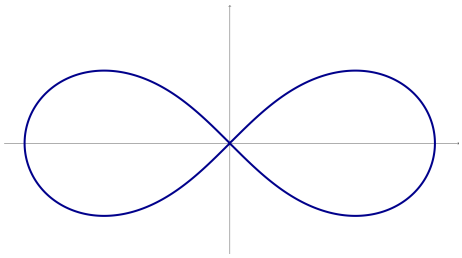
La question de l'existence de telles solutions a été soulevée pour la première fois par Fermat au 17-ème siècle et ce n'est qu'en 1994 que le mathématicien Andrew Wiles a proposé une démonstration du fait qu'il n'existe aucune solution entière non-triviale [3] de $a^n + b^n = c^n$. Il est intéressant de noter que les courbes elliptiques ont joué un rôle central dans la preuve de Wiles.

L'étude des points rationnels d'une courbe algébrique peut donc se révéler être un problème extrêmement difficile. ■

■ **Exemple 1.6 — Courbe elliptique affine.** Considérons la courbe C_f où $f(X,Y) = Y^2 - X^3 + X$ sur un corps k. C'est une cubique. L'ensemble de ses points rationnels est représenté sur la figure 1.1 pour $k = \mathbb{R}$, puis $k = \mathbb{F}_{53}$.

■

■ **Exemple 1.7 — Autres exemples de tracés réels.** On donne quelques exemples de courbes réelles « jolies » sur la figure 1.2. ■



(a) Lemniscate de Bernoulli $(x^2+y^2)^2 = x^2 - y^2$

(b) Cardioïde $(x^2+y^2-x)^2 = x^2+y^2$ (au fond de votre tasse préférée)

FIGURE 1.2 – Courbes remarquables

1.1.2 Tangentes et points singuliers des courbes affines

Soit $a, b \in k$. Lorsqu'on écrit un polynôme $f \in k[X,Y]$ dans la base $(X-a, Y-b)$ de l'algèbre $k[X,Y]$, on a

$$f(X,Y) = f(a,b) + u_{(a,b)}(X-a) + v_{(a,b)}(Y-b) + \text{ termes de degré } \geq 2.$$

Il s'agit du développement de Taylor de f en (a,b), on a $u_{(a,b)} = \partial f/\partial X(a,b)$ et $v_{(a,b)} = \partial f/\partial Y(a,b)$.

3. Les solutions non-triviales sont celles pour lesquelles a et b sont tous deux non-nuls.

Lorsque $P=(a,b)$ est un point de $C_f(K)$, *i.e.* $f(a,b)=0$, on dit que P est un point *singulier* lorsque

$$\frac{\partial f}{\partial X}(P)=\frac{\partial f}{\partial Y}(P)=0.$$

Si P n'est pas singulier, il est dit *non-singulier* ou *lisse*[4]. Dans ce cas, le polynôme $T_P=\partial f/\partial X(P)\cdot(X-a)+\partial f/\partial Y(P)\cdot(Y-b)$ de degré 1 définit une droite C_{T_P} appelée *droite tangente* à C_f en P. Une courbe sans point singulier est dite *non-singulière* ou *lisse*.

Exercice 1.8 — (★).

1. Parmi les courbes données dans les exemples 1.2 à 1.7, lesquelles sont lisses ? (certains points singuliers se voient facilement quand la courbe présente un croisement ou un point de rebroussement comme celui de la cardioïde)
2. Montrer que la courbe d'équation $y^3=x^5$ a un point singulier en $(0,0)$. (pourtant son graphe a l'air lisse !)
3. Montrer que le point $(2,i\sqrt{3})$ est un point singulier de la courbe d'équation $(x-2)(x^2+y^2-1)=0$ définie sur $\mathbb{R}$ (il s'agit de l'union de la droite verticale $x=2$ et du cercle unité centré en $(0,0)$). Il faut donc faire attention au fait que les singularités peuvent être sur une extension du corps que l'on considère. ■

Exercice 1.9 — (★★).

Montrer que la courbe sur k de caractéristique $\neq 2$ d'équation $y^2=x^3+ax+b$ admet un point singulier si et seulement si $4a^3+27b^2=0$ (on peut utiliser le fait que le discriminant de x^3+ax+b est $-4a^3-27b^2$). ■

1.2 Géométrie projective

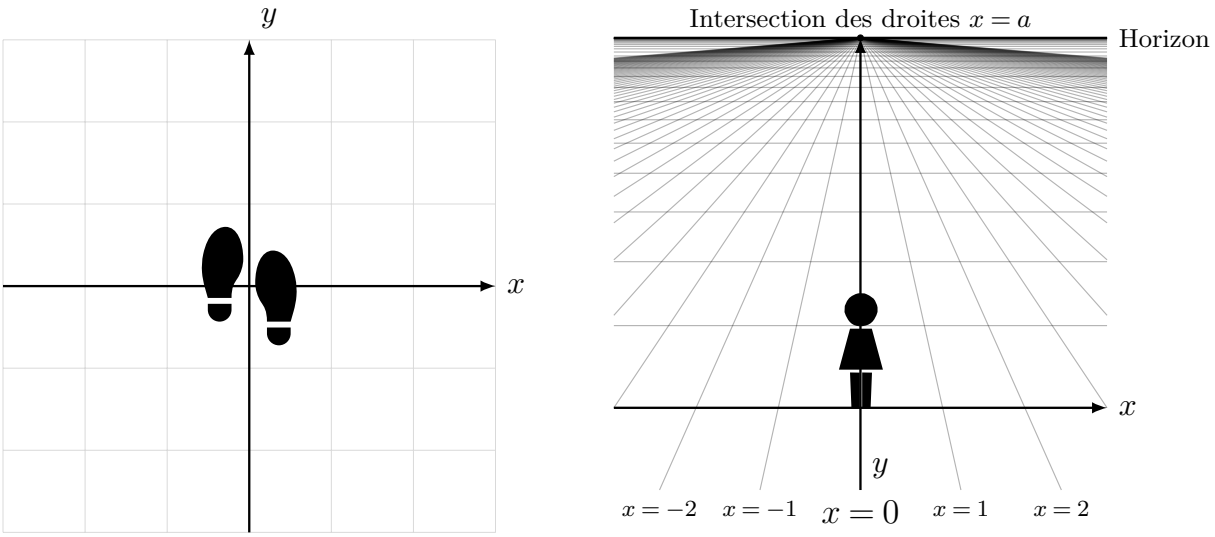
Bien qu'on puisse très facilement se représenter et travailler dans $\mathbb{A}^2$ cet espace présente de nombreux défauts. Nous souhaitons ici présenter l'espace $\mathbb{P}^2$ qui sert d'espace ambiant aux objets que nous manipulerons ensuite, en particulier les courbes elliptiques. Nous commençons par présenter une approche intuitive de cet espace. On va voir que, bien qu'on ne puisse pas se représenter entièrement[5] $\mathbb{P}^2(\mathbb{R})$, on peut tout de même en apercevoir des morceaux.

1.2.1 L'intuition projective : perspective et horizon

Une motivation pour introduire $\mathbb{P}^2$ peut être le théorème de Bézout qui affirme que deux courbes planes sur k sans composante commune de degrés respectifs n et m se coupent en exactement nm points $\bar{k}$-rationnels. Ce théorème présente un contre-exemple immédiat : les droites sont de degré 1 et deux droites parallèles ne s'intersectent pas. Puisque nous voulons qu'elles se croisent pour rendre correct ce théorème[6], inventons ce point qui nous manque.

Imaginons que nous sommes debout sur un plan infini quadrillé. Si l'on regarde sous nos pieds, nous voyons la même chose que sur la figure 1.3a. En revanche, si l'on regarde droit devant vous, nous voyons la même chose que sur la figure 1.3b. Lorsque l'on regarde dans une direction, toutes les droites pointant dans cette direction semblent se croiser en un unique point situé sur l'horizon. C'est la vue en perspective.

4. En anglais *smooth*.
5. Et ce n'est pas la peine d'essayer ; il n'existe aucun plongement de $\mathbb{P}^2(\mathbb{R})$ dans $\mathbb{R}^3$!
6. Pour une superbe introduction au théorème de Bézout, aux courbes planes et à $\mathbb{P}^2(\mathbb{R})$, on recommande la vidéo de la chaîne El Jj [ElJ16].



(a) Plan affine (b) Plan projectif

FIGURE 1.3 – Géométrie plane

C'est ainsi que l'on peut se représenter intuitivement $\mathbb{P}^2(\mathbb{R})$. Il s'agit du plan $\mathbb{R}^2$ auquel on rajoute une droite à l'infini ; l'horizon. Malheureusement, rajouter cette droite à l'infini ne suffit pas. En effet, si vous vous retournez, les mêmes droites parallèles semblent se croiser aussi en un point situé sur l'horizon, à l'opposé. Puisqu'on veut que les droites se croisent en un unique point il faut donc identifier ces deux points. On note $\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup L_\infty$ pour désigner l'union du plan et de la ligne d'horizon (quotientée).

Nous allons donné un sens rigoureux à cette ligne d'horizon, à ces points, et nous verrons que, dans notre définition, ces deux points sont identiques.

1.2.2 Le formalisme projectif

Soit k un corps quelconque. On appelle *espace projectif* de dimension n sur k l'ensemble des droites vectorielles de k^{n+1} et on le note $\mathbb{P}^n(k)$. Cette définition est simple mais manque de coordonnées. On préfère celle-ci qui est équivalente $\mathbb{P}^n(k) = k^{n+1}/\sim$, où $\sim$ est la relation d'équivalence sur $k^{n+1} \setminus \{0\}$ donnée par

$$v \sim w \text{ si et seulement s'il existe } \lambda \in k \setminus \{0\},\ v = \lambda w.$$

On note $[x_0 : \ldots : x_n]$ la classe d'un vecteur $(x_0, \ldots, x_n) \in k^{n+1} \setminus \{0\}$ dans le quotient $\mathbb{P}^n(k)$. On a alors, par définition, pour tout $\lambda \in k \setminus \{0\}, [\lambda x_0 : \ldots : \lambda x_n] = [x_0 : \ldots : x_n]$.

■ **Exemple 1.10 — (script MAGMA).**

```
> k := Rationals() ;                // Corps des rationnels
> P<X, Y, Z> := PolynomialRing(k, 3); // Polynômes à 3 variables sur k
> PP := ProjectiveSpace(P);         // Plan projective sur Q
> P0 := PP![1, 2, 1];
> P1 := PP![2, 4, 2];
> P1 eq P0;
true
```

■

Exercice 1.11 — (★).

1. Vérifier que $\sim$ est bien une relation d'équivalence.
2. Expliciter une surjection entre $k^{n+1}\setminus\{0\}$ et l'ensemble des droites vectorielles de k^{n+1}. En déduire que les deux définitions données sont équivalentes.
3. Montrer que l'application
$$\begin{array}{ccc} k^n & \longrightarrow & \mathbb{P}^n(k), \\ (x_0,\dots,x_{n-1}) & \longmapsto & [x_0 : \dots : x_{n-1} : 1], \end{array}$$
est injective. Est-elle surjective ?

■

On rappelle qu'un polynôme $f \in k[X_0,\dots,X_n]$ est dit homogène de degré d si pour tout $\lambda \in \bar{k}$, on a $f(\lambda X_0,\dots,\lambda X_n) = \lambda^d f(X_0,\dots,X_n)$.

Exercice 1.12 — (★).

1. Parmi les polynômes suivants de $k[X,Y,Z]$ lesquels sont homogènes ?
$$X,\ X+Y^2+Z^3,\ X^3+XYZ+Z^3,\ Y^2Z-X^3-XZ^2.$$
2. Montrer qu'un polynôme $f \in k[X,Y,Z]$ est homogène de degré d si et seulement s'il est combinaison linéaire de monômes de degré d, *i.e.* de polynômes de la forme $X^\alpha Y^\beta Z^\gamma$ avec $\alpha+\beta+\gamma = d$ (on peut considérer $f(TX,TY,TZ) = T^d f(X,Y,Z) \in k[X,Y,Z,T]$ pour le sens qui n'est pas immédiat).

■

Définition 1.13 — Courbe projective plane. Le plan projectif sur k est $\mathbb{P}^2(k)$.

Soit $f \in k[X,Y,Z]$ un polynôme **homogène** non constant géométriquement irréductible. La *courbe projective plane* C_f sur k est l'ensemble des solutions $[x : y : z] \in \mathbb{P}^2\left(\bar{k}\right)$ de l'équation $f(x,y,z) = 0$. Pour toute extension de corps $k \to K$, on pose

$$C_f(K) = \left\{[x : y : z] \in \mathbb{P}^2(K),\ f(x,y,z) = 0\right\}$$

et on appelle cet ensemble les points *K-rationnels* de C_f. On parle souvent des points rationnels pour désigner les points k-rationnels. On appelle degré de C_f le degré de f dans $k[X,Y,Z]$.

Rq Il est absolument **nécessaire** de considérer des polynômes homogènes pour que la relation $f(x,y,z) = 0$ ne dépende pas de la classe de (x,y,z) dans $\mathbb{P}^2\left(\bar{k}\right)$. On a alors pour tout $\lambda \in \bar{k}\setminus\{0\}$, $f(\lambda x,\lambda y,\lambda z) = \lambda^d f(x,y,z)$ où $d = \deg f$. Il faut tout de même faire attention au fait que l'évaluation de f en un point de $\mathbb{P}^2\left(\bar{k}\right)$ n'a pas de sens.

Dans la prochaine définition on définit une courbe projective à partir d'une courbe affine.

Définition 1.14 — Clôture projective. Soit $f \in k[X,Y]$ un polynôme non constant géométriquement réduit de degré d. On pose $\bar{f} = Z^d f(X/Z, Y/Z) \in k[X,Y,Z]$. Il s'agit d'un polynôme homogène de degré d géométriquement réduit. On pose $\bar{C}_f = C_{\bar{f}}$ la courbe projective plane correspondante et on l'appelle *clôture projective* de C_f.

Exercice 1.15 — (★).

Justifier les affirmations faites dans la définition ci-dessus. C'est-à-dire, montrer que $\bar{f}$ est bien un polynôme homogène et qu'il est aussi géométriquement réduit.

■

Dans la prochaine définition on définit une courbe affine à partir d'une courbe projective.

Définition 1.16 — Carte affine. Soit $f \in k[X,Y,Z]$ un polynôme homogène non constant géométriquement réduit. On pose $f_Z \in k[X,Y]$ défini par $f_Z(X,Y) = f(X,Y,1)$. Si $f \neq Z$, alors f_Z est de même degré que f. On pose C_{f_Z} la courbe affine plane correspondante. On dit que C_{f_Z} est la courbe C_f dans la *carte affine* $Z = 1$.

Si on évalue f en $X = 1$ ou $Y = 1$, on parle alors de carte affine $X = 1$ ou $Y = 1$.

Exercice 1.17 — (★).

1. Soit $f \in k[X,Y,Z]$ un polynôme homogène. Montrer que $\bar{f}_Z = f$ (on retrouve la même courbe projective en prenant la clôture projective dans la carte affine $Z = 1$).
2. Soit $g \in k[X,Y]$ un polynôme quelconque. Montrer que $\bar{g}_Z = g$ (on retrouve la même courbe affine en prenant la carte affine $Z = 1$ de la clôture projective). ∎

Exercice 1.18 — (★) Recollement de cartes affines.

On considère les trois applications

$$\iota_Z : \begin{array}{ccc} \mathbb{A}^2 & \longrightarrow & \mathbb{P}^2 \\ (x,y) & \longmapsto & [x:y:1] \end{array}, \quad \iota_Y : \begin{array}{ccc} \mathbb{A}^2 & \longrightarrow & \mathbb{P}^2 \\ (x,z) & \longmapsto & [x:1:z] \end{array}, \quad \iota_X : \begin{array}{ccc} \mathbb{A}^2 & \longrightarrow & \mathbb{P}^2 \\ (y,z) & \longmapsto & [1:y:z] \end{array}.$$

et $f \in k[X,Y,Z]$ un polynôme homogène non constant géométriquement réduit.

1. Montrer que $C_{f_Z} = \iota_Z^{-1}(C_f)$.
2. Montrer que

$$C_f = \iota_X(C_{f_X}) \cup \iota_Y(C_{f_Y}) \cup \iota_Z(C_{f_Z}).$$

∎

La morale de cette section est qu'on peut considérer tout courbe affine comme étant un bout de courbe projective et toute courbe projective comme un recollement de courbes affines ou comme la clôture projective d'une courbe affine.

Rq C'est en fait la façon moderne de faire de la géométrie. On définit des objets dans des cartes puis on recolle les cartes. La façon de recoller les cartes dépend des objets que l'on souhaite manipuler :

- les cartes dans $\mathbb{R}^n$ et recollements continus (ou C^1 ou C^∞) donnent la géométrie réelle ; l'étude des *variétés différentielles* ;
- les cartes dans $\mathbb{C}^n$ et recollements holomorphes donnent la géométrie complexe ; l'étude des *variétés complexes* ;
- les cartes dans k^n et recollements algébriques donnent la géométrie algébrique. Il existe une théorie plus moderne et plus générale qui permet de recoller des *spectres d'anneau* pour définir des *schémas* (une généralisation des variétés algébriques).

L'avantage conceptuel de ce type de construction est qu'on s'affranchit de la notion d'espace ambiant. Par exemple, nos courbes affines sont définies dans $\mathbb{A}^2$, nos courbes projectives sont dans $\mathbb{P}^2$ (et ça suffira amplement pour nos besoins) mais les variétés différentielles, les variétés complexes ou les schémas n'ont pas besoin d'être définis dans un espace plus grand.

1.2.3 Tangentes et points singuliers des courbes projectives

Soit $f \in k[X,Y,Z]$ un polynôme homogène. Soit $[x:y:z]$ un point de la courbe C_f. On dit que P est un point *singulier* de C_f si

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f}{\partial Y}(P) = \frac{\partial f}{\partial Z}(P) = 0.$$

Lorsqu'un point n'est pas singulier, il est dit *non-singulier* ou *lisse*. Une courbe sans point singulier est dite *non-singulière* ou *lisse*.

■ **Exemple 1.19 — (script MAGMA).**

```
> k := Rationals() ;
> P<X, Y, Z> := PolynomialRing(k, 3);
> PP := ProjectiveSpace(P);
> C := Curve(PP, [ Y^2*Z - (X^3+X*Z^2+Z^3) ]); // Cloture de y^2=x^3+x+1
> IsSingular(C);
false
> Cp := ChangeRing(C, GF(31));                 // Même courbe, sur F_31
> IsSingular(Cp);
true
> SingularPoints(Cp);
{@ (14 : 0 : 1) @}
```

■

Si P est non-singulier, on définit la tangente de C_f en P comme étant la clôture projective de la tangente à C_f en P dans une carte affine. L'exercice suivant donne une équation de cette tangente.

Exercice 1.20 — (★★) Calcul pratique des points singuliers d'une courbe projective.

1. Soit $f \in k[X,Y,Z]$ un polynôme homogène de degré d. Montrer qu'on a la relation polynomiale suivante

$$X\frac{\partial f}{\partial X} + Y\frac{\partial f}{\partial Y} + Z\frac{\partial f}{\partial Z} = df(X,Y,Z) \qquad \text{(relation d'Euler)}$$

   (on peut dériver la relation $f(\lambda X, \lambda Y, \lambda Z) = \lambda^d f(X,Y,Z)$ en fonction de λ).
2. Si $P = [x\colon y\colon z]$ est un point de C_f, montrer qu'on a la relation

$$x\frac{\partial f}{\partial X}(P) + y\frac{\partial f}{\partial Y}(P) + z\frac{\partial f}{\partial Z}(P) = 0.$$

3. Montrer que C_f est lisse en P si et seulement si le polynôme suivant est non nul,

$$T_P = X\frac{\partial f}{\partial X}(P) + Y\frac{\partial f}{\partial Y}(P) + Z\frac{\partial f}{\partial Z}(P).$$

   Montrer que si P est un point lisse, alors T_P est la tangente à C_f en P (en particulier, la tangente ne dépend pas de la carte affine choisie). ■

■ **Exemple 1.21** On peut se servir l'exercice 1.20 pour calculer les équations des tangentes en affine. Par exemple si on considère l'hyperbole $C\colon xy = 1$ donnée par $f = XY - 1$ et on souhaite obtenir une équation de la tangente à C en $(1,1)$. Sa clôture projective est $\bar{C}\colon xy = z^2$ donnée par $\bar{f} = XY - Z^2$ et $P = [1\colon 1\colon 1]$. On a alors $\partial f/\partial X(P) = Y(P) \neq 0$ donc $\bar{C}$ (et donc C) est lisse en P. L'équation de sa tangente est donnée par

$$X\frac{\partial f}{\partial X}(P) + Y\frac{\partial f}{\partial Y}(P) + Z\frac{\partial f}{\partial Z}(P) = X + Y - 2Z = 0.$$

En se replaçant dans la carte $Z = 1$, on a $y = 2 - x$ tangente à C en $(1,1)$. ■

■ **Exemple 1.22** On considère la parabole $C\colon y = x^2$, *i.e.* $f = Y - X^2 \in k[X,Y]$. Sa clôture projective est la courbe $\bar{C}\colon yz = x^2$. Les points de $\bar{C}$ sont ceux de la forme $[x\colon y\colon 1]$ (qui sont en bijection avec les points de la courbe affine) plus les points sur la droite à l'infini $z = 0$. Sur cette droite, on a $x^2 = 0$, soit $x = 0$ et y vaut n'importe quelle valeur disons

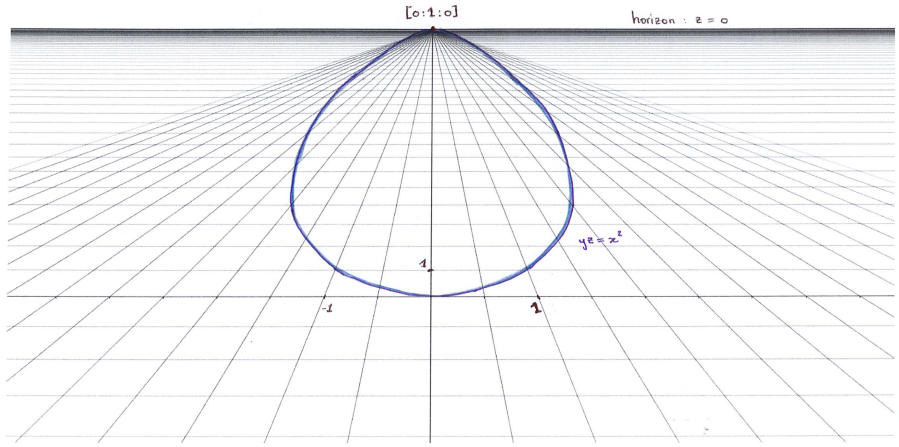


FIGURE 1.4 – Vue en perspective d'une parabole

y_0. Le point $[0\colon y_0\colon 0] = [0\colon 1\colon 0]$ est donc l'unique point de $\bar{C}$ sur la droite d'horizon. On pouvait s'y attendre intuitivement car en regardant une parabole en perspective on verrait quelque chose semblable à la figure 1.4.

Tous les points affines de cette courbe sont lisses, en effet pour $P = (a, a^2)$ on a $\frac{\partial f}{\partial X}(P) = -2a$ et $\frac{\partial f}{\partial Y}(P) = 1$ donc le point P est lisse et la tangente à C passant par P est donnée par

$$(x-a)\cdot(-2a) + (y-a^2)\cdot 1 = 0 \text{ soit } y = 2ax - a^2\,.$$

Pour savoir si $\bar{C}$ est lisse il faut aussi vérifier que le point $P = [0\colon 1\colon 0]$ à l'infini est lisse au même titre que les autres. On peut le faire grâce à l'exercice 1.20 appliqué à $\bar{f} = YZ - X^2$ et avoir une équation de la tangente en ce point au passage. On a

$$X\frac{\partial \bar{f}}{\partial X}(P) + Y\frac{\partial \bar{f}}{\partial Y}(P) + Z\frac{\partial \bar{f}}{\partial Z}(P) = -2\cdot 0\cdot X + 1\cdot 0\cdot Y + 1\cdot 1\cdot Z \neq 0.$$

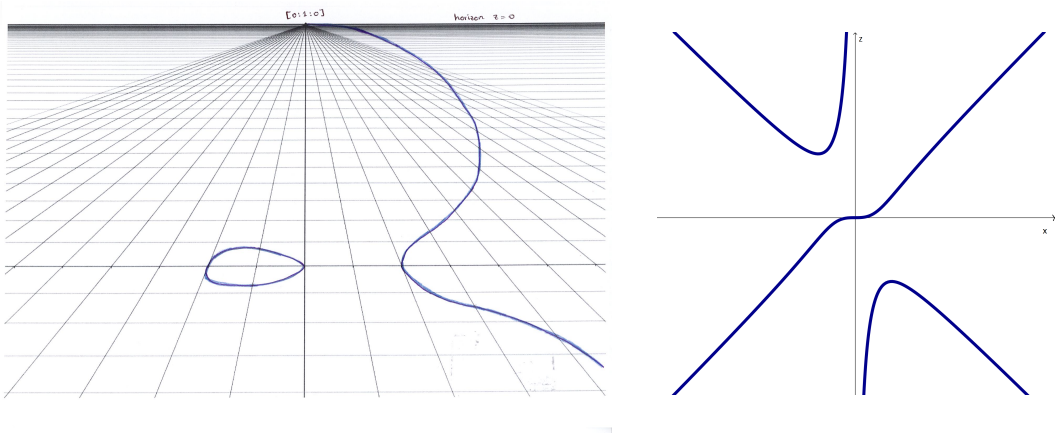
Donc $[0\colon 1\colon 0]$ est un point lisse de $\bar{C}_f$ dont la tangente est la droite d'équation $z = 0$ (*i.e.* l'horizon ; la droite à l'infini).

Remarque. Pouvait-on s'y attendre ? À quoi ressemblerait la courbe sous nos pied si on était debout sur le point $[0\colon 1\colon 0]$ à l'infini et qu'on regardait vers l'origine $[0\colon 0\colon 1]$? Ceci revient à se placer dans la carte affine $Y = 1$, l'équation de $\bar{C}_f$ dans cette carte affine (x, z) est $C_{f_Y}\colon z = x^2$, on voit donc exactement la même chose qu'en se plaçant à l'origine en regardant vers l'infini ! ∎

∎ **Exemple 1.23** On reprend l'exemple de la courbe $C\colon y^2 = x^3 - x$, sa clôture projective est $\bar{C}\colon y^2 z = x^3 - xz^2$. Lorsque $z = 0$ on a $x^3 = 0$ soit $x = 0$. Il y a donc un unique point à l'infini qui est $[0\colon 1\colon 0]$. En nous plaçant sur le plan et en regardant vers l'horizon nous verrions quelque chose de semblable à la figure 1.5a.

Dans l'exercice 1.8, il est demandé de déterminer si les points affines de cette courbe étaient lisses ou non. On doit trouver qu'elle l'est (sauf si le corps k est de caractéristique 2, auquel cas le point $(1,0)$ est singulier). Il reste à déterminer si le point à l'infini est lisse ou non. On peut appliquer le critère de l'exercice 1.20 à $\bar{f} = Y^2Z - X^3 + XZ^2$ en $[0\colon 1\colon 0]$ ce qui donne

$$X\frac{\partial \bar{f}}{\partial X}(P) + Y\frac{\partial \bar{f}}{\partial Y}(P) + Z\frac{\partial \bar{f}}{\partial Z}(P) = Z \neq 0\,.$$



(a) Vue en perspective (b) Vue sur la carte affine $Y = 1$

FIGURE 1.5 – Graphes de la courbe projective $y^2 z = x^3 - x z^2$

Donc le point à l'infini est lisse et sa tangente est la droite $z = 0$.

Remarque. À quoi ressemblerait cette courbe sous nos pieds en nous plaçant debout sur le point à l'infini ? Il s'agit encore de se placer dans la carte affine $Y = 1$, *i.e.* $C_{f_Y} : z = x^3 - xz^2$ qui ressemble à la figure 1.5b. ∎

Exercice 1.24 — (★).
Faire le lien entre le tracé de la figure 1.5b et celui de la figure 1.1 (à quoi correspondent ces deux branches qui ressemblent à une hyperbole [a] ? Pourquoi vont-elles à l'infini et pourquoi dans ces directions ?). ∎

a. Attention ! Il ne s'agit pas d'une hyperbole ! Ça en a seulement l'apparence.

Exercice 1.25 — (★).
Soit $f \in k[X, Z]$ un polynôme homogène de degré $d \geq 4$. On considère la courbe [a] $C : y^2 z^{d-2} = f(x, z)$. Montrer que C a un unique point à l'infini et que celui-ci est un point singulier (lorsque f n'a que des racines simples tous les points affines de C sont lisses, il ne suffit donc pas de montrer que les points d'une courbe dans un carte sont lisses pour que cette courbe soit lisse). ∎

a. Il s'agit d'une courbe *hyperelliptique*.

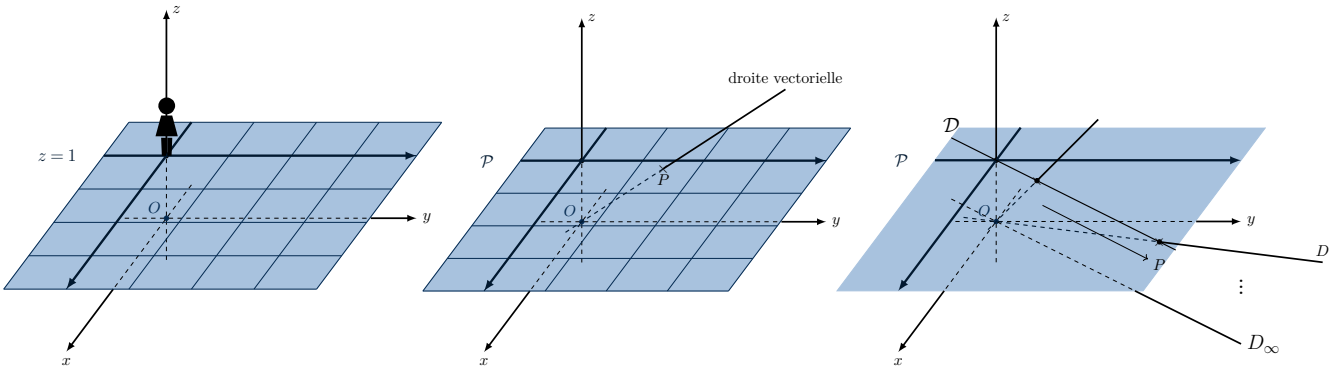
1.2.4 Lien entre l'intuition et la définition

Nous avons vu une approche intuitive de l'espace projectif puis des définitions mathématiques (équivalentes) de $\mathbb{P}^2(\mathbb{R})$. Dans cette section nous faisons le lien entre l'approche intuitive et les définitions rigoureuses.

Replaçons nous debout sur un plan $\mathcal{P}$ mais imaginons-le plongé dans l'espace $\mathbb{R}^3$ de coordonnées (x, y, z), disons que $\mathcal{P}$ est le plan $z = 1$ (parallèle au plan vectoriel $z = 0$). La situation est celle de la figure 1.6a.

Rappelons que $\mathbb{P}^2(\mathbb{R})$ est défini comme étant l'ensemble des droites vectorielles de $\mathbb{R}^3$ (les droites passant par l'origine O). Chaque point P de notre plan $\mathcal{P} : z = 1$ définit une unique droite vectorielle ; la droite passant par ce point et O. L'injection $\mathcal{P} \longrightarrow \mathbb{P}^2(\mathbb{R})$ est exactement celle définie dans l'exercice 1.11.3, en identifiant $\mathcal{P}$ avec $\mathbb{R}^2$ (*cf.* figure 1.6b).

Toutes les droites vont couper notre plan $\mathcal{P} : z = 1$ en un unique point à l'exception des droites parallèles à $\mathcal{P}$, c'est-à-dire les droites contenues dans le plan $z = 0$. Ces droites



(a) Plan $\mathcal{P}$ (b) Projection de $\mathbb{P}^2(\mathbb{R})$ sur $\mathcal{P}$ (c) Droite à l'infini

FIGURE 1.6 – Plan projectif $\mathbb{P}^2(\mathbb{R})$

parallèles à $\mathcal{P}$ représentent les points à l'infini sur l'horizon. En effet, choisissons une droite $\mathcal{D}$ contenue dans $\mathcal{P}$ ainsi qu'un point P sur cette droite. Considérons l'unique droite vectorielle D de $\mathbb{R}^3$ passant par P et faisons glisser P le long de $\mathcal{D}$« vers l'infini ». Cette droite D, qui correspond au point P de $\mathcal{P}$, converge vers une droite D_∞ correspondant au point à l'infini sur l'horizon (*cf.* figure 1.6c).

Récapitulons, une droite vectorielle de $\mathbb{R}^3$ correspond à un unique point de $\mathbb{P}^2(\mathbb{R}) = \mathcal{P} \cup L_\infty$. Donc une droite de $\mathbb{P}^2(\mathbb{R})$ correspond à l'union des droites vectorielles de $\mathbb{R}^3$ qui coupent $\mathcal{P}$ en cette droite. Autrement dit il s'agit d'un plan (vectoriel) de $\mathbb{R}^3$. On peut alors facilement voir que dans $\mathbb{P}^2(\mathbb{R})$ deux droites distinctes se coupent toujours en un unique point. En effet, ces droites correspondent à deux plans distincts de $\mathbb{R}^3$, ces deux plans se coupent en une droite vectorielle qui correspond à un unique point de $\mathbb{P}^2(\mathbb{R})$.

Exercice 1.26 — (★).

1. Vérifier par le calcul en coordonnées que deux droites quelconques ont bien une unique intersection (une droite de $\mathbb{P}^2(k)$ est une courbe définie par l'annulation d'un polynôme homogène de degré 1, *i.e.* $\mathcal{D}\colon ax+by+cz=0$).
2. Se convaincre grâce aux constructions faites ci-dessus que les deux points opposés que nous voyons à l'horizon en regardant dans une direction définissent un même point de $\mathbb{P}^2(\mathbb{R})$ (c'est-à-dire la même droite de $\mathbb{R}^3$). ■

Rq Dans un but pédagogique, on a nommé la droite d'équation $z=0$ « droite à l'infini » ou encore « horizon » et les points sur cette droite les points « à l'infini ». Bien entendu, ni cette droite, ni ces points, n'ont de statut particulier vis à vis des autres droites et points de $\mathbb{P}^2$. En fait, si on prend n'importe quelle droite D du plan projectif il existe un isomorphisme $\iota\colon \mathbb{A}^2 \longrightarrow \mathbb{P}^2 \setminus D$, interprété comme une carte affine de $\mathbb{P}^2$.
On a mentionné que les cas particuliers où D est donnée par $x=0$, $y=0$ ou $z=0$ mais, bien sûr, n'importe quelle droite convient, l'expression de ι en coordonnée est seulement plus compliquée.

Un autre exemple de plan projectif est le plan de Fano, $\mathbb{P}^2(\mathbb{F}_2)$ que l'on représente souvent comme sur la figure 1.7. Il s'agit du plus petit plan projectif. Il s'agit de l'ensemble des droites vectorielles de $\mathbb{F}_2^3$. Chaque droite possède exactement 2 points dont l'origine. Ainsi, chaque point non nul de $\mathbb{F}_2^3$ définit une unique droite, il y a donc $8-1$ points dans $\mathbb{P}^2(\mathbb{F}_2)$. Sur la figure 1.7 sont représentés ces 7 points ainsi que toutes les droites qui sont aussi au nombre de 7. On peut constater que chaque droite coupe chaque autre droite en exactement 1 point.

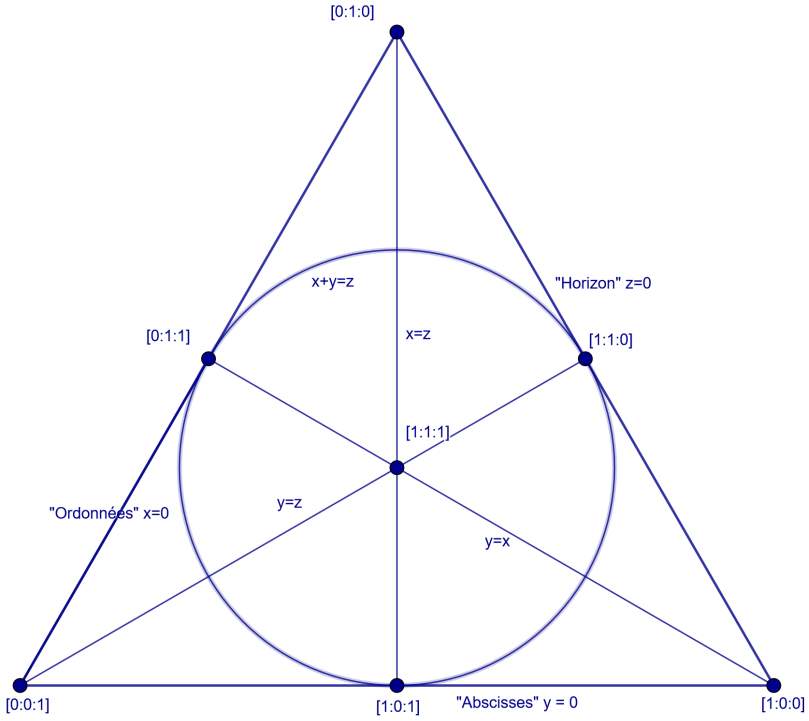


FIGURE 1.7 – Plan de Fano $\mathbb{P}^2(\mathbb{F}_2)$

1.3 Morphismes

En mathématiques, quand on créé des objets, se pose naturellement la question de comment on peut les comparer. On définit les groupes puis les morphismes de groupes, les espaces topologiques puis les applications continues, les espaces vectoriels puis les applications linéaires. Comment faire pour les courbes ? Cela a-t-il un sens de dire qu'un cercle est isomorphe à une ellipse ? Que l'application de l'hyperbole $yx = 1$ vers la droite $y = 0$ donnée par $(x, y) \mapsto (x, 0)$ est un morphisme entre deux courbes affines ?

1.3.1 Applications régulières entre courbes affines

Soit $f \in k[X,Y]$ géométriquement réduit et $C = C_f$ la courbe correspondante. On appelle anneau des fonctions régulières sur C l'anneau quotient

$$k[C] = k[X,Y]/\langle f \rangle = k[x,y]$$

où x et y sont les classes de X et de Y dans le quotient. On peut voir une fonction régulière $g \in k[C]$ comme une fonction polynomiale $C \to \mathbb{A}^1$, c'est-à-dire que pour toute extension de corps $k \to K$ on a une fonction

$$\begin{array}{ccc} C(K) & \longrightarrow & \mathbb{A}^1(K) = K \\ (a,b) & \longmapsto & g(a,b). \end{array}$$

Lorsque f est irréductible (donc premier car $k[X,Y]$ est factoriel), l'anneau $k[C]$ est intègre et on peut considérer son corps des fractions

$$k(C) = \mathrm{Frac}\,(k[C]) = \left\{ \frac{g}{h} : g, h \in k[C] \right\}.$$

On appelle les éléments de $k(C)$ les fonctions rationnelles de C.

Rq Attention au fait qu'une fonction rationnelle ne définit pas exactement une fonction $C(K) \to K$ pour tout $k \to K$ mais seulement sur $C(K) \setminus \{\text{zéros de } h \text{ sur } K\}$.

Définition 1.27 — Application régulière. Soient C_{f_1} et C_{f_2} deux courbes affines planes. Une *application régulière* $\varphi\colon C_{f_1} \longrightarrow C_{f_2}$ est une paire de fonctions régulières (g_1, g_2) de C_{f_1} telles que $f_2(g_1, g_2) = 0$. Pour tout $k \to K$ on a une application

$$\begin{array}{rcl} C_{f_1}(K) & \longrightarrow & C_{f_2}(K) \\ (a,b) & \longmapsto & (g_1(a,b), g_2(a,b)). \end{array}$$

Deux courbes affines planes C et C' sont dites isomorphes s'il existe des applications régulières $\varphi\colon C \to C'$ et $\psi\colon C' \to C$ telles que $\varphi \circ \psi = \mathrm{id}_{C'}$ et $\psi \circ \varphi = \mathrm{id}_C$.

■ **Exemple 1.28** Considérons la parabole $C\colon y = x^2$ et la droite des abscisses $D\colon y = 0$. Le morphisme donné par le couple $(X, 0)$ induit une application régulière

$$\begin{array}{rccc} \varphi\colon & C & \longrightarrow & D \\ & (a,b) & \longmapsto & (a,0). \end{array}$$

Réciproquement, l'application donnée par

$$\psi\colon D \longrightarrow C, \quad (a,0) \longmapsto (a,a^2).$$

est bien définie et satisfait $\varphi \circ \psi(a,0) = \varphi(a,a^2) = (a,0)$ et $\psi \circ \varphi(a,b) = (a,a^2) = (a,b)$. On peut donc en conclure que la parabole et la droite sont isomorphes. ■

Proposition 1.29 Soit C_{f_1} et C_{f_2} des courbes affines planes.
Il y a une correspondance

$$\begin{array}{rcl} \{C_{f_1} \to C_{f_2} \text{ régulière}\} & \longleftrightarrow & \{\text{Morphismes de } k\text{-algèbres } k[C_{f_2}] \to k[C_{f_1}]\} \\ \varphi = (g_1, g_2) & \longmapsto & g \mapsto g(g_1, g_2) \\ (\gamma(X), \gamma(Y)) & \longleftarrow\!\shortmid & \gamma\colon k[C_{f_2}] = k[X,Y]/\langle f_2\rangle \to k[C_{f_1}] \end{array}$$

En particulier, deux courbes sont isomorphes si et seulement si leurs algèbres des fonctions régulières sont isomorphes.

Démonstration. Soit $\varphi = (g_1, g_2)$ une application régulière, *i.e.* $f_2(g_1, g_2) = 0$. On considère le morphisme de k-algèbre $\widetilde{\gamma}\colon k[X,Y] \to k[X,Y]/\langle f_1\rangle$ donné par $\widetilde{\gamma}(g) = g(g_1, g_2)$. Puisque $f_2(g_1, g_2) = 0, f_2 \in \ker \widetilde{\gamma}$, par passage au quotient on donc a bien un morphisme de k-algèbre $\gamma\colon k[C_{f_2}] = k[X,Y]/\langle f_2\rangle \to k[C_{f_1}]$.

Réciproquement, considérons un morphisme de k-algèbre $\gamma\colon k[C_{f_2}] = k[X,Y]/\langle f_2\rangle = k[x,y] \to k[C_{f_1}]$ et $g_1 = \gamma(x) \in k[C_{f_1}]$ et $g_2 = \gamma(y) \in k[C_{f_1}]$. Puisque $f_2(x,y) = 0 \in k[C_{f_2}]$ on a bien $f_2(g_1, g_2) = \gamma(f_2(x,y)) = 0 \in k[C_{f_1}]$. ■

■ **Exemple 1.30** Reprenons l'exemple de la parabole et de la droite. L'anneau des fonctions régulières de $y = x^2$ est $k[X,Y]/\langle Y - X^2\rangle$ et celui de la droite $y = 0$ est $k[X,Y]/\langle Y\rangle \simeq k[X]$. On voit directement que $k[X,Y]/\langle Y - X^2\rangle \simeq k[X, X^2] = k[X]$ donc leurs anneaux sont effectivement isomorphes ! ■

■ **Exemple 1.31** On peut se demander si l'hyperbole $H\colon xy = 1$ et la droite des abscisses $D\colon y = 0$ sont isomorphes. Leurs anneaux sont $k[X,Y]/\langle XY - 1\rangle \simeq k[X, X^{-1}]$ et $k[X,Y]/\langle Y\rangle \simeq k[X]$. Un morphisme de D vers H correspond à un morphisme d'algèbres $k[X, X^{-1}] \to k[X]$. Ce dernier est caractérisé par son image de X qui doit être un inversible de $k[X]$. Or les inversibles de $k[X]$ sont exactement les polynômes constants ; les éléments de k (à prouver !). Donc un tel morphisme n'est jamais surjectif. En d'autres termes, il n'existe pas d'isomorphisme entre les deux courbes (autrement il existerait aussi un isomorphisme entre leurs algèbres). ■

Exercice 1.32 — (★★★).
On considère $E\colon y^2 = x^3 + x^2$, montrer que l'application

$$\begin{array}{rcl} \mathbb{A}^1 & \longrightarrow & E\,, \\ t & \longrightarrow & (t^2-1, t^3-t^2)\,, \end{array}$$

est bien définie. S'agît-il d'un isomorphisme ? ∎

1.3.2 Applications régulières entre courbes projectives

Soient f_1, f_2 deux polynômes homogènes de $k[X,Y,Z]$ et C_{f_1}, C_{f_2} les courbes projectives correspondantes. Soient g_1, g_2, g_3 des polynômes homogènes de même degré d tels que $f_2(g_1,g_2,g_3) = 0$ alors l'application

$$\begin{array}{rccl} \varphi\colon & C_{f_1} & \longrightarrow & C_{f_2} \\ & [x\colon y\colon z] & \longmapsto & [g_1(x,y,z)\colon g_2(x,y,z)\colon g_3(x,y,z)] \end{array}$$

est appelée *application rationnelle* et notée $\varphi = [g_1 : g_2 : g_3]$.

Rq Attention, bien qu'on appelle cet objet une application rationnelle il ne s'agit pas littéralement d'une application. En effet, elle est bien définie seulement pour les (x,y,z) tels que les g_i ne s'annulent pas tous simultanément.

■ **Exemple 1.33** On considère la parabole $C\colon YZ = X^2$ et « l'application »

$$\varphi\colon C \longrightarrow \mathbb{P}^1, \quad [x\colon y\colon z] \longmapsto [x\colon y]$$

est une application rationnelle. Elle est bien définie partout sauf en $O = [0\colon 0\colon 1]$ (qui correspond à l'origine). Pourtant, lorsque $x, y \neq 0$, on a pour tout $[x\colon y\colon z] \in C$,

$$[x\colon y] = \left[x^2\colon yx\right] = [yz\colon yx] = [z\colon x]\,.$$

Il semble donc raisonnable de prolonger φ en O en posant $\varphi(O) = [1\colon 0]$. Nous donnons un sens à ce prolongement ci-dessous. ∎

Soit $f \in k[X,Y,Z]$ un polynôme homogène. On pose $k[x,y,z] = k[X,Y,Z]/(f)$ et

$$k[x,y,z]_d = \{g \in k[x,y,z],\ g \text{ a un représentant homogène de degré } d\}\,.$$

■ **Exemple 1.34** Le polynôme $g = x + yz - x^2$ avec $f = YZ - X^2$ est bien homogène, bien que $x + yz - x^2$ ne le soit pas, car il a la même classe dans $k[x,y,z]$ que x. ∎

Lorsque f est irréductible on peut définir $k(x,y,z) = \operatorname{Frac} k[x,y,z]$. On pose

$$k(C_f) = \left\{ \frac{g}{h} \in k(x,y,z), g, h \in k[x,y,z]_d \text{ pour un certain } d \in \mathbb{N} \right\}.$$

On peut enfin définir les applications régulières entre courbes projectives planes.

Définition 1.35 — Application régulière entre courbes projectives. Soit l'application rationnelle $\varphi = [g_1\colon g_2\colon g_3]\colon C_{f_1} \to C_{f_2}$. On dit que φ est régulière en $P \in C_{f_1}$ s'il existe $g \in k(C_{f_1})$ telle que
— pour tout i, $g \cdot g_i$ est bien définie en P,
— il existe i tel que $(g \cdot g_i)(P) \neq 0$.
On dit que φ est *régulière* ou que c'est un *morphisme* si elle est régulière en P pour tout $P \in C_{f_1}$. S'il existe $\varphi\colon C_{f_1} \longrightarrow C_{f_2}$ et $\psi\colon C_{f_2} \longrightarrow C_{f_1}$ régulières telles que $\varphi \circ \psi = \mathrm{id}$ et $\psi \circ \varphi = \mathrm{id}$, alors C_{f_1} et C_{f_2} sont dites isomorphes.

■ **Exemple 1.36** On reprend l'exemple 1.33, *i.e.* la courbe $YZ = X^2$ et $\varphi([x\colon y\colon z]) = [x\colon y]$. Alors $g = y/x$ convient. En effet, on a bien $x \cdot (y/x) = y$ qui est bien définie en P et vaut 0 et $y \cdot (y/x) = y^2/x = xz/x = z \in k(x,y,z)$ est bien définie et vaut 1 en O. ∎

Exercice 1.37 — (★).
Montrer que φ définie dans l'exemple 1.33 est un isomorphisme d'inverse $\psi([x:y]) = [x^2 : xy : y^2]$. ∎

Proposition 1.38 Soient C_{f_1} et C_{f_2} deux courbes projectives planes. Une application régulière $C_{f_1} \to C_{f_2}$ induit une extension de corps $k(C_{f_2}) \to k(C_{f_1})$ dont la restriction à k est l'identité et réciproquement toute extension de corps $k(C_{f_2}) \to k(C_{f_1})$ fixant k provient d'un unique morphisme $C_{f_1} \to C_{f_2}$. On a un isomorphisme

$$\mathrm{Hom}(C, C') \simeq \mathrm{Hom}_k(k(C_{f_2}), k(C_{f_1})).$$

En particulier, C_1 et C_2 sont isomorphes si et seulement si $k(C_{f_2})$ et $k(C_{f_1})$ sont isomorphes.

Plutôt que de montrer ce résultat on va expliquer comment s'en servir.

Proposition 1.39 Soit $f \in k[X,Y]$ et C_f la courbe affine correspondante. Alors le morphisme de corps

$$\begin{aligned} \iota : \quad k\left(C_{\bar{f}}\right) &\longrightarrow k(C_f), \\ \frac{g}{h} &\longrightarrow \frac{g(x,y,1)}{h(x,y,1)}, \end{aligned}$$

est un isomorphisme de corps.

Démonstration. Il s'agit d'un morphisme de corps, il est donc injectif. Par ailleurs, $\iota(x/z) = x$ et $\iota(y/z) = y$, donc $k(x,y) = k(C_f) \subseteq \mathrm{im}\,\iota$ et ι est surjectif.

■

Exercice 1.40
Montrer que l'inverse du morphisme de corps de la proposition 1.39 est

$$\begin{aligned} k(C_f) &\longrightarrow k\left(C_{\bar{f}}\right), \\ \frac{g}{h} &\longrightarrow z^{\deg h - \deg g} \frac{\bar{g}}{\bar{h}}. \end{aligned}$$

∎

■ **Exemple 1.41** On a déjà vu que les courbes affines données par les équations $H : xy = 1$ et $y = 0$ (qui est isomorphe à $\mathbb{A}^1$) ne sont pas isomorphes car leurs anneaux des fonctions régulières ne sont pas isomorphes. Il s'agit des anneaux $k[X, X^{-1}]$ et $k[X]$. Pourtant, $\bar{H} : xy = z^2$ et on a vu que cette dernière est isomorphe à $\mathbb{P}^1 = \bar{\mathbb{A}}^1$. On peut le vérifier facilement en montrant que les corps de fractions de $k[X, X^{-1}]$ et $k[X]$ sont isomorphes. ∎

1.3.3 Rationalité des morphismes

Définition 1.42 — Changement de corps de base. Soit C_f une courbe (affine ou projective) définie sur un corps k, *i.e.* f est à coefficient dans k et $k \to K$ une extension de corps. On pose $C_f \times_k K$ la courbe sur K définie par f vu comme étant à coefficients dans K.

On a alors $K[C_f \times_k K] = k[C_f] \otimes_k K$ et $K(C_f \times_k K) = k(C_f) \otimes_k K$.

Définition 1.43 Soit C une courbe définie sur un corps k et $k \to K$ une extension. On note $K[C_f]$ et $K(C_f)$.

— Soit C' définie sur k, on dit qu'un morphisme $C \times_k K \to C' \times_k K$ est défini sur K. Cela revient à dire que les coefficients des polynômes intervenant comme coordonnées du morphisme sont à coefficients dans K. Par abus, on dit qu'il s'agit d'un morphisme de C vers C' défini sur K.

— Soit C' définie sur K. S'il existe un isomorphisme $C \times_k K \to C'$ on dit que C est un *modèle* de C' sur k ou encore que C' *descend* sur k.

■ **Exemple 1.44** On considère les courbes $C\colon X^2+Y^2=1$ et $C'\colon X^2+Y^2=-1$ sur $\mathbb{R}$. Elles ne sont pas isomorphes[7] sur $\mathbb{R}$ car $C(\mathbb{R})$ est le cercle unité tandis que $C'(\mathbb{R})=\emptyset$. Pourtant l'application

$$\begin{array}{ccc} C & \longrightarrow & C' \\ (x,y) & \longmapsto & (ix,iy) \end{array}$$

est un isomorphisme. Ainsi C et C' sont isomorphes sur $\mathbb{C}$ mais pas sur $\mathbb{R}$. ■

■ **Exemple 1.45** On considère $E'\colon y^2=x^3+1$ sur $\mathbb{R}$ et $E\colon y^2=x^3+3ix^2-3x-i+1$ sur $\mathbb{C}$. L'isomorphisme $(x,y)\mapsto(x+i,y)$ définit un isomorphisme entre E et E'. On peut donc affirmer que E est un modèle de E' sur $\mathbb{R}$. ■

1.4 Diviseurs et espaces de Riemann-Roch

1.4.1 Ordre d'une fonction rationnelle en un point

Soit $C = C_f$ une courbe affine géométriquement irréductible, *i.e.* $f \in k[X,Y]$ irréductible dans $\bar{k}[X,Y]$. On suppose aussi que C est lisse dans toute la suite. On considère $P \in C\left(\bar{k}\right)$ et on pose

$$\mathfrak{m}_P = \left\{ g \in \bar{k}[C] \colon g(P) = 0 \right\}$$
$$\bar{k}[C]_P = \bar{k}[C]_{\mathfrak{m}_P} = \left\{ \frac{g}{h} \in \bar{k}(C) \colon h(P) \neq 0 \right\}$$

On appelle $\bar{k}[C]_P$ *l'anneau local de* C *en* P ou le *localisé* de $\bar{k}[C]$ en P. Il s'agit d'un anneau de valuation discrète[8], c'est-à-dire d'un anneau principal ayant un unique idéal maximal $\mathfrak{m}_P$. On définit alors la valuation de $g \in \bar{k}[C]_P$ comme suit,

$$\begin{array}{rccl} \mathrm{ord}_P\colon & \bar{k}[C]_P & \longrightarrow & \mathbb{N} \cup \{\infty\}, \\ & g \neq 0 & \longmapsto & \max\left\{ j \in \mathbb{N} \colon g \in \mathfrak{m}_P^j \right\}, \\ & 0 & \longmapsto & \infty. \end{array}$$

Un élément $t \in \bar{k}[C]_P$ tel que $\mathrm{ord}_P(t) = 1$ est appelé une *uniformisante* de C en P. Puisque $\bar{k}[C]_P$ est principal, on a alors $\mathfrak{m}_P = \langle t \rangle$ et pour toute fonction g on a $g = u\,t^{\mathrm{ord}_P(g)}$ avec u inversible dans $\bar{k}[C]_P$.

Pour $P=(a,b)$ on a $\mathfrak{m}_P = \langle x-a,\ y-b \rangle$ avec x et y les classes de X et de Y dans $\bar{k}[C] = \bar{k}[X,Y]/\langle f \rangle$. En particulier, $x-a$ ou $y-b$ est toujours une uniformisante.

Enfin, on étend la valuation aux fonctions rationnelles de la façon suivante

$$\text{pour } \alpha = \frac{g}{h} \in \bar{k}(C),\ \mathrm{ord}_P\left(\frac{g}{h}\right) = \mathrm{ord}_P(g) - \mathrm{ord}_P(h).$$

7. Un isomorphisme sur k entre deux courbes fait correspondre leur points k-rationnels.
8. En anglais, *discrete valuation ring*, souvent abrégé DVR.

Si pour $\alpha \in \bar{k}(C)$, $\mathrm{ord}_P(\alpha) > 0$ on dit que P est un zéro d'*ordre* $\mathrm{ord}_P(\alpha)$ de α, et si $\mathrm{ord}_P(\alpha) < 0$, on dit que c'est un *pôle* d'ordre $-\mathrm{ord}_P(\alpha)$ de α.

Si C est une courbe projective et P un point de C, alors on se place dans une carte affine de C dans laquelle est P et on définit l'ordre d'une fraction rationnelle g/h via l'isomorphisme ι de la proposition 1.39.

▪ **Exemple 1.46** On considère la courbe $C\colon yz = x^2$ (une parabole). On considère $P = [0\colon 0\colon 1] \in C$ (l'origine) et $\alpha = y/z \in \bar{k}(C)$. Le point P se trouve dans la carte affine $Z = 1$. L'ordre de α en P est donc l'ordre de $y \in \bar{k}(C_Z) = \bar{k}(x,y) = \mathrm{Frac}\left(\bar{k}[X,Y]/\langle Y - X^2\rangle\right)$ en $O = (0,0)$ avec $C_Z\colon y = x^2$. Il faut maintenant trouver une uniformisante de $\bar{k}[C]_O$ (il faut penser à cet anneau comme à l'anneau $\bar{k}[C]$ des fonctions sur C où les fonctions qui ne s'annulent pas en $(0,0)$ sont rendues inversibles). On a évidemment $\mathfrak{m}_O = \langle x, y\rangle$ mais on voudrait bien n'avoir qu'un générateur (qui est alors notre uniformisante). Par définition de C on a $y = x^2 \in \bar{k}[C]$, autrement dit $y \in \langle x\rangle$ et donc $\mathfrak{m}_O = \langle x\rangle$, *i.e.* x est une uniformisante de C en O.

On voit que $\alpha = y/z$ s'annule en $z = 0$ (sur l'horizon), donc en $P' = [0\colon 1\colon 0]$. On se propose de calculer l'ordre en P' de α. Malheureusement, P' n'est pas dans la carte $Z = 1$. Ce n'est pas un gros problème, il est dans la carte $Y = 1$. Dans cette carte on a $C_Y\colon z = x^2$ et on veut calculer $\mathrm{ord}_{P'}(1/z) = -\mathrm{ord}_{P'} z$. C'est donc exactement le même calcul que précédemment (en remplaçant partout y par z). Donc $\mathrm{ord}_P(\alpha) = -2$. ▪

Exercice 1.47 — (★★). En reprenant les notations ci-dessus montrer que
1. $\mathrm{ord}_P\left(\frac{x}{z}\right) = 1$ et $\mathrm{ord}_{P'}\left(\frac{x}{z}\right) = -1$.
2. On pose $Q = [1\colon 1\colon 1]$ que vaut $\mathrm{ord}_Q\left(\frac{y}{z}\right)$?
3. $\mathrm{ord}_P\left(\frac{2x-y}{z}\right) = 1$ et $\mathrm{ord}_{P'}\left(\frac{2x-y}{z}\right) = -2$. ▪

Exercice 1.48 — (★★★). On considère $E\colon y^2z = x^3 - xz^2$ sur k de caractéristique $\neq 2$ et $P = [0\colon 0\colon 1] \in E$ et $P' = [0\colon 1\colon 0]$.
1. Montrer que y est une uniformisante de $\bar{k}[E]_P$. Montrer que $\mathrm{ord}_P(x) = 2$ (on peut se rappeler que $y^2 = x(x^2-1)$ dans la carte $Z = 1$).
2. Montrer que x est une uniformisante de
$$\bar{k}[E]_{P'} = \bar{k}[x,z]_{P'} = \left(\bar{k}[X,Z]/\left\langle Z - X^3 + XZ^2\right\rangle\right)_{P'}.$$
Montrer que $\mathrm{ord}_{P'}(x/z) = -2$.

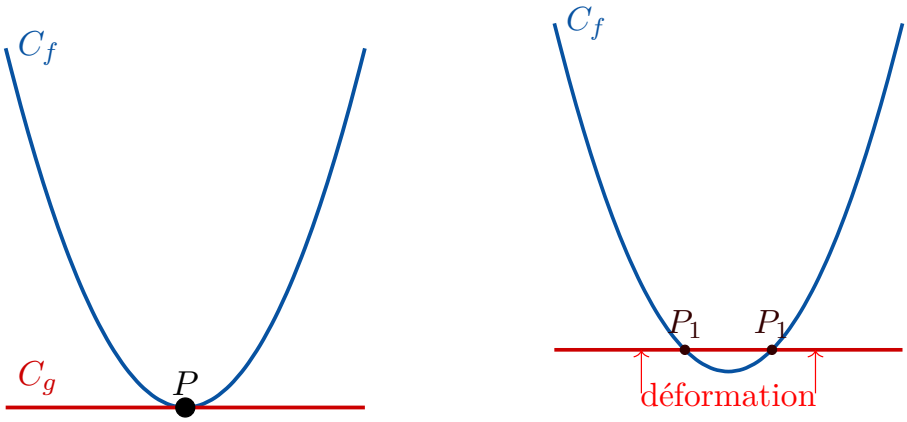
```
> k := GF(5);
> E := EllipticCurve([k!-1, 0]);// La courbe Y^2*Z = X^3 - X*Z^2 sur F_5
> FF<x, y> := FunctionField(E);
> P := E![0, 0];
> Pp := PointsAtInfinity(E)[1];
> Valuation(y, P);                // y est une uniformisante en P ?
1
> Valuation(x, P);
2
> Valuation(x, Pp);
-2
```

(attention, MAGMA comprend x comme X/Z et y comme Y/Z. Ceci ne change rien pour les points affines mais il faut être prudent·e pour les points à l'infini). ▪

Enfin, une dernière notion qui nous est utile est la suivante.

Définition 1.49 — Multiplicité d'intersection. Soit $f, g \in k[X,Y]$ géométriquement réduits et non constants et $P \in C_f$. La *multiplicité d'intersection* entre les courbes C_f et C_g en $P \in C_f$ est l'entier $\mathrm{ord}_P(g)$ avec g vu comme un élément de $\bar{k}[C]_P$.

Une façon intuitive de se représenter la multiplicité d'intersection sur $\mathbb{R}$ est la suivante : la multiplicité d'intersection de deux courbes en un point est le nombre maximum de points d'intersections de ces courbes autour de P en en déformant légèrement l'une des deux. La figure 1.8 illustre le fait que la multiplicité d'intersection entre la parabole et sa tangente en un point est égale à 2.



(a) Situation initiale (b) Déformation

FIGURE 1.8 – Multiplicité d'intersection

Exercice 1.50 — (★★★).
On pose $E = C_f : y^2 = x^3 - 1$ avec $f = Y^2 - X^3 + 1$ sur un corps k de caractéristique $\neq 2, 3$ et $P = (a,b)$ un point de E.

1. Montrer que si $a \neq 0$ alors $x - a$, est une uniformisante de E en P. Montrer que si $b \neq 0$ alors $y - b$ est une uniformisante de E en P.
2. Montrer que $\alpha = (x-a)\,\partial f/\partial X(a,b) + (y-b)\,\partial f/\partial X(a,b) \in \bar{k}(E)$ est d'ordre 2 en P (on peut penser à exprimer f dans la base $(X-a, Y-b)$, *i.e.* son développement de Taylor).
3. Justifier que la multiplicité d'intersection entre une courbe non singulière et sa tangente en un point est toujours supérieure ou égale à 2 en ce point. ■

1.4.2 Diviseurs sur une courbe

Soit C une courbe projective plane sur un corps k. Un *diviseur* D sur C est une somme formelle

$$D = \sum_{P \in C(\bar{k})} n_P [P]$$

avec $n_P \in \mathbb{Z}$ et $\mathrm{Supp}(D) = \left\{ n_P \neq 0,\ P \in C\left(\bar{k}\right) \right\}$ fini.

L'ensemble des diviseurs forme un groupe noté $\mathrm{Div}(C)$. Le groupe des diviseurs, en lui-même ne capture pas vraiment d'information sur la géométrie de la courbe ; on a $\mathrm{Div}(C) \simeq \mathbb{Z}^{(C(\bar{k}))}$, c'est un groupe libre ennuyant. On va donc le quotienter pour en faire un objet central dans l'étude des courbes.

Le degré D d'un diviseur est l'entier $\deg D = \sum_P n_P$. L'ensemble des diviseurs de degré 0 forme un sous-groupe de $\mathrm{Div}(C)$ noté $\mathrm{Div}^0(C)$ On dit qu'un diviseur est *effectif* et on note $D \geq 0$ si $\forall P,\, n_P \geq 0$.

À toute fonction rationnelle $\alpha \in \bar{k}(C) \setminus \{0\}$, on peut associer un diviseur (appelé *diviseurs principal*),

$$\mathrm{div}\,\alpha = \sum_{P \in C(\bar{k})} \mathrm{ord}_P(\alpha)[P].$$

Deux diviseurs D et D' sont dits linéairement équivalents si $D - D'$ est un diviseur principal.Un résultat essentiel est qu'une fonction rationnelle a autant de zéros que de pôles.

Proposition 1.51 Soit C une courbe projective lisse. Alors
- $\deg(\mathrm{div}(\alpha)) = 0$,
- $\mathrm{div}\,\alpha = 0 \;\Leftrightarrow\; \alpha \in \bar{k} \setminus \{0\}$.

On voit facilement que

$$\mathrm{div}(\alpha\beta) = \mathrm{div}(\alpha) + \mathrm{div}(\beta). \tag{1.2}$$

Ainsi, l'ensemble des diviseurs principaux forme un sous-groupe $P(C)$ de $\mathrm{Div}(C)$, mais aussi de $\mathrm{Div}^0(C)$ d'après la proposition 1.51. On pose alors

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/P(C) \text{ et } \mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/P(C)$$

appelés groupes de Picard de C, et pour tout diviseur D, l'ensemble

$$\mathcal{L}(D) = \left\{\alpha \in \bar{k}(C) \setminus \{0\} : \mathrm{div}\,\alpha + D \geq 0\right\} \cup \{0\}$$

appelé *espace de Riemann-Roch* de D.

Pour $D = \sum_P n_P[P]$, cet espace s'interprète comme l'ensemble des $\alpha \in \mathcal{L}(D) \setminus \{0\}$ tels que
- pour $P \in C\left(\bar{k}\right)$ tel que $n_P > 0, \alpha$ *peut* avoir un pôle en P d'ordre au plus n_P.
- pour $P \in C\left(\bar{k}\right)$ tel que $n_P < 0, \alpha$ *doit* avoir un zéro d'ordre au moins $-n_P$ en P.

Exercice 1.52 — (★).
1. Montrer que $\mathcal{L}(D)$ est un $\bar{k}$-espace vectoriel (on peut se servir de la relation (1.2) et de la proposition 1.51).
2. Montrer que si $\deg D \leq 0$ alors $\mathcal{L}(D) = \{0\}$.
3. Montrer que si $D \geq 0$ alors $\bar{k} \subseteq \mathcal{L}(D)$ (en particulier $\dim_{\bar{k}}(\mathcal{L}(D)) \geq 1$). ∎

On note $\ell(D) = \dim_{\bar{k}}(\mathcal{L}(D))$. L'espace $\mathcal{L}(D)$ est en fait un espace vectoriel de dimension finie, *i.e.* $\ell(D) < +\infty$ et on peut (souvent [9]) calculer sa dimension grâce au théorème suivant.

Théorème 1.53 Soit C une courbe projective plane lisse.
1. **Inégalité de Riemann :** Soit D un diviseur sur C alors il existe un entier g, appelé genre de C, tel que $\ell(D) \geq \deg D + 1 - g$ avec égalité lorsque $\deg D \geq 2g - 2$.
2. L'entier g vérifie $g = (\deg C - 1)(\deg C - 2)/2$.

9. Le Théorème de Riemann-Roch permet d'avoir une égalité mais exige plus de travail pour être énoncé.

■ **Exemple 1.54** On considère la courbe $E\colon y^2z = x^3 - xz^2$ sur un corps k de caractéristique $\neq 2$. il s'agit d'une courbe de genre a $g = (3-1)(3-2)/2 = 1$. On considère le diviseur $[P]$ pour $P \in E$. On a $\deg[P] = 1 \geq 2g-2$, donc on est dans le cas d'égalité de l'inégalité de Riemann. Donc $\ell([P]) = \deg([P]) + 1 - g = 1$.

Par ailleurs, $[P] \geq 0$ donc, d'après l'exercice 1.52, $\bar{k} \subseteq \mathcal{L}([P])$ donc $\mathcal{L}([P])$ est composé uniquement des fonctions constantes. Autrement dit, une fonction rationnelle non constante sur E ne peut avoir un pôle d'ordre 1 en un unique point de E. ■

Exercice 1.55 — (★).

On reprend les notations de l'exemple 1.54. Existe-t-il toujours des fonctions rationnelles non constantes sur E avec un pôle d'ordre exactement 2 en un point $P \in E$? (on peut remarquer que $\mathcal{L}([P]) \subseteq \mathcal{L}([2P])$ et calculer $\ell([2P])$). ■

2. Généralités sur les courbes elliptiques

L'essentiel de ce chapitre porte sur la loi de composition (ou d'addition) définie sur une courbe elliptiques. On fait le choix de la présenter sous sa forme géométrique, via l'addition de diviseurs dans $\mathrm{Pic}^0(E)$. On n'en parle pas plus ici, mais ce point de vue a l'avantage de pouvoir se généraliser aux courbes de genre plus grand, lorsque l'on définit leurs Jacobiennes.

2.1 Modèle de Weierstrass

Définition 2.1 Une courbe d'équation

$$E\colon Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

avec $a_1, a_2, a_3, a_4, a_5, a_6 \in k$, notée $E = E_{a_1,\dots,a_6}$ est appelée courbe elliptique sur k si elle est lisse. Une écriture de la forme (2.1) est appelé un *modèle de Weierstrass* de E.

On écrit parfois $E\colon y^2 + h(x)y = f(x)$ avec $\deg h \leq 1$ et $\deg f = 3$ pour désigner la courbe elliptique correspondant à la clôture projective de cette courbe affine.

La proposition suivante est très utile lorsqu'on travaille sur un corps de caractéristique $\neq 2, 3$. Elle nous permet de travailler en toute généralité avec des courbes elliptiques ayant un modèle de Weierstrass avec moins de coefficients. Nous démontrons la plupart des résultats dans ce cadre là car les calculs sont bien moins fastidieux et, lorsqu'il y a des formules, nous les donnons aussi dans le cas général.

Proposition 2.2 Soit k tel que $\mathrm{char}\, k \neq 2, 3$. Soit $E_{a_1,\dots,a_6}$ une cubique définie sur k alors E est isomorphe à une cubique E', notée $E_{a,b}$, de la forme

$$E'\colon Y^2Z = X^3 + aXZ^2 + bZ^3,\ a, b \in k. \tag{2.2}$$

Démonstration. Le morphisme $[x\colon y\colon z] \mapsto \left[x\colon y - \frac{a_1}{2}x\colon z\right]$ définit un isomorphisme entre E et une courbe elliptique de la forme

$$Y^2Z + a_3YZ^2 = X^3 + a_2X^2 + \text{polynôme homogène de degré } \leq 1 \text{ en } X, Z.$$

Le morphisme $[x\colon y\colon z] \mapsto \left[x - \frac{a_2}{3}\colon y - \frac{a_3}{2}x\colon z\right]$ définit un isomorphisme entre E et une courbe elliptique donnée par l'équation (2.2). ∎

2.2 Structure de groupe

Théorème 2.3 — Bézout faible. Soit E une courbe elliptique et L une droite de $\mathbb{P}^2$, alors L coupe E en exactement 3 points comptés avec multiplicité. De plus, si deux des points sont K-rationnels, alors le troisième l'est aussi.

Démonstration. Pour simplifier on suppose que E est donnée par un modèle du type $E\colon y^2 = x^3 + Ax + B$ et on suppose que $L\colon y = ax + b$. On pose $f(X,Y) = Y^2 - (X^3 + AX + B) \in k[X,Y]$. Il s'agit donc de résoudre

$$\begin{cases} y^2 = x^3 + Ax + B \\ y = ax + b \end{cases} \Leftrightarrow \begin{cases} f(x,y) = 0 \\ y = ax + b \end{cases}$$

En remplaçant, dans la première ligne la valeur de y dans la seconde. On est ramené à résoudre l'équation du type $h(X) = f(X, aX+b) = X^3 + \text{polynôme de degré } 2 = 0$.

Tout polynôme de degré n est scindé dans $\bar{k}$, donc h a trois racines x_1, x_2 et x_3 (pas nécessairement distinctes). En réinjectant ces valeurs dans la deuxième ligne on obtient trois points affines $P_1 = (x_1, y_1) = (x_1, ax_1 + b)$, $P_2 = (x_2, y_2)$ et $P_3 = (x_3, y_3)$ (pas nécessairement distincts). Si ces trois points sont distincts on a terminé. On va seulement montrer que si deux points sont identiques, disons $P_1 = P_2$, alors $y = ax + b$ est la tangente à E en P_1 et donc l'intersection est au moins d'ordre 2 d'après l'exercice 1.50. On a dans la base $(X - x_1, Y - y_1)$ de $\bar{k}[X,Y]$,

$$\begin{aligned} f(X,Y) &= \overbrace{f(x_1,y_1)}^{0} + \frac{\partial f}{\partial X}(x_1,y_1)(X-x_1) + \frac{\partial f}{\partial Y}(x_1,y_1)(Y-y_1) + \dots \\ &\text{donc} \\ h(X) &= f(X, aX+b) \\ &= \frac{\partial f}{\partial X}(x_1,y_1)(X-x_1) + \frac{\partial f}{\partial Y}(x_1,y_1)(aX+b-y_1) + \dots \\ &= \frac{\partial f}{\partial X}(x_1,y_1)(X-x_1) + a\frac{\partial f}{\partial Y}(x_1,y_1)(X-x_1) + \dots \text{ car } y_1 = ax_1 + b \\ &= \left(a\frac{\partial f}{\partial Y}(x_1,y_1) + \frac{\partial f}{\partial X}(x_1,y_1)\right)(X-x_1) + \dots \end{aligned}$$

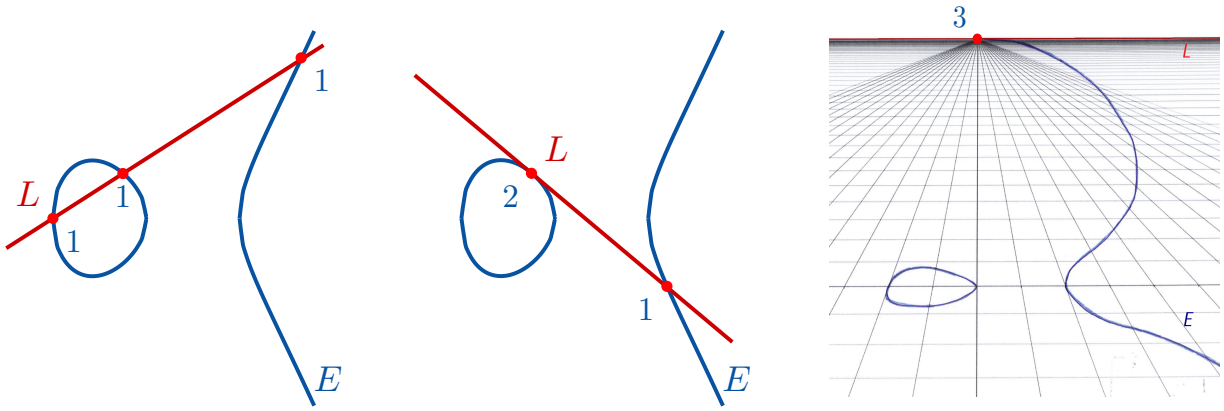
Puisque x_1 est une racine multiple de h, on a $h(X) \in (X-x_1)^2\bar{k}[X]$. Autrement dit, le coefficient en $X - x_1$ de h est nul, *i.e.* $a\partial f/\partial Y(x_1,y_1) + \partial f/\partial X(x_1,y_1) = 0$. Ceci revient à dire que a est le coefficient directeur de la tangente à E en P_1. Par ailleurs, les deux droites passent par le même point, elles sont donc identiques.

D'autre part, si P_1 et P_2 sont K-rationnels, alors par les relations entre coefficients et racines, P_3 est aussi à coordonnées dans K. ■

Rq Il s'agit d'un cas particulier du théorème de Bézout qui affirme que deux courbes projectives planes (pas nécessairement lisses) de degré n et m s'intersectent en exactement $n \cdot m$ points comptés avec multiplicité.

Exercice 2.4 — (★) Quelques éléments manquants de la preuve.

1. Montrer que la droite à l'infini $z = 0$ coupe $E\colon y^2 = x^3 + Ax + B$ en un unique point $O = [0\colon 1\colon 0]$ avec multiplicité d'intersection 3 (on dit que c'est un *point d'inflexion* de E).
2. Montrer que la droite $x = a$ coupe E en trois points distincts dont O si $a^3 + Aa + b \neq 0$, et en $[a\colon 0\colon 1]$ avec multiplicité 2 et O sinon. ■



(a) Trois points de mult. 1 (b) Un point de mult. 2 (c) Un point de mult. 3

FIGURE 2.1 – Intersections d'une droite avec une courbe elliptique

Définition 2.5 — Loi de composition sur une courbe elliptique. Soit E une courbe elliptique sur un corps k donné par le modèle affine $y^2+h(x)y=f(x)$. Étant donné un point affine $R=(x,y)\in E$, le point $\widetilde{R}=(x,-y-h(x))$ est aussi un point de E appelé l'opposé [a] de R. On pose $\widetilde{O}=O$ pour $O=[0:1:0]$ le point à l'infini.

Soient P et Q deux points de E et L la droite passant par P et Q (si $P=Q$ prendre L la tangente à E en P). Soit R le troisième point d'intersection de L avec E. On pose $P+Q=\widetilde{R}$.

a. Si $h=0$, alors $\widetilde{R}$ est juste le symétrique de R par rapport à l'axe des abscisses.

Exercice 2.6 — (★).

1. Pourquoi cette loi est-elle commutative ?
2. Que vaut $O+O$?
3. Soit $P\in E$, distinct de O. Montrer que $P+O=P$, autrement dit que O est l'élément neutre de E pour la loi $+$ (on peut poser $P=[x_0:y_0:z_0]$ et constater que $L:z_0x=x_0z$ est la droite (OP)).
4. Soit $P\in E$, distinct de O. Montrer que $P+\widetilde{P}=O$. ∎

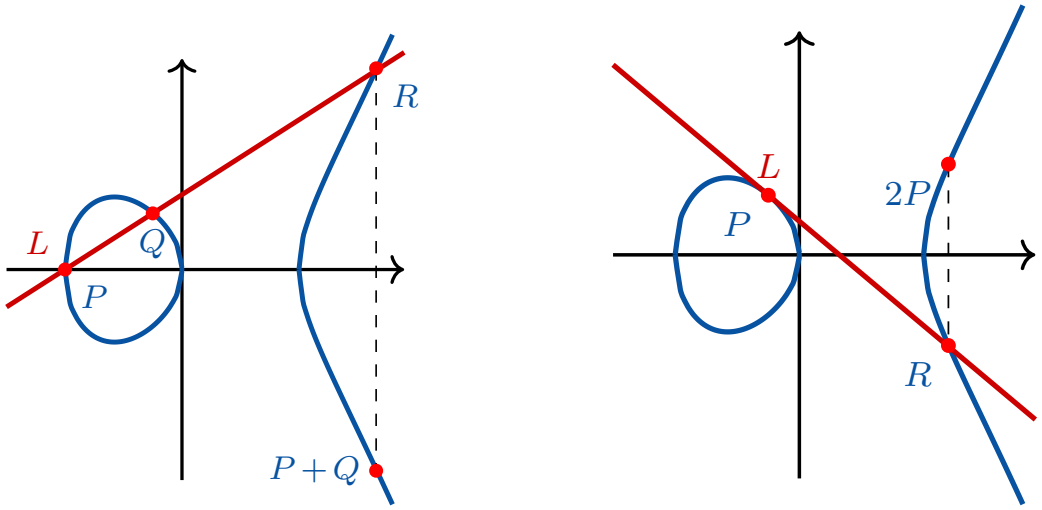
Théorème 2.7 Soit E une courbe elliptique sur un corps k. Alors $(E,+)$ est un groupe commutatif. De plus, pour toute extension de corps $k\to K\to\bar{k}$, $(E(K),+)$ est un sous-groupe de $(E,+)$.

Remarquons que, d'après l'exercice 2.6, il ne reste que l'associativité de la loi $+$ à montrer. Elle découle de la proposition suivante.

Proposition 2.8 Soit E une courbe elliptique sur un corps k et $O=[0:1:0]$ le point à l'infini. Alors l'application

$$\begin{array}{rccc} J: & E & \longrightarrow & \mathrm{Pic}^0(E) \\ & P & \longrightarrow & [P]-[O] \end{array}$$

est une bijection qui satisfait $J(\underbrace{P+Q}_{\text{« + » de } (E,+)}) = \underbrace{J(P)+J(Q)}_{\text{« + » de } (\mathrm{Pic}^0(E),+)}$.



(a) Somme de deux points (b) Duplication d'un point

FIGURE 2.2 – Loi d'addition sur une courbe elliptique

Démonstration.

Injectivité de J : Soient $P, Q \in E$ tels que $J(P) = J(Q)$, *i.e.* $[P] = [Q] \in \mathrm{Pic}^0(E)$. Ceci revient à dire qu'il existe $\alpha \in \bar{k}(E)$ telle que $[P] = [Q] + \mathrm{div}(\alpha) \geq 0 \in \mathrm{Div}(E)$. Autrement dit, $\alpha \in \mathcal{L}([Q])$ mais $\mathcal{L}([Q])$ n'est composé que des fonctions constantes d'après l'exemple 1.54. Donc α est constante, *i.e.* $\mathrm{div}(\alpha) = 0$ et $[P] = [Q] \in \mathrm{Div}(E)$, donc $P = Q$.

Surjectivité de J : Soit $D \in \mathrm{Pic}^0(E)$, un diviseur de degré 0. On a $D + [O]$ de degré 1 donc $\mathcal{L}(D + [O]) = \mathrm{Vect}(\alpha)$ pour une certaine $\alpha \in \bar{k}(E)$ car $\ell(D + [O]) = 1$ d'après le cas d'égalité de l'inégalité de Riemann.
Par définition de $\mathcal{L}(D + [O])$, on a $\mathrm{div}(\alpha) + D + [O] \geq 0$. Il s'agit donc d'un diviseur effectif de degré 1, donc forcément de la forme $[P]$. On a donc

$$D = [P] - [O] = J(P) \in \mathrm{Pic}^0(E).$$

J est un morphisme : On pose $P, Q \in E$, $L\colon ax + by + cz = 0$, la droite (PQ) (ou la tangente à E en P si $P = Q$) et $\widetilde{R}$ le troisième point de l'intersection de L avec E et $R = P + Q$. On pose $L'\colon a'x + b'y + c'z = 0$ la droite $(R\widetilde{R})$ qui coupe E en O aussi (*i.e.* $b' = 0$ mais ça n'a pas d'importance).
On considère $\alpha = (ax + by + cz)/(a'x + b'y + c'z) \in \bar{k}(E)$. Par définition, $ax + by + cz$ s'annule exactement en P, Q et $\widetilde{R}$ et $a'x + b'y + c'z$ en R, $\widetilde{R}$ et O. Autrement dit,

$$\mathrm{div}(\alpha) = \underbrace{[P] + [Q] + [\widetilde{R}]}_{\text{zéros de } \alpha} - \underbrace{\big([R] + [\widetilde{R}] + [O]\big)}_{\text{pôles de } \alpha} = 0 \in \mathrm{Pic}^0(E).$$

Donc $[P] + [Q] - [R] - [O] = 0 \in \mathrm{Pic}^0(E)$, *i.e.*

$$\begin{aligned} J(P+Q) &= [P+Q] - [O] \\ &= [R] - [O] \\ &= [P] - [O] + [Q] - [O] \\ &= J(P) + J(Q). \end{aligned}$$

■

Preuve du théorème 2.7. La bijection J vérifie $J(P+Q) = J(P)+J(Q)$. Puisque $\mathrm{Pic}^0(E)$ est un groupe (par définition) alors $(E,+)$ bénéficie des mêmes propriétés que $(\mathrm{Pic}^0(E),+)$, *i.e.* $+$ admet un élément neutre, tous les éléments ont un inverse et $+$ est associative et commutative.

Montrons par exemple l'associativité. Soient P, Q, R trois points de E alors

$$\begin{aligned} J((P+Q)+R) &= J(P+Q)+J(R) \\ &= (J(P)+J(Q))+J(R) \\ &= J(P)+(J(Q)+J(R)) \\ &= J(P+(Q+R)) \end{aligned}$$

Par injectivité de J on a alors $(P+Q)+R = P+(Q+R) \in E$ donc $(E,+)$ est associatif.

Enfin, pour $k \to K$ une extension, on a $O \in E(K)$, et d'après le théorème 2.3, si $P,Q \in E(K)$ alors $P-Q \in E(K)$, et donc $E(K)$ est un sous-groupe de E. ■

Exercice 2.9 — (★).
Montrer grâce à la bijection J que O est l'élément neutre de $(E,+)$ et que $(E,+)$ est un groupe commutatif. ■

Rq Nous avons développé la théorie des diviseurs qui, comme on vient de le voir, s'avère terriblement efficace pour démontrer le théorème 2.7. Cependant, on aurait pu se passer des diviseurs qui sont des objets compliqués à mettre en place. En effet, l'associativité (le seul axiome réellement difficile à justifier) peut être montrée sans les diviseurs (voir [Mil06, Section I.3] ou encore [Hin08, Chapitre V]).

Rq Ce groupe $\mathrm{Pic}^0(C)$ est d'importance dans l'étude des courbes. On vient de montrer que lorsque C est une courbe elliptique ce groupe peut-être muni d'une structure géométrique en plus de sa structure de groupe (car $\mathrm{Pic}^0(E) \simeq E$). Lorsque C est une courbe qui admet un point rationnel alors c'est toujours vrai que $\mathrm{Pic}^0(C)$ a une structure de variété algébrique, on l'appelle la *jacobienne* de C. Malheureusement ce n'est plus une courbe algébrique en général. Si C est de genre g alors $\mathrm{Pic}^0(C)$ est de dimension g.

Rq Il est très classique faire de la cryptographie sur une courbe elliptique E grâce au problème du logarithme discret sur E. Malheureusement, il existe des algorithmes quantiques efficaces d'attaque du logarithme discret sur une courbe elliptique. En prévision de l'arrivée d'ordinateurs quantiques fonctionnels certain·es mathématicien·nes réfléchissent à des protocoles qui résistent aux attaques quantiques ; il s'agit de la cryptographie post-quantique (*cf.* [Wik]).

2.3 Discriminant et j-invariant

Corps de caractéristique $\neq 2, 3$

Définition 2.10 Soit $E\colon y^2 = x^3+ax+b$ une courbe elliptique. On appelle $\Delta(E) = 4a^3+27b^2$ le *discriminant* de E, et $j(E) = 1728 \cdot 4a^3/(4a^3+27b^2)$ le j-invariant de E.

Théorème 2.11 Soit $E = E_{a,b}$ la courbe d'équation $y^2 = x^3+ax+b$.

1. $E_{a,b}$ est singulière si et seulement si $\Delta(E) = 4a^3+27b^2 = 0$.
2. Il existe un isomorphisme $E_{a',b'} \to E_{a,b}$ qui envoie $[0\colon 1\colon 0]$ sur $[0\colon 1\colon 0]$ si et seulement s'il existe $c \in k \setminus \{0\}$ tel que $a' = c^4 a$ et $b' = c^6 b$.
3. On suppose E lisse. Alors $j(E)$ caractérise la classe d'isomorphisme de E sur $\bar{k}$. C'est à dire que $E' = E_{a',b'}$ est isomorphe sur $\bar{k}$ à E si et seulement si $j(E') = j(E)$.

Démonstration.

1. D'après l'exercice 1.9, la courbe $E_{a,b}$ a un point singulier affine si et seulement si $4a^3+27b^2=0$. Et le même argument que dans l'exemple 1.22 montre que le point $[0:1:0]$ n'est jamais singulier.
2. et 3. Voir [Mil06, Theorem II.2.1]. ■

Cas général

Soit $E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ une courbe cubique. On pose

$$b_2=a_1^2+4a_2,\quad b_4=2a_4+a_1a_3,\quad b_6=a_3^2+4a_6,\quad b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2,$$

puis

$$c_4=b_2^2-24b_4,\ \Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6 \text{ et } j=c_4^3/\Delta \text{ (lorsque } \Delta\neq 0).$$

Définition 2.12 Avec les notations ci-dessus on appelle Δ le *discriminant* de E et j le j-invariant de E.

Théorème 2.13 Soit $E=E_{a,b}$ la courbe d'équation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$.

1. E est singulière si et seulement si $\Delta=0$.
2. On suppose E lisse. Alors j caractérise la classe d'isomorphisme de E sur $\bar{k}$. C'est à dire que $E'=E_{a',b'}$ est isomorphe sur $\bar{k}$ à E si et seulement si $j(E')=j(E)$.

Il existe une version du point 2. du théorème 2.11 dans le cas général mais son énoncé est fastidieux. On le retrouve dans [Mil06, Theorem 2.4.(b)].

2.4 Formules d'addition

Corps de caractéristique $\neq 2, 3$

Soit $E_{a,b}$ une courbe elliptique sur un corps k. Soit $P_1=[x_1:y_1:1]$, $P_2=[x_2:y_2:1]\in E$ et $P=P_1+P_2$.

Inverse : Si $P_1=-P_2=[x_1:-y_1:1]$, alors $P=O$.

Formule d'addition : Si $P_1\neq P_2$ et $P_1\neq -P_2$, alors $P=[x:y:1]=P_1+P_2$ avec

$$x=\frac{1}{(x_1-x_2)^2}\left(x_1x_2^2+x_1^2x_2-2y_1y_2+a(x_1+x_2)+2b\right),$$
$$y=\frac{1}{(x_1-x_2)^3}\left(W_2y_2-W_1y_1\right)$$

avec

$$W_1=3x_1x_2^2+x_2^3+a(x_1+3x_2)+4b,$$
$$W_2=3x_2x_1^2+x_1^3+a(x_2+3x_1)+4b.$$

Formule de duplication : Si $P_1=P_2$. Alors si $y_1=0$, on a $2P_1=O$.

Sinon $P=[x:y:1]=2P_1$ avec

$$x=\frac{(3x_1^2+a)^2-8x_1y_1^2}{4y_1^2},$$
$$y=\frac{x_1^6+5ax_1^4+20bx^3-5a^2x_1^2-4abx-a^3-8b^2}{8y_1^3}.$$

■ **Exemple 2.14** On considère $E\colon y^2 = x^3 + x + 1$ sur $\mathbb{F}_7$. La courbe E a 5 points rationnels (donc $(E(\mathbb{F}_7), +) \simeq \mathbb{Z}/5\mathbb{Z}$). On considère $P_1 = (0,1)$ et $P_2 = (2,2)$. Alors $P = (x,y) = P_1 + P_2$ avec

$$x = \frac{1}{(0-2)^2}(-2\cdot 2 + 2 + 2) = 0 \quad \text{et} \quad y = \frac{1}{(0-2)^3}(W_2 \cdot 2 - W_1) = -(6\cdot 2 - 4) = -1.$$

Donc $P_1 + P_2 = (0,-1)$. ■

Cas général

On considère une courbe elliptique $E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Soit $P_1 = [x_1 : y_1 : 1], P_2 = [x_2 : y_2 : 1] \in E$ et $P = P_1 + P_2$.

Inverse : Alors $-P_1 = [x_1 : -y_1 - a_1x_1 - a_3 : 1]$ et $P_1 - P_1 = O$.

Formule d'addition et de duplication : On pose $y = \lambda x + \nu$, avec λ et ν définis par la table 2.1, la droite passant par P_1 et P_2 ou la droite tangente à E en P_1 si $P_1 = P_2$. Le point $P = (x,y) = P_1 + P_2$ satisfait

$$x = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y = -(\lambda + a_1)x - \nu - a_3.$$

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

TABLE 2.1 – Pente λ et ordonnée à l'origine ν de la droite (P_1P_2).

2.5 Isogénie et torsion

2.5.1 Torsion

Soit $E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. On dit qu'un point $P \in E$ est de *m-torsion* si $[m]P = \underbrace{P + \cdots + P}_{m \text{ fois}} = 0$. On note $E[m] = \{\text{points de m-torsion de } E\}$.

On définit les *polynômes de m-division* $\psi_m \in \mathbb{Z}[a_1, \ldots, a_6, x, y]$ par

$$\psi_1 = 1,$$
$$\psi_2 = 2y + a_1x + a_3,$$
$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$
$$\psi_4 = \psi_2 \cdot \left(2x^6 + b_2x^5 + 5b_4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\right),$$

où les b_i sont définies dans la section 2.3, et par récurrence ensuite

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \text{ pour } m \geq 2,$$
$$\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2, \text{ pour } m \geq 3.$$

Enfin, on pose

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \quad \text{et} \quad 2\psi_2\omega_m = \psi_{m-2}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.$$

Théorème 2.15 Soit $E_{a_1,\dots,a_6}$ une courbe elliptique et $P=(x_P,y_P)\in E$. Alors

1. On a $[m]P=\underbrace{P+\cdots+P}_{m \text{ fois}}=\left(\dfrac{\phi_m(P)}{\psi_m(P)^2},\dfrac{\omega_m(P)}{\psi_m(P)^3}\right)$.
2. La fonction ψ_m (et donc aussi ϕ_m) vue dans $k(E)$ a un représentant dans $k[X]$ (on peut donc la considérer comme une fonction polynomiale).
3. On a $\deg\phi_m=m^2$ et $\deg\psi_m^2\leq m^2-1$.
4. On a $[m]P=0$ si et seulement si $\psi_m(x_P)=0$. En d'autres termes, les racines de ψ_m sont exactement les abscisses des points de m-torsion de E.

■ **Exemple 2.16 — (script MAGMA).**

```
> Pol<x> := PolynomialRing(GF(7));
> f := x^3 + x + 1;
> E := EllipticCurve(f);        // E : y^2 = f(x)
> #E;
5
> psi3 := Pol!DivisionPolynomial(E, 3); psi3;
3*x^4 + 6*x^2 + 5*x + 6
> K<a> := SplittingField(psi3) ;
> Roots(ChangeRing(psi3, K));   // psi3 est scindé dans K ?
[ <a^5, 1>, <a^33, 1>, <a^35, 1>, <a^39, 1> ]
> Degree(K);                    // K est de degré 2 ?
2
> // On a les abscisses x0, quelles sont les ordonnées y0 = +/-f(x0) ?
> IsSquare(K!Evaluate(f, a^5));  //On vérifie si f(a^5) est un carré dans K
false
> PolK<y> := PolynomialRing(K);
> L<b> := ext<K|y^2-Evaluate(f, a^5)>; // On étend encore notre corps
> P := RationalPoints(E, L)![a^5, b];  // P est de 3-torsion ?
> 3*P;
(0 : 1 : 0)
> T3 := TorsionSubgroupScheme(E, 3);   // Autre solution
> RationalPoints(T3, L);               // Les 9 points de torsion de E sur L
{@ (a^35 : a^15*b : 1), (a^35 : a^39*b : 1), (a^39 : a^22*b : 1), (a^39 : a^46*b :
    1), (a^5 : b : 1), (a^5 : 6*b : 1), (a^33 : a*b : 1), (a^33 : a^25*b : 1), (0 : 1
: 0) @}
> // D'après le Théorème 2.6.4, i.e. E(L) contient un sous-groupe d'ordre 9.
> N := #RationalPoints(E, GF(7^Degree(L)));
> N, ":", Factorization(N);
2475 : [ <3, 2>, <5, 2>, <11, 1> ]
```

■

Rq Étant donnée une courbe elliptique $E\colon y^2+yh(x)=f(x)$ sur un corps k, ces formules nous permettent de déterminer la plus petite extension K de k telle que $E[m]\subseteq E(K)$. Il s'agit de la plus petite extension de k contenant toutes les racines $x_1,\dots,x_r$ de ψ_m ainsi que des éléments y_i tels que $y_i^2+y_ih(x_i)=f(x_i)$ pour tout i.

Exercice 2.17 — (★).

On pose $\mathbb{F}_9=\mathbb{F}_3[i]=\mathbb{F}_3[X]/\langle X^2+1\rangle$ (i est la classe de X dans $\mathbb{F}_3[X]/\langle X^2+1\rangle$, i.e. $i^2=-1$). On pose $E\colon y^2=x^3+x+i$ sur $\mathbb{F}_9$.

1. Montrer que les carrés de $\mathbb{F}_9$ sont $\{0,\,1,\,2,\,i,\,2i\}$.
2. Montrer que pour tout $x=a+ib\in\mathbb{F}_9$, $x^3+x+i=2a+i$.
3. En vous servant de la question précédente montrer que $\#E(\mathbb{F}_9)=7$. On admet que $\#E(\mathbb{F}_{81})=91$.

4. On admet que le polynôme de 4-division de E est

$$\psi_4 = 2X^9 + X + 2i = 2\,(X^3 + X + i)\,(X^3 + X + i + 1)\,(X^3 + X + i + 2)\,.$$

   a. Pourquoi peut-on affirmer que les trois polynômes de la factorisation de ψ_4 sont irréductibles ?
   b. Pourquoi peut-on affirmer que la 4-torsion de E est dans $E(\mathbb{F}_{9^3})$? ■

2.5.2 Isogénies

Définition 2.18 — Isogénie. Soient E_1 et E_2 deux courbes elliptiques dont on note O les points à l'infini. Une isogénie de E_1 vers E_2 est un morphisme $\phi\colon E_1 \to E_2$ tel que $\phi(O) = O$. On dit que deux courbes sont isogènes s'il existe une isogénie entre les deux.

On pose $\mathrm{Hom}(E_1, E_2)$ le groupe des isogénies de E_1 vers E_2 où la somme de deux isogénies ϕ et ψ est donnée par $(\phi+\psi)(P) = \phi(P) + \psi(P)$ et $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ appelé l'*anneau d'endomorphismes* de E où la multiplication est donnée par la composition.

Proposition 2.19 Soit E_1, E_2 des courbes elliptiques et $\phi\colon E_1 \to E_2$ une isogénie. Alors ϕ est un morphisme de groupes, *i.e.* pour tout $P, Q \in E_1$ on a

$$\phi(\underbrace{P+Q}_{(E_1,+)}) = \underbrace{\phi(P)+\phi(Q)}_{(E_2,+)}.$$

Démonstration. Remarquons qu'une isogénie $\phi\colon E_1 \to E_2$ induit un morphisme [1] de groupes

$$\begin{array}{rccc} \phi_*\colon & \mathrm{Pic}^0(E_1) & \longrightarrow & \mathrm{Pic}^0(E_2) \\ & \sum n_P[P] & \longmapsto & \sum n_P[\phi(P)]\,. \end{array}$$

En posant $J_i\colon E_i \longrightarrow \mathrm{Pic}^0(E_i)$ les isomorphismes de groupes donnés par le théorème 2.7 on a alors un diagramme commutatif,

$$\begin{array}{ccc} E_1 & \xrightarrow{J_1} & \mathrm{Pic}^0(E_1) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E_2 & \xleftarrow[J_2^{-1}]{} & \mathrm{Pic}^0(E_2)\,. \end{array}$$

On a alors $\phi = J_2^{-1} \circ \phi_* J_1$ qui est un morphisme de groupe, car composé de trois morphismes de groupes. ■

Proposition 2.20 Soit $E_i\colon y^2 = f_i(x)$ deux courbes elliptiques sur un corps k de caractéristique $\neq 2$ et $\phi \in \mathrm{Hom}(E_1, E_2)$ une isogénie. Alors il existe des polynômes $U_1, V_1, U_2, V_2 \in k[X]$ tels que

$$\phi(x, y) = \left(\frac{U_1(x)}{V_1(x)}, y\frac{U_2(x)}{V_2(x)}\right).$$

1. Le fait que ϕ_* passe au quotient provient de la relation $\phi_* \operatorname{div} \alpha = \operatorname{div} \phi_* \alpha$ où l'application $\phi_*\colon k(E_1) \to k(E_2)$ est définie dans [Sil09, Section II.2], nous ne détaillerons pas d'avantage ici.

Démonstration. On pose $P=(x,y)\in E_1$. On rappelle que d'après la proposition 1.39 qu'on peut représenter un morphisme par deux fonctions rationnelles $g_1,g_2\in k(E_1)$ de telle sorte que

$$\phi(x,y)=(g_1(x,y),g_2(x,y))=\left(\frac{p_1(x)+yp_2(x)}{q_1(x)+yq_2(x)},\frac{r_1(x)+yr_2(x)}{s_1(x)+ys_2(x)}\right)$$

(par hypothèse $y^2\in yk[x]+k[x]$). Par ailleurs,

$$\frac{p_1(x)+yp_2(x)}{q_1(x)+yq_2(x)}=\frac{(p_1(x)+yp_2(x))(q_1(x)-yq_2(x))}{q_1(x)^2-y^2q_2(x)^2}=\frac{U_1(x)+yp_3(x)}{V_1(x)}.$$

Mais d'après la proposition 2.19, ϕ est un morphisme de groupes [2] donc $\phi(-P)=-\phi(P)$,

$$\frac{U_1(x)+yp_3(x)}{V_1(x)}=\frac{U_1(x)-yp_3(x)}{V_1(x)}.$$

Ceci implique $p_3=0$. De la même manière, on a

$$\frac{r_1(x)+yr_2(x)}{s_1(x)+ys_2(x)}=\frac{r_3(x)+yU_2(x)}{V_2(x)}=-\frac{r_3(x)-yU_2(x)}{V_2(x)},$$

donc $r_3=0$. Ce qui prouve le résultat. ■

Définition 2.21 — Degré et séparabilité. Soit E une courbe elliptique sur un corps k. Soit $\phi\in\mathrm{End}(E)$ donnée par $\phi(x,y)=(U_1(x)/V_1(x),yU_2(x)/V_2(x))$ avec U_1 et V_1 premiers entre eux. Alors on pose $\deg\phi=\max\{\deg U_1,\deg V_1\}$ appelé le degré de ϕ.

On dit que ϕ est un endomorphisme séparable si $(U_1(x)/V_1(x))'\neq 0$. Autrement, on dit que ϕ est inséparable.

▪ **Exemple 2.22** L'exemple le plus classique d'isogénie est l'application de multiplication par m pour un entier $m\in\mathbb{Z}$, que l'on note ainsi

$$\begin{array}{rccc}[m]_E \text{ ou } [m]: & E & \longrightarrow & E\\ & P & \longrightarrow & \underbrace{P+\cdots+P}_{m\text{ fois}}.\end{array}$$

Il s'agit d'un endomorphisme et son degré est m^2 d'après le théorème 2.15.3. ▪

Théorème 2.23 Soit E une courbe elliptique et $\phi\in\mathrm{End}(E)$ un endomorphisme non nul de degré m. Alors

1. $\phi^{-1}(O)=\ker\phi$ est un sous-groupe fini de E.
2. Lorsque ϕ est séparable, on a alors
$$\#\ker\phi=\deg\phi$$
3. Si m est premier à la caractéristique de k, alors ϕ est séparable.
4. Si m est premier à la caractéristique de k, alors
$$E[m]=\ker[m]\simeq\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}.$$
5. Si $p=\mathrm{char}\,k$, alors $E[p]\simeq\mathbb{Z}/p\mathbb{Z}$ ou $E[p]\simeq\{O\}$.
6. Soit $\psi\in\mathrm{End}(E)$, alors $\deg(\phi\psi)=\deg(\phi)\deg(\psi)$.

2. On se sert de l'hypothèse $\mathrm{char}\,k\neq 2$ ici pour que l'expression de $-P$ soit $(x,-y)$. Si l'on avait $E_1: y^2+yh_1(x)=f_1(x)$, alors on aurait $-P=(x,-y-h_1(x))$.

Rq De façon alternative, un morphisme $\phi\colon E_1 \to E_2$ non constant induit une extension de corps $\phi^*\colon k(E_2) \to k(E_1)$. Le degré $\deg\phi$ d'une isogénie ϕ est le degré de l'extension de corps $k(E_1)/\phi^*(k(E_2))$. On pose $\deg 0 = 0$ pour l'application nulle. On applique alors le même vocabulaire pour ϕ que pour l'extension correspondante. On dit que ϕ est une isogénie séparable (resp. purement inséparable, inséparable) si $k(E_1)/\phi^*(k(E_2))$ est séparable (resp. purement inséparable, inséparable). On note aussi $\deg_s\phi$ et $\deg_i\phi$ pour les degrés de séparabilité et inséparabilité de ϕ.

Exercice 2.24 — (★★).
Soit k un corps de caractéristique p et $f \in k[X]$ un polynôme.
1. Montrer que $f' = 0$ si et seulement si $f(X) = g(X^p)$ pour un certain $g \in k[X]$.
2. On pose $\phi\colon E_1 \to E_2$ une isogénie telle que $\phi(x,y) = \left(\frac{U_1(x)}{V_1(x)}, y\frac{U_2(x)}{V_2(x)}\right)$ avec U_1 et V_1 premiers entre eux.
   a. Montrer que si ϕ est inséparable si et seulement si $U_1' = V_1' = 0$, *i.e.* $U_1(x)/V_1(x) = r(x^p)$ pour un certain $r \in k(X)$.
   b. En déduire que si ϕ est inséparable alors $p | \deg\phi$.
   c. En déduire que si m et p sont premiers entre eux alors $[m]_{E_1}$ est toujours séparable. ∎

2.5.3 Isogénie duale

Théorème 2.25 Soit $\phi\colon E_1 \to E_2$ une isogénie non nulle de degré m entre deux courbes elliptiques sur un corps k. Alors il existe une unique isogénie $\widehat{\phi}\colon E_2 \to E_1$ telle que

$$\phi \circ \widehat{\phi} = [m]_{E_2} \text{ et } \widehat{\phi} \circ \phi = [m]_{E_1}$$

appelée l'*isogénie duale* ou *contragrédiente* à ϕ.

Ceci montre que la relation $E_1 \sim E_2$ s'il existe une isogénie $E_1 \to E_2$ est une relation d'équivalence (la symétrie était le seul point difficile). La classe d'équivalence d'une courbe E pour cette relation est appelée *classe d'isogénie* de E.

Proposition 2.26 Soit $\phi, \psi \in \mathrm{End}(E)$. Alors, on a
1. $\widehat{\phi+\psi} = \widehat{\phi} + \widehat{\psi}$,
2. $\widehat{\phi\psi} = \widehat{\psi}\widehat{\phi}$.
3. $\widehat{\widehat{\phi}} = \phi$.
4. $\phi + \widehat{\phi} = [1 + \deg\phi - \deg(1-\phi)]$.

Définition 2.27 — Trace. On définit la trace d'un endomorphisme $\phi \in \mathrm{End}(E)$ comme l'entier

$$\mathrm{Tr}(\phi) = 1 + \deg\phi - \deg(1-\phi).$$

Exercice 2.28 — (★).
Soient $\phi, \psi \in \mathrm{End}(E)$, montrer que
1. $\mathrm{Tr}(\phi+\psi) = \mathrm{Tr}(\phi) + \mathrm{Tr}(\psi)$.
2. $\mathrm{Tr}\left(\widehat{\phi}\right) = \mathrm{Tr}(\phi)$
3. $\deg(\phi+\psi) = \deg(\phi) + \deg(\psi) + \mathrm{Tr}(\widehat{\phi}\psi)$
4. $\mathrm{Tr}([m]\circ\phi) = m\,\mathrm{Tr}(\phi)$. ∎

Exercice 2.29 — (★).
Soit $E\colon y^2 = f(x)$ une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ avec q impair. On considère le morphisme

$$\begin{array}{rccc} \phi_q\colon & E & \longrightarrow & E \\ & (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

Montrer que ϕ_q est une isogénie inséparable de degré q. On l'appelle l'endomorphisme de Frobenius de E. ∎

3. Courbes elliptiques sur les corps finis

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, alors $E(\mathbb{F}_q) \subseteq \mathbb{P}^2(\mathbb{F}_q)$. On a donc en particulier,

$$\#E(\mathbb{F}_q) \leq \#\mathbb{P}^2(\mathbb{F}_q) = q^2+q+1\,.$$

Mais on va voir dans ce chapitre que l'on peut obtenir une borne beaucoup plus précise de $\#E(\mathbb{F}_q)$.

Nous allons aussi voir que connaissant $\#E(\mathbb{F}_q)$, on est capable de calculer $\#E(\mathbb{F}_{q^m})$ pour tout $m \geq 1$. En d'autres termes, le nombre de point $\mathbb{F}_q$-rationnels d'une courbe elliptique sur un corps fini détermine son nombre de points rationnels sur toute extension finie de $\mathbb{F}_q$.

3.1 Structure de $E(\mathbb{F}_q)$

Proposition 3.1 Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, alors

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z} \quad \text{ou} \quad E(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \text{ avec } n \,|\, m\,.$$

Démonstration. On sait que $E(\mathbb{F}_q)$ est un groupe fini commutatif. Donc, d'après le théorème de structure des groupes finis commutatifs, il existe des entiers $n_1 \,|\, n_2 \,|\, \ldots \,|\, n_r$ tels que

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}\,.$$

Soit ℓ un diviseur premier de n_1 (donc de tous les autres n_i). Puisque $\mathbb{Z}/n_i\mathbb{Z}$ est cyclique, il a ℓ éléments d'ordre qui divise ℓ. Ainsi, $E(\mathbb{F}_q)$ a ℓ^r éléments d'ordre qui divise ℓ (donc de ℓ-torsion). Mais, puisque $\#E[\ell] \leq \ell^2$, il suit $r \leq 2$. ■

3.2 Borne de Hasse et nombre de points rationnels

3.2.1 Borne de Hasse

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. On pose

$$\begin{array}{rccc} \phi_q\colon & E & \longrightarrow & E \\ & (x,y) & \longmapsto & (x^q, y^q)\,, \end{array}$$

l'endomorphisme de Frobenius de E qui, d'après l'exercice 2.29, est un élément de E de degré q et inséparable. On définit la trace de E par $t_E = \mathrm{Tr}(\phi_q)$.

Proposition 3.2 Avec les notations ci-dessus, on a $\#E(\mathbb{F}_q) = 1 + q - t_E$.

Démonstration. On remarque que $P = (x, y) \in E$ est un point rationnel si et seulement si ses coordonnées sont dans $\mathbb{F}_q$, *i.e.* $\phi_q(P) = (x^q, y^q) = (x, y) = P$.

Autrement dit, $P \in E(\mathbb{F}_q)$ si et seulement si $P \in \ker(1 - \phi_q)$. Par ailleurs, en admettant que la somme d'endomorphismes inséparables est elle-même inséparable (ceci découle de [Sut17, Note 7, Lemma 7.18] par exemple), l'endomorphisme $1 - \phi_q$ est un endomorphisme séparable. Autrement, $(1 - \phi_q) + \phi_q = 1$ serait inséparable et ce n'est pas le cas.

On en déduit du théorème 2.23.2 que $\deg(1 - \phi_q) = \#\ker(1 - \phi_q) = \#E(\mathbb{F}_q)$, puis de la proposition 2.26.3 que

$$\#E(\mathbb{F}_q) = \deg(1 - \phi_q) = \deg(1) + \deg(\phi_q) - \mathrm{Tr}(\phi_q) = 1 + q - t_E.$$

■

Théorème 3.3 — Borne de Hasse. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. Alors

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Démonstration. On considère l'endomorphisme $[n] \circ \phi_q + [m]$ pour m premier à q. L'endomorphisme $[m]$ est séparable (voir l'exercice 2.24). Par un argument du même type, on en déduit aussi que $[n] \circ \phi_q + [m]$ est séparable. Donc, grâce à l'exercice 2.28, on a

$$\deg([n] \circ \phi_q + [m]) = \\ \deg([n] \circ \phi_q) + \deg([m]) + \mathrm{Tr}([n] \circ \phi_q \circ [m]) = n^2 q + m^2 + nm\, t_E \geq 0.$$

Si bien que pour tout entier n et pour tout entier m premier à q, on a

$$q\left(\frac{n}{m}\right)^2 + t_E \frac{n}{m} + 1 \geq 0.$$

Puisque l'ensemble $\{n/m,\ n \in \mathbb{Z},\ m \in \mathbb{Z} \text{ premier à } p\}$ est dense dans $\mathbb{R}$, on a

$$\forall x \in \mathbb{R}, \quad q x^2 + t_E x + 1 \geq 0.$$

Le discriminant de $qX^2 + t_E X + 1$ est donc négatif, *i.e.* $|t_E| \leq 2\sqrt{q}$. On conclut grâce à la proposition 3.2. ■

3.2.2 Polynôme caractéristique de E

Proposition 3.4 Soit E une courbe elliptique sur un corps k et $\phi \in \mathrm{End}(E)$ son endomorphisme de Frobenius. Alors, le polynôme

$$\chi_\phi = T^2 - \mathrm{Tr}(\phi)\, T + \deg \phi \ \in \ \mathbb{Z}[T]$$

annule ϕ, *i.e.* $\phi^2 - [\mathrm{Tr}(\phi)]_E \circ \phi + [\deg \phi]_E = 0 \in \mathrm{End}(E)$.

Démonstration. On a $\phi^2 - [\mathrm{Tr}(\phi)]\phi + [\deg \phi] = \phi^2 - (\phi + \widehat{\phi})\phi + \widehat{\phi}\phi = 0$. ■

En particulier, pour ϕ_q, le morphisme de Frobenius sur une courbe E sur $\mathbb{F}_q$, on a $\chi_E = \chi_{\phi_q} = T^2 - t_E T + q = 0 \in \mathbb{Z}[T]$ qui annule ϕ_q. On appelle χ_E le *polynôme caractéristique* de E.

Théorème 3.5 Soit E une courbe elliptique sur $\mathbb{F}_q$ et $\chi_E = T^2 - t_E T + q \in \mathbb{Z}[T]$ le polynôme caractéristique de E et α, β les deux racines de χ_E dans $\bar{\mathbb{Q}}$. Alors

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

Démonstration. Voir l'exercice 3.6. ■

Rq On peut penser à une démonstration qui se base sur l'égalité

$$\mathrm{Tr}(\phi_q) = \mathrm{Tr}_{\mathbb{Q}(\phi_q)/\mathbb{Q}}(\phi_q)$$

où $\mathrm{Tr}_{\mathbb{Q}(\phi_q)/\mathbb{Q}}$ désigne la forme trace sur l'extension de corps $\mathbb{Q}(\phi_q)/\mathbb{Q}$. L'égalité n'est pas vraie lorsque $\mathbb{Q}(\phi_q) = \mathbb{Q}$ (*i.e.* lorsque ϕ_q est la multiplication par un entier). Mais cette distinction complique la preuve au lieu de la simplifier.

Il est possible de corriger le problème en justifiant que $\mathbb{Q}(\phi_q)$ est toujours inclus dans une extension K de $\mathbb{Q}$ de degré 2. Dans ce cas on a toujours $\mathrm{Tr}(\phi_q) = \mathrm{Tr}_{\mathbb{Q}(\phi_q)/\mathbb{Q}}(\phi_q)$ sans condition sur ϕ_q. Mais ce résultat nécessite de travailler plus en détail sur la structure d'anneau de $\mathrm{End}(E)$.

Ce résultat est intéressant car il permet de calculer le nombre de point $\mathbb{F}_{q^n}$-rationnels d'une courbe elliptique pour tout n sachant son nombre de point $\mathbb{F}_q$-rationnels. Voici comment on procède :

1. On calcule $\#E(\mathbb{F}_q)$.
2. On en déduit t_E, la trace de E et $\chi_E = T^2 - t_E T + q$.
3. On calcule α et β les racines de χ_E.
4. On applique le théorème 3.5.

Exercice 3.6 Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. On pose $\chi_E = T^2 - t_E T + q \in \mathbb{Z}[T]$ le polynôme caractéristique de E, α et β ses racines, $t_E = \alpha + \beta$ la trace de E. On considère la suite $s_n = \alpha^n + \beta^n$.

1. Justifier que $\beta = \bar{\alpha}$.
2. Montrer que $|\alpha| = |\beta| = \sqrt{q}$.
3. Montrer que pour tout $n \geq 1$, on a $s_{n+1} = t_E s_n - q s_{n-1}$.
4. Montrer que pour tout $n \geq 1$, le polynôme $T^{2n} - s_n T^n + q^n$ est divisible par $T^2 - t_E T + q$. En déduire que la trace de $\phi_{q^n} = \phi_q^n$ est égale à s_n et que

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

■

■ **Exemple 3.7** On considère la courbe $y^2 = x^3 + x + 2$ sur $\mathbb{F}_5$, dont on peut facilement prouver qu'elle a 4 points rationnels. On a $\#E(\mathbb{F}_5) = 5 + 1 - t_E = 4$, donc $t_E = 2$. On en déduit que $\chi_E = T^2 - 2T + 5$, qui a pour discriminant $\Delta = 2^2 - 20 = -16$. Ses racines sont donc $1 \pm 2i$. On peut vérifier que $\#E(\mathbb{F}_5) = 5 + 1 - (1 + 2i + 1 - 2i)$. On a aussi

$$\#E(\mathbb{F}_{25}) = 25 + 1 - ((1+2i)^2 + (1-2i)^2) = 26 - (1 + 4i - 4 + 1 - 4i - 4) = 26 + 6 = 32.$$

■

Exercice 3.8 — (★).
On considère la courbe $E\colon y^2 = x^3 + x + i$ sur $\mathbb{F}_9 = \mathbb{F}_3[i] = \mathbb{F}_3[X]/\langle X^2+1\rangle$ de l'exercice 2.17. On y conclut que $\#E(\mathbb{F}_9) = 7$, puis on y admet que $\#E(\mathbb{F}_{81}) = 91$.
À prouver ! ∎

3.2.3 Nombre de points et symbole de Legendre

On considère $\left(\frac{\cdot}{q}\right)$, le symbole de Legendre sur $\mathbb{F}_q$ avec q impair (voir l'appendice A pour la définition et les propriétés du symbole).

Proposition 3.9 Soit $E\colon y^2 = f(x)$, avec f de degré 3, une courbe elliptique sur $\mathbb{F}_q$ alors

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{f(x)}{q}\right).$$

Démonstration. On fixe $x \in \mathbb{F}_q$. Il s'agit de l'abscisse d'un point $P = (x,y)$ de E si et seulement si $y^2 = f(x)$, *i.e.* $f(x)$ est un carré dans $\mathbb{F}_q$. Si $f(x)$ est un carré non nul alors $y^2 = f(x)$ a deux solutions y_1, y_2 distinctes, si $f(x) = 0$ alors la seule solution de $y^2 = f(x)$ est $y_0 = 0$.

On peut vérifier que la quantité $\left(\frac{f(x)}{q}\right) + 1 \in \mathbb{Z}$ est le nombre de solutions de $y^2 = f(x)$. On en déduit que

$$\#E(\mathbb{F}_q) = \underbrace{1}_{[0\colon 1\colon 0]} + \underbrace{\sum_{x\in\mathbb{F}_q} \left(\left(\frac{f(x)}{q}\right) + 1\right)}_{\text{points affines}} = q + 1 + \sum_{x\in\mathbb{F}_q} \left(\frac{f(x)}{q}\right).$$

■

3.3 Courbes elliptiques supersingulières

Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ de caractéristique p. On rappelle que $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ ou $E[p] = \{O\}$. Dans le premier cas, on dit que E est une courbe elliptique *ordinaire* et dans le second cas, on dit que E est *supersingulière*.

Rq Attention, le terme « supersingulière » s'oppose à « ordinaire » dans le sens qu'il y a beaucoup de courbes ordinaires, elles sont très communes, donc « supersingulière » est à comprendre comme « super rare ». Les *courbes supersingulières* sont toujours lisses, donc *ne sont pas singulières* !

Proposition 3.10 Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ alors
1. E est supersingulière si et seulement si $t_E = 0 \bmod p$;
2. si $q = p$ et $p \geq 5$, alors E est supersingulière si et seulement si $t_E = 0$, *i.e.*

$$\#E(\mathbb{F}_p) = p + 1.$$

Démonstration. Voir l'exercice 3.11. ■

Exercice 3.11 — (★★).

Soit E une courbe elliptique de trace t_E définie sur un corps fini $\mathbb{F}_q$ avec $q = p^r$. On considère la suite s_n de l'exercice 3.6.

1. Montrer que pour $n \geq 1$, on a $s_n = t_E^n \bmod p$. En déduire que pour tout $n \geq 1$, on a $\#E(\mathbb{F}_{q^n}) = 1 - t_E^n \bmod p$.
2. Montrer que si $t_E = 0 \bmod p$, alors E est supersingulière.
3. On suppose que $t_E \neq 0 \bmod p$.
   a. Montrer que $E(\mathbb{F}_{q^{p-1}})$ contient un élément d'ordre p (petit théorème de Fermat).
   b. En déduire que E n'est pas supersingulière.
4. On suppose que $q = p$ (i.e. $r = 1$) et $p \geq 5$.
   a. Montrer que E est supersingulière si et seulement si $t_E = 0$.
   b. Montrer que
      — si n est impair : $\#E(\mathbb{F}_{p^n}) = p^n + 1$,
      — si n est pair : $\#E(\mathbb{F}_{p^n}) = \left(p^{n/2} - (-1)^{n/2}\right)^2$. ■

II Applications

Introduction

Dans cette seconde partie, nous abordons deux questions essentielles.

— Étant donné un corps fini $\mathbb{F}_q$ et un entier N, comment trouver une courbe elliptique sur $\mathbb{F}_q$ ayant N point rationnels (si une telle courbe existe) ?
— Comment calculer efficacement le nombre de points rationnels d'une courbe elliptique définie sur un corps fini ?

Pour répondre à la première question, nous avons besoin d'aborder au chapitre 5 la théorie des courbes elliptiques sur le corps des complexes et d'étudier plus en détails l'anneau des endomorphismes des courbes elliptiques. En particulier, nous avons le théorème suivant.

Théorème 3.12 Soit E une courbe elliptique sur un corps k. Alors $\mathrm{End}_{\bar{k}}(E)$ est un $\mathbb{Z}$-module sans torsion de rang 4 au plus.

Plus précisément $\mathrm{End}(E)$ est :

— soit $\mathbb{Z}$, *i.e.* $\mathrm{End}(E) = \{[n]_E : n \in \mathbb{Z}\}$ (rang 1) ;
— soit un ordre dans un corps quadratique imaginaire (rang 2) ;
— soit un ordre dans une algèbre de quaternions (rang 4, E est supersingulière).

Lorsque k est de caractéristique positive, seuls les deux derniers cas sont possibles. Lorsque k est de caractéristique 0, seuls les deux premiers sont possibles.

Ici, nous nous intéressons exclusivement aux courbes dont l'anneau des endomorphismes est un ordre dans un corps quadratique imaginaire, que nous abrégeons en « ordre quadratique ». Nous abordons cette notion dans un premier chapitre, le chapitre 4.

La question de la détermination du nombre de points d'une courbe elliptique définie sur un corps fini fait l'objet du chapitre 6. Nous y présentons le premier algorithme de complexité polynomiale en la taille du corps fini, l'algorithme de Schoof. Et nous terminons par une variante, l'algorithme SEA (pour Schoof, Elkies et Atkin), qui est aujourd'hui l'algorithme le plus rapide pour des corps finis de grande caractéristique.

4. Ordres quadratiques imaginaires

Les multiplications scalaires sont certainement les premiers endomorphismes de courbes elliptiques auxquels on peut penser. Rappelons que la multiplication sur une courbe E par un entier $m \in \mathbb{N}$ est définie par

$$\begin{array}{rccc} [m] \text{ ou } [m]_E\colon & E & \longrightarrow & E, \\ & P & \longmapsto & [m]_E(P) = \underbrace{P + \cdots + P}_{m \text{ fois}}. \end{array}$$

La définition s'étend à $\mathbb{Z}$ en appliquant $[-m]$ à $-P$ quand m est négatif. Ceci nous permet de considérer les éléments de $\mathbb{Z}$ comme des éléments de $\mathrm{End}(E)$.

Considérons ensuite le Frobenius $\pi\colon (x,y) \mapsto (x^q, y^q)$ d'une courbe elliptique E ordinaire sur $\mathbb{F}_q$, qui est aussi un élément de $\mathrm{End}(E)$. Il est alors classique d'écrire un endomorphisme sous la forme abrégée $\pi^2 + a\pi + b$, ce qui revient à écrire $\pi \circ \pi + [a]_E \circ \pi + [b]_E$. Plus largement, lorsque l'on écrit $\mathbb{Z}[\pi] = \{P(\pi),\ P = \sum a_i X^i\}$, il s'agit de l'ensemble des endomorphismes $P(\pi) = \sum [a_i]_E \circ \underbrace{\pi \circ \cdots \circ \pi}_{i \text{ fois}}$.

Maintenant, le polynôme minimal de π, *i.e.* $\chi_\pi = X^2 - tX + q$ où t est la trace de E, peut être lui aussi vu comme un entier algébrique. Ainsi, $\mathbb{Z}[\pi]$ est isomorphe à $\mathbb{Z}[X]/\langle\chi\rangle$, et tout élément de $\mathbb{Z}[\pi]$ peut s'écrire de façon unique comme $a + b\pi$ (après division euclidenne par χ_π). On en déduit alors facilement que son corps des fractions est $\mathbb{Q}(\pi) = \mathbb{Q}[X]/\langle\chi\rangle$, qui est une extension de degré 2 de $\mathbb{Q}$, et qu'on peut voir comme un corps de rupture de χ. On remarque que les racines α, β de χ sont

$$\frac{a \pm \sqrt{a^2 - 4q}}{2} = \frac{a \pm \sqrt{\Delta}}{2} = \frac{a}{2} \pm \frac{1}{2}\sqrt{\Delta}.$$

Autrement dit, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$.

Si on ajoute que dans cette histoire Δ est négatif, on comprends mieux pourquoi l'étude des endomorphismes d'une courbe elliptique définie sur $\mathbb{F}_q$ est très liée à celle des corps quadratiques imaginaires, l'objet de ce chapitre. On s'appuie sur [Cox22 ; Lem21].

4.1 Ordres maximaux

4.1.1 Généralités

On rappelle que l'anneau des *entiers algébriques* d'une extension K de $\mathbb{Q}$ de degré n est l'ensemble des éléments de K annulés par un polynôme à coefficients dans $\mathbb{Z}$ et unitaire. On le note $\mathcal{O}_K$.

Proposition 4.1 Soit K une extension de $\mathbb{Q}$ de degré n. Alors $\mathcal{O}_K$ est un anneau de rang n en tant que $\mathbb{Z}$-module. De plus, un élément a de K est un entier algébrique si et seulement si il vérifie l'une des conditions équivalentes suivantes :

1. a est annulé par un polynôme unitaire à coefficients dans $\mathbb{Z}$;
2. le polynôme minimal de a sur $\mathbb{Q}$ est à coefficients entiers ;
3. le sous-anneau $\mathbb{Z}[a]$ de K est un $\mathbb{Z}$-module de rang fini.

■ **Exemple 4.2**

1. L'ensemble des entiers (algébriques [1]) de $\mathbb{Q}$ est $\mathbb{Z}$.
2. On considère $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$. Le polynôme minimal de i est $X^2+1 \in \mathbb{Z}[X]$ qui est unitaire et à coefficients entiers, il s'agit donc d'un entier de K. En revanche, $i/2$ est annulé par $4X^2+1$ qui est bien à coefficients entiers mais il n'est pas unitaire. Son polynôme minimal est $X^2+1/4$ donc ce n'est pas un entier algébrique.
3. On remarque que $j = (1+\sqrt{-3})/2 = e^{2i\pi/3}$ (racine 3-ème de l'unité) est annulé par X^2+X+1. C'est donc un entier algébrique de $\mathbb{Q}(\sqrt{-3})$.
4. Plus généralement, le polynôme minimal de $e^{2i\pi/n}$ est le n-ème polynôme cyclotomique $\phi_n \in \mathbb{Z}[X]$ unitaire. Donc les racines de l'unité sont toutes des entiers algébriques.

■

On considère un entier d strictement négatif et sans facteur carré. On pose $K = \mathbb{Q}\left(\sqrt{d}\right) = \left\{a+b\sqrt{d},\ a,b \in \mathbb{Q}\right\}$ qui est une extension de degré 2 de $\mathbb{Q}$ appelée extension *quadratique imaginaire* [2]. À partir de maintenant, K est une telle extension et $\mathcal{O}_K$ son anneau des entiers. On sait alors que $\mathcal{O}_K$ est un anneau qui est de rang 2. On peut en fait décrire $\mathcal{O}_K$ très précisément par la proposition suivante.

Proposition 4.3 Soit $K = \mathbb{Q}(\sqrt{d})$ avec $d < 0$.

— Si $d = 1 \bmod 4$, on a $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a+b\frac{1+\sqrt{d}}{2},\ a,b \in \mathbb{Z}\right\}$.

— Si $d \neq 1 \bmod 4$, on a $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right] = \left\{a+b\sqrt{d},\ a,b \in \mathbb{Z}\right\}$.

Le *discriminant* [3] de $\mathcal{O}_K$ est défini par

$$\Delta_K = \begin{cases} d \text{ si } d = 1 \bmod 4, \\ 4d \text{ sinon.} \end{cases}$$

On peut remarquer qu'on a la formule plus générale, sans condition sur d,

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta_K + \sqrt{\Delta_K}}{2}\right].$$

■ **Exemple 4.4**

1. Pour $d = -1$, $K = \mathbb{Q}(i)$, $\Delta_K = -4$ et $\mathcal{O}_K = \mathbb{Z}[i]$
2. Pour $d = -3$, $K = \mathbb{Q}(\sqrt{-3})$, $\Delta_K = -3$ et $\mathcal{O}_K = \mathbb{Z}[j] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Attention on a $\mathbb{Z}\left[\sqrt{-3}\right] \subsetneq \mathbb{Z}[j]$.

■

1. On écrit souvent « les entiers de K » sans préciser « algébriques » à chaque fois.
2. *Quadratique* car de degré 2 sur $\mathbb{Q}$ et *imaginaire* pour $d < 0$, par opposition au cas réel avec $d > 0$.
3. Il s'agit du discriminant du polynôme minimal de n'importe quel générateur ω de $\mathcal{O}_K = \mathbb{Z}[\omega]$.

4.1.2 Arithmétique des ordres maximaux

4.1.2.1 Norme et trace

Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$ un corps quadratique imaginaire et $a \in K$. On pose

— $N(a) = a\bar{a} \in \mathbb{Q}$, la *norme* de a.

— $\mathrm{Tr}(a) = a + \bar{a}$, la *trace* de a.

Lorsque $a \in K \setminus \mathbb{Q}$, le polynôme minimal de a est $X^2 - \mathrm{Tr}(a)X + N(a) \in \mathbb{Q}[X]$.

Proposition 4.5 La norme est multiplicative et la trace est additive. De plus, un élément $a \in \mathcal{O}_K$ est inversible si et seulement si $N(a) = 1$.

Démonstration. La première partie est immédiate. Il est immédiat que la norme d'éléments de $\mathcal{O}_K$ est un entier positif. Si a est inversible, alors il existe $a^{-1} \in \mathcal{O}_K$ tel que $aa^{-1} = 1$ donc $N(aa^{-1}) = N(a)N(a^{-1}) = 1$. Donc $N(a) = 1$ et $N(a^{-1}) = 1$. Réciproquement si $N(a) = a\bar{a} = 1$, alors $a^{-1} = \bar{a}$. ■

Corollaire 4.6 Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire. Alors l'ensemble des inversibles $\mathcal{O}_K^\times$ de $\mathcal{O}_K$ est

— $\mathcal{O}_K^\times = \{\pm 1,\ \pm i\}$ si $\mathcal{O}_K = \mathbb{Z}[i]$, *i.e.* $d = -1$,

— $\mathcal{O}_K^\times = \{\pm 1,\ \pm j,\ \pm j^2\}$ si $\mathcal{O}_K = \mathbb{Z}[j]$, *i.e.* $d = -3$,

— $\mathcal{O}_K^\times = \{\pm 1\}$ sinon.

Démonstration. Soit $a + b\omega \in \mathcal{O}_K$. On a $N(a + b\omega) = a^2 + N(\omega)b^2 + \mathrm{Tr}(\omega)ab$.

Si $d \neq 1 \bmod 4$ alors on peut choisir $\omega = \sqrt{d}$ comme générateur de $\mathcal{O}_K$. On a alors $\mathrm{Tr}(\omega) = 0$ et $N(\omega) = -d$. Ainsi, si $N(a + b\omega) = a^2 - db^2 = 1$ et si $-d > 1$ alors $b = 0$ et $a = \pm 1$. Si $d = -1$ alors on a aussi $a = 0$ et $b = \pm 1$ qui vérifient $N(a + b\omega) = 1$.

Si $d = 1 \bmod 4$ on peut prendre $\omega = (1 + \sqrt{d})/2$ de trace 1 et de norme $n = (1 - d)/4$. On a alors $N(a + b\omega) = a^2 + nb^2 + ab$. Donc si $-d > 3$, alors $b = 0$ et $a = \pm 1$. Sinon $d = -3$ et on peut alors avoir les 6 possibilités annoncées. ■

Bien qu'une grande partie de la théorie des entiers dans les corps quadratiques $\mathbb{Q}\left(\sqrt{d}\right)$ soit commune entre le cas imaginaire ($d < 0$) et le cas réel ($d > 0$), ce dernier résultat est spécifique au cas imaginaire. Il est en effet possible de démontrer que lorsque $d > 0$, on a toujours $\#\mathcal{O}_K^\times = \infty$.

4.1.2.2 Factorisation unique ?

On veut savoir si les anneaux d'entiers algébriques des corps quadratiques imaginaires ont de bonnes propriétés arithmétiques. Sont-ils euclidiens ? Principaux ? Factoriels ? On sait déjà que l'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien (donc principal, factoriel, *etc.*) mais il y en a peu qui vérifient cette propriété. La proposition suivante les donne tous.

Proposition 4.7 Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$ avec d un entier strictement négatif sans facteur carré. Alors $\mathcal{O}_K$ est principal si et seulement si

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Démonstration. Voir les exercices 4.37 et 4.38 à la fin du chapitre. ■

Prenons l'exemple de $\mathbb{Q}(\sqrt{d})$ avec $d=-5$, donc $\mathcal{O}_K=\mathbb{Z}\left[\sqrt{-5}\right]$. On a

$$N(1+\sqrt{-5})=(1+\sqrt{-5})(1-\sqrt{-5})=6=2\times 3. \tag{4.1}$$

On voit donc que 6 a deux factorisations distinctes et on peut prouver que ces factorisations sont des factorisations en irréductibles non-associés, *i.e.* 2 et 3 ne sont pas $1+\sqrt{-5}$ ou $1-\sqrt{-5}$ à un facteur inversible près (voir exercice 4.8). Donc l'anneau $\mathbb{Z}\left[\sqrt{-5}\right]$ n'est pas factoriel. On va voir que ces anneaux ont quand même une propriété intéressante ; ils sont de *Dedekind* c'est-à-dire que bien que les éléments de $\mathcal{O}_K$ n'admettent pas de décomposition unique en irréductibles, les idéaux de $\mathcal{O}_K$ admettent une unique décomposition en idéaux premiers.

Exercice 4.8 — (★★).

1. Montrer que $\mathbb{Z}\left[\sqrt{-5}\right]$ n'admet pas d'élément de norme 2 ou 3 (on peut supposer que $a+b\sqrt{-5}$ est de norme 2 ou 3 et en déduire qu'alors 2 est un carré dans $\mathbb{Z}/5\mathbb{Z}$).
2. En déduire que 2, 3, $1+\sqrt{-5}$ et $1-\sqrt{-5}$ sont des éléments irréductibles de $\mathbb{Z}\left[\sqrt{-5}\right]$.
3. Montrer que si $\mathbb{Z}\left[\sqrt{-5}\right]$ était factoriel, alors on aurait $2\,|\,1+\sqrt{-5}$ ou $2\,|\,1-\sqrt{-5}$ (indication : le lemme d'Euclide est valable dans tous les anneaux factoriels).
4. En déduire que $\mathbb{Z}\left[\sqrt{-5}\right]$ n'est pas factoriel. ■

4.2 Ordres quelconques

Nous définissons maintenant les *ordres* dans un corps quadratique imaginaire. Les anneaux d'entiers que nous avons étudiés dans la section précédente sont des ordres qui sont les éléments maximaux (pour la relation d'ordre $\subseteq$) parmi tous les ordres possibles. Bien que nous puissions définir les ordres dans des corps de nombre quelconque on se restreindra encore une fois au cas qui nous intéresse ; les extensions quadratiques imaginaires où l'étude des ordres est grandement simplifiée.

Définition 4.9 Soit $K=\mathbb{Q}\left(\sqrt{d}\right)$ un corps quadratique imaginaire et R un sous-anneau de K. On dit que R est un *ordre* de K s'il est de type fini sur $\mathbb{Z}$ et satisfait $\mathbb{Q}R=K$ (*i.e.* R contient une $\mathbb{Q}$-base de K).

■ **Exemple 4.10**

1. Pour tout corps $K=\mathbb{Q}\left(\sqrt{d}\right)$, $\mathbb{Z}$ est un sous-anneau de K, mais $\mathbb{Q}\mathbb{Z}=\mathbb{Q}\neq K$. Donc $\mathbb{Z}$ n'est pas un ordre.
2. On sait que $\mathcal{O}_K\simeq\mathbb{Z}^2$ en tant que $\mathbb{Z}$-module et c'est un sous-anneau de K qui contient une $\mathbb{Q}$-base de K, c'est donc un ordre.
3. Soit R un ordre de K et $a\in R$, alors $\mathbb{Z}[a]\subseteq R$ qui est de type fini. D'après la proposition 4.1, l'élément a est un entier algébrique de K et donc $R\subseteq\mathcal{O}_K$ (ceci prouve que $\mathcal{O}_K$ est maximal pour la relation d'ordre $\subseteq$). À partir de maintenant on parle davantage de $\mathcal{O}_K$ comme de l'ordre maximal de K plutôt que comme son anneau des entiers.
4. $R=\mathbb{Z}[2i]=\{a+2ib,\ a,b\in\mathbb{Z}\}$ est un ordre de $\mathbb{Q}(i)$. Ce n'est pas $\mathbb{Z}[i]$ car R ne contient pas i.

■

Proposition 4.11 Soit R un ordre d'un corps quadratique imaginaire K et $\mathcal{O}_K = \mathbb{Z}[\omega]$ son ordre maximal. Alors il existe un entier f, appelé le *conducteur* de R, tel que $R = \mathbb{Z}[f\omega]$.

Démonstration. On considère R et $\mathcal{O}_K$ comme des sous $\mathbb{Z}$-modules de $K \simeq \mathbb{Q}^2$. Il sont tous les deux de rang 2 car ce sont des ordres. On considère une base adaptée (e_1, e_2) de $R \subseteq \mathcal{O}_K$, *i.e.* une base de $\mathcal{O}_K$ telle qu'il existe des entiers $d_1 \mid d_2$ tels que $(d_1 e_1, d_2 e_2)$ est une base de R. On a alors $\mathcal{O}_K / R = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ de cardinal $f = d_1 d_2$. Par le théorème de Lagrange, $f\omega \in R$. Donc $\mathbb{Z}[f\omega] \subseteq R$. Puisque $\# \mathcal{O}_K / \mathbb{Z}[f\omega] = f$, on a $R = \mathbb{Z}[f\omega]$. ■

On définit alors le *discriminant* d'un ordre R par $\Delta_R = f^2 \Delta_K$.

Pour chaque discriminant il existe un unique ordre correspondant. Il n'y a donc aucune ambiguïté à parler de l'ordre de discriminant -27 par exemple. Puisque $27 = 3^2 \times 3$, il s'agit de l'ordre de $\mathbb{Q}(\sqrt{-3})$ de conducteur 3, *i.e.* $\mathbb{Z}[3j]$. Ou encore l'ordre de discriminant -16. Puisque $16 = 2^2 \times 4$, il s'agit de l'ordre de $\mathbb{Q}(i)$ (discriminant -4) de conducteur 2, *i.e.* $\mathbb{Z}[2i]$.

Il existe plusieurs façon de définir un ordre en MAGMA et certaines sont plus commodes que d'autres suivant les situations. Par exemple, définir l'ordre quadratique directement à partir du polynôme minimal d'un générateur est particulièrement approprié lorsqu'on souhaite déterminer l'ordre engendré par le Frobenius d'une courbe elliptique sur un corps fini.

Première approche : comme sous-ordre de l'ordre maximal.

```
> K := QuadraticField(-3); // Le corps quadratique
> O := MaximalOrder(K);    // Son ordre maximal (ou anneau des entiers)
> R := sub<O|3>;           // L'ordre de conducteur 3 dans O.
> Conductor(R);            // Bon conducteur ?
3
> Discriminant(R);         // Bon discriminant ?
-27
```

Seconde approche : comme ordre de l'élément de polynôme minimal $X^2 - X + 7 \in \mathbb{Z}[X]$.

```
> _<X> := PolynomialRing(Integers());       // Z[X]
> R := EquationOrder(X^2-X+7);              // L'ordre correspondant
> Norm(Conductor(R));                       // Ici, Conductor() renvoie un ideal
3
> Discriminant(R);                          // Discriminant de l'ordre
-27
> _, K := IsQuadratic(FieldOfFractions(R)); // Le corps quadratique
> K eq QuadraticField(-3);
true
```

4.3 Groupe des classes

On a vu qu'il y a peu d'anneaux d'entiers principaux. On aimerait cependant mesurer à quel point un tel anneau échoue à être principal. Le *groupe des classes* que nous définissons dans cette section peut s'interpréter ainsi pour les ordres maximaux (mais malheureusement cette interprétation ne tient plus pour les ordres quelconques).

4.3.1 Idéaux fractionnaires

Comme dans certains corps de nombres algébriques il existe des éléments irréductibles qui ne possèdent pas toutes les propriétés attendues des nombres premiers, le théorème de la factorisation unique ne s'applique pas. Dans le cas des anneaux de nombres quadratiques, il était historiquement parfois possible de justifier les calculs nécessaires à la résolution de certaines équations diophantiennes en invoquant le langage des formes quadratiques binaires. Mais pour répondre à la question en toute généralité, Kümmer a inventé la notion "d'idéaux" premiers.

Un sous-anneau I d'un ordre R est un un idéal entier de R si $I \cdot R \subseteq I$. Un idéal est donc stable pour l'addition, $I+I \subseteq I$, et pour la multiplication par des éléments arbitraires de R.

Comme le produit de deux idéaux est encore un idéal, l'ensemble des idéaux entiers forme un monoïde. De tels monoïdes peuvent être transformés en un groupe d'une manière assez formelle ressemblant à la construction du corps $\mathbb{Q}$ des nombres rationnels à partir du monoïde multiplicatif $\mathbb{Z}$. De tels quotients d'idéaux sont appelés idéaux fractionnaires. Formellement, deux idéaux de ce type $\mathfrak{a}/\mathfrak{b}$ et $\mathfrak{c}/\mathfrak{d}$ sont multipliés de la même manière que des fractions de nombres, et nous pouvons bien sûr annuler les facteurs communs. Les idéaux principaux de la forme $\langle a \rangle = a\mathcal{O}_K$, où l'élément a n'est pas nécessairement un entier algébrique, sont appelés idéaux fractionnaires principaux.

En fait, si on réécrit un idéal fractionnaire $\mathfrak{a}\mathfrak{b}^{-1}$ comme $\mathfrak{a}\mathfrak{b}'(\mathfrak{b}\mathfrak{b}')^{-1} = (1/b)\mathfrak{a}\mathfrak{b}'$, où b désigne la norme de $\mathfrak{b}$, on se rend compte que l'on peut finalement définir les idéaux fractionnaires comme le quotient d'idéaux entiers par des entiers de $\mathbb{N}$.

Définition 4.12 Soit R un ordre dans un corps quadratique imaginaire K . On appelle *idéal fractionnaire* de R tout sous R-module de K de type fini, ou de manière équivalente tout sous R-module $\mathfrak{a}$ de K tel qu'il existe $n \in \mathbb{N}$ pour que $n\,\mathfrak{a}$ soit un idéal de R .

Un idéal fractionnaire $\mathfrak{a}$ de R est dit *inversible* ou *propre* s'il existe un idéal fractionnaire $\mathfrak{b}$ de R tel que $\mathfrak{a}\,\mathfrak{b} = R$ auquel cas on note $\mathfrak{b} = \mathfrak{a}^{-1}$.

■ **Exemple 4.13**

— Les idéaux d'un ordre sont des idéaux fractionnaires.

— Dans tout sous-ordre strict $R \subsetneq \mathcal{O}_K = \mathbb{Z}[\omega]$, $\mathcal{O}_K$ est un R-idéal fractionnaire (attention ce n'est pas un idéal car $\mathcal{O}_K \nsubseteq R$). Il n'est jamais inversible dans R car ceci signifierait qu'il existe un idéal fractionnaire $\mathfrak{b}$ tel que $\mathfrak{b}\mathcal{O}_K = R$. Or $\mathfrak{b}\mathcal{O}_K$ est un $\mathcal{O}_K$-module et R n'en est pas un (car $1 \times \omega \notin R$ par exemple). Ainsi tout ordre qui n'est pas maximal admet systématiquement des idéaux fractionnaires non-inversibles.

— Dans tout ordre R, pour tout élément $a \in K \setminus \{0\}$, l'idéal fractionnaire $\langle a \rangle$ est inversible d'inverse $\langle 1/a \rangle$.

■

Proposition 4.14 Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux fractionnaires. Alors :

1. $\mathfrak{a}+\mathfrak{b}$ est un idéal fractionnaire ;
2. $\mathfrak{a}\mathfrak{b} = \langle \alpha\beta, \alpha \in \mathfrak{a}, \beta \in \mathfrak{b} \rangle$ est un idéal fractionnaire ;
3. $\mathfrak{a} \,|\, \mathfrak{b}$ si et seulement si $\mathfrak{b} \subset \mathfrak{a}$;
4. $(\mathfrak{a}\colon \mathfrak{b}) = \{a \in K,\ a\mathfrak{b} \subseteq \mathfrak{a}\}$ est un idéal fractionnaire, l'idéal *quotient*[a] de $\mathfrak{a}$ et $\mathfrak{b}$.
5. L'idéal fractionnaire $\mathfrak{a}$ est inversible si et seulement si $\mathfrak{a}(R\colon \mathfrak{a}) = R$ (auquel cas on a $\mathfrak{a}^{-1} = (R\colon \mathfrak{a})$).

a. Ce nom, mal choisi, fait penser au quotient d'un anneau par un idéal. En anglais on utilise parfois la dénomination *colon ideal* pour désigner le « : ».

On a donc une correspondance assez naturelle entre les opérations usuelles sur les rationnels et celles sur les idéaux.

Corps algébriques		$\mathbb{Q}$
Idéal entiers	$\longleftrightarrow$	Entier
Idéal fractionnaires	$\longleftrightarrow$	Rationnel
Produit	$\longleftrightarrow$	Produit

Corps algébriques		$\mathbb{Q}$
Inclusion	$\longleftrightarrow$	Divisibilité
Somme	$\longleftrightarrow$	pgcd
Intersection	$\longleftrightarrow$	ppcm

Définition 4.15 Soit R un ordre de discriminant Δ dans un corps quadratique imaginaire K. On pose $I(R)$ le groupe (pour la loi $\times$) des idéaux fractionnaires inversibles. On pose $P(R)$ le sous-groupe de $I(R)$ formé des idéaux fractionnaires principaux. Enfin, on définit $\mathrm{Cl}(R) = I(R)/P(R)$ (ou $\mathrm{Cl}(\Delta)$) le *groupe des classes*[a] ou *groupe de Picard* de R. Le cardinal de $\mathrm{Cl}(R)$ est appelé *nombre de classes* de R et on le note $h(R)$ ou $h(\Delta)$.

a. Dans certains ouvrages, on préfère réserver *groupe des classes* pour l'ordre maximal $\mathcal{O}_K$ et parler de groupe des classes de K sans ambiguïté.

Autrement dit, deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ sont dans la même classe de $\mathrm{Cl}(R)$ si et seulement si il existe deux entiers α, β de $\mathcal{O}_K$ tels que $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

Le théorème suivant permet de trouver des représentants « petits » du groupe des classes (nous renvoyons au paragraphe 4.3.5 pour sa preuve).

Théorème 4.16 Soit R un ordre dans un corps quadratique imaginaire K. Alors tout idéal fractionnaire $\mathfrak{a}$ a un représentant $\mathfrak{b}$ dans R (*i.e.* un idéal de R de même classe que $\mathfrak{a}$ dans $\mathrm{Cl}(R)$) de norme $N(\mathfrak{b}) \leq \sqrt{-\Delta/3}$. En particulier, $h(\Delta)$ est fini.

On pose $\mu_R = \left\lfloor \sqrt{-\Delta/3} \right\rfloor$, appelé la *borne de Gauss* de R.

Rq Attention, ce théorème ne signifie pas que $h(\Delta) \leq \mu_R$; en effet, il peut y avoir dans R beaucoup d'idéaux d'une norme donnée.

Rq **Interprétation du groupe des classes :** Par définition du quotient, deux idéaux inversibles $\mathfrak{a}$ et $\mathfrak{b}$ d'un ordre R ont la même classe dans $\mathrm{Cl}(R)$ s'ils diffèrent d'un facteur dans K, *i.e.* s'il existe $a \in K$ tel que $\mathfrak{a} = a\mathfrak{b}$. Ainsi, le groupe des classes $\mathrm{Cl}(R)$ est trivial si et seulement si les seuls idéaux inversibles sont les idéaux principaux. Lorsque R est l'ordre maximal on a dit que tous les idéaux sont inversibles. Donc si le groupe des classes est trivial, c'est que tous les idéaux sont principaux.

Si R n'est pas maximal, il se peut que le groupe des classes soit trivial sans que R soit principal. Par exemple, $R = \mathbb{Z}[\sqrt{-3}]$ a un groupe des classes trivial mais n'est pas principal. En fait, lorsque R n'est pas maximal, il n'est jamais principal d'après l'exemple 4.13 qui indique qu'il y a toujours des idéaux non-inversibles, et aussi que les idéaux principaux sont tous inversibles.

```
> K := QuadraticField(-3);
> R<w> := sub<MaximalOrder(K)|2>; // L'ordre Z[sqrt(-3)]
> #PicardGroup(R);                // Le groupe des classes est trivial
1
> IsPrincipal(ideal<R|2, 1+w>);
false
```

■ **Exemple 4.17**

1. Pour $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$ et $K = \mathbb{Q}\left(\sqrt{d}\right)$, on a $\#\mathrm{Cl}(\mathcal{O}_K) = 1$.
2. On a $\#\mathrm{Cl}\left(\mathbb{Z}\left[\sqrt{-5}\right]\right) = 2$, il n'est donc pas principal (mais presque).

■

4.3.2 Anneau multiplicateur

Soit R un ordre quadratique et $\mathfrak{a}$ un idéal fractionnaire de R. On pose $R_\mathfrak{a} = (\mathfrak{a}\colon \mathfrak{a})$, appelé l'*anneau multiplicateur* de $\mathfrak{a}$.

Exercice 4.18 — (★).
1. Montrer qu'il s'agit d'un ordre contenant R (*i.e.* un sur-ordre de R).
2. Justifier qu'il s'agit du plus grand sur-ordre S de R tel que l'ensemble $\mathfrak{a}$ est un S-idéal. ∎

Proposition 4.19 Soit R un ordre quadratique imaginaire et $\mathfrak{a}$ un R-idéal fractionnaire. Alors $\mathfrak{a}$ est inversible dans l'ordre $R_\mathfrak{a}$. En particulier $\mathfrak{a}$ est un R-idéal fractionnaire inversible si et seulement si $R_\mathfrak{a} = R$.

Proposition 4.20 Si $\mathfrak{a}$ est inversible, alors $R_\mathfrak{a} = R$ (la réciproque est vraie , mais difficile).

Démonstration. Si $\mathfrak{a}$ est inversible, alors il existe un idéal $\mathfrak{b}$ tel que $\mathfrak{ab} = R$. Et donc, si $\beta \in K$, alors $\beta R = \beta(\mathfrak{ab}) = (\beta\mathfrak{a})\mathfrak{b} \subseteq \mathfrak{ab} = R$. ■

4.3.3 Norme et factorisation

On définit la norme d'un idéal $\mathfrak{a} \subseteq R$ par $N(\mathfrak{a}) = \#R/\mathfrak{a} = [R\colon \mathfrak{a}]$.

Ceci nous permet de définir la norme d'un idéal fractionnaire quelconque. Soit $\mathfrak{a}$ un idéal fractionnaire et n tel que $n\mathfrak{a} \subseteq R$. On définit la norme de $\mathfrak{a}$ par $N(\mathfrak{a}) = N(n\mathfrak{a})/n^2$.

Proposition 4.21 Soit $\mathfrak{a}, \mathfrak{b}$ des idéaux fractionnaires de R avec $\mathfrak{a}$ *inversible* et $a \in K$, alors
- $N(aR) = N(a) = a\bar{a}$ (voir l'exercice 4.22).
- $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ où $\mathfrak{ab} = \langle ab,\ a \in \mathfrak{a},\ b \in \mathfrak{b}\rangle$, *i.e.* l'idéal engendré [a] par les produits d'éléments dans $\mathfrak{a}$ et dans $\mathfrak{b}$.
- $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})R$ où $\bar{\mathfrak{a}} = \{\bar{a},\ a \in \mathfrak{a}\}$.

a. Attention, ce n'est pas l'ensemble des produits (ce n'est pas un idéal en général).

D'après le dernier point de la proposition 4.21 on peut expliciter facilement l'inverse d'un idéal inversible, *i.e.*

$$\mathfrak{a}^{-1} = \frac{1}{N(\mathfrak{a})}\bar{\mathfrak{a}}.$$

Attention, les deux derniers points de la proposition 4.21 sont faux sans l'hypothèse $\mathfrak{a}$ inversible.

Exercice 4.22 — (★★).
Soit $R = \mathbb{Z}[\omega]$ un ordre quadratique imaginaire et $\alpha = a + b\omega \in R$. On considère $\chi = X^2 - tX + n \in \mathbb{Z}[X]$ le polynôme minimal de ω. On pose $N(\alpha) = \bar{\alpha}\alpha$ et $\widetilde{N}(\alpha R) = \#R/\alpha R$. On veut montrer que $N(\alpha) = \widetilde{N}(\alpha R)$.
1. On identifie R à $\mathbb{Z}^2$ grâce à sa $\mathbb{Z}$-base $\mathcal{B} = (1, \omega)$. Montrer que $M = \left(\begin{smallmatrix} a & -nb \\ b & a+bt \end{smallmatrix}\right)$ est une matrice de présentation de $\alpha R \subseteq R$.
2. Montrer que $\#(R/\alpha R) = |\det M|$
   (on peut penser aux formes de Smith ou au théorème de la base adaptée).
3. Conclure. ∎

Théorème 4.23

1. Soit $\mathfrak{a}$ un idéal inversible de R, alors il existe des idéaux premiers $\mathfrak{p}_1,\dots,\mathfrak{p}_m$ de R et des entiers non nuls $\alpha_1,\dots,\alpha_m$ tels que

$$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_m^{\alpha_m}.$$

   De plus, cette décomposition est unique à permutation des facteurs près.
2. Un ordre R est maximal si et seulement si tous ses idéaux sont inversibles.

4.3.4 Idéaux d'un ordre

Proposition 4.24 Soit R un ordre quadratique et $\mathfrak{a}$ un idéal de R.

1. Si la norme de $\mathfrak{a}$ est un nombre premier, alors $\mathfrak{a}$ est un idéal premier.
2. Si la norme de $\mathfrak{a}$ est première avec le conducteur f de R, alors $\mathfrak{a}$ est inversible.

Démonstration.

1. Si $N(\mathfrak{a}) = p$ est premier, alors $R/\mathfrak{a}$ est un anneau de cardinal premier contenant p éléments. C'est donc $\mathbb{Z}/p\mathbb{Z}$ et $\mathfrak{a}$ est premier.
2. Voir l'exercice 4.25. ■

Exercice 4.25 — (★★).

Soit $\mathfrak{a}$ un idéal d'un ordre quadratique R de norme première à f, le conducteur de R dans $\mathcal{O}_K$. On veut montrer que $\mathfrak{a}$ est inversible. On pose $m_f\colon R/\mathfrak{a} \longrightarrow R/\mathfrak{a},\ \ a \longmapsto af$.

1. Montrer que m_f est un isomorphisme de groupes (on peut considérer une relation de Bézout entre f et $N(\mathfrak{a})$).
2. En déduire que $\mathfrak{a} + fR = R$.
3. Soit $\beta \in K$ tel que $\beta\mathfrak{a} \subseteq \mathfrak{a}$, i.e. $\beta \in R_{\mathfrak{a}}$.
   a. Justifier que $\beta \in \mathcal{O}_K$.
   b. Montrer que $\beta R \subseteq R$.
   c. En déduire que $\mathfrak{a}$ est inversible. ■

Proposition 4.26 Soit $R = \mathbb{Z}[\omega]$ un ordre quadratique imaginaire.

1. Tout sous $\mathbb{Z}$-module de R est de la forme $\langle n, a+m\omega\rangle$ pour des uniques $n,\ m \in \mathbb{N}$ et a unique modulo n.
2. Avec les mêmes notations, si $n,m \neq 0$ on a $\#R/\langle n, a+m\omega\rangle_{\mathbb{Z}} = nm$.
3. Un sous $\mathbb{Z}$-module $\mathfrak{a} = \langle n, a+m\omega\rangle_{\mathbb{Z}}$ de R est un idéal si et seulement si $m \mid n, m \mid a$ (*i.e.* $a = mb$) et $n \mid m\cdot N(b+\omega)$.

Démonstration.

1. Soit $\mathfrak{a}$ un sous $\mathbb{Z}$-module de R. Alors $\mathfrak{a}\cap\mathbb{Z}$ est un sous $\mathbb{Z}$-module de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$. Par ailleurs, il est clair que $H = \{s \in \mathbb{Z},\ \exists a \in \mathbb{Z},\ a + s\omega\}$ est un sous-groupe de $\mathbb{Z}$, donc aussi de la forme $m\mathbb{Z}$. On a donc une inclusion de $\langle n, a+m\omega\rangle_{\mathbb{Z}} \subseteq \mathfrak{a}$ où a est n'importe quel entier tel que $a + m\omega \in \mathfrak{a}$.

   Soit $x = r + s\omega \in \mathfrak{a}$. Donc $s \in H = m\mathbb{Z}$, on pose $s = um$. On a alors $r - ua = r + s\omega - ua - um\omega = x - u(a+m\omega) \in \mathfrak{a}\cap\mathbb{Z} = n\mathbb{Z}$. Donc $r - ua = nv$ pour un certain $v \in \mathbb{Z}$. Au final, on a $x = r + s\omega = r - ua + ua + s\omega = nv + (a+m\omega)u \in \langle n, a+m\omega\rangle_{\mathbb{Z}}$.

2. La présentation du $\mathbb{Z}$-module $\mathfrak{a} = n\mathbb{Z} + (a+m\omega)\mathbb{Z}$ dans la R-base $(1,\omega)$ est égale à $M = \left(\begin{smallmatrix} n & a \\ 0 & m \end{smallmatrix}\right)$. On en déduit que $\#R/\langle n, a+m\omega\rangle_{\mathbb{Z}} = \#R/\operatorname{im} M = |\det(M)| = nm$. Pour la seconde égalité, considérons une forme de Smith $S = PMQ$ de M et, puisque P et Q sont inversibles, on a $R/\operatorname{im} M \simeq R/\operatorname{im} S$ et $|\det S| = |\det M|$.

3. Avant toute chose, commençons par remarquer que puisque $\mathfrak{a}$ est un $\mathbb{Z}$-module, c'est un groupe additif (stable par somme) stable par produit par un entier. Ainsi $\mathfrak{a}$ est un R-module si et seulement si il est stable par multiplication par ω. Ce qui est équivalent à ce que les générateurs n et $a+m\omega$ le soient.

   $\Rightarrow$ Supposons que $\mathfrak{a}$ soit un R-idéal, alors $n\cdot\omega\in\mathfrak{a}$. Donc $n\in H=m\mathbb{Z}$, ce qui prouve que $m\,|\,n$. Écrivons $\omega^2=t\omega-N$. On a $(a+m\omega)\omega=a\omega+m(t\omega-N)=-mN+(a+tm)\omega$. Donc $a+tm\in H=m\mathbb{Z}$, *i.e.* $m\,|\,a$. Enfin, $(a+m\omega)(b+\bar{\omega})=mN(b+\omega)\in\mathbb{Z}\cap\mathfrak{a}=n\mathbb{Z}$, ce qui conclut la preuve de ce sens.

   $\Leftarrow$ Remarquons tout d'abord qu'il suffit de montrer que $n(u+\omega)\in\mathfrak{a}$ et $(a+m\omega)(v+\omega)\in\mathfrak{a}$ pour des $u,v\in\mathbb{Z}$. On a alors $n\omega=n(u+\omega)-nu\in\mathfrak{a}$, puisque $\mathfrak{a}$ est un $\mathbb{Z}$-module.

   Puisque $m\,|\,n$, on peut écrire $n=mu$ par exemple. On a alors $n(b+\omega)=um(b+\omega)=u(a+m\omega)\in\mathfrak{a}$, et donc $n\omega\in\mathfrak{a}$. On remarque que par définition de la trace, $\bar{\omega}=t-\omega$ avec $t\in\mathbb{Z}$ la trace de ω. Ainsi,

$$(a+m\omega)(b+\bar{\omega})=(a+m\omega)(b+t-\omega)=mN(b+\omega)\in n\mathbb{Z}\subseteq\mathfrak{a}.$$

   Ceci conclut la preuve. ■

Il faut bien comprendre comment utiliser la proposition 4.26. Le premier point affirme que tout sous $\mathbb{Z}$-module de R s'écrit $\mathfrak{a}=\langle n,a+m\omega\rangle_{\mathbb{Z}}$ et que le cardinal du quotient de groupe $\#R/\mathfrak{a}=nm$, c'est donc facile de calculer le cardinal de ce type de quotient ! Cependant, tout $\mathbb{Z}$-module n'est pas nécessairement un R-module. Par exemple, $\mathbb{Z}\subseteq R$ est un sous $\mathbb{Z}$-module de R qui n'est pas un idéal. Ainsi, si on écrit $\mathfrak{a}=\langle n,a+m\omega\rangle=nR+(a+m\omega)R$ il faut s'assurer que $\mathfrak{a}=\langle n,a+m\omega\rangle_{\mathbb{Z}}=n\mathbb{Z}+(a+m\omega)\mathbb{Z}$ pour pouvoir affirmer que $\#R/\mathfrak{a}=nm$. Et ce n'est pas évident, c'est la condition que donne le troisième point de la proposition.

Pour des raisons pratiques on utilise très souvent des idéaux de la forme $\langle n,a+\omega\rangle$ (*i.e.* $m=1$). Il suffit alors de vérifier que $n\,|\,N(a+\omega)$ pour conclure que $R/\mathfrak{a}$ est de cardinal n.

■ **Exemple 4.27** On prend $R=\mathbb{Z}\left[\sqrt{-2}\right]$; donc $\omega=\sqrt{-2}$. On considère $\mathfrak{a}=\langle 3,1+\omega\rangle_{\mathbb{Z}}$, donc $n=3$, $a=1$ et $m=1$. On a bien $m\,|\,a$ et $m\,|\,n$. De plus, $N(1+\omega)=1^2+2\cdot1^2=3$, donc $n\,|\,N(1+\omega)$. On peut donc en déduire que $N(\mathfrak{a})=3\times1=3$.

Si on considère maintenant $\mathfrak{b}=\langle 3,\omega\rangle_{\mathbb{Z}}$; on a $N(\omega)=2$ et $3\nmid 2$. Donc, d'après la proposition 4.26, $\mathfrak{b}\neq\mathfrak{b}R$ (le R-module engendré par $\mathfrak{b}$ n'est pas égal au $\mathbb{Z}$-module qu'il engendre). Il peut être instructif de le vérifier à la main. On considère $\mathfrak{c}=\mathfrak{b}R$ et dans ce cas $\underbrace{\omega}_{\in\mathfrak{c}}\underbrace{\bar{\omega}}_{\in R}=2\in\mathfrak{c}$. Mais $\mathfrak{c}$ est en particulier un groupe, donc $3-2=1\in\mathfrak{c}$.
Donc $1\cdot R\subseteq\mathfrak{c}\subseteq R$, *i.e.* $\mathfrak{c}=R$ et $\#R/\langle 3,\omega\rangle_R=1$, tandis que $\#R/\langle 3,\omega\rangle_{\mathbb{Z}}=3$.

```
> O<w> := MaximalOrder(QuadraticField(-2)); // Z[sqrt(-2)]
> fa := ideal<O|3,1+w>;                     // Idéal engendré par 3 et 1 + sqrt(-2)
> Norm(fa);
3
> fc := ideal<O|3,w>;                       // Idéal engendré par 3 et sqrt(-2)
> Norm(fc);
1
```

■

Exercice 4.28 — (★).

1. Les sous $\mathbb{Z}$-modules de $\mathbb{Z}[i]$ suivants sont-ils des idéaux ?

$$\mathfrak{a}_1 = \langle 2, 1+2i\rangle_{\mathbb{Z}},\ \mathfrak{a}_2 = \langle 3, 1+i\rangle_{\mathbb{Z}},\ \mathfrak{a}_3 = \langle 2, 2i\rangle_{\mathbb{Z}}\,.$$

2. Pour chaque $\mathfrak{a}_i$, écrire $\mathfrak{a}_i R$ sous la forme $\langle n, a+m\omega\rangle_{\mathbb{Z}}$.
3. Vérifier vos calculs à l'aide de MAGMA. ■

Proposition 4.29 — Entiers premiers. Soit p un nombre premier impair et $\mathcal{O}_K = \mathbb{Z}[\omega] = \mathbb{Z}[X]/\langle\chi\rangle$ l'ordre maximal d'un corps quadratique imaginaire de discriminant Δ.
Alors,

si $p\,|\,\Delta$: il existe $\mathfrak{p} \subseteq \mathcal{O}_K$ premier tel que $\langle p\rangle = \mathfrak{p}^2$. De plus, $\mathfrak{p} = \langle p, \omega - a\rangle$ avec a l'unique racine de χ mod p.

si Δ est un carré non nul dans $\mathbb{F}_p$: il existe deux idéaux premiers $\mathfrak{p}_1$ et $\mathfrak{p}_2$ distincts tels que $\langle p\rangle = \mathfrak{p}_1\mathfrak{p}_2$. De plus, on a $\mathfrak{p}_i = \langle p, \omega - a_i\rangle$ avec a_1, a_2 les racines de χ mod p.

si Δ n'est pas un carré dans $\mathbb{F}_p$: $\langle p\rangle$ est un idéal premier de $\mathcal{O}_K$.

Dans le premier cas on dit que p *ramifie* dans $\mathcal{O}_K$, dans le second on dit que p *se décompose complètement* dans $\mathcal{O}_K$ et dans le dernier on dit que p est *inerte* dans $\mathcal{O}_K$.

Démonstration. Voir l'exercice 4.32 (on montre mieux, en fait ; on montre que les résultats annoncés sont vrais sans l'hypothèse de maximalité pour les deux derniers points). ■

Il existe un résultat similaire pour $p = 2$ (voir l'exercice 4.35).

Exercice 4.30 — (★).

Soit $\mathcal{O}_K$ un ordre maximal dans un corps quadratique imaginaire. Soit ℓ un nombre premier impair. Montrer qu'il existe exactement $1 + \left(\frac{\Delta_K}{\ell}\right)$ idéaux de $\mathcal{O}_K$ de norme ℓ. Montrer qu'un ordre R admet au plus 2 idéaux de norme 2. ■

Exercice 4.31 — (★).

On dit qu'un idéal $\mathfrak{a} = \langle n, a+m\omega\rangle_{\mathbb{Z}}$ d'un ordre quadratique R est *primitif* si $m = 1$.

1. Soit $\mathfrak{a}$ un idéal de R dont la norme est sans facteur premier. Montrer que $\mathfrak{a}$ est primitif (on peut remarquer que $m^2\,|\,nm$).
2. On suppose que $R = \mathcal{O}_K$ est maximal. On pose $N = p_1 \cdots p_r$ avec p_i premiers distincts. Montrer que R admet au plus 2^r idéaux de norme N. ■

Exercice 4.32 — (★★) Décomposition des premiers impairs. Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire, $\mathcal{O}_K = \mathbb{Z}[\omega_K] = \mathbb{Z}[X]/\langle\chi\rangle$ son ordre maximal de discriminant Δ_K et $R = \mathbb{Z}[X]/\langle\chi_\omega\rangle$ un ordre quelconque de discriminant Δ. On considère un nombre premier impair p.

1. Montrer que $R/\langle p\rangle \simeq \mathbb{F}_p[X]/\langle\chi_\omega\rangle$.
2. Montrer que si Δ n'est pas un carré modulo p alors $\langle p\rangle$ est premier dans R.
3. On suppose que $p|\Delta$ et on pose $\mathfrak{p} = \left\langle p, \sqrt{\Delta_K}\right\rangle$.
   a. Montrer que $\mathfrak{p}^2 = \langle p\rangle$.
   b. Justifier que $\chi \mod p$ possède une unique racine a. Montrer qu'alors $\mathfrak{p} = \langle p, \omega_K - a\rangle$.

4. On suppose que $\Delta \mod p$ est un carré non nul.
   a. Montrer que χ possède deux racines distinctes a_1 et a_2 modulo p.
   b. Montrer que les idéaux $\mathfrak{p}_i = \langle p, \omega - a_i \rangle$ définissent des idéaux premiers inversibles de R.
   c. Montrer que $\mathfrak{p}_1\mathfrak{p}_2 \subseteq \langle p \rangle$.
   d. En déduire que $\mathfrak{p}_1\mathfrak{p}_2 = \langle p \rangle$.
   e. Montrer que $R/\langle p \rangle \simeq \mathbb{F}_p \times \mathbb{F}_p$ en déduire que $\mathfrak{p}_2 \neq \mathfrak{p}_1$ (on peut remarquer que $\mathbb{F}_p \times \mathbb{F}_p$ ne contient pas d'élément nilpotent). ■

■ **Exemple 4.33**

1. On considère l'idéal $\mathfrak{p}_1 = \langle 2, 1+\sqrt{-5} \rangle$ dans $R = \mathbb{Z}[\sqrt{-5}]$. Les conditions de la proposition 4.26 sont bien vérifiées et donc il s'agit d'un idéal de norme 2. C'est donc un idéal premier. Il vérifie $\mathfrak{p}_1\bar{\mathfrak{p}}_1 = \langle 2 \rangle$ d'après la proposition 4.21. On a $\bar{\mathfrak{p}}_1 = \langle 2, 1-\sqrt{-5} \rangle = \langle 2, 1-\sqrt{-5}-2 \rangle = \mathfrak{p}_1$. Donc $\langle 2 \rangle = \mathfrak{p}_1^2$ est la décomposition de 2 en idéaux premiers.
2. On souhaite décomposer $\langle 3 \rangle$ dans $\mathbb{Z}[\sqrt{-5}]$. On a $\left(\frac{-20}{3}\right) = \left(\frac{1}{3}\right) = 1$, donc Δ est un carré non nul dans $\mathbb{F}_3$. L'idéal $\langle 3 \rangle$ se décompose donc en un produit de deux idéaux premiers distincts. On remarque que $\mathfrak{p}_2 = \langle 3, 1+\sqrt{-5} \rangle$ vérifie aussi les conditions de la proposition 4.26. C'est donc un idéal premier de norme 3. Il vérifie $\mathfrak{p}_2\bar{\mathfrak{p}}_2 = \langle 3 \rangle$ avec $\bar{\mathfrak{p}}_2 = \langle 3, 5+\sqrt{-5} \rangle$.
3. On reprend la décomposition (4.1) : $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \times 3$. On pose les idéaux premiers $\mathfrak{p}_1 = \langle 2, 1+\sqrt{-5} \rangle, \mathfrak{p}_2 = \langle 3, 1+\sqrt{-5} \rangle$ et $\mathfrak{p}_3 = \langle 3, 5+\sqrt{-5} \rangle = \bar{\mathfrak{p}}_2$. On a alors

$$\left\langle 1+\sqrt{-5} \right\rangle = \mathfrak{p}_1\mathfrak{p}_2, \quad \left\langle 1-\sqrt{-5} \right\rangle = \mathfrak{p}_1\mathfrak{p}_3, \quad \langle 2 \rangle = \mathfrak{p}_1^2, \quad \langle 3 \rangle = \mathfrak{p}_2\mathfrak{p}_3.$$

   Si bien que les deux factorisations de la relation (4.1) donnent bien une unique factorisation en idéaux premiers de $\langle 6 \rangle$, en l'occurrence $\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$.

```
> K<a> := QuadraticField(-5);
> O<w> := MaximalOrder(K);      // Anneau des entiers de K avec w^2 = -5
> fa   := ideal<O|1+w>; fb := ideal<O|1-w>; f2 := ideal<O|2>;  f3 := ideal<O|3>;
> // Factorization(fa); Factorization(fb);  Factorization(f2); Factorization(f3);
```

■

Exercice 4.34 — (★).
On pose $R = \mathbb{Z}[\sqrt{-6}]$.
1. S'agît-il d'un ordre maximal ? Quel est son discriminant ?
2. Décomposer $\mathfrak{a} = \langle 3+\sqrt{-6} \rangle$ en idéaux premiers dans R.
3. Est-ce que 7 est inerte dans R ? ■

Exercice 4.35 — (★★) Décomposition de 2. Soit $\mathcal{O}_K = \mathbb{Z}[\omega]$ l'ordre maximal d'un corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$.
1. On suppose que $2 \mid \Delta_K$. On pose $\mathfrak{p} = \left\langle 2, 1+\sqrt{d} \right\rangle$ si d impair et $\mathfrak{p} = \left\langle 2, \sqrt{d} \right\rangle$ sinon.
   a. Montrer que $\mathfrak{p}^2 = \langle 2 \rangle$.
2. On suppose que $2 \nmid \Delta_K$.
   a. Justifier qu'on a $d = 1 \mod 4$ et que $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. On pose $\omega = 1+\sqrt{d}/2$.
   b. On suppose que $d = 1 \mod 8$. Montrer que $\mathfrak{p} = \langle 2, 1+\omega \rangle$ vérifie $\mathfrak{p}\bar{\mathfrak{p}} = \langle 2 \rangle$. Justifier que $\mathfrak{p} \neq \bar{\mathfrak{p}}$ (on peut montrer que $R/\langle 2 \rangle$ n'a pas de nilpotent).
   c. On suppose que $d = 5 \mod 8$. Montrer qu'alors $\langle 2 \rangle$ est un idéal premier. ■

4.3.5 Preuve du théorème 4.16

On est maintenant en mesure de donnée une démonstration du théorème 4.16.

Démonstration. Soit $\mathfrak{a}$ un idéal fractionnaire, alors il existe $r \in \mathbb{N}$ tel que $r\mathfrak{a} = \langle n', a+m\omega\rangle = rm\left\langle \frac{n'}{m}, b+\omega\right\rangle$ avec $a = mb$. On peut donc supposer sans perte de généralité que $\mathfrak{a} = \langle n, b+\omega\rangle \subseteq \mathcal{O}_K$ (car $rm\left\langle \frac{n'}{m}, b+\omega\right\rangle$ et $\left\langle \frac{n'}{m}, b+\omega\right\rangle$ diffèrent de idéal principal $\langle rm\rangle$). Si $n \leq \mu_K$ c'est terminé. Sinon on écrit $b+\omega = s+\sqrt{\Delta}/2$ avec $s \in (1/2)\mathbb{Z}$. On pose $q \in \mathbb{Z}$ tel que $s-qn = r$ avec $r \in (1/2)\mathbb{Z}$ et $|r| \leq n/2$ (pour l'existence d'un tel q il suffit de retirer n à $s-qn$ tant que $s-qn \geq n/2$). On pose alors $\alpha = r+\sqrt{\Delta}/2 = s+\sqrt{\Delta}/2-qn$ c'est donc un élément de $\mathfrak{a}$. On a aussi

$$N(\alpha) = r^2 - \frac{\Delta}{4} \leq \frac{n^2-\Delta}{4} < n^2.$$

La dernière inégalité provient de l'hypothèse $n > \mu_K$, *i.e.* $-\Delta < 3n^2$.

Enfin, on pose $\mathfrak{a}' = (1/n)\,\bar{\alpha}\,\mathfrak{a}$. On affirme qu'il s'agit d'un idéal de $\mathcal{O}_K$ de norme strictement inférieure à celle de $\mathfrak{a}$. En effet, on a $N(\mathfrak{a}') = (N(\alpha)/n^2)\,N(\mathfrak{a}) < N(\mathfrak{a})$. Par ailleurs,

$$\begin{aligned}
\mathfrak{a}' = \frac{\bar{\alpha}}{n}\mathfrak{a} &= \left\langle \bar{\alpha}, \frac{\bar{\alpha}}{n}(b+\omega)\right\rangle, \\
&= \left\langle \bar{\alpha}, \frac{1}{n}(\bar{\alpha}+qn-qn)(\alpha+qn)\right\rangle, \\
&= \left\langle \bar{\alpha}, \frac{1}{n}\left(N(b+\omega)-qn(\alpha+qn)\right)\right\rangle, \\
&= \left\langle \bar{\alpha}, \underbrace{\frac{N(b+\omega)}{n}}_{\in\mathbb{Z}} - q(\alpha+qn)\right\rangle \subseteq \mathcal{O}_K.
\end{aligned}$$

■

Exercice 4.36 — (★) Nombre de classes $h(-20) = 2$.

On considère $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-5}\right]$.

1. Quel est le discriminant Δ de $\mathcal{O}_K$?
2. Montrer que tout idéal fractionnaire de $\mathcal{O}_K$ admet un représentant de norme 1 ou 2 dans $\mathcal{O}_K$.
3. Montrer que $\mathfrak{a} = \langle 2, 1\sqrt{-5}\rangle$ n'est pas principal (on peut utiliser le fait que $\mathcal{O}_K$ n'admet pas d'élément de norme 2, *cf.* l'exercice 4.8).
4. Montrer que $\mathrm{Cl}(\mathcal{O}_K) = \{[\mathcal{O}_K], [\mathfrak{a}]\}$ où $[\mathfrak{a}]$ désigne la classe de l'idéal fractionnaire $\mathfrak{a}$ dans le quotient $\mathrm{Cl}(\mathcal{O}_K)$.

■

Exercice 4.37 — (★) Principalité de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ pour $d \in \{-1,-2,-3,-7,-11\}$.

Montrer que tout idéal fractionnaire $\mathfrak{a}$ d'un ordre quadratique de discriminant $\Delta > -12$ vérifie $\mathfrak{a} = \alpha R$. En déduire que les ordres maximaux de $\mathbb{Q}\left(\sqrt{d}\right)$ pour $d \in \{-1,-2,-3,-7,-11\}$ sont tous principaux. ■

Exercice 4.38 — (★★) Principalité de $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

1. Montrer que tout idéal fractionnaire de $\mathcal{O}_K$ a un représentant de norme 1 ou 2 dans $\mathcal{O}_K$.
2. Montrer que 2 est inerte dans $\mathcal{O}_K$.
3. En déduire que $\mathcal{O}_K$ est principal. ∎

Exercice 4.39 — (★★) $h(-12) = 1$.

On pose $R = \mathbb{Z}\left[\sqrt{-3}\right]$.

1. Montrer que tout idéal fractionnaire de R est de norme 1 ou 2.
2. Montrer que $\mathfrak{b} = \langle 2, 1+\sqrt{-3}\rangle$ est l'unique idéal de R de norme 2.
3. Montrer que $\mathfrak{b}$ n'est pas inversible.
4. En déduire que $h(-12) = 1$. ∎

5. Courbes elliptiques complexes

Dans ce chapitre, on étudie les courbes elliptiques définies sur le corps des complexes. Une propriété fondamentale des courbes sur $\mathbb{C}$ est qu'il existe une correspondance entre les courbes sur $\mathbb{C}$ et les *tores complexes*, *i.e.* les quotients de $\mathbb{C}$ par un réseau Λ. Travailler dans le groupe $E(\mathbb{C})$ revient donc à travailler dans le quotient $\mathbb{C}/\Lambda$, ce qui est en général plus facile.

Une classe particulière de courbes elliptiques qui nous intéresse davantage est celle des courbes à multiplication complexe, *i.e.* les courbes qui ont pour anneau d'endomorphismes un ordre dans un corps quadratique imaginaire. Nous introduisons les polynômes de classe de Hilbert et les polynômes modulaires, des outils puissants qui nous permettent de classifier les courbes elliptiques à multiplication complexe par un ordre donné, puis d'étudier les isogénies existantes entre elles.

De façon surprenante ces résultats développés sur le corps des complexes à l'aide de la correspondance avec les tores complexes s'étendent aux courbes elliptiques définies sur un corps finis.

5.1 Tores complexes

Un sous-groupe $\Lambda \subseteq \mathbb{C}$ engendré par une $\mathbb{R}$-base de $\mathbb{C}$ est appelé un *réseau* de $\mathbb{C}$. Le groupe quotient $\mathbb{C}/\Lambda$ est appelé un *tore complexe*.

▪ Exemple 5.1

1. Tout ordre quadratique $R = \mathbb{Z}[\omega] \subseteq \mathbb{C}$ définit un réseau de $\mathbb{C}$. Mais attention, on n'a pas besoin qu'un réseau ait une structure d'anneau, seulement de groupe. Par exemple $\pi\mathbb{Z}[i] = \pi\mathbb{Z} + \pi i\mathbb{Z}$ ou $2\mathbb{Z}[i] = 2\mathbb{Z} + 2i\mathbb{Z}$ sont des réseaux de $\mathbb{C}$, mais ne sont pas des anneaux.
2. Pour n'importe quel $\tau \in \mathbb{C} \setminus \mathbb{R}$, $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ est un réseau de $\mathbb{C}$.
3. Soit $\mathfrak{a} \subseteq \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$ un idéal fractionnaire d'un ordre quadratique, alors $\mathfrak{a}$ est un réseau de $\mathbb{C}$.
4. $\mathbb{Z}$ n'est pas un réseau de $\mathbb{C}$ car $\mathbb{Z}\mathbb{R} = \mathbb{R}$. Donc $\mathbb{Z}$ ne contient pas de $\mathbb{R}$-base de $\mathbb{C}$.

▪

5.1.1 Morphismes de tores complexes

On considère deux tores complexes $X = \mathbb{C}/\Lambda$ et $X' = \mathbb{C}/\Lambda'$. Un morphisme de tores complexes $f\colon X \to X'$ est un morphisme de groupe holomorphe. Lorsque $f \neq 0$ on dit que f est une isogénie.

Proposition 5.2 Soit $f\colon X=\mathbb{C}/\Lambda \to X'=\mathbb{C}/\Lambda'$ un morphisme de tores complexes. Alors il existe un unique nombre complexe α appelé *représentation analytique* de f et noté $\rho_a(f)$ tel que $\alpha\Lambda\subseteq\Lambda'$ et tel que le diagramme suivant commute,

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{z\mapsto \alpha z} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda'. \end{array}$$

Réciproquement, tout complexe α tel que $\alpha\Lambda\subseteq\Lambda'$ induit un morphisme de tores complexes.

Démonstration. Le morphisme f se relève en une application holomorphe $\widetilde{f}\colon \mathbb{C}\to\mathbb{C}$. Puisque f est un morphisme de groupe on a pour tout $z,w\in\mathbb{C}$, $\widetilde{f}(z+w)-\widetilde{f}(z)-\widetilde{f}(w)\in\Lambda'$. Puisque $(z,w)\mapsto \widetilde{f}(z+w)-\widetilde{f}(z)-\widetilde{f}(w)$ est continue et contenue dans un ensemble discret, alors il existe $\lambda'\in\Lambda'$ tel que pour tout z,w on a $\widetilde{f}(z+w)-\widetilde{f}(z)-\widetilde{f}(w)=\lambda'$. Ceci implique que $\alpha=\widetilde{f}+\lambda'$ est un morphisme de groupe (holomorphe).

On a alors pour tout $a/b\in\mathbb{Q}$, $z\in\mathbb{C}$, $b\alpha((a/b)z)=a\alpha(z)$. Donc α est $\mathbb{Q}$-linéaire. Finalement, pour tout $z\in\mathbb{C}$, $w\mapsto\alpha(wz)-w\alpha(z)$ est holomorphe et identiquement nulle sur $\mathbb{Q}$, et par extension identiquement nulle sur $\mathbb{C}$. Ce qui prouve que α est $\mathbb{C}$-linéaire sur $\mathbb{C}$. On peut donc l'identifier avec son image de 1 (pour tout z, $\alpha(z)=z\cdot\alpha(1)$ par linéarité, donc totalement définie par son image de 1). ■

On peut aussi définir la *représentation rationnelle* de $f\colon X\to X'$ par le morphisme de groupes

$$\begin{array}{rccc} \rho_r(f)=\rho_a(f)_{|\Lambda}\ : & \Lambda & \longrightarrow & \Lambda', \\ & \lambda & \longmapsto & \alpha\lambda. \end{array}$$

On a immédiatement pour tout f, g morphismes de tores complexes $\rho_a(f\circ g)=\rho_a(f)\rho_a(g)$, et donc $\rho_r(f\circ g)=\rho_r(f)\rho_r(g)$.

Définition 5.3 Soit $f\colon\mathbb{C}/\Lambda\to\mathbb{C}/\Lambda'$ un morphisme non nul de tores complexes. On appelle degré de f l'entier $\deg f=\#\ker f$.

Corollaire 5.4 Deux tores complexes $X=\mathbb{C}/\Lambda$ et $X'=\mathbb{C}/\Lambda'$ sont isomorphes si et seulement si il existe $\alpha\in\mathbb{C}$ tel que $\alpha\Lambda=\Lambda'$, *i.e.* les réseaux Λ et Λ' sont homothétiques.

Démonstration. Supposons qu'il existe $f\colon X\to X'$ et $g\colon X'\to X$ tel que $f\circ g=\mathrm{id}_{X'}$ et $g\circ f=\mathrm{id}_X$. Alors, d'après la proposition 5.2, il existe $\alpha,\beta\in\mathbb{C}$ tels que $\alpha\Lambda\subseteq\Lambda'$ et $\beta\Lambda'\subseteq\Lambda$. Par unicité de la représentation analytique on doit avoir $\alpha\beta=1$. On a donc

$$\alpha\beta\Lambda'=\Lambda'\subseteq\alpha\Lambda\subseteq\Lambda'.$$

Donc, par double inclusion, $\alpha\Lambda=\Lambda'$. L'autre sens est immédiat. ■

L'anneau des endomorphismes d'un tore complexe $X=\mathbb{C}/\Lambda$ est

$$\mathrm{End}(X)=\{\alpha\in\mathbb{C}\colon \alpha\Lambda\subseteq\Lambda\}\,.$$

■ **Exemple 5.5**

1. Soit $\Lambda\subseteq\mathbb{C}$ un réseau et $X=\mathbb{C}/\Lambda$. Puisque c'est un groupe, on a pour tout $n\in\mathbb{Z}$, $n\Lambda\subseteq\Lambda$, donc $\mathbb{Z}\subseteq\mathrm{End}(\mathbb{C}/\Lambda)$. On note $[n]_\Lambda$ ou $[n]_X$, ou simplement $[n]$, l'endomorphisme

$$\begin{array}{ccc} X & \longrightarrow & X \\ z & \longmapsto & nz \end{array}$$

2. Soit $\mathfrak{a}$ un idéal fractionnaire d'un ordre quadratique vu comme un réseau de $\mathbb{C}$ alors

$$\mathrm{End}(\mathbb{C}/\mathfrak{a}) = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = (\mathfrak{a} : \mathfrak{a}) = R_{\mathfrak{a}}.$$

■

Proposition 5.6 Soit $X = \mathbb{C}/\Lambda$ un tore complexe. Alors $\mathrm{End}(X)$ est soit isomorphe à $\mathbb{Z}$, soit un ordre R dans un corps quadratique imaginaire.

Démonstration. Voir l'exercice 5.9. ■

Exercice 5.7

Soit $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ un morphisme non nul et $\alpha \in \mathbb{C}$ sa représentation analytique.

1. Montrer que $\deg f = [\Lambda' : \alpha\Lambda]$.
2. Montrer que $\deg[n]_\Lambda = n^2$. ■

Corollaire 5.8 Tout tore complexe $\mathbb{C}/\Lambda$ est isomorphe à un tore de la forme $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ avec $\mathrm{im}\,\tau > 0$.

Démonstration. On pose $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. On pose $\tau = \omega_1/\omega_2$ si $\mathrm{im}\,(\omega_1/\omega_2) > 0$ et $\tau = \omega_2/\omega_1$ sinon, et $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$. On a alors $(1/\omega_1)\Lambda = \Lambda_\tau$ ou $(1/\omega_2)\Lambda = \Lambda_\tau$. ■

Exercice 5.9 — (★★) Anneau d'endomorphisme.

Soit $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathbb{C}$ et $X = \mathbb{C}/\Lambda$ le tore complexe correspondant. On veut montrer que $R = \mathrm{End}(X) = \{\alpha \in \mathbb{C}/\alpha\Lambda \subseteq \Lambda\}$ est soit $\mathbb{Z}$, soit un ordre quadratique. Considérons $\alpha \in \mathrm{End}(X)$ et j, k, m, $n \in \mathbb{Z}$ tels que $\alpha\omega_1 = j\omega_1 + k\omega_2$ et $\alpha\omega_2 = m\omega_1 + n\omega_2$.

1. On pose $M = \begin{pmatrix} \alpha - j & -k \\ -m & \alpha - n \end{pmatrix} \in \mathrm{M}_2(\mathbb{C})$. Montrer que $\det(M) = 0$.
2. En déduire que $X^2 - (j+n)X + jn - km \in \mathbb{Z}[X]$ annule α et donc que α est un entier algébrique.
3. En déduire que $R \cap \mathbb{R} = \mathbb{Z}$.
4. Montrer que si $\alpha \notin \mathbb{Z}$, alors α est dans un ordre dans un corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{d})$.
5. Soit $\beta \in R \setminus \mathbb{Z}$ un autre élément. D'après ce qui précède β est aussi dans un ordre quadratique imaginaire dans un corps $\mathbb{Q}(\sqrt{d'})$.
   a. Soit $\alpha \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$, $\beta \in \mathbb{Q}(\sqrt{d'}) \setminus \mathbb{Q}$ avec d et d' des entiers sans facteur carré. Supposons que $\alpha + \beta$ de degré ≤ 2. Montrer qu'alors $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ (on peut se ramener au cas $\alpha = \sqrt{d}$ et $\beta = \sqrt{d'}$, puis déduire d'une relation de degré 2 en $\alpha + \beta$ que $\sqrt{d} \in \mathbb{Q}(\sqrt{d'})$).
   b. Conclure. ■

5.1.2 Tores complexes et courbes elliptiques

On appelle fonction elliptique sur $\mathbb{C}/\Lambda$ toute fonction méromorphe $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ telle que $f(z + \lambda) = f(z)$ pour tout $\lambda \in \Lambda$, $z \in \mathbb{C}$.

■ **Exemple 5.10**

1. La fonction nulle est une fonction elliptique.
2. La fonction

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

est une fonction elliptique appelée la fonction $\wp$ de Weierstrass associée à Λ.

3. Tous les éléments de $\mathbb{C}(\wp_\Lambda)$ (les fractions rationnelles en $\wp_\Lambda$) sont aussi des fonctions elliptiques.
4. Toutes les dérivées de $\wp_\Lambda$ sont aussi des fonctions elliptiques, en particulier $\wp'_\Lambda(z) = -2\sum_{\lambda\in\Lambda} 1/(z-\lambda)^3$.

∎

La proposition suivante affirme qu'il n'y a pas d'autres fonctions elliptiques que celles données dans l'exemple 5.10.

Proposition 5.11 L'ensemble $\mathbb{C}(\Lambda)$ des fonctions elliptiques sur $\mathbb{C}/\Lambda$ est $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$.

Soit $\Lambda \subseteq \mathbb{C}$ un réseau. On pose

$$G_k(\Lambda) = \sum_{\lambda\in\Lambda\setminus\{0\}} \lambda^{-k}$$

appelée série d'Eisenstein associée au réseau Λ. On pose aussi $g_2(\Lambda) = 60G_4(\Lambda)$ et $g_3(\Lambda) = 140G_6(\Lambda)$. Lorsqu'il n'y a pas d'ambiguïté sur le réseau Λ, on préfère note g_k, G_k ou $\wp$ au lieu de $g_k(\Lambda)$, $G_k(\Lambda)$ et $\wp_\Lambda$ pour les séries d'Eisenstein et la fonction $\wp$ de Weiestrass.

Théorème 5.12 — Théorème d'uniformisation. Soit $\Lambda \subseteq \mathbb{C}$ un réseau. On pose $\wp$ la fonction de Weierstrass associée au tore $\mathbb{C}/\Lambda$.

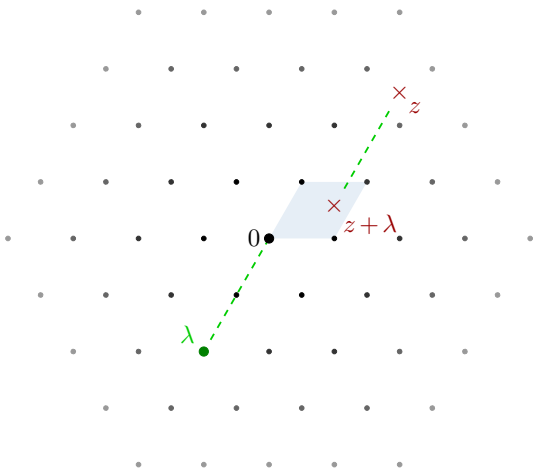
1. On a $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$.
2. L'application
$$\begin{array}{rccc} \phi_\Lambda\colon & \mathbb{C}/\Lambda & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ & z \neq 0 & \longmapsto & [\wp(z)\colon \wp'(z)\colon 1] \\ & 0 & \longmapsto & \infty = [0\colon 1\colon 0] \end{array}$$
définit un isomorphisme de groupes sur son image qui est $E_\Lambda(\mathbb{C})$ où E_Λ est la courbe elliptique définie par
$$E_\Lambda\colon y^2 = 4x^3 - g_2x - g_3\,.$$
3. Soit $E\colon y^2 = 4x^3 - Ax - B$ une courbe elliptique complexe. Alors il existe un unique réseau $\Lambda \subseteq \mathbb{C}$ tel que $g_2(\Lambda) = A$ et $g_3(\Lambda) = B$.
4. Soit $\varphi\colon E \to E'$ une isogénie entre courbes elliptiques complexes et $\phi_\Lambda\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ et $\phi_{\Lambda'}\colon \mathbb{C}/\Lambda \to E'(\mathbb{C})$ deux isomorphismes de groupes. Alors φ se relève en un morphisme de tores complexes $f\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$, *i.e.* on a le diagramme commutatif
$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda' \\ \downarrow{\scriptstyle \phi_\Lambda} & & \downarrow{\scriptstyle \phi_{\Lambda'}} \\ E(\mathbb{C}) & \xrightarrow{\varphi} & E'(\mathbb{C})\,. \end{array}$$

Autrement dit :
— tout réseau Λ permet de définir une courbe elliptique sur $\mathbb{C}$;
— toute courbe elliptique sur $\mathbb{C}$ provient d'un réseau ;
— lorsqu'on fixe deux tores (ou deux réseaux), alors on a une correspondance entre les morphismes de tores et ceux des courbes associées aux tores.

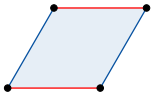
On peut résumer ces propriétés en disant qu'il y a une *équivalence de catégories* entre la catégorie des tores complexes et celle des courbes elliptiques. Sans rentrer dans les détails,

ceci signifie que ces deux mondes sont les mêmes : travailler avec des tores ou travailler avec des courbes elliptiques complexes revient au même.

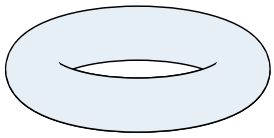
Géométrie des courbes elliptiques complexes



(a) Réseau $\Lambda \subseteq \mathbb{C}$



(b) Domaine fondamental de $\mathbb{C}/\Lambda$



(c) Identification des côtés rouges et bleus

FIGURE 5.1 – Courbes elliptiques sur les complexes

Un tore complexe, donc une courbe elliptique complexe, est homéomorphe à la surface d'un donut ! Malheureusement, cette représentation n'est que homéomorphe à une courbe elliptique complexe. En particulier, elle ne respecte pas la courbure. Il est difficile de se représenter fidèlement de courbes elliptiques complexes ; leur partie affine vit dans $\mathbb{C} \times \mathbb{C}$ donc en dimension 4 et en chaque point elles se propagent dans les 4 dimensions.

5.2 Espace de module des courbes elliptiques complexes

Soit $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subseteq \mathbb{C}$ un réseau. On définit le *discriminant* de $\mathbb{C}/\Lambda$ (ou de Λ) et son *j-invariant* par

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \text{ et } j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}$$

(il s'agit simplement du discriminant et du j-invariant de la courbe elliptique E_Λ correspondante).

On pose $\mathcal{H} = \{\tau \in \mathbb{C}, \operatorname{im}\tau > 0\}$, appelé demi-plan de Poincaré. On rappelle que d'après le corollaire 5.8, pour tout réseau Λ il existe $\tau \in \mathcal{H}$ tel que $\Lambda \simeq \Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$.

Lorsque $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ est un réseau avec $\operatorname{im}\tau > 0$, on écrit plutôt $g_k(\tau)$, $\Delta(\tau)$ et $j(\tau)$ au lieu de $g_k(\Lambda_\tau)$, $\Delta(\Lambda_\tau)$ et $j(\Lambda_\tau)$.

Exercice 5.13

Montrer que $g_k(\alpha\Lambda) = \alpha^{-2k}g_k(\Lambda)$. En déduire que pour tout réseau Λ et $\alpha \in \mathbb{C}$, on a $j(\Lambda') = j(\Lambda)$. ∎

Exercice 5.14

Montrer que $j(\mathbb{Z}[i]) = 1728$ (on peut montrer que $g_3(\mathbb{Z}[i]) = -g_3(\mathbb{Z}[i])$ en utilisant le fait que $i\mathbb{Z}[i] = \mathbb{Z}[i]$ et l'exercice précédent). ∎

Proposition 5.15 On pose $q = e^{2i\pi\tau} \in \mathbb{C}$. On a les formules suivantes :

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240\sum_{j=1}^{\infty}\frac{j^3 q^j}{1-q^j}\right),$$
$$g_3(\tau) = \frac{8\pi^6}{27}\left(1 - 504\sum_{j=1}^{\infty}\frac{j^5 q^j}{1-q^j}\right),$$
$$j(\tau) = \frac{\left(1 + 240\sum_{j=1}^{\infty}\frac{j^3 q^j}{1-q^j}\right)^3}{q\prod_{j=1}^{\infty}(1-q^k)^{24}}.$$

On utilise habituellement ces formules pour évaluer $j(\tau)$ car elles convergent rapidement.

On souhaite classifier toutes les classes d'isomorphismes de tores complexes (donc de courbes elliptiques complexes). C'est à dire être capable de déterminer un unique Λ pour chaque classe d'isomorphisme. On sait déjà que chaque classe d'isomorphisme contient un réseau de la forme Λ_τ avec $\tau \in \mathcal{H}$.

On note $\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a,b,c,d \in \mathbb{Z},\ ad-bc=1 \right\}$, et on définit par $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\cdot\tau = \frac{a\tau+b}{c\tau+d}$ l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathcal{H}$.

Exercice 5.16
Vérifier que pour tout $M \in \mathrm{M}_2(\mathbb{Z})$ tel que $\det(M) > 0$, on a pour $\tau \in \mathcal{H}$, $M\cdot\tau \in \mathcal{H}$. En déduire que l'action est bien définie. ∎

Proposition 5.17 Soit $\tau \in \mathcal{H}$ et $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, on a

$$j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau).$$

Démonstration. On a pour tout $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$,

$$\begin{aligned} G_k(M\cdot\tau) &= \sum_{m,n\neq(0,0)} \frac{1}{\left(m\frac{a\tau+b}{c\tau+d}+n\right)^k}, \\ &= (c\tau+d)^k \sum_{m,n\neq(0,0)} \frac{1}{(m(a\tau+b)+n(c\tau+d))^k}, \\ &= (c\tau+d)^k \sum_{m,n\neq(0,0)} \frac{1}{(mb+nd+(ma+nc)\tau)^k}. \end{aligned}$$

Or, l'application

$$\begin{aligned} M: \quad \mathbb{Z}^2 &\longrightarrow \mathbb{Z}^2, \\ (m,n) &\longmapsto M\cdot(m,n) = (ma+nc, mb+nd) = (m',n'), \end{aligned}$$

est une bijection d'inverse M^{-1} puisque M est inversible dans $\mathrm{M}_2(\mathbb{Z})$. Sommer sur $M\cdot\mathbb{Z}^2 = \mathbb{Z}^2$ revient donc à sommer sur $\mathbb{Z}^2$. Ainsi,

$$\begin{aligned} G_k(M\cdot\tau) &= (c\tau+d)^k \sum_{(m',n')\neq(0,0)} \frac{1}{(n'+m'\tau)^k}, \\ &= (c\tau+d)^k G_k(\tau). \end{aligned}$$

On a donc $g_2(M\cdot\tau) = (c\tau+d)^4 g_2(\tau)$ et $g_3(M\cdot\tau) = (c\tau+d)^6 g_3(\tau)$. On en déduit que

$$j(M\tau) = 1728\frac{g_2(M\cdot\tau)^3}{g_2(M\cdot\tau)^3 - 27g_3(M\cdot\tau)^2} = 1728\frac{(c\tau+d)^6 g_2(\tau)^3}{(c\tau+d)^6(g_2(\tau)^3 - g_3(\tau)^2)} = j(\tau).$$

■

Théorème 5.18

1. On a une bijection
$$\begin{array}{rccc} j: & \mathcal{H}/\operatorname{SL}_2(\mathbb{Z}) & \longrightarrow & \mathbb{C} \\ & \tau & \longmapsto & j(\tau). \end{array}$$
2. Un domaine fondamental de $\mathcal{H}/\operatorname{SL}_2(\mathbb{Z})$ est la bande
$$\mathcal{F} = \left\{ z\in\mathcal{H}, -\frac{1}{2} \le \Re(z) < \frac{1}{2}, |z|\ge 1 \text{ et } z\neq e^{i\theta} \text{ pour } \frac{\pi}{3} < \theta < \frac{\pi}{2} \right\}.$$

Démonstration.

1. Pas facile, voir [Was08, Corollary 9.18, Corollary 9.19].
2. Pour avoir l'idée de la preuve, faire un dessin en s'appuyant sur le fait que $\operatorname{SL}_2(\mathbb{Z})$ est engendré par $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. ■

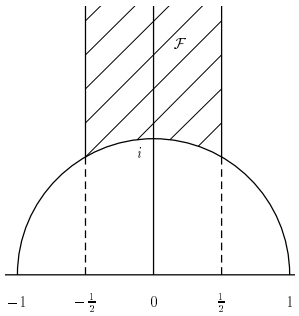


FIGURE 5.2 – Domaine fondamental de $\mathcal{H}/\operatorname{SL}_2(\mathbb{Z})$.

Rq **Interprétation du théorème.** Ceci signifie que pour n'importe quel réseau $\Lambda\subseteq\mathbb{C}$, il existe un unique $\alpha\in\mathbb{C}$ tel que $\alpha\Lambda = \Lambda_\tau$. Ainsi chaque point du domaine fondamental $\mathcal{F}$ correspond à une unique classe d'isomorphisme de tore complexe et donc de courbe elliptique. Cet espace paramétrise donc l'ensemble des courbes elliptiques complexes, on appelle cet objet un *espace de modules*.

Rq Pour celles et ceux familier avec la géométrie complexe, on peut remarquer que $\mathcal{F}$ a une structure de variété complexe de dimension 1 : c'est localement des petits bouts de $\mathbb{C}$. Cette variété n'est pas compacte à cause de l'axe des imaginaires de module >1 contenu dans $\mathcal{F}$. Pour la compactifier on peut rajouter astucieusement un point à l'infini. On obtient une surface de Riemann appelée *courbe modulaire* $X(1)$. On a donc paramétré l'ensemble des surfaces de Riemann de genre 1 (les courbes elliptiques complexes) par une variété complexe, *i.e.* chaque point de cette variété complexe correspond à une et une seule courbe elliptique.

On peut plus généralement définir d'autres courbes modulaires $X_0(N)$ sur le modèle de la construction de $X(1)$. Ces dernières permettent de définir les polynômes modulaires Φ_N que nous voyons plus tard comme les polynômes minimaux de certaines fonctions. On peut consulter sur le sujet les très complets [Sut17, Note 19 and 20].

5.2.1 Reconstruction du réseau

Si on a un réseau $\Lambda \subseteq \mathbb{C}$ et que l'on souhaite déterminer la courbe elliptique $E/\mathbb{C}$ correspondante via l'isomorphisme ϕ_Λ du théorème 5.12, on peut simplement approximer $g_2(\Lambda)$ et $g_3(\Lambda)$ et en déduire

$$E\colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Dans l'autre sens, c'est plus difficile. Pour simplifier supposons que l'on ait $E\colon y^2 = 4x^3 - ax - b = 4(x-e_1)(x-e_2)(x-e_3)$ avec $e_1 < e_2 < e_3$ réels. Alors E correspond au réseau $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ avec

$$\begin{cases} \omega_1 = \dfrac{\pi}{M\left(\sqrt{e_3-e_1}, \sqrt{e_3-e_2}\right)}, \\ \omega_2 = \dfrac{\pi i}{M\left(\sqrt{e_3-e_1}, \sqrt{e_2-e_1}\right)}, \end{cases}$$

où $M(a,b)$ désigne la moyenne arithmético-géométrique (voir [Was08, Theorem 9.26]. Elle est définie comme suit : on considère les suite (a_n) et (b_n) définies par $a_0 = a$, $b_0 = b$ et pour tout $n \geq 1$,

$$a_n = \frac{1}{2}(a_{n-1} + b_{n-1}) \text{ et } b_n = \sqrt{a_{n-1}b_{n-1}}.$$

Les deux suites convergent (rapidement) vers une limite commune notée $M(a,b)$.

Exercice 5.19
Montrer que $M(a,b) = M(b,a)$. ■

■ **Exemple 5.20** Si on considère $E\colon y^2 = 4x^3 - 4x = 4x(x-1)(x+1)$, alors on calcule

$$\begin{cases} \omega_1 = \dfrac{\pi}{M\left(\sqrt{2},\ 1\right)} = 2.62205755429211981046483958989\ldots \\ \omega_2 = \dfrac{\pi i}{M\left(\sqrt{2},\ 1\right)} = 2.62205755429211981046483958989\ldots i = \omega_1 i. \end{cases} \tag{5.1}$$

Ce réseau est isomorphe à $\Lambda_\tau = \frac{1}{\omega_2}(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \mathbb{Z}[i]$. Ce n'est pas complètement une surprise, car E admet l'endomorphisme $\iota\colon (x,y) \mapsto (-x,\ iy)$, que l'on peut identifier à i.

```
> RR := RealField(30);    // Corps des réels avec 30 décimales de précision
> CC := ComplexField(RR); // Le corps C considéré comme une extension de R
> Pi(RR) / ArithmeticGeometricMean(Sqrt(RR!2), RR!1); // Constante pi / M(sqrt(2),1)
2.62205755429211981046483958989
```

■

5.3 Courbes à multiplication complexe sur $\mathbb{C}$

Soit $X = \mathbb{C}/\Lambda$ un tore complexe et E_Λ la courbe elliptique telle que $E_\Lambda(\mathbb{C}) \underset{\phi_\Lambda}{\simeq} \mathbb{C}/\Lambda$ via l'isomorphisme du théorème 5.12. On a alors un isomorphisme d'anneaux

$$[\cdot]\colon R = \mathrm{End}(X) \longrightarrow \mathrm{End}(E)$$

donné par $[\alpha] = \phi_\Lambda \circ \alpha \circ \phi_\Lambda^{-1}$, *i.e.* de telle sorte qu'on ait un diagramme commutatif

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & X \\ \downarrow{\scriptstyle \phi_\Lambda} & & \downarrow{\scriptstyle \phi_\Lambda} \\ E_\Lambda & \xrightarrow{[\alpha]} & E_\Lambda . \end{array}$$

Lorsqu'on identifie un élément $\alpha \in R = \mathrm{End}(X) \subseteq \mathbb{C}$ à un endomorphisme de la courbe E_Λ correspondante, c'est toujours via cet isomorphisme.

D'après la proposition 5.6, étant donnée une courbe elliptique E sur $\mathbb{C}$, l'anneau $\mathrm{End}(E_\Lambda)$ ne peut donc prendre que deux formes possibles : $\mathbb{Z}$, ou un ordre R dans un corps quadratique imaginaire. Dans le second cas on dit que E est à *multiplication complexe*[1] par R, abrégé CM (pour *Complex Multiplication* en anglais).

Proposition 5.21 Soit $\tau \in \mathcal{H}, \Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ et E la courbe elliptique associée à Λ_τ (via ϕ_{Λ_τ}). Alors E est à multiplication complexe si et seulement s'il existe K corps quadratique imaginaire tel que $\tau \in K$.

Démonstration. Voir l'exercice 5.23. ■

On pose

$$\mathrm{Ell}_R(\mathbb{C}) = \{E \text{ courbe elliptique complexe telle que } \mathrm{End}(E) = R\} / \simeq,$$

l'ensemble[2] des classes d'isomorphisme de courbes elliptiques sur $\mathbb{C}$ à multiplication complexe par R.

Théorème 5.22 Soit R un ordre de nombre de classes $h(R) = h$ dans un corps quadratique imaginaire K. Alors

1. On a une bijection
$$\begin{array}{ccc} \mathrm{Cl}(R) & \longrightarrow & \mathrm{Ell}_R(\mathbb{C}), \\ [\mathfrak{a}] & \longmapsto & E_\mathfrak{a}, \end{array}$$
où $E_\mathfrak{a}$ est la courbe elliptique correspondant au réseau $\Lambda = \mathfrak{a} \subseteq \mathbb{C}$ via l'isomorphisme ϕ_Λ du théorème 5.12. En particulier, $\#\mathrm{Ell}_R(\mathbb{C}) = h$.
2. Le polynôme
$$H_R(X) = \prod_{\mathrm{Ell}_R(\mathbb{C})} (X - j(E)),$$
appelé *polynôme de classes de Hilbert*, est de degré h, à coefficients dans $\mathbb{Z}$ et irréductible sur $\mathbb{Q}$.

Démonstration.

1. Voir l'exercice 5.23.
2. Voir [Sil94, Theorem II.6.1]. ■

Le corps $L = K(j(E))$, avec $E \in \mathrm{Ell}_R(\mathbb{C})$, est une extension de degré $h(R)$ de K appelé *corps de classes de Hilbert*.

En particulier, pour toute courbe elliptique E à multiplication complexe par R, on a $j(E)$ entier algébrique de degré h. D'après la proposition 5.21, il existe un $\tau \in K$ tel que $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_\tau$ et $j(\tau) = j(E)$.

1. La terminologie vient du fait que si $\mathrm{End}(E) \neq \mathbb{Z}$, alors E admet des endomorphismes $\alpha \in \mathbb{C} \setminus \mathbb{R}$ qui agissent par multiplication sur le tore correspondant.
2. On peut aussi voir cet ensemble comme l'ensemble des j-invariants de ces courbes.

Exercice 5.23 — (★★) Multiplication complexe.
Soit $X = \mathbb{C}/\Lambda$ un tore complexe à multiplication complexe par un ordre quadratique $R = \mathrm{End}(X) = \{\alpha \in \mathbb{C}, \alpha\Lambda \subseteq \Lambda\}$ dans un corps quadratique K. On pose $\tau \in \mathcal{H}$ tel que $\Lambda \simeq \Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$.

1. Montrer que $\tau \in K$.
2. En déduire qu'il existe $u \in R$ tel que $u\Lambda_\tau$ est un idéal $\mathfrak{a}$ de R.
3. Montrer que $\mathfrak{a}$ est un idéal inversible (on peut considérer l'anneau des endomorphismes de $\mathfrak{a} \subseteq \mathbb{C}$ en tant que réseau).
4. Soit $\Lambda' \subseteq \mathbb{C}$ et $X' = \mathbb{C}/\Lambda'$ tel que $\Lambda' \simeq \mathfrak{a}'$ un idéal inversible de R. Montrer que $X \simeq X'$ si et seulement si $\mathfrak{a}$ et $\mathfrak{a}'$ ont la même classe dans $\mathrm{Cl}(R)$.
5. En déduire que $\#\mathrm{Ell}_{\mathbb{C}}(R) = \#\mathrm{Cl}(R) = h(R)$. ■

Les polynômes de classes de Hilbert permettent de déterminer les courbes elliptiques définies sur $\mathbb{F}_q$ d'anneaux d'endomorphismes maximaux.

Proposition 5.24 Soit $\mathbb{F}_q$ un corps fini et R un ordre quadratique de discriminant Δ avec Δ et q premiers entre eux. On suppose qu'il existe $a, r \in \mathbb{Z}$ tel que $4q = a^2 - r^2\Delta$. Alors les racines de $H_R(X)$ dans $\mathbb{F}_q$ sont exactement les j-invariants des courbes $E/\mathbb{F}_q$ à multiplication complexe par R.

5.4 Polynômes modulaires

Soit $N \geq 1$ un entier. On pose $S_N = \left\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}),\ ad = N \text{ et } 0 \leq b < d\right\}$ et, pour $\tau \in \mathcal{H}$, on définit le polynôme

$$F_N(X,\tau) = \prod_{S \in S_N} (X - j(S \cdot \tau)) = \sum_k a_k(\tau) X^k.$$

Théorème 5.25 On a les propriétés suivantes.

1. Pour tout $S \in \mathrm{SL}_2(\mathbb{Z})$, $a_k(S \cdot \tau) = a_k(\tau)$.
2. $a_k(\tau) \in \mathbb{Z}[j(\tau)]$.
3. Il existe un polynôme symétrique $\Phi_N(X,Y) \in \mathbb{Z}[X,Y]$, appelé N-ème polynôme modulaire, tel que
$$\Phi_N(X, j(\tau)) = F_N(X,\tau).$$
De plus, si N est premier alors Φ_N est degré $N+1$ en X et en Y.
4. Soient E et E' deux courbes elliptiques sur $\mathbb{C}$. Alors il existe une isogénie de degré N entre E et E' si et seulement si $\Phi_N(j(E), j(E')) = 0$.

Il est remarquable que cette façon de de détecter l'existence d'isogénies de degré N s'étende à n'importe quel corps de caractéristique $p \nmid N$, en particulier sur les corps fini ! Plus précisément on a le résultat suivant.

Théorème 5.26 Soit k un corps de caractéristique ne divisant pas $N > 1$. Pour tout j_1, $j_2 \in k$, on a $\Phi_N(j_1, j_2) = 0$ si et seulement si j_1 et j_2 sont les j-invariants de courbes elliptiques reliées par une isogénie de degré N sur k.

Démonstration. Voir [Sut17, Note 21, Theorem 21.4]. ■

■ **Exemple 5.27** Par exemple on a

$$\Phi_2(X,Y) = -(XY)^2 + X^3 + Y^3 + 2^4\cdot 3\cdot 31\cdot XY(X+Y) + \\ 3^4\cdot 5^3\cdot 4027\cdot XY - 2^4\cdot 3^4\cdot 5^3(X^2+Y^2) + 2^8\cdot 3^7\cdot 5^6(X+Y) - 2^{12}\cdot 3^9\cdot 5^9.$$

ou encore le code suivant donne le polynôme modulaire $\Phi_3(X,Y)$

```
> Pol<X, Y> := PolynomialRing(Integers(), 2);
> Pol!ClassicalModularPolynomial(3);
X^4 - X^3*Y^3 + 2232*X^3*Y^2 - 1069956*X^3*Y + 36864000*X^3 + 2232*X^2*Y^3 +
    2587918086*X^2*Y^2 + 8900222976000*X^2*Y + 452984832000000*X^2 - 1069956*X*Y^3 +
    8900222976000*X*Y^2 - 770845966336000000*X*Y + 1855425871872000000000*X + Y^4 +
    36864000*Y^3 + 452984832000000*Y^2 + 1855425871872000000000*Y
```

■

Rq Les exemples de polynôme modulaire que l'on peut donner sont malheureusement très limités à cause de la taille des coefficients. Le polynôme Φ_{10} a des coefficients qui ont jusqu'à 150 décimales, il faut environ 4GB pour stocker les coefficients de Φ_{1009} et 5TB pour ceux de Φ_{10007}.

6. Cardinalité des courbes sur les corps finis

Nous commençons par une application du chapitre 5 à la détermination de courbes elliptiques d'anneau d'endomorphismes donné (et donc sur un corps fini de nombre de points donné), pour des ordres quadratiques de discriminant petit.

Nous attaquons ensuite le problème inverse, *i.e.* trouver le nombre de points d'une courbe elliptique dont on se donne l'équation. Nous pouvons déjà imaginer certains algorithmes de comptage de points.

— Par exemple en utilisant la formule de la proposition 3.9, on peut calculer le cardinal de $\#E(\mathbb{F}_q)$ en q calculs de symboles de Legendre (envisageable jusqu'à $q \sim 10^9$).

— Une autre façon de faire serait de choisir un point rationnel aléatoire P sur la courbe E et de calculer son ordre d (par exemple à l'aide de l'algorithme *baby-giant steps*). On a $d \mid \#E(\mathbb{F}_q)$. Si de plus $q+1-2\sqrt{q} \leq d \leq q+1+2\sqrt{q}$, alors $\#E(\mathbb{F}_q) = d$. Sinon on choisit un nouveau point et on prend d égal au ppcm des ordres déjà calculés. Cette méthode est de complexité $O(q^{1/4})$ opérations élémentaires.

Nous présentons ici l'algorithme de Schoof, qui permet de répondre à la question en temps polynomial en $\log q$, en l'occurrence $O(\log^8 q)$. Il consiste à calculer $\#E(\mathbb{F}_q) \bmod \ell_i$ pour suffisamment de nombres premiers ℓ_i, ce qui nous permet d'avoir $\#E(\mathbb{F}_q) \bmod \prod_i \ell_i$ grâce au théorème des restes et de conclure à l'aide de la borne de Hasse. Sa complexité est de $O(\log^8 q)$ opérations élémentaires.

Enfin, nous présentons une amélioration, l'algorithme SEA pour (Schoof, Elkies et Atkin), qui permet de calculer $\#E(\mathbb{F}_q)$ en complexité $O(\log^4 q)$. Les plus récentes améliorations permettent de calculer $\#E(\mathbb{F}_p)$ pour des nombres premiers p de 500 décimales.

6.1 Méthode CM

6.1.1 Bref rappel sur les tordues

On rappelle que deux courbes elliptiques E et E' définies sur un corps k de caractéristique différente [1] de 2 et 3 peuvent être isomorphes sur $\bar{k}$, *i.e.* elles ont le même j-invariant, sans être isomorphes sur k. La courbe E' est alors appelée *tordue* de E.

■ **Exemple 6.1** Si on considère $E\colon y^2 = x^3 + x + 2$ et $E'\colon y^2 = x^3 - x - 1$ définie sur $\mathbb{F}_5$ alors leur j-invariant est 1. Elles sont donc isomorphes sur $\bar{\mathbb{F}}_5$. Pourtant elles ne sont pas isomorphes sur $\mathbb{F}_5$, sinon on aurait $\#E(\mathbb{F}_5) = \#E'(\mathbb{F}_5)$. Or leur cardinaux respectifs sont 4 et 8. ■

1. Les corps de caractéristique 2 ou 3 ne font pas exception, mais la théorie des tordues est plus compliquée.

Lorsque $E\colon y^2 = x^3 + Ax + B$ et E' sont isomorphes sur $\bar{k}$, et que leur j-invariant est $\neq 0, 1728$, alors on peut montrer qu'elles sont toujours isomorphes sur une extension de degré 2 de k, *i.e.* il existe un élément $\delta \in k$ qui n'est pas un carré dans k tel que

$$E' = E_\delta\colon y^2 = x^3 + \delta^2 Ax + \delta^3 B\,.$$

Ces courbes E_δ sont appelées les *tordues quadratiques* de E (le quadratique vient du fait que l'isomorphisme entre les deux courbes est sur une extension de degré 2). Lorsque $j = 0$ ou 1728 alors les tordues peuvent être isomorphes sur une extension de degré 4 ou 6.

Exercice 6.2
Montrer que si $E\colon y^2 = x^3 + Ax + B$ sur $\mathbb{F}_q$ a $q+1-a$ points rationnels alors pour tout $\delta \in \mathbb{F}_q$ non carré $E'\colon y^2 = x^3 + \delta^2 Ax + \delta^3 B$ a $q+1+a$ points rationnels (on peut utiliser la formule de la proposition 3.9 et constater que $x \mapsto \delta x$ est une bijection de $\mathbb{F}_q$). ■

■ **Exemple 6.3** Si on reprend l'exemple précédent on a bien $\#E(\mathbb{F}_5) = 5+1-2 = 4$ et $\#E'(\mathbb{F}_5) = 5+1+2 = 8$. ■

6.1.2 Méthode CM

Soit $k = \mathbb{F}_q$ un corps fini à $q = p^s$ éléments avec $p \neq 2$, 3 et N un entier. On cherche à déterminer une courbe ordinaire $E/\mathbb{F}_q$ telle que $\#E(\mathbb{F}_q) = N$. Pour simplifier on cherche E telle que $j(E) \neq 0, 1728$. [2]

On remarque que si une telle courbe existe alors sa trace, *i.e.* la trace du Frobenius, est $a = t_E = q+1-N$ (voir le paragraphe 3.2). On en déduit que le Frobenius π est une racine du polynôme $\chi = X^2 - aX + q \in \mathbb{Z}[X]$.

L'hypothèse E ordinaire est équivalente à ce que χ soit le polynôme minimal de π sur $\mathbb{Q}$ vu comme un élément de $K = \mathrm{End}(E) \otimes \mathbb{Q}$. On en déduit que $\mathbb{Z}[\pi] = \mathbb{Z}[X]/\langle\chi\rangle$ est un ordre dans le corps quadratique $K = \mathbb{Q}\left(\sqrt{a^2-4q}\right)$ et on a les inclusions suivantes,

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K \subseteq K\,. \tag{6.1}$$

Commençons par énumérer des résultats faciles mais essentiels.

1. Si E et E' sont des courbes elliptiques ordinaires de Frobenius π_E et $\pi_{E'}$ sur un même corps $\mathbb{F}_q$ et ont le même nombre de points rationnels N, alors

   $$\mathbb{Z}[\pi_E] \simeq \mathbb{Z}[\pi_{E'}].$$

   En effet, si elles ont le même nombre de points, elles ont la même trace et les polynômes minimaux de leurs Frobenius sont identiques.

2. Si E et E' sont des courbes elliptiques ordinaires de Frobenius π_E et $\pi_{E'}$ sur un même corps $\mathbb{F}_q$ telles que $\mathbb{Z}[\pi_E] \simeq \mathbb{Z}[\pi_{E'}]$, alors E' a le même nombre de points que E ou qu'une tordue quadratique de E.

   On a dit dans au chapitre 4 que le discriminant détermine l'ordre. Si on a un tel isomorphisme alors $a^2 - 4q = b^2 - 4q$ donc $b = \pm a$ avec a et b les traces de E et E'.

Là où c'est plus flou, c'est lorsqu'on n'impose pas que l'ordre engendré par le Frobenius soit fixé. Si on prend deux courbes E et E' dont les anneaux d'endomorphismes vivent dans un même corps quadratique K, peut on toujours en déduire que les ordres engendrés

2. Ceci implique que l'anneau des endomorphismes de E n'est pas $\mathbb{Z}[i]$, ni $\mathbb{Z}[j]$. En particulier ; ses seuls inversibles sont $\{\pm 1\}$ d'après le corollaire 4.6.

par leur Frobenius sont isomorphes ? Autrement dit, est-ce possible qu'on se retrouve dans une situation comme celle-ci ?

$$\begin{array}{ccc} \mathbb{Z}[\pi_E] & \hookrightarrow & \mathrm{End}(E) \\ \not\parallel & & \searrow \\ & & \mathcal{O}_K \subseteq K\,. \\ \nearrow & & \\ \mathbb{Z}[\pi_{E'}] & \hookrightarrow & \mathrm{End}(E') \end{array}$$

La réponse est non, en d'autres termes si on considère l'ensemble de toutes les courbes elliptiques E sur $\mathbb{F}_q$ à multiplication complexe par un ordre dans un corps quadratique imaginaire fixé K alors l'ordre engendré par leur Frobenius est un sous-ordre commun à tous les anneaux d'endomorphismes de ces courbes. C'est donc un ordre minimal pour ces ordres en quelques sorte.

Proposition 6.4 Soit E et E' deux courbes elliptiques ordinaires définies sur $\mathbb{F}_q$ de traces a et b. On suppose que $\mathrm{End}(E)\otimes\mathbb{Q} \simeq \mathrm{End}(E')\otimes\mathbb{Q}$ *i.e.* $\mathrm{End}(E)$ et $\mathrm{End}(E')$ sont des ordres dans le même corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$. On suppose que $d \neq -1, -3$. Alors $b = \pm a$, *i.e.* E' a le même nombre de points rationnels que E ou le même nombre de points qu'une de ses tordues.

Démonstration. Par simplicité on fait la preuve dans le cas d'un corps premier, *i.e.* $q = p$ (voir la remarque qui suit pour la généralisation).

Les Frobenius de E et E' ont pour polynômes minimaux respectifs $\chi = X^2 - aX + p$ et $\chi' = X^2 - bX + p$, et ont donc pour discriminants $\Delta = a^2 - 4p$ et $\Delta' = b^2 - 4p$. Par hypothèse, ils sont dans le même ordre quadratique $\mathbb{Q}\left(\sqrt{\Delta}\right) = \mathbb{Q}\left(\sqrt{\Delta'}\right) = \mathbb{Q}\left(\sqrt{\Delta_K}\right) = \mathbb{Q}(\sqrt{d})$ avec Δ_K le discriminant de l'ordre maximal $\mathcal{O}_K$. On note f et g leur conducteurs respectifs. On a alors $\Delta = f^2\Delta_K$ et $\Delta' = g^2\Delta_K$. On écrit alors

$$\begin{cases} a^2 - f^2\Delta_K = N\left(a + f\sqrt{\Delta_K}\right) &= 4p, \\ b^2 - g^2\Delta_K = N\left(b + g\sqrt{\Delta_K}\right) &= 4p. \end{cases} \tag{6.2}$$

Par l'hypothèse E et E' ordinaires, on a $a,\ b \neq 0 \bmod p$. Donc $\Delta_K \neq 0 \bmod p$ et on a $\Delta_K = a^2/f^2 \bmod p$ c'est donc un carré ce qui prouve, d'après la proposition 4.29, que p se décompose complètement dans $\mathcal{O}_K$. On a donc $\langle p\rangle = \mathfrak{p}\bar{\mathfrak{p}}$ pour $\mathfrak{p}$ un idéal de norme p distinct de $\bar{\mathfrak{p}}$.

On distingue alors deux cas.

Si $2 \mid \Delta_K$ **:** Ce cas est équivalent à ce que $d \neq 1 \bmod 4$. On remarque alors que, d'après les relations (6.2), a et b doivent être pairs. Disons $a = 2a'$ et $b = 2b'$. On a alors les égalités de $\mathcal{O}_K$-idéaux

$$\begin{aligned} \left\langle a^2 - f^2\Delta_K \right\rangle &= \left\langle a + f\sqrt{\Delta_K} \right\rangle \left\langle a - f\sqrt{\Delta_K} \right\rangle \\ &= \langle 4\rangle \left\langle a' + f\frac{\sqrt{\Delta_K}}{2} \right\rangle \left\langle a' - f\frac{\sqrt{\Delta_K}}{2} \right\rangle \\ &= \langle 4p\rangle \;=\; \langle 4\rangle\, \mathfrak{p}\bar{\mathfrak{p}}. \end{aligned}$$

Donc,

$$\left\langle a' + f\frac{\sqrt{\Delta_K}}{2} \right\rangle \left\langle a' - f\frac{\sqrt{\Delta_K}}{2} \right\rangle = \mathfrak{p}\bar{\mathfrak{p}}\,.$$

Et, de la même façon,

$$\left\langle b' + g\frac{\sqrt{\Delta_K}}{2} \right\rangle \left\langle b' - g\frac{\sqrt{\Delta_K}}{2} \right\rangle = \mathfrak{p}\bar{\mathfrak{p}}\,.$$

Par ailleurs, aucun de ces idéaux principaux n'est trivial car $f,\, g \neq 0$. Donc l'élément générateur n'est pas inversible dans $\mathcal{O}_K$. Il s'agit donc de deux décomposition de l'idéal $\langle p\rangle$ dans $\mathcal{O}_K$, elles sont donc identiques, *i.e.* $\left\langle a' + f\sqrt{\Delta_K}/2 \right\rangle = \mathfrak{p}$ ou $\bar{\mathfrak{p}}$, et pareil pour $\left\langle b' + g\sqrt{\Delta_K}/2 \right\rangle$. On en déduit que $\left\langle a' + f\sqrt{\Delta_K}/2 \right\rangle = \left\langle b' + g\sqrt{\Delta_K}/2 \right\rangle$ ou son conjugué. C'est-à-dire,

$$a' + f\frac{\sqrt{\Delta_K}}{2} = \pm\left(b' + g\frac{\sqrt{\Delta_K}}{2}\right) \text{ ou } a' + f\frac{\sqrt{\Delta_K}}{2} = \pm\left(b' - g\frac{\sqrt{\Delta_K}}{2}\right)$$

(le ± 1 vient du fait que les seuls inversibles de $\mathcal{O}_K$ sont $\{\pm 1\}$, c'est ici qu'on utilise l'hypothèse $d \neq -1, -3$). Dans tous les cas, on a $b' = \pm a'$, et donc $b = \pm a$.

Si $2 \nmid \Delta_K$: Dans ce cas, d'après l'exercice 4.35), 2 est inerte dans $\mathcal{O}_K$, *i.e.* $\langle 2\rangle$ est premier. Par la relation

$$\left\langle a + f\sqrt{\Delta_K} \right\rangle \left\langle a - f\sqrt{\Delta_K} \right\rangle = \langle 4\rangle\, \mathfrak{p}\bar{\mathfrak{p}}$$

on en déduit que $2 \,|\, a \pm f\sqrt{\Delta_K}$ et, de la même façon, $2 \,|\, b \pm g\sqrt{\Delta_K}$. On en déduit encore que

$$a + f\sqrt{\Delta_K} = \pm\left(b + g\sqrt{\Delta_K}\right) \text{ ou } a + f\sqrt{\Delta_K} = \pm\left(b - g\sqrt{\Delta_K}\right),$$

et donc que $b = \pm a$. ■

Il est important de comprendre ce que cette proposition implique. Si on arrive à trouver une courbe elliptique E telle que $\mathrm{End}(E)$ est un ordre dans $\mathbb{Q}\left(\sqrt{a^2 - 4p}\right)$ avec $a = q + 1 - N$, alors, quel que soit l'ordre $\mathrm{End}(E)$, soit E a le bon nombre de points $N = q + 1 - a$, soit sa tordue quadratique a N points. Peu importe qui est $\mathrm{End}(E)$. D'autre part, on sait qu'on ne doit chercher $\mathrm{End}(E)$ que dans les ordres « coincés » entre $\mathbb{Z}[\pi]$ et $\mathcal{O}_K$.

Rq Si nous avions voulu faire la preuve dans le cas général $q = p^s$, nous aurions eu comme égalité à gérer, par exemple dans le premier cas,

$$\left\langle a' + f\frac{\sqrt{\Delta_K}}{2} \right\rangle \left\langle a' - f\frac{\sqrt{\Delta_K}}{2} \right\rangle = \mathfrak{p}^s\bar{\mathfrak{p}}^s\,.$$

Le problème c'est qu'on peut alors avoir, *a priori*, $\left\langle a' + f\sqrt{\Delta_K}/2 \right\rangle \mathfrak{p}^{n-i}\bar{\mathfrak{p}}^i$ (car $a' + f\sqrt{\Delta_K}/2$ et son conjugué ont la même norme p^n).

Mais si $i \neq 0, n$, on a alors un $\mathfrak{p}\bar{\mathfrak{p}} = \langle p\rangle$ en facteur. Ceci implique que $p \,|\, a' + f\sqrt{\Delta_K}/2$ donc p divise a' donc a ce qui contredit l'hypothèse E ordinaire. La conclusion est la même ensuite.

Rq Le résultat de la proposition 6.4 est faux sans l'hypothèse $d \neq -1, -3$. Sur $\mathbb{F}_5$ par exemple, on a des courbes dont le discriminant de l'ordre engendré par leur Frobenius égal à -4 (par exemple $E\colon y^2 = x^3 + 2x$) et d'autre -16 (par exemple $E'\colon y^2 = x^3 + x$). On peut aussi trouver des contre-exemples dans $\mathbb{F}_7$ avec les discriminants $-3, -12$ et -27 qui ont pour conducteur respectifs 1 (l'ordre maximal), 2 et 3 dans $\mathbb{Z}[j]$.

Le problème étant que deux courbes E et E' dont le Frobenius est respectivement annulé par $X^2 - aX + q$ et $X^2 + aX + q$ donnent le même ordre $\mathbb{Z}[\pi]$. Ceci n'est pas très grave car ces deux courbes ont le même j-invariant et sont donc isomorphes sur $\mathbb{F}_{q^2}$, l'une

est la tordue quadratique de l'autre ($j(E) \neq 0,\ 1728$). En d'autres termes si E a pour équation $y^2 = x^3 + Ax + B$, alors il existe $\delta \in \mathbb{F}_q$ qui n'est pas un carré tel que E' est donnée par $y^2 = x^3 + \delta^2 Ax + \delta^3 B$.

Il est maintenant possible d'énoncer l'algorithme 1.

Algorithme 1 : Trouver une courbe elliptique à N points sur $\mathbb{F}_q$

Input : Un corps fini $\mathbb{F}_q$ avec q impair et entier N.
Output : Une courbe elliptique $E/\mathbb{F}_q$ telle que $\#E(\mathbb{F}_q) = N$.

1 Calculer la trace $a = q + 1 - N$;
2 S'assurer que $a \neq 0 \bmod p$;
3 Calculer le discriminant du Frobenius $r^2\Delta = a^2 - 4q$;
4 S'assurer que $\Delta \leq 0$;
5 Construire le corps $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{d})$ et l'ordre maximal $\mathcal{O}_K = \mathbb{Z}[\omega]$;
6 En déduire le conducteur f de $\mathbb{Z}[\pi]$;
7 **for** $f' \mid f$ **do**
8 Poser $R = \mathbb{Z}[f'\omega]$;
9 Calculer le polynôme de classes de Hilbert $H_R(X) \in \mathbb{F}_q[X]$.;
10 **if** H_R a une racine $j \in \mathbb{F}_q \setminus \{0, 1728\}$ **then**
11 Construire une courbe $E\colon y^2 = x^3 + Ax + B/\mathbb{F}_q$ ayant pour j-invariant j;
12 **if** $\#E(\mathbb{F}_q) = N$ **then**
13 Retourner E;
14 **else**
15 Choisir $\delta \in \mathbb{F}_q$ un non-carré;
16 Retourner $y^2 = x^3 + \delta^2 Ax + \delta^3 B$;

Rq Quelques précisions sur l'algorithme.

- L'étape 2 sert à s'assurer que les courbes à N points ne sont pas supersingulières.
- L'étape 4 sert à s'assurer que la borne de Hasse est satisfaite. Sans cela il n'existe pas de courbe $E/\mathbb{F}_q$ à N points.
- l'étape 6 peut se faire en calculant la partie carré de $\Delta = r^2 d$. Il y a alors deux cas à distinguer :
  - soit $d = 1 \bmod 4$, et alors $f = r$;
  - sinon $\Delta = f^2 \cdot 4d$, et $f = r/2$.
- On boucle sur $f' \mid f$ et non sur f' de 1 à f car on sait que pour un ordre de conducteur f' coincé entre R, de conducteur f, et $\mathcal{O}_K$, on a $f' \mid f$.
- Pour l'étape 9, on peut approximer les j-invariants $j(\mathfrak{a})$ des réseaux $\mathfrak{a} \subseteq \mathbb{C}$ pour $\mathfrak{a}$ parcourant des représentants du groupe des classes $\mathrm{Cl}(R)$. Ça nous donne un polynôme

$$H_R(X) = \prod_{[\mathfrak{a}] \in \mathrm{Cl}(R)} (X - j(\mathfrak{a})) \in \mathbb{Z}[X].$$

  Suivant la précision du calcul des j-invariant on peut reconnaître un polynôme à coefficients dans $\mathbb{Z}$, qu'il suffit ici de réduire modulo p.
- Pour l'étape 11, étant donné $j \in \mathbb{F}_q \setminus \{0, 1728\}$ on peut construire la courbe

$$E\colon y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j} \tag{6.3}$$

  définie sur $\mathbb{F}_q$ et de j-invariant j (exercice).
- Il faut comprendre qu'à ce stade on a pas encore gagné. Le j-invariant détermine seulement la classe de $\overline{\mathbb{F}}_q$-isomorphisme d'une courbe elliptique. On peut affirmer que si $E/\mathbb{F}_q$ a N points rationnels, alors son j-invariant est une racine de H_R (pour R un ordre entre $\mathbb{Z}[\pi]$ et $\mathcal{O}_K$). Cependant la réciproque n'est pas vraie si on prend une tordue.

— L'hypothèse $j \neq 0, 1728$ sert à deux endroits :
  1. Construire systématiquement une courbe sur $\mathbb{F}_q$ ayant un j-invariant donné. Ceci n'est pas une vraie restriction car on sait que les courbes $y^2 = x^3 + B$ et $y^2 = x^3 + Ax$ ont pour j-invariants respectifs 0 et 1728.
  2. Déterminer toutes les tordues de E ayant pour j-invariant $j \neq 0, 1728$. Cette restriction est beaucoup plus contraignante. En effet, lorsque $j \neq 0, 1728$ il existe une unique tordue de E, celle quadratique. En revanche, pour $j = 0, 1728$ il peut y en avoir plus et les trouver est plus compliqué.

— La condition $\#E(\mathbb{F}_q) = N = q+1-a$ peut, en pratique, être considérablement accélérée. En effet, à ce stade on sait seulement que E est soit la courbe qui nous intéresse, *i.e.* $\#E(\mathbb{F}_q) = N$ soit sa tordue quadratique E' dont la trace satisfait alors $t_{E'} = -t_E$. Pour déterminer ce qu'il en est, on peut prendre un point P au hasard sur E et calculer $(q+1+a)P$ et $(q+1-a)P$. Si les deux points sont égaux à l'élément neutre, pas de chance, on recommence avec un autre P. Sinon, exactement l'un des deux est le l'élément neutre, on peut en déduire que :
  — si $(q+1-a)P = O$ et $(q+1+a)P \neq O$ alors $\#E(\mathbb{F}_q) = q+1-a = N$ on renvoie cette courbe ;
  — si $(q+1+a)P = O$ et $(q+1-a)P \neq O$ alors $\#E(\mathbb{F}_q) = q+1+a \neq N$ et on renvoie une tordue quadratique qui, elle, a le bon nombre de point N (inutile de le vérifier).

— En pratique, l'étape $f' = 1$ suffit, on se contente de courbes à multiplication complexe par un ordre maximal. On doit parcourir d'autres conducteurs $f' \neq 1$ lorsque l'ordre maximal est $\mathbb{Z}[i]$ ou $\mathbb{Z}[j]$ (*i.e.* lorsque le j-invariant est 0 ou 1728).

On va maintenant donner plusieurs exemples d'application de cet algorithme.

■ **Exemple 6.5** Commençons par un cas simple. Si on prend $q = 31$ et $N = 32$ alors $a = q+1-N = 0$ donc les courbes correspondantes sont supersingulières. On abandonne. ■

■ **Exemple 6.6** On prend $N = 37$ et $q = 31$. On a alors $a = q+1-37 = -5$ et $\Delta = a^2 - 4q = -11$. Il s'agit du discriminant de l'ordre maximal $\mathcal{O}_K$ de $\mathbb{Q}(\sqrt{-11})$. On calcule $H = H_{\mathcal{O}_K} = X + 32768 \in \mathbb{Z}[X]$ (il est bien de degré $1 = h(\mathcal{O}_K)$). On a donc $H = X + 1 \bmod 31$. Une courbe à 37 points sur $\mathbb{F}_{31}$ a pour j-invariant $-1 \neq 1728$.

On calcule une telle courbe grâce à la formule (6.3). On obtient $E\colon y^2 = x^3 + 27x + 18$. À ce stade on sait que $\#E(\mathbb{F}_{31}) = 37$ ou $\#E(\mathbb{F}_{31}) = q+1+a = 27$. On calcule un point choisi au hasard sur E, par exemple $P = (21, 9)$ et $37 \cdot P = (10, 20) \neq [0\colon 1\colon 0]$. Donc E n'est pas la courbe qu'on cherche, mais sa tordue quadratique ! La réciprocité quadratique nous dit que $\left(\frac{-1}{31}\right) = (-1)^{\frac{30}{2}} = -1$ donc une tordue quadratique est donnée par $E'\colon y^2 = x^3 + 27x - 18$ qui a 37 points rationnels.

```
> q := 31; k := GF(q);
> Pol<x> := PolynomialRing(k);
> N := 37;
> a := q+1-N; a;           // La trace
-5
> Delta := a^2-4*q; Delta; // Le discriminant de l'ordre engendré par le Frobenius
-99
> d, r := SquareFree(Delta); d, r; // Les entiers positifs tels que Delta = r^2*d
-11 3
> K := QuadraticField(d); O<w> := MaximalOrder(K);
> H := ChangeRing(HilbertClassPolynomial(Discriminant(O)), k);H;
x + 1
> j := Roots(H)[1][1];j;   // j = -1
30
> E := EllipticCurve([3*j/(1728-j), 2*j/(1728-j)]);E; // Courbe avec q+1 +/- a points
Elliptic Curve defined by y^2 = x^3 + 27*x + 18 over GF(31)
> P := Random(E);P;
(22 : 21 : 1)
```

```
> 37*P;       // Différent de 0, donc E n'à pas 37 points, c'est sa tordue la bonne !
(22 : 21 : 1)
> IsSquare(k!-1);
false
> EllipticCurve([3*j/(1728-j), -2*j/(1728-j)]); //La tordue que voici
Elliptic Curve defined by y^2 = x^3 + 27*x + 13 over GF(31)
```

■

■ **Exemple 6.7** On considère $\mathbb{F}_{2197} = \mathbb{F}_{13^3}$ et $N = 2110$. On a $a = q+1-N = 88$ et

$$\Delta = a^2 - 4q = 88^2 - 4 \cdot 2197 = -1044 = -6^2 \cdot 29.$$

Donc $d = -29 = 3 \bmod 4$ et $f = 6/2$. On en déduit que le Frobenius de telles courbes engendrent l'ordre

$$\mathbb{Z}[\pi] \simeq \mathbb{Z}[3\omega] \subseteq \mathbb{Z}[\omega] = \mathbb{Z}\left[\sqrt{-29}\right] \subseteq \mathbb{Q}\left(\sqrt{-29}\right).$$

On commence par déterminer le polynôme de Hilbert de l'ordre maximal,

$$H(X) = X^6 + 9X^5 + 3X^4 + 6X^3 + 5X^2 + 10X + 12 = (X - j_1) \cdots (X - j_6) \in \mathbb{F}_{13^3}[X]$$

qui a 6 racines $j_1, \ldots, j_6$ dans $\mathbb{F}_{13^3}$. Son degré est égal à $h(\mathcal{O}_K) = 6$.

Dans le script MAGMA ci-dessous, on détermine une courbe E ayant j_1 comme j-invariant. En prenant un point au hasard on a $2110 \cdot P = [0 : 1 : 0]$ tandis que $2286 \cdot P \neq [0 : 1 : 0]$. C'est donc la courbe qu'on cherche (pas besoin de prendre sa tordue quadratique).

```
> q := 13^3; k<u> := GF(q);
> Pol<x> := PolynomialRing(k);
> N := 2110;
> a := q+1-N; a;
88
> Delta := a^2-4*q;
> d, r := SquareFree(Delta); d, r;
-29 6
> K := QuadraticField(d); O<w> := MaximalOrder(K);
> H := ChangeRing(HilbertClassPolynomial(Discriminant(O)), k); H;
x^6 + 9*x^5 + 3*x^4 + 6*x^3 + 5*x^2 + 10*x + 12
> j := Roots(H)[1][1];
> E := EllipticCurve([3*j/(1728-j), 2*j/(1728-j)]);
> P := Random(E); P;
(u^1014 : u^1984 : 1)
> (q+1-a)*P eq Zero(E), (q+1+a)*P eq Zero(E);
true false
```

■

6.2 Algorithme de Schoof

Soit $E/\mathbb{F}_q$ une courbe elliptique. On suppose que $q = p^s$ avec $p \neq 2, 3$ ce qui nous permet de supposer que E à un modèle de Weierstrass de la forme $E : y^2 = x^3 + Ax + B = f(x)$. On souhaite déterminer son nombre de points $N = \#E(\mathbb{F}_q) = q + 1 - a$ ou de façon équivalente sa trace a.

L'idée de l'algorithme est la suivante.

— Choisir un ensemble S de nombres premiers distincts de p tels que $\prod_{\ell\in S}\ell > 4\sqrt{q}$. En pratique on prend les plus petits nombres premiers possibles, $S=\{2,3,\dots,L\}$.
— Pour chaque $\ell\in S$, calculer $a_\ell = a \bmod \ell$.
— En déduire $a \bmod \prod_{\ell\in S}\ell$ par le théorème chinois.
— Conclure grâce à la borne de Hasse. En effet, si on connaît $a \bmod \prod \ell$ alors on peut en choisir un représentant a égal à la trace de E, qui satisfait

$$-2\sqrt{q} < -\frac{1}{2}\prod \ell \le a < \frac{1}{2}\prod \ell < 2\sqrt{q}.$$

Cas $\ell = 2$: Comme $a_2 = 0$ si et seulement si $\#E(\mathbb{F}_q) = 0 \bmod 2$, la question est donc de déterminer les points d'ordre 2 de E. On rappelle qu'un point affine $P=(x,y)$ a pour opposé $-P=(x,-y)$. Il est donc d'ordre 2 si et seulement si $P=-P$, *i.e.* $y=-y=0$. Ceci impose à x de vérifier la relation $f(x)=y^2=0$.
Un moyen rapide de déterminer l'existence de points rationnels d'ordre 2 est donc de vérifier si f admet une racine. Les racines de x^q-x dans $\bar{\mathbb{F}}_q$ sont exactement les éléments de $\mathbb{F}_q$. Si x^q-x et $f(x)$ ont un pgcd non constant, ça signifie donc qu'ils ont une racine commune dans $\bar{\mathbb{F}}_q$ et donc dans $\mathbb{F}_q$.
On en conclut que

$$a_2 = a \bmod 2 = \begin{cases} 0 \text{ si } \deg\left(\operatorname{pgcd}\left(x^q-x, x^3+Ax+B\right)\right) > 0 \\ 1 \text{ sinon.} \end{cases}$$

Cas ℓ impair : Lorsque ℓ est impair, l'idée est d'utiliser la relation $\pi^2 - a\pi + q = 0$, où $\pi(x,y)=(x^q,y^q)$ est le morphisme de Frobenius de E, en l'appliquant à des points de ℓ-torsion de E. Si on considère $P=(x,y)\in E[\ell]$, alors on a

$$\pi^2(P) - [a \bmod \ell]\pi(P) + [q \bmod \ell]P = \left(x^{q^2}, y^{q^2}\right) - [a_\ell]\,(x^q,y^q) + [q_\ell](x,y) = O_E$$

avec $q = q_\ell \bmod \ell$, $|q_\ell| < \frac{\ell}{2}$. Ce qui donne de façon équivalente,

$$[a_\ell]\,(x^q,y^q) = (x^{q^2},y^{q^2}) + [q_\ell](x,y)\,. \tag{6.4}$$

Ceci provient du fait que puisque π est un morphisme injectif (et donc l'image d'un point d'ordre ℓ est aussi d'ordre ℓ).

À partir de là, on obtient un premier algorithme, l'algorithme 2.

Rq Quelques précisions sur l'algorithme.
— Tel qu'il est écrit, la majeure partie du temps est passée à l'étape 5. Calculer une extension qui contient une racine de ψ_ℓ nécessite de factoriser ce polynôme. Mais pour un polynôme de degré $\deg\psi_\ell = (\ell^2-1)/2$, cela peut devenir très vite difficile, typiquement à partir de $\ell \ge 23$.
— Dans l'étape 10, on ne calcule pas les points $j\cdot P$ et $-j\cdot P$ séparément ; on se rappelle que $-(x,y)=(x,-y)$ donc une fois qu'on a $j\cdot P=(x_j,y_j)$ on a alors $-j\cdot P=(x_j,-y_j)$.

L'idée principale pour améliorer l'algorithme est de faire les calculs dans l'anneau des polynômes $\mathbb{F}_q[x,y] = \mathbb{F}_q[X,Y]/\langle Y^2-f(X),\ \psi_\ell(X)\rangle$, ou plutôt dans son « corps des fractions [3] ». En effet, on remarque qu'on a l'équivalence

$$P\in E[\ell] \in \bar{\mathbb{F}}_q^2 \Leftrightarrow \begin{cases} y^2 = f(x) & (\textit{ i.e., } P \text{ est dans } E), \\ \psi_\ell(x) = 0 & (\textit{ i.e. } P\in E[\ell]). \end{cases} \tag{6.5}$$

3. Lorsque ψ_ℓ n'est pas irréductible, cet anneau n'est pas intègre et donc n'a pas vraiment de corps des fractions. Mais on va faire comme s'il n'y avait aucun problème, on revient sur ce détail plus tard.

Algorithme 2 : Algorithme de Schoof (avec ℓ-torsion

Input : Une courbe elliptique $E\colon y^2 = f(x)$ sur $\mathbb{F}_q$ de caractéristique $p \neq 2, 3$.
Output : Le nombre de points rationnels N de E.

Déterminer un ensemble S de premiers $\ell \neq p$ tels que $\prod_{\ell \in S} \ell > 4\sqrt{q}$;
Si $\operatorname{pgcd}(f(x), x^q - x) \neq 1$ alors poser $a_2 = 0$ sinon $a_2 = 1$;
for $\ell \in S \setminus \{2\}$ **do**
  Calculer q_ℓ tel que $q_\ell = q \bmod \ell$ et $|q_\ell| < \ell/2$;
  Trouver une racine x de ψ_ℓ dans $\bar{\mathbb{F}}_q$;
  Déterminer une racine y de $f(x)$ dans $\bar{\mathbb{F}}_q$;
  Poser $P = (x, y) \in E[\ell]$;
  Poser $P' = P^{q^2} + [q_\ell] \cdot P = \left(x^{q^2}, y^{q^2}\right) + [q_\ell] \cdot (x, y)$;
  Poser $j = 0$;
  while $j \cdot P \neq P'$ *ou* $-j \cdot P \neq P'$ **do**
    Poser $j = j + 1$;
  Poser $a_\ell = j$;
Renvoyer l'unique entier a tel que $-2\sqrt{q} \leq a \leq 2\sqrt{q}$ et $a_\ell = a \bmod \ell$ pour tout $\ell \in S$.

On ne manipule donc plus vraiment des points (x, y) de $E(\bar{\mathbb{F}}_q)$, mais bien des polynômes ou des fractions rationnelles de polynômes soumis à des relations.

On rappelle que l'isogénie $[j]_E\colon E \to E$ de multiplication scalaire par j s'écrit

$$[j]P = \underbrace{P + \cdots + P}_{j \text{ fois}} = \left(\frac{\phi_j(P)}{\psi_j(P)^2}, \frac{\omega_j(P)}{\psi_j(P)^3}\right). \tag{6.6}$$

où ψ_j est le polynôme de j-division de E, $\phi_j \in \mathbb{F}_q[x]$ et $\omega_j \in y\mathbb{F}_q[x]$ (*cf.* paragraphe 2.5.1). On a maintenant tous les outils en main pour expliquer comment calculer efficacement a_ℓ à partir de la relation (6.4).

On commence par poser $P' = (x', y') = (x^{q^2}, y^{q^2}) + [q_\ell(x, y)] \bmod \langle \psi_\ell,\ y^2 - f(x) \rangle$, en fonction de x et de y. Ceci revient à calculer $x^{q^2} \bmod \psi_\ell$, puis à écrire $y^{q^2} = \left(y^2\right)^{\frac{q^2-1}{2}} y = f(x)^{\frac{q^2-1}{2}} y$ et à calculer $f(x)^{\frac{q^2-1}{2}} \bmod \psi_\ell$. On pose aussi pour tout $j \in \mathbb{N}^*$ la notation

$$[j](x, y) = (x_j, y_j) = \left(\frac{\phi_j(x)}{\psi_j(x)^2}, \frac{\omega_j(x, y)}{\psi_j(x)^3}\right) = (r_{1,j}(x), r_{2,j}(x)y).$$

Pour calculer la somme $(x^{q^2}, y^{q^2}) + [q_\ell](x, y)$, on peut utiliser les formules d'addition de la courbe modulo le système (6.5). En général, $\left(x^{q^2}, y^{q^2}\right) \neq \pm[q_\ell](x, y)$ et on peut utiliser les formules de de la somme de deux points, ce qui revient à

$$x' = \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}}\right)^2 - x^{q^2} - x_{q_\ell} = \left(\frac{y^{q^2} - r_{2,q_\ell}(x)y}{x^{q^2} - r_{1,q_\ell}(x)}\right)^2 - x^{q^2} - r_{1,q_\ell}(x),$$

et

$$\left(y^{q^2} - y_{q_\ell}\right)^2 = y^2 \cdot \left(y^{q^2-1} - r_{2,q_\ell}(x)\right)^2 = f(x)\left(f(x)^{\frac{q^2-1}{2}} - r_{2,q_\ell}(x)\right)^2.$$

Ainsi, on a pu exprimer x' comme une fraction rationnelle de x. On veut désormais déterminer j tel que $(x', y') = (x_j^q, y_j^q)$. Pour cela on commence calcule successivement x_j^q, la coordonnée en x de $[j](x^q, y^q)$, et on la compare avec x'. Si on trouve un tel j alors on a

$$(x', y') = \pm(x_j^q, y_j^q) = (x_j^q, \pm y_j^q).$$

Pour déterminer le signe il suffit alors de calculer $(y' - y_j^q)/y \bmod \psi_\ell$ (qui est une fraction rationnelle en x). Si le résultat est 0 alors le signe est $+$ et donc $j\,(x^q, y^q) = (x', y') = (x^{q^2}, y^{q^2}) + q_\ell(x,y)$, *i.e.* $a_\ell = j$. Sinon $a_\ell = -j$.

Sinon,

— soit $(x^{q^2}, y^{q^2}) = [q_\ell](x,y)$ et (x', y') s'obtient avec les formules de doublement de points plutôt que de somme (ou bien comme $[2q_\ell](x,y)$) ;
— soit $(x^{q^2}, y^{q^2}) = -[q_\ell](x,y)$, et P' est le point à l'infini, et on en déduit $a = 0 \bmod \ell$.

Tous mis bout à bout, on arrive à l'algorithme 3.

Algorithme 3 : Algorithme de Schoof

Input : Une courbe elliptique E sur un corps $\mathbb{F}_q$ de caractéristique $p \neq 2, 3$
Output : $\#E(\mathbb{F}_q)$

Déterminer un ensemble S de nombres premiers $\ell \neq p$ tel que $\prod_{\ell \in S} \ell > 4\sqrt{q}$;
Si $\operatorname{pgcd}(f(x), x^q - x) \neq 1$ alors poser $a_2 = 0$ sinon $a_2 = 1$;
for $\ell \in S$ **do**
    Poser $q_\ell = q \bmod \ell$ avec $|q_\ell| < \ell/2$;
    Calculer $P' = (x^{q^2}, y^{q^2}) + [q_\ell](x,y) \bmod \langle \psi_\ell, y^2 - f(x) \rangle$;
    Si $P' \neq O_E$ alors poser $(x', y') = P'$ sinon $a_\ell = 0$ et continuer en 3;
    for $j = 1, \ldots, (\ell - 1)/2$ **do**
        Calculer la coordonnée en x de $(x_j, y_j) = [j](x,y)$;
        if $x' - x_j^q = 0 \bmod \psi_\ell$ **then**
            Calculer y_j;
            Si $(y' - y_j^q)/y = 0 \bmod \psi_\ell$ alors $a_\ell = j$. Sinon $a_\ell = -j$;
Calculer l'unique a tel que $a_\ell = a \bmod \ell$ et $|a| \leq 2\sqrt{q}$;
Renvoyer $q + 1 - a$;

Rq Comme on effectue ces calculs dans un anneau, celui défini par le système (6.5), on peut rencontrer des dénominateurs non inversibles. Lorsque cela se produit, on a en retour un facteur $g(x)$ de $\psi_\ell(x)$. Il est intéressant de noter que chaque fois que cela se produit, le degré de g est presque toujours de degré $(\ell - 1)/2$, une conséquence de la structure $(\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})$ des points de ℓ-torsion.

Quand c'est le cas, il suffit de reprendre l'algorithme avec ce facteur g plutôt que ψ_ℓ. C'est alors plutôt une chance, car l'algorithme s'accélère alors d'un facteur ℓ au moins : nous pouvons travailler modulo un polynôme de degré $(\ell - 1)/2$ plutôt que $(\ell^2 - 1)/2$.

6.3 Volcans d'isogénies

Soit k un corps et ℓ un nombre premier. On rappelle que, d'après le théorème 5.26, pour ℓ premier à la caractéristique du corps k, le polynôme modulaire $\Phi_\ell(X,Y)$ satisfait $\phi_\ell(j_1, j_2) = 0$ si et seulement si j_1 et j_2 sont les j-invariants de courbes elliptiques définie sur k telles qu'il existe une isogénie $E_1 \to E_2$ définie sur k.

Si on fixe une courbe elliptique E de j-invariant j sur k et qu'on considère le polynôme $\phi_\ell(j, Y) \in k[Y]$ alors ses racines dans k correspondent aux j-invariants des courbes E' définies sur k reliées à E par une isogénie de degré ℓ. Il existe donc, à isomorphisme près, un nombre fini de telles courbes. C'est pour cela qu'on ne va travailler qu'à isomorphisme près dans cette section. On dit que deux isogénies $\varphi_1 \colon E_1 \longrightarrow E_1'$ et $\varphi_2 \colon E_2 \longrightarrow E_2'$ sont *isomorphes* s'il existe des isomorphismes, *i.e.* des isogénies de degré 1, $\alpha \colon E_1 \to E_2$ et

$\alpha' : E_1' \to E_2'$ tels que le diagramme suivant commute,

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi_1} & E_1' \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha'} \\ E_2 & \xrightarrow{\varphi_2} & E_2' . \end{array}$$

Par exemple une isogénie $\varphi : E \to E'$ est isomorphe à $-\varphi$ car il s'agit de la composition de φ avec $[-1]_{E'}$ qui est un isomorphisme.

Proposition 6.8 — Formules de Vélu. Soit E une courbe elliptique définie sur un corps k et $G \subseteq E(\bar{k})$ un sous groupe fini. Alors, il existe une courbe elliptique [a] E' et une isogénie séparable $E \to E'$ de noyau exactement G.

a. Attention, E' n'est *a priori* pas définie sur k. Si G est stable par l'action de $\mathrm{Gal}\left(\bar{k}/k\right) = \left\{\sigma : \bar{k} \to \bar{k}, \forall x \in k, \sigma(x) = x\right\}$ (*i.e.* $\forall \sigma \in \mathrm{Gal}\left(\bar{k}/k\right)$, on a $\forall P \in G$, $P^\sigma \in G$), alors E' peut être choisie à coefficients dans k.

Rq La proposition s'appelle "formules de Vélu" même si aucune formules n'apparaît. Dans l'énoncé original, Vélu donne des formules explicites pour l'isogénie et la courbe E' en fonction des points de G. Les formules sont assez longues à énoncer et nous n'en n'aurons pas besoin (voir [Was08, Theorem 12.16]).

Corollaire 6.9 Soit E une courbe elliptique ordinaire sur un corps k et ℓ un nombre premier différent de la caractéristique p de k. On suppose que $j(E) \neq 0, 1728$. Alors il existe, à isomorphisme près, $\ell+1$ isogénies de degré ℓ partant de E.

On dit qu'une isogénie de degré ℓ est une *ℓ-isogénie*.

Démonstration. On commence par un constat simple. Si G est un sous groupe de E d'ordre ℓ alors $\forall P \in G$, $\ell \cdot P = O$. Donc $G \subseteq E[\ell]$.

On rappelle que $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ car $\ell \neq p$. Il suffit alors, d'après les formules de Vélu, de compter les sous-groupes de cardinal ℓ de $(\mathbb{Z}/\ell\mathbb{Z})^2$. Chaque élément non trivial de $(\mathbb{Z}/\ell\mathbb{Z})^2$ est d'ordre ℓ donc engendre un sous-groupe d'ordre ℓ. On peut prendre les éléments de la forme $(a,1)$ pour $a \in \mathbb{Z}/\ell\mathbb{Z}$ qui donnent ℓ sous-groupes distinctes et $(1,0)$ engendre un $\ell+1$-ème sous-groupe. Il n'y en a pas d'autres car si (a',b') engendre un sous groupe d'ordre ℓ alors si $b' \neq 0$, $(a'b'^{-1},1)$ est un générateur déjà cité, sinon $(a',0)a'^{-1} = (1,0)$.

On en déduit que $E[\ell]$ a exactement $\ell+1$ sous-groupes G qui engendrent chacun une isogénie de noyau G. Il reste à déterminer si certaines de ces isogénies sont isomorphes. Puisque E est supposée ordinaire, l'anneau $\mathrm{End}(E) = R$ est un ordre dans un corps quadratique imaginaire. Puisque que $j(E) \neq 0, 1728$, on a de plus $R \neq \mathbb{Z}[i]$ et $R \neq \mathbb{Z}\left[(1+\sqrt{-3})/2\right]$. Donc les inversibles de R, *i.e.* les automorphismes de E, sont uniquement $\{\pm 1\}$.

Or, tout sous-groupe G de $E[\ell]$ est stable par multiplication par -1. Donc toutes les isogénies induites par les sous-groupes d'ordre ℓ de $E[\ell]$ ont des noyaux non-isomorphes. Elles sont donc distinctes à isomorphisme près. ■

Définition 6.10 — Graphe des ℓ-isogénies. Soit k un corps et ℓ un nombre premier. On pose $G_\ell(k)$ *le graphe des ℓ-isogénie de k* dont les sommets sont les éléments de k et deux sommets j_1 et j_2 sont reliés par une arête si $\Phi_\ell(j_1, j_2) = 0$. La multiplicité de l'arête est la multiplicité de j_2 comme racine du polynôme $\Phi(j_1, Y) \in k[Y]$.

On rappelle que le degré d'un sommet v est le nombre d'arêtes partant de v comptées avec multiplicités.

Définition 6.11 — ℓ-volcan. Un *ℓ-volcan* est un graphe connexe dont les sommets sont partitionnés en niveaux V_0, V_1,...,V_{pr} tels que :
- le sous-graphe V_0, appelé le *cratère* ou la *surface* du volcan, est un graphe de degré au plus 2 ;
- pour tout $i>0$ tout sommet de V_i à un unique voisin dans V_{i-1} ;
- pour tout $i<\mathrm{pr}$ tout sommet est de degré $\ell+1$.

Le sous-graphe V_{pr} est appelé le *sol* du volcan et l'entier pr est appelé la *profondeur* du volcan.

Rq Attention, le fait que deux isogénies partant de E soient distinctes à isomorphisme près ne signifie pas que les courbes d'arrivée ne sont pas isomorphes. On peut très bien avoir deux isogénies non-isomorphes $\varphi_i\colon E\to E'$, avec des noyaux de même cardinaux ℓ.

■ **Exemple 6.12** Si on considère E une courbe elliptique à multiplication complexe par l'ordre maximal $\mathcal{O}_K=\mathbb{Z}[\omega]$ avec $\omega=(1+\sqrt{-15})/2$ et qu'on considère $\mathfrak{a}=\langle 2,1+\omega\rangle$ qui est un générateur de $\mathrm{Cl}(\mathcal{O}_K)$.

On a $\bar{\mathfrak{a}}\neq\mathfrak{a}$, mais $[\bar{\mathfrak{a}}]=[\mathfrak{a}]$ car $h(\mathcal{O}_K)=2$. On considère $E[\mathfrak{a}]=\ker[2]\cap\ker(1+\omega)$ de cardinal 2, ainsi que $E[\bar{\mathfrak{a}}]$, de cardinal 2 aussi. Puisque $\bar{\mathfrak{a}}$ et $\mathfrak{a}$ sont dans la même classe $E/E[\mathfrak{a}]$ et $E/E[\bar{\mathfrak{a}}]$, sont isomorphes.

Pourtant on peut montrer que les deux noyaux sont d'intersection nulle. En effet, si $P\in E[\mathfrak{a}]\cap E[\bar{\mathfrak{a}}]$ alors $(1+\omega)P=O$ et $(1+\bar{\omega})P=O$ donc $\mathrm{Tr}(1+\omega)P=3P=O$ mais $2P=O$ donc $3P-2P=P=O$. ■

On pose $\mathrm{End}^0(E)=\mathrm{End}(E)\otimes\mathbb{Q}$. Lorsque E est à multiplication complexe par un ordre quadratique, $\mathrm{End}^0(E)$ est un corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$. C'est, dans ce cas, le corps des fractions de $\mathrm{End}(E)$.

Théorème 6.13 Soit $\varphi\colon E\to E'$ une ℓ-isogénie entre courbes elliptiques à multiplication complexe définie sur un corps k. Alors $\mathrm{End}^0(E)\simeq\mathrm{End}^0(E')$ (*i.e.* elles sont à CM dans un même corps quadratique imaginaire).
Et, en notant $R=\mathrm{End}(E)$ et $R'=\mathrm{End}(E')$, on a une des trois possibilités.
1. $R=R'$
2. $[R\colon R']=\ell$
3. $[R'\colon R]=\ell$

Dans le premier cas on dit que φ est une isogénie *horizontale* et qu'elle est *verticale* dans les deux derniers. Dans le troisième cas on dit que l'isogénie est *descendante* et dans le dernier on dit qu'elle est *montante*.

Démonstration. On considère $\alpha\in R$ et $\widehat{\varphi}\colon E'\to E$ l'isogénie duale de φ (donc $\varphi\circ\widehat{\varphi}=[\ell]_{E'}$ et $\widehat{\varphi}\circ\varphi=[\ell]_E$). On considère $\beta=\varphi\circ\alpha\circ\widehat{\varphi}\in R'$. On a

$$\mathrm{Tr}(\beta)=\beta+\widehat{\beta}=\varphi\circ\alpha\circ\widehat{\varphi}+\varphi\circ\widehat{\alpha}\circ\widehat{\varphi}=\varphi\circ(\alpha+\widehat{\alpha})\circ\widehat{\varphi}=\ell\,\mathrm{Tr}(\alpha)$$
$$N(\beta)=\beta\circ\widehat{\beta}=\varphi\circ\alpha\circ\widehat{\varphi}\circ\varphi\circ\widehat{\alpha}\circ\widehat{\varphi}=\varphi\circ\alpha\circ\ell\circ\widehat{\alpha}\circ\widehat{\varphi}=\varphi\circ\ell N(\alpha)\circ\widehat{\varphi}=\ell^2N(\alpha).$$

On en déduit que β est annulé par $X^2-\mathrm{Tr}(\beta)X+N(\beta)=X^2-\ell\,\mathrm{Tr}(\alpha)X+\ell^2N(\alpha)\in\mathbb{Z}[X]$. Donc $\beta/\ell\in\mathrm{End}^0(E')$. On en déduit que $\mathrm{End}^0(E)\subseteq\mathrm{End}^0(E')$. Le même raisonnement dans l'autre sens donne l'autre inclusion. Donc $\mathrm{End}^0(E)=\mathrm{End}^0(E')$.

Si on pose $R=\mathbb{Z}[\omega]$ et $R'=\mathbb{Z}[\omega']$, on a $\varphi\circ\omega\circ\widehat{\varphi}=\ell\omega$. C'est donc un élément de R'. Et de même, on $\ell\omega'\in R$. Donc $\mathbb{Z}[\ell\omega]\subseteq\mathbb{Z}[\omega']$ et $\mathbb{Z}[\ell\omega']\subseteq\mathbb{Z}[\omega]$ d'où la suite d'inclusions $\mathbb{Z}[\ell^2\omega]\subseteq\mathbb{Z}[\ell\omega']\subseteq\mathbb{Z}[\omega]$. Puisque $[\mathbb{Z}[\omega]\colon\mathbb{Z}[\ell^2\omega]=\ell^2$, l'indice de $\mathbb{Z}[\ell\omega']$ dans $\mathbb{Z}[\omega]$ est
- soit 1, auquel cas on a $R=\mathbb{Z}[\ell\omega']$, *i.e.* $[R'\colon R]=\ell$,
- soit ℓ, auquel cas on a $R=\mathbb{Z}[\omega']$, *i.e.* $R=R'$,
- soit ℓ^2, et finalement $R'=\mathbb{Z}[\ell\omega]$.

■

On pose $\mathrm{Ell}_R(k)$ l'ensemble des classes de $\bar{k}$-isomorphismes de courbes elliptiques définies sur k avec multiplication complexe par R.

Théorème 6.14 Soit k un corps fini et ℓ un nombre premier différent de la caractéristique p de k. Soit E une courbe elliptique à multiplication complexe par un ordre $R=\mathbb{Z}[\omega]$ dans un corps quadratique K. On note f le conducteur de R dans $\mathcal{O}_K$.
Alors, si $\mathrm{Ell}_{\mathbb{Z}[\ell\omega]}(k)\neq\emptyset$,

— si $\ell\nmid f$, il y a $1+\left(\frac{\Delta}{\ell}\right)$ ℓ-isogénies horizontales, $\ell-\left(\frac{\Delta}{\ell}\right)$ isogénies descendantes et aucune montante partant de E ;
— sinon, il n'y a aucune ℓ-isogénie horizontale, il y en a ℓ descendantes et une montante partant de E.

Si $\mathrm{Ell}_{\mathbb{Z}[\ell\omega]}(k)=\emptyset$, alors il n'y a pas d'isogénies descendantes.

Idées de la preuve dans $\mathbb{C}$. On peut supposer que $E(\mathbb{C})\simeq\mathbb{C}/\Lambda$ avec $\mathrm{End}(\Lambda)=R$ par le théorème d'uniformisation. Puisque E est à multiplication complexe, Λ est homothétique à un réseau de la forme $\mathfrak{a}$ avec $\mathfrak{a}$ un idéal inversible de R. On commence par le cas particulier où $\mathfrak{a}=R$. On remarque tout d'abord que les sous-groupes de $X=\mathbb{C}/R$ de cardinal ℓ correspondent exactement aux sous-réseaux $\mathfrak{m}$ de R d'indice ℓ. De plus les sous-réseaux $\mathfrak{m}$ de R d'indice ℓ sont les sur-réseaux de ℓR dans lequel ℓR est d'indice ℓ par la formule

$$[R\colon \ell R]=[R\colon \mathfrak{m}]\cdot[\mathfrak{m}\colon \ell R].$$

Ainsi, un sous-réseau $\mathfrak{m}$ de R d'indice ℓ induit une ℓ-isogénie $\mathbb{C}/R\simeq\mathbb{C}/\ell R\to\mathbb{C}/\mathfrak{m}$ par l'inclusion $\ell R\subseteq\mathfrak{m}$. Ces sous-réseaux s'écrivent $\mathfrak{m}=\langle n,a+m\omega\rangle_{\mathbb{Z}}$ et sont d'indice $nm=\ell$ dans R. On voit facilement que ces réseaux sont donc

$$\mathfrak{m}_i=\langle \ell, i+\omega\rangle,\ 0\leq i\leq \ell-1 \text{ et } \langle 1,\ell\omega\rangle=\mathbb{Z}[\ell\omega].$$

Chacun de ces sous-réseaux $\mathfrak{m}$ engendre une isogénie $\mathbb{C}/R\to\mathbb{C}/\mathfrak{m}$ de degré $[R\colon\mathfrak{m}]=\ell$.

On remarque tout d'abord que l'isogénie correspondant à $\mathfrak{m}=\mathbb{Z}[\ell\omega]$ est une isogénie descendante car $\mathrm{End}(\mathbb{C}/\mathbb{Z}[\ell\omega])=\mathbb{Z}[\ell\omega]$.

Maintenant considérons le cas $\ell\nmid f$. Si Δ est un carré modulo ℓ, alors ℓ se décompose complètement dans R en un produit de deux idéaux inversibles, $\mathfrak{p}=\langle\ell,a+\omega\rangle$ et $\bar{\mathfrak{p}}$. Puisque ces idéaux sont inversibles on a $\mathrm{End}(\mathbb{C}/\mathfrak{p})=(\mathfrak{p}\colon\mathfrak{p})=R_{\mathfrak{p}}=R$ et pareil pour $\bar{\mathfrak{p}}$. Ceci nous donne donc deux isogénies horizontales.

Enfin, considérons $\mathfrak{m}_j\in\{\mathfrak{m}_i, 0\leq i\leq\ell-1\}\setminus\{\mathfrak{p},\bar{\mathfrak{p}}\}$. On voit qu'ils ne sont pas de norme ℓ (seuls $\mathfrak{p}$ et $\bar{\mathfrak{p}}$ le sont). Ce ne sont donc pas des idéaux de R, et en particulier $\ell\nmid N(j+\omega)$. Cherchons le plus grand sous-ordre S de R dans lequel $\mathfrak{m}_j$ est un S-idéal fractionnaire. On peut écrire $S=\mathbb{Z}[g\omega]=\mathbb{Z}[\omega']$ et on a $\mathfrak{m}_j=(1/g)\langle g\ell, gj+g\omega\rangle=(1/g)\langle g\ell, gj+\omega'\rangle$. On a

$$g\ell\,|\,N(g\ell+\omega')=g^2N(\ell+\omega')\ \Leftrightarrow\ \ell\,|\,g$$

puisque ℓ premier avec $N(\ell+\omega')$. On remarque donc que $S=\mathbb{Z}[\ell\omega]$ est le plus grand sous-ordre de R dans lequel $\mathfrak{m}_j$ est un idéal fractionnaire. Donc $(\mathfrak{m}_j\colon\mathfrak{m}_j)=S$ et les $\mathfrak{m}_j$ sont des idéaux fractionnaires inversibles de S donc $\mathrm{End}(\mathbb{C}/\mathfrak{m}_j)=S$: on a $\ell-1$ isogénies descendantes. ■

On énonce le théorème principal des volcans d'isogénies démontré par D. Kohel [Koh96].

Théorème 6.15 — Kohel. Soit $\mathbb{F}_q$ un corps fini, un nombre premier ℓ, premier avec q. On considère V une composante connexe de $G_\ell(\mathbb{F}_q)$ qui ne contient pas les j-invariants 0 ou 1728. Alors V est un ℓ-volcan tel qu'on ait les propriétés suivantes.

1. Les sommets de V_i sont les j-invariants de courbes elliptiques à CM par un même ordre R_i.
2. Les sommets du sous-graphe V_0 sont de degré $1+\left(\frac{\Delta_0}{\ell}\right)$, avec Δ_0 le discriminant de R_0.
3. Si $\left(\frac{\Delta_0}{\ell}\right) \geq 0$, alors R_0 admet un idéal $\mathfrak{p}$ de norme ℓ. et $|V_0| = \mathrm{ord}[\mathfrak{p}]$ (l'ordre de la classe de $\mathfrak{p}$ dans $\mathrm{Cl}(R_0)$). Sinon $|V_0| = 1$.
4. La profondeur de V est l'entier positif pr qui satisfait $4q = a^2 - \ell^{2\,\mathrm{pr}} g^2 \Delta_0$ avec $\ell \nmid g$ et $a^2 = \mathrm{Tr}(\pi_E)$, où E est n'importe quelle courbe telle que $j(E) \in V$. En d'autres termes, pr est la valuation ℓ-adique du conducteur de l'ordre $\mathbb{Z}[\pi_E]$.
5. On a $\ell \nmid [\mathcal{O}_K : R_0]$ et $\ell = [R_i : R_{i-1}]$.

■ **Exemple 6.16** On considère la courbe $E: y^2 = x^3 + 25x + 25$ sur $\mathbb{F}_{89}$. Elle a 96 points rationnels. Donc sa trace est $a = 89 + 1 - 96 = -6$ et le discriminant de l'ordre $\mathbb{Z}[\pi]$ engendré par son Frobenius est

$$\Delta_\pi = (-6)^2 - 4 \times 89 = -320 = \underbrace{4^2}_{f^2} \times \underbrace{-20}_{\Delta_K}.$$

$\mathbb{Z}[\pi]$ correspond à un ordre de conducteur $f = 4$ dans $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[\omega]$. On pose $\mathrm{End}(E) = R = \mathbb{Z}[\omega']$. Puisque $\mathbb{Z}[\pi] \subseteq R \subseteq \mathcal{O}_K$ alors R est soit $\mathbb{Z}[\pi] = \mathbb{Z}[4\omega]$ (conducteur 4 dans $\mathcal{O}_K$), soit $\mathbb{Z}[2\omega]$ (conducteur 2), soit $\mathcal{O}_K$.

On considère le polynôme modulaire Φ_2 dans $\mathbb{F}_{89}[X,Y]$. Il s'agit du polynôme

$$\Phi_2(X,Y) = X^3 - X^2Y^2 + 64X^2Y + 69X^2 + 64XY^2 + 72XY + 74X + Y^3 + 69Y^2 + 74Y + 63.$$

Pour déterminer les courbes E' sur $\mathbb{F}_{89}$ telles qu'il existe une 2-isogénie de E vers E', on calcule $j(E) = -1$ et $\rho_{-1}(Y) = \Phi_2(-1,Y) = Y^3 + 4Y^2 + 66Y + 57$. Les racines du polynôme ρ_{-1} dans $\mathbb{F}_{89}$ sont les j-invariants des courbes E' définies sur $\mathbb{F}_{89}$ qui sont 2-isogènes à E. La factorisation en irréductibles de ρ_{-1} est

$$\rho_{-1}(Y) = (Y - 54)(Y^2 + 58Y + 83).$$

On en déduit que E admet une unique 2-isogénie (à isomorphisme près), vers une courbe E' de j-invariant 54. On en déduit que E n'admet aucune isogénie descendante sinon il y aurait au total 2 isogénies descendantes partant de E (qui correspondraient à 2 racines de ρ_{-1}). C'est donc qu'il n'existe pas de courbe elliptique avec anneau d'endomorphismes $\mathbb{Z}[2\omega']$. On a donc $R = \mathbb{Z}[\pi]$, R est déjà l'ordre minimal. On en déduit aussi que la 2-isogénie est montante. En d'autres termes, $j(E) = -1$ se situe sur le sol du volcan.

Une courbe E', de j-invariant 54, est la courbe $E': y^2 = x^3 + 80x + 37$. Elle a pour anneau d'endomorphismes $R' = \mathbb{Z}[2\omega]$. On peut déjà affirmer, d'après le théorème 6.14, qu'il n'y a aucune 2-isogénie horizontale partant de E', qu'il y a 2 isogénies descendantes (dont une est la duale de l'isogénie montante de E vers E') et une isogénie montante. La factorisation de $\rho_{54}(Y) = \Phi_2(54,Y)$ est

$$\rho_{54} = \underbrace{(Y - (-1))}_{\text{isogénie descendante}} \underbrace{(Y - 83)\,(Y - 21)}_{?}$$

Donc une des courbes de j-invariant 21 ou 83 correspond à une courbe dont l'anneau des endomorphismes est $\mathcal{O}_K$ et l'autre est $\mathbb{Z}[\pi]$. On a maintenant

$$\rho_{83}(Y) = \Phi_2(83,Y) = (Y - 54)(Y^2 + 59Y + 59).$$

C'est donc le j-invariant de la courbe correspondant à l'autre isogénie descendante partant de E' (donc 83 est sur le sol). Et celle de j-invariant 21 a pour anneau d'endomorphismes $\mathcal{O}_K$, elle est donc sur le cratère du volcan. En continuant de factoriser $\Phi_2(j,Y)$ pour les j-invariants que l'on trouve successivement, on arrive au volcan suivant.

— Niveau 0 (cratère) : on a les j-invariants 21 et 1.
— Niveau 1 : on a les j-invariants 54 et 41 (sous 21) et 55 et 59 (sous 1).
— Niveau 2 (sol) : on a les j-invariants -1, 83, 80, 44, 9, 49, 30 et 50.

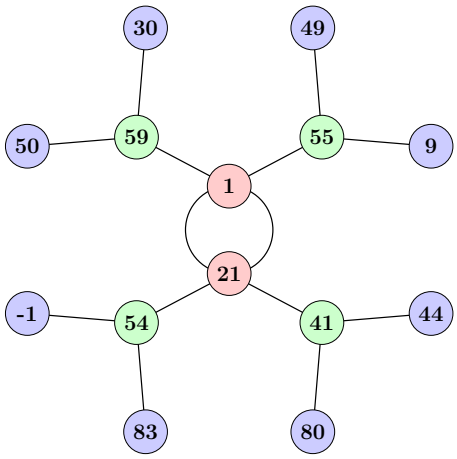


FIGURE 6.1 – Une composante connexe de $G_2(\mathbb{F}_{89})$

■

■ **Exemple 6.17** On considère $E\colon y^2 = x^3 + 157x + 214$ sur $\mathbb{F}_{223}$. La courbe E possède 225 points rationnels donc a pour trace $a = 223 + 1 - 225 = -1$ et le discriminant de l'ordre $\mathbb{Z}[\pi]$ engendré par le Frobenius est

$$a^2 - 4 \times 223 = -891 = \underbrace{9^2}_{f^2} \times \underbrace{-11}_{\Delta_K}.$$

Posons $\omega = (1+\sqrt{-11})/2$, l'ordre $R = \mathrm{End}(E)$ est donc $\mathbb{Z}[\omega]$, $\mathbb{Z}[3\omega]$, ou $\mathbb{Z}[9\omega] = \mathbb{Z}[\pi]$. Le j-invariant de E est 206.

On a $\rho_{206}(Y) = \Phi_3(206,\ Y) = Y^4 + 43Y^3 + 209Y^2 + 70Y + 182$ qui a pour racines 13, 25, 161 et 204. Puisque ρ_{206} n'a pas qu'une seule racine, E n'a pas pour anneau des endomorphismes $\mathbb{Z}[\pi]$. En revanche, on remarque que ρ_{25}, ρ_{161} et ρ_{204} admettent pour unique racine 206. Ces dernières correspondent à des isogénies montantes et les anneaux d'endomorphismes des courbes ayant ces j-invariants sont $\mathbb{Z}[\pi]$. En revanche, on a

$$\rho_{13}(Y) = \Phi_3(13,Y) = (Y-13)^2\,(Y-206)\,(Y-222).$$

La (classe d'isomorphisme de) courbe E' ayant pour j-invariant 13 correspond à la courbe ayant pour anneau des endomorphismes l'ordre maximal. On a deux 3-isogénies de $E \to E$ qui correspondent aux deux idéaux distincts $\langle 3,\omega\rangle$ et $\langle 3,\bar{\omega}\rangle$ d'où le facteur $(Y-13)^2$, une isogénie descendante vers E et une autre descendant vers la courbe de j-invariant $222 = -1$ aussi d'anneau d'endomorphismes $\mathbb{Z}[3\omega]$.

Enfin, on peut calculer

$$\rho_{222}(Y) = \Phi_3(222,Y) = Y^4 + 98Y^3 + 8Y^2 + 59Y + 206 = \underbrace{(Y-13)}_{\text{isogénie montante}} \times \underbrace{(Y-9)\,(Y-143)\,(Y-183)}_{\text{isogénies descendantes}}.$$

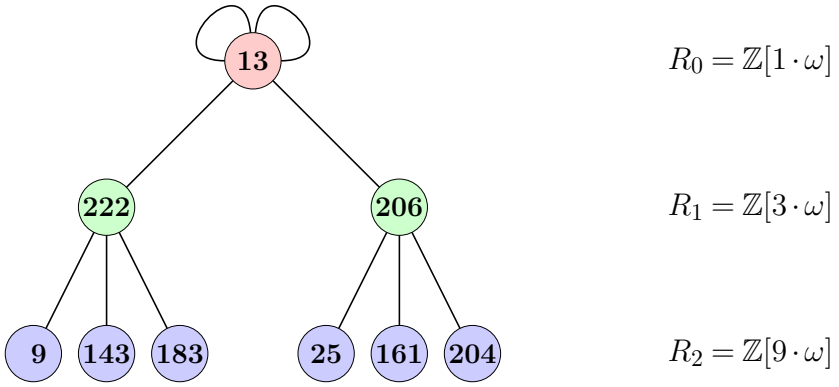


FIGURE 6.2 – Une composante connexe de $G_3(\mathbb{F}_{223})$.

```
> k := GF(223);
> E := EllipticCurve([k| 157, 214]);
> pol<X, Y> := PolynomialRing(k, 2);
> Pol<x> := PolynomialRing(k);
> Phi3 := pol!ClassicalModularPolynomial(3);
> Roots(Pol!Evaluate(Phi3, [jInvariant(E), x]));
[ <13, 1>, <25, 1>, <161, 1>, <204, 1> ]
> Roots(Pol!Evaluate(Phi3, [k!25, x]));
[ <206, 1> ]
> Roots(Pol!Evaluate(Phi3, [k!13, x]));
[ <13, 2>, <206, 1>, <222, 1> ]
> // etc...
```

■

Une application directe des volcans d'isogénie est le calcul de l'anneau des endormorphismes d'une courbe elliptique définie sur un corps fini (*cf.* l'algorithme 4).

Algorithme 4 : Endomorphismes d'une courbe elliptique sur $\mathbb{F}_q$.

Input : Une courbe elliptique E ordinaire sur un corps fini $\mathbb{F}_q$ de caractéristique p.
Output : Le discriminant de $\mathrm{End}(E)$.

1 Calculer $a = \mathrm{Tr}(E)$;
2 Vérifier que $a \neq 0 \bmod p$;
3 Calculer $\Delta_\pi = a^2 - 4q$ et $j = j(E)$;
4 En déduire le conducteur f du sous-ordre de $\mathcal{O}_K$ engendré par le Frobenius;
5 **for** $\ell \mid f$ **do**
6 Calculer $\Phi_\ell(X, Y) \bmod p$;
7 Parcourir le ℓ-volcan en partant de $j(E)$ jusqu'à trouver le sol;
8 En déduire la distance $\mathrm{pr}_{\ell,j}$ de j au sol du ℓ-volcan;
9 Renvoyer $\left(\prod_{\ell \mid f} \ell^{2\,\mathrm{pr}_{\ell,j}}\right) \cdot \Delta_K$;

Rq Il existe de nombreuses autres applications aux volcans d'isogénies parmi lesquelles (voir [Sut13a]) :

— calcul des polynômes de classe de Hilbert H_R ;
— calcul des polynômes modulaires Φ_ℓ(X, Y) ;
— détermination de la supersingularité d'une courbe elliptique ;
— calcul du nombre de points d'une courbe elliptique : dans l'algorihme SEA, il est nécessaire de calculer le polynôme $\Phi_\ell(j(E), Y)$. Le problème étant que le

calcul sur $\mathbb{Z}$ de $\Phi_\ell(X,Y)$ est terriblement coûteux pour ℓ grand. Dans [Sut13b, Algorithm 2], Sutherland explique comment éviter ce calcul en utilisant les volcans d'isogénies. Cette amélioration a, en particulier, permis le calcul d'un nouveau record du nombre de points d'une courbe elliptique. À savoir le calcul du nombre de points de $E\colon y^2 = x^3 + 2718281828x + 3141592653$ sur $\mathbb{F}_p$ avec $p = 6219299585 \cdot 2^{16612} - 1$ qui possède 5011 décimales.

6.4 Algorithme SEA

L'algorithme de Schoof a été publié pour la première fois en 1985 [Sch85]. Bien qu'à la base R. Schoof l'utilisait pour déterminer efficacement le calcul de racines carrées modulo p (ce n'était pas clair avec les connaissances de l'époque qu'il était meilleur que l'algorithme Baby-steps, Giant-steps utilisé alors), il s'est par la suite imposé notamment grâce aux amélioration apportées par Elkies puis Atkin.

6.4.1 Idée générale

On pose $E\colon y^2 = x^3 + Ax + B$ une courbe elliptique sur $\mathbb{F}_q$. Soit $\pi(x,y) = (x^q, y^q)$ son endomorphisme de Frobenius, et $a = \mathrm{Tr}(\pi)$ la trace de E. On souhaite, comme à la section 6.2, expliquer comment déterminer $a_\ell = a \bmod \ell$ de façon efficace.

La partie coûteuse de l'algorithme de Schoof concerne les calculs faits modulo $\psi_\ell(x)$ qui est de degré $(\ell^2-1)/2$ pour ℓ impair (le cas $\ell = 2$ ne pose aucune difficulté). Mais on remarque à la fin du paragraphe 6.2 qu'il peut arriver dans l'exécution de l'algorithme de Schoof que l'on retrouve un facteur de degré $(\ell-1)/2$ du polynôme $\psi_\ell(x)$. On peut alors ramener les calculs de l'algorithme de Schoof à un sous-groupe C de la torsion $E[\ell]$: on travaille dans $\mathrm{End}(C)$ au lieu de $\mathrm{End}(E[\ell])$.

Le groupe $E[\ell]$ étant d'ordre ℓ^2, ses sous-groupes sont d'ordre 0, ℓ ou ℓ^2. Puisqu'on veut travailler sur un sous-groupe strict C non trivial on s'intéresse donc aux sous-groupes d'ordre ℓ de $E[\ell]$. D'après les formules de Vélu, chaque sous-groupe C de $E[\ell]$ de cardinal ℓ est le noyau d'une ℓ-isogénie $\varphi\colon E \to E'$. Dans le cas où ce noyau est stable par l'action de π, le Frobenius de E, on peut choisir E' définie sur $\mathbb{F}_q$. Dans ce cas là, pour un point $P \in C \setminus \{O_E\}$, on a $\pi(P) \in C \setminus \{O_E\}$. Puisque C est d'ordre ℓ, tout élément non-nul est générateur. Il existe donc $\lambda \in \mathbb{Z}/\ell\mathbb{Z}$ tel que $\pi(P) = \lambda \cdot P$. De plus, puisque π est un morphisme de groupe, on a plus largement

$$\forall P \in C,\ \pi(P) = \lambda \cdot P. \tag{6.7}$$

En identifiant $E[\ell]$ à un $\mathbb{Z}/\ell\mathbb{Z}$-espace vectoriel de dimension 2, et en choisissant une $\mathbb{Z}/\ell\mathbb{Z}$-base de $E[\ell]$, on peut identifier $\pi_\ell = \pi_{|E[\ell]}$ à sa matrice dans cette base,

$$\pi_\ell = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

On a alors (voir [Was08, Proposition 4.11]),

$$\mathrm{Tr}(\pi_\ell) = a_\ell \quad \text{et} \quad \det(\pi_\ell) = \deg \pi \bmod \ell = q \bmod \ell. \tag{6.8}$$

Un élément $P \in C \setminus \{O\}$ tel que $\pi(P) = \lambda \cdot P$ peut se compléter en une base (P,Q) de $E[\ell]$ dans laquelle π_ℓ a pour matrice

$$\begin{pmatrix} \lambda & \gamma \\ 0 & \mu \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

D'après la relation (6.8), on a alors d'une part $a = \lambda + \mu \bmod \ell$ et d'autre part $q = \lambda\mu \bmod \ell$, donc $a = \lambda + q/\lambda \bmod \ell$.

Enfin, on pose $P_m = m \cdot P = (x_m, y_m) \in C$ et

$$g = \prod_{m=1}^{(\ell-1)/2} (X - x_m) \in \bar{\mathbb{F}}_q[X].$$

On a $\pi(P_m) = (x_m^q, y_m^q) = \lambda \cdot P_m = P_{\lambda m} = (x_{\lambda m}, y_{\lambda m})$. On remarque que le Frobenius permute les racines de g. En effet, si $m \in \{1, \ldots, (\ell-1)/2\}$, alors $x_m^q = x_{\lambda m}$ et si $\lambda m \in \left\{1, \ldots, \frac{\ell-1}{2}\right\}$, c'est gagné. Sinon $(\ell-1)/2 < \lambda m \leq \ell - 1$, et on a $x_m^q = x_{-\lambda m + \ell}$ avec encore $-\lambda m + \ell \in \{1, \ldots, (\ell-1)/2\}$ (c'est juste que si $P_m \in C$, on a aussi $-P_m \in C$, et ces deux points ont la même abscisse). Il en découle que $g(x)$ a ses racines permutées par un automorphisme de corps. Grâce aux relations coefficients-racines, ses coefficients sont fixés par cet automorphisme. Il est donc à coefficients dans $\mathbb{F}_q$.

Pour résumer, on voit que lorsqu'il existe un sous-groupe C de $E[\ell]$ d'ordre ℓ stable par le Frobenius π, alors il existe un polynôme g de degré $(\ell-1)/2$ qui nous permet de calculer a_ℓ de cette manière :

1. poser $\lambda = 1$, et tant que $\pi_\ell \neq \lambda \cdot [1]_\ell$ ou $\pi_\ell \neq -\lambda \cdot [1]_\ell$, incrémenter λ ;
2. renvoyer $a_\ell = \lambda + q/\lambda \bmod \ell$.

La force de l'amélioration apportée par Elkies et Atkin est surtout de ne plus travailler dans $\mathrm{End}(E[\ell])$, *i.e.* de considérer les coordonnées des points non plus comme des polynômes modulo ψ_ℓ (de degré $(\ell^2-1)/2$) mais plutôt de travailler modulo g (de degré $(\ell-1)/2$).

Il reste cependant des questions en suspend.

1. Comment savoir s'il existe un tel sous-groupe C de $E[\ell]$ stable par le Frobenius, *i.e.* un point P de $E[\ell]$ tel que $\pi(P) = \lambda \cdot P$?
2. Si on sait qu'un tel sous-groupe existe, comment calculer $g(X)$ *efficacement* ?

6.4.2 Détermination de l'existence de C

Tout d'abord rappelons que l'existence du sous-groupe C d'ordre ℓ stable par le Frobenius n'est pas du tout garantie. Elle implique l'existence d'un diviseur non-trivial de $\psi_\ell \in \mathbb{F}_q[X]$, or il se peut parfaitement que ce dernier soit irréductible. On peut alors dire adieu à notre désir de travailler modulo un polynôme g de degré $(\ell-1)/2$.

Maintenant, la matrice $\pi_\ell \in \mathrm{M}_2(\mathbb{F}_\ell)$ a pour polynôme caractéristique $\chi(T) = T^2 - a_\ell T + q_\ell \in \mathbb{F}_\ell[T]$. Ses racines sont les valeurs propres de π_ℓ et elles sont dans $\mathbb{F}_\ell$ si et seulement si χ a des racines dans $\mathbb{F}_\ell$, *i.e.* si et seulement si $\Delta = a_\ell^2 - 4q_\ell$ est un carré modulo ℓ.

Autrement dit, le facteur g existe si Δ est un carré modulo ℓ. On dit dans ce cas que ℓ est un *premier d'Elkies*. On appelle les autres les *premiers de Atkin*. Et un nombre premier ℓ a donc à peu de choses près une chance sur deux d'être un premier d'Elkies, ou d'Atkin.

Malheureusement, pour calculer ce discriminant il faut connaître a_ℓ, ce qui est précisément l'objet de cette section... Il va donc falloir s'y prendre autrement. La solution au problème se trouve dans l'usage des polynômes modulaires. En effet, avoir un sous-groupe C stable par π revient à dire que l'on peut choisir une ℓ-isogénie $E \to E'$ de noyau C avec E' définie sur $\mathbb{F}_q$. Ceci est équivalent à ce que $j(E') \in \mathbb{F}_q$ et $\Phi_\ell(j(E), j(E')) = 0$.

L'idée est donc de calculer $\gcd(Y^q - Y,\ \Phi_\ell(j(E), Y)) \in \mathbb{F}_q[Y]$.

— Si ce pgcd est de degré ≥ 1, alors $\Phi_\ell(j(E), Y)$ a une racine dans $\mathbb{F}_q$ correspondant au j-invariant de la courbe E' qu'on cherche et dans ce cas là le groupe C et le polynôme g existent bel et bien. L'entier ℓ est d'Elkies.

— En revanche, si le pgcd est constant alors $\Phi_\ell(j(E), Y)$ n'a pas de racine dans $\mathbb{F}_q$ et, au mieux, on ne peut conclure qu'avec l'algorithme de Schoof. L'entier ℓ est d'Atkin.

Rq Lorsque ℓ est d'Atkin, il est possible d'avoir à moindre coût des renseignements partiels sur a_ℓ, à partir des degré des facteurs irréductibles de $\Phi_\ell(j(E),Y)$. Mais en pratique, on arrête assez vite à chercher à déterminer a_ℓ quand ℓ est d'Atkin. Mieux vaut doubler le nombre de premiers d'Elkies à considérer !

6.4.3 Calcul du facteur $g(x)$

Le calcul efficace de $g(x)$, lorsqu'il existe, est assez difficile à expliquer. On veut pouvoir le déterminer sans calculer, ni factoriser, ψ_ℓ.

En gros, l'idée est la suivante. On note j_1 une racine de $\Phi_\ell(j(E),Y)$ dans $\mathbb{F}_q$ et on construit une courbe elliptique E' sur $\mathbb{F}_q$ de j-invariant j_1 (voir la remarque qui suit l'algorithme 1). On sait désormais qu'il existe une ℓ-isogénie $E \to E'$. Une telle isogénie s'écrit

$$\begin{array}{rcl} E & \longrightarrow & E' \\ (x,y) & \longmapsto & \left(\dfrac{U_1(x)}{V_1(x)}, \dfrac{U_2(x)}{V_2(x)}y\right) \end{array}$$

avec $U_1(x)$ et $V_1(x)$ premiers entre eux (voir proposition 2.20). Le polynôme $V_1(x)$ est $g^2(x)$, le polynôme $V_2(x)$ est $g^3(x)$ et les polynômes $U_1(x)$ et $U_2(x)$ s'expriment aussi en fonction de $g(x)$, mais par des expressions moins simples qui proviennent des formules de Vélu. En fait, pour trouver efficacement ces polynômes à partir des coefficients de E et E', les méthodes les plus rapides résolvent une équation différentielle (voir [BSS00 ; Sch95]).

Bibliographie

[BSS00] I. F. Blake, G. Seroussi et N. P. Smart. *Elliptic curves in cryptography*. T. 265. Reprint of the 1999 original. Cambridge University Press, Cambridge, 2000, p. xvi+204 (cf. p. 95).

[Cox22] D. A. Cox. *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication*. Third. With contributions by Roger Lipsett. AMS Chelsea Publishing, Providence, RI, 2022, p. xv+533 (cf. p. 51).

[ElJ16] El Jj. *Deux (deux ?) minutes pour... le théorème de Bézout*. Youtube. Juill. 2016. URL : https://www.youtube.com/watch?v=0_ZzZzvxnP0, accédé le 25/01/2024 (cf. p. 12).

[Hin08] M. Hindry. *Arithmétique: primalité et codes, théorie analytique des nombres, équations diophantiennes, courbes elliptiques*. Calvage & Mounet, 2008 (cf. p. 33).

[Kob89] N. Koblitz. "Hyperelliptic cryptosystems". In : *J. Cryptology* 1.3 (1989), p. 139-150 (cf. p. 7).

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD. University of California, Berkeley, 1996 (cf. p. 89).

[Lem21] F. Lemmermeyer. *Quadratic number fields*. Translated from the 2017 German original. Springer, Cham, 2021, p. xi+343 (cf. p. 51).

[LN97] R. Lidl et H. Niederreiter. *Finite fields*. Second. T. 20. With a foreword by P. M. Cohn. Cambridge University Press, Cambridge, 1997, p. xiv+755 (cf. p. 99).

[Mil06] J. S. Milne. *Elliptic curves*. BookSurge Publishers, Charleston, SC, 2006, p. viii+238. URL : https://www.jmilne.org/math/Books/ectext6.pdf, accédé le 25/01/2024 (cf. p. 7, 33, 34).

[Sch85] R. Schoof. "Elliptic curves over finite fields and the computation of square roots mod p". In : *Math. Comp.* 44.170 (1985), p. 483-494 (cf. p. 93).

[Sch95] R. Schoof. "Counting points on elliptic curves over finite fields". In : *J. Théor. Nombres Bordeaux* 7.1 (1995). Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993), p. 219-254 (cf. p. 95).

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. T. 151. Springer-Verlag, New York, 1994, p. xiv+525 (cf. p. 73).

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. Second. T. 106. Springer, Dordrecht, 2009, p. xx+513 (cf. p. 7, 37).

[Sut13a] A. V. Sutherland. *Isogeny volcanoes,* Palmetto Number Theory Series (PANTS XX). Davidson College. Sept. 2013. URL : https://math.mit.edu/~drew/PANTSXX.pdf, accédé le 25/01/2024 (cf. p. 92).

[Sut13b] A. V. Sutherland. "On the evaluation of modular polynomials". In : *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*. T. 1. Math. Sci. Publ., Berkeley, CA, 2013, p. 531-555 (cf. p. 93).

[Sut17] A. V. Sutherland. *Elliptic Curves*. A computationally focused course. Fév. 2017. URL : https://math.mit.edu/classes/18.783/2017/, accédé le 25/01/2024 (cf. p. 7, 42, 71, 74).

[Was08] L. C. Washington. *Elliptic curves*. Second. Number theory and cryptography. Chapman & Hall/CRC, Boca Raton, FL, 2008, p. xviii+513 (cf. p. 71, 72, 87, 93).

[Wik] Wikipedia contributors. *Post-quantum cryptography — Wikipedia, The Free Encyclopedia*. URL : https://en.wikipedia.org/wiki/Post-quantum_cryptography, accédé le 25/01/2024 (cf. p. 33).

A. Rappels sur les corps finis

En grande majorité, nous considérons dans ce texte des courbes elliptiques définies sur des corps finis. Pour familiariser les lectrices et lecteurs non avertis à ces concepts, nous en synthétisons ici les aspects principaux.

Nous fournissons quand cela nous semble intéressant quelques schémas de démonstration. Des justifications plus rigoureuses sont disponibles dans de nombreux ouvrages de références, citons parmi d'autres [LN97].

A.1 Définition

Un corps est un ensemble muni de deux lois de groupe vérifiant une relation de distributivité ; une loi d'addition commutative $+$ et une de loi de multiplication $\times$.

Définition A.1 Un corps est un anneau dont les éléments non nuls sont inversibles.

Il n'est pas difficile d'exhiber des corps dont le nombre d'éléments est fini. Un mécanisme général utilisé dans les implantations consiste à quotienter certains anneaux euclidiens $\mathbb{A}$ par l'un de leurs idéaux premiers $\mathfrak{p}$. Ainsi ;

— avec $\mathbb{A} = \mathbb{Z}$ et $\mathfrak{p} = p\mathbb{Z}$ où p est un nombre premier, nous obtenons $\mathbb{Z}/p\mathbb{Z}$, le corps à p éléments des "entiers modulo p".

— avec $\mathbb{A} = \mathbb{F}_q[X]$, l'ensemble des polynômes à coefficients dans un corps fini à q éléments et $\mathfrak{p} = P(X)\mathbb{F}_q$ où $P(X)$ est un polynôme irréductible de degré n de $\mathbb{F}_q[X]$, nous obtenons un corps à q^n éléments que nous appellerons une "extension de degré n" de $\mathbb{F}_q$.

Dans la suite, nous montrons que ces corps finis sont uniques à isomorphisme près. Auparavant, notons qu'un corps est parfois défini dans la littérature comme étant commutatif (c'est-à-dire de groupe multiplicatif commutatif). Dans notre cas, la finitude lève toute ambiguïté grâce à un théorème de Wedderburn.

Théorème A.2 Tout corps fini est commutatif.

La démonstration de ce théorème est assez lourde. Par contre, il est beaucoup plus aisé d'obtenir le résultat suivant.

Proposition A.3 Tout anneau fini intègre, c'est-à-dire sans diviseur de zéro, est un corps fini.

Esquisse de démonstration. Si a est un élément d'un tel anneau, il suffit de montrer que lorsque b décrit cet anneau, les éléments ab sont distincts et donc il existe un élément $\bar{a}$ tel que $a\bar{a} = \bar{a}a = 1$. ■

A.2 Cardinalité

La cardinalité des corps finis est particulière.

Théorème A.4 Soit $\mathbb{F}_q$ un corps fini de cardinal q. Alors il existe un nombre premier p et un entier n strictement positif tel que $q = p^n$.

Esquisse de démonstration. Tout découle du morphisme d'anneau f défini de $\mathbb{Z}$ vers $\mathbb{F}_q$ et qui envoie l'entier n sur $n \times 1$. En effet, $\ker(f)$ étant un idéal non nul de $\mathbb{Z}$, il est égal à $p\mathbb{Z}$ où p doit être un nombre premier. Donc $\mathrm{im}(f)$, étant isomorphe à $\mathbb{Z}/\ker(f)$, est en fait isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Il suffit ensuite de considérer $\mathbb{F}_q$ comme un espace vectoriel de dimension finie n sur $\mathrm{im}(f)$ pour conclure. ■

Le nombre premier p est appelé la caractéristique de $\mathbb{F}_q$.

A.3 Groupe multiplicatif

Nous prouvons par une succession de lemmes que le groupe multiplicatif $\mathbb{F}_q^\times$ d'un corps fini $\mathbb{F}_q$ est cyclique (corollaire A.11). Nous aurons besoin pour cela de la fonction d'Euler.

Définition A.5 La fonction d'Euler φ est l'application définie de $\mathbb{N}^*$ dans $\mathbb{N}^*$ par

$$\forall n \in \mathbb{N}^*,\ \varphi(n) = \#\{1 \leq i \leq n,\ \mathrm{pgcd}(i,n) = 1\}.$$

Outre que cette fonction soit multiplicative, $\forall (p,q) \in \mathbb{N}^{*2}$, $\mathrm{pgcd}(p,q) = 1$, $\varphi(pq) = \varphi(p)\varphi(q)$, cette fonction a aussi la propriété suivante.

Proposition A.6 La fonction d'Euler φ vérifie

$$\sum_{d|n} \varphi(d) = n.$$

Le premier lemme n'est que le théorème de Lagrange spécialisé à notre cas.

Lemma A.7 Soit $\alpha \in \mathbb{F}_q^\times$. Alors $\mathrm{ord}(\alpha)$ divise $q-1$.

Le lemme suivant se démontre alors par un simple raisonnement sur les ordres des éléments.

Lemma A.8 Soit $\alpha \in \mathbb{F}_q^\times$. Alors $\mathrm{ord}(\alpha^i) = \mathrm{ord}(\alpha)/\mathrm{pgcd}(i, \mathrm{ord}(\alpha))$.

Le point crucial est ce lemme.

Lemma A.9 Soit un entier t divisant $q-1$ où $\mathbb{F}_q$ est un corps fini. Alors, soit il n'y a pas d'éléments d'ordre t, soit il y a $\varphi(t)$ éléments d'ordre t.

Esquisse de démonstration : supposons qu'il existe un élément α d'ordre t. De manière générale, les éléments d'ordre t sont les racines de $X^t - 1$. Or les t racines de ce polynôme sont α^i pour i variant de 1 à t. Comme d'autre part $\mathrm{ord}(\alpha^i) = t/\mathrm{pgcd}(i,t)$, il y a $\varphi(t)$ éléments d'ordre t. ■

Nous arrivons au résultat principal.

Théorème A.10 Soit un entier t divisant $q-1$ où $\mathbb{F}_q$ est un corps fini. Alors il y a $\varphi(t)$ éléments d'ordre t.

Esquisse de démonstration : soit $\psi(t)$ le nombre d'éléments d'ordre t, nous avons d'une part $\sum_{t \text{ divise } q-1} \psi(t) = q-1$ et d'autre part $\psi(t) \leq \varphi(t)$ d'après le lemme A.9. D'après la proposition A.6, nous avons donc $\sum_{t \text{ divise } q-1} \varphi(t) - \psi(t) = 0$ et comme les termes de cette somme sont positifs, nous avons finalement $\psi(t) = \varphi(t)$. ■

Par conséquent, il y a $\varphi(q-1)$ éléments d'ordre $q-1$ dans un corps fini $\mathbb{F}_q$.

Corollaire A.11 Le groupe multiplicatif $(\mathbb{F}_q^\times, \times)$ est un groupe cyclique.

à ce stade, il est facile d'introduire la notion de racine primitive.

Définition A.12 Un générateur de $(\mathbb{F}_q^\times, \times)$ est appelé une racine primitive de $\mathbb{F}_q$.

Ainsi deux corps finis de même cardinalité sont isomorphes.

A.4 Sous-corps d'un corps fini

Les sous-ensembles d'un corps fini qui sont eux-mêmes des corps sont clairement caractérisés.

Théorème A.13 Soit $\mathbb{K}$ un sous-corps d'un corps fini $\mathbb{F}_{p^n}$. Alors $\mathbb{K} = \mathbb{F}_{p^m}$ avec m divise n.

Esquisse de démonstration : elle consiste à prouver que $\mathbb{F}_{p^n}$ est un $\mathbb{K}$-espace vectoriel. ■

Le théorème suivant nous donne un moyen de tester si un élément d'un corps fini appartient à un de ses sous-corps.

Théorème A.14 Soit $\mathbb{F}_{p^m}$ un sous-corps d'un corps fini $\mathbb{F}_{p^n}$. Alors un élément x de $\mathbb{F}_{p^n}$ appartient à $\mathbb{F}_{p^m}$ si et seulement si $x^{p^m} = x$.

Esquisse de démonstration : d'une part, on a $\forall x \in \mathbb{F}_{p^m}$, $x^{p^m} = x$ et réciproquement le polynôme $X^{p^m} - X$ a au plus p^m racines qui se trouvent être les éléments de $\mathbb{F}_{p^m}$. ■

A.5 Automorphismes d'un corps fini

On associe à un élément α d'un corps fini un unique polynôme $p_\alpha(X)$ appelé polynôme minimal de α et défini comme suit.

Théorème A.15 Soit $\alpha \in \mathbb{F}_{p^n}$. Alors il existe un unique polynôme unitaire et irréductible $p_\alpha(X) \in \mathbb{F}_p[X]$ tel que $p_\alpha(\alpha) = 0$ et $p_\alpha(X)$ divise tout polynôme $f(X)$ de $\mathbb{F}_p[X]$ ayant α comme zéro. De plus $\deg(p_\alpha) \leq n$.

Esquisse de démonstration : il suffit de remarquer que l'ensemble $\mathfrak{p} = \{f \in \mathbb{F}_p[X], f(\alpha) = 0\}$ est un idéal principal distinct de $\{0\}$. Il est alors égal à $p_\alpha(X)\mathbb{F}_p[X]$ où $p_\alpha(X)$ est le polynôme recherché. ■

Définissons les conjugués d'un élément α comme suit.

Définition A.16 Soit $\alpha \in \mathbb{F}_{p^n}$. Alors les conjugués de α sont les racines dans $\mathbb{F}_{p^n}$ de $p_\alpha(X)$.

Grâce au lemme suivant fort utile dans les applications, il n'est pas difficile de prouver que α^p, α^{p^2}, ...,$\alpha^{p^{n-1}}$ sont racines de $p_\alpha(X)$.

Lemma A.17 Soient $\alpha_1, \ldots, \alpha_k$, k éléments d'un corps de caractéristique p. Alors

$$\forall i \in \mathbb{N}, (\alpha_1 + \cdots + \alpha_k)^{p^i} = \alpha_1^{p^i} + \cdots + \alpha_k^{p^i}.$$

Esquisse de démonstration : il suffit de voir que les coefficients de la somme

$$(\alpha_1 + \cdots + \alpha_k)^{p^i} = \sum_{j_1 + \cdots + j_k = p^i} \frac{p^i!}{j_1! \cdots j_k!} \alpha_1^{j_1} \cdots \alpha_k^{j_k},$$

sont des multiples de p excepté pour $j_l = p^i$ $(0 \leq l \leq k)$. ■

Le degré de p_α ou encore le nombre de conjugués associés à α est alors donné après une démonstration purement technique par le théorème suivant.

Théorème A.18 Soit $\alpha \in \mathbb{F}_{p^n}$. Le nombre de conjugués de α divise n. C'est le plus petit entier d tel que $p^d \equiv 1 \bmod \mathrm{ord}(\alpha)$.

Enfin, le groupe des automorphismes d'un corps fini est lui aussi cyclique.

Proposition A.19 Les automorphismes d'un corps fini $\mathbb{F}_{p^n}$ sont id, π, π^2, … π^{n-1} où l'automorphisme de Frobenius π est donné par

$$\begin{array}{rcl} \mathbb{F}_{p^n} & \to & \mathbb{F}_{p^n}, \\ x & \mapsto & x^p. \end{array}$$

Esquisse de démonstration : d'après le lemme A.17, π et ses composés π^i sont des automorphismes, distincts dès que $i < n$. Réciproquement, soit f un morphisme et α une racine primitive de $\mathbb{F}_q$ de polynôme minimal $p_\alpha(X)$. Nous avons $p_\alpha(f(\alpha)) = f(p_\alpha(\alpha)) = 0$, et donc il existe un indice $i < n$ tel que $f(\alpha) = \alpha^{p^i}$ d'où on conclut facilement que $f = \pi^i$. ■

A.6 Carrés de $\mathbb{F}_q$ et symbole de Legendre

Soit $q = p^s$ avec p impair [1]. On définit le symbole de Legendre sur $\mathbb{F}_q$ par $\left(\frac{x}{q}\right) = x^{(q-1)/2}$. Restreint à $\mathbb{F}_q^\times$, il définit un morphisme de groupes vers $\mathbb{F}_q^\times$.

Théorème A.20 Le symbole de Legendre vérifie $\left(\frac{\cdot}{q}\right)$ est à valeurs dans $\{-1, 0, 1\}$ et

$$\left(\frac{x}{q}\right) = 1 \text{ si et seulement si } x \text{ est un carré non nul},$$
$$\left(\frac{x}{q}\right) = -1 \text{ si et seulement si } x \text{ est un non carré non nul},$$
$$\left(\frac{x}{q}\right) = 0 \text{ si et seulement si } x = 0.$$

Démonstration. Soit $x \in \mathbb{F}_q^\times$, alors $\left(x^{(q-1)/2}\right)^2 = 1$ et donc $x^{(q-1)/2} \in \{\pm 1\}$. Comme $\mathbb{F}_q^\times$ est cyclique, il existe une racine primitive $\gamma \in \mathbb{F}_q^\times$ telle que $\langle \gamma \rangle = \mathbb{F}_q^\times$. On a $\gamma^{(q-1)/2} = -1$ car $\mathrm{ord}(\gamma) = q - 1$. On peut donc écrire $x = \gamma^n$, et on remarque que x est un carré si et seulement si n est pair. Ceci prouve le théorème. ■

1. L'étude des carrés dans $k = \mathbb{F}_{2^s}$ est relativement ennuyante étant donné que $x \mapsto x^2$ est surjectif (c'est le morphisme de Frobenius). Autrement dit, dans $\mathbb{F}_{2^s}$ tous les éléments sont des carrés.

On a les conséquences suivantes du théorème A.20.

Corollaire A.21
1. Un corps fini $\mathbb{F}_q$ contient $(q-1)/2$ carrés non-nuls.
2. -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q = 1 \bmod 4$.
3. Le produit de deux carrés est un carré. Le produit de deux non-carrés est un carrés. Le produit d'un non-carré avec est un carré est un non-carré.

Démonstration.
1. Il s'agit d'appliquer le théorème d'isomorphisme à $\left(\frac{\cdot}{q}\right) : \mathbb{F}_q^\times \longrightarrow \{-1,1\}$. Son noyau est exactement les carrés non nuls et il est surjectif.
2. $(-1)^{(q-1)/2} = 1$ si et seulement si $(q-1)/2$ est pair, *i.e.* $q = 1 \bmod 4$.
3. Ce point découle directement du théorème A.20 et du fait que le symbole de Legendre est un morphisme de groupe. ■

Théorème A.22 — Lois de réciprocité quadratique. Soient p et q deux nombres premiers impairs distincts.
- Première loi : -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p = -1 \bmod 4$.
- Deuxième loi : on a $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
- Théorème fondamental : on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proposition A.23 Soit $\mathbb{F}_q \subseteq \mathbb{F}_{q^s}$ une extension de corps finis. Soit $a \in \mathbb{F}_q$.
- Si s pair : a est un carré dans $\mathbb{F}_{q^s}$.
- Si s impair : a est un carré dans $\mathbb{F}_{q^s}$ si et seulement si a est un carré dans $\mathbb{F}_q$.

Démonstration. Puisque $a \in \mathbb{F}_q$ on sait que $a^{(q-1)/2} \in \{-1, 0, 1\}$. On a aussi l'égalité $a^{(q^s-1)/2} = a^{(q-1)(q^{s-1}+\cdots+1)/2}$.

Si s est pair alors $q^{s-1}+\cdots+1$ est une somme de s éléments impairs. Donc la somme est paire et le produit $(q-1)(q^{s-1}+\cdots+1)/2$ reste pair. a est donc bien un carré.

Si s est impair, alors $q^{s-1}+\cdots+1$ est impair. Donc $a^{(q^s-1)/2} = a^{(q-1)/2}$ et a est un carré dans $\mathbb{F}_{q^s}$ si et seulement si a est un carré dans $\mathbb{F}_q$. ■

A.7 Existence

Nous savons grâce au théorème A.4 que le cardinal d'un corps fini est p^n. Inversement, la question est maintenant de savoir s'il existe pour tout entier p^n un corps fini de cette cardinalité. Pour $n = 1$, le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ répond à la question. Pour $n > 1$, nous prouvons qu'il existe toujours un polynôme irréductible $P(X)$ de degré n à coefficients dans $\mathbb{F}_p$ car le corps $\mathbb{F}_p[X]/P(X)\mathbb{F}_p[X]$ répond à la question.

En fait, nous sommes en mesure plus généralement de compter le nombre de polynômes irréductibles à l'aide de la fonction de Möbius μ définie de $\mathbb{N}^*$ dans $\mathbb{N}^*$ par

$$\forall n \in \mathbb{N}^*,\ \mu(n) = \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n = p_1^{e_1}\cdots p_k^{e_k} \text{ et s'il existe } i \text{ tel que } e_i \geq 2, \\ (-1)^k & \text{si } n = p_1\cdots p_k. \end{cases}$$

Pour cela, nous partons du théorème suivant.

Théorème A.24 Soient $V_d(X)$, le produit des polynômes irréductibles de degré d sur $\mathbb{F}_q[X]$. Alors

$$X^{q^n} - X = \prod_{d \text{ divise } n} V_d(X). \tag{A.1}$$

Par passage aux degrés des polynômes qui interviennent dans l'égalité (A.1), nous obtenons alors le corollaire suivant.

Corollaire A.25 Soit I_d le nombre de polynômes irréductibles de degré d de $\mathbb{F}_q$. Alors

$$q^n = \sum_{d \text{ divise } n} dI_d.$$

Il ne reste plus alors qu'à utiliser la formule classique "d'inversion de Möbius" pour compléter notre calcul.

Proposition A.26 Le nombre de polynômes irréductibles de degré n à coefficients dans un corps fini $\mathbb{F}_q$ est donné par

$$I_n = \frac{1}{n} \sum_{d \text{ divise } n} \mu(d) q^{n/d}. \tag{A.2}$$

Un examen plus approfondi de la formule (A.2) montre que l'entier I_n est strictement positif pour tout couple $(n,\ q)$, ce qui permet de conclure.

Corollaire A.27 Pour tout nombre premier p et tout entier n strictement positif, il existe un corps fini à p^n éléments.

■ **Exemple A.28** Soit $a \in \mathbb{F}_q$ un élément qui n'est pas un carré. Ceci revient à dire que le polynôme $X^2 - a \in \mathbb{F}_q[X]$ est irréductible et donc que $\mathbb{K} = \mathbb{F}_q[X]/\langle X^2 - a\rangle \simeq \mathbb{F}_{q^2}$ est une extension de degré 2 de $\mathbb{F}_q$. La classe α de X dans $\mathbb{K}$ vérifie $\alpha^2 = \bar{X}^2 = a$. On peut donc considérer $\mathbb{K}$ comme la plus petite extension de $\mathbb{F}_q$ dans laquelle a est un carré, *i.e.* $\mathbb{K} = \mathbb{F}_q[\sqrt{a}]$.

Si on veut aller plus loin, on peut voir que dans $\mathbb{K}$ tous les éléments de $\mathbb{F}_q$ sont des carrés. En effet, si on considère un autre élément $b \in \mathbb{F}_q$ qui n'est pas un carré dans $\mathbb{F}_q$ on peut alors construire $\mathbb{K}' = \mathbb{F}_q[X]/\langle X^2 - b\rangle \simeq \mathbb{F}_{q^2}$ par unicité des corps de cardinaux q^2. Ainsi $\mathbb{K}' \simeq \mathbb{K}$ et b est aussi un carré dans $\mathbb{K}$ (on peut aussi appliquer la proposition A.23). C'est vraiment une particularité unique des corps finis. ■

https://www.univ-rennes.fr/