Université de Bourgogne
UFR de Mathématiques

M1 Mathématiques Approfondies
Mémoire de Master

Les Courbes Elliptiques

Théophile Hontang

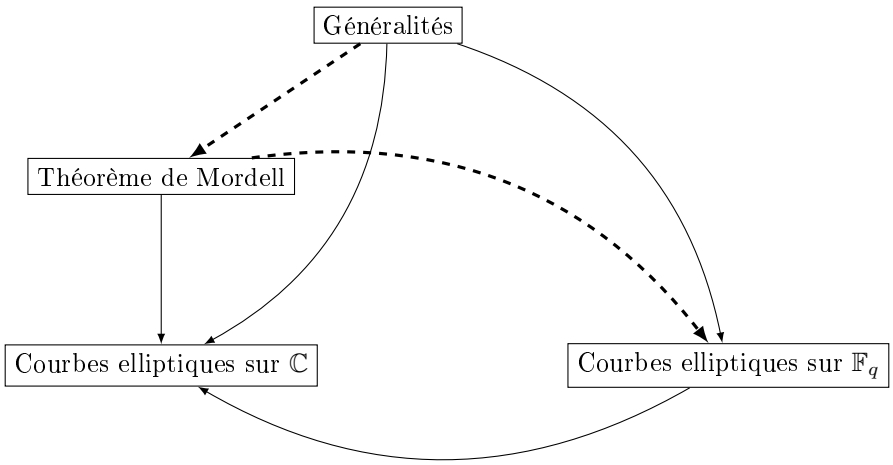
Sous la direction de Ronan Terpereau

Le 22 mai 2017

Table des matières

Introduction

Le but de ce mémoire est de présenter les aspects de la théorie des courbes elliptiques. On a préféré faire une introduction à cette théorie dont le lecteur pourra choisir les parties qu'il décidera de lire (un schéma en bas de page représente ces "parcours"). Il est conseillé au lecteur de commencer sa lecture par la première section "Généralités" où est définit la loi de groupe sur les courbes elliptiques, notion cruciale par la suite.
La deuxième section porte sur le théorème de Mordell, théorème bien connu des algébristes. La démonstration est longue (six pages) mais elle reste élémentaire, le lecteur peut faire l'impasse sur cette section. Dans une troisième partie, on présente brièvement les applications en cryptographie très utilisées de nos jours. En annexe, certains algorithmes sont présentés par le logiciel Maple.
Pour conclure ce mémoire, on étudie les courbes elliptiques sur $\mathbb{C}$, étude qui aurait pu être un sujet de mémoire à lui seul. Cette partie demande des pré-requis, principalement, en analyse complexe et en théorie des corps.
Ce mémoire est influencé par les livres de Joseph H. Silverman[ST15],[Sil09] et [Sil94], livres conseillés après la lecture de ce mémoire.



Remerciements
Je voudrais remercier toutes les personnes qui m'ont aidé dans la réalisation de ce mémoire. Tout d'abord, je remercie M.Terpereau pour m'avoir guidé tout au long de ces cinq mois. Ensuite, je remercie M.Nagel, M.Faenzi et M.Kitanine pour avoir répondu à mes questions.

I Généralités

I.1 Loi de groupe

Soit $\mathbb{K}$ un corps quelconque.

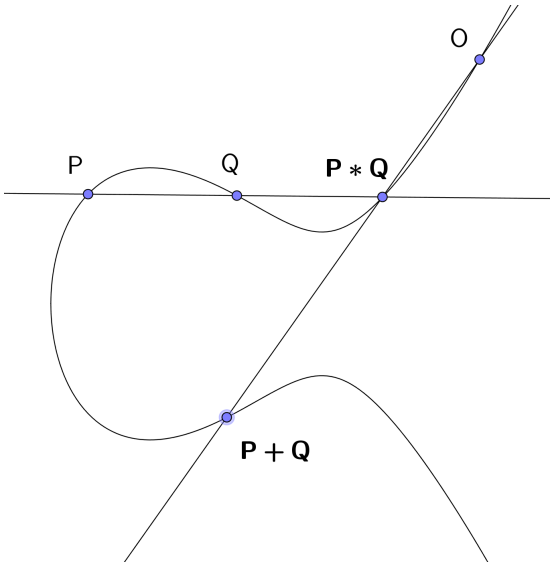


FIGURE 1 – Loi d'addition

Définition I.1. *Dans le plan projectif $\mathbb{P}^2(\mathbb{K})$, C est une* ***courbe cubique*** *sur un corps $\mathbb{K}$ si son équation est $F(X,Y,Z) = 0$ où $F(X,Y,Z)$ est un polynôme homogène de degré 3.*
Si la cubique C est lisse alors on dit que C est une ***courbe elliptique****.*

Remarque I.2.

1. *Pour les corps de caractéristique différente de 2 et 3, cette équation peut être réduite à*

$$y^2 = x^3 + ax + b$$

où $a, b \in \mathbb{K}$. Cette forme n'est pas unique. Les seuls changements de variable préservant cette forme sont :

$$x \mapsto u^2 x \qquad y \mapsto u^3 y$$

où $u \in \mathbb{K}$. Nous allons considérer cette forme tout au long du mémoire (sauf mention contraire). Voir [ST15] pour un exemple.

2. *En utilisant les coordonnées non homogènes $x = X/Z$ et $y = Y/Z$, nous obtenons*

$$Y^2 Z = X^3 + aXZ^2 + bZ^3$$

Cette forme est dite de ***Weierstrass****.*

Soit $P = (x, y)$ avec $x, y \in \mathbb{K}$. Un des résultats centraux sur les points P des courbes elliptique est le fait qu'ils forment un groupe abélien. Avant de définir la loi de composition du groupe, rappelons le théorème de Bézout (Voir [Cha13] pour une démonstration).

Théorème I.3 (Bézout)**.** *Soient C et C' deux courbes projectives planes de degrés d et d' définies sur un corps algébriquement clos, sans composante commune. Alors le nombre de points d'intersection de C et C', comptés avec leurs multiplicités, est égal à dd'.*

Par le théorème de Bézout, une droite L intersecte C en trois points(Ces points ne sont pas forcément distincts). Nous allons considérer un point à l'infini, qu'on note $\mathcal{O}$, comme l'ensemble des points $(X : Y : Z) \in C$ tels que $Z = 0$. Cet ensemble est réduit au point $\mathcal{O} = (0 : 1 : 0)$.
Définissons la loi de composition $+$ de C par la règle suivante.

Loi de Composition I.4 ([ST15]). *Soient $P, Q \in C$, la droite L joignant P et Q (ou la tangente si $P = Q$), et $P * Q$ le troisième point d'intersection de L par C. Soit L' la droite joignant $P * Q$ et $\mathcal{O}$. Alors $P + Q$ est le point tel que L' intersecte C aux points $P * Q$, $\mathcal{O}$ et $P + Q$. C'est à dire :*

$$P + Q = \mathcal{O} * (P * Q).$$

Proposition I.5 ([ST15]). *La courbe elliptique C, munie de la loi de composition $+$, est un groupe abélien avec $\mathcal{O}$ comme élément neutre.*

Démonstration. Si $Q = \mathcal{O}$, L et L' coïncident. L intersecte C aux points $P, \mathcal{O}, R$ et L' intersecte C aux points $P + \mathcal{O}, \mathcal{O}, R$ d'où $P + \mathcal{O} = P$.
Si L intersecte C aux points $P, \mathcal{O}$ et un troisième point qu'on note R, alors

$$(P + Q) + R = \mathcal{O}$$

par la définition de loi de groupe. Nous obtenons

$$\mathcal{O} = (P + \mathcal{O}) + R = P + R$$

L'associativité est démontré par la figure 5 dans l'annexe.
La commutativité provient du fait que la construction de la loi est symétrique en P et Q. □

Remarque I.6. *Le point $P * Q = (x, y)$ donne le point $P + Q = (x, -y)$, point symétrique par rapport l'axe des abscisses. Nous remarquons alors que si $P = (x, y) \in C$ alors $-P = (x, -y) \in C$.*

Dorénavant, nous notons $(C(\mathbb{K}), +)$ ce groupe abélien.

I.2 Formules de duplication

La loi étant définie précédemment, nous pouvons calculer la somme de deux points ou le double d'un point. Ces formules, qu'on nomme **formules de duplication**, seront utilisées dans les prochaines parties.

Proposition I.7 (Formules de duplication [ST15]). *Soit C une courbe elliptique d'équation $y^2 = x^3 + ax^2 + bx + c$.*

1. *Soient $P_i = (x_i, y_i) \in C$ pour $i \in \{1, 2\}$. Alors $P_1 + P_2 = (x_3, y_3)$ avec*

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad y_3 = \lambda x_3 + \nu \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = y_1 - \lambda x_1$$

2. *Soit $P_0 = (x_0, y_0) \in C$. Alors la coordonnée en x de $2P$ est :*

$$x(2P) = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}$$

Démonstration. 1) Soient $P_1 * P_2 = (x_*, y_*)$. La droite joignant P_1 et P_2 est définie par l'équation $y = \lambda x + \nu$ avec $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ et $\nu = y_1 - \lambda x_1$. L'intersection de cette droite avec C est définie par :

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$$

Les trois racines de ce polynôme sont x_1, x_2 et x_*. Par les relations de Viète qui expriment les coefficients du polynôme par les racines, nous obtenons :

$$a - \lambda^2 = -(x_1 + x_2 + x_3)$$

Comme $x_3 = x_*$ et $y_3 = -y_*$, nous obtenons bien les coordonnées de $P_1 + P_2$.
2) $P * P$ est obtenu par l'intersection de C et de la tangente de C en P. La pente est $\lambda = \frac{dy}{dx}(P_0) = \frac{f'(x_0)}{2y_0}$. En substituant λ dans les équations obtenues en 1) et en remplaçant y^2 par $x^3 + ax^2 + bx + c$, nous obtenons le résultat.

□

I.3 Points d'ordre fini

Nous allons maintenant définir l'ordre d'un élément du groupe $(C(\mathbb{K}), +)$.

Définition I.8. *Pour $n \in \mathbb{Z}$, on définit l'application*

$$[n] : C \to C$$
$$P \mapsto \begin{cases} [n]\ P = \underbrace{P + ... + P}_{n fois} & si\ n > 0 \\ [n]\ P = \left[-n\right](-P) & si\ n < 0 \end{cases}$$

Si $n = 0$ alors $[0]P = \mathcal{O}$.
Cette application sera utile pour la section "Multiplication complexe", section IV.4.
Un point P est d'ordre fini $n > 0$ si $[n]P = \mathcal{O}$ et $[m]P \neq \mathcal{O}$ pour $m < n$. Sinon P est d'ordre infini.

Il existe une caractérisation simple des points d'ordre 2 et 3.

Théorème I.9 (Points d'ordre 2 et 3 [ST15])**.** *Soit C une courbe elliptique.*

1. *Un point $P = (x, y) \neq \mathcal{O}$ sur C est d'ordre 2 si et seulement si $y = 0$.*
2. *C a quatre points d'ordre divisant 2. Ces quatre points forment un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*
3. *Un point $P = (x, y)$ est d'ordre 3 si et seulement si x est racine du polynôme :*

$$\chi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

4. *C a neuf points d'ordre divisant 3. Ces neuf points forment un groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Démonstration. 1) et 2) Les points P d'ordre 2 sont les points tels que $2P = \mathcal{O}$ i.e $P = -P$. Il est clair que $y = 0$ d'où il y a alors trois points distincts d'ordre 2.
3) Supposons $3P = \mathcal{O}$, nous l'écrivons $2P = -P$ d'où $x(2P) = x(-P) = x(P)$. Réciproquement, si $x(2P) = x(P)$ $(P \neq \mathcal{O})$ alors $2P = \pm P$ d'où $3P = \mathcal{O}$. On a alors une caractérisation des points d'ordre trois, ils satisfont $x(2P) = x(P)$. Par la formule de duplication, nous avons

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x.$$

On retrouve alors le polynôme χ.
4) Nous utilisons une autre expression de χ,

$$\chi(x) = 2f(x)f''(x) - f'(x)^2.$$

En effet, il suffit d'utiliser $x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x$ dans la preuve de 3). Nous prétendons que χ doit avoir quatre racines distinctes i.e χ et χ' n'ont pas de racines communes. Mais

$$\chi'(x) = 2f(x)f'''(x) = 12f(x).$$

Comme C est non-singulière, f et f' n'ont pas de racines communes, il en ait alors ainsi pour χ et χ'.
Maintenant, posons $\beta_1, \beta_2, \beta_3$ et β_4 ces quatre racines. Par 3), l'ensemble

$$\{(\beta_1, \pm\sqrt{f(\beta_1)}), (\beta_2, \pm\sqrt{f(\beta_2)}), (\beta_3, \pm\sqrt{f(\beta_3)}), (\beta_4, \pm\sqrt{f(\beta_4)})\}$$

constitue l'ensemble des points d'ordre trois. Les coordonnées en y ne peuvent être nulles puisque c'est la caractérisation des points d'ordre deux vus en 1). De plus, l'ensemble contient huit points distincts d'ordre trois, le point manquant est bien sûr $\mathcal{O}$. Comme chaque point est d'ordre trois, le groupe est bien isomorphe à $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, ce qui conclut la démonstration. □

Deux théorèmes importants sont à noter sur les points d'ordre fini. Nous les donnons sans démonstration. Le premier nous dit que les coordonnées des points de torsion sont des entiers. Le second nous renseigne sur le sous-groupe de torsion.

Théorème I.10 (Nagell-Lutz [Nag35] [Lut37])**.** *Soient*

$$C : y^2 = x^3 + ax^2 + bx + c$$

une courbe elliptique avec $a, b, c \in \mathbb{N}$ et Δ le discriminant ; i.e

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3$$

Soit $P = (x, y)$ un point rationnel d'ordre fini.
Alors $x, y \in \mathbb{N}$ et soit P est d'ordre 2, soit y^2 divise Δ.

Théorème I.11 (Mazur [1] [Maz77] [Maz78])**.** *Soit C une courbe elliptique. Le sous-groupe de torsion $C(\mathbb{Q})_{tors}$ du groupe des points $\mathbb{Q} - rationnels$ est l'un des groupes suivants :*

$$\mathbb{Z}/n\mathbb{Z} \quad 0 \leqslant n \leqslant 10 \quad ou \quad n = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad 1 \leqslant n \leqslant 4$$

Dans la seconde partie du mémoire, nous allons montrer que $C(\mathbb{Q})$ est de type fini, i.e $C(\mathbb{Q}) \cong \mathbb{Z}^r \times C(\mathbb{Q})_{tors}$ où r est le rang de la courbe.

Remarque I.12. Très peu de résultats concernent le rang d'une courbe elliptique et il existe de nombreuses conjectures le concernant. L'une d'eux est qu'on peut trouver une courbe elliptique de n'importe quel rang. La courbe elliptique de plus grand rang, connue à ce jour, est celle de Noam Elkies et elle est donnée par l'équation

$$y^2 + xy + y = x^3 - x^2 - \alpha x + \beta$$

où $\alpha = 20067762415575526585033208209338542750930230312178956502$
$\beta = 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$
Cette courbe est de rang 28.

I.4 Le j-invariant

Soit $\mathbb{K}$ un corps de caractéristique différente de 2.
Dans cette section, nous allons aborder le j-invariant. Cette notion permet de classer les courbes elliptiques à isomorphisme près. Elle a surtout été étudié au XIXème siècle par Dedekind et Klein qui l'a nommé j.

Considérons C une courbe elliptique sur $\mathbb{K}$ de la forme $y^2 = f(x) = x^3 + ax + b$.

1. La démonstration du théorème est présente dans un cours "Course on Mazur's theorem" par Andrew Snowden de l'Université du Michigan. Voir ici : `http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html`

Comme C est non-singulière, la fonction f admet trois racines distinctes, disons α, β et γ. En réalisant le changement de variables $x \mapsto \frac{x-\alpha}{\beta-\alpha}$, l'équation de C devient

$$y^2 = x(x-1)(x-\lambda)$$

avec $\lambda \in \mathbb{K}\backslash\{0,1\}$. Cette forme est dite **de Legendre** et λ est le paramètre de Legendre. Le paramètre de Legendre n'est pas unique (nous verrons dans le prochain théorème que $\mathfrak{S}^3$ agit sur λ). Le principe de la section est de trouver un invariant à C. Malheureusement, le paramètre de Legendre n'en ait pas un, en effet on peut trouver deux courbes elliptiques isomorphes mais avec des paramètres de Legendre différents. Nous introduisons alors le j-invariant l'expression ci-dessous.

Définition I.13. *Le j-invariant d'une courbe elliptique C (qu'on note indifféremment j,$j(\lambda)$ ou $j(C)$) est défini par*

$$j(\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

avec λ le paramètre de Legendre.

Théorème I.14 ([Har77])**.** *Soit $\mathbb{K}$ un corps algébriquement clos et $car(\mathbb{K}) \neq 2$.*

1. *Pour toute courbe elliptique C sur $\mathbb{K}$, le j-invariant dépend seulement de C et pas de la forme de Legendre choisie.*
2. *Deux courbes elliptiques C et C' sont isomorphes si et seulement si $j(C) = j(C')$.*
3. *Le j-invariant, vu comme une fonction des courbes elliptiques sur $\mathbb{K}$ vers $\mathbb{K}$, est surjective.*

   Il y a alors une bijection par le j-invariant entre l'ensemble des courbes elliptiques sur $\mathbb{K}$ et les éléments de $\mathbb{K}$.

Démonstration. Nous allons utiliser le lemme suivant.

Lemme I.15. *Soit $\mathfrak{S}^3$ le groupe symétrique d'ordre 6. Le groupe $\mathfrak{S}^3$ agit sur $\mathbb{K}\backslash\{0,1\}$ de la manière suivante :*

$$\begin{aligned}\mathfrak{S}^3 \times \mathbb{K}\backslash\{0,1\} &\to \mathbb{K}\backslash\{0,1\} \\ (\sigma,\lambda) &\mapsto \sigma(\lambda) \in \{\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}\end{aligned}$$

et qu'on ait $\sigma(a) = 0$ et $\sigma(b) = 1$ pour $a, b \in \mathbb{K}\backslash\{0,1\}$.

Démonstration. La transformation linéaire, vue dans l'introduction de la section,

$$x \mapsto \frac{x-a}{b-a}$$

envoie a sur 0 et b sur 1. Il suffit d'appliquer la transformation linéaire en $\{0,1,\lambda\}$ lorsque $a, b \in \{0,1,\lambda\}$ pour obtenir les orbites de λ. □

1. et 2. Soit C une courbe elliptique de la forme de Legendre : $y^2 = x(x-1)(x-\lambda)$. Appliquons le changement de variables $(x,y) \mapsto (1-x, iy)$, nous obtenons :

   $$y^2 = x(x-1)(x-(1-\lambda)).$$

   De même, avec la transformation $(x,y) \mapsto (\lambda x, \lambda^{3/2} y)$ à la courbe initiale, nous avons :

   $$y^2 = x(x-1)\Big(x - \frac{1}{\lambda}\Big).$$

Ces deux changements de variables engendrent un groupe d'ordre 6 non abélien donc isomorphe à $\mathfrak{S}^3$. On retrouve alors les deux orbites de l'action définie dans le lemme I.15. Deux courbes elliptiques de paramètres de Legendre λ et λ' respectivement sont isomorphes si les trois points d'ordre 2 sont préservés donc il existe $\sigma \in \mathfrak{S}^3$ tel que $\sigma(\lambda) = \lambda'$. Comme deux éléments engendrent $\mathfrak{S}^3$, il suffit de regarder si $j(\lambda) = j(1-\lambda) = j\left(\frac{1}{\lambda}\right)$ ce qui évident par des calculs élémentaires.
Maintenant, prouvons le sens indirect. Regardons j comme la fonction

$$\begin{aligned} j : \mathbb{P}^1(\mathbb{K}) &\to \mathbb{P}^1(\mathbb{K}) \\ (\lambda : 1) &\mapsto (j(\lambda) : 1) \end{aligned}$$

On a alors :

$$\begin{aligned} (j(\lambda) : 1) &= \left(2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} : 1\right) = (2^8(\lambda^2-\lambda+1)^3 : \lambda^2(\lambda-1)^2) \\ &= (X : Y) \end{aligned}$$

C'est-à-dire $Y2^8(\lambda^2-\lambda+1)^3 - X\lambda^2(\lambda-1)^2 = 0$ d'où $\lambda \mapsto j$ est un morphisme $\mathbb{P}^1(\mathbb{K}) \to \mathbb{P}^1(\mathbb{K})$ de degré 6. Avec des outils de la théorie de Galois, on peut montrer que si $j(\lambda) = j(\lambda')$ alors il existe $\sigma \in \mathfrak{S}^3$ tel que $\sigma(\lambda) = \lambda'$. Ainsi les deux courbes sont isomorphes.

2. Soient $j \in \mathbb{K}$ et λ une racine de l'équation

$$2^8(\lambda^2-\lambda+1)^3 - j\lambda^2(\lambda-1)^2 = 0$$

Alors $C : y^2 = x(x-1)(x-\lambda)$ est une courbe elliptique dont j est son invariant.

□

Corollaire I.16 ([Har77]). *Soit C une courbe elliptique sur un corps $\mathbb{K}$. Soient $P \in C$ et $Aut(C,P)$ le groupe des automorphismes de C laissant P fixe. Alors $Aut(C,P)$ est un groupe d'ordre*

2	*si* $j \neq 0, 1728$;
4	*si* $j = 1728$; *et* $car(\mathbb{K}) \neq 2, 3$;
6	*si* $j = 0$ *et* $car(\mathbb{K}) \neq 2, 3$;
12	*si* $j = 0 = 1728$; *et* $car(\mathbb{K}) = 3$;
24	*si* $j = 0 = 1728$ *et* $car(\mathbb{K}) = 2$;

Remarque I.17. *Le j-invariant d'une courbe elliptique donnée par la forme de Weierstrass $y^2 = x^3 + ax + b$ est*

$$j = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

II Théorème de Mordell

Nous consacrons une section à part entière sur le théorème principal de ce mémoire : le théorème de Mordell. La conjecture a été énoncé par Henri Poincaré en 1901 et a été démontré par Louis Mordell en 1922. En 1928, André Weil, dans sa thèse, étend le résultat avec les variétés abéliennes définies sur un corps de nombre. Cette généralisation est dénommée théorème de **Mordell-Weil**.
L'utilisation du corps $\mathbb{Q}$ permet une démonstration qui demande peu de prérequis pour le lecteur et sa structure est identique à celui de Mordell-Weil. La démonstration est basée sur quatre lemmes et l'utilisation de la méthode de la descente infinie de Fermat. Le lecteur pourra éviter les détails de la démonstration mais devra être attentif à sa structure. Énonçons maintenant le théorème.

II.1 Preuve

Théorème II.1 ([Mor22]). *Soit C une courbe elliptique définie par l'équation*

$$C : y^2 = x^3 + ax^2 + bx \tag{1}$$

avec $a, b \in \mathbb{N}$. Alors $(C(\mathbb{Q}), +)$ est un groupe abélien de type fini.

Démonstration. Nous allons commencer par la fin en démontrant le théorème de la "descente".

Théorème II.2 (Descente). *Soit Γ un groupe commutatif et soit la fonction*

$$h : \Gamma \to [0, \infty]$$

vérifiant les propriétés suivantes :

1. *Pour tout $M \in \mathbb{R}$, $\{P \in \Gamma : h(P) \leqslant M\}$ est fini*
2. *Pour tout $P_0 \in \Gamma$, il existe κ_0 tel que*

$$\forall P \in \Gamma, \quad h(P + P_0) \leqslant 2h(P) + \kappa_0.$$

3. *Il existe une constante κ telle que :*

$$\forall P \in \Gamma, \quad h(2P) \geqslant 4h(P) - \kappa.$$

4. *L'indice $|\Gamma : 2\Gamma|$ est fini.*

Alors Γ est de type fini.

Démonstration. D'après 4), il existe un nombre fini de représentants de classe de $\Gamma/2\Gamma$ qu'on note $Q_1, Q_2, ..., Q_n$. Cela signifie que pour tout $P \in \Gamma$, il existe un indice i_1, dépendant de P, tel que $P - Q_{i_1} \in 2\Gamma$. On peut alors noter $P - Q_{i_1} = 2P_1$ pour $P_1 \in \Gamma$. En procédant de même, on peut écrire :

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

où $Q_{i_1}, ..., Q_{i_m}$ sont choisis parmi les représentants $Q_1, ..., Q_n$ et $P_1, ..., P_m \in \Gamma$. En substituant la j-ème ligne dans la $j-1$ ème ligne, et par une rapide récurrence, nous obtenons :

$$P = Q_{i_1} + 2Q_{i_2} + ... + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Nous allons appliquer la méthode de descente infinie dans le but de contrôler P_m par la hauteur. Par 2), $h(P - Q_i) \leqslant 2h(P) + \kappa_i \leqslant 2h(P) + \kappa'$ pour tout $P \in \Gamma$ et $\kappa' = \max_{1 \leqslant j \leqslant n} k_j$. Par 3), pour tout $j \in [\![1, n]\!]$

$$4h(P_j) \leqslant h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leqslant 2h(P_{j-1}) + \kappa' + \kappa$$

$$h(P_j) \leqslant \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa))$$

Si $h(P_{j-1}) \geqslant \kappa' + \kappa$ alors $h(P_j) \leqslant \frac{3}{4}h(P_{j-1})$. Tant que la condition $h(P_{j-1}) \geqslant \kappa' + \kappa$ est vraie, le prochain point dans la suite $P_1, ..., P_n$ possède une hauteur plus petite. Il existe un indice m tel que $h(P_m) \leqslant \kappa' + \kappa$. Ainsi, l'ensemble

$$\{Q_1, Q_2, ..., Q_n\} \cup \{P \in \Gamma; h(P) \leqslant \kappa' + \kappa\}$$

engendre Γ. Par 1) et 4), l'ensemble est fini d'où Γ est de type fini. □

Introduisons la notion de "complexité arithmétique d'un nombre". Une idée simple est de comparer $\frac{1}{2}$ et $\frac{9999}{20000}$, qui sont deux nombres proches et pourtant l'un est plus "complexe" que l'autre.

Définition II.3. *1. Soit $t \in \mathbb{Q}$ et $t = p/q$ avec $pgcd(p, q) = 1$.*
*La **hauteur** $H(t)$ de t est définie par*

$$H(t) = \max\{|p|, |q|\}$$

*2. La **hauteur** sur $C(\mathbb{Q})$ est la fonction*

$$h : C(\mathbb{Q}) \to \mathbb{R}$$

$$h(P(x, y)) = log(H(x))$$

Remarque II.4. *La hauteur peut être généralisée sur un corps de nombre via la notion de valuation.*

La hauteur et $(C(\mathbb{Q}), +)$ seront la fonction et le groupe commutatif respectivement dans le théorème de la descente. Les quatre hypothèses sur h sont démontrées ci-dessous et ainsi le théorème de Mordell sera démontré. Pour les trois futures lemmes, la courbe C est supposée être de la forme suivante : $y^2 = x^3 + ax^2 + bx + c$ avec $a, b, c \in \mathbb{N}$.

Lemme II.5. *L'ensemble des points rationnels, dont la hauteur est plus petit qu'un nombre fixé, est un ensemble fini i.e pour tout $M \in \mathbb{R}, \{P \in \Gamma : h(P) \leqslant M\}$ est fini.*

Démonstration. Si $x = \frac{m}{n}$ est plus petite qu'une constante, alors $|m|$ et $|n|$ sont plus petites que cette constante donc il existe un nombre fini de possibilités pour m et n. □

Lemme II.6. *Pour tout $P_0 \in \Gamma$, il existe κ_0 (dépendant de P_0, a, b, c) tel que*

$$\forall P \in \Gamma, \quad h(P + P_0) \leqslant 2h(P) + \kappa_0.$$

Démonstration. Par des opérations élémentaires, on peut montrer que chaque point rationnel $P = (x, y)$ peut être mis sous la forme suivante :

$$x = \frac{m}{e^2} \qquad y = \frac{n}{e^3} \qquad e, m, n \in \mathbb{N}^*$$

avec $\text{pgcd}(e, m) = 1$ et $\text{pgcd}(e, n) = 1$.
En la mettant dans l'équation de la courbe C, on a :

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6.$$

En utilisant le fait que : $|m| \leqslant H(P)$ et $e^2 \leqslant H(P)$ et par l'inégalité triangulaire, on a :

$$|n^2| \leqslant KH(P)^3 \qquad K = \sqrt{1+|a|+|b|+|c|}.$$

Supposons que $P = (x,y) \notin \{P_0, -P_0, \mathcal{O}\}$ avec $P_0 = (x_0, y_0)$ et que $P + P_0 = (\xi, \eta)$. En effet, on peut démontrer le lemme pour tout point P excepté un nombre fini. Dans ce cas, il suffit de prendre κ_0 plus grand que le nombre de points exemptés.
La formule de duplication nous donne :

$$\begin{aligned} \xi + x + x_0 &= \Big(\frac{y-y_0}{x-x_0}\Big)^2 - a \\ \iff \xi &= \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4} \end{aligned}$$

avec $A, B, C, D, E, F, G \in \mathbb{N}$. D'où $H(\xi) \leqslant \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}$ Par les inégalités obtenues précédemment, on a

$$H(P + P_0) = H(\xi) \leqslant \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\} H(P)^2.$$

En appliquant la fonction logarithme, on a bien le résultat avec $\kappa_0 = \log(\max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\})$ □

Lemme II.7. *Il existe une constante κ(dépendant de a, b, c) tel que :*

$$\forall P \in \Gamma \quad h(2P) \geqslant 4h(P) - \kappa.$$

Démonstration. Soit $P = (x, y)$ un point qui n'est pas d'ordre 2 et $2P = (\xi, \eta)$. Par la formule de duplication,

$$\xi + 2x = \Big(\frac{f'(x)}{2y}\Big)^2 - a$$

$$\xi = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + ...}{4x^3 + ...}$$

ξ est le quotient de deux polynômes qui n'ont aucune racine complexe commune car C est non-singulière.
Comme $h(P) = h(x)$ et $h(2P) = h(\xi)$, nous allons prouver

$$h(\xi) \leqslant 4h(x) - \kappa$$

Sous-lemme II.8. *Soient ϕ et ψ deux polynômes à coefficients entiers et avec aucune racine complexe commune et $d = \max(\deg(\phi), \deg(\psi))$.*

i) Il existe un entier $R \geqslant 1$ dépendant de ϕ et ψ tel que, pour tout rationnel m/n,

$$pgcd\Big(n^d\phi\Big(\frac{m}{n}\Big), n^d\psi\Big(\frac{m}{n}\Big)\Big) \mid R.$$

ii) Il existe de constantes κ_1 et κ_2 (dépendant de ϕ et ψ) telles que, pour tout rationnel m/n,

$$dh\Big(\frac{m}{n}\Big) - \kappa_1 \leqslant h\Big(\frac{\phi(m/n)}{\psi(m/n)}\Big).$$

Démonstration. Posons $\deg(\phi) = d$ et $\deg(\psi) = e \leqslant d$. On peut écrire

$$\begin{aligned} n^d\phi\Big(\frac{m}{n}\Big) &= a_0m^d + a_1m^{d-1}n + ... + a_dn^d \\ n^d\psi\Big(\frac{m}{n}\Big) &= b_0m^en^{d-e} + b_1m^{e-1}n^{d-e-1} + ... + b_en^d. \end{aligned}$$

On va poser $\Phi(m,n) = n^d\phi\Big(\frac{m}{n}\Big)$ et $\Psi(m,n) = n^d\psi\Big(\frac{m}{n}\Big)$ Comme ψ et ϕ n'ont pas de racines communes, ils sont premiers dans l'anneau euclidien $\mathbb{Q}[X]$. Il existe alors deux polynômes F et G de $\mathbb{Q}[X]$ tels que

$$F(X)\phi(X) + G(X)\psi(X) = 1$$

Soit A un entier tel que $AG(X)$ et $AF(X)$ soient à coefficients entiers.
Soit $D = \max(\deg(F), \deg(G))$. En évaluant en $X = m/n$,

$$n^D AF\Big(\frac{m}{n}\Big) \times n^d\phi\Big(\frac{m}{n}\Big) + n^D AG\Big(\frac{m}{n}\Big) \times n^d\psi\Big(\frac{m}{n}\Big) = An^{D+d}$$

d'où $\gamma = \text{pgcd}(\Phi(m,n), \Psi(m,n)) \mid An^{D+d}$. Comme γ divise $\Phi(m,n)$, γ divise aussi :

$$An^{D+d-1}\Phi(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + ... + Aa_dn^{D+2d-1}.$$

Chaque terme contient An^{D+d} et on vient de prouver que γ divise An^{D+d}. Alors γ divise $Aa_0m^dn^{D+d-1}$. Ensuite

$$\gamma \quad \text{divise} \quad \text{pgcd}(Aa_0m^dn^{D+d-1}, An^{D+d}).$$

Comme m et n sont premiers entre eux, γ divise $Aa_0m^dn^{D+d-1}$. En utilisant le fait que γ divise $Aa_0m^dn^{D+d-2}\Phi(m,n)$ et en répétant les mêmes arguments, γ divise $Aa_0^2m^dn^{D+d-2}$. Par récurrence, on arrive à la conclusion suivante : γ divise Aa_0^{d+D}, ce qui montre *i)*.
Pour *ii)*, en continuant avec les notations de *i)*,

$$\xi = \frac{\phi\Big(\frac{m}{n}\Big)}{\psi\Big(\frac{m}{n}\Big)} = \frac{\Phi(m,n)}{\Psi(m,n)}.$$

D'après *i)*, il existe un entier $R \geqslant 1$ tel que $\text{pgcd}(\Phi(m,n), \Psi(m,n))$ divise R.
On a :

$$\begin{aligned} H(\xi) \geqslant & \frac{1}{R}\max\{|\Phi(m,n)|, |\ \Psi(m,n)|\} \\ \geqslant & \frac{1}{2R}\Big(|n^d\phi\Big(\frac{m}{n}\Big)| + |n^d\psi\Big(\frac{m}{n}\Big)|\Big). \end{aligned}$$

Ce qui équivaut à :

$$\frac{H(\xi)}{H(m/n)^d} \geqslant \frac{1}{2R}\frac{|n^d\phi\Big(\frac{m}{n}\Big)| + |n^d\psi\Big(\frac{m}{n}\Big)|}{\max\{|m|^d, |n|^d\}} = \frac{1}{2R}\frac{|\phi\Big(\frac{m}{n}\Big)| + |\psi\Big(\frac{m}{n}\Big)|}{\max\{|\frac{m}{n}|^d, 1\}}.$$

Considérons la fonction d'une variable réelle :

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\max\{|t^d|, 1\}}.$$

Comme ϕ est de degré d et ψ de degré au moins d, les limites en l'infini de p ne sont pas nulles. Dans un intervalle fermé, p est continue donc atteint ses bornes. Comme la fonction ne s'annule jamais (ϕ et ψ n'ont pas de racines communes), il existe une constante $C_1 > 0$ telle que $p(t) \geqslant C_1$ pour tout t. En utilisant l'inégalité précédente, on peut dire :

$$H(\xi) \geqslant \frac{C_1}{2R}H\Big(\frac{m}{n}\Big)^d.$$

Par l'image du logarithme, on arrive au résultat avec $\kappa_1 = \log(2R/C_1)$. □

Le lemme II.7 est un cas particulier du sous-lemme II.8. □

Lemme II.9 (Mordell-Weil Faible)**.** *L'indice* $|C(\mathbb{Q}) : 2C(\mathbb{Q})|$ *est fini.*

Démonstration. Posons $\Gamma = C(\mathbb{Q})$. Soit $C : y^2 = f(x) = x^3 + ax^2 + bx + c$. Supposons que f ait une racine rationnel x_0. Comme f est un polynômes à coefficients entiers, par le théorème de Nagell-Lutz, l'élément x_0 est entier. Par un changement de coordonnées, on peut déplacer le point $(x_0, 0)$ à l'origine. La courbe C est alors de la forme : $y^2 = x^3 + ax^2 + bx$. Soient $T = (0,0)$, $\overline{C} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$ avec $\overline{a} = -2a$ et $\overline{b} = a^2 - 4b$.

Sous-lemme II.10. *On considère les applications suivantes :*

$$\phi((x,y)) = \Big(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\Big) \qquad \psi((\overline{x},\overline{y})) = \Big(\frac{\overline{y}^2}{\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{\overline{x}^2}\Big)$$

et $\phi(\mathcal{O}) = \phi(T) = \overline{\mathcal{O}}$ *et* $\psi(\overline{\mathcal{O}}) = \psi(\overline{T}) = \mathcal{O}$.

1. $\phi : C \to \overline{C}$ *et* $\psi : \overline{C} \to C$ *sont des homomorphismes.*
2. $\psi \circ \phi(P) = 2P$.

Démonstration. 1. Plusieurs cas sont à distinguer. Si l'un des points est $\mathcal{O}$, il n'y a rien à prouver. Si l'un des points est T, en utilisant la loi d'addition, on a pour $P = (x, y)$,

$$P + T = \Big(\frac{b}{x}, -\frac{by}{x^2}\Big).$$

En les remettant dans l'application ϕ, nous obtenons bien : $\phi(P+T) = \phi(P)$. Par un calcul rapide, on obtient que ϕ envoie les inverses sur les inverses. $\phi(-P) = \phi(x,-y) = -\phi(x,y) = -\phi(P)$. Si nous supposons que $P_1+P_2+P_3 = \mathcal{O}$ $(P_1, P_2, P_3 \neq T)$ et en réalisant l'intersection de la droite passant par ces trois points et la courbe, on peut alors montrer que $\phi(P_1)+\phi(P_2)+\phi(P_3) = \overline{\mathcal{O}}$. Ce qui montre que $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$ et donc que ϕ est un homomorphisme En posant $\overline{\overline{C}} : y^2 = x^3 + 4ax^2 + 16bx$, il est clair que $\overline{\overline{C}} \simeq C$. Nous pouvons alors associer $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$ à ψ d'où ψ est un homomorphisme.

2. Le point $2P$ est donné par la formule de duplication vue dans la section précédente. Les calculs de $\psi \circ \phi(P)$ ne sont pas détaillés ici.

□

Sous-lemme II.11. *1.* $\overline{\mathcal{O}} \in \phi(\Gamma)$.

2. $\overline{T} = (0,0) \in \phi(\Gamma)$ *si et seulement si* $\overline{b} = a^2 - 4b$ *est un carré parfait.*
3. $\overline{P} \in \phi(\Gamma)$ *si et seulement si* $\overline{x}$ *est le carré d'un rationnel.*

Démonstration. 1) Trivial par $\phi(\mathcal{O}) = \overline{\mathcal{O}}$.
2) $\overline{T} = (0,0) \in \phi(\Gamma)$ ssi $x(x^2 + ax + b) = 0$ et $x^2 + ax + b$ n'admet qu'une racine rationnelle si et seulement si le discriminant $a^2 - 4b$ est un carré parfait.
3) Si $\overline{P} = (\overline{x}, \overline{y}) \in \phi(\Gamma)$, par la définition de ϕ, $\overline{x} = y^2/x^2$ qui est le carré d'un rationnel. Supposons maintenant que $\overline{x} = \omega^2$ avec $\omega \in \mathbb{Q}$. Comme le noyau de ϕ contient deux éléments, deux points de Γ correspondent au point $\overline{P} = (\overline{x}, \overline{y}) \in \phi(\Gamma)$. Les points $P_i = (x_i, y_i)$ avec $i \in \{1, 2\}$ données par :

$$\begin{cases} x_1 &= \frac{1}{2}\Big(\omega^2 - a + \frac{\overline{y}}{\omega}\Big) \\ y_1 &= x_1\omega \end{cases} \qquad \begin{cases} x_2 &= \frac{1}{2}\Big(\omega^2 - a - \frac{\overline{y}}{\omega}\Big) \\ y_2 &= -x_2\omega \end{cases}$$

sont sur C et $\phi(P_i) = (\overline{x}, \overline{y})$, ce qui conclut la démonstration. □

Sous-lemme II.12. *Soit* $\mathbb{Q}^{*2} = \{p^2; p \in \mathbb{Q}^*\}$.

1. *L'application* $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ *définie par*

$$\alpha(\mathcal{O}) = [1] \quad \alpha(T) = [b] \quad \alpha(x,y) = [x]$$

est un homomorphisme et $\ker(\alpha) = \Psi(\overline{\Gamma})$.

2. *Soient $p_1, p_2, ..., p_t$ les premiers divisant b. Alors :*

$$\Gamma/\psi(\overline{\Gamma}) \cong \alpha(\Gamma) \subset \{p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t}, \epsilon_i = 0, 1\}.$$

3. $|\Gamma : \psi(\overline{\Gamma})| \leqslant 2^{t+1}$.
4. $|\Gamma : 2\Gamma| \leqslant |\Gamma : \psi(\overline{\Gamma})||\overline{\Gamma} : \phi(\Gamma)|$.

Démonstration. 1) Comme $\alpha(-P) = \alpha(x, -y)$, nous avons que :

$$\alpha(-P) = x = \frac{1}{x}x^2 \equiv \frac{1}{x} = \frac{1}{\alpha(P)}[\mathbb{Q}^{*2}]$$

,alors α envoie les inverses sur les inverses. Nous allons procéder de la même manière que le sous-lemme II.10. Supposons que $P_1 + P_2 + P_3 = \mathcal{O}$. En intersectant C avec une droite et en utilisant la formule de Viète, nous obtenons :

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = \nu^2 \equiv 1[\mathbb{Q}^{*2}]$$

ce qui montre le résultat si P_1, P_2, P_3 sont différents de $\mathcal{O}$. Les autres cas ne seront pas traités ici. L'égalité $\ker(\alpha) = \Psi(\overline{\Gamma})$ n'est qu'une conséquence de le sous-lemme II.11.
2) L'isomorphisme est dû au théorème de l'isomorphie. Nous avons vus dans dans lemme II.6 que les points rationnels peuvent être mis sous la forme $x = m/e^2$ et $y = n/e^3$. En substituant dans C, nous obtenons

$$n^2 = m(m^2 + ame^2 + be^4).$$

Comme m et e sont premiers entre eux, $\text{pgcd}(m, m^2 + ame^2 + be^4)$ divise b. Alors m est de la forme $m = \pm(entier)^2 p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t}$ avec $\epsilon_i = 0$ ou 1. Et :

$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t}[\mathbb{Q}^{*2}]$$

ce qui nous montre bien le résultat.
3) C'est une conséquence directe de 2) : $|\Gamma : \psi(\overline{\Gamma})| \leqslant \#\{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t}\} = 2^{t+1}$.
4) Soit $\gamma \in \Gamma$. Soient $\gamma_1, ..., \gamma_n$ des représentants des classes de $\psi(\overline{\Gamma})$ dans Γ. Il existe des γ_i tels que $\gamma - \gamma_i = \psi(\bar{\gamma})$. Soient $\bar{\gamma_1}, ..., \bar{\gamma_n}$ des représentants des classes de $\phi(\Gamma)$ dans $\overline{\Gamma}$. Il existe des $\bar{\gamma_j}$ tels que $\bar{\gamma} - \bar{\gamma_j} = \phi(\gamma')$. On a : $\gamma = \gamma_i + \psi(\bar{\gamma_j} + \phi(\gamma'))$ En utilisant le sous-lemme II.10.2, on a :

$$\gamma = \gamma_i + \psi(\bar{\gamma_j}) + 2\gamma'$$

d'où le résultat. □

De même, $|\overline{\Gamma} : \phi(\Gamma)| < \infty$ et donc par 4), $|\Gamma : 2\Gamma| < \infty$. □

Nous avons prouvé les lemmes II.5,II.6,II.7 et II.9 et le théorème de la descente. La démonstration est ainsi finie. □

Remarque II.13. On peut illustrer le théorème de Mordell en calculant le rang de courbes elliptiques. Malheureusement, le calcul du rang est une tâche difficile, il n'existe pas de méthode générale pour calculer le rang d'une courbe elliptique quelconque. Certains exemples sont présents dans la référence [ST15].

Remarque II.14. Un problème du millénaire est lié aux courbes elliptiques sur $\mathbb{Q}$. La conjecture est ouverte depuis quarante ans.
Un théorème, que nous verrons plus tard, nous renseigne sur le cardinal du groupe sur un corps fini (Voir Théorème III.4 dit théorème de Hasse). Le théorème de Hasse donne l'égalité suivante :

$$\#C(\mathbb{F}_q) = p + 1 - \epsilon_p$$

avec $|\epsilon| \leqslant 2\sqrt{p}$.
Définissons la L-fonction de C comme le produit

$$L(C,s) = \prod_{p \text{ premier}} \left(1 - \frac{\epsilon_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}$$

Nous pouvons maintenant énoncer la conjecture.

Conjecture II.15 (Birch Swinnerton-Dyer)**.** *Soient C une courbe elliptique sur $\mathbb{Q}$, r son rang et $L(C,s)$ sa L-fonction. L'ordre d'annulation de $L(C,s)$ pour $s=1$ est égal au rang de $C(\mathbb{Q})$ i.e*

$$ord\ L(C,1) = r.$$

III Courbes elliptiques sur les corps finis

Tout au long de cette section III, les courbes elliptiques sont définies sur des corps finis $\mathbb{F}_q$ avec q une puissante d'un nombre premier p.

L'étude des courbes elliptiques sur les corps finis a des applications importantes en cryptographie. Cette application est basée sur deux notions que nous définissons tout de suite.

Définition III.1 (DLP). *Le probème du logarithme discret consiste à trouver m telle que $a^m \equiv b[p]$.*

Définition III.2 (ECDLP). *Soient C une courbe elliptique définie sur $\mathbb{F}_q$ et P un point de C. Le problème du logarithme discret (pour la base P) est la résolution de l'équation $mP = Q$ pour $Q \in C$.*

En 1985, Koblitz [Kob87] et Miller [Mil85] ont publié indépendamment des articles sur l'utilisation des courbes elliptiques en cryptographie. La principale raison de l'utilisation des courbes elliptiques en cryptographie est le fait qu'il n'existe pas d'algorithme pour résoudre ECDLP en moins de $O(\sqrt{p})$ étapes. ECDLP apparait alors comme un problème plus difficile que DLP.
Le potentiel des courbes elliptiques dans les années 80 a été très vite remarqué, et étant donné, que Koblitz et Miller n'ont pas breveté leurs idées, une entreprise de cryptographie Certicom a été crée. Les brevets de Certicom empêchent la propagation des courbes elliptiques. Selon B.Schneier [2], Certicom peut prétendre la propriété des courbes elliptiques en cryptographie. Il existe quand même des incertitudes sur quels algorithmes sont libres de droit ou non.
Dans la suite, nous vous proposons les algorithmes les plus utilisés : l'algorithme de Lenstra qui a permis la reconnaisance des courbes elliptiques, les clés de Diffie-Hellman utilisées par tous les navigateurs Internet ou encore les tests de primalités utilisant l'algorithme de Schoof. Il est conseillé de s'intéresser, après la lecture de cette section, à l'algorithme ρ-Pollard ou encore ECDHE avec signature RSA.

III.1 Algorithme de Lenstra

Dans les années 70, la méthode RSA a propulsé la recherche d'algorithmes sur les facteurs d'un nombre. Déjà en 1984, Hendrick Lenstra [Len87] trouve un algorithme qui décompose un entier en utilisant les courbes elliptiques. Il est , aujourd'hui, le troisième algorithme le plus rapide pour trouver un facteur, précédant le crible quadratique et le crible algébrique. Si p est un facteur, le nombre d'opérations est de l'ordre $\exp(\sqrt{(2+\epsilon)\log(p)\log(\log(p))})$. Avant la présentation de l'algorithme de Lenstra, nous allons décrire un algorithme analogue à Lenstra mais qui n'utilise pas les courbes elliptiques : **l'algorithme p-1 de Pollard**. Son nom provient du fait que l'algorithme est efficace lorsque $p-1$ est un produit de nombres premiers avec des puissances petites [3]. L'idée est de calculer $b = a^d \mod n$ avec n l'entier donné, a, d quelconque. Tant que $b-1$ est premier avec n, on choisit d'autres a et d et l'algorithme s'arrête lorsque $\text{pgcd}(b-1, n)$ est différent de 1, i.e on a trouvé un facteur de n.

2. Bruce Schneier (1963-) : un cryptologue américain mondialement reconnu
3. L'algorithme est surtout utilisé pour les nombres friables. Voir *Introduction à la théorie analytique et probabiliste des nombres* de Gérald Tenenbaum

Data: n
Result: p tel que p divise n
$a := 2$ ou un nombre compris entre 2 et $n-2$
k une borne
for d *from* 2 *to* k **do**
  $b := a^d \mod n$
  $p := \text{pgcd}(b-1, n)$
  if $p > 1$ **then**
    return p
  end
end

Algorithm 1: Algorithme p-1 de Pollard

Remarque III.3. *La nomination de $p-1$ vient du fait que le groupe multiplicatif $\mathbb{F}_p^*$ est d'ordre $p-1$. Par conséquent, n et $a^{d!}-1$ partagent un facteur commun de p dès que $p-1$ divise $d!$.*

Un théorème important des courbes elliptiques sur les corps finis est **le théorème de Hasse** conjecturé par Emil Artin en 1924 et démontré par Hasse en 1936 [Has36].

Théorème III.4 (Hasse)**.** *Soit C une courbe elliptique définie sur $\mathbb{F}_q$. Alors*

$$|\#C(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q}.$$

La preuve est identique à celle de l'inégalité de Cauchy-Schwarz. Voir [Sil09] pour la démonstration.

Bryan Birch a conjecturé que l'ensemble $\{\#C(\mathbb{F}_q); C \text{ courbe elliptique}\}$ est bien répartie sur l'intervalle $[-2\sqrt{q}+(q+1); 2\sqrt{q}+(q+1)]$. L'idée de Lenstra est qu'on va trouver une courbe elliptique dont le cardinal est un produit de nombres premiers petits.

L'**algorithme de Lenstra** ou **ECM** est alors schématisé ainsi.

Data: n, x_1, y_1, b
Result: p tel que p divise n
$c := y_1^2 - x_1^3 - bx$
Vérifier si $\text{pgcd}(\Delta, n) = 1$ avec $\Delta := 4b^3 + 27c^2$
Si ce n'est pas le cas, return$(\text{pgcd}(\Delta, n))$
k une borne
for d *from* 2 *to* k **do**
  Calculer $Q := dP$ avec $P := (x_1, y_1) \mod n$
  Si l'inverse d'un nombre q modulo n n'existe pas, return $\text{pgcd}(q, n)$.
  Si le calcul arrive à son terme, essayer une nouvelle courbe elliptique et un nouveau point
end

Algorithm 2: Algorithme de Lenstra

Il existe une méthode basique qui permet de calculer dP de manière efficace : l'algorithme **Double-and-Add**.

Data: d, P
Result: dP
Posons $R := P$ et $Q := \mathcal{O}$.
while $n > 0$ **do**
  Si $n \equiv 1[2]$ alors $Q \leftarrow Q + R$
  $Q \leftarrow 2Q$ et $n \leftarrow \lfloor \frac{n}{2} \rfloor$
end
Retournez $Q = nP$.

Algorithm 3: Algorithme Double-and-Add

Le lecteur pourra se reporter à l'annexe pour trouver l'algorithme programmé sur Maple. On choisit une courbe elliptique aléatoirement et on prend, par exemple, $n = M_8 \times M_9$ où M_i est le i-ème nombre de Mersenne premier.

$$M_8 = 2^{31} - 1 = 2147483647 \qquad M_9 = 2^{61} - 1 = 2305843009213693951$$

Nous avons lancé le programme cent fois. Voici le tableau des temps pris par l'algorithme pour ce n. Les données sont en secondes.

23.421	26.921	16.859	96.890	88.296	94.906	3.515	69.703	43.281	24.984
32.406	50.390	21.406	62.062	7.031	58.343	39.625	12.421	69.062	32.781
66.046	27.171	26.593	36.765	73.843	22.187	75.000	36.781	25.921	272.265
55.250	1.343	52.281	154.234	21.296	7.906	17.625	57.828	32.296	40.640
225.375	48.671	22.726	20.328	143.593	7.187	40.046	77.324	35.234	23.640
23.781	21.984	169.484	78.359	56.390	14.406	107.109	16.343	108.140	7.921
29.406	31.328	5.296	66.968	75.359	1.343	105.968	29.390	62.562	144.156
24.984	25.125	68.953	3.390	3.781	17.859	5.703	13.765	20.765	43.656
163.015	44.468	27.125	31.171	26.750	29.125	27.968	98.328	62.593	32.218
16.281	4.343	19.984	4.062	57.484	58.140	30.500	13.921	101.546	35.093

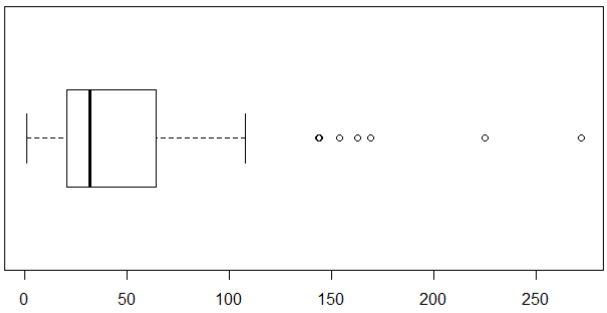


FIGURE 2 – Boîte à moustache

La moyenne est à 48.89487 secondes. Le temps s'étend de 1.3s à 4min30s. Nous remarquons alors que des courbes elliptiques sont plus efficaces que d'autres.

Remarque III.5. *Des courbes elliptiques ont été construites pour qu'elles soient rapides pour certains algorithmes. En voici deux exemples.*

1. *Curve25519 est une courbe elliptique très performante pour le protocole d'échange de clé de Diffie-Hellman. En particulier, c'est une courbe de Montgomery, qu'on verra au prochaine exemple.*
2. *Les courbes de Koblitz sont les courbes sur $\mathbb{F}_{2^k}$ de la forme suivante :*

$$y^2 + xy = x^3 + ax^2 + 1$$

Elles sont très appréciées pour les échanges de Bitcoin.

L'une des courbes elliptiques le plus rapide, pour l'algorithme de Lenstra, est la courbe de **Montgomery**. Elle est de la forme

$$By^2 = x^3 + Ax^2 + x$$

On utilise alors une variante de l'algorithme Double-and-Add : **l'Echelle de Montgomery** [Mon87]. Cet algorithme est applicable à n'importe quelle courbe et peut être exécuté en coordonnées affines et projectives. Cependant, il est utile quand la courbe est de la forme de Montgomery en coordonnées projectives. Dans ce cas, tous les calculs peuvent être menées avec seulement les coordonnées x et z. En effet, les formules de duplication dépendent de x_{P-Q} et z_{P-Q}, et on peut faire en sorte que $P_0 = (x_0 :: z_0) = (x_{P-Q} :: z_{P-Q})$.

Data: $P_0 := (x_0 :: z_0)$ sur C et $k := (k_{s-1}k_{s-2}...k_0)_2$
Result: kP_0
$Q \leftarrow P_0; P \leftarrow 2P_0$
for *i from $s-2$ down to 0* **do**
  if $k_i = 1$ **then**
    $Q \leftarrow P + Q, P \leftarrow 2P$
  end
  if $k_i = 0$ **then**
    $P \leftarrow P + Q, Q \leftarrow 2Q$
  end
end
return Q

Algorithm 4: Echelle de Montgomery

Remarque III.6. La méthode de Lenstra possède plusieurs avantages par rapport aux autres algorithmes de factorisation comme le crible algébrique et quadratique.

1. C'est la méthode la plus rapide si n est divisible par un nombre premier qui est petit par rapport à $\sqrt{n}$. Pour cette raison, elle peut être utilisé en combinaison avec d'autres algorithmes
2. Elle utilise très peu de mémoire par rapport à ses concurrentes.

Voici les différentes complexités des algorithmes présentés et de leurs concurrentes.

Algirithmes	Compléxité
Crible algébrique	$O(\exp((\frac{64}{9}\log(n))^{\frac{1}{3}}\log(\log(n))^{\frac{2}{3}}))$
Crible quadratique	$O(\exp(\sqrt{\log(n)\log(\log(n))}))$
ECM	$O(\exp(\sqrt{(1+\epsilon)\log(n)\log(\log(n))}))$
p-1 Pollard	$O(k\log(k)\log^2(n))$

(ϵ proche de 0 pour p grand et on rappelle que k est une borne.)
L'auteur a tenté $M_8 \times M_9$ avec l'algorithme $p-1$ Pollard et abandonna au bout de 3 heures.

III.2 Clé d'échange de Diffie-Hellman

L'échange de clé de Diffie-Hellman a été révélé en 1976 [DH76]. L'échange d'une clé secrète est important en cryptographie. Effectivement, tout chiffrement d'une grande quantité de données ne peut se faire qu'avec du chiffrement à clé secrète, surtout si cet échange a lieu en temps réel, en raison de la lenteur des chiffrements à clé publique. Il s'agit alors d'échanger entre deux interlocuteurs une clé secrète. Les clés d'échange de Diffie-Hellman sur les courbes elliptiques sont très utilisés de nos jours. Elles proposent des clés plus courtes que celles du RSA et le niveau de sécurité est la même que des ses concurrentes. En effet, une troisième personne doit résoudre ECDLP puiqu'il doit retouver n_A de n_AP. L'échange de Diffie-Hellman est sensible à l'attaque de l'homme du milieu. En effet, si une troisième personne intercepte les communications entre Alice et Bob alors elle peut se faire passer pour Bob ou Alice.

Données publiques
p premier, C courbe elliptique sur $\mathbb{F}_q$ et un point P

Données Privées
Alice et Bob choisissent chacun un nombre entier. (n_A pour Alice et n_B pour Bob).
Alice calcule $Q_A = n_AP$ et envoie Q_A à Bob. Bob calcule $Q_B = n_BP$ et envoie Q_B à Alice.
Alice calcule n_AQ_B Bob calcule n_BQ_A
La clé secrète commune est $n_AQ_B = n_A(n_BP) = n_B(n_AP) = n_BQ_A$.

III.3 Algorithmes de comptage de points

Actuellement, la pensée courante, introduite par Koblitz et Miller, est que pour les courbes elliptique sur les corps finis, la difficulté du logarithme discrète croît exponentiellement avec la taille du plus grand facteur du cardinal du groupe. Le théorème de Hasse nous renseigne sur un intervalle contenant le cardinal. Un algorithme naïf pour le comptage des points est l'algorithme de **Baby-step Giant-step** ou **algorithme de Shanks**. Le principe est de calculer des points dans deux listes jusqu'à leur "collision" i.e un point commun.

La méthode est la suivante :

1. Procédons au *baby-step* : calculer $P, 2P, ..., sP$ avec $s \approx p^{1/4}$.
2. Calculer $Q = (2s+1)P$ et $R = (p+1)P$.
3. Procédons au *giant-step* : calculer $R, R \pm Q, R \pm 2Q, .., R \pm tQ$ avec $t = \frac{2\sqrt{p}}{2s-1} \approx p^{1/4}$.
4. Par le théorème de Hasse, pour $i = 0, \pm 1, \pm 2, ..., \pm t$, $R \pm iQ$ est égal à un des points de la liste du *baby-step*. Pour ce i, $R + iQ = jP$. Alors $\#C(\mathbb{F}_q) = p + 1 + (2s+1)i - j$.

L'inconvénient est que la compléxité est exponentielle. Une percée majeure pour ce problème est l'**algorithme de Schoof** publié par René Schoof en 1985 [Sch95]. C'est le premier algorithme à temps polynomial. Son principe est basée sur la proposition suivante qu'on ne démontera pas.

Proposition III.7. *Soit* $\phi : C(\overline{\mathbb{F}_q}) \to C(\overline{\mathbb{F}_q})$ *définie par*

$$\phi((x, y)) = (x^q, y^q)$$

l'homomorphisme de Frobenius où $\overline{\mathbb{F}_q}$ *est la clôture algébrique de* $\mathbb{F}_q$. *Définissons la trace de* ϕ *par* $tr(\phi) = q + 1 - \#C(\mathbb{F}_q)$.

1. $\phi^2 - (tr(\phi))\phi + q = 0$ *(Ce polynôme est appelé le polynôme caractéristique de Frobenius).*

2. *Pour les points $P = (X, Y)$ d'ordres l finis, on a :*

$$(X^{q^2} + Y^{q^2}) + [q \mod l](X, Y) = [tr(\phi) \mod l](X^q, Y^q)$$

L'algorithme consiste alors à calculer la partie gauche de l'équation pour un point P d'ordre l puis à calculer la partie droite jusqu'à que l'égalité soit vraie. On réitère et par le théorème des restes chinois, on peut trouver $tr(\phi)$.

Remarque III.8. *De nombreuses améliorations ont été réalisés dans les années 90 par Elkies et Atkin [AM93]. L'algorithme est aujourd'hui nommé par **SEA**(Schoof-Elkies-Atkin). Il est implémenté comme un algorithme probabiliste (du type Las Vegas).*

III.4 Tests de Primalité

Les tests de primalité sont primordials pour la cryptographie. L'idée de l'utilisation des courbes elliptiques pour des tests de primalités date de 1986 et a été promue par Shafi Goldwasser et Joe Kilian. L'usage des courbes elliptiques permettent des tests de primalité rapide et peuvent être implémentés. L'algorithme le plus connu est celui de Goldwasser-Killian qui fut amélioré par Atkin et Morin [AM93]. L'algorithme de Goldwasser-Killian est basé sur ce théorème [GK86].

Théorème III.9 (Goldwasser,Kilian)**.** *Soient n un entier premier avec 6, C une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$, P un point de C et s, m deux entiers telles que $s|m$.*
Pour chaque q premier divisant s, posons $(\frac{m}{q})P = (x_q : y_q : z_q)$. Supposons que $mP = \mathcal{O}$ et $pgcd(z_q, n) = 1$ pour chaque q.
Alors il existe p premier divisant n tel que $\#C(\mathbb{F}_p) \equiv 0[s]$.

Corollaire III.10 (Goldwasser,Kilian)**.** *Soient n un entier naturel et C une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$. Supposons qu'il existe $Q \in C(\mathbb{Z}/n\mathbb{Z})$ d'ordre s avec $s > (n^{1/4} + 1)^2$. Alors n est premier.*

Preuve du Corollaire. Soit p un diviseur de n. On a $\#C(\mathbb{Z}/p\mathbb{Z}) > (n^{1/4} + 1)^2$. D'après le théorème de Hasse, $\#C(\mathbb{Z}/p\mathbb{Z}) \leqslant (\sqrt{p} + 1)^2$. D'où

$$(\sqrt{p} + 1)^2 > (n^{1/4} + 1)^2.$$

Ainsi, tout diviseur p de n vérifie $p > \sqrt{n}$. Ainsi n est premier. □

L'algorithme de Goldwasser-Kilian, pour un entier p, consiste à prouver que ce nombre est premier. On peut résumer l'algorithme ainsi :
On veut tester la primalité de n.

1. Choisir une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$ telle que $\#C(\mathbb{Z}/n\mathbb{Z})$ est de la forme $2q$ avec q "premier probablement".
2. Si $(C, \#C(\mathbb{Z}/n\mathbb{Z}))$ satisfait les conditions du théorème III.9 avec $s = \#C(\mathbb{Z}/n\mathbb{Z})$ alors n est premier, sinon n est composé.
3. La primalité de q est faite de la même manière.

IV Courbes elliptiques sur le corps des nombres complexes

Tout au long de cette section IV, les courbes elliptiques sont définis sur le corps des nombres complexes $\mathbb{C}$.
Les courbes elliptiques sur $\mathbb{C}$ possèdent des propriétés intéressantes. Sa richesse provient des nombreux liens réalisés avec d'autres domaines dont l'analyse complexe et surtout l'arithmétique (avec les formes modulaires). Plusieurs notions apparaissent dans cette théorie : les intégrales elliptiques, les fonctions elliptiques, le j-invariant et les formes modulaires. Dans la première partie, nous allons voir les correspondances entre les courbes elliptiques et les tores complexes par les fonctions elliptiques. Ensuite, nous utiliserons les fonctions modulaires pour classifier les courbes elliptiques. Nous allons finir ce mémoire par des courbes elliptiques particulières dites munies d'une multiplication complexe.

IV.1 Fonctions elliptiques

Un sujet classique des courbes elliptiques est la théorie des fonctions elliptiques i.e lesfonctions méromorphes sur $\mathbb{C}$. Historiquement, Niels Abel a découvert ces fonctions comme fonctions réciproques des intégrales elliptiques, le nom provenant du calcul de la longueur d'arc d'une ellipse. Grâce à cette notion, nous pourrons voir que sur $\mathbb{C}$, une courbe elliptique est identifiée à un tore. Tout d'abord, définissons la notion de réseau et de fonction elliptique.

Définition IV.1. *1. Soit $\omega_1, \omega_2 \in \mathbb{C}$ tel que $\frac{\omega_2}{\omega_1} \notin \mathbb{R}$. Un **réseau** Λ du plan complexe est un sous-groupe abélien libre de rang 2. Il peut s'écrire $\Lambda = \{\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\}$.*

*2. Une **fonction elliptique**, pour un réseau Λ, est une fonction méromorphe $f(z)$ d'une variable complexe telle que*

$$\text{pour tout } \omega \in \Lambda, z \in \mathbb{C} \qquad f(z+\omega) = f(z).$$

*On les appelle parfois **fonctions doublement périodiques**. On note $\mathbb{C}(\Lambda)$ l'ensemble de telles fonctions.*

*3. Un **parallélogramme fondamental** pour Λ est l'ensemble*

$$D = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leqslant t_1, t_2 < 1\}$$

où $a \in \mathbb{C}$, $\omega_1, \omega_2 \in \mathbb{C}$ tels que $\frac{\omega_2}{\omega_1} \notin \mathbb{R}$.

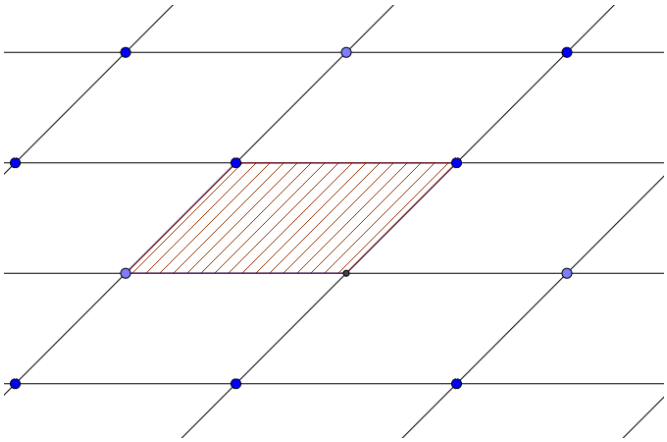


FIGURE 3 – Un réseau avec un parallélogramme fondamental

Rappelons un théorème classique issu de l'analyse complexe. Voir [Cha90] pour une démonstration.

Théorème IV.2 (Théorème de Liouville)**.** *Une fonction holomorphe sur $\mathbb{C}$ et bornée est constante.*

Nous pouvons maintenant démontrer le lemme suivant :

Lemme IV.3 (Liouville[4])**.** *Une fonction elliptique qui n'a aucun pôle est constante.*

Démonstration. Soient f une fonction elliptique sur un réseau Λ n'admettant aucun pôle et D un parallélogramme fondamental. Comme f n'admet aucun pôle, on a

$$\sup_{z\in\mathbb{C}}|f(z)| = \sup_{z\in\overline{D}}|f(z)|.$$

Sachant que f est continue sur un compact $\overline{D}$ alors $|f(z)|$ est bornée sur $\overline{D}$ donc aussi sur $\mathbb{C}$. Par le théorème de Liouville, f est constante. □

Par la suite, on note le résidu de f au point ω $\mathrm{Res}(f,\omega)$ et l'ordre de f en ω est noté $\mathrm{Ord}(f,\omega)$.

Théorème IV.4 ([Sil09])**.** *Soient f une fonction elliptique sur un réseau Λ et D un parallélogramme fondamental. Alors :*

1. $\sum_{\omega\in D} Res(f,\omega) = 0.$
2. $\sum_{\omega\in D} Ord(f,\omega) = 0.$

Démonstration. 1. Posons $a, a+\omega_1, a+\omega_2$ et $a+\omega_1+\omega_2$ les sommets de D. Par le théorème des résidus, nous obtenons

$$\sum_{\omega\in D}\mathrm{Res}(f,\omega) = \frac{1}{2\pi i}\int_{\partial D} f(z)\,\mathrm{d}z = \frac{1}{2\pi i}(I_1+I_2)$$

où

$$I_1 = \int_a^{a+\omega_1} f(z)\,\mathrm{d}z + \int_{a+\omega_2}^{a} f(z)\,\mathrm{d}z \qquad I_2 = \int_{a+\omega_1}^{a+\omega_1+\omega_2} f(z)\,\mathrm{d}z + \int_{a+\omega_1+\omega_2}^{a+\omega_2} f(z)\,\mathrm{d}z.$$

Par changement de variables, il est clair que

$$I_2 = \int_a^{a+\omega_2} f(z+\omega_1)\,\mathrm{d}z + \int_{a+\omega_1}^{a} f(z+\omega_2)\,\mathrm{d}z$$

En réorganisant les termes et comme f est doublement périodique, nous obtenons

$$\begin{aligned}\sum_{\omega\in D}\mathrm{Res}(f,\omega) &= \frac{1}{2\pi i}\Big(\int_a^{a+\omega_1} f(z)-f(z+\omega_2)\,\mathrm{d}z - \int_a^{a+\omega_2} f(z)-f(z+\omega_1)\,\mathrm{d}z\Big)\\ &= 0.\end{aligned}$$

2. Comme f' est périodique par la périodicité de f, on peut appliquer 1) au quotient $f'/f \in \mathbb{C}(\Lambda)$. Nous avons alors

$$\sum_{\omega\in D}\mathrm{Ord}(f,\omega) = \frac{1}{2\pi i}\int_{\partial D}\frac{f'(z)}{f(z)}\,\mathrm{d}z = 0.$$

□

4. Ce lemme est dû à Liouville alors que le théorème IV.2 est dû en réalité à Cauchy.

L'ordre d'une fonction elliptique est la somme des ordres des pôles de tout parallélogramme fondamental. Une conséquence immédiate du théorème est alors :

Corollaire IV.5 ([Sil09]). *Une fonction elliptique non-constante est d'ordre supérieure à 2.*

Démonstration. Supposons, par l'absurde, que f est d'ordre 1. Un de ses résidus doit être non nul, ce qui contredit le théorème précédent. □

Pour illustrer ces notions, étudions une classe importante des fonctions elliptiques : la fonction $\wp$ de Weierstrass.

Définition IV.6. *La fonction $\wp$ de Weierstrass est définie par :*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

où $\Lambda' = \Lambda \setminus \{0\}$.

La convergence est bien définie par le théorème suivant.

Théorème IV.7 ([Sil09]). *Soit Λ un réseau.*

1. *La série de la fonction $\wp$ converge absolument et uniformément sur chaque compact de $\mathbb{C} \setminus \Lambda$. La fonction est alors méromorphe sur $\mathbb{C}$.*
2. *La fonction $\wp$ est une fonction elliptique paire.*

Démonstration. Tout d'abord, démontrons le lemme suivant.

Lemme IV.8 ([Sil09]). *La série G_{2k} définie par*

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda'} \frac{1}{\omega^{2k}}$$

où $\Lambda' = \Lambda \setminus \{0\}$, converge absolument pour $k > 1$. La série G_{2k} est appelé la série d'Eisenstein de poids $2k$.

Démonstration. Comme Λ est discret, il existe une constante c tel que pour tout entier naturel n non nul

$$\#\{\omega \in \Lambda : n \leqslant |\omega| < n+1\} < cn.$$

Par conséquent,

$$\sum_{\substack{\omega \in \Lambda \\ |\omega| \geqslant 1}} \frac{1}{|\omega|^{2k}} \leqslant \sum_{n=1}^{\infty} \frac{\#\{\omega \in \Lambda : n \leqslant |\omega| < n+1\}}{n^{2k}} < \sum_{n=1}^{\infty} \frac{c}{n^{2k-1}} < \infty.$$

□

On revient à la preuve du théorème IV.7.

1. Montrons que la série converge uniformément sur les disques $|z| \leqslant R$. Sachant que le réseau est discret, l'intersection avec les disques est finie et on a $\omega \geqslant 2R$ pour tout ω sauf un nombre fini. Pour $\omega \geqslant 2R$ et z dans le disque de rayon R, on a

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{|z||2 - \frac{z}{\omega}|}{|\omega^3||1 - \frac{z}{\omega}|} \right|.$$

Or $|z| \leqslant R, |2 - \frac{z}{\omega}| \leqslant \frac{5}{2}$ et $|1 - \frac{z}{\omega}| \geqslant \frac{1}{2}$ d'où

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \leqslant \frac{10R}{|\omega|^3}.$$

Par le lemme précédent, nous avons bien le résultat souhaité.

2. En remplaçant ω par $-\omega$, il est clair que $\wp(-z) = \wp(z)$. Comme la série de $\wp$ converge uniformément, la dérivée est bien définie et nous pouvons dériver terme à terme. Nous obtenons

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}. \tag{2}$$

Il est aussi clair que $\wp'$ est une fonction elliptique.
En intégrant (2), on a

$$\wp(z+\omega) - \wp(z) = c(\omega)$$

pour tout $z \in \mathbb{C}\backslash\Lambda$, où $c(\omega) \in \mathbb{C}$ est indépendant de z. En posant $z = \omega/2$, l'équation devient

$$\wp\Big(\frac{\omega}{2}\Big) - \wp\Big(\frac{-\omega}{2}\Big) = c(\omega).$$

Comme la fonction $\wp$ est paire, $c(\omega) = 0$, ce qui conclut la démonstration.

□

Le prochain théorème est crucial, il nous dit que toute fonction elliptique peut être exprimée par la fonction $\wp$ de Weierstrass et ainsi on peut se focaliser sur $\wp$.

Théorème IV.9 ([Sil09])**.** *Soit Λ un réseau de $\mathbb{C}$. Toute fonction elliptique est une fraction rationnelle de $\wp$ et $\wp'$. Autrement dit, $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$.*

Démonstration. Tout d'abord, montrons que toute fonction elliptique paire est une fraction rationnelle de $\wp$. Pour cela, nous utilisons le lemme suivant :

Lemme IV.10. *1. Soient f une fonction paire sur $\mathbb{C}(\Lambda)\backslash\mathbb{C}$ et $a \in \mathbb{C}$ tel que $2a \in \Lambda$. Alors $Ord(f, a)$ est un entier pair.*

2. Pour $a \in \mathbb{C}\backslash\Lambda$, la fonction $h_a : z \mapsto \wp(z) - \wp(a)$ possède un zéro aux points $\pm a$ si $2a \notin \Lambda$, un zéro d'ordre 2 si $2a \in \Lambda$.

Démonstration. 1. Le développement de Taylor de f en a est

$$f(z) = c_m(z-a)^m + c_{m+1}(z-a)^{m+1} + ... \qquad c_m \neq 0.$$

La périodicité de f nous donne

$$f(z) = f(-z+2a) = (-1)^m c_m(z-a)^m + ...$$

d'où $m = \mathrm{Ord}(f, a)$ est pair.

2. Comme $\wp$ (et donc h_a) possède un unique pôle, d'après le théorème IV.4, la somme des ordres des zéros de h_a est égal à l'ordre du pôle i.e 2. Donc si $2a \notin \Lambda$, a et $-a$ sont deux zéros de h_a. D'après 1), si $2a \in \Lambda$, a est d'ordre exactement 2.

□

Soient f une fonction elliptique paire et $a_1, ..., a_s$ les points où $\mathrm{Ord}(f, a_i) \neq 0$ pour tout $i \in \{1, ..., s\}$. Posons $m_i' = \mathrm{Ord}(f, a_i)$ si $2a_i \notin \Lambda$, $m_i' = \mathrm{Ord}(f, a_i)/2$ sinon. Posons

$$g(z) = f(z) \prod_{i=1}^{s} (\wp(z) - \wp(a_i))^{-m_i'}$$

Par le lemme précédent, g ne possède des zéros ou pôles que sur Λ. Par le lemme IV.3, g est constante donc f est une fonction rationnelle de $\wp$.
Maintenant, nous supposons que f est une fonction elliptique quelconque. On peut écrire f sous la forme

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2\wp'(z)} \wp'(z).$$

La fonction f est alors une combinaison de 1 et $\wp'$ dont les coefficients sont des fonctions elliptiques paires. On conclut alors que f est rationnelle de $\wp$ et $\wp'$.

□

Le lien entre les courbes elliptiques et les fonctions elliptiques est réalisé par le fait que $\wp$ est solution d'une équation différentielle. Cette démonstration est basée sur sa série de Laurent.

Théorème IV.11 ([Sil09]). *1. La série de Laurent de $\wp(z)$ autour de $z = 0$ est donnée par*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$$

où G_{2k} est la série d'Eisenstein définie dans le lemme IV.8.

2. $\forall z \in \mathbb{C}\backslash\Lambda$,

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Démonstration. 1. Pour $|z| < |\omega|$, on a

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left[\frac{1}{(1-\frac{z}{\omega})^2} - 1\right] = \sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}}$$

d'où

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda'}\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}}.$$

Comme la série converge absolument et que $G_{2k+1} = 0$ pour $k > 1$, on a bien le résultat.

2. Calculons les premiers termes des séries de Laurent de $\wp(z), \wp'(z)^2$ et $\wp(z)^3$.

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_4z^2 + ...\\ \wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + ...\\ \wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + ...\end{aligned}$$

Posons la fonction

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = \frac{(60G_4)^2}{20}z^2 + \frac{(60G_4)(140G_6)}{28}z^4 + ...$$

La fonction f est holomorphe autour de $z = 0$ et satisfait $f(0) = 0$. Par le théorème IV.7, f est une fonction elliptique sans pôle. Par le lemme IV.3 et comme $f(0) = 0$ alors f est la fonction nulle d'où le résultat.

□

On rappelle qu'une courbe elliptique peut être réduit à une forme de Weierstrass $y^2 = x^3 + ax + b$. Par le changement de variable $y \mapsto \frac{1}{2}y$, on peut se ramener à

$$y^2 = 4x^3 - g_2x - g_3$$

Maintenant, on peut montrer la correspondance entre les tores complexes et les courbes elliptiques.

Théorème IV.12 ([Sil09]). *Soient Λ un réseau, $\wp$ la fonction de Weierstrass et C une courbe elliptique de la forme*

$$y^2 = 4x^3 - g_2x - g_3.$$

L'application

$$\begin{aligned}\Psi : \mathbb{C}/\Lambda \to C \subset \mathbb{P}^2(\mathbb{C}) \qquad & z \mapsto (\wp(z) : \wp'(z) : 1)\\ & 0 \mapsto (0 : 1 : 0)\end{aligned}$$

est une bijection entre le tore complexe $\mathbb{C}/\Lambda$ et la courbe elliptique C.

Démonstration. Montrons, tout d'abord, que Ψ est surjective. Par le théorème IV.11, $\mathrm{Im}(\Psi) \subset C$. Soit $P = (x, y) \in C$. Alors $\wp(z) - x$ est une fonction elliptique non constante donc d'après le lemme IV.3, elle possède un pôle, disons $z = a$. Il s'ensuit que $\wp'(a)^2 = y^2$. Quitte à remplacer a par $-a$ au besoin, nous avons $\Psi'(a) = y$. D'où $\psi(a) = (x, y)$, ce qui démontre la surjectivité.
Supposons maintenant que $\Psi(z_1) = \Psi(z_2)$. Nous distinguons deux cas : supposons que $2z_1 \notin \Lambda$. Alors la fonction $\wp(z) - \wp(z_1)$ est d'ordre 2 et dont les zéros sont $z_1, -z_1$ et z_2. Par conséquent,

$$z_2 \equiv \pm z_1 \mod \Lambda \qquad \text{et} \qquad \wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm \wp'(z_1).$$

Ainsi, $z_2 \equiv z_1 \mod \Lambda$.
De manière similaire, si $2z_1 \notin \Lambda$, $\wp(z) - \wp(z_1)$ a un zéro d'ordre 2 en z_1 et s'annule en z_2. La conclusion est alors la même : $z_2 \equiv z_1 \mod \Lambda$. Ainsi Ψ est injective, et cela conclut la preuve. □

Théorème IV.13 ([Sil09]). *L'application Ψ, définie dans le théorème IV.12,*

$$\begin{aligned} \Psi : \mathbb{C}/\Lambda \to C \subset \mathbb{P}^2(\mathbb{C}) \qquad & z \mapsto (\wp(z) : \wp'(z) : 1)) \\ & 0 \mapsto (0 : 1 : 0) \end{aligned}$$

est un biholomorphisme.

Nous ne démontrerons pas ce résultat, la preuve fait intervenir le groupe d'homologie $H_1(C, \mathbb{Z})$.

Remarque IV.14. Le théorème IV.12 montre qu'à tout réseau Λ de $\mathbb{C}$, on peut associer une courbe elliptique. Le théorème d'uniformisation (que nous verrons dans la section IV.2) est la réciproque. Il nous dit que toute courbe elliptique sur $\mathbb{C}$ est paramétrée par les fonctions elliptiques.

Avant de poursuivre, nous allons définir la notion d'isogénie. Les isogénies seront notamment utilisées dans la section 'Multiplication complexe'.

Définition IV.15.
1. *Soient C_1, C_2 deux courbes elliptiques. Une **isogénie** de C_1 dans C_2 est un morphisme de groupe $\phi : C_1 \to C_2$ préservant l'élément neutre.*
2. *L'**anneau des endomorphismes** d'une courbe elliptique C est l'ensemble $End(C) = \{\phi : C \to C : \phi \text{ isogénie }\} \cup \{0\}$.*

Remarque IV.16. *Généralement, on définit une isogénie comme un morphisme de groupe algébrique qui est surjectif et qui a un noyau fini.*

Exemple IV.17 ([ST15]).
1. Les applications définies dans la sous-lemme II.10 sont des isogénies.

$$\begin{aligned} \phi : C_1 &\to C_2 \\ (x, y) &\to \Big(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\Big) \end{aligned}$$

   La preuve de Mordell-Weil se fait avec des isogénies.
2. Dans la section I.3, nous avons vu l'application

$$\begin{aligned} [n] : C &\to C \\ P &\mapsto nP \end{aligned}$$

   où $n \in \mathbb{Z}$. Cette application est une isogénie.

Pour finir cette partie, on veut montrer une correspondance entre les isogénies, les fonctions holomorphes et les réseaux homothétiques (i.e qui différent d'un élément de $\mathbb{C}^*$, voir IV.19). Soient Λ_1, Λ_2 deux réseaux de $\mathbb{C}$. On peut définir une fonction holomorphe, entre deux tores complexes, $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ par le diagramme suivant :

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow[\phi]{} & \mathbb{C}/\Lambda_2 \end{array}$$

Ce diagramme commute car $\mathbb{C}$ est simplement connexe.

Théorème IV.18 ([Sil09]). *Soient Λ_1, Λ_2 deux réseaux de $\mathbb{C}$. Posons $\mathcal{H}$ l'ensemble des fonctions holomorphes $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ avec $\phi(0) = 0$.*

1. *Soit l'application ϕ_α :*

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \qquad \phi_\alpha(z) = \alpha z \mod \Lambda_2.$$

   L'application

$$\begin{aligned} \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} &\to \mathcal{H} \\ \alpha &\mapsto \phi_\alpha \end{aligned}$$

   est une bijection.

2. *Soient C_1, C_2 deux courbes elliptiques correspondant aux réseaux Λ_1, Λ_2. Il existe une bijection*

$$\psi : \{\phi : C_1 \to C_2 : \phi \ \textit{isogénie}\} \to \mathcal{H}.$$

Démonstration. 1. Supposons que $\phi_\alpha = \phi_\beta$ alors

$$\forall z \in \mathbb{C}, \qquad \alpha z \equiv \beta z \mod \Lambda_2.$$

Par conséquent, l'application $z \mapsto (\alpha - \beta)z$ envoie $\mathbb{C}$ sur Λ_2. Comme Λ_2 est discret, cette application est constante d'où $\alpha = \beta$, l'application est alors injective. Soit $\phi \in \mathcal{H}$. On peut se ramener à une fonction holomorphe f par le diagramme suivant

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow[\phi]{} & \mathbb{C}/\Lambda_2 \end{array}$$

Ce diagramme commute car $\mathbb{C}$ est simplement connexe. Ainsi

$$\forall \omega \in \Lambda_1, \forall z \in \mathbb{C}, \qquad f(z + \omega) \equiv f(z) \mod \Lambda_2.$$

Comme Λ_2 est discret, la quantité $f(z + \omega) - f(\omega)$ est indépendante de z. En dérivant,

$$\forall \omega \in \Lambda_1, \forall z \in \mathbb{C}, \qquad f'(z + \omega) = f'(z)$$

,on trouve alors que $f'(z)$ est une fonction elliptique. Par le lemme IV.3, $f'(z)$ est constante d'où $f(z)$ est un polynôme en z de degré 1. Comme $f(0) = 0$, $f(z)$ est de la forme αz. Ainsi $f(\Lambda_1) = \alpha\Lambda_1 \subset \Lambda_2$ d'où $\phi = \phi_\alpha$, ce qui conclut la première partie.

2. Par définition, une isogénie est un morphisme, l'image par ψ est alors une fonction holomorphe entre les deux tores. L'application ψ est alors bien définie et est clairement injective.
   Pour la surjectivité, nous utilisons la correspondance vue en 1., en considérant

l'application ϕ_α avec $\alpha \in \mathbb{C}^*$ tel que $\alpha\Lambda_1 \subset \Lambda_2$. Par le théorème IV.12, on peut définir l'application suivante

$$C_1 \to C_2$$
$$(\wp(z,\Lambda_1) : \wp'(z,\Lambda_1) : 1) \mapsto (\wp(\alpha z,\Lambda_2) : \wp'(\alpha z,\Lambda_2) : 1)$$

où $\wp(z,\Lambda)$ correspond à la fonction de Weierstrass associée à Λ. En utilisant le théorème IV.9, si $\wp(\alpha z,\Lambda_2)$ et $\wp'(\alpha z,\Lambda_2)$ sont des fractions rationnelles en $\wp(\alpha z,\Lambda_1)$ et $\wp'(\alpha z,\Lambda_1)$ alors le théorème est démontré.
Comme $\alpha\Lambda_1 \subset \Lambda_2$, nous avons, pour tout $\omega_1 \in \Lambda_1$,

$$\wp(\alpha(z+\omega),\Lambda_2) = \wp(\alpha z + \alpha\omega,\Lambda_2) = \wp(\alpha z,\Lambda_2).$$

Il en est de même pour $\wp'(\alpha z,\Lambda_2)$. Ainsi $\wp(\alpha z,\Lambda_2) \in \mathbb{C}(\Lambda_1)$ et $\wp'(\alpha z,\Lambda_2) \in \mathbb{C}(\Lambda_1)$ et le théorème est démontré.

□

Corollaire IV.19 ([Sil09]). *Soient C_1 et C_2 deux courbes elliptiques de réseaux Λ_1, Λ_2 respectivement. Les courbes C_1 et C_2 sont isomorphes si et seulement si il existe $\alpha \in \mathbb{C}^*$ tel que $\Lambda_1 = \alpha\Lambda_2$ (dans ce cas, on dit que Λ_1 et Λ_2 sont homothétiques).*

La preuve est admise.

Remarque IV.20 ([LC72]). Posons $\wp(z) = w$, nous écrivons l'équation sous la forme

$$\frac{dz}{dw} = \frac{1}{\sqrt{4w^3 - 4g_2 - g_3}}$$

d'où nous concluons que $\wp(z)$ est la fonction inverse de l'intégrale

$$z - z_0 = \int_{\wp(z_0)}^{w} \frac{dw}{\sqrt{4w^3 - 4g_2 - g_3}}.$$

En faisant tendre z_0 vers 0, nous obtenons l'intégrale elliptique sous forme de Weierstrass

$$z = \int_{\infty}^{w} \frac{dw}{\sqrt{4w^3 - 4g_2 - g_3}}$$

dont l'inverse est la fonction $\wp$.
Historiquement, la notion de fonction elliptique provient des études sur les intégrales elliptiques et nous venons de voir ce lien. Le nom "elliptique" vient du fait que le calcul de longueur d'arc d'une ellipse donne une intégrale qui est de la forme vue précédemment.

IV.2 Groupe modulaire

Rappelons que le groupe $\mathrm{SL}_2(\mathbb{Z})$ est défini par

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z} \text{ et } ad - bc = 1 \right\}.$$

et on appelle **groupe modulaire** le groupe $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{Id}_2\}$.
Comme nous travaillons sur $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ à homothétie près, on peut normaliser la base du réseau

$$\frac{1}{\omega_2}\Lambda = \mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}.$$

On peut alors choisir $\omega_1, \omega_2 \in \mathbb{C}$ tel que $\Im(\omega_1/\omega_2) > 0$, ce qui nous suggère de travailler sur le demi-plan supérieur $\mathbb{H} = \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$ de $\mathbb{C}$. Le but de cette

section est démontrer que pour $\tau, \tau' \in \mathbb{H}$, $C_\tau \cong \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ et $C_{\tau'} \cong \mathbb{C}/(\mathbb{Z}+\tau'\mathbb{Z})$ sont isomorphes si et seulement si il existe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $\tau' = \frac{a\tau+b}{c\tau+d}$. On peut résumer cette section IV.2 de ce mémoire par le schéma suivant :

$$\begin{array}{ccccccc} \mathcal{ERR}_{\mathbb{C}} & \xleftarrow{\text{IV.28}} & \mathscr{R}/\mathbb{C}^* & \xleftarrow{\text{IV.28}} & \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) & \xrightarrow{\text{IV.27}} & \mathbb{C} \\ \{C_\Lambda\} & \longleftarrow & \{\Lambda\} = \{\Lambda_\tau\} & \longleftarrow & \tau & \longrightarrow & j(\tau) \end{array}$$

où $\mathcal{ERR}_{\mathbb{C}}$ est l'ensemble des classes d'isomorphisme des courbes elliptiques et $\Lambda_\tau = \mathbb{Z}+\tau\mathbb{Z}$.
Pour démontrer cela, on va décrire l'action de groupe de $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$ (qui sera définie dans la proposition IV.22) et on va utiliser les fonctions modulaires pour démontrer le théorème d'uniformisation vu dans la remarque IV.14.

Définition IV.21. *Soient G un groupe et X un ensemble sur lequel G agit. On note $g.x$ l'image de $x \in X$ par l'action de l'élément $g \in G$. Un sous-ensemble Y de X est un **domaine fondamental** si :*

1. $\bigcup_{g\in G} g.Y = X$.
2. $\forall g, g' \in G$ *tels que* $g \neq g'$, $g.Y \cap g'.Y = \emptyset$.

Le domaine fondamental contient alors exactement un point par orbite du groupe.

Proposition IV.22 ([Ser95])**.** *Avec les notations ci-dessus, on a :*

1. *Le groupe $SL_2(\mathbb{Z})$ agit sur $\mathbb{H}$ par*

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \forall \tau \in \mathbb{H}, \qquad \gamma.\tau = \frac{a\tau+b}{c\tau+d}.$$

   Le groupe modulaire $PSL_2(\mathbb{Z})$ agit de la même manière sur $\mathbb{H}$. Le lemme IV.23 montre que l'action du groupe modulaire sur $\mathbb{H}$ est fidèle.
2. *Posons $\mathcal{F}' = \{\tau \in \mathbb{H} : |\Re(\tau)| \leqslant \frac{1}{2} \ \ et \ \ |\tau| \geqslant 1\}$. La région $\mathcal{F}$ de $\mathbb{H}$ définie par*

$$\mathcal{F} = \mathcal{F}' \setminus \Big(\{\tau \in \mathcal{F} : \Re(\tau) = \frac{1}{2}\} \cup \{\tau \in \mathcal{F} : (|\tau| = 1 \ \ et \ \ \Re(\tau) > 0)\} \Big)$$

   est un domaine fondamental pour l'action de groupe de $SL_2(\mathbb{Z})$ sur $\mathbb{H}$.
3. *Le groupe modulaire $PSL_2(\mathbb{Z})$ est engendré par S et T où $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, ce qui équivaut à $S.\tau = -1/\tau$, $T.\tau = \tau + 1$.*

Démonstration. On pose $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

1. Posons $\tau = s + it \in \mathbb{H}$. En multipliant le numérateur et le dénominateur du quotient $\gamma\tau$ par $c\overline{\tau}$, nous trouvons

$$\frac{a\tau+b}{c\tau+d} = \frac{ac|\tau|^2 + (ad+bc)s + bd + (ad-bc)it}{|c\tau+d|^2}.$$

   Nous avons alors

$$\Im\Big(\frac{a\tau+b}{c\tau+d}\Big) = \frac{(ad-bc)\Im(\tau)}{|c\tau+d|^2} = \frac{\Im(\tau)}{|c\tau+d|^2} \tag{3}$$

   qui est positive par la définition de $\mathbb{H}$. L'application est alors bien définie. On ne détaille pas ici les calculs pour montrer que c'est une action de groupe.

   Les points a et b du lemme suivant montrent le point 2 du théorème et le point c démontre le point 3.

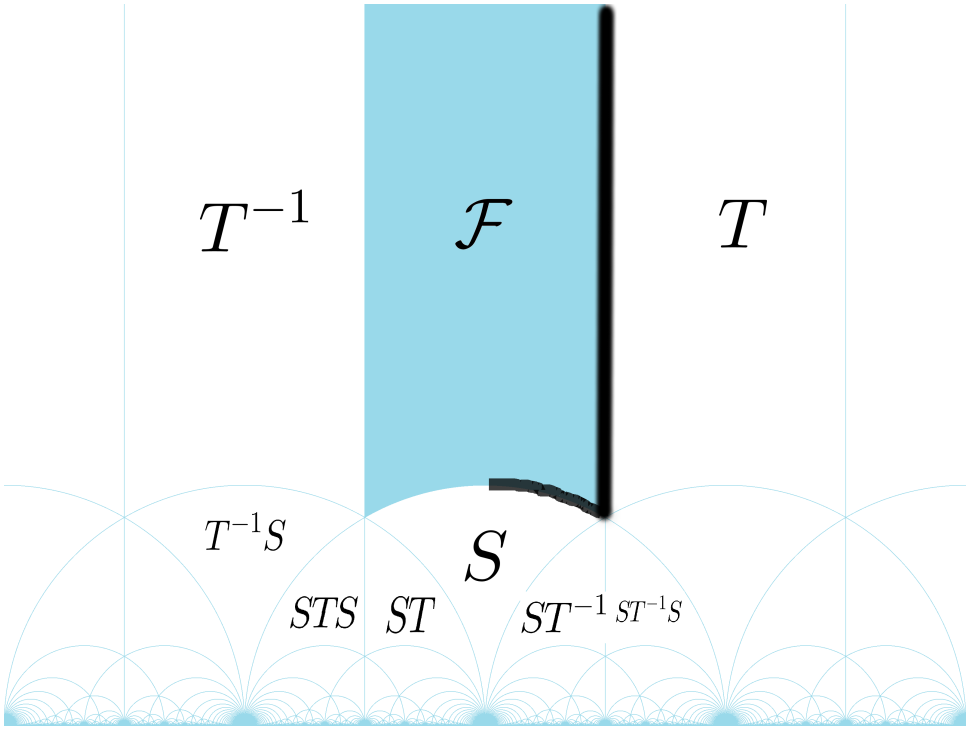


FIGURE 4 – Domaine fondamental $\mathcal{F}$ du groupe modulaire et des images de $\mathcal{F}$ pour certains éléments de $\mathrm{PSL}_2(\mathbb{Z})$. (Image de Arnaud Chéritat avec son autorisation)

Lemme IV.23 ([Che15]). *(a) Pour tout $\tau \in \mathbb{H}$, l'orbite $\Gamma.\tau$ rencontre $\mathcal{F}'$.*

(b) Si τ et τ' deux points distincts de $\mathcal{F}'$ tels que $\Gamma.\tau = \Gamma.\tau'$ alors on a :

- *soit $\Re(\tau) = \pm\frac{1}{2}$ et $\tau = \tau' \pm 1$,*
- *soit $|\tau| = 1$ et $\tau' = -\frac{1}{\tau}$.*

(c) Si $\tau \in \mathcal{F}'$ alors le stabilisateur de τ dans Γ est $\{\pm 1\}$ sauf dans le cas où $\tau = i$ (resp. $\tau = e^{2i\pi/3}$ et $\tau = e^{i\pi/3}$) auquel cas le stabilisateur est engendré par S (resp. ST).

Démonstration. (a) Soit $\tau \in \mathbb{H}$. La forme quadratique $q : \mathbb{R}^2 \to \mathbb{R}$, $(c,d) \mapsto |c\tau+d|^2$ est définie positive, alors q admet un minimum sur $\mathbb{Z}^2\backslash\{0\}$. D'après l'égalité (3), on peut considérer l'ensemble $A = \{\tau' \in \mathbb{H} : \Im(\tau') \text{ maximal}\} \subset \Gamma.\tau$. L'ensemble A est invariant par T de sorte qu'il existe $\tau' \in A$ tel que $|\Re(\tau')| \leqslant \frac{1}{2}$. Mais $-1/\tau' \in \Gamma.\tau$ et $\Im(-1/\tau') = \frac{\Im(\tau')}{|\tau'|^2}$ donc $|\tau'| \leqslant 1$. D'où $\tau' \in \Gamma.\tau \cap \mathcal{F}'$.

(b) et (c) Soient $\tau, \tau' \in \mathcal{F}'$ tels que $\Im(\tau') \geqslant \Im(\tau)$ et $\tau' = \gamma.\tau$ avec $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Cela implique que $|c\tau+d| \leqslant 1$. Comme $|c\Im(\tau)| \leqslant 1$, alors $|c| \leqslant 1$. Si $c = 0$ alors $a = d = \pm 1$ et donc $\pm\gamma$ est une puissance de T et on est dans le premier cas du lemme IV.23 (*b*). Sinon, on peut supposer que $c = 1$, quitte à remplacer γ par $-\gamma$. Si $|\tau + d| \leqslant 1$ alors $|\tau| = 1$. Les cas possibles sont alors :

i. $\tau \neq e^{2i\pi/3}, e^{i\pi/3}$ et $d = 0$. Dans ce cas, $b = -1$ et $\tau' = a - 1/\tau$ puis $a = 0$ car $|\Re(-1/\tau)| < 1/2$. Ainsi $\gamma = S$ et $\tau' = \tau = i$.

ii. $\tau = e^{2i\pi/3}$ et $d = 0, -1$. Si $d = 0$, on a $b = -1$ et $\tau' = a - e^{-2i\pi/3} = a + e^{i\pi/3}$. On a alors deux cas : soit $\tau' = e^{i\pi/3}, a = 0$ et $\gamma \pm S$, soit $\tau' = \tau, a = -1$ et $\gamma = (ST)^2$.

iii. Pour $\tau = e^{i\pi/3}$ et $d = 0$ et 1, la manière est identique que dans ii.

□

On revient à la démonstration de la proposition IV.22.

2. Les points a et b du lemme IV.23 montrent que pour tout $\tau \in \mathbb{H}$, l'orbite $\Gamma.\tau$ rencontre $\mathcal{F}$ en un unique point d'où $\mathcal{F}$ est un domaine fondamental pour l'action de groupe de Γ sur $\mathbb{H}$.
3. Soient G le groupe engendré par S et T, τ un point de l'intérieur de $\mathcal{F}'$ et $\gamma \in \Gamma$. D'après la démonstration du lemme IV.23 point a, il existe $g \in G$ tel que $g^{-1}\gamma.\tau \in \mathcal{F}'$. Ainsi, $g^{-1}\gamma \in \Gamma$ fixe τ d'où $\tau = \pm 1$ par le lemme IV.23 point c. D'où $\gamma \in G$ car $S^2 = -\mathrm{Id}_2 \in G$.

□

Corollaire IV.24 ([Sil09]). *Tous les réseaux complexes Λ sont homothétiques à $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ pour $\tau \in \mathcal{F}$.*

La preuve est admise.

Définition IV.25. *1. Une fonction méromorphe f sur $\mathbb{H}$ est une **fonction modulaire** de poids k si les deux conditions suivantes sont satisfaites :*

(a) Pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $f(\tau) = (c\tau + d)^{-k} f(\gamma\tau)$.

(b) La série de Fourier de f en $q = e^{2i\pi\tau}$ est de la forme

$$f(\tau) = \sum_{n=n_0}^{\infty} c(n) q^n$$

pour $n_0 \in \mathbb{Z}$.

*2. Une fonction modulaire f est une **forme modulaire** de poids k si f est holomorphe sur $\mathbb{H}$ et $n_0 = 0$.*

Avec les fonctions modulaires, nous pouvons démontrer le théorème d'uniformisation évoqué dans la remarque IV.14.

Théorème IV.26 (Uniformisation [Sil94]). *Soit C une courbe elliptique de la forme de Weierstrass $y^2 = x^3 + ax + b$ telle que $4a^3 + 27b^2 \neq 0$. Il existe alors un unique réseau Λ telle que $g_2(\Lambda) = 60G_4(\Lambda) = -4a$, $g_3(\Lambda) = 140G_6(\Lambda) = -4b$ et donc une bijection $\mathbb{C}/\Lambda \to C$.*

Démonstration. Nous utiliserons le lemme suivant.

Lemme IV.27 (admis). *Le j-invariant, défini dans la section I.4, est une fonction modulaire de poids 0 qui induit un isomorphisme entre $\mathbb{H}/PSL_2(\mathbb{Z})$ et $\mathbb{C}$.*

D'après l'identification vue dans le lemme IV.27 et la remarque de la section "j-invariant", on peut choisir $\tau \in \mathbb{H}$ tel que

$$j(\tau) = 1728\frac{4a^3}{4a^3 + 27b^2} = -1728\frac{g_2(\tau)^3}{-g_2(\tau)^3 + 27g_3(\tau)^2}.$$

Ce qui revient aux égalités suivantes :

$$\frac{27b^2}{4a^3} = \frac{1728}{j(\tau)} - 1 = -\frac{27g_3(\tau)^2}{g_2(\tau)^3}$$
$$\left(\frac{b}{g_3(\tau)}\right)^2 \left(\frac{g_2(\tau)}{a}\right)^3 = -4.$$

Posons

$$\alpha = \sqrt{\frac{ag_3(\tau)}{bg_2(\tau)}}$$

et $\Lambda = \alpha\Lambda_\tau = \alpha\tau\mathbb{Z} + \alpha\mathbb{Z}$. Alors

$$g_2(\Lambda) = \frac{g_2(\Lambda_\tau)}{\alpha^4} = \frac{b^2 g_2(\tau)^3}{a^2 g_3(\tau)^2} = -4a$$
$$g_3(\Lambda) = \frac{g_3(\Lambda_\tau)}{\alpha^6} = \frac{b^3 g_2(\tau)^3}{a^3 g_3(\tau)^2} = -4b$$

De même, si $a = 0$ alors $j(\tau) = g_2(\tau) = 0$, et si $b = 0$ alors $j(\tau) = 1728$ et $g_3(\tau) = 0$. Dans les deux cas, il suffit de prendre

$$\alpha = \sqrt[6]{\frac{g_3(\tau)}{-4b}} \qquad \text{si } a = 0$$
$$\alpha = \sqrt[4]{\frac{g_2(\tau)}{-4a}} \qquad \text{si } b = 0$$

pour que $\Lambda = \alpha\Lambda_\tau$, ce qui démontre l'existence.
Démontrons l'unicité. Supposons que

$$G_4(\Lambda_1) = G_4(\Lambda_2) \qquad G_6(\Lambda_1) = G_6(\Lambda_2).$$

Remarquons que $j(\Lambda_1) = j(\Lambda_2)$. D'après le théorème I.14, les courbes elliptiques associées aux réseaux Λ_1 et Λ_2 sont isomorphes. D'après le corollaire IV.19, Λ_1 et Λ_2 sont homothétiques i.e il existe $\alpha \in \mathbb{C}$ tel que $\Lambda_1 = \alpha\Lambda_2$. En utilisant l'égalité

$$G_{2k}(\alpha\Lambda) = \sum_{\omega\in\Lambda'} \frac{1}{\alpha^{2k}\omega^{2k}} = \alpha^{-2k} G_{2k}(\Lambda)$$

on a alors, par les hypothèses,

$$G_4(\Lambda_1) = G_4(\alpha\Lambda_2) = \alpha^{-4} G_4(\Lambda_2) = G_4(\Lambda_2)$$

d'où $\alpha^4 = 1$. De même, en utilisant $G_6(\Lambda_1) = G_6(\Lambda_2)$, on a $\alpha^6 = 1$.
On conclut la démonstration avec $\alpha^2 = 1$ i.e $\alpha = \pm 1$ et $\Lambda_1 = \pm\Lambda_2 = \Lambda_2$. □

On a vu que le j-invariant permet de classifier les courbes elliptiques mais il est possible de le faire avec les réseaux du plan.

Théorème IV.28 ([CG17]). *Soit $\mathscr{R}$ l'ensemble des réseaux de $\mathbb{C}$ (c'est-à-dire les sous-groupes de $\mathbb{C}$ isomorphes à $\mathbb{Z}^2$ non contenus dans une droite réelle). On a alors l'équivalence $\mathscr{R}/\mathbb{C}^* \cong \mathbb{H}/SL_2(\mathbb{Z})$ qui permet d'identifier $\mathscr{R}/\mathbb{C}^*$ aux classes d'isomorphisme des courbes elliptiques.*

$$\begin{array}{ccc} \mathscr{R} & \longrightarrow & \mathbb{H} \\ \downarrow & & \downarrow \\ \mathscr{R}/\mathbb{C}^* & \sim & \mathbb{H}/SL_2(\mathbb{Z}) \end{array}$$

Démonstration. On note M l'ensemble des couples $(\omega_1, \omega_2) \in \mathbb{C}^* \times \mathbb{C}^*$ tels que $\Im(\omega_1/\omega_2) > 0$. Soit l'application

$$\pi : M \to \mathbb{H}$$
$$(\omega_1, \omega_2) \mapsto \frac{\omega_1}{\omega_2}$$

D'une part, π est surjective par la définition de $\mathbb{H}$. D'autre part, $\pi(\omega_1, \omega_2) = \pi(\omega_1', \omega_2')$ si et seulement si il existe λ non nul tel que $(\omega_1, \omega_2) = \lambda(\omega_1', \omega_2')$. L'application π induit alors par passage au quotient une bijection $M/\mathbb{C}^* \to \mathbb{H}$.
Posons l'application

$$\Lambda : M \to \mathscr{R}$$
$$(\omega_1, \omega_2) \mapsto \omega_1\mathbb{Z} + \omega_2\mathbb{Z}.$$

L'application Λ est surjective. En effet, prenons un réseau $\omega_1\mathbb{Z}+\omega_2\mathbb{Z}$, quitte à changer ω_2 en $-\omega_2$, on peut supposer que $\Im(\omega_1/\omega_2) \geqslant 0$ d'où la surjectivité. On veut montrer que $M/SL_2(\mathbb{Z}) \cong \mathscr{R}$. On utilise l'action de groupe suivant

$$\mathrm{SL}_2(\mathbb{Z}) \times M \to M$$
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, (\omega_1, \omega_2) \right) \to (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2).$$

Soit $R = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ un réseau avec (ω_1, ω_2). Alors, $(\omega_1', \omega_2') \in \mathbb{Z}^2$ est une base de R si et seulement si il existe $g \in \mathrm{GL}_2(\mathbb{Z})$ tel que $g(\omega_1, \omega_2) = (\omega_1', \omega_2')$. Quitte à changer ω_2' en $-\omega_2'$, on peut supposer $(\omega_1', \omega_2') \in M$. Si $g \in \mathrm{GL}_2$ (de déterminant ± 1 puisque inversible) vérifie $g(\omega_1, \omega_2) = (\omega_1', \omega_2')$ alors le signe de $\Im(\omega_1'/\omega_2')$ est le signe de $\Im(\omega_1/\omega_2)$ fois $\det(g)$. Donc $\det(g) > 0$ d'où $g \in \mathrm{SL}_2(\mathbb{Z})$.
On a alors montré que $(\omega_1', \omega_2') \in \mathbb{Z}^2$ est une base de R si et seulement si il existe $g \in \mathrm{SL}_2(\mathbb{Z})$ tel que $g(\omega_1, \omega_2) = (\omega_1', \omega_2')$. Autrement dit, Λ induit un isomorphisme $M/\mathrm{SL}_2(\mathbb{Z}) \cong \mathscr{R}$. Comme $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{Z})$ agit de façon $\mathbb{C}$-linéaire, les actions de groupes $\mathbb{C}^*$ et $\mathrm{SL}_2(\mathbb{Z})$ sur M commutent. Or on a prouvé que $M/\mathbb{C}^* \cong \mathbb{H}$ d'où

$$(M/\mathrm{SL}_2(\mathbb{Z}))/\mathbb{C}^* = (M/\mathbb{C}^*)/\mathrm{SL}_2(\mathbb{Z})$$

,ce qui nous donne l'isomorphisme $\mathscr{R}/\mathbb{C}^* \cong \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. □

IV.3 Multiplication complexe

Par le théorème IV.18, $\mathrm{End}(C)$ est identifié à l'ensemble $\{\alpha \in \mathbb{C} : \alpha\Lambda = \Lambda\}$. L'anneau $\mathrm{End}(C)$ est alors un sous-anneau de $\mathbb{C}$ d'où $\mathbb{Z} \subset \mathrm{End}(C)$. Nous avons vu la notion d'isogénie dans la section précédente et on sait que chaque courbe elliptique contient l'isogénie multiplicative $[n]$ définie dans la section I.3. Pour la plupart des courbes elliptiques, il n'y a pas d'autres isogénies, mais nous nous intéressons dans cette section aux courbes elliptiques munies d'autres isogénies.

Définition IV.29. *Si C est une courbe elliptique, on dit que C est munie d'une **multiplication complexe** si End(C) est plus grand que $\mathbb{Z}$, i.e il existe un endomorphisme autre que $[n]$.*

Exemple IV.30 ([ST15])**.** Soit C la courbe elliptique suivante : $C : y^2 = x^3 + x$. Elle possède la multiplication complexe

$$\phi(x, y) = (-x, iy).$$

On pourra montrer que $(-x, iy) \in C$ et que $\phi^2(P) = -P$.

Le résultat suivant est le théorème clé de la section : il permet de caractériser la multiplication complexe avec les extensions quadratiques.

Théorème IV.31 ([Har77])**.** *Soit C une courbe elliptique et $\Lambda = \tau\mathbb{Z} + \mathbb{Z}$ son réseau correspondant. Si la courbe C possède une multiplication complexe alors $\tau \in \mathbb{Q}(\sqrt{-d})$ avec $d \in \mathbb{N}^*$. L'anneau End(C) est alors un sous-anneau des entiers de $\mathbb{Q}(\sqrt{-d})$. La réciproque est vraie, si $\tau = r + s\sqrt{-d} \in \mathbb{Q}(\sqrt{-d})$ alors la courbe C est munie une multiplication complexe.*
Dans ce cas,

$$End(C) = \{\alpha + \beta\tau : \alpha, \beta \in \mathbb{Z} \quad et \quad 2\beta r, \beta(r^2 + ds^2) \in \mathbb{Z}\}.$$

Démonstration. Prouvons le sens direct. Par le théorème IV.18, nous allons déterminer $\mathrm{End}(C)$ comme l'ensemble $A = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. Pour que $\alpha \in A$, il faut et il suffit qu'il existe $a, b, c, e \in \mathbb{N}$ tel que

$$\alpha = a + b\tau$$
$$\alpha\tau = c + e\tau$$

D'une part, si $\alpha \in \mathbb{R}$ alors $\alpha \in \mathbb{Z}$ car $\Im(\tau) > 0$. D'où $\mathrm{End}(C) \cap \mathbb{R} = \mathbb{Z}$.
D'autre part, si C a une multiplication complexe alors il existe $\alpha \in \mathbb{C}\backslash\mathbb{R}$, i.e $b \neq 0$. En éliminant α, nous obtenons

$$b\tau^2 + (a-e)\tau - c = 0$$

τ est alors une extension quadratique de $\mathbb{Q}$. Comme $\Im(\tau) > 0$, c'est une extension quadratique imaginaire d'où il existe $d \in \mathbb{N}^*$ tel que $\tau \in \mathbb{Q}(\sqrt{-d})$.
De même, en éliminant τ,

$$\alpha^2 - (a-e)\alpha + (ae - bc) = 0$$

alors α est un élément entier sur $\mathbb{Z}$, ce qui conclut la première partie de la démonstration. Maintenant, supposons que $\tau = r + s\sqrt{-d} \in \mathbb{Q}(\sqrt{-d})$. Par le théorème IV.18, $\mathrm{End}(C)$ est l'ensemble des $\alpha = a + b\tau$, $a, b \in \mathbb{Z}$ tels que $\alpha\tau \in \Lambda$. En multipliant par τ, i.e $\alpha\tau = a\tau + b\tau^2$, il faut que $b\tau^2 \in \Lambda$.
Par ailleurs,

$$\tau^2 = r^2 - ds^2 + 2rs\sqrt{-d} = 2r\tau - (r^2 + ds^2).$$

Ainsi, il est nécessaire et suffisant d'avoir $2br \in \mathbb{Z}$ et $b(r^2 + ds^2) \in \mathbb{Z}$.
En particulier, $\mathrm{End}(C) \ncong \mathbb{Z}$, ce qui conclut la démonstration. □

Corollaire IV.32 ([Har77]). *Il y a un nombre dénombrable de $j \in \mathbb{C}$ tel que la courbe elliptique associée soit munie d'une multiplication complexe.*

Démonstration. En effet, il y a un nombre dénombrable d'extensions quadratiques de $\mathbb{Q}$. □

En clair, il existe peu de courbes elliptiques munies d'une multiplication complexe. La plupart du temps, $\mathrm{End}(C) \cong \mathbb{Z}$.

Exemple IV.33 ([Har77]).
1. Prenons $\tau = i$ alors $\mathrm{End}(C)$ est l'anneau des entiers de Gauss $\mathbb{Z}[i]$, par le théorème IV.31. Le groupe des unités $\mathrm{End}(C)^*$ est $\{\pm 1, \pm i\}$, groupe cyclique d'ordre 4 donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Comme $\mathrm{Aut}(C)$ est d'ordre 4, par le corollaire I.16, son j-invariant est 1728. Une autre manière de le voir est par le réseau $\Lambda = \mathbb{Z} + i\mathbb{Z}$ et que

$$g_3 = 140 \sum_{\omega \in \Lambda'} \frac{1}{\omega^6} = 140 \sum_{\omega \in \Lambda'} \frac{1}{(i\omega)^6} = -g_3$$

   Ce qui implique $g_3 = 0$. L'équation de C est de la forme $y^2 = x^3 - b$.
2. Pour $\tau = \rho$ où $\rho^3 = 1$. Dans ce cas, $\mathrm{End}(C) = \mathbb{Z}[\rho]$, i.e l'anneau des entiers $\mathbb{Q}(\sqrt{-3})$. Comme $\mathrm{End}(C)^* = \{\pm 1, \pm\rho, \pm\rho^2\} \cong \mathbb{Z}/6\mathbb{Z}$, $j = 0$ par le corollaire I.16. L'équation est alors $y^2 = x^3 - b$.

Remarque IV.34 ([Sil09]). Notre étude des courbes elliptiques sur $\mathbb{C}$ se généralise sur des corps algébriquement clos de caractéristiques 0, c'est le principe de Lefschetz.

A Bibliographie

Références

[AM93] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, pages 29–68, Juillet 1993.

[CG17] Philippe Caldero and Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries*. Calvage et Mounet, 2017.

[Cha90] Boris Chabat. *Introduction à l'analyse complexe, Tome I*. Mir Moscou, 1990.

[Cha13] Igor Chafarevitch. *Basic Algebraic Geometry I*. Springer, 2013.

[Che15] Gaëtan Chenevier. Introduction aux formes modulaires. Leçon à l'Ecole Normale Supérieure, Mars 2015.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE transactions on information theory*, pages 644–654, Juillet 1976.

[GK86] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. *ACM*, pages 316–329, Juillet 1986.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[Has36] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper. i, ii iii. *Journal de Crelle*, page 175, 1936.

[HPS08] J. Hoffstein, J. Pipher, and J. Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.

[Hus75] Dale Husemoller. *Elliptic Curves*. Springer, 1975.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, pages 203–209, 1987.

[Kob94] Neal Koblitz. *A course in Number Theory and Cryptography*. Springer, 1994.

[LC72] Mikhaïl Lavrantiev and Boris Chabat. *Méthodes de la théorie des fonctions d'une variable complexe*. Mir Moscou, 1972.

[Len87] Hendrick Lenstra. Factoring integers with elliptic curves. *Annals of Math.*, pages 649–673, 1987.

[Lut37] Elisabeth Lutz. Sur l'équation $y^2 = x^3 - ax - b$ dans les corps p-adic. *J.Reine Angew. Math.177*, pages 237–247, 1937.

[Maz77] Barry Mazur. Modular curves and the einsenstein ideal. *IHES Publ. Math. 47*, pages 33–186, 1977.

[Maz78] Barry Mazur. Rational isogenies of prime degree. *Invent. Math. 44*, pages 129–162, 1978.

[Mil85] Victor Miller. Use of elliptic curves in cryptography. *Proc. Cambridge Philos. Soc.*, pages 417–426, 1985.

[Mon87] Peter Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of Computation*, pages 243–264, 1987.

[Mor22] Louis Mordell. On the rational solutions of the indetermine equations of the third and fourth degrees. *Proc. Camb. Philos. Soc. 21*, pages 179–192, 1922.

[Nag35] Trygve Nagell. Solutions de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. *Wid. Acad. Skrifter Oslo I*, 1935.

[Sch95] Renée Schoof. Counting points on elliptic curves over finite fields. *Journal Théorie Nombres Bordeaux*, pages 219–254, 1995.

[Ser95] Jean-Pierre Serre. *Cours d'arithmétique*. PUF, 1995.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1994.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[ST15] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer, 2015.

B Annexe

I.1 Loi de groupe

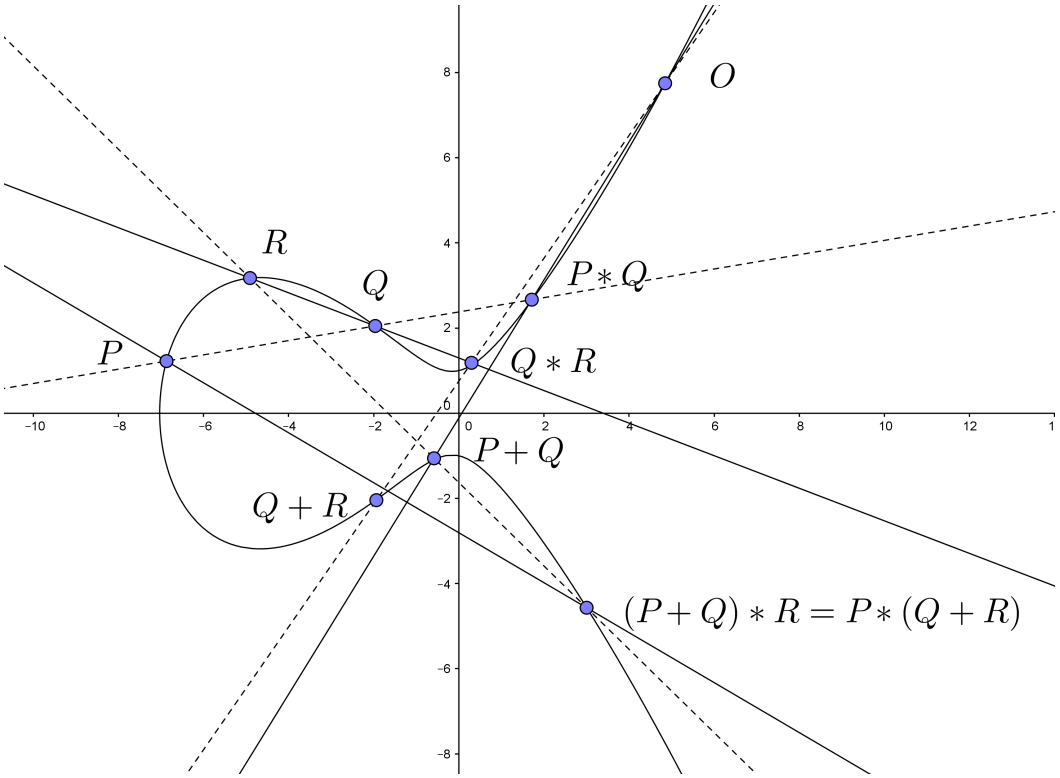


FIGURE 5 – Associativité

khhhhhhhhhhhhhhhhhhhhhh