Courbes elliptiques : Structure, Théorème de Hasse, et Au-Delà
Une Introduction Géométrique et Arithmétique

Mohammad Djezzar

2025

Table des matières

1 Introduction

Introduction historique

L'étude des courbes elliptiques trouve ses racines dans le calcul des arcs d'ellipses au XVII^{e} siècle, mais c'est véritablement avec les travaux d'Euler au XVIII^{e} siècle qu'émerge leur propriété additive remarquable. Le XIX^{e} siècle voit Jacobi et Abel approfondir cette voie par l'étude des fonctions elliptiques inverses, tandis que Poincaré en systématise l'approche géométrique. La théorie connaît un tournant décisif en 1922 avec le théorème de Mordell-Weil qui révèle la structure algébrique profonde de ces objets. Leur importance contemporaine s'est affirmée à travers deux révolutions : la preuve du théorème de Fermat par Wiles en 1994, et leur utilisation en cryptographie depuis les années 1980.

Pourquoi s'intéresser aux courbes elliptiques ?

Les courbes elliptiques offrent un cadre idéal pour découvrir les concepts clés de la géométrie algébrique moderne. Leur étude révèle progressivement la profonde interaction entre géométrie et algèbre qui caractérise cette discipline.

D'un point de vue géométrique, ces courbes présentent une structure suffisamment riche pour illustrer les notions de variétés projectives, de fibrés vectoriels et de diviseurs, tout en restant visuellement accessibles. Leur interprétation comme tores complexes dans le cas archimédien fournit un pont concret entre la géométrie différentielle classique et la géométrie algébrique abstraite.

Sur le plan algébrique, la théorie des courbes elliptiques met en lumière le pouvoir des méthodes fonctorielles. La loi de groupe, définie par la construction géométrique de la corde-tangente, se révèle être un morphisme de variétés algébriques. Ce phénomène montre comment les propriétés universelles gouvernent en réalité les constructions géométriques.

La cohomologie des faisceaux, souvent perçue comme technique en dimension supérieure, devient particulièrement tangible dans ce contexte. Le théorème de Riemann-Roch pour les courbes elliptiques prend une forme explicite qui éclaire la dualité entre diviseurs et espaces de sections globales. Cette transparence permet d'appréhender intuitivement des concepts qui, en dimension supérieure, nécessitent un formalisme lourd.

"Une porte ouverte entre le fini et l'infini."
— André Weil

Notations et conventions

Dans ce mémoire, nous utilisons des notions élémentaires de géométrie algébrique concernant les courbes elliptiques. Pour les définitions précises des termes utilisés (tels que corps de définition, variété algébrique, morphisme de variétés, ou diviseur), ainsi que pour les propriétés fondamentales des courbes projectives, le lecteur pourra se reporter à l'annexe.

Pour alléger l'exposition, nous adoptons les conventions suivantes :

- k désignera toujours un corps parfait de caractéristique différente de 2 et 3,
- $\overline{k}$ sa clôture algébrique.

2 Théorème de Riemann-Roch

Nous allons ici introduire un outil indispensable pour étudier les courbes elliptiques, le théorème de Riemann-Roch. Initialement prouvé sous une forme plus faible par Riemann : l'inégalité de Riemann, le théorème fut par la suite prouvé par son élève, qui marquera un tournant dans la géométrie algébrique.

2.1 $L(D)$ est de dimension finie

Proposition 2.1. Pour tout diviseur D sur une courbe projective lisse C, l'espace $L(D)$ est de dimension finie sur k.

Démonstration. On procède par récurrence forte sur $\deg(D)$.

Initialisation ($\deg(D) < 0$) :
Toute fonction $f \in L(D)$ vérifie $\operatorname{div}(f) \geq -D$. Comme $\deg(\operatorname{div}(f)) = 0$ mais $\deg(-D) > 0$, la seule solution est $f = 0$.

Hérédité ($\deg(D) \geq 0$) :
Supposons la propriété vraie pour tout diviseur de degré $< d$. Choisissons un point $P \in C$.

$L(D+P) \neq L(D)$, choisissons $f_0 \in L(D+P) \setminus L(D)$. Alors :
Notons $V = \{f \in L(D+P) \mid f(P) = 0\}$ et remarquons que $V = L(D)$ car $f \in V \Leftrightarrow \operatorname{div}(f) \geq -D - (P) + (P) = -D$

L'espace $L(D+P)$ est engendré par V et f_0 donc $\dim L(D+P) \leq \dim V + 1 = \dim L(D) + 1 < \infty$.

Conclusion : Par récurrence forte, la propriété est vraie pour tout degré. □

Théorème 2.1 (Riemann-Roch)**.** Soit C une courbe projective lisse de genre g sur un corps k. Pour tout diviseur $D \in \operatorname{Div}(C)$, on a :

$$\ell(D) - \ell(K_C - D) = \deg(D) + 1 - g$$

où :

- K_C est le diviseur canonique
- $\ell(D) := \dim_k \{f \in k(C) \mid (f) + D \geq 0\}$
- $\deg(D)$ est le degré du diviseur

2.2 Applications Typiques

Exemple 2.1 (Courbes rationnelles)**.** Pour $C = \mathbb{P}^1$, $g = 0$, $K = -2[\infty]$:

$$\ell(D) = \deg(D) + 1 \quad \text{si} \quad \deg(D) \geq -1$$

Car $\ell(K - D) = 0$ dès que $\deg(D) \geq -1$.
Ainsi, si on suppose simplement C de genre 0, on a pour P et Q deux points distincts, l'existence de f une fonction rationnelle telle que $div(f) = [P] - [Q]$. Cette condition implique alors que f définit un isomorphisme de C sur $\mathbb{P}^1$.

Exemple 2.2 (Courbes elliptiques)**.** Pour $g = 1$, $K \sim 0$:

$$\ell(D) = \begin{cases} 0 & \text{si } \deg(D) < 0 \\ \deg(D) & \text{si } \deg(D) > 0 \end{cases}$$

3 Courbes Elliptiques

3.1 Définitions

Définition 3.1. Une courbe elliptique $(E, \mathcal{O})$ est une courbe algébrique projective non-singulière de genre 1, où $\mathcal{O}$ est un point rationnel choisi comme élément neutre pour la loi de groupe.

Exemple 3.1. Prenons la courbe $E \subset \mathbb{P}^2(\mathbb{R})$ définie par $F(x, y, z) = y^2z - x^3 + xz^2 = 0$.

Pour comprendre sa lissité, rappelons qu'une variété algébrique est dite *lisse* (ou non-singulière) si en tout point $P \in E$, l'espace tangent T_PE est de dimension égale à la dimension de la variété (ici 1). Concrètement, cela se vérifie en montrant que le gradient ∇F ne s'annule en aucun point de E.

Détaillons cette vérification dans les deux cartes affines :

Cas $z = 1$: L'équation devient $f(x, y) = y^2 - x^3 + x = 0$. Le gradient vaut :

$$\nabla f = (-3x^2 + 1, 2y)$$

Un point singulier nécessiterait $-3x^2 + 1 = 0$ et $2y = 0$ simultanément, donc $x = \pm\frac{1}{\sqrt{3}}$ et $y = 0$. Mais en substituant dans f :

$$0 - \left(\pm\frac{1}{\sqrt{3}}\right)^3 + \left(\pm\frac{1}{\sqrt{3}}\right) = \pm\frac{2}{3\sqrt{3}} \neq 0$$

Il n'y a donc pas de points singuliers dans cette carte.

Carte affine $y = 1$: L'équation devient $g(x, z) = z - x^3 + xz^2 = 0$. Le gradient est :

$$\nabla g = (-3x^2 + z^2, 1 + 2xz)$$

Les points singuliers vérifieraient :

$$\begin{cases} -3x^2 + z^2 = 0 \\ 1 + 2xz = 0 \end{cases}$$

En substituant $z^2 = 3x^2$ dans la seconde équation :

$$1 + 2x(\pm x\sqrt{3}) = 0 \Rightarrow x = \pm\frac{i}{\sqrt[4]{12}} \notin \mathbb{R}$$

Aucun point singulier réel dans cette carte.

Point à l'infini $(0:1:0)$: Calculons le gradient projectif :

$$\nabla F = \left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}\right) = (-3x^2 + z^2, 2yz, y^2 + 2xz)$$

En $(0:1:0)$:

$$\nabla F = (0, 0, 1) \neq \mathbf{0}$$

La courbe E est donc lisse sur tout $\mathbb{P}^2(\mathbb{R})$.

3.2 Forme de Weierstrass

Théorème 3.1. Toute courbe elliptique $(E, \mathcal{O})$ admet une équation de Weierstrass :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Démonstration. La preuve repose sur une analyse systématique des espaces de fonctions $L(n\mathcal{O})$ via le théorème de Riemann-Roch. Plus précisément :

Choisissons d'abord une fonction x ayant un pôle double en $\mathcal{O}$ et une fonction y avec un pôle triple. L'espace $L(2\mathcal{O})$ est engendré par $\{1, x\}$ tandis que $L(3\mathcal{O})$ admet $\{1, x, y\}$ comme base.

Puisque $dim(L(6\mathcal{O})) = 6$, les sept fonctions $1, x, y, x^2, xy, y^2, x^3$ sont nécessairement liées. On a alors une relation de la forme :

$$Ay^2 + (\alpha x + \beta)y = Bx^3 + \gamma x^2 + \delta x + \epsilon$$

où les coefficients dépendent des choix initiaux de x et y. Quitte à diviser par A, on a $A = 1$. La non-singularité de E impose que le discriminant associé à cette équation soit non nul et que $D = A = 1$ (Sinon on aurait une singularité en $\mathcal{O}$ puisqu'il n'y a pas d'autre terme d'ordre 6) $\square$

3.3 Réduction Canonique

Théorème 3.2. Soit E une courbe elliptique sur un corps K avec $\text{char}(K) \neq 2, 3$. Alors E admet une représentation affine par l'équation :

$$y^2 = x^3 + Ax + B$$

où $A, B \in K$ vérifient $\Delta = -16(4A^3 + 27B^2) \neq 0$.

Démonstration. Partons de la forme générale :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Complétion du carré Posons $y = \tilde{y} - \frac{a_1x+a_3}{2}$. L'équation devient :

$$\left(\tilde{y} - \frac{a_1x + a_3}{2}\right)^2 + a_1x\left(\tilde{y} - \frac{a_1x + a_3}{2}\right) + a_3\left(\tilde{y} - \frac{a_1x + a_3}{2}\right) = x^3 + a_2x^2 + a_4x + a_6$$

Développons chaque terme :

$$\left(\tilde{y} - \frac{a_1x + a_3}{2}\right)^2 = \tilde{y}^2 - a_1x\tilde{y} - a_3\tilde{y} + \frac{a_1^2x^2}{4} + \frac{a_1a_3x}{2} + \frac{a_3^2}{4}$$
$$a_1x\left(\tilde{y} - \frac{a_1x + a_3}{2}\right) = a_1x\tilde{y} - \frac{a_1^2x^2}{2} - \frac{a_1a_3x}{2}$$
$$a_3\left(\tilde{y} - \frac{a_1x + a_3}{2}\right) = a_3\tilde{y} - \frac{a_1a_3x}{2} - \frac{a_3^2}{2}$$

En regroupant tous les termes :

$$\tilde{y}^2 + (-a_1x\tilde{y} + a_1x\tilde{y}) + (-a_3\tilde{y} + a_3\tilde{y}) + \left(\frac{a_1^2x^2}{4} - \frac{a_1^2x^2}{2}\right)$$

$$+ \left(\frac{a_1a_3x}{2} - \frac{a_1a_3x}{2} - \frac{a_1a_3x}{2}\right) + \left(\frac{a_3^2}{4} - \frac{a_3^2}{2}\right) = x^3 + a_2x^2 + a_4x + a_6$$

Simplification :

$$\tilde{y}^2 - \frac{a_1^2x^2}{4} - \frac{a_1a_3x}{2} - \frac{a_3^2}{4} = x^3 + a_2x^2 + a_4x + a_6$$

Réarrangement final :

$$\tilde{y}^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(a_6 + \frac{a_3^2}{4}\right)$$

Élimination du terme en x^2 Posons $x = \hat{x} - \frac{a_2+\frac{a_1^2}{4}}{3}$ et développons :

$$x^3 = \hat{x}^3 - 3\left(\frac{a_2 + \frac{a_1^2}{4}}{3}\right)\hat{x}^2 + 3\left(\frac{a_2 + \frac{a_1^2}{4}}{3}\right)^2\hat{x} - \left(\frac{a_2 + \frac{a_1^2}{4}}{3}\right)^3$$
$$x^2 = \hat{x}^2 - 2\left(\frac{a_2 + \frac{a_1^2}{4}}{3}\right)\hat{x} + \left(\frac{a_2 + \frac{a_1^2}{4}}{3}\right)^2$$

Le coefficient de $\hat{x}^2$ est :

$$-3\left(\frac{a_2 + \frac{a_1^2}{4}}{3}\right) + \left(a_2 + \frac{a_1^2}{4}\right) = 0$$

Après calcul , on obtient bien la forme :

$$y^2 = x^3 + Ax + B$$

avec $\Delta = -16(4A^3 + 27B^2)$ non nul pour la lissité. □

4 Loi de Groupe

4.1 Définition géométrique

Soit E une courbe elliptique définie sur un corps K par l'équation de Weierstrass :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Définition 4.1 (Loi de groupe)**.** La somme $P \oplus Q$ de deux points $P, Q \in E$ est une loi de groupe définie par :

- Si $P = Q$, prendre la tangente à E en P
- Si $P \neq Q$, tracer la droite (PQ)
- Trouver le troisième point d'intersection R' avec E (l'existence étant due au théorème de Bezout)
- Définir $P \oplus Q$ comme le symétrique de R' par rapport à l'axe x

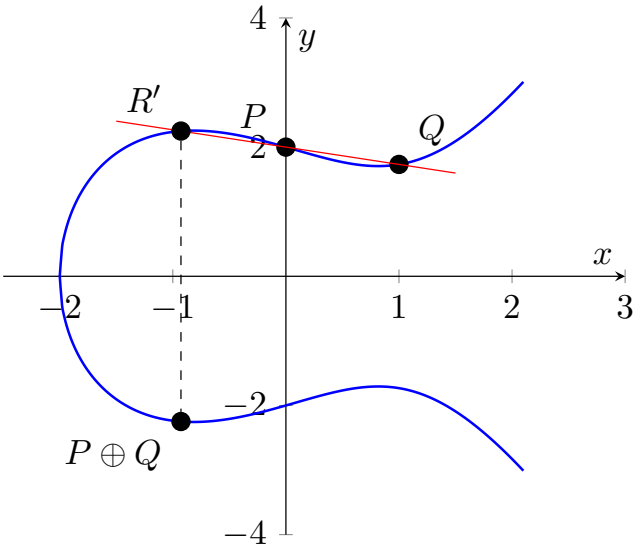

FIGURE 1 – Addition sur $E : y^2 = x^3 - 2x + 4$

4.2 Formules algébriques

Pour la forme courte $y^2 = x^3 + ax + b$ (car $K \neq 2, 3$) :

Proposition 4.1 (Addition)**.** Soient $P = (x_1, y_1)$, $Q = (x_2, y_2)$ alors $P \oplus Q = (x_3, y_3) \in E$:

- Si $x_1 \neq x_2$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

- Si $P = Q$ (doublement) :

$$\lambda = \frac{3x_1^2 + a}{2y_1}, \quad x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

Théorème 4.1. $(E(K), +)$ est un groupe abélien.

Remarque 4.1. Les calculs étant fastidieux et très peu intéressants, on se propose de le prouver d'une autre manière un peu plus tard.

5 Loi de groupe sur les diviseurs

5.1 Structure de groupe

Théorème 5.1. Le quotient $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E)$ hérite naturellement d'une structure de groupe abélien.

Démonstration. L'ensemble $\mathrm{Div}(E)$ des diviseurs forme un groupe abélien pour l'addition des diviseurs. Le degré $\deg : \mathrm{Div}(E) \to \mathbb{Z}$ étant un morphisme de groupes, son noyau $\mathrm{Div}^0(E) = \ker(\deg)$ est un sous-groupe abélien. Comme tout diviseur principal a degré nul, $\mathrm{Prin}(E)$ est un sous-groupe de $\mathrm{Div}^0(E)$.

Puisque $\mathrm{Div}^0(E)$ est abélien, le sous-groupe $\mathrm{Prin}(E)$ est automatiquement distingué. Le quotient $\mathrm{Div}^0(E)/\mathrm{Prin}(E)$ hérite donc d'une structure de groupe abélien où l'addition est donnée par $[D_1]+[D_2] = [D_1+D_2]$, l'élément neutre est $[0]$, et l'inverse de $[D]$ est $[-D]$. Cette construction ne nécessite aucun calcul explicite et découle uniquement des propriétés des groupes abéliens. □

5.2 Représentation canonique

Théorème 5.2. Pour tout $D \in \mathrm{Div}^0(E)$, il existe un unique $P \in E$ tel que

$$D \sim (P) - (\mathcal{O})$$

Démonstration. Soit $D \in \mathrm{Div}^0(E)$. Par le théorème de Riemann-Roch appliqué à $D + (\mathcal{O})$, il existe une fonction $f \in K(E)^*$ telle que :

$$\mathrm{div}(f) = (P) - (\mathcal{O}) + D$$

ce qui montre que $D \sim (P) - (\mathcal{O})$.

Pour l'unicité, supposons $(P) - (\mathcal{O}) \sim (Q) - (\mathcal{O})$. Alors il existe $g \in K(E)^*$ telle que :

$$\mathrm{div}(g) = (P) - (Q)$$

Cette fonction g a un unique zéro simple en P et un unique pôle simple en Q.

Comme g a un seul pôle simple, c'est une fonction de degré 1 (par définition du degré d'une application). Mais pour une courbe elliptique, toute fonction non constante a un degré ≥ 2 (car le genre est 1 et on a la formule $\deg(g) = 1 + \sum_P (e_P(g) - 1)$), sauf dans le cas trivial où $P = Q$.

Ainsi, nécessairement $P = Q$, ce qui prouve l'unicité. □

5.3 Expression concrète de la loi

Proposition 5.1. Soient $D_1 = (P_1) - (\mathcal{O})$, $D_2 = (P_2) - (\mathcal{O})$. Alors :

$$[D_1] + [D_2] = [(P_3) - (\mathcal{O})]$$

où P_3 est l'unique point tel que :

$$(P_1) + (P_2) + (P_3') \sim 3(\mathcal{O})$$

et P_3 est le symétrique de P_3' par rapport à l'axe des x.

Démonstration. Considérons la droite L passant par P_1 et P_2 (tangente si $P_1 = P_2$). Elle intersecte E en un troisième point P_3'. Alors :

$$\mathrm{div}(L) = (P_1) + (P_2) + (P_3') - 3(\mathcal{O})$$

Ainsi :

$$(P_1) - (\mathcal{O}) + (P_2) - (\mathcal{O}) \sim -[(P_3') - (\mathcal{O})] \sim (P_3) - (\mathcal{O})$$

où la dernière équivalence vient de la fonction verticale $x - x_{P_3'}$. □

6 Identification des structures de groupe

6.1 Isomorphisme canonique

Théorème 6.1. Soit E une courbe elliptique. L'application

$$\begin{aligned} \phi : E &\to \mathrm{Pic}^0(E) \\ P &\mapsto [(P) - (\mathcal{O})] \end{aligned}$$

est un isomorphisme de groupes, où :
— La loi sur E est la loi additive usuelle des courbes elliptiques
— La loi sur $\mathrm{Pic}^0(E)$ est celle définie par l'addition des diviseurs

Démonstration. Nous procédons en trois étapes :
Injectivité : Si $\phi(P) = \phi(Q)$, alors $(P) - (\mathcal{O}) \sim (Q) - (\mathcal{O})$, donc $(P) \sim (Q)$. Par étude des espaces $L((P))$, ceci implique $P = Q$.
Surjectivité : Tout élément de $\mathrm{Pic}^0(E)$ s'écrit $[D]$ avec $\deg D = 0$. Le théorème de Riemann-Roch montre qu'il existe $P \in E$ tel que $D \sim (P) - (\mathcal{O})$, donc $[D] = \phi(P)$.
Morphisme : Soient $P, Q \in E$. Par définition de la loi sur E, on a :

$$P + Q + R = \mathcal{O} \Rightarrow (P) + (Q) + (R) \sim 3(\mathcal{O})$$

où R est le troisième point d'intersection de la droite PQ avec E. Ceci donne :

$$\phi(P) + \phi(Q) = [(P) - (\mathcal{O})] + [(Q) - (\mathcal{O})] = [(P) + (Q) - 2(\mathcal{O})]$$

$$= [-(R) + (\mathcal{O})] = [(R) - (\mathcal{O})]^{-1} = [(-R) - (\mathcal{O})] = \phi(P + Q)$$

en utilisant la symétrie $(R) \sim (-R)$ modulo les diviseurs principaux. □

6.2 Conséquences structurelles

Corollaire 6.1. Les lois suivantes sont donc équivalentes :

1. La loi additive sur E définie géométriquement
2. La loi induite par $\mathrm{Pic}^0(E)$ via ϕ
3. La loi donnée par les formules d'addition algébriques

7 Le théorème de Hasse par la géométrie algébrique

7.1 Contexte historique

Le théorème de Hasse, démontré en 1933, marque un tournant dans l'étude arithmétique des courbes elliptiques sur les corps finis. Initialement conjecturé par Emil Artin, ce résultat établit des bornes très précises sur le nombre de points rationnels.

Théorème 7.1 (Hasse)**.** Pour toute courbe elliptique E définie sur $\mathbb{F}_q$, le nombre de points rationnels $\#E(\mathbb{F}_q)$ vérifie :

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

Démonstration. Considérons l'endomorphisme de Frobenius $\phi : E \to E$ défini par $\phi(x, y) = (x^q, y^q)$. Les points rationnels correspondent exactement aux points fixes de ϕ, ce qui donne :

$$\#E(\mathbb{F}_q) = \deg(1 - \phi)$$

La théorie des endomorphismes des courbes elliptiques établit que pour tout $\psi \in (E)$, on a la relation fondamentale :

$$\deg(1 - \psi) = 1 - tr(\psi) + \deg(\psi)$$

En appliquant cette formule à $\psi = \phi$ (avec $\deg(\phi) = q$), on obtient :

$$\#E(\mathbb{F}_q) = q + 1 - tr(\phi)$$

La forme de Rosati, produit scalaire canonique sur (E), impose la condition de positivité :

$$\langle \phi, \phi \rangle = 2\deg(\phi) - tr(\phi)^2 \geq 0$$

Ce qui se réécrit :

$$tr(\phi)^2 \leq 4\deg(\phi) = 4q$$

En substituant $tr(\phi) = q + 1 - \#E(\mathbb{F}_q)$, on obtient finalement :

$$(q + 1 - \#E(\mathbb{F}_q))^2 \leq 4q$$

qui est exactement l'inégalité de Hasse après extraction de la racine carrée. □

Théorème 7.2 (Théorème de Hasse faible)**.** Soit $E/\mathbb{F}_q$ une courbe elliptique définie sur un corps fini. Alors

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

pour une constante absolue $C > 0$.

8 Démonstration

8.1 Préliminaires

Fixons une courbe elliptique $E/\mathbb{F}_q$ et notons O son point à l'infini. Soit $\mathscr{L}(D)$ l'espace des fonctions rationnelles sur E avec diviseur des pôles borné par D.

Proposition 8.1. L'espace $\mathscr{L}(kO)$ a pour dimension k lorsque $k \geq 1$.

8.2 Construction clé

Choisissons deux entiers $n, m \geq 0$ (à fixer ultérieurement) et :

— Une base $\{f_1, \ldots, f_m\}$ de $\mathscr{L}(mO)$ avec $f_i \in \mathscr{L}(iO) \setminus \mathscr{L}((i-1)O)$

— Des fonctions $s_1, \ldots, s_m \in \mathscr{L}(nO)$

Pour $f \in \mathbb{F}_q(E)$, on note $f^{(q)}$ la fonction définie par $f^{(q)}(x, y) = f(x^q, y^q)$.

8.3 Énoncés techniques

Lemme 8.1 (Non-annulation)**.** Soit $b \geq 1$ tel que $q > np^b$. Si les s_i ne sont pas tous nuls, alors la fonction

$$\Phi := \sum_{i=1}^{m} s_i^{p^b} f_i^{(q)}$$

est non identiquement nulle.

Démonstration. Supposons par contradiction que $\Phi = 0$. Soit h maximal tel que $s_h \neq 0$. Alors :

$$s_h^{p^b} f_h^{(q)} = -\sum_{i=1}^{h-1} s_i^{p^b} f_i^{(q)}$$

En évaluant les valuations en O, on obtient :

$$p^b v_O(s_h) + q v_O(f_h) \geq \min_{i<h}\{p^b v_O(s_i) + q v_O(f_i)\} \geq -p^b n - q(h-1)$$

Ce qui implique :

$$p^b v_O(s_h) \geq -p^b n - q(h - 1 + v_O(f_h)) = -p^b n + q > 0$$

Ainsi $s_h(O) = 0$, mais s_h n'a pas d'autres pôles que O, donc $s_h = 0$, contradiction. □

Lemme 8.2 (Existence)**.** Si $mn > p^b n + m$, alors il existe des $s_1, \ldots, s_m \in \mathscr{L}(nO)$ non tous nuls tels que

$$\sum_{i=1}^{m} s_i^{p^b} f_i = 0.$$

Démonstration. L'application $(s_1, \ldots, s_m) \mapsto \sum s_i^{p^b} f_i$ est $\mathbb{F}_q$-linéaire entre espaces de dimensions respectives mn et $p^b n + m$. Le noyau est non trivial sous l'hypothèse. □

8.4 Application

Choisissons maintenant :

$$q = p^{2b}, \quad n = p^b - 1, \quad m = p^b + 2$$

Vérifions les hypothèses :

— $q = p^{2b} > (p^b - 1)p^b = np^b$

— $mn = (p^b + 2)(p^b - 1) > p^b(p^b - 1) + (p^b + 2) = p^b n + m$

Construisons Φ comme dans le Lemme 8.1. On observe que :

— Φ est non nulle

— $\Phi(P) = 0$ pour tout $P \in E(\mathbb{F}_q) \setminus \{O\}$

— Φ n'a de pôles qu'en O, d'ordre au plus $p^b n + mq$

Par la formule des résidus :

$$p^b(\#E(\mathbb{F}_q) - 1) \leq p^b n + mq$$

Ce qui donne avec nos paramètres :

$$\#E(\mathbb{F}_q) - q - 1 \leq 3\sqrt{q}$$

8.5 Borne inférieure

Considérons l'endomorphisme de Frobenius $F_q : (x, y) \mapsto (x^q, y^q)$. Par une analyse similaire des points fixes de F_q et $-F_q$, on obtient la borne complète :

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

pour une constante C universelle.

A Fondements de Géométrie Algébrique

A.1 Variétés Algébriques

Définition A.1 (Espace affine)**.** Soit k un corps algébriquement clos. L'**espace affine** de dimension n sur k est l'ensemble :

$$\mathbb{A}^n(k) = \{(a_1, ..., a_n) \mid a_i \in k\}$$

Définition A.2 (Topologie de Zariski)**.** La **topologie de Zariski** sur $\mathbb{A}^n$ est définie par :

— Les fermés sont les ensembles algébriques $V(I) = \{P \in \mathbb{A}^n \mid \forall f \in I, f(P) = 0\}$ pour I idéal de $k[X_1, ..., X_n]$

— Une base d'ouverts est donnée par les $D(f) = \mathbb{A}^n \setminus V(f)$ pour $f \in k[X_1, ..., X_n]$

Propriétés clés :

— Topologie non-Hausdorff (mais noethérienne)

— Les ouverts principaux $D(f)$ sont appelés **ouverts standard**

— La topologie induite sur tout sous-ensemble algébrique est la **topologie de Zariski relative**

Exemple A.1. Dans $\mathbb{A}^2$:

— $V(x^2 + y^2 - 1)$ est le cercle unité

— $D(x) = \mathbb{A}^2 \setminus V(x)$ est le complémentaire de l'axe y

A.2 Variétés Affines

Définition A.3. Une **variété affine** est un ensemble algébrique irréductible muni de :

— La topologie de Zariski induite

— Son **anneau de coordonnées** $\Gamma(V) = A(V) = k[X_1, ..., X_n]/I(V)$

— Son **corps des fonctions rationnelles** $k(V) = \mathrm{Frac}(A(V))$

Théorème A.1 (Correspondance)**.** Il y a équivalence entre :

— Variétés affines dans $\mathbb{A}^n$

— k-algèbres de type fini réduites intègres

A.3 Variétés Projectives

Définition A.4 (Espace projectif)**.** L'**espace projectif** de dimension n est :

$$\mathbb{P}^n(k) = (k^{n+1} \setminus \{0\})/\sim$$

où $(x_0, ..., x_n) \sim (y_0, ..., y_n)$ ssi $\exists \lambda \neq 0$ tel que $y_i = \lambda x_i$.

Définition A.5 (Topologie projective)**.** Les fermés de Zariski sur $\mathbb{P}^n$ sont les $V(I) = \{[x_0 : ... : x_n] \mid \forall f \in I, f(x_0, ..., x_n) = 0\}$ pour I idéal homogène.

Théorème A.2 (Recouvrement standard)**.** $\mathbb{P}^n$ est recouvert par les ouverts affines :

$$U_i = \{[x_0 : ... : x_n] \mid x_i \neq 0\} \simeq \mathbb{A}^n$$

A.4 Dimension Et Lissité

Soit X une variété algébrique sur un corps k. La **dimension** de X, notée $\dim X$, est définie comme la longueur maximale n des chaînes strictement croissantes de sous-variétés irréductibles fermées :

$$\emptyset \subsetneq X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \subseteq X.$$

Pour une variété irréductible, cette coïncide avec le degré de transcendance du corps des fonctions rationnelles $K(X)$ sur k.

La variété X est dite **lisse** en un point $x \in X$ si l'espace tangent T_xX a dimension égale à $\dim X$. Plus formellement, si $\mathcal{O}_{X,x}$ est l'anneau local en x et $\mathfrak{m}_x$ son idéal maximal, alors X est lisse en x si :

$$\dim_{\kappa(x)} \mathfrak{m}_x/\mathfrak{m}_x^2 = \dim \mathcal{O}_{X,x},$$

où $\kappa(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$ est le corps résiduel. On dit que X est une **variété lisse** si elle est lisse en tout point. Dans le cas contraire, les points de non-lissité forment un sous-ensemble fermé appelé le *lieu singulier* de X.

A.5 Morphismes entre Variétés Algébriques

Définition A.6. Soit $\varphi : X \to Y$ une application entre variétés affines. On dit que φ est un **morphisme régulier** s'il existe des polynômes $\varphi_1, ..., \varphi_m \in k[X_1, ..., X_n]$ tels que pour tout point $P \in X$, on ait $\varphi(P) = (\varphi_1(P), ..., \varphi_m(P))$.

Exemple fondamental La projection $\pi : \mathbb{A}^2 \to \mathbb{A}^1$ donnée par $\pi(x, y) = x$ est un morphisme régulier. En effet, sa seule composante est le polynôme $\pi_1(x, y) = x$, qui est clairement régulier. Géométriquement, cette application envoie chaque point verticalement sur l'axe des abscisses.

Définition A.7. Soit $\varphi : X \to Y$ un morphisme régulier. On définit son **morphisme dual** (ou morphisme d'algèbres associé) comme étant l'application :

$$\varphi^* : k[Y] \to k[X]$$

$$f \mapsto f \circ \varphi$$

Cette application est un morphisme de k-algèbres.

Application Reprenons l'exemple de la projection π. Son dual est :

$$\pi^* : k[x] \to k[x, y]$$

$$f(x) \mapsto f(x)$$

C'est bien un morphisme d'algèbres qui "oublie" la coordonnée y.

Définition A.8. Un morphisme $\varphi : X \to Y$ est un **isomorphisme** s'il existe un morphisme $\psi : Y \to X$ tel que $\varphi \circ \psi = \mathrm{id}_Y$ et $\psi \circ \varphi = \mathrm{id}_X$.

Exemple important Considérons l'application $\varphi : \mathbb{A}^1 \setminus \{0\} \to Z(y^2 - x^3) \setminus \{(0, 0)\}$ définie par $\varphi(t) = (t^2, t^3)$.

Pour montrer que c'est un isomorphisme, construisons son inverse $\psi(x, y) = y/x$. On vérifie :

$$\psi(\varphi(t)) = \psi(t^2, t^3) = t^3/t^2 = t$$

$$\varphi(\psi(x, y)) = \varphi(y/x) = ((y/x)^2, (y/x)^3) = (x, y)$$

où la dernière égalité utilise que $y^2 = x^3$ sur la variété cible.

Définition A.9. Un morphisme $\varphi : X \to Y$ est dit **fini** si le morphisme dual φ^* fait de $k[X]$ un $k[Y]$-module de type fini.

Exemple caractéristique La projection de la parabole $X = Z(y - x^2)$ sur $\mathbb{A}^1$ via $\varphi(x, y) = x$ est finie. En effet, φ^* identifie $k[x]$ comme sous-algèbre de $k[x, y]/(y - x^2) \simeq k[x]$, qui est bien finiment engendré (par 1 et x) comme module sur lui-même.

A.6 Diviseurs sur les Courbes

Définition A.10. Soit C une courbe algébrique lisse. Le **groupe des diviseurs** $\mathrm{Div}(C)$ est le groupe abélien libre engendré par les points fermés de C :

$$\mathrm{Div}(C) = \bigoplus_{P \in C} \mathbb{Z} \cdot P$$

Un diviseur D s'écrit donc $D = \sum_{P \in C} n_P P$ où $n_P \in \mathbb{Z}$ et $n_P = 0$ sauf pour un nombre fini de P.

Exemple concret. Sur la droite projective $\mathbb{P}^1$, considérons le diviseur $D = 2[0] - 3[1] + [\infty]$. Ce diviseur a trois termes non nuls : un coefficient 2 en le point 0, -3 en le point 1, et 1 au point à l'infini. Le degré de D vaut $\deg(D) = 2 - 3 + 1 = 0$.

Définition A.11. Le **diviseur d'une fonction rationnelle** $f \in k(C)^\times$ est :

$$(f) = \sum_{P \in C} \mathrm{ord}_P(f) \cdot P$$

où $\mathrm{ord}_P(f)$ est l'ordre d'annulation (ou de pôle) de f en P.

Exemple critique. Soit $C = \mathbb{P}^1$ et $f(x) = \frac{(x-1)^2}{x}$. Alors :

$$(f) = 2[1] - [0] - [\infty]$$

Cette égalité se démontre en trois étapes. Premièrement, en $x = 1$, la fonction f s'annule à l'ordre 2 car $(x - 1)^2$ est présent au numérateur. Deuxièmement, en $x = 0$, f a un pôle simple car x est au dénominateur. Troisièmement, en $x = \infty$, on fait le changement de variable $x = 1/t$ et on trouve $f(1/t) = \frac{(1/t-1)^2}{1/t} = t(1 - t)^2/t^2 = (1 - t)^2/t$, qui présente un pôle simple en $t = 0$ (c'est-à-dire en $x = \infty$).

A.7 Propriétés Essentielles

Théorème A.3 (Degré des diviseurs principaux)**.** Pour toute fonction rationnelle non nulle $f \in k(C)^\times$, on a :

$$\deg((f)) = 0$$

Motivation. L'idée centrale repose sur deux observations. Pour une courbe projective lisse C, le nombre de zéros et de pôles d'une fonction est fini. De plus, lorsque l'on compte ces zéros et pôles avec multiplicité, leurs contributions s'annulent exactement. Ce résultat profond est une version algébrique du théorème de Liouville en analyse complexe.

Définition A.12. Le **groupe de Picard** $\mathrm{Pic}(C)$ est le quotient du groupe des diviseurs par les diviseurs principaux :

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\sim$$

où $D \sim D'$ ssi $D - D' = (f)$ pour une certaine fonction rationnelle f.

A.8 Diviseur Canonique

A.9 Unicité du Diviseur Canonique

Théorème A.4. Pour une courbe lisse C, deux formes différentielles méromorphes non nulles $\omega_1, \omega_2 \in \Omega^1_{k(C)/k}$ ont des diviseurs linéairement équivalents :

$$(\omega_1) \sim (\omega_2)$$

Démonstration. Soit $\omega_1, \omega_2 \neq 0$. Alors $\exists f \in k(C)^\times$ telle que $\omega_2 = f\omega_1$ (car $\dim_{k(C)} \Omega^1 = 1$). On a donc :

$$(\omega_2) = (f) + (\omega_1)$$

Ainsi, $(\omega_2) - (\omega_1) = (f)$ est principal. □

A.10 Exemples Détaillés

Droite projective $\mathbb{P}^1$ Considérons la forme dz sur $\mathbb{A}^1 \subset \mathbb{P}^1$. Au voisinage de ∞, posons $w = 1/z$:

$$dz = d(1/w) = -\frac{dw}{w^2} \quad \Rightarrow \quad \mathrm{ord}_\infty(dz) = -2$$

Ainsi :

$$(dz) = -2[\infty] \quad \text{(diviseur canonique standard)}$$

Courbe elliptique $E : y^2 = x^3 + ax + b$ La forme différentielle $\omega = \frac{dx}{2y}$ est régulière partout :

— Sur $\mathbb{A}^2$: ω n'a ni zéros ni pôles (car y et dx ne s'annulent simultanément nulle part)

— À l'infini : En coordonnées homogènes $[X : Y : Z]$, posons $x = X/Z$, $y = Y/Z$:

$$\omega = \frac{d(X/Z)}{2(Y/Z)} = \frac{ZdX - XdZ}{2YZ} \quad \text{est régulière en } Z = 0$$

Donc $(\omega) = 0$ et $K_E \sim 0$.

Bibliographie complète

HARTSHORNE, R. (1977). *Algebraic Geometry*. Springer.

HASSE, Helmut (1936). "Zur Theorie der abstrakten elliptischen Funktionenkörper". In : *Journal für die reine und angewandte Mathematik* 175. L'article original du théorème, p. 55-62.

SILVERMAN, J.H. (2009). *The Arithmetic of Elliptic Curves*. Springer.

SZAMUELY, Tamas (s. d.). "Lectures On Elliptic Curves". In : (). Preuve de Hasse faible, p. 26-27.