ELLIPTIC CURVES : MORDELL-WEIL THEOREM

Gwendal SOISNARD

Supervisor : Luis NARVÁEZ MACARRO

June - July 2017, Seville, Spain

Abstract

The aim of this document is to explain the proof of the Mordell-Weil theorem given in the book of Joseph H. Silverman [Sil86] which states that the group of K-rational points of an elliptic curve over a number field is finitely generated. To introduce this result we will define the general concept of algebraic varieties and curves. Then we will study the properties of elliptic curves, in particular notions and results we will need for the proof of the Mordell-Weil theorem which follows in the next part. To conclude, we will say some words about the natural continuations like the Mazur's theorem and the Birch Swinnerton-Dyer conjecture.

Foreword

This document represents the achievement of my internship at the university of Seville between the 5^{th} of June and the 4^{th} of August. This internship was focused on the proof of the Mordell-Weil theorem presented in the Silverman's book : *The arithmetic of elliptic curves* [Sil86].

For the sake of clarity and for the logical succession of the ideas presented, I decided to focus my writing on the main subject of my internship, the Mordell-Weil theorem. Thus many topics covered during my internship will not appear here, I only kept the results which are important in order to prove the theorem.

To avoid copying proof from books, many theorems are stated there without proof even if they have been studied. Some references are given when theorems are not fully proved and we can find all the material needed in [Sil86], [Har77] and [Neu99]. I focused on including only proofs in which I provided new materials as details and explanations of specific statements. On the other hand, to show the way I studied during this period and the points I deeply worked on, I sometimes develop subjects more than it could be necessary.

These subjects have been pointed out by my supervisor Luis Naváez Macarro who oriented me through this internship. I would like to thank him especially for the numerous hours he spent with me. He was really available and taught me a lot, in particular he helped me to take a step back to understand concepts in a general way. I also thank the department of algebra of the university of Seville for receiving me in really good conditions.

Contents

Introduction

In the context of algebraic geometry, if we have for example an polynomial equation with rational coefficients $f(x, y) = 0$, the question of finding rational solutions $(x, y) \in \mathbb{Q}^2$ is interpreted as describing the rational points on the curve C defined as the zeros of f in $\overline{\mathbb{Q}}^2$.

Thus, it is natural to be interested in properties of the rational points on a given algebraic curve or more generally, on a given algebraic variety. One question is to know if there are only finitely many such points. The answer depends on the genus of the curve. The notion of genus can be defined topologically in the complex case but also over any algebraically closed field. In the case of complex smooth curves, the two definition coincided.

In case of genus $g = 0$, there are two cases : either C has no rational points, or C is isomorphic to $\mathbb{P}^1$ in which case it has infinitely many rational points. In genus $g \geqslant 2$, Faltings's theorem, conjectured by Mordell in 1922 and finally proved in 1983, states that the number of rational points is finite.

In the last case $g = 1$, the one we will study here, the number of rational points is not always finite. In this case, smooth projective curves are called elliptic curves. Elliptic curves have the great property that we can geometrically define an abelian group law on them and the set of rational points form a subgroup. The Mordell theorem, proved in 1922, states that this group is finitely generated. Lastly, the Mordell-Weil theorem developed in the Weil's thesis in 1928 is its generalisation to number fields :

Theorem (Mordell-Weil)**.** *Let* K *be a number field and* E/K *an elliptic curve.*
Then the subgroup of K*-rational points* $E(K)$ *is finitely generated.*

The road I will take to reach the proof of the Mordell-Weil theorem, suggested in the Silverman's book, is as follows : We will start by setting the general framework by defining algebraic varieties in the first chapter. Definitions of dimension and smoothness of a variety will allow us to talk about smooth curves, which are the smooth varieties of dimension 1, in the second chapter. One of our main goals in this chapter will be to define algebraically the genus of a curve.

Then we will focus on the elliptic curves, the smooth curves of genus one, in the third chapter. We will characterise them with Weierstrass equations and we will geometrically define the group law. This chapter will also cover an important result needed for the proof of the Mordell-Weil theorem : the m-torsion group is a finite group. We will finish this third chapter with an explanation of the reduction of a curve over a residue field and then we will be ready to start the proof of the Mordell-Weil theorem.

This proof will be the topic of the fourth chapter which is decomposed in several parts : The weak Mordell-Weil theorem, the descent procedure, the Mordell theorem,

and the generalisation : the Mordell-Weil theorem.

We will conclude this document with a small discussion on the natural questions we can ask ourselves. We will answer the questions “What is the structure of the torsion group ?” and “What can we say about integral points ?” using Mazur’s and Siegel’s theorems. We will also discuss about open problems as “What about the highest rank that an elliptic curve can have ?” and the famous Birch Swinnerton-Dyer conjecture, one of the seven millennium problems, which is directly linked with the Mordell-Weil theorem.

Chapter 1

Algebraic Varieties

The aim of this first chapter is to set a rigorous general framework of our subject. We will define affine algebraic varieties and projective ones and talk about dimension, regularity and maps between varieties. Thus we will able to talk about curves, which are the varieties of dimension 1, in the next chapter.

Let $n, m \in \mathbb{N}$. Let K be a perfect field and $\overline{K}$ a fixed algebraic closure of K.

1.1 Affine varieties

In this section, we will give many definitions about about the general theory of algebraic varieties in the affine context. First of all, let us define the affine space :

Definition (Affine space)**.** An **affine space** of dimension n over K is the set of n-tuples :

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \left\{ P = (x_1, \ldots, x_n) \mid x_i \in \bar{K} \right\}$$

And the set of **rational points** in the affine space $\mathbb{A}^n$ is :

$$\mathbb{A}^n(K) = \left\{ P = (x_1, \ldots, x_n) \mid x_i \in K \right\}$$

And then, let us define algebraic sets and varieties in the affine context :

Definition (Affine algebraic set)**.** An **affine algebraic set** is any set of the form :

$$V = \left\{ P \in \mathbb{A}^n \mid \forall f \in I : f(P) = 0 \right\}$$

Where I is an ideal of $\bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$, the ring of polynomials in n variables over $\bar{K}$. To each algebraic set V we can associate an ideal which is :

$$I(V) = \left\{ f \in \bar{K}[X] \mid \forall P \in V : f(P) = 0 \right\}$$

We say that an algebraic set V is defined over K if $I(V)$ is generated by polynomials in $K[X]$. We denote this by V/K and in this case, the set of K-rational points of V is :

$$V(K) = V \cap \mathbb{A}^n(K)$$

Remark 1. Since a field is noetherian $\bar{K}[X]$ is also noetherian from the Hilbert basis theorem. This ensures that any ideal of the form $I(V)$ is finitely generated.

Example 1. Let $\bar{K} = \mathbb{C}$ and V the algebraic set associated with $I = \langle X^2 + Y^2 - 1 \rangle$.

Then $V(\mathbb{R})$ is the unit circle.

Definition (Affine variety)**.** An affine algebraic set V is called **affine variety** if $I(V)$ is a prime ideal in $\bar{K}[X]$.

Remark 2. The condition "$I(V)$ is prime" means the variety is irreducible, it has only one component. This condition is not always required but as we can always come back to the study over one component, this definition is convenient.

Example 2. The algebraic set associated with $\langle X^2 - Y^2 \rangle$ is not a variety because this ideal is not prime since $X^2 - Y^2$ admit the decomposition $(X + Y)(X - Y)$. This algebraic set has two components which are the lines $y = x$ and $y = -x$. The real locus $V(\mathbb{R})$ is the union of the two principal bisectors.

Definition (Function field)**.** Let V be an affine variety. We define the **affine coordinate ring** of V as :

$$\bar{K}[V] = \bar{K}[X]/I(V)$$

And if V is defined over K, we define the affine coordinate ring of V/K as :

$$K[V] = K[X]/I(V/K)$$

Then, we define the **function field** of V as the quotient field $\bar{K}(V)$ of $\bar{K}[V]$.

In case in which V is defined over K, we get $K(V)$ from $K[V]$.

Remark 3. Polynomials in $\bar{K}[V]$ are defined up to a polynomial vanishing on V. So, an element $f \in \bar{K}[V]$ induces a well-defined function $f : V \to \bar{K}$ and we can see $\bar{K}[V]$ as the set of functions on V defined by restriction on V of a polynomial on $\mathbb{A}^n$.

Now, we would like to define the local ring at a point $P \in V$. For this, we will need to introduce the maximal ideal M_P of functions vanishing at P.

Proposition 1.1. *Let V be a variety and $P \in V$. We define the ideal of functions vanishing at P as :*

$$M_p = \left\{ f \in \bar{K}[V] \mid f(P) = 0 \right\}$$

This is a maximal ideal of the coordinate ring $\bar{K}[V]$.

Proof. Let us find an isomorphism between the quotient by M_P and a field.

Let us define φ as :

$$\begin{array}{rccc} \varphi : & \bar{K}[V] & \longrightarrow & \bar{K} \\ & f & \longmapsto & f(P) \end{array}$$

It is surjective because $\overline{Id} \in \bar{K}[V]$ and its kernel is M_p by definition.

By quotient's universal property, φ induces an isomorphism :

$$\begin{array}{rccc} \overline{\varphi} : & \bar{K}[V]/M_P & \longrightarrow & \bar{K} \\ & f & \longmapsto & f(P) \end{array}$$

□

Definition (Local ring at a point)**.** Let V be an affine variety and $P \in V$. We define the **local ring** of V at P as the localization of $\bar{K}[V]$ at M_P.

$$\bar{K}[V]_P = \left\{ \Phi = \frac{f}{g} \in \bar{K}(V) \;\middle|\; f, g \in \bar{K}[V], g(P) \neq 0 \right\}$$

We often denote it by $\mathcal{O}_{V,P}$ and its maximal ideal by $\mathfrak{m}_{V,P}$.

An important quantity linked to a variety is its dimension :

Definition (Dimension of an affine variety)**.** Let V be an affine variety. The **dimension** of V, denoted by $\dim(V)$, is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Example 3. The dimension of $\mathbb{A}^n$ is n because $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, \ldots, X_n)$ and its transcendence degree is naturally n. The dimension of an affine variety defined by a single equation is $n-1$ and the reverse is also true.

Now, we can talk about the regularity of a variety at a point :

Definition (Regularity and singular points)**.** Let V be an affine variety, $f_1, \ldots, f_m \in \bar{K}[X]$ a set of generators for $I(V)$ and $P \in V$. Then V is **smooth** at P if the $m \times n$ jacobian J has rank $n - \dim(V)$:

$$J = \left[\frac{\partial f_i}{\partial X_j} \right]_{i \in [\![1,m]\!], j \in [\![1,n]\!]}$$

If V is **non-singular** at every point, then we say that V is non-singular or smooth.

Remark 4. We have a special case when V is defined by a single equation.

In that case, $\dim(V) = n - 1$ so $P \in V$ in singular if and only if :

$$\frac{\partial f}{\partial X_1}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0$$

There is another useful characterization of smoothness related to M_p which is :

Proposition 1.2. *Let V be a variety and $P \in V$. The quotient ${}^{M_P}\!/_{M_P^2}$ is a finite dimensional $\bar{K}$-vector space. Furthermore, V is smooth at P if and only if $\dim_{\bar{K}} {}^{M_P}\!/_{M_P^2} = \dim(V)$.*

Proof. Let $P = (P_1, \dots, P_n) \in V$. We will prove the result only in the special case in which V is defined by a single equation :

$$V = \{f = 0\} \quad ; \quad I(V) = \langle f \rangle$$

Step 1 : Let us justify that the dimension over $\bar{K}$ of ${}^{M_P}\!/_{M_P^2}$ is defined.

The quotient ${}^{M_P}\!/_{M_P^2}$ is $\bar{K}[V]$-module, annulated by the ideal M_P. Then we have a finite generated module over ${}^{\bar{K}[V]}\!/_{M_P} = \bar{K}$, so a finite dimensional $\bar{K}$-vector space.

Step 2 : To prove the result we will use that φ is a perfect pairing of $\bar{K}$-vector space.

$$\begin{array}{rccc} \varphi : & {}^{M_p}\!/_{M_P^2} \times T_P & \longrightarrow & \bar{K} \\ & \left(\overline{g}, y\right) & \longmapsto & \displaystyle\sum_{i=1}^{n} \frac{\partial \overline{g}}{\partial X_i}(P) y_i = \nabla \overline{g}(P) \cdot y \end{array}$$

Where $T_P = \left\{ y \in \mathbb{A}^n \mid \displaystyle\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(P) y_i = 0 \right\}$.

First of all, we have to prove it is a well-defined map : We have to check the sum does not depend on the choice of a representative element. Let $\overline{g}$ be an element of ${}^{M_p}\!/_{M_P^2}$. We have to understand this quotient to tell something about $\overline{g}$. As we know, $M_p \subseteq \bar{K}[V]$ is a maximal ideal. So, by Hilbert's Nullstellensatz theorem :

$$M_p = \frac{\left\langle X_i - P_i \mid i \in [\![1, n]\!] \right\rangle}{I(V)} = \frac{\langle \underline{X} - \underline{P} \rangle}{I(V)}$$

So now :

$$M_P/M_P^2 \cong \frac{\langle \underline{X} - \underline{P} \rangle}{\langle \underline{X} - \underline{P} \rangle^2 + I(V)}$$

Let g_1 and g_2 be two elements of M_P such that $\overline{g_1} = \overline{g_2}$:

$$\begin{cases} g_1 = \displaystyle\sum_{j=1}^{n} \alpha_j \left(X_j - P_j\right) + h_1 f \\ g_2 = \displaystyle\sum_{j=1}^{n} \beta \left(X_j - P_j\right) + h_2 f \end{cases} \qquad \text{with } \alpha_j, \beta_j \in \bar{K}[V]$$

We have to show that $\varphi\left(\overline{g_1}, y\right) = \varphi\left(\overline{g_2}, y\right)$.

$$\frac{\partial g_1}{\partial X_i}(P) = \frac{\partial}{\partial X_i}\left[\sum_{j=1}^{n} \alpha_j\big(X_j - P_j\big) + h_1 f\right](P) = \alpha_i(P) + h_1(P)\frac{\partial f}{\partial X_i}(P)$$
$$\frac{\partial g_2}{\partial X_i}(P) = \frac{\partial}{\partial X_i}\left[\sum_{j=1}^{n} \beta_j\big(X_j - P_j\big) + h_2 f\right](P) = \beta_i(P) + h_2(P)\frac{\partial f}{\partial X_i}(P)$$

And then, using the fact that $y \in T_p$:

$$\varphi\Big(\overline{g_1}, y\Big) = \sum_{i=1}^{n} \alpha_i(P)y_i + h_1(P)\sum_{i=1}^{n}\frac{\partial f}{\partial X_i}(P)y_i = \sum_{i=1}^{n}\alpha_i(P)y_i$$
$$\varphi\Big(\overline{g_2}, y\Big) = \sum_{i=1}^{n} \beta_i(P)y_i + h_2(P)\sum_{i=1}^{n}\frac{\partial f}{\partial X_i}(P)y_i = \sum_{i=1}^{n}\beta_i(P)y_i$$

And finally, using $g_1 - g_2 = h_3 f$ because it is in $I(V)$:

$$\begin{aligned}\varphi\Big(\overline{g_1}, y\Big) - \varphi\Big(\overline{g_2}, y\Big) &= \sum_{i=1}^{n}(\alpha_i - \beta_i)(P)y_i \\ &= \sum_{i=1}^{n}\frac{\partial g_1 - g_2}{\partial X_i}(P)y_i \\ &= \sum_{i=1}^{n}\frac{\partial h_3 f}{\partial X_i}(P)y_i = h_3(P)\sum_{i=1}^{n}\frac{\partial f}{\partial X_i}(P)y_i = 0\end{aligned}$$

Step 3 : Let us prove that φ is a perfect pairing.

We can easily see that φ is a $\bar{K}$-bilinear map. Moreover it is perfect because :

- Let $y \in T_p$ such that $\forall \overline{g} \in {}^{M_p}\!/_{M_P^2} : \varphi\Big(\overline{g}, y\Big) = 0$.

  Consider $g_i = \alpha_i(X_i - P_i) + h_i f$ with $\alpha_i \neq 0$. Then :

  $$\forall i \in \{1, \dots, n\} : \varphi\Big(\overline{g_i}, y\Big) = \alpha_i y_i = 0 \text{ and then } y_i = 0$$

- Let $\overline{g} \in {}^{M_P}\!/_{M_P^2}$ such that $\forall y \in T_p : \varphi\Big(\overline{g}, y\Big) = 0$, which means $\nabla g(P) \in T_P^{\perp}$.

  If P is singular, then $T_p = \mathbb{A}^n$ and $T_P^{\perp} = \{0\}$ so $\nabla g(P) = 0$ and $g = 0$.

  If P is smooth, then $\dim T_p = n - 1$ and $\dim T_P^{\perp} = 1$. Since $\nabla f(P) \in T_P^{\perp}$ we have $\nabla g(P) = \lambda \nabla f(P)$. Then $g = 0$ in ${}^{M_P}\!/_{M_P^2}$ because :

  $$\begin{array}{rcl} {}^{M_P}\!/_{M_P^2} & \cong & {}^{\bar{K}^n}\!/_{\langle \nabla f(P) \rangle} \\ g = \sum a_\nu (\underline{X} - \underline{P})^\nu & \longmapsto & \nabla g(P) = \big(a_{e_1}, \dots, a_{e_n}\big) \end{array}$$

To conclude, φ is a perfect pairing so $\dim_{\bar{K}} {}^{M_P}\!/_{M_P^2} = \dim T_P$ and P is smooth if and only if $\dim T_P = n - 1$. This concludes the special case $V = \{f = 0\}$. □

1.2 Projective varieties

We will now define projective varieties which are often better than affine ones because they take advantage of the good properties of projective spaces.

Definition (Projective space)**.** The **projective space** of dimension n over K is the set of non-zero $n+1$-tuples modulo collinearity :

$$\mathbb{P}^n = \mathbb{P}^n(\bar{K}) = \frac{\mathbb{A}^n \setminus \{0\}}{\sim}$$

Where $P \sim Q \Leftrightarrow \exists \lambda \in \bar{K}^* : P = \lambda Q$. We denoted by $[x_0, \dots, x_n]$ the equivalence class of P.

As usual, we define the set of K-rational points as :

$$\mathbb{P}^n(K) = \left\{ [x_0, \dots, x_n] \in \mathbb{P}^n \ \mid \ x_i \in K \right\}$$

As we are now working on a quotient, we have to be sure that our polynomials can move to the quotient. This will be possible if they are homogeneous :

Definition (Homogeneous polynomial)**.** A polynomial $f \in \bar{K}[X]$ is said **homogeneous** of degree d if :

$$\forall \lambda \in \bar{K} : f(\lambda X) = \lambda^d f(X)$$

An ideal $I \subseteq \bar{K}[X]$ is said homogeneous if it is generated only by homogeneous polynomials.

Definition (Projective algebraic set)**.** Let I be a homogeneous ideal of $\bar{K}[X] = \bar{K}[X_1, \dots, X_n]$, the ring of polynomials in n variables over $\bar{K}$. A **projective algebraic set** is any set of the form :

$$V = \left\{ P \in \mathbb{P}^n \ \mid \ \forall f \in I \text{ homogeneous } : f(P) = 0 \right\}$$

Each algebraic set V is associated with a homogeneous ideal which is :

$$I(V) = \left\{ f \in \bar{K}[X] \ \mid \ f \text{ homogeneous and } \forall P \in V : f(P) = 0 \right\}$$

We say that an algebraic set V is defined over K if $I(V)$ is generated by homogeneous polynomials in $K[X]$. We denote this by V/K and in this case, the set of K-rational points of V is :

$$V(K) = V \cap \mathbb{P}^n(K)$$

Definition (Projective variety)**.** A projective algebraic set is called **projective variety** if $I(V)$ is a prime ideal in $\bar{K}[X]$.

We want to make a link between affine and projective varieties. We can show that the projective space $\mathbb{P}^n$ is covered by **affine charts** $U_0, \dots, U_n$ which are isomorphic to $\mathbb{A}^n$:

$$U_i = \{X_i \neq 0\}$$

They are included in the projective space and we have a natural bijection :

$$\begin{array}{rccc} \phi_i : & \mathbb{A}^n & \longrightarrow & U_i \subseteq \mathbb{P}^n \\ & (x_1, \dots, x_n) & \longmapsto & [x_1, \dots, x_{i-1}, 1, x_i, \dots, x_n] \end{array}$$

With inverse :

$$\begin{array}{rccc} \phi_i^{-1} : & U_i & \longrightarrow & \mathbb{A}^n \\ & [x_0, \dots, x_n] & \longmapsto & \left(\dfrac{x_0}{x_i}, \dots, \dfrac{x_{i-1}}{x_i}, \dfrac{x_{i+1}}{x_i}, \dots, \dfrac{x_n}{x_i}\right) \end{array}$$

Let V be a projective algebraic set with ideal $I(V) \subseteq \bar{K}[X]$. Let denote $V \cap \mathbb{A}^n$ the space $\phi_i^{-1}(V \cap U_i)$ for a good choice of i. Then :

$$I\big(V \cap \mathbb{A}^n\big) = \Big\{ f\big(Y_1, \dots, Y_{i-1}, 1, Y_i, \dots, Y_n\big) \;\mid\; f(X_0, \dots, X_n) \in I(V) \Big\} \subseteq \bar{K}[Y]$$

This transformation is called **dehomogenization** with respect X_i. The reverse process, called **homogenization**, consist in homogenizing the polynomial using the new variable :

$$\forall f \in \bar{K}[Y] : \qquad \hat{f}(X_0, \dots, X_n) = X_i^d f\left(\frac{X_0}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_n}{X_i}\right) \quad ; \quad X_j = X_i Y_j$$

Where $d = \deg(f)$ is the smallest integer for which $\hat{f}$ is a polynomial.

Definition (Projective closure)**.** Let V be an affine algebraic set seen as subset of $\mathbb{P}^n$. The **projective closure** of V, denoted $\overline{V}$, is the projective algebraic set associated with the homogeneous ideal :

$$I(\overline{V}) = \Big\langle \hat{f}(X) \in \bar{K}[X] \mid f \in I(V) \Big\rangle$$

An important property of the projective closure is the link that it establishes between projective and affine varieties :

Proposition 1.3. *Let V be an affine variety. Then $\overline{V}$ is a projective variety and $V = \overline{V} \cap \mathbb{A}^n$. Let V be a projective variety. Then $V \cap \mathbb{A}^n$ is an affine variety and either $V \cap \mathbb{A}^n = \varnothing$ or $V = \overline{V \cap \mathbb{A}^n}$.*

Proof. [Har77, p. 11, I.2.3] □

Now we can extend the notions defined for affine varieties to projective varieties. For that, we will get back in the affine context and define the properties of protective varieties from the properties of the associated affine varieties.

Definition (Function field)**.** Let V/K be a projective variety. Let us choose an affine chart $U_i \subseteq \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \varnothing$. Then the function field of V is the function field of $V \cap \mathbb{A}^n$.

Definition (Dimension)**.** Let V/K be a projective variety. Let us choose an affine chart $U_i \subseteq \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \varnothing$. Then the dimension of V is the dimension of $V \cap \mathbb{A}^n$.

Definition (Regularity and singular points)**.** Let V be a projective variety and $P \in V$. Let us choose $\mathbb{A}^n \subseteq \mathbb{P}^n$ such that $P \in \mathbb{A}^n$. Then P is singular at P if $V \cap \mathbb{A}^n$ is singular at P.

Definition (Local ring at P)**.** Let V be a projective variety and $P \in V$. Let us choose $\mathbb{A}^n \subseteq \mathbb{P}^n$ such that $P \in \mathbb{A}^n$. Then the local ring of V at P is the local ring of $V \cap \mathbb{A}^n$ at P.

A function $\Phi \in \bar{K}(V)$ is regular or defined at P if $\Phi \in \bar{K}[V]_P$.

1.3 Maps between varieties

As usual, since now we have defined objects we are interested in the link between them, in other words in good maps between them :

Definition (Rational map : First definition)**.** Let V_1 and V_2 be two projective varieties. A **rational map** from V_1 to V_2 is a map :

$$\begin{array}{rccc} \phi : & V_1 & \longrightarrow & V_2 \\ & P & \longmapsto & [f_0, \ldots, f_n] \end{array}$$

Where $f_0, \ldots, f_n \in \bar{K}(V_1)$ satisfy the following condition for all $P \in V_1$ in which they are defined :

$$\phi(P) = \big[f_0(P), \ldots, f_n(P)\big] \in V_2$$

We say that ϕ is defined over K if it exists $\lambda \in \bar{K}^*$ such that $\lambda f_0, \ldots, \lambda f_n \in K(V_1)$.

A rational map ϕ is not necessarily defined on all V_1, but sometimes it can be possible to evaluate ϕ at P even if some f_i are not regular. We regularize the situation by replacing each f_i with gf_i for an appropriate $g \in \bar{K}(V_1)$:

Definition (Morphism : First definition)**.** Let V_1 and V_2 be two projective varieties. A rational map $\phi : V_1 \to V_2$ is said **regular** or **defined** at $P \in V_1$ if there is a function $g \in \bar{K}(V_1)$ such that each gf_i is regular at P and there is one gf_i which is non-zero at P. If such a g exists, we set :

$$\phi(P) = \big[(gf_0)(P), \ldots, (gf_n)(P)\big]$$

A rational map which is regular everywhere is called **morphism**.

As we work with projective spaces, we can clear the denominator which leads to another definitions which only use regular functions :

Definition (Rational map : Reworked definition)**.** Let V_1 and V_2 be two projective varieties. A rational map from V_1 to V_2 is a map :

$$\begin{array}{rccc} \phi : & V_1 & \longrightarrow & V_2 \\ & P & \longmapsto & [\phi_0, \dots, \phi_n] \end{array}$$

Where $\phi_0, \dots, \phi_n \in \bar{K}[V_1]$ are homogeneous polynomials with same degree and not all in $I(V_1)$ such that :

$$\forall f \in I(V_2) : \quad f\big(\phi_0(X), \dots, \phi_n(X)\big) \in I(V_1)$$

Such a ϕ is well-defined provided it exists i such that $\phi_i(P) \neq 0$. However, as before, if all ϕ_i are zero at P, we can alter ϕ to make sense of $\phi(P)$:

Definition (Morphism : Reworked definition)**.** Let V_1 and V_2 be two projective varieties. A rational map $\phi : V_1 \to V_2$ is said regular or defined at $P \in V_1$ if there exists homogeneous polynomials of same degree $\psi_0, \dots, \psi_n \in \bar{K}[X]$ such that at least one is non-zero at P and :

$$\forall i, j : \phi_i \psi_j \equiv \phi_j \psi_i \mod I(V_1)$$

If this occurs, we set $\phi(P) = \big[\psi_0(P), \dots, \psi_n(P)\big]$. A rational map which is regular everywhere is called morphism.

Definition (Isomorphism)**.** Let V_1 and V_2 be two varieties.

- An **isomorphism** between V_1 and V_2 is a morphism $\phi : V_1 \to V_2$ such that it exists a morphism $\psi : V_2 \to V_1$ satisfying $\psi \circ \phi$ and $\phi \circ \psi$ are identity maps on V_1 and V_2 respectively.
- We say that V_1 and V_2 are **isomorphic**, denoted $V_1 \cong V_2$, if it exists an isomorphism between them. We say that V_1/K and V_2/K are isomorphic over K if the morphisms ϕ and ψ can be defined over K.

Exercise 1 (Silverman I.1.6). Let V be the variety defined by $Y^2Z = X^3 + Z^3$.

Show the map ϕ is a morphism :

$$\begin{array}{rccc} \phi : & V & \longrightarrow & \mathbb{P}^2 \\ & [X, Y, Z] & \longmapsto & \left[X^2, XY, Z^2\right] \end{array}$$

Answer. Let us focus on $P = [0, 1, 0]$ which is the only point where ϕ is not clearly regular.

Method 1 :

To prove that ϕ is regular at P, we can find $g \in \bar{K}(V)$ such that all $g\phi_i$'s are regular and at least one is non-zero.

After some calculations, we find a solution $g = \dfrac{X^2Y}{Z}$. Then we can calculate $\phi(P)$:

$$\phi(P) = \left[XZ\left(Y^2 - Z^2\right), Y^2\left(Y^2 - Z^2\right), X^2YZ\right](P) = [0,1,0]$$

So ϕ is regular at P and then it is a morphism.

Method 2 :

Another equivalent solution is to find ψ_0, ψ_1 and ψ_2 such that :

- The ψ_i's are homogeneous polynomials in $\bar{K}[X]$ with the same degree.
- The image of P is not zero : $\exists i : \psi_i(P) \neq 0$.
- The cross products are equals : $\forall i, j : \phi_i\psi_j \equiv \phi_j\psi_i \mod I(V)$.

The aim is to alter ϕ by replacing it by the ψ_i's. The ψ_i's are chosen in respect of $I(V)$ to preserve ϕ, this is what the last condition says. It is a way to define the same function ϕ at P.

Well, let us find the ψ_i's. We are looking for something which is non-zero at P :

$$Y^2Z = X^3 + Z^3 \Rightarrow X^3 = Z\left(Y^2 - Z^2\right) \Rightarrow \frac{X^3}{Z} = Y^2 - Z^2$$

Let put $\psi_1 = Y^2 - Z^2$ at first. Let us check some conditions :

$$\phi_0\psi_1 = \phi_1\psi_0 \Leftrightarrow X^2\left(Y^2 - Z^2\right) = XY\psi_0$$

We see we miss a Y, so let correct : $\psi_1 = Y\left(Y^2 - Z^2\right)$. Now :

$$\phi_0\psi_1 = \phi_1\psi_0 \Leftrightarrow X^2Y\left(Y^2 - Z^2\right) = XY\psi_0 \Rightarrow \psi_0 = X\left(Y^2 - Z^2\right)$$

Let us check another condition :

$$\phi_0\psi_2 = \phi_2\psi_0 \Leftrightarrow X^2\psi_2 = Z^2X\left(Y^2 - Z^2\right) = ZX^4 \Rightarrow \psi_2 = ZX^2$$

Let us verify the last one :

$$\phi_1\psi_2 = \phi_2\psi_1 \Leftrightarrow XYZX^2 = Z^2Y\left(Y^2 - Z^2\right) \text{ yet } YZX^3 = YZ^2\left(Y^2 - Z^2\right)$$

So ϕ is regular at P and $\phi(P) = \left[\psi_0(P), \psi_1(P), \psi_2(P)\right] = [0,1,0]$.

Then, ϕ is regular on V, it is a morphism.

However $\phi : \mathbb{P}^2 \to \mathbb{P}^2$ cannot be a morphism because we have seen the ϕ_i's have a common zero which is P. Then, as $I(\mathbb{P}^2) = \{0\}$, we cannot alter the ϕ_i's to regulate the situation like we did before : ϕ is not regular at P.

Exercise 2 (Silverman I.1.7). Let V be the variety defined by $Y^2Z = X^3$ and let ϕ be the map :

$$\begin{array}{rccc} \phi : & \mathbb{P}^1 & \longrightarrow & V \\ & [S,T] & \longmapsto & \left[S^2T, S^3, T^3\right] \end{array}$$

1. Show that ϕ is a morphism.
2. Find a rational map $\psi : V \to \mathbb{P}^1$ so that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps wherever they are defined.
3. Is ϕ an isomorphism ?

Answer. Let us develop all the details.

The map ϕ is regular everywhere. Moreover, $\forall P \in \mathbb{P}^1$, $\phi(P) \in V$ because :

$$X^3 = \left(S^2T\right)^3 = \left(S^3\right)^2 T^3 = Y^2Z$$

Then ϕ is a morphism. An inverse, where it can be defined, is :

$$\psi = \left[X^5, Z^2Y^3\right] = \left[X^2, YZ\right] = [Y, X]$$

We can verify :

$$\begin{aligned} \psi\left(\left[S^2T, S^3, T^3\right]\right) &= \left[S^3, S^2T\right] = [S,T] \\ \phi\big([Y,X]\big) &= \left[Y^2X, Y^3, X^3\right] = \left[Y^2X, Y^3, Y^2Z\right] = [X,Y,Z] \end{aligned}$$

Now, the question is : Does that inverse make ϕ be an isomorphism ? The first indication is to see that V is singular while $\mathbb{P}^1$ is smooth. Then ϕ cannot be a isomorphism.

This is concluding the exercise but I would like to develop. We know that P is singular so his local ring cannot be a regular local ring. That means $\mathfrak{m}_{V,P}$ is not principal.

As $\mathfrak{m}_{\mathbb{P}^1,Q}$ is principal, ϕ^* cannot be an isomorphism :

$$\begin{array}{rccc} \phi^* : & \mathcal{O}_{V,P} & \longrightarrow & \mathcal{O}_{\mathbb{P}^1,Q} \\ & f & \longmapsto & f \circ \phi \end{array} \qquad \text{where } Q = [0,1] \text{ and } \phi(Q) = P$$

We conclude that ϕ is not a isomorphism.

To develop a bit more, we will prove that $\mathcal{O}_{V,P}$ is not regular without using that P is singular. We will use Nakayama's lemma to prove that the maximal ideal of $\mathcal{O}_{V,P}$ cannot be generated by a single element.

We will work in the affine chart $\{Z = 1\} \ni P$. We have :

$$\mathcal{O}_{V,P} = \left(\frac{\bar{K}[X,Y]}{\langle X^3 - Y^2\rangle}\right)_{\langle \overline{X},\overline{Y}\rangle} \quad ; \quad \mathcal{O}_{\mathbb{P}^1,Q} = K[S]_{\langle S\rangle}$$

The aim is to prove that $\left\langle \overline{X}, \overline{Y} \right\rangle$ cannot be generated by a single element.

Let us remind the Nakayama's lemma :

Lemma 1.4 (Nakayama). *Let* $(R, \mathfrak{m})$ *be a local ring and* M *be a finitely generated* R*-module. Then* $M/\mathfrak{m}M$ *has a structure of* $R/\mathfrak{m}$*-vector space and the set* $\{m_1, \dots, m_k\}$ *is a minimal generator set for* M *if and only if* $\{\overline{m_1}, \dots, \overline{m_k}\}$ *is a basis for* $M/\mathfrak{m}M$.

Let us denote $A = \dfrac{\bar{K}[X,Y]}{\langle X^3 - Y^2 \rangle}$ and $\mathfrak{m} = \left\langle \overline{X}, \overline{Y} \right\rangle$. Then $\mathfrak{m}A_{\mathfrak{m}}$ is a finite generated A-module and $\{\overline{X}, \overline{Y}\}$ is basis of $\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}}$:

Now, we can notice that :

$$\mathfrak{m}^2 = \left\langle \overline{X}^2, \overline{XY}, \overline{Y}^2 \right\rangle = \left\langle \overline{X}^2, \overline{XY}, \overline{X}^3 \right\rangle = \left\langle \overline{X}^2, \overline{XY} \right\rangle$$

Let α and β be in $\bar{K}$. Then :

$$\begin{aligned}
& \alpha\overline{X} + \beta\overline{Y} = 0 \text{ in } \mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}} \\
\Leftrightarrow \quad & \alpha\overline{X} + \beta\overline{Y} \in \mathfrak{m}^2A_{\mathfrak{m}} = \left\langle \overline{X}^2, \overline{XY} \right\rangle \text{ in } A \\
\Leftrightarrow \quad & \alpha\overline{X} + \beta\overline{Y} = G\overline{X}^2 + H\overline{XY} \text{ in } A \text{ where } G, H \in A_{\mathfrak{m}} \\
\Leftrightarrow \quad & P\left(\alpha\overline{X} + \beta\overline{Y}\right) = Q\overline{X}^2 + R\overline{XY} \text{ in } A \text{ where } P, Q, R \in A \text{ and } P \notin \mathfrak{m} \\
\Leftrightarrow \quad & P(\alpha X + \beta Y) - QX^2 - RXY \in \langle X^3 - Y^2 \rangle \text{ in } \bar{K}[X,Y] \\
\Leftrightarrow \quad & P_{0,0}\alpha X + P_{0,0}\beta Y = 0 \text{ in } \bar{K}[X,Y] \\
\Leftrightarrow \quad & P_{0,0}\alpha = P_{0,0}\beta = 0 \Leftrightarrow \alpha = \beta = 0 \text{ because } P_{0,0} \neq 0
\end{aligned}$$

And we conclude that $\{\overline{X}, \overline{Y}\}$ is a basis of $\dfrac{\mathfrak{m}A_{\mathfrak{m}}}{\mathfrak{m}^2A_{\mathfrak{m}}}$ so the cardinal of a minimal set of generators for $\mathfrak{m}A_{\mathfrak{m}}$ is 2. We have proved that $\mathcal{O}_{V,P}$ is not a regular ring, which concludes.

Chapter 2

Algebraic curves

Now we will focus our study on curves which are the varieties of dimension 1, and more specifically we will often work with smooth curves. Our aim is to study the general geometric properties of curves and to define the genus of a curve. Thus, we will be able to define the main object of our subject : the elliptic curves which are the curves of genus 1.

2.1 Curves

Definition (Curves)**.** We call **projective curve** any projective variety of dimension 1.

From now on, all curves will be understood as projective. A very important property in the case of smooth curves is that the locals rings $\bar{K}[C]_P$ are discrete valuation rings.

Definition (Discrete valuation ring)**.** A **discrete valuation** on a ring R is a function :

$$\nu : R \setminus \{0\} \longrightarrow \mathbb{Z}$$

Which satisfies for all $x, y \in R \setminus \{0\}$:

- $\nu(xy) = \nu(x) + \nu(y)$
- $\nu(x + y) \geqslant \min\{\nu(x), \nu(y)\}$

A **discrete valuation ring** is a ring admitting a discrete valuation ν.

Proposition 2.1. *A ring is a discrete valuation ring if and only if it is a principal ideal domain with only one non-zero maximal ideal.*

Proposition 2.2. *Let C be a curve and $P \in C$ a smooth point. Then $\bar{K}[C]_P$ is a discrete valuation ring. Its maximal ideal M_P is principal.*

Proof.

We know that $\bar{K}[C]_P$ is a local ring defined as the localisation at P, ie. relative to the maximal ideal M_P. Let us show that M_P is principal. Since P is a smooth point, we know from [1.2] that :

$$\dim_{\bar{K}} {}^{M_P}\!/_{M_P^2} = 1$$

Then by Nakayama [1.4], M_P is principal and we conclude that $\bar{K}[C]_P$ is a discrete valuation ring using [2.1]. □

Let us define the valuation on our locals fields $\bar{K}[C]_P$:

Definition (Valuation on $\mathcal{O}_{C,P}$)**.** Let C be a curve and $P \in C$ a smooth point. The **normalized valuation** on $\bar{K}[C]_P$ is defined by :

$$\begin{array}{rccl} \mathrm{ord}_P : & \bar{K}[C]_P & \longrightarrow & \mathbb{N} \cup \{\infty\} \\ & f & \longmapsto & \mathrm{ord}_P(f) = \max\left\{ d \in \mathbb{N} \mid f \in M_P^d \right\} \end{array}$$

We can extend $\mathrm{ord}_P : \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}$ by defining :

$$\mathrm{ord}_P\left(\frac{f}{g}\right) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$$

A **uniformizer** for C at P is a generator of the principal maximal ideal M_P, this means a function $\pi \in \bar{K}(C)$ such as $\mathrm{ord}_P(\pi) = 1$.

Definition (Order of function)**.** Let C be a curve and $P \in C$ a smooth point. The **order** of f at P is $\mathrm{ord}_P(f)$.

- If $\mathrm{ord}_P(f) > 0$ then f has a **zero** at P.
- If $\mathrm{ord}_P(f) < 0$ then f has a **pole** at P.

If $\mathrm{ord}_P(f) \geqslant 0$ then f is **regular** or **defined** at P. Otherwise f has a pole and we set $f(P) = \infty$. The order of f at P is the multiplicity of the zero or the pole of f at P.

Proposition 2.3. *Let C be a smooth curve and $f \in \bar{K}(C)^*$. Then there are only finitely many points of C at which f has a zero or a pole. If f has no poles, then $f \in \bar{K}$.*

Proof. See [Har77, p. 41, I.6.5] for the finiteness of poles. The finiteness of zeros is deduced considering $1/f$. For the last statement, see [Har77, p. 18, I.3.4]. □

2.2 Map between curves

In the case of curves, we have a bijection :

$$\begin{array}{rcl} K(C) \cup \{\infty\} & \longleftrightarrow & \{f : C \to \mathbb{P}^1 \text{ defined over } K\} \\ f & \longmapsto & \phi = \begin{cases} [1,0] & \text{at poles of } f \\ [f,1] & \text{otherwise} \end{cases} \end{array}$$

Let C/K be a smooth curve and $f \in K(C)$. Then f defines a rational map :

$$\begin{array}{rccc} f : & C & \longrightarrow & \mathbb{P}^1 \\ & P & \longmapsto & \big[f(P), 1\big] \end{array}$$

Using the next proposition, f is a morphism, given by :

$$f(P) = \begin{cases} [1,0] = \infty & \text{if } f \text{ has a pole at } P \\ \big[f(P), 1\big] & \text{if } f \text{ is regular at } P \end{cases}$$

Conversely, let $\phi : C \to \mathbb{P}^1$ be the rational map defined over K by $\phi = [f, g]$. Then :

- Either $g = 0$ and in this case ϕ is the constant map $[1,0]$ and we denote $\phi = \infty$.
- Or $g \neq 0$ and ϕ correspond to the function $\dfrac{f}{g} \in K(C)$.

The next proposition is an important result which will motivate us to work with smooth curves :

Proposition 2.4. *Le C be a curve and $P \in C$ a smooth point. Let $\phi : C \to V$ be a rational map to a variety $V \subseteq \mathbb{P}^N$. Then ϕ is regular at P. In particular, if C is smooth ϕ is a morphism.*

Proof. Let us define $\phi = [f_0, \ldots, f_N]$ with $f_i \in \bar{K}(C)$. Let us choose an uniformizer $t \in \bar{K}(C)$ for C at P. For $n = \min\{\operatorname{ord}_P f_i \mid i \in [\![0, N]\!]\}$ we have $\operatorname{ord}_P\big(t^{-n} f_i\big) \geqslant 0$ and equal zero for at least one i. Then each $t^{-n} f_i$ is regular at P and they are not all zero. We conclude that ϕ is regular at P. □

Theorem 2.5. *Let C_1 and C_2 be two curves and $\phi : C_1 \to C_2$ a morphism. Then ϕ is either constant or surjective.*

Proof. [Har77, p. 137, II.6.8] □

Definition (Induced map on function field)**.** Let C_1/K and C_2/K be two curves and $\phi : C_1 \to C_2$ a non-constant rational map defined over K. Then the composition by ϕ induces an injection on function fields :

$$\begin{array}{rccc} \phi^* : & K(C_2) & \longrightarrow & K(C_1) \\ & f & \longmapsto & \phi^* f = f \circ \phi \end{array}$$

Definition (Degree of map of curves)**.** Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the **degree** of ϕ to be 0. Otherwise we define its degree to be as :

$$\deg \phi = \left[K(C_1) : \phi^* K(C_2)\right]$$

Proposition 2.6. *Let C_1 and C_2 be smooth curves and let $\phi : C_1 \to C_2$ be a map of degree* 1*. Then ϕ is an isomorphism.*

Proof. [Sil86, p. 21, II.2.4.1] □

Definition (Ramification index)**.** Let C_1 and C_2 be two smooth curves and $\phi : C_1 \to C_2$ a non-constant map. The **ramification index** of ϕ at $P \in C_1$, denoted $e_\phi(P)$, is defined by :

$$e_\phi(P) = \mathrm{ord}_P\left(\phi^* t_{\phi P}\right) \text{ where } t_{\phi P} \in K(C_2) \text{ is a uniformizer at } \phi(P)$$

A map ϕ is said **unramified** at P if $e_\phi(P) = 1$ and unramified if it is unramified at every point.

Remark 5. The notion of ramification is a generalisation of the notion of multiplicity of a zero or a pole but for any point. To give an intuition, let us remind the classical case :

Let h be a holomorphic function with a zero of multiplicity m at x_0. Then :

$$h(x_0) = 0 \quad ; \quad h(x) = 0 + \cdots + 0 + \frac{h^{(m)}(x_0)}{m!}(x - x_0)^m + \cdots$$

We notice that h has the same behaviour at x_0 than $x \mapsto (x - x_0)^m$. Let us generalise the description of the behaviour at a point by saying that for $h(x_0) = y_0$, h is ramified of order e if :

$$h(x_0) = y_0 \quad ; \quad h(x) = y_0 + \cdots + 0 + \frac{h^{(m)}(x_0)}{m!}(x - x_0)^e + \cdots$$

So h has the same behaviour at x_0 than $x \mapsto y_0 + (x - x_0)^e$. The behaviour at a point can be expressed as a power e and that is exactly why we introduce the ramification index.

Well, we would like to say that ϕ is ramified at P_0 with index ramification e if :

$$\text{“ } \phi(P_0) = Q \quad ; \quad \phi(P) = Q + 0 + \cdots + 0 + \frac{\phi^{(e)}(P_0)}{e!}(P - P_0)^e + \cdots \text{ ”}$$

But that is not defined because we obviously could not talk about addition or derivative. The idea to generalize it is to say that $\phi : C_1 \to C_2$ is ramified at P_0 with ramification index e if e is the highest power of t dividing $\phi^* s$ according to the following diagram :

$$\begin{array}{ccc} C_1 & \xrightarrow{\quad\phi\quad} & C_2 \\ \\ \mathcal{O}_{C_1,P} & \xleftarrow[\phi^*]{} & \mathcal{O}_{C_2,Q} \\ \uparrow & & \uparrow \\ \mathfrak{m}_{C_1,P} = \langle t \rangle & & \mathfrak{m}_{C_2,Q} = \langle s \rangle \\ \uparrow & \swarrow_{\phi^*} & \\ I = \langle \phi^*(s) \rangle = \mathfrak{m}^e_{C_1,P} & & \end{array}$$

We keep the intuition of expressing ϕ as a power of a fundamental element : the uniformizer. In this construction, the uniformizer t plays the role of "$P - P_0$".

To conclude, to talk locally about the behaviour of a function between curves at a point, it is enough to talk about the highest power of the uniformizer dividing this function in the local ring associated to this point.

Proposition 2.7. *Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves and $f \in K(C_2)^*$.*

$$\operatorname{ord}_P\left(\phi^* f\right) = e_{\phi(P)} \operatorname{ord}_{\phi(P)}(f)$$

Proof. As C_1 and C_2 are smooth curves, $\mathcal{O}_{C_1,P}$ and $\mathcal{O}_{C_2,\phi P}$ are regular local rings.

That means $\mathfrak{m}_{C_1,P}$ and $\mathfrak{m}_{C_2,\phi P}$ are principal. Once again we have the following diagram :

$$\begin{array}{ccccc} C_1 & \xrightarrow{\quad\phi\quad} & C_2 & \xrightarrow{\quad f\quad} & K \\ & & \mathcal{O}_{C_1,P} & \xleftarrow{\phi^*} & \mathcal{O}_{C_2,\phi P} \\ & & \uparrow & & \uparrow \\ & & \mathfrak{m}_{C_1,P} = \langle s \rangle & & \mathfrak{m}_{C_2,\phi P} = \langle t \rangle \\ & & \uparrow & \swarrow_{\phi^*(\mathfrak{m}_{C_2,\phi P})} & \\ & & \langle \phi^*(t) \rangle = \mathfrak{m}^e_{C_1,P} & & \end{array}$$

Let $f_{\phi P} \in \mathcal{O}_{C_2,\phi P}$ be the germ of f around $\phi(P)$ and ν be the order of $f_{\phi P}$ at $\phi(P)$. Then $f_{\phi P} = u t^\nu$ where u is a unit of $\mathcal{O}_{C_2,\phi P}$ and we have $\phi^*\left(f_{\phi P}\right) = \phi^*(u t^\nu) = \phi^*(u)\phi^*(t)^\nu \in \mathfrak{m}^e_{C_1,P}$. Indeed, we have $\left\langle \phi^*(t) \right\rangle = \mathfrak{m}^e_{C_1,P} = \langle s^e \rangle$ with by definition $e = e_\phi(P)$. So $\phi^*(t) = \nu s^e$ and :

$$\phi^*\left(f_{\phi P}\right) = \phi^*(u)\phi^*(t)^\nu = \phi^*(u)\nu^\nu\left(s^e\right)^\nu$$

To conclude :

$$\mathrm{ord}_P\left(\phi^* f\right) = e\nu = e_\phi(P)\,\mathrm{ord}_{\phi P}(f)$$

□

Proposition 2.8. *Let $\phi : C_1 \to C_2$ and $\psi : C_2 \to C_3$ two non-constant maps of smooth curves. We have a link between degree and ramification :*

$$\forall Q \in C_2 : \quad \deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$$

Then, ϕ is unramified if and only if $\forall Q \in C_2 : \deg(\phi) = \sharp\phi^{-1}(Q)$.

Plus, ramification index is compatible with composition :

$$\forall P \in C_1 : \quad e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi P)$$

Proof. [Har77, pp. 137-138, II.6.8, II.6.9] □

2.3 Divisors

Divisors are weighted sums of points which can be used to characterise the multiplicity of functions at each point. It is a notion needed to state the Riemann-Roch theorem and then to define the genus of a curve.

Definition (Divisor group)**.** Let C be a curve. The **divisor group** of C, denoted $\mathrm{Div}(C)$, is the free abelian group generated by the points of C.

The elements of $\mathrm{Div}(C)$, the **divisors** of C, are formal sums :

$$D = \sum_{P \in C} n_P \cdot (P) \text{ where } n_P \in \mathbb{Z} \text{ are all zero except for finitely many } P \in C.$$

Definition (Degree of a divisor)**.** Let C be a curve and $D \in \mathrm{Div}(C)$. The **degree** of D is :

$$\deg(D) = \sum_{P \in C} n_P$$

Definition (Special divisor group)**.** Let C be a curve. We define the group of divisors of degree 0 as :

$$\mathrm{Div}^0(C) = \left\{D \in \mathrm{Div}(C) \mid \deg(D) = 0\right\}$$

We define the group of divisors defined over K as :

$$\mathrm{Div}_K(C) = \left\{D \in \mathrm{Div}(C) \mid \forall \sigma \in G_{\bar{K}/K} : D^\sigma = D\right\}$$

Remark 6. The action of the Galois group $G_{\bar{K}/K}$ on projective points is $P^\sigma = \left[x_0^\sigma, \dots, x_n^\sigma\right]$ then the action over divisors is defined by :

$$D^\sigma = \Big(\sum_{P\in C} n_P \cdot (P)\Big)^\sigma = \sum_{P\in C} n_P \cdot \left(P^\sigma\right)$$

Definition (Divisor of a map)**.** Let C be a smooth curve and $f \in \bar{K}(C)^*$. We can associate to f the divisor $\mathrm{div}(f)$ given by :

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

Remark 7. Let us recall that $\mathrm{ord}_P(f)$ is non zero if and only if P is a zero or a pole of f. So it is well defined because from [2.3], the number of poles and zeros is finite. Then the divisor associated to a function is the weighted sum of its zeros and poles. Coefficients of the weighting are the multiplicities.

Remark 8. If $f \in K(C)$ then $\mathrm{div}(f)^\sigma = \mathrm{div}(f^\sigma) = \mathrm{div}(f)$ so $\mathrm{div}(f) \in \mathrm{Div}_K(C)$.

Definition (Principal divisors and Picard group)**.** Let C be a smooth curve. A divisor $D \in \mathrm{Div}(C)$ is **principal** if it exists $f \in \bar{K}(C)^*$ such as $D = \mathrm{div}(f)$. Two divisors D_1 and D_2 are **linearly equivalent** if $D_1 - D_2$ is principal.

The **divisor class group**, denoted $\mathrm{Pic}(C)$ is the quotient of $\mathrm{Div}(C)$ by the subgroup of principal divisors. We define $\mathrm{Pic}_K(C)$ as the subgroup of $\mathrm{Pic}(C)$ fixed by $G_{\bar{K}/K}$.

Proposition 2.9. *Let C be a smooth curve and $f \in \bar{K}(C)^*$. Then $\mathrm{div}(f) = 0$ if and only if $f \in \bar{K}^*$. And we know that f has the same number of zero and poles :*

$$\deg \mathrm{div}(f) = 0$$

Proof. Look at the remark [10]. □

Definition (Induced map on divisors)**.** Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. Then ϕ induces a $\mathbb{Z}$-linear map :

$$\begin{array}{rccc} \phi^* : & \mathrm{Div}(C_2) & \longrightarrow & \mathrm{Div}(C_1) \\ & (Q) & \longmapsto & \displaystyle\sum_{P\in\phi^{-1}(Q)} e_\phi(P) \cdot (P) \end{array}$$

Remark 9. Let C be a smooth curve and $f \in \bar{K}(C)^*$ be a non-constant polynomial.

As we have seen, f induces a map $f : C \to \mathbb{P}^1$ and then $f^* : \mathrm{Div}\,(\mathbb{P}^1) \to \mathrm{Div}(C)$.

Finally, we remark that $\mathrm{div}(f) = f^*\big((0) - (\infty)\big)$. It is a special case where we are looking at the image of the difference between the two special points (0) and (∞). We are looking at the order of zeros and poles.

Proposition 2.10. *Let* $\phi : C_1 \to C_2$ *and* $\psi : C_2 \to C_3$ *be two non-constant maps of smooth curves. Then* $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ *and* $\forall D \in \mathrm{Div}(C_2), \forall f \in \bar{K}(C_2)^*$ *:*

$$\deg\big(\phi^* D\big) = \big(\deg \phi\big)\big(\deg D\big) \quad ; \quad \phi^*\big(\mathrm{div}(f)\big) = \mathrm{div}\big(\phi^* f\big)$$

Proof. [Sil86, p. 29, II.3.6] □

Remark 10. Now we can prove easily that, for $f \in \bar{K}(C)$:

$$\deg \mathrm{div}(f) = \deg f^*\big((0) - (\infty)\big) = \deg(f) - \deg(f) = 0$$

2.4 Differentials

Our goal in this section is to define the canonical divisor which is used in the Riemann-Roch theorem. It is the last notion we need to define the genus algebraically.

Definition (Differentials)**.** Let C be a curve. We denoted by Ω_C the **space of meromorphic differential** forms on C. It is the $\bar{K}$-vector space generated by the **differentials**, the symbols dx for $x \in \bar{K}(C)$ satisfying :

- $\forall x, y \in \bar{K}(C) : d(x + y) = dx + dy$
- $\forall x, y \in \bar{K}(C) : d(xy) = x\,dy + y\,dx$
- $\forall a \in \bar{K} : \qquad da = 0$

Definition (Induced map on differentials)**.** Let $\phi : C_1 \to C_2$ be a non-constant map of curves. The associated field map $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ induces a map on differentials :

$$\begin{array}{rccc} \phi^* : & \Omega_{C_1} & \longrightarrow & \Omega_{C_2} \\ & \sum f_i\,dx_i & \longmapsto & \sum \big(\phi^* f_i\big)\,d\big(\phi^* x_i\big) \end{array}$$

Proposition 2.11. *Let* C *be a curve. Then* Ω_C *is a one dimensional* $\bar{K}(C)$*-vector space.*

Proof. [Mat80, 27.A.B] □

Proposition 2.12. *Let* C *be a curve,* $P \in C$ *and* $t \in \bar{K}(C)$ *a uniformizer at* P*. Then for each* $\omega \in \Omega_C$*, it exists a unique* $g \in \bar{K}(C)$ *which only depends on* ω *and* t *and satisfies :*

$$\omega = g\,dt$$

The function g *is denoted by* $\dfrac{\omega}{dt}$.

Proof. [Sil86, p.31, II.4.3] □

Definition (Order on differentials)**.** Let C be a curve, $P \in C$ and $t \in \bar{K}(C)$ a uniformizer at P. Then we define the order of $\omega \in \Omega_C$ at P as :

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(\frac{\omega}{dt}\right)$$

This quantity is well defined because it is independent of the choice of the uniformizer.

Proof. Let us show that $\mathrm{ord}_P(\omega)$ does not depends on the choice of the uniformizer.

Let t and t' be two different uniformizers at P. Then $\dfrac{dt}{dt'}$ is regular at P from the next lemma and we conclude using :

$$\mathrm{ord}_P\left(\frac{\omega}{dt}\right) = \mathrm{ord}_P\left(\frac{\omega}{dt}\frac{dt}{dt'}\right) = \mathrm{ord}_P\left(\frac{\omega}{dt'}\right) + \mathrm{ord}_P\left(\frac{dt}{dt'}\right) = \mathrm{ord}_P\left(\frac{\omega}{dt'}\right)$$

□

Lemma 2.13. *Let C be a curve, $P \in C$ and $t \in \bar{K}(C)^*$ a uniformizer at P. Let $f \in \bar{K}(C)^*$ be regular at P. Then $\dfrac{df}{dt}$ is regular at P.*

Proof. [Har77, p. 300] □

Proposition 2.14. *Let C be a curve and $\omega \in \Omega_C$ be a non-zero differential. Then $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.*

Proof. [Sil86, p. 31, II.4.3] □

We can now define the divisor of a differential :

Definition (Divisor of differentials)**.** Let ω be a differential on C. The divisor associated to $\omega \in \Omega_C$ is the formal sum :

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

The differential ω is said :

- **regular** or **holomorphic** if $\forall P \in C : \mathrm{ord}_P(\omega) \geqslant 0$.
- **non-vanishing** if $\forall P \in C : \mathrm{ord}_P(\omega) \leqslant 0$.

Definition (Canonical divisor)**.** Let C be a curve. The **canonical divisor class** on C is the class of $\mathrm{div}(\omega)$ seen in $\mathrm{Pic}(C)$ for any non-zero differential $\omega \in \Omega_C$. We call **canonical divisor** any element of $\mathrm{Div}(C)$ for which its class in $\mathrm{Pic}(C)$ is the canonical divisor class.

Remark 11. Canonical divisor class is well defined because for ω_1 and ω_2 two non-zero differentials, it exists a function $f \in \bar{K}(C)^*$ such that $\omega_1 = f\omega_2$. Then :

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$$

Then the image of $\mathrm{div}(\omega_1)$ and $\mathrm{div}(\omega_2)$ is the same in $\mathrm{Pic}(C)$. A canonical divisor is simply a divisor D which can be written as $D = \mathrm{div}(\omega)$ where ω is a non-zero differential.

Example 4. The canonical divisor of the projective line $\mathbb{P}^1$ is $K_{\mathbb{P}^1} = -2(\infty)$.

Indeed, let $x \in \bar{K}[\mathbb{P}^1] \subseteq \bar{K}(\mathbb{P}^1)$ be the coordinate function. We are looking for the value :

$$\mathrm{div}\big(dx\big) = \sum_{P \in \mathbb{P}^1} \mathrm{ord}_P\big(df\big) \cdot (P)$$

Let P be an element of the affine chart $U_0 = \{P = [x, y] \mid x \neq 0\}$. We can take $t = x - x(P)$ as uniformizer at P. Then :

$$\mathrm{ord}_P\big(dx\big) = \mathrm{ord}_P\Big(d\big(x - x(P)\big)\Big) = \mathrm{ord}_P(1) = 0$$

At the infinity, we take $\dfrac{1}{x}$ as uniformizer and then :

$$\mathrm{ord}_\infty\big(dx\big) = \mathrm{ord}_\infty\left(-x^2\, d\frac{1}{x}\right) = \mathrm{ord}_\infty\Big(-x^2\Big) = -2$$

Because polynomials over $\mathbb{P}^1$ of degree d have a pole of multiplicity d at ∞.

2.5 Riemann-Roch theorem

We will now enunciate the Riemann-Roch theorem which algebraically define the notion of genus of a curve as the unique integer g which satisfies a given equation.

In the case of a smooth projective curve C defined over the complex numbers, the notion of genus we will define coincides with the topological genus associated with C seen as a Riemann surface. However, as we will work over general fields we need this algebraic definition but the idea is similar.

To state this equation we have to start by defining the space $\mathscr{L}(D)$.

Definition (Ordering relation on divisors)**.** Let C be a curve and $D \in \mathrm{Div}(C)$.

- We say that D is **positive**, denoted $D \geqslant 0$, if $n_P \geqslant 0$ for all $P \in C$.
- We say than D_1 is **greater than** D_2, denoted $D_1 \geqslant D_2$, if $D_1 - D_2$ is positive.

Remark 12. The comparison between divisors is an easy way to impose conditions about multiplicity order of zeros or poles at a point. For example, $\operatorname{div}(f) \geqslant (P) - n(Q)$ means f is a regular function with at least one zero at P and a pole at most order n at Q.

This is a direct consequence of the definition of $\operatorname{div}(f)$ as $f^*\big((0) - (\infty)\big)$.

Definition ($\mathscr{L}(D)$ space)**.** Let C be a smooth curve and $D \in \operatorname{Div}(C)$ a divisor. We define $\mathscr{L}(D)$ as the set of maps with divisor greater than $-D$:

$$\mathscr{L}(D) = \left\{ f \in \bar{K}(C)^* \mid \operatorname{div}(f) \geqslant -D \right\} \cup \{0\}$$

Remark 13. Thus $\mathscr{L}(D)$ is the set of functions f which have poles at P with multiplicity at most n_P for all $n_P > 0$ and zeros at P with multiplicity at least n_P for all $n_P < 0$.

Proposition 2.15. *Let C be a curve and $D \in \operatorname{Div}(C)$. Then $\mathscr{L}(D)$ is a finite dimensional $\bar{K}$-vector space and we denote by $\ell(D)$ its dimension $\dim_{\bar{K}} \mathscr{L}(D)$.*

Moreover :

- *If $D < 0$ then $\mathscr{L}(D) = \{0\}$ and $\ell(D) = 0$.*
- *If $D' \sim D$ then $\mathscr{L}\big(D'\big) \cong \mathscr{L}(D)$ and $\ell\big(D'\big) = \ell(D)$.*

Proof. For the finiteness of the dimension, see [Har77, II.5.19].

Now, let us prove the two other results. Let $f \in \mathscr{L}(D)$ a non-zero function. Then :

$$\deg \operatorname{div}(f) = 0 \text{ and } 0 \geqslant \deg(-D) = -\deg(D) \text{ then } \deg(D) \geqslant 0$$

Finally, if $D' \sim D$ then $D = D' + \operatorname{div}(g)$ and the map $f \mapsto fg$ is an isomorphism between $\mathscr{L}(D)$ and $\mathscr{L}\big(D'\big)$. □

Let us finally state this Riemann-Roch theorem :

Theorem 2.16 (Riemann-Roch 1865)**.** *Let C be a smooth curve and K_C a canonical divisor. Then it exists an integer $g \geqslant 0$ such that for all $D \in \operatorname{Div}(C)$:*

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

*This integer g is called **genus** of the curve C.*

Proof. See at [Har77, IV.1.3]. □

Corollary 2.17. *Let C be a smooth curve and K_C a canonical divisor. So we have :*

- $\ell(K_C) = g$.
- $\deg(K_C) = 2g - 2$.
- *For all* $D \in \mathrm{Div}(C)$ *such as* $\deg(D) > 2g - 2$, $\ell(D) = \deg(D) - g + 1$.

Proof. For the first point, let us consider $D = 0$. Then $\mathscr{L}(0) = \bar{K}$ and $\ell(0) = 1$ so :

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

For the second point, let us consider $D = K_C$. We have :

$$\deg(K_C) = \ell(K_C) - \ell(K_C - K_C) + g - 1 = g - 1 + g - 1 = 2g - 2$$

Finally, if $\deg(D) > 2g - 2$ then $\deg(K_C - D) < 0$ and $\ell(K_C - D) = 0$ from [2.15]. □

Remark 14. The number $\ell(D)$ is the dimension of the space of functions which are solutions to the problem of finding functions with a prescribed number of zeroes and allowed number of poles.

We can notice in the case of meromorphic function, ie. C is the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$, that for a divisor D such as $\deg(D) = 0$ we found an unique solution to this problem, up to a constant :

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

Because the genus of $\mathbb{P}^1$ is $g = 0$ and $\deg(D) = 0 > 2g - 2$ so $\ell(K_C - D) = 0$.

The assumption $\deg(D) = 0$ could seems restrictive but in fact it is a natural assumption since the number of zeros and poles counted with multiplicities of an holomorphic functions on $\mathbb{C}$, extended in a meromorphic function on $\overline{\mathbb{C}}$, are equals. Then for any meromorphic function on the Riemann sphere, we already knew from complex analysis that $\deg\big(\mathrm{div}(f)\big) = 0$. We conclude that meromorphic function on $\mathbb{P}^1_{\mathbb{C}}$ are uniquely determined, up to a multiplicative constant, by the specification of its zeros and poles which is a really nice result also well known in complex analysis.

Proposition 2.18. *Let* C/K *be a smooth curve and* $D \in \mathrm{Div}_K(C)$.
Then $\mathscr{L}(D)$ *has a basis of functions in* $K(C)$.

Proof. [Sil86, p. 36, II.5.8] □

Chapter 3

Elliptic curves

In this chapter we will study our main object : the elliptic curves. We will develop all the necessary stuff for the proof of the Mordell-Weil theorem which will be stated and proved in the next chapter.

Our study will start with the link between elliptic curves and equations in Weierstrass form. Then we will define the group structure on an elliptic curve. Finally we will explain the procedure of reduction of an elliptic curve over a residue field. This last point will be used at a crucial moment in the proof of the Mordell-Weil theorem.

3.1 Elliptic curves and Weierstrass Equations

Definition (Elliptic curve)**.** We call **elliptic curve** any non-singular projective curve of genus 1. More precisely, an elliptic curve is a couple (E, O) where E is the curve and $O \in E$ is a specified point. An elliptic curve is defined over K, denoted E/K, if E is defined over K and $O \in E(K)$.

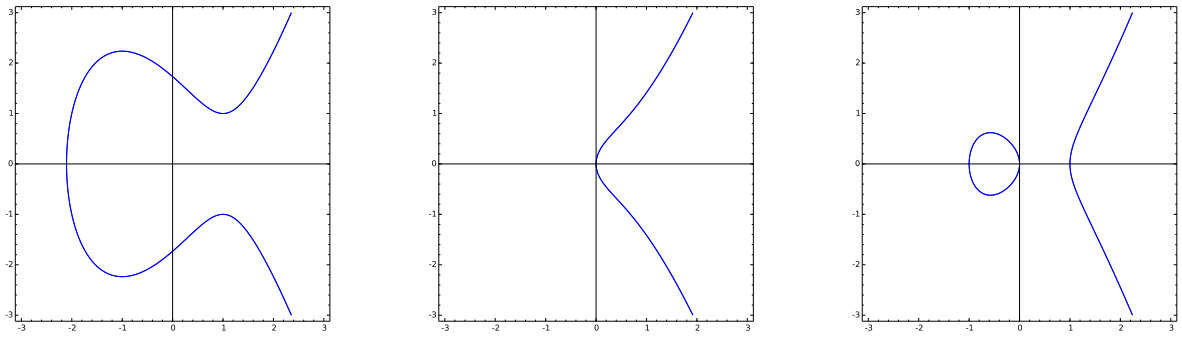
Remark 15. The specification of the point O is needed to put a group structure without ambiguity. We will choose O as the identity of the group $(E, \oplus)$. However, we will often omit it when it is not problematic.

We will now see that any elliptic curve can be defined as a locus in $\mathbb{P}^2$ by a Weierstrass equation and that each non-singular Weierstrass equation can be seen as an elliptic curve with base point $O = [0, 1, 0]$. This will give us a geometrical visualisation of the elliptic curves as plane cubics.

Let us study Weierstrass equations.

Definition (Weierstrass equation)**.** A **Weierstrass equation** is an equation of the form :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad \text{with } a_1, \dots, a_6 \in \bar{K}$$



$y^2 = x^3 - 3x + 3$ $y^2 = x^3 + x$ $y^2 = x^3 - x$

Figure 3.1: Three elliptic curves

Remark 16. I follow the standard labelling notation which are comfortable to use even if at first sight it can be surprising. To remember them, think that even numbers are associated to powers of x and odd numbers to terms with y.

We will now show that in characteristic different from 2 and 3 we can reduce, by linear change of variables, such type of equation to a simpler form.

Proposition 3.1. *Let* K *be a field of characteristic different from* 2 *and* 3*. Then any Weierstrass equation can be reduced to the form :*

$$y^2 = x^3 + Ax + B \quad \textit{with } A, B \in \bar{K}$$

The homogenized equation still defines a locus in $\mathbb{P}^2$*.*

Remark 17. Even if we will focus our study on number fields, which means we will be in characteristic zero, we will still stay in the general case for a moment. Indeed, we will need general results to talk about elliptic curves on number fields when we will reduce them modulo p and look at the reduced curves over residue fields.

Proof. Let us consider a general Weierstrass equation :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad \text{with } a_1, \dots, a_6 \in \bar{K} \qquad (*)$$

Then we consider the dehomogenized equation :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{with } a_1, \dots, a_6 \in \bar{K}$$

First of all, we want to remove the xy and y terms. For this, we want to complete the square. The trick is to consider $4(*)$ and so we can find y_1 such as $y_1^2 = 4y^2 + 4a_1xy + 4a_3y + f(x)$. A solution is $y_1 = 2y + a_1x + a_2$, we apply the change of variables $y \mapsto \frac{1}{2}(y_1 - a_1x - a_3)$:

$$\frac{4}{2^2}(y_1 - a_1x - a_3)^2 + \frac{4}{2}(y_1 - a_1x - a_3)[a_1x + a_3] = 4x^3 + 4a_2x^2 + 4a_4x + 4a_6$$

$$\begin{aligned}
\Leftrightarrow \quad & \left(y_1^2 + a_1^2x^2 + a_3^2 - 2a_1xy_1 - 2a_3y_1 - 2a_1a_3x\right) \\
& + \left(2a_1xy_1 - 2a_2^2x^2 - 2a_1a_3x\right) \\
& + \left(2a_3y_1 - 2a_1a_3 - 2a_3^2\right) = 4x^3 + 4a_2x^2 + 4a_4x + 4a_6 \\
\Leftrightarrow \quad & y_1^2 = 4x^3 + \left(4a_2 - a_1^2\right)x^2 + (4a_4 + 2a_1a_3)x + \left(4a_6 + a_3^2\right) \\
\Leftrightarrow \quad & y_1^2 = 4x^3 + b_2x^2 + 2b_4x + b_6
\end{aligned}$$

Now we are trying to delete the term with x^2. The idea is to apply a change of variables $x \mapsto \lambda(x_1 + \mu)$. A good choice of (λ, μ) is $\left(36^{-1}, -3b_2\right)$ as the calculation shows :

$$\begin{aligned}
y_1^2 &= 4 \cdot 36^{-3}(x_1 - 3b_2)^3 + 36^{-2}b_2(x_1 - 3b_2)^2 + 2 \cdot 36^{-1}b_4(x_1 - 3b_2) + b_6 \\
y_1^2 &= 4 \cdot 36^{-3}\left(x_1^3 - 3^2b_2x_1^2 + 3^3b_2^2x_1 + 3^3b_2^3\right) + 36^{-2}\left(b_2x_1^2 - 2 \cdot 3b_2x_1 + 3^2b_2^3\right) \\
&\quad + 2 \cdot 36^{-1}b_4x_1 - 3 \cdot 36^{-1}b_2b_4 + b_6 \\
y_1^2 &= 108^{-2}x_1^3 + 108^{-2}\left(3^3b_2^2 - 2 \cdot 3 \cdot 36 \cdot 4^{-1}b_2 + 2 \cdot 36^2 \cdot 4^{-1}b_4\right)x_1 \\
&\quad + 108^{-2}\left(3^3b_2^3 + 3^2 \cdot 36 \cdot 4^{-1}b_2^3 - 3 \cdot 36^2 \cdot 4^{-1}b_2b_4 + 108^2b_6\right) \\
y_1^2 &= 108^{-2}\left(x_1^3 + \left(-27b_2^2 + 24 \cdot 27b_4\right)x_1 + \left(54b_2^3 - 27 \cdot 54b_2b_4 + 54 \cdot 216b_6\right)\right) \\
y_1^2 &= 108^{-2}\left(x_1^3 - 27c_4x_1 - 54c_6\right) \\
y_1^2 &= 108^{-2}\left(x^3 + Ax + B\right)
\end{aligned}$$

We conclude by the change of variable $y_1 \mapsto 108^{-1}y_2$. Notice that the characteristic must not be 2 or 3 to be able to do these changes of variables. We already could have concluded at the 3rd step but we develop the calculation to obtain this table of constants we will need for the next calculations :

Let us sum up. In the general case :

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

If $\mathrm{Char}(K) \neq 2$:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

If $\mathrm{Char}(K) \neq 2$ and 3 :

$$y^2 = x^3 + Ax + B = x^3 - 27c_4x - 54c_6$$

Constant	In function of a_i and b_i
b_2	$4a_2 + a_1^2$
b_4	$2a_4 + a_1a_3$
b_6	$4a_6 + a_3^2$
c_4	$b_2^2 - 24b_4$
c_6	$-b_2^3 + 36b_2b_4 - 216b_6$

Table 3.1: Constants values

□

Let us introduce the discriminant of a Weierstrass equation. It will be a useful quantity for characterise the smoothness of the curve.

Definition (Discriminant)**.** Let C be a curve defined by a Weierstrass equation :

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

We define the **discriminant** of E as $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ with $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. In characteristic different form 2 and 3, the elliptic curve can be rewritten as $y^2 = x^3 + Ax + B$ and $\Delta = -16(4A^3 + 27B^2)$.

Let us now check what can happens at a non-smooth point.

Definition (Node and cusp)**.** Let C be a curve given by a Weierstrass equation :

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

Let $P = (x_0, y_0)$ be a singular point. Then $\partial_x f(P) = 0$ and $\partial_y f(P) = 0$ so :

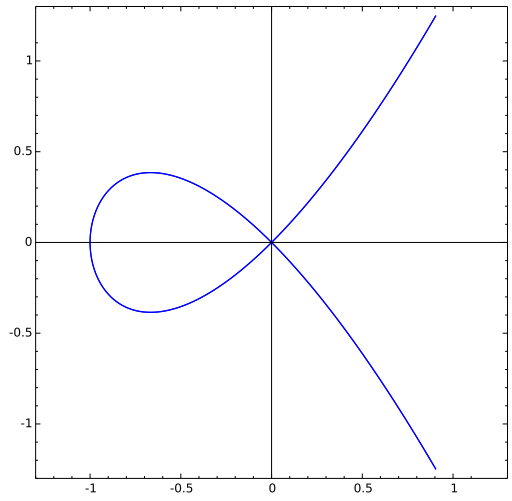
$$\begin{aligned} f(x,y) - f(x_0,y_0) &= \partial_x^2 f(P)\frac{(x-x_0)^2}{2} + \partial_x\partial_y f(P)(x-x_0)(y-y_0) \\ &\quad + \partial_y^2 f(P)\frac{(y-y_0)^2}{2} + \partial_x^3 f(P)\frac{(x-x_0)^3}{3!} \\ &= \big((y-y_0) - \alpha(x-x_0)\big)\big((y-y_0) - \text{œ}\beta(x-x_0)\big) - (x-x_0)^3 \end{aligned}$$

- We say that P is a **node** if $\alpha \neq \beta$. Then we have two tangent lines at P :

$$y - y_0 = \alpha(x - x_0) \quad ; \quad y - y_0 = \beta(x - x_0)$$

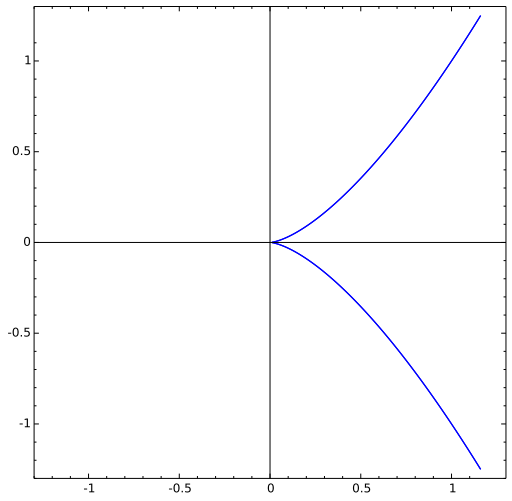
- We say that P is a **cusp** if $\alpha = \beta$. Then we have only one tangent line at P :

$$y - y_0 = \alpha(x - x_0)$$



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

Figure 3.2: Node singularity



$y^2 = x^3$

Figure 3.3: Cusp singularity

Finally, let us classify the different the cases of regularity.

Proposition 3.2. *Let C be given by a Weierstrass equation with discriminant Δ. Let c_4 be the quantity defined in [Table 3.1]. Then :*

- *C is smooth if and only if $\Delta \neq 0$.*
- *C has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.*
- *C has a cusp if and only if $\Delta = 0$ and $c_4 = 0$.*

Proof. [Sil86, p.46, III.1.4] □

Once we have defined Weierstrass equations and characterised their smoothness, we could state a main theorem of the elliptic curves theory :

Theorem 3.3 (Elliptic curves and Weierstrass equations)**.** *Let E be an elliptic curve defined over K. There are functions $x, y \in K(E)$ such that the following function ϕ is an isomorphism between E/K and the curve C with $\phi(O) = [0,1,0]$.*

$$\begin{array}{rccc} \phi : & E & \longrightarrow & C \subseteq \mathbb{P}^2 \\ & P & \longmapsto & \big[x(P), y(P), 1\big] \end{array}$$

Where the curve C is defined by the Weierstrass equation :

$$C : \; Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad \textit{with } a_1, \ldots, a_6 \in K$$

*The functions x and y are called **Weierstrass coordinates** for the elliptic curve E/K. Reciprocally, any smooth curve C defined by a Weierstrass equation is an elliptic curve over*

K *with base point* $O = [0,1,0]$. *Furthermore, two Weierstrass equations for* E *are related by a linear change of variables :*

$$X = u^2X' + r \quad ; \quad Y = u^3Y' + su^2X' + t \quad \textit{with } u \in K^* \text{ and } r,s,t \in K$$

Proof.

We are looking for Weierstrass coordinates. We will find them as elements of $\mathscr{L}\big(n(O)\big)$ using the Riemann-Roch theorem. Let $n \geqslant 1$ and let us look at the vector space associated to the divisor $n(O)$:

$$\mathscr{L}\big(n(O)\big) = \{f \in \bar{K}(E)^* \mid \operatorname{div}(f) \geqslant -n(O)\} \cup \{0\}$$

So $\mathscr{L}\big(n(O)\big)$ represents the vector space of all functions with poles of multiplicity less or equal to n at O. From 2.17 in the special case $g = 1$:

$$\dim_{\bar{K}} \mathscr{L}\big(n(O)\big) = n$$

Furthermore, $\mathscr{L}\big(n(O)\big) \subseteq \mathscr{L}\big((n+1)(O)\big)$ because $-n(O) \geqslant -(n+1)(O)$. Let us choose $x, y \in K(E)$ such that $\{1, x\}$ is a basis of $\mathscr{L}\big(2(O)\big)$ and $\{1, x, y\}$ is a basis of $\mathscr{L}\big(3(O)\big)$. Then we can choose K-rational coefficients using [2.18] because $n(O) \in \operatorname{Div}_K(E)$.

Now we consider $\mathscr{L}\big(6(O)\big)$. Its dimension is 6 but it also contains the seven functions $1, x, y, xy, x^2, y^2, x^3$ because x (resp. y) have a pole of exact order 2 (resp. 3). The upper bound is clear by definition of $\mathscr{L}\big(n(O)\big)$ and the lower bound is deduced by the fact that if the order of the pole at O of x (resp. y) is less than 2 (resp. 3) then $x \in \mathscr{L}\big(1(O)\big)$ (resp. $y \in \mathscr{L}\big(2(O)\big)$) and the sets considered are not basis.

Thus, we have a linear combination between these functions :

$$\exists \lambda_i \in K \text{ with at leat one non-zero } : \quad \lambda_1 + \lambda_2 x + \lambda_3 y + \lambda_4 xy + \lambda_5 x^2 + \lambda_6 y^2 + \lambda_7 x^3 = 0$$

We can take $\lambda_i \in K$, still from [2.18]. Let us notice that λ_6 and λ_7 are non zero because all the other terms have poles at O of different orders so all the λ_j should vanish. We would like to find a Weierstrass equation with x and y as coordinates, so we proceed to the change of variables $(x, y) \mapsto \Big(-\lambda_6\lambda_7 x_1, \lambda_6\lambda_7^2 y_1\Big)$:

$$\lambda_1 - \lambda_2\lambda_6\lambda_7 x + \lambda_3\lambda_6\lambda_7^2 y + \lambda_4\lambda_6^2\lambda_7^2 y + \lambda_4\lambda_6^2\lambda_7^2 x^2 - \lambda_5\lambda_6^2\lambda_7^3 xy + \lambda_6^3\lambda_7^4 y^2 - \lambda_6^3\lambda_7^4 x_3 = 0$$

Thus, dividing by $\lambda_6^3\lambda_7^4$ we get a cubic equation in Weierstrass form.

Let us prove that $\phi : E \to C$ has degree 1, or equivalently that $K(E) = K(x, y)$. Consider the map $[x, 1] : E \to \mathbb{P}^1$. Since x has a double pole at O and no other poles, this map has degree 2 from [2.8]. Thus $\big[K(E) : K(x)\big] = 2$. Similarly the map $[1, y] : E \to \mathbb{P}^1$ has degree 3 so $\big[K(E) : K(y)\big] = 3$. Thus $\big[K(E) : K(x, y)\big]$ divides both 2 and 3 so it is 1.

Finally, let us prove that C is smooth to conclude that ϕ is an isomorphism Suppose that C is singular. Then it exists a rational map $\psi : C \to \mathbb{P}^1$ of degree one. It follows that the composition $\psi \circ \phi : E \to \mathbb{P}^1$ is a map of degree one between smooth curve. Therefore, from [2.6], it is an isomorphism But this contradicts the fact that E has genus one and $\mathbb{P}^1$ has genus zero. Thus C is smooth, and now another use of [2.6] tell us that the degree one map $\phi : E \to C$ is an isomorphism. □

Corollary 3.4. *Let* E/K *be an elliptic curve with Weierstrass coordinates* x *and* y*.*

$$K(E) = K(x, y) \quad ; \quad \big[K(E) : K(x)\big] = 2$$

3.2 Group law on elliptic curves

In this section, we develop one of the most fundamental properties of elliptic curves, the abelian group structure.

Then we will be able to talk about m-torsion points and we will show that they form a finite group, which is a result we will need in the next chapter.

3.2.1 Geometric group law

We will now define the group law using Weierstrass equations.

Definition (Composition law)**.** Let E be an elliptic curve and P, Q in E.

To construct $P + Q$, we consider the line L between P and Q, which is the tangent line if $P = Q$. Let R be the third intersection point of L with E. Let L' be the line between R and O. We set $P + Q$ as the third intersection point of L' with E.

Remark 18. From Bézout's theorem, two projective curves intersects in $n \times m$ points counted with multiplicities where n and m are the degree of each curve. This theorem ensures that the line L intersects E in three points counted with multiplicities.

Remark 19. Geometrically, in an affine piece, the algorithm consists in considering the point R aligned with P and Q and taking its symmetrical with respect to (Ox). Indeed, O is considered as the point at the infinity in this chart. Then L' is the vertical line passing through R. This construction is then really clear geometrically speaking.

Proposition 3.5. *The composition law* $+$ *is a commutative group law on* E*.*

- O *is the neutral element :* $\forall P \in E : \ P + O = P$*.*
- *Every element has a inverse :* $\forall P \in E, \exists (-P) \in E : P + (-P) = O$*.*
- *The law is associative :* $\forall P, Q, R \in E : \ (P + Q) + R = P + (Q + R)$*.*

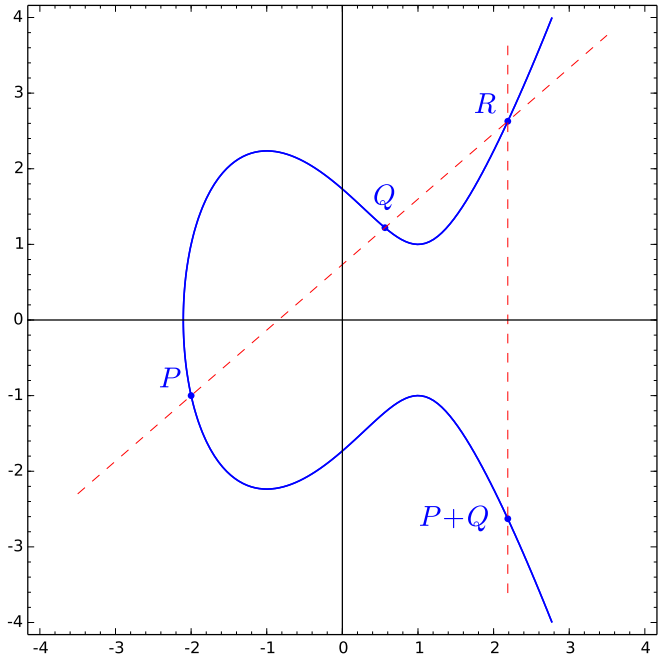


Figure 3.4: Addition algorithm on the curve $y^2 = x^3 - 3x + 3$

- *The law is commutative :* $\forall P, Q \in E : \ P + Q = Q + P$.

Furthermore, if the not necessarily distinct points P, Q *and* R *are aligned then* $P + Q + R = O$.

Then any elliptic curve has a group structure defined geometrically and which satisfy the formulas stated in the next subsection. There is another way to define a group law on an elliptic curve which consist of noticing that for every $D \in \mathrm{Pic}^0(E)$ there is a unique $P \in E$ such that $D \sim (P) - (O)$. Thus we can look at the following function.

$$\begin{array}{rccc} \sigma : & \mathrm{Pic}^0(E) & \longrightarrow & E \\ & D & \longmapsto & (P) - (O) \end{array}$$

It is an isomorphism between the abelian group $\mathrm{Pic}^0(E)$ and E. This give us another group structure. In fact, these two definitions coincides and will we will content ourselves with the first one.

3.2.2 Addition and duplication formulas

Let us give explicit formula which will be used in the following chapter. Calculation are not developed here and can be found in [Sil86, III.2].

Proposition 3.6. *Let* E *be an elliptic curve defined by a Weierstrass equation.*

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

Let $P = (x, y)$. *Then* $-P = (x, -y - a_1x - a_3)$. *Let* $P_1 + P_2 = P_3$ *with* $P_i = (x_i, y_i)$.

- *If* $x_1 = x_2$ *and* $y_1 + y_2 + a_1x_2 + a_3 = 0$ *then* $P_1 + P_2 = O$.
- *Otherwise* $y = \lambda x + \nu$ *is the line passing by* P_1 *and* P_2 *so :*

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = -(\lambda + a_1)x_3 - \nu - a_3 \end{cases}$$

Where λ *and* ν *are calculated as :*

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

As a special case we have :

$$x\big([2]P\big) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

In characteristic zero, we get the reduced formulas :

$$-P = (x, -y) \quad ; \quad \begin{aligned} x(P_1 + P_2) &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ x\big([2]P\big) &= \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B} \end{aligned}$$

An important remark is that the group law can be defined using rational functions. Thus, if P and Q are K-rational points, their sum $P + Q$ too. This gives us the stability of the K-rationality by addition. Then we can define the group of K-rational points on which we will be focused on.

Definition (K-rational point subgroup)**.** Let E be an elliptic curve defined over K.

$$E(K) = E \cap \mathbb{P}^2(K) = \Big\{(x, y) \in K^2 \ \mid \ f(x, y) = 0\Big\} \cup \{O\} \text{ is a subgroup of } E.$$

Our aim is to prove that this subgroup is finitely generated. To do that, we will need an intermediate result : the finiteness of m-torsion points.

3.2.3 Torsion points

Definition (m-multiplication map)**.** Let E be an elliptic curve and $m \in \mathbb{Z}$.

We define the m-multiplication map by :

$$[m] : E \longrightarrow E$$

$$[m]P = \begin{cases} P + \cdots + P & \text{if } m > 0 \\ O & \text{if } m = 0 \\ [-m](-P) & \text{if } m < 0 \end{cases}$$

Proposition 3.7 (Finiteness of m torsion group)**.** *Let E be an elliptic curve. The group of m-torsion points $E[m]$ is finite.*

Proof.

To shorten the proof, we will admit[1] that the $[m]$ multiplication map has degree m^2. Since $\deg\big([m]\big) = m^2$, $[m]$ is a finite separable map. Hence [Sil86, p. 72, III.4.10] :

$$\big|E[m]\big| = \Big|\ker\big([m]\big)\Big| = \deg\big([m]\big) = m^2$$

□

3.3 Reduction

In this section, let K be a number field. We denote M_K the set of inequivalent absolute values on K, M_K^∞ and M_K^0 the subsets of archimedean and nonarchimedean absolute values in M_K respectively. For any $\nu \in M_K^0$, we denote K_ν the completion of K with respect to the discrete valuation ν. We define its local ring R_ν as :

$$R_\nu = \Big\{x \in K_\nu \,|\, \nu(x) \geqslant 0\Big\}$$

We also define the group of unit of R_ν as $R_\nu^* = \Big\{x \in K \,|\, \nu(x) = 0\Big\}$ and its maximal ideal $\mathfrak{m}_\nu = \Big\{x \in K \,|\, \nu(x) > 0\Big\}$. Finally we define its residue field k_ν as $R_\nu/\mathfrak{m}_\nu$.

In the following section, we will introduce the reduction of elliptic curves, namely the procedure which given an elliptic curve E/K and $\nu \in M_K^0$ match a curve $\tilde{E}_\nu/k_\nu$ over the residue field. We will see that this curve may not be smooth at some point and thus not an elliptic curve.

3.3.1 Minimal Weierstrass equation

Let $\nu \in M_K^0$. Let C/K be a curve defined by a Weierstrass equation :

$$C : \; Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad \text{with } a_1, \ldots, a_6 \in K$$

If $a_i \in K$ then $a_i \in K_\nu$ but we are not sure that $a_i \in R_\nu$. However, we will need that condition to reduce the curve. Then, the idea is to find a good change of variables

[1] In fact, we could develop this fact but we would need introduce isogeny and dual isogeny.

such that all coefficients are in R_v. We also look for minimize the valuation $v(\Delta)$ of the discriminant.

Definition (Minimal Weierstrass equation)**.** Let E/K_v be an elliptic curve with $v \in M_K^0$. A Weierstrass equation for E is called a **minimal Weierstrass equation** for E at v if $v(\Delta)$ is minimized with the condition $a_1, a_2, a_3, a_4, a_6 \in R_v$.

Proposition 3.8. *Every elliptic curve* E/K_v *has a minimal Weierstrass equation.*

Proof. It is easy to find some Weierstrass equation with all $a_i \in R_v$. For that, look at the substitution $(x, y) \mapsto \left(u^{-2}x, u^{-3}y\right)$. This leads to a new equation in which a_i is replaced by $u^i a_i$. Then it suffices to choose $u \in R_v$ with a valuation large enough.

As soon as we have $v(a_i) \geqslant 0$ for all i, we get $v(\Delta) \geqslant 0$. Then there is at least one of the equations that minimizes $v(\Delta)$ since v is a discrete valuation. □

Remark 20. For arbitrary K, there is an algorithm of Tate that determines whether a given equation is minimal.

3.3.2 Reduction modulo v

Let K be a number field and $v \in M_K^0$. We look at the reduction map :

$$\begin{array}{ccc} R_v & \longrightarrow & k_v \\ a & \longmapsto & \tilde{a} \end{array}$$

Using this map, we can reduce an elliptic curve modulo a residue field by reducing all the coefficients of one of its minimal Weierstrass equations for v. We get a curve $\tilde{E}_v/k_v$ which can be singular and thus not an elliptic curve.

$$\tilde{E}_v : \ y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$$

We can define a reduction map on the points :

$$\begin{array}{rccc} \rho_v : & E(K_v) & \longrightarrow & \tilde{E}_v(k_v) \\ & P = [x, y, z] & \longmapsto & \tilde{P} = [\tilde{x}, \tilde{y}, \tilde{z}] \end{array}$$

This is the reduction of an elliptic curve. Of course, the curve $\tilde{E}_v/k_v$ may be singular. In this case, we consider the set $\tilde{E}_{ns}(k_v)$ of the non-singular points which is in fact a group.

3.3.3 Good and bad reduction

Finally we can define the concept we will need in the next chapter.

Definition (Good and bad reduction over K)**.** Let K be a number field, v be a discrete valuation, K_v be a local field complete for v and E/K_v be an elliptic curve. We say that :

- E has a **good** or **stable** reduction over K_v if $\tilde{E}_v/k_v$ is non singular.
- E has a **bad** reduction over K_v if $\tilde{E}_v/k_v$ is singular.
  - E has a **multiplicative** or **semi-stable** reduction if $\tilde{E}_v/k_v$ has a node.
  - E has an **additive** or **unstable** reduction if $\tilde{E}_v/k_v$ has a cusp.

Using the proposition [3.2], we can characterise each case.

Proposition 3.9. *Let E/K_v be an elliptic curve given by a minimal Weierstrass equation :*

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

Let Δ be the associated discriminant and c_4 the usual quantity [Table 3.1].

- E *has a good reduction if and only if* $v(\Delta) = 0$.
  In this case $\tilde{E}_v/k_v$ *is an elliptic curve.*
- E *has a multiplicative reduction if and only if* $v(\Delta) > 0$ *and* $v(c_4) = 0$.
  In this case $\tilde{E}_{ns}$ *is a multiplicative group :*
  $$\tilde{E}_{ns}(\overline{k}_v) \cong \overline{k}_v^{\times}$$
- E *has an additive reduction if and only if* $v(\Delta) > 0$ *and* $v(c_4) > 0$
  In this case $\tilde{E}_{ns}$ *is an additive group :*
  $$\tilde{E}_{ns}(\overline{k}_v) \cong \overline{k}_v^{+}$$

Proof. [Sil86, p. 196, VII.5.1] □

Definition (Reduction at v)**.** Let K be a number field and E/K be an elliptic curve. Let $v \in M_K^0$ be a discrete valuation. Then E is said to have good (respectively bad) reduction at v if E has good (respectively bad) reduction when it is so considered over the completion K_v. Taking a minimal Weierstrass equation for E over K_v, we denote $\tilde{E}_v/k_v$ the reduced curve over the residue field.

Proposition 3.10 (Reduction map)**.** *Let $\nu \in M_K^0$ be a discrete valuation such that $\nu(\mathfrak{m}) = 0$ and such that E has a good reduction at ν. Then the reduction map $\rho_{\mathfrak{m},\nu} : E(K)[\mathfrak{m}] \longrightarrow \tilde{E}_\nu(k_\nu)$ is injective.*

Proof. [Sil86, p. 192 ,VII.3.1] □

Chapter 4

Mordell-Weil Theorem

The moment of the core theorem and proof has now arrived. As announced in the introduction, we will divide this chapter in a few parts to clarify the idea of the proof. Let us introduce it properly. Mordell-Weil theorem tells us that the number of generators of $E(K)$ is finite :

Theorem 4.1 (Mordell-Weil 1928)**.** *Let* K *be a number field and* E/K *an elliptic curve. Then the subgroup of* K*-rational points* $E(K)$ *is finitely generated.*

As an immediate corollary, we deduce that the torsion group $E(K)_{\text{tors}}$ is finite and our knowledge about finitely generated abelian groups leads us to this description of the structure of $E(K)$:

Corollary 4.2. *Let* K *be a number field and* E/K *be an elliptic curve.*

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$$

The integer r *is called the* ***rank*** *of* E/K*.*

In the next chapter, we will talk more about the structure of $E(K)_{\text{tors}}$ and the rank. But for the moment, we will focus on the main part of our development, namely the proof of this theorem.

4.1 Weak Mordell-Weil Theorem

The first part and also the hardest one is to prove the so called weak Mordell-Weil theorem which will be used to deduce the Mordell-Weil theorem using the descent procedure presented in the second part.

4.1.1 Theorem and reduction lemma

Let us state this weak theorem :

Theorem 4.3 (Weak Mordell-Weil theorem)**.** *Let* K *be a number field and* E/K *be an elliptic curve. Then for all* $m \geqslant 2$ *the quotient* $\dfrac{E(K)}{mE(K)}$ *is a finite group.*

The idea behind the proof of the Mordell-Weil theorem is to think that generators of the group $E(K)$ can be chosen as the representatives of the classes of the group $\frac{E(K)}{2E(K)}$, with some additional finite number of points with a special property. Then the finiteness of this group is necessary to proceed like that. The following lemma will enable us to assume that $E[m] \subseteq E(K)$ which will used further :

Lemma 4.4. *Let* L/K *be a finite Galois extension.*
If $\dfrac{E(L)}{mE(L)}$ *is finite then* $\dfrac{E(K)}{mE(K)}$ *is finite.*

Proof. Let us consider the inclusion $E(K) \hookrightarrow E(L)$. It induce a natural map

$$\frac{E(K)}{mE(K)} \to \frac{E(L)}{mE(L)}$$

which has I as kernel :

$$I = \frac{E(K) \cap mE(L)}{mE(K)}$$

For each P in I, we can choose $Q_P \in E(L)$ such that $[m]Q_P = P$. Then we can define :

$$\begin{array}{rccl} \lambda_P : & G_{L/K} & \longrightarrow & E[m] \\ & \sigma & \longmapsto & \lambda_P(\sigma) = Q_P^\sigma - Q_P \end{array}$$

Since $[m]\left(Q_P^\sigma - Q_P\right) = \left([m]Q_P\right)^\sigma - Q = P^\sigma - P = 0$, $\left(Q_P^\sigma - Q_P\right)$ is effectively in $E[m]$.

We will now prove that Λ is a injective :

$$\begin{array}{rccl} \Lambda : & I & \longrightarrow & \mathrm{Map}\Big(G_{L/K}, E[m]\Big) \\ & P & \longmapsto & \lambda_P \end{array}$$

Let P and P' be points in $E(K) \cap mE(L)$ such that $\lambda_P = \lambda_{P'}$. Then :

$$\forall \sigma \in G_{L/K} : (Q_P - Q_{P'})^\sigma = Q_P - Q_{P'}$$

So $Q_P - Q_{P'} \in E(K)$ and it follows that :

$$P - P' = [m]Q_p - [m]Q_{P'} = [m](Q_P - Q_{P'}) \in mE(K)$$

Then $P = P'$ in I and Λ is injective. Since $G_{L/K}$ and $E[m]$ are finite sets, there is only a finite number of maps between them. Thus, I is finite and we have an exact sequence of finite groups :

$$0 \longrightarrow I \longrightarrow \frac{E(K)}{mE(K)} \longrightarrow \frac{E(L)}{mE(L)}$$

□

Remark 21. Now we can assume that $E[m] \subseteq E(K)$ because, K does not satisfy this assumption, we could consider the Galois extension L of K containing all points of m torsion. It is again a finite Galois extension. Then using the lemma, we prove the weak Mordell-Weil theorem for L and it will imply the result for K.

4.1.2 Kummer Pairing

To prove the finiteness of the group $\frac{E(K)}{mE(K)}$ we will use the Kummer pairing to find an equivalent property easier to prove because we have more tools, especially thanks to the Galois and discrete valuation theory.

Definition (Kummer pairing)**.** Let P be in $E(K)$ and $Q \in E(\bar{K})$ such as $[m]Q = P$.

We define :

$$\begin{array}{rccc} \kappa : & E(K) \times G_{\bar{K}/K} & \longrightarrow & E[m] \\ & (P, \sigma) & \longmapsto & Q^{\sigma} - Q \end{array}$$

This application is called Kummer pairing.

We will prove that is a perfect paring and then the finiteness of $\frac{E(K)}{mE(K)}$ will be equivalent to the finiteness of $G_{L/K}$, for an appropriate L, since from [3.7] we know that $E[m]$ is finite. Finally, we prove that the weak Mordell-Weil theorem will be equivalent to the finiteness of this specific extension L/K.

Proposition 4.5. *The Kummer pairing is well defined, bilinear and :*

- *Its kernel on the left is* $mE(K)$.
- *Its kernel on the right is* $G_{\bar{K}/L}$ *where* $L = K\Big([m]^{-1}E(K)\Big)$.

Hence, the Kummer pairing induces a perfect pairing :

$$\tilde{\kappa} : \frac{E(K)}{mE(K)} \times G_{L/K} \longrightarrow E[m]$$

Proof.

To show that κ is well defined, we have to prove that $\kappa(P, \sigma)$ does not depend on the choice of Q associated to P and that $\kappa(P, \sigma) \in E[m]$.

- Let Q and Q' be such as $[m]Q = [m]Q' = P$. Then $Q' = Q + T$ with $T \in E[m]$ and we have :

$$\kappa\big(Q', \sigma\big) = (Q+T)^\sigma - (Q+T) = Q^\sigma + T^\sigma - Q - T = Q^\sigma - Q$$

  Because since $E[m] \subseteq E(K)$, $T^\sigma = T$.

- Let $P \in E(K)$ and $\sigma \in G_{\bar{K}/K}$. Then :

$$[m]\kappa(P, \sigma) = [m]Q^\sigma - [m]Q = P^\sigma - P = O$$

Let us prove that κ is bilinear.

- For linearity in P, let $P, R \in E(K)$ and we write $[m]P' = P$, $[m]R' = R$. Then for $Q = P' + R'$:

$$\kappa(P+R, \sigma) = Q^\sigma - Q = \big(P' + R'\big)^\sigma - \big(P' + R'\big) = \kappa(P, \sigma) + \kappa(R, \sigma)$$

- For linearity in σ, let $\sigma, \tau \in G_{\bar{K}/K}$. We have :

$$\begin{aligned}\kappa(P, \sigma \circ \tau) &= Q^{\sigma\circ\tau} - Q \\ &= \big(Q^\sigma - Q\big)^\tau + \big(Q^\tau - Q\big) \\ &= \kappa(P, \sigma)^\tau + \kappa(P, \tau) \\ &= \kappa(P, \sigma) + \kappa(P, \tau)\end{aligned}$$

  Since $\kappa(P, \sigma) \in E[m] \subseteq E(K)$.

Let us calculate the kernel on the left and on the right :

- Suppose that $P \in mE(K)$ and $Q \in E(K)$ such that $[m]Q = P$. Then :

$$\kappa(P, \sigma) = Q^\sigma - Q = O$$

  Suppose that for all $\sigma \in G_{\bar{K}/K}$, $\kappa(P, \sigma) = 0$. Then Q is in the fixed field, $Q \in E(K)$ and then $P \in mE(K)$.

- Suppose that $\sigma \in G_{\bar{K}/L}$. By definition $Q \in [m]^{-1}E(K) \subseteq L$ then :

$$\kappa(P, \sigma) = Q^\sigma - Q = O$$

  Suppose that for all P, $\kappa(P, \sigma) = 0$. Then σ fixes all points of L and $\sigma \in G_{\bar{K}/L}$.

The induced perfect bilinear pairing is clear from what precedes. □

4.1.3 Properties of L and finiteness theorem

We will now introduce some of the properties of L/K. Then we will show that any extension with such properties is finite which will enable us to conclude the proof of the weak theorem.

Proposition 4.6. *Let* L/K *be an extension and* v *be a discrete valuation on* K.
Let $w \in M_L$ *such that the restriction of* w *at* K *is* v. *Then :*

$$[L_w : K_v] = e_v[l_w : k_v]$$

The integer e_v *is called the index of ramification of* L/K *at* v. *The extension* L/K *is* ***unramified*** *at* v *if* $e_v = 1$. *For any* $S \subseteq M_K$, *we say that the extension* L/K *is* ***unramified outside*** S *if it is unramified at all* $v \notin S$.

Remark 22. The condition $e_v = w(\pi_K) = 1$ where π_K is an uniformizer of K means that π_K is inert in L. In other words, if π_K is an uniformizer of K it will also be an uniformizer of L.

There is another way to define the unramification using the inertia group :

Definition (Inertia group)**.** Let K_v be a complete local field and k_v be his residue field. The **inertia group** of K_v is the set $I_v \subseteq G_{\bar{K}_v/K_v}$ of the elements that act trivially on the residue field k_v.

Definition (Unramified set)**.** Let A be a set on which $G_{\bar{K}_v/K_v}$ acts. We say that A is **unramified** at v if the action of I_v on A is trivial. Let $S \subseteq M_K$. We say that A is **unramified outside** S if it is unramified at all $v \notin S$.

Let us look at the properties of L :

Proposition 4.7. *Let* $L = K\Big([m]^{-1}E(K)\Big)$. *We have the following properties :*

- *The extension* L/K *is abelian and has exponent* m.
- *The extension* L/K *in unramified outside* S.

$$S = M_K^\infty \cup \Big\{v \in M_K^0 \ \mid \ E \text{ has bad reduction at } v\Big\} \cup \Big\{v \in M_K^0 \ \mid \ v(m) \neq 0\Big\}$$

Proof. For the first point, we just have to consider the injection :

$$\begin{array}{rccc} \Lambda : & G_{L/K} & \longrightarrow & \mathrm{Hom}\big(E(K), E[m]\big) \\ & \sigma & \longmapsto & \kappa\big(\bullet, \sigma\big) \end{array}$$

This gives an abelian structure on $G_{L/K}$ since :

$$\begin{aligned}\Lambda(\sigma\circ\tau)(P) &= Q^{\sigma\circ\tau} - Q = \left(Q^{\sigma} - Q\right)^{\tau} + \left(Q^{\tau} - Q\right)\\ &= \Lambda(\sigma)(P)^{\tau} + \Lambda(\tau)(P)\\ &= \Lambda(\sigma)(P) + \Lambda(\tau)(P) \quad \text{since } E[m] \subseteq E(K)\\ &= \Lambda(\sigma)(P) + \Lambda(\tau)(P)^{\sigma}\\ &= \Lambda(\tau\circ\sigma)(P)\end{aligned}$$

And with exponent m because remembering $\Lambda(\sigma)(P) \in E[m]$:

$$\Lambda\left(\sigma^{m}\right)(P) = [m]\Lambda(\sigma)(P) = O$$

Let us prove that L/K is unramified outside S.

Let $v \in M_k \setminus S$. Let $Q \in E(\bar{K})$ such that $[m]Q \in E(K)$ and let $K' = K(Q)$. It is enough to show that K'/K is unramified at v because L is the compositum of all these K'.

Let $v' \in M_{K'}$ be a place lying above v and let $k'_{v'}/k_v$ be the corresponding extension of residue fields. Since we assume that $v \notin S$, E has a good reduction at v so it also has good reduction at v'. We have the reduction map :

$$\begin{array}{rccc}\rho_{v'}: & E\left(K'\right) & \longrightarrow & \tilde{E}\left(k'_{v'}\right)\\ & P & \longmapsto & \tilde{P}\end{array}$$

Let $I_{v'/v} \subseteq G_{\bar{K}/K}$ be the inertia group of v'/v and take $\sigma \in I_{v'/v}$.

- By definition, σ act trivially on $\tilde{E}\left(k'_{v'}\right)$ thus :

$$\widetilde{Q^{\sigma} - Q} = \tilde{Q}^{\sigma} - \tilde{Q} = \tilde{O}$$

- Since $[m]Q \in E(K)$:

$$[m]\left(Q^{\sigma} - Q\right) = \left([m]Q\right)^{\sigma} - [m]Q = O$$

Then $Q^{\sigma} - Q \in E(K)[m]$ is in the kernel of $\rho_{m,v}$, so from [3.10] : $Q^{\sigma} = Q$. This proves that Q is fixed by every element of the inertia group $I_{v'/v}$, hence $K' = K(Q)$ is unramified over K at v'. Since it is true for all v' lying over v and for every $v \notin S$, this completes the proof that K'/K is unramified outside S. We conclude that L is unramified outside S. □

Remark 23. Furthermore, the set S is finite since E has a good reduction for all but finitely many $v \in M_K^0$. Indeed, if E is defined by a Weierstrass equation and has discriminant Δ, we have $v(\Delta) = 0$ for all but finitely many $v \in M_K^0$ and in these conditions the reduced curve $\tilde{E}_v/k_v$ is non-singular.

We will now prove that all extensions satisfying these properties are finite.

Proposition 4.8. *Let* K *be a number field and* $S \subseteq M_K$ *be a finite set of places that contains* M_K^∞*. Let* L/K *be the maximal abelian extension of* K *having exponent* m *and that is unramified outside of* S*. Then* L/K *is a finite extension.*

In the following proof, we will use some fundamental theorems of algebraic number theory : the main theorem of Kummer theory, the ideal class theorem and another one, the Dirichlet's S-units theorem. To keep the proof as fluid as possible I made the choice not to explain this classical number theory concepts and theorems here. This would lead me too far away from the main topic. A good book to understand them is [Neu99].

Proof.

Step 1 : Reduction Case

First of all, we can make the assumption that K contains the m^{th} roots of the unity. Indeed, if we have the result for a finite extension K' over K with S' the set of places of K' lying over S, that means that the abelian extension L/K' of exponent m and unramified outside S' is finite, then L/K is also finite.

Furthermore, we can also increase the size of S by adding new places because it will only make L larger. Then we adjoin to S all the absolute values $v \in M_K$ such that $v(m) \neq 0$. We also adjoin a finite number of places such that the ring of S integer R_S is a principal ideal domain :

$$R_S = \left\{ a \in K \mid \forall v \in M_K \setminus S : v(a) \geqslant 0 \right\}$$

This is possible using the fact that the class number of K is finite.

Step 2 : Kummer theorem

We know apply the main theorem of Kummer theory, which says that if a field of characteristic 0 contains $\mathbb{U}_m$, then its maximal abelian extension of exponent m is obtained by adjoining all m^{th} roots of all his elements. We deduce that L is the largest subfield of $K\left(\sqrt[m]{a} \mid a \in K \right)$ which is also unramified outside S.

Step 3 : Expression of L.

Let us take $v \in M_K \setminus S$ and consider the equation $X^m - a = 0$ over the local field K_v. Since $v(m) = 0$ and the discriminant of $X^m - a$ is $\pm m^m a^{m-1}$ we see that $K_v(\sqrt[m]{a})/K_v$ is unramified if and only if $\text{ord}_v(a) \equiv 0 \mod m$. Indeed, let w be the unique extension at $K_v\left(\sqrt[m]{a} \right)$ of the valuation v. Then $K_v\left(\sqrt[m]{a} \right)/K_v$ is unramified if and only if $v(K_v) = w\Big(K_v\left(\sqrt[m]{a} \right)\Big)$ [Neu99, (7.11)]. So this extension is unramified if and only if :

$$w\left(\sqrt[m]{a} \right) = 0 + \frac{\text{ord}_v(a)}{m} \in v(K_v) \Leftrightarrow m \mid \text{ord}_v(a) \Leftrightarrow \text{ord}_v(a) \equiv 0 \mod m$$

Finally, we note that when we adjoin m^{th} roots, it is necessary to take only one representative for each class in $K^*/(K^*)^m$ so for :

$$T_S = \left\{ a \in K^*/\left(K^*\right)^m \mid \forall v \in M_K \setminus S : \mathrm{ord}_v(a) \equiv 0 \mod m \right\}$$

We have $L = K\big(\sqrt[m]{a} \mid a \in T_S\big)$. To conclude the proof, it is enough to show that T_S is finite.

Step 4 : Finiteness of T_S

Let us show that the natural map $\Lambda : R_S^* \to T_S$ is surjective. Let $a \in K^*$ represent an element of T_S. Then the ideal aR_S is the m^{th} power of an ideal in R_S since the prime ideal of R_S corresponds to the valuation $v \notin S$. As R_S is a principal ideal domain, we can find $b \in K^*$ such that $aR_S = I^m = \langle b \rangle^m = b^m R_S$ then :

$$\exists u \in R_S^* : a = ub^m$$

We conclude that a and u represents the same element in T_S which proves that R_S^* surjects onto T_S. Moreover, $\left(R_S^*\right)^m$ is contained in the kernel of Λ then we have a surjection :

$$\overline{\Lambda} : {R_S^*}\big/{\left(R_S^*\right)^m} \longrightarrow\!\!\!\!\!\rightarrow T_S$$

Finally, the Dirichlet's S-unit theorem indicates us that R_S^* is finitely generated so we have a surjection onto T_S from a finite group. It follows that T_S is finite and it completes the proof : L/K is a finite extension. □

Now that we have all ingredients let us put them together :

Proof of the weak Mordell-Weil Theorem. Let $L = K([m]^{-1}E(K))$. From [3.7], we know that $E[m]$ is finite. Thus $\frac{E(K)}{mE(K)}$ is finite if and only if $G_{L/K}$ is finite by [4.5]. Now, [4.7] shows that L satisfies the assumptions of [4.8]. Then L/K is finite and we deduce the result. □

4.2 The Descent Procedure

Now we know that $\frac{E(K)}{mE(K)}$ is finite we would like to deduce a result on $E(K)$ now. We can easily check that is not enough to affirm that $E(K)$ is finitely generated. But with some additional assumptions, in particular the existence of a height function, this is true. It is what the descent procedure states. We state it in the general context of abelian groups which include our case.

Theorem 4.9 (Descent Theorem)**.** *Let A be an abelian group. Suppose that there is a height function $h : A \to \mathbb{R}$ with the three following properties :*

- *Let* $Q \in A$. *There is a constant* C_1, *depending on* A *and* Q *such that :*

$$\forall P \in A : h(P+Q) \leqslant 2h(P) + C_1 \tag{1}$$

- *There is an integer* $m \geqslant 2$ *and a constant* C_2, *depending on* A *such that :*

$$\forall P \in A : h(mP) \geqslant m^2 h(P) - C_2 \tag{2}$$

- *For every constant* C_3, *the set* $\{P \in A \mid h(P) \leqslant C_3\}$ *is finite.*

Then we have the following result :

If $\dfrac{A}{mA}$ *is finite then* A *is finitely generated.*

The idea of the procedure is to express any point $P \in A$ as a linear combination of representatives of the cosets in $\frac{A}{mA}$ and a point with height less than a constant. This is possible as soon as h satisfies the two first assumptions. Finally, we can conclude if the set of points with height less than a constant is finite : the third assumption.

All the smartness of this idea is based on the introduction of the notion of height. A height is a function which will satisfy the exact properties we need. All that we expect is that such height functions exist. It is the subject of the next part.

Proof. Let $P \in A$. Let $Q_1, \dots, Q_r \in A$ be representatives of the finitely many cosets in $\frac{A}{mA}$. We now show that the difference between P and an appropriate linear combination of $Q_1, \dots, Q_r$ is a multiple of a point whose height is smaller than a constant C_3 independent of P. Then $Q_1, \dots, Q_r$ and the finitely many points with height less than C_3 are generators for A.

Let us start by writing $P - Q_{i_1} = mP_1$ for the appropriate $i_1 \in [\![1, r]\!]$ such as $\overline{P} = \overline{Q_{i_1}}$ in $\frac{A}{mA}$. We continue by defining $P_{n-1} - Q_{i_n} = mP_n$. We have :

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}$$

And for any index j :

$$\begin{aligned}
h(P_j) &\leqslant \frac{1}{m^2}\Big(h(mP_j) + C_2\Big) && \text{from (2)} \\
&= \frac{1}{m^2}\left(h\Big(P_{j-1} - Q_{i_j}\Big) + C_2\right) && \text{from definition} \\
&\leqslant \frac{1}{m^2}\Big(2h(P_{j-1}) + C_1' + C_2\Big) && \text{from (1)}
\end{aligned}$$

Where C_1' is the maximum of the constants associated to the points $\{-Q_{i_l} \mid l \in [\![1, r]\!]\}$.

We deduce by induction :

$$\begin{aligned} h(P_n) &\leqslant \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2) \\ &\leqslant \left(\frac{2}{m^2}\right)^n h(P) + \frac{2}{m^2}(C_1' + C_2) \\ &\leqslant \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2) \end{aligned}$$

Indeed, $\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}} = \frac{1}{m^2}\sum_{k=0}^{n-1}\left(\frac{2}{m^2}\right)^k \leqslant \frac{1}{m^2}\sum_{k=0}^{n-1}\left(\frac{1}{2}\right)^k \leqslant \frac{2}{m^2}$.

Then for n big enough :

$$h(P_n) \leqslant 1 + \frac{1}{2}(C_1' + C_2)$$

We conclude that every point $P \in A$ is a linear combination of points of the set :

$$\mathscr{G} = \{Q_1, \ldots, Q_r\} \cup \left\{Q_0 \in A \mid h(Q_0) \leqslant C_3\right\} \text{ where } C_3 = 1 + \frac{1}{2}(C_1' + C_2)$$

From the third assumption of the height function h, $\mathscr{G}$ is a finite set, forming a generator set of A. □

In order to prove the Mordell-Weil theorem, we now just have to find a height function satisfying these conditions and we deduce the result from the weak Mordell-Weil theorem and the descent procedure.

4.3 Mordell Theorem

Let us focus on the case of $K = \mathbb{Q}$ to illustrate the mechanisms of the proof before resolving the general case. Let us find a good height function on $E(\mathbb{Q})$.

4.3.1 Definition of height function on $E(\mathbb{Q})$

Definition (Height on $\mathbb{Q}$)**.** Let $t \in \mathbb{Q}$ and write $t = \frac{a}{b}$ as a fraction in lowest terms.

The height of t is defined by :

$$H(t) = \max\left\{|a|, |b|\right\}$$

A height function is somehow a way to compute the complexity of a point. For example, $\frac{2}{3}$ and $\frac{162}{244}$ are very close but $\frac{162}{244}$ seem more complicated and we effectively have:

$$H\left(\frac{2}{3}\right) = 3 < 244 = H\left(\frac{162}{244}\right)$$

Then, we will only keep points which are simple, let us say $H(P) \leqslant C_3$. It will be obvious that there are only finite number of such points, and we have already one of our wanted properties.

Definition (Height on $E(\mathbb{Q})$)**.** Let $E/\mathbb{Q}$ be an elliptic curve defined by its Weierstrass equation :

$$(E): \quad y^2 = x^3 + Ax + B \text{ with } A, B \in \mathbb{Z}$$

The logarithmic height on $E(\mathbb{Q})$ relative to the given Weierstrass equation is the function :

$$\begin{array}{rccl} h_x: & E(\mathbb{Q}) & \longrightarrow & \mathbb{R}_+ \\ & P & \longmapsto & h_x(P) = \begin{cases} \log H\big(x(P)\big) & \text{if } P \neq O \\ 0 & \text{if } P = O \end{cases} \end{array}$$

4.3.2 Verification of its properties

Now, we are going to show that h_x is a good height function, which means that is satisfies the expected properties :

Lemma 4.10. *Let $E/\mathbb{Q}$ be an elliptic curve defined by its Weierstrass equation :*

$$(E): \quad y^2 = x^3 + Ax + B \text{ with } A, B \in \mathbb{Z}$$

Then we have the following properties :

- *Let $Q \in E(\mathbb{Q})$. There is a constant C_1 that depends on Q and E such that :*

$$\forall P \in E(\mathbb{Q}): \quad h_x(P+Q) \leqslant 2h_x(P) + C_1$$

- *There is a constant C_2 that depends on E such that :*

$$h_x\big([2]P\big) \geqslant 4h_x(P) - C_2$$

- *For every constant C_3, the set of points with height less than C_3 is finite :*

$$\sharp\big\{P \in E(\mathbb{Q}) \mid h_x(P) \leqslant C_3\big\} < +\infty$$

Proof.

For $P_0 = O$ or $P \in \{O, \pm P_0\}$ assuming that $C_1 > \max\{h_x(P_0), h\big([2]P_0\big)\}$ is enough.

In the other case, let us write :

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \quad ; \quad P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right)$$

The addition formula [3.6] gives us :

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0$$

Then, after developing and using relation from the Weierstrass equation, we have :

$$x(P + P_0) = \frac{\left(aa_0 + Ad^2d_0^2\right)\left(ad_0^2 + a_0d^2\right) + 2Bd^4d_0^4 - 2bb_0dd_0}{\left(ad_0^2 + a_0d^2\right)^2}$$

So we get $H\big(x(P + P_0)\big) \leqslant C_1' \max\{|a|^2, |d|^2, |bd|\}$ where C_1' only depends on P_0 and E. Indeed, cancellation between numerator and denominator can only decrease the height of the fraction so we have easily the previous estimation. To conclude, it suffices to find an upper bound to $|bd|$ since $H\big(x(P)\big) = \max\{|a|, |d|^2\}$.

Once again we use the Weierstrass equation :

$$b^2 = a^3 + Aad^4 + Bd^6$$

So we get $|b| \leqslant C_1'' \max\{|a|^{3/2}, |d|^3\}$. Then we have :

$$H\big(x(P + P_0)\big) \leqslant C_1 \max\{|a|^2, |d|^4\} = C_1 H\big(x(P)\big)^2$$

Thus, by applying logarithm :

$$h_x(P + P_0) \leqslant 2h_x(P) + C_1$$

Let us show the second point : For $P = (x, y)$ such that $[2]P = O$, we just have to take $C_2 \leqslant 4 \max\big\{h_x(Q) \mid Q \in E(\mathbb{Q})\big\}$. In the other case, duplication formula [3.6] says that we have :

$$x\big([2]P\big) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}$$

Let us define F and G the associated homogeneous polynomials :

$$F(X, Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4 \quad ; \quad G(X, Z) = 4X^3Z + 4AXZ^3 + 4BZ^4$$

Then, writing $x = \dfrac{a}{b}$, we obtain :

$$x\big([2]P\big) = \frac{F(a, b)}{G(a, b)}$$

Now, we have to lower bound the height of this fraction. So this time we need to control the cancellation between the numerator and the denominator.

To do this, we will need some relations, which will be given by F and G. Indeed, $F(X,1)$ and $G(X,1)$ are relatively prime polynomials so they generate the unit ideal in $\mathbb{Q}[X]$. It is implies the existence of identities :

$$f_1F + g_1G = 4\Delta Z^7 \quad ; \quad f_2F + g_2G = 4\Delta X^7 \tag{$*$}$$

With :

$$\begin{aligned}
\Delta &= 4A^3 + 27B^2 \\
f_1(X,Z) &= 12X^2Z + 16AZ^3 \\
g_1(X,Z) &= 3X^3 - 5AXZ^2 - 27BZ^3 \\
f_2(X,Z) &= 4\big(4A^3 + 27B^2\big)X^3 - 4A^2BX^2Z + 4A\big(3A^3 + ZZB^2\big)XZ^2 + 12B\big(A^3 + 8B^2\big)Z^3 \\
g_2(X,Z) &= A^2bX^2 + A\big(5A^3 + 32B^2\big)X^2Z + 2B\big(13A^3 + 96B^2\big)XZ^2 - 3A^2\big(A^3 + 8B^2\big)Z^3
\end{aligned}$$

Let $\delta = \gcd(F(a,b), G(a,b))$ be the cancellation in the fraction $x([2]P)$. From the equations $(*)$, δ divide 4Δ so we get $|\delta| \leqslant |4\Delta|$ and we have bound the reduction of height :

$$H(x([2]P)) \geqslant \frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4\Delta|}$$

We now want to lower bound this quantity in term of H so we need to higher bound the $|4\Delta|$. Using $(*)$ we have :

$$\begin{aligned}
\left|4\Delta b^7\right| &\leqslant 2\max\{|f_1|, |g_1|\}\max\{|F|, |G|\} \\
\left|4\Delta a^7\right| &\leqslant 2\max\{|f_2|, |g_2|\}\max\{|F|, |G|\}
\end{aligned}$$

We also know that from expression of f_1, f_2, g_1, g_2 :

$$\max\{|f_1|, |f_2|, |g_1|, |g_2|\} \leqslant C\max\{|a|^2, |b|^3\}$$

Where C depends on E. Combining all these informations we deduce :

$$\max\{\left|4\Delta a^7\right|, \left|4\Delta b^7\right|\} \leqslant 2C\max\{|a|^3, |b|^3\}\max\{|F|, |G|\}$$

So we obtain :

$$H(x([2]P)) \geqslant \frac{\max\{|F|, |G|\}}{|4\Delta|} \geqslant (2C)^{-1}\max\{|a|^4, |b|^4\}$$

And remembering $H(x(P)) = \max\{|a|, |b|\}$ we have :

$$H(x([2]P)) \geqslant (2C)^{-1}H(x(P))^4$$

Which gives us the result by applying logarithm :

$$h_x([2]P) \geqslant 4h_x(P) - C_2$$

Let us show the last point :

For any constant C, $\left\{t \in Q \mid H(t) \leqslant C\right\} = \left\{\frac{a}{b} \in \mathbb{Q} \mid |a| \leqslant C \text{ and } |b| \leqslant C\right\}$ is clearly finite. Furthermore, for each value of x, there are at most two values of y such that $(x, y) \in E$. Thus $\left\{P \in E(\mathbb{Q}) \mid h_x(P) \leqslant C_3\right\}$ is finite. □

4.3.3 Mordell-Weil Theorem on $\mathbb{Q}$

Now that we have defined a height function on $E(\mathbb{Q})$ with the good properties, we can use the weak theorem and the descent procedure together to conclude the proof of the Mordell-Weil theorem for $K = \mathbb{Q}$.

Theorem 4.11 (Mordell 1922)**.** *Let $E/\mathbb{Q}$ be an elliptic curve.*
Then the group $E(\mathbb{Q})$ is finitely generated.

Proof. The weak Mordell-Weil theorem [4.3] tells us that $\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}$ is finite. From [4.10], $h_x : E(\mathbb{Q}) \to \mathbb{R}$ is a height function satisfying descent procedure's assumptions ([4.9]) for $m = 2$. Then $E(\mathbb{Q})$ is finitely generated. □

4.4 Mordell-Weil Theorem

4.4.1 General height function

Let us look at the general case. In fact, we just have to find a good height function on $E(K)$ for any number field K, that is a function which satisfy the assumptions of [4.9]. And then the weak theorem and the descent procedure that we developed in the general case will induce the Mordell-Weil theorem.

We will not explain the details of the construction but only give the idea about how it works. One can look at the book of Silverman [Sil86] to find the proof and details.

The first step is to define the height of a point $P \in \mathbb{P}^N(K)$. The idea is to generalise the height function $H_{\mathbb{Q}}$ defined on $\mathbb{P}^N(\mathbb{Q})$ as follows. Let $P \in \mathbb{P}^N(\mathbb{Q})$. Then we can find homogeneous coordinates $[x_0, \ldots, x_n]$ of P such that :

$$x_0, \ldots, x_N \in \mathbb{Z} \text{ and } \gcd(x_0, \ldots, x_N) = 1$$

For such choices of coordinates, we define :

$$H_{\mathbb{Q}}(P) = \max\{|x_0|, \dots, |x_N|\}$$

To generalise this definition, we need to introduce the local degree :

Definition (Local degree)**.** Let K be a number field and $v \in M_K$ a valuation.
We call **local degree** the quantity $n_v = [K_v : \mathbb{Q}_v]$.

Then we can define a height function on $\mathbb{P}^N(K)$ as follows. For $P = [x_0, \dots, x_N] \in \mathbb{P}^N(K)$ with $x_0, \dots, x_N \in K$:

$$H_K(P) = \prod_{v \in M_K} \max\left\{|x_0|_v, \dots, |x_N|_v\right\}^{n_v}$$

Using two important standard lemmas, the extension lemma and the product lemma we can deduce interesting properties, in particular for a finite extension L/K we have :

$$H_L(P) = H_K(P)^{[L:K]}$$

Which permit us to define a height H independently of the choice of field :

$$\forall P \in \mathbb{P}^N(K) : H(P) = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$$

The proof of following lemmas can be found in [Lan94, II.1, V.1].

Lemma 4.12 (Extension lemma)**.** *Let $L/K/\mathbb{Q}$ be a tower of number fields and let $v \in M_K$. Let denote $w \mid v$ the valuations $w \in M_L$ which restricted to K are equal to v. Then :*

$$\sum_{\substack{w \in M_L \\ w|v}} n_w = [L : K] n_v$$

Lemma 4.13 (Product lemma)**.** *Let x be a non-zero element of K. Then :*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1$$

Finally we can define our height function on $E(\bar{K})$ as :

$$\begin{array}{rccc} h_f : & E(\bar{K}) & \longrightarrow & \mathbb{R} \\ & P & \longmapsto & h_f(P) = h\big(f(P)\big) \end{array}$$

Where $f \in \bar{K}(E)$ and $h(P) = \log\big(H(P)\big)$ is the absolute logarithmic height.

The hard part is to show that this function is well defined and satisfies the three expected properties. Then, as in the case of $K = \mathbb{Q}$, we deduce the Mordell-Weil theorem from the weak theorem and the descent procedure.

4.4.2 Mordell-Weil theorem

Theorem 4.14 (Mordell-Weil 1928)**.** *Let* K *be a number field and* E/K *be an elliptic curve. Then the group* $E(K)$ *is finitely generated.*

Proof. The weak Mordell-Weil theorem [4.3] tells us that $\frac{E(K)}{2E(K)}$ is finite. Furthermore, $h_f : E(\mathbb{Q}) \to \mathbb{R}$ is a height function satisfying descent procedure's assumptions [4.9] for $m = 2$. Then $E(K)$ is finitely generated. □

Chapter 5

Continuation and open questions

We already know that $E(K)$ is a finitely generated abelian group, there are natural questions appearing about its fundamentals characteristics namely its rank and its torsion group. We are going say some words about it before introducing the famous Birch Swinnerton-Dyer conjecture.

5.1 Torsion group and rank

The first question that we could ask is :

"What is the structure of the torsion group $E(K)_{\text{tors}}$?"

For that question, answers are more satisfying. In the case $K = \mathbb{Q}$ we have Mazur's theorem which precisely gives the possible torsion groups :

Theorem (Mazur 1978)**.** *Let $E/\mathbb{Q}$ be an elliptic curve.*
Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of these 15 groups :

$$\mathbb{Z}/n\mathbb{Z} \text{ for } n \in \{1,\dots,10\} \cup \{12\} \quad ; \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n \in \{1,2,3,4\}$$

Furthermore, each of theses cases occur.

The generalisation to a general number field has been studied by Kamienny which proved the result with Mazur in 1995 for the quadratic fields. Finally, the general result was procured by Merel :

Theorem 5.1 (Merel 1996)**.** *Let $d \in \mathbb{N}^*$. Then it exists a number $B(d)$ such that for all number fields K with $[K : \mathbb{Q}] \leqslant d$ and all elliptic curves E/K :*

$$\text{Card}\big(E(K)_{tors}\big) \leqslant B(d)$$

This is non-trivially equivalent to say that the set $S(d)$ of prime numbers p for which there exists a number field $K/\mathbb{Q}$ of degree at most d and an elliptic curve E/K such that E has a K-rational point of order p, is finite and more precisely that if $d > 1$, $p \in S(d)$ then $p < d^{3d^2}$.

Remark 24. Mazur's theorem shows that $S(1) = \{2, 3, 5, 7\}$ and the extended theorem to the quadratic field established with Kamienny that $S(2) = \{2, 3, 5, 7, 11, 13\}$.

The Merel theorem is a special case of the torsion conjecture or uniform boundedness conjecture which states that the order of the torsion group of an abelian variety over a number field can be bounded in terms of the dimension of the variety and the number field.

Another natural question which follows the previous one is :

"Is the rank of an elliptic curve bounded ?"

To this question very few is known and it is an still open question. The conjecture is that the rank can be arbitrary large. However the elliptic curve over $\mathbb{Q}$ with the highest observed rank [Duj17], found by Elkies in 2006, has a rank at least 28 but we do not even known its exact rank.

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502\,x + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

However, in contrast with this conjecture, there is another which states that the "average rank" of an elliptic curve is $\frac{1}{2}$ and that the repartition is 50% for each case $r = 0$ and $r = 1$, and 0% for $r \geqslant 2$. In 2015, Bhargava and Shankar proved that the average rank of an elliptic curve over $\mathbb{Q}$ is bounded above by $\frac{7}{6}$.

5.2 Birch Swinnerton-Dyer conjecture

These theorems give very precise informations on the torsion group $E(K)$ of K-rational points but the rank is still mysterious because we do not have general theorems and in practice there is no universal procedure to calculate it. So it is a really hard problem to establish the rank of an elliptic curve.

However, the Birch Swinnerton-Dyer conjecture states a link between the rank of an elliptic curve E/K and an analytic quantity, namely a specific function called Hasse-Weil L-function. The Birch Swinnerton-Dyer conjecture is an open question since the 1960s and is one of the seven problems of the millennium put on prize by the Clay institute of mathematics. A simplified version of the conjecture could be stated as follows :

"The rank of an elliptic curve E/K is the annulation order
of its associated L-function at $s = 1$."

Let us define this L-function. It is a variation of the Riemann's zeta function and Dirichlet's L-function. It is defined as a Euler product of terms defined for each prime number :

$$L(E,s) = \prod_p L_p(E,s)$$

Where $L_p(E,s) = (1 - ap^{-s} + p^{1-2s})^{-1}$ and $a = 1 + p - |\tilde{E}_p(\mathbb{F}_p)|$ for good primes. There is some more tricks and definitions for the finite number of primes where the reduction is bad.

We notice that this product converges only for $\mathrm{Re}(z) > \frac{3}{2}$ and it was not even know when the conjecture have been stated that we can extend this function by analytic continuation over the whole complex plane. This property was conjectured by Hasse and proved by Deuring in 1941 for elliptic curves with complex multiplication. It was then proved for all elliptic curves over $\mathbb{Q}$ as a consequence of the modularity theorem.

A partial result have been given by Kolyvagin in 1990. Since we know that every elliptic curve over $\mathbb{Q}$ is modular (2001), we can formulate it as follows :

" If $L(E,s) \sim c(s-1)^m$ for $c \neq 0$ and $m \in \{0,1\}$ then the conjecture holds."

So the conjecture is true if the elliptic curve $E/\mathbb{Q}$ has rank zero or one.

Another important partial result is the case of elliptic curve over function fields. Artin and Tate showed in the 1960s that the conjecture holds in this case if and only if the Tate-Shafarevich group $Ш(E)$ is finite. The finiteness of this group was, with the analytic continuation on $\mathbb{C}$, the two main conjecture in the 1960s. But if the last one have been solved, the finiteness of $Ш(E)$ is still an open question.

And that is all. Nothing have been proved for elliptic curve of rank greater than 1, but computations suggest that this conjecture is true even if the road to a general proof still seems to be very long. Many references could be checked and a lot of interesting articles have been published on this subject. For my part, I will only cite the official description [Wil01] given by the Clay institute through an article written by A. Wiles.

Bibliography

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer-Verlag New York, 1977.

[Mat80] Hideyuki Matsumura. *Commutative algebra*. Benjamin/Cummings Publishing Co., 1980.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[Lan94] Serge Lang. *Algebraic number theory*. Springer-Verlag, 1994.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag, Berlin Heidelberg, 1999.

[Wil01] Andrew Wiles. *The Birch and Swinnerton-Dyer Conjecture : Official Problem Description*. 2001. URL: `http://www.claymath.org/sites/default/files/birchswin.pdf`.

[Swi02] H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*. Cambridge University Press, 2002.

[Sno13] Andrew Snowden. *Course on Mazur's theorem*. 2013. URL: `http://www-personal.umich.edu/~asnowden/teaching/2013/679/`.

[Li15] Chao Li. *What is the Birch and Swinnerton-Dyer conjecture?* 2015. URL: `http://www.math.columbia.edu/~chaoli/docs/BSD.html`.

[Duj17] Andrej Dujella. *History of elliptic curves rank records*. 2017. URL: `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`.