ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Dipartimento di Matematica

Corso di Laurea in Matematica

Diophantine Approximation and Integral Points on Algebraic Curves

Tesi di Laurea in Teoria dei Numeri

Relatore:
Chiar.mo Prof.
Lars Halvard Halle

Presentata da:
Alessio Concetti

Anno Accademico 2024/2025

Introduction

The thesis lies within the field of Diophantine approximation, which aims to study how well elements of a number field can be approximated by rational numbers or by elements of simpler subfields. This approach, originally developed in the study of Diophantine equations, has made it possible to deepen the understanding of the interactions between the arithmetic properties of numbers and the structures of number fields. To address such problems it is essential to analyze the properties of absolute values on number fields, through which one can define the notion of distance between two elements, as well as the "height" of an element, understood informally as a measure of its arithmetic size and complexity. This perspective naturally leads to the study of algebraic varieties and curves, with particular attention to elliptic curves, which provide a privileged setting in which Diophantine techniques can be applied effectively. We will see how elliptic curves are endowed with a group structure, which will be essential in determining properties related to height and distances defined on the curve. Finally, the analysis culminates in Siegel's Theorem, which provides a fundamental result concerning the finite number of integral points on elliptic curves defined over number fields. The thesis aims to illustrate how the ideas of Diophantine approximation, combined with geometric and arithmetic tools, lead to concrete results in the understanding of integral solutions of algebraic equations.

Contents

Introduction i

1 Preliminary notions 1

1.1 Fields . . . 1

1.2 Affine and Projective spaces . . . 3

1.3 Rings . . . 4

2 Diophantine approximation 9

2.1 Classical results on Diophantine approximation . . . 9

2.2 Absolute values for fields . . . 14

2.3 Heights . . . 20

2.4 Roth's theorem . . . 24

3 Introduction to Curves 27

3.1 Varieties . . . 27

3.2 Maps between curves . . . 32

3.3 Divisors and differentials . . . 35

3.4 The genus of a curve . . . 37

4 Elliptic curves 41

4.1 Weierstrass equation . . . 41

4.2 Group Law and Isogenies . . . 46

4.3 Height for elliptic curves . . . 52

4.4 Mordell-Weil Theorem . . . 54

5 Diophantine Approximation on Curves 57

5.1 Distances on curves . . . 57

5.2 Siegel's theorem and consequences . . . 61

Bibliografia 65

Chapter 1

Preliminary notions

In this chapter we gathers the fundamental concepts and theoretical tools necessary for the development of the main results of the thesis. We will remark what is a number field and the basic properties that it has, standard properties of the Galois group, what is an algebraic closure of a field and some facts about the ring of integers of a field. Then we will also see what is an affine space and a projective space over a field, necessary tools that will be used to introduce varieties and curves.

1.1 Fields

In this section we summarize some of the basic definitions and facts about fields that we will use throughout all the thesis. We give particular attentions to number fields, finite extension of the rational numbers, which will be the main object of interest.

Definition 1.1.1. *Let K be a field. An element β is called* ***algebraic*** *over K if there exists $K \subseteq L$ extension of field such that $\beta \in L$ and it is possible to find a polynomial $f \in K[x]$ such that $f(\beta) = 0$. β is* ***transcendental*** *over K if it is not algebraic. We call algebraic (transcendental) number an element β that is algebraic (transcendental) over $\mathbb{Q}$.*

Definition 1.1.2. *Let K be a field and β algebraic over K. Then $q \in K[x]$ is the* ***minimal polynomial of*** *β over K if $q(\beta) = 0$ and q is a monic polynomial of least degree among all polynomials $F \in K[x]$ such that $F(\beta) = 0$.*

The fact that this polynomial has minimal degree and is monic ensures that it is unique.

Definition 1.1.3. *Let β algebraic over $\mathbb{Q}$ and $f \in \mathbb{Q}[x]$ its minimal polynomial; we define* ***the degree of*** *β as $\deg \beta = \deg f$. Suppose $\deg \beta = n$ and consider $\beta = \beta_1, \ldots, \beta_n \in \mathbb{C}$ all complex roots of f; these are called* ***conjugates of*** *β. Notice that:*

$$f(x) = \prod_{i=1}^{n} (x - \beta_i)$$

Remark 1.1.4. If β is an algebraic number and $q(x) = x^n + r_1 x^{n-1} + \ldots + r_n$ his minimal polynomial, with $r_i \in \mathbb{Q}$ (and $r_0 = 1$). We can suppose $r_i = a_i/b_i$ with $a_i, b_i \in \mathbb{Z}$; then we can multiply this polynomial by $B = \operatorname{lcm}(b_1, \ldots, b_n)$ and get $r_i B \in \mathbb{Z}$. If $d = \gcd(r_1 B, \ldots, r_n B)$, we get $f(x) := \frac{B}{d} g(x) = c_0 x^n + c_1 x^{n-1} + c_n$, with $c_i = r_i B/d \in \mathbb{Z}$ and $\gcd(c_0, \ldots, c_n) = 1$. f is called the **primitive minimal polynomial for** β.

Definition 1.1.5. *Let K a number field , $[K : \mathbb{Q}] = n$. $\sigma : K \hookrightarrow \mathbb{C}$ is an* ***embedding of*** *K* ***in*** *$\mathbb{C}$ if σ is a field homomorphism and $\sigma(q) = q$ for all $q \in \mathbb{Q}$.*

Notice that, if $\beta \in K$ such that $K = \mathbb{Q}[\beta]$, called **primitive element for** K, then an embedding σ is uniquely determined by the image of β.

Proposition 1.1.6. *If K number field, suppose $[K : \mathbb{Q}] = n$, $\beta \in K$ such that $K = \mathbb{Q}[\beta]$ and f minimal polynomial for β and $\beta = \beta_1, \ldots, \beta_n$ conjugates of β. Then there are exactly n distinct embeddings corresponding to the roots of f, more precisely, there is exactly an embedding sending $\beta \mapsto \beta_i$ for all i.*

If an embedding sends β in a real root, then its image in contained in $\mathbb{R}$ and we call it a real embedding. Otherwise, there will be two distinct embeddings $\sigma, \bar{\sigma}$ corresponding to complex conjugates root. The notation is justified from the fact that $\overline{\sigma(x)} = \bar{\sigma}(x)$ for all $x \in K$.

Definition 1.1.7. *Let K a field. We say that K is* ***algebraically closed*** *if every non constant polynomial $f \in K[x]$ has at least a root in K.*

Example 1.1.8. $\mathbb{R}$ is not algebraically closed, because the polynomial $x^2 + 1$ has no real roots. The fundamental theorem of algebra says that $\mathbb{C}$ is algebraically closed.

Definition 1.1.9. *Let K be a field. An* ***algebraic closure of*** *K is a field L that contains K and it is algebraically closed.*

It can be proved that an algebraic closure of a field K always exists and that is unique up up to an isomorphism that fixes K. We will usually denote the algebraic closure $\bar{K}$. Note that the algebraic closure of K is exactly the set of all algebraic elements over K.

Example 1.1.10. $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$. $\bar{\mathbb{Q}}$ is the set of all algebraic elements over $\mathbb{Q}$. Note that $\bar{\mathbb{Q}} \subset \mathbb{C}$.

Then we define the norm function for an algebraic field extension.

Definition 1.1.11. *Let L/K be a finite extension. Then, for all $\alpha \in L$, we can consider the linear map*

$$m_\alpha : L \to L, \quad m_\alpha(x) = \alpha \cdot x$$

Then, we define:

$$\mathrm{Nm}_{L/K}(\alpha) := \det(m_\alpha)$$

Next we see some properties about this norm.

Proposition 1.1.12. *Let L/K be a finite extension, $[L : K] = n$. Then :*

- $\mathrm{Nm}_{L/K}(\alpha\beta) = \mathrm{Nm}_{L/K}(\alpha) \cdot \mathrm{Nm}_{L/K}(\beta)$, *for all $\alpha, \beta \in L$;*
- $\mathrm{Nm}_{L/K}(\alpha) = 0 \iff \alpha = 0$;
- *If $L/K/\mathbb{Q}$ finite extension, $\mathrm{Nm}_{L/K}(\alpha) = \prod \sigma(\alpha)$, where the product is for every embedding of L in $\mathbb{C}$ fixing K.*

Example 1.1.13. Consider $K = \mathbb{Q}[\sqrt{d}]$ with $d \in \mathbb{Z}$ square free, $[K : \mathbb{Q}] = 2$. Then

$$\mathrm{Nm}_{K/\mathbb{Q}}(a + b\sqrt{d}) = \sigma_1(a + b\sqrt{d}) \cdot \sigma_2(a + b\sqrt{d}) = a^2 - db^2$$

where we wrote $\alpha \in \mathbb{Q}[\sqrt{d}]$ as $a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$.

1.2 Affine and Projective spaces

In this section we just give the definitions of Affine spaces and Projective spaces. We will see later that a variety is a subset of this spaces.

Definition 1.2.1 (Affine space)**.** *An **Affine n-space** over K is :*

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

The set of K-rational points of $\mathbb{A}^n$ is

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) : x_i \in K\}.$$

We can image an affine space as a n- dimensional vector space. Then, defining an equivalence relation on an affine space, we can define a projective space. We can image it as the set of all "lines" in the affine space.

Definition 1.2.2. *Given a field K, we can define $\mathbb{P}^n(K)$ n-dimensional projective space as*

$$\mathbb{P}^n(K) := (\mathbb{A}^{n+1}\backslash\{0\})/\sim$$

where $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff$ there exists $\lambda \in K^\times : y_i = \lambda x_i$ for all $i = 0, ..., n$. We will usually denote an element of $\mathbb{P}^n(K)$ by $[x_0, ..., x_n]$.

1.3 Rings

In this section, we quickly review some facts about rings, such as prime ideals, which will be needed when introducing curves. We then define and examine the properties of the ring of integers of a field. Studying the ring of integers forms the foundation of number theory, but the proofs of certain results are far from trivial, so we limit ourselves to the statements only. Readers who wish to explore this topic further can consult J.S. Milne's notes "Algebraic Number Theory" [4].

Definition 1.3.1. *Given a commutative ring $(A, +, \cdot)$, we say that $I \subseteq A$ is an **Ideal** of A if it is an additive subgroup and for all $x \in I$, for all $a \in A$, $ax \in I$.*
*An ideal I is **prime** if $I \neq A$ and the following is true for all $x, y \in A$:*

$$xy \in I \implies x \in I \text{ or } y \in I$$

Let $x \in I$, then we define $(x) := \{ax : a \in A\}$ to be the ideal generated by x.

Example 1.3.2. An ideal $\{0\} \neq I \subset \mathbb{Z}$ is prime if and only if $I = (p) = p\mathbb{Z}$ for some prime p. If $0 \neq f \in K[x]$ irreducible over K, then (f) is a prime ideal.

Definition 1.3.3. *An ideal $I \subsetneq A$ is a **maximal ideal** if there is no ideal $J \neq A$ such that $I \subset J$.*

It can be easily proved that a maximal ideal is always prime.

Definition 1.3.4. *A ring A is a **local ring** if A has a unique maximal ideal $\mathfrak{m}$.*

Next we state a result about local rings that we will use later.

Proposition 1.3.5. *Let A local ring with maximal ideal $\mathfrak{m}$, then $A\backslash\mathfrak{m}$ corresponds to the units of the ring.*

Before giving some examples, let's give a useful definition:

Definition 1.3.6. *Let A be a domain. We can define its* ***fraction field*** *as:*

$$\mathrm{Frac}(A) := \left\{ \frac{a}{b} : a, b \in A, b \neq 0 \right\}$$

where a/b is an equivalence class of $A \times (A \backslash \{0\})$ and we define operations between fractions as usual.

Obviously the fraction field is a field. Moreover, it's the smallest field containing the ring A.

Example 1.3.7. Let $\mathfrak{p} \subset A$ be a prime ideal, then

$$A_{\mathfrak{p}} := \left\{ \frac{a}{b} \in \mathrm{Frac}(A) : b \notin \mathfrak{p} \right\}$$

is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$. This ring is called the **localization of A at $\mathfrak{p}$**.To see an easy example, take:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \not\equiv 0 \mod (p) \right\}$$

where p is a prime.

Definition 1.3.8. *A ring A is said to be a* ***discrete valuation ring*** *if it is local and its unique maximal ideal is principal.*

For a discrete valuation ring, it is easy to see that any non zero ideal is a power of its unique maximal ideal. Then it is easy to see that, if we consider $K = \mathrm{Frac}(A)$, then for all $x \in K^{\times}$, $x = u \cdot \pi^n$, where u invertible in A,π is a generator of the unique maximal ideal and $n \in \mathbb{Z}$. Then we can define a function:

$$v : K^{\times} \longrightarrow \mathbb{Z} \quad v(x) := n$$

This function is called discrete valuation. Then we introduce the ring of integers of a number field.

Definition 1.3.9. *Let K be a number field. We say that $\alpha \in K$ is integral over A, where $A \subset K$ ring if there exists $f \in A[x]$ monic polynomial such that $f(\alpha) = 0$. Then we define the* ***ring of integers of*** *K as*

$$\mathcal{O}_K := \{x \in K : x \text{ is integral over } \mathbb{Z}\}.$$

The ring of integers of a field is very important to understand properties of the field. For example it can be proved that a ring K is the fraction field of $\mathcal{O}_K$. Another non trivial fact is that the ring of integers is finitely generated as a $\mathbb{Z}$- module, namely there exists $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ such that all $x \in \mathcal{O}_K$ is a linear combination of the ω_i-s.

Example 1.3.10. As expected,the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$. The ring of integers of a quadratic extension of $\mathbb{Q}$, say $K = \mathbb{Q}[\sqrt{d}]$, with $d \in \mathbb{Z}$ square-free has ring of integers equals to

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] \text{ if d} \equiv 2, 3 \mod 4;$$
$$\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{d})/2] \text{ if d} \equiv 1 \mod 4.$$

It can be also proven that $\mathcal{O}_K$ is integrally closed, i.e. if an element of K is integral over $\mathcal{O}_K$ then it is in $\mathcal{O}_K$ and that every prime ideal of the ring of integers is maximal. This properties ensures that $\mathcal{O}_K$ is a **Dedeking Domain**. Then every localization $(\mathcal{O}_K)_{\mathfrak{p}}$ at some prime ideal $\mathfrak{p}$ is discrete valuation ring. We denote $v_{\mathfrak{p}}$ the discrete valuation associated to $(\mathcal{O}_K)_{\mathfrak{p}}$. Then we state a useful theorem, that it is true for all Dedeking's domain but we see its application only for the ring of integers:

Theorem 1.3.11. *Let K be a field and $\mathcal{O}_K$ its ring of integers. Then for all proper non zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ can be written in the form:*

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{r_i}$$

where $\mathfrak{p}_i \subset \mathcal{O}_K$ distinct prime ideals and $n, r_i \in \mathbb{Z}, n, r_i > 0$ for all i. All $\mathfrak{p}_i$-s and r_i-s are uniquely determined.

Remark 1.3.12. Let $x \in K^\times$ and consider $x\mathcal{O}_K = \{x\alpha : \alpha \in \mathcal{O}_K\}$. Since K is the fraction field of $\mathcal{O}_K$, there exists $a, b \in \mathcal{O}_K$, $b \neq 0$, such that $x = a/b$. Since $a.b$ can be written as product of powers of prime ideals, we can say that

$$(x) = \prod_{i=1}^{n} \mathfrak{p}_i^{n}$$

with $n_i \in \mathbb{Z}$. (x) is what is called a **fractional ideal**. In this case, we can easily prove that $v_{\mathfrak{p}}(x) = n_i \in \mathbb{Z}$.

Thanks to this remark we can characterize the ring of integers in terms of all $v_{\mathfrak{p}}$:

Proposition 1.3.13. *Let K be a field and $\mathcal{O}_K$ its ring of integers. Then:*

$$\mathcal{O}_K = \{x \in K : v_{\mathfrak{p}}(x) \geq 0 \,\text{forall}\, \mathfrak{p}\, \text{primeideal}\}$$

Proof. Given $x \in \mathcal{O}_K$, since $\mathcal{O}_K \subset (\mathcal{O}_K)_{\mathfrak{p}}$ for all $\mathfrak{p}$ prime ideal, then it must be $v_{\mathfrak{p}}(x) \geq 0$. Conversely, suppose x has $v_{\mathfrak{p}}(x) \geq 0$ for all prime ideals. From what we have seen in the last remark, since (x) can be written as :

$$(x) = \prod_{i=1}^{n} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$$

The hypothesis on x, implies that $(x) \subset \mathcal{O}_K$, then $x \in \mathcal{O}_K$. □

Definition 1.3.14. *Let K be a field and S a finite set of prime ideals of $\mathcal{O}_K$. We define the* ***ring of S-integers*** *as :*

$$\mathcal{O}_{K,S} := \{x \in K : v_{\mathfrak{p}}(x) \geq 0, \text{forall}\, \mathfrak{p} \notin S\}$$

Example 1.3.15. If $S = M_K^{\infty}$, $\mathcal{O}_{K,S} = \mathcal{O}_K$. Note that $\mathcal{O}_K \subset \mathcal{O}_{K,S}$. In general , taking the ring of S-integers means to take elements from the ring of integers and allow them to have denominators that are product of elements in the primes in S. For example, for $K = \mathbb{Q}$, $S = \{p_1, \ldots, p_n\}$ finite set of prime numbers, then

$$\mathcal{O}_{\mathbb{Q},S} = \mathbb{Z}\left[\frac{1}{p_1}, \ldots, \frac{1}{p_n}\right]$$

Chapter 2

Diophantine approximation

In this chapter we introduce the fundamental concepts of Diophantine approximation. Historically, the problem arose in the study of solutions of Diophantine equations, and aims to understand how well an algebraic number can be approximated by a rational number. We will present the main results related to this problem, and then show that the problem can be generalized to an arbitrary number field, thanks to the introduction of the concepts of absolute value, which allows us to measure how close two elements are, and of height, which allows us to measure the quality of the approximation in terms of the 'complexity' of the approximating elements. Finally, we will present Roth's theorem, which represents the best possible result in this area.

2.1 Classical results on Diophantine approximation

We formally introduce the problem of Diophantine approximation, as well as a notion of height for rational numbers, and then we review historically the main theorems that have contributed to the field of Diophantine approximation. We will also see how some of these results can be used to determine how many solutions there are for Diophantine equations and, more generally, the close connection between Diophantine equations and Diophantine approximation.

Definition 2.1.1 (Height of a rational number)**.** *Let* $r \in \mathbb{Q}$*. If* $r = p/q$*, with* $\gcd(p, q) = 1$ *, we define*

$$H(r) := \max(|p|, |q|).$$

Definition 2.1.2 (Mahler measure)**.** *Let β be an algebraic number and $q(x) = a_0x^d + a_1x^{d-1} + \ldots + a_d = a_0\prod_{i=1}^{d}(x-\beta_i)$ be the primitive minimal polynomial of $\beta = \beta_1$. The **Mahler Measure** of β is defined as*

$$M(\beta) := a_0\prod_{i=1}^{d}\max(1,|\beta_i|)$$

One of the first results on the diophantine approximation of algebraic numbers was given by Dirichlet and Liouville.

Theorem 2.1.3 (Dirichlet, 1842)**.** *Let β be an algebraic number, then the inequality*

$$\left|\beta - \frac{p}{q}\right| \leq \frac{1}{q^2} \tag{2.1.1}$$

has infinitely many integer solutions $(p,q) \in \mathbb{Z}^2$

Proof. Let $N \in \mathbb{N}$ and let's consider $\theta_n := \{n\beta\} = n\beta - \lfloor n\beta \rfloor \in [0,1)$ for $n \in 0,1,\ldots,N$. We can now divide $[0,1)$ into N subintervals of length $1/N$. So, since there are N+1 terms and N subintervals, according to the pigeonhole principle, $\exists i,j \in 0,\ldots,N, i<j$ such that $|\theta_j - \theta_i| < 1/N$. If $q := j-i \leq N$ and $p := \lfloor j\beta \rfloor - \lfloor i\beta \rfloor$, we get $|\theta_j - \theta_i| = |q\beta - p| < 1/N$. This implies:

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{Nq} \leq \frac{1}{q^2}$$

The second inequality is true because $N \geq q$. For each N, we choose a solution for which $|\beta - p/q|$ is minimal. Then choose a natural number N_0 and take the solution p_0/q_0 following the above procedure. By induction, suppose we have p_n/q_n solution to the inequality; then by choosing $N > |p_n/q_n - \beta|^{-1}$, we can take p_{n+1}/q_{n+1} solution different from the others. In fact:

$$\left|\beta - \frac{p_{n+1}}{q_{n+1}}\right| \leq \frac{1}{Nq_{n+1}} < \left|\beta - \frac{p_n}{q_n}\right| q_{n+1}^{-1}$$

Then p_{n+1}/q_{n+1} must be different from the previous solutions. We proved that $\forall n \in \mathbb{N}, \exists (p_n,q_n) \in \mathbb{Z}^2$ different solutions to (2.1.1). □

So, we proved that there exist infinitely many pairs of integers x,y such that $|\beta - \frac{x}{y}| \leq |y|^{-2}$. For such solutions, we have $|y\beta - x| \leq |y|^{-1} \leq 1$, because $y \in \mathbb{Z}$, then $|x| \leq |\beta y| + 1 \leq (|\beta|+1)|y|$. Writing $r = x/y$ we can deduce that $\exists c(\beta) > 0$, $c(\beta) = (|\beta|+1)^2$ such that

$$|\beta - r| \leq c(\beta)H(r)^{-2} \quad \text{for infinitely many } r \in \mathbb{Q}. \tag{2.1.2}$$

This is true because $1/y^2 \leq c(\beta)/H(r)^2$; this can be verified easily.
Below I report the theorem but with an alternative proof with respect to Liouville, took from [6], Theorem 6.1 .

Theorem 2.1.4 (Liouville, 1851)**.** *If β is an algebraic number, then there is a computable number $c(\beta) > 0$ such that*

$$|\beta - r| \geq c(\beta) H(r)^{-deg(\beta)} \tag{2.1.3}$$

is true $\forall r \in \mathbb{Q}, r \neq \beta$

Proof. Let's consider $q(x)$ primitive minimal polynomial of β and $P(X,Y) = Y^d q(X/Y) = a_0 \prod_{i=1}^{d}(X - \beta_i Y)$. Let $r = x/y, (x,y) \in \mathbb{Z}^2, \gcd(x,y) = 1$ and $r \neq \beta$, then

$$\begin{aligned}\frac{|P(x,y)|}{2^{d-1}M(\beta)H(r)^d} &\overset{def}{=} \frac{a_0 \prod_{i=1}^{d}(x - \beta_i y)}{2^{d-1} a_0 \prod_{i=1}^{d} \max(1, |\beta_i|)(\max(|x|, |y|))} \\ &= \frac{|x - \beta y|}{\max(1,\beta) \cdot \max(|x|,|y|)} \cdot \prod_{i=2}^{d} \frac{|x - \beta_i y|}{2\max(1, |\beta_i|) \cdot \max(|x|,|y|)}\end{aligned}$$

We can easily see that the last productory is ≤ 1, because $|x - \beta_i y| \leq |x| + |\beta_i y|$, so we can split it in two fractions, both $\leq 1/2$, for all i; also

$$\frac{|x - \beta y|}{\max(1,\beta) \cdot max(|x|,|y|)} \leq |\beta - \frac{x}{y}|$$

because the denominator is $\geq |y|$. Then we get

$$\frac{|P(x,y)|}{2^{d-1}M(\beta)H(r)^d} \leq \left|\beta - \frac{x}{y}\right|$$

Since $r \neq \beta$, $|P(x,y)| \geq 1$. Together with the inequality above, this implies (2.1.3) with $c(\beta) := 2^{1-d} M(\beta)^{-1}$.

□

One of the central problems in Diophantine approximation is to obtain improvements of (2.1.3). More precisely the problem is whether $\exists \tau < d$ and $\exists c(\beta, \tau) > 0$ such that

$$|\beta - r| \geq c(\beta, \tau) H(r)^{-\tau} \quad \forall r \in \mathbb{Q} \tag{2.1.4}$$

By Dirichlet's theorem, precisely in equation 2.1.2, we proved that there exist infinitely many rationals $r \in \mathbb{Q}$ such that $|\beta - r| \leq c(\beta) H(r)^{-2}$. This shows that it's impossible to put $\tau < 2$ in (2.1.4). In particular, for rationals and quadratic numbers ($deg(\beta) = 1$ or 2), Liouville's Theorem gives the best possible result.

Proposition 2.1.5. *Let β be a real algebraic number of $deg(\beta) \geq 3$ and $m > 2$, $m \in \mathbb{R}$. Then they are equivalent:*

1. $\forall \tau > m, \exists c(\beta, \tau) > 0$ *such that (2.1.4) is true*

2. $\forall \tau > m, \forall C > 0$ *the inequality*

$$|\beta - r| \leq CH(r)^{-\tau} \tag{2.1.5}$$

has only finitely many solutions $r \in \mathbb{Q}$

Proof. (1. $\implies$ 2.)
Let $\tau, \delta > m, \delta > \tau$, then , by contradiction, let's suppose that (2.1.5) has infinitely many rational solutions, then $\exists \{r_n\} \in \mathbb{Q}$, with $H(r_n) \overset{n \to +\infty}{\longrightarrow} \infty$ (if $H(r_n)$ were limited, then we would have only finitely choices for different r_n). With (1), we get

$$c(\beta, \tau) H(r_n)^{-\tau} \leq |\beta - r_n| \leq CH(r_n)^{-\delta},$$

this implies $c(\beta, \tau) \leq CH(r_n)^{\tau - \delta} \to 0$ as $n \to \infty$, but this contradicts $c(\beta, \tau) > 0$.
(2. $\implies$ 1.)
Let $\tau > m$ and

$$c(\beta, \tau) := \inf_{r \in \mathbb{Q}} H(r)^{\tau} |\beta - r|.$$

By contradiction, if it were $c(\beta, \tau) = 0$ then $\exists \{r_n\}_{n \in \mathbb{N}} \in \mathbb{Q}$ all distinct, such that $H(r_n)^{\tau} |\beta - r_n| \to 0$. So $\exists \bar{n} > 0$ such that $|\beta - r_n| \leq CH(r)^{-\tau}, \forall n \geq \bar{n}$, but this gives infinitely many rationals solutions to (2), so it is a contradiction. Then it must be $c(\beta, \tau) > 0$ and $c(\beta, \tau) \leq H(r)^{\tau} |\beta - r|, \forall r \in \mathbb{Q}$. □

Theorem 2.1.6 (**Thue's theorem**). *If β is an algebraic number, with $deg(\beta) > 1$ (i.e. β irrational), and $\tau > deg(\beta)/2 + 1$, then the inequality:*

$$|\beta - r| \leq H(r)^{-\tau}$$

has only finitely many rational solutions $r \in \mathbb{Q}$.

Corollary 2.1.7. *Let $P \in \mathbb{Z}[x, y]$ be an homogeneous polynomial of degree $d \geq 3$ irreducible over $\mathbb{Z}$. If $m \in \mathbb{Z}$, then equation $P(x, y) = m$ has finitely many integer solutions $(x, y) \in \mathbb{Z}^2$.*

Proof. Let $P(x, y) \in \mathbb{Z}[x, y]$ be an homogeneous polynomial of degree $d \geq 3$, irreducible over $\mathbb{Z}$, $m \in \mathbb{Z}$. Suppose $(x, y) \in \mathbb{Z}^2$ solution to $P(x, y) = m$. Let $r := x/y$

and let $\tau > d/2+1$. By proposition (2.1.5), we can assume an equivalent form of Thue's theorem, i.e. if β is an algebraic number, $\tau > d/2+1, \exists c(\beta,\tau) > 0$ such that

$$|\beta - r| \geq c(\beta,\tau)H(r)^{-\tau} \quad \forall r \in \mathbb{Q} \tag{2.1.6}$$

Now, if $y = 0$ then $P(x,0) = a_0x^d = m$ has a maximum of d roots in $\mathbb{C}$ .We can repeat the argument for solutions $(0,y)$. Then we can consider solutions (x,y) with $x, y \neq 0$.

We prove the inequality only for pairs of integers(x,y) with $|y| \geq |x|$, so $|y| \geq H(r)$ (it is $y = H(r)$ if and only if $\gcd(x,y) = 1$). Then the inequality can be deduced for pairs (x,y) with $|x| > |y|$ by interchanging x and y and repeating the argument below.

Let $p(X) := P(X,1), p \in \mathbb{Z}[x]$. p is irreducible over $\mathbb{Z}$ with degree ≥ 3. We can write $p(x) = a_0\prod_{i=1}^{n}(x-\beta_i)$. Note that, as p is irreducible , the β_i-s are all distinct. Using the homogeneity of P once again, we have $P(x,y) = y^dp(r)$, then

$$P(x,y) = m \iff a_0y^d\prod_{i=1}^{d}(r-\beta_i) = m.$$

Now let $r = x/y$, $j \in 1,...,d$ such that $|\beta_j - r| = \min_i|\beta_i - r|$. Note that $\forall i \neq j$ we have

$$|\beta_j - \beta_i| \leq |\beta_j - r| + |r - \beta_i| \leq 2|\beta_i - r|.$$

then $|\beta_i - r| \geq \frac{1}{2}|\beta_j - \beta_i|$. Using this inequality, the assumption $|y| \geq |x|$ and (2.1.6), we get

$$|m| = |y^d||a_0|\prod_{i=1}^{d}|r-\beta_i| \geq |a_0|\left(\prod_{i\neq j}\frac{1}{2}|\beta_j - \beta_i|\right)c(\beta_j,\tau)H(r)^{d-\tau}$$

Calling $C := |a_0|c(\beta_j,\tau)\prod_{i\neq j}\frac{1}{2}|\beta_j - \beta_i|$, we can see that $C > 0$, because $a_0 \neq 0$, $c(\beta_j,\tau) > 0$, and being the β_i-s all distinct, the productory isn't 0. Therefore C does not depend on x and y. So we get:

$$H(r) \leq \left(\frac{|m|}{C}\right)^{\frac{1}{d-\tau}}$$

Where we chose $d/2+1 < \tau < d$; such τ exists because $d \geq 3$. In other words, $H(r)$ is bounded, and this implies that we have limited choices for x and y, so finitely many solutions. □

Remark 2.1.8. This result stands in sharp contrast with the case $deg(P) = 2$, in which it is possible to have an infinite number of solutions. For example, Pell's

equation $x^2 - Dy^2 = 1$ has infinite many solutions if $D \in \mathbb{Z}$ not a perfect square. Hence, we can deduce an important fact: considering the equation $x^n - Dy^n = 1$, with $D \in \mathbb{Z}, n \geq 2$, and $(x, y) \in \mathbb{Z}^2$ is a solution then

$$\left(\frac{x}{y}\right)^n - D = \frac{1}{y^n},$$

i.e. x/y is a good approximation of the n-th root of D. So, the results above tell us that every square root can be approximated by infinitely many rational numbers, but this property does not hold for cubic, quartic, and higher roots.

2.2 Absolute values for fields

Here we define formally what an absolute value is, see how an absolute value define a distance and then a topology, and we will ask how many absolute values that induce different topologies on K there are. We will see that the answer is strictly related to the algebraic property of a number field. We will report only the theorems and fundamental properties that we will use later, leaving aside more technical details or advanced developments that go beyond the main focus of this discussion.

Definition 2.2.1. *Let K be a field, $|\cdot| : K \to \mathbb{R}$ is an **absolute value** for K if*

- $|x| > 0, \forall x \in K^\times$ *and* $|0| = 0$*;*
- $|xy| = |x||y|, \forall x, y \in K$*;*
- $|x + y| \leq |x| + |y|, \forall x, y \in K$ *(triangle inequality).*

*Therefore, if the stronger condition $|x + y| \leq \max(|x|, |y|)$, called **ultrametric inequality** or strong triangle inequality, holds for all $x, y \in K$, then $|\cdot|$ is called **non-archimedean absolute value**. If it does not satisfy the ultrametric inequality, then the absolute value is called Archimedean.*

We can remark that $|\cdot|$ is a group homomorphism $K^\times$ to $\mathbb{R}^+$(multiplicative group). This implies that on every finite field K can be defined only the trivial absolute value,because $v(K^\times)$ is a finite multiplicative subgroup of $\mathbb{R}^+$, then $v(K^\times) = \{1\}$.

Definition 2.2.2. *If $|\cdot|$ nonarchimeden absolute value, we can also define $v(x) := -log|x|$ (log with base $e > 1$ for some real e. v is an **additive valuation**,i.e. it's*

true that $v(xy) = v(x) + v(y)$ *and* $v(x+y) \geq \min(v(x), v(y))$. *An additive valuation is* ***discrete*** *if* $v(K^\times) = \mathbb{Z}$. *We formally define* $v(0) := \infty$.

Example 2.2.3.

1. For every field K we can define the **trivial absolute value** $|x| = 1, \forall x \in K^\times$ and $|0| = 0$. It is obviously non-archimedean.
2. For $\mathbb{C}$, the standard euclidean norm $|z| = \sqrt{(\Re z)^2 + (\Im z)^2}$ is archimedean.
3. If K number field and $\sigma : K \hookrightarrow \mathbb{C}$ embedding, then $|x| = |\sigma(x)|$ is an absolute value.
4. In $\mathbb{Q}$, for every p prime we define $\mathrm{ord_p}(x) = r$ if $x = \frac{a}{b}p^r$, with $r \in \mathbb{Z}$ and $p \nmid ab$. Then if $e \in \mathbb{R}, e > 1$, $|x|_p := e^{-\mathrm{ord}_p(x)}$ is a non-archimedean absolute value, called **p-adic absolute value**. If $e = p$, we call $|\cdot|_p$ the normalized absolute value; in this case $v_p(x) = \mathrm{ord}_p(x)$. We can generalize to K, taking $\mathrm{ord} : K^\times \to \mathbb{Z}$ discrete valuation and set $|x| = e^{-\mathrm{ord}(x)}$

Remark 2.2.4. An absolute value on K defines a distance function $d(x, y) = |x-y|$, so we can consider the topology associated with the metric d on K. Therefore it seems natural to ask the following question: when do two absolute values induce the same topology on K?

Proposition 2.2.5. *Let* $|\cdot|_1, |\cdot|_2$ *be absolute values on* K. *The following conditions are equivalent:*

1. $|\cdot|_1$ *and* $|\cdot|_2$ *defines the same topology on* K.
2. $\exists c > 0$ *such that* $|x|_1 = |x|_2^c$, $\forall x \in K$.

If one of these two is true we say that $|\cdot|_1$ *and* $|\cdot|_2$ *are* ***equivalent*** *and write* $|\cdot|_1 \sim |\cdot|_2$.

Definition 2.2.6. *For a field* K, *we can define* $M_K :=\{\ |\cdot|$ *nontrivial absolute value on* $K\}/\sim$. *Therefore we can define* $M_K^\infty \subset M_K$ *to be the set of archimedean absolute values and* $M_K^0 \subset M_K$ *to be the set of non-archimedean ones. The elements of* M_K *are called* ***places*** *(or* ***primes*** *of* K *). Notice that* $M_K = M_k^0 \sqcup M_k^\infty$.

Example 2.2.7. If $K = \mathbb{Q}$, there is a theorem of Ostrowski (see [4] Theorem 7.12) that tells us that

$$M_{\mathbb{Q}} = \{|\cdot|_\infty\} \cup \{|\cdot|_p \text{ with } p \text{ prime }\},$$

where $|\cdot|_\infty$ is the standard absolute value on $\mathbb{Q}$.

Theorem 2.2.8 (Product formula for $\mathbb{Q}$)**.** *For all $x \in \mathbb{Q}$ different than 0:*

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1$$

Proof. If we set $\pi(x) := \prod_{v \in M_{\mathbb{Q}}} |x|_v$, we notice that π is multiplicative, then if suffices to show that $\pi(-1) = 1$ (that it's trivial) and $\pi(p) = 1$ for every prime p. From the example $v = p$, with p prime or $v = \infty$. We have $|p|_p = 1/p$, $|p|_q = 1$ for every prime $q \neq p$ and $|p|_\infty = p$, then $\pi(p) = 1$. □

Now we can ask if it is possible to extend this result to a number field K and the answer is "yes", up to slightly modifying this formula. To do this we need to know how absolute values extends to an extension of K. If we have w, v places respectively of L and K, L extension of K, we say that w **divides** v and write $w|v$ if $|\cdot|_w$ restricted to K is equal to $|\cdot|_v$. Then we introduce complete fields in respect to an absolute value.

Definition 2.2.9. *Let K be a field and $v \in M_K$. A sequence $(a_n)_{n \in \mathbb{N}} \in K$ is said to be a **Cauchy sequence** if , for all $\varepsilon > 0$, there exists $n_\varepsilon \in \mathbb{N}$ such that:*

$$|a_n - a_m|_v < \varepsilon, \text{for all } n, m > n_\varepsilon.$$

*K is said to be **complete** if every Cauchy sequence has a limit in K,i.e. it exists $r \in \mathbb{Q}$ such that:*

$$\lim_{n \to \infty} |a_n - r|_v = 0$$

Note that, if we consider $v \in M_K^0$, then it suffices to have $|a_{n+1} - a_n|_v < \varepsilon$ for all $n > n_\varepsilon$ to prove that a sequence is Cauchy, thanks to the ultrametric inequality.

Example 2.2.10. By its definition, $\mathbb{R}$ is complete in respect to the standard absolute value, while $\mathbb{Q}$ isn't complete. Moreover, $\mathbb{Q}$ isn't complete in respect to every p-adic absolute value. A way to prove this is to consider the sequence (a_n) defined as $a_0 = 1$ and

$$a_{n+1} = a_n - \frac{a_n^2 - p}{2a_n}.$$

It is a Cauchy sequence, in fact

$$|a_{n+1} - a_n|_p \leq |a_n^2 - p|_p \leq p^{-n} \xrightarrow{n \to \infty} 0.$$

If it had a rational limit $x \in \mathbb{Q}$, then , by continuity, it should hold $x^2 = p$, then we get a contradiction.

Now it would naturally arise to ask whether it is possible, by extending the field and the absolute value, to obtain a complete field.

Definition 2.2.11. *Let K be a field and $v \in M_K$. A completion of K is a field $\hat{K}$ with $w \in M_{\hat{K}}$, and an embedding $i : K \hookrightarrow \hat{K}$, such that $w|v$, $\hat{K}$ is complete in respect to w and the following property holds:*
If L is another field with $w' \in M_L$, $w'|v$, then there exists a unique homomorphism:

$$\phi : \hat{K} \longrightarrow L$$

such that $\phi \circ i = \mathrm{id}_K$, preserving the absolute value, i.e. $w'(\phi(x)) = w(x)$, for all $x \in \hat{K}$.

It can be proven that it is always possible to find a completion and it is unique up to field isomorphism. It is also possible to consider the completion as a field extension, identifying K as a subfield of $\hat{K}$ through i. We usually denote the completion of K in respect to $v \in M_K$ as K_v.

Example 2.2.12. $\mathbb{R}$ is the completion of $\mathbb{Q}$ in respect to the standard absolute value. The completion of $\mathbb{Q}$ in respect to a p-adic absolute value can be described as :

$$\mathbb{Q}_p = \left\{ \sum_{n=n_0}^{\infty} a_n p^n : a_n, n_0 \in \mathbb{Z}, 0 \leq a_n < p \right\}.$$

To verify this equality, one must show that every series written in that form, called the **p-adic expansion** of $\alpha \in \mathbb{Q}_p$, converges in $\mathbb{Q}_p$ and that every $\alpha \in \mathbb{Q}_p$ has a unique p-adic expansion. Therefore, for $\alpha = \sum_{n=n_0}^{\infty} a_n p^n$ it must be $v_p(\alpha) = n_0$.

Theorem 2.2.13. *Let K be a number field, then there is exactly one place $v \in M_K$:*

1. *for each prime ideal $\mathfrak{p}$, when $v \in M_K^0$;*
2. *for each $\sigma : K \hookrightarrow \mathbb{R}$ real embedding;*
3. *for each $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$ pair of conjugate complex embeddings.*

This theorem allows us to completely characterize classes of equivalence of absolute values on a field K:

- to $\mathfrak{p} \subset \mathcal{O}_K$ corresponds $v_{\mathfrak{p}}(x)$, discrete additive valuation associated to $(\mathcal{O}_K)_{\mathfrak{p}}$, defined in I.1.2. ;
- to $\sigma : K \hookrightarrow \mathbb{R}$ corresponds $|x|_\sigma = |\sigma(x)|$;

- to $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$ corresponds $|x|_\sigma = |\sigma(x)| = |\bar{\sigma}(x)|$.

Where in the last two, we consider the standard absolute value for $\mathbb{R}$ and $\mathbb{C}$. Showing the correspondence between prime ideals and non-archimedean absolute values is rather involved; therefore, we shall omit its proof. Instead, we will illustrate how to establish the correspondence between archimedean absolute values and embeddings. Before seeing this, we first see a useful result.

Proposition 2.2.14.

Let L/K be a finite separable extension. If K is complete in respect to $v \in M_K$, this absolute value extends uniquely to $w \in M_L$ and we have the following equality:

$$|\alpha|_w^{[L:K]} = |\operatorname{Nm}_{L/K}(\alpha)|_v \tag{2.2.1}$$

for all $\alpha \in L$.

Note that this theorem implies that a non archimedean absolute value can only extend to a non archimedean absolute value, and the same holds for archimedean ones. Then we can reinterpret a characterization of the ring of integers, proposition 1.3.13, and the ring of S-integers , as follows

Corollary 2.2.15. *Let K be a number field, $\mathcal{O}_K$ its ring of integers and $M_K^\infty \subset S \subset M_K$, S finite set. Then:*

$$\mathcal{O}_K = \{x \in K : v(x) \geq 0, \text{for all } v \in M_K^0\}$$
$$\mathcal{O}_{K,S} = \{x \in K : v(x) \geq 0 \text{ for all } v \notin S\}$$

Note that, thanks to Theorem 2.2.13 , the number of archimedean absolute values corresponds to the number of embeddings , then it is finite for a number field.

Remark 2.2.16. If we let L/K be a finite separable extension , say $L = K[\alpha]$, and we consider $|\cdot|_v$ in K, an extension $|\cdot|_w$ in L (then $w|v$), we can complete K respect to v and L in respect to w and obtain L_w and K_v. By construction, L_w is an extension of K_v . More precisely $L_w = K_v[\alpha]$, since $K_v[\alpha]$ is complete (In respect to unique extension v) and contains L. If we take $f \in K[x]$ minimal polynomial for α, we can consider thanks to the natural inclusion $i : K \hookrightarrow K_v$, $f \in K_v[x]$. Then the minimal polynomial of α in $K_v[x]$ must divide f. We get

$$[L_w : K_v] \leq [L : K] < \infty$$

Thanks to this remark we can give a powerful definition:

Definition 2.2.17 (Local degree)**.** *Let $K/\mathbb{Q}$ be a finite extension, w, v places of, respectively, K and $\mathbb{Q}$, such that $w|v$. We define the* ***local degree at w*** *the following natural number:*

$$n_w := [K_w : \mathbb{Q}_v].$$

Remark 2.2.18. If $v|\infty$, then $\mathbb{Q}_\infty = \mathbb{R}$ and K_v is a finite complete extension of $\mathbb{R}$, then $K_v \cong \mathbb{R}$ or $K_v \cong \mathbb{C}$, then $n_w = 1$ or 2,respectively. If we consider $j : K \to K_v$ natural map and $i : K_v \to \mathbb{R}$ (or $\mathbb{C}$) topological isomorphism, then $|x|_v = |j(x)|_v = |i(j(x))|$. Notice that $\sigma := i \circ j : K \to \mathbb{R}$ (or $\mathbb{C}$) is an embedding. Conversely, two embeddings σ_1, σ_2 defines the same place in K if and only if they are real and equal or complex conjugates. This follows easily from the definition of equivalent places. In particular there are exactly $r_1 + r_2$ absolute values in M_K extending standard absolute value, where $r_1 = \#\{\sigma : K \hookrightarrow \mathbb{R} \text{ embedding}\}$ and $r_2 = \#\{\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}\}$ pair of conjugates embeddings$\}$. Therefore, we see that

$$\sum_{w|\infty} n_w = r_1 + 2r_2 = [K : \mathbb{Q}] \tag{2.2.2}$$

Actually this is a specific case of the formula (2.2.5) that we state in the next proposition. In addition to this one, in the next proposition we present other important properties that will be used to prove the product formula for K.

Proposition 2.2.19. *Let L/K be a finite separable field extension, $\alpha \in L, v \in M_K$, then:*

- *v extends to finitely many places w in L. Therefore:*

$$\mathrm{Nm}_{L/K}(\alpha) = \prod_{w \in M_L, w|v} \mathrm{Nm}_{L_w/K_v}(\alpha) \tag{2.2.3}$$

- *From the previous results it follows easily that:*

$$\prod_{w \in M_L, w|v} |\alpha|_w^{n_w} = |\,\mathrm{Nm}_{L/K}(\alpha)|_v \tag{2.2.4}$$

- *if $L/K/\mathbb{Q}$ is a finite separable extension, then*

$$\sum_{w \in M_L, w|v} n_w = [L : K] n_v \tag{2.2.5}$$

Proof. We don't prove (2.2.3), but using it and (2.2.1) we can prove (2.2.4) and (2.2.5): Since K_v is complete, $|\alpha|_w^{n_w} = |\,\mathrm{Nm}_{L_w/K_v}(\alpha)|_v$, then $\prod_{w|v} |\alpha|_w^{n_w} = \prod_{w|v} |\,\mathrm{Nm}_{L_w/K_v}(\alpha)|_v = |\,\mathrm{Nm}_{L/K}(\alpha)|_v$. Then (2.2.3) is true $\forall \alpha \in L$, in particular if $\alpha \in K^\times$ we have $\mathrm{Nm}_{L/K}(\alpha) = \alpha^{[L:K]}$ and $\prod_{w|v} |\alpha|_w^{n_w} = |\alpha|_v^{\sum n_w}$. Putting these 3 together we see that $|\alpha|_v^{[L:K]n_v} = |\alpha|_v^{\sum n_w}$. From here (2.2.5) follows. □

Now we are ready to state and prove the following theorem:

Theorem 2.2.20 (Product formula for K number field)**.** *Let K be a number field. Then, for all $\alpha \in K$, $\alpha \neq 0$, we have*

$$\prod_{w \in M_K} |\alpha|_w^{n_w} = 1. \tag{2.2.6}$$

Proof.

$$\prod_{w \in M_K} |\alpha|_w^{n_w} = \prod_{v \in M_{\mathbb{Q}}} \left(\prod_{w \in M_K, w|v} |\alpha|_w^{n_w} \right) \overset{(2.2.3)}{=} \prod_{v \in M_{\mathbb{Q}}} |\operatorname{Nm}_{L/K}(\alpha)|_v = 1$$

Where the last equality comes from the product formula for $\mathbb{Q}$, since, by definition, $\operatorname{Nm}_{L/K}(\alpha) \in \mathbb{Q}$. □

2.3 Heights

Now we are ready to define the concept of Height for any number field K. To do this we will use projective space. It is not necessary to do this but it will be needed later for define heights also on curves. We will see how the height over a number field K is defined via the absolute values on K, and we will derive many properties of the height from those of the absolute values. We will also introduce the definition of the absolute height, which makes it possible to measure the height of an algebraic number, thus removing the dependence of the height on the number field. It will be crucial to see that the set of elements whose height is bounded by a given constant is finite. This property is in fact at the heart of Roth's proof of his theorem.

Definition 2.3.1 (Height for $\mathbb{P}^n(K)$)**.** *Let K be a number field. For every $P \in \mathbb{P}^n(K), P = [x_0, \ldots, x_n]$ we set*

$$H_K(P) := \prod_{v \in M_K} \max(|x_0|_v, \ldots, |x_n|_v)^{n_v}$$

*We call this object the **Height of P relative to K**.*

Next we see that the height is well defined and some basic properties.

Proposition 2.3.2. *let K be a number field, $P \in \mathbb{P}^n(K)$, then the following properties are true:*

1. *$H_K(P)$ does not depends on the choice of coordinates for P.*

2. *for every* P, $H_K(P) \geq 1$.

3. *If* L/K *finite separable extension,*

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

Proof. 1) For $\lambda \in K^\times$,

$$\prod_{v \in M_K} \max_i (|\lambda x_i|_v)^{n_v} = \prod_{v \in M_K} |\lambda|_v^{n_v} \prod_{v \in M_K} \max_i (|x_i|_v)^{n_v}$$

Then 1 follows from the product formula (2.2.6), indeed $\lambda \in K^\times$ implies $\prod_{v \in M_K} |\lambda|_v^{n_v} = 1$.

2) It is trivial, because , since it can't be that every coordinates of P is 0, it is always possible to choose homogeneous coordinates for P such that one of the coordinates is 1. Then every factors defining the height of P is at least 1.

3)

$$\begin{aligned} H_L(P) &= \prod_{w \in M_L} \max_i (|x_i|_w)^{n_w} = \prod_{v \in M_K} \prod_{w \in M_K, w|v} \max_i (|x_i|_v)^{n_w} \\ &= \prod_{v \in M_K} \max_i (|x_i|_v)^{[L:K] n_v} = H_K(P)^{[L:K]}, \end{aligned}$$

where in the first equality we use only the definition, in the second we use an equivalent way of viewing the product, and we replace w with v since x_i is in K; then we use (2.2.3) and again the definition. □

Remark 2.3.3 (Height in $\mathbb{P}^n(\mathbb{Q})$)**.** The projective n-dimensional space over $\mathbb{Q}$ has a very good property: for every $P \in \mathbb{P}^n(\mathbb{Q})$, we can choose homogeneous coordinates for P, $x_0, \ldots, x_n$ such that $x_i \in \mathbb{Z}$ and $\gcd(x_i) = 1$. This is easy to see since from rational coordinates we can multiply them all to the least common denominator to turn them into integers and then divide by the greatest common divisor of those integers. With this choice, if $v \in M_{\mathbb{Q}}^0$, $|x_i|_v \leq 1$ and and it must hold for at least one index i, $|x_i|_v = 1$ (otherwise there will be a common factor for all the x_i-s), then $\max_i |x_i|_v = 1$. Hence, using the definition for $H_{\mathbb{Q}}$, we get

$$H_{\mathbb{Q}}(P) = \max(|x_0|_\infty, \ldots, |x_n|_\infty)$$

We can observe that for every constant $C > 0$, the set:

$$\{P \in \mathbb{P}^n(\mathbb{Q}) | H_{\mathbb{Q}}(P) \leq C\}$$

is finite. That's because every index x_i can assume only $2C + 1$ values, then the set has a maximum of $(2C + 1)^n$ elements. An important fact , more difficult to prove, is that this result is true also for K number field.

Now we are finally ready to define the height of a point in an algebraic closure of $\mathbb{Q}$, i.e. of overy algebraic number over $\mathbb{Q}$.

Definition 2.3.4. *For $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$, chosen a number field K such that $P \in \mathbb{P}^n(K)$ we set the **absolute height of P** as $H(P) := H_K(P)^{1/[K:\mathbb{Q}]}$. For $x \in \bar{\mathbb{Q}}$, $H(x) := H([x,1])$. Similarly for a field K, $H_K(x) := H_K([x,1])$.*

Remark 2.3.5.

- The absolute height is well defined thanks to propostion (2.3.2) point 3 and the tower law, indeed if $L/K/\mathbb{Q}$ separable finite extension:
$$H_L(P)^{1/[L:\mathbb{Q}]} = H_K(P)^{[L:K]/[L:\mathbb{Q}]} = H_K(P)^{1/[K:\mathbb{Q}]}.$$
- Our initial definition of the height for $\mathbb{Q}$ is coherent with this definition, indeed if $r = p/q$
$$H(r) = H_{\mathbb{Q}}([p/q,1]) = \max(|p|_\infty, |q|_\infty).$$

Example 2.3.6. Taking $\alpha = \sqrt[n]{k}, k \in \mathbb{Z}$, k square-free, we choose $K = \mathbb{Q}[\alpha], \alpha \in K$. Since k square-free, $x^n - k$ is irreducible in $\mathbb{Q}$, then it must be the minimal polynomial of α and $[K : \mathbb{Q}] = 1$. Then
$$H(\alpha) = H_K([\alpha,1]) = \prod_{v \in M_K} \max(1, |\alpha|_v)^{n_v}.$$
Note that $|\alpha|_v^n = |\sqrt[n]{k}|_v^n = |k|_v$ for the multiplicative property of absolute values, then $|\alpha|_v = |k|_v^{1/n}$ $\forall v \in M_K$. If $v \in M_K^0$, $v|p$ for some prime p; since $k \in \mathbb{Z}$, we have that $|k|_v = |k|_p \leq 1$, then $\forall v \in M_K^0$, $\max(1, |\alpha|_v) = 1$. If $v \in M_K^\infty$, $v|\infty$ and $|\alpha|_v = |k|^{1/n}$, then we have:
$$H(\alpha) = \prod_{v|\infty} (|k|^{1/n})^{n_v} = (|k|^{1/n})^{\sum_{v|\infty} n_v}$$
From (2.2.2) we know that the exponent is equal to $[K : \mathbb{Q}] = n$, then $H(\alpha) = |k|$.

As we said before, an important result we would like to have is that the set of elements of K with bounded height is a finite set. This result would allow us, given a problem in which one seeks solutions in $\bar{\mathbb{Q}}$ (or $\mathbb{P}^n(\bar{\mathbb{Q}})$, to search for an upper bound on the height of a solution; if such a bound is found, then the problem has a finite number of solutions.

Proposition 2.3.7. *Let $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$ and $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then*
$$H(P) = H(P^\sigma) \tag{2.3.1}$$

Proof. Let $K/\mathbb{Q}$ such that P is defined in $\mathbb{P}^n(K)$; then σ gives an isomorphism $\sigma : K \to K^\sigma$, also σ likewise identifies the absolute values of K and K^σ :

$$\sigma : M_K \xrightarrow{\cong} M_{K^\sigma} \ , \ v \to v^\sigma$$

Then, fixed $v \in M_K$ sigma gives also an isomorphism between K_v and $K^\sigma_{v^\sigma}$. So the local degrees satisfies $n_v = n_{v^\sigma}$. Also if $x \in K$, $|x^\sigma|_{v^\sigma} = |x|_v$. Putting all together:

$$H_{K^\sigma}(P^\sigma) = \prod_{w \in M_{K^\sigma}} \max_i |x_i^\sigma|_w^{n_w} = \prod_{v \in M_K} \max_i |x_i|_{v^\sigma}^{n_{v^\sigma}} = \prod_{v \in M_K} \max_i |x_i|_v^{n_v} = H_K(P)$$

Since $[K : \mathbb{Q}] = [K^\sigma : \mathbb{Q}]$, we have the desired result. □

Proposition 2.3.8. *Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_d = a_0 \prod_{i=1}^d (x - \alpha_j)$ polynomial in $\bar{\mathbb{Q}}[x]$, then:*

$$H([a_0, \ldots, a_d]) \leq 2^{d-1} \prod_{i=1}^d H(\alpha_j) \tag{2.3.2}$$

We do not give the proof of this fact, as it involves a lot of calculations.

Theorem 2.3.9. *Let $K/\mathbb{Q}$ finite separable extension, $C > 0$ a constant. Then*

$$\{P \in \mathbb{P}^n(K) : H_K(P) \leq C\} \tag{2.3.3}$$

is a finite set of points.

Proof. Let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(K)$. Easily we have:

$$H_K(P) = \prod_{v \in M_K} \max_i |x_i|_v^{n_v} \geq \max_i \prod_{v \in M_k} \max(|x_i|_v, 1)^{n_v} = \max_i H_K(x_i)$$

Thus it suffices to prove that the set $\{\alpha \in K : H_K(\alpha) \leq C\}$ is finite. In fact, if this were true, then $H_K(P) \leq C \implies H_K(x_i) \leq C$ for all i, but then we can choose every coordinate x_i in finitely many way and therefore there would be only finitely many points P. Suppose $\alpha \in K$ with $H_K(\alpha) \leq C$, we can then take the minimal polynomial for α, call it $f(x) = x^d + a_1x^{d-1} + \ldots + a_d$. Notice that $d \leq [K : \mathbb{Q}]$. If $\alpha = \alpha_1, \ldots, \alpha_d$ are the conjugates of α, for (2.3.2) we have:

$$H([1, a_1, \ldots, a_d]) \leq 2^{d-1} \prod_{i=1}^d H(\alpha_i) = 2^{d-1} H(\alpha)^d$$

Where the equality comes from (2.3.1). Now, since $a_i \in \mathbb{Q}$, $H([1, a_1, \ldots, a_d]) = H_\mathbb{Q}([1, a_1, \ldots, a_d])$ and $H(\alpha) = H_K(\alpha)^{1/[K:\mathbb{Q}]}$, we have:

$$H_\mathbb{Q}([1, a_0, \ldots, a_d]) \leq 2^{d-1} H_K(\alpha)^{d/[K:\mathbb{Q}]} \leq 2^d C^{d/[K:\mathbb{Q}]}$$

From what we have already seen in the example (2.3.3), this fact implies that there are finitely many possibilities for the a_i-s , and therefore for f. Since f has at most $[K : \mathbb{Q}]$ roots , from this finite set of polynomials , each of them contributes to our set with at most d elements, then our set must be finite. □

2.4 Roth's theorem

Finally, we have all the necessary tools to generalize the concept of approximation of algebraic numbers, over a field K rather than only over $\mathbb{Q}$, using rationals (which will now be elements of the field). With these tools it is possible to reinterpret Liouville's and Thue's theorems in a field K, and moreover we will state Roth's theorem. To do all this, we first give the following definition:

Definition 2.4.1 (Approximation exponent)**.** *Let K be a number field , $v \in M_K$ and $\tau : \mathbb{N} \to \mathbb{R}^+$. We say that K* ***has approximation exponent*** *τ (in respect to v) if the following property holds true:*
Let $\alpha \in \bar{K}$, $d = [K[\alpha] : K]$ and choose one of the extensions of v in $K[\alpha]$, which we still call v. Then, for all $C > 0$, the inequality:

$$|\alpha - x|_v \leq C H_K(x)^{-\tau(d)} \tag{2.4.1}$$

has only finitely many solutions.

Example 2.4.2. Liouville (2.1.3) says that $\mathbb{Q}$ has approximation exponent $\tau(d) = d$ in respect to the standard absolute value.
Thue (2.1.5) says that $\mathbb{Q}$ has approximation exponent $\tau(d) = d/2 + 1 + \varepsilon$ for all $\varepsilon > 0$ in respect to the standard absolute value.

Theorem 2.4.3 (**Roth's Theorem**)**.** *For every $\varepsilon > 0$, every number field K of degree d has approximation exponent:*

$$\tau(d) = 2 + \varepsilon.$$

The proof does not require very deep results, but the details required are lenghty. We only describe how the proof proceeds.

Sketch of the proof of Roth's Theorem. Fixed $\alpha \in \bar{K}$, through elementary estimates and the pigeonhole principle, one can construct a polynomial $P(X_1, \ldots, X_m) \in \mathcal{O}_K[X_1, \ldots, X_m]$ that vanishes of high order at $(\alpha, \ldots, \alpha)$ with controlled degree and

coefficients with controlled heights. Then we proceed by contradiction, supposing there are infinitely many different $x_i \in K$ such that inequality 2.4.1 with $\tau(d) = 2+\varepsilon$ holds. Using Taylor expansion, we can prove that $|P(x_1, \dots, x_m)|_v$ is fairy small. Then, one must prove a non vanishing result, namely Roth's Lemma. This result says that a polynomial that vanishes to $(x_1, \dots, x_m)$ such that the height of this element is fairly increasing, depending on m and the degree of the polynomial, then P cannot vanish to high order at $(x_1, \dots, x_m)$. This part is the most delicate of the proof. Indeed, Thue did not have this result at his disposal, but a weaker one, which led him to prove a weaker version of Roth's theorem. Once we have this results, making assumption on the rate of growth of the height of x_i, using Roth's Lemma, we can prove that there is a low order partial derivative such that, calculated at $(x_1, \dots, x_m)$, is different from 0. We call this element z and we can prove that $|z|_v$ is fairly small, from what we said earlier. On the other hand, using product formula, we can prove that $|z|_v \geq H_K(z)^{-1}$. Using another bound for $H_K(z)^{-1}$, we obtain a contradiction for $|z|_v$, which would be both too small and too large. □

Chapter 3

Introduction to Curves

The study of curves constitutes a natural point of contact between algebra, geometry, and number theory. Historically, curves arise as the zero sets of polynomials in two variables, but their importance goes far beyond this elementary viewpoint: they provide the natural setting for understanding deep geometric phenomena through purely algebraic tools. In this chapter we introduce the fundamental notions related to algebraic curves, with the aim of developing a rigorous language that allows us to describe their properties. The main purpose of this discussion is to prepare the ground for the introduction of the genus of a curve, a fundamental invariant. We will then study divisors and differentials associated with the curve, and the Riemann–Roch theorem, which will illustrate a relation between these objects and will allow us to define the genus.

3.1 Varieties

We briefly recall the notion of an algebraic variety, both in the affine and projective setting. This provides the basic geometric framework in which curves naturally arise and allows us to fix the language and notation that will be used throughout the chapter.
Given a field K and its algebraic closure $\bar{K}$, from each ideal $I \subset \bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$ we associate the set:

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

Definition 3.1.1. *$V \subset \mathbb{A}^n$ is an **algebraic set** if there exists $I \subset \bar{K}[X]$ such that $V = V_I$. In this case, such an ideal is called **ideal of V** and:*

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in \mathbb{A}^n\}$$

*V is said to be **defined over K** if $I(V)$ can be generated by polynomials in $K[X]$; in this case we write V/K and define $I(V/K) := I(V) \cap K[X]$.*

Definition 3.1.2. *Let $V \subset \mathbb{A}^n$ be an algebraic set with ideal $I(V)$. V is a **variety** if $I(V)$ is a prime ideal of $\bar{K}[X]$.*

Definition 3.1.3. *If V/K is a variety, we define **the set of K-rational points of V** as follows*

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

*If $\mathcal{O}_{K,S}$ ring of S integers for some finite $S \subset M_K$, we can similarly define **the set of S-integral points of** V :*

$$V(\mathcal{O}_{K,S}) := V \cap \mathbb{A}^n(\mathcal{O}_{K,S})$$

Notice that $\mathbb{A}^n$ is a variety, because $I(V) = (0)$ is a prime ideal.
In this thesis we will always consider variety in $\mathbb{A}^2$, usually defined over K, which ideal is generated by only one polynomial $f \in K[X]$ irreducible. In this case we will write:

$$V : f(x, y) = 0 \tag{a}$$

This is a notation meaning $V = \{(x, y) \in \bar{K} : f(x, y) = 0\}$. An interesting and very complicated problem concerning this objects is to determine the set of K-integral points $V(K)$.

Definition 3.1.4. *Let V/K be a variety. We define **affine coordinate ring** of V/K as:*

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

*We define also the **function field** of V/K its fraction field $K(V) := \mathrm{Frac}(K[V])$. Similarly are defined $\bar{K}[V]$ and $\bar{K}(V)$, replacing K with $\bar{K}$.*

Next we want to define a notion of dimension for a variety ; we notice that $\bar{K}(V)$ is an extension of $\bar{K}$ but it may not be algebraic, so we have to define the concept of "transcendence degree" for a trascendence field extension.

Definition 3.1.5. *Let L/K field extension. We say that $S = \{x_1, \ldots, x_n\} \subset L$ is **algebraically independent** over K, if*

$$\forall P \in K[X_1, \ldots, X_n] \backslash \{0\}, P(s_1, \ldots, s_n) \neq 0$$

*L/K is a **finite transcendental extension** if $\exists S = \{s_1, \ldots, s_n\} \subset L$ non empty algebraically independent such that L is an algebraic extension of $K(s_1, \ldots, s_n)$. In*

this case that n is unique and it is called the ***transcendental degree*** *of L/K. Notice that if S is empty, then $n = 0$ and L/K is an algebraic extension.*

Definition 3.1.6 (Dimension of a variety and Curve)**.** *Let V be a variety. We define its dimension as the transcendental degree of $\bar{K}(V)$ over $\bar{K}$. V is a* ***curve*** *if its dimension is equal to* 1*.*

Example 3.1.7. The dimension of $\mathbb{A}^n$ is n because $\bar{K}(\mathbb{A}^n) = \bar{K}(x_1, \ldots, x_n)$. Then if V variety defined by a non constant polynomial f, $V : f(x_1, \ldots, x_n) = 0$, then $\dim(V) = n - 1$.

Then the objects we are interested in are curves. We will usually denote curves by C.

Remark 3.1.8. Notice that we can give all these definitions replacing $\mathbb{A}^n(K)$ with $\mathbb{P}^n(K)$. Then $V \subset \mathbb{P}^n(K)$ makes sense when V is generated by homogeneous polynomials, in fact $f(P) = 0$ does not depend on the choice of homogeneous coordinates for P. In this case V is called **projective variety**. There is a very close connection between varieties and projective varieties. In fact, given a variety, one can uniquely associate a projective variety to it by "homogenizing" the polynomials in its ideal. This process is done like this: Let $f(x_1, \ldots, x_n)$ polynomial of degree d, we can homogenize it adding one variable obtaining :

$$f^*(x_1, \ldots, x_{n+1}) = x_{n+1}^d f\left(\frac{x_0}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right).$$

This remark leads us to give the following definition.

Definition 3.1.9. *Let $V \subset \mathbb{A}^n$ be a variety. We define the* ***projective closure*** *of V as $\bar{V} \subset \mathbb{P}^n$ by his ideal $I(\bar{V}) = \{f^*(X) : f \in I(V)\}$. Notice that to every $\bar{P} = [x_0, \ldots, x_{n+1}] \in \bar{V}$ with $x_{n+1} \neq 0$ corresponds a unique point in V , namely $P = (x_0/x_{n+1}, \ldots, x_n/x_{n+1})$. Points in $\bar{V}$ with $x_{n+1} = 0$ are called* ***points at infinity****.*

Usually, given a variety V is useful to consider its projective closure, because it may be easier to deal with homogeneous polynomials, for example to determine $V(K)$.

Example 3.1.10. Consider

$$C : x^2 + y^2 = p$$

where p is a prime, $p \not\equiv 1 \bmod (4)$. We want to determine $V(\mathbb{Q})$. If we consider $\bar{C} : x^2+y^2 = pz^2$; suppose $P \in \bar{C}(\mathbb{Q})$, it is possible to find homogeneous coordinates x, y, z such that $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$, then $x^2 \equiv -y^2 \bmod(p)$. Since $p \not\equiv 1 \bmod 4$, -1 is not a square $\bmod(p)$, then it must be $x \equiv y \equiv 0 \bmod (p)$. Then it must be , from the equation, that $3|z$, in contradiction with $\gcd(x, y, z) = 1$. Then $C(\mathbb{Q}) = \emptyset$.

Definition 3.1.11. *Let V/K be a variety, $V : f(x_1, \ldots, x_n) = 0$. $P \in V$ is a **singularity** for V if $\frac{\partial f}{\partial x_i}(P) = 0$ for all $i = 1, \ldots, n$. If V does not have singularities is said to be **smooth**.*

Definition 3.1.12. *Let C/K be a curve and $P \in C$ a smooth point. The Local ring of C at P is $K[X]_P = \{F \in K(C) : F(X) = f(x)/g(x)$ and $g(P) \neq 0\}$. $f \in K(C)$ is regular at P if $f \in K[C]_P$. Therefore $M_P := \{f \in K[C] : f(P) = 0\}$ is the maximal ideal of the local ring. For $d \in \mathbb{N}$, $M_P^d = \langle f_1 \ldots f_d : f_i \in M_P \rangle$. The valuation on this ring is given by:*

$$\begin{aligned} \mathrm{ord}_P : K[C]_P &\longrightarrow \mathbb{N} \cup \{\infty\} \\ f &\longmapsto \max(d \in \mathbb{Z} : f \in M_P^d). \end{aligned}$$

Since $K(C)$ is the fraction field of $K[C]$ we can extend the valuation at P to $K(C)$ in the following way:

Definition 3.1.13. *Let C/K be a curve and P a smooth point. We define the **order of f at P** as*

$$\begin{aligned} \mathrm{ord}_P : K(C) &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ F = f/g &\longmapsto \mathrm{ord}_P(f) - \mathrm{ord}_P(g) \end{aligned}$$

*We call a **uniformizer of C at P** any function $t \in K(C)$ with $\mathrm{ord}_P(t) = 1$, i.e. a generator for M_P. Also if $\mathrm{ord}_P(f) \geq 0$, f is said to be **regular at P**; if $\mathrm{ord}_P(f) > 0$, f has a **zero** at P; else $\mathrm{ord}_P(f) < 0$, f has a **pole** at P.*

Remark 3.1.14. Notice that if t, t' uniformizers at P, then they are generators for M_P, then $\exists u \in K[V]_P$ such that $t' = ut$. But $u \notin M_P$, otherwise $t' = ut \in M_P^2$ contradicts the fact that t' is a generator for M_P. Then $u \in K[V]_P \backslash M_P$, that it's the group units for $K[V]_P$, so u invertible.

Notice that the definition of M_P can be given also for varieties. Next we give a proposition that would be useful to calculate orders.

Proposition 3.1.15. *Let V/K be a variety and $P \in V$ a smooth point. Then:*

$$\dim_K M_P/M_P^2 = \dim V.$$

Example 3.1.16. Consider

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

and $P = (0,0) \in C$. P is a smooth point. Notice that M_P is surely generated by the polynomials $X, Y \in K(C)$, then $\mathrm{ord}_P(X)$ and $\mathrm{ord}_P(Y)$ are greater or equal to 1. Now M_P^2 is generated by X^2, Y^2, XY, but in $K(C)$ we have $X = Y^2 - X^2 \cdot X \in M_P^2$, then M_P/M_P^2 is generated by only Y. Observe that in M_P^2/M_P^3, $X \equiv Y^2 \neq 0 \mod M_P^3$. From what we observed follows that:

$$\mathrm{ord}_P(Y) = 1; \quad \mathrm{ord}_P(X) = 2.$$

Below we give the definition of morphism between varieties. We will use only morphisms between curves, but it is useful to see the most general definition possible. We divide it into several parts.

Definition 3.1.17. *Let $V_1, V_2 \subset \mathbb{P}^n(\bar{K})$ varieties defined over K. A **rational map** (defined over K) from V_1 to V_2 is a map of the form $\phi = [f_0, \ldots, f_n]$ with $f_i \in K(V_1)$, not necessarily defined at every point of V_1, but if f_i is regular at P for all i, then $\phi(P) \in V_2$. We say that ϕ is **regular** at P if there exists $g \in K(V_1)$ such that gf_i is regular at P and $[(gf_1)(P), \ldots, (gf_n)(P)] \in V_2$. In this case we define $\phi(P) := [(gf_0)(P), \ldots, (gf_n)(P)]$.*

Definition 3.1.18. *Let $V_1, V_2 \subset \mathbb{P}^n(\bar{K})$ and $\phi : V_1 \to V_2$ rational map. ϕ is a **morphism** if it is regular at every point of V_1. Then ϕ can be defined for all point $P \in V_1$. We say that ϕ is an **isomorphism** if there exists a morphism $\psi : V_2 \to V_1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are identities.*

Example 3.1.19. Let $V : X^2 + Y^2 = Z^2$, $V \subset \mathbb{P}^2(K)$. Consider

$$\phi : V \to \mathbb{P}^1; \quad \phi([X, Y, Z]) = [X + Z, Y].$$

We can see that ϕ is regular at every P, except possibly at points of V such that $X + Z = Y = 0$. The only point with this property is $[1, 0, -1]$. Take $g \in K(V), g = X - Z$. We have that:

$$[(X+Z)(X-Z), Y(X-Z)] = [X^2 - Z^2, Y(X-Z)] = [-Y^2, Y(X-Z)] = [-Y, X-Z].$$

where we used that $X^2 - Z^2 \equiv -Y^2$ in $K[V]$. Then $\phi([1, 0, -1]) = [0, 2] = [0, 1]$ and ϕ is a morphism. One can also prove that ϕ is an isomorphism.

3.2 Maps between curves

We could generalize and define a morphism between varieties of projective space of different dimensions. It's not hard to do, but since we are mainly interested in elliptic curves and we will see them as subset of $\mathbb{P}^2$, is not necessary. Let's note some properties of maps between curves.

Proposition 3.2.1. *Let C be a curve and V a variety. If C is smooth and $\phi : C \to V$ rational map, then ϕ is a morphism.*

Proof. Suppose $\phi = [f_0, \dots, f_n]$, with $f_i \in K(C)$ and $P \in C$. Choose $t \in K(C)$ uniformizer at P, then if $n = \min_i(\mathrm{ord}_P(f_i))$, then:

$$\mathrm{ord}_P(t^{-n} f_i) \geq 0, \quad \mathrm{ord}_P(t^{-n} f_j) = 0 \quad \text{for some j.}$$

Then $t^{-n} f_i$ is regular at P for all i and $t^{-n} f_j(P) \neq 0$. □

Proposition 3.2.2. *Let $\phi : C_1 \to C_2$ be a morphism between curves, then ϕ is constant or surjective.*

Proof. □

We will use this fact later.

Remark 3.2.3. Let C/K be a smooth curve and $f \in \bar{K}(C)$. Then we can define a rational map, that we also call f, in this way:

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

By proposition (3.2.1), f is a morphism. Following the proof , we can give f an explicit form $f(P) = [f(P), 1]$ if f is regular at P, otherwise $f(P) = [1 : 0]$. Conversely if we have a rational map, $\phi : C \to \mathbb{P}^1$, $\phi = [f, g]$ and $f, g \in \bar{K}(C)$, then or $g = 0$ then $\phi = [1 : 0]$ constant map, otherwise ϕ corresponds to the map defined by f/g . We can repeat this argument replacing K and $\bar{K}$, then there is a one to one correspondence between $K(C) \cup \{\infty\}$ and rational maps C to $\mathbb{P}^1$ defined over K.

Proposition 3.2.4. *Let C be a smooth curve, then $f \in \bar{K}(C)$, $f \neq 0$ has finitely many zeros and poles.*

Proof. Suppose $f \in \bar{K}[C]$ and $f \neq 0$ and f non constant (this case is trivial). We first prove that f has finitely many zeros. We can consider $\bar{K}[f] \subset \bar{K}[C]$. Since

$f \notin \bar{K}$ and $\bar{K}$ algebraically closed, then $\bar{K}[f]$ has trascendental degree equal to 1 and $\bar{K}[C]/\bar{K}[f]$ is a finite algebraic extension. If we consider B to be the integral closure of $\bar{K}[f]$ in $\bar{K}[C]$, then it is not hard to see that B is a Dedeking domain. Then we can consider the ideal (f) in B , using Theorem 1.3.11, we get

$$(f)B = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$$

where $n < \infty$ and each ideal $\mathfrak{p}_i$ corresponds to zeros of f. Then f must have finitely many zeros. Now, taking $F \in \bar{K}(C)$, $F = f/g$ where $f, g \in \bar{K}[C]$, zeros of F corresponds to the zeros of f and poles of F corresponds to zeros of g, then the conclusion follows from what was shown above. □

Notice that, given $C_1/K, C_2/K$ curves defined over K, and a non constant map $\phi : C_1 \to C_2$ we can induce an injection :

$$\phi^* : K(C_2) \to K(C_1), \quad \phi^*(f) := f \circ \phi.$$

Then, since ϕ^* is injective , $K(C_1)$ is an extension of the field $\phi^*(K(C_2))$ and we can easily see that ϕ^* fixes K.

Proposition 3.2.5. *Let $\phi : C_1 \to C_2$ be a non constant morphism of curves defined over K, then:*

$$[K(C_1) : \phi^*(K(C_2))] < \infty.$$

Proof. By definition $K(C_1)$ and $K(C_2)$ are finitely generated extension fields of transcendence degree 1 of K, then also $\phi^*(K(C_2))$ have this property. Then it must be that this extension if algebraic and finite. □

Definition 3.2.6. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves defined over K. We define its degree to be* $\deg \phi := [K(C_1) : \phi^*(K(C_2))]$. *If ϕ is constant, we set* $\deg \phi = 0$. *We say that ϕ is* ***separable*** *(or inseparable) if the extension $K(C_1)/\phi^*(K(C_2))$ have the correspondent property and define* $\deg_s(\phi)$ *and* $\deg_i(\phi)$ *to be the separable and inseparable degree of the extension.*

Remark 3.2.7. We don't see all details, but a morphism of degree 1 between smooth curves is an isomorphism. This can be proved using proposition (3.2.1) and the fact that given $i : K(C_2) \to K(C_1)$ injection fixing K , then there exists a unique $\phi : C_1 \to C_2$ morphism such that $\phi^* = i$. This is why we have called this function ϕ^*.

Definition 3.2.8 (Ramification index)**.** *Let $\phi : C_1 \to C_2$ be a non-constant morphism of smooth curves and $P \in C_1$. We define the **ramification index** of ϕ at P as :*

$$e_\phi(P) := \mathrm{ord}_P(\phi^*(t_{\phi(P)})) = \mathrm{ord}_P(t_{\phi(P)} \circ \phi),$$

*where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. Note that $e_\phi(P) \geq 1$. We say that ϕ ramifies at P if $e_\phi(P) > 1$. Therefore, ϕ is **unramified** if, for all $P \in C_1$, we have $e_\phi(P) = 1$.*

From remark (3.1.14), we see that the ramification index does not depend on the choice of the uniformizer, indeed if t, t' uniformizers at $\phi(P)$, $\exists u \in K(C_2)$ invertible such that $t' = ut$, then

$$\mathrm{ord}_P(\phi^*(t')) = \mathrm{ord}_P(\phi^*(u)\phi^*(t)) = \mathrm{ord}_p(\phi^*(u)) + \mathrm{ord}_P(\phi^*(t)) = \mathrm{ord}_P(\phi^*(t)),$$

where we used the fact that ϕ^* is an homomorphism of fields, then $\phi^*(u)$ must be invertible. This fact implies that $\mathrm{ord}_P(\phi^*(u)) = 0$.

Proposition 3.2.9. *Let $\phi : C_1 \to C_2$ be a non-constant map between smooth curves, then*

- *for all $Q \in C_2$, $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$;*
- *For all but finitely many $Q \in C_2$, $\#\phi^{-1}(Q) = \deg_s \phi$.*

Observe that this two properties implies that if ϕ separable map, then it has finitely many ramification points. In fact, in this case $\#\phi^{-1}(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$ implies $e_\phi(P) = 1$ for all but finitely many $Q \in C_2$, then all points $P \in \phi^{-1}(Q)$ are unramified.

Example 3.2.10. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, $\phi([X : Y]) = [X^n : Y^n]$ for some $n \in \mathbb{Z}$, $n \geq 2$. In affine coordinates, say $t = X/Y$, we can describe this map as $\phi(t) = t^n$. For $P = 0$, we can choose $t_{\phi(P)} = t$, then

$$e_\phi(P) = \mathrm{ord}_P(t^n) = n$$

We get the same result for $P = \infty$, considering $t_{\phi(P)} = s = 1/t$. For $P = a \neq 0, \infty$, we can choose $t_{\phi(a)} = t - a$ and see that

$$e_\phi(P) = 1.$$

We notice that what we have found is consistent with the last proposition; indeed for $P \neq 0, \infty$, we have $\#\phi^{-1}(P) = \deg \phi = n$, while for $P = 0$ or $P = \infty$, $\phi^{-1}(P)$ has only one point, but the first point of the last proposition is satisfied.

3.3 Divisors and differentials

Now let us give an introduction to divisors and differentials. Divisors allow us to encode algebraically the distribution of zeros and poles of rational functions, while differentials provide a tool to study finer properties of the curve, such as its fundamental invariants. These concepts will form the basis for the definition of genus and for the application of the Riemann–Roch theorem.

Definition 3.3.1. *Let C be a smooth curve, then we define* $\mathrm{Div}(C)$ *as a free abelian group generated by points of C. Then*

$$\mathrm{Div}(C) := \left\{ D = \sum_{P \in C} n_P(P) : n_P \in \mathbb{Z}, n_p = 0 \text{ for all but finitely many } P \in C \right\}$$

If $D \in \mathrm{Div}(C)$, then we define its degree as $\deg D := \sum_{P \in C_1} n_p \in \mathbb{Z}$. *We can also define :*

$$\begin{array}{rcl} \mathrm{div} : \bar{K}(C)^* & \longrightarrow & \mathrm{Div}(C) \\ f & \longmapsto & \sum_{P \in C} \mathrm{ord}_P(f)(P) \end{array}$$

Note that the map div is well defined thanks to proposition (3.2.4), and it is also an homomorphism of groups, because ord_P is an additive valuation. Then the following is true for all $f, g \in \bar{K}(C)$: $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$. Thanks to this property, we can define an equivalence relation $\sim$ on $\mathrm{Div}(C)$ as follows: if $D_1, D_2 \in \mathrm{Div}(C)$, $D_1 \sim D_2$ if $\exists f \in \bar{K}(C)$, such that $D_1 - D_2 = \mathrm{div}(f)$. If $D \sim 0$, we say that D is **principal**.

Definition 3.3.2. *Let C a smooth curve, then we define its* ***Picard group*** *(or divisor class group) as* $\mathrm{Pic}(C) := \mathrm{Div}(C)/\sim$.

Definition 3.3.3. *Given $\phi : C_1 \to C_2$ map between smooth curves, we can induce:*

$$\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1) \quad \phi((Q)) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$$

and extends by $\mathbb{Z}$-linearity to all divisors.

Notice that we have the same notation ϕ^* for two different functions , one between divisors and one between function fields. Then we give some useful properties of divisors:

Proposition 3.3.4. *Let $\phi : C_1 \to C_2$ be a map between smooth curves, then:*

a) $\deg(\phi^*(D)) = \deg(\phi)\deg(D)$*;*

b) $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$*;*

c) for all $f \in \bar{K}(C_1)^*$, $\deg(\mathrm{div}(f)) = 0$.

Proof. a) Since $\deg : \mathrm{Div}(C_2) \to \mathbb{Z}$ and ϕ^* are both $\mathbb{Z}$-linear, it suffices to prove this only for $D = (Q)$, for some point $Q \in C_2$. By definition:

$$\deg(\phi^*(Q)) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$$

where the last equality comes from proposition (3.2.9).
b) By linearity, it suffices to prove that $\mathrm{ord}_P(\phi^*(f)) = e_\phi(P)\,\mathrm{ord}_{\phi(P)}(f)$. Take a uniformizer $t_{\phi(P)}$ at $\phi(P)$, then we can suppose $f = u t_{\phi(P)}^m$, where $m = \mathrm{ord}_{\phi(P)}(f)$ and u invertible, then

$$\mathrm{ord}_P(\phi^*(f)) = \mathrm{ord}_P(\phi^*(u t_{\phi(P)}^m)) = m\,\mathrm{ord}_P(\phi^*(t_{\phi(P)}).$$

The last element is equal, by definitions, to $e_\phi(P)\,\mathrm{ord}_{\phi(P)}(f)$.
c) Recall that, if $f \in \bar{K}(C_1)^*$, we defined $f : C \to \mathbb{P}^1$. Identifying $\mathbb{P}^1 \cong \bar{K} \cup \{\infty\}$, so that $[0:1]$ corresponds to 0 and $[1:0]$ to ∞, we obatin directly from definitions:

$$\mathrm{div}(f) = \sum_{P \in C_1} \mathrm{ord}_P(f)(P) = \sum_{P \in f^{-1}(0)} e_f(P)(P) - \sum_{P \in f^{-1}(\infty)} e_f(P)(P) = f^*((0) - (\infty)).$$

Then we get $\deg(\mathrm{div(f)}) = \deg(f^*((0) - (\infty)) = \deg f(1-1) = 0$ using a). □

This proposition tells us that if $D \in \mathrm{Div}(C)$ principal divisor, $\deg(D) = \deg(\mathrm{div(f)}) = 0$, for some $f \in \bar{K}(C_1)$. Then we can define $\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(C) : \deg(D) = 0\}$ and notice that the set of principal divisor is a subgroup of $\mathrm{Div}^0(C)$. Then we can define $\mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/\sim$. The first two points tell us that ϕ^* sends divisors of degree 0 in divisors of degree 0 (a) and principal divisors to principal divisors, then ϕ^* induces a well defined map between $\mathrm{Pic}^0(C_2)$ to $\mathrm{Pic}^0(C_1)$. Next, we talk a bit about differentials:

Definition 3.3.5. *Let* C *be a smooth curve, the* ***space of differential forms*** *on* C*, is*

$$\Omega_C := \{df : f \in \bar{K}(C)\}$$

where we want the usual relations, for all $f, g \in \bar{K}(C)$*:*

- $d(f+g) = df + dg$*;*
- $d(fg) = df \cdot g + f \cdot dg$*;*

- $d\alpha = 0$ *for all* $\alpha \in \bar{K}$.

With this definition, we can prove that Ω_C is a $\bar{K}(C)$ vector space of dimension 1, generated by any uniformizer t. Then, for every $\omega \in \Omega_C$, chosen a uniformizer t, there must exists a unique $g \in \bar{K}(C)$, such that:

$$\omega = g \cdot dt.$$

We can also prove that, if $f \in \bar{K}(C)$ is regular at P, t uniformizer at P, then df/dt is regular at P. It is easy to define all these things also for functions in $\bar{K}(C)$.

Definition 3.3.6. *Let* $\omega \in \Omega_C$, $P \in C$ *and* t_P *uniformizer at* P, *then we can define* $\mathrm{ord}_P(\omega) := \mathrm{ord}_P(\omega/dt)$. *Also* $\mathrm{div}(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega/dt_P)(P) \in \mathrm{Div}(C)$. *For a divisor* $D \in \mathrm{Div}(C)$, *we say that* D *is* ***canonical*** *if there exists* $\omega \in \Omega_C$ *such that* $D = \mathrm{div}(\omega)$.

Observe that the first definition does not depend on the choice of the uniformizer: let t, t' be two uniformizers at P, then we have $\omega = g \cdot dt = g' \cdot dt'$:

$$\mathrm{ord}_P(\omega/dt') = \mathrm{ord}_P(\omega/dt) + \mathrm{ord}_P(dt/dt')$$

but $\mathrm{ord}_P(dt/dt') = 0$ because t, t' are regular at P, then dt/dt' and dt'/dt are both regular at P and this can happen only if $\mathrm{ord}_P(dt/dt') = 0$.

3.4 The genus of a curve

Now we are ready to define the genus of a curve. We will introduce the notion of ordering among divisors, and thanks to this we can construct vector spaces associated with each divisor. Finally, the Riemann–Roch theorem provides a formula relating the dimension of these vector spaces to the divisors that define them, showing how the dimension of a vector space associated with a canonical divisor does not depend on the divisor itself. This last invariant will be the definition of the genus.

Definition 3.4.1. *Let* $D_1, D_2 \in \mathrm{Div}(C)$. *If* $D_1 = \sum_{P \in C} n_P(P)$, *we say that* D_1 *is positive and write* $D_1 \geq 0$, *if* $n_P \geq 0$ *for all* $P \in C$. *Also* $D_1 \leq D_2$ *if* $D_2 - D_1 \geq 0$. *We define*

$$\mathcal{L}(D) := \{f \in \bar{K}(C)^* : \mathrm{div(f)} \geq \text{-D}\} \cup \{0\}.$$

This notation is useful to summarize informations about poles and zeros of a function f, for example: $f \in \mathcal{L}(n(P) - (Q))$ tells us that f has a pole of order at

most n in P and a zero at Q. Notice also that $\mathcal{L}(D)$ is a $\bar{K}$-vector space. This is easy to see, because $\mathrm{div}(f_1 + f_2) \geq \min(\mathrm{div}(f_1), \mathrm{div}(\mathrm{f}_2))$ and $\mathrm{div}(\lambda f_1) = \mathrm{div}(f_1)$ are true for all $f_1, f_2 \in \bar{K}(C)$ and $\lambda \in \bar{K}^*$.

Definition 3.4.2. *Let $D \in \mathrm{Div}(C)$, then $\ell(D) := \dim_{\bar{K}} \mathcal{L}(D)$.*

Remark 3.4.3. We want to prove that $\ell(D) < \infty$. It is easy to see that , if $f \in \mathcal{L}(D)\backslash\{0\}$, then, from proposition 3.3.4.c:

$$0 = \deg(\mathrm{div}(f)) \geq -\deg D.$$

Then, if $\deg D < 0$, $\mathcal{L}(D) = \{0\}$ and $\ell(D) = 0$. Observe also that $\mathcal{L}(0) = \bar{K}$ and $\ell(0) = 1$. This comes from the fact that $\mathrm{div}(f) \geq 0$ implies that f has no poles, but then f cannot have any zeros in order to respect $\deg(\mathrm{div}(f)) = 0$. This implies $f \in \bar{K}$.
Lastly, if $\deg D > 0$, we can prove that $\ell(D) \leq \deg D + 1$. First, suppose $D = n(P)$, for some point P and $n > 0$; then $\mathrm{div}(f) \geq -n(P)$ implies that $\mathrm{ord}_P(f) \geq -n$ and f regular at all other points. We know that $\ell(0) = 1$, then by induction, we can suppose $\ell(n(P)) \leq n+1$ and prove that $\ell((n+1)(P)) \leq n+2$. Suppose there exists $f, g \in \mathcal{L}((n+1)(P))/\mathcal{L}(n(P))$ linearly independent, then f, g have poles at P of order $-n-1$ and no other zeros. Then $\phi := f/g$ is such that $\mathrm{ord}_P\, \phi = 0$. If we take $\lambda = \phi(P)$, then $h := f - \lambda g$ is such that $\mathrm{ord}_P(h) > -n-1$ and $h \in \mathcal{L}(n(P))$, then $f = \lambda g$. This implies $\ell((n+1)(P)) \leq \ell(n(P)) + 1 \leq n+2$.

We are finally ready to state, but don't prove, the Riemann-Roch theorem.

Theorem 3.4.4 (Riemann-Roch theorem)**.** *Let C be a smooth curve and $K_C \in \mathrm{Div}(C)$ canonical divisor on C and $D \in \mathrm{Div}(C)$. Then there exists a unique $g(C) = g \in \mathbb{Z}$, $g \geq 0$, depending only on C, that we call the **genus of** C such that:*

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

Corollary 3.4.5. *Let C be a smooth curve and $K_C \in \mathrm{Div}(C)$ canonical divisor on C. Then*

a) $g = \ell(K_C)$;

b) $\deg K_C = 2g - 2$;

c) if $\deg D > 2g - 2$, *then :*

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

Proof. a) This comes directly from the Riemann-Roch theorem with $D = 0$ and the fact that $\ell(0) = 1$.
b) We use (a) and Riemann-Roch theorem with $D = K_C$ and we get that $\deg K_C = 2g - 2$.
c) Using b), we get that, if $\deg D > 2g - 2$, $\deg(K_C - D) < 0$, and from a previous remark , this implies $\ell(K_C - D) = 0$. Applying again Riemann-Roch theorem we finish the proof. □

Example 3.4.6 (Genus of $\mathbb{P}^1$)**.** We are gonna prove that the genus of $\mathbb{P}^1(K)$ is equal to 0. We can take $t \in K(\mathbb{P}^1)$ coordinate function, i.e. $t([X, Y] = X/Y$ and $t([1, 0]) = \infty$ (a bijection $\mathbb{P}^1(K) \cong K \cup \infty$). Now we can see that $\forall \alpha \in K, t - \alpha$ is a uniformizer at $P = [x, y]$ if $\alpha = x/y$, then $\mathrm{ord}_P(dt) = \mathrm{ord}_P(d(t - \alpha)) = 0$. Else $P = [1 : 0] = \infty$, then $\mathrm{ord}_P(dt) = \mathrm{ord}_P(-t^2 d(1/t)) = -2$, because $1/t$ uniformizer at ∞. Then:

$$\mathrm{div}(dt) = -2(\infty) \quad \deg(\mathrm{div}(dt)) = -2$$

Then, from the fact that if $\omega \in \Omega_C$, there exists $g \in K(C)$ such that $\omega = g \cdot dt$, we have $\mathrm{div}(\omega) = \mathrm{div(g)} + \mathrm{div}(dt)$, taking the degree:

$$\deg(\mathrm{div}(\omega)) = \deg(\mathrm{div}(\omega)) = -2$$

Using Corollary.3.4.5.b, we get $g(\mathbb{P}^1(K)) = 0$.

Then we can give a theorem that gives a relation between the genus of two curves if there is a non constant separable map linking them:

Theorem 3.4.7 (Hurwitz)**.** *Let $\phi : C_1 \to C_2$, be a non-constant separable map between smooth curves defined over K, with g_1, g_2 being, respectively, the genus of C_1 and C_2. If one of the following is true:*

- $\mathrm{char}(K) = 0$
- $\mathrm{char}(K) = p > 0$ *and p does not divide $e_\phi(P)$ for all $P \in C_1$*

We then have the following formula :

$$2g_1 - 2 = (\deg \phi)(2g_2 - 2) + \sum_{P \in C} (e_\phi(P) - 1).$$

Example 3.4.8 (Genus of an elliptic curve)**.** We want to use this theorem to determine the genus of a curve C defined as follows:

$$C : y^2 = f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3$$

where $f \in K[x]$ for some field K with $\text{char}(K) \neq 2$, and suppose $f(x)$ has distinct roots, i.e. $\gcd(f, f') = 1$. $P_0 = (x_0, y_0) \in C$ singularity for C if and only if

$$2y_0 = f'(x_0) = 0$$

But then (since $2 \neq 0$), $y_0 = 0$ and x_0 would be a double root of f, then C must be non singular.

Notice that there is only one point at infinity $O = [0, 1, 0]$, in fact homogenizing and put $z = 0$, it must be $x = 0$. Then we can define $\phi : C \to \mathbb{P}^1$, $\phi(x, y) = x$ and sending O to $[1, 0] = \infty \in \mathbb{P}^1$. Notice that ϕ is separable , then $\deg \phi = \#\phi^{-1}(x)$ for all but finitely many x. It is clear that for a generic $x_0 \in K$, $y^2 = f(x_0)$ has two solutions, then $\deg \phi = 2$. Also a point is of ramification if and only if $\phi^{-1}(x_0)$ has only one point, because $\sum_{P \in \phi^{-1}(x_0)} e_\phi(P) = 2$. In that case, x_0 is a root of f or $x_0 = \infty$. Then ϕ has exactly 4 ramification points with ramification index 2. Using Hurwitz's theorem 3.4.7 we get:

$$2g(C) - 2 = 2(2 \cdot 0 - 2) + 4 = 0 \implies g(C) = 1.$$

Chapter 4

Elliptic curves

Finally we can introduce Elliptic curves. We will begin by providing the definition of an elliptic curve as a non-singular curve of genus one equipped with a base point, and we will illustrate its representation via the Weierstrass equation. Next, we will introduce the group structure on elliptic curves, which allows us to define a law of addition between points, and we will discuss the main properties of isogenies, i.e. group morphisms between elliptic curves. We will then consider heights on elliptic curves, and finally, using Roth's theorem, we will show how these notions allow us to prove Siegel's theorem, which ensures that an elliptic curve defined over a number field has only a finite number of integral points.

4.1 Weierstrass equation

In this section, we see how every elliptic curve can be described by a Weierstrass equation. We then consider the inverse problem, that is, when a curve defined by a Weierstrass equation is an elliptic curve, introducing the discriminant and j-invariant.

Definition 4.1.1 (**Elliptic curve**). *An Elliptic curve is a pair (E, O), where E/K is a non singular curve of genus 1 and $O \in E$. There exists $x, y \in K(E)$, called such that the map $\phi : E \to \mathbb{P}^2(\bar{K})$, $\phi = [x, y, 1]$ gives an isomorphism between E/K and a curve $C \in \mathbb{P}^2$, given by a* ***Weierstrass equation****:*

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{4.1.1}$$

where $a_i \in K$ and $\phi(O) = [0, 1, 0]$.

We will consider an elliptic curve to be a curve given by a Weierstrass equation with base point $[0,1,0]$. However, we will often write it in its non-homogeneous form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1.2}$$

keeping in mind that $[0,1,0]$ is the only point at infinity. Now we need to focus on a problem, namely when a Weierstrass equation gives a singular curve or not, because we would like to consider only non singular curves. Before doing this, let's analyze a Weierstrass equation more closely.

Remark 4.1.2. Suppose $\mathrm{char}(\bar{K}) \neq 2,3$ and let E elliptic curve given by a Weierstrass equation of the form (4.1.2). Then the substitution

$$y \longrightarrow \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form:

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

where we have defined $b_2 = a_1 + 4a_4$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$.
Another substitution of the form:

$$(x,y) \longrightarrow \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

gives the simpler equation:

$$E : y^2 = x^3 - 27c_4x - 54c_6$$

where $c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. We can also define $b_8 = a_1a_6^2 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. This tell us that if we are in characteristic different than 2 and 3, we can find $A, B \in K$ such that our elliptic curve E/K has the form:

$$E : y^2 = x^3 + Ax + B \tag{4.1.3}$$

All these quantities we have defined along the way are useful for the next definition of a quantity related to the elliptic curve and its properties.

Definition 4.1.3. *Let E be an elliptic curve given by a Weierstrass equation (4.1.2), we define* ***the discriminant*** *of E the following:*

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

When $\Delta \neq 0$, we can also define the j- invariant $j := c_4^3/\Delta$.

This definition might seem like a tedious and useless computation, but in reality calculating this discriminant will allow us to determine immediately whether a curve is singular or not. Meanwhile, the j-invariant will be used to compare two curves, which will be isomorphic if and only if they have the same j-invariant. Moreover, Δ and j have a simpler and more compact form in the case of the simpler equation (4.1.3):

$$\Delta = -16(4A^3 + 27B^2), \quad j = -1728\frac{(4A)^3}{\Delta}$$

Remark 4.1.4. We may ask how Δ and j behave if we change coordinates of a Weierstrass equation, and also when a change of coordinate effectively gives us another Weierstrass equation (and fixes the point at infinity $[0 : 1 : 0]$. One can prove that the change of variables

$$x' = u^2x + r, \quad y' = u^3y + u^2sy + t \tag{4.1.4}$$

where $u, r, s, t \in \bar{K}, u \neq 0$ fixes $[0, 1, 0]$ and, calling Δ', j', respectively, the discriminant and the j-invariant of the new Weierstrass equation, $u^{12}\Delta' = \Delta$ and $c_4' = u^4c_4$. $\Delta \neq 0$ implies $\Delta' \neq 0$, so in that case $j' = j$. This requires a lot of calculations so we don't see the proof; an important thing is that actually only this type of change of coordinates preserves the Weierstrass form. If one have this result , then it's clear why the j-invariant is called like this.

Remark 4.1.5 (Singular points of E)**.** $P = (x, y)$ is a singular point for E if $P \in E$ and , if $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$, $\frac{\partial f}{\partial x}(x, y) = \frac{\partial f}{\partial y}(x, y) = 0$. It follows that there are $\alpha, \beta \in \bar{K}$ such that the Taylor expansion of $f(x, y)$ at P has the form:

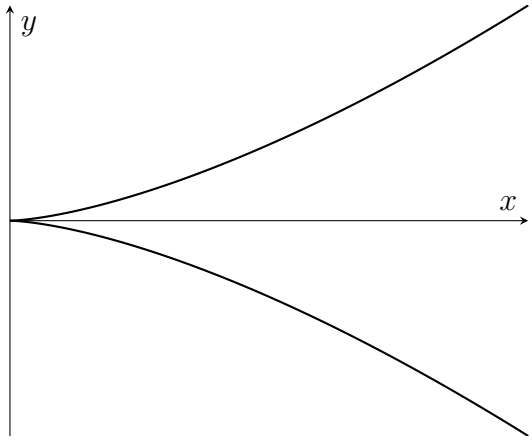
$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3$$

with $y - y_0 = \alpha(x - x_0)$ and $y - y_0 = \beta(x - x_0)$ tangent lines at P.

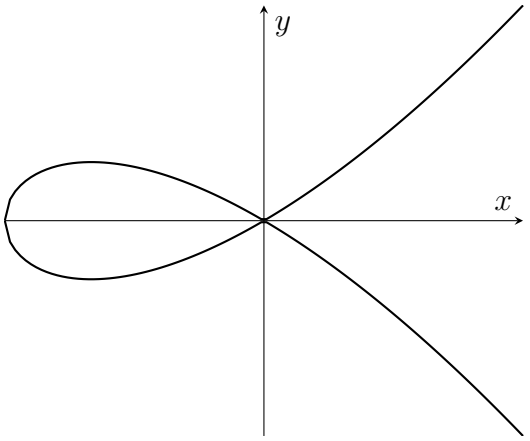
Definition 4.1.6. *Let E elliptic curve, $P \in E$ a singular point and $\alpha, \beta \in \bar{K}$ obtained as in (4.1.5). Then :*

- *P is a **node** if $\alpha \neq \beta$; in this case there exists two distinct tangent lines at P;*
- *P is a **cusp** if $\alpha = \beta$; in this case there is only one tangent line at P.*

The names "node" and "cusp" derive from their geometric visualization. Here I report an example:



$y^2 = x^3, P = (0,0)$ cusp



$y^2 = x^3 + x^2, P = (0,0)$ node

Proposition 4.1.7. *Let E/K elliptic curve with Weierstrass equation (4.1.2). Then*

1. *E is singular $\iff$ $\Delta = 0$;*
2. *E has a node $\iff$ $\Delta = 0$ and $c_4 \neq 0$;*
3. *E has a cusp $\iff$ $\Delta = 0$ and $c_4 = 0$.*

Proof. Firstly, we show that the point at infinity $O = [0,1,0]$ is never singular. If E has Weierstrass equation in homogeneous form:

$$E : F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

Then $\frac{\partial F}{\partial Z}(O) = 1 \neq 0$, then O isn't a singular point. Now suppose E with Weierstrass equation non homogeneous (4.1.2) singular at $P_0 = (x_0, y_0)$, then the substitution $x = x' + x_0$ and $y = y' + y_0$ leaves Δ and c_4 invariant (as we have seen in Remark.4.1.4), so without loss of generality we can suppose $P = (0,0)$. Then :

$$a_6 = f(0,0) = 0, \quad a_4 = \frac{\partial f}{\partial x}(0,0) = 0, \quad a_3 = \frac{\partial f}{\partial y}(0,0) = 0.$$

so E has equation of the form:

$$E : y^2 + a_1xy - x^3 - a_2x^2 = 0$$

Calculating the discriminant and c_4 ,we get $\Delta = 0$ and $c_4 = (a_1^2 + 4a_2)^2$. By definition, P is a node (respectively a cusp) if the quadratic form $y^2 + a_1xy - a_2x^2$ has distinct factors (respectively equal), which occurs if and only if its discriminant is different than 0 (respectively equal to 0), but the discriminant is $(a_1^2 + 4a_2)$. This proves the "if" part of 1), 2) and 3). It remains to prove that E non singular implies

$\Delta \neq 0$. To simplify the computation, we assume $\text{char}(\bar{K}) \neq 2$, then we can consider E with Weierstrass equation $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$. $P = (x_0, y_0)$ is singular for E if

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0$$

Since $2 \neq 0$, it must be $y_0 = 0$. Then $P = (x_0, 0)$ and x_0 is a double root of the cubic polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$; this occurs only if its discriminant, which is equal to 16Δ (from Remark.4.1.4), is 0. This completes the proof. □

Proposition 4.1.8. *Let $E/K, E'/K$ be elliptic curves with $j(E), j(E')$ their j-invariant. Then E and E' are isomorphic if and only if $j(E) = j(E')$.*

Proof. If E and E' are isomorphic, then there exists a change of coordinates of the Weierstrass equation for E that gives the equation for E', then from Remark(4.1.4) they have same j- invariant. Conversely, suppose $\text{char}(\bar{K}) \geq 5$, then there exists $A, B, A', B' \in K$ such that

$$E : y^2 = x^3 + Ax + B; \quad E' : y'^2 = x'^3 + A'x' + B.$$

Having the same j- invariant means that:

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}$$

From this we obtain:

$$A^3B'^2 = A'^3B^2.$$

If we find a change of coordinates $(x, y) \to (u^3x', u^2y'^2)$, $u \in \bar{K}$, such that the equation defining E becomes the equation of E' we finish. Consider three cases:

- $A = 0$, then $j(E) = j(E') = 0$ and $B \neq 0$ (the case $A = B = 0$ leads us to a curve of the form $y^2 = x^3$ which is singular, then not an elliptic curve). It must be that $A' = 0$ and $B' \neq 0$. In this case we have an isomorphism if $u = (B/B')^{1/6}$;

- $B = 0$, then $j(E) = j(E') = 1728$ and $A \neq 0$, that implies $B' = 0$ and $A' \neq 0$. We can take $u = (A/A')^{1/4}$;

- $AB \neq 0$, then we have $A'B' \neq 0$, since if one of them were 0, then both of them would be 0. We can take $u = (A/A')^{1/4} = (B/B')^{1/6}$.

□

Now we have an effectively computable method to determine whether a Weierstrass equation defines an elliptic curve — namely, compute the discriminant and check that it is nonzero — and a method to compare two Weierstrass equations to see whether they define isomorphic elliptic curve. Another important fact is that "there are many different elliptic curves"; that is, given $j_0 \in K$,one can find a curve with j-invariant equal to j_0. We do not show this formally (although it reduces to simple calculations), but the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

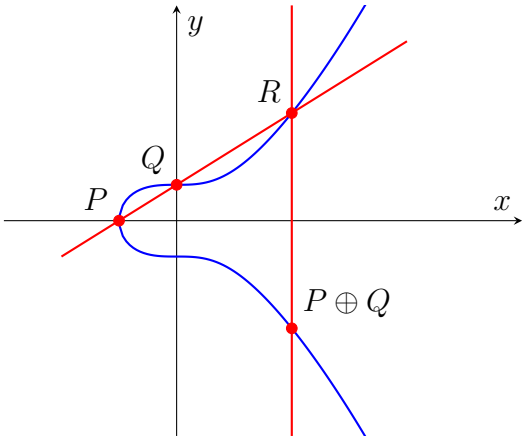
have $j-$invariant equals to j_0. Notice that the cases $j_0 = 0, 1728$ are special cases not covered from this equation (if $j_0 = 0$ its discriminant is 0, then it isn't an elliptic curve). Looking at the last proof , these cases correspond ,respectively, to curves $E : y^2 = x^3 + Ax + B$ with $A = 0$ and $B = 0$.

4.2 Group Law and Isogenies

In this chapter we will see how to define a group structure on an elliptic curve and how this structure can help us determine the K-rational points of the curve. We will also study isogenies, which are morphisms between elliptic curves. We will then examine the properties that distinguish elliptic curves from other curves and how these properties can be used to understand their arithmetic and geometric structure.

Definition 4.2.1 (**Group Law**). *Given E elliptic curve, with $O = [0, 1, 0]$ point at infinity. We can define a group law in this way. Let $P, Q \in E$ and take the line L through P and Q (if $P = Q$ we define L as the tangent line of the curve at P) ; L intersects E in another point, call it R. Then take the line L' through O and R . L' intersects our curve E at R, O and another point, that we call $P \oplus Q$.*

Note that this definition use the fact that we have an equation of degree 3, so the intersection between a line $L \subset \mathbb{P}^2$ and the curve consists of three points , not necessarily distinct. We give next a geometric visualization of how this operation works:



$E : y^2 = x^3 + 1$

Proposition 4.2.2. *Let E be an elliptic curve and $\oplus : E \times E \to E$ defined as above. So the following are true:*

a) If L line and $L \cap E$ consists of three points P, Q, R not necessarily distinct, then

$$(P \oplus Q) \oplus R = O$$

b) $P \oplus O = P$ for every $P \in E$

c) $P \oplus Q = Q \oplus P$, for every $Q, P \in E$

d) for $P \in E$, there exists $\ominus P \in E$ such that $P \oplus (\ominus P) = O$

e) Let $P, Q, R \in E$ then $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$

Proof. a) It is obvious by construction, because $P \oplus Q$ gives us a point that is on the line through R and O, then we sum that point to R and obtain O.
b) From definition, if $Q = O$, we have that L and L' are the same. Then L intersects E at P, O, R and L' at $R, O, P \oplus O$, then $P \oplus O = P$.
c) It is clear by definition.
d) From a), we can take the line though P and O intersects R then:

$$O = (P \oplus O) \oplus R = P \oplus R$$

Then $\ominus P = R$,
e) The geometric proof requires to verify a lot of different cases . One can also give explicit formulas for sum and verify by calculations. We skip this part.

□

Remark 4.2.3. This theorem tells us that $(E, \oplus)$ is an abelian group with identity element O. From now on, to easy notation, we will denote the operation $\oplus$ simply with $+$.
Having this structure of group on an elliptic curve helps us to study them , in particular to try to determine the set of K rational points $E(K)$. In fact , letting E with Weierstrass equation with non homogeneous coordinates (4.1.2) , $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$, one can give an explicit formula for calculate coordinates of $P + Q$ and $-Q$, namely:

$$\begin{aligned} -P_0 &= (x_0, -y_0 - a_1 x_0 - a_3); \\ P_1 + P_2 &= (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3) \end{aligned} \tag{4.2.1}$$

where x_3 is the first coordinate of $P + Q$ and λ and ν are functions depending on x_1, x_2, y_1, y_2 if $P \neq Q$ and also on a_i, with $i = 1, \ldots, 6$. If E/K , from this formulas ,even if we don't have an explicit one for $P + Q$, we can easily see that $E(K)$ is a subgroup of E, because starting from points with coordinates in K, we obtain coordinates of $P + Q$ with operations in K. We can see this also geometrically, in fact λ and ν are defined in such a way that $y = \lambda x + \nu$ is the line through P and Q.

Another important fact that we will use later is that the operations $+$ and $-$ defines morphisms. Next we give the definition of even function for an elliptic curve, that will be used later.

Definition 4.2.4. *Let E/K be an elliptic curve, $f \in K(E)$ is said to be an* ***even function*** *if $f(P) = f(-P)$, for all $P \in K(C)$*

Example 4.2.5. Let $f = x \in K(E)$ the x-coordinate function. x is an even function, because we have seen in equation 4.2.1 that P and $-P$ have the same x-coordinates.

Let's see another property of the x-coordinate and y-coordinate for an elliptic curve.

Proposition 4.2.6. *Let E elliptic curve, and consider $x, y \in K(E)$ respectively x and y coordinate, then*

a) O is the only pole for x, with $\mathrm{ord}_O(x) = -2$*;*

b) O is the only pole for y with $\mathrm{ord}_O(y) = -3$.

Proof. As we have seen , to the function $x \in K(E)$ is associated a morphism $\phi_x : E \to \mathbb{P}^1$, such that $\phi_x(P) = [x(P), 1]$, and $\phi_x(P) = [1 : 0] = \infty$ if P is a pole for

x. But consider E in its homogeneous form, $x = X/Z$, then P is a pole for x if P is a point at infinity, then it must be $P = O$, because O is the only point at infinity. Now $\deg \phi_x = [K(E) : K(\mathbb{P}^1)] = [K(x, y) : K(x)]$, but now , the weierstrass equation defining E, tells us that y is a root of a degree 2 polynomial in $K(x)$, then $\deg \phi_x = 2$. Then we can use the first point of Proposition 3.2.9 with $Q = O$ to get that

$$e_{\phi_x}(O) = 2 = -\operatorname{ord}_O(x)$$

This proves a). Using the same type of argument for y, we get $\deg \phi_y = 3$ and then $\operatorname{ord}_O(y) = -3$.

□

Now we define isogenies, that are particular map between elliptic curves.

Definition 4.2.7. *Let E_1, E_2 be elliptic curves . $\phi : E_1 \to E_2$ is an **isogeny** if ϕ is a morphism and $\phi(O) = O$. If ϕ non-constant , we say that E_1 and E_2 are **isogenous**.*

It follows from proposition (3.2.2) that $\phi(E_1) = \{O\}$ or $\phi(E_1) = E_2$. Next we see that an isogeny respects the group law; before doing that, let's see that $(\operatorname{Pic}(E), +)$, where "+" is the natural operation of summing two divisors (actually class of divisors), is isomorphic to $(E, \oplus)$ as groups.

Proposition 4.2.8. *Let E elliptic curve, then there exists a map $\psi : E \longrightarrow \operatorname{Pic}^0(E)$ bijection of sets.*

Proof. We can define this function as :

$$\begin{array}{rcl} \phi : E & \longrightarrow & \operatorname{Pic}^0(E) \\ P & \longmapsto & [(P) - (O)] \end{array} \tag{4.2.2}$$

where $[(P)-(O)]$ means the class of that divisor. Now we prove that ϕ is a bijection. It is an injection , because if $\psi(P) = \psi(Q)$, then $(P) \sim (Q)$, then $\exists f \in K(C)$ such that $\operatorname{div}(f) = (P) - (Q)$. But then $f \in \mathcal{L}((Q))$. From Riemann-Roch theorem, precisely Corollary (3.4.5.c), $\ell((Q)) = 1$, then f must be a constant and $f(P) = 0$ implies $f = 0$ and $P = Q$. To prove that it is surjective, we have to prove that $\forall D \in \operatorname{Div}^0(E)$ there exists a point $P \in E$ such that $D \sim (P) - (O)$. Reapplying Corollary (3.4.5.c) to $D + (O)$, that is a divisor of degree 1, we get:

$$\ell(D + (O)) = \dim_{\bar{K}} \mathcal{L}(D + (O)) = 1$$

We can choose $f \in \mathcal{L}(D + (O))$ non zero, then we know that :

$$\operatorname{div}(f) \geq -D - (O) \quad \deg(\operatorname{div}(f)) = 0$$

Then there exists $P \in E$ such that $\operatorname{div}(f) = -D - (O) + (P)$, which means that $D \sim (P) - (O)$. □

Proposition 4.2.9. *Let $\psi : E \longrightarrow \operatorname{Pic}^0(E)$ defined as in the proof of last proposition (4.2.2), then $\psi(P+Q) = \psi(P)+\psi(Q)$ for all $P, Q \in E$, in other words ψ is a group isomorphism.*

Proof. Fixed $P, Q \in E$, take, ,as in the definition of group law $L : f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$ line through P and Q and a third point R, $L' : f'(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ line through R, O and $P + Q$. Then, since the line $Z = 0$ intersects O with multiplicity 3, we have:

$$\operatorname{div}(f/Z) = (P) + (Q) + (R) - 3(O), \quad \operatorname{div}(f'/Z) = (R) + (P + Q) - 2(O)$$

Then:

$$\operatorname{div}(f'/f) = (P + Q) - (P) - (Q) + (O)$$

This means that $(P + Q) - (P) - (Q) + (O) \sim 0$; in terms of image through ψ:

$$\psi(P + Q) - \psi(P) - \psi(Q) = 0$$

□

Proposition 4.2.10. *Let $\phi : E_1 \to E_2$ be an isogeny, then if $P, Q \in E_1$*

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

Proof. If we take $\phi_* : \operatorname{Div}^0(E_1) \to \operatorname{Div}^0(E_2)$ defined by $(P) \to (\phi(P))$ and then extending by $\mathbb{Z}$-linearity, we can see that this map is well defined and sends principal divisors to principal divisors, then we can quotient and obtain a map $\phi_* : \operatorname{Pic}^0(E_1) \to \operatorname{Pic}^0(E_2)$ and this is an homomorphism (in respect to "+" for classes of divisors). By last proposition , there exists $\psi_i : E_i \to \operatorname{Pic}^0(E_i)$ group isomorphisms for $i = 1, 2$, then $\phi = \psi_2^{-1} \circ \phi_* \circ \psi_1$, in other words ϕ is a composition of homomorphisms. □

From this proposition follows the fact that an isomorphism of elliptic curves E_1, E_2 (an injective isogeny) gives a group isomorphism between $E_1(K)$ and $E_2(K)$. Now that our curve has a structure of group we may ask if there are points with finite or infinite order, then we give next definition:

Definition 4.2.11. *For $P \in E$ and $m \in \mathbb{Z}$, we define the point $[m]P$ as :*

- *if $m = 0$, $[0]P := O$*
- *if $m > 0$, $[m]P := P + P + \ldots + P$, m times*
- *if $m < 0$, $[m]P := -P - P - \ldots - P$, $|m|$ times*

*Notice that $[m] : E \to E$ is a morphism and also an isogeny (O is clearly sent in itself). One can prove that $\forall m \neq 0$ the map $[m]$ is nonconstant, then it is surjective. So we can also define the m-**torsion group** as $E[m] := \ker([m]) = \{P \in E : [m]P = O\}$ and the torsion group as the set of all elements of finite order:*

$$E_{tors} := \bigcup_{m \in \mathbb{Z}} E[m].$$

If E is defined over K, then $E_{tors}(K)$ is the set of points of finite order in $E(K)$.

Next we want to prove that $E[m]$ is a finite group .

Proposition 4.2.12. *Let $\phi : E_1 \to E_2$ be a non-zero isogeny. Then $\ker \phi = \phi^{-1}(O)$ is a finite group of E_1.*

Proof. It is a subgroup thanks to proposition (4.2.10) and it is finite because, from proposition (3.2.9) :

$$\# \ker \phi = \#\phi^{-1}(O) \leq \sum_{P \in \phi^{-1}(O)} e_{\phi(P)} = \deg \phi$$

□

In particular, from this proposition follows that $E[m] = \ker[m]$ is a finite group of order at most $\deg[m]$. We don't see the details, but we can characterize $E[m]$ for all $m \in \mathbb{Z}\backslash\{0\}$. This can be done by proving that $[m]$ is separable and that $\deg[m] = m^2$ and from this deduce that $\#E[m] = m^2$. Moreover if $\mathrm{char}(\bar{K}) = 0$ or $p = \mathrm{char}(K) > 0$ and $p \nmid m$, $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$, otherwise $E[p^e] = \{O\}$ or $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1, 2, \ldots$. It is not the main goal of this thesis, but this results helps to determine $E_{tors}(K)$, because $E(K)[m]$ is a subgroup of $E[m]$; then knowing the structure of $E[m]$ reduces possibilities for $E(K)[m]$. Next, we give a lemma that would be useful later.

Lemma 4.2.13. *Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \geq 2$. Then, for $R \in E$, there are exactly m^2 solutions to*

$$[m]P = R$$

for $P \in E$.

Proof. Notice that, from what we said early, $[m] : E \to E$ has $\#\ker[m] = \#E[m] = m^2$. Since

$$\tau_{-R} : E \to E \quad \tau(P) = P - R$$

is an isomorphism, then $\tau_{-R} \circ [m]$ has a kernel of exactly m^2 elements. But $P \in \ker(\tau_R \circ [m])$ if and only if

$$[m]P = R.$$

□

4.3 Height for elliptic curves

In this section, we will focus on the concept of height on elliptic curves. We will begin by illustrating how to define the height of a point by choosing an element in the function field of the curve, starting from the absolute height already defined over $\bar{\mathbb{Q}}$. Next, we will see how to relate the group structure to heights, connecting the height of the sum of two points to the heights of the individual points. These properties will be central in the proof of Siegel's theorem.

Definition 4.3.1. *In $\mathbb{P}^n(\bar{\mathbb{Q}})$, we can define the **absolute logarithmic height** as*

$$\begin{array}{rcl} h : \mathbb{P}^n(\bar{\mathbb{Q}}) & \longrightarrow & \mathbb{R} \\ P & \longmapsto & \log(H(P)) \end{array}$$

where H is the absolute height, already defined in Definition 2.3.4.

This new definition will be useful to have an "addition behavior" and not a multiplicative one, so it will simplify a little bit. Therefore it doesn't change much the properties of H. Notice that, from Proposition 2.3.2.b, we have $H(P) \geq 1$ and then $h(P) \geq 0$ for all $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$. Now, we want to extend the concept of height to an elliptic curve. Recalling the fact that every element f of the function field $\bar{K}(C)$ determines a surjective morphism, also called f, such that $f : E \to \mathbb{P}^1$. We can use this to give the next definition:

Definition 4.3.2. *Let E be an elliptic curve, $f \in \bar{K}(E)$ non-constant function. We define **the height on E** (relative to f) as*

$$h_f(P) := h(f(P)).$$

Observe that, fixed $f \in \bar{K}(E)$, if P is a pole or a zero for f, then $h_f(P) = 0$. That is because $f(P) = [0, 1]$, if P is a zero ,and $f(P) = [1, 0]$ if P is a pole for f, but

$H([1,0]) = H([0,1]) = H_{\mathbb{Q}}([1,0]) = \max(|0|,|1|) = 1$, then $h_f(P) = 0$. Next we see that the finiteness result of Proposition 2.3.9 holds true also for the height on elliptic curve.

Proposition 4.3.3. *Let E/K be an elliptic curve , $f \in \bar{K}(E)$ non-constant , and $C > 0$ a real constant, then*

$$\{P \in K(E) : h_f(P) \leq C\}$$

is a finite set.

Proof. We know that f maps point of $E(K)$ to point of $\mathbb{P}^1(K)$, and an element of $\mathbb{P}^1(K)$ can only have finitely many preimages, otherwise it would be possible to define a nonzero $g \in K(C)$ with infinitely many zeros. We can see that f maps the set $\{P \in K(E) : h_f(P) \leq C\}$ in

$$\{Q \in \mathbb{P}^1(K) : H(Q) \leq e^C\} \tag{4.3.1}$$

The condition $H(Q) \leq e^C$, since $Q \in \mathbb{P}^1(K)$, is equivalent to

$$H_K(Q) \leq e^{[K:\mathbb{Q}]C}.$$

Then we know that the set in (4.3.1) is finite, from Proposition 2.3.9. Since for every point of this set there are only finitely many preimages, we get what we wanted to prove. □

We recall the standard definition of $O(1)$ for real- valued functions:
If f, g real valued functions, then $f = g + O(1)$ if there exists $C_1, C_2 \in \mathbb{R}$ such that for all P:

$$C_1 \leq f(P) - g(P) \leq C_2$$

Then we give a property for heights that would be useful later to prove Siegel's theorem. We do not prove it because the proof is very long and full of explicit calculations.

Proposition 4.3.4. *Let E/K be an elliptic curve, $f \in K(E)$ even function, i.e. $f(P) = f(-P)$ for all $P \in E(K)$. Then, for all $P, Q \in E(\bar{K})$, we have:*

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1),$$

where $O(1)$ depend only on E and f and not on the points P, Q.

Corollary 4.3.5. *Let E/K be an elliptic curve, $f \in K(E)$ even function.*

a) Let $Q \in E(\bar{K})$, then for all $P \in E(\bar{K})$

$$h_f(P+Q) \leq 2h_f(P) + O(1)$$

where $O(1)$ depends only on E, f and Q.

b) Let $m \in \mathbb{Z}$, then

$$h_f([m]P) = m^2 h_f(P) + O(1)$$

for all $P \in E(\bar{K})$, where $O(1)$ depends only on E, f and m.

Proof. a) From the previos proposition, since $h_f(P-Q) \geq 0$ we get that a) is true. b) Notice that for $m = 0, 1$, the result is trivial. Then we can use induction to finish the proof. Suppose the formula holds true for $m \in \mathbb{Z}$ and $m-1$, we prove it for $m+1$. We use previous proposition with $[m]P$ and P, then we get:

$$\begin{aligned} h_f([m+1]P) &= -h_f([m-1]P) + 2h_f([m]P) + 2h_f(P) + O(1) \\ &= -(m-1)^2 h_f(P) + 2h_f(P)(m^2+1) + O(1) \\ &= (m+1)^2 h_f(P) + O(1). \end{aligned}$$

□

4.4 Mordell-Weil Theorem

In this section, we will present a sketch of the proof of the Mordell–Weil theorem in its strong form, starting from the weak form. We will show how the properties of heights on the rational points of an elliptic curve, together with the descent procedure, allow one to pass from the weak result to the strong form. We first stating its weak form.

Theorem 4.4.1 (Weak Mordell-Weil Theorem)**.** *Let K be a number field, and E/K an elliptic curve defined over K, then for all $m \in \mathbb{Z}$, $m \geq 2$ we have that:*

$$E(K)/mE(K)$$

is a finite group.

Only through the tools defined in these theses it is difficult to prove this theorem, which requires precise properties and a function called the "Kummer pairing." If one wishes to see the proof, one can read chapter VIII.1 of the book "The Arithmetic of Elliptic Curves" of Joseph H. Silverman [1]. Then we can state its stronger form.

Theorem 4.4.2 (Mordell-Weil Theorem)**.** *Let E/K be an elliptic curve defined over K number field. Then $E(K)$ is finitely generated.*

Since $E(K)$ is abelian and finitely generated, by the classification theorem of these groups, we have

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

with $r \in \mathbb{Z}$, $r \geq 0$, called the **rank of an elliptic curve**.
Now we state a key theorem, which holds for any abelian group and is the key to the proof of the Mordell-Weil Theorem.

Theorem 4.4.3 (Descent procedure)**.** *Let A an abelian group, and suppose there exists a function $h : A \to \mathbb{R}$ with the following properties:*

a) Let $Q \in A$, then there exists a constant C_1 depending only on A, Q such that:

$$h(P + Q) \leq 2h(P) + C_1$$

for all $P \in A$

b) There exists $m \in \mathbb{Z}$,$m \geq 2$ and a constant C_2 depending only on A, such that:

$$h(mP) \leq m^2 h(P) - C_2$$

for all $P \in A$.

c) For any constant $C > 0$, the set

$$\{P \in A : h(P) \leq C\}$$

is a finite set.

d) for the same integer m of b), suppose A/mA is a finite group. If we have all these properties, then A is finitely generated.

This theorem is not very hard to prove, but we don't see its proof here. Then we see how the Mordell-Weil theorem can be proved using all the tools we have.

Proof (of Mordell-Weil Theorem 4.4.2). Let $f \in K(E)$ be a non-constant even function, for example $f = x$, where x is the first coordinate function. Now let'see that the height function $h_f : E(K) \to \mathbb{R}$ satisfies all the required properties to apply the descent procedure theorem 4.4.3.
Properties a) and b), for $m = 2$, are exactly a) and b) of the corollary 4.3.5 applying the definition of $O(1)$. c) is exactly the proposition 4.3.3, while d) is the Weak Mordell-Weil theorem 4.4.1 applied for $m = 2$. Then we can apply descent procedure theorem and conclude that $E(K)$ is finitely generated. □

Chapter 5

Diophantine Approximation on Curves

In this chapter, we will finally see how the methods of Diophantine approximation and its results, in particular Roth's theorem, can be reinterpreted on elliptic curves. Starting from the fundamental definition of distance on curves, we will illustrate how to combine these notions with the properties of the group of points of an elliptic curve to obtain finiteness results. In particular, we will show how these techniques allow us to prove Siegel's theorem, which states that the number of S-integral solutions on an elliptic curve defined over a number field is finite, thus directly linking Diophantine approximation with classical arithmetic problems on curves.

5.1 Distances on curves

Firstly, we must introduce the notion of the distance between two points on a curve, defined in terms of the image of one point under a uniformizer at the other. Then we will consider certain useful limits in the v-adic topology, which will allow us to understand how a morphism changes the distance between two points and how to reinterpret Roth's theorem in this setting. Note that everything we discuss in this section holds for all curves, not just elliptic ones. We begin with a lemma.

Lemma 5.1.1. *Let C/K be a smooth curve defined over K, with genus g, and let $e \in \mathbb{Z}$, $e \geq g+1$. For every $Q \in C$, there exists a function $t_Q \in K(C)$ such that*

- *Q is a zero for t_Q with $\mathrm{ord}_Q(t_Q) \geq e$;*
- *Q is the only zero for t_Q.*

Proof. From Riemann-Roch theorem 3.4.4, then since $e(Q)$ is a divisor of degree e, fixing K_C a canonical divisor, we have:

$$\ell(e(Q)) = e + 1 - g + \ell(K_C - D) \geq 2$$

Then there must exists a non constant $f \in \mathcal{L}(e(Q))$, but this means that f has a pole at Q of order at least e and no other poles. Take $t_Q := 1/f$ finishes the proof. □

Now we can use this lemma to define a distance function , depending on a fixed absolute value in K, on a curve.

Definition 5.1.2. *Let C/K be a smooth curve, $v \in M_K$ and a point $Q \in C(K_v)$ and choose $t_Q \in K(C)$ as in the previous lemma. Then we can define the* ***v-adic distance from P to t_Q*** *, for all point $P \in C(K_v)$ as*

$$d_v(P, t_Q) := \min\left(|t_Q(P)|_v^{1/e}, 1\right).$$

Where if P is a pole at t_Q, we set $|t_Q(P)| = \infty$ to have $d_v(P, t_Q) = 1$. Also, for $P \in C(K_v)$, we say that P ***approaches Q in the v-adic topology*** *and write $P \underset{v}{\to} Q$, if $d_v(P, Q) \to 0$.*

Remark 5.1.3. For our purposes, we will write $d_v(P, Q)$ to mean $d_v(P, t_Q)$, where we choose some t_Q. Actually, if we fix a point P, the value of $d_v(P, Q)$ depend on the choice of the function t_Q. Since we will use d_v , fixed a point Q and see how d_v behave where we take points that approach to Q, this will not be a problem for the next theorem.

Proposition 5.1.4. *Let $Q \in C(K_v)$ and $F \in K_v(C)$ that vanishes at Q, then the limit:*

$$\lim_{P \underset{v}{\to} Q} \frac{\log |F(P)|_v}{\log d_v(P, Q)} = \mathrm{ord}_Q(F)$$

then the limit does not depend on the choice of t_Q used to define d_v.

Proof. Choose a function t_Q to define $d_v(P, Q)$ and define $e := \mathrm{ord}_Q(t_Q) \geq 1$, $f = \mathrm{ord}_Q(F) \geq 1$. We can take $\phi := F^e/t_Q^f$ and this function has $\mathrm{ord}_Q(\phi) = ef - ef = 0$. Since ϕ doesn't have poles, because if $P \neq Q$ pole, it would be a zero for t_Q, but this isn't possible for its definition. Then $|\phi(P)|_v < \infty$ as P approaches Q. We can also suppose , since P approaches Q that $d_v(P, t_Q) < 1$. We get

$$\lim_{P \underset{v}{\to} Q} \frac{\log |F(P)|_v}{\log d_v(P, Q)} = \lim_{P \underset{v}{\to} Q} \frac{\log |\phi(P)|_v^{1/e} + \log |t_Q(P)|_v^{f/e}}{\log |t_Q(P)|_v^{1/e}} = f + \lim_{P \underset{v}{\to} Q} \frac{\log |\phi(P)|_v}{\log |t_Q(P)|_v} = f$$

□

Now we see a property of the distance functions:

Lemma 5.1.5. *Let C/K be a smooth curve and suppose $f \in K(C)$ such that*

$$\operatorname{div}(f) = n_1(Q_1) + \ldots + n_r(Q_r).$$

Replacing K with an extension such that $Q_i \in K(C)$ and let $v \in M_K$, we have

$$\log \min(|f(P)|_v, 1) = \sum_{i=1}^{r} n_i d_v(P_i, Q) + O(1)$$

for all $P \in C(K_v)$. Here $O(1)$ depends only on f

Proof. We have the expression of $\operatorname{div}(f)$ that tells us that Q_i-s are the only zeros for f of order n_i. Then we can suppose

$$f = \alpha \cdot \prod_{i=1}^{r} t_{Q_i}^{n_i} \cdot u$$

where $\alpha \in K_v$ and t_{Q_i} uniformizers at Q_i, and $u \in C(K_v)$ invertible. Then it must be that $|u(P)|_v = 1$ for all $P \in K_v(C)$. Then , doing some computation, we get

$$\log \min(|f(P)|_v, 1) = \sum_{i=1}^{r} n_i d_v(P, Q_i) + O(1).$$

□

Next we see how maps between curves change the distance between points:

Proposition 5.1.6. *Let $\phi : C_1 \to C_2$ be a non-constant map defined over K and v an absolute value for K. Let $Q \in C_1(K_v)$ and $e_\phi(Q)$ its ramification index. Then*

$$\lim_{P \underset{v}{\to} Q} \frac{\log d_v(\phi(P), \phi(Q))}{\log d_v(P, Q)} = e_\phi(Q)$$

Proof. Let $t_Q \in K_v(C_1)$ function to define $d_v(P, Q)$ and $t_{\phi(Q)} \in K_v(C_2)$ to define $d_v(\phi(P), \phi(Q))$, respectively with order $e_1, e_2 \geq 1$ at Q. From the definition of ramification index:

$$\operatorname{ord}_Q(t_{\phi(Q)} \circ \phi) = e_\phi(Q) \operatorname{ord}_{\phi(Q)} t_{\phi(Q)} = e_\phi(Q) e_2.$$

Similarly to the previous proposition, we can take

$$f := \frac{(t_{\phi(Q)} \circ \phi)^{e_1}}{t_Q^{e_\phi(Q) e_2}} \in K_v(C_1).$$

This is a function of order zero at Q, then $|f(P)|_v < \infty$ as P approaches Q. We finally get

$$\lim_{\substack{P \to Q \\ v}} \frac{\log d_v(\phi(P), \phi(Q))}{\log(d_v(P,Q))} = \lim_{\substack{P \to Q \\ v}} e_\phi(Q) + \frac{\log |f(P)|_v}{\log |t_Q(P)|_v^{1/e_1}} = e_\phi(Q).$$

□

In the next proposition we can reinterpret Roth's theorem in terms of distance function, a result that will allow us to transfer this statement into the setting of functions between curves and height functions, and which will be essential in the proof of Siegel's Theorem.

Proposition 5.1.7. *Let C/K be a curve defined over K, $v \in M_K$,$f \in K(C)$ non constant function and $Q \in C(K)$. Then*

$$\liminf_{\substack{P \to Q \\ v}} \frac{\log d_v(P,Q)}{\log H_K(f(P))} \geq -2.$$

Proof. Noticing that $H_K((1/f)(P)) = H_K(f(P))$, we can replace f with $1/f$ in order to have Q not a pole for f. Then the function $f - f(Q) \in K(C)$ certainly has a zero at Q; call $e \geq 1$ its order at Q. Then for Proposition 5.1.4, we have:

$$\liminf_{\substack{P \to Q \\ v}} \frac{\log |f(P) - f(Q)|_v}{\log d_v(P,Q)} = e$$

Next, we use this fact into our limit:

$$\liminf_{\substack{P \to Q \\ v}} \frac{\log d_v(P,Q)}{\log H_K(f(P))} = \frac{1}{e} \liminf_{\substack{P \to Q \\ v}} \frac{\log |f(P) - f(Q)|_v}{\log H_K(f(P))} =$$
$$= \frac{1}{e} \liminf_{\substack{P \to Q \\ v}} \left(\frac{\log(H_K(f(P))^\tau |f(P) - f(Q)|_v)}{\log H_K(f(P))} - \tau \right)$$

We can take $\tau = 2 + \varepsilon$, for any $\varepsilon > 0$, then from Roth's theorem 2.4.3, we know that:

$$H_K(f(P))^\tau |f(P) - f(Q)|_v \geq 1$$

for almost all $P \in K(C)$. Using this inequality into our limit we get

$$\liminf_{\substack{P \to Q \\ v}} \frac{\log d_v(P,Q)}{\log H_K(f(P))} \geq -\frac{\tau}{e} \geq -(2 + \varepsilon).$$

Here we used $e \geq 1$. Since the inequality holds for all $\varepsilon > 0$, taking the limit as $\varepsilon \to 0$, we get the desired result. □

Remark 5.1.8. We can see the limit in the previous theorem in another way. Notice that, chosen $f \in K(E)$,

$$h_f(P) = h(f(P)) = \log H(f(P)) = \frac{1}{[K:\mathbb{Q}]} \log H_K(f(P)).$$

If we suppose $P \in E(K)$, the previous limit can be written as:

$$\liminf_{P \underset{v}{\to} Q} \frac{\log d_v(P,Q)}{h_f(P)} \geq -2[K:\mathbb{Q}].$$

5.2 Siegel's theorem and consequences

We are finally ready to state and prove Siegel's theorem. This theorem then tells us that as a point on the curve becomes "large" relative to the chosen height function, its distance to any fixed point becomes negligible compared to that height. Next, we will examine two consequences of Siegel's theorem. The first, which was largely anticipated earlier in the thesis, concerns the finiteness of S-integer points on a curve, while the second reinterprets this result in the case of rational points, showing that if one considers an infinite sequence of rational points on an elliptic curve and looks at their x-coordinates, then the numerator and denominator of x will tend to have the same number of digits.

Theorem 5.2.1 (**Siegel's Theorem**). *Let E/K be an elliptic curve, $v \in M_K$, suppose that $\#E(K) = \infty$, fix $Q \in E(K)$ and $f \in K(E)$ non-constant even function. Then,*

$$\lim_{\substack{P \in E(K) \\ h_f(P) \to \infty}} \frac{\log d_v(P,Q)}{h_f(P)} = 0.$$

Proof. Let's choose a sequence of points $P_i \in E(K)$ such that:

$$\lim_{i \to \infty} \frac{\log d_v(P_i,Q)}{h_f(P_i)} = L = \liminf_{\substack{P \in E(K) \\ h_f(P) \to \infty}} \frac{\log d_v(P,Q)}{h_f(P)}$$

Since $d_v(P_i,Q) \leq 1$ and $h_f(P_i) \geq 0$ for all P_i, it must be $L \leq 0$. Then it suffices to prove that $L \geq 0$. Notice also that, if it is not true that $P_i \underset{v}{\to} Q$, the thesis is trivial, because in that case $d_v(P_i,Q)$ is bounded away from 0 , that implies that $\log d_v(P_i,Q)$ is bounded away from infinity. This means that L must be 0. So we can suppose $P_i \underset{v}{\to} Q$. Take $m \in \mathbb{Z}$, $m \geq 2$, by the weak Mordell-Weil Theorem 4.4.1, we have that $E(K)/mE(K)$ is finite. By the pigeon principle, there are infinitely many P_i-s in one of the classes of $E(K)/mE(K)$. By replacing $\{P_i\}$ with a subsequence,

which does not change the limit, we can assume $[P_i] = [R]$, where $R \in E(K)$, in other words

$$P_i = [m]P_i' + R$$

where $P_i' \in E(K)$, for all $i \in \mathbb{N}$. Now , since we have $P_i \underset{v}{\to} Q$, it must be that $[m]P_i' \underset{v}{\to} Q - R$. This implies that the sequence P_i' approaches v-adically at least one of the m^2 solutions Q' to $[m]Q' = Q - R$ (using Lemma 4.2.13). Again, by replacing $\{P_i'\}$ by a subsequence, we can assume

$$P_i' \underset{v}{\to} Q', \quad Q = [m]Q' + R.$$

Define $\phi : E \to E$ as $\phi(P) = [m]P + R$, since $[m]$ is non constant, also ϕ is. Then we can apply Proposition 5.1.6, we get:

$$\lim_{i\to\infty} \frac{\log d_v(P_i, Q)}{\log d_v(P_i', Q')} = e_\phi(Q') := e \geq 1$$

Let's relate the height of P_i and P_i', using Proposition 4.3.5 a) and b):

$$m^2 h_f(P_i') = h_f([m]P_i') + O(1) = h_f(P_i - R) + O(1) \leq 2h_f(P_i) + O(1)$$

Notice also that

$$h_f(P_i') = h_f(P_i - R) \geq \frac{1}{2}h_f(P_i) + O(1).$$

Again by using Proposition 4.3.5.a. Since as $i \to \infty$, $h_f(P_i) \to \infty$, it must be that also $h_f(P_i') \xrightarrow{i\to\infty} \infty$. Now, using the last three facts, we get:

$$L = \lim_{i\to\infty} \frac{\log d_v(P_i, Q)}{h_f(P_i)} \geq \lim_{i\to\infty} \frac{e \log d_v(P_i', Q')}{\frac{1}{2}m^2 h_f(P_i') + O(1)} = \frac{2e}{m^2} \lim_{i\to\infty} \frac{\log d_v(P_i', Q')}{h_f(P_i')}$$

Where we inverted the inequality due to the fact that the term "$\log d_v$" are negative. Now we know that $P_i' \underset{v}{\to} Q'$ and $P_i' \in E(K)$, then we can use the result of Diophantine approximation, Theorem 5.1.7, precisely, we use what we saw in Remark 5.1.8:

$$\lim_{i\to\infty} \frac{\log d_v(P_i', Q')}{h_f(P_i')} \geq -2[K : \mathbb{Q}]$$

Finally, we get

$$L \geq \frac{-4e[K : \mathbb{Q}]}{m^2}.$$

Since we took m as an arbitrary integer, then $L \geq 0$, which finishes the proof.

□

We proved this theorem only for even function, but it can be proved for every function $f \in K(E)$. Thanks to this theorem, various finiteness results for solutions to different problems can be shown; we focus on one in particular, namely the following:

Corollary 5.2.2. *Let E/K be an elliptic curve, $S \subset M_K$ a finite set containing all archimedean absolute values, so $M_K^\infty \subset S \subset M_K$ and let R_S be the ring of S-integers. Then*

$$\{P \in E(K) : x(P) \in R_S\}$$

is a finite set.

Proof. By contradiction, suppose there is a sequence $\{P_i\}_{i\in\mathbb{N}}$ of distinct points, all points with $x(P_i) \in R_S$. By definition, we have:

$$h_x(P_i) = \frac{1}{[K:\mathbb{Q}]} \log H_K(x(P_i)) = \frac{1}{[K:\mathbb{Q}]} \sum_{v\in S} \log(\max(1, |x(P_i)|_v^{n_v}))$$

where we take the sum only for $v \in S$, because if $v \notin S$ we have $|x(P_i)|_v \leq 1$ and then the part of the sum for $v \notin S$ is equal to 0. Since S is finite, we can find a $\bar{v} \in S$ such that $\log(\max(1, |x(P_i)|_{\bar{v}}^{n_{\bar{v}}}))$ maximized among all $v \in S$ for infinitely many i. Then we can take a subsequence, call it again $\{P_i\}_{i\in\mathbb{N}}$, such that:

$$h_x(P_i) \leq \#S \log(\max(1, |x(P_i)|_{\bar{v}}))$$

where we used that $n_{\bar{v}} \leq [K:\mathbb{Q}]$ (see Remark 2.2.16). Notice that it must be that, since P_i are all distinct, Proposition 4.3.3 implies that $|x(P_i)|_{\bar{v}} \xrightarrow{i\to\infty} \infty$. We know from Proposition 4.2.6, that $1/x$ is a function with only zero O of order 2, then we can see that, by the definition of $\bar{v}$-adic distance:

$$d_{\bar{v}}(P_i, O) = \min\left(|x(P_i)|_{\bar{v}}^{-1/2}, 1\right) \xrightarrow{i\to\infty} 0.$$

Then , for i sufficiently large:

$$\frac{-\log(d_{\bar{v}}(P_i, O))}{h_x(P_i)} \geq \frac{1}{2\#S}$$

but this contradicts Siegel's theorem 5.2.1 since the first term must tend to 0 as $i \to \infty$. □

From this corollary, it easily follows that all the points with S-integral coordinates are finite. this finiteness result is striking because, in general, the number of points on a curve with coordinates in a given field K can be infinite, but if we restrict to S-integral points, they are always finite in number. Note that, having used Roth's theorem, this result is also ineffective: we only know that the S-integral points of an elliptic curve are finite, but we cannot give an estimate of how many there are.

Notice also that this result slightly improved what we had in Corollary 2.1.7: taking $K = \mathbb{Q}$ and a weierstrass equation:

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

with $a_i \in \mathbb{Q}$, then there are finitely many solutions $(x, y) \in \mathbb{Z}^2$ (taking $S = \{\infty\}$). This result says also that if we allow $x, y \in \mathbb{Z}[1/p_1, \dots, 1/p_r]$, where p_i finitely distinct primes, then there are finitely many solutions. Now we remark how we can restate Siegel's theorem 5.2.1 with $K = \mathbb{Q}$.

Corollary 5.2.3. *Let $E/\mathbb{Q}$ be an elliptic curve with x, y Weierstrass coordinates for E and suppose $\#E(\mathbb{Q}) = \infty$. Suppose $\{P_i\}_{i\in\mathbb{N}} \in E(\mathbb{Q})$ in order of non decreasing height, for the height h_x. If $x(P_i) = a_i/b_i$, $a_i, b_i \in \mathbb{Z}$, we have*

$$\lim_{i\to\infty} \frac{\log |a_i|_\infty}{\log |b_i|_\infty} = 1.$$

Proof. Let $v = \infty$ and assume $\{P_i\}_{i\in\mathbb{N}}$ as in the hypotheses; then from the definitions we have

$$\log d_v(P_i, O) = \log \min\left(|1/x(P_i)|^{\frac{1}{2}}, 1\right) = \tfrac{1}{2} \log \min\left(\left|\tfrac{b_i}{a_i}\right|, 1\right);$$
$$h_x(P_i) = h(a_i/b_i) = \log \max(|a_i|, |b_i|).$$

where we used that O is the only pole for x of order 2. Next, using Siegel's Theorem with $K = \mathbb{Q}$, $Q = O$, $S = \{\infty\}$, we get:

$$2 \lim_{i\to\infty} \frac{\log d_v(P_i, O)}{h_x(P_i)} = \lim_{i\to\infty} \frac{\min(\log(|b_i/a_i|, 0)}{\log(\max(|a_i|, |b_i|))} = 0$$

Then we can use Lemma 5.1.5, suppose that Q_1 and Q_2 are the two zeros for x (note that the case $Q_1 = Q_2$ is allowed), and we get:

$$\log \min(|x(P)|_v, 1) = d_v(P, Q_1) + d_v(P, Q_2) + O(1)$$

for all $P \in E(\mathbb{Q})$. Then we obtain:

$$\lim_{i\to\infty} \frac{\min(\log |a_i/b_i|, 0)}{\log(\max(|a_i|, |b_i|))} = \lim_{i\to\infty} \frac{\log \min(|x(P_i)|, 1)}{h_x(P_i)} =$$
$$= \lim_{i\to\infty} \frac{d_v(P_i, Q_1) + d_v(P_i, Q_2) + O(1)}{h_x(P_i)} = 0.$$

Where in the last inequality we used Siegel's Theorem 5.2.1 and the fact that $O(1)$ doesn't depend on P_i. Putting together the two limits we wrote, we prove the thesis. □

Bibliography

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[2] Marc Hindry , J.H. Silverman, *Diophantine Geometry: An Introduction* Graduate Texts in Mathematics, vol. 201, Springer, New York, 2000.

[3] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1997.

[4] James S. Milne, *Algebraic Number Theory*, lecture notes, J.S. Milne, 2020, available online at https://www.jmilne.org/math/CourseNotes/ANT.pdf.

[5] Lawrence Guth, *Introduction to Thue's Theorem in Diophantine Approximation*, lecture notes, MIT OpenCourseWare, The polynomial method, 2012, available online at https://ocw.mit.edu/courses/18-s997-the-polynomial-method-fall-2012/pages/lecture-notes/.

[6] Jan Hendrik Evertse, *Approximation of algebraic numbers by rationals*, lecture notes, Universiteit Leiden, available online at https://pub.math.leidenuniv.nl/~evertsejh/dio19-6.pdf.