Dept. of Mathematics and Applied Mathematics,
University of Crete

Mordell-Weil Theorem

for elliptic curves defined over number fields

Alexandros G. Galanakis

Supervisor:
Jannis A. Antoniadis

Heraklion, March 2017

To the people who always support my choices,
Giorgos and Marianthi,
my parents.

Contents

Preface

We find it appropriate to start with the statement that all of the work presented henceforth is not a result of research or innovative approach to the theorem of Mordell and Weil or the elliptic curves over the rationals. This master thesis is more a detailed survey of one proof of the Mordell-Weil theorem and a brief description of the main results of elliptic curves over the rationals. The main chapters are two.

In the first chapter we formulate and show the Mordell-Weil theorem for elliptic curves defined over any number field. The proof consists of two basic steps. The first one is the proof of the weak version of Mordell-Weil theorem for the special case $m = 2$, which can be found in [**20**]. The second step is the definition and the thorough study of heights. For these, we mainly used [**21**] and [**18**]. Finally, the proof of the Mordell-Weil theorem is based again in [**20**].

The second chapter of this master thesis is focused on the study of elliptic curves over $\mathbb{Q}$. This chapter has also two parts. The first one is the statement of the basic results regarding the torsion points and the complete proof of the Lutz-Nagell theorem. This part is follows the approach of [**9**]. The next part is about the rank of an elliptic curve over the rationals. The proofs of the results here are beyond the scope of this master thesis. Except for the elements of cohomology theory in which [**18**] was used, the rest of the chapter is based on personal notes taken in various lectures.

There are also two appendices. We choose to write an appendix for absolute values and valuations in number fields, since they are extensively used in the first chapter, particularly in defining and examining the properties of heights. This appendix is based on [**8**], [**12**] and [**18**]. The second appendix is about the canonical height, and it is also based on [**18**]. We also use [**15**]. The first chapter is focused on the proof of Mordell-Weil theorem, for which we do not need the Néron-Tate height, but it is used for the formulation of the strong version of Birch and Swinnerton-Dyer conjecture. Therefore, it is impossible to avoid the study of the Néron-Tate height.

As we already mentioned the content of this thesis is the complete proof of a significant result due to the work of two of the leading mathematicians of the previous century. Our purpose is to present proof using "elementary" notions, in order to arouse the interest, not only of the expert, but also of the inexperienced reader. We tried to do this to the second chapter, too, but at some point it is inevitable to avoid the heavy machinery. However, we hope that anyone will enjoy reading this master thesis!

Acknowledgments

Personally, I have to express my deepest thanks to my supervisor, prof. Jiannis A. Antoniadis, who helped me all the way to the completion of this thesis, and my master studies in general. I have to note that, except for the lectures I gave in order to present in detail the content of master thesis to my colleagues Anthi Zervou and Emmanouil Doulgerakis (and I have to thank them for their patience!), prof. Antoniadis gave us various lectures about the mathematics regarding my master thesis. His support and his guidance were crucial not only during the writing of this thesis, but also since I first met him. I feel grateful for the cooperation with prof. Antoniadis.

Master's thesis examination committee:

- prof. Jannis A. Antoniadis (supervisor),
- prof. Alexandros Kouvidakis, and
- prof. Nikolaos G. Tzanakis.

Alexandros G. Galanakis,
Heraklion, March 2017.

Introduction

A natural question that arises is why the Mordell-Weil theorem is important. Apparently, it provides us with a very useful information about the structure of the group of rational points of an elliptic curve, but is there any deeper reason, that makes the Mordell-Weil theorem worth-studying?

*Louis Joel. Mordell (*1888-1972*)*

The answer to that question is simple enough, if we think of an elliptic curve as a geometric object defined by a diophantine equation. One of the goals of number theory, even from ancient times, is the study of diophantine equations, and the determination of their integral or rational solutions, the so called diophantine problems. The geometric analogous of that, is the finding of integral or rational points of the curve that a diophantine equation defines. So, the general problem that we are interested in, is the following:

Given any curve, are we able to describe the set of the rational points on it,
or even better, to determine it explicitly?

The formulation of this general problem is rather imprecise, because the term "curve" has not been specified. Historically, the first curves that were studied, were defined over $\mathbb{Q}$. For simplicity, we stick to the case of smooth curves. Given any smooth curve C, the problem is to determine the set $C(\mathbb{Q})$ of the rational points on C. It turns out that we may consider the projective model of the curve, since it differs only in a finite set of points, i.e. the singularities and the point at infinity. Of course, there is always the possibility for C not to have any rational points, i.e. $C(\mathbb{Q}) = \varnothing$. If otherwise, using the classification of curves according to their genus, we obtain the following brief solution to our problem.

- If C is curve of genus 0, then the set $C(\bar{\mathbb{Q}})$ is isomorphic to the projective line $\mathbb{P}^1(\bar{\mathbb{Q}})$. In other words, we may give a parameterization of $C(\bar{\mathbb{Q}})$ in terms of one-variable rational functions.
- If C is a curve of genus 1, then it is an elliptic curve. Mordell (1922) proved that in this case the set $C(\mathbb{Q})$ is a finitely generated abelian group.
- Finally, if C is a curve of genus ≥ 2, then the set $C(\mathbb{Q})$ is finite, which is a result of great importance due to Faltings.

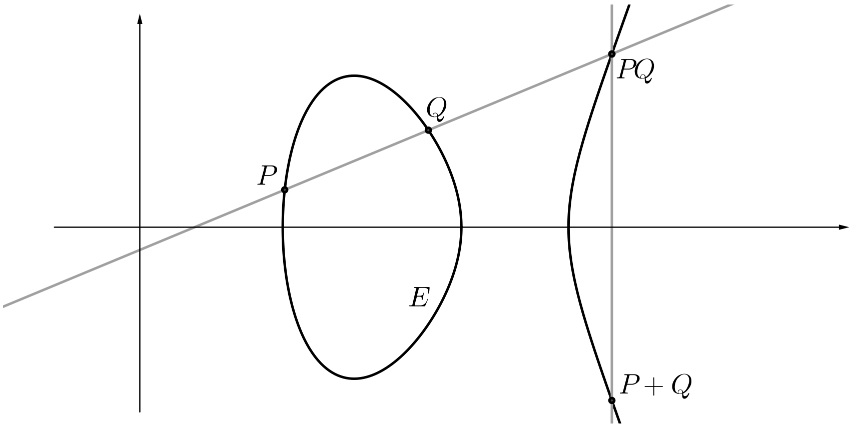
*André Weil (*1906-1998*)*

Weil (1929) extended the result of Mordell for elliptic curves defined over arbitrary number field.

Strictly speaking, an elliptic curve E defined over a number field K is a nonsingular projective algebraic curve of genus 1, with at least one K-rational point. The elliptic curve E is defined by

$$E|_K : Y^2 = X^3 + \alpha X + \beta,$$

with $\alpha, \beta \in K$. The interesting is that we are able to define the operation of addition on E, as it seems in the following figure.



It turns out that $(E(\bar{K}), +)$ is an abelian group, and so is $(E(K), +)$. The theorem of Mordell and Weil states that the group $(E(K), +)$ is finitely generated.

CHAPTER 1

Mordell-Weil Theorem for Elliptic Curves over Number Fields

This chapter is focused on the formulation and the proof of the Mordell-Weil theorem for elliptic curves defined over number fields. We will prove the Mordell-Weil theorem, which is a generalization of what Mordell showed about rational elliptic curves.

Theorem 0.1 (Mordell,Weil). *Let K be a number field and $E|_K$ be an elliptic curve defined over K. The group $E(K)$ of the K-rational points of E is finitely generated.*

1. Proof of the weak Mordell-Weil theorem for $m = 2$

Our first step is to prove a weaker version of Mordell-Weil theorem. This is necessary and, as it is obvious by the proof, it is also not straightforward.

Theorem 1.1 (Weak Mordell-Weil Theorem). *Let $E|_K$ be an elliptic curve defined over the number field K, and $m \in \mathbb{N} \setminus \{1\}$. The quotient group $E(K)/mE(K)$ is finite.*

There are proofs of 1.1, and we will mention one of these in the next chapter. However, it turns out that it suffices to show the weak Mordell-Weil theorem for a specific choice of m in order to prove the strong version of the theorem. And since we try to present a proof with elementary tools, we will prove it only for $m = 2$. The rest of this paragraph is focused on that proof.

Proposition 1.2. *Let L be a finite Galois extension of the number field K, E an elliptic curve defined over K and $m \in \mathbb{N} \setminus \{1\}$. If the quotient group $E(L)/mE(L)$ is finite, then so is the quotient group $E(K)/mE(K)$.*

Proof. Let

$$\begin{aligned} \iota \ : \ & E(K)/mE(K) \longrightarrow E(L)/mE(L) \\ & [P]_{mE(K)} \longmapsto [P]_{mE(L)} \end{aligned}$$

be the natural homomorphism. Then

$$\begin{aligned} \ker(\iota) &= \{[P]_{mE(K)} \in E(K)/mE(K) \mid \iota(P) = 1_{E(L)/mE(L)}\} \\ &= \{[P]_{mE(K)} \in E(K)/mE(K) \mid P \in mE(L)\} \\ &= (E(K) \cap mE(L))/mE(K). \end{aligned}$$

It suffices to show that this kernel is finite. If so, the result is immediate by the first isomorphism theorem of groups. Let $[P]_{mE(K)} \in \ker(\iota)$. There exists[1] a point $Q_P \in E(L)$, such that $mQ_P = P$. We define the map

$$\begin{aligned} \lambda_P \ &: \ \mathrm{Gal}(L/K) \longrightarrow E[m](\bar{K}) \\ & \sigma \longmapsto \sigma(Q_P) - Q_P, \end{aligned}$$

where $E[m](\bar{K}) := \{P \in E(\bar{K}) \mid mP = O\}$. Furthermore, we define

$$\begin{aligned} \lambda \ &: \ \ker(\iota) \longrightarrow \mathrm{Map}(\mathrm{Gal}(L/K), E[m]) \\ & P \longmapsto \lambda_P. \end{aligned}$$

We observe that for two points $P_1, P_2 \in E(K)$ we have

$$\lambda_{P_1} = \lambda_{P_2} \Rightarrow \sigma(Q_{P_1}) - Q_{P_1} = \sigma(Q_{P_2}) - Q_{P_2} \Rightarrow \sigma(Q_{P_1} - Q_{P_2}) = Q_{P_1} - Q_{P_2}\ ,\ \forall \sigma \in \mathrm{Gal}(L/K)$$

$$\Rightarrow Q_{P_1} - Q_{P_2} \in E(K) \Rightarrow [P_1]_{mE(K)} = [P_2]_{mE(K)}.$$

This means that the map λ is injective. We know that the sets $\mathrm{Gal}(L/K)$ and $E[m](\bar{K})$ are finite, so the set $\mathrm{Map}(\mathrm{Gal}(L/K), E[m])$ is finite, too. Hence, the kernel of ι is also finite. □

Remark 1.3. Let E be an elliptic curve defined over K, of the form

$$E|_K : Y^2 = X^3 + \alpha X + \beta,$$

where $\alpha, \beta \in K$. We denote by e_1, e_2 and e_3 the roots of the polynomial $X^3 + \alpha X + \beta$. In general $e_1, e_2, e_3 \in \bar{K}$. Proposition 1.2 allows us to replace the field K by its finite Galois extension $L := K(e_1, e_2, e_3)$, and prove the finiteness of the quotient group $E(L)/mE(L)$. It also allows us to assume without loss of generality that E is of the form

$$E : Y^2 = (X - e_1)(X - e_2)(X - e_3) \quad , \quad e_1, e_2, e_3 \in K. \tag{1}$$

Moreover, we may assume that $e_1, e_2, e_3 \in R_K$, that is they are algebraic integers of K. Indeed, we know that there exists a number $\delta \in R_K$ such that $\delta e_1, \delta e_2, \delta e_3 \in R_K$. Therefore, setting $X' := \delta X$, we obtain that

$$(X - e_1)(X - e_2)(X - e_3) = \frac{1}{\delta^3}(X' - \delta e_1)(X' - \delta e_3)(X' - \delta e_3).$$

If necessary, we enlarge the field K by considering the field $K(\sqrt{\delta})$ for instance, in order δ to be a perfect square in K, and we set $Y' := \delta\sqrt{\delta}Y$. Thus, we end up to an elliptic curve of the form

$$Y'^2 = (X' - e_1')(X' - e_2')(X' - e_3'),$$

where $e_i' := \delta e_i \in R_K$, for every $i \in \{1, 2, 3\}$, which is the form (1), with the difference that the roots of the polynomial at the right-hand side of the equation are algebraic integers of the field K.

At that point, the problem is that, unlikely to the case of $\mathbb{Q}$, we do not have unique factorization. However, we know that R_K is a Dedekind domain and so we have unique factorization for the fractional ideals of K.

[1] But it is not unique!

PROPOSITION 1.4. *Let E be an elliptic curve over the number field K, of the form* (1). *Then we may assume that $e_1, e_2, e_3 \in R_K$. Furthermore, for any point $P = [x : y : 1] \in E(K) \setminus \{O\}$ there are $r, t, s \in R_K$, such that*

$$x = \frac{r}{t^2} \quad \textit{and} \quad y = \frac{s}{t^3},$$

with g.c.d.$(r, t^2) = \mathfrak{c}^2$ and g.c.d.$(s, t^3) = \mathfrak{c}^3$, where $\mathfrak{c}$ is an integral ideal of the ring R_K.

PROOF. Since we proved that we may suppose that $e_1, e_2, e_3 \in R_K$, we assume that the given elliptic curve E, is of the form

$$E|_K : Y^2 = X^3 + \alpha X + \beta,$$

where $\alpha, \beta \in R_K$. Particularly,

$$\alpha = e_1e_2 + e_2e_3 + e_3e_1 \quad \text{and} \quad \beta = -e_1e_2e_3.$$

Let $a \in K$. For the ideal $\langle a \rangle$, we know that it can be written in the form

$$\langle a \rangle = \prod_{i=1}^{r} \mathfrak{p}_i{}^{n_i},$$

where $\mathfrak{p}_i$ is a prime ideal and $n_i \in \mathbb{Z}$, for every $i \in \{1, 2, \dots, r\}$. If $\alpha \in R_K$, then the power n_i of the prime ideal $\mathfrak{p}_i$ is a positive integer, for every $i \in \{1, 2, \dots, r\}$. Then the map

$$\begin{aligned} \upsilon_{\mathfrak{p}} \;:\; & K \longrightarrow \mathbb{Z} \cup \{\infty\} \\ & 0 \longmapsto \infty \\ & a \longmapsto \begin{cases} n_i & \text{, if } \mathfrak{p} = \mathfrak{p}_i \text{ , } i \in \{1, 2, \dots, r\} \\ 0 & \text{, otherwise} \end{cases} \end{aligned}$$

is a (discrete) valuation. Let $P = [x : y : 1] \in E(K)$. We will prove the double equivalence

$$\upsilon_{\mathfrak{p}}(x) < 0 \Leftrightarrow \upsilon_{\mathfrak{p}}(y) < 0 \Leftrightarrow \exists\, l \in \mathbb{N} : \upsilon_{\mathfrak{p}}(x) = -2l \text{ and } \upsilon_{\mathfrak{p}}(y) = -3l. \tag{2}$$

Suppose that $\upsilon_{\mathfrak{p}}(x) < 0$. Then $\upsilon_{\mathfrak{p}}(x) = -k$, for some $k \in \mathbb{N}$. We observe that

$$\begin{aligned} \upsilon_{\mathfrak{p}}(\alpha x + \beta) & \geq \min\{\upsilon_{\mathfrak{p}}(\alpha x), \upsilon_{\mathfrak{p}}(\beta)\} \\ & = \min\{\upsilon_{\mathfrak{p}}(\alpha) + \upsilon_{\mathfrak{p}}(x), \upsilon_{\mathfrak{p}}(\beta)\} \end{aligned}$$

Since $\alpha, \beta \in R_K$, it holds that $\upsilon_{\mathfrak{p}}(\alpha), \upsilon_{\mathfrak{p}}(\beta) \geq 0$. Therefore,

$$\upsilon_{\mathfrak{p}}(\alpha) + \upsilon_{\mathfrak{p}}(x) \geq -k \quad \text{and} \quad \upsilon_{\mathfrak{p}}(\beta) \geq 0.$$

From these inequalities it follows that

$$\upsilon_{\mathfrak{p}}(\alpha x + \beta) \geq \min\{\upsilon_{\mathfrak{p}}(\alpha) + \upsilon_{\mathfrak{p}}(x), \upsilon_{\mathfrak{p}}(\beta)\} \geq -k > -3k = \upsilon_{\mathfrak{p}}(x^3)$$
$$\Rightarrow \upsilon_{\mathfrak{p}}(x^3 + \alpha x + \beta) = \min\{\upsilon_{\mathfrak{p}}(x^3), \upsilon_{\mathfrak{p}}(\alpha x + \beta)\} = -3k.$$

But,

$$\upsilon_{\mathfrak{p}}(x^3 + \alpha x + \beta) = \upsilon_{\mathfrak{p}}(y^2) \Leftrightarrow 2\upsilon_{\mathfrak{p}}(y) = -3k \Rightarrow \upsilon_{\mathfrak{p}}(y) < 0.$$

Also,

$$2\upsilon_{\mathfrak{p}}(y) = -3k \Rightarrow 2 \mid k \Rightarrow \exists\, l \in \mathbb{N} : k = 2l.$$

So we have proved (2). Hence, there are integral ideals $\mathfrak{m}, \mathfrak{n}$ and $\mathfrak{t}$, such that

$$\langle x \rangle = \frac{\mathfrak{m}}{\mathfrak{t}^2} \quad \text{and} \quad \langle y \rangle = \frac{\mathfrak{n}}{\mathfrak{t}^3},$$

and g.c.d.$(\mathfrak{m}, \mathfrak{t}^2) = R_K =$ g.c.d.$(\mathfrak{n}, \mathfrak{t}^3)$. Let $t \in \mathfrak{t}$. Then

$$t \in \mathfrak{t} \Leftrightarrow \mathfrak{t} \mid \langle t \rangle \Leftrightarrow \exists\, \mathfrak{c} \trianglelefteq R_K : \langle t \rangle = \mathfrak{t}\mathfrak{c}.$$

So,

$$\langle x \rangle = \frac{\mathfrak{m}}{\mathfrak{t}^2} = \frac{\mathfrak{m}\mathfrak{c}^2}{\mathfrak{t}^2\mathfrak{c}^2} = \frac{\mathfrak{m}\mathfrak{c}^2}{\langle t \rangle^2}.$$

Similarly,

$$\langle y \rangle = \frac{\mathfrak{n}\mathfrak{c}^3}{\langle t \rangle^3}.$$

These relations inform us that $\mathfrak{m}\mathfrak{c}^2$ and $\mathfrak{n}\mathfrak{c}^3$ are principal ideals of R_K. Let $r', s' \in R_K$ such that,

$$\mathfrak{m}\mathfrak{c}^2 = \langle r' \rangle \quad \text{and} \quad \mathfrak{n}\mathfrak{c}^3 = \langle s' \rangle.$$

Then

$$\langle x \rangle = \frac{\langle r' \rangle}{\langle t \rangle^2} \quad \text{and} \quad \langle y \rangle = \frac{\langle s' \rangle}{\langle t \rangle^3}.$$

Equivalently, there are $\varepsilon_1, \varepsilon_2 \in R_K^\times$, such that

$$x = \varepsilon_1 \frac{r'}{t^2} \quad \text{and} \quad y = \varepsilon_2 \frac{s'}{t^3}.$$

The result is now immediate, if we set[2] $r := r'\varepsilon_1$ and $s := s'\varepsilon_2$. □

Definition 1.5. Let E be an elliptic curve of the form (1). For every $i \in \{1, 2, 3\}$, we define the maps

$$\begin{array}{rcll} \varphi_i & : & E(K) \longrightarrow K^\times/(K^\times)^2 & \\ & & O \longmapsto [1]_{(K^\times)^2} & \\ & & [e_i : 0 : 1] \longmapsto [(e_i - e_j)(e_i - e_k)]_{(K^\times)^2} & , \quad \{i, j, k\} = \{1, 2, 3\} \\ & & [x : y : 1] \longmapsto [x - e_i]_{(K^\times)^2}. & \end{array}$$

We observe that for points $\neq O$ the definition of φ_i is essentially the same, since

$$\begin{aligned} Y^2 = (X - e_1)(X - e_2)(X - e_3) &= (X - e_i)(X - e_j)(X - e_k) \\ \Rightarrow Y^2(X - e_i) &= (X - e_i)^2(X - e_j)(X - e_k) \\ \Rightarrow [X - e_i]_{(K^\times)^2} &= [(X - e_j)(X - e_k)]_{(K^\times)^2}. \end{aligned}$$

Further, define

$$\begin{array}{rcl} \varphi & : & E(K) \longrightarrow K^\times/(K^\times)^2 \oplus K^\times/(K^\times)^2 \oplus K^\times/(K^\times)^2 \\ & & P \longmapsto (\varphi_1(P), \varphi_2(P), \varphi_3(P)). \end{array}$$

Theorem 1.6. *Let*

$$E|_K : Y^2 = (X - e_1)(X - e_2)(X - e_3),$$

where $e_1, e_2, e_3 \in R_K$, be an elliptic curve over K. Then the map φ, as it was defined in 1.5, has the following properties:

(i) *φ is a group homomorphism.*
(ii) $\ker(\varphi) = 2E(K)$

[2] Of course, this representation of x and y is not unique.

(iii) the image $\varphi(E(K))$ is finite.

Proof. (i) In order to show that φ is a group homomorphism indeed, it suffices to show that

$$\varphi_i(P_1 + P_2) = \varphi_i(P_1)\varphi_i(P_2) \quad , \quad \forall\, i \in \{1, 2, 3\}. \tag{3}$$

For this, we have to will consider the following cases for the points P_1 and P_2.

Case 1. If $P_1 = O$ or $P_2 = O$, then (3) holds trivially.

Case 2. Let $P_1 + P_2 = O \Leftrightarrow P_1 = -P_2$. Then for each $i \in \{1, 2, 3\}$, we have

$$\varphi_i(P_1 + P_2) = \varphi_i(O) = [1]_{(K^\times)^2},$$

and $\varphi_i(-P_2) = \varphi_i(P_2)$. So,

$$\varphi_i(P_1)\varphi_i(P_2) = \varphi_i(-P_2)\varphi_i(P_2) = (\varphi_i(P_2))^2 = [1]_{(K^\times)^2},$$

so (3) is also true.

Case 3. Let $P_1 = [x_1 : y_1 : 1]$ and $P_2 = [x_2 : y_2 : 1]$ be points of $E(K)$, such that

$$P_1 + P_2 \notin \{[e_i : 0 : 1] \mid i \in \{1, 2, 3\}\} \cup \{O\}.$$

Set $P_1 + P_2 =: P_3 = [x_3 : y_3 : 1]$. Consider the line

$$Y = \lambda X + \nu,$$

which passes through the points P_1 and P_2. Then the numbers x_1, x_2 and x_3 are solutions of the qubic equation

$$(\lambda X + \nu)^2 = (X - e_1)(X - e_2)(X - e_3).$$

Equivalently,

$$(\lambda X + \nu)^2 - (X - e_1)(X - e_2)(X - e_3) = -(X - x_1)(X - x_2)(X - x_3).$$

So,

$$\begin{aligned}
(e_i - x_1)(e_i - x_2)(e_i - x_3) = -(\lambda e_i + \nu)^2 \qquad \forall\, i \in \{1, 2, 3\}\\
\Rightarrow x_3 - e_i = (x_1 - e_i)(x_2 - e_i)\frac{-(\lambda e_i + \nu)^2}{(x_1 - e_i)^2(x_2 - e_i)^2}\\
\Rightarrow [x_3 - e_i]_{(K^\times)^2} = [(x_1 - e_i)(x_2 - e_i)]_{(K^\times)^2} = [(x_1 - e_i)]_{(K^\times)^2}[(x_2 - e_i)]_{(K^\times)^2}\\
\Rightarrow \varphi_i(P_3) = \varphi_i(P_1 + P_2) = \varphi_i(P_1)\varphi_i(P_2).
\end{aligned}$$

Case 4. Let $P_1 = [x_1 : y_1 : 1]$, $P_2 = [e_i : 0 : 1]$ and $P_3 = P_1 + P_2 = [x_3 : y_3 : 1]$, where $x_1 \notin \{e_j, e_k\}$, where $\{1, 2, 3\} = \{i, j, k\}$. That means that $x_3 \notin \{e_1, e_2, e_3\}$. So,

$$\begin{aligned}
\varphi_i(P_1 + P_2) = \varphi_i(P_3) &= [x_3 - e_i]_{(K^\times)^2} = [(x_3 - e_j)(x_3 - e_k)]_{(K^\times)^2}\\
&= [(x_3 - e_j)]_{(K^\times)^2}[(x_3 - e_k)]_{(K^\times)^2}\\
&= [(x_1 - e_j)(x_2 - e_j)]_{(K^\times)^2}[(x_1 - e_k)(x_2 - e_k)]_{(K^\times)^2}\\
&= [(x_1 - e_i)(x_1 - e_k)]_{(K^\times)^2}[(x_2 - e_i)(x_2 - e_k)]_{(K^\times)^2}\\
&= [(x_1 - e_i)]_{(K^\times)^2}[(x_2 - e_i)]_{(K^\times)^2}\\
&= \varphi_i(P_1)\varphi_i(P_2)
\end{aligned}$$

Case 5. Let $P_1 = [e_i : 0 : 1]$ and $P_2 = [e_j : 0 : 1]$. Then $P_1 + P_2 = [e_k : 0 : 1]$, where $\{i, j, k\} = \{1, 2, 3\}$. In that case we obtain

$$\begin{aligned} \varphi_i(P_1 + P_2) &= [e_k - e_i]_{(K^\times)^2} \\ &= [(e_k - e_i)(e_j - e_i)^2]_{(K^\times)^2} \\ &= [(e_k - e_i)(e_j - e_i)]_{(K^\times)^2}[(e_j - e_i)]_{(K^\times)^2} \\ &= \varphi_i(P_1)\varphi_i(P_2). \end{aligned}$$

Case 6. Let P_1 and P_2 be points of $E(K)$ such that $P_1 + P_2 = [e_i : 0 : 1]$ and $P_1, P_2 \notin \{[e_j : 0 : 1], [e_k : 0 : 1]\}$, where $\{i, j, k\} = \{1, 2, 3\}$. If one of the points is equal to $[e_i : 0 : 1]$, the result follows immediately. If otherwise, we have

$$P_1 + P_2 + [e_i : 0 : 1] = O,$$

since the points $[e_i : 0 : 1]$, are points of order 2, for each $i \in \{1, 2, 3\}$. Then using the second case, it follows that

$$\varphi_i(P_1)\varphi_i(P_2 + [e_i : 0 : 1]) = [1]_{(K^\times)^2}.$$

We use now the previous case and we have,

$$\varphi_i(P_1)\varphi_i(P_2)[(e_i - e_j)(e_i - e_k)]_{(K^\times)^2} = [1]_{(K^\times)^2}$$

$$\Rightarrow \varphi_i(P_1)\varphi_i(P_2) = [(e_i - e_j)(e_i - e_k)]_{(K^\times)^2} = \varphi_i(P_1 + P_2).$$

Now, it is easy to check that any choice of P_1 and P_2 falls into these six cases.

(ii) According to (i) we know that φ is a homomorphism, and so

$$\varphi(2P) = (\varphi(P))^2 = [1]_{(K^\times)^2} \quad , \quad \forall P \in E(K)$$

$$\Rightarrow 2E(K) \subseteq \ker(\varphi).$$

We will now prove that $\ker(\varphi) \subseteq 2E(K)$. First we observe that $O \in 2E(K)$. Let, now $P = [x : y : 1] \in \ker(\varphi)$, with $x \neq 0$. Setting

$$X' := X - x \quad \text{and} \quad Y' := Y,$$

we map the point P to the point $P' := [0 : y : 1]$. This means that without loss of generality we may assume that $x = 0$, and so $P = [0 : y : 1]$.

- If $y = 0$, then by defining equation of the elliptic curve we obtain that $e_1e_2e_3 = 0$. Without loss of generality we assume that $e_3 = 0$. Since $P \in \ker(\varphi)$, we have

$$\varphi_i(P) = [1]_{(K^\times)^2} \quad , \quad \forall i \in \{1, 2, 3\}.$$

But

$$\varphi_1(P) = -e_1 \quad , \quad \varphi_2(P) = -e_2 \quad \text{and} \quad \varphi_3(P) = -e_3 = 0.$$

Hence,

$$-e_1, -e_2, -e_3 \in K^2.$$

- If $y \neq 0$, then $y^2 = -e_1e_2e_3$ and so, using again the defining equation of the elliptic curve, we end up to the same conclusion, i.e. that $-e_1, -e_3, -e_3 \in K^2$.

Let $Q = [x_Q : y_Q : 0] \in E(\bar{K})$, such that $P = 2Q$. In order to complete the proof of (ii) we will show that

$$-e_1, -e_3, -e_3 \in K^2 \Rightarrow Q \in E(K).$$

Let

$$Y = \lambda' X + \nu'$$

be the tangent of E at the point Q. Then the point $-2Q = [0 : -y : 1]$ lies on the tangent, and so

$$\nu' = -y \in K.$$

The intersection of the elliptic curve with the tangent at Q can be expressed by the equation

$$\begin{aligned}(\lambda' X + \nu')^2 &= (X - e_1)(X - e_2)(X - e_3)\\ &= X^3 + \alpha X + \beta,\end{aligned}$$

where

$$\alpha = e_1 e_2 + e_2 e_3 + e_3 e_1 \quad \text{and} \quad \beta = -e_1 e_2 e_3 = y^2 = \nu'^2.$$

Equivalently, we have that

$$X^3 + (-\lambda'^2)X^2 + (\alpha - 2\nu'\lambda')X = 0.$$

The roots of that equation are 0 and x_Q (double root). This means that the number x_Q is double root of the equation

$$X^2 + (-\lambda'^2)X + (\alpha - 2\nu'\lambda') = 0.$$

Therefore,

$$\lambda'^4 = 4(\alpha - 2\nu'\lambda') \quad \text{and} \quad x_Q = \frac{\lambda'^2}{2}.$$

For any $u \in K$, we have that

$$\begin{aligned}(\lambda'^2 + u)^2 &= \lambda'^4 + 2(\lambda'^2)u + u^2\\ &= (\sqrt{2u}\lambda')^2 - \frac{8\nu'}{\sqrt{2u}}(\sqrt{2u}\lambda') + (u^2 + 4\alpha)\end{aligned}$$

The left-hand side of this equation is a trinomial of variable $\sqrt{2u}\lambda'$. The discriminant of it is

$$\left(\frac{8\nu'}{\sqrt{2u}}\right)^2 - 4(u^2 + 4\alpha) = 4\left(\frac{8\nu'^2}{u} - (u^2 + 4\alpha)\right) = 0.$$

By multiplying with u and using the relation $\beta = \nu^2$, we obtain

$$-u^3 - 4\alpha u + 8\beta = 0.$$

Setting $u' := -\frac{u}{2}$, we end up to the qubic equation[3]

$$8(u'^3 + \alpha u' + \beta) = 0,$$

for which we know that the roots are the numbers e_1, e_2 and e_3. So,

$$u' \in \{e_1, e_2, e_3\} \Rightarrow u \in \{-2e_1, -2e_2, -2e_3\}.$$

[3] If P is the point $[0 : 0 : 1]$ we have to be careful at the calculations, but we end up in the same equation.

Assume without loss of generality that $u = -2e_3$. Then

$$(\lambda'^2 - 2e_3)^2 = \lambda'^4 - 4\lambda'^2 e_3 + 4{e_3}^2.$$

Using the equality $\alpha = e_1e_2 + e_2e_3 + e_3e_1$, we have that

$$\begin{aligned}
(\lambda'^2 - 2e_3)^2 &= 4(e_1e_2 + e_2e_3 + e_3e_1) - 8\nu'\lambda' + 4{e_3}^2 - 4e_3\lambda'^2 \\
&= 4(e_1e_2 + {e_3}^2 + e_2e_3 + e_3e_1) - 8\nu'\lambda' - 4e_3\lambda'^2 \\
&= 4e_1e_2 - 8\nu'\lambda' - 4e_3\lambda'^2 \\
&= \frac{-4}{e_3}(-e_1e_2e_3 + 2\nu'\lambda' + \lambda'^2) \\
&= \frac{-4}{e_3}(\nu'^2 + 2\nu'\lambda' + \lambda'^2) \\
&= \frac{-4}{e_3}(\nu' + \lambda' e_3)^2
\end{aligned}$$

Thus,

$$\begin{gathered}
\lambda'^2 - 2e_3 = \pm\frac{2}{\sqrt{-e_3}}(\lambda' e_3 + \nu) = \pm\frac{2}{\sqrt{-e_3}}(\lambda' e_3 \pm \sqrt{-e_1e_2e_3}) \\
\Rightarrow \lambda'^2 - 2e_3 = \pm 2\lambda'\sqrt{-e_3} \pm 2\sqrt{-e_2}\sqrt{-e_3}. \\
\Rightarrow \lambda'^2 - e_3 + e_1 + e_2 = \pm 2\lambda'\sqrt{-e_3} \pm 2\sqrt{-e_2}\sqrt{-e_3}. \\
\Rightarrow (\lambda' \mp \sqrt{-e_2})^2 = (\sqrt{-e_1} \pm \sqrt{-e_2})^2 \\
\Rightarrow \lambda' = \pm\sqrt{-e_1} \pm \sqrt{-e_2} \pm \sqrt{-e_3}.
\end{gathered}$$

But

$$-e_i \in K^2 \ , \ \forall i \in \{1,2,3\} \Rightarrow \sqrt{-e_i} \in K \ , \ \forall i \in \{1,2,3\} \Rightarrow \lambda' \in K.$$

Finally, it follows that

$$x_Q = \frac{\lambda'^2 - a_2}{2} \in K \quad \text{and} \quad y_Q = \lambda' x_Q + \nu' \in K,$$

i.e. that $Q \in E(K)$, which was the desired result in order to complete the proof.

(iii) Let P_K be the group of all principal ideals of the ring R_K of integers of K. We define the map

$$\begin{aligned}
\eta \ : \ & K^\times/(K^\times)^2 \longrightarrow \mathrm{P}_K/(\mathrm{P}_K)^2 \\
& [x]_{(K^\times)^2} \longmapsto [\langle x\rangle]_{(\mathrm{P}_K)^2}
\end{aligned}$$

It is easy to check that η is a group homomorphism. Also,

$$\begin{aligned}
\ker(\eta) &= \{[x]_{(K^\times)^2} \in K^\times/(K^\times)^2 \mid \eta([x]_{(K^\times)^2}) = 1_{\mathrm{P}_K/(\mathrm{P}_K)^2}\} \\
&= \{[x]_{(K^\times)^2} \in K^\times/(K^\times)^2 \mid \langle x\rangle \in (\mathrm{P}_K)^2\} \\
&= \{[x]_{(K^\times)^2} \in K^\times/(K^\times)^2 \mid \exists t \in K : \langle x\rangle = \langle t\rangle^2\} \\
&= \{[x]_{(K^\times)^2} \in K^\times/(K^\times)^2 \mid \exists t \in K, \exists \varepsilon \in R_K^\times : x = \varepsilon t^2\} \\
&= R_K^\times K^\times/(K^\times)^2 \\
&\cong R_K^\times/(R_K^\times \cap (K^\times)^2) \\
&= R_K^\times/(R_K^\times)^2
\end{aligned}$$

In other words,

$$\ker(\eta) \cong R_K^\times/(R_K^\times)^2.$$

But the last quotient group is finite, which is an immediate consequence of Dirichlet's units theorem. This means that the kernel of η is also finite. We define the map

$$\begin{aligned} \hat{\varphi} \ : \ & E(K) \longrightarrow \mathrm{P}_K/(\mathrm{P}_K)^2 \oplus \mathrm{P}_K/(\mathrm{P}_K)^2 \oplus \mathrm{P}_K/(\mathrm{P}_K)^2 \\ & P \longrightarrow (\eta(\varphi_1(P)), \eta(\varphi_2(P)), \eta(\varphi_3(P))) \end{aligned}$$

i.e. the map $\hat{\varphi} := \eta \circ \varphi$. In order to prove the finiteness of $\varphi(E(K))$, it suffices to prove that the image $\hat{\varphi}(E(K))$ is finite. Let $P = [x : y : 1] \in E(K)$, i.e. we assume without loss of generality that $P \neq O$. By proposition 1.4, we know that there are $r, s, t \in R_K$ such that

$$x = \frac{r}{t^2} \quad \text{and} \quad y = \frac{s}{t^3},$$

with g.c.d.$(r, t^2) = \mathfrak{c}^2$ and g.c.d.$(s, t^3) = \mathfrak{c}^3$, where $\mathfrak{c}$ is an integral ideal of the ring R_K. Then

$$\varphi_i(P) = [x - e_i]_{(K^\times)^2} = \left[\frac{r}{t^2} - e_i\right]_{(K^\times)^2} = [r - t^2 e_i]_{(K^\times)^2}.$$

We may factorize the integral ideal $\langle r - t^2 e_i\rangle$ in a unique way, such that

$$\langle r - t^2 e_i\rangle = \mathfrak{a}\mathfrak{b}^2,$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals of R_K and the ideal $\mathfrak{a}$ is square-free. Let, now, $\mathfrak{m}$ be an integral ideal of R_K, such that $\mathfrak{b} \in [\mathfrak{m}]_{\mathrm{Cl}(K)}$, where $\mathrm{Cl}(K)$ is the class group of the field K. Therefore, there exists a $b \in K^\times$ such that $\mathfrak{b} = \mathfrak{m}\langle b\rangle$. So,

$$\langle r - t^2 e_i\rangle = \mathfrak{a}\mathfrak{b}^2 = \mathfrak{a}\mathfrak{m}^2\langle b\rangle^2 \Rightarrow \mathfrak{a}\mathfrak{m}^2 \in \mathrm{P}_K \Rightarrow \exists\, c \in K^\times : \langle c\rangle = \mathfrak{a}\mathfrak{m}^2.$$

Since we assumed that the ideals $\mathfrak{a}$ and $\mathfrak{m}$ are integral, it follows that $c \in R_K$. Hence,

$$\eta(\varphi_i(P)) = \eta([r - t^2 e_i]_{(K^\times)^2}) = [\langle r - t^2 e_i\rangle]_{(\mathrm{P}_K)^2} = \left[\langle c\rangle \langle b\rangle^2\right]_{(\mathrm{P}_K)^2} = [\langle c\rangle]_{(\mathrm{P}_K)^2}.$$

By the equation $\langle c\rangle = \mathfrak{a}\mathfrak{m}^2$ is finite. Indeed, the ideal $\mathfrak{a}$ has been chosen uniquely, and the class group $\mathrm{Cl}(K)$ of K is finite. We will prove that $\langle c\rangle$ has finite prime divisors. Let $\mathfrak{p}$ be a prime ideal, so that $v_{\mathfrak{p}}(c) \neq 0$.

- Let $v_{\mathfrak{p}}(c) = 1$. This means that

  $$\mathfrak{p} \mid \langle r - t^2 e_i\rangle.$$

  For $P = [x : y : 1] \in E(K)$, we have that

  $$y^2 = (x - e_1)(x - e_2)(x - e_3).$$

  Therefore,

  $$\begin{aligned} y^2 t^2 &= (r - t^2 e_1)(r - t^2 e_2)(r - t^2 e_3) \\ \Rightarrow 1_{\mathrm{P}_K/(\mathrm{P}_K)^2} &= [\langle r - t^2 e_1\rangle]_{(\mathrm{P}_K)^2}[\langle r - t^2 e_2\rangle]_{(\mathrm{P}_K)^2}[\langle r - t^2 e_3\rangle]_{(\mathrm{P}_K)^2}. \end{aligned}$$

  Hence, there exists a $j \in \{1, 2, 3\}$, so that $j \neq i$ and $v_{\mathfrak{p}}(c_j) \equiv 1 \pmod 2$, where the c_j is constructed as c, for φ_j instead of φ_i. Then

  $$\mathfrak{p} \mid \langle r - t^2 e_i\rangle.$$

  Thus,

  $$\mathfrak{p} \mid \langle t^2(e_i - e_j)\rangle \quad \text{and} \quad \mathfrak{p} \mid \langle r(e_i - e_j)\rangle$$

From these relations it follows that the prime ideal $\mathfrak{p}$ divides the discriminant of the polynomial $(X - e_1)(X - e_2)(X - e_3)$ and the ideal g.c.d.(r, t^2). This product can be made independent of the point P and of i.

- If $|\upsilon_{\mathfrak{p}}(c)| \geq 2$ then $\mathfrak{p}$ is a divisor of $\mathfrak{m}$ and therefore, is in a finite set.

□

Theorem 1.7 (Weak Mordell-Weil Theorem for $m = 2$). *Let E be an elliptic curve defined over the number field K. Then the quotient group $E(K)/2(K)$ is finite.*

Proof. For the group homomorphism φ, as it was defined in 1.5, we obtain that

$$E(K)/\ker(\varphi) \cong \varphi(E(K)),$$

by the first group isomorphism theorem. But by theorem 1.6, we know that $\ker(\varphi) = 2E(K)$ and the image $\varphi(E(K))$ is finite. So $E(K)/2E(K)$ is finite, indeed. □

2. Heights

Mordell-Weil theorem deals with the construction of the group of the K-rational points of an elliptic curve. It is necessary to introduce a notion of measuring the "size" of the K-rational points. Therefore, we define some functions that are called *height functions*, or simply *heights*.

The goal of this paragraph is to define such functions over elliptic curves, in a way that they satisfy some appropriate properties. To achieve that, we start by introducing the notion of height on $\mathbb{Q}$.

2.1. Height of rational numbers.

Every reduced rational number is characterized by its numerator and denominator. Therefore, a natural definition of the height of a rational point is the following.

Definition 2.1. Let $\alpha = \dfrac{x}{y} \in \mathbb{Q}$, such as $x, y \in \mathbb{Z}$ with g.c.d.$(x, y) = 1$. We define the *height of α* by

$$H(\alpha) := \max\{|x|, |y|\}.$$

Proposition 2.2. *For any given $B \in \mathbb{R}_{>0}$, the set*

$$\{\alpha \in \mathbb{Q} \mid H(\alpha) \leq B\}$$

is finite.

Proposition 2.3. *For any $\alpha \in \mathbb{Q}^\times$ we have*

$$H(\alpha) = \max\{1, |\alpha|_\infty\} \prod_{p\ prime} \max\{1, |\alpha|_p\}.$$

Proof. Let $\alpha = \dfrac{x}{y}$, where $x, y \in \mathbb{Z}$ with g.c.d.$(x, y) = 1$. Then

$$\prod_{p \text{ prime}} \max\{1, |\alpha|_p\} = \prod_{\substack{p \text{ prime} \\ p|y}} \max\{1, |\alpha|_p\} \prod_{\substack{p \text{ prime} \\ p|x}} \max\{1, |\alpha|_p\} \prod_{\substack{p \text{ prime} \\ p\nmid xy}} \max\{1, |\alpha|_p\}.$$

Since $|\alpha|_p = 1$, for every prime $p \nmid xy$ and $|\alpha_p| < 1$, for every $p \mid x$, we obtain

$$\prod_{p \text{ prime}} \max\{1, |\alpha|_p\} = |y|.$$

Thus, it suffices to show that

$$H(\alpha) = |y| \max\{1, |\alpha|\}.$$

- If $|\alpha| > 1$, then $|x| > |y|$, and so
$$H(\alpha) = \max\{|x|, |y|\} = |x| = \frac{|x|}{|y|}|y| = |y| \max\{1, |\alpha|\}.$$
- If $|\alpha| < 1$, then $|x| < |y|$, and so
$$H(\alpha) = \max\{|x|, |y|\} = |y| = |y| \max\{1, |\alpha|\}.$$
- Finally, if $|\alpha| = 1$, we easily check that
$$H(\alpha) = |x| = |y| = |y| \max\{1, |\alpha|\}.$$

Therefore, we proved the desired equality in each case. □

2.2. Height of algebraic numbers. By definition, an algebraic number is a root of a rational polynomial. So, we can associate an algebraic number to all polynomials, which have it as root. In order to choose uniquely such a polynomial, we do some additional assumptions.

Definition 2.4. Let α be an algebraic integer. The polynomial f with the properties:

(i) $f(X) \in \mathbb{Z}[X]$,
(ii) $f(\alpha) = 0$,
(iii) the leading coefficient is positive,
(iv) the g.c.d. of the coefficients is equal to 1, and
(v) for every polynomial $g(X) \in \mathbb{Z}[X] \setminus \{f(X)\}$ that satisfies properties (i)-(iv), holds that $\deg(g) > \deg(f)$.

is called *normalized minimal polynomial of* α.

It is obvious, now, that for any algebraic integer α its the normalized minimal polynomial is unique. So, we could associate the height of α with a measure of the "size" of its normalized minimal polynomial. This leads us to introduce the notion of Mahler measure of a polynomial.

Definition 2.5. [4] Let $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X] \setminus \{0\}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f. We define *the Mahler measure of* f by

$$\mu(f) := |a_n| \prod_{i=1}^{n} \max(1, |\alpha_i|).$$

[4] Since we are dealing with algebraic numbers, the normalized minimal polynomials have rational coefficients. However, the Mahler measure is defined more generally for polynomials with complex coefficients.

Remark 2.6. By definition, the Mahler measure $\mu(f)$ of a polynomial f is, up to the leading coefficient of f, the product of the roots of f outside the complex unit circle. An explicit way of computing Mahler measure $\mu(f)$, without knowing the roots of f, is given by Jensen's formula.

Corollary 2.7. *Let polynomials $f(X), g(X) \in \mathbb{C}[X] \setminus \{0\}$ and $f^*(X) \in \mathbb{C}[X] \setminus \{0\}$ be the reciprocal polynomial of f, i.e, the polynomial defined by*

$$f^*(X) := X^{\deg(f)} \cdot f\left(\frac{1}{X}\right).$$

For the Mahler measures of the above polynomials we have

$$\mu(fg) = \mu(f)\mu(g) \quad \textit{and} \quad \mu(f^*) = \mu(f).$$

Proof. The first equation is obvious by the definition of the Mahler measure. We assume that $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Then

$$\mu(f) = |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f. Then by definition of f^*, we obtain that

$$\mu(f^*) = |a_0| \prod_{i=1}^{n} \max\{1, \frac{1}{|\alpha_i|}\}.$$

Thus,

$$\frac{\mu(f)}{\mu(f^*)} = \frac{|a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}}{|a_0| \prod_{i=1}^{n} \max\{1, \frac{1}{|\alpha_i|}\}} = \frac{|a_n|}{|a_0|} \prod_{i=1}^{n} |\alpha_i| = 1,$$

since by Vieta's formulas for the polynomial f, we have

$$\frac{a_0}{a_n} = (-1)^n \prod_{i=1}^{n} \alpha_i.$$

□

Lemma 2.8 (Norm Inequality). *Let $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$. Then*

$$|a_j| \leq \binom{n}{j}\mu(f) \quad , \quad \forall j \in \{0, 1, \ldots, n-1\}.$$

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f. By Vieta's formulas we obtain

$$\frac{a_j}{\alpha_n} = (-1)^{n-j} \sum_{\{j_1, j_2, \ldots, j_{n-j}\} \subseteq \{1,2,\ldots,n\}} \alpha_{j_1}\alpha_{j_2} \cdots \alpha_{j_{n-j}}.$$

Hence,

$$\left|\frac{a_j}{\alpha_n}\right| = \left| \sum_{\{j_1, j_2, \ldots, j_{n-j}\} \subseteq \{1,2,\ldots,n\}} \alpha_{j_1}\alpha_{j_2} \cdots \alpha_{j_{n-j}} \right| \leq \sum_{\{j_1, j_2, \ldots, j_{n-j}\} \subseteq \{1,2,\ldots,n\}} |\alpha_{j_1}||\alpha_{j_2}| \cdots |\alpha_{j_{n-j}}|$$

$$\leq \sum_{\{j_1, j_2, \ldots, j_{n-j}\} \subseteq \{1,2,\ldots,n\}} \max\{1, |\alpha_{j_1}|\} \max\{1, |\alpha_{j_2}|\} \cdots \max\{1, |\alpha_{j_{n-j}}|\}$$

$$\leq \sum_{\{j_1,j_2,\ldots,j_{n-j}\}\subseteq\{1,2,\ldots,n\}} \max\{1,|\alpha_1|\}\max\{1,|\alpha_2|\}\cdots\max\{1,|\alpha_n|\} = \binom{n}{j}\prod_{i=1}^{n}\max\{1,|\alpha_i|\}.$$

$$\Rightarrow |a_j| \leq \binom{n}{j}\mu(f).$$

□

Theorem 2.9 (Kronecker). *Let $f(X)$ be a monic polynomial with integer coefficients. Then $\mu(f) = 1$ if and only of all nontrivial roots of f are equal to roots of unity.*

Proof. ($\Leftarrow$) Trivial.
($\Rightarrow$) Let $f(X) \in \mathbb{Z}[X]$, of degree n, with $\mu(f) = 1$ and $f(0) \neq 0$. We will show that the roots of f are equal to roots of unity. According to the norm inequality and the fact that $\mu(f) = 1$, for the j-th coefficient a_j of f we obtain that

$$|a_j| \leq \binom{n}{j}.$$

For $j = 0$, we have $|a_0| \leq 1 \Rightarrow a_0 \in \{-1,0,1\}$. Since $f(0) \neq 0$, the standard coefficient $|a_0|$ is equal to 1. Thus, if we denote by $\alpha_1,\alpha_2,\ldots,\alpha_n$ the roots of f, by the Vieta's relations we obtain that

$$\left|\prod_{i=1}^{n}\alpha_i\right| = \prod_{i=1}^{n}|\alpha_i| = 1. \tag{4}$$

By corollary 2.7 we conclude that $\mu(f^*) = 1$, and because $|a_0| = 1$, we have

$$\prod_{i=1}^{n}\max\left\{1,\frac{1}{|\alpha_i|}\right\} = 1. \tag{5}$$

We will prove that from the system of the equations (4) and (5) it follows that

$$|\alpha_i| = 1 \quad , \quad \forall i \in \{1,2,\ldots,n\}.$$

We assume that

$$\exists\, k \in \{1,2,\ldots,n\} : |\alpha_k| \neq 1.$$

Let $|\alpha_k| > 1$. In order for (4) to be true, there must exists an $l \in \{1,2,\ldots,n\} \smallsetminus \{k\}$ such that $|\alpha_l| < 1$. Then

$$\max\left\{1,\frac{1}{|\alpha_l|}\right\} = \frac{1}{|\alpha_l|}.$$

And so,

$$1 = \prod_{i=1}^{n}\max\left\{1,\frac{1}{|\alpha_i|}\right\} = \frac{1}{|\alpha_l|}\prod_{\substack{i=1\\ i\neq l}}^{n}\max\left\{1,\frac{1}{|\alpha_i|}\right\} \geq \frac{1}{|\alpha_l|} > 1,$$

which is a contradiction. Assume now that $|\alpha_k| < 1$. Then the contradiction follows similarly to the previous case. □

Definition 2.10. Let α be an algebraic number. We define the *height* of α to be the number $H(\alpha)$ given by

$$H(\alpha) := \mu(f)^{1/\deg(f)},$$

where f is the normalized minimal polynomial of α.

Remark 2.11. Note that the above definition is a generalization of the height of rational number. Indeed, if $\alpha = \frac{r}{s}$, with g.c.d.$(r, s) = 1$, then the normalized minimal polynomial of α is $f(X) = sX - r$. Thus

$$H(\alpha) = (|s| \max\{1, |\alpha|\})^{\frac{1}{1}},$$

which is equal to $|s|$ if $|\alpha| < 1$, or $|r|$ if $|\alpha| > 1$, as expected.

Proposition 2.3 provides us with a decomposition formula, since the height of the rational point can be calculated using all archimedean and non archimedean valuations of $\mathbb{Q}$. Our next step is to establish a decomposition formula for heights of algebraic numbers.

Definition 2.12. Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$, where K is a number field. For[5] $v \in \mathrm{M}_K$ we define *the content of f at v* to be[6]

$$\mathrm{cont}_v(f) := \max_{0 \le j \le n} \{\|a_j\|_v\}.$$

Lemma 2.13 (Gauss). *The content is multiplicative for every $v \in M_K \setminus M_K^\infty$, i.e. for $f_1, f_2 \in K[X]$ it holds that*

$$cont_v(f_1 f_2) = cont_v(f_1) cont_v(f_2).$$

Proof. Let

$$f_1(X) = a_0 + a_1 X + \cdots + a_m X^m \quad \text{and} \quad f_2(X) = b_0 + b_1 X + \cdots + b_n X^n.$$

We assume that a_r, with $r \in \{1, 2, \ldots, m\}$, is a coefficient of f_1, such as

$$\|a_r\|_v \ge \|a_i\|_v \quad , \quad \forall i \in \{0, 1 \ldots, m\}$$

and it lies the furthest to the right with that property. Similarly, we choose b_s, with $s \in \{0, 1, \ldots, n\}$, in order to have the same properties as a_r, with respect to f_2. Then,

$$a_r{}^{-1} f_1(X) = \frac{a_0}{a_r} + \cdots + X^r + \cdots + \frac{a_m}{a_r}$$

and

$$b_s{}^{-1} f_2(X) = \frac{b_0}{b_s} + \cdots + X^s + \cdots + \frac{b_n}{b_s}.$$

The coefficients of the polynomials at the left hand side are ≤ 1. Considering the product

$$\frac{1}{a_r b_s} f_1 f_2$$

we observe that the coefficient of X^{r+s} is of the form $1 + c$, where $\|c\|_v < 1$. For the coefficient of X^i, where $i \ne r + s$, we can easily check that its valuation is ≤ 1. That is,

$$\mathrm{cont}_v\left(\frac{1}{a_r b_s} f_1 f_2\right) = 1 \Rightarrow \mathrm{cont}_v(f_1 f_2) = \|a_r b_s\|_v = \|a_r\|_v \|b_s\|_v = \mathrm{cont}_v(f_1)\mathrm{cont}_v(f_2).$$

□

[5] By M_K we denote the set of all equivalence classes of absolute values of K (see Appendix A).

[6] By $\|\cdot\|_v$ we denote the normalized absolute value associated to the place v of K (see Appendix A).

Theorem 2.14. *Let K be a number field and $\alpha \in K$.Then*

$$H(\alpha) = \left(\prod_{v \in M_K} \max\{1, \|\alpha\|_v\} \right)^{\frac{1}{[K:\mathbb{Q}]}}.$$

Proof. We first assume that $K = \mathbb{Q}(\alpha)$, and $\alpha \in R_K = R_{\mathbb{Q}(\alpha)}$, where R_K is the ring of algebraic integers of the field K. In this case, we have[7]

$$\|\alpha\|_v \leq 1 \quad , \quad \forall v \in \mathrm{M}_{\mathbb{Q}(\alpha)} \smallsetminus \mathrm{M}^{\infty}_{\mathbb{Q}(\alpha)}.$$

Therefore,

$$\prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)} \smallsetminus \mathrm{M}^{\infty}_{\mathbb{Q}(\alpha)}} \max\{1, \|\alpha\|_v\} = 1.$$

We will, now, examine the infinite places of α. Archimedean places of K are determined by its embeddings to $\mathbb{R}$ or to $\mathbb{C}$. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the real embeddings of $\mathbb{Q}(\alpha)$ and $\sigma_{r+1}, \overline{\sigma}_{r+1}, \sigma_{r+2}, \overline{\sigma}_{r+2}, \ldots, \sigma_s, \overline{\sigma}_s$ its complex embeddings. Then,

$$\prod_{v \in \mathrm{M}^{\infty}_{\mathbb{Q}(\alpha)}} \max\{1 \|\alpha\|_v\} = \prod_{i=1}^{r} \max\{1, |\sigma_i(\alpha)|\} \prod_{i=r+1}^{s} \max\{1, |\sigma_i(\alpha)|^2\}.$$

But this is exactly the Mahler measure of the normalized minimal polynomial of α, let f. So,

$$\prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)}} \max\{1, \|\alpha\|_v\} = \prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)} \smallsetminus \mathrm{M}^{\infty}_{\mathbb{Q}(\alpha)}} \max\{1, \|\alpha\|_v\} \prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)}} \max\{1, \|\alpha\|_v\} = \mu(f)$$

$$= H(\alpha)^{\deg(f)} = H(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}]} \Rightarrow H(\alpha) = \left(\prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)}} \max\{1, \|\alpha\|_v\} \right)^{\frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]}}.$$

We showed the desired result in the case of $K = \mathbb{Q}(\alpha)$, where α is an algebraic integer. We will prove now the theorem in the case of algebraic integer $\alpha \in R_K$, where K is a number field, such that $\mathbb{Q}(\alpha) \leq K$. So

$$\|\alpha\|_v{}^{[K:\mathbb{Q}(\alpha)]} = \prod_{w|v} \|\alpha\|_w.$$

We also recall that

$$\|\alpha\|_v \leq 1 \Leftrightarrow \|\alpha\|_w \leq 1 \ , \ \forall w \mid v.$$

Since $\alpha \in R_K$ and $\mathbb{Q}(\alpha) \leq K$, α is also an algebraic integer of $\mathbb{Q}(\alpha)$ and hence

$$\begin{aligned} H(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}]} &= \prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)}} \max\{1, \|\alpha\|_v\} \\ &= \prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)}} \max \left\{ 1, \left(\prod_{w|v} \|\alpha\|_w \right)^{\frac{1}{[K:\mathbb{Q}(\alpha)]}} \right\} \\ &= \prod_{v \in \mathrm{M}_{\mathbb{Q}(\alpha)}} \prod_{w|v} \max\{1, \|\alpha\|_w\}^{\frac{1}{[K:\mathbb{Q}(\alpha]}} \end{aligned}$$

[7] By $\mathrm{M}^{\infty}_{\mathbb{Q}(\alpha)}$ we denote the archimedean places of $\mathbb{Q}(\alpha)$.

So, we obtain

$$H(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}][K:\mathbb{Q}(\alpha)]} = \prod_{v\in M_{\mathbb{Q}(\alpha)}} \prod_{w|v} \max\{1, \|\alpha\|_w\} = \prod_{w\in M_K} \max\{1, \|\alpha\|_w\}$$

$$\Rightarrow H(\alpha)^{[K:\mathbb{Q}]} = \prod_{w\in M_K} \max\{1, \|\alpha\|_w\}.$$

In order to complete the proof we have to remove the assumption that α is an algebraic integer. To that end we enlarge, if necessary, the field K, so that K is a Galois extension of $\mathbb{Q}$. Then the normalized minimal polynomial of α is of the form

$$f(X)^{[K:\mathbb{Q}(\alpha)]} = a_n{}^{[K:\mathbb{Q}(\alpha]} \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} (X - \sigma(\alpha)) \in \mathbb{Q}[X].$$

Let p be a prime number. Since the g.c.d. of the coefficient of f is equal to 1, we have that $\mathrm{cont}_p(f) := \mathrm{cont}_{|\cdot|_p}(f) = 1$. Consequently,

$$(6)\quad 1 = \mathrm{cont}_p\left(a_n^{[K:\mathbb{Q}(\alpha]} \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} (X - \sigma(\alpha))\right) = |a_n|_p{}^{[K:\mathbb{Q}(\alpha)]} \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} \mathrm{cont}_p(X - \sigma(\alpha)),$$

using the multiplicativity proven in Gauss' lemma (2.13). But

$$\begin{aligned}
\prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} \mathrm{cont}_p(X - \sigma(\alpha)) &= \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} \max\{1, |\sigma(\alpha)|_p\} \\
&= \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} \max\left\{1, \left(\prod_{v|p} \|\sigma(\alpha)\|_v\right)^{\frac{1}{[K:\mathbb{Q}]}}\right\} \\
&= \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} \prod_{v|p} \max\{1, \|\sigma(\alpha)\|_v\}^{\frac{1}{[K:\mathbb{Q}]}} \\
&= \left(\prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} \prod_{v|p} \max\{1, \|\sigma(\alpha)\|_v\}\right)^{\frac{1}{[K:\mathbb{Q}]}}. \\
&= \left(\prod_{v|p} \prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} \max\{1, \|\sigma(\alpha)\|_v\}\right)^{\frac{1}{[K:\mathbb{Q}]}} \\
&= \prod_{v|p} \max\{1, \|\alpha\|_v\}.
\end{aligned}$$

The last equality is immediate by the identification of the norms $\|\sigma(\alpha)\|_{\sigma(v)} := \|\alpha\|_v$, for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ (see more on Appendix A). And so by (6), we have

$$|a_n|_p{}^{[K:\mathbb{Q}(\alpha)]} = \left(\prod_{v|p} \max\{1, \|\alpha\|_v\}\right)^{-1}.$$

According to the product formula, we have

$$|a_n| \prod_{p \text{ prime}} |a_n|_p = 1 \Rightarrow a_n = \prod_{p \text{ prime}} \frac{1}{|a_n|_p} = \prod_{p \text{ prime}} \prod_{v|p} \max\{1, \|\alpha\|_v\}^{\frac{1}{[K:\mathbb{Q}(\alpha)]}}$$

$$= \left(\prod_{v \in \mathrm{M}_K \setminus \mathrm{M}_K^\infty} \max\{1, \|\alpha\|_v\} \right)^{\frac{1}{[K:\mathbb{Q}(\alpha)]}} \Rightarrow a_n{}^{[K:\mathbb{Q}(\alpha)]} = \prod_{v \in \mathrm{M}_K \setminus \mathrm{M}_K^\infty} \max\{1, \|\alpha\|_v\}.$$

Since the Mahler measure is multiplicative, by the form of f we obtain

$$\mu(f)^{[K:\mathbb{Q}(\alpha)]} = a_n{}^{[K:\mathbb{Q}(\alpha)]} \prod_{v \in \mathrm{M}_K^\infty} \max\{1, \|\alpha\|_v\}$$

$$\Rightarrow \left(H(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}]} \right)^{[K:\mathbb{Q}(\alpha)]} = \prod_{v \in \mathrm{M}_K \setminus \mathrm{M}_K^\infty} \max\{1, \|\alpha\|_v\} \prod_{v \in \mathrm{M}_K^\infty} \max\{1, \|\alpha\|_v\}$$

$$\Rightarrow H(\alpha)^{[K:\mathbb{Q}]} = \prod_{v \in \mathrm{M}_K} \max\{1, \|\alpha\|_v\}.$$

□

Definition 2.15. Let α be an algebraic number. We call the number $H(\alpha)$, which we defined in 2.10, *the global absolute height of* α, or just, *the height of* α. Furthermore, we define *the local K-height of* α by

$$H_{K,v}(\alpha) = \max\{1, \|\alpha\|_v\},$$

where $v \in \mathrm{M}_K$, and the *global K-height of* α by

$$H_K(\alpha) = \prod_{v \in \mathrm{M}_K} \max\{1, \|\alpha\|_v\} = \prod_{v \in \mathrm{M}_K} H_{K,v}(\alpha).$$

Remark 2.16. By the definition of the global K-height and the decomposition formula (2.14), we have that

$$H_K(\alpha) = H(\alpha)^{[K:\mathbb{Q}]}.$$

2.3. Heights on projective spaces. Since elliptic curves are objects in the projective space, we have to extend the definition of the height.

Definition 2.17. Let K be a number field and $\mathbb{P}^n(K)$ its $(n+1)$-dimensional projective space. For the point $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(K)$ and some $v \in \mathrm{M}_K$ we define *the local K-height of P* by

$$H_{K,v}(P) := \max_{0 \le j \le n} \{\|x_j\|_v\},$$

the global K-height of P by

$$H_K(P) := \prod_{v \in \mathrm{M}_K} \max_{0 \le j \le n} \{\|x_j\|_v\} = \prod_{v \in \mathrm{M}_K} H_{K,v}(P)$$

and *the global absolute height of P*, or just, *the height of P*, by

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

We also define *the absolute logarithmic height of P*, or simply, *the logarithmic height of P*, by

$$h(P) := \log\left(H(P)\right).$$

Corollary 2.18. *According to the definition 2.17 for the point $P \in \mathbb{P}^n(K)$ we obtain the following results:*

(i) The global K-height of P is independent of the choice of homogeneous coordinates.
(ii) If L/K is a finite extension, then for the heights of the point P we have

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

Proof. (i) We choose two different expressions $[a_0 : a_1 : \cdots : a_n]$ and $[b_0 : b_1 : \cdots : b_n]$ for P. Then, there exists $\lambda \in K^{\times}$, such that

$$a_i = \lambda b_i \quad , \quad \forall\, i \in \{0, 1, \ldots, n\}.$$

Then we have

$$H_K([a_0 : a_1 : \cdots : a_n]) = \prod_{v \in \mathrm{M}_K} \max_{0 \le j \le n} \{\|a_j\|_v\} = \prod_{v \in \mathrm{M}_K} \max_{0 \le j \le n} \{\|\lambda b_j\|_v\}$$

$$= \prod_{v \in \mathrm{M}_K} \max_{0 \le j \le n} \{\|\lambda\|_v \|b_j\|_v\} = \prod_{v \in \mathrm{M}_K} \|\lambda\|_v \max_{0 \le j \le n} \{\|b_j\|_v\} = \prod_{v \in \mathrm{M}_K} \|\lambda\|_v \prod_{v \in \mathrm{M}_K} \max_{0 \le j \le n} \{\|b_j\|_v\}$$

By the product formula we have that

$$\prod_{v \in \mathrm{M}_K} \|\lambda\|_v = 1,$$

and so

$$= \prod_{v \in \mathrm{M}_K} \max_{0 \le j \le n} \{\|b_j\|_v\} = H_K([a_0 : a_1 : \cdots : a_n]).$$

(ii) It is immediate by the theorem 2.14 and the multiplicativity of the degree of field extensions.

□

Remark 2.19. We assume now that $\alpha \in K$. We observe that

$$H(\alpha) = H([\alpha : 1]),$$

where $[\alpha : 1] \in \mathbb{P}^1(K)$. This means that we could start by examining the heights on projective spaces and extending to the heights on number fields, without using the Mahler measure.

Proposition 2.20. *Let*

$$f(X) = a_0 + a_1 X + \cdots + a_d X^d = a_d \prod_{i=1}^{d} (X - \alpha_i) \in \bar{\mathbb{Q}}[X].$$

Then

$$2^{-d} \prod_{i=1}^{d} H(\alpha_i) \le H([a_0 : a_0 : \cdots : a_d]) \le 2^d \prod_{i=1}^{d} H(\alpha_i).$$

Proof. Without loss of generality we assume that $a_d = 1$. Let $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_d)$. In order to prove the desired inequality we must show for any $v \in \mathrm{M}_K$, that

$$2^{-d} \prod_{i=1}^{n} \max\{1, \|\alpha_i\|_v\} \leq \max_{0\leq j\leq d}\{\|a_j\|_v\} \leq 2^d \prod_{i=1}^{d} \max\{1, \|\alpha_i\|_v\}. \tag{7}$$

We will prove (7) using induction on the degree d. For $d = 1$ the desired inequality holds trivially. We assume that (7) holds for every polynomial of degree $\leq d-1$, with roots that belong in K. Let

$$f(X) = a_0 + a_1 X + \cdots + X^d = \prod_{i=1}^{d}(X - \alpha_i) \in \bar{\mathbb{Q}}[X].$$

Let also $k \in \{1, 2, \ldots, d\}$ such that

$$\|\alpha_k\| \geq \|\alpha_j\| \quad , \quad \forall j \in \{1, 2, \ldots, d\}.$$

We define the polynomial

$$g(X) := \frac{f(X)}{X - \alpha_k} = b_0 + b_1 X + \cdots + b_{d-2}X^{d-2} + X^{d-1}.$$

Then

$$f(X) = g(X)(X - \alpha_k).$$

Therefore,

$$a_i = b_{i-1} - \alpha_k b_i \quad , \quad \forall\, i \in \{1, 2, \ldots, d\},$$

where we set $b_{-1} := 0$ and $b_{n-1} := 1$. If

$$\varepsilon(v) = \begin{cases} 2 & \text{, if } v \in \mathrm{M}_K^\infty, \\ 1 & \text{, if otherwise} \end{cases},$$

then

$$\begin{aligned} \max_{0\leq j\leq d}\{\|\alpha_j\|_v\} &= \max_{0\leq j\leq d}\{\|b_{j-1} - \alpha_k b_j\|_v\} \leq \varepsilon(v) \max_{0\leq j\leq d}\{\|b_{j-1}\|_v, \|\alpha_k b_j\|_v\} \\ &\leq \varepsilon(v) \max_{0\leq j\leq d}\{\|b_j\|_v\} \max\{1, \|\alpha_k\|_v\} \\ &\leq \varepsilon(v)^{d-1} \prod_{\substack{i=1 \\ i\neq k}}^{d} \max\{1, \|\alpha_i\|_v\} \cdot \varepsilon(v) \max\{1, \|\alpha_k\|_v\} \leq 2^d \prod_{i=1}^{d} \max\{1, \|\alpha_i\|_v\}, \end{aligned}$$

where for the last step we used the induction's hypothesis. Now, it remains to prove that

$$2^{-d} \prod_{i=1}^{d} \max\{1, \|\alpha_i\|_v\} \leq \max_{0\leq j\leq d}\{\|\alpha_j\|_v\}.$$

We consider two cases.

- If $\|\alpha_k\| \leq 2$, then

$$\prod_{i=1}^{d} \max_{0\leq j\leq d}\{1, \|\alpha_j\|_v\} \leq \max\{1, \|\alpha_k\|_v\}^d \leq 2^d$$

$$\Rightarrow 2^{-d}\prod_{i=1}^{d}\max_{0\leq j\leq d}\{1, \|\alpha_j\|_v\} \leq 1 \leq \|\alpha_k\|_v = \max_{0\leq j\leq d}\{\|\alpha_j\|_v\}.$$

- Let $\|\alpha_k\| > 2$. We set $\|b_t\|_v = \max_{0\leq i\leq d-1}\{\|b_i\|_v\}$, for some $t \in \{0, 1, \ldots, d-1\}$, and so we obtain that

$$\begin{aligned}\max_{0\leq j\leq d}\{\|\alpha_j\|_v\} &= \max_{0\leq j\leq d}\{\|b_{j-1} - \alpha_k b_j\|_v\} \geq \|b_{t-1} - \alpha_k b_t\|_v \\ &\geq \|\alpha_k b_t\|_v - \|b_{t-1}\|_v \geq (\|\alpha_k\|_v - 1)\|b_t\|_v \\ &\geq \frac{\|\alpha_k\|_v}{2}\|b_t\|_v\end{aligned}$$

Using the induction's hypothesis for g, we obtain

$$\|b_t\|_v = \max_{0\leq i\leq d-1}\{\|b_i\|_v\} \geq 2^{-(d-1)}\prod_{\substack{i=1\\ i\neq k}}^{d}\max\{1, \|\alpha_i\|_v\}.$$

Hence,

$$\max_{0\leq j\leq d}\{\|\alpha_j\|_v\} \geq \frac{\|\alpha_k\|_v}{2}\cdot 2^{-(d-1)}\prod_{\substack{i=1\\ i\neq k}}^{d}\max\{1, \|\alpha_i\|_v\} = 2^{-d}\prod_{i=1}^{d}\max\{1, \|\alpha_i\|_v\}.$$

□

Theorem 2.21. *Let B and D be positive constants. Then the set*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) \mid H(P) \leq B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\},$$

is finite. Particularly, the set

$$\{P \in \mathbb{P}^n(K) \mid H(P) \leq B\},$$

where K is a number field, is finite.

Proof. We choose the homogeneous coordinates of $P = [x_0 : x_1 : \cdots : x_n]$ so that at least one of x_i's is equal to 1. Then, for every $v \in \mathbb{P}^n(\mathbb{Q}(P))$, we have

$$\max_{0\leq j\leq n}\{\|x_j\|_v\} \geq \max\{1, \|x_i\|_v\} \quad , \quad \forall i \in \{0, 1, \ldots, n\}.$$

Equivalently,

$$H_{\mathbb{Q}(P),v}(P) \geq H_{\mathbb{Q}(P),v}([1 : x_i]) \Rightarrow H(P) \geq H([1 : x_i]) = H(x_i) \quad , \quad \forall i \in \{0, 1, \ldots, n\}.$$

It is obvious that $\mathbb{Q}(x_i) \leq \mathbb{Q}(P)$, for every $i \in \{0, 1, \ldots, n\}$, and so it suffices to prove that the set

$$\Sigma_d := \{x \in \bar{\mathbb{Q}} \mid H(x) \leq B \text{ and } [\mathbb{Q}(x_i) : \mathbb{Q}] = d\},$$

is finite for every $1 \leq d \leq D$. Let $x \in \bar{\mathbb{Q}}$ of degree d and $K = \mathbb{Q}(x)$. If f is the normalized minimal polynomial[8] of x, then it is of the form

$$f(T) = a_0 + a_1 T + \cdots + a_{d-1}T^{d-1} + T^d \in \mathbb{Z}[T].$$

[8] Here the normalized minimal polynomial coincides with the irreducible polynomial, and so it is monic.

By norm inequality, for the coefficients of f we have

$$|a_j| \leq \binom{d}{j}\mu(f) = \binom{d}{j}H(x)^d \quad , \quad \forall\, j \in \{0, 1, \ldots, d-1\}.$$

Assuming that $x \in \Sigma_d$, we obtain that

$$|a_j| \leq \binom{d}{j}B^d \quad , \quad \forall\, j \in \{0, 1, \ldots, d-1\}.$$

Thus, for every coefficient of f we have finite possible values. In other words, x is a root of a polynomial, the coefficients of which are elements of a finite set. Therefore, there are finitely many x's, such that $H(x) \leq B$ and $[\mathbb{Q}(x) : \mathbb{Q}] = d$, for $1 \leq d \leq D$, fact that completes our proof. □

REMARK 2.22. We will restate Kronecker's theorem in a projective version. This result gives us an explicit description of the projective points of height 1 and it is a consequence of theorem 2.21.

COROLLARY 2.23 (KRONECKER). *Let K be a number field and $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(K)$. Let also $k \in \{0, 1, \ldots, n\}$, such that $x_k \neq 0$. Then $H(P) = 1$ if, and only if either $\dfrac{x_i}{x_k}$ is a root of unity, or $x_i = 0$, for every $i \in \{0, 1, \ldots, n\} \setminus \{k\}$.*

DEFINITION 2.24. *A morphism F of degree d* is a map between projective spaces, of the form

$$\begin{aligned} F \; : \; & \mathbb{P}^n(\bar{\mathbb{Q}}) \longrightarrow \mathbb{P}^m(\bar{\mathbb{Q}}) \\ & P \longmapsto [f_0(P) : f_1(P) : \cdots : f_m(P)], \end{aligned}$$

where $f_0, f_1, \ldots, f_m \in \bar{\mathbb{Q}}[X_0, X_1, \ldots, X_n]$ are homogeneous polynomials, of degree d, with no (non trivial) common zeros in $\bar{\mathbb{Q}}^n$. In case $f_0, f_1, \ldots, f_m \in K[X_0, X_1, \ldots, X_n]$, we say that the morphism F is *defined over K*.

DEFINITION 2.25. We define *the content of the morphism $F : \mathbb{P}^n(\bar{\mathbb{Q}}) \longrightarrow \mathbb{P}^m(\bar{\mathbb{Q}})$ at v*, where $F(P) = [f_0(P) : f_1(P) : \cdots : f_m(P)]$ and $v \in \mathrm{M}_K$, by

$$\begin{aligned} \mathrm{cont}_v(F) \; &:= \; \max\{|a|_v : a \text{ is a coefficient of some } f_i\} \\ &= \; \max\{\mathrm{cont}_v(f_i) : i \in \{0, 1, \ldots, m\}\}. \end{aligned}$$

PROPOSITION 2.26. *Let $F : \mathbb{P}^n(\bar{\mathbb{Q}}) \longrightarrow \mathbb{P}^m(\bar{\mathbb{Q}})$ be a morphism of degree d. Then there are constants $c_1, c_2 > 0$, depending on F, such that*

$$c_1 H(P)^d \leq H(F(P)) \leq c_2 H(P)^d \quad , \quad \forall\, P \in \mathbb{P}^n(\bar{\mathbb{Q}}).$$

PROOF. Let $P = [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$ and $F = [f_0 : f_1 : \cdots : f_m]$, where $f_0, f_1, \ldots, f_m \in \mathbb{P}^m(\bar{\mathbb{Q}})$ are homogeneous polynomials of degree d. We choose an algebraic number field K, which contains all the coordinates of P and the all the coefficients of the polynomials f_i. We set

$$\epsilon(v) = \begin{cases} 1 & , \text{if } v \in \mathrm{M}_K^\infty \\ 0 & , \text{otherwise} \end{cases}.$$

Using this function, we are able to concisely write the triangle inequality

$$\|t_1 + t_2 + \cdots + t_n\|_v \leq n^{\epsilon(v)} \max\{\|t_1\|_v, \|t_2\|_v, \ldots, \|t_n\|_v\},$$

for every $v \in \mathrm{M}_K$. After all these preliminaries it is easy to compute an upper bound for $H(F(P))$. We have

$$\|f_i(P)\|_v \leq {C_{2,i}}^{\epsilon(v)}\mathrm{cont}_v(F)H_{K,v}(P)^d \quad , \quad \forall\, i \in \{0, 1 \ldots, m\}.$$

The constant $C_{2,i}$ is equal to the number of monomials of f_i. Indeed, assuming that

$$f_i(X_0, X_1, \ldots, X_n) = \sum_{j=0}^{m} a_{ij}{X_0}^{d_{0,j}}{X_1}^{d_{1,j}}\cdots{X_m}^{d_{m,j}},$$

where $d_{0,j} + d_{1,j} + \cdots + d_{m,j} = d$ for every $j \in \{0, 1, \ldots, n\}$, we obtain that

$$\begin{aligned}
\|f_i(P)\|_v &= \left\|\sum_{j=0}^{m} a_{ij}{x_0}^{d_{0,j}}{x_1}^{d_{1,j}}\cdots{x_m}^{d_{m,j}}\right\|_v \\
&\leq {C_{2,i}}^{\epsilon(v)} \max_{0\leq j\leq n}\left\{\left\|a_{ij}{x_0}^{d_{0,j}}{x_1}^{d_{1,j}}\cdots{x_m}^{d_{m,j}}\right\|_v\right\} \\
&\leq {C_{2,i}}^{\epsilon(v)} \max_{\substack{0\leq i\leq n\\ 0\leq j\leq m}}\{\|a_{ij}\|_v\}\cdot\max_{0\leq j\leq m}\{\|x_j\|_v\} \\
&= {C_{2,i}}^{\epsilon(v)}\mathrm{cont}_v(F)H_{K,v}(P)^d.
\end{aligned}$$

Let

$$C_2 = \max\{C_{2,i},\ i \in \{0, 1, \ldots, n\}\}$$

Then

$$\|f_i(P)\|_v \leq {C_2}^{\epsilon(v)}\mathrm{cont}_v(F)H_{K,v}(P)^d \quad , \quad \forall\, i \in \{0, 1, \ldots, n\}$$
$$\Rightarrow \max_{0\leq i\leq n}\{\|f_i(P)\|_v\} \leq {C_2}^{\epsilon(v)}\mathrm{cont}_v(F)H_{K,v}(P)^d \quad , \quad \forall\, i \in \{0, 1, \ldots, n\}.$$

Ans so,

$$H_{K,v}(F(P)) \leq {C_2}^{\epsilon(v)}\mathrm{cont}_v(F)H_{K,v}(P)^d.$$

Finally, setting $c_2 := {C_2}^{\epsilon(v)}\mathrm{cont}_v(F)$, we have

$$H_{K,v}(F(P)) \leq c_2 H_{K,v}(P)^d.$$

Therefore, changing the constant c_2 if necessary, we obtain the inequality

$$H(F(P)) \leq c_2 H(P)^d.$$

We turn now to the proof of the lower bound of $H(F(P))$. Observe that for the upper bound we did not use the fact that the f_i's have no nontrivial common roots. Let

$$I = \langle f_0, f_1, \ldots, f_m\rangle \trianglelefteq K[X_0, X_1, \ldots, X_n]$$

Then

$$(0, 0, \ldots, 0) \in \mathbf{V}(I),$$

where by $\mathbf{V}(I)$ we denote the set of zeros of all polynomials of I Thus,

$$X_i \in \mathbf{I}(\mathbf{V}(I)) \quad , \quad \forall\, i \in \{0, 1, \ldots, n\}.$$

By Nullstellensatz of Hilbert we know that

$$\mathbf{I}(\mathbf{V}(I)) = \mathrm{Rad}(I),$$

where by $\mathbf{I}(\mathbf{V}(I))$ we denote the vanishing ideal of $\mathbf{V}(I)$ and by $\mathrm{Rad}(I)$ we denote the radical ideal of I. That means that

$$\exists\, e \in \mathbb{N} : {X_i}^e \in I \quad , \quad \forall\, i \in \{0, 1, \dots, n\}.$$

And so

$${X_i}^e = \sum_{j=0}^{m} g_{ij}(X_0, X_1, \dots, X_n) f_j(X_0, X_1, \dots, X_n) \quad , \quad \forall\, i \in \{0, 1, \dots, n\}.$$

Enlarging the field K if necessary, we assume that $g_{ij} \in K[X_0, X_1, \dots, X_n]$. We can also assume that each g_{ij} is homogeneous polynomial of degree $e-d$. We observe that the numbers e and

$$\mathrm{cont}_v(G) := \prod_{v \in \mathrm{M}_K} \max\{\|b\|_v : b \text{ is a coefficient of some } g_{ij}\}$$

are bounded in terms of m, n, d and $\mathrm{cont}_v(F)$. So, recalling that $P = [x_0 : x_1 : \cdots : x_n]$, we have

$$\begin{aligned} \|x_i\|_v{}^e = \left\| \sum_{j=0}^{m} g_{ij}(P) f_j(P) \right\|_v &\leq {c_2}^{\epsilon(v)} \max_{0 \leq j \leq m} \{\|g_{ij}(P) f_j(P)\|_v\} \\ &\leq {c_2}^{\epsilon(v)} \max_{0 \leq j \leq m} \{\|g_{ij}(P)\|_v\} H_{K,v}(F(P)). \end{aligned}$$

Hence, we obtain

$$(8) \qquad H_{K,v}(P)^e = \max_{0 \leq i \leq n} \{\|x_i\|_v\} \leq {c_2}^{\epsilon(v)} \max_{(i,j) \in \{0,1,\dots,n\} \times \{0,1,\dots,m\}} \{\|g_{ij}(P)\|_v\} \cdot H_{K,v}(F(P)).$$

We apply the triangle's inequality for the polynomials g_{ij}, ans so we have

$$(9) \qquad \|g_{ij}(P)\|_v \leq {c_3}^{\epsilon(v)} \max\{\|b\|_v : b \text{ is a coefficient of some } g_{ij}\} H_{K,v}(P)^{e-d},$$

where c_3 is a constant that may depend on e, but as we mentioned before e is bounded. Substituting the relation (9) to (8), it follows that

$$H_{K,v}(P)^d \leq C^{\epsilon(v)} \max\{\|b\|_v : b \text{ is a coefficient of some } g_{ij}\} H_{K,v}(F(P)),$$

for some constant C. Setting

$$\frac{1}{c_1} := C^{\epsilon(v)} \max\{\|b\|_v : b \text{ is a coefficient of some } g_{ij}\},$$

we conclude that

$$c_1 H_{K,v}(P)^d \leq H_{K,v}(F(P)),$$

and so the result follows. □

2.4. Heights on elliptic curves. Every elliptic curve E, defined over a number field K, is determined by an equation of the form

$$Y^2 = X^3 + \alpha X + \beta \quad , \quad \alpha, \beta \in K.$$

Viewing E as a projective plane curve, the abelian group $E(\bar{K})$, where $\bar{K}$ is the algebraic closure of K, of the points of E has the following form

$$E(\bar{K}) = \left\{ [x : y : 1] \in \mathbb{P}^2(\bar{K}) \mid y^2 = x^3 + \alpha x + \beta \right\} \cup \{[0 : 1 : 0]\}.$$

The height of $O = [0 : 1 : 0]$ is defined to be equal to 1. Let $[x : y : 1] \in E(\bar{\mathbb{Q}}(x,y))$. Then the height of P is given by

$$H(P) = \left(\prod_{v \in \mathrm{M}_{\mathbb{Q}(x,y)}} \max\{\|x\|_v, \|y\|_v, 1\} \right)^{\frac{1}{[\mathbb{Q}(x,y):\mathbb{Q}]}}.$$

But for given x, we obtain two possible values for y by the equation $y^2 = x^3 + \alpha x + \beta$, which are actually opposite numbers and so their valuations are the same. In other words, for every $v \in \mathrm{M}_{K_1}$, the number $\|y\|_v$ is uniquely determined by the choice of the first coordinate x. This observation leads to the following definition.

Definition 2.27. Let E be an elliptic curve defined over the number field K, $P = [x : y : z] \in E(\bar{K})$ and $\mathbb{Q}(P)$ be the minimal extension of $\mathbb{Q}$ containing the coordinates of P. We define the *height of P on E* to be the number

$$H_E(P) := \left(\prod_{v \in \mathrm{M}_{\mathbb{Q}(P)}} \max\{1, \|x\|_v\} \right)^{\frac{1}{[\mathbb{Q}(P):\mathbb{Q}]}}.$$

Furthermore, we define *the logarithmic height of P on E* by the equation

$$h_E(P) := \log\left(H_E(P)\right).$$

Of course, we define $H_E(O) = 1$ and so $h_E(O) = 0$.

The following proposition reminds us the parallelogram law. Indeed, we prove that up to an error, the height of a point on an elliptic curve is a quadratic form.

Proposition 2.28. *Let E be an elliptic curve over the number field K. There are constants $C_1, C_2 \in \mathbb{R}$, depending only on E, such that for all $P, Q \in E(\bar{K})$, it holds that*

$$2h_E(P) + 2h_E(Q) - c_1 \leq h_E(P+Q) + h_E(P-Q) \leq 2h_E(P) + 2h_E(Q) + c_2.$$

Proof. We assume that the elliptic curve is of the form

$$E|_K : Y^2 = X^3 + \alpha X + \beta,$$

where $\alpha, \beta \in K$. At first, we observe that $h(O) = 0$ and $h(-P) = h(P)$, for any $P \in E(\bar{K})$. We define the map

$$\begin{aligned} x \ : \ \mathbb{P}^2(\bar{K}) &\longrightarrow \mathbb{P}^1(\bar{K}) \\ P &\longmapsto [x_P : 1], \end{aligned}$$

where $P = [x_p : y_p : z_p]$, and let

$$x(P) = [x_1 : 1] \quad , \quad x(Q) = [x_2 : 1] \quad , \quad x(P+Q) = [x_3 : 1] \quad , \quad x(P-Q) = [x_4 : 1].$$

Here $P \pm Q$ may be equal to the point at infinity, if $P = \pm Q$. By the addition law for points on E, follows that

$$x_3 + x_4 = \frac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2}$$

and

$$x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1x_2}.$$

We define the map

$$\begin{aligned} g \;:\; & \mathbb{P}^2(\bar{K}) \longrightarrow \mathbb{P}^2(\bar{K}) \\ & [t:u:v] \longmapsto [u^2-4tv : 2u(At+v)+4Bt^2 : (v-At)^2-4Btu]. \end{aligned}$$

and the map $\sigma : E(\bar{K}) \longrightarrow E(\bar{K})$ as the composition of the maps

$$\begin{aligned} E(\bar{K}) \times E(\bar{K}) &\longrightarrow \mathbb{P}^1(\bar{K}) \times \mathbb{P}^1(\bar{K}) \\ (P,Q) &\longmapsto (x(P), x(Q)), \end{aligned}$$

and[9]

$$\begin{aligned} \mathbb{P}^1(\bar{K}) \times \mathbb{P}^1(\bar{K}) &\longrightarrow \mathbb{P}^2(\bar{K}) \\ ([a_1:b_1],[a_2:b_2]) &\longmapsto [b_1b_2 : a_1b_2+a_2b_1 : a_1a_2] \end{aligned}$$

Furthermore, we define the map

$$\begin{aligned} G \;:\; & E(\bar{K}) \times E(\bar{K}) \longrightarrow E(\bar{K}) \times E(\bar{K}) \\ & (P,Q) \longmapsto (P+Q, P-Q) \end{aligned}$$

Then the diagram

$$\begin{tikzcd} E(\bar{K}) \times E(\bar{K}) \arrow[r, "G"] \arrow[d] \arrow[dd, bend right, "\sigma"'] & E(\bar{K}) \times E(\bar{K}) \arrow[d] \arrow[dd, bend left, "\sigma"] \\ \mathbb{P}^1(\bar{K}) \times \mathbb{P}^1(\bar{K}) \arrow[d] & \mathbb{P}^1(\bar{K}) \times \mathbb{P}^1(\bar{K}) \arrow[d] \\ \mathbb{P}^2(\bar{K}) \arrow[r, "g"'] & \mathbb{P}^2(\bar{K}) \end{tikzcd}$$

easily follows that is commutative, i.e.

$$g \circ \sigma = \sigma \circ G.$$

Our next step is to prove that g is a morphism. Obviously, every coordinate of g is a homogeneous polynomial of degree 2. So, it suffices to show that

$$\begin{cases} u^2-4tv = 0 \\ 2u(At+v)+4Bt^2 = 0 \\ (v-At)^2-4Btu = 0 \end{cases} \Rightarrow t = u = v = 0.$$

If $t = 0$, it is easy to prove that $u = v = 0$. If otherwise, let $x := \frac{u}{2t}$. Then using the first equation of the system it follows that

$$x^2 = \frac{v}{t}.$$

Thus, we obtain that

$$2u(At+v)+4Bt^2 = 0 \Rightarrow 4x(A+x^2)+4B = 4x^3+4Ax+4B = 0$$

and

$$(v-At)^2-4Btu = 0 \Rightarrow (x^2-A)^2-8Bx = x^4-2Ax^2-8Bx+A^2 = 0.$$

[9] This is a natural way to map a product of projective spaces to a projective space of greater dimension. Actually this map is a special case of the so called Veronese map.

Let

$$\psi_1(X) := 4X^3 + 4AX + 4B \quad \text{and} \quad \psi_2(X) := X^4 - 2AX^2 - 8BX + A^2.$$

An easy calculation shows that

$$(12X^2 + 16A)\psi_2(X) - (3X^3 - 5AX - 27B)\psi_1(X) = 4(4A^3 + 27B^2) \neq 0.$$

This means that ψ_1 and ψ_2 have no common roots. So g is a morphism indeed. By the commutativity of the diagram we have

$$h(\sigma(P+Q, P-Q)) = h\big((\sigma \circ G)(P,Q)\big) = h\big((g \circ \sigma)(P,Q)\big).$$

According to the proposition 2.26 we know that

$$c_1 H(\sigma(P,Q))^2 \leq H(g(\sigma(P,Q))) \leq c_2 H(\sigma(P,Q))^2$$

$$\Rightarrow 2h(\sigma(P,Q)) + c_1 \leq h(g(\sigma(P,Q))) \leq 2h(\sigma(P,Q)) + c_2$$

$$\Rightarrow 2h(\sigma(P,Q)) + c_1 \leq h\big((g \circ \sigma)(P,Q)\big) \leq 2h(\sigma(P,Q)) + c_2, \tag{10}$$

for some positive constants c_1 and c_2. We will prove now that

$$h(x(P_1)) + h(x(P_2)) + \tilde{c_1} \leq h(\sigma(P_1,P_2)) \leq h(x(P_1)) + h(x(P_2)) + \tilde{c_2}, \tag{11}$$

for $P_1, P_2 \in E(\bar{K})$ and some positive constants $\tilde{c_1}$ and $\tilde{c_2}$. It is easy to verify that if $P_1 = O$, or $P_2 = O$, then

$$h(\sigma(P_1,P_2)) = h(x(P_1)) + h(x(P_2)),$$

which is stronger than the desired inequality. If otherwise, we assume that

$$x(P_1) = [a_1 : 1] \quad \text{and} \quad x(P_2) = [a_2 : 1],$$

and so

$$\sigma(P_1,P_2) = [1 : a_1 + a_2 : a_1a_2] \Rightarrow h(\sigma(P_1,P_2)) = h([1 : a_1 + a_2 : a_1a_2]).$$

Consider the polynomial $f(X) = (X + a_1)(X + a_2) \in \bar{K}[X]$. Then by proposition 2.20 we obtain that

$$\frac{1}{4}H(a_1)H(a_2) \leq H([1 : a_1 + a_2 : a_1a_2]) \leq 4H(a_1)H(a_2) \Rightarrow$$

$$h(a_1) + h(a_2) - \log 4 \leq h([1 : a_1 + a_2 : a_1a_2]) \leq h(a_1) + h(a_2) + \log 4.$$

Hence, we proved (11)[10]. Since

$$h(x(P)) = h([x_P : 1]) = h_E(P),$$

we are able to rewrite equation (11) in the form

$$h_E(P_1) + h_E(P_2) + \tilde{c_1} \leq h(\sigma(P_1,P_2)) \leq h_E(P_1) + h_E(P_2) + \tilde{c_2}.$$

Consequently, applying for $P_1 = P + Q$ and $P_2 = P - Q$, we have

$$\begin{array}{rcl} h_E(P+Q) + h_E(P-Q) & \leq & h(\sigma(P+Q, P-Q)) - \tilde{c_1} \\ & = & h(\sigma(G(P,Q))) - \tilde{c_1} \\ & \leq & c_2 + 2h(\sigma(P,Q)) - \tilde{c_1} \\ & \leq & 2(h_E(P) + h_E(Q) + \tilde{\tilde{c_2}}) + c_2 - \tilde{c_1} \\ & = & 2h_E(P) + 2h_E(Q) + C_1, \end{array}$$

[10] Remember that $H(a) = H([a : 1])$.

where $C_1 := 2\tilde{\tilde{c}}_2 + c_2 - \tilde{c}_1$. Similarly, we prove the other half of the desired inequality. □

The next result is significant for the proof of the Mordell-Weil theorem. It states the three necessary properties that the function h_E must have, in order to complete the proof of Mordell-Weil theorem. In the literature it is also referred as descent theorem.

Theorem 2.29. *Let E be an elliptic curve over the number field K.*

(i) Let $Q \in E(K)$. There exists a constant $C_1 = C_1(E, Q)$, such that for all $P \in E(K)$ it holds that
$$h_E(P+Q) \leq 2h_E(P) + C_1.$$
(ii) For each $m \in \mathbb{Z}$ there exists a constant $C_2 = C_2(E, m) \geq 0$, such that for all $P \in E(K)$ we have
$$h_E(mP) \geq m^2 h_E(P) - C_2.$$
(iii) For every constant $C_3 \in \mathbb{R}_{>0}$ the set
$$\{P \in E(K) \mid h_E(P) \leq C_3\}$$
is finite.

Proof. (i) We have
$$h_E(P+Q) \leq h_E(P+Q) + h_E(P-Q) \leq 2h_E(P) + c_2,$$
using the notation of 2.28. The result now is immediate if we set $C_1 := 2h_E(Q) + c_2$.

(ii) We will prove a stronger result. Particularly, we will show that
$$m^2 h_E(P) - C_2 \leq h_E(mP) \leq m^2 h_E(P) + C_2.$$
We will prove these estimates by induction for $m \in \mathbb{N}_0$. For $m = 0$ and $m = 1$, the result is trivial. Let $m \geq 2$. By proposition 2.28, we have
$$\begin{aligned} 2h_E(mP) + 2h_E(P) - c_1 \leq h_E((m-1)P) + h_E((m+1)P) \leq 2h_E(mP) + 2h_E(P) + c_2 \\ \Rightarrow -h_E((m-1)P) + 2h_E(mP) + 2h_E(P) - c_1 \leq h_E((m+1)P) \\ \leq -h_E((m-1)P) + 2h_E(mP) + 2h_E(P) + c_2 \end{aligned}$$
Using the induction hypothesis we obtain
$$\begin{aligned} h_E((m+1)P) &\geq -h_E((m-1)P) + 2h_E(mP) + 2h_E(P) - c_1 \\ &\geq -(m-1)^2 h_E(P) + 2h_E(P) + 2m^2 h_E(P) \\ &\quad -2c_2(E,m) + c_2(E,m-1) - c_1 \\ &= \left(-(m-1)^2 + 2 + 2m^2\right) h_E(P) + c_2(E,m-1) \\ &\quad -2c_2(E,m) - c_1 \\ &= (m+1)^2 h_E(P) + c_2(E,m-1) - 2c_2(E,m) - c_1 \end{aligned}$$
Similarly, we prove that
$$h_E((m+1)P) \leq (m+1)^2 h_E(P) + c_2(E,m-1) + 2c_2(E,m) + c_1.$$
Setting
$$\begin{aligned} C_2 = C_2(E,m+1) \;:=\; &\max\{0, c_2(E,m-1) + 2c_2(E,m) + c_2, \\ &c_2(E,m-1) - 2c_2(E,m) - c_2\} \end{aligned}$$

we get

$$(m+1)^2 h_E(P) - C_2 \leq h_E((m+1)P) \leq (m+1)^2 h_E(P) + C_2,$$

which is what we need to complete the induction. So we proved our result for $m \geq 0$. For $m < 0$ the result follows immediately, using the relation $h_E(mP) = h_E(-mP)$.

(iii) It suffices to show that the set

$$\{P \in E(K) \mid H_E(P) \leq e^B\}$$

is finite. Let $P = [x_P : y_P : 1] \in E(K)$. Without loss of generality we assume that $P \neq O$. Then for every $v \in \mathrm{M}_{\mathbb{Q}(P)}$ we have

$$\|{y_P}^2\|_v = \|{x_P}^3 + \alpha x_P + \beta\|_v \leq \max\{\|{x_P}^3\|_v, \|\alpha x_P\|_v, \|\beta\|_v\}. \tag{12}$$

Since the height $H_E(P)$ is bounded, then so is $\|x_P\|_v$ for every $v \in \mathrm{M}_{\mathbb{Q}(P)}$. This means that by (12) the $\|y_P\|_v$ is bounded by a positive number which depends on B, for each $v \in \mathrm{M}_{\mathbb{Q}(P)}$. This means that

$$\max\{\|x_P\|_v, \|x_P\|_v, 1\} \leq B' \quad , \quad \forall\, v \in \mathrm{M}_{\mathbb{Q}(P)},$$

where B' is a positive constant, which depends on B. Therefore, the number $H(P)$ is bounded. This means that we have finite choices for P. And so, the desired set is also finite.

□

3. The proof of Mordell-Weil Theorem

We are now in position to prove the Mordell-Weil theorem, which gives us a significant property about the K-rational points of an elliptic curve. In particular, this theorem states that every K-rational point of an elliptic curve can be generated by finite K-rational points.

Proof of 0.1. Since $E(K)/2E(K)$ is finite, as we proved in 1.7, there is a complete system of representatives

$$\{Q_1, Q_2, \cdots, Q_r\}$$

of it. Let $P \in E(K)$. Then

$$P = 2P_1 + Q_{i_1}$$

for some $i_1 \in \{1, 2, \ldots, r\}$ and $P_1 \in E(K)$. Analogously, we write

$$P_1 = 2P_2 + Q_{i_2},$$

for some $i_2 \in \{1, 2, \ldots, r\}$ and $P_2 \in E(K)$. Continuing as above, we obtain the relations

$$P_{j-1} = 2P_j + Q_{i_j},$$

where $P_0 := P$, $i_j \in \{1, 2, \ldots, r\}$ and $P_j \in E(K)$ for each $i \in \{1, 2, \ldots, n\}$ $(n \in \mathbb{N})$. By theorem 2.29 for $m = 2$, we obtain

$$h_E(P_j) \leq \frac{1}{2^2}\Big(h_E(2P_j) + C_2\Big) = \frac{1}{4}\Big(h_E(P_{j-1} - Q_{i_j}) + C_2\Big) \leq \frac{1}{4}\Big(2h_E(P_{j-1}) + C_1 + C_2\Big)$$

$$h_E(P_j) \leq \frac{1}{4}\Big(2h_E(P_{j-1}) + C_1 + C_2\Big),$$

Using this inequality n-times and taking the maximum of all constants that appear, it follows that

$$\begin{aligned} h_E(P_n) &\leq \left(\frac{2}{4}\right)^n h_E(P_0) + \left(\frac{1}{2^2} + \frac{2}{2^4} + \cdots + \frac{2^{n-1}}{2^{2n}}\right) C \\ &< 2^{-n} h_E(P) + 2C, \end{aligned}$$

where C is a constant that depends on E and the points Q_i, with $i \in \{1, 2, \ldots, r\}$. Without loss of generality we assume that n is large enough, so that $2^{-n} h_E(P) \leq 1$. Thus,

$$h_E(P_n) \leq 1 + 2C.$$

And since

$$P_{j-1} = 2P_j + Q_{i_j} \quad , \quad \forall j \in \{1, 2, \ldots, n\},$$

it follows that

$$P = 2^n P_n + \sum_{j=1}^{n} 2^{j-1} Q_{i_j}.$$

This equation states that the every point P may be written as linear combination of the elements of the set

$$\{Q_1, Q_2, \ldots, Q_r\} \cup \{R \in E(K) \mid h_E(R) \leq 1 + 2C\}.$$

The second set of this union is finite according to 2.29. This fact completes the proof. □

We just shown that the abelian group $E(K)$ is finitely generated. Since abelian groups are $\mathbb{Z}$-modules, we shall use the structure theorem of finitely generated modules over principal ideal domains and we obtain the following result.

Corollary 3.1. *Let E be an elliptic curve defined over the number field K. For the group $E(K)$ of the K-rational points of E, we have*

$$E(K) \cong E(K)_{tor} \oplus \mathbb{Z}^r,$$

where by $E(K)_{tor}$ we denote the torsion group of E over K, i.e. the group of all points of finite order, and $r \in \mathbb{N}_0$.

Definition 3.2. Let E be an elliptic curve over the number field E. The nonnegative integer r, that appears in 3.1 is called *rank of the elliptic curve E*, and it is denoted by $\operatorname{rank}(E)$.

CHAPTER 2

Elliptic Curves over the Rationals

The last few decades have witnessed a huge progress in the study of elliptic curves, notably the study of elliptic curves defined over $\mathbb{Q}$. The purpose of this chapter is to present the most important results concerning the study of elliptic curves over the rational numbers.

Due to Mordell's theorem for the group $E(\mathbb{Q})$ of the rational points of the elliptic curve E we have that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r.$$

This means that the problem of the study of $E(\mathbb{Q})$ initially consists in the study of the torsion points and of the rank r of E. We begin with the determination of the group $E(\mathbb{Q})_{\text{tor}}$ and the characterization of the torsion points.

1. Torsion points of $E(\mathbb{Q})$

Two theorems about torsion points are of great significance. We start with the theorem stated independently by Nagell (1935) and Lutz (1937).

Theorem 1.1 (Lutz-Nagell). *Let E be an elliptic curve over the rationals,*

$$E|_{\mathbb{Q}} : Y^2 = X^3 + \alpha X + \beta \quad , \quad \alpha, \beta \in \mathbb{Z}.$$

If P is a nonzero rational point on E of finite order, i.e. if $P = [x_P : y_P : 1] \in E(\mathbb{Q})_{tor}$, then

(i) $x_P, y_P \in \mathbb{Z}$, and
(ii) $y_P = 0$, in case P is a point of order 2, or ${y_P}^2 \mid 4\alpha^3 + 27\beta^2$.

This result does not give information about the structure of $E(\mathbb{Q})_{\text{tor}}$ in general. The major step was done by Mazur in 1977, who determined explicitly the possibilities for the structure of the group $E(\mathbb{Q})_{\text{tor}}$ for any elliptic curve E over the rationals.

Before we state Mazur's theorem let us recall the affine picture of an elliptic curve, assuming that it is defined over the field $\mathbb{R}$.

The affine picture of an elliptic curve has either one, or two connected components, as it is clear by Figure 1. Projectively, we must consider the point at infinity, in which the open-ended component of the elliptic curve is closed up. This, in combination with the fact that elliptic curves, are smooth, means that topologically we get one or two circles. And so, it turns out that the group $E(\mathbb{R})$ of the real points of E is isomorphic either to $\mathbf{S}^1$, or to $\mathbf{S}^1 \oplus \mathbb{Z}/2\mathbb{Z}$. If we ask the same question about the torsion subgroup $E(\mathbb{C})_{\text{tor}}$ of $E(\mathbb{C})$, the

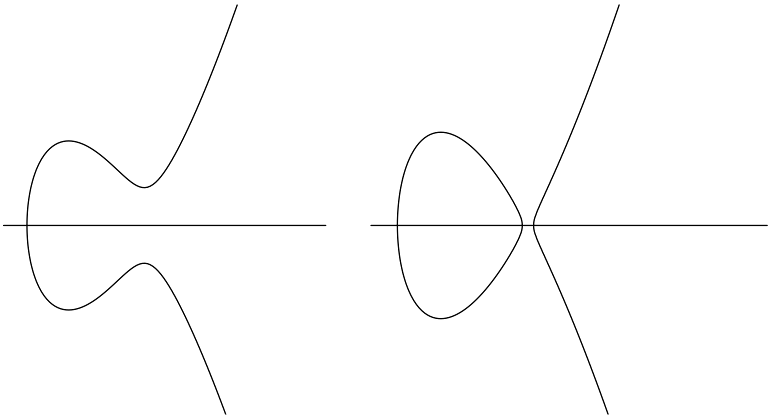


FIGURE 1. Affine picture of elliptic curves, depending on how many real roots the defining polynomial has.

answer is straightforward. Using the fact that $E(\mathbb{C}) \cong \mathbb{C}/L$, where L is a lattice of $\mathbb{C}$, it follows that

$$E(\mathbb{C})_{\text{tor}} \cong \mathbb{Q}/\mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}.$$

Therefore, the group $E(\mathbb{Q})_{\text{tor}} \subseteq E(\mathbb{Q})$ is a finite and abelian subgroup either of $\mathbf{S}^1$, or of $\mathbf{S}^1 \oplus \mathbb{Z}/2\mathbb{Z}$. So, it is of the form $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, for some natural number n. Mazur's theorem determines exactly the possible choices for the number $n \in \mathbb{N}$.

THEOREM 1.2 (MAZUR). *Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion group $E(\mathbb{Q})_{tor}$ of E over $\mathbb{Q}$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z}\ ,\ \ n \in \{1, 2, \ldots, 10, 12\} \quad \textit{or} \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}\ ,\ \ n \in \{1, 2, 3, 4\}.$$

Further, each of these groups occur as torsion group over $\mathbb{Q}$ of some elliptic curve over the rationals.

The proof of Mazur's theorem is beyond the scope of this master thesis. However, as another indication of its validity, we give examples of elliptic curves, that have one of the fifteen groups Mazur's result, as torsion group.

$E\|_{\mathbb{Q}}$	$E(\mathbb{Q})_{\text{tor}}$
$Y^2 = X^3 + 2$	$\{O\}$
$Y^2 = X^3 + X$	$\mathbb{Z}/2\mathbb{Z}$
$Y^2 = X^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$
$Y^2 = X^3 + 4X$	$\mathbb{Z}/4\mathbb{Z}$
$Y^2 + Y = X^3 - X^2$	$\mathbb{Z}/5\mathbb{Z}$
$Y^2 = X^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$
$Y^2 - XY + 2Y = X^3 + 2X^2$	$\mathbb{Z}/7\mathbb{Z}$
$Y^2 + 7XY - 6Y = X^2 - 6X^2$	$\mathbb{Z}/8\mathbb{Z}$
$Y^2 + 3XY + 6Y = X^3 + 6X^2$	$\mathbb{Z}/9\mathbb{Z}$
$Y^2 - 7XY - 36Y = X^3 - 18X^2$	$\mathbb{Z}/10\mathbb{Z}$
$Y^2 + 43XY - 210Y = X^3 - 210X^2$	$\mathbb{Z}/12\mathbb{Z}$
$Y^2 = X^3 - X$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
$Y^2 = X^3 + 5X^2 + 4X$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
$Y^2 + 5XY - 6Y = X^3 - 3X^2$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
$Y^2 = X^3 + 337X^2 + 20736X$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

1.1. The proof of Lutz-Nagell theorem. This section of the chapter is focused on the proof of the theorem of Lutz and Nagell.

The theorem informs us that if P is a rational point on an elliptic curve E, defined over $\mathbb{Q}$, then its coordinates must be integer numbers. To prove that we would like to show that if $P = [x_P : y_P : 1] \in E(\mathbb{Q})$, then

$$|x_P|_p \leq 1 \quad \text{and} \quad |y_P|_p \leq 1,$$

for each prime number p. Therefore, it makes sense to reduce the given elliptic curve modulo p.

Definition 1.3. Let p be a prime. The rational number r is called *p-integral*, if $|r|_p \leq 1$. The set of all p-integral rationals is a ring and it is denoted by $\mathbb{Z}_{(p)}$.

Let r be a rational number. Then it can be written in the form

$$r = p^n \frac{a}{b},$$

where $a, b, n \in \mathbb{Z}$, such that g.c.d.$(a, b) = 1$ and $p \nmid ab$. If $n < 0$, i.e. the prime number p is a divisor of the denominator of r, then it is impossible to reduce r modulo p, because we can not extend naturally the notation for integer residues modulo p. Hence, we initially restrict the definition of the reduction map of rational numbers in the case of p-integral r. So, we define the map

$$\begin{aligned} \mathrm{r}_p \ : \ \mathbb{Z}_{(p)} &\longrightarrow \mathbb{F}_p \\ r &\longmapsto \begin{cases} [a]_p[b]_p^{-1} & \text{, if } n = 0 \\ [0]_p & \text{, if } n > 0. \end{cases} \end{aligned}$$

This definition suggests that we should normalize the coordinates of a point by multiplication with a power of p, in order that the reduction map to make sense. And there lies another advantage of considering our curves projectively.

Definition 1.4. Let $P \in \mathbb{P}^2(\mathbb{Q})$ and p be a prime number. A choice $[x : y : z]$ of homogeneous coordinates for P, that satisfies the properties

(i) $|w|_p \leq 1$, for every $w \in \{x, y, z\}$, and
(ii) there exists $w \in \{x, y, z\}$ such that $|w|_p = 1$,

is called *p-reduced representation of P*.

Remark 1.5. Let $P = [p^{n_1}x_1 : p^{n_1}y_1 : p^{n_3}z_1] \in \mathbb{P}^2(\mathbb{Q})$, where $n_1, n_2, n_3 \in \mathbb{Z}$ and $x_1, y_1, z_1 \in \mathbb{Q}$ such that $|x_1|_p = |y_1|_p = |z_1|_p = 1$. Then a p-reduced representation is obtained by multiplying the components of P by $p^{-\min\{n_1,n_2,n_3\}}$. A p-reduced representation of a point P is unique, up to a factor of p-adic norm equal to 1. Indeed, if $c \in \mathbb{Q}$, such that $|c|_p = 1$, then $[x_0 : x_1 : x_2] = [cx_0 : cx_1 : cx_2]$ and for each $i \in \{0, 1, 2\}$, we obtain

$$|x_i|_p \leq 1 \Leftrightarrow |cx_i|_p \leq 1$$

and

$$|x_i|_p = 1 \Leftrightarrow |cx_i|_p = 1.$$

Moreover, for any given point there is a p-reduced representation with integer coefficients.

Hence, we may extend the definition of the reduction map, as follows:

$$\begin{aligned} \mathrm{red}_p \ : \ & \mathbb{P}^2(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{F}_p) \\ & [x : y : z] \longmapsto [\mathrm{r}_p(x) : \mathrm{r}_p(y) : \mathrm{r}_p(z)], \end{aligned}$$

where $[x : y : z]$ is a p-reduced representation. It is easy to check that this reduction map is well defined, which is exactly why we introduced the notion of the p-reduced representation.

We consider now the elliptic curve E. We know that, as a projective curve, E is the zero locus of a homogeneous polynomial F, of degree 3. Since we can assume without loss of generality that $F \in \mathbb{Z}[X, Y, Z]$, such that the g.c.d of its coefficients is equal to 1, then the reduced polynomial F_p is a nonzero homogeneous polynomial of $\mathbb{F}_p[X, Y, Z]$, of degree 3. In particular, this polynomial F_p is uniquely determined, up to multiplication by scalar, and so is its zero locus, which is a curve E_p. So, using the reduction map we are able to show that

$$P \in E(\mathbb{Q}) \Rightarrow \mathrm{red}_p(P) \in E_p(\mathbb{F}_p),$$

and more generally, that

$$P \in E(\bar{\mathbb{Q}}) \Rightarrow \mathrm{red}_p(P) \in E_p(\bar{\mathbb{F}}_p),$$

Therefore we are able to redefine the reduction map, using the same notation for simplicity, as a map of curves i.e,

$$\mathrm{red}_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p).$$

Definition 1.6. Let p be a prime number and E be an elliptic curve defined over $\mathbb{Q}$. If E_p is an elliptic curve, then we say that *E has a good reduction to p.*

A priori we do not know that the reduced curve E_p, is nonsingular. In order to examine that we need to check the discriminant of E_p. Clearly, the discriminant Δ_p of E_p and the discriminant Δ of E are related as follows

$$\Delta_p = [\Delta]_p = \Delta \pmod{p}.$$

Hence, the good reduction of E at p, is equivalent to the convention $p \nmid \Delta$.

If E has a good reduction at p, both $E(\mathbb{Q})$ and $E(\mathbb{F}_p)$ are groups.

Proposition 1.7. *Let E be an elliptic curve defined over $\mathbb{Q}$, and p be a prime such that E has a good reduction at it. Then the reduction map*

$$\begin{array}{rcl} red_p & : & E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p) \\ & & [x:y:z] \longmapsto [r_p(x):r_p(y):r_p(z)], \end{array}$$

is a group homomorphism.

Proof. (see corrections to [**9**] at http://www.math.stonybrook.edu/ aknapp/) □

Remark 1.8. For the rest of this section, we have to introduce some new coordinates for the points of the elliptic curve E. For each point $P \in E(\mathbb{Q}) \setminus \{O\}$, so that $P = [x : y : 1]$ and P is not of order 2 in $E(\mathbb{Q})$, we set

$$u := \frac{x}{y} \quad \text{and} \quad w := \frac{1}{y}.$$

Then

$$P = [x : y : 1] = [u : 1 : w],$$

that is we normalize by dividing by y. We will use widely these coordinates for the points of E.

Proposition 1.9. *For the reduction map defined in 1.7, we have that*

$$\ker(red_p) = \{[u : 1 : w] \in E(\mathbb{Q}) \mid |u|_p < 1 \textit{ and } |w|_p < 1\}.$$

Proof. Let $[x : y : z] \in E(\mathbb{Q})$, such that $\text{red}_p([x : y : z]) = O_p$. The reduction map is a group homomorphism, so $O \in \ker(\text{red}_p)$. So, without loss of generality we assume that $z = 1$, and we try to describe the point $[x : y : 1] \in \ker(\text{red}_p)$. Of course, for such a point we have that $y \neq 0$, since it would be reduced to 0 otherwise, so we normalize as in remark 1.8. In order for u and w to reduce to 0, they must be p-adic integers, i.e. $|u|_p < 1$ and $|w|_p < 1$. Hence, we obtain the desired result. □

Set

$$E^1(\mathbb{Q}) := \{[u : 1 : w] \in E(\mathbb{Q}) \mid |u|_p < 1 \text{ and } |w|_p < 1\}.$$

This is exactly the kernel of the reduction map red_p, only for the prime numbers p, for which E_p is an elliptic curve. But we want to remove the assumption of good reduction, or equivalently, the condition $p \nmid \Delta$. So we shall study the set $E^1(\mathbb{Q})$, independently of the choice of the prime number.

Lemma 1.10. *Let $[u : 1 : w] \in E(\mathbb{Q})$ and a prime number p. If $|w|_p < 1$, then $|u|_p < 1$ and $|w|_p = |u|_p{}^3$.*

Proof. The elliptic curve E is of the form

$$E|_{\mathbb{Q}} : Y^2 = X^3 + \alpha X + \beta.$$

Let $[x : y : 1] \in E(\mathbb{Q})$. We recall the equivalence (2) (see page 7). This was proved generally for any finite valuation of a number field. We apply it for p-adic valuations of $\mathbb{Q}$. We have

$$v_p(x) < 0 \Leftrightarrow v_p(y) < 0 \Leftrightarrow \exists\, l \in \mathbb{N} : v_p(x) = -2l \text{ and } v_p(y) = -3l. \tag{13}$$

By definition, we have that

$$|r|_p = p^{-v_p(r)} \quad , \quad \forall\, r \in \mathbb{Q}.$$

So, we rewrite (13) in the form

$$|x|_p > 1 \Leftrightarrow |y|_p > 1 \Leftrightarrow \exists\, l \in \mathbb{N} : |x|_p = p^{2l} \text{ and } |y|_p = p^{3l}. \tag{14}$$

But then

$$|w|_p < 1 \Leftrightarrow \left|\frac{1}{y}\right|_p < 1 \Leftrightarrow |y|_p > 1 \Leftrightarrow \exists\, l \in \mathbb{N} : |x|_p = p^{2l} \text{ and } |y|_p = p^{3l}.$$

Thus,

$$|u|_p = \left|\frac{x}{y}\right|_p = \frac{|x|_p}{|y|_p} = \frac{p^{2l}}{p^{3l}} = p^{-l} < 1.$$

Also,

$$|u|_p{}^3 = (p^{-l})^3 = p^{-3l} = |y|_p{}^{-1} = |w|_p.$$

□

Definition 1.11. For any $n \in \mathbb{N}$, set

$$E^n(\mathbb{Q}) := \{[u : 1 : w] \in E(\mathbb{Q}) \mid |w|_p < 1 \text{ and } |u|_p \leq p^{-n}\}.$$

The p-adic filtration of $E^1(\mathbb{Q})$ is

$$\{O\} \subseteq \cdots \subseteq E^n(\mathbb{Q}) \subseteq \cdots \subseteq E^2(\mathbb{Q}) \subseteq E^1(\mathbb{Q}) \subseteq E(\mathbb{Q}).$$

We have

$$\bigcap_{n=1}^{\infty} E^n(\mathbb{Q}) = \{O\}.$$

Corollary 1.12. *For the set* $E^n(\mathbb{Q})$ *it holds that*

$$E^n(\mathbb{Q}) = \{[u : 1 : w] \in E(\mathbb{Q}) \mid |w|_p \leq p^{-3n}\}.$$

Remark 1.13. An important observation based on the lemma 1.10 is that for any point $P \in E^1(\mathbb{Q})$, there exists a unique number $n \in \mathbb{N}$ such that

$$P \in E^n(\mathbb{Q}) \setminus E^{n+1}(\mathbb{Q}).$$

This helps us to have a better check of the point P.

Proposition 1.14. *For any* $n \in \mathbb{N}$ *the set* $E^n(\mathbb{Q})$ *is a subgroup of* $E(\mathbb{Q})$. *Also, the map*

$$\begin{aligned} \eta_n \quad : \quad & E^n(\mathbb{Q}) \longrightarrow p^n\mathbb{Z}_{(p)}/p^{3n}\mathbb{Z}_{(p)} \\ & [u : 1 : w] \longmapsto [u]_{p^{3n}\mathbb{Z}_{(p)}} \end{aligned}$$

is a group homomorphism, such that

$$\ker(\eta_n) \subseteq E^{3n}(\mathbb{Q}).$$

Consequently, the homomorphism

$$E^n(\mathbb{Q})/E^{3n}(\mathbb{Q}) \longrightarrow p^n\mathbb{Z}_{(p)}/p^{3n}\mathbb{Z}_{(p)}$$

is injective.

Proof. The elliptic curve E is of the form

$$E|_{\mathbb{Q}} : Y^2 = X^3 + \alpha X + \beta,$$

with $\alpha, \beta \in \mathbb{Z}$. Since we use another coordinates' system, that of u and w, we have to reform the equation that defines E. By dividing by Y^3, we obtain that

$$\frac{1}{Y} = \left(\frac{X}{Y}\right)^3 + \alpha\frac{X}{Y}\left(\frac{1}{Y}\right)^2 + \beta\left(\frac{1}{Y}\right)^3 \Rightarrow W = U^3 + \alpha U W^2 + \beta W^3.$$

Let $P_1, P_2 \in E^n(\mathbb{Q})$. Our goal is to show that $P_3 := P_1 + P_2 \in E^n(\mathbb{Q})$, too. Consider the coordinates $[u_1 : 1 : w_1], [u_2 : 1 : w_2]$ and $[u_3 : 1 : w_3]$ for the points P_1, P_2 and P_3, respectively. Then

$$w_1 = {u_1}^3 + \alpha u_1 {w_1}^2 + \beta {w_1}^3 \quad \text{and} \quad w_2 = {u_2}^3 + \alpha u_2 {w_2}^2 + \beta {w_2}^3,$$

and so

$$\begin{aligned} w_1 - w_2 &= {u_1}^3 - {u_2}^3 + \alpha u_1 {w_1}^2 - \alpha u_2 {w_2}^2 + \beta {w_1}^3 - \beta {w_2}^3 \\ &= {u_1}^3 - {u_2}^3 + \alpha {w_1}^2(u_1 - u_2) + \alpha u_2({w_1}^2 - {w_2}^2) + \beta({w_1}^3 - {w_2}^3) \\ &= (u_1 - u_2)({u_1}^2 + u_1u_2 + {u_2}^2) + \alpha {w_1}^2(u_1 - u_2) + \alpha u_2(w_1 - w_2)(w_1 + w_2) \\ &\quad +\beta(w_1 - w_2)({w_1}^2 + w_1w_2 + {w_2}^2). \end{aligned}$$

Equivalently, for

$$A := 1 - \alpha u_2(w_1 + w_2) - \beta({w_1}^2 + w_1w_2 + {w_2}^2) \quad \text{and} \quad B := {u_1}^2 + u_1u_2 + {u_2}^2 + \alpha {w_1}^2,$$

we have that

$$(w_1 - w_2)A = (u_1 - u_2)B.$$

Let

$$W = \lambda U + \nu,$$

be the defining equation of the line L that passes through the points P_1 and P_2.

Case 1. If $P_1 \neq P_2$, then the slope λ is given by

$$\lambda = \frac{w_1 - w_2}{u_1 - u_2} = \frac{B}{A}.$$

But,

$$\begin{aligned} |A|_p &= |1 - \alpha u_2(w_1 + w_2) - \beta({w_1}^2 + w_1w_2 + {w_2}^2)|_p \\ &\leq \max\{1, |\alpha u_2(w_1 + w_2)|_p, |\beta({w_1}^2 + w_1w_2 + {w_2}^2)|_p\} \end{aligned}$$

We have

$$|\alpha u_2(w_1 + w_2)|_p \leq |\alpha|_p|u_2|_p \max\{|w_1|_p, |w_2|_p\} < 1$$

and

$$|\beta({w_1}^2 + w_1w_2 + {w_2}^2)|_p \leq |\beta|_p \max\{|w_1|_p{}^2, |w_1|_p|w_2|_p, |w_2|_p{}^2\} < 1,$$

so

$$|A|_p = \max\{1, |\alpha u_2(w_1 + w_2)|_p, |\beta({w_1}^2 + w_1 w_2 + {w_2}^2)|_p\} = 1.$$

Similarly,

$$\begin{aligned} |B|_p &= |{u_1}^2 + u_1u_2 + {u_2}^2 + \alpha {w_1}^2|_p \\ &\leq \max\{{|u_1|_p}^2, |u_1|_p|u_2|_p, {|u_2|_p}^2, |\alpha|_p{|w_1|_p}^2\} \\ &\leq \max\{p^{-2n}, p^{-2n}, p^{-2n}, p^{-3n}\} \\ &= p^{-2n}. \end{aligned}$$

Hence, we obtain an upper bound for the slope, i.e.

$$|\lambda|_p = \left|\frac{B}{A}\right|_p = \frac{|B|_p}{|A|_p} \leq p^{-2n}.$$

Case 2. We assume now that $P_1 = P_2$. Then the line L is actually the tangent of E at the point P_1. So we compute the slope, in order to find again an upper bound, by differentiation. We have

$$W = U^3 + \alpha U W^2 + \beta W^3 \Rightarrow (1 - 2\alpha UW - 3\beta W^3)\mathrm{d}W = (3U^2 + \alpha W^2)\mathrm{d}U$$

$$\Rightarrow \left.\frac{\mathrm{d}W}{\mathrm{d}U}\right|_{U=u_1} = \frac{3{u_1}^2 + \alpha {w_1}^2}{1 - 2\alpha u_1 w_1 - 3\beta {w_1}^3}.$$

But

$$|1 - 2\alpha u_1 w_1 - 3\beta {w_1}^3|_p \leq \max\{1, |2\alpha u_1 w_1|_p, |3\beta {w_1}^3|_p\},$$

and

$$|2\alpha u_1 w_1|_p < 1 \quad , \quad |3\beta {w_1}^3|_p < 1,$$

and so

$$|1 - 2\alpha u_1 w_1 - 3\beta {w_1}^3|_p = 1.$$

Therefore,

$$|\lambda|_p = \left|\left.\frac{\mathrm{d}W}{\mathrm{d}U}\right|_{U=u_1}\right|_p = \left|\frac{3{u_1}^2 + \alpha {w_1}^2}{1 - 2\alpha u_1 w_1 - 3\beta {w_1}^3}\right|_p = \left|3{u_1}^2 + \alpha {w_1}^2\right|_p$$

$$\leq \max\{|3|_p{|u_1|_p}^2, |\alpha|_p{|w_1|_p}^2\} \leq p^{-2n}.$$

Thus, in each case we have that

$$|\lambda|_p \leq p^{-2n}.$$

Since we need to prove that $P_3 \in E^n(\mathbb{Q})$, using that $P_1, P_2 \in E^n(\mathbb{Q})$, we need to determine the relations that their coordinates satisfy. Let $P_1P_2 = [\tilde{u} : 1 : \tilde{w}]$ be the third point of intersection of the elliptic curve E and the line passing through P_1 and P_2. We first recall that u_1, u_2 and $\tilde{u}$ are solutions of the cubic equation

$$\lambda U + \nu = U^3 + \alpha U(\lambda U + \nu)^2 + \beta(\lambda U + \nu)^3$$

$$\Leftrightarrow (1 + \alpha\lambda^2 + \beta\lambda^3)U^3 + (2\alpha\lambda\nu + 3\beta\lambda^2\nu)U^2 + (\alpha\nu^2 + 3\beta\lambda\nu^2 - \lambda)U + (\beta\nu^3 - \nu) = 0.$$

Consequently,

$$u_1 + u_2 + \tilde{u} = -\frac{2\alpha\lambda\nu + 3\beta\lambda^2\nu}{1 + \alpha\lambda^2 + \beta\lambda^3}.$$

Applying again the same argument we have that

$$\begin{cases} |1+\alpha\lambda^2+\beta\lambda^3|_p \leq \max\{1, |\alpha\lambda^2|_p, |\beta\lambda^3|_p\} \\ |\alpha|_p|\lambda|_p{}^2 < 1 \\ |\beta|_p|\lambda|_p{}^3 < 1 \end{cases} \Rightarrow |1+\alpha\lambda^2+\beta\lambda^3|_p = 1,$$

which means that

$$|u_1+u_2+\tilde{u}|_p = |2\alpha\lambda\nu + 3\beta\lambda^2\nu|_p.$$

We also have that,

$$|\nu|_p = |w_1 - \lambda u_1|_p \leq \max\{|w_1|_p, |\lambda|_p|u_1|_p\} \leq p^{-3n}.$$

Thus,

$$|2\alpha\lambda\nu + 3\beta\lambda^2\nu|_p \leq \max\{|2|_p|\alpha|_p|\lambda|_p|\nu|_p\,,\ |3|_p|\beta|_p|\lambda|_p{}^2|\nu|_p\} \leq p^{-3n}$$

$$\Rightarrow |u_1+u_2+\tilde{u}|_p \leq p^{-3n}. \tag{15}$$

By construction we have that $P_3 = -P_1P_2$. This means that $[u_3 : 1 : w_3] = [-\tilde{u} : 1 : -\tilde{w}]$. So, for u_3 we have

$$|u_3|_p = |-\tilde{u}|_p = |u_1+u_2+\tilde{u}-u_1-u_2|_p \leq \max\{|u_1+u_2+\tilde{u}|_p, |u_1|_p, |u_2|_p\} \leq p^{-n}.$$

Also,

$$|w_3|_p = |-\tilde{w}|_p = |\lambda\tilde{u}+\nu|_p \leq \max\{|\lambda|_p|\tilde{u}|_p, |\nu|_p\} \leq \max\{p^{-n}p^{-2n}, p^{-3n}\} < 1.$$

So, by definition we have that $P_3 = P_1 + P_2 \in E^n(\mathbb{Q})$. Hence, $E^n(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$. Let $P = [u : 1 : w] \in E^n(\mathbb{Q})$. This means that $|u|_p \leq p^{-n}$. So,

$$p^n|u|_p \leq 1 \Leftrightarrow |p^{-n}u|_p \leq 1 \Leftrightarrow p^{-n}u \in \mathbb{Z}_{(p)} \Leftrightarrow u \in p^n\mathbb{Z}_{(p)}.$$

Hence, η_n is indeed a map from $E^n(\mathbb{Q})$ to $p^n\mathbb{Z}_{(p)}/p^{3n}\mathbb{Z}_{(p)}$. It is obvious that $\eta_n(O) = [0]_{p^{3n}\mathbb{Z}_{(p)}}$. Also, according to (15), we have that

$$u_1+u_2-u_3 \in p^{3n}\mathbb{Z}_{(p)} \Rightarrow [u_1+u_2-u_3]_{p^{3n}\mathbb{Z}_{(p)}} = [0]_{p^{3n}\mathbb{Z}_{(p)}} \Rightarrow [u_1+u_2]_{p^{3n}\mathbb{Z}_{(p)}} = [u_3]_{p^{3n}\mathbb{Z}_{(p)}}.$$

$$[u_1]_{p^{3n}\mathbb{Z}_{(p)}} + [u_2]_{p^{3n}\mathbb{Z}_{(p)}} = [u_3]_{p^{3n}\mathbb{Z}_{(p)}} \Rightarrow \eta_n(P_1)+\eta_n(P_2) = \eta_n(P_3) = \eta_n(P_1+P_2),$$

so η_n is a homomorphism.
Consider the point $P = [u : 1 : w] \in \ker(\eta_n)$. Then

$$\eta_n(P) = [0]_{p^{3n}\mathbb{Z}_{(p)}} \Rightarrow u \in p^{3n}\mathbb{Z}_{(p)} \Rightarrow |p^{-3n}u|_p \leq 1 \Rightarrow |u|_p \leq p^{-3n}.$$

By the last inequality and the fact that $|w|_p = |u|_p{}^3$, follows that $|w|_p < 1$, and so we proved that $P \in E^{3n}(\mathbb{Q})$. Hence, $\ker(\eta_n) \subseteq E^{3n}(\mathbb{Q})$. This completes the proof, since it is obvious that $E^{3n}(\mathbb{Q}) \subseteq \ker(\eta_n)$. □

Proposition 1.15. *For each prime p, we have*

$$E(\mathbb{Q})_{tor} \cap E^1(\mathbb{Q}) = \{O\}.$$

Proof. Let $E(\mathbb{Q})_{\text{tor}} \cap E^1(\mathbb{Q}) \neq \{O\}$. So, there is a nonzero point in the intersection $E(\mathbb{Q})_{\text{tor}} \cap E^1(\mathbb{Q})$. Particularly, there is a point $Q = [u_Q : 1 : w_Q]$ of prime order[1] q, i.e. $qQ = O$. Also, there exists unique $n \in \mathbb{N}$, such that

$$Q \in E^n(\mathbb{Q}) \setminus E^{n+1}(\mathbb{Q}).$$

For that specific n, we define the homomorphism η_n, as in proposition 1.14. Then

$$\eta_n(qQ) = \eta_n(O) = [0]_{p^{3n}\mathbb{Z}_{(p)}} \Rightarrow qu_Q \in p^{3n}\mathbb{Z}_{(p)}.$$

If $p \neq q$, then $u_Q \in p^{3n}\mathbb{Z}_{(p)} \subseteq p^{2n}\mathbb{Z}_{(p)}$, while if $p = q$, then $u_Q \in p^{3n-1}\mathbb{Z}_{(p)} \subseteq p^{2n}\mathbb{Z}_{(p)}$. In each case, we have by injectivity that

$$u_Q \in p^{2n}\mathbb{Z}_{(p)} \Rightarrow Q \in E^{2n}(\mathbb{Q}) \subseteq E^{n+1}(\mathbb{Q}),$$

which is a contradiction. □

The previous results are necessary for the proof of Lutz-Nagell theorem, which is actually an easy-to-state theorem, but its proof is elaborate.

Proof of Theorem 1.1. (i) We consider two cases. If $y_P = 0$, then the point P is of order 2, and x_P is a rational root of the polynomial $X^3 + \alpha X + \beta$, and so an integer by Gauss' lemma. If otherwise, i.e. if $y_P \neq 0$, we consider the change of coordinates

$$u_P := \frac{x_P}{y_P} \quad \text{and} \quad w_P := \frac{1}{y_P}.$$

Then

$$P = [x_P : y_P : 1] = [u_P : 1 : w_P].$$

We fix a prime number p. By proposition 1.15 we have that $P \notin E^1(\mathbb{Q})$. This means that $|w_P|_p \geq 1 \Leftrightarrow |y_P|_p \leq 1$. Since this is true for any prime p, we have that $y_P \in \mathbb{Z}$. Then by (14), we also have $|x_P|_p \leq 1$, for every prime p. And, so $x_P \in \mathbb{Z}$.

(ii) For the first coordinate x_{2P} of the point $2P$, we have that

$$x_{2P} = \frac{{x_P}^4 - 2\alpha {x_P}^2 - 8\beta x_P + A^2}{4({x_P}^3 + \alpha x_P + \beta)} = \frac{{x_P}^4 - 2\alpha {x_P}^2 - 8\beta x_P + \alpha^2}{4{y_P}^2}.$$

Set $\lambda(x_P) := {x_P}^4 - 2\alpha {x_P}^2 - 8\beta x_P + \alpha^2$. Then

$$\lambda(x_P) = 4{y_P}^2 x_{2P}.$$

According to (i), the numbers $\lambda(x_P)$, ${y_P}^2$ and x_{2P} are integers, and so it follows that ${y_P}^2 \mid \lambda(x_P)$. An easy calculation shows that

$$(3{x_P}^3 + 4\alpha)\lambda(x_P) - (3{x_P}^3 - 5\alpha x_P - 27\beta){y_P}^2 = 4\alpha^3 + 27\beta^2.$$

By the last equation and the fact the ${y_P}^2 \mid \lambda(x_P)$, we conclude that ${y_P}^2 \mid 4\alpha^3 + 27\beta^2$, which is the desired result.

[1] Let $Q' \in E(\mathbb{Q})_{\text{tor}}$. Then there exists a natural number $k \geq 2$, so that $kQ' = O$. Let q be a prime divisor of k. Then

$$q\left(\frac{k}{q}Q'\right) = O,$$

so the point $\frac{k}{q}Q'$ easily follows that it is of order 2.

□

REMARK 1.16. The Lutz-Nagell theorem provides us with a rather not fast algorithm for finding torsion points on an elliptic curve E, defined over the rationals. For any y, in the set

$$\{k \in \mathbb{Z} : k^2 \mid 4\alpha^3 + 27\beta^2\},$$

we try to find all integers x, which are roots of the polynomial $X^3 + \alpha X + \beta - y^2$. For those x, we check whether the point $[x : y : 1]$ is a torsion point, or not.
Moreover, given a point $P \in E(\mathbb{Q})$ we are able to determine if its order is infinite. We simply calculate the coordinates of the points nP. If these are not integer numbers, then the point P is of infinite order. Actually, it turns out that we need to check only the points $2P$, $4P$ and $8P$, to check if the point P is of finite order.

The following propositions (see [**9**]) give us some examples of families of elliptic curves, the finite points of which, can be explicitly determined.

PROPOSITION 1.17. *Let $\alpha \in \mathbb{Z}$, such that $p^4 \nmid \alpha$, for every prime number p. Consider the elliptic curve*

$$E|_{\mathbb{Q}} : Y^2 = X^3 + \alpha X.$$

Then, its torsion points, that differ from the point O, are the following:

(i) the point $[0 : 0 : 1]$ *of order* 2.
(ii) if $\alpha = 4$, the points $[2 : \pm 4 : 1]$ *of order* 4.
(iii) if $\alpha = -r^2$, for some $r \in \mathbb{Z}$, then $[r : 0 : 1]$, *of order* 2.

In other words,

$$E(\mathbb{Q})_{tor} \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & , \textit{if } \alpha = 4 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & , \textit{if } \exists\, r \in \mathbb{Z} : \alpha = -r^2 \\ \mathbb{Z}/2\mathbb{Z} & , \textit{if otherwise} \end{cases}.$$

The previous result is due to Feuter in 1930, based broadly on an argument suggested by Mordell. Five years later, Nagell proved the following result for another family of elliptic curves.

PROPOSITION 1.18. *Let $\beta \in \mathbb{Z}$, such that $p^6 \nmid \beta$, for every prime number p, and let*

$$E|_{\mathbb{Q}} : Y^2 = X^3 + \beta.$$

Then the torsion points of E, that differ from the point O, are the following:

(i) if $\beta = r^2$, for some $r \in \mathbb{Z}$, then the finite order points are the points $[0 : \pm r : 1]$ *of order* 3.
(ii) if $\beta = s^3$, for some $s \in \mathbb{Z}$, then the only finite point is the point $[-s : 0 : 1]$, *of order* 2.

In other words,

$$E(\mathbb{Q})_{tor} \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & , \textit{if } \exists\, r \in \mathbb{Z} : \beta = r^2 \\ \mathbb{Z}/2\mathbb{Z} & , \textit{if } \exists\, s \in \mathbb{Z} : \beta = s^3 \end{cases}.$$

2. Torsion Group of Elliptic Curves over Number Fields

The goal of this paragraph is to describe briefly what it is known about the group $E(K)_{\text{tor}}$ of an elliptic curve defined over an arbitrary number field K. One of the most significant results concerning the torsion subgroup $E(K)_{\text{tor}}$ is the following.

Theorem 2.1 (Merel). *For every $d \in \mathbb{N}$, there exists a positive integer B_d, such that for every number field K of degree d and elliptic curve E over K, it holds that*

$$|E(K)_{tor}| < B_d.$$

This theorem is also known as "the strong uniform boundedness conjecture". The word "strong" indicates that the bound is uniform in all number fields of the same degree over $\mathbb{Q}$. It is known as a conjecture of Ogg, but Levi was the first that conjectured the finiteness of $|E(K)_{\text{tor}}|$. Manin proved a local version of this conjecture in 1969 (see [**14**]).

Theorem 2.2 (Manin). *For any number field K and any prime number p, there exists an integer $e \geq 0$, such that no elliptic curve defined over K has rational point of order p^e.*

Merel published an existential proof of this conjecture in 1996, but it was Parent, who gave precise values for the constant B_d some years later.

We introduce now some standard notation. For $d \in \mathbb{N}$, we define the following sets, which depend only on the choice of the natural number d, as a consequence of the strong uniform boundedness conjecture.

$\Phi(d)$:= the set of all possible isomorphism classes of the torsion group $E(K)_{\text{tor}}$ of an elliptic curve E defined over a number field K of degree d over $\mathbb{Q}$.

$S(d)$:= the set of primes that can appear as the order of a torsion point of an elliptic curve E defined over a number field of degree d over $\mathbb{Q}$.

= the set of primes p for which there exists an elliptic curve E over a number field of degree d over $\mathbb{Q}$, such that $|E(K)_{\text{tor}}|$ is divided by p.

As a consequence of Frey's and Falting's work, we have that

$$\Phi(d) \text{ is finite} \Leftrightarrow S(d) \text{ is finite.}$$

Merel proved the finiteness of $S(d)$ for each $d \geq 1$, and so the strong uniform boundedness conjecture.

The ideal, for the study of the elliptic curves, would be to establish the set $\Phi(d)$, for any choice of the natural number d. Until today, this is an open question. Mazur's theorem determines the set $\Phi(1)$. Due to the work of Kamienny, Kenku and Momose the set $\Phi(2)$ has been determined explicitly.

Theorem 2.3 (Kamienny, Kenku, Momose). *Let $K = \mathbb{Q}(\sqrt{d})$, be a quadratic number field and E be an elliptic curve over K. Then*

(i) for $d = -3$, we have $E(\mathbb{Q}(\sqrt{-3}))_{tor} \cong \mathbb{Z}/3m\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$, with $m \in \{1, 2\}$,
(ii) for $d = -1$, we have that $E(\mathbb{Q}(\sqrt{-1}))_{tor} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, and

(iii) for any other choice of d, we have either that $E(K)_{tor} \cong \mathbb{Z}/m\mathbb{Z}$, for $m \in \{1, 2, \ldots, 16, 18\}$, or that $E(K)_{tor} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, with $m \in \{1, 2, \ldots, 6\}$.

For $d \geq 3$, we have some results for the torsion subgroup, but not conclusive answer for the set $\Phi(d)$. It is worth-noting that the study of the torsion points of elliptic curves is an active field of research. Even if the set $\Phi(d)$ has not been established for any d, there are several results concerning specific subsets of $\Phi(d)$. We give an indicative example of such a subset of $\Phi(d)$ and of what it is known about it. Let

$\Phi_{\mathbb{Q}}(d)$:= the set of possible isomorphism classes of groups $E(K)_{\text{tor}}$, where K is a number field K of degree d over $\mathbb{Q}$ and E is an elliptic curve defined over $\mathbb{Q}$.

Due to recent work of Conzalez-Jimenez and Najman the set $\Phi_{\mathbb{Q}}(p)$, where p is a prime number, is determined. Practically, this means that we know all possible torsion groups over prime degree number fields of elliptic curves with rational coefficients.

3. The rank of elliptic curves over $\mathbb{Q}$

We recall that for the group $E(\mathbb{Q})$ of rational points of an elliptic curve E over the rationals, it holds that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{\text{tor}}$ is the torsion subgroup of $E(\mathbb{Q})$ and $r \in \mathbb{N}_0$ is the rank of the elliptic curve E. We studied thoroughly the group $E(\mathbb{Q})_{\text{tor}}$, and so in this section we focus on the rank of E.

The first question that arises is, whether we are able to determine the rank of an elliptic curve, or not. For specific cases the rank has been determined, but in its generality this is an open problem for now. In fact we do not know which nonnegative integers appear as rank of an elliptic curve, or even better if the rank is a bounded number or not.

Another important question that we are interested in is about the generators of $\mathbb{Z}^r$. Assuming that we know the rank of an elliptic curve, are we able to establish a system of generators of $\mathbb{Z}^r$?

3.1. The algebraic approach.

3.1.1. *Cohomology of profinite groups.* First, we note that the definitions and the results we will mention are more general[2], but for simplicity we stick to the case that concerns us.

Let K be a number field and $\bar{K}$ be its algebraic closure. It is known that $\bar{K}$ is the direct limit of all finite Galois extensions L of K, i.e.

$$\bar{K} = \varinjlim_{L/K \text{ finite \& Galois}} L.$$

Moreover, the extension $\bar{K}/K$ is an infinite Galois extension[3], such that the group $\text{Gal}(\bar{K}/K)$ is profinite. In particular,

$$\text{Gal}(\bar{K}/K) = \varprojlim_{L/K \text{ finite \& Galois}} \text{Gal}(L/K).$$

[2] Instead of the profinite group $\text{Gal}(\bar{K})$, we could state the results for any profinite group G.

[3] Sometimes the extension $\bar{K}$ of K is referred as the absolute Galois extension of K.

This means that $\mathrm{Gal}(\bar{K}/K)$ is also a topological group, such that a basis of open sets around the identity consists of all subgroups of $\mathrm{Gal}(\bar{K}/K)$ of finite index.

Let M be an abelian group on which the group $\mathrm{Gal}(\bar{K}/K)$ acts. We denote the action of $\sigma \in \mathrm{Gal}(\bar{K}/K)$ on $m \in M$, by

$$m \longmapsto m^{\sigma}.$$

The M is a (right) $\mathrm{Gal}(\bar{K}/K)$-module if the action of G on M satisfies the properties

$$m^1 = m \quad , \quad (m+m')^{\sigma} = m^{\sigma} + m'^{\sigma} \quad \text{and} \quad (m^{\sigma})^{\tau} = m^{\sigma\tau}.$$

If M and N are both $\mathrm{Gal}(\bar{K}/K)$-modules, a $\mathrm{Gal}(\bar{K}/K)$-homomorphism is a homomorphism $\phi : M \longrightarrow N$ of abelian groups commuting with the action of G, i.e.

$$\phi(m^{\sigma}) = \phi(m)^{\sigma},$$

for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $m \in M$.

Definition 3.1. A *discrete $Gal(\bar{K}/K)$-module* is an abelian group M, on which the group $\mathrm{Gal}(\bar{K}/K)$ acts continuously with respect to the topology on $\mathrm{Gal}(\bar{K}/K)$, which described above, and the discrete topology on M. In other words, the map

$$\mathrm{Gal}(\bar{K}/K) \times M \longrightarrow M \quad , \quad (\sigma, m) \longmapsto m^{\sigma}$$

is continuous.

The definition of a discrete $\mathrm{Gal}(\bar{K}/K)$-module is rather not so practical, and so we need other equivalent characterizations.

Proposition 3.2. *Let M be a $Gal(\bar{K}/K)$-module. The following are equivalent:*

(i) M is a discrete $Gal(\bar{K}/K)$-module.

(ii) For each $m \in M$, the stabilizer

$$G_m := \{\sigma \in Gal(\bar{K}/K) \mid m^{\sigma} = m\}$$

is an open subgroup of $Gal(\bar{K}/K)$.

(iii) If $B(1)$ is a basis of sets around the identity, which consists of open normal subgroups H of $Gal(\bar{K}/K)$, then

$$M = \bigcup_{H \in B(1)} M^H,$$

where

$$M^H := \{m \in M \mid m^{\sigma} = m, \forall\, \sigma \in H\}.$$

Theorem 3.3 (Structure Theorem of Profinite Groups (for $\mathrm{Gal}(\bar{K}/K)$)). *(i) Let H be a normal subgroup of $Gal(\bar{K}/K)$. Then H is open if, and only if the group $Gal(\bar{K}/K)/H$ is finite.*

(ii) Let H be a subgroup of $Gal(\bar{K}/K)$. The following are equivalent:

(1) H is close.

(2) H is profinite.

(3) H is intersection of infinitely many open subgroups of $Gal(\bar{K}/K)$.

Proof. (see [**17**], or [**?**]) □

Example 3.4. Let M be the additive abelian group $(\bar{K}, +)$ and the action

$$\mathrm{Gal}(\bar{K}/K) \times \bar{K} \longrightarrow \bar{K}$$

be the usual one. Since

$$\bar{K} = \bigcup_{\substack{K \leq L \leq \bar{K} \\ L/K \text{ finite}}} L,$$

the $\bar{K}$ is discrete $\mathrm{Gal}(\bar{K}/K)$-module. It holds the same if we consider the corresponding multiplicative group. In other words, the group $\bar{K}^{\times}$ is also a discrete $\mathrm{Gal}(\bar{K}/K)$-module.

Example 3.5. Let E be an elliptic curve defined over an arbitrary number field K. Then $E(\bar{K})$ is an additive abelian group and a discrete $\mathrm{Gal}(\bar{K}/K)$-module, because

$$E(\bar{K}) = \bigcup_{\substack{K \leq L \leq \bar{K} \\ L/K \text{ finite}}} E(L).$$

We are interested in calculating the largest submodule of a given $\mathrm{Gal}(\bar{K}/K)$-module, on which $\mathrm{Gal}(\bar{K}/K)$ acts trivially. To that purpose, we define the 0th cohomology group.

Definition 3.6. The *0th cohomology group of the Gal$(\bar{K}/K)$-module M* is defined by

$$\mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), M) := \{m \in M \mid m^{\sigma} = m, \forall \sigma \in \mathrm{Gal}(\bar{K}/K)\}.$$

That is the submodule of M, that consist of all $\mathrm{Gal}(\bar{K}/K)$-invariant elements.

This definition implies the existence of cohomology groups of higher order. Indeed, we could define the n-th cohomology group for any $n \in \mathbb{N}_0$, but this not necessary for our goal. We need only the 0th and the 1st cohomology group. Therefore, it remains to define the 1st cohomology group.

Let

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

be a short exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules. That is, ϕ and ψ are $\mathrm{Gal}(\bar{K}/K)$-modules homomorphisms such that ϕ is injective, ψ is surjective and

$$\mathrm{Im}(\phi) = \ker(\psi).$$

Easily follows that taking the corresponding cohomology groups, we may write the following exact sequence

$$0 \longrightarrow \mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), A) \longrightarrow \mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), B) \longrightarrow \mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), C).$$

The problem now is that the map on the right fails to be surjective. We would like to measure this failure, i.e. this lack of surjectivity.

Definition 3.7. Let M be a $\mathrm{Gal}(\bar{K}/K)$-module, and $C^1(\mathrm{Gal}(\bar{K}/K), M)$ the set of all maps

$$\mathrm{Gal}(\bar{K}/K) \longrightarrow M.$$

This is a group and it is called *the group of* 1*-cochains from Gal$(\bar{K}/K)$ to M*. We define the *group of* 1*-cocycles (from Gal$(\bar{K}/K)$ to M)* by

$$\mathcal{Z}^1(\mathrm{Gal}(\bar{K}/K), M) := \left\{\xi \in C^1(\mathrm{Gal}(\bar{K}/K), M) \middle| \, \xi(\sigma\tau) = \xi(\sigma)^{\tau} + \xi(\tau), \, \forall \sigma, \tau \in \mathrm{Gal}(\bar{K}/K)\right\}.$$

We also define *the group of* 1*-coboundaries (from Gal*$(\bar{K}/K)$ *to M)* to be

$$\mathcal{B}^1(\mathrm{Gal}(\bar{K}/K), M) := \left\{\xi \in C^1(\mathrm{Gal}(\bar{K}/K), M)\middle| \exists\, m \in M : \xi(\sigma) = m^\sigma - m,\ \forall\, \sigma \in \mathrm{Gal}(\bar{K}/K)\right\}.$$

By these definitions we can prove that the group of 1-coboundaries is a normal subgroup of the group of 1-cochains. *The* 1*st cohomology group of the Gal*$(\bar{K}/K)$*-module* M is denoted by $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), M)$ and it is the quotient group of these groups, i.e.

$$\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), M) = \mathcal{Z}^1(\mathrm{Gal}(\bar{K}/K), M)/\mathcal{B}^1(\mathrm{Gal}(\bar{K}/K), M).$$

Remark 3.8. If we consider the trivial action of $\mathrm{Gal}(\bar{K}/K)$ on M, then

$$\mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), M) = M \quad \text{and} \quad \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), M) = \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), M).$$

Indeed, the first relation is immediate by the definition of 0th cohomology. For the second relation, it suffices to observe that all maps from $\mathrm{Gal}(\bar{K}/K)$ to M, i.e. all the 1-cocycles, are group homomorphisms and the only 1-coboundary is the trivial one.

We consider again the short exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0.$$

Let $c \in \mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), C)$. Then there exists an $b \in B$, such that $\psi(b) = c$. We define the $\xi \in C^1(\mathrm{Gal}(\bar{K}/K), M)$ by

$$\xi(\sigma) = m^\sigma - m.$$

Then $\xi \in \mathcal{Z}^1(\mathrm{Gal}(\bar{K}/K), A)$. We define the $\delta(c)$, to be the cohomology class in $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), A)$ of the 1-cocycle ξ. This δ is a homomorphism, and by diagram chasing it follows that the sequence

$$0 \longrightarrow \mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), A) \longrightarrow \mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), B) \longrightarrow \mathcal{H}^0(\mathrm{Gal}(\bar{K}/K), C)$$

$$\xrightarrow{\delta} \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), A) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), B) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), C),$$

is exact.

Let now M be a discrete $\mathrm{Gal}(\bar{K}/K)$-module and L/K be a finite Galois extension. Since L/K is Galois the group $\mathrm{Gal}(\bar{K}/L)$ is a normal subgroup of $\mathrm{Gal}(\bar{K}/K)$. Further, it is known that

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L)$$

and

$$[\mathrm{Gal}(\bar{K}/K) : \mathrm{Gal}(\bar{K}/L)] = [L : K] < \infty.$$

This means that M can be considered as a discrete $\mathrm{Gal}(\bar{K}/L)$-module, and so both 1st cohomology groups, $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), M)$ and $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/L), M)$, are defined. If $\xi : \mathrm{Gal}(\bar{K}/K) \longrightarrow M$ is a 1-cochain, then its restriction $\xi|_{\mathrm{Gal}(\bar{K}/L)}$ is a 1-cochain from $\mathrm{Gal}(\bar{K}/L)$ to M. Therefore, it is clear that this restriction of ξ takes cocylces to cocycles and coboundaries to coboundaries. So, we obtain a *restriction homomorphism*

$$\mathrm{Res} : \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), M) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/L), M).$$

Since $\mathrm{Gal}(\bar{K}/L) \trianglelefteq \mathrm{Gal}(\bar{K}/K)$, the submodule

$$M^{\mathrm{Gal}(\bar{K}/L)} := \{m \in M \mid m^\sigma = m,\ \forall\, \sigma \in \mathrm{Gal}(\bar{K}/L)\}$$

is a $\mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L)$-module. This observation leads us to write the following composition of maps

$$\mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L) \xrightarrow{\xi} M^{\mathrm{Gal}(\bar{K}/L)} \hookrightarrow M,$$

where the map on the left is the natural projection and the map on the right is the natural inclusion. That is actually a 1-cochain of $\mathrm{Gal}(\bar{K}/K)$ to M. If ξ is a cocycle or coboundary, the composition has the same property as well. Thus, we obtain an *inflation homomorphism*

$$\mathrm{Inf} : \mathcal{H}^1\left(\mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L), M^{\mathrm{Gal}(\bar{K}/L)}\right) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), M).$$

Using these homomorphisms, the restriction and the inflation, we can construct the following exact sequence

$$0 \longrightarrow \mathcal{H}^1\left(\mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L), M^{\mathrm{Gal}(\bar{K}/L)}\right) \xrightarrow{\mathrm{Inf}} \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), M)$$

$$\xrightarrow{\mathrm{Res}} \mathcal{H}^1(\mathrm{Gal}(\bar{K}/L), M).$$

3.1.2. *The groups of Selmer and Shafarevich.* Let E be an elliptic curve defined over the rationals and $m \in \mathbb{N}$. Recall that the m-torsion subgroup of $E(\mathbb{Q})$ is defined by

$$E[m](\mathbb{Q}) = \{P \in E(\mathbb{Q}) \mid mP = O\}$$

and it holds that

$$E(\mathbb{Q})_{\mathrm{tor}} = \bigcup_{m \in \mathbb{N}} E[m](\mathbb{Q}).$$

Generally if an elliptic curve E is defined over a number field K, with $\bar{K}$ be its algebraic closure, then

$$E[m](\bar{K}) \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Moreover, if the field K is algebraically closed field, the m-multiplication of a point, that is, the homomorphism

$$\begin{aligned} [m] \quad : \quad & E(\bar{K}) \longrightarrow E(\bar{K}) \\ & P \longmapsto mP, \end{aligned}$$

is a surjective homomorphism (see [**18**], p. 98). We distinguish two cases. If $K = \mathbb{C}$, then

$$E[m](\mathbb{C}) \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

If K is algebraically closed but not the field of complex numbers, then $K \hookrightarrow \mathbb{C}$, and so it holds the same.

As we have mentioned the additive group $E(\bar{K})$ is a discrete $\mathrm{Gal}(\bar{K}/K)$-module. This means that the sequence

$$0 \longrightarrow E[m](\bar{K}) \longrightarrow E(\bar{K}) \longrightarrow E(\bar{K}) \longrightarrow 0,$$

is a short exact sequence, where the map on the right is the m-multiplication of points of $E(\bar{K})$. Hence, we have the exact sequence

$$0 \longrightarrow E[m](K) \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K}))$$

$$\longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K})) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K})),$$

where δ is the connecting homomorphism, as we defined it in the previous paragraph. We denote by $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K}))[m]$ the group of all elements of $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K}))$ that have order, which divides the natural number m. Then the sequence

$$\begin{aligned}(16)\qquad 0 \longrightarrow E(K)/mE(K) \xrightarrow{\delta} \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K}))&\\ \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K}))[m] \longrightarrow 0&\end{aligned}$$

is exact.

Our purpose now is to determine a bound for the quotient group $E(K)/mE(K)$. We observe that the group $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K}))$ depends only on the structure of the group $\mathrm{Gal}(\bar{K}/K)$, and not on the elliptic curve E, and if it is finite, then so is $E(K)/mE(K)$. But the group $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K}))$ is infinite. The basic idea in order to overcome this obstacle is to study our problem locally.

Let M_K be the set of all places of K and $v \in \mathrm{M}_K$. We denote by K_v the completion of K with respect to v, and by $\bar{K}_v$ its algebraic closure. Then it is easy to verify that

$$\mathrm{Gal}(\bar{K}_v/K_v) \leq \mathrm{Gal}(\bar{K}/K).$$

Indeed, the profinite group $\mathrm{Gal}(\bar{K}_v/K_v)$ acts on K_v, and a fortiori on K, since $K \leq K_v$. This means that each K_v-automorphism of $\bar{K}_v$, restricted to $\bar{K}$, can be seen as K-automorphism of $\bar{K}$. Also, since we have assumed that the elliptic curve E is defined over K and $K \leq K_v$, it is also defined over K_v. As in (16), we have an exact sequence

$$\begin{aligned}0 \longrightarrow E(K_v)/mE(K_v) \xrightarrow{\delta} \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E[m](\bar{K}_v))&\\ \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v))[m] \longrightarrow 0&\end{aligned}$$

of discrete $\mathrm{Gal}(\bar{K}_v/K_v)$-modules. Each 1-cochain of $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K}))$ induces a 1-cochain of $\mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v))$. This means that we shall define a homomorphsim

$$\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K})) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v)).$$

Similarly, we define a homomorphism

$$\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K})) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E[m](\bar{K}_v)).$$

Therefore, we obtain the following commutative diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & E(K)/mE(K) \arrow[r, "\delta"] \arrow[d] & \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K})) \arrow[r, "\varphi"] \arrow[d] \arrow[dr, dashed, "s"'] & \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K}))[m] \arrow[r] \arrow[d, "\psi"] & 0 \\
0 \arrow[r] & E(K_v)/mE(K_v) \arrow[r, "\delta"'] & \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E[m](\bar{K}_v)) \arrow[r] & \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v))[m] \arrow[r] & 0
\end{tikzcd}$$

We would like now to replace the cohomology group $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K}))$, with a subset of it, so that it contains the image $\delta(E(K)/mE(K))$. It is obvious that

$$\delta(E(K)/mE(K)) \subseteq \ker(\varphi).$$

This means that

$$\varphi(\delta(E(K)/mE(K))) = 0 \Rightarrow \psi\,(\varphi(\delta(E(K)/mE(K)))) = 0$$

$$\Rightarrow \delta(E(K)/mE(K)) \subseteq \ker(\psi \circ \varphi) = \ker(\mathrm{s}).$$

DEFINITION 3.9. The *m-Selmer group of an elliptic curve E defined over K*,which is denoted by $\mathrm{Sel}^{(m)}(E,K)$, is defined to be the kernel of the map s for all $v \in \mathrm{M}_K$. In other words,

$$\mathrm{Sel}^{(m)}(E,K) := \ker\left(\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K})) \longrightarrow \bigoplus_{v\in \mathrm{M}_K} \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v))[m]\right).$$

Analogously, we define *the Tate-Shafarevich group*, usually denoted by $\text{Ш}(E,K)$, as follows:

$$\text{Ш}(E,K) := \ker\left(\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K})) \longrightarrow \bigoplus_{v\in \mathrm{M}_K} \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v))\right).$$

REMARK 3.10. The Tate-Shafarevich group is the set of all elements of $\mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E(\bar{K}))$, so that restricted[4] to $v \in \mathrm{M}_K$, are equal to the identity. This means that this group gives us a measure of the difference between the local and the global.

LEMMA 3.11. *For each pair of homomorphisms of abelian groups $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$, the following sequence*

$$0 \longrightarrow \ker(\alpha) \longrightarrow \ker(\beta\circ\alpha) \longrightarrow \ker(\beta) \longrightarrow \mathrm{coker}(\alpha) \longrightarrow \mathrm{coker}(\beta\circ\alpha) \longrightarrow \mathrm{coker}(\beta) \longrightarrow 0.$$

is exact.

Using this lemma, we may prove that the

$$0 \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}/K), E[m](\bar{K})) \longrightarrow \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v))[m] \longrightarrow \bigoplus_{v\in \mathrm{M}_K} \mathcal{H}^1(\mathrm{Gal}(\bar{K}_v/K_v), E(\bar{K}_v))[m] \longrightarrow 0$$

is a short exact sequence. This means that the

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{Sel}^{(m)}(E,K) \longrightarrow \text{Ш}(E,K)[m] \longrightarrow 0$$

is a short exact sequence as well, where by $\text{Ш}(E,K)[m]$, we denote the group of all elements of the group $\text{Ш}(E,K)$, that they have order that divides m.

THEOREM 3.12. *The m-Selmer group $Sel^{(m)}(E,K)$ of an elliptic curve E defined over a number field K is finite, for each $m \in \mathbb{N}$.*

PROOF. (see [**15**], p. 110-117, or [**18**], p. 60-65) □

COROLLARY 3.13. *The groups $E(K)/mE(K)$ and $\text{Ш}(E,K)[m]$ are finite. In other words, the finiteness of the group $Sel^{(m)}(E,K)$ implies the weak Mordell-Weil theorem and the finiteness of the group $\text{Ш}(E,K)[m]$.*

[4] This restriction is induced by the inclusion $\mathrm{Gal}(\bar{K}_v/K_v) \subseteq \mathrm{Gal}(\bar{K}/K)$.

We are interested in the group $E(K)/mE(K)$, in order to determine the rank of the elliptic curve E. We just mentioned that the m-Selmer group is close to $E(K)/mE(K)$, meaning that the difference of the orders of these groups is finite. This difference is a number that depends on the choice of m.

Conjecture 3.14 (Tate). The Tate-Shafarevich group $Ш(E, K)$ of an elliptic curve E defined over K if finite.

Assuming the truth of the conjecture of Tate, we would be able to conclude, not only that the difference of the orders of $E(K)/mE(K)$ and $\mathrm{Sel}^{(m)}(E, K)$ is a number that is independent of the choice of m, but also that the two groups are equal for almost every $m \in \mathbb{N}$.

Till the end of 80's there was no known example of elliptic curve with finite Tate-Shafarevich group. This conjecture is still an open question. The importance of that conjecture will become more clear, when we will present the strong version of the Birch and Swinnerton-Dyer conjecture. We will mention some results at the end of the next paragraph.

3.2. The analytic approach. One of our goals is the formulation of the conjecture of Birch and Swinnerton-Dyer, as part of the study of elliptic curves over the rationals. The weak version of this conjecture is stated using L-series, and it turns out that L-series is a necessary tool for attacking many conjectures and open questions in number theory.

3.2.1. *The minimal discriminant.* We begin by considering an elliptic curve E defined over the rationals and given in long Weiestrass form, that is

$$E|_{\mathbb{Q}} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{17}$$

Without loss of generality we assume that $a_i \in \mathbb{Z}$, for every $i \in \{1, 2, 3, 4, 6\}$. Therefore, the discriminant Δ_E of the elliptic curve E is an integer number. Equivalently, it holds that $|\Delta_E|_p \leq 1$, for every prime number p. Further,

$$|\Delta_E|_p = 1 \Leftrightarrow p \nmid \Delta_E.$$

The problem now is that there are more than one long Weiestrass forms with integer coefficients for an elliptic curve E. Indeed, applying admissible change of variables, it is possible to get a long Weierstrass form with integer coefficients from another one with the same property. Such change of variables are of the form

$$X = u^2X' + r \quad \text{and} \quad Y = u^3Y' + su^2X' + t, \tag{18}$$

where $r, s, t, u \in \mathbb{Q}$ and $u \neq 0$. The observation that for such a form it holds that $|\Delta_E|_p \leq 1$, or equivalently $\upsilon_p(\Delta_E) \geq 0$, implies that the set

$$S_p := \{|\Delta_E|_p \mid E \text{ is given in long Weierstrass form with integer coefficients}\}$$

has an upper bound, and even better, a maximum.

Definition 3.15. Let E be an elliptic curve defined over the rationals and p be a prime number. The equation (17) is called *p-minimal model of E*, if the number $|\Delta_E|_p$, where Δ_E is the discriminant of E , is equal to the maximal element of the set S_p. If (17) is p-minimal model for every prime number p, then it is called *global minimal model of E*.

The next result ensures that there exists a minimal model for every elliptic curve over the rationals, and so we may assume that every elliptic curve is given in long Weierstrass form, which is a global minimal model.

THEOREM 3.16 (NÉRON). *Given an elliptic curve E over the rationals, there exists an admissible change of variables, so that the resulting equation is a global minimal model for E. Two global minimal models for an elliptic curve E are related by an admissible change of variable of the form* (18)*, such that $r, s, t \in \mathbb{Z}$ and $u \in \{-1, 1\}$.*

REMARK 3.17. We can generalize the notion of the global minimal model to elliptic curves defined over an arbitrary number fields. For the elliptic curve E over K, we are able to define the v-minimal model of an elliptic curve for any $v \in \mathrm{M}_K$. However, it is not sure if a given elliptic curve has global minimal model, i.e. Néron's theorem is not true for elliptic curves over number fields.

3.2.2. *Reduction of elliptic curves over* $\mathbb{Q}$. We first dealt with the idea of reduction modulo prime number for the proof of the Lutz-Nagell theorem. We will now give more details, that we will need in order to define the conductor and so, the L-series of an elliptic curve.

Let E be an elliptic curve over the rationals and p be a prime number. The curve that is obtained after reduction modulo p is not necessarily an elliptic curve, too. In case it is we say that E has good reduction at p. Otherwise, it is a singular cubic curve. This means that E_p has a unique singularity, which is either a node, or a cusp.

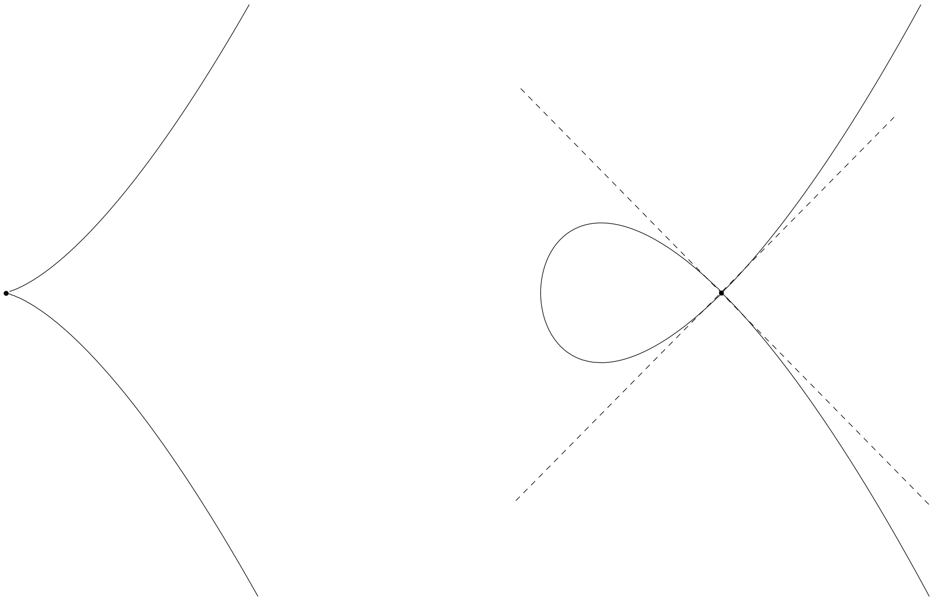


FIGURE 2. Affine picture of an elliptic curve with cusp (on the left), and an elliptic curve with a nodal point and the tangents on it (on the right).

These two cases of singularities leads us to discrete to different types of bad reduction.

DEFINITION 3.18. Let E be an elliptic curve and p be a prime, so that E has bad reduction at p. We say that E has *multiplicative reduction modulo p*, if the singularity of the curve E_p is a node. Otherwise, we say that E has *additive reduction at p.*

In case of multiplicative reduction we have to give an extra characterization, depending on where the tangents are defined.

Definition 3.19. Let E be an elliptic curve over $\mathbb{Q}$ and p be a prime number, such that E has multiplicative reduction at p. Then the multiplicative reduction at p is said to be *split*, if the slopes of the tangent lines at the node are in $\mathbb{F}_p$, and nonsplit otherwise.

Definition 3.20. Let E be an elliptic curve over the rationals and

$$f_p := \begin{cases} 0 & \text{, if } E \text{ has good reduction at } p, \\ 1 & \text{, if } E \text{ has multiplicative reduction modulo } p \text{ at } p, \\ 2 & \text{, if } E \text{ has additive reduction modulo } p \text{ and } p \notin \{2,3\}, \\ 2+\delta_p & \text{, if } E \text{ has additive reduction modulo } p \text{ and } p \in \{2,3\} \end{cases},$$

where δ_p is defined by Ogg's formula (see [**16**]) and is calculated by Tate's algorithm (see [**22**]). The natural number

$$N_E = \prod_{p \text{ prime}} p^{f_p},$$

is called *conductor of E*.

3.2.3. *Elliptic curves defined over finite fields.* We are interested now in elliptic curves over finite fields. Let q be a prime number and E be an elliptic curve over the finite field $\mathbb{F}_q$. We would like to valuate the order of the group $E(\mathbb{F}_q)$, that is to find appropriate upper bound for the number $N(q) := \#E(\mathbb{F}_q)$. We assume that E is defined by an equation of the form 17, i.e. a long Weierstrass form with integer coefficients. Using the observation that for any x, we get at most two different values of y, we conlude that

$$1 \leq N(q) \leq 1 + 2q.$$

But this is a rather not so useful bound and of course it is not the best possible. Heuristically, we would expect that for any quadratic equation of variable Y in terms of a given X, there exists a solution with probability $1/2$. This means that perhaps the number $1 + q$ is close to $N(q)$. Up to an error of $2\sqrt{q}$ this is true, due to Hasse's work.

Theorem 3.21 (Hasse). *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. Then*

$$|N(q) - (1+q)| \leq 2\sqrt{q}.$$

Proof. (see [**7**]) □

This is a result of great importance since it is equivalent to the Riemann hypothesis for elliptic curves. An elementary proof was given by Manin (see [**4**], or [**13**]).

3.2.4. *Definition of $L(E, s)$ and their properties.* The algebraic approach we tried in order to compute the rank of an elliptic curve E over the rationals is not useful enough. We obtained an upper bound by computing the order of the group $\mathrm{Sel}^{(m)}(E, \mathbb{Q})$, but the difference between this order and the rank of E, is given by the mysterious group $\text{Ш}(E, \mathbb{Q})$.

This conversation makes it clear that we need to try a different approach. The idea of Birch and Swinnerton-Dyer was elementary. They claimed that, if the rank of E is a large number, then so is $N(p)$ for many primes p. The two mathematicians worked on this idea at late 50's until early 60's (see [**2**]). They computed the value of the function

$$f(B) = \prod_{\substack{p \text{ prime} \\ p \leq B}} \frac{N(p)}{p},$$

for several positive real numbers B. The conclusion was the statement of the following conjecture.

CONJECTURE 3.22. For every elliptic curve E over the rationals, with rank r, there is a constant c, so that

$$\lim_{B \to +\infty} \frac{f(B)}{c(\log B)^r} = 1.$$

Or equivalently,

$$f(B) \sim c(\log B)^r,$$

as $B \to +\infty$.

This conjecture anticipates that the computation of the rank r is possible if we compute the values of $N(p)$ and constant c. However, Birch and Swinnerton-Dyer observed that as B increases, the constant c can not be determined explicitly, not even approximated with accuracy. They modified their idea, and so the conjecture itself.

To do so, they defined the L-series of an elliptic curve, using the ζ-function of an elliptic curve over the rationals. Consider an elliptic curve E defined over $\mathbb{Q}$ and given by a global minimal model. In this case the reduction modulo some prime p is singular if, and only if $p \mid \Delta_E$, where Δ_E is the discriminant of E. Since the conductor N_E of E has the same prime factors with the discriminant of E, then

$$p \mid \Delta_E \Leftrightarrow p \mid N_E.$$

We will define the L-series of E locally, i.e. for any prime number. Let p be a prime number. If E has good reduction modulo the prime p, then the L-series is defined, as follows

$$L_p(E, T) := 1 - a(p)T + pT^2,$$

where $a(p) := p + 1 - N(p)$. Otherwise, we define

$$L_p(E, T) := 1 - a(p)T,$$

where

$$a(p) := \begin{cases} 1 & \text{, if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{, if } E \text{ has nonsplit multiplicative reduction at } p \\ 0 & \text{, if } E \text{ has additive reduction at } p \end{cases}.$$

DEFINITION 3.23. The L-series of the elliptic curve E over $\mathbb{Q}$, is defined by

$$L(E, s) = \prod_{p \text{ prime}} L_p(E, p^{-s})^{-1},$$

for each $s \in \mathbb{C}$.

Due to Hasse's theorem, it can be proven that the infinite product which defines the L-function converges for all $s \in \mathbb{C}$, such that $\Re(s) \geq \frac{3}{2}$. Let, now,

$$\Lambda(E,s) := (2\pi)^{-s} N_E{}^{\frac{s}{2}} \Gamma(s) L(E,s).$$

Conjecture 3.24. The L-series $L(E,s)$ has an analytic continuation to the entire complex plane and satisfies the functional equation

$$\Lambda(E,s) = w\Lambda(E,2-s),$$

where $w \in \{-1,1\}$

This conjecture was proven by Deuring for elliptic curves with complex multiplication. Wiles and R. Taylor (see [**25**] and [**23**]) proved it in case of square free conductor. Finally, the conjecture was proven for all elliptic curves over the rationals by Breuil, B. Conrad, Diamond and R. Taylor (see [**3**]).

The number w in the conjecture is called root number, and the order of the root 1 of $\Lambda(E,s)$ depends on it. If for example $w=-1$, then

$$\Lambda(E,1) = -\Lambda(E,2-1) \Rightarrow \Lambda(E,1) = 0.$$

Further, it holds that

$$w = (-1)^{\mathrm{ord}_{s=1}(L(E,s))}.$$

Now we are ready to state the weak version of Birch and Swinnerton-Dyer.

Conjecture 3.25 (Birch, Swinnerton-Dyer). Let E be an elliptic curve over the rationals. Then

$$\mathrm{ord}_{s=1}(L(E,s)) = \mathrm{rank}(E).$$

In other words, the conjecture informs us the the Taylor expansion of the L-series of E at $s=1$, is of the form

$$L(E,s) = a(s-1)^r + \text{higher order terms},$$

such that $a \neq 0$ and $r = \mathrm{rank}(E)$. Consequently,

$$L(E,1) = 0 \Leftrightarrow E(\mathbb{Q}) \text{ is infinite}.$$

An indicative of the significance and the elegance of the conjecture of Birch and Swinnerton-Dyer is that it is one of the seven millennium problems, that Clay Mathematical Institute announced on May, 2000, in Paris.

The first general result regarding this conjecture is due to Coates and Wiles (see [**5**]).

Theorem 3.26 (Coates,Wiles). *If E is an elliptic curve over the rationals, with complex multiplication, then*

$$\mathrm{rank}(E) \geq 1 \Rightarrow L(E,1) = 1.$$

As a combination of the results of Gross and Zagier (see [**6**]) and Kolyvagin (see [**10**]), we have the following theorem

THEOREM 3.27 (GROSS,ZAGIER, KOLYVAGIN). *Let E be an elliptic curve defined over $\mathbb{Q}$. If*

$$ord_{s=1}(L(E,s)) \leq 1,$$

then the Birch and Swinnerton-Dyer conjecture is true, that is

$$rank(E) = ord_{s=1}(L(E,s)),$$

and the group $Ш(E,\mathbb{Q})$ is finite.

This result has been generalized by Zhang (see [**26**]) for modular elliptic curves defined over totally real number fields.

The weak version of the conjecture was stated in 1963. There exists also a strong version of the Birch and Swinnerton-Dyer conjecture, stated in 1965. In order ti formulate it, we need some additional notions.

- Let
$$E_0(\mathbb{Q}_p) := \left\{P \in E(\mathbb{Q}_p) \mid P \pmod{p} \in E_p^{\text{ns}}(\mathbb{F}_p)\right\}$$
This is a subgroup of $E(\mathbb{Q}_p)$, and so we define the index
$$c_p := [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)].$$
Of course, if E has good reduction at a prime p, then $c_p = 1$. This means that the number c_p is equal to 1 for almost every prime number p.
- Ω is the positive real period of the differential form
$$\omega := \frac{dy}{2y}$$
up to the number of connected components of E, that is
$$\Omega = \nu \int_{E(\mathbb{R})} |\omega|,$$
where by ν we define the number of connected components of E. It is known that
$$\int_{E(\mathbb{R})} |\omega| = \frac{c_p N_p}{p}.$$
For the proof of this equation Haar measure is used.
- We know (see Appendix B), that for any elliptic curve E, we can define the Néron-Tate pairing
$$\begin{aligned} \langle\cdot,\cdot\rangle \quad : \quad & E(\bar{K}) \times E(\bar{K}) \longrightarrow \mathbb{R} \\ & (P,Q) \longmapsto \hat{h}_E(P+Q) - \hat{h}_E(P) - \hat{h}_E(Q). \end{aligned}$$
This is a $\mathbb{Z}$-bilinear basis. If the set $\{P_1, P_2, \ldots, P_r\}$, with $r = \text{rank}(E)$, is a $\mathbb{Z}$-basis of the quotient group $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tor}}$, then we define the regulator of E, by
$$\text{Reg}(E,\mathbb{Q}) := \det\left(\langle P_i, P_j\rangle_{1\leq i,j\leq r}\right).$$
We note that if E has zero rank then $\text{Reg}(E,\mathbb{Q}) := 1$. Since the canonical height $\hat{h}_E$ is a positively defined quadratic form, the regulator is a positive number.

Conjecture 3.28 (Birch, Swinnerton-Dyer). Let E be an elliptic curve over the rationals, so that $r = \operatorname{rank}(E)$. Then

$$\lim_{s\to 1}\left((s-1)^{-r}L(E,s)\right) = |E(\mathbb{Q})_{\mathrm{tor}}|^{-2}\cdot\Omega\cdot\prod_{p\text{ prime}} c_p\cdot|\text{Ш}(E,\mathbb{Q})|\cdot\operatorname{Reg}(E,\mathbb{Q}).$$

Remark 3.29. (i) Every number that appears in the strong version of the Birch and Swinnerton Dyer conjecture, except for the order of the Tate-Shafarevich group $\text{Ш}(E,\mathbb{Q})$, can be computed by programs such as PARI, SAGE e.t.c.

(ii) The number

$$\det\left(\langle P_i,P_j\rangle_{1\le i,j\le r}\right)/\left[E(\mathbb{Q}):\sum_{i=1}^{r}P_i\mathbb{Z}\right]$$

is independent of the choice of P_i's. It turns out that it is also equal to the number

$$|E(\mathbb{Q})_{\mathrm{tor}}|^{-2}\cdot\operatorname{Reg}(E,\mathbb{Q}).$$

We finish this section chapter with the remark that until today, all the partial results that have been proved, indicate that the conjecture of Birch and Swinnerton-Dyer is true. As an indication of that, we mention that Bhargava, Skinner and Zhang proved that the majority of elliptic curves, that is at least the $66,48\%$ of them, have rank equal to 0 or 1, and so they satisfy the desired conjecture (see [**1**]). Also, this lower bound can be improved.

As it seems from this brief introduction to this field of mathematics, there are interesting open problems and questions to be answered, including the Birch and Swinnerton-Dyer conjecture.

All we have to do is keep searching for answers...

Appendix A: Valuations and Absolute Values

In this paragraph we present elements of the theory of valuations that are necessary for the definition of heights and the proof of their properties.

Given a real or complex number, a naive measure of its size is its absolute value, which actually indicates its distance from the origin of the real axis or the origin of the complex plane, respectively. We would like to generalize the notion of the absolute values to algebraic number fields.

Definition 3.30. Let K be a number field. A real-valued *absolute value*, is called a map

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0},$$

that, for each $\alpha, \beta \in K$, satisfies the following properties:

(i) $|\alpha| = 0 \Leftrightarrow \alpha = 0$.
(ii) Multiplicative: $|\alpha\beta| = |\alpha| \cdot |\beta|$.
(iii) Triangle inequality: $|\alpha + \beta| \leq |\alpha| + |\beta|$.

If the absolute value, satisfies the following property:

(iii)* Ultrametric inequality: $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$,

then it is called *nonarchimedean*[5]. Otherwise, it is called *archimedean*.

Definition 3.31. Let K be a number field and $|\cdot|_1$ and $|\cdot|_2$ two real-valued absolute values of K. These are called *equivalent*, if it holds that

$$|\alpha|_1 < 1 \Leftrightarrow |\alpha|_2 < 1,$$

for every $\alpha \in K$.

Using this definition, we are able to prove the following result, which is a probably more helpful characterization of the equivalence of absolute values.

Proposition 3.32. *Let K be a number field and $|\cdot|_1$ and $|\cdot|_2$ two real-valued absolute values of K. These are equivalent if, and only if, there is a positive real number s, such that*

$$|\alpha|_2 = {|\alpha|_1}^s,$$

for each $\alpha \in K$.

[5] The ultrametric inequality is stronger than the triangle inequality. Obviously, every nonarchimedean absolute value satisfies the triangle inequality.

This proposition makes it clear that, what we defined as equivalence of real-valued absolute values of a number field, is actually an equivalence relation. This leads us to the following definition.

Definition 3.33. An equivalence class of absolute values of a number field K is called *place of K*. The set of all places of the number field K is denoted by M_K. Moreover, we denote the set of all archimedean places of K, by M_K^∞.

By definition, an absolute value is a multiplicative map. The exponential analogous of the absolute value, is also important.

Definition 3.34. Let K be a number field and

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\},$$

be a map, which satisfies the following properties:

(i) $v(\alpha) = \infty \Leftrightarrow \alpha = 0$,
(ii) $v(\alpha\beta) = v(\alpha) + v(\beta)$, for any $\alpha, \beta \in K$, and
(iii) $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$. The equality holds in case $v(\alpha) \neq v(\beta)$.

The map v is called *(real-valued) valuation of K*.

Remark 3.35. As it is obvious the notions of valuations and absolute values are dual. Some authors use the term "exponential valuation", rather than "valuation". In this case the terms "valuation" and "absolute value" are identified.

Remark 3.36. Given a valuation v of K, we can define a (nonarchimedean) absolute value $|\cdot|$, by

$$|\alpha| := c^{v(\alpha)},$$

with c is a real number such that $0 < c < 1$. The inverse is also true. Given an absolute value $|\cdot|$, we can define a valuation v as the logarithm of the absolute value, i.e. by

$$v(\alpha) := \log_c |\alpha|,$$

such that $0 < c < 1$, with the convention $v(0) := \infty$.

We begin with the most simple number field, the field $\mathbb{Q}$. The only archimedean absolute value is the usual one, and it is denoted by $|\cdot|_\infty$. In other words, if $\alpha \in \mathbb{Q}$, then

$$|\alpha|_\infty = \max\{-\alpha, \alpha\}.$$

We want to determine the nonarchimedean absolute valuations. Every rational number α is written uniquely in the form

$$\alpha = \mathrm{sign}(\alpha) \prod_{i=1}^{r} {p_i}^{n_i},$$

where $\mathrm{sign}(\alpha) \in \{-1, 1\}$, p_i's are prime numbers and $n_i \in \mathbb{Z}$, for every $i \in \{1, 2, \ldots, r\}$. For any prime p, we define the map

$$\begin{aligned} v_p \quad : \quad & \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\} \\ & \alpha \longmapsto \begin{cases} n_i & \text{, if } p = p_i \text{, for some } i \in \{1, 2, \ldots, r\} \\ 0 & \text{, if otherwise} \end{cases}, \end{aligned}$$

with the the convention that $\upsilon(0) = \infty$. We define now the map

$$\begin{aligned} |\cdot|_p \quad : \quad & \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0} \\ & \alpha \longmapsto p^{-\upsilon_p(\alpha)} \end{aligned}$$

It follows easily that υ_p is a valuation[6] of $\mathbb{Q}$ and $|\cdot|_p$ is an nonarchimedean absolute value of $\mathbb{Q}$.

Definition 3.37. The valuation υ_p, is called *p-adic valuation of* $\mathbb{Q}$ and the absolute value $|\cdot|_p$ is called *p-adic absolute value*, or *p-adic norm of* $\mathbb{Q}$.

By the definition of p-adic absolute values, we obtain a bijection between p-adic valuations and p-adic absolute values. Indeed, if $\alpha \in \mathbb{Q}$, then

$$|\alpha|_p = p^{-\upsilon_p(\alpha)} \Leftrightarrow \upsilon_p(\alpha) = -\log_p(|\alpha|_p).$$

Proposition 3.38. *Every archimedean real-valued absolute value of* $\mathbb{Q}$ *is equivalent to the usual one, i.e. to the absolute value* $|\cdot|_\infty$*, and every nonarchimedean real-valued absolute value of* $\mathbb{Q}$ *is equivalent to a p-adic norm* $|\cdot|_p$*, for some prime number p.*

Let now $p \in \mathrm{M}_{\mathbb{Q}}$ be a place[7] of $\mathbb{Q}$ and $|\cdot|_p$ its representative. The absolute value $|\cdot|_p$ induces a metric

$$d_p(x,y) := |x-y|_p \quad , \quad \forall\, x,y \in \mathbb{Q}.$$

We denote by $\mathbb{Q}_p$ the completion of the field $\mathbb{Q}$, with respect to the metric d_p. It is also known that equivalent absolute values induce the same completion of $\mathbb{Q}$. If the absolute value $|\cdot|_p$ is equivalent to the usual one, which symbolically means that $p = \infty$, then the completion is the field $\mathbb{R}$ of the real numbers, i.e. $\mathbb{Q}_\infty = \mathbb{R}$. Otherwise, the absolute value $|\cdot|_p$ is a p-adic norm $|\cdot|_p$, and so the completion is the field $\mathbb{Q}_p$, i.e. the field of p-adic rational numbers.

A natural question that arises is why we choose the p-adic norms as representatives of the equivalence classes of $\mathrm{M}_{\mathbb{Q}}$. The answer is given by the following proposition, which is an immediate consequence of the uniqueness of the factorization of a rational into prime numbers.

Proposition 3.39 (Product Formula). *Let* $\alpha \in \mathbb{Q}$*. Then*

$$|\alpha|_\infty \prod_{p\ prime} |\alpha|_p = 1.$$

We would like, now, to study the absolute values of number fields. One of our purposes is to define the representatives of places, in a way that they satisfy a relation like the product formula. In order to do that we need some notation.

Definition 3.40. Let L/K be an extension of number fields, $v \in \mathrm{M}_K$ and $w \in \mathrm{M}_L$. We say that *w lies over v*, or *w is an extension of v*, and we write $w \mid v$, if the restriction of w to K is v, i.e. if $w|_K = v$.

[6] More precisely, υ_p is a discrete valuation.

[7] By that we mean that p is equal either to a prime number, or to ∞.

Let $|\cdot|_p$ be a representative of the place $v \in \mathrm{M}_K$. Then this absolute value induces a metric d_v, as in the case of $\mathbb{Q}$. We denote by K_v, the completion of K, with respect to v. Easily follows that if v is a place of the number field K, its restriction in $\mathbb{Q}$ a place p of $\mathbb{Q}$, and the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ is a subfield of the completion K_v of K, with respect to v.

Definition 3.41. Let K be a number field and $v \in \mathrm{M}_K$, which is extension of the place p of $\mathbb{Q}$. The local degree of v is the number

$$n_v := [K_v : \mathbb{Q}_p].$$

We shall generalize the definition of the local degree to any extension of number fields, and study the relation of it with the global degree of the extension. This leads us to the following well-known result.

Proposition 3.42 (Degree Formula). *Let L/K be an extension of number fields, and let $v \in M_K$. Then*

$$[L : K] = \sum_{w|v} [L_w : K_v].$$

Proof. (see [**12**], p. 14) □

Definition 3.43. Let $|\cdot|_v$ be an absolute value corresponding to the place $v \in \mathrm{M}_K$. If by n_v we denote the local degree of v, the *normalized absolute value associated to* v is the $||\cdot||_v$, defined by

$$||\alpha||_v := |\alpha|_v{}^{n_v}$$

for each $\alpha \in K$.

Using the degree formula, we can prove the next result.

Proposition 3.44. *Let K be a number field, $\alpha \in K$, and $|\cdot|_v$ be an absolute value of $\mathbb{Q}$ corresponding to the place $v \in M_{\mathbb{Q}}$. Then*

$$\prod_{w|v} ||\alpha||_w = |N_{K/\mathbb{Q}}(\alpha)|_v.$$

Proof. (see [**11**], p. 39) □

Proposition 3.45 (Generalized Product Formula). *Let K be a number field and $v \in M_K$. Then for each $\alpha \in K^\times$, it holds that*

$$\prod_{v \in M_K} ||\alpha||_v = 1.$$

Proof. (see [**8**],p. 172) □

We want now to describe precisely the absolute values of a number field K. Let $n = [K : \mathbb{Q}]$. We begin with the description of the archimedean absolute values of K. The field K admits n pairwise distinct embeddings $\sigma : K \hookrightarrow \mathbb{C}$. Each of these embeddings define an absolute value, by

$$|\alpha|_\sigma = |\sigma(\alpha)|_\infty \quad , \quad \forall\, \alpha \in K$$

where by $|\cdot|_\infty$ we denote the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$. Of course, these embeddings are either real, if $\sigma(K) \subseteq \mathbb{R}$, or complex, if $\sigma(K) \not\subseteq \mathbb{R}$. In the case of complex embeddings, it is easy to verify that conjugate complex embeddings define the same absolute value. The opposite is also true. Let $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{C}$ be two embeddings of the number field K to the complex field $\mathbb{C}$. Then $|\cdot|_{\sigma_1} = |\cdot|_{\sigma_2}$ if, and only if σ_1 and σ_2 are complex conjugate embeddings of K.

We turn our attention to the nonarchimedean absolute values of K. In the case of $\mathbb{Q}$, we used the p-adic valuations, in order to describe the p-adic norms. We will do the same, except we will use the prime ideals of K. Let R_K be the ring of the algebraic integers of K and $\mathfrak{p}$ be a prime ideal of K which lies above the prime number p, i.e. a prime ideal $\mathfrak{p}$ of the ring R_K, such that $\mathfrak{p} \mid pR_K$. Using the fact that R_K is a Dedekind domain, we extend the notion of p-adic valuations to the notion of $\mathfrak{p}$-adic valuations. Let $\alpha \in K$. For the ideal $\langle\alpha\rangle$, we know that there is unique factorization into prime ideals, up to rearrangement, of the form

$$\langle\alpha\rangle = \prod_{i=1}^{r} \mathfrak{p}_i{}^{n_i},$$

where $\mathfrak{p}_i$ is a prime ideal and $n_i \in \mathbb{Z}$, for every $i \in \{1, 2, \ldots, r\}$. Then the map

$$\begin{aligned} v_\mathfrak{p} \quad : \quad & K \longrightarrow \mathbb{Z} \cup \{\infty\} \\ & 0 \longmapsto \infty \\ & \alpha \longmapsto \begin{cases} n_i & , \text{if } \mathfrak{p} = \mathfrak{p}_i \ , \ i \in \{1, 2, \ldots, r\} \\ 0 & , \text{otherwise} \end{cases} \end{aligned}$$

is a valuation[8]. Since the prime ideal $\mathfrak{p}$ lies above the prime number p, the $\mathfrak{p}$-adic absolute value is an extension of the p-adic norm. So, we would like to define a $\mathfrak{p}$-adic absolute value $|\cdot|_\mathfrak{p}$, such that

$$|p|_\mathfrak{p} = |p|_p = p^{-1}.$$

In order to accomplish that, we need to define $|\cdot|_p$ using the ramification index[9] $e_\mathfrak{p}$ of $\mathfrak{p}$. Indeed, we define the $\mathfrak{p}$-adic norm, as follows

$$\begin{aligned} |\cdot|_\mathfrak{p} \quad : \quad & K \longrightarrow \mathbb{R}_{\geq 0} \\ & \alpha \longmapsto p^{-v_\mathfrak{p}(\alpha)/e_\mathfrak{p}} \end{aligned}$$

The normal absolute value associated to the prime ideal $\mathfrak{p}$ is defined by,

$$\|\alpha\|_\mathfrak{p} := (N_{K/\mathbb{Q}}(\mathfrak{p}))^{-v_\mathfrak{p}(\alpha)},$$

for every $\alpha \in K$.

The above discussion for the absolute values of a number field K, is summarized in the next proposition.

Proposition 3.46. *Let K be a number field of degree n over $\mathbb{Q}$.*

[8] Actually, like p-adic valuations, the map v_p is also a discrete valuation

[9] The ramification index of the prime ideal $\mathfrak{p}$ is the nonnegative integer number $e_\mathfrak{p}$, with the property that $\mathfrak{p}^{e_\mathfrak{p}} \| \langle p\rangle$.

(i) *Let* $\sigma_1, \sigma_2, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ *be the real embeddings of* K *and* $\tau_1, \overline{\tau}_1, \tau_2, \overline{\tau}_2, \ldots, \tau_s, \overline{\tau}_s : K \hookrightarrow \mathbb{C}$ *be the complex embeddings of* K*. Then, there is a bijection*

$$M_K^{\infty} \longleftrightarrow \{\sigma_1, \sigma_2, \ldots, \sigma_r, \tau_1, \tau_2, \ldots, \tau_s\} \quad , \quad \varrho \longmapsto |\cdot|_{\varrho}.$$

(ii) *Let* R_K *be the ring of algebraic integers of the field* K*. Let also* p *be a prime number, such that*

$$pR_K = \prod_{i=1}^{r} \mathfrak{p}_1{}^{e_1}.$$

Then there is a bijection

$$\{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r\} \longleftrightarrow \{p\text{-adic valuations on } K\} \quad , \quad \mathfrak{p} \longmapsto \|\cdot\|_{\mathfrak{p}}$$

Consequently, a number field K has one absolute value for each prime ideal, one absolute value for each real embedding and one for each pair of conjugate complex embedding of K. Further, the set of all nonarchimedean absolute values corresponds to the set of all prime ideals.

Let now K be a number field and σ be an automorphism of $\bar{K}$. Then σ induces an isomorphism $\sigma : K \longrightarrow \sigma(K)$. We could likewise identify the sets M_K and $\mathrm{M}_{\sigma(K)}$. Indeed, if for each $v \in \mathrm{M}_K$, we define

$$|\sigma(\alpha)|_{\sigma(v)} := |\alpha|_v,$$

then the map

$$\begin{aligned} \hat{\sigma} \quad : \quad \mathrm{M}_K &\longrightarrow \mathrm{M}_{\sigma(K)} \\ v &\longmapsto \sigma(v) \end{aligned}$$

is a bijection. So, it follows that $K_v \cong \sigma(K)_{\sigma(v)}$ and so the local degrees n_v and $n_{\sigma(v)}$ are equal.

Appendix B: Néron-Tate Height

Given elliptic curve E defined over a number field K we defined the height and the logarithmic height of a point on E. Particularly, for two points $P, Q \in E(\bar{K})$ we proved that there are constants $c_1, c_2 > 0$, that depend only on E, so that

$$2h_E(P) + 2h_E(Q) - c_1 \leq h_E(P+Q) + h_E(P-Q) \leq 2h_E(P) + 2h_E(Q) + c_2.$$

Using to $O(1)$ notation[10], we have that

$$h_E(P+Q) + h_E(P-Q) = 2h_E(P) + 2h_E(Q) + O(1).$$

It is clear now that the logarithmic height on E satisfies the parallelogram law up to an error, which is expressed by this $O(1)$. Similarly, by the descent theorem, we obtain that

$$h_E(mP) = m^2 h_E(P) + O(1),$$

for each $P \in E(\bar{K})$ and $m \in \mathbb{Z}$. A natural question that arises is if we could modify the logarithmic height h_E, so that it becomes a quadratic form.

That was exactly the idea of Néron. He wondered if there is a function which is a quadratic form and its difference from the height is bounded. To be precise, Néron gave the answer for every height defined by a morphism, but we will stick to the case of h_E.

We begin with the following observation. For each $n \in \mathbb{N}$, we have that

$$h_E(2^n P) = 4h_E(2^{n-1}P) + O(1) = 4^2 h_E(2^{n-2}P) + O(1) = \cdots = 4^n h_E(P) + O(1).$$

Therefore, it follows that

$$\frac{h_E(2^n P)}{4^n} = h_E(P) + \frac{O(1)}{4^n}.$$

From this equation we conclude that if the sequence $4^{-n} h_E(2^n P)$ converges, then the limit possibly has the desired properties.

Lemma 3.47. *For every $P \in E(\bar{K})$, the sequence $4^{-n} h_E(2^n P)$ is a Cauchy sequence.*

Proof. Let $P \in E(\bar{K})$ and $m, n \in \mathbb{N}$, such that $n \geq m$. We have

$$\left|\frac{h_E(2^n P)}{4^n} - \frac{h_E(2^m P)}{4^m}\right| = \left|\sum_{i=m}^{n-1} \frac{h_E(2^{i+1}P)}{4^{i+1}} - \frac{h_E(2^i P)}{4^i}\right| \leq \left|\sum_{i=m}^{n-1} \frac{1}{4^{i+1}} \left(h_E(2^{i+1}P) - 4h_E(2^i P)\right)\right|.$$

We know that

$$h_E(2(2^i P)) = 4h_E(2^i P) + O(1),$$

[10] When we write that $f = O(1)$ for a function f, we mean that f is bounded by a constant, i.e. there exists $M > 0$, so that $|f(x)| \leq M$, for each x in which f is defined.

so there exists a constant $c > 0$, so that

$$\left|\frac{h_E(2^nP)}{4^n} - \frac{h_E(2^mP)}{4^m}\right| \leq \sum_{i=m}^{n} \frac{c}{4^{i+1}} \leq \frac{c}{3 \cdot 4^m}.$$

Now it is immediate that the sequence $4^{-n}h_E(2^nP)$ is Cauchy. □

Definition 3.48. Let E be an elliptic curve over K, and $P \in E(\bar{K})$. We define the *canonical height* or the *Néron-Tate height of* P, by

$$\hat{h}_E(P) := \lim_{n\to+\infty} \frac{h_E(2^nP)}{4^n}.$$

Proposition 3.49. *Let E be an elliptic curve defined over the number field K.*

(i) For each $P \in E(\bar{K})$, it holds that

$$\hat{h}_E(2P) = 4\hat{h}_E(P).$$

(ii) For every $P \in E(\bar{K})$, we have that

$$\hat{h}_E(P) = h_E(P) + O(1).$$

(iii) For each $B \in \mathbb{R}_{>0}$, the set

$$\{P \in E(K) \mid \hat{h}_E(P) \leq B\}$$

is finite.

(iv) For each point $P \in E(\bar{K})$, we have that $\hat{h}_E(P) \geq 0$. The equality holds if, and only if P is a torsion point of E.

Proof. (i) We have that

$$\hat{h}_E(2P) = \lim_{n\to+\infty} \frac{h_E(2^n \cdot 2P)}{4^n} = \lim_{n\to+\infty} \frac{h_E(2^{n+1}P)}{4^n} = 4 \lim_{n+1\to+\infty} \frac{h_E(2^{n+1}P)}{4^{n+1}} = 4\hat{h}_E(P).$$

(ii) It is immediate from the equation

$$\frac{h_E(2^nP)}{4^n} = h_E(P) + \frac{O(1)}{4^n}.$$

(iii) From (ii), we have that

$$|\hat{h}_E(P) - h_E(P)| \leq c,$$

for some positive constant c. Then

$$\hat{h}_E(P) \leq B \Leftrightarrow h_E(P) \leq B + h_E(P) - \hat{h}_E(P) \leq B + |h_E(P) - \hat{h}_E(P)| \leq B + c.$$

That is

$$\{P \in E(K) \mid \hat{h}_E(P) \leq B\} \subseteq \{P \in E(K) \mid h_E(P) \leq B + c\}.$$

But the last set is finite due to 2.29. This means that the desired set is also finite.

(iv) The fact that $\hat{h}_E(P) \geq 0$ is immediate by its definition. We will prove now that

$$\hat{h}_E(P) = 0 \Leftrightarrow P \in E(\bar{K})_{\text{tor}}.$$

($\Leftarrow$) Let P be a torsion point of E. This means that the set

$$\{2^nP \mid n \in \mathbb{N}_0\}$$

is finite. This means that there exists a positive constant D, so that

$$h_E(2^nP) \leq D \quad , \quad \forall\, n \in \mathbb{N}_0.$$

Thus,

$$\frac{h_E(2^nP)}{4^n} \leq \frac{D}{4^n} \quad , \quad \forall\, n \in \mathbb{N}_0.$$

Taking $n \to +\infty$ we obtain that $\hat{h}_E(P) \leq 0$. And since we know that the Néron-Tate height is nonnegative number, it follows that $\hat{h}_E(P) = 0$.
($\Rightarrow$) Let $P \in E(\bar{K})$, so that $\hat{h}_E(P) = 0$. By (ii) we have that

$$\hat{h}_E(P) = h_E(P) + O(1) \Rightarrow h_E(P) = O(1) \Rightarrow \exists\, c > 0 : |h_E(P)| \leq c.$$

And since $h_E(P) \geq 0$, we have that $h_E(P) \leq c$. From (i) it follows by induction, that

$$\hat{h}_E(2^nP) = 4^n\hat{h}_E(P) = 0.$$

Hence,

$$\{2^nP \mid n \in \mathbb{N}_0\} \subseteq \{Q \in E(\bar{K}) \mid h_E(Q) \leq c\}.$$

The set on the right is finite, and so is the set $\{2^nP \mid n \in \mathbb{N}_0\}$. This means that the point P is a torsion point.

□

Proposition 3.50. *Let E be an elliptic curve defined over the number field K. For every $P, Q \in E(\bar{K})$, the following are true*

(i) $2\hat{h}_E(P+Q) + 2\hat{h}_E(P-Q) = 2\hat{h}_E(P) + 2\hat{h}_E(Q)$, *and*
(ii) $\hat{h}_E(mP) = m^2\hat{h}_E(P)$, $\forall m \in \mathbb{N}_0$.

Proof. (i) From the equation

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

we have

$$\frac{h_E(P+Q)}{4^n} + \frac{h_E(P-Q)}{4^n} = 2\,\frac{h_E(P)}{4^n} + 2\,\frac{h_E(Q)}{4^n} + \frac{O(1)}{4^n}.$$

Taking $n \to +\infty$, we obtain the desired result.
(ii) Analogously.

□

This proposition informs us that the Néron-Tate height is a quadratic form, and so we are able to define a bilinear form.

Corollary 3.51. *Let E be an elliptic curve over the number field K. The pairing*

$$\begin{aligned} \langle \cdot, \cdot \rangle \quad : \quad & E(\bar{K}) \times E(\bar{K}) \longrightarrow \mathbb{R} \\ & (P, Q) \longmapsto \hat{h}_E(P+Q) - \hat{h}_E(P) - \hat{h}_E(Q) \end{aligned}$$

is bilinear.

Definition 3.52. The pairing that defined in the corollary 3.51 is called *Néron-Tate pairing*.

Without proving it, we mention the following important result.

Proposition 3.53. *The Néron-Tate height is a positive definite quadratic form.*

Proof. (see [**18**], p. 232) □

Bibliography

[1] M. Bhargava, C. Skinner, W. Zhang: *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture.* arXiv:1407.1826 [math.NT] (2014).

[2] B.J. Birch, H. P. F. Swinnerton-Dyer: *Notes on elliptic curves. (I) and (II)* J. Reine Angew. Math. 212, p. 725 (1963) and 218 p.79-108 (1965).

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor: *On the Modularity of Elliptic Curves over $\mathbb{Q}$: Wild* 3*-adic Exercises* J. Amer. Math. Soc. 14, p.843-939 (2001).

[4] J.S. Chahal: *Topics in Number Theory.* Plenum Press, New York (1988).

[5] J. Coates, A. Wiles: *On the conjecture of Birch and Swinnerton-Dyer* Invent. Math., 39(3), p. 223-251 (1977).

[6] B. Gross, D. Zagier: *Heegner points and derivatives of L-series.* Invent. Math. 84, p.225-320 (1986).

[7] H. Hasse: *Zur Theorie der abstrakten elliptischen Funktionenkörper I, II und III.* J. Reine Angew. Math. 175, p. 55-62, 69-88, 193-208 (1936).

[8] M. Hindry, J.H. Silverman: *Diophantine Geometry, An Introduction.* Grad. Texts in Math. 201, Springer-Verlag (2000).

[9] A.W. Knapp: *Elliptic curves.* Math. Notes 40, Princeton University Press (1992).

[10] V.A. Kolyvagin: *Finiteness of $E(\mathbb{Q})$ and $Ш(E,Q)$ for a subclass of Weil curves.* Akad. Nauk SSSR Ser. Mat., 52(3), p. 522-540, 670-671, (1988).

[11] S. Lang: *Algebraic Number Theory.* Grad. Texts in Math. 110, Springer-Verlag (1986).

[12] S. Lang: *Fundamentals of Diophantine Geometry.* Springer-Verlag, New York (1983).

[13] M. Magioladitis: *Algebraic curves, Riemann conjecture and Coding Theory.* Bachelor thesis (in greek), Department of Mathematics, Heraklion, Crete (2001).

[14] Y. Manin: *A uniform bound for p-torsion in elliptic curves.* Izv. Akad. Nauk. CCCP 33, p.459-465 (1969).

[15] J.S. Milne: *Elliptic curves.* BookSurge Publishers (2006).

[16] A. Ogg: *Elliptic curves and wild ramification.* J. Reine Angew. Math., 226, p. 204-215 (1967).

[17] L. Ribes: *Introduction to Profinite Groups.* Lecture notes (Travaux mathématiques, Volume 22, p. 179-230 (2013).

[18] J.H Silverman: *The Arithmetic of Elliptic Curves.* Grad. Texts in Math. 106, Springer-Verlag (1985).

[19] P-N. Skoruppa: *Heights.* Notes, University of Bordeaux (1998).

[20] S. Schmitt, H. Zimmer: *Elliptic Curves, A Computational Approach* de Gruyter Studies in Mathematics 31 (2003).

[21] M. Stoll: *Rational points on curves.* arXiv:1008.1905 [math.NT] (2010).

[22] J. Tate: *Algorithm for determining the type of a singular fiber in an elliptic pencil. In Modular functions of one variable.* Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, p 3352. Lecture Notes in Math., Vol. 476. Springer, Berlin (1975).

[23] R. Taylor, A. Wiles: *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141, no. 3, p. 553-572 (1995).

[24] A. Wiles: *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141, no. 3, p. 443-551 (1995).

[25] A. Zervou: *Galois Cohomology and Number fields.* Master thesis, Heraklion (2017).

[26] S. Zhang: *Heights of Heegner points on Shimura curves.* Ann. of Math. (2), p.27-147 (2001).