MÁSTERES de la UAM

Facultad de Ciencias / 16-17

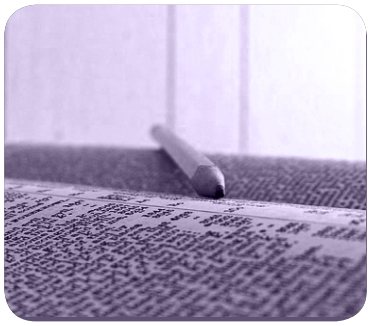
Matemáticas y Aplicaciones

UNIVERSIDAD AUTONOMA DE MADRID

Campus Internacional excelencia UAM CSIC

Elliptic curves and Galois representations

Javier Pliego García



UAM EDICIONES

978-84-8344-6215

Elliptic curves and Galois representations

Javier Pliego García

Master thesis supervised by Enrique González Jiménez

Universidad Autónoma de Madrid
Facultad de Ciencias
Departamento de Matemáticas

June 27, 2017

Contents

Introduction

One of the main problems in number theory are diophantine equations. They are perhaps some of the oldest problems in the history of mathematics and they have fascinated mathematicians of all periods. They are the object of study of the Diophantine geometry, which is a more recent term that involves the use of tecniques from Algebraic Geometry and Number Theory. Diophantine equations are systems of equations of the type

$$\begin{cases} F_1(x_1, x_2, ..., x_n) = 0 \\ F_2(x_1, x_2, ..., x_n) = 0 \\ \qquad \vdots \\ F_m(x_1, x_2, ..., x_n) = 0 \end{cases},$$

where $F_j \in \mathbb{Z}[x_1, ..., x_n]$ are polynomials with coefficients in $\mathbb{Z}$. One of the possible question that naturally arises is whether that system has solutions of the type $(x_1, ..., x_n) \in \mathbb{Z}^n$, or even over $\mathbb{Q}$. This system also defines an algebraic set over the field $\mathbb{Q}$ or even the field $\overline{\mathbb{Q}}$. Hence though we are studying a problem from the number theory point of view, we can use the language and the tools of the algebraic and arithmetic geometry to obtain useful properties.

The easiest diophantine equations are the linear ones:

$$aX + bY = c, \qquad a, b, c \in \mathbb{Z}, \quad a \neq 0 \ or \ b \neq 0.$$

By using the Euclidean Algorithm, it is easy to write all the possible solutions of pairs $(x, y) \in \mathbb{Z}^2$. In fact, the equation will have integer solutions if and only if $(a, b)|c$, and for the rational solutions, it is even more easy to describe all the solutions. This results have been known since Greek times. Increasing by one the degree of the equation, we have the quadratic equations:

$$aX^2 + bXY + cY^2 + dX + eY + f = 0 \qquad a, b \ or \ c \neq 0.$$

These equations are much more interesting both from the point of view of the arithmetic and the geometry. It was not until 1921 that mathematicians reached a satisfactory answer for the existence of rational points.

Theorem 0.0.1. *(Hasse-Minkowski) Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a quadratic polynomial. Then, $f(X,Y)$ has a solution $(x,y) \in \mathbb{Q}^2$ if and only if it has a solution $(x,y) \in \mathbb{R}^2$ and it has a solution $(x,y) \in \mathbb{Q}_p$ for all primes $p \in \mathbb{Z}$.*

Checking that a quadratic polynomial has solutions in $\mathbb{Q}_p$ is much easier than cheking it in $\mathbb{Q}$, Therefore, answering whether an equation has rational solutions is not so difficult.

These two example of families of curves represent the case when the genus of the curve [1] is 0. The Hasse-Minkowski theorem was proven at the beginning of the twentieth century, and since then mathematicians tried to search for similar answers to the cases of positive genus.

Finally, in 1983, Gerard Faltings proved that when the genus is bigger than 1 then the curve can only have a finite number of solutions over the rational numbers. This result does not give an easy condition that ensures if there are rational solutions or not, which was something that could be done with the other cases. Nevertheless, it is satisfactory enough. In fact, this result is also true for curves of genus 2 over number fields.

However, there is no satisfactory method that ensures the existence of a finite (or an infinite) number of solutions for curves of genus 1. For this reason (and for many other reasons) these curves have been studied so much in comparison with curves of other genus. They are also called elliptic curves[2], and they are the central object of study of this work.

As we mentioned before, we can also think of the points of the elliptic curve in $\overline{\mathbb{Q}}^2$. There is an interesting operation that can be defined in the $\overline{\mathbb{Q}}$-points of the elliptic curve which is based on a geometrical definition that provides the elliptic curve with a group structure. It was introduced by Poincare, though Fermat probably knew it before. Furthermore, this operation, when restricted to the rational points, defines a subgroup of that group. By the general theory of modules over principal domains, this means that if $E(\mathbb{Q})$ are the rational points of the elliptic curve, then

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tor} \oplus E(\mathbb{Q})_{free},$$

where $E(\mathbb{Q})_{tor}$ are the torsion points of $E(\mathbb{Q})$ and $E(\mathbb{Q})_{free}$ is a free $\mathbb{Z}$-module. In 1923, Mordell proved that $E(\mathbb{Q})$ is finitely generated, which implied that

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

where $r \geq 0$ is a positive integer and the subgroup $E(\mathbb{Q})_{tors}$ is finite. Aparently, this theorem partially answers our question, because $E(\mathbb{Q})$ will be infinite if and only if $r \geq 1$. Nagell-Lutz theorem says that the points in $E(\mathbb{Q})_{tors}$ are integral, and they verify an easy property that makes them very easy to be computed. The problem is

[1] Chek [43] for the definition of genus.

[2] See Chapter 2 for a more precise definition of elliptic curve.

that the rank is much more difficult to calculate, even for particular curves, and it is not even known whether there are curves with arbitrary large rank. Mordell-Weil theorem can also be proven for number fields.

There is a well-known conjecture that relates the rank of the elliptic curve with the order at $s = 1$ of an L-function whose coefficients depend on the elliptic curve. If it is true, it would provide an effective method to determine relatively easily if given an elliptic curve it has an infinite number of rational solutions or not. This is because computing the order of a zero of an L-function is in general easier than computing the rank of an elliptic curve. This conjecture is known as the Birch and Swinnerton-Dyer conjecture and it can also be formulated for elliptic curves over number fields.

In addition to the theoretical interest that the study of the properties of elliptic curves has itself, many people work on them because it has some applications to other problems and/or fields such as:

- The study of the class number for quadratic number fields (in relation with the Birch-Swinnerton-Dyer conjecture) ([19]).
- Applications to criptography ([23]):

  -Factorization of integers as a product of prime numbers.

  -Primality tests.

  -Encryption based on elliptic curves.
- Fermat's Last Theorem and a prove of it using elliptic curves and modularity.
- Congruent number problem.

The main goal of this work is to review some basic definitions and concepts about algebraic number theory and elliptic curves, to give an overview of the proof of some classic theorems about elliptic curves, such as the Mordell-Weil theorem, to learn a few of the main conjectures in this topic and to get familiar with some modern techniques, such as Galois representations and other analytical tools that are nowadays being used for solving a lot of problems in the theory of elliptic curves.

Generally speaking, the first two chapters are just an introduction to algebraic number theory and elliptic curves, while chapters 3, 4 and 6 cover some more recent topics. In this work I focus mainly on 4 big theorems. For the first one, which is the Mordell-Weil Theorem over number fields, I give all the details and I study all the preliminaries to be able to complete it and understand it. For the other three, which are the estimation of the analytic rank of elliptic curves, a theorem of Serre about Galois representations and Fermat's Last Theorem, I enumerate all the steps of the proof and I explain some of them, but I don't give all the details because of the difficulty of it.

In chapter 1, I try to cover all the preliminaries about algebraic number theory, mainly focusing on number fields, the study of the ring of integers and the class number. Since I have not taken any course on these topics, I have included the proof of many of the propositions that are written.

Chapter 2 just pretends to be a brief summary of the basic aspects of elliptic curves. There are perhaps some more elementary constructions that are not included in this section because I have tried to write only the things that I am going to need for the following ones. In contraposition with chapter 1, there are almost no proofs in this section, and this is because I did take a course on algebraic curves which covered all the contents of this chapter, so it did not make much sense repeating everything.

Chapter 3 is dedicated to the study of Mordell-Weil Theorem. It covers the proof of the Weak Mordell-Weil theorem, the Mordell-Weil theorem for the case $K = \mathbb{Q}$, an overview about height functions in proyective spaces and in elliptic curves and the application of these functions to prove the Mordell-Weil Theorem for number fields.

Chapter 4 is perhaps the most analytical part of the work. In the first part, some of the main known theorems about the torsion subgroup of elliptic curves over $\mathbb{Q}$ and number fields are mentioned. The second part is mainly about the L-fuctions of elliptic curves, the definition of them, some conjectures about the analytic extension of these functions and other conjectures that relate the algebraic rank of the curves with the order of the zero at $s = 1$. This last section ends with a deeper study of some theorems that give bounds the analytic rank of elliptic curves.

Chapter 5 is just a brief introduction to modular forms. The objective of this chapter is to give all the definitions that are going to appear in the previous and in the following chapter. It also includes a version of the modularity theorem. Therefore, there are many basic concepts, such as the modular curves, the Petterson inner product or the computation of dimensions of the different subspaces that are not mentioned.

Chapter 6 is probably the main chapter of this work. It is dedicated to Galois representations attached to elliptic curves over number fields, mainly focusing on the mod p case, though there are some comments about the l-adic representations. It begins with some definitions about the subgroups of $GL_2(\mathbb{F}_p)$ and it contains a very deep study due to Dickson of all the possibilities for the subgroups of $GL_2(\mathbb{F}_p)$(c.f.[11]). It also contains the proof of a theorem about the possible simple groups of 60 elements, which I thought it was worth including it. The second part of this chapter gives an overview of one of the main theorems about Galois representations of elliptic curves without complex multiplication, which was proved by Serre and that declares that for almost all primes, the representation is surjective. Then it also includes some other theorems, such as the one that was proven by many mathematicians and that ensures that the integer N such that for all $p > N$ the representation mod p is surjective does not depend on the elliptic curve for the

case of $\mathbb{Q}$. In addition, a summary of the possible images of the representations for small primes, and another summary of the case when the elliptic curve has complex multiplication is included.

To conclude this last chapter, there is a small section about Galois modular forms in which another version of modularity is mentioned (the version concerning Galois representations). Finally, there is a quick overview of the main steps to prove the Last Fermat's Theorem.

All the results and theorems that are included in this work are well-known and are not original. However, most of the proofs that are included here contain details and steps which are not included in the books. The main theorems which are worth reading them because of that reason are Proposition 1.4.18, whose proof is entirely original and not based on any text book (in fact I did not find any proof of it in any book), Theorem 4.2.13 and Theorem 6.1.7. Proposition 1.5.17 also contains some interesting details that are not found in [43]. Theorems 6.2.4 and 6.5.1 are also worth reading them because they are a good summary of the main steps of big theorems, but they do not contain original details. In Theorem 4.2.13, which is about the bounding of the average analytic rank of elliptic curves, the details that are added are mainly focused of the explanation of some formulas applying some complex analysis methods such as the Cauchy's residue theorem. In Theorem 6.1.7, which is about the classification of the subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, the explanations that are given on [24] are really poor, so what I basically do is to complete it. Furthermore, I also include an original proof which is not based on any text of the fact that if a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ contains two specific matrices, then it contains $\mathrm{SL}_2(\mathbb{F}_p)$.

The content of this work, as well as the tools and the arguments used are mainly algebraic, and many mathematicians that work on elliptic curves focus on the algebra beneath them. However, there are many number theorists that study the properties of elliptic curves from the point of view of the analysis. For that reason I decided to include a deep overview of the proof of Theorem 4.2.13 in Chapter 4.

Chapter 1

Algebraic Number Theory

1.1 Norm, trace and discriminant.

In this section we will introduce some basic tools about finite extensions of fields and we will study some properties of number fields.

Let L/K be a finite field extension and $x \in L$. We define the linear application $T_x : L \to L$ by $T_x(\alpha) = x\alpha$, and the following quantities

$$Tr_{L/K}(x) = Tr(T_x), \qquad N_{L/K}(x) = \det(T_x).$$

Denote $f_x(t) = \det(tId - T_x)$, hence

$$f_x(t) = t^n - Tr(T_x)t^{n-1} + ... + (-1)^n N_{L/K}.$$

Proposition 1.1.1. *If L/K is separable and $\sigma : L \to \overline{K}$ are the different embeddings that fix K then:*

i) $f_x(t) = \prod_\sigma (t - \sigma(x))$,

ii) $Tr_{L/K}(x) = \sum_\sigma \sigma(x)$,

iii) $N_{L/K}(x) = \prod_\sigma \sigma(x)$.

Proof. Let $m = [K(x) : K]$ and $d = [L : K(x)]$ and let $p_x(t)$ be the minimal polynomial of x over K,

$$p_x(t) = t^m + c_{m-1}t^{m-1} + ... + c_1 t + c_0.$$

Let $\alpha_1, \alpha_2, ...\alpha_d$ be a basis of $L/K(x)$, so

$$\alpha_1, \alpha_1 x, ..., \alpha_1 x^{m-1}; \alpha_2, \alpha_2 x, ..., \alpha_2 x^{m-1}; \alpha_d, \alpha_d x, ..., \alpha_d x^{m-1}$$

is a basis of L/K. The matrix representing T_x is diagonal by blocks (it has d blocks), and each block is

$$B = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{pmatrix},$$

so if $j(t) = \det(B - tId)$ then $f_x(t) = j(t)^d$, and we obtain that $j(t) = p_x(t)$, hence

$$f_x(t) = p_x(t)^d.$$

Since L/K is separable, $p_x(t)$ has m distinct roots, and for each root α_i $(i = 1, ..., m)$ there are exactly d embeddings such that $\sigma(x) = \alpha_i$. Let $\{\sigma_1, ..., \sigma_m\}$ be a set of representatives of such embeddings. Then

$$p_x(t) = \prod_{i=1}^{m}(t - \sigma_i(x)),$$

and consequently

$$f_x(t) = p_x(t)^d = \prod_{i=1}^{m}(t - \sigma_i(x))^d = \prod_{\sigma}(t - \sigma(x)).$$

Next, using that $-Tr_{L/K}$ and $(-1)^n N_{L/K}$ are the coefficients of $p_x(t)$ we obtain that

$$Tr_{L/K}(x) = \sum_{\sigma} \sigma(x)$$

and

$$N_{L/K}(x) = \prod_{\sigma} \sigma(x).$$

□

Suppose L/K is again a finite separable extension, $[L : K] = n$, $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ is a basis and $\sigma_i : L \to \overline{K}$, $i = 1, 2, ..., n$ are the different embeddings of L over K. Define the **discriminant** as follows:

$$d = d(\alpha_1, \alpha_2, ..., \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Since

$$Tr_{L/K}(\alpha_i \alpha_j) = \sum_{k} \sigma_k(\alpha_i)\sigma_k(\alpha_j),$$

denoting $A = (\sigma_i(\alpha_j))_{i,j}$ and $M = (Tr_{L/K}(\alpha_i\alpha_j))_{i,j}$, we have that $M = A^t A$ so

$$d(\alpha_1, \alpha_2, ..., \alpha_n) = \det(Tr_{L/K}).$$

Let the basis of L/K be $1, \theta, \theta^2, ..., \theta^{n-1}$. Writing $\sigma_i(\theta) = \theta_i$, the matrix A has the following expression:

$$A = \begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix},$$

so it is a Vandermonde matrix and its determinant is $\prod_{i<j}(\alpha_i - \alpha_j)$. Therefore, $d = \prod_{i<j}(\alpha_i - \alpha_j)^2 \neq 0$.

Consider the bilinear form $(x, y) \to Tr_{L/K}(xy)$. Let x and y be column vectors whose entries are the coefficients over the base $1, \theta, \theta^2..., \theta^{n-1}$. Consequently, $(x, y) = x^t My$, and if $\alpha_1, \alpha_2, ..., \alpha_n$ is another base with change of basis matrix P and $M' = (Tr_{L/K}(\alpha_i\alpha_j))_{i,j}$, then $M' = MP$. Thus, as the determinant of P and M are not zero, $\det(M') \neq 0$ and the bilinear form is non-degenerate. Next, let A be an integrally closed domain over its quotient field K, let L/K be a finite separable extension and let B be the integral closure of A in L. By Proposition 1.1.1, if $\alpha \in B$ then as its conjugates are also integral over A, $Tr_{L/K}(x)$ and $N_{L/K}(x)$ are integral over A because they are a sum (resp. a product) of integral elements. Since they also lie in K, they lie in A because A is integrally closed over K.

Lemma 1.1.2. *Let $\alpha_1, \alpha_2, ..., \alpha_n$ be a basis of L/K contained in B. Then*

$$dB \subset A\alpha_1 + A\alpha_2 + ... + A\alpha_n.$$

Given $\beta \in L$, there exist $c \in K$ such that $c\beta \in A$ because as K is the quotient field of A and β is algebraic over K,

$$\beta^m + \frac{a_{m-1}}{a'_{m-1}}\beta^{m-1} + ... + \frac{a_1}{a'_1}\beta + \frac{a_0}{a'_0} = 0,$$

with $a_i, a'_i \in A$, so if $c = a'_0a'_1 \cdots a'_{m-1}$,

$$(c\beta)^m + a_{m-1}a'_0a'_1 \cdots a'_{m-2}a'_m(c\beta)^{m-1} + ... + a_0(a'_0)^{m-1}(a'_1 \cdots a'_m)^m = 0,$$

which proves our assertion. Therefore, we can always find a basis of L/K contained in B.

Proof. Let $\alpha \in B$ and $\alpha = a_1\alpha_1 + ... + a_n\alpha_n$ with $a_i \in K$. We have the linear system

$$Tr_{L/K}(\alpha\alpha_i) = \sum_{j=1}^{n} Tr_{L/K}(\alpha_j\alpha_i)a_j,$$

so using the previous observation, $\alpha\alpha_i \in B$ and $\alpha_i\alpha_j \in B$, hence $Tr_{L/K}(\alpha\alpha_i) \in A$ and $Tr_{L/K}(\alpha_j\alpha_i) \in A$. Since the matrix $F = (Tr_{L/K}(\alpha_j\alpha_i))_{i,j}$ has determinant $d = d(\alpha_1, \alpha_2, ..., \alpha_n) \neq 0$, denoting $b = (Tr_{L/K}(\alpha\alpha_i))_i$, and $a = (a_j)_j$,

$$Adj(F)b = da.$$

Therefore, as the elements of $Adj(F)$ are sums and multiplications of elements in A, $da_i \in A$ for $i = 1, 2, ..., n$ and consequently $d\alpha \in A\alpha_1 + A\alpha_2 + ... + A\alpha_n$. $\square$

1.2 Modules and number fields.

We will give now some basic properties about modules and modules over principal domains.

Definition 1.2.1. Let R be a ring and M be a $R-$module. We say that $(x_i)_{i\in I}$ is a **basis** when it is linearly independent and it generates M. We say that M is a free-module if it admits a basis.

Lemma 1.2.2. *Let R be a principal ring and F a free $R-$module. Then the cardinality of a basis is unique and is called the* **dimension** *or the* **rank**.

Proof. First suppose we have the finite case (the infinite one is very similar). Let $x_1, ..., x_n$ be a basis of F. Let p be a prime in R. Then F/pF is a R/pR-vector space ((p) is a maximal ideal, so R/pR is a field), $\overline{x_1}, ..., \overline{x_n}$ obviously generates F/pF and if

$$\overline{\lambda_1}\overline{x_1} + ... + \overline{\lambda_n}\overline{x_n} = \overline{0},$$

then

$$\lambda_1 x_1 + ... + \lambda_n x_n \in pF,$$

so $\lambda_1 x_1 + ... + \lambda_n x_n = p\lambda_1' x_1 + p\lambda_n' x_n$. Therefore, $\overline{\lambda_1} = ... = \overline{\lambda_n} = \overline{0}$, because $x_1, ..., x_n$ is a basis. This implies that the cardinality of each basis $x_1, ..., x_n$ is the same as the dimension of the vectorial space F/pF, which is a constant number, hence all basis in F have the same cardinality. $\square$

Now we will prove a useful lemma about the dimension of submodules.

Lemma 1.2.3. *Let R be a principal ring, F a free $R-$module and M a $R-$submodule of F. Then M is a free module of dimension less than or equal to the dimension of M.*

Proof. We will do just the finite case (the infinite one is again similar). Let $(x_i)_i$, $i = 1, ..., n$ be the basis of F and consider the submodule $M_r = M \cap (x_1, ..., x_r)$ for each $r = 1, ..., n$, where $(x_1, x_2, ..., x_r)$ is the $R-$module generated by $x_1, ..., x_r$. We will prove it by induction of r. For $r = 1$, $M_1 \subset (x_1)$ and $\{a \in R : ax_1 \in M_1\}$ is clearly an ideal, so since R is principal, $\{a \in R : ax_1 \in M_1\} = (b)$ and $M_1 = (bx_1)$, which is a free submodule of dimension 1. Assume that it is true for r and let $\mathcal{A}$ be the set of elements $a \in R$ for which there exists $x \in M_{r+1}$ that can be written as

$$x = b_1 x_1 + b_2 x_2 + ... + b_r x_r + a x_{r+1}.$$

Then $\mathcal{A}$ is obviously an ideal, so let $\mathcal{A} = (a_{r+1})$. Suppose $a_{r+1} = 0$. Then $M_{r+1} = M_r$, hence applying induction we obtain the result. If $a_{r+1} \neq 0$, let $w \in R$ be the element such that the coefficient of x_{r+1} is a_{r+1}. Consequently, for all $x \in M_{r+1}$, there exists $c \in R$ such that $x - cw \in M_r$, so $M_{r+1} = M_r + (w)$. Applying induction we obtain that M_{r+1} is free and its dimension is less than or equal to $r+1$, as we wanted to prove. □

The following lemma is similar but instead of taking a principal ring we take a Noetherian one.

Lemma 1.2.4. *Let R be a Noetherian ring, F a finitely generated $R-$module and M a $R-$submodule of F. Then M is also finitely generated.*

Proof. Let $x_1, ...x_n$ be a set that generates F, and consider the submodule $M_r = M \cap (x_1, ..., x_r)$ for each $r = 1, ..., n$, where $(x_1, x_2, ..., x_r)$ is the $R-$module generated by $x_1, ..., x_r$. If $M_1 = M \cap (x_1)$, $\{a \in R : ax_1 \in M_1\}$ is clearly an ideal, so as R is Noetherian, $\{a \in R : ax_1 \in M_1\} = (b_1, ..., b_k)$ and $M_1 = (b_1x_1, ..., b_kx_1)$, which is finitely generated. Assume that it is true for r and let $\mathcal{A}$ be the set of elements $a \in R$ for which there exists $x \in M_{r+1}$ that can be written in the form

$$x = b_1x_1 + b_2x_2 + ... + b_rx_r + ax_{r+1}.$$

Then $\mathcal{A}$ is obviously an ideal, so let $\mathcal{A} = (a_1, ..., a_l)$. Let $w_1, ..., w_l$ be the elements of M_{r+1} with x_{r+1}-coefficient a_i. Consequently, for $x \in M_{r+1}$, there exists $c_1, ..., c_l$ such that $x - c_1w_1 - ... - c_lw_l \in M_r$, so applying induction we obtain that M_{r+1} is finitely generated, as we wanted to prove. □

Definition 1.2.5. Let R be a ring and E be a $R-$module. The **torsion submodule** E_{tors} is the set of elements $x \in E$ such that there exists $a \in R$, $a \neq 0$ for which

$$ax = 0.$$

Finally, we will just formulate the following lemma.

Lemma 1.2.6. *Let R a principal ring and E a R-module. Then there exists a free submodule $F \subset E$ such that*

$$E = E_{tors} \oplus F.$$

We will apply all this theory to the case of number fields.

Definition 1.2.7. By a **number field** we mean a finite algebraic extension K of $\mathbb{Q}$.

The ring $\mathbb{Z}$ is a principal domain and it is therefore integrally closed over its quotient field $\mathbb{Q}$. If K is a number field, we will call O_K the integral closure of $\mathbb{Z}$ in K. It is also known as the ring of integers of K.

Corollary 1.2.8. *Let K be a number field and $[K:\mathbb{Q}] = n$. Then O_K is a free module of rank n.*

Proof. Let $[K:\mathbb{Q}] = n$. By 1.1.2, we know that there exists a basis $\alpha_1, ..., \alpha_n$ such that $O_K \subset \mathbb{Z}\frac{\alpha_1}{d} + ... + \mathbb{Z}\frac{\alpha_n}{d}$. Since this last module is free of rank n, applying Lemma 1.2.3 we obtain that O_K is a free module of rank less than or equal to n. As $\mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_n \subset O_K$, using again the lemma we obtain that the rank of O_K is n. □

1.3 Dedekind rings

In this section, instead of working just with number fields and ring of integers of them, we will work in a more general context.

Definition 1.3.1. Let A be a ring and K its quotient ring. We say that I is a **fractional ideal** if I is an $A-$module such that there exists $c \neq 0$, $c \in A$ for which $cI \subset A$.

Definition 1.3.2. A **Dedekind ring** is a ring which is Noetherian, integrally closed in its quotient field and such that every non-zero prime ideal is maximal.

Next we will prove the main theorem about Dedekind domains, but first we will deal with the following technical lemma.

Lemma 1.3.3. *Let A be a ring, L a field containing A and $x \in L$. If there exists a finitely generated A-module M such that $xM \subset M$, then x is integral over A.*

Proof. Let $\alpha_1, ..., \alpha_n$ be the elements that generate M. We have that

$$x\alpha_1 = a_{1,1}\alpha_1 + a_{1,2}\alpha_2 + ... + a_{1,n}\alpha_n,$$

$$x\alpha_2 = a_{2,1}\alpha_1 + a_{2,2}\alpha_2 + ... + a_{2,n}\alpha_n,$$

$$\vdots$$

$$x\alpha_n = a_{n,1}\alpha_1 + a_{n,2}\alpha_2 + ... + a_{n,n}\alpha_n,$$

with all the coefficients belonging to A. Let

$$A = \begin{pmatrix} a_{1,1} - x & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} - x & \cdots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n-1} & a_{n,n} - x \end{pmatrix}$$

and

$$b = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Then $Ab = 0$, and therefore $\det(A)b = Adj(A)Ab = 0$, which implies that $\det(A)\alpha_i = 0$ for each i. If $1 = a_1\alpha_1 + ... + a_n\alpha_n$,

$$\det(A) = \det(A)a_1\alpha_1 + ... + \det(A)a_n\alpha_n = 0,$$

so x is the zero of a monic polynomial with coefficients in A. □

Theorem 1.3.4. *Let A be a Dedekind ring. Every ideal of A can be uniquely factored into prime ideals. Furthermore, the set of non-zero fracional ideals form a group under multiplication.*

Proof. We will first prove the second assertion. We will do it in several steps.

i) Every non-zero ideal I contains a product of prime ideals:

Suppose that there exists an ideal for which it doesn't happen. Then the set of ideals for which that condition does not occur is not empty, so as A is Noetherian, there exists an ideal I which is maximal with respect to that hypothesis. In particular, I is not prime, and therefore there exists a, b such that $a \notin I$, $b \notin I$ but $ab \in I$. If $a_1 = I + (a)$, $a_2 = I + (b)$ then $I \subset a_1$, $I \subset a_2$ and $a_1 \neq I \neq a_2$, hence since I is maximal, $a_1 = p_1 \cdots p_m$ and $a_2 = q_1 \cdots q_n$, with p_i, q_i prime ideals. As $ab \in I$, $a_1a_2 \subset I$. Consequently, $p_1 \cdots p_m q_1 \cdots q_n = a_1a_2 \subset I$, which is a contradiction.

ii) Every prime ideal p is invertible, i.e. $Bp = A$ for some fractional ideal B:

Let K be the quotient field of A. We define $p^{-1} = \{x \in K : xp \in A\}$. Clearly $A \subset p^{-1}$. Let $a \neq 0$ with $a \in p$. Then by the first step there exist $p_1, ..., p_m$ primes such that

$$p_1p_2 \cdots p_m \subset (a) \subset p$$

and m is minimal. If there exist $a_i \in p_i$ and $a_i \notin p$, since p is prime, $\prod_i a_i \notin p$ but $\prod_i a_i \in p_1p_2 \cdots p_m \subset p$, which is a contradiction. Therefore, one of the primes is contained in p (we can assume that it is p_1), $p_1 \subset p$, and since p_1 is maximal, $p_1 = p$. Now, as m is minimal,

$$p_2 \cdots p_m \not\subset (a),$$

so there exists $b \in p_2 \cdots p_m$ such that $b \notin (a)$ and $pb = p_1b \subset (a)$, hence $a^{-1}bp \subset A$, which means that $a^{-1}b \in p^{-1}$. Since $b \notin (a)$, $a^{-1}b \notin A$, and consequently $A \neq p^{-1}$.

Using the definition of p^{-1} and the fact that $A \subset p^{-1}$ we have that $p \subset p^{-1}p \subset A$. Let $\sum_i p_i x_i$ with $p_i \in p$ and $x_i \in p^{-1}$. Then $\sum_j p'_j x'_j + \sum_i p_i x_i$ is again a sum of the same type, so it belongs to $p^{-1}p$. If $r \in A$, $\sum_i p_i r x_i \in p^{-1}p$ because $r x_i p \subset A$, so $p^{-1}p$ is an ideal, and since p is maximal, it must be either p or A. Suppose $p^{-1}p = p$. Consequently, as p is a finitely generated A module because A is Noetherian, using Lemma 1.3.3 we have that p^{-1} is integral over A. This is a contradiction because $A \subset p^{-1}$, $A \neq p^{-1}$, and the fact that A is integrally closed. Therefore $p^{-1}p = A$.

iii) Every non-zero ideal is invertible:

Suppose that is not true. Then there exists an ideal I maximal with respect to that condition, so by the previous step it cannot be maximal. Therefore, there exists p maximal such that $I \subset p$ and $I \neq p$. Consequently,

$$I \subset Ip^{-1} \subset II^{-1} \subset A,$$

where in the first inclusion we have used that $A \subset p^{-1}$, in the second that since $I \subset p$, $p^{-1} \subset I^{-1}$ and in the third one the definition of I^{-1}. Applying a similar argument than in the previous step, we have that Ip^{-1} is an ideal. Again, using Lemma 1.3.3 and the fact that A is a Dedekind ring, $I \neq Ip^{-1}$. Therefore, by the maximality of I, there exists a fractional ideal B such that $Ip^{-1}B = A$, which implies that I has an inverse, which is a contradiction.

iv) Let a be a non-zero ideal and c a fractional ideal such that $ac = A$. Then $c = a^{-1}$:

First of all, $c \subset a^{-1}$ by definition of a^{-1} and if $xa \subset A$, $xac \subset c$ because c is a A-module, and since $ac = A$, $x \in c$, as we wanted to prove.

Finally, we conclude that every fractional ideal is invertible. Let a a fractional ideal and $c \in K$ such that $ca \subset A$. Then using a similar argument than in the previous steps, ca is an ideal, so it is invertible, and therefore there exists b such that $cab = A$. Hence using the fourth step, $cb = a^{-1}$. In addition, for any fractional ideal a, $Aa \subset a$ because a is an $A-$module, and $a \subset Aa$ because $1 \times a = a$. Moreover, let a' be another fractional ideal, hence there exist c such that $ca \in A$, and thus $caa' \subset A$ because a' is an $A-$module. This proves that the non-zero fractional ideals form a group (the associativity is obvious).

For the existence of a factorization, suppose it does not occur. Then there exists I maximal with respect to that property, so there exists a prime p such that $I \subset p$ and as I cannot be a prime, $p \neq I$. Therefore $I \subset Ip^{-1} \subset A$, and again by Lemma 1.3.3 we have that $I \neq Ip^{-1}$, which implies by maximality that $Ip^{-1} = p_1 \cdots p_r$, hence $I = pp_1 \cdots p_r$, which is a contradiction.

For the uniqueness, let a, b be ideals and p a prime. Then $ab \subset p$ implies that one of them is contained in p (if not there would exist $a' \in a$, $b' \in b$ with $a' \notin p$,

$b' \notin p$ such that $a'b' \in p$, which is a contradiction). If

$$p_1 \cdots p_s = q_1 \cdots q_r,$$

using that argument we have that since $q_1 \cdots q_r \subset p_1$ the inclusion $q_i \subset p_1$ holds for some i. In addition, as q_i is also maximal, $q_i = p_1$, and multiplying on both sides by p_1^{-1} we have an expression with $s-1$ and $r-1$ terms, so by induction we have the uniqueness. □

Let I be a fractional ideal. There exists $c \in A$ such that $cI \subset A$. Since cI is an ideal, $cI = p_1 \cdots p_m$ and $(c) = q_1 \cdots q_s$, so using that the set of fractional ideals is a group,

$$I = \frac{p_1 \cdots p_m}{q_1 \cdots q_s}.$$

After cancellation, uniqueness follows from the uniqueness of the factorization of non-zero ideals.

We will now show several easy lemmas related to conmmutative algebra that will be left without proof.

Lemma 1.3.5. *(Chinese remainder Theorem) Let A be a ring and $I_1, ..., I_r$ ideals such that $I_i + I_j = A$ for all $i \neq j$. Then if $a = \cap_i I_i$,*

$$A/a \cong \bigoplus_i A/I_i.$$

Lemma 1.3.6. *Let A be a ring and $I_1, ..., I_r$ ideals such that $I_i + I_j = A$ for all $i \neq j$. Then*

$$\bigcap_i I_i = \prod_i I_i.$$

Lemma 1.3.7. *Suppose $A \subset B$ and $B \subset C$ are integral extensions. Then $A \subset C$ is again an integral extension.*

Lemma 1.3.8. *Let $A \subset B$ be an integral extension of domains. Then A is a field if and only if B is a field.*

Lemma 1.3.9. *Let $A \subset B$ be an integral extension of rings and $J \subset B$ an ideal. We have that*

$$A/(J \cap A) \subset B/J$$

is an integral extension of rings.

Corollary 1.3.10. *Let A be a Dedekind ring, B an integral extension of A and β a prime ideal of B. Then β is maximal.*

Proof. The extension $A \subset B$ is a homomorphism of rings, so $\beta \cap A$ is the preimage of a prime and is therefore a prime. Using that A is a Dedekind ring, $\beta \cap A$ is maximal, and applying the previous lemmas we have that β is maximal. □

Next we are going to study Dedekind rings in extensions of fields.

Proposition 1.3.11. *Let A be a Dedekind domain and K its field of fractions. Let L/K be a separable extension of fields. If B is the integral closure of A in L, B is again a Dedekind domain.*

Proof. Let $x \in L$ be integral over B. Then $B[x]$ is obviously finitely generated and hence by Lemma 1.3.3 it is integral, so $A \subset B[x]$ is integral and therefore x is integral over A. Consequently, $x \in B$. This proves that B is integrally closed. Corollary 1.3.10 shows that every non-zero prime is maximal. To prove that it is Noetherian, by Lemma 1.1.2 we have that $B \subset A\frac{\omega_1}{d} + ... + A\frac{\omega_n}{d}$. Thus, by Lemma 1.2.4 we have that B is a finitely generated A-module (A is Noetherian). Using that B is isomorphic to $A[x_1, ..., x_l]/J$, where J is an ideal of the polynomial ring, and using Hilbert's basis Theorem, we have that B is Noetherian. □

Corollary 1.3.12. *If K is a number field then O_K is a Dedekind domain.*

Proof. $K/\mathbb{Q}$ is a separable extension, $\mathbb{Z}$ is obviously Noetherian and $\mathbb{Q}$ is its quotient field. From the previous proposition it follows that O_K is a Dedekind domain. □

Lemma 1.3.13. *Let A be a Dedekind ring and S a multiplicative set. Then $S^{-1}A$ is a Dedekind ring.*

Now given $p \in A$ a prime ideal, it is not difficult to see that $pB \neq B$. Therefore, as B is a Dedekind domain,

$$pB = \beta_1^{e_1} \cdots \beta_m^{e_m},$$

and for each i, since $pB \subset \beta_i$, $p \subset \beta_i$, so $p = \beta_i \cap A$. We say that each e_i is the **ramification index**, and we define

$$f_i = [B/\beta_i : A/p]$$

as the **residual degree** ($(B/\beta_i)/(A/p)$ is an extension of fields because $p \in \beta_i$). In addition, if $\beta_i \neq \beta_j$, $\beta_i \subset \beta_i + \beta_j$ and $\beta_j \subset \beta_i + \beta_j$. Since both are maximal and different, $\beta_i + \beta_j = B$. Therefore, there exist $a \in \beta_i$, $b \in \beta_j$ such that $a + b = 1$. Consider $\beta_i^{e_i} + \beta_j^{e_j}$. Then $1 = (a+b)^{e_i+e_j} \in \beta_i^{e_i} + \beta_j^{e_j}$ because when we expand that expression, either the exponent of a is bigger than or equal to e_i or the exponent of a is bigger than or equal to e_j, hence applying Lemma 1.3.6, we obtain that

$$\prod_i \beta_i^{e_i} = \bigcap_i \beta_i^{e_i}.$$

Lemma 1.3.14. *Let O be a dedekind ring and I an ideal with $I = \beta_1^{e_1} \cdots \beta_n^{e_n}$. Then $I \subset \beta^k$ if and only if $\beta = \beta_i$ for some i and $k \leq e_i$.*

Proof. The second assertion implies the first is obvious. Suppose $\beta \neq \beta_i$ for any i. Then using the previous remark we have that $\prod_i \beta_i^{e_i} = \bigcap_i \beta_i^{e_i}$, so if $\bigcap_i \beta_i^{e_i} = I \subset \beta^k$,

$$\bigcap_i \beta_i^{e_i} = \bigcap_i \beta_i^{e_i} \bigcap_i \beta_i^{e_i} \subset (\bigcap_i \beta_i^{e_i}) \cap \beta^k \subset \bigcap_i \beta_i^{e_i}.$$

Therefore

$$\bigcap_i \beta_i^{e_i} \cap \beta^k = \bigcap_i \beta_i^{e_i},$$

and since β is coprime with the rest of primes,

$$\beta^k \prod_i \beta_i^{e_i} = \bigcap_i \beta_i^{e_i} \cap \beta^k = \bigcap_i \beta_i^{e_i} = \prod_i \beta_i^{e_i},$$

which contradicts the uniqueness of the factorization. Suppose $\beta = \beta_j$ and $k > e_j$. Then using a similar argument,

$$\bigcap_i \beta_i^{e_i} = \beta_j^k \bigcap_{i \neq j} \beta_i^{e_i},$$

and applying that intersections are the same as products we have a contradiction. □

We will prove the following result about the numerical relation of the ramification indexes and the residual degrees.

Theorem 1.3.15. *Let L/K be separable and $[L : K] = n$. Then we have*

$$\sum_i e_i f_i = n.$$

Proof. Applying the previous observation and the Chinese Remainder Theorem,

$$B/pB \approx \bigoplus_i B/\beta_i^{e_i}.$$

It will suffice to show that $\dim_{A/p}(B/pB) = n$ and $\dim_{A/p}(B/\beta_i^{e_i}) = e_i f_i$. The number $\dim_{A/p}(B/pB)$ is finite because B is a finitely generated A module, so $B = A[\alpha_1, ..., \alpha_s]$ and clearly $\overline{\alpha_i}$ generates (B/pB) over A/p. Let $\omega_1, ..., \omega_m$ be a set of representatives in B of a basis of B/pB. If there is a non trivial combination of them with coefficients in K, then there is a non-trivial combination of them over A, and thus

$$a_1\omega_1 + ... + a_m\omega_m = 0. \tag{1.3.1}$$

Let $\mathcal{A} = (a_1, ..., a_m) \neq 0$, so there exists $\mathcal{A}^{-1}$ and as the factorization is unique, $\mathcal{A}^{-1} \neq \mathcal{A}^{-1}p$ ($\mathcal{A}^{-1}p \subset \mathcal{A}^{-1}$), hence there exists $a \in \mathcal{A}^{-1}$ with $a \notin \mathcal{A}^{-1}p$. Therefore,

$a\mathcal{A} \not\subset p$ and consequently at least for one i, $aa_i \notin p$. Multiplying 1.3.1 by a we have that

$$\overline{aa_1}\ \overline{\omega_1} + ... + \overline{aa_m}\ \overline{\omega_m} = 0$$

is a non trivial combination, which is a contradiction, hence $\omega_1, ..., \omega_m$ is linearly independent over K.

Now we consider the finitely generated $A-$modules $M = A\omega_1 + ... + A\omega_m$ and $N = B/M$. Then $B = M + pB$ because if $b \in B$, $\overline{b} = \overline{b_1}\overline{\omega_1} + ... + \overline{b_m}\overline{\omega_m}$, so $b - b_1\omega_1 + ... + b_m\omega_m \in pB$. Therefore, $N = pN$. Suppose $\alpha_1, ..., \alpha_r$ are generators of N.

$$\alpha_i = p_1 n_1 + ... + p_d n_d = \sum_{j=1}^{r} a_{i,j}\alpha_j$$

with $a_{i,j} \in p$. Let $A = (a_{i,j} - Id)$. Thus $\det(A) \neq 0$ because $\det(A) \equiv (-1)^r \mod p$. Let $\alpha = (\alpha_i)_i$. We have that $A\alpha_i = 0$, so $\det(A)\alpha = Adj(A)A\alpha = 0$, which implies that $dN = 0$. Therefore, $dB \in A\omega_1 + ... + A\omega_m$, and since every $x \in L$ can be expressed as $x = bk$ with $b \in B$ and $k \in K$, then $L \subset K[\omega_1, ..., \omega_m] \subset L$, hence $\omega_1, ..., \omega_m$ is a basis of L over K and $n = \dim_{A/p}(B/pB)$.

For the other equality to prove,

$$(0) \subset \beta_i^{e_i-1}/\beta_i^{e_i} \subset \beta_i^{e_i-2}/\beta_i^{e_i} \subset ... \subset B/\beta_i^{e_i}.$$

Denote $I_j = \beta_i^{e_i-j}/\beta_i^{e_i}$, $I_0 = 0$ and $I_{e_i} = B/\beta_i^{e_i}$. We have that

$$\dim(I_{e_i}) = \sum_{j=0}^{e_j-1} \dim(I_{j+1}) - \dim(I_j) = \sum_{j=0}^{e_j-1} \dim(\beta_i^{e_i-j-1}/\beta_i^{e_i-j}).$$

Let $\beta_i = \beta$, $\alpha \in \beta^n - \beta^{n+1}$ and define $B \to \beta^n/\beta^{n+1}$ by $a \to \alpha a$. The kernel of that application is β because if $a \notin \beta$ then (a) doesn't have a power of β in its representation. Therefore, in the representation of $(a)(\alpha)$, β is raised to a power less than or equal to n, which implies that $(a\alpha) \not\subset \beta^{n+1}$, which means that $a\alpha \notin \beta^{n+1}$. We also have the equation

$$\beta^n = (\alpha) + \beta^{n+1},$$

because using Lemma 1.3.14, no prime different to β appear in the factorization of $(\alpha) + \beta^{n+1}$, so $\beta^k = (\alpha) + \beta^{n+1} \subset \beta^n$ and $\beta^k = (\alpha) + \beta^{n+1} \not\subset \beta^{n+1}$. Consequently, since $\beta^{n+1} \subset (\alpha) + \beta^{n+1} \subset \beta^n$, then $(\alpha) + \beta^{n+1} = \beta^n$, which implies the surjectivity of the previous function. For that reason,

$$B/\beta \simeq \beta^n/\beta^{n+1},$$

so if $f_i = [B/\beta_i : A/p]$ then we have

$$\dim(B/\beta_i^{e_i}) = \sum_{j=1}^{e_i-1} f_i = e_i f_i,$$

which concludes the proof.

□

1.4 Valuations and some classical formulas

Definition 1.4.1. Let K be a field. We say that

$$|.|_v : K \to \mathbb{R}_+$$

is an absolute value or a valuation when

i) $|x|_v = 0 \iff x = 0$.

ii) For all $x, y \in K$, $|xy|_v = |x|_v|y|_v$.

iii) For all $x, y \in K$, $|x + y|_v \leq |x|_v + |x|_v$. If instead of having property iii) we have $|x+y|_v \leq \max(|x|_v, |y|_v)$ we call it non-archimedean absolute value, and if it is not non-archimedean, we call it just archimedean.

Definition 1.4.2. Let K be a field. We say that

$$v : K \to \mathbb{R}$$

is an exponential valuation when

i) $v(x) = \infty \iff x = 0$.

ii) For all $x, y \in K$, $v(xy) = v(x) + v(y)$.

iii) For all $x, y \in K$, $v(x + y) \geq \min(v(x), v(y))$.

Using the above properties, it can be proved that the set $R = \{x \in K : v(x) \geq 0\}$ is a local ring with maximal ideal $m = \{x \in K : v(x) > 0\}$. We call it discrete valuation ring.

Definition 1.4.3. Let K be a field and v an absolute value. We say that K is complete if it is complete with respect to the topology induced by the absolute value.

Now we will outline some lemmas about those fields and we will leave them without proof.

Lemma 1.4.4. *Let K be a complete field with respect to an absolute value $|.|_v$ and L an algebraic extension. Then there is a unique absolute value in L that extends $|.|_v$.*

With this lemma it can be deduced that if A is the discrete valuation ring of K, and B is the integral closure of A in L, there is a unique maximal ideal β such that $\beta \cap A = p$ with p the unique maximal ideal of A. Suppose $w|v$ extends v in L. Then as $v(K)$ is a subgroup of $w(L)$, $e = (w(L) : v(K))$, makes sense and is called the ramification index. Let $f = [B/\beta : A/p]$.

Lemma 1.4.5.

$$ef \geq [L : K]$$

and for the case L/K separable, $ef = [L : K]$.

Definition 1.4.6. Suppose K is complete. We say that a finite extension L/K is unramified if the extension $(B/\beta)/(A/p)$ is separable and

$$f = [L : K].$$

An arbitrary algebraic extension is unramified when it is a union of finite unramified subextensions.

Proposition 1.4.7. *Let L/K and K'/K be algebraic extensions. Then*

$$L/K \text{ is unramified} \Longrightarrow L'/K' \text{ is unramified.}$$

The composite of unramified extensions is unramified.

Definition 1.4.8. Let K be a complete field with respect to a valuation, with Dedekind A and maximal ideal p. Let E be a finite extension, let B be the integral closure and β its maximal ideal. We say that β (or E) is **tamely ramified** over p if $char(A/p)$ does not divide e, where $e = e(\beta : p)$ is the ramification index.

Let K_{nr} be the maximal unramified extension of K and E_u the maximal tamely ramified extension of K. Then we have the following inclusions:

$$K \hookrightarrow K_{nr} \hookrightarrow E_u \hookrightarrow E.$$

Let L/K be an extension of fields, let v be a valuation of K and $w|v$ a valuation in L. Let $G = Gal(L/K)$ and $\sigma \in G$. Let p the prime associated to v and β the prime associated to ω, and let O the valuation ring of L. We define the following valuation $\omega \circ \sigma$ as follows:

$$|x|_{\omega\circ\sigma} = |\sigma(x)|_\omega.$$

It is easy to prove that it is indeed a valuation that extends v.

Definition 1.4.9. The **decomposition group** of the extension $\omega|v$ is defined as:

$$G_\omega = G_\omega(L/K) = \Big\{\sigma \in G(L/K) : \omega \circ \sigma = \omega\Big\}.$$

The **inertia group** is defined as:

$$I_\omega = I_\omega(L/K) = \Big\{\sigma \in G_\omega : \sigma(x) \equiv x \mod \beta \quad for\ all\ x \in O\Big\}.$$

The **ramification group** is defined as:

$$R_\omega = R_\omega(L/K) = \Big\{\sigma \in G_\omega : \sigma(x)/x \equiv 1 \mod \beta \quad for\ all\ x \in L^*\Big\}.$$

Obviously, we have the relations

$$R_\omega \subset I_\omega \subset G_\omega.$$

From now on, we will quote some basic and useful results.

Proposition 1.4.10. *In the above situation,*

$$G_\omega(L/K) \cong G(L_\omega/K_v),$$

$$I_\omega(L/K) \cong I(L_\omega/K_v),$$

and

$$R_\omega(L/K) \cong R(L_\omega/K_v).$$

Proposition 1.4.11. *Let Z_ω be the fixed field of G_ω, T_ω the fixed field of I_ω and L_ω the fixed field of R_ω. Then, T_ω/Z_ω is the maximal unramified extension of L/Z_ω, and L_ω/Z_ω is the maximal tamelly ramified extension of L/Z_ω.*

Proposition 1.4.12. *In the above situation, the subgroup R_ω is the only p-Sylow subgroup of G_ω. Therefore, the order of $I_\omega/R_\omega = Gal(L_\omega/T_\omega)$ is prime to p.*

Proposition 1.4.13. *Let K be the quotient field of a discrete valuation ring with valuation v and let E be an algebraic extension of K. Let w be a valuation in E extending v. Denote E_w, K_v as the completions of such fields with respect to those valuations and $n_w = [E_w : K_v]$. Then we have the formula*

$$\sum_{w|v} n_w = [E : K].$$

Proposition 1.4.14. *Let K be the quotient field of a discrete valuation ring and E/K a finite extension. If v_0 is a valuation in K and $\alpha \in E$ then*

$$\prod_{v|v_0} |\alpha|_v^{n_v} = |N_K^E(\alpha)|_{v_0}.$$

Now we consider the set $M_{\mathbb{Q}}$ of absolute values in $\mathbb{Q}$ that consist on the p-adic valuations plus the usual norm; that is, for any prime p, any $m \in \mathbb{Q}$ can be written in the form

$$m = p^n \frac{a}{b}$$

with $a, b \in \mathbb{Z}$ and $(a, p) = (b, p) = 1$. We define the p-adic valuation as

$$|m|_p = \frac{1}{p^n},$$

and $|m|_\infty = |m|$ will denote the standard absolute value. In fact, there is a famous theorem which says that these valuations are the only ones:

Theorem 1.4.15 (Ostrowski)**.** *Consider the field $\mathbb{Q}$. Then v is an absolute value in $\mathbb{Q}$ if and only if there exists $\lambda > 0$ and a prime number $p \in \mathbb{N}$ such that for all $r \in \mathbb{Q}$,*

$$|r|_v = |r|_p^\lambda$$

or

$$|r|_v = |r|_\infty^\lambda.$$

Now, using this theorem we are going to prove the same with number fields.

Let A be a Dedekind ring and K its quotient field. As we saw in the previous section, for each $\alpha \in K$,

$$(\alpha)A = p_1^{e_1} \cdots p_r^{e_r},$$

where αA is a fractional ideal and the exponents could be negative. Let p be a prime ideal of A. We define v_p as

$$v_p(\alpha) = e_i$$

if $p = p_i$ for some $1 \leq i \leq r$, and

$$v_p(\alpha) = 0$$

in other case. This function is a non-archimedean discrete (exponential) valuation:

Using the fact that the set of fractional ideals form a group under multiplication, let $\beta \in K$ and

$$\beta A = (p_1')^{e_1'} \cdots (p_l')^{e_l'}.$$

Then

$$\alpha\beta A = (p_1')^{e_1'} \cdots (p_l')^{e_l'} p_1^{e_1} \cdots p_r^{e_r},$$

so if $p_i = p_j'$ for some i, j,

$$v_{p_i}(\alpha\beta) = e_i + e_j' = v_{p_i}(\alpha) + v_{p_j'}(\beta),$$

and the rest of cases are done in the same way. The lower bound of the valuation of a sum is also easy to check and is again a consequence of the unique factorization of ideals and the definition of products of ideals. Since v is a non-archimedean discrete (exponential) valuation, given any $T > 1$ then $T^{-v_p(\alpha)}$ is a non-archimedean discrete absolute value.

Let's now deal with the case of number fields. Let K be a number field and O_K its ring of integers. As we saw before, if β is a prime ideal in O_K, then there exists a prime $p \in \mathbb{Z}$ such that $\beta \cap \mathbb{Z} = p\mathbb{Z}$. Therefore,

$$pO_K = \beta^e \beta_1^{e_1} \cdots \beta_r^{e_r},$$

with β_i prime ideals in O_K and $e_i > 0$. Let $\mathbf{N}\beta = p^{[O_K/\beta:\mathbb{F}_p]} = p^{f_\beta}$.

Let $\pi \in O_K$ such that $v_\beta(\pi) = 1$. Then $p = \pi^e u$ with $v_\beta(u) = 0$. For any $\alpha \in K$ we define

$$|\alpha|_\beta = \frac{1}{p^{\frac{v_\beta(\alpha)}{e}}} = (p^{1/e})^{-v_\beta(\alpha)},$$

so by the previous observation $|.|_\beta$ is a non-archimedean absolute value and it extends $|.|_p$ because $|p|_\beta = \frac{1}{p}$ and for the rest of prime numbers q in $\mathbb{Z}$, $v_\beta(q) = 0$. If not, $qO_K \subset \beta$, so

$$q\mathbb{Z} \subset \beta \cap \mathbb{Z} = p\mathbb{Z},$$

which is a contradiction.

We also define

$$||\alpha||_\beta = (\frac{1}{\mathbf{N}\beta})^{-v_\beta(\alpha)} = (|\alpha|_\beta)^{e_\beta f_\beta}.$$

Next we will prove two easy lemmas.

Lemma 1.4.16. *Let K be a number field, O_K its ring of integers, $|.|_v$ a non-archimedean absolute value and $\alpha \in O_K$. Then, $|\alpha|_v \leq 1$. Furthermore, when α is an invertible element in O_K, $|\alpha|_v = 1$.*

Proof. Let $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ with $a_i \in \mathbb{Z}$ such that $p(\alpha) = 0$. By Ostrowski Theorem, $|a_i|_v = |a_i|_p^\lambda \leq 1$ because $a_i \in \mathbb{Z}$. Then if $|\alpha|_v > 1$, for all $i < n$,

$$|\alpha|_v^n > |\alpha|_v^i \geq |\alpha|_v^i |a_i|_v,$$

so

$$|\alpha|_v^n = |\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha_1|_v = |a_0|_v,$$

which is a contradiction because $|\alpha|_v^n > 1$ and $|a_0|_v \leq 1$. Therefore, $|\alpha|_v \leq 1$, and when α is invertible in O_K, by the same reasoning, as $\alpha^{-1} \in O_K$,

$$|\alpha^{-1}|_v \leq 1,$$

which implies that

$$|\alpha|_v = 1.$$

□

Lemma 1.4.17. *Let E/K be an extension of fields, let v_0 be a valuation in K and let $v|v_0$ be a valuation in E. Suppose v_0 is non-archimedean. Then v is also non-archimedean.*

Proof. Let $s, r \in E$.

$$|r+s|_v^n = |\sum_{j=0}^{n} \binom{n}{j} r^j s^{n-j}|_v \leq \sum_{j=0}^{n} |\binom{n}{j}|_{v_0} |r|_v^j |s|_v^{n-j} \tag{1.4.1}$$

$$\leq \sum_{j=0}^{n} |\binom{n}{j}|_{v_0} \max(|r|_v, |s|_v)^n \leq n \max(|r|_v, |s|_v)^n, \tag{1.4.2}$$

where in the last step we have used that $\binom{n}{j} \in K$ and that v_0 is non-archimedean, so

$$|r+s|_v \leq \sqrt[n]{n}\max(|r|_v, |s|_v),$$

for all n. Letting n tend to infinity,

$$|r+s|_v \leq \max(|r|_v, |s|_v),$$

as we wished to prove. □

The following proposition is a generalization of the previous one in number fields. Though many authors are constantly assuming it, I have not found a proof of it in any book.

Proposition 1.4.18. *Let $|.|_v$ be a non-archimedean valuation in K. Then it is of the form $|.|_\beta^\lambda$ for some prime β and some $\lambda > 0$.*

Proof. Using Ostrowski theorem and the previous lemma, we have that $|.|_v$ restricted to $\mathbb{Q}$ is a non-archimedean value, so it is of the form $|.|_p^\lambda$ for some prime $p \in \mathbb{Z}$. Therefore, if we prove that $|.|_v^{1/\lambda}$ is of the form $|.|_\beta$ for some β prime in O_K we will have finished.

It suffices to show the result for O_K because K is the quotient field of O_K. We can also suppose that $|.|_v$ restricted to $\mathbb{Q}$ is $|.|_p$, so we must show that $|.|_v = |.|_\beta$ for some β. Now, let

$$pO_K = \beta_1^{e_1} \cdots \beta_r^{e_r}.$$

Suppose there is some $\alpha \in O_K$ such that $\alpha \notin \beta_i$ for all $i = 1, ..., r$. Then if α is invertible in O_K, using Lemma 1.4.16 we have that $|\alpha|_v = 1$. Suppose α is not invertible,

$$\alpha O_K = \tilde{p}_1^{l_1} \cdots \tilde{p}_h^{l_h},$$

and all of those primes are different from the β_i for all $i = 1, ..., r$. Let $\tilde{p_i} \cap \mathbb{Z} = p_i\mathbb{Z}$. As

$$\prod_{i=1}^{h} \tilde{p}_i^{l_i} = \bigcap_{i=1}^{h} \tilde{p}_i^{l_i},$$

$$(\prod_{i=1}^{h} p_i^{l_i})\mathbb{Z} \subset \bigcap_{i=1}^{h} (\tilde{p_i}^{l_i} \cap \mathbb{Z}) = \alpha O_K \cap \mathbb{Z},$$

but since β_i and $\tilde{p}_i$ are all different and β_i are the only ones for which $\beta_i \cap \mathbb{Z} = p$ then we have that $p_i \neq p$ for all i. If $|\alpha|_v < 1$, then using Lemma 1.4.16 we would have that all elements belonging to $\alpha O_K \cap \mathbb{Z}$ would have absolute value less than one. This is because they are a product of an element in O_K, which has absolute

value less than or equal to 1 and α, whose absolute value is less than 1. However, as $|.|_v$ extends $|.|_p$ and $\prod_{i=1}^{h} p_i^{l_i} \in \alpha O_K \cap \mathbb{Z}$,

$$|\prod_{i=1}^{h} p_i^{l_i}|_v < 1,$$

so at least one of the p_i must verify that $|p_i|_p = |p_i|_v < 1$, which contradicts the fact that $p_i \neq p$. Therefore, $|\alpha|_v = 1$.

If we are able to prove that there exists i such that for $\alpha \in O_K$ with $\alpha \notin \beta_i$ then $|\alpha|_v = 1$, we would have finished, because taking $\pi \in O_K$ that verifies $v_{\beta_i}(\pi) = 1$ then for $\gamma \in O_K$ with $v_{\beta_i}(\gamma) = n$, $\pi^n/\gamma \notin \beta_i$, so $|\pi^n/\gamma|_v = 1$. Therefore

$$|\pi^n|_v = |\gamma|_v,$$

and since $p = \pi^e u$ with $u \notin \beta_i$,

$$\frac{1}{p} = |\pi^e|_v |u|_v = |\pi|_v^e.$$

Consequently,

$$|\gamma|_v = \frac{1}{p^{\frac{ord_{\beta_i}(\gamma)}{e}}}.$$

As a consequence of the finiteness of the class number, which will be proved in the next subsection, for each β_i the set of ideals $\{\beta_i^j\}_{j=1}^{\infty}$ is infinite. Therefore, there exist two numbers r, s such that $\beta_i^r \sim \beta_i^s$, which means that for $m = r - s > 0$, there exists $\xi_i \in O_K$ such that $(\xi_i) = \beta_i^m$. Now imagine that $\{\xi_{i_j}\}_{j=1}$ is the subset of those elements for which $|\xi_{i_j}|_v < 1$ and suppose[1] $j \geq 2$. Then

$$|\xi_{i_1} + \prod_{l \neq i_1} \xi_l|_v < 1$$

because for each of the addends the non-archimedean absolute value is less than one[2]. However,

$$\xi_{i_1} + \prod_{l \neq i_1} \xi_l \notin \beta_i$$

because if $b_i \in \beta_i$ with $i \neq i_1$ and $b_i = \xi_{i_1} + \prod_{l \neq i_1} \xi_l$ then

$$\xi_{i_1} = b_i - \prod_{l \neq i_1} \xi_l \in \beta_i,$$

which is a contradiction, and the same with i_1. Hence by the observation we did at the beginning of the proof,

$$|\xi_{i_1} + \prod_{l \neq i_1} \xi_l|_v = 1,$$

[1]This means that for at least two of the prime ideals β_i, the elements ξ_i verifiy $|\xi_i|_v < 1$.

[2]Here the product is taking over all the indexes of the prime ideals β_i except β_{i_1}.

which is again a contradiction, so $j \leq 1$. Imagine that $j = 0$. Then

$$(p^m)/(\xi_1^{e_1} \cdots \xi_r^{e_r}) = (p^m)/(\beta_1^{me_1} \cdots \beta_r^{me_r}) = O_K,$$

which implies that $\tilde{\alpha} = p^m/(\xi_{i_1}^{e_1} \cdots \xi_{i_r}^{e_r})$ is a unit of O_K. Furthermore, by Lemma 1.4.16, using that it is a unit, $|\tilde{\alpha}|_v = 1$, and as $|\xi_i|_v = 1$ for all i, $|p|_v = 1$, which contradicts the fact that it extends the p-adic absolute value.

If $j = 1$, let's say that the element for which its absolute value is not 1 has index 1. Using a similar reasoning, take $a \in O_K$ with $a \notin \beta_1$. Let $f_i = ord_{\beta_i}(a)$. Then,

$$a^m/(\xi_2^{f_2} \cdots \xi_r^{f_r}) \notin \beta_j$$

for all $j = 1, ..., r$, and it belongs to O_K, since

$$(a^m)/(\xi_2^{f_2} \cdots \xi_r^{f_r}) = (a^m)/(\beta_2^{f_2} \cdots \beta_r^{f_r})^m$$

is an ideal in O_K. Therefore,

$$|a/(\xi_2^{f_2} \cdots \xi_r^{f_r})|_v = 1,$$

which implies that $|a|_v = 1$ as we wanted to prove. □

From now on, when we talk about the set M_K of absoulte values in K we would refer to those values (the values whose restriction to K is either the p-adic value or the standard norm in $\mathbb{R}$). The set of non-archimedean values will be denoted by M_K^0, and the set of archimedean values by M_K^∞. Returning to the l-adic absolute values in $\mathbb{Q}$, we obviously have that those absolute values are multiplicative and for l prime,

$$|l|_p = 1$$

if $p \neq l$ and

$$|l|_p = \frac{1}{p}$$

if $p = l$ so

$$\prod_p |l|_p = \frac{1}{l}$$

and therefore,

$$\prod_{v \in M_\mathbb{Q}} |l|_v = |l|_\infty \prod_p |l|_p = 1. \tag{1.4.3}$$

Corollary 1.4.19. *Let K be a number field and $\alpha \in K$. Let M_K be the set of absolute values of K,*

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

Proof. By the definition of norm, $N_{\mathbb{Q}}^K(\alpha) \in \mathbb{Q}$, hence using equation 1.4.3,

$$1 = \prod_{v \in M_{\mathbb{Q}}} |N_{\mathbb{Q}}^K(\alpha)|_v.$$

Applying Proposition 1.4.14 we have that for fixed $v_0 \in M_{\mathbb{Q}}$,

$$\prod_{v|v_0} |\alpha|_v^{n_v} = |N_K^E(\alpha)|_{v_0},$$

so putting together the two formulas,

$$1 = \prod_{v_0 \in M_{\mathbb{Q}}} |N_{\mathbb{Q}}^K(\alpha)|_{v_0} = \prod_{v_0 \in M_{\mathbb{Q}}} \prod_{v|v_0} |\alpha|_v^{n_v} = \prod_{v \in M_K} |\alpha|_v^{n_v},$$

as we wished to prove. Note that $|\alpha|_v = 1$ except for a finite number of v, so we can rearrange the terms of the product without changing the result. This expression is also known as the *product formula*. □

To end this section we present a classic result that will be used later on.

Proposition 1.4.20. *Let K be a number field. Then there is a finite number of primes $p \in \mathbb{Z}$ for which (p) is ramified.*

Though this result could be generalized, we will just need this version.

1.5 Three classic results of Galois theory and number fields

In this subsection we will deal with a well-known result about Abelian Kummer theory and we will also prove the Dirichlet unit-theorem and other propositions.

1.5.1 Abelian Kummer theory

We will prove a classic result used in the Mordell-Weill proof. But before we will need some basic lemmas.

Lemma 1.5.1. *Let k be a field and K a finite Galois extension with Galois group $G = G_1 \times G_2 \times \cdots \times G_{n-1} \times G_n$, where G_i are finite groups $\forall i$ and K_i is the fixed field of*

$$H_i = G_1 \times G_2 \times \cdots \times G_{i-1} \times \{1\} \times G_{i+1} \times \cdots \times G_n.$$

Then K_i is Galois over k and $K = K_1 K_2 \cdots K_n$

Proof. For proving that K_i/k is Galois it is enough to show that H_i is normal, but that is trivial because $g \in G$, $g = (g_1, g_2, ..., g_n)$ with $g_i \in G_i$, $h \in H_i$, $h = (h_1, ...h_{i-1}, 1, h_{i+1}, h_n)$, then

$$(g_1, g_2, ..., g_n) \cdot (h_1, ...h_{i-1},\ 1\ , h_{i+1}, h_n) \cdot (g_1^{-1}, g_2^{-1}, ..., g_n^{-1}) = \\ (g_1 h_1 g_1^{-1}, ..., g_{i-1} h_{i-1} g_{i-1}^{-1},\ 1\ , g_{i+1} h_{i+1} g_{i+1}^{-1}, ..., g_n h_n g_n^{-1}) \in H_i.$$

Let $L = K_1 K_2 \cdots K_n$. Now, as $\forall i$, $K_i \subset K_1 K_2 \cdots K_n$, if $g \in G$ fixes $K_1 K_2 \cdots K_n$, in particular it fixes K_i, hence $g \in H_i$ and consequently $Gal(K/L) \subset \bigcap_i H_i = \{1\}$, so $Gal(K/L)$ is trivial and therefore $K_1 K_2 \cdots K_n = L = K$.

□

Lemma 1.5.2. *Let K/k be a Galois extension of fields and let G be its Galois group. Let $\{\sigma_1, \sigma_2 \cdots, \sigma_n\}$ be a set of distinct embeddings from K to $\overline{K}$, $\sigma_i \in G$ $\forall i$, and let $a_i \in K$. Then*

$$a_1\sigma_1 + a_2\sigma_2 + \cdots + a_n\sigma_n \equiv 0$$

if and only if $a_i = 0$ $\forall i = 1 \cdots n$.

Proof. For $n = 1$ the result is trivial because σ_1 is an embedding. Suppose we have a set of n embeddings in which there is a non-trivial linear combination of them. We choose a combination in which not all the coefficients are zero and the number k of embeddings is minimun, so $k \geq 2$ and $\sigma_i \neq 0$ $\forall i = 1 \cdots n$,

$$a_1\sigma_1 + a_2\sigma_2 + \cdots + a_k\sigma_k \equiv 0. \tag{1.5.1}$$

As $\sigma_1 \neq \sigma_2$, there exists $a \in K$ for which $\sigma_1(a) \neq \sigma_2(a)$, then since σ_i are homomorphisms, we have for all $x \in K$

$$a_1\sigma_1(a)\sigma_1(x) + a_2\sigma_2(a)\sigma_2(x) + \cdots + a_k\sigma_k(a)\sigma_k(x) = 0. \tag{1.5.2}$$

Therefore, multiplying 1.5.1 by $\sigma_1(a)$ and subtracting that equation and 1.5.2 we have

$$a_2(\sigma_1(a) - \sigma_2(a))\sigma_2 + \cdots + a_k(\sigma_1(a) - \sigma_k(a))\sigma_k \equiv 0,$$

so as $a_2(\sigma_1(a) - \sigma_2(a)) \neq 0$ we have a relation with less terms in which not all the coefficients are zero, which is a contradiction. □

With this last lemma we can prove the following corollary.

Corollary 1.5.3. *Let K/k be a cyclic extension of fields of degree n with Galois group G and generator σ. Suppose $\beta \in K$. Then $N_k^K(\beta) = 1$ if and only if there exists $\alpha \in K$ for which $\beta = \alpha/\sigma(\alpha)$.*

Proof. Let $\beta = \alpha/\sigma(\alpha)$. Then

$$N(\beta) = \prod_{\overline{\sigma}\in G} \overline{\sigma}(\alpha)/\overline{\sigma}\sigma(\alpha) = \prod_{\overline{\sigma}\in G} \overline{\sigma}(\alpha)/\prod_{\overline{\sigma}\in G} \overline{\sigma}(\alpha) = 1.$$

Conversely, if $N_k^K(\beta) = 1$, using Lemma 1.5.2 and the notation $\xi^\sigma = \sigma(\xi)$ and $\xi^{\tau+\sigma} = \xi^\tau \xi^\sigma$ we have that

$$\beta + \beta^{1+\sigma}\sigma + \cdots + \beta^{1+\sigma+\sigma^2+\cdots+\sigma^{n-1}}\sigma^{n-1} \neq 0$$

because all the coefficients are non-zero and σ has order n, so all embeddings are different. Therefore there exist $\alpha, \gamma \in K$ such that

$$\alpha = \beta\gamma + \beta^{1+\sigma}\sigma(\gamma) + \beta^{1+\sigma+\sigma^2}\sigma^2(\gamma) + \cdots + \beta^{1+\sigma+\sigma^2+\cdots+\sigma^{n-1}}\sigma^{n-1}(\gamma) \neq 0,$$

hence

$$\sigma(\alpha) = \beta^\sigma\sigma(\gamma) + \beta^{\sigma+\sigma^2}\sigma^2(\gamma) + \beta^{\sigma+\sigma^2+\sigma^3}\sigma^3(\gamma) + \cdots + \beta^{1+\sigma+\sigma^2+\cdots+\sigma^{n-1}}\gamma,$$

and since $1 = N_k^K(\beta) = \beta^{1+\sigma+\sigma^2+\cdots+\sigma^{n-1}}$, we have that $\alpha = \beta\sigma(\alpha)$, which concludes the proof. □

Definition 1.5.4. We say that a Galois extension of fields K/k is said to be of *exponent* m if for all $\sigma \in G$ we have $\sigma^m = 1$. We also say that a Galois extension of fields K/k is *abelian* when its Galois group G is abelian.

With all those previous lemmas and definitions we are ready to prove the following proposition.

Proposition 1.5.5. *Let m be an integer, k a field of characteristic prime to m containing an m-primitive root and K its maximal abelian extension of exponent m. Then K is Galois and is obtained by adjoining the m-roots of the elements of k to k.*

Proof. Let L be a subextension of K (a finite extension of k contained in K), and let G be the Galois group of K/k. Then by assumption L/k is abelian and Galois because $G(K/L)$ is normal in G as G is abelian and any element of $G(L/k)$ can be obtained by retricting some $\sigma \in G$ to L. Therefore, since G is abelian, $G(L/k)$ will also be abelian (by Galois Theory we know that $G(K/k)/G(K/L) \simeq G(L/k)$. The group $G(L/k)$ will be abelian because $G(K/k)/G(K/L)$ is abelian). Since $G(L/k)$ is abelian and finite, it can be written as a direct product of cyclic groups:

$$G(L/k) = C_1 \times C_2 \times \cdots \times C_{n-1} \times \cdots C_n.$$

Using Lemma 1.5.1 we have that if K_i is the fixed group of $H_i = C_1 \times C_2 \times \cdots \times C_{i-1} \times \{1\} \times C_{i+1} \times \cdots \times C_n$, K_i is Galois over k and its Galois group is $G(K_i/k) \simeq G(L/k)/H_i \simeq C_i$. Therefore, it is cyclic of exponent m, so if the order

n_i of its generator τ_i is equal to the order of the group and $\tau_i^m = 1$, $n_i | m$, and again applying the lemma we know that $L = K_1 K_2 \cdots K_n$.

Using the hypothesis that k contains an m-primitive root of the unit ζ, as $\zeta^{-1} \in k$,

$$N_k^{K_i}(\zeta^{-1}) = (\zeta^{-1})^m = 1/(\zeta)^m = 1,$$

hence applying corollary 1.5.3, if σ_i is the generator of $Gal(K_i/k)$, there exists $\alpha \in K_i$ such that $\zeta^{-1} = \alpha/\sigma_i(\alpha)$, so $\sigma_i(\alpha) = \zeta\alpha$. Let $n_i = Gal(K_i/k) = [K_i : k]$. Since $\sigma_i^j(\alpha) = \zeta^j\alpha$, and $\zeta^j\alpha$ are all distinct for all $j = 0, 1, ..., m-1$, the minimal polynomial of α over k has degree at least m, so $[k(\alpha) : k] \geq m$, but as $n_i | m$, in particular $n_i \leq m$, so we have

$$m \leq [k(\alpha) : k] \leq [K_i : k] = n_i \leq m,$$

which implies that $k(\alpha) = K_i$. In fact,

$$\sigma_i(\alpha^m) = \sigma_i(\alpha)^m = \zeta^m \alpha^m = \alpha^m,$$

hence since σ_i generates $Gal(K_i/k)$, we conclude that $a_i = \alpha^m \in K$, and then $K_i = k(a_i^{1/m})$, so therefore, as $L = K_1 K_2 \cdots K_n$,

$$L = k(a_1^{1/m}, a_2^{1/m}, ..., a_n^{1/m}).$$

This implies that $K \subset k(A)$, where $A = \{a^{1/m} : \ a \in k\}$.

But now if $G' = Gal(k(A)/k)$, by the definition of $k(A)$, every $\beta \in k(A)$ belongs to $k(b_1^{1/m}, b_2^{1/m}, ..., b_l^{1/m})$ for some $b_i \in k$. Therefore, to prove that $\tau, \tau' \in G'$ implies that $\tau\tau'(x) = \tau'\tau(x)$ for all $x \in k(A)$ it suffices to prove it for the $b_i^{1/m}$. Since $\tau(b_i^{1/m})$ must be a root of the polynomial equation $x^m - b_i = 0$, then $\tau(b_i^{1/m}) = \zeta^{j_\tau} b_i^{1/m}$ and $\tau'(b_i^{1/m}) = \zeta^{j_{\tau'}} b_i^{1/m}$, so

$$\begin{aligned}\tau\tau'(b_i^{1/m}) &= \tau(\zeta^{j_{\tau'}} b_i^{1/m}) = \zeta^{j_{\tau'}} \zeta^{j_\tau} b_i^{1/m} = \zeta^{j_\tau} \zeta^{j_{\tau'}} b_i^{1/m} \\ &= \tau'(\zeta^{j_\tau} b_i^{1/m}) = \tau'\tau(b_i^{1/m}),\end{aligned}$$

which means that $k(A)$ is abelian, hence $k(A) \subset K$ and $k(A) = K$, as we wanted to prove. □

Remark 1.5.6. Indeed what we actually showed during the proof of the proposition is that all abelian extensions of k of exponent m are contained in $k(A)$, which is something we will use later.

1.5.2 Class number and unit theorem

In this subsection we will prove two classic results concerning the class number of the integer ring of a number field and the finiteness of a certain set in $\mathbb{R}^s$.

Let K be a number field and O_K. As we saw in the last section, O_K is a Dedeking ring, so the set I_K of its non-zero fractional ideals form a multiplicative group. By a **principal fracional ideal** we shall mean the fractional ideal (α) generated by α, where α belongs to the quotient field of O_K (it is indeed a fractional ideal because if $\alpha = \alpha_1/\alpha_2$ with $\alpha_1, \alpha_2 \in O_K$ then $\alpha_2(\alpha) \subset O_K$). The group of non-zero fractional ideals modulo the principal fractional ideals will form a group (the group of non-zero fractional ideals is abelian, so every subgroup is normal) and will be called the **ideal class group**. The cardinal of that group is called the **class number**. Before proving the main theorem about it, we will show a definition and a lemma which can be found in [25].

Definition 1.5.7. Let K be a number field and a be an ideal of O_K. Define $\mathbf{N}a$ as the number of elements of O_K/a.

Lemma 1.5.8. *Let K be a number field and let $\beta \in K$, $\beta \neq 0$. Then*

$$\mathbf{N}(\beta) = N_{\mathbb{Q}}^{K}(\beta).$$

Proposition 1.5.9. *Let K be a number field and O_K its integer ring. Then the class number is finite.*

Proof. Let a be an ideal of O_K. It suffices to show that there exists another ideal b such that b^{-1} belongs to the same ideal class and $\mathbf{N}b \leq C$ where C is a constant that only depends on K. This is because there is only a finite number of ideals for which that inequality holds.

To prove this last assertion, suppose that $\mathbf{N}b \leq C$ and let $b = \rho_1^{n_1} \cdots \rho_l^{n_l}$, where ρ_i are prime ideals in O_K for all i. We have that $O_K/b = \prod_i O_K/\rho_i^{n_i}$, so $\mathbf{N}b = \prod(\mathbf{N}\rho_i)^{n_i}$, and $(\mathbf{N}\rho_i)^{n_i} = p_i^{n_i f_i}$, where the exponents $f_i \geq 1$ are integers and $p_i\mathbb{Z} = \rho_i \cap \mathbb{Z}$. As there is only a finite set P of primes p that satisfy $p \leq C$, and since there is only a finite set of prime ideals in O_K lying above each $p\mathbb{Z}$, there is only a finite set Q of prime ideals in O_K (which is in fact contained in the set of the prime ideals lying above those in P) satisfying $\mathbf{N}b \leq C$. Therefore, each ρ_i must belong to Q and for each ρ_i, since $(\mathbf{N}\rho_i)^{n_i} \leq C$, $n_i \leq m_i$ where m_i is a constant that depends on the prime ideal. Let T be the set of ideals for which the inequality holds and $|Q| = k$. Then

$$T \subset \{\beta_1^{e_1}\beta_2^{e_2} \cdots \beta_{k-1}^{e_{k-1}}\beta_k^{e_k}, \quad 0 \leq e_i \leq m_i, \quad \beta_i \in Q \ , \quad \beta_i \neq \beta_j \Longleftrightarrow i \neq j\},$$

and the size of that set is bounded by $\prod_i(m_i + 1)$, so in particular T is finite, as we wanted to prove.

Let's now prove the first affirmation. Let a be an ideal and let $\omega_1, \omega_2, ..., \omega_N$ be the generators of O_K. We consider the set S of elements of the form

$$a_1\omega_1 + a_2\omega_2 + ... + a_N\omega_N,$$

where

$$0 \leq a_i \leq (\mathbf{N}a)^{1/N} + 1,$$

and $a_i \in \mathbb{Z}$. Then, clearly $|S| > \mathbf{N}a$, so there exist $x, y \in S$ such that $\xi = x - y \in a$ and therefore if $a = \rho_1^{m_1} \cdots \rho_n^{m_n}$, we have that $(\xi) = \rho_1^{m_1'} \cdots \rho_n^{m_n'} \cdots \rho_s^{m_s'}$, where $m_i \leq m_i'$ which means that there is an ideal b with $ab = (\xi)$.

Let $\xi = a_1'\omega_1 + ... + a_N'\omega_N$. Then,

$$|N_{\mathbb{Q}}^K(\xi)| = \prod_{\sigma \in G} |a_1'\sigma(\omega_1) + \cdots + a_N'\sigma(\omega_N)|,$$

where $0 \leq |a_i'| \leq (\mathbf{N}a)^{1/N} + 1$, so denoting $C^{1/N} = 2N \max_{1 \leq i \leq N,\ \sigma \in G}\{|\sigma(\omega_i)|\}$,

$$|N_{\mathbb{Q}}^K(\xi)| \leq (C/2^N)((\mathbf{N}a)^{1/N} + 1)^N \leq (C/2^N)\Big((\mathbf{N}a)^{1/N} + (\mathbf{N}a)^{1/N}\Big)^N = C(\mathbf{N}a).$$

Using Lemma 1.5.8 we obtain that

$$\mathbf{N}((\xi)) = N_{\mathbb{Q}}^K(\xi).$$

Since the function $\mathbf{N}$ is (completely) multiplicative,

$$\mathbf{N}(a)\mathbf{N}(b) = \mathbf{N}((\xi)) \leq C\mathbf{N}(a),$$

so $\mathbf{N}(b) \leq C$, and a and b^{-1} belong to the same class ideal, as we wanted to prove. □

Next we are going to prove another result concerning the finiteness of a certain group, but for doing so we need some previous definitions.

Definition 1.5.10. Let M_K be the set of all absolute values of the number field K. We define a $\mathbf{M_K}$**−divisor** c to be a real function of the absolute values such that

i) $c(v) > 0$ for all absolute values.

ii) $c(v) = 1$ for all but a finite number of v.

iii) If v is a discrete valuation there exists $\alpha \in K$ such that $|\alpha|_v = c(v)$.

Sometimes we will also write $|c|_v$ instead of $c(v)$.

Using that K can be uniquely factored as a (finite) product of prime ideals, we have that for $\alpha \in K$ then $|\alpha|_v = 1$ for all but a finite number of v, hence $|\alpha|_v$ is also a $\mathbf{M_K}$**−divisor** and therefore

$$|\alpha c|_v = |\alpha|_v c(v)$$

is again a $\mathbf{M_K-divisor}$. We also define the following quantities:

$$||c||_v = c(v)^{N_v},$$

$$||c||_K = \prod_v ||c||_v.$$

Let $L(c)$ be the elements of K such that for each v,

$$|\alpha|_v \leq c(v),$$

and denote $\lambda(c)$ as the number of elements of $L(c)$. By the product formula, $||\alpha c||_K = ||c||_K$, and the function

$$x \to \alpha x$$

is clearly a biyection from $L(\alpha c)$ to $L(c)$, so $\lambda(\alpha c) = \lambda(c)$. Now we will prove a useful lemma.

Lemma 1.5.11. *There exist two constants, c_1, c_2 depending on K such that*

$$c_1||c||_K \leq \lambda(c) \leq \sup(1, c_2||c||_K).$$

Proof. Suppose there is one complex value v_0 in M_K, so we identify K_{v_0} with the complex plane. Let's take the square of side $2c(v_0)$ centered at the origin and let m be an integer such that

$$m < \lambda(c)^{1/2} \leq m + 1. \tag{1.5.3}$$

If $m = 0$ then the right inequality is obvious, hence we can assume $m \neq 0$. Divide the square into m^2 equal squares. Then by the inequality 1.5.3, there exists $x, y \in L(c)$ such that both of them belong to the same square, so

$$|x - y|_{v_0} \leq (2c(v_0)/m)\sqrt{2}.$$

Suppose v is another archimedean absolute value. Then

$$|x - y|_v \leq |x|_v + |y|_v \leq 2c(v),$$

and if v is non-archimedean,

$$|x - y|_v \leq c(v).$$

By the product formula,

$$1 = \prod_v |x - y|^{N_v} \leq (8/m^2)2^j||c||_K = c_2||c||_K/4m^2,$$

where j is the number of archimedean values minus one and $c_2 = 2^{j+5}$. Then since $(m + 1)^2 \leq 4m^2$,

$$\lambda(c) \leq (m + 1)^2 \leq 4m^2 \leq c_2||c||_K,$$

as we wanted to prove. Suppose M_K contains a real value v_0. Then we consider the interval of radius v_0 centered at the origin, we divide it in m equal subintervals and we proceed in a similar way.

For the other inequality, let $c_0 = N \sup_{i,v}(|\omega_i|_v)$ where v are the archimedean values. Let $t = c_0 \min_v(c(v)^{-1})$. Take $x_v \in \mathbb{Q}$ such that $(5/4)c_0/c(v) < x_v < (7/4)c_0/c(v)$. By the approximation theorem[3] there exists $\alpha \in K$ such that $|\alpha - x_v| < t/4$. If $q \in \mathbb{Q}$, $|q|_v = |q|$, then for each v, $|\alpha|_v \leq |\alpha - x_v|_v + x_v \leq c_0 c(v)^{-1}/4 + (7/4)c_0 c(v)^{-1} = 2c_0/c(v)$, and $|\alpha|_v \geq x_v - |\alpha - x_v| \geq (5/4)c_0 c(v)^{-1} - c_0 c(v)^{-1} = c_0$, so we have

$$c_0 \leq |\alpha c|_v \leq 2c_0.$$

As there are only a finite number of non-archimedean valuations such that $|\alpha c|_v \neq 1$, we multiply by an integer $a \in \mathbb{Z}$. This integer will be divisible by a big power of the prime that belongs to each of the primes in O_K that correspond to each of the valuations for which $|\alpha c|_v \neq 1$. Therefore, we get that $|\alpha c a|_v \leq 1$ for all non-archimedean valuations, hence

$$c_0|a|_v \leq |\alpha c a|_v \leq 2c_0|a|_v.$$

Using the fact that $\lambda(c)$ and $||c||_K$ don't change if c is multiplied by a constant in K, it suffices to prove the inequality for $\alpha a c$ (we can call it just c), so we can suppose

$$c_0|a|_v \leq |c|_v \leq 2c_0|a|_v \tag{1.5.4}$$

for the archimedean values. Let L be the set of elements belonging to O_K that can be written

$$a_1\omega_1 + ... + a_N\omega_N,$$

where $0 \leq a_i \leq a$, so the size of L is bigger than a^N. As for each non-archimedean v there exists $\alpha \in K$ such that $|\alpha|_v = c(v) \leq 1$, we can consider $n_\rho = ord_\rho(\alpha) \geq 0$, where ρ is the prime associated with v. Therefore, considering the image of L under the natural homomorphism from O_K into $O_K/\prod_\rho \rho^{n_\rho}$, there will be a subset L' of L for which at least

$$\frac{a^N}{\prod(\mathbf{N}\rho)^{n_\rho}}$$

elements will belong to the same class. Then, if we fix $x \in L'$ and y belongs to L',

$$|x - y|_v \leq c(v)$$

for each non-archimedean value, and for the archimedean values, using that the absolute values (in $\mathbb{Q}$) of the coefficients of $x - y$ are smaller or equal than a, the definition of c_0 and 1.5.4,

$$|x - y|_v \leq |a|(N \sup_{i,v}(|\omega_i|_v)) = |a|c_0 \leq |c|_v.$$

[3]Check [25] for a proof of this theorem.

Therefore, at least

$$\frac{a^N}{\prod(\mathbf{N}\rho)^{n_\rho}}$$

elements belong to $L(c)$, which implies that

$$\lambda(c) \geq a^N \prod 1/(\mathbf{N}\rho)^{n_\rho}, \tag{1.5.5}$$

and as $a = |a|_v$ for all the archimedean values, using 1.5.4,

$$a^N = \prod_{v|v_\infty} |a|^{N_v} \geq c_1 \prod_{v|v_\infty} ||c||_v, \tag{1.5.6}$$

where $c_1 = 1/(2c_0)^N$. Finally, using that if $p \in \rho$ for a prime p, and $ord_\rho(p) = e$, $|O_K/\rho| = p^f$ then $ef = N_v$,

$$c(v) = |\alpha|_v = \frac{1}{p^{n_\rho/e}} = \frac{1}{(\mathbf{N}\rho)^{n_\rho/ef}} = \frac{1}{(\mathbf{N}\rho)^{n_\rho/N_v}},$$

$$||c||_v = \frac{1}{(\mathbf{N}\rho)^{n_\rho}}. \tag{1.5.7}$$

Joining the formulas 1.5.5, 1.5.6 and 1.5.7,

$$\lambda(c) \geq c_1 ||c||_K,$$

as we wanted to prove.

□

Next, let S be a finite subset of M_K containing the archimedean values S_∞. We will call $\mathbf{S-units}$ the elements α of K for which

$$|\alpha|_v = 1$$

for all $v \notin S$. We will denote it by K_S. Let $v_1, v_2, ..., v_s$ the absolute values of S, and consider the application

$$x \to (\log ||x||_1, \log ||x||_2, ..., \log ||x||_s)$$

that goes from k_S to $\mathbb{R}^s$. Let $\log(k_S)$ be the image of this application and log the name of the application.

Definition 1.5.12. A **k-dimensional lattice** is a discrete group of $\mathbb{R}^s$ that generates a subspace of dimension k over $\mathbb{R}$.

We are going to prove that $\log(k_S)$ is a $s-1$-dimensional lattice, but first we will prove a technical lemma.

Lemma 1.5.13. *Given $v_0 \in M_K$ there exists a constant $c(v_0)$ for which for all $M_K - divisor$ c, there exists $\beta \in K$ such that*

$$1 \leq ||\beta c||_v \leq c(v_0)$$

for all $v \neq v_0$.

Proof. Let c_1 be the constant of Lemma 1.5.11. Then we choose $c_0 = 1$ if v_0 is archimedean and $c_0 = \mathbf{N}p_0$ if v_0 is non-archimedean. Let c' be a $M_K - divisor$ which differs from c only at v_0 and such that

$$1/c_1 \leq ||c'||_K \leq c_0/c_1.$$

To check that we there exists such divisor, suppose v_0 is archimedean. We can take then $||c'||_{v_0} = \frac{||c||_{v_0}}{c_1||c||_K}$. Suppose v_0 is non-archimedean. Since $||c'||_{v_0}$ must be a power of c_0 then multiplying $||c||_K/||c||_{v_0}$ by a suitable power of c_0 we will obtain a number that satisfies the above inequality. Let $c(v_0) = c_0/c_1$. Using Lemma 1.5.11 we obtain that $\lambda(c') \geq 1$, hence there exists α such that $||\alpha||_v \leq c'(v)$, so $||\alpha||_v \leq c(v)\ \forall\ v \neq v_0$, and if $\beta = 1/\alpha$, then $1 \leq ||\beta c'||_v\ \forall\ v$ and consequently $1 \leq ||\beta c||_v\ \forall\ v \neq v_0$. For the other inequality,

$$||\beta c'||_v \leq ||\beta c'||_K = ||\beta||_K||c'||_K = ||c'||_K \leq c(v_0),$$

where we have used the product formula and the fact that $||\beta c'||_K$ is a product of numbers greater or equal to one.

□

We will now prove the theorem.

Theorem 1.5.14. $\log(k_S)$ *is a $s-1$-dimensional lattice.*

Proof. Let $x \in k_S$. As $|\alpha|_v = 1$ for all $v \notin S$, by the product formula we have that $||x||_1||x||_2 \cdots ||x||_s = 1$, so $\log||x||_1 + \log||x||_2 + ... + \log||x||_s = 0$. Therefore $\log(k_S)$ is contained in a $s-1$ dimensional subspace. To show that it is discrete it suffices to show that for any close ball centered at the origin there is only a finite number of points of $\log(k_S)$ contained on it.

Let $M > 0$ and $B_M = \{x : |x| \leq k\} \subset \mathbb{R}^s$. We must show that $B_M \cap \log(k_S)$ is finite. Let $\alpha \in k_S$ such that $\log(x) \in B_M$. Then

$$(\log||\alpha||_1)^2 + (\log||\alpha||_2)^2 + ... + (\log||\alpha||_s)^2 \leq M^2,$$

so in particular $|\log||\alpha||_i| \leq M$ and $e^{-M} \leq ||\alpha||_i \leq e^M$ for all $i = 1, 2, ..., s$, and for the rest of absolute values $||\alpha||_v = 1$, so

$$e^{-M} \leq ||\alpha||_v \leq e^M \tag{1.5.8}$$

for all $v \in M_K$.

It can be proven that in this situation there is only a finite number of α for which that happens.

Now, given a valuation $v_0 \in S$ we have that as the constant $c(v_0)$ of Lemma 1.5.13 is fixed, there is only a finite number of primes of O_K such that $\mathbf{N}\rho \leq c(v_0)$ (because there is only a finite number of primes that lies above $p\mathbb{Z}$ for each p and only a finite number of primes satisfies $p \leq c(v_0)$). Therefore, denoting S' as the finite set of primes that satisfy the inequality plus S ($S \subset S'$), then using Lemma 1.5.13 we have that for each c there exists $\beta \in K$ for which

$$1 = ||\beta c||_v$$

for all $v \notin S'$. This is because if $\rho \notin S'$ then $||\beta c||_v$ must be a non-negative power of $\mathbf{N}\rho$, hence it must be 1 as $\mathbf{N}\rho > c(v_0)$.

Now we only consider c such that $c(v) \geq 1$ for all v and $c(v) = 1$ for $v \notin S$. Then

$$1 = ||\beta c||_v = ||\beta||_v$$

if $v \notin S'$ and

$$1 \leq ||\beta c||_v \leq c(v_0)$$

if $v \neq v_0$, so

$$1 \leq ||\beta||_v \leq c(v_0) \tag{1.5.9}$$

if $v \notin S$.

Suppose B is the set of such β and consider the application

$$\beta \to \{||\beta||_v\}_{(v \in S'-S)}.$$

The image then is finite because for each entry the possible values are powers of $\mathbf{N}\rho$ with positive bounded exponent as a consequence of 1.5.9. Suppose $\beta_1, \beta_2 ..., \beta_m$ is a set whose image is precisely the image of B. Since $\forall\ \beta \in B$, $||\beta||_v = 1$ for all $v \notin S'$, given $\beta \in B$ we have that there exists β_i with $\beta/\beta_i = u_\beta$, where u_β is a $S-$unit. Denoting

$$b = \min_{\substack{v \in S'-S \\ i=1,2...m}} (||\beta_i||_v),$$

then given c a M_K-divisor satisfying the previous hypothesis we have that there exists $\beta \in B$ such that $||\beta||_v = 1$ for all $v \notin S'$ and

$$||\beta c||_v \leq c(v_0)$$

$\forall\ v \neq v_0$. Consequently, as $\beta = u_\beta \beta_i$, with u_β a S-unit,

$$b||u_\beta c||_v \leq ||\beta c||_v \leq c(v_0),$$

so

$$||u_\beta c||_v \leq \frac{c(v_0)}{b}, \tag{1.5.10}$$

for all $v \neq v_0$, where $b, c(v_0)$ are constants that only depend on v_0. Therefore, given $c(v_0)$ we take c with the above properties such that for all $v \in S$, $v \neq v_0$ $c(v)$ is big enough so that $||u_\beta||_v < 1$, and then by the product formula $||u_\beta||_{v_0} > 1$.

If $v_1, v_2, ..v_{s-1} \in S$ are $s-1$ distinct absolute values in S we take $x_1, x_2..., x_{s-1} \in K_S$ such that for each x_i, $||x_i||_{v_i} > 1$, and $||x_i||_{v_j} < 1$, for each $i \neq j$. Denote

$$\log(x_1) = (\log(||x_1||_{v_1}), \log(||x_1||_{v_2})..., \log(||x_1||_{v_s})) = (\xi_{1,1}, \xi_{1,2}, \xi_{1,3}, ..., \xi_{1,s})$$
$$\log(x_2) = (\log(||x_1||_{v_1}), \log(||x_2||_{v_2})..., \log(||x_2||_{v_s})) = (\xi_{2,1}, \xi_{2,2}, \xi_{2,3}, ..., \xi_{2,s})),$$
$$\vdots$$
$$\log(x_{s-1}) = (\log(||x_{s-1}||_{v_1}), \log(||x_{s-1}||_{v_2})..., \log(||x_{s-1}||_{v_s}))$$
$$= (\xi_{s-1,1}, \xi_{s-2,2}, \xi_{s-1,3}, ..., \xi_{s-1,s}).$$

We are going to prove now that $\log(x_1), \log(x_2)..., \log(x_{s-1})$ are linearly independent over $\mathbb{R}$. Let M be the matrix

$$M = (\xi_{i,j})_{\substack{1 \leq i \leq s \\ 1 \leq j \leq s-1}}$$

and suppose we have a non-trivial combination of the first $s-1$ columns:

$$\lambda_1 Y_1 + \lambda_2 Y_2 + ... + \lambda_{s-1} Y_{s-1} = 0.$$

Then, multiplying by -1 if necessary and rearranging the terms we can suppose that $\lambda_1 > 0$ and $\lambda_1 \geq \lambda_j$ for all $j \neq i$. Since $\xi_{1,1} > 0$ and $\xi_{1,i} < 0$ for all $i \neq 1$,

$$0 = \lambda_1 \xi_{1,1} + \lambda_2 \xi_{2,1} + ... + \lambda_{s-1} \xi_{s,1} \geq \lambda_1 (\xi_{1,1} + \xi_{2,1} + ... + \xi_{s,1}) = \lambda_1 (-\xi_{1,s}) > 0,$$

where in the last equality we have used the product formula, so we have a contradiction. As $\log(K_s)$ is contained (by the product formula) in a $s-1$-dimensional space, we conclude that $\log(K_s)$ is a $s-1$-dimensional lattice.

□

Next, we are going to prove a general result about k-dimensional lattices.

Lemma 1.5.15. *Let Γ be a m-dimensional lattice in $\mathbb{R}^s$. Then Γ is a free abelian group of rank m.*

Proof. We will do it by induction on m. Let $\xi_1, \xi_2, ..., \xi_m$ be a set of independent vectors in Γ and Γ_0 be the subgroup of Γ included in the subspace generated by $\xi_1, \xi_2, ..., \xi_{m-1}$ (it is obviously discrete, so it is a $m-1$-dimensional lattice). By

induction, Γ_0 is generated (as a $\mathbb{Z}$-module) by $\xi_1, ...\xi_{m-1}$. Now we consider the set T of all $\xi \in \Gamma$ such that

$$\xi = a_1\xi_1 + a_2\xi_2 + ... + a_m\xi_m$$

where $0 \leq a_i < 1$ for all $i = 1, 2, .., m-1$ and $0 \leq a_m \leq 1$. We can take ξ'_m whose coefficient b_m of ξ_m is minimun and not 0, because if there was an infinite number of elements in T with the a_m different from each other, $|T| = \infty$, but T is a bounded set, so as Γ is discrete, T must be finite. Suppose $\xi \in T$ is arbitrary:

$$\xi = a_1\xi_1 + a_2\xi_2 + ... + a_m\xi_m.$$

We can multiply ξ'_m by a suitable integer c_m and substract it to ξ so that the coefficient a'_m of ξ_m satisfies $0 \leq a'_m < b_m$. Therefore, if we substract $\xi - c_m\xi'_m$ by an appropiate integral combination of $\xi_1, .., \xi_{m-1}$, the resulting vector will be in T and the coefficient of ξ_m will satisfy $0 \leq a'_m < b_m$, hence it must be 0 and therefore

$$\xi - c_m\xi'_m - c_1\xi_1 - ... - c_{m-1}\xi_{m-1} \in \Gamma_0.$$

Consequently, by induction, there exists $c'_1, c'_2...c'_{m-1}$ such that

$$\xi = c'_1\xi_1 + c'_2\xi_2 + ... + c'_{m-1}\xi_{m-1} + c_m\xi_m,$$

which implies that Γ is a free abelian group of rank m.

□

Corollary 1.5.16. *The set* $\log(K_S)$ *is a free abelian group of rank* $s-1$*, and* K_S *modulo the roots of unity form a free abelian group of rank* $s-1$*. In particular, if* m *is a positive integer,* $K_S/(K_S)^m$ *is finite.*

Proof. The first assertion is an inmediate consequence of the previous lemma and Theorem 1.5.14. For the second one, the elements of the kernel of $\log(x)$ (this application is clearly a group homomorphism) have all absolute values bounded (equal to 1) hence using a similar argument than the one we used in the proof of Theorem 1.5.14, it must be finite. Since it is a group in K_S, all the elements must have finite order, so they are the roots of unity belonging to K.

Let $\beta_1, \beta_2...\beta_{s-1}$ be elements whose images are the generators of $\log(K_S)$. Then for $\beta \in K_S$,

$$\log(\beta) = c_1\log(\beta_1) + ... + c_{s-1}\log(\beta_{s-1}) = \log(\beta_1^{c_1}\beta_2^{c_2}\cdots\beta_{s-1}^{c_{s-1}}),$$

for some integers c_i, $i = 1, ...s-1$, so $\log(\beta/\beta_1^{c_1}\beta_2^{c_2}\cdots\beta_{s-1}^{c_{s-1}}) = 0$ and therefore there exists a root of unit u_β such that

$$\beta = u_\beta\beta_1^{c_1}\beta_2^{c_2}\cdots\beta_{s-1}^{c_{s-1}},$$

as we wanted to prove. For the last assertion, since the group of roots of unity in K is finite, and the coefficients c_i in $K_S/(K_S)^m$ are bounded by m, it follows that $K_S/(K_S)^m$ is finite.

□

1.5.3 A theorem about the finiteness of a maximal abelian extension

The following proposition will also be very important for the proof of the Mordell-Weil Theorem.

Proposition 1.5.17. *Let K a number field, S a finite set of places such that $M_K^\infty \subset S$ and m a positive integer. If L is the maximal extension of K having exponent m which is unramified at all $v \notin S$, L/K is finite.*

Proof. First we note that when K' is a finite extension of K for which the theorem is valid then LK'/K' is unramified by Proposition 1.4.7. Furthermore, for $x \in LK'$ then $x = k_1 l_1 + ... + k_r l_r$ so if $\sigma, \sigma' \in G(LK'/K')$ (LK'/K' is Galois because L/K is Galois and $K \subset K'$),

$$\begin{aligned}\sigma(\sigma'(x)) &= \sigma(k_1\sigma'(l_1) + ... + k_r\sigma'(l_r)) = k_1\sigma\sigma'(l_1) + ... + k_r\sigma\sigma'(l_r)\\ &= k_1\sigma'\sigma(l_1) + ... + k_r\sigma'\sigma(l_r) = \sigma'(\sigma(x)),\end{aligned}$$

where we have used that $\sigma|_L, \sigma'|_L \in G(L/K)$, which is an abelian group, and

$$\sigma^m(x) = k_1\sigma^m(l_1) + ... + k_r\sigma^m(l_r) = k_1 l_1 + ... + k_r l_r = x.$$

Therefore, LK'/K' is also abelian and of exponent m, so LK' is thus contained in the maximal extension with respect to those properties, and it is finite. Consequently, LK'/K is finite because K'/K is finite and for that reason L/K is finte. Hence, we can suppose that K contains the $m-$roots of unity μ_m.

Suppose $S_1 \subset S_2$. Let L_i be the maximal extension unramified outside S_i for each $i = 1, 2$. Then $L_1 \subset L_2$, and if we prove the finiteness for L_2, we will also have it for L_1, so we can enlarge S a finite number of places. Consider the subset of K

$$R_S = \{a \in K : v(a) \geq 0 \ for\ all\ v \notin S\}.$$

Then R_S is obviously a ring because of the properties of the valuation, and $O_K \subset K$. Therefore, R_S is the ring we obtain when we localize O_K at the elements b for which $v(b) = 0$ for all $v \notin S$ and $v(b) \geq 0$ for $v \in S - M_K^\infty$, which is obviously a multiplicative set. We call that set P.

Indeed, we have that for all the elements x of the localized ring $P^{-1}O_K$, the inequality $v(a) \geq 0$ holds for all $v \notin S$. Conversely, when $y \in R_S$ then using the same argument than in the inequality 1.5.10, if $v_\infty \in M_K^\infty$, there exists $b \in k_S$ for which $v(b)$ is very large for all $v \neq v_\infty$ and $v \in S$, and $v_\infty(b)$ is (by the product formula) very big. Then, $yb \in O_K$ because $v(yb) \geq 0$ for all $v \notin M_K^\infty$, hence $y = \frac{yb}{b}$ with $yb \in O_K$ and $v(b) \geq 0$ for $v \in S - M_K^\infty$, so $y \in P^{-1}O_K$.

We have therefore that $R_S = P^{-1}O_K$, which by Lemma 1.3.13 implies that R_S is a Dedekind ring and its prime ideals are in biyective correspondence with those in O_K that does not contain any element of P. Using the same argument

as in equation 1.5.10, it can be proven that for each $v \in S - M_K^\infty$, there exists a_v such that $a_v \in P$ and $v(a_v) > 0$. Thus the only primes in $P^{-1}O_K$ are those corresponding to $v \notin S$. Applying Proposition 1.5.9, since the class number is finite, the size of the quotient group of fractional ideals modulo principal ideals in $P^{-1}O_K$ is also finite (and bounded by the class number of K). Let

$$I_1 = p_{i_{11}}^{e_{11}} \cdots p_{i_{1r_1}}^{e_{1r_1}}$$

$$\vdots$$

$$I_m = p_{i_{m1}}^{e_{m1}} \cdots p_{i_{mr_m}}^{e_{ir_m}}$$

be the ideals in O_K such that $P^{-1}I_1, ..., P^{-1}I_m$ are a set of representatives of elements in the quotient group. Adding to S the valuations corresponding to all the p_j appearing in the decomposition of each of the ideals $I_1, ..., I_m$ (which is of course a finite number of them) then the quotient group is trivial, so $R_S = P^{-1}O_K$ is now a principal ring.

As $v(m) \neq 0$ for a finite number of valuations, we may also add those valuations to the set S so that outside S, $v(m) = 0$.

Since L/K is the maximal abelian extension of exponent m unramified outside S, by Kummer theory (Remark 1.5.6) we have that L is of the form $K(\sqrt[m]{a} : a \in F)$, where $F \in K$ is a certain set. As the subextensions of an unramified extension are unramified, $K(\sqrt[m]{a})/K$ is unramified for all $a \in F$, so if

$$F' = \{a \in K : K(\sqrt[m]{a})/K \; is \; unramified\},$$

$K(\sqrt[m]{a} : a \in F) \subset K(\sqrt[m]{a} : a \in F')$, and reciprocally, as the composite of unramified extensions is unramified, $K(\sqrt[m]{a} : a \in F')$ is unramified, and thus

$$K(\sqrt[m]{a} : a \in F') = K(\sqrt[m]{a} : a \in F).$$

Let $v'|v$ be a valuation in $K(\sqrt[m]{a})$ that extends v. Since the valuation v is normalized, $(v(K^*) = \mathbb{Z})$, if $K(\sqrt[m]{a})/K$ is unramified, then $(v'(K(\sqrt[m]{a})^*) : v(K^*)) = 1$. Hence $v'(K(\sqrt[m]{a})^*) = \mathbb{Z}$ and $mv'(\sqrt[m]{a}) = v'(a) = v(a) \in \mathbb{Z}$ which implies that since $v'(\sqrt[m]{a}) \in \mathbb{Z}$,

$$v(a) \equiv 0 \mod (m).$$

Furthermore, let $a = a'b^m$ with $b \in K$. Then $K(\sqrt[m]{a}) = K(\sqrt[m]{a'})$, so each representative in the group $K^*/(K^*)^m$ defines a unique extension, and $v(a) \mod (m)$ does not depend on the representative, hence we can suppose that

$$F \subset T_S = \{a \in K^*/(K^*)^m : v(a) \equiv 0 \mod (m), v \notin S\}$$

(we can take F so that there is just one representative of each element for each class in the group $K^*/(K^*)^m$. Therefore, there is an injection of F into T_S).

Consequently, for proving the finiteness of L it suffices to prove that the set T_S is finite. Consider the map

$$R_S^* \to T_S,$$

which consists on taking classes. It is well defined because $v(a) = 0$ for all $a \in R_S^*$ and $v \notin S$. In fact, $R_S^* = \{a \in K^* : v(a) = 0 \ \ \forall v \notin S\}$ because if $v(a) > 0$ for some $v \notin S$, then $v(a^{-1}) < 0$, hence $a^{-1} \notin R_S$, and if $v(a) = 0$ for all $v \notin S$ then $v(a^{-1}) = 0$ so $a^{-1} \in R_S$. We are going to prove that the map is surjective.

Indeed, let $a \in K$ be a representative of any class in T_S. Then

$$(a) = p_{i_1}^{mr_1} \cdots p_{i_l}^{mr_l} \beta_{j_1} \cdots \beta_{j_s},$$

where $p_{i_1}, ..., p_{i_l} \notin S$ and $\beta_i \in S$ (r_k may be negative). Therefore, when localizing as before, $aR_S = (\overline{p_{i_1}}^{r_1} \cdots \overline{p_{i_l}}^{r_l})^m$. Furthermore, since R_S is principal, there exists $b \in K^*$ such that

$$bR_S = \overline{p_{i_1}}^{r_1} \cdots \overline{p_{i_l}}^{r_l}.$$

Consequently, $aR_S = b^m R_S$. Thus, there exists a unit $u \in R_S$ such that $a = ub^m$, so $u = ab^{-m}$, and therefore the image of u under the map is the class of a, as we wished to prove. The map is of course a homomorphism, and the subgroup R_S^m is included in the kernel of that map, so we have that

$$R_S^*/(R_S^*)^m \twoheadrightarrow R_S/Ker \simeq T_S,$$

where the first map is surjective, hence

$$R_S^*/(R_S^*)^m \twoheadrightarrow T_S$$

is surjective, and using Corollary 1.5.16, $R_S^*/(R_S^*)^m$ is finite. Therefore, T_S is also finite, as we wanted to prove. $\square$

Chapter 2

The arithmetic and geometry of elliptic curves.

The following section just pretends to be a very brief summary of basic definitions and properties about elliptic curves. For more details, check Silverman [43].

Given a field K, an elliptic curve is a pair (E, O), where E is a smooth proyective curve over $\overline{K}$ of genus 1 [1] and O is a point of E. The elliptic curve is said to be defined over K if the curve and O are defined over K. Thus it can be proven (using Riemann-Roch) that an elliptic curve can be embedded in $\mathbb{P}^2(\overline{K})$ and has the following expression:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_1, ..., a_6 \in \overline{K}$. The only point with $Z = 0$ is $O = [0 : 1 : 0]$, so taking non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$ and dehomogenizing the previous equation,

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

This last expression is called Weiestrass equation. Therefore, the points of E are the points that satisfies this last equation plus the point O. We say that E/K is defined over K when $a_1, ..., a_6 \in K$. We always think of the elliptic curve as the points $E(\overline{K})$ in $\mathbb{P}^2(\overline{K})$ satisfying the first equation, and if E/K is defined over K,

$$E(K) = E(\overline{K}) \cap \mathbb{P}^2(K)$$

will be the points in E with coordinates in K. Suppose $char(K) \neq 2$. Then applying the change of coordinates

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

[1] For basic information about the genus of a curve, check [43]

we obtain the equation:

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

where

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3,$$
$$b_6 = a_3^2 + 4a_6.$$

We also define

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4,$$
$$c_6 = b_2^3 + 36b_2b_4 - 216b_6,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$
$$j = c_4^3/\Delta.$$

Now, if $char(K) \neq 2, 3$, then making the change of variables

$$(x, y) \to ((x - 3b_2)/36, y/216),$$

we obtain the following equation

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

The only change of variables that preserves this equation is

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t,$$

with $u, r, s, t \in \overline{K}$. With this change of variables,

$$c_4' = u^{-4}c_4, \quad c_6' = u^{-6}c_6, \quad \Delta' = u^{-12}\Delta.$$

Throughout most of the work we will deal with elliptic curves over number fields, so we can always suppose that

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

for some $A, B \in K$ $(char(K) = 0)$. With this notation,

$$\Delta = -16(4A^3 + 27B^2).$$

The only change of variables that preserves this equation is

$$x = u^2x', \qquad y = u^3y',$$

for some $u \in \overline{K}^*$, and then the corresponding new coefficients will be

$$A' = u^{-4}A, \quad B' = u^{-6}B, \quad \Delta' = u^{-12}\Delta.$$

Definition 2.0.1. Let K be a field and E/K a curve given by a Weiestrass equation. We say that

- i) E is non-singular if $\Delta \neq 0$ (and in particular (E, O) is an elliptic curve).
- ii) E has a node if $\Delta = 0$ and $c_4 \neq 0$.
- iii) E has a cusp if $\Delta = c_4 = 0$.

Furthermore, the above conditions can also be characterized by the derivaties of the function

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

More precisely,

- E is singular if and only if there exists a point (x_0, y_0) for which

$$(\partial f/\partial X(x_0, y_0), \partial f/\partial Y(x_0, y_0)) = (0, 0).$$

- E has a node if and only if E is singular and the tangent lines of E at (x_0, y_0) are different.
- E has a cusp if and only if it E is singular and it has just one tangent line.

2.1 Definition and properties of the group law

Let E/K an elliptic curve. We can define a group law as follows: Let $P, Q \in E$. Take the line L joining them and let R be the intersection of that point with E (by Bezout's theorem, there will be three intersection points). Let L' be the line that joins R and O. Then, the third intersection point will be the definition of $P + Q$. The following lemma, which will be left without proof, will assert that E with this operation is a group.

Lemma 2.1.1. *The operation $+$ has the following properties:*

- *i) If the intersection points of a line L with E are P, Q and R, then*

$$P + Q + R = O.$$

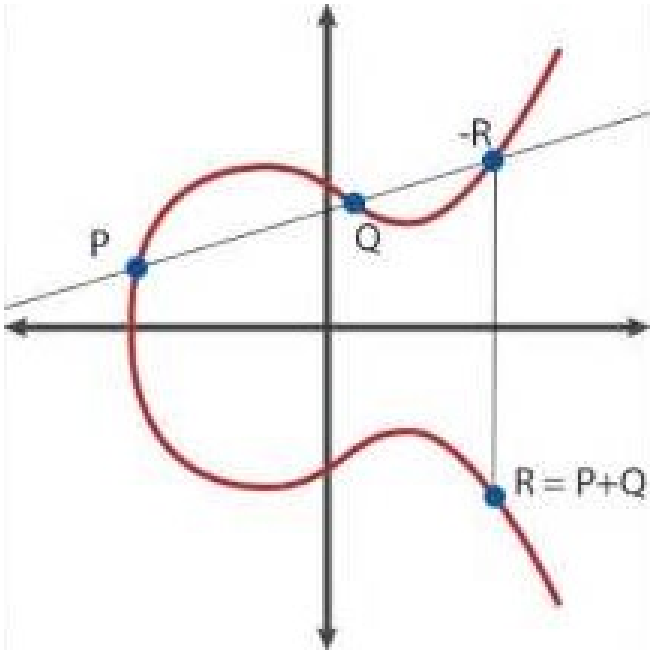
- *ii) $P + O = P$ for all $P \in E$.*
- *iii) $P + Q = Q + P$ for all $P, Q \in E$.*
- *iv) Let $P \in E$. There exists a point denoted by $-P$ such that*

$$P + (-P) = O.$$

- *v) Let $P, Q, R \in E$. Then,*

$$(P + Q) + R = P + (Q + R).$$

- *vi) $E(K)$ is a subgroup of $E(\overline{K})$ with the same operation.*



Though we are not going to prove them, all of them are obvious except *vi*), which will be clear when we show the explicit formulas of the operation, and the associativity, because doing it by hand could be quite tedious. However, using divisors, it can be proven that there is a biyection between a certain picard group $Pic^0(E)$ [2] and the points of the elliptic curve that preserves the group operation, so associativity then follows by the fact that it holds in that picard group.

From now on, if $m \in \mathbb{N}$ and $P \in E$, we will write

$$[m]P = mP = P + ... + P \ (m \ times),$$

and if $m < 0$,

$$[m]P = (-P) + ... + (-P) \ (\ -m \ times).$$

We also define $E[m]$ as the torsion subgroup, that is,

$$E[m] = \{P \in E : [m]P = 0\}.$$

The following proposition contains all the explicit formulas for the group operation.

[2] For the definition and properties of this subgroup of the divisors, check [43].

Proposition 2.1.2. *Let E be an elliptic curve given by the Weiestrass equation:*

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

Then

- *i) Let $P_0 = (x_0, y_0) \in E$. Then,*

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

- *ii) Let $P_1 = (x_1, y_1)$, and $P_2 = (x_2, y_2)$. Then by the previous case, if $x_1 = x_2$ and*

$$y_2 = -y_1 - a_1x_1 - a_3$$

then $P_1 = -P_2$. Otherwise,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \quad if\ x_1 \neq x_2;$$

and

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1y_1 + a_3},$$

$$\nu = \frac{-x_1^3 + a_4x + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad if\ x_1 = x_2,\ y_1 = y_2.$$

- *iii) With the quantities defined before, $P_3 = P_1 + P_2$ has the following coordinates*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Therefore, if $P_1 \neq \pm P_2$, then

$$x(P_1 + P_2) = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 + a_1\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big) - a_2 - x_1 - x_2,$$

and denoting $P = (x, y)$,

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

The fact that $E(K)$ is a subgroup is now obvious because all the coefficients involved in the formulas belong to K. Furthermore, let $\sigma \in Gal(\overline{K}/K)$ and $P_1, P_2 \in E(\overline{K})$ with $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Suppose $x_1 \neq x_2$ (the other case is done the same way). Let λ, ν be the quantities involved in the sum of P_1 and P_2 and λ', ν' the quantities involved in the sum of $\sigma(P_1)$ and $\sigma(P_2)$. Then,

$$\sigma(\lambda) = \frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)} = \lambda'$$

and

$$\sigma(\nu) = \frac{\sigma(y_1)\sigma(x_2) - \sigma(y_2)\sigma(x_1)}{\sigma(x_2) - \sigma(x_1)} = \nu',$$

hence

$$\sigma(x_3) = \lambda'^2 + a_1\lambda' - a_2 - \sigma(x_1) - \sigma(x_2) = x(\sigma(P_1) + \sigma(P_2)),$$

and

$$\sigma(y_3) = -(\lambda' + a_1)\sigma(x_3) - \nu' - a_3 = y(\sigma(P_1) + \sigma(P_2)),$$

so we obtain that $\forall\ P, Q \in E$,

$$\sigma(P_1 + P_2) = \sigma(P_1) + \sigma(P_2). \tag{2.1.1}$$

In particular, using induction we have that for all $m \in \mathbb{Z}$ and all $P \in E(\overline{K})$,

$$\sigma([m]P) = [m]\sigma(P).$$

2.2 Morphisms, isogenies and torsion groups.

In ths subsection we will just present some definitions and properties of some objects without proving them.

Definition 2.2.1. Let $\phi : C_1 \to C_2$ be a morphism of curves over K. If ϕ is constant we define $\deg(\phi) = 0$, and if not,

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

where for $f \in K(C_2)$, $\phi^*(f) = f \circ \phi \in K(C_1)$. We say that ϕ is separable (resp. inseparable, purely inseparable) when the above extension is separable (resp. inseparable, purely inseparable). $K(C_1)$ and $K(C_2)$ are the function fields of C_1 and C_2 respectively.

Definition 2.2.2. Let $\phi : C_1 \to C_2$ be a morphism of curves and $P \in C_1$. The ramification index $e_\phi(P)$ is defined as

$$e_\phi(P) = ord_P(\phi^* t_{\phi(P)}),$$

where $t_{\phi(P)}$ is a uniformizer at $\phi(P)$ (which means that $ord_{\phi(P)}(t_{\phi(P)}) = 1$). We recall that for each curve C and $P \in C$, the local ring $\overline{K}[C]_P$ is a discrete valuation ring, so ord_P is well defined, and in fact it can be extended to the function field $\overline{K}(C)$.

With the above notation, we have the following proposition relating all those terms.

Proposition 2.2.3. *Let $\phi : C_1 \to C_2$ be a non-constant map of non-singular curves.*

- *i) For every $Q \in C_2$,*

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

- *ii) In fact, for all $Q \in C_2$ except for a finite number of them,*

$$\#\phi^{-1}(Q) = \deg_s(\phi),$$

where $\deg_s(\phi) = \deg_s(\overline{K}(C_1)/\phi^*\overline{K}(C_2))$ is the separable degree of that extension.

This last proposition implies that every non-constant morphism of non-singular curves is surjective.

Now, though there are some properties which can be extended to curves in general, we will restrict to elliptic curves.

Definition 2.2.4. Let (E_1, O_{E_1}) and (E_2, O_{E_2}) be elliptic curves. We say that ϕ is an *isogeny* if ϕ is a morphism and

$$\phi(O_{E_1}) = O_{E_2}.$$

Proposition 2.2.5. *Let (E_1, O_{E_1}) and (E_2, O_{E_2}) be elliptic curves. Suppose ϕ is an isogeny. Then for all $P, Q \in E_1$,*

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

The proof of this theorem is again based on the biyection that preserves the group law between $Pic^0(E)$ and E. It is quite an impressive result, because just assuming some 'regularity' conditions and the fact that $\phi(O_{E_1}) = O_{E_2}$ we obtain that ϕ is a homomorphism of groups.

Definition 2.2.6. Let K a field and C/K a smooth curve defined over K. We say that C'/K is a *twist* when it is a smooth curve defined over K and there is an isomorphism

$$\phi : C \to C'$$

which is defined over $\overline{K}$. We say that C'/K is a *quadratic twist* if there is an isomorphism

$$\phi' : C \to C'$$

defined over a quadratic extension of K.

Proposition 2.2.7. *Let $\phi : E_1 \to E_2$ an isogeny of elliptic curves. Then*

- *i) For every $Q \in E_2$,*
$$\#\phi^{-1}(Q) = \deg_s(\phi).$$
In fact, for every $P \in E_1$,
$$e_\phi(P) = \deg_i(\phi),$$
which is something stronger since by Proposition 2.2.3,
$$\#\phi^{-1}(Q)\deg_i(\phi) = \deg(\phi),$$
which implies that
$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

- *ii) If ϕ is separable, then using the above formula,*
$$\#\ker(\phi) = \#\phi^{-1}(O_{E_2}) = \deg_s(\phi) = \deg(\phi),$$
and $e_\phi(P) = 1$, which means that ϕ is unramified.

Now, using the above explicit formulas for addition of points, it can be proven (by induction) that
$$[m] : E \to E$$
is a morphism of (non-singular) elliptic curves because it can be expressed as a quotient of polynomials and because we assume that E is a non-singular curve. Thus, since $[m](O) = O$, $[m]$ is an isogeny, hence it is an endomorphism of E (we already knew that it preserved the group operation since the group is commutative).

Using the duplication formula, it is easy to see that for almost all points, $[2]P \neq O$, and it is also easy to see that there are points Q different from O such that $[2]Q = O$, so for all m odd, $[m]Q = Q \neq O$. This implies that as for all n integer, $[n]$ is the composition of isogenies of the previous forms, using Proposition 2.2.7 we have that since all of them are not constant, they are surjective. Therefore, the composition of them is also surjective and consequently, $[n]$ is surjective.

Definition 2.2.8. Let E be an elliptic curve and ϕ, ψ two isogenies. Then, $(\psi+\phi)$ defined as
$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$
is an isogeny (by the definition of isogeny and the explicit formulas). Furthermore, $\phi\psi$ defined as
$$(\phi\psi)(P) = \phi(\psi(P))$$
is also an isogeny. Therefore, denoting $End(E) = \{\phi : E \to E,\ \phi \ \ isogeny\}$, $End(E)$ has a ring structure.

Definition 2.2.9. We say that an elliptic curve E has no complex multiplication if the following map:

$$[\ .\ ] \to End(E)$$

is an isomorphism, so in other words, the only isogenies of E are the multiplication by an integer.

Example 2.2.10. Let K be a field with $char(K) \neq 2$ and E/K the elliptic curve

$$E : y^2 = x^3 - x.$$

Take i an element of $\overline{K}$ such that

$$i^4 = 1$$

but $i^2 \neq 1$. Then

$$[i] : (x, y) \to (-x, iy)$$

is an isogeny which is not constant and such that

$$[i]^4 = [1].$$

Therefore, $[i]$ cannot be of the form $[m]$ for any $m \in \mathbb{Z}$ because $[i] \neq [1]$, and if $[i] = [m]$ with $m \neq 1$ then

$$[m^4] = [m]^4 = [1],$$

which is a contradiction. Hence E has complex multiplication.

Definition 2.2.11. Let $\mathcal{K}$ be an algebra finitely generated over $\mathbb{Q}$. We say that an *order* $\mathcal{R}$ of $\mathcal{K}$ is a subring of $\mathcal{K}$ finitely generated as a $\mathbb{Z}$-module such that $\mathcal{R} \bigotimes \mathbb{Q} = \mathcal{K}$.

Lemma 2.2.12. *Let $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field ($D < 0$). Then if $\mathcal{R}$ is an order of $\mathcal{K}$, there exists an integer $d > 0$ such that*

$$\mathbb{Z} + d\mathcal{O} = \mathcal{R},$$

where $\mathcal{O}$ is the ring of integers of $\mathcal{K}$.

Definition 2.2.13. A *quaternion algebra* is an algebra of the form

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \beta + \mathbb{Q}\alpha\beta$$

with the properties

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

Through the next proposition, whose proof can be found in [43], we are going to show all the possibilities for the ring $End(E)$.

Proposition 2.2.14. *The endomorphism ring of an elliptic curve is either $\mathbb{Z}$, an order of a quadratic imaginary field or an order in a quaternion algebra. Besides, if $char(K) = 0$ then $End(E)$ can only be either $\mathbb{Z}$ or an order of a quadratic imaginary field.*

The proof of this proposition uses the fact that the natural map

$$End(E) \bigotimes \mathbb{Z}_p \to End(T_p(E)) \cong M_2(\mathbb{Z}_p)$$

is an injection (We will define later on the group $T_p(E)$) (See [43]).

Corollary 2.2.15. *Let K a number field and E/K an elliptic curve with complex multiplication. Then*

$$End(E) \cong \mathbb{Z} + d\mathcal{O},$$

where d is an integer and $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\sqrt{D})$ with $D < 0$ for some integer D.

Definition 2.2.16. Let $q = p^r$ with p a prime number, $K = \mathbb{F}_q$ and let E/K be an elliptic curve. If $P = [X_0 : Y_0 : Z_0] \in E$, we define

$$\phi(P) = [X_0^q : Y_0^q : Z_0^q].$$

As the coefficients of the elliptic curve lie in K, they are fixed when raised to the power q, therefore $\phi(P) \in E$, and so ϕ is a morphism (in fact it is an isogeny). We will call it the *Frobenius endomorphism.*

Proposition 2.2.17. *Let $q = p^r$, E an elliptic curve defined over $\mathbb{F}_q$ and $\phi : E \to E$ the Frobenius endomorphism. Then $m + n\phi$ is separable if and only if $p \nmid m$. In particular, $1 - \phi$ is separable.*

This last result also holds when E is defined over K, where $\mathbb{F}_q \subset K$. We will now present a certain type of isogeny that will allow us to compute $E[m]$.

Theorem 2.2.18. *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then there exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1$$

such that $\hat{\phi} \circ \phi = [m]$ where $m = \deg(\phi)$. This isogeny is called the Dual isogeny *Furthermore,*

- *a) $\phi \circ \hat{\phi} = [m]$.*
- *b) If $\psi : E_1 \to E_2$ is another isogeny,*

$$\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}.$$

- *c) For all* $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m],$$

and

$$\deg([m]) = m^2.$$

- *d)* $\deg(\hat{\phi}) = \deg(\phi)$, *so* $\hat{\hat{\phi}} = \phi$.

The 'difficult' items are the existence of such isogeny (it is proven using the biyective correspondence between $Pic^0(E)$ and points in the curve), and section b). Section three is a consequence of b) plus induction. Therefore,

$$[m^2] = [m][m] = [\deg([m])],$$

hence $m^2 = \deg(m)$.

Corollary 2.2.19. *Let* E *be an elliptic curve and* $m \in \mathbb{Z}$, $m \neq 0$. *Then*

- *a) If* $char(K) = 0$ *or if* $(m, char(K)) = 1$,

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

- *b) If* $char(K) = p$ *then either*

$$E[p^e] \cong \{O\}, \quad or$$

$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}.$$

Proof. For the first case, using Proposition 2.2.17 we have that $[m]$ is separable, so $\#E[m] = \deg([m]) = m^2$. Using the classification of finite abelian groups, for each prime $q|m$,

$$E[q] \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

because $E[q]$ does not contain any element of order q^2. Applying induction, we have the result for powers of q, and using that in both sides we can express both groups as a direct product of p-Sylow groups, we conclude the result. For b), check [43]. □

Corollary 2.2.20. *The map* $\deg : Hom(E_1, E_2) \to \mathbb{Z}$ *is a positive definite quadratic form, which means that*

- *a)* $\deg(\phi) \geq 0$ *and* $\deg(\phi) = 0$ *if and only if* $\phi = O$.

- *b) The pairing* $\deg : E_1 \times E_2 \to \mathbb{Z}$ *defined as*

$$(\phi, \psi) = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

is bilinear.

The proof of it can be found in [43]. It is just a consequence of the properties of the dual isogeny.

Definition 2.2.21. Let E be an elliptic curve and l a prime number. Then we define the l-adic *Tate module* as the group

$$T_l(E) = \lim_{\longleftarrow n} E[l^n],$$

where we have taken the inverse limit with respect to the maps

$$[l] : E[l^{n+1}] \to E[l^n].$$

These maps are obviously well defined because if $P \in E[l^{n+1}]$ then $[l^n][l]P = O$. Since each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, $T_l(E)$ is also a $\mathbb{Z}_l$-module with the following operation:

$$(\sum_{n=0} a_n l^n, (P_0, P_1, ...)) \to (a_0 P_0, [a_0 + a_1 l]P_1, ..., [\sum_{n=0}^{N-1} a_n l^n]P_N, ...),$$

where $(P_0, P_1, ..., P_N, ...) \in T_l(E)$. We have that $[l][\sum_{n=0}^{N} a_n l^n]P_{N+1} = [\sum_{n=0}^{N-1} a_n l^n]P_N$, so

$$(a_0 P_0, [a_0 + a_1 l]P_1, ..., [\sum_{n=0}^{N-1} a_n l^n]P_N, ...) \in T_l(E)$$

and therefore the application is well defined and is linear. As with $E[l^n]$, we also have a similar expression for $T_l[E]$.

Proposition 2.2.22. *The Tate Module $T_l(E)$ has the following structure:*

- $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ *if* $l \neq char(K)$.
- $T_l(E) \cong \{0\}$ *or* $\mathbb{Z}_l$ *if* $l = char(K) > 0$.

This result is an immediate consequence of Corollary 2.2.19.

2.3 Reduction in elliptic curves

Let K be a local field with a normalized discrete valuation, and let

$$R = \Big\{a \in K : v(a) \geq 0\Big\},$$

$$M = \Big\{a \in K : v(x) > 0\Big\},$$

$$R^* = \Big\{a \in K : v(a) = 0\Big\},$$

and $k = R/M$. Let $\pi \in R$ such that $v(\pi) = 1$, and denote $\tilde{t}$ the image of the application

$$R \to R/M = k.$$

Let E/K an elliptic curve with equation

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

Definition 2.3.1. We say that a Weiestrass equation is *minimal* when $v(\Delta)$ is minimun provided that $a_1, ..., a_6 \in R$, that is, if we make any change of variables then either $v(\Delta)$ is not smaller or any of the coefficients don't belong to R.

As we saw before, the only possible changes of variable are

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t.$$

Recall that with this change of variables, $u^{12}\Delta' = \Delta$, so then it is easy to see that when $a_i \in R$ for all $i = 1, ..., 6$ and $v(\Delta) < 12$, the equation is minimal. In fact, a minimal equation is unique up to a change of coordinates of the form

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

with $u \in R^*$ and $r, s, t \in R$.

Suppose that the equation

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

is minimal, and consider

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6},$$

which is called the *reduction of E modulo π*, and has coefficients in k. For $P \in E(K)$, multiplying by an adequate positive power of π we can suppose that

$$P = [X_0 : Y_0 : Z_0],$$

where X_0, Y_0, Z_0 are homogeneous coordinates of P such that $X_0, Y_0, Z_0 \in R$ and at least one of them is in R^*. Thus when taking classes modulo M we obtain a proyective point

$$\tilde{P} = [\tilde{X_0}, \tilde{Y_0}, \tilde{Z_0}],$$

because at least one of the coordinates of P does not belong to M. Furthermore, $\tilde{P} \in \tilde{E}$, so we have an application

$$E(K) \to \tilde{E}(k)$$

given by

$$P \to \tilde{P}$$

which is in fact an homomorphism of groups because when taking classes the group law is preserved. The curve $\tilde{E}/k$ may be (or not) singular depending on the valuation of Δ. However, it can be proven that for any elliptic curve there can only be one singular point, and the non-singular part E_{ns} forms a group. Thus we can define

$$E_0(K) = \Big\{ P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k) \Big\},$$

$$E_1(K) = \Big\{ P \in E(K) : \tilde{P} = \tilde{O} \Big\}.$$

Furthermore, if K is complete, there is an exact sequence

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0.$$

Definition 2.3.2. Let E/K an elliptic curve and let $\tilde{E}$ the reduced curve of a minimal equation. Then we say that

- *i*) E has a *good reduction* over K if $\tilde{E}$ is non-singular.
- *ii*) E has *multiplicative* (or *semi-stable*) *reduction* over K if $\tilde{E}$ has a node.
- *iii*) E has *additive* (or *unstable*) *reduction* over K if $\tilde{E}$ has a cusp.

We also say that E has bad reduction at K if either *ii*) or *iii*) occur. When E has multiplicative reduction we say that the reduction is *split* if the slopes of the tangent lines at the node are in k, and we say that it is *non-split* if they are not in k.

Equivalently,

- *i*) E has a *good reduction* over K if and only if $v(\Delta) = 0$.
- *ii*) E has *multiplicative reduction* over K if and only if $v(\Delta) > 0$ and $v(c_4) = 0$.
- *iii*) E has *additive reduction* over K if and only if $v(\Delta) > 0$ and $v(c_4) > 0$.

The proof of this equivalence is just based on the above study of the singularity of general elliptic curves and the fact that

$$v(\Delta) = 0 \iff \tilde{\Delta} = \tilde{0},$$

and the same with c_4.

The following definition was very important for the resolution of Fermat's Last Theorem.

Definition 2.3.3. Let K be a number field. We say that an elliptic curve E/K is semistable if it only has good reduction or multiplicative reduction at all its valuations.

Let L/K be an extension of fields, v a discrete non-archimedean valuation and $\omega|v$ a valuation in L. Then the subgroup G_ω acts on $\widetilde{E}(k)$. This is because if $P = [X_0 : Y_0 : Z_0]$ and

$$P' = [X_0 + x_0 : Y_0 + y_0 : Z_0 + z_0]$$

with $\omega(x_0), \omega(y_0), \omega(z_0) > 0$, then for $\sigma \in G_\omega$, and $x \in L$,

$$\omega(\sigma(x)) = \omega(x).$$

Hence

$$\omega(\sigma(x_0)), \omega(\sigma(y_0)), \omega(\sigma(z_0)) > 0,$$

and therefore

$$\widetilde{\sigma(P)} = [\widetilde{\sigma(X_0)}, \widetilde{\sigma(Y_0)}, \widetilde{\sigma(Z_0)}] = [\sigma(\widetilde{X_0 + x_0}) : \sigma(\widetilde{Y_0 + y_0}) : \sigma(\widetilde{Z_0 + z_0})] = \widetilde{\sigma(P')},$$

so

$$\sigma(\widetilde{P}) = \widetilde{\sigma(P)},$$

is well defined.

2.4 Elliptic curves over finite fields.

In this section we are just going to mention an important estimation of the number of points of an elliptic curve over a finite field. Let $q = p^r$ with p a prime number and $K = \mathbb{F}_q$. Let ϕ be the Frobenius automorphism

$$\phi_q(x) = x^q$$

with $x \in \overline{K}$. Then clearly $\phi(x) = x^q = x$ if and only if $x \in K$ because taking the polynomial $f(t) = x^q - x$, then $f(x) = 0$ and the q roots of f are precisely the elements of $\mathbb{F}_q$. Therefore, if E/K is an elliptic curve over K then

$$P \in E(K) \Longleftrightarrow \phi(P) = P,$$

where ϕ is the Frobenius endomorphism. Now we will show a version of the Cauchy -Schwarz inequality that will be useful for our estimation.

Lemma 2.4.1. *Let A be an abelian group and*

$$d : A \to \mathbb{Z}$$

a positive definite quadratic form. Then, for all elements $\phi, \psi \in A$, the following inequality holds:

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}.$$

Proof. If $\phi = 0$ then the inequality is obvious. If not let

$$L(\psi, \phi) = d(\psi - \phi) - d(\phi) - d(\psi)$$

be the bilinear form. Then, as d is definite positive, for all $m, n \in \mathbb{Z}$

$$0 \leq d(m\psi - n\phi) = d(m\psi) + mnL(\psi, \phi) + d(n\phi). \tag{2.4.1}$$

Now,

$$-2md(\phi) = L(m\phi, \phi) = d((m-1)\phi) - d(m\phi) - d(\phi),$$

and using the induction hypothesis, $d((m-1)\phi) = (m-1)^2 d(\phi)$, so

$$-2md(\phi) = (m-1)^2 d(\phi) - d(m\phi) - d(\phi),$$

and therefore rearranging the terms,

$$d(m\phi) = m^2 d(\phi).$$

Returning to equation 2.4.1,

$$0 \leq d(m\psi) + mnL(\psi, \phi) + d(n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi),$$

and taking $m = -L(\psi, \phi)$ and $n = 2d(\psi)$,

$$0 \leq d(\psi)(4d(\phi)d(\psi) - L(\psi, \phi)^2).$$

Since $d(\psi) > 0$,

$$|L(\psi, \phi)| \leq 2\sqrt{d(\phi)d(\psi)},$$

as we wanted to prove.

□

With this technical lemma in mind, we are going to prove the following theorem.

Theorem 2.4.2. *Let E/K be an elliptic curve defined ofver K with $|K| = q$. Then*

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

Proof. It can be proven that $\deg(\phi) = q$ (check [43]). Then as

$$P \in E(K) \iff \phi(P) = P,$$

$$E(K) = \ker(1 - \phi).$$

Using Proposition 2.2.17, $1 - \phi$ is separable, so by Proposition 2.2.7,

$$\#E(K) = \#\ker(1 - \phi) = \deg(1 - \phi),$$

and now applying Lemma 3.4.7,

$$|\#E(K) - 1 - q| = |\deg(1 - \phi) - \deg(1) - \deg(\phi)| \leq 2\sqrt{\deg(\phi)} = 2\sqrt{q},$$

as we wanted to prove.

□

This last theorem will be useful to define later on the L-functions and to formulate the Birch and Swinnerton-Dyer conjecture .

Next, fix a prime l which is prime to $char(K)$ and recall the obvious map

$$End(E) \to End(T_l(E))$$

given by

$$\psi \to \psi_l,$$

where if $(P_0, P_1, ..., P_N, ...) \in T_l(E)$,

$$\psi_l(P_0, P_1, ..., P_N, ...) = (\psi(P_0), \psi(P_1), ..., \psi(P_N), ...).$$

Since $T_l(E)$ is a $\mathbb{Z}_l$-module of rank 2, $End(T_l(E))$ can be seen as the matrices $M_2(\mathbb{Z}_l)$, hence talking about $\det(\psi_l)$ and $tr(\psi_l)$ makes sense. The following result gives some information about those numbers.

Proposition 2.4.3. *Let $\psi \in End(E)$. Then*

$$\det(\psi_l) = \deg(\psi), \quad \text{and} \quad tr(\psi_l) = 1 + \deg(\psi) - deg(1 - \psi),$$

so in particular $\det(\psi_l)$ and $tr(\psi_l)$ belong to $\mathbb{Z}$ and don't depend on l.

With this proposition we are able to prove the following lemma.

Lemma 2.4.4. *Let E/K an elliptic curve. Then there exists $\alpha \in \mathbb{C}$ such that $|\alpha| = \sqrt{q}$ and*

$$\#E(K) = 1 - \alpha - \overline{\alpha} + q.$$

Proof. Let

$$\phi : E \to E$$

be the Frobenius endomorphism and recall that

$$E(K) = \deg(1 - \phi).$$

The characteristic polynomial of ϕ_l has coefficients in $\mathbb{Z}$ and thus it has roots in $\mathbb{C}$. Consequently,

$$\det(t - \phi_l) = t^2 - tr(\phi_l)t + \det(\phi_l) = (t - \alpha)(t - \beta),$$

where $\alpha, \beta \in \mathbb{C}$. For every rational number m/n, with $m, n \in \mathbb{Z}$,

$$\det((m/n) - \phi_l) = \det(m - n\phi_l)/n^2 = \deg(m - n\phi)/n^2 \geq 0,$$

as deg(.) is a non-negative function. Thus, by density we have that the same inequality holds for the real numbers, so either $\det(t - \phi_l)$ has one double real root or it has two complex conjugate roots. Anyway,

$$|\alpha| = |\beta| = \sqrt{\det(\phi_l)} = \sqrt{\deg(\phi)} = \sqrt{q},$$

and $\beta = \overline{\alpha}$.

Furthermore,

$$\#E(K) = \deg(1-\phi) = \det(1-\phi_l) = (1-\alpha)(1-\beta) = 1-\alpha-\beta+q. \qquad (2.4.2)$$

□

Chapter 3

Mordell-Weil Theorem

The main goal of this chapter is to prove the Mordell-Weil Theorem for elliptic curves over number fields. Throughout this chapter K denotes a number field.

3.1 The descendent procedure

In this section we are going to introduce a common tool for proving that an abelian group is finitely generated.

Proposition 3.1.1. *Let A be an abelian group and h a function $h : A \to \mathbb{R}$ with the following properties:*

i) If $Q \in A$, then there exists a constant $C_1 = C_1(Q) > 0$ such that for all $P \in A$ we have

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

ii) There exists an integer $m \geq 2$ and a constant $C_2 \geq 0$ depending on A such that for all $P \in A$,

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

iii) For all constant $C_3 \geq 0$ the set

$$\{P \in A : h(P) \leq C_3\}$$

is finite.

If in addition A/mA is finite, A is finitely generated.

Proof. Let $Q_1, ..., Q_s$ be a set of representatives of all the elements of A/mA. Let $P \in A$. Then $\overline{P} = \overline{Q_{i_1}}$ for some $1 \leq i_1 \leq s$. Therefore

$$P = mP_1 + Q_{i_1}$$

for some $P \in A$. Repeating the process,

$$P_1 = mP_2 + Q_{i_2},$$

$$P_2 = mP_3 + Q_{i_3},$$

$$\vdots$$

$$P_{n-1} = mP_n + Q_{i_n}.$$

Using the first and the second property of h,

$$m^2 h(P_n) \leq h(mP_n) + C_2 = h(P_{n-1} - Q_{i_n}) + C_2 \leq 2h(P_{n-1}) + C_1' + C_2,$$

where if $C_1(Q_i)$ is the constant of the first property of h depending on Q_i then $C_1' = \max_{1 \leq i \leq s}(C_1(Q_i))$, so

$$h(P_n) \leq 1/m^2(2h(P_{n-1}) + C_1' + C_2).$$

Applying the same inequality for the rest of the P_i,

$$h(P_n) \leq \frac{2^n}{m^{2n}} h(P) + (\frac{1}{m^2} + \frac{2}{m^4} + \frac{2^2}{m^6} + ... + \frac{2^{n-1}}{m^{2n}})(C_1' + C_2),$$

and as $m \geq 2$,

$$\begin{aligned} h(P_n) &\leq 2^{-n} h(P) + (2^{-2} + 2^{-3} + .. + 2^{-n-1})(C_1' + C_2) \\ &\leq 2^{-n} h(P) + (C_1' + C_2) \leq 1 + C_1' + C_2 \end{aligned}$$

if we choose n sufficiently large. Now the set $\{P : h(P) \leq 1 + C_1' + C_2\}$ is finite by the third property, and $P_n \in \{P : h(P) \leq 1 + C_1' + C_2\}$. Joining all the equalities of the sums of points,

$$P = m^n P_n + \sum_{k=1}^{n} m^{k-1} Q_{i_k}.$$

Consequently, we have that all $P \in A$ can be written as an integral combination of points in the finite set $\{P : h(P) \leq 1 + C_1' + C_2\} \cup \{Q_1, ..., Q_s\}$. We conclude that A is finitely generated with sets of generators $\{P : h(P) \leq 1 + C_1' + C_2\} \cup \{Q_1, ..., Q_s\}$.

□

3.2 Weak Mordell-Weil Theorem

This part of the proof is perhaps the most difficult one because it involves the use of valuations and completions and certain properties of number fields proven before.

Theorem 3.2.1. *Let $m \geq 2$ be an integer and E an elliptic curve over K. Then the group*

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

is finite.

We will prove it through some lemmas and propositions.

Lemma 3.2.2. *Let L/K be a finite Galois extension. Then if $E(L)/mE(L)$ is finite, $E(K)/mE(K)$ is also finite.*

Proof. Consider the natural application $E(K)/mE(K) \to E(L)/mE(L)$, which is obviously well defined because $E(K) \subset E(L)$ and $mE(K) \subset mE(L)$. Let Φ the kernel of the application, thus

$$\Phi = (E(K) \cap mE(L))/mE(K).$$

For each $\overline{P} \in \Phi$ take one of its representant $P \in E(K) \cap mE(L)$, choose $Q_P \in E(L)$ so that $[m]Q_P = P$, and consider the application

$$\lambda_P : G_{L/K} \to E[m]$$

defined by $\lambda_P(\sigma) = Q_P^\sigma - Q_P$, which in general is not an homomorphism. The image is in $E[m]$ because

$$[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = P^\sigma - P = 0,$$

since $P \in E(K)$. If we had $\lambda_P = \lambda_{P'}$ for some $P, P' \in E(K) \cap mE(L)$ then

$$(Q_P - Q_{P'})^\sigma = Q_P - Q_{P'}$$

for all $\sigma \in G_{L/K}$, which implies that $Q_P - Q_{P'} \in E(K)$, and thus $P - P' = [m]Q_P - [m]Q_{P'} \in E(K)$, hence $\overline{P} = \overline{P'}$. Therefore we have constructed a one-to-one function

$$\Phi \to Map(G_{L/K}, E[m]), \quad P \to \lambda_P.$$

Note that this is not an homomorphism, and that the function depends on the choice of P among those that belong to the same class, and also depends on the election of Q. The groups $G_{L/K}$ and $E[m]$ are finite. Consequently, $Map(G_{L/K}, E[m])$ is also finite, so Φ is finite, and since

$$(E(K)/mE(K))/\Phi \hookrightarrow E(L)/mE(L),$$

then as $E(L)/mE(L)$ and Φ are finite, $E(K)/mE(K)$ is also finite. In fact,

$$|(E(K)/mE(K))|/|\Phi| = |(E(K)/mE(K))/\Phi| \leq |E(L)/mE(L)|.$$

This proves our assertion. □

Since for each point $P \in E[m]$, $x(P)$ is a root of a fixed polynomial $\xi_m(x)$ with coefficients in K and the same for $y(P)$, then the extension of K obtained by adjoining those $x(P)$ and $y(P)$ is finite. In fact, it is Galois because it is the decomposition field of the polynomial $\xi_m(x)$ and the quadratic polynomial obtained when evaluating at $x(P)$ the Weiestras equation. Hence, using the Lemma, we can suppose that $E[m] \subset K$.

Proposition 3.2.3. *Let the Kummer pairing*

$$\kappa : E(K) \times G_{\overline{K}/K} \to E[m]$$

be defined as follows: Let $P \in E(K)$ and choose $Q \in E(\overline{K})$ such that $[m]Q = P$ (we can do that because the isogeny $[m]$ is non-constant and hence surjective). Then

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

The Kummer pairing has the following properties:

i) It is well defined.

ii) It is bilinear.

iii) The kernel on the left (the elements in $E(K)$ whose image is zero for all σ) is $mE(K)$.

iv) The kernel on the right is $G_{\overline{K}/L}$, where

$$L = K([m]^{-1}E(K))$$

is the composite of all fields $K(Q)$ where $Q \in E(\overline{K})$ and $[m]Q \in E(K)$.

Therefore, the Kummer pairing induces a perfect pairing

$$E(K)/mE(K) \times G_{L/K} \to E[m].$$

Proof. The Kummer pairing does not depend on the choice of Q because if $[m]Q = [m]Q' = P$ then

$$[m](Q - Q') = 0,$$

which means that $Q - Q' \in E[m]$, hence $Q - Q' \in E(K)$, and therefore $(Q - Q')^\sigma = (Q - Q')$, so $Q^\sigma - Q = Q'^\sigma - Q'$. Furthermore, $Q^\sigma - Q \in E[m]$ because $[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = P^\sigma - P = 0$ since $P \in E(K)$.

Let $P, P' \in E(K)$. As κ does not depend on the choice of Q, we can choose $Q + Q'$ for $P + P'$ where $[m]Q = P$ and $[m]Q' = P'$, hence

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

as we wanted to prove. If $\sigma, \sigma' \in G_{\overline{K}/K}$ then

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

where we have used that

$$[m]Q^{\sigma'} = ([m]Q)^{\sigma'} = P^{\sigma'} = P$$

because $P \in E(K)$, hence bilinearity holds.

For the third assertion, fixing P and Q,

$$Q^{\sigma} - Q = 0 \ \forall \sigma \in G_{\overline{K},K} \iff Q \in E(K),$$

which happens if and only if $P = [m]Q \in mE(K)$; and fixing σ, suppose σ fixes all Q for which $[m]Q = P$ where $P \in E(K)$. Therefore, σ fixes $L = K([m]^{-1}E(K))$ and hence the kernel is $G_{\overline{K},L}$.

Consequently,

$$E(K)/mE(K) \times G_{L/K} \to E[m]$$

is a bilinear form which is well-defined and is perfect because if an element is on the kernel, then it must be zero since we have just taken the quotient group. Furthermore, L/K is Galois because for $\sigma \in G_{\overline{K},K}$ and $[m]Q = P$ with $P \in E(K)$,

$$P = \sigma(P) = \sigma([m]Q) = [m]\sigma(Q).$$

Hence $\sigma(Q) \in L$, and therefore $\sigma(L) = L$, so L/K is Galois and

$$G_{\overline{K},K}/G_{\overline{K},L} \simeq G_{L/K}.$$

□

Corollary 3.2.4. *The group $E(K)/mE(K)$ is finite if and only if $G_{L/K}$ is finite.*

Proof. Suppose $G_{L/K}$ is finite (the other case is done the same way). Let $G_{L/K} = \{\sigma_1, ..., \sigma_n\}$, $E[m] = \{P_1, ..., P_{m^2}\}$ and fixing $\overline{P}$, there are at most m^{2n} possibilities for the function $\kappa(\overline{P}, -)$, which is a finite number, hence if $|E(K)/mE(K)| > m^{2n}$ there exists $\overline{P}, \overline{P'}$ with $\overline{P} \neq \overline{P'}$ and $\kappa(\overline{P}, -) = \kappa(\overline{P'}, -)$, so $\kappa(\overline{P} - \overline{P'}, -) = O$, which implies that $\overline{P} = \overline{P'}$, which is a contradiction. Therefore, $|E(K)/mE(K)| \leq m^{2n}$ and hence it is finite. □

Thus, to prove the Weak Mordell-Weil theorem, it suffices to show that $G_{L/K}$ is finite. We will formulate now an important result whose proof can be found in [43] and that uses the formal group.

Proposition 3.2.5. *Let K be a number field, v a valuation, k_v the residue field of its completion K_v, E/K an elliptic curve, m an integer such that $v(m) = 0$, and suppose that E has good reduction at v. Then the natural map*

$$E(K)[m] \to \tilde{E}(k_v)$$

is inyective.

Now we are going to give some properties of the extension of fields L/K from proposition 3.2.3.

Proposition 3.2.6. *The extension of fields L/K where*

$$L = ([m]^{-1}E(K))$$

is abelian and of exponent m (i.e. all its elements have order which divides m). Furthermore, if

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

then the extension L/K is unramified outside S.

Proof. By proposition 3.2.3 we have that $E(K)/mE(K) \times G_{L/K} \to E[m]$ is perfect, hence the homomorphism

$$G_{L/K} \to Hom(E(K)/mE(K), E[m])$$

given by

$$\sigma \to \kappa(-, \sigma)$$

is inyective. The group $Hom(E(K)/mE(K), E[m])$ is abelian because $E[m]$ is abelian and is of exponent m because $E[m]$ is of exponent m, so L/K is abelian and of exponent m.

To prove that L/K is unramified for each $v \notin S$ it suffices to prove it for each $K(Q)/K$ where $[m]Q \in E(K)$ as L is the composite of those fields and the composite of unramified fields is again unramified. Hence it suffices to prove that if $v'|v$ is a valuation at $K(Q)$ with $v \notin S$ then for $\sigma \in I_{v'|v}$, where $I_{v'|v}$ is the inertia subgroup, $Q^\sigma = Q$. Since $v(\Delta) = 0$ because E has good reduction at v, $v'(\Delta) = 0$ because $\Delta \in K$ and $v'|_K = v$. Therefore, E has good reduction at v', and using the definition of the inertia subgroup and taking classes mod the maximal ideal $m_{v'}$,

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

But as $[m]Q \in E(K)$,

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

so $Q^\sigma - Q \in E(K)[m]$ because $E(K)$ contains the m-torsion points. Using Proposition 3.2.5, since the reduction map from $E(K)[m]$ is inyective and $Q^\sigma - Q$ is in the kernel of that application, $Q^\sigma - Q = 0$, which proves our assertion. □

To finish the proof of Theorem 3.2.1, we will prove that an extension of fields with the properties of the previous one is finite (if we assume, of course, that K is a number field). To do that we will use some of the work done at the introduction section.

Proof of the Weak Mordell-Weil Theorem.

Let L/K be the extension of fields of Proposition 3.2.3. The composite of two unramified fields of exponent m is again unramified, abelian and of exponent m. Let L' be the maximal extension with respect to those two properties. Using Proposition 1.5.17, L' has those properties, and applying the previous remark, $L'L$ also has those properties. Therefore, by maximality $L'L \subset L'$, hence $L'L = L'$. Consequently,

$$K \subset L \subset \ L',$$

so L/K is finite, which concludes the proof.

3.3 Proof of the Mordell-Weil Theorem for the case $K = \mathbb{Q}$.

We will use the following easy lemma.

Lemma 3.3.1. *If $(x, y) \in E(\mathbb{Q})$, where E is given by the equation*

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

with $A, B \in \mathbb{Z}$, then (x, y) can be written as $(x, y) = (\frac{a}{d^2}, \frac{b}{d^3})$ with $(a, d) = (b, d) = 1$.

Proof. Let $(x, y) = (\frac{m_1}{n_1}, \frac{m_2}{n_2})$ with $(m_1, n_1) = (m_2, n_2) = 1$. Then, substituting it into the equation of E,

$$\frac{m_2^2}{n_2^2} = \frac{m_1^3}{n_1^3} + A\frac{m_1}{n_1} + B,$$

so

$$m_2^2 n_1^3 = n_2^2(m_1^3 + Am_1 n_1^2 + Bn_1^3)$$

As $(n_1, m_1) = 1$ then $(n_1^3, m_1^3 + Am_1n_1^2 + Bn_1^3) = 1$, hence $n_1^3 | n_2^2$, and since $(n_2, m_2) = 1$, $m_2^2 | (m_1^3 + Am_1n_1^2 + Bn_1^3)$, thus

$$n_1^3 = n_2^2$$

and

$$m_2^2 = m_1^3 + Am_1n_1^2 + Bn_1^3.$$

Therefore, $n_1^3 = n_2^2$ implies that the exponent of each prime in the descomposition of n_1 must be even, and the exponent of each prime in the descomposition of n_2 must be divisible by 3. Consequently, $n_1 = d^2$ for d an integer, and hence $n_2 = d^3$, which proves our assertion. □

For each $t \in \mathbb{Q}$, t can be written as $t = \frac{p}{q}$ where $(p,q) = 1$, and we define $H : \mathbb{Q} \to \mathbb{N}$ as

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

Therefore, for each $P \in E(\mathbb{Q})$,

$$h_x(P) = \log(H(x(P)))$$

if $P \neq O$ and

$$h_x(P) = 0$$

if $P = 0$.

Then clearly h_x is a non-negative function. We are going to prove now that it satisfies the three conditions from above.

Proposition 3.3.2. *a) Let $P_0 \in E(\mathbb{Q})$. Then there exists a constant $C_1 > 0$ depending on P_0, A and B such that for all $P \in E(\mathbb{Q})$ we have*

$$h_x(P + P_0) \leq 2h_x(P) + C_1,$$

b) There exists an integer $m \geq 2$ and a constant $C_2 \geq 0$ depending on A, B such that for all $P \in E(\mathbb{Q})$,

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

c) For all constant $C_3 \geq 0$ the set

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$$

is finite.

Proof. Let $P_0 = (x_0, y_0) \in E(\mathbb{Q})$ and $P = (x, y) \in E(\mathbb{Q})$. By the previous lemma, $(x, y) = (\frac{a}{d^2}, \frac{b}{d^3})$ and $(x_0, y_0) = (\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3})$, where a, b, d, a_0, b_0, d_0 are like those in the lemma. Taking $C_1 \geq \max(h_x(P_0), h_x([2]P_0))$, we can suppose that $P \neq O, \pm P_0$. Therefore, we have that

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

so eliminating denominators,

$$x(P + P_0) = \frac{y^2 + y_0^2 - 2yy_0 - x^3 + x^2x_0 + xx_0^2 - x_0^3}{(x - x_0)^2}.$$

Using that both points belong to the curve,

$$\begin{aligned} x(P + P_0) &= \frac{A(x + x_0) + 2B - 2yy_0 + x^2x_0 + xx_0^2}{(x - x_0)^2} \\ &= \frac{(A + xx_0)(x + x_0) + 2B - 2yy_0}{(x - x_0)^2}, \end{aligned}$$

and substituying,

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

We have that

$$|ad_0^2 - a_0d^2|^2 \leq ||a|d_0^2 + |a_0|d^2|^2 \leq (d_0^2 + |a_0|)\max(a^2, d^4) = C\max(a^2, d^4),$$

and similarly,

$$\begin{aligned} |numerator\ of\ x(P+P_0)| &\leq ((|A|d_0^2 + |a_0|)(d_0^2 + |a_0|) + 2|B|d_0^4)\max(a^2, d^4) \\ &\quad + 2|b_0d_0||bd| \leq C'\max(a^2, d^4, |bd|), \end{aligned}$$

where $C' = \max(((|A|d_0^2 + |a_0|)(d_0^2 + |a_0|) + 2|B|d_0^4), 2|b_0d_0|)$ and $C, C' > 0$ are constants that depend on A, B and P_0. We also have that since $(x, y) \in E$,

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

Consequently,

$$b^2 \leq (1 + |A| + |B|)\max(|a|, |d|^2)^3 = C''\max(|a|, |d|^2)^3,$$

which implies that

$$\begin{aligned} |bd| &\leq \sqrt{C''}\max(|a|, d^2)^{3/2}\sqrt{\max(|a|, d^2)} \\ &= \sqrt{C''}\max(|a|, d^2)^2 = \sqrt{C''}\max(a^2, d^4). \end{aligned}$$

Therefore,

$$|numerator\ of\ x(P+P_0)| \leq \max(C', C'\sqrt{C''})\max(a^2, d^4),$$

and so if $C''' = \max(C', C'\sqrt{C''})$, then $H(x(P+P_0)) \leq C'''\max(a^2, d^4)$, hence taking logarithms,

$$h_x(P+P_0) \leq \log(C''') + 2\log(\max(|a|, d^2)) = \log(C''') + 2h_x(P).$$

Taking $C_1 = \max(\log(C'''), h_x(P_0), h_x([2]P_0))$, we have the first property of h_x. Now by choosing $C_2 \geq 4h_x(T)$ where $T \in E(\mathbb{Q})[2]$, we can assume that $2[P] \neq O$, and then by the duplication formula, denoting $P = (x, y)$,

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

Define the homogeneous polynomials,

$$F(X, Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4,$$

$$G(X, Z) = 4X^3Z + 4AXZ^3 + 4BZ^4,$$

and if we write $x = x(P) = a/b$ where $(a, b) = 1$, then $x([2]P) = F(a, b)/G(a, b)$. We would like to give a lower bound for the amount of cancellation in that fraction. For that reason, we apply the Euclides Algorithm to polynomials $f(x) = x^4 - 2Ax^2 - 8Bx + A^2$ and $g(x) = 4x^3 + 4Ax + 4B$.

$$x^4 - 2Ax^2 - 8Bx + A^2 = \frac{x}{4}(4x^3 + 4Ax + 4B) + (-3Ax^2 - 9Bx + A^2),$$

$$4x^3 + 4Ax + 4B = (-\frac{4}{3A}x + \frac{4B}{A^2})(-3Ax^2 - 9Bx + A^2) + (\frac{16}{3}A + 36\frac{B^2}{A^2})x,$$

$$-3Ax^2 - 9Bx + A^2 = (\frac{-9A^3}{108B^2 + 16A^3}x - \frac{27BA^2}{108B^2 + 16A^3})(\frac{16}{3}A + 36\frac{B^2}{A^2})x + A^2,$$

so rearranging the equations,

$$\begin{aligned} -3Ax^2 - 9Bx + A^2 = (\frac{-9A^3}{108B^2 + 16A^3}x - \frac{27BA^2}{108B^2 + 16A^3})\Big(&4x^3 + 4Ax + 4B \\ &- (-\frac{4}{3A}x + \frac{4B}{A^2})(-3Ax^2 - 9Bx + A^2)\Big) + A^2, \end{aligned}$$

hence

$$\begin{aligned} \frac{3}{4\Delta}\Big(\frac{4\Delta}{3} - 36B^2 + 4A^2x^2\Big)\Big(-3Ax^2 - 9Bx + A^2\Big) \\ = A^2 - \frac{9A^2}{4\Delta}(Ax + 3B)g(x). \end{aligned}$$

Therefore,

$$\begin{aligned} \frac{3}{4\Delta}(\frac{4\Delta}{3} - 36B^2 + 4A^2x^2)f(x) + \frac{1}{4\Delta}\Big(-x\Delta + 27B^2x - 3A^2x^3 + 9A^3x + 27A^2B\Big)g(x) \\ = A^2, \end{aligned}$$

and doing a little of algebra we obtain

$$\begin{aligned} \frac{3}{4\Delta}(\frac{16A^3}{3} + 4A^2x^2)f(x) + \frac{1}{4\Delta}\Big(-4A^3x - 3A^2x^3 + 9A^3x + 27A^2B\Big)g(x) \\ = A^2, \end{aligned}$$

so

$$(16A + 12x^2)f(x) + \Big(5Ax - 3x^3 + 27B\Big)g(x) = 4\Delta. \tag{3.3.1}$$

Homogenizing,

$$\Big(16AZ^2 + 12X^2\Big)F(X, Z) + \Big(5AXZ^2 - 3X^3 + 27BZ^3\Big)G(X, Z) = 4\Delta Z^7, \tag{3.3.2}$$

and applying the same method with $F(1, z)$ and $G(1, z)$, if

$$f_2(X, Z) = 4\Delta X^3 - 4A^2BX^2Z + 4A(3A^3 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3,$$

$$g_2(X,Z) = A^2BX^3 + A(5A^3+32B^2)X^2Z + 2B(13A^3+96B^2)XZ^2 \\ - 3A^2(A^3+8B^2)Z^3,$$

then

$$f_2(X,Z)F(X,Z) + g_2(X,Z)G(X,Z) = 4\Delta X^7. \tag{3.3.3}$$

Let $\delta = m.c.d.(F(a,b), G(a,b))$. Using equations 3.3.2 and 3.3.3, $\delta|4\Delta b^7$ and $\delta|4\Delta a^7$, and as $(a,b)=1$, $\delta|4\Delta$, so $\delta \leq |4\Delta|$. Consequently,

$$H(x([2]P)) = \max(|F(a,b)|, |G(a,b)|)/\delta \geq \max(|F(a,b)|, |G(a,b)|)/4|\Delta|. \tag{3.3.4}$$

On the other hand, applying equations 3.3.2 and 3.3.3,

$$|4\Delta a^7| \leq 2\max(|f_2(a,b)|, |g_2(a,b)|)\max(|F(a,b)|, |G(a,b)|),$$
$$|4\Delta b^7| \leq 2\max(|f_1(a,b)|, |g_1(a,b)|)\max(|F(a,b)|, |G(a,b)|),$$

Using that the coefficients of polynomials f_1, f_2, g_1, g_2 only depend on A and B and that they are homogeneous of degree 3,

$$\max(|g_1(a,b)|, |f_1(a,b)|) \leq C_2' \max(|a|^3, |b|^3),$$
$$\max(|g_2(a,b)|, |f_2(a,b)|) \leq C_2'' \max(|a|^3, |b|^3),$$

Putting the four last equations together,

$$|4\Delta a^7| \leq 2C_2' \max(|a|^3, |b|^3)\max(|F(a,b)|, |G(a,b)|),$$
$$|4\Delta b^7| \leq 2C_2'' \max(|a|^3, |b|^3)\max(|F(a,b)|, |G(a,b)|),$$

Applying these two last equations and 3.3.4,

$$\min(\frac{1}{C_2'}, \frac{1}{C_2''})\max(|a|,|b|)^4 \leq 1/(4|\Delta|)\max(|F(a,b)|, |G(a,b)|) \leq H(x([2]P)),$$

hence if $C_2''' = \max_{T\in E(\mathbb{Q})[2]}(4h_x(T))$ and we take $C_2 = \max(-\log(\min(\frac{1}{C_2'}, \frac{1}{C_2''})), C_2''')$, then we will have that taking logarithms on the last equation,

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

For the third property of h_x, first we observe that for a constant $C_3 > 0$,

$$\{q \in \mathbb{Q} : H(q) \leq e^{C_3}\}$$

is finite because if $q = \frac{a}{b}$ where $(a,b)=1$, then $|a|, |b| \leq e^{C_3}$. Consequently, there are at most $2e^{C_3}+1$ possibilities for a and $2e^{C_3}$ possibilities for b, hence there are at most $2e^{C_3}(2e^{C_3}+1)$ rational numbers in the set, so for

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$$

the set of x-coordinates of points of that set is finite. Since for a given t there are at most 2 possible points in $E(\mathbb{Q})$ with t as the $x-$coordinate, the set

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$$

is finite, which concludes the proposition. □

If we join this last proposition, Theorem 3.2.1 and Proposition 3.1.1, we obtain the Mordell-Weil Theorem for elliptic curves in $\mathbb{Q}$.

3.4 Heights on Projective Space

The main goal of this section is to introduce some height functions on the proyective space over number fields and to use them for constructing some height functions in elliptic curves.

First we introduce a height function on $\mathbb{P}^N(\mathbb{Q})$. Let $P \in \mathbb{P}^N(\mathbb{Q})$. Then P can be expressed uniquely as $P = [x_0, ..., x_N]$ where $x_i \in \mathbb{Z}$ for $i = 0, ..., N$ and $gcd(x_0, x_1, ..., x_N) = 1$. We define

$$H(P) = \max(|x_0|, ..., |x_N|),$$

and by the same reason as in the previous chapter,

$$\{P \in \mathbb{P}^N(\mathbb{Q}) : \ H(P) \leq C\}$$

has size bounded by $(2C + 1)^{N+1}$.

Let K be a number field, consider $\mathbb{P}^N(K)$ and let

$$P = [x_0, ..., x_N]$$

with

$$x_1, ..., x_N \in K.$$

Recall that for a valuation $v|p$ in K, $n_v = [K_v : \mathbb{Q}_p]$. Define

$$H_K(P) = \prod_{v \in M_K} \max(|x_1|_v, ..., |x_N|_v)^{n_v}.$$

There are a few things that need to be checked if we want a consistent definition.

Lemma 3.4.1. *With the above definition,*

i) $H_K(P)$ *does not depend on the choice of the representative for* P*.*

ii) If L/K *is finite, then for* $P \in \mathbb{P}^N(K)$*,*

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

iii) $H_K(P) \geq 1$*.*

Proof. Let $P = [x_0, ..., x_N]$ and $\lambda \in K^*$. Then

$$\prod_{v \in M_K} \max(|\lambda x_1|_v, ..., |\lambda x_N|_v)^{n_v} = \prod_{v \in M_K} \prod_{v \in M_K} |\lambda|_v^{n_v} \max(|x_1|_v, ..., |x_N|_v)^{n_v}$$
$$= \prod_{v \in M_K} |\lambda|_v^{n_v} \prod_{v \in M_K} \max(|x_1|_v, ..., |x_N|_v)^{n_v} = \prod_{v \in M_K} \max(|x_1|_v, ..., |x_N|_v)^{n_v},$$

where in the last line we have used Proposition 1.4.14.

For the second part, let $P = [x_0, ..., x_N] \in \mathbb{P}^N(K)$. Then

$$\prod_{w \in M_L} \max(|x_1|_w, ..., |x_N|_w)^{n_w} = \prod_{v \in M_K} \prod_{w|v \in M_L} \max(|x_1|_w, ..., |x_N|_w)^{n_w}$$
$$= \prod_{v \in M_K} \prod_{w|v \in M_L} \max(|x_1|_v, ..., |x_N|_v)^{n_w}$$
$$= \prod_{v \in M_K} \max(|x_1|_v, ..., |x_N|_v)^{\sum_{w|v} n_w}$$
$$= \prod_{v \in M_K} \max(|x_1|_v, ..., |x_N|_v)^{n_v[L:K]} = H_K(P)^{[L:K]},$$

where in the second step we used that $x_0, ..., x_N \in K$ and therefore $|x_i|_w = |x_i|_v$ for all i, and in the last one we applied Proposition 1.4.13 and the fact that if $n'_w = [L_w : K_v]$,

$$\sum_{w|v} n_w = \sum_{w|v} n'_w n_v = [L : K] n_v.$$

For the last part, taking some $x_i \neq 0$ and dividing by it, we have that one of the coordinates is 1, so

$$\max(|x_1|_v, ..., 1, ..., |x_N|_v) \geq 1.$$

□

Considering the special case of $\mathbb{Q}$ for this definition and taking $P = [x_0, ..., x_N]$ with $x_i \in \mathbb{Z}$ for all i and $gcd(x_0, ..., x_N) = 1$, then

$$H_{\mathbb{Q}}(P) = \prod_{v \in M_{\mathbb{Q}}} \max(|x_0|_v, ..., |x_N|_v)^{n_v} = \tag{3.4.1}$$
$$\prod_{v \in M_{\mathbb{Q}}} \max(|x_0|_v, ..., |x_N|_v) = \max(|x_0|, ..., |x_N|). \tag{3.4.2}$$

This is because as $gcd(x_0, ..., x_N) = 1$, for each prime at least one of the components is not divisible by p, thus its valuation is 1 and for the rest of components, $|x_i|_p \leq 1$ because they are integers. Therefore, we have that for the special case of $\mathbb{Q}$, this height coincides with the one given at the beginning of the section.

Definition 3.4.2. Let $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$. The *(absolute) height of P* is defined as follows. Choose any K number field for which $P \in K$ (there is a representative whose components belong to K). Then

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

The height does not depend on the choice of K because if we choose L then denoting LK as the minimal field containing L and K, using Lemma 3.4.1 we would have that

$$H_{LK}(P)^{1/[LK:\mathbb{Q}]} = H_L(P)^{[LK:L]/[LK:\mathbb{Q}]} = H_L(P)^{1/[L:\mathbb{Q}]},$$

and using the same argument,

$$H_{LK}(P)^{1/[LK:\mathbb{Q}]} = H_K(P)^{1/[K:\mathbb{Q}]},$$

so

$$H_K(P)^{1/[K:\mathbb{Q}]} = H_{LK}(P)^{1/[LK:\mathbb{Q}]} = H_L(P)^{1/[L:\mathbb{Q}]}.$$

Definition 3.4.3. We say that

$$F : \mathbb{P}^N(\overline{\mathbb{Q}}) \to \mathbb{P}^M(\overline{\mathbb{Q}})$$

is a *morphism of degree d* of proyective spaces if

$$F(P) = [f_1(P), ..., f_M(P)],$$

where $f_0, ..., f_M \in \overline{\mathbb{Q}}[x_0, ..., x_N]$ are homogeneous polynomials of degree d and the only common zero that have those polynomials is $x_0 = ... = x_N = 0$, hence evaluating F at P is well defined in $\mathbb{P}^M(\overline{\mathbb{Q}})$.

Proposition 3.4.4. *Let F a morphism of degree d of proyectives spaces as above. Then there exist two constants C_1, C_2 that depend only on F such that for all $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$,*

$$C_2 H(P)^d \leq H(F(P)) \leq C_1 H(P)^d.$$

Proof. Let $P = [x_0, ..., x_N]$. Choose a number field K containing all the coordinates of P and the coefficients of f_i for each i. Let $v \in M_K$ and define the following quantities:

$$|P|_v = \max_{0 \leq i \leq N}(|x_i|_v),$$

$$|F(P)|_v = \max_{0 \leq j \leq M}(|f_j(P)|_v),$$

and

$$|F|_v = \max(|a|_v \ where\ a\ is\ any\ coefficient\ of\ any\ f_i).$$

We also define

$$H_K(F) = \prod_{v \in M_K} |F|_v^{n_v}$$

and

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

$H_K(F)$ is well defined because there are only a finite number of coefficients, and thus there are a finite number of absolute values that, when they are evaluated at each coefficient, at least one of them is different from 1. Thus there is only a finite number of terms different from 1 in that product. Then, with the above definitions,

$$H_K(P) = \prod_{v \in M_K} |P|_v^{n_v},$$

$$H_K(F(P)) = \prod_{v \in M_K} |F(P)|_v^{n_v}.$$

For each $v \in M_K$ we define

$$\varepsilon(v) = 1,$$

if v is archimedean and

$$\varepsilon(v) = 0,$$

if v is non-archimedean.

Then, for each j and each v,

$$|f_j(P)|_v \leq \tilde{C}_1^{\varepsilon(v)} |F|_v |P|_v^d, \tag{3.4.3}$$

where $\tilde{C}_1$ is the maximun number of possible monomials in a homogeneous polynomial of degree d (which in fact is $\binom{N+d}{N}$), because when v is non-archimedean,

$$|f_j(P)|_v \leq |F|_v |P|_v^d,$$

while if v is archimedean,

$$|f_j(P)|_v \leq \tilde{C}_1 F|_v |P|_v^d.$$

Taking the maximun over j in 3.4.3 we have that

$$|F(P)|_v \leq \tilde{C}_1^{\varepsilon(v)} |F|_v |P|_v^d,$$

and raising to the power n_v this last equation and multiplying over all $v \in M_K$,

$$H_K(F(P)) \leq \tilde{C}_1^{\sum_{v|\in M_K^\infty} n_v} H_K(F) H_K(P)^d = \tilde{C}_1^{[K:\mathbb{Q}]} H_K(F) H_K(P)^d.$$

Taking $[K:\mathbb{Q}]$-roots we have that if $C_1 = \tilde{C}_1 H(F)$,

$$H(F(P)) \leq C_1 H(P)^d,$$

as we wanted to prove.

For the other inequality, let $I =< f_1, ..., f_M >$. Then by hypothesis, $\mathbb{V}(I) = \{0\}$, so using the Nullstellensatz Theorem,

$$< X_1, ..., X_N >= \mathbb{II}(\mathbb{V}(I)) = \sqrt{I},$$

which means that for each i there exists e_i such that $X_i^{e_i} \in I$, hence

$$X_i^{e_i} = \sum_{j=1}^{M} g_{ij} f_j$$

for some polynomials g_{ij}. Since f_j are homogenoeus of degree d, the homogeneous part of degree l for $l \neq e_i$ is just the sum of the homogenous parts of degree $l - d$ of the polynomials g_{ij} multiplied by each f_j, hence since the sum of all the terms is 0, we can suppose that g_{ij} are homogeneous of degree $e_i - d$.

Again we take K such that all the coefficients are in K, and for $v \in M_K$ let

$$|G|_v = \max\{|g|_v : \ g \ is \ a \ coefficient \ of \ any \ g_{ij}\},$$

and

$$H_K(G) = \prod_{v \in M_K} |G|_v^{n_v}.$$

We also define

$$H(G) = H_K(G)^{1/[K:\mathbb{Q}]},$$

and using the same argument as in Lemma 3.4.1, if L/K is finite,

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

Proceeding as in Definition 3.4.2, for any two fields L and K containing the coefficients of g_{ij},

$$H_K(G)^{1/[K:\mathbb{Q}]} = H_L(G)^{1/[L:\mathbb{Q}]},$$

thus $H(G)$ is well defined. Now, for each x_i,

$$|x_i|_v^{e_i} \leq \sum_{j=1}^{M} |g_{ij}(P)|_v |f_j(P)|_v \leq M^{\varepsilon(v)} |F(P)|_v \max_j(|g_{ij}(P)|_v).$$

Since g_{ij} is homogeneous of degree $e_i - d$,

$$|g_{ij}(P)|_v \leq \binom{N + e_i - d}{N}^{\varepsilon(v)} |G|_v |P|_v^{e_i - d},$$

and thus joining the last two equations, if $C_3 = M\binom{N+e_i-d}{N}$,

$$|x_i|_v^{e_i} \leq C_3^{\varepsilon(v)} |G|_v |F(P)|_v |P|_v^{e_i - d}.$$

Taking maximun over i,

$$|P|_v^{e_i} \leq C_3^{\varepsilon(v)} |G|_v |F(P)|_v |P|_v^{e_i - d},$$

hence

$$|P|_v^d \leq C_3^{\varepsilon(v)} |G|_v |F(P)|_v.$$

Now, raising to the power n_v, multiplying over all $v \in M_K$ and taking $[K:\mathbb{Q}]$-roots, denoting $C_2 = \frac{1}{C_3 H(G)}$,

$$C_2 H(P)^d \leq H(F(P)),$$

as we wanted to prove. Note that $H(G)$, the g_{ij}, e_i and therefore C_2 only depend on the polynomials f_i for $i = 1, ..., M$, though we don't know how to estimate them. □

Definition 3.4.5. For $x \in \overline{\mathbb{Q}}$,

$$H(x) = H([x, 1]),$$

and if $x \in K$,

$$H_K(x) = H_K([x, 1]).$$

Proposition 3.4.6. *Let* $f(t) = a_0 t^d + a_1 t^{d-1} + ... + a_{d-1} t + a_d$
$= a_0 (t - \alpha_1) \cdots (t - \alpha_d) \in \overline{\mathbb{Q}}[t]$. *Then*

$$2^{-d} \prod_{j=1}^{d} H(\alpha_j) \leq H([a_0, ..., a_d]) \leq 2^{d-1} \prod_{j=1}^{d} H(\alpha_j).$$

Proof. We can replace the polynomial by $(1/a_0) f(t)$ because the right and the left side does not depend on a_0, and the point $[a_0, ..., a_N]$ is the same as $[1, ..., a_N/a_0]$ in the projective space. We take $K = \mathbb{Q}[\alpha_1, ..., \alpha_d]$. Let

$$\varepsilon(v) = 1$$

if v is non-archimedean and

$$\varepsilon(v) = 2$$

if it is archimedean. We will prove

$$\varepsilon(v)^{-d} \prod_{j=1}^{d} \max(|\alpha_j|_v, 1) \leq \max_{0 \leq i \leq d} \{|a_i|_v\} \leq \varepsilon(v)^{d-1} \prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\},$$

and raising to the power n_v, multiplying over all $v \in M_K$ and taking $[K:\mathbb{Q}]$-roots we obtain the desired result (using the same arguments as in the previous proposition). We will do it by induction on d.

First, if $d = 1$, $f(t) = t - \alpha$ with $a_1 = \alpha$ and $a_0 = 1$, so

$$\varepsilon(v)^{-1} \max(|\alpha|_v, 1) \leq \max(|\alpha|_v, 1) = \max(|a_1|_v, |a_0|_v) \leq \max\{|\alpha|_v, 1\}.$$

Assume that the result holds for $d-1$. Let $f(t)$ be as above and k such that

$$|\alpha_k|_v \geq |\alpha|_v.$$

We define

$$\begin{aligned} g(t) =& (t-\alpha_1)\cdots(t-\alpha_{k-1})(t-\alpha_{k+1})\cdots(t-\alpha_d) \\ &= b_0 t^{d-1} + b_1 t^{d-2} + ... + b_{d-1}, \end{aligned}$$

hence

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

Therefore, for all $0 \leq i \leq d$,

$$a_i = b_i - \alpha_k b_{i-1}$$

(this also holds if $i = 0$ and we set $b_{-1} = 0$). Consequently,

$$\begin{aligned} \max_{0\leq i\leq d}\{|a_i|_v\} &= \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \leq \varepsilon(v) \max_{0\leq i\leq d}\{|b_i|_v, \max\{|\alpha_k|_v, 1\}|b_{i-1}|_v\} \\ &\leq \varepsilon(v) \max_{0\leq i\leq d}\{|b_i|_v\} \max\{|\alpha_k|_v, 1\} \leq \varepsilon(v)^{d-1} \prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\}, \end{aligned}$$

where in the last step we have used the induction hypothesis applied to g. To prove the other inequality, suppose $|\alpha_k|_v \leq \varepsilon(v)$. Then

$$\prod_{j=1}^{d} \max\{|\alpha_j|_v, 1\} \leq \varepsilon(v)^d \leq \varepsilon(v)^d \max_{0\leq i\leq d}\{|a_i|_v\},$$

where we have used that $\max_{0\leq i\leq d}\{|a_i|_v\} \geq 1$.

If $|\alpha_k|_v > \varepsilon(v)$,

$$\begin{aligned} \max_{0\leq i\leq d}\{|a_i|_v\} &= \max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} \\ &\geq \varepsilon(v)^{-1} \max_{0\leq i\leq d}\{|b_i|_v\} \max\{|\alpha_k|_v, 1\}. \end{aligned}$$

To see that, suppose v is non-archimedean. Since $|\alpha_k|_v > \varepsilon(v) = 1$, denoting b_j as the number where the maximun is reached, when $i - 1 = j$ we have that $|b_i - \alpha_k b_{i-1}|_v = |\alpha_k|_v |b_j|_v$, and for the rest of i the absolute value of all the differences is bounded by that quantity, so

$$\max_{0\leq i\leq d}\{|b_i - \alpha_k b_{i-1}|_v\} = 1^{-1} \max_{0\leq i\leq d}\{|b_i|_v\} \max\{|\alpha_k|_v, 1\}.$$

Suppose v is archimedean. Then

$$\begin{aligned}\max_{0\le i\le d}\{|b_i-\alpha_k b_{i-1}|_v\} &\ge \max_{0\le i\le d}\{|\alpha_k b_{i-1}|_v-|b_i|_v\}\\ &\ge |\alpha_k|_v|b_j|_v-|b_{j+1}|_v\ge (|\alpha_k|_v-1)\max_{0\le i\le d}\{|b_i|_v\}\\ &\ge \varepsilon(v)^{-1}\max_{0\le i\le d}\{|b_i|_v\}|\alpha_k|_v\end{aligned}$$

because

$$(|\alpha_k|_v-1)\ge\frac{|\alpha_k|_v}{2}$$

as $|\alpha_k|_v>\varepsilon=2$.

Applying induction on g we have that

$$\max_{0\le i\le d}\{|a_i|_v\}\ge\varepsilon(v)^{-1}\max_{0\le i\le d}\{|b_i|_v\}\max\{|\alpha_k|_v,1\}\ge\varepsilon(v)^{-d}\prod_{j=1}^{d}\max\{|\alpha_j|_v,1\}.$$

□

Lemma 3.4.7. *Let K be a number field. For $P\in\mathbb{P}^N(K)$, $P=[x_0,...,x_n]$ and $\sigma\in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$,*

$$H(P)=H(P^\sigma).$$

Proof. We have that $\sigma:K\simeq K^\sigma$, so $[K:\mathbb{Q}]=[K^\sigma:\mathbb{Q}]$. Furthermore, if $v^\sigma\in M_{K^\sigma}$, for all $x\in K$,

$$|\sigma(x)|_{v^\sigma}=|x|_v$$

is a valuation in K and using a similar argument, we have that there is a 1-to-1 correspondence between M_K and M_{K^σ}. Then for each v, we can extend (by density) the isomorphism σ to

$$K_v\simeq K_{v^\sigma}$$

since σ respects valuations. Therefore, $n_v=n_{v^\sigma}$.

$$H_{K^\sigma}(P^\sigma)=\prod_{v\in M_K}|\sigma(x)|_{v^\sigma}^{n_{v^\sigma}}=\prod_{v\in M_K}|x|_v^{n_v},$$

and taking $[K:\mathbb{Q}]-$roots we obtain the result.

□

Now we will prove a theorem that will be one of the keys to prove Mordell-Weil.

Theorem 3.4.8. *Let C,d constants. Then the set*

$$\{P\in\mathbb{P}^N(\overline{\mathbb{Q}}):H(P)\le C\ \ and\ \ [\mathbb{Q}(P):\mathbb{Q}]\le d\}$$

is finite. In particular, for any K number field

$$\{P \in \mathbb{P}^N(K) : H_K(P) \leq C\}$$

and

$$\{P \in \mathbb{P}^N(K) : H(P) \leq C\}$$

are also finite.

Proof. For the last assertion, assume that the first one is true. Then $P \in K$ implies

$$[\mathbb{Q}(P) : \mathbb{Q}] \leq [K : \mathbb{Q}],$$

hence

$$\begin{aligned}&\{P \in \mathbb{P}^N(K) : H_K(P) \leq C\}\\ &\quad \subset \{P \in \mathbb{P}^N(\overline{\mathbb{Q}}) : H(P) \leq C^{1/[K:\mathbb{Q}]} \ \textit{ and } \ [\mathbb{Q}(P) : \mathbb{Q}] \leq [K : \mathbb{Q}]\}.\end{aligned}$$

As this last set is finite, the first one is also finite.

$$\{P \in \mathbb{P}^N(K) : H(P) \leq C\} = \{P \in \mathbb{P}^N(K) : H_K(P) \leq C^{[K:\mathbb{Q}]}\},$$

which is also finite.

Let's prove now the first assertion. Let $P = [x_0, ..., x_N]$ with at least one component equal to 1. Then $\mathbb{Q}(P) = \mathbb{Q}[x_0, ..., x_N]$, and

$$\begin{aligned}H_{\mathbb{Q}(P)}(P) &= \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \leq i \leq N} \{|x_i|_v\}^{n_v} \geq \max_{1 \leq i \leq N} \Big(\prod_{v \in M_{\mathbb{Q}(P)}} \max\{|x_i|_v, 1\}^{n_v} \Big)\\ &= \max_{1 \leq i \leq N} H_{\mathbb{Q}(P)}(x_i),\end{aligned}$$

where we have used that

$$\prod_{v \in M_{\mathbb{Q}(P)}} \max\{|x_i|_v, 1\}^{n_v} \leq \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \leq i \leq N} \{|x_i|_v\}^{n_v}$$

for each i.

We have then that for each i, $H_{\mathbb{Q}(P)}(x_i) \leq C$ and $[\mathbb{Q}(x_i) : \mathbb{Q}] \leq d$, so if we prove the result for $N = 1$ we would have that there would be a finite number of possibilities for x_i, hence there would be a finite number of P in that set.

Let

$$E = \{x \in \overline{\mathbb{Q}} : H(x) \leq C, \ \ \mathbb{Q}(x) \leq d\},$$

and let $f_x(t)$ be the minimal polynomial of degree $e \leq d$ with roots $x, \alpha_1, ..., \alpha_{e-1}$ and coefficients $1, a_1, ..., a_e \in \mathbb{Q}$. Using Proposition 3.4.6 and Lemma 3.4.7

$$H([1, a_1, ..., a_e]) \leq 2^{e-1} H(x) \prod_{j=1}^{e-1} H(\alpha_j) = 2^{e-1} H(x)^e \leq (2C)^d,$$

Therefore, using the observation at the beginning of the section, there is only a finite number of e-tuples $a_1, ..., a_e$ for which that inequality holds. Consequently, there is a finite number of polynomials whose roots are in E, and as polynomials have a finite number of roots, E is finite.

□

3.4.1 Heights on Elliptic Curves

Using the definitions of heights over the proyective space and their properties we are going to define heights on Elliptic Curves.

First, recall that for E an elliptic curve and $f \in \overline{K}(E)$ in the function field, then

$$f : E \to \mathbb{P}^1$$

defined by

$$f(p) = [f(p), 1]$$

if p is not a pole of f, and

$$f(p) = [1, 0]$$

if p is a pole of f is a morphism.

Now, define $h : \mathbb{P}^1 \to \mathbb{R}$ as

$$h(P) = \log(H(P)).$$

Let $f \in \overline{K}(E)$. Define $h_f : E \to \mathbb{R}$ as

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

Proposition 3.4.9. *Let E be an elliptic curve over K a number field and let $C > 0$ be a constant. Then*

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

is a finite set.

From now on, if f is a real function taking values in a certain set E and there exists a constant C such that

$$|f(P)| \leq C$$

for all $P \in E$ then we will say that $f = O(1)$.

Proof.

$$\{P \in E(K) : \quad h_f(P) \leq C\} = \{P \in E(K) : \quad H(f(P)) \leq e^C\},$$

so by Theorem 3.4.8, $f(P)$ is contained in a finite set, and for each Q, by Proposition 2.2.7 there are only a finite number of P such that $f(P) = Q$, hence

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

is finite.

□

Theorem 3.4.10. *Let E be an elliptic curve and consider the function $x \in K(E)$. Then, for all $P, Q \in E(\overline{K})$,*

$$h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1).$$

Proof. Let

$$E : y^2 = x^3 + Ax + B.$$

Then, as $x[-P] = x[P]$, the result is obvious for $\pm Q, \pm P = O$ (and in fact it is an equality). Given P, Q,

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

and if $P \neq \pm Q$ then $x(P+Q) = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$, so

$$\begin{aligned} x_3 + x_4 &= \frac{(y_1+y_2)^2 + (y_2-y_1)^2 - 2(x_1+x_2)(x_2-x_1)^2}{(x_2-x_1)^2} \\ &= 2\frac{x_1^3 + Ax_1 + B + x_2^3 + Ax_2 + B - x_1^3 - x_2^3 + x_1^2x_2 + x_2^2x_1}{(x_2-x_1)^2} \\ &= 2\frac{(x_1+x_2)(x_1x_2+A) + 2B}{(x_2-x_1)^2}, \end{aligned}$$

and

$$\begin{aligned} x_3x_4 &= \frac{2y_1y_2 + (x_1+x_2)(x_1x_2+A) + 2B}{(x_2-x_1)^2} \frac{-2y_1y_2 + (x_1+x_2)(x_1x_2+A) + 2B}{(x_2-x_1)^2} \\ &= \frac{4y_1^2y_2^2 + \Big((x_1+x_2)(x_1x_2+A) + 2B\Big)}{(x_2-x_1)^4} = \frac{(x_1x_2-A)^2 - 4B(x_1+x_2)}{(x_1-x_2)^2}. \end{aligned}$$

In fact this formula is also valid when $P = \pm Q$ because the result is ∞. Define $g : \mathbb{P}^2 \to \mathbb{P}^2$ as

$$g([t,u,v]) = [u^2 - 4tv, 2u(At+v) + 4Bt^2, (v-At)^2 - 4Btu].$$

In order to verify that g is a morphism of degree 2 we have to check that the only common zero of the three entries is $(0,0,0)$. But first, if we define the following functions: $\sigma : E \times E \to \mathbb{P}^1 \times \mathbb{P}^1$ as

$$\sigma(P,Q) = (x(P), x(Q)),$$

$\tau : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ as

$$([\alpha_1, \beta_1], [\alpha_2, \beta_2]) \to [\beta_1\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1, \alpha_1\alpha_2],$$

and $G : E \times E \to E \times E$ as

$$G(P, Q) = (P + Q, P - Q),$$

then the following identity holds:

$$\tau(\sigma(G(P, Q))) = g(\tau(\sigma(P, Q))). \tag{3.4.4}$$

The left side of that equation is

$$\tau([x_3, 1], [x_4, 1]) = [1, x_3 + x_4, x_3 x_4],$$

while the right side is

$$\begin{aligned}&([1, x_1 + x_2, x_1 x_2]) \\ &= [(x_1 + x_2)^2 - 4x_1 x_2, 2(x_1 + x_2)(A + x_1 x_2) + 4B, (x_1 x_2 - A)^2 - 4B(x_1 + x_2)].\end{aligned}$$

Taking into account that $(x_1 + x_2)^2 - 4x_1 x_2 = (x_1 - x_2)^2$ and using the above formulas for $x_3 x_4$ and $x_3 + x_4$, we obtain the desired result.

Next we are going to prove that the only common zero of the entries of g is $(0, 0, 0)$. If $t = 0$,

$$u^2 - 4tv = 0,$$

hence $u = 0$ and $v = 0$. Therefore, we can suppose that $t \neq 0$. Taking a new variable $x = u/2t$, then since $u^2 - 4vt = 0$,

$$x^2 = v/t.$$

Dividing by t^2 the second and the third polynomial we have that

$$\Phi(x) = 4B + 4x(A + x^2) = 4^3 + 4Ax + 4B,$$

and

$$\Psi(x) = (x^2 - A)^2 - 8Bx = x^4 - 2Ax^2 - 8Bx + A^2.$$

Using equation 3.3.1 from the previous section,

$$(16A + 12x^2)\Psi(x) + \Big(5Ax - 3x^3 + 27B\Big)\Phi(x) = 4\Delta,$$

and as $\Delta \neq 0$, this implies that $\Psi(x)$ and $\Phi(x)$ have no common zeros, which finishes the proof.

Denote $\sigma' = \tau\sigma$. Then, taking h on each side of the equation 3.4.4 we have that

$$h(\sigma'(P + Q, P - Q)) = h(g(\sigma'(P, Q)).$$

Applying Proposition 3.4.4,

$$C_1 H(\sigma'(P, Q))^2 \leq H(g(\sigma'(P, Q))) \leq C_2 H(\sigma'(P, Q))^2.$$

Taking logarithms,

$$\log(C_1) + 2h(\sigma'(P,Q)) \leq h(g(\sigma'(P,Q))) \leq \log(C_2) + 2h(\sigma'(P,Q)),$$

and therefore

$$h(g(\sigma'(P,Q)) = 2h(\sigma'(P,Q)) + O(1),$$

so

$$h(\sigma'(P+Q,P-Q)) = 2h(\sigma'(P,Q)) + O(1). \tag{3.4.5}$$

Next we are going to prove that for any $R_1, R_2 \in E(\overline{K})$,

$$h(\sigma'(R_1,R_2)) = h_x(R_1) + h_x(R_2) + O(1), \tag{3.4.6}$$

and if we are able to do it, applying it two times in 3.4.5,

$$\begin{aligned} h_x(P+Q) + h_x(P-Q) + O(1) &= h(\sigma'(P+Q,P-Q)) = 2h(\sigma'(P,Q)) + O(1) \\ &= 2h_x(P) + 2h_x(Q) + O(1), \end{aligned}$$

which is the desired result we want to prove.

Let's now prove 3.4.6. First, suppose $R_1 = O$ (and $R_2 \neq O$). Then,

$$h(\sigma'(O,R_2)) = h(\tau([1,0],[x(R_2),1])) = h([0,1,x(R_2)]) = h([1,x(R_2)]) = h_x(R_2),$$

hence we can suppose that none of them is O. Let

$$x(R_1) = [\alpha_1, 1],$$

$$x(R_2) = [\alpha_2, 1].$$

Then taking into account that $h(\sigma'(R_1,R_2)) = h([1,\alpha_1+\alpha_2,\alpha_1\alpha_2])$, if we consider the polynomial $f(t) = (t+\alpha_1)(t+\alpha_2)$, applying Proposition 3.4.6,

$$(1/4)H(-\alpha_1)H(-\alpha_2) \leq H([1,\alpha_1+\alpha_2,\alpha_1\alpha_2]) \leq 2H(-\alpha_1)H(-\alpha_2).$$

Since $H(-\alpha_i) = H(\alpha_i)$ for $i = 1, 2$, taking logarithms and using that $h(\alpha_i) = h_x(R_i)$ for each i,

$$h_x(R_1) + h_x(R_2) - \log(4) \leq h([1,\alpha_1+\alpha_2,\alpha_1\alpha_2]) \leq \log(2) + h_x(R_1) + h_x(R_2),$$

which completes the proof. □

3.5 Proof of the Mordell-Weil Theorem for number fields

The previous theorem allows us to prove the (sufficient) conditions that a height function should verify to conclude the finiteness of the generators of a group.

Corollary 3.5.1. *Let E be an elliptic curve and h_x the height as above. Then, given $P, Q \in E(\overline{K})$ we have:*

i) For fixed $Q \in E(\overline{K})$ there exists a constant $C_1 > 0$ depending on Q and the curve E such that if $P \in E(\overline{K})$,

$$h_x(P+Q) \leq 2h_x(P) + C_1.$$

ii) For all $m \geq 2$ and all $P \in E(\overline{K})$,

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

In particular this implies that there exists a constant $C_2 > 0$ depending only on E such that

$$h([m]P) \geq m^2 h_x(P) - C_2.$$

Proof. We begin with the first part. Using Theorem 3.4.10,

$$h_x(P+Q) \leq h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1),$$

so there exists C_1' such that $O(1) \leq C_1'$. Let $C_1 = C_1' + 2h_x(Q)$, which only depends on the curve and on Q. We have that

$$h_x(P+Q) \leq h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1) \leq 2h_x(P) + C_1.$$

For the second part we will use induction. First if $m = 0, 1$ the result is obvious. Assume it is true for all numbers less than or equal to m. Using Theorem 3.4.10 for points P', Q', taking $P' = [m]P$, $Q' = P$ we have

$$h_x([m+1]P) + h_x([m-1]P) = 2h_x[m]P) + 2h_x(P) + O(1).$$

Applying the induction hypothesis,

$$h_x([m+1]P) + (m-1)^2 h_x(P) = 2(m^2+1)h_x(P) + O(1),$$

and rearranging the terms,

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

From this equation, the existence of a constant C_2 that only depends on the curve such that

$$h([m]P) \geq m^2 h_x(P) - C_2$$

is obvious. □

The following proposition gathers all this work.

Proposition 3.5.2. *a) If $P_0 \in E(K)$, there exists a constant $C_1 > 0$ depending on P_0 and the elliptic curve E such that for all $P \in E(K)$ we have*

$$h_x(P + P_0) \leq 2h_x(P) + C_1,$$

b) For all integers $m \geq 2$, there exists a constant $C_2 \geq 0$ depending on A, B such that for $P \in E(K)$,

$$h_x([m]P) \geq m^2 h_x(P) - C_2.$$

c) For all constant $C_3 \geq 0$, the set

$$\{P \in E(K) : h_x(P) \leq C_3\}$$

is finite.

Proof. The first two parts are a particular case of Corollary 3.5.1, because we are now restricting to $E(K)$, while there we had the same results for $E(\overline{K})$, which is more general. The third one is a consequence of Proposition 3.4.9 applied to the case $f = x$. □

Theorem 3.5.3 (Mordell-Weil Theorem)**.** *Let K be a number field and E/K an elliptic curve defined over K. Then $E(K)$ is finitely generated.*

Proof. Using this last proposition, Proposition 3.1.1 and the fact that for each integer $m \geq 2$, $E(K)/mE(K)$ is finite, which was the conclusion of Theorem 3.2.1 (Weak Mordell-Weil Theorem), we obtain that the group $E(K)$ is finitely generated. □

The group $E(K)$ can be thought as a $\mathbb{Z}$-module, so it is a module over a principal ring, and thus using Lemma 1.2.6,

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

where $r \in \mathbb{Z}$ and $r \geq 0$. Since $E(K)_{tors}$ is finitely generated and all its elements have finite order, $E(K)_{tors}$ is also finite.

Chapter 4

Torsion and rank of elliptic curves.

4.1 Torsion group of elliptic curves.

In this subsection we are just going to formulate a few well-known results about the torsion group of elliptic curves over number fields.

Theorem 4.1.1. *(Nagell-Lutz) Let $E/\mathbb{Q}$ an elliptic curve with Weiestrass equation*

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

where $A, B \in \mathbb{Z}$. Then, if $P = (x(P), y(P))$ is a torsion point,

$$x(P), y(P) \in \mathbb{Z},$$

and either $2[P] = O$ or

$$y(P)^2 | (4A^3 + 27B^2).$$

Though we are not going to show it, the proof of this theorem is relatively simple. For the second part it suffices to make easy manipulations similar to the ones we did during the Mordell-Weil theorem for the case of $\mathbb{Q}$. The first part, which is a bit difficult, can be done in a more general context (in fields with a discrete non-archimedean valuation), and can be found in [43].

The next theorem shows that there are not many possibilities for the torsion group of an elliptic curve over $\mathbb{Q}$, and that it is indeed quite 'small'.

Theorem 4.1.2. *(Mazur) Let $E/\mathbb{Q}$ an elliptic curve. Then, there are only fifteen possibilities for the subgroup $E(\mathbb{Q})_{tors}$:*

$$\mathbb{Z}/N\mathbb{Z} \quad for \quad 1 \leq N \leq 10 \quad or \quad N = 12,$$

$$\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \quad 1 \leq N \leq 4.$$

The proof of this theorem can be found in [28] and [29].

However, the torsion subgroup of elliptic curves over arbitrary number fields is not so well-known. The following theorem tries to approach to the previous one.

Theorem 4.1.3. *Let $K/\mathbb{Q}$ a number field and p a prime number. Then there exists a positive integer $N = N(K,p)$ for which for all elliptic curves E/K over K, the cardinality of the p-group of $E(K)_{tors}$ is bounded by p^N.*

Notice that in particular Theorem 4.1.2 implies that the cardinality of the torsion subgroup of the elliptic curves over $\mathbb{Q}$ is uniformly bounded. In the same way,

Theorem 4.1.4. *Let $K/\mathbb{Q}$ a number field. Then there is a positive integer $N = N(K)$ such that for all elliptic curves E/K,*

$$|E(K)_{tors}| \leq N.$$

Of course, if we eliminate the restriction that N should depend on K then the previous theorem is false. This is because for any elliptic curve over $\mathbb{Q}$ and any N positive integer the subgroup

$$E[N] = \left\{ P \in \overline{\mathbb{Q}} : [N]P = 0 \right\}$$

has cardinality N^2 and the coordinates of its points are algebraic over $\mathbb{Q}$. Therefore, there exists a number field K such that $E[N] \subset E(K)_{tors}$, and thus there are number fields with torsion subgroup arbitrary large.

To show how Theorem 4.1.4 has been solved, we will introduce some notation.

Notation 4.1.5. *Let $d \geq 1$ an integer. Consider the set $S(d)$ of prime numbers p such that there exists a number field K with $[K:\mathbb{Q}] \leq d$ and an elliptic curve E/K such that $p||E(K)_{tors}|$.*

Let $\Phi(d)$ the set of possible groups $E(K)_{tors}$ up to isomorphism, where K runs over all number fields such that $|K:\mathbb{Q}| \leq d$ and E/K is defined over K.

This first theorem was proven by Faltings and Frey ([13],[16]):

Theorem 4.1.6. *If $S(d)$ is finite, then $\Phi(d)$ is finite.*

The following theorem was proven by Merel ([30]).

Theorem 4.1.7. *For all $d \geq 1$, the set $S(d)$ is finite, hence by Theorem 4.1.6, $\Phi(d)$ is also finite. Moreover, when $d > 1$ and $p \in S(d)$, we have the bound*

$$p \leq d^{3d^2}.$$

This last theorem shows that the number of possible subgroups of $E(K)_{tors}$ with $[K:\mathbb{Q}] \leq d$ is finite, so in particular there exists $N = N(d)$ such that

$$|E(K)_{tors}| \leq N(d),$$

which is in fact stronger than Theorem 4.1.4.

Note that Theorem 4.1.2 implies that $S(1) = \{2, 3, 5, 7\}$ and $|\Phi(1)| = 15$. In a similar way, Kamienny and Mazur ([22]) proved that $S(2) = \{2, 3, 5, 7, 11, 13\}$ and $|\Phi(d)| = 26$, and Parent ([33]) proved that $S(3) = S(2)$. Furthermore, Derickx, Kamienny, Stein and Stoll ([8]) have also proven that

$$S(4) = S(3) \cup \{17\}, \quad S(5) = S(4) \cup \{19\}, \quad \textit{and} \quad S(6) \subset S(5) \cup \{37, 73\}.$$

4.2 The rank of elliptic curves.

In this subsection we are going to define the L-functions of elliptic curves. We are also going to mention and outline the proof of some results and conjectures relating those L-functions with the (algebraic) rank of the elliptic curves.

4.2.1 L-function of an elliptic curve.

Let K be a number field with $[K:\mathbb{Q}] = n$ and M_K^0 the set of non-archimedean absolute values. Let $v \in M_K^0$, k_v its residue field and $q_v = \#k_v$. Define

$$a_v = q_v + 1 - \#E(k_v) = \alpha_v + \overline{\alpha_v}, \tag{4.2.1}$$

where we have applied equation 2.4.2.

Define

$$L_v(T) = 1 - a_v T + q_v T^2$$

when E has good reduction at v and

$$L_v(T) = 1 - T$$

if E has split multiplicative reduction at v,

$$L_v(T) = 1 + T$$

if E has non-split multiplicative reduction at v and

$$L_v(T) = 1$$

if E has additive reduction at v.

Definition 4.2.1. The L-series of E/K is defined by the following infinite product:

$$L_{E/K}(s) = \prod_{v \in M_K^0} L_v(q_v^{-s})^{-1}.$$

In fact,

$$\prod_{v \in M_K^0} L_v(q_v^{-s})^{-1} = \prod_{v(\Delta_E)=0} \frac{1}{1 - a_v q_v^{-s} + q_v^{1-2s}} \prod_{v(\Delta_E)>0} L_v(q_v^{-s})^{-1},$$

and the second product is a finite product, hence for checking the convergence of the product, it suffices to look at the first part.

Lemma 4.2.2. *The expression $L_{E/K}(s)$ defines an analytic function in $Re(s) > 3/2$.*

Proof. It suffices to show that

$$\prod_{v(\Delta_E)=0} \frac{1}{1 - a_v q_v^{-s} + q_v^{1-2s}}$$

defines an analytic function.

Take any compact subset $C \subset T = \{s \in \mathbb{C} : \ Re(s) > 3/2\}$. There exists $\delta > 3/2$ such that for $z \in C$ then $Re(z) \geq \delta$, because the function $Re(z)$ is continous, so it reaches a minimun in C. If we show that there exist constants M_v such that for all $s \in C$,

$$\left\| \frac{1}{1 - a_v q_v^{-s} + q_v^{1-2s}} - 1 \right\| \leq M_v$$

for each v with $v(\Delta_E) = 0$ and

$$\sum_{v(\Delta_E)=0} M_v < \infty,$$

then by the Weiestrass criterium

$$\prod_{v(\Delta_E)=0} \frac{1}{1 - a_v q_v^{-s} + q_v^{1-2s}}$$

will converge uniformly over compact sets of T. Therefore it will converge pointwise on T. Thus, let $C \subset T$ a compact set and $\delta = \delta_C > 3/2$. If $q_v = 2$ then

$$|a_v| = |E(k_v) - 3| \leq 2$$

because as k_v only has two elements, we have the trivial bound

$$1 \leq \#E(k_v) \leq 5.$$

Therefore, by the (inverse) triangular inequality,

$$\begin{aligned}&\left\|1-a_v q_v^{-s}+q_v^{1-2s}\right\| \geq 1-|a_v| q_v^{-Re(s)}-q_v^{1-2Re(s)} \\ &=1-|a_v| 2^{-Re(s)}-2^{1-2Re(s)} \geq 1-2^{1-\delta}-2^{1-2\delta} \geq 1-\frac{1}{\sqrt{2}}-\frac{1}{4}=\frac{3}{4}-\frac{1}{\sqrt{2}}.\end{aligned}$$

If $q_v \geq 3$, using Theorem 2.4.2,

$$\begin{aligned}&\left\|1-a_v q_v^{-s}+q_v^{1-2s}\right\| \geq 1-|a_v| q_v^{-Re(s)}-q_v^{1-2Re(s)} \\ &=1-2\sqrt{q_v} q_v^{-Re(s)}-q_v^{1-2Re(s)}=1-2q_v^{1/2-\delta}-q_v^{1-2\delta} \geq 1-\frac{2}{3}-\frac{1}{9}=\frac{2}{9}.\end{aligned}$$

This estimations ensure that the finite products make sense because the denominator is never 0. Let $C_1=\max(\frac{9}{2}, \frac{1}{\frac{3}{4}-\frac{1}{\sqrt{2}}})$. For $s \in C$,

$$\begin{aligned}\left\|\frac{1}{1-a_v q_v^{-s}+q_v^{1-2s}}-1\right\| &= \left\|\frac{a_v q_v^{-s}-q_v^{1-2s}}{1-a_v q_v^{-s}+q_v^{1-2s}}\right\| \\ &\leq C_1\left\|a_v q_v^{-s}-q_v^{1-2s}\right\| \\ &\leq C_1(2q_v^{1/2-Re(s)}+q_v^{1-2Re(s)}) \\ &\leq C_1(2q_v^{1/2-\delta}+q_v^{1-2\delta}),\end{aligned}$$

so we must prove that if

$$M_v = C_1(2q_v^{1/2-\delta}+q_v^{1-2\delta}),$$

then

$$\sum_{\substack{v \in M_K^0 \\ v(\Delta_E)=0}} M_v < \infty.$$

Notice that $q_v = p^r$ for some prime number p and some positive integer r. Denote β the prime ideal corresponding to v. We have that

$$k_v/\mathbb{F}_p$$

is a field extension, hence

$$\beta \cap \mathbb{Z} = p\mathbb{Z},$$

and therefore $p|\beta$. By Theorem 1.3.15, for each prime number p, the number of ideal primes β of O_K such that $p|\beta$ is bounded by n. Therefore the number of valuations v such that $\#k_v = q_v$ will also be bounded by n.

Since $\delta > 3/2$, we can write it as $\delta = 3/2 + \varepsilon$ where $\varepsilon > 0$, hence

$$\begin{aligned}\sum_{\substack{v \in M_K^0 \\ v(\Delta_E)=0}} M_v &\leq C_1 n \sum_{\substack{q=p^r \\ p \ prime}} (2q^{1/2-\delta} + q^{1-2\delta}) \\ &= C_1 n \sum_{\substack{q=p^r \\ p \ prime}} (2q^{-1-\varepsilon} + q^{-2-2\varepsilon}) \\ &\leq C_1 n \sum_{m} 2m^{-1-\varepsilon} + m^{-2-2\varepsilon} < \infty,\end{aligned}$$

as we wanted to prove. □

Next we are going to define the conductor of an elliptic curve E/K. For all $v \in M_K^0$,

$$f_v = 0$$

if E has good reduction at v,

$$f_v = 1$$

if E has multiplicative reduction at v and

$$f_v = 2 + \delta_v,$$

where $\delta_v \geq 0$ is the dimension of a certain group of homomorphisms. It is a measure of the 'wild ramification' of the action of the inertia subgroup in $T_l(E)$ (for more details, check [32]).

Definition 4.2.3. Define the conductor as the ideal

$$N_{E/K} = \prod_{v \in M_K^0} p_v^{f_v},$$

where p_v is the prime ideal in O_K corresponding to v.

It is well defined because v has bad reduction for a finite number of valuations, so $f_v \neq 0$ for a finite number of places.

Let $K = \mathbb{Q}$. Then $N_E = N_{E/\mathbb{Q}}$ can be thought as a number. Let $E/\mathbb{Q}$ be an elliptic curve and p a prime for which E has split multiplicative reduction at p. Define

$$a_p = 1.$$

If E has non-split multiplicative reduction at p, define

$$a_p = -1,$$

and if E has additive reduction at p, then

$$a_p = 0.$$

With all this notation,

$$p|N_E \iff p|\Delta_E \iff v_p(\Delta) > 0.$$

Therefore, $p|N_E$ if and only if E has bad reduction at p. Besides, when E has good reduction at p then using equation 4.2.1 and the fact that $\alpha_p\overline{\alpha_p} = p$,

$$L_v(p^{-s}) = 1 - a_p p^{-s} + p^{1-2s} = (1 - \frac{\alpha_p}{p^s})(1 - \frac{\overline{\alpha_p}}{p^s}),$$

thus the L-function for E can be written in the following way:

$$L(s, E) = L_{E/\mathbb{Q}}(s) = \prod_{p|N_E} (1 - \frac{a_p}{p^s})^{-1} \prod_{p\nmid N_E} (1 - \frac{\alpha_p}{p^s})^{-1} \prod_{p\nmid N_E} (1 - \frac{\overline{\alpha_p}}{p^s})^{-1}. \qquad (4.2.2)$$

4.2.2 Conjectures and theorems about L-functions and the rank of elliptic curves

The first conjecture we are going to talk about does not involve L-functions, it is just about the rank, and nowadays is still an open problem.

Conjecture 4.2.4. *There exist elliptic curves $E/\mathbb{Q}$ of arbitrary large rank.*

The main evidence for this conjecture is found in the work of Tate and Shafarevich. They proved that the analogous theorem is true for elliptic curves over the field $\mathbb{F}_q(T)$, where q is the power of a prime number.

Theorem 4.2.5. *There exist elliptic curves $E/\mathbb{F}_q(T)$ of arbitrary large rank.*

Conjecture 4.2.6. *For all K number field and all elliptic curves E/K, the function $L_{E/K}(s)$ has an analytic continuation to the entire complex plane, and it satisfies a functional ecuation.*

This conjecture is known to be true for the elliptic curves having complex multiplication (check [9] and [46]). Furthermore, for the case $K = \mathbb{Q}$, if E is modular (we will define this concept in the next section), $L_{E/\mathbb{Q}}$ can be extended to the whole complex plane.

Next, for any elliptic curve $E/\mathbb{Q}$ we define the following function

$$\xi_E(s) = (\frac{\sqrt{N_E}}{2\pi})^s \Gamma(s) L_E(s), \qquad (4.2.3)$$

where Γ is the usual Gamma function of complex analysis. Conjecture 4.2.6 then has another reformulation:

Theorem 4.2.7. *The function $\xi_E(s)$ has an analytic continuation to the whole complex plane, and it satisfies the functional equation*

$$\xi_E(s) = w\xi_E(2-s),$$

where $w = \pm 1$.

We will discuss a bit more about this theorem (which was a conjecture till 2001) later on.

The following conjecture is one of the Millennium Problems and it is still open.

Conjecture 4.2.8 (Birch and Swinnerton-Dyer)**.** *Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ and let $L(s,E)$ be its L-function. Then*

$$rank(E(\mathbb{Q})) = ord_{s=1}L(s,E),$$

where $ord_{s=1}L(s,E)$ denotes the order of the zero of the function $L(s,E)$ at $s=1$.

This conjecture can also be formulated in curves defined over number fields. It is of course based on some numerical and theoretical evidence. For some numerical evidence, check [3]. For the theoretical ones,

Theorem 4.2.9. *(Coates, Wiles). If $E/\mathbb{Q}$ has complex multiplication and $E(\mathbb{Q})$ is infinite (so $r \geq 1$) then*

$$L(1,E) = 0.$$

For the proof, check [7]. Some other works of mathematicians such as Gross, Zagier and Kolyvagin have shown that this conjecture holds for some special cases.

Theorem 4.2.10. *(Gross-Zagier,1986). Let $E/\mathbb{Q}$ be a modular elliptic curve. If $L_E(s)$ has a simple zero at $s=1$ then $E(\mathbb{Q})$ is inifinite.*

Theorem 4.2.11. *(Kolyvagin) Let $E/\mathbb{Q}$ an elliptic curve either modular or with complex multiplication. If $ord_{s=1}L_E(s) \leq 1$, then*

$$rank(E(\mathbb{Q})) = ord_{s=1}L_E(s).$$

The hypothesis of being modular can be eliminated[1] from the two last theorems.

For the rest of the section we are just going to focus on a certain problem involving just the analytic rank, which will be denoted as $r(E)$, so

$$r(E) = ord_{s=1}L(s,E).$$

Thus the following part is much more analytic. Before showing the results, we need some definitions.

[1] See Chapter 5

Recall that making a change of variables, each elliptic curve over $\mathbb{Q}$ has a unique model

$$E_{r,s} : y^2 = x^3 + rx + s,$$

where $r, s \in \mathbb{Z}$ and verify that if there is a prime such that

$$p^4 | r$$

then p^6 does not divide s. We call this condition (1). It is a consequence of the fact that for the change of variables $x = u^2 x'$, $y = u^3 y'$, then $r' = u^{-4} r$ and $s' = u^{-6} s$.

We consider the family of elliptic curves

$$\mathfrak{C}(T) = \Big\{ E_{r,s} : |r| \leq T^{1/3}, |s| \leq T^{1/2}, \quad E_{r,s} \; satisfies \; condition \; (1) \Big\}.$$

Conjecture 4.2.12. *Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. Then the only zeros of the L-function*

$$L(s, E)$$

are found in $Re(s) = 1$. This conjecture is known as the generalized Riemann Hypothesis.

Theorem 4.2.13. *(Brumer) Assuming that all elliptic curves are modular and that their L-function satisfy the generalized Riemann Hypothesis, the average analytic rank is bounded. More precisely,*

$$\frac{1}{|\mathfrak{C}(T)|} \sum_{E \in \mathfrak{C}(T)} r(E) \leq 2.3 + o(1),$$

where $o(1)$ is a certain function that tends to 0 as $T \to \infty$.

The publication of this theorem was in 1992, so at that time the fact that all curves are modular was a conjecture. This conjecture was proven in 2001 (we will talk more about this later on), hence we can eliminate this hypothesis. Therefore, the only hypothesis that we don't know if it is true is the generalized Riemann Hypothesis. Though we are not going to show all the details of the proof, we will give a brief sketch of it. We will do it through some lemmas.

Lemma 4.2.14. *Let F be a holomorphic function in $\Big\{ s \in \mathbb{C} : \; -c_0 \leq Re(s) \leq c_0 \Big\}$ for some $c_0 > 0$ such that*

- $F(s) = F(-s)$.
- *$F(s)$ is real and positive when s is pure-imaginary.*
- $\int_{c-i\infty}^{c+\infty} |F(s)||s|^{\varepsilon} |ds| = O(1)$.

Then, the following identity holds:

$$\frac{1}{\pi i}\int_{-i\infty}^{i\infty}\frac{\xi_E'}{\xi_E}(1+s)F(s)ds = \sum_{\substack{t\in\mathbb{R}\\ L(1+it,E)=0}} F(it). \tag{4.2.4}$$

Proof. Using Theorem 4.2.7,

$$\frac{\xi_E'}{\xi_E}(s) = -\frac{\xi_E'}{\xi_E}(2-s).$$

Let $R>0$. Then, by the Isolated Zeros Theorem, ξ_E can only have a finite number of zeros in $[-iR, iR]$. Therefore, we can take a sequence of R_n such that

$$\lim_{n\to\infty} R_n = \infty$$

and $\xi_E(R_n)\neq 0$. Take any $\varepsilon>0$ and consider the region

$$T_{\varepsilon,n} = \Big\{ s\in\mathbb{C}:\ -\varepsilon < Re(s) < \varepsilon,\ \ -R_n < Im(s) < R_n \Big\}.$$

By the residue theorem

$$\begin{aligned}
\frac{1}{2\pi i}\int_{\partial T_{\varepsilon,n}}\frac{\xi_E'}{\xi_E}(1+s)F(s)ds &= \sum_{\substack{a\in T_{\varepsilon,n}\\ \xi_E(a)=0}} Res\Big(\frac{\xi_E'}{\xi_E}(1+-)F(-),a\Big)\\
&= \sum_{\substack{-R_n\le t\le R_n\\ \xi_E(1+it)=0}} ord_{s=1+it}(\xi_E)F(it)\\
&= \sum_{\substack{-R_n\le t\le R_n\\ L(1+it,E)=0}} F(it),
\end{aligned}$$

where we have used that

$$\xi_E(a)=0 \Longleftrightarrow L(a,E)=0$$

because of the functional equation. In the second step we have applied the generalized Riemann Hypothesis and the fact that if $ord_{s=a}\xi_E(s)=n$ then there exists g_E holomorphic in a disc around a with $g_E(a)\neq 0$ such that

$$\xi_E(z) = (z-a)^n g_E(z),$$

so

$$\frac{\xi_E'}{\xi_E}F(z) = \frac{nF(z)}{z-a} + \frac{g_E'(z)F(z)}{g_E(z)}.$$

In the last step expression we are counting multiplicities.

On the other hand, by the definition of integral,

$$\begin{aligned}\frac{1}{2\pi i}\int_{\partial T_{\varepsilon,n}}\frac{\xi_E'}{\xi_E}(1+s)F(s)ds &= \frac{1}{2\pi i}\int_{-R_n}^{R_n}\frac{\xi_E'}{\xi_E}(1-\varepsilon+it)F(-\varepsilon+it)idt\\ &+\frac{1}{2\pi i}\int_{R_n}^{-R_n}\frac{\xi_E'}{\xi_E}(1+\varepsilon+it)F(\varepsilon+it)idt\\ &+\frac{1}{2\pi i}\int_{-\varepsilon}^{\varepsilon}\frac{\xi_E'}{\xi_E}(1+iR_n+t)F(iR_n+t)dt\\ &+\frac{1}{2\pi i}\int_{\varepsilon}^{-\varepsilon}\frac{\xi_E'}{\xi_E}(1-iR_n+t)F(-iR_n+t)dt.\end{aligned}$$

By the simetries of $\frac{\xi_E'}{\xi_E}(s)$ and $F(s)$,

$$\begin{aligned}\frac{1}{2\pi i}\int_{-R_n}^{R_n}\frac{\xi_E'}{\xi_E}(1-\varepsilon+it)F(-\varepsilon+it)idt &= -\frac{1}{2\pi i}\int_{-R_n}^{R_n}\frac{\xi_E'}{\xi_E}(1+\varepsilon-it)F(\varepsilon-it)idt\\ &= \frac{1}{2\pi i}\int_{R_n}^{-R_n}\frac{\xi_E'}{\xi_E}(1+\varepsilon+it)F(\varepsilon+it)idt,\end{aligned}$$

where in this last step we have made a change of variables. Doing the same with the other two integrals we obtain

$$\begin{aligned}\frac{1}{2\pi i}\int_{\partial T_{\varepsilon,n}}\frac{\xi_E'}{\xi_E}(1+s)F(s)ds &= 2\frac{1}{2\pi i}\int_{R_n}^{-R_n}\frac{\xi_E'}{\xi_E}(1+\varepsilon+it)F(\varepsilon+it)idt\\ &+2\frac{1}{2\pi i}\int_{-\varepsilon}^{\varepsilon}\frac{\xi_E'}{\xi_E}(1+iR_n+t)F(iR_n+t)dt.\end{aligned}$$

Furthermore, in the segment $[-\varepsilon+iR_n.\varepsilon+iR_n]$, ξ_E does not have any zero, so the function $\frac{\xi_E'}{\xi_E}(1+s)F(s)$ is continous. Therefore, for fixed ε_0, it is bounded by M, hence

$$\left\|\frac{1}{2\pi i}\int_{-\varepsilon}^{\varepsilon}\frac{\xi_E'}{\xi_E}(1+iR_n+t)F(iR_n+t)dt\right\| \leq \frac{2M\varepsilon}{2\pi}.$$

As $\varepsilon\to 0$, that integral tends to 0. Putting everything together,

$$\begin{aligned}\lim_{\varepsilon\to 0}\frac{1}{\pi i}\int_{R_n}^{-R_n}\frac{\xi_E'}{\xi_E}(1+\varepsilon+it)F(\varepsilon+it)idt &= \lim_{\varepsilon\to 0}\frac{1}{2\pi i}\int_{\partial T_{\varepsilon,n}}\frac{\xi_E'}{\xi_E}(1+s)F(s)ds\\ &= \sum_{\substack{-R_n\leq t\leq R_n\\ L(1+it,E)=0}}F(it).\end{aligned}$$

Consequently,

$$\begin{aligned}\frac{1}{\pi i}\int_{-R_n}^{R_n}\frac{\xi_E'}{\xi_E}(1+it)F(it)idt &= \frac{1}{\pi i}\int_{R_n}^{-R_n}\frac{\xi_E'}{\xi_E}(1+it)F(it)idt\\ &= \sum_{\substack{-R_n\leq t\leq R_n\\ L(1+it,E)=0}}F(it),\end{aligned}$$

(passing the limit inside the integral is not trivial, something must be done to justify it). Letting n tend to infinity, we obtain the expression 4.2.4.

□

Let $F(t)$ be any continuous function of compact support F. Define the Fourier transform as

$$\widehat{F}(s) = \int_{-\infty}^{\infty} e^{isx} F(x) dx.$$

In fact, since F is continuous and has compact support, $\widehat{F}(s)$ can be seen as an holomorphic function, where s is a complex variable. For $t \in \mathbb{R}$, we have the inversion formula:

$$\widehat{\widehat{F}}(t) = 2\pi F(-t).$$

If F is even, $\widehat{F}(z)$ is also even.

With the previous formula, we are going to prove the following lemma, which approaches a bit more to our theorem.

Lemma 4.2.15. *Let F be an even continuous function of compact support and assume the hypothesis of Theorem 4.2.13. Then,*

$$r(E)\widehat{F}(0) + \sum_{\substack{\tau \neq 0 \\ L_E(1+i\tau)=0}} \widehat{F}(\tau) = F(0)\log N_E + \frac{1}{\pi}\int_{-\infty}^{\infty} \Big(\frac{\Gamma'}{\Gamma}(1+it) - \log 2\pi\Big)\hat{F}(t)dt + 2\sum_{n=1}^{\infty} c_n(E) F(\log n)\log n,$$

where

$$c_n(E) = \frac{-a_p^k}{kp^k} \quad if\ n = p^k \text{ and } p \text{ divides } N_E,$$

$$c_n(E) = \frac{-(\alpha_p^k + \overline{\alpha_p}^k)}{kp^k} \quad if\ n = p^k \text{ and } p \text{ does not divide } N_E,$$

and

$$c_n(E) = 0 \quad if\ n \neq p^k.$$

Proof. Using the equation 4.2.3,

$$\begin{aligned}\frac{\xi_E'(s)}{\xi_E(s)} &= \frac{\log(N_E)}{2} - \log(2\pi) + \frac{\Gamma'(s)}{\Gamma(s)} + \frac{L_E'(s)}{L_E(s)} = \frac{\log(N_E)}{2} - \log(2\pi) + \frac{\Gamma'(s)}{\Gamma(s)} \\ &- \sum_{p|N_E} \frac{a_p \log(p) p^{-s}}{1 - \frac{a_p}{p^s}} - \sum_{p\nmid N_E} \frac{\alpha_p \log(p) p^{-s}}{1 - \frac{\alpha_p}{p^s}} - \sum_{p\nmid N_E} \frac{\overline{\alpha_p} \log(p) p^{-s}}{1 - \frac{\overline{\alpha_p}}{p^s}} \\ &= \frac{\log(N_E)}{2} - \log(2\pi) + \frac{\Gamma'(s)}{\Gamma(s)} - \sum_{p|N_E} \sum_{k=1}^{\infty} \frac{a_p^k \log(p)}{p^{ks}} \\ &- \sum_{p\nmid N_E} \sum_{k=1}^{\infty} \frac{(\alpha_p^k + \overline{\alpha_p}^k) \log(p)}{p^{ks}},\end{aligned}$$

where in the second step we have used expression 4.2.2 and in the third one we have expanded

$$\frac{1}{1 - \frac{a_p}{p^s}}$$

for each p because when $s = 1 + it$, $|\frac{a_p}{p^{1+it}}| < 1$).

Define the function $G(z) = \hat{F}(-iz)$, which is holomorphic and even. Putting function G in equation 4.2.4 instead of F and using the previous expression for $\frac{\xi_E'(s)}{\xi_E(s)}$,

$$\begin{aligned}\frac{1}{\pi i} \int_{-i\infty}^{i\infty} \frac{\xi_E'}{\xi_E}(1+s) G(s) ds &= \frac{1}{\pi i} \int_{-i\infty}^{i\infty} \frac{\log(N_E)}{2} G(s) ds \\ &+ \frac{1}{\pi i} \int_{-i\infty}^{i\infty} (\frac{\Gamma'}{\Gamma}(1+s) - \log(2\pi)) G(s) ds \\ &- \frac{1}{\pi i} \int_{-i\infty}^{i\infty} \Big(\sum_{p|N_E} \sum_{k=1}^{\infty} \frac{a_p^k \log(p)}{p^{k(s+1)}} - \sum_{p\nmid N_E} \sum_{k=1}^{\infty} \frac{(\alpha_p^k + \overline{\alpha_p}^k) \log(p)}{p^{k(s+1)}} \Big) G(s) ds \\ &= \frac{\log(N_E)}{2\pi} \int_{-\infty}^{\infty} \hat{F}(t) dt + \frac{1}{\pi} \int_{-\infty}^{\infty} (\frac{\Gamma'}{\Gamma}(1+it) - \log(2\pi)) \hat{F}(t) dt \\ &- \frac{1}{\pi} \int_{-\infty}^{\infty} \Big(\sum_{p|N_E} \sum_{k=1}^{\infty} \frac{a_p^k \log(p)}{p^{k(it+1)}} - \sum_{p\nmid N_E} \sum_{k=1}^{\infty} \frac{(\alpha_p^k + \overline{\alpha_p}^k) \log(p)}{p^{k(it+1)}} \Big) \hat{F}(t) dt \\ &= \log(N_E) F(0) + \frac{1}{\pi} \int_{-\infty}^{\infty} (\frac{\Gamma'}{\Gamma}(1+it) - \log(2\pi)) \hat{F}(t) dt \\ &- \sum_{p|N_E} \sum_{k=1}^{\infty} \frac{a_p^k \log(p)}{\pi p^k} \int_{-\infty}^{\infty} e^{-it \log(p^k)} \hat{F}(t) dt \\ &- \sum_{p\nmid N_E} \sum_{k=1}^{\infty} \frac{(\alpha_p^k + \overline{\alpha_p}^k) \log(p)}{\pi p^k} \int_{-\infty}^{\infty} e^{-it \log(p^k)} \hat{F}(t) dt,\end{aligned}$$

where we have used the fact that $\hat{\hat{F}}(t) = 2\pi F(-t)$ and we have exchanged sums and integrals in the third step (something should be justified about this step). Therefore,

$$\begin{aligned}
&\frac{1}{\pi i}\int_{-i\infty}^{i\infty}\frac{\xi_E'}{\xi_E}(1+s)G(s)ds = \log(N_E)F(0)\\
&\quad+\frac{1}{\pi}\int_{-\infty}^{\infty}(\frac{\Gamma'}{\Gamma}(1+it)-\log(2\pi))\hat{F}(t)dt\\
&\quad-2\sum_{p|N_E}\sum_{k=1}^{\infty}\frac{a_p^k\log(p)}{p^k}F(\log(p^k))\\
&\quad-2\sum_{p\nmid N_E}\sum_{k=1}^{\infty}\frac{(\alpha_p^k+\overline{\alpha_p}^k)\log(p)}{p^k}F(\log(p^k))\\
&\quad=\log(N_E)F(0)+\frac{1}{\pi}\int_{-\infty}^{\infty}(\frac{\Gamma'}{\Gamma}(1+it)-\log(2\pi))\hat{F}(t)dt\\
&\quad+2\sum_{p|N_E}\sum_{k=1}^{\infty}\frac{-a_p^k\log(p^k)}{kp^k}F(\log(p^k))\\
&\quad+2\sum_{p\nmid N_E}\sum_{k=1}^{\infty}\frac{-(\alpha_p^k+\overline{\alpha_p}^k)\log(p^k)}{kp^k}F(\log(p^k))\\
&\quad=F(0)\log N_E+\frac{1}{\pi}\int_{-\infty}^{\infty}\Big(\frac{\Gamma'}{\Gamma}(1+it)-\log 2\pi\Big)\hat{F}(t)dt\\
&\quad+2\sum_{n=1}^{\infty}c_n(E)F(\log n)\log n,
\end{aligned}$$

and thus using Lemma 4.2.14,

$$\begin{aligned}
r(E)\widehat{F}(0)+\sum_{\substack{t\neq 0\\ L_E(1+it)=0}}\widehat{F}(t) &= \sum_{\substack{t\in\mathbb{R}\\ L_E(1+it)=0}}G(it)\\
&=F(0)\log N_E+\frac{1}{\pi}\int_{-\infty}^{\infty}\Big(\frac{\Gamma'}{\Gamma}(1+it)-\log 2\pi\Big)\hat{F}(t)dt\\
&\quad+2\sum_{n=1}^{\infty}c_n(E)F(\log n)\log n,
\end{aligned}$$

as we wanted to prove. □

Next, suppose that h is an even continuous function with support contained in $[-1,1]$ with piecewise derivative. Define

$$h_X(t) = h(\frac{t}{\log X})$$

where X is a parameter that will be specified later on. Then,

$$\widehat{h}_X(u) = \widehat{h}(u \log X) \log X.$$

Taking $F(t) = h_X(t)$ in the expression of Lemma 4.2.15, we obtain

$$\begin{aligned} r(E)\widehat{h}(0) + \sum_{\substack{t\neq 0 \\ L_E(1+it)=0}} \widehat{h}(t) &= h(0)\frac{\log N_E}{\log X} + \frac{2}{\log X}\sum_{n=1}^{\infty} c_n(E) h(\frac{\log n}{\log X}) \log n \\ &+ \frac{1}{\pi}\int_{-\infty}^{\infty} \Big(\frac{\Gamma'}{\Gamma}(1+it) - \log 2\pi\Big)\widehat{h}(t\log X)dt \\ &= h(0)\frac{\log N_E}{\log X} + \frac{2}{\log X}\sum_{n\leq X}^{\infty} c_n(E) h(\frac{\log n}{\log X}) \log n \\ &+ \frac{1}{\pi}\int_{-\infty}^{\infty} \Big(\frac{\Gamma'}{\Gamma}(1+it) - \log 2\pi\Big)\widehat{h}(t\log X)dt, \end{aligned}$$

where in the last step we have used that the support of h is contained in $[-1, 1]$.

Next, we define the sums

$$U_k(E, X, h) = \sum_{p^k \leq X} c_{p^k}(E) \log p^k h_X(\log p^k),$$

so with this notation,

$$\sum_{n\leq X} c_n(E) \log n h_X(\log n) = \sum_{k\geq 1} U_k(E, X, h).$$

Lemma 4.2.16. *For $0 \leq Re(s) \leq 2$ and $t = Im(s)$ we have the following estimate:*

$$\left\| \frac{\Gamma'}{\Gamma}(s) \right\| = O(\log(|t| + 2).$$

Define

$$\mathfrak{L}(T) = \frac{1}{|\mathfrak{C}(T)|}\sum_{E\in\mathfrak{C}(T)} \log N_E,$$

$$U_1(\mathfrak{C}(T), X, h) = \frac{1}{|\mathfrak{C}(T)|}\sum_{p\leq X} c_p(E) \log p h_x(\log p),$$

and

$$U_2(\mathfrak{C}(T), X, h) = \frac{1}{|\mathfrak{C}(T)|}\sum_{p^2\leq X} c_{p^2}(E) \log p^2 h_x(\log p^2).$$

Lemma 4.2.17. *Suppose $\log(|u| + 2)\widehat{h}(u) \in L^1(\mathbb{R})$ and $\widehat{h} \in L^1(\mathbb{R})$. Then,*

$$\begin{aligned} \frac{1}{|\mathfrak{C}(T)|}\sum_{E\in\mathfrak{C}(T)} \sum_{\substack{t\in\mathbb{R} \\ L_E(1+it)=0}} \widehat{h}(t\log X) &= \frac{h(0)\mathfrak{L}(T)}{\log X} \\ &+ \frac{2}{\log X}\Big(U_1(\mathfrak{C}(T), X, h) + U_2(\mathfrak{C}(T), X, h)\Big) + O\Big(\frac{1}{\log X}\Big). \end{aligned}$$

Proof. First of all,

$$\begin{aligned}\sum_{k\geq 3} U_k(E,X,h) &\leq \sum_{k\geq 3}\sum_{p^k\leq X} \frac{2\sqrt{p}}{p^k}\log p||h||_\infty = 2||h||_\infty \sum_{p^k\leq X}\sum_{k\geq 3}\frac{\log p}{p^{k-\frac{1}{2}}}\\ &\leq 2||h||_\infty \sum_{p^k\leq X}\frac{\log p}{\sqrt{p}}\sum_{k\geq 3}\frac{1}{p^k} = 2||h||_\infty \sum_{p^k\leq X}\frac{\log p}{\sqrt{p}}\frac{1}{p^3}\frac{p}{p-1}\\ &\leq 4||h||_\infty \sum_{p=2}^{\infty}\frac{\log p}{p^{\frac{7}{2}}} = O(1),\end{aligned}$$

so that sum is bounded by a universal constant that only depends on h.

Next, using lemma 4.2.16, if $X > 3$,

$$\begin{aligned}\frac{1}{\pi}\int_{-\infty}^{\infty}\left\|\Big(\frac{\Gamma'}{\Gamma}(1+it)-\log 2\pi\Big)\widehat{h}(t\log X)\right\|dt &\leq \frac{C}{\pi}\int_{-\infty}^{\infty}\log(|t|+2)|\widehat{h}(t\log X)|dt\\ &+\frac{\log 2\pi}{\pi}\int_{-\infty}^{\infty}|\widehat{h}(t\log X)|dt \leq \frac{C}{\pi\log X}\int_{-\infty}^{\infty}\log(\frac{|s|}{\log X}+2)|\widehat{h}(s)|ds\\ &+\frac{\log 2\pi}{\pi\log X}||\widehat{h}||_{L^1} \leq \frac{C}{\pi\log X}\int_{-\infty}^{\infty}\log(|s|+2)|\widehat{h}(s)|ds+\frac{\log 2\pi}{\pi\log X}||\widehat{h}||_{L^1}\\ &=\frac{C'}{\log X},\end{aligned}$$

where

$$C' = \frac{C}{\pi}\int_{-\infty}^{\infty}\log(|s|+2)|\widehat{h}(s)|ds+\frac{\log 2\pi||\widehat{h}||_{L^1}}{\pi}$$

is a constant.

Finally, adding over all the elliptic curves in $\mathfrak{C}(T)$ the expression of Lemma 4.2.15 with $F(t) = h_X(t)$, and taking into account the estimations made before,

$$\begin{aligned}\frac{1}{|\mathfrak{C}(T)|}\sum_{E\in\mathfrak{C}(T)}\sum_{\substack{t\in\mathbb{R}\\ L_E(1+it)=0}}\widehat{h}(t\log X) &= \frac{h(0)\mathfrak{L}(T)}{\log X}\\ &+\frac{2}{\log X}\Big(U_1(\mathfrak{C}(T),X,h)+U_2(\mathfrak{C}(T),X,h)\Big)+O\Big(\frac{1}{\log X}\Big),\end{aligned}$$

where we have used that

$$\sum_{k\geq 3}U_k(E,X,h)$$

and

$$\frac{1}{\pi}\int_{-\infty}^{\infty}\Big(\frac{\Gamma'}{\Gamma}(1+it)-\log 2\pi\Big)\widehat{h}(t\log X)dt$$

are bounded by constants that don't depend on the elliptic curve.

□

We are ready to show the most important lemma of the proof, but first we will formulate another technical lemma whose proof can be found in [5].

Lemma 4.2.18. *We have the following identity:*

$$|\mathfrak{C}(T)| = \frac{4T^{\frac{5}{6}}}{\zeta(10)} + O(T^{\frac{1}{2}}).$$

Lemma 4.2.19. *Assume that the L-functions of elliptic curves satisfy the Riemann Hypothesis. Let h be an even, continous, piecewise C^1 function with compact support on $[-1,1]$. Suppose that $\log(|u|+2)\widehat{h}(u) \in L^1(\mathbb{R})$ and $\widehat{h}(u) \in L^1(\mathbb{R})$. Then, for any $X \leq \frac{T^c}{\log^2 T}$ with $c = \frac{5}{9}$,*

$$\frac{1}{|\mathfrak{C}(T)|} \sum_{E \in \mathfrak{C}(T)} \sum_{\substack{t \in \mathbb{R} \\ L_E(1+it)=0}} \widehat{h}(t \log X) = \frac{h(0)\mathfrak{L}(T)}{\log X} + \frac{\widehat{h}(0)}{2} + O\Big(\frac{1}{\log X}\Big).$$

Proof. We are just going to outline the steps that are followed in [5]. In that article, Brumer proves that

$$|\mathfrak{C}(T)||U_1(\mathfrak{C}(T), X, h)| \ll X^{\frac{27}{20}} T^{\frac{1}{12}} \log^{\frac{1}{10}} T \log^{-\frac{1}{10}} X + X^{\frac{7}{20}} T^{\frac{5}{12}} \log^{\frac{1}{10}} T \log^{\frac{9}{10}} X + T^{\frac{1}{6}} \log X,$$

so if $X \leq \frac{T^c}{\log^2 T}$ and $c = \frac{5}{9}$, recalling Lemma 4.2.18,

$$U_1(\mathfrak{C}(T), X, h) = o(1).$$

In particular

$$U_1(\mathfrak{C}(T), X, h) = O(1).$$

Similarly,

$$U_2(\mathfrak{C}(T), X, h) = \frac{\widehat{h}(0)}{4} \log X + o(1)$$

when $X \leq \frac{T^c}{\log^2 T}$. Using this bounds and Lemma 4.2.17,

$$\frac{1}{|\mathfrak{C}(T)|} \sum_{E \in \mathfrak{C}(T)} \sum_{\substack{t \in \mathbb{R} \\ L_E(1+it)=0}} \widehat{h}(t \log X) = \frac{h(0)\mathfrak{L}(T)}{\log X} + \frac{\widehat{h}(0)}{2} + O\Big(\frac{1}{\log X}\Big),$$

as we wished to prove. □

We are almost ready to prove Theorem 4.2.13, but first we will formulate another technical lemma of Fouvry, whose proof can be found in [14]:

Lemma 4.2.20. *For any $\varepsilon > 0$ the average $\mathfrak{L}(T)$ of $\log N_E$ over $\mathfrak{C}(T)$ verifies the following estimation:*

$$(1-\varepsilon)\log T + o(\log T) \leq \mathfrak{L}(T) \leq \log T + O(1).$$

Proof of Theorem 4.2.13.

Choose $h(t) = g(t)$, where

$$g(t) = \begin{cases} 1-|t| & \text{if } |t| \leq 1 \\ 0 & \text{if } |t| > 1 \end{cases}.$$

A tedious computation shows that

$$\widehat{g}(u) = \begin{cases} 4\frac{\sin^2(u/2)}{u^2} & \text{if } u \neq 0 \\ 0 & \text{if } u = 0 \end{cases}.$$

The function h verifies the conditions of Lemma 4.2.19, so taking $X = \frac{T^c}{\log^2 T}$ with $c = \frac{5}{9}$, we have that $O(\frac{1}{\log X})$ tends to zero as $T \to \infty$. Using Lemma 4.2.20, for all $\varepsilon > 0$,

$$(1-\varepsilon)\frac{\log T}{\frac{5}{9}\log T - 2\log\log T} + o(1) \leq \frac{h(0)\mathfrak{L}(T)}{\log X} \leq \frac{\log T}{\frac{5}{9}\log T - 2\log\log T} + O(\frac{1}{\log T}).$$

When $T \to \infty$,

$$\frac{9}{5}(1-\varepsilon) \leq \liminf_{T\to\infty} \frac{h(0)\mathfrak{L}(T)}{\log X},$$

and

$$\limsup_{T\to\infty} \frac{h(0)\mathfrak{L}(T)}{\log X} \leq \frac{9}{5},$$

which implies that

$$\lim_{T\to\infty} \frac{h(0)\mathfrak{L}(T)}{\log X} = \frac{9}{5},$$

hence

$$\frac{h(0)\mathfrak{L}(T)}{\log X} = \frac{9}{5} + o(1).$$

For the left side of the equation of Lemma 4.2.19, by the positivity of $\widehat{h}$,

$$\begin{aligned} \frac{1}{|\mathfrak{C}(T)|}\sum_{E\in\mathfrak{C}(T)} r(E) &\leq \frac{1}{|\mathfrak{C}(T)|}\sum_{E\in\mathfrak{C}(T)} \sum_{\substack{t\in\mathbb{R} \\ L_E(1+it)=0}} \widehat{h}\Big(t\log\frac{T^c}{\log^2 T}\Big) \\ &= \frac{9}{5} + \frac{1}{2} + o(1) = 2.3 + o(1), \end{aligned}$$

as we wanted to prove. This finishes the proof of Theorem 4.2.13. After this theorem, some improvements have been made. To show them, we have to introduce some notation.

Let

$$E_{r,s} : y^2 = x^3 + rx + s$$

a collection of curves with $r, s \in \mathbb{Z}$ and let

$$\mathcal{C} = \Big\{ E_{r,s} : p^4 | r \to p^6 \nmid s, \Delta_E \neq 0 \Big\}.$$

Let

$$\omega_T(E) = \omega_1(T^{-\frac{1}{3}} r)\omega_2(T^{-\frac{1}{2}} s),$$

where $\omega_1, \omega_2 \in C^\infty$ are non-negative functions with compact support. Define

$$\mathcal{S}(T) = \sum_{E \in \mathcal{C}} \omega_T(E).$$

We have then the following result, whose proof can be found in [21]:

Theorem 4.2.21. *(Heath-Brown, 2003) Assume that the L-functions of the curves $E_{r,s}$ satisfy the Riemann Hypothesis. Then*

$$\frac{1}{\mathcal{S}(T)} \sum_{E \in \mathcal{C}} \omega_T(E) r(E) \leq 2 + o(1),$$

as $T \to \infty$, where $r(E)$ is the analytic rank of E.

The definition of average rank here is slightly different than the definition in the paper of Brumer.

Chapter 5

Modular forms

This section only pretends to be a brief summary of the basic aspects of modular forms that we are going to use, so though there are many important things to say about modular forms and modular curves, we will just focus on the few things that we will need for our purposes.

5.1 Definitions and first examples

Definition 5.1.1. We call *modular group* to the group formed by the invertible matrices 2×2 with coefficients in $\mathbb{Z}$ and such that its determinant is 1:

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

For each matrix, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and each element of the extended complex plane, $\tau \in \widehat{\mathbb{C}}$, we define

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d},$$

where for $c \neq 0$ then $\gamma(-d/c) = \infty$ and $\gamma(\infty) = a/c$, while if $c = 0$ then $\gamma(\infty) = \infty$.

Consider the *upper halfplane*,

$$\mathcal{H} = \left\{ \tau \in \mathbb{C} : Im(\tau) > 0 \right\}.$$

Next we are going to show two technical lemmas that will be used throughout all the section.

Lemma 5.1.2. *For each $\tau \in \mathcal{H}$ and each $\gamma \in SL_2(\mathbb{Z})$ we have that $\gamma(\tau) \in \mathcal{H}$.*

Proof. Given $\tau = x + iy$ with $y > 0$,

$$\begin{aligned}\gamma(\tau) = \frac{a\tau + b}{c\tau + d} &= \frac{ac\,|\tau|^2 + bd + ad\tau + bc\overline{\tau}}{|c\tau + d|^2} \\ &= \frac{ac\,|\tau|^2 + bd + (ad + bc)x + iy(ad - bc)}{|c\tau + d|^2} \\ &= \frac{ac\,|\tau|^2 + bd + (ad + bc)x}{|c\tau + d|^2} + \frac{iy}{|c\tau + d|^2},\end{aligned}$$

where in the last step we have used that $det(\gamma) = 1$, and therefore

$$Im(\gamma(\tau)) = \frac{Im(\tau)}{|c\tau + d|^2} > 0, \tag{5.1.1}$$

which implies that $\gamma(\tau) \in \mathcal{H}$. □

Lemma 5.1.3. *If $\gamma, \gamma' \in SL_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$ then*

$$(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau)).$$

Definition 5.1.4. Let $k \in \mathbb{N}$. A meromorphic function in the upper halfplane, $f : \mathcal{H} \to \mathbb{C}$ is *weakly modular of weight k* if:

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$$

for all matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $\tau \in \mathcal{H}$.

Lemma 5.1.2 implies that $f(\gamma(\tau))$ makes sense because f is a function defined in $\mathcal{H}$. Thus weakly modular functions of weight k satisfiy that

$$f(\tau + 1) = f(\tau), \quad f(-1/\tau) = \tau^k f(\tau).$$

By the periodicity of f, using complex analysis arguments, it is not hard to see that there exists a holomorphic function

$$g : \mathbb{D}\backslash\{0\} \to \mathbb{C}$$

such that for all $\tau \in \mathcal{H}$,

$$g(e^{2\pi i\tau}) = f(\tau).$$

The function g has a Laurent series

$$g(q) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Let $q = e^{2\pi i\tau}$. Then $|q| = e^{-2\pi Im(\tau)}$ and $q \to 0$ when $Im(\tau) \to \infty$. We will say that f is *holomorphic in* ∞ if g can be extended in a holomorphic way in 0. This is equivalent to saying that (by a complex analysis theorem) $|g|$ is bounded in a neighbourhood of zero. It is also equivalent to the fact that $\lim_{Im(\tau)\to\infty} f(\tau)$ does exist, or that in a neighbourhood of ∞, $|f|$ is bounded. Consequently, if g can be extended in a holomorphic way in 0, $g(q) = \sum_{n=0}^{\infty} a_n q^n$ for $q \in \mathbb{D}$ and thus

$$f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i\tau n}.$$

With all this discussion we are now ready to give the following definition of modular form.

Definition 5.1.5. Let $k \in \mathbb{N}$. We say that $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight* k if:

i) f is holomorphic in $\mathcal{H}$;

ii) f is weakly modular of weight k.

iii) f is holomorphic at ∞.

The set of modular forms of weight k is denoted by $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$, and it can be proven that it is a vectorial space. Next, we will introduce a new definition related to the previous ones.

Definition 5.1.6. A *cusp form* of weight k is a modular form of weight k with 0 as the first term of the Fourier expansion. In other words, if

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n$$

with $q = e^{2\pi i\tau}$ then $a_0 = 0$. The set of cusp forms of weight k is denoted by $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Definition 5.1.7. We will call *principal congruent subgroup of level* N to

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Consider the homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ defined taking classes modulo N. Applying the First Isomorphism Theorem we obtain that, as the kernel of that isomorphism is precisely $\Gamma(N)$ (which in turn implies that $\Gamma(N)$ is normal),

$$SL_2(\mathbb{Z})/\Gamma(N) \simeq SL_2(\mathbb{Z}/N\mathbb{Z}). \tag{5.1.2}$$

Definition 5.1.8. We say that the subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a *congruent subgroup* if there exists some $N \in \mathbb{N}$ with $\Gamma(N) \subset \Gamma$.

Some of the most common subgroups are:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\},$$

or

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Obviously both subgroups contain $\Gamma(N)$, and besides this, again considering some natural functions and using the first Isomorphism Theorem, we obtain some interesting relations among these subgroups:

$$\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to b \mod N$$

is obviously surjective and has kernel $\Gamma(N)$.

$$\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to d \mod N$$

is also surjective and has kernel $\Gamma_1(N)$. In this way we obtain that

$$\Gamma_1(N)/\Gamma(N) \simeq \mathbb{Z}/N\mathbb{Z}$$

and

$$\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^*.$$

Definition 5.1.9. For each matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the function

$$j(\gamma, \tau) = c\tau + d$$

is an *automorphic factor*. Define the *operator of weight k* that acts over meromorphic functions in $\mathcal{H}$ as

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \quad \tau \in \mathcal{H}.$$

Finally, we say that f is *weakly modular of weight k with respect to* Γ if f is a meromorphic function in $\mathcal{H}$ and satisfies that

$$f[\gamma]_k = f$$

for all $\gamma \in \Gamma$.

This last definition is a generalization of the weak modularity of weight k (definition 5.1.4). The next lemma lists some of the properties of this operator:

Lemma 5.1.10. *Given $\gamma, \gamma' \in SL_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$,*

i) $j(\gamma\gamma', \tau) = j(\gamma, \gamma'(\tau))j(\gamma', \tau)$,

ii) $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$,

Going back to the congruent subgroup, we take the smaller $h \in \mathbb{N}$ that verifies that $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$. Such h exists because for some $N \in \mathbb{N}$, $\Gamma(N) \subset \Gamma$ so $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N) \subset \Gamma$.

Therefore, we have that given Γ, if f is weakly modular of weight k then f is h-periodic. Using a similar reasoning to the one we used for modular forms of weight k, there exists a function $g : \mathbb{D}\backslash\{0\} \to \mathbb{C}$ which is holomorphic in the disc minus the origin and such that $f(\tau) = g(e^{2\pi i\tau/h})$. We will say that f is holomorphic in ∞ if g can be extended in a holomorphic way in 0, or equivalently, if

$$f(\tau) = \sum_{n=0} a_n e^{2\pi i\tau/h}.$$

The following definition is a generalization of modular forms.

Definition 5.1.11. Let Γ be a congruent subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We will say that a function $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight k with respect to* Γ if

i) f is holomorphic in $\mathcal{H}$.

ii) f is weakly modular of weight k with respect to Γ.

iii) $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

If besides this, $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then f is a *cusp form* of weight k with respect to Γ. The space of modular forms of weight k with respect to Γ, which is again a vectorial space, is denoted by $\mathcal{M}_k(\Gamma)$, and the space of cusp forms, $\mathcal{S}_k(\Gamma)$.

5.2 Hecke operators

In this subsection we will briefly introduce the Hecke operators. In the last subsection we saw that

$$\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*,$$

and so $\Gamma_1(N)$ is normal in $\Gamma_0(N)$.

Thus given $\overline{d} \in (\mathbb{Z}/N\mathbb{Z})^*$, for any representative d of $\overline{d}$, there exists $\alpha \in \Gamma_0(N)$ such that

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and for

$$\alpha' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

with

$$d \equiv d' \mod N,$$

then $\alpha_1 = \alpha'\alpha^{-1} \in \Gamma_1(N)$. Define

$$< d >: M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$

by

$$< d > (f) = f[\alpha]_k,$$

Then

$$f[\alpha']_k = f[\alpha_1\alpha]_k = f[\alpha_1]_k[\alpha]_k = f[\alpha]_k,$$

hence $< d > (f)$ does not depend on the election of α. By normality, given any $\alpha_1' \in \Gamma_1(N)$, there exists $\alpha_1' \in \Gamma_1(N)$ such that

$$\alpha\alpha_1' = \alpha_1''\alpha,$$

and thus

$$f[\alpha]_k[\alpha_1']_k = f[\alpha\alpha_1']_k = f[\alpha_1''\alpha]_k = f[\alpha_1'']_k[\alpha]_k = f[\alpha]_k,$$

so

$$< d > (f) \in M_k(\Gamma_1(N)).$$

Therefore, this *Hecke* operator is well defined. In fact, we have defined it for any number d with the property $(d, N) = 1$. This operator can be extended to all $\mathbb{Z}$.

In a similar way, for $\beta \in GL_2(\mathbb{Q})$ we define the *weight-k* operator on functions $f : \mathcal{H} \to \mathbb{C}$ as

$$(f[\beta]_k)(\tau) = (\det \beta)^{k-1} j(\beta, \tau)^{-k} f(\beta(\tau)),$$

with $\tau \in \mathcal{H}$. This definition is an extension of the definition we had for matrices in $SL_2(\mathbb{Z})$.

Definition 5.2.1. Let Γ_1, Γ_2 be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in GL_2(\mathbb{Q})$. For $f \in \mathcal{M}_k(\Gamma_1)$ we define the **weight-k $\Gamma_1\alpha\Gamma_2$ operator**

$$[\Gamma_1\alpha\Gamma_2] : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$$

as

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k,$$

where $\{\beta_j\}$ are the orbit representatives of $\Gamma_1\alpha\Gamma_2$, so $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$.

Of course there are some things to be checked, for example the fact that $f[\Gamma_1 \alpha \Gamma_2]_k \in \mathcal{M}_k(\Gamma_2)$.

Next, let p a prime number and N a positive integer. We define T_p as

$$T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)),$$

where

$$T_p f = f[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)]_k.$$

In a similar way as before, the definition of T_p can be extended to all integers.

Definition 5.2.2. A nonzero modular form $f \in \mathcal{M}_k(\Gamma_1(N))$ that is an eigenvector for all the Hecke operators T_n and $< n >$ with $n \in \mathbb{Z}^+$ is a **Hecke eigenform**. For

$$f(\tau) = \sum_n a_n q^n,$$

where $q = e^{2\pi i \tau}$, we say that f is normalized if $a_1 = 1$, and we say that f is a **newform** of conductor N when it is a normalized eigenform in $\mathcal{S}_k(\Gamma_1(N))^{new}$.

The vector space $\mathcal{S}_k(\Gamma_1(N))^{new}$ is a subspace of $\mathcal{S}_k(\Gamma_1(N))$ whose definition involves an inner product (Petterson inner product) that we are not going to define.

Note that $\Gamma_1(N) \subset \Gamma_0(N)$, so $\mathcal{S}_k(\Gamma_0(N)) \subset \mathcal{S}_k(\Gamma_1(N))$ and the same with modular forms, hence all the operators we are defining act on $\mathcal{M}_k(\Gamma_0(N))$.

5.3 L-functions and Modularity

Definition 5.3.1. Let N an integer. We define the character $\mathbf{1}_N$ as

$$\mathbf{1}_N(n) = 1 \quad if \quad (N, n) = 1$$

and

$$\mathbf{1}_N(n) = 0 \quad if \quad (N, n) > 1.$$

Proposition 5.3.2. *Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a newform. Then it has an associated L-function that has the following expression*

$$L(s, f) = \sum_{n=1}^{\infty} a_n(f) n^{-s} = \prod_p (1 - a_p(f) p^{-s} + \mathbf{1}_N(p) p^{1-2s})^{-1}.$$

Note that this expression is very similar to the L-functions of the elliptic curves. Now we are ready to define the concept of modularity.

Definition 5.3.3. Let $E/\mathbb{Q}$ an elliptic curve of conductor N_E. We say that E is **modular** if there exists a newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$ such that

$$L(s, f) = L(s, E),$$

where $L(s, E)$ is the L-function of the elliptic curve we defined in the last section.

There are more equivalent definitions. We will mention one of them in the following section.

We saw in the previous section that the condition for an elliptic curve of being modular provides it with some important consequences, such as for example the analytic continuation of its L-function that was mentioned in Conjecture 4.2.6. Thus one of the main important questions that arise naturally is under which hypothesis an elliptic curve is modular. One of the first affirmative answer to this question supposed the key left to prove Fermat's Last Theorem.

Theorem 5.3.4. *(Wiles, 1995) Every semistable elliptic curve over $\mathbb{Q}$ is modular.*

The proof of this theorem can be found in [47]. We will discuss more about it later on. Finally, on 2001, C.Breuil, B.Conrad, F.Diamond and R.Taylor proved modularity for all elliptic curves.

Theorem 5.3.5. *(2001) Let $E/\mathbb{Q}$ be an elliptic curve. Then, E is modular.*

The proof of this theorem can be found in [4]. As we saw in the previous section, Conjectures 4.2.6 and 4.2.7 were true for modular elliptic curves over $\mathbb{Q}$, so the modularity theorem implies that those conjectures are true for all elliptic curves over the rationals.

Corollary 5.3.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Then its L-function and the function ξ_E of Conjecture 4.2.7 in the previous chapter are defined in all the complex plane. Furthermore, the functional equation*

$$\xi_E(s) = w\xi_E(2 - s)$$

holds for all elliptic curves over $\mathbb{Q}$.

Chapter 6

Galois representations

Let E/K be an elliptic curve and p a prime number. Consider the group $G = Gal(\overline{K}/K)$ and the group $E[p]$. We saw in the second chapter that for $\sigma \in G$ then when $Q \in E(\overline{K})$,

$$\sigma([p]Q) = [p]\sigma(Q),$$

hence in particular if $Q \in E[p]$, $\sigma(Q) \in E[p]$. Furthermore,

$$\sigma : E[p] \to E[p]$$

is an homomorphism of groups (because σ is a homomorphism of groups in $E(\overline{K})$), and σ^{-1} is its inverse, so σ is in fact an isomorphism of groups.

Using Corollary 2.2.19 we have that (under the hypothesis that $char(K) = 0$ or $(char(K), p) = 1$) $E[p]$ is a free module of rank 2 over $\mathbb{Z}/p\mathbb{Z}$. In fact, as $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field, $E[p]$ is a 2 dimensional vector space over $\mathbb{F}_p$. Let P, Q be a basis of $E[p]$. Then, since σ is an isomorphism, $\sigma(P), \sigma(Q)$ is another basis of $E[p]$. Therefore,

$$\sigma(P) = a_1 P + a_2 Q,$$

$$\sigma(Q) = b_1 P + b_2 Q,$$

with $a_1, a_2, b_1, b_2 \in \mathbb{F}_p$, and if $P' = (a', b')$ (expressed with coordinates in the basis P, Q) then

$$\sigma(P') = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} a' \\ b' \end{pmatrix}.$$

The matrix $\overline{\rho}_{E,p}(\sigma) = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ is invertible because σ is an isomorphism, and (or) because $\{\sigma(P), \sigma(Q)\}$ is a basis of $E[p]$. Thus we have created an aplication

$$\overline{\rho}_{E,p} : Gal(\overline{K}/K) \to GL_2(\mathbb{F}_p)$$

defined by

$$\overline{\rho}_{E,p}(\sigma) = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}.$$

In fact, this application is a homomorphism. It is also called a representation (mod p).

On the other way, $Gal(\overline{K}/K)$ acts over the Tate module $T_p(E)$, because if $(P_0, P_1, ..., P_n, ...) \in T_p(E)$ then

$$[p]\sigma(P_{n+1}) = \sigma([p]P_{n+1}) = \sigma(P_n),$$

so

$$(\sigma(P_0), \sigma(P_1), ..., \sigma(P_n), ...) \in T_p(E).$$

Therefore, we could define

$$\sigma : T_p(E) \to T_p(E),$$

which will be again an isomorphism. Since $T_p(E)$ is a free module of rank 2 over $\mathbb{Z}_p$, then in a similar way, taking a basis P, Q,

$$\sigma(P) = a_1 P + a_2 Q,$$

$$\sigma(Q) = b_1 P + b_2 P,$$

with $a_1, a_2, b_1, b_2 \in \mathbb{Z}_p$. For $P' = (a', b')$ (expressed with coordinates in the basis P, Q),

$$\sigma(P') = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} a' \\ b' \end{pmatrix}.$$

The matrix $\rho_{E,p}(\sigma) = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ is again invertible because σ is an isomorphism, so we have obtained another aplication

$$\rho_{E,p} : Gal(\overline{K}/K) \to GL_2(\mathbb{Z}_p)$$

defined by

$$\rho_{E,p}(\sigma) = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix},$$

which is in fact an homomorphism.

One of the main problems that arise naturally is to determine the possible images of this application, and over the last decades, the study of these images under certain hypothesis has been a tool to solve open problems in Number Theory.

6.1 Subgroups of $GL_2(\mathbb{F}_p)$.

In what follows we are going to make a classification of the possible subgroups of $GL_2(\mathbb{F}_p)$ in order to have a better idea about what could be the possible image of $\rho_{E,p}$.

Definition 6.1.1. A **Borel subgroup** of $GL_2(\mathbb{F}_p)$ is any subroup which is conjugate to the subgroup of the non-singular upper triangular matrices, that is, any subroup of the form

$$\left\{ P \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} P^{-1}, \quad a, b, c \in \mathbb{F}_p : ac \neq 0 \right\}$$

with P an arbitrary matrix in $GL_2(\mathbb{F}_p)$.

In other words, each Borel subgroup is completely determined by the one-dimensional subspace that each of the elements of the subgroup fixes (the eigenspace).

Definition 6.1.2. A **half Borel subgroup** is any subgroup of the form

$$\left\{ P \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} P^{-1}, \quad a, b \in \mathbb{F}_p : a \neq 0 \right\}$$

with P an arbitrary matrix in $\in GL_2(\mathbb{F}_p)$. It is obviously contained in a Borel subgroup and it has order $p(p-1)$.

Definition 6.1.3. A **quasi-half Borel subgroup** is any subgroup generated by

$$P \begin{pmatrix} x & b \\ 0 & 1 \end{pmatrix} P^{-1},$$

where P is an arbitrary matrix in $\in GL_2(\mathbb{F}_p)$, x generates $\mathbb{F}_p^*$ and $b \in \mathbb{F}_p$.

Other subgroups that appear naturally are the Cartan subgroups. There are in fact two types of them.

Definition 6.1.4. A **split Cartan subgroup** is a conjugate of any non-singular diagonal matrix, so it is of the form

$$\left\{ P \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} P^{-1}, \quad a, b \in \mathbb{F}_p : ab \neq 0 \right\}$$

with P an arbitrary matrix in $\in GL_2(\mathbb{F}_p)$.

Again, each subgroup is completely determined by the two one-dimensional spaces that each of the elements of the subgroup fixes. In fact, each subgroup is isomorphic to $\mathbb{F}_p^* \times \mathbb{F}_p^*$ with the isomorphism given by

$$P \begin{pmatrix} x^e & 0 \\ 0 & x^f \end{pmatrix} P^{-1} \to (x^e, x^f),$$

where x is the generator of the multiplicative group of $\mathbb{F}_p$. Thus, each split Cartan subroup has order $(p-1)^2$. In a similar way as with the Borel subgroup, we have the following subgroup of a Cartan subgroup.

Definition 6.1.5. A **half split Cartan subgroup** is any subgroup which can be expressed as follows:

$$\left\{ P \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} P^{-1}, \quad a \in \mathbb{F}_p : a \neq 0 \right\}$$

or

$$\left\{ P \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} P^{-1}, \quad b \in \mathbb{F}_p : b \neq 0 \right\},$$

with P an arbitrary matrix in $\in GL_2(\mathbb{F}_p)$. All subgroups of this type are isomorphic to $\mathbb{F}_p^*$, so they are cyclic of order $p-1$, and they are thus the subgroups that fix one of the vectors of the basis and fix the other eigenspace (but not necessarily the eigenvector).

Consider $\mathbb{F}_{p^2}$ the field of p^2 elements, which is a quadratic extension of $\mathbb{F}_p$, and $Gal(\mathbb{F}_{p^2}/\mathbb{F}_p) = \{Id, \phi\}$ with $\phi(x) = x^p$. Consider the vector space $V = \mathbb{F}_{p^2}^2$ and for each one-dimensional subspace

$$W =< (a, b) >$$

with $a, b \in \mathbb{F}_{p^2}$, we take the conjugate $W' =< (\phi(a), \phi(b)) >$.

Definition 6.1.6. A **non-split Cartan subgroup** is the subgroup of the matrices which fix any one-dimensional subspace W of $\mathbb{F}_{p^2}^2$ that can't be generated by a vector of $\mathbb{F}_p^2$. Therefore, the elements of the subgroup fix W'. Thus, it is of the form

$$\left\{ P \begin{pmatrix} \lambda & 0 \\ 0 & \phi(\lambda) \end{pmatrix} P^{-1}, \quad \lambda \in \mathbb{F}_{p^2} : \lambda \neq 0 \right\}$$

with

$$P = \begin{pmatrix} a & \phi(a) \\ b & \phi(b) \end{pmatrix},$$

where $a, b \in \mathbb{F}_{p^2}$ and the subspace $< (a, b) >$ in V cannot be generated by a vector of $\mathbb{F}_p^2$. This last condition ensures that P is non-singular because neither a nor b can't then be 0, and if $a\phi(b) = b\phi(a)$ then

$$\phi(ba^{-1}) = ba^{-1},$$

which implies that $ba^{-1} \in \mathbb{F}_p$. Consequently, $k \in \mathbb{F}_p$, $b = ka$, so

$$< (a, b) >=< (a, ak) >=< (1, k) >,$$

which is a contradiction. Furthermore, as $\phi^2 = Id$,

$$
\begin{aligned}
&\phi\Big(P\begin{pmatrix}\lambda & 0\\ 0 & \phi(\lambda)\end{pmatrix}P^{-1}\Big)\\
&=\phi\Big(\begin{pmatrix}a & \phi(a)\\ b & \phi(b)\end{pmatrix}\begin{pmatrix}\lambda & 0\\ 0 & \phi(\lambda)\end{pmatrix}\frac{1}{a\phi(b)-b\phi(a)}\begin{pmatrix}\phi(b) & -\phi(a)\\ -b & a\end{pmatrix}\Big)\\
&=\begin{pmatrix}\phi(a) & a\\ \phi(b) & b\end{pmatrix}\begin{pmatrix}\phi(\lambda) & 0\\ 0 & \lambda\end{pmatrix}\frac{1}{a\phi(b)-b\phi(a)}\begin{pmatrix}-b & a\\ \phi(b) & -\phi(a)\end{pmatrix}\\
&=\frac{1}{a\phi(b)-b\phi(a)}\begin{pmatrix}\phi(a) & a\\ \phi(b) & b\end{pmatrix}\begin{pmatrix}-\phi(\lambda)b & \phi(\lambda)a\\ \lambda\phi(b) & -\lambda\phi(a)\end{pmatrix}\\
&=\frac{1}{a\phi(b)-b\phi(a)}\begin{pmatrix}a & \phi(a)\\ b & \phi(b)\end{pmatrix}\begin{pmatrix}\lambda\phi(b) & -\lambda\phi(a)\\ -b\phi(\lambda) & \phi(\lambda)a\end{pmatrix}\\
&=P\begin{pmatrix}\lambda & 0\\ 0 & \phi(\lambda)\end{pmatrix}P^{-1},
\end{aligned}
$$

which means that $P\begin{pmatrix}\lambda & 0\\ 0 & \phi(\lambda)\end{pmatrix}P^{-1}\in GL_2(\mathbb{F}_p)$

This implies that indeed if we fix a one dimensional subspace of V and define the subgroup of matrices which fix that subspace and its conjugate, then all of them lie in $GL_2(\mathbb{F}_p)$ (instead of just lying in $GL_2(\mathbb{F}_{p^2})$).

Furthermore, each subgroup is isomorphic to $\mathbb{F}_{p^2}^*$ with isomorphism given by

$$P\begin{pmatrix}\lambda & 0\\ 0 & \phi(\lambda)\end{pmatrix}P^{-1}\Longrightarrow\lambda,$$

so each non-split Cartan subgroup is cyclic of order p^2-1.

Besides this, consider the normalizer N_H of each Cartan subgroup H (split and non-split). Let W, W' be the subspaces which are fixed by H and $g\in N_H$, and $U=g(W)$, $U'=g(W')$. Then for any $h\in H$,

$$ghg^{-1}(U)=ghg^{-1}g(W)=gh(W)=g(W)=U,$$

and

$$ghg^{-1}(U')=ghg^{-1}g(W')=gh(W')=g(W')=U'.$$

Thus ghg^{-1} will be in H if and only if it fixes W and W'. Since ghg^{-1} can only fix two subspaces, either $g(W)=U=W$ and $g(W')=U'=W'$ or $g(W')=U'=W$ and $g(W)=U=W'$. The first case would correspond to the case when $g\in H$ and the second one would correspond to a matrix that exchanges both subspaces. Anyway, if $g\in N_H$ and $g\notin H$ then gH are the elements of N_H which does not belong to H, because for each $g'\notin H$, $g^{-1}g'$ fixes W and W'. This implies that for all Cartan subgroups H,

$$[N_H:H]=2.$$

We also define $PGL_2(\mathbb{F}_p)$ as $GL_2(\mathbb{F}_p)/\mathbb{F}_p^*$, which means that we identify the matrices that differ by a constant scalar. Consider the natural homomorphism

$$\varphi : GL_2(\mathbb{F}_p) \to GL_2(\mathbb{F}_p)/\mathbb{F}_p^*,$$

which consists on taking classes. The following theorem will give us a classification of the possible subgroups of $GL_2(\mathbb{F}_p)$. It is due to Dickson [11]. However, this proof is based on the few ideas gaven in [24].

Theorem 6.1.7. *Let G be a subgroup of $GL_2(\mathbb{F}_p)$. Then if the order of G is divisible by p, either G is contained in a Borel subgroup or G contains $SL_2(\mathbb{F}_p)$ (which are the matrices with determinant 1). Suppose the order of G is prime to p. Denoting H as the image of G in $PGL_2(\mathbb{F}_p)$,*

- *i) H is cyclic and G is contained in a Cartan subgroup.*
- *ii) H is dihedral and G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup.*
- *iii) H is isomorphic to either A_4, S_4 or A_5, where S_n is the permutation group and A_n is the alternating group.*

  In ii), $p \neq 2$ and in iii), p cannot be 2 or 3 in the first and second case, and cannot be $2, 3$ or 5 in the third one.

Proof. First of all, suppose p divides the order of G. Choose σ to be an element of order exactly p (we can do that by Sylow theorems). We write σ in its Jordan form, and if the matrix was diagonalizable, taking the base formed by its eigenvectors,

$$\sigma = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},$$

and $a^p = b^p = 1$, but the polynomial $f(x) = x^p - 1 = (x-1)^p$ has just one (multiple) root in $\mathbb{F}_p$, so $a = b = 1$, which contradicts the fact that the order of σ is p. Similarly, if σ is not diagonalizable, then the elements of its diagonal must be 1 by the same reasoning, hence

$$\sigma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

The order of that matrix, provided that $b \neq 0$, is p. Therefore, σ fixes one single one-dimensional subspace W. If all the elements of G fixed that subspace then G would be contained in a Borel subgroup. If not, let σ_1 be an element of G which does not fix W. Then, $\sigma_1\sigma\sigma_1^{-1}$ has order p because conjugation is an isomorphism, so it preserves the order. Let $W' = \sigma_1(W)$. Then W' is different to W by hypothesis, and

$$\sigma_1\sigma\sigma_1^{-1}(W') = \sigma_1\sigma\sigma_1^{-1}\sigma_1(W) = \sigma_1\sigma(W) = \sigma_1(W) = W'.$$

Therefore, taking the basis W, W' and writing both linear applications as matrices over that basis, since $\sigma_1\sigma\sigma_1^{-1}$ preserves W',

$$\sigma_1\sigma\sigma_1^{-1} = \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix}.$$

The matrix $\sigma_1\sigma\sigma_1^{-1}$ has order p, hence by the same reasoning as before, $a' = 1 = d'$. Consequently,

$$\sigma_1\sigma\sigma_1^{-1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}.$$

To conclude this case it suffices to prove that σ and $\sigma_1\sigma\sigma_1^{-1}$ generate $SL_2(\mathbb{F}_p)$. Since both of them lie in G, then we would have that $SL_2(\mathbb{F}_p) \subset G$. In other words, we have to prove that if $T =< \sigma, \sigma_1\sigma\sigma_1^{-1} >$ then $T = SL_2(\mathbb{F}_p)$. Obviously, $T \subset SL_2(\mathbb{F}_p)$ because both elements have determinant 1. First of all,

$$(\sigma_1\sigma\sigma_1^{-1})^n = \begin{pmatrix} 1 & 0 \\ nc & 1 \end{pmatrix}.$$

Since the order of $\sigma_1\sigma\sigma_1^{-1}$ is p, then $c \neq 0$, hence T contains all the lower triangular matrices with ones on their diagonals. In a similar way, it also contains all the upper triangular matrices with ones on their diagonals.

Take any matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p)$, and suppose that $a \neq 0$. The matrix $T_0 = \begin{pmatrix} 1 & 0 \\ -ca^{-1} & 1 \end{pmatrix}$ lies in T, and

$$T_0M = \begin{pmatrix} 1 & 0 \\ -ca^{-1} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix},$$

because this last matrix must have determinant 1. The matrix

$$T_1 = \begin{pmatrix} 0 & a \\ -a^{-1} & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix}$$

belongs to T because it is a product of elements of T. Then,

$$T_1T_0M = \begin{pmatrix} 0 & a \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -a^{-1}b + a^{-1} \end{pmatrix}.$$

Let $c' = -a^{-1}b + a^{-1}$, and take $T_2 = \begin{pmatrix} 1 & c' - 1 \\ 0 & 1 \end{pmatrix} \in T$. We have that

$$T_1T_0MT_2 = \begin{pmatrix} 0 & 1 \\ -1 & c' \end{pmatrix} \begin{pmatrix} 1 & c' - 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix},$$

and this last matrix belongs to T because it is a product of matrices of T:

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Therefore, for $T_3 = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, $T_3 \in T$ and $M = T_0^{-1} T_1^{-1} T_3 T_2^{-1} \in T$, as we wished to prove.

Suppose $a = 0$. Then $M = \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}$ because M must have determinant 1. The matrix $T_4 = \begin{pmatrix} 1 & b(d-1) \\ 0 & 1 \end{pmatrix}$ lies in T, and

$$MT_4 = \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix} \begin{pmatrix} 1 & b(d-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ -b^{-1} & 1 \end{pmatrix}.$$

Therefore, MT_4 lies in T because

$$T_5 = \begin{pmatrix} 0 & b \\ -b^{-1} & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -b^{-1} & 1 \end{pmatrix},$$

which is a product of matrices of T. Consequently, $MT_4 = T_5$, so $M = T_5 T_4^{-1} \in T$, as we wished to prove. Hence we have shown that $T = SL_2(\mathbb{F}_p)$ and therefore $SL_2(\mathbb{F}_p) \subset G$.

Suppose that the order of G is prime to p. Then, the order of H, which is the image of G in $PGL_2(\mathbb{F}_p)$ is also prime to p. Therefore, for $\overline{\sigma} \in H$ with $\sigma \in G$, we write the Jordan form of σ. If it is not diagonalizable then its eigenvalues must be in $\mathbb{F}_p$ because the eigenvalues are conjugate to each other. Hence taking classes we can suppose that both of them are 1, thus the order of $\overline{\sigma}$ would be 1 or p, which is a contradiction. Consequently, σ is diagonalizable. In fact, if two elements σ_1, σ_2 have just one eigenvector in common, they have both of them in common, because if not,

$$\sigma_1 = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

and

$$\sigma_2 = \begin{pmatrix} b & c \\ 0 & e \end{pmatrix},$$

with $a \neq d$ because if not they would have more than just one eigenvector in common, and $a \neq 0$. Compute

$$\sigma_1^{-1} \sigma_2^{-1} \sigma_1 \sigma_2 = \begin{pmatrix} 1 & b^{-1}c(1 - a^{-1}d) \\ 0 & 1 \end{pmatrix}.$$

This last element lies in G and has order p because $1 - a^{-1}d \neq 0$, which is a contradiction.

The set of the eigenvectors of the elements of H is of course a finite set because $\mathbb{F}_{p^2}$ is finite. Let $\xi_1, ..., \xi_v$ be the representatives of the orbits of them under the action of H. For each $i = 1, ..., v$, denote M_i as the set of elements in H that fix ξ_i. Then M_i is clearly a subgroup of H and we have a biyective correspondence between elements of H/M_i and elements in the set $H\xi_i$. Let $\mu_i = |M_i|$. Obviously $\mu_i > 1$ and denoting $h = |H|$,

$$h/\mu_i = |H/M_i| = |H\xi_i|.$$

Furthermore, if we count the pairs formed by a non-trivial element of H and one of its eigenvectors then we will count each element of H twice, so that number would be $2(h-1)$. On the other hand, for each vector in the coset $H\xi_i$, there are exactly $\mu_i - 1$ non-trivial elements that fix it. This is because for $h \in H$, any element of the group hM_ih^{-1} fixes $h\xi_i$ since for $m_i \in M_i$ then

$$hm_ih^{-1}(h\xi_i) = hm_i(\xi_i) = h\xi_i.$$

Suppose g fixes $h\xi_i$. Then

$$h^{-1}gh(\xi_i) = h^{-1}h(\xi_i) = \xi_i,$$

hence $g \in hM_ih^{-1}$ and therefore the subgroup of H which fixes $h\xi_i$ is exactly hM_ih^{-1}. Consequently, it has cardinality μ_i, and therefore there are $\mu_i - 1$ non-trivial elements that fix $h\xi_i$. Hence since every eigenvector is on some class (we have made a partition), then adding the number of (non-trivial) elements of H which have them as an eigenvector will give us $2(h-1)$. Therefore, we have the formula

$$2(h-1) = \sum_{i=1}^{v} \frac{h}{\mu_i}(\mu_i - 1),$$

which can also be written as

$$2(1-h^{-1}) = \sum_{i=1}^{v}(1-\mu_i^{-1}).$$

Of course, $1 < \mu_i \leq h$ because μ_i is the cardinality of a subgroup of H, and in fact $\mu_i | h$. We are going to show now that there are not many possibilities for this equation to occur.

First of all, if $v = 1$ then

$$2(1-h^{-1}) = 1-\mu^{-1},$$

hence

$$1+\mu^{-1} = 2h^{-1}$$

and

$$1+h^{-1} \leq 1+\mu^{-1} = 2h^{-1}.$$

Therefore $h \leq 1$, which implies that $h = 1$ and so G will be a subgroup of the matrices of the form

$$\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{F}_p^* \right\},$$

which is cyclic because it is isomorphic to $\mathbb{F}_p^*$. Consequently, G would also be cyclic and contained in a Cartan subgroup.

If $v = 2$ then

$$2h^{-1} = \mu_1^{-1} + \mu_2^{-1}.$$

By the estimation $1 < \mu_i \leq h$ we have that

$$2h^{-1} = \mu_1^{-1} + \mu_2^{-1} \geq h^{-1} + h^{-1},$$

hence we have an equality and so $\mu_1 = h = \mu_2$.

Suppose $v \geq 4$. Since $\mu_i \geq 2$,

$$2 - 2h^{-1} = \sum_{i=1}^{v} (1 - \mu_i^{-1}) \geq \sum_{i=1}^{v} (1/2) = v/2 \geq 2,$$

that would imply that $h \leq 0$, which is a contradiction.

For the case $v = 3$, then if none of the μ_i was 2,

$$2 - 2h^{-1} = 1 - \mu_1^{-1} + 1 - \mu_2^{-1} + 1 - \mu_3^{-1} \geq 1 - 1/3 + 1 - 1/3 + 1 - 1/3 = 2,$$

which implies that $h \leq 0$, which is again a contradiction. Then, at least one of them must be 2. Suppose two of them are 2. Then

$$2 - 2h^{-1} = 1/2 + 1/2 + 1 - \mu_3^{-1},$$

so

$$2h^{-1} = \mu_3^{-1},$$

which implies that $\mu_3 = h/2$, which can only happen when h is even.

Suppose only one of them is 2. Then another one must be 3. Else,

$$2 - 2h^{-1} = 1/2 + 1 - \mu_2^{-1} + 1 - \mu_3^{-1} \geq 1/2 + 3/4 + 3/4 = 2,$$

which is a contradiction. Therefore, the only cases that remain to check are the cases in which one of them is 2, and another one is 3. If the third one verifies $\mu_3 \geq 6$ then

$$2 - 2h^{-1} = 1/2 + 2/3 + 1 - \mu_3^{-1} \geq 1/2 + 2/3 + 5/6 = 2,$$

which is a contradiction. Thus μ_3 can only be $3, 4$ or 5. For $\mu_3 = 3$, $h = 12$; for $\mu_3 = 4$, $h = 24$; and for $\mu_3 = 5$, $h = 60$ (note that in all of them μ_3 is a divisor of h). Summarizing, we only have the following possibilities:

- i) $v = 2$, and $\mu_1 = \mu_2 = h$.

- ii) $v = 3$, h is even and $\mu_1 = \mu_2 = 2$, $\mu_3 = h/2$.
- iii) $v = 3$, $h = 12$, $\mu_1 = 2$, $\mu_2 = 3$ and $\mu_3 = 3$.
- iv) $v = 3$, $h = 24$, $\mu_1 = 2$, $\mu_2 = 3$ and $\mu_3 = 4$.
- v) $v = 3$, $h = 60$, $\mu_1 = 2$, $\mu_2 = 3$ and $\mu_3 = 5$.

Now, let's examine each case:

- i) For the first one, since all the elements of H fix the two eigenvectors, all the elements of G will also have the same eigenvectors. Therefore, G lies in a Cartan subgroup, and H is cyclic because the image of any Cartan subgroup in $PGL_2(\mathbb{F}_p)$ is
$$\left\{\overline{\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}}, x \in \mathbb{F}_p^*\right\}$$
in the case of the split Cartan subgroup. This is because as the matrices of the form $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ are the identity in $PGL_2(\mathbb{F}_p)$, we can suppose that the first element is 1. In the case of the non-split Cartan subgroup,
$$\left\{\overline{\begin{pmatrix} x & 0 \\ 0 & \phi(x) \end{pmatrix}}, x, y \in \mathbb{F}_{p^2}^*\right\}.$$
Hence in the first case the image of the Cartan subgroup would be isomorphic to $\mathbb{F}_p^*$, which is cyclic. Therefore H would also be cyclic because it would be a subgroup of a cyclic group. In the second case, since the non-split Cartan subgroups are cyclic, their subgroups are also cyclic. The image under a homomorphism of a cyclic subgroup is again cyclic, thus in both cases H would be cyclic.

- ii) In this case, half the elements of H fix the eigenvector ξ_3. Consequently, as we saw previously, these elements form a subgroup H_0 of H, and all of them have the same eigenvectors and fix the same subspaces W and W'. In fact, if $h \notin H_0$ then $h^2 \in H_0$ because H_0 has index 2 in H, hence
$$h(h(W)) = W$$
and
$$h \circ h(h(W)) = h(W),$$
which means that $h \circ h$ fixes W and $h(W)$, so $W' = h(W)$ and $h(W') = W$. As we saw in the previous case, H is cyclic and the inverse image of H_0 in G, that is, $\varphi^{-1}(H_0) \cap G$, is contained in a Cartan subgroup G'. The inverse image in G of the elements in $H - H_0$ lie in the normalizer of the Cartan subgroup because if $h_0 \notin H_0$ with $g = \varphi^{-1}(h_0)$, $g \in G$ and $h \in G$ with $\varphi(h) \in H$ then
$$ghg^{-1}g(W) = gh(W) = g(W)$$

and

$$ghg^{-1}(W) = gh(W') = g(W') = W.$$

Hence ghg^{-1} fixes W and $g(W) = W'$, which implies that $ghg^{-1} \in G'$. Furthermore, $g \notin G'$ because g does not fix W. Therefore, G is contained in the normalizer of a Cartan subgroup but is not contained in the Cartan subgroup, as we wished to prove.

- *iii*) For this case, the orbit of ξ_3 contains $12/3 = 4$ elements $\{v_1, v_2, v_3, v_4\}$. Since each element of H is invertible, it permutes the eigenspaces, so there is a natural group homomorphism

$$\rho : H \to S_4$$

that assigns to each element of H the permutation of the subspaces that it induces. As each non-trivial matrix fixes only two eigenspaces then the kernel of that application is trivial, hence the homomorphism is inyective. Thus it suffices to prove that the image under that homomorphism is precisely A_4.

In order to do that, $\{v_1, v_2, v_3, v_4\}$ can be written as

$$\{\xi, h_1\xi, h_2\xi, h_3\xi\},$$

where $h_1, h_2, h_3 \in H$ and all the eigenspaces are different. The order of the subgroup $A \subset H$ that fixes ξ is 3, so it is a cyclic subgroup generated by an element of order 3,

$$A =< \sigma > .$$

Consider the subgroup

$$h_1 < \sigma > h_1^{-1}.$$

Then it has order 3 and

$$h_1 < \sigma > h_1^{-1}(h_1(\xi)) = h_1 < \sigma > (\xi) = h_1(\xi),$$

so it fixes $h_1\xi$. Furthermore,

$$(h_1 < \sigma > h_1^{-1}) \cap < \sigma >= \{e\}$$

because if that intersection was not trivial, it would have order 3 and therefore both subgroups should be equal, but that cannot happen because σ would fix ξ and $h_1\xi$. The image $\rho(\sigma)$ then would be either the identity (which is not possible as the order of σ is 3) or a transposition, which has order 2. Similarly,

$$(h_1 < \sigma > h_1^{-1}) \bigcap (h_2 < \sigma > h_2^{-1}) = \{e\},$$

$$(h_1 < \sigma > h_1^{-1}) \bigcap (h_3 < \sigma > h_3^{-1}) = \{e\},$$

$$(h_2 < \sigma > h_2^{-1}) \bigcap (h_3 < \sigma > h_3^{-1}) = \{e\},$$

$$< \sigma > \bigcap (h_2 < \sigma > h_2^{-1}) = \{e\}$$

and

$$< \sigma > \bigcap (h_3 < \sigma > h_3^{-1}) = \{e\}$$

because if not each of the elements of the groups would fix two elements, which is impossible as they have order 3. Since each of the four subgroups $h_i < \sigma > h_i^{-1}$ has order 3 and they have trivial intersection, we have that H contains $4 \times 2 = 8$ elements of order 3.

S_4 is formed by the identity, single transpositions, $3-$ cycles, 4-cycles and elements of the form

$$(a\ b)(c\ d),$$

where all the numbers a, b, c, d are different from each other. Thus the only elements of order 3 are the 3-cycles, and in fact there are just $\frac{4\times3\times2}{3} = 8$ 3-cycles, so $\rho(H)$ (which is isomorphic to H) contains all the 3-cycles. Suppose $\rho(H)$ contained any odd permutation σ'. Then if T is the set of 3-cycles,

$$\sigma'(T) \bigcap T = \left\{ \sigma' t : \quad t \in T \right\} \bigcap T = \varnothing$$

because the permutations of $\sigma'(T)$ are odd and the permutations of T are even. Therefore,

$$|\rho(H)| \geq 16,$$

which is a contradiction, hence

$$\rho(H) \subset A_4$$

and as $|\rho(H)| = 12$,

$$\rho(H) = A_4.$$

- *iv*) In this case we have 8 elements in the orbit of ξ_2, thus they can be written as

$$\{\xi, h_1\xi, h_2\xi, ..., h_7\xi\}$$

with $h_1, ..., h_7 \in H$. Again, let $A =< \sigma >$ be the subgroup of order 3 that fixes ξ. Since each element of H is invertible, it permutes the eigenspaces, so there is a natural homomorphism

$$\rho : H \to S_8$$

that assigns to each element of H the permutation of the subspaces that it induces. As each non-trivial matrix fixes only two eigenspaces then the kernel of that application is trivial, hence the homomorphism is inyective. For each h_i with $i = 1, ..., 7$, $h_i \sigma h_i^{-1}$ has order 3. Thus when writting them as a product of disjoint cycles, there can only be disjoint 3-cycles (either one or two of them). Therefore, each element will fix two eigenspaces of the orbit of ξ_2,

hence rearranging the elements we can suppose that $(\xi, h_1\xi)$ are eigenvectors of $<\sigma>$ and $h_1 <\sigma> h_1^{-1}$, $(h_2\xi, h_3\xi)$ are eigenvectors of $h_2 <\sigma> h_2^{-1}$ and $h_3 <\sigma> h_3^{-1}$ and so on. We are using here that if two elements have a common eigenvector then they have two common eigenvectors, and thus the pairs are unique.

Furthermore, suppose ξ and $h_1\xi$ are the eigenspaces which are fixed by σ (and hence by A). Then, given $f \in H$,

$$f = h_i\sigma^j$$

with $i = 0, 1, ..., 7$ and $j = 0, 1, 2$, and

$$h_i <\sigma> h_i^{-1}(f(\xi)) = f\sigma^{-j} <\sigma> \sigma^j f^{-1} f(\xi) = f(\xi),$$

and in the same way

$$h_i <\sigma> h_i^{-1}(f(h_1\xi)) = f(h_1\xi).$$

This means that f sends the pair $(\xi, h_1\xi)$ to another pair of eigenvectors that are fixed by two of the conjugates of $<\sigma>$. In a similar way, f sends the rest of the pairs to other pairs, so as f is invertible, f permutes the eigenspaces. Therefore, there is a natural group homomorphism

$$\rho' : H \to S_4$$

that assigns to each element of H the corresponding permutation of pairs. Suppose there was a non-trivial element g such that $\rho'(g) = e$. Then g would fix each pair, and it would either fix or exchange the eigenspaces of the pair. Therefore g^2 would fix all the eigenspaces, so $g^2 = Id$. However, g cannot fix two eigenspaces because if $g(h_j\xi) = h_j\xi$ and $g(h_{j+1}\xi) = h_{j+1}\xi$, then

$$h_j^{-1} g h_j(\xi) = h_j^{-1}(h_j\xi) = \xi.$$

Consequently, $h_j^{-1} g h_j \in <\sigma>$, but

$$ord(h_j^{-1} g h_j) = 2,$$

which is a contradiction. Hence g exchanges the eigenspaces of each pair.

From now on we are going to consider the elements of H as elements of S_8. In order to be able to write the permutations properly we assign the number $i + 1$ to each $h_i\xi$ for each $i = 0, ..., 7$. For each element i we will denote the other element of its pair as i'. Consider σ, which is an element of order 3, so it is of the form

$$(i\ j\ k)(i'\ j'\ k')$$

because it must be a product of disjoint 3-cycles and because σ sends pairs of eigenspaces to pairs of eigenspaces. Since g corresponds to the permutation

$$(i\ i')(j\ j')(k\ k')(l\ l'),$$

where

$$\{i, l, j, k, i', l', j', k'\} = \{1, 2, 3, 4, 5, 6, 7, 8\},$$

$$\begin{aligned} g\sigma g^{-1} &= \Big((i\ i')(j\ j')(k\ k')(l\ l')\Big)\Big((i\ j\ k)(i'\ j'\ k')\Big)\Big((i\ i')(j\ j')(k\ k')(l\ l')\Big) \\ &= (i\ j\ k)(i'\ j'\ k'), \end{aligned}$$

which means that g and σ conmutes. The order of the element σg must be a divisor of 6 because

$$ord(\sigma) = 3, \quad ord(g) = 2.$$

As they commute,

$$(\sigma g)^6 = \sigma^6 g^6 = e.$$

However, $\sigma g \neq e$ because σ and g have different order, and

$$(\sigma g)^3 = \sigma^3 g^3 = g^3 = g \neq e,$$

and in a similar way,

$$(\sigma g)^2 = \sigma^2 g^2 = \sigma^2 \neq e.$$

Therefore, σg must have order 6 but that cannot be possible because any of the two eigenvectors of σg would be fixed by at least 6 elements. This is impossible since the maximun size of a subgroup that fixes an eigenspace is 4 (recall that $\mu_1 = 2$, $\mu_2 = 3$ and $\mu_3 = 4$).

This proves that the kernel of the application

$$\rho' : H \to S_4$$

is trivial. Since $|H| = 24 = |S_4|$, then ρ' is an isomorphism and

$$H \cong S_4,$$

as we wished to prove.

- *v)* Note that $\mu_1 = 2$, $\mu_2 = 3$ and $\mu_3 = 5$. Therefore, all the elements of H must have order 2, 3 or 5 because all the elements of H are conjugate to an element of the subgroup that fixes either ξ_1, ξ_2 or ξ_3.

  To prove this, let $\sigma' \in H$ and $h\xi_j$ any of the two eigenspaces of it with j either $1, 2$, or 3 and $h \in H$. Then,

$$h^{-1}\sigma' h(\xi_j) = h^{-1}h(\xi_j) = \xi_j,$$

so $h^{-1}\sigma' h \in M_i$, as we wished to prove.

Hence, the order of the elements of H is a divisor of either μ_1, μ_2 or μ_3, which are 2, 3 or 5. For each $p = 2, 3$ or 5, consider any element g of order p. By the above argument, g must be conjugate to an element of M_i for some i, thus it must be conjugate to an element with the same order, and therefore there exists $h \in H$ such that

$$h < g > h^{-1} = M_i.$$

We have proven that all cyclic subgroups of order p are conjugate to the corresponding M_i. As conjugacy is an equivalence relation, all cyclic subgroups of the same order are conjugate. This means that if N is a normal subgroup of H then given a prime p, either N contains all the elements of order p or N does not contain any element of order p.

Using the Sylow theorems, denoting n_5 by the number of 5-Sylow groups,

$$n_5 \equiv 1 \mod 5 \quad and \quad n_5 | 12.$$

Hence n_5 can be 6 or 1. Similarly, the number of 3-Sylow groups n_3 must verify

$$n_3 \equiv 1 \mod 3 \quad and \quad n_3 | 20,$$

so n_3 can be $1, 4$ or 10. The number of 2-Sylow groups n_2 must verify

$$n_2 \equiv 1 \mod 2 \quad and \quad n_2 | 15.$$

The intersection of subgroups of order 3 has order either 1 or 3, hence the intersection of different 3-Sylow subgroups is the neutral element, and the same happens with 5. Suppose H contains a non-trivial normal subgroup. Let's consider the different posibilities:

- $n_3 = 10$ and $n_5 = 1$. Then H would contain 4 elements of order 5, 20 elements of order 3 and 35 elements of order 2. The only possibility for a normal subgroup would be the subgroup of order 5. But that could not happen because if $M_3 =< \sigma >$ is normal, then taking h such that $h\xi_3$ is not an eigenspace of σ (which can be done because $|H|/\mu_3 = 12$),

  $$h\sigma h^{-1}(h\xi_3) = h(\xi_3),$$

  and $h\sigma h^{-1}$ would have the same eigenspaces as σ, which is a contradiction.
- $n_3 = 4$ and $n_5 = 6$. Then H would contain 8 elements of order 3, 24 elements of order 5 and 27 of order 2. Consider the sets

  $$A_2 = \Big\{ a \in H : \ ord(a) = 2 \Big\},$$

  $$A_3 = \Big\{ a \in H : \ ord(a) = 3 \Big\},$$

$$A_5 = \Big\{ a \in H : \ ord(a) = 5 \Big\}.$$

If we add the identity to any of them, that set cannot be a subgroup because the order would not be a divisor of 60 (it would be 9, 25 and 28). The union of two of the sets has more than 30 elements, so in this case there cannot be any non-trivial normal subgroup.

- A similar argument as in the first point shows that $n_3 \neq 1$.
- The situation $n_3 = 4$ and $n_5 = 1$ cannot happen because $n_2 \leq 15$, hence the number of elements of order 2 is bounded by 45, and $45 + 8 + 5 = 58 < 60$.
- $n_3 = 10$ and $n_5 = 6$. Then H would contain 24 elements of order 5, 20 elements of order 3 and 15 of order 2. Again,

$$A_2 = \Big\{ a \in H : \ ord(a) = 2 \Big\},$$

$$A_3 = \Big\{ a \in H : \ ord(a) = 3 \Big\},$$

$$A_5 = \Big\{ a \in H : \ ord(a) = 5 \Big\},$$

and if we add the identity to any of them, that set cannot be a subgroup because the order would not be a divisor of 60. The union of two of the sets has more than 30 elements, so in this case there cannot be any non-trivial normal subgroup.

As we have covered all the hypothesis, there cannot be any non-trivial normal subgroup in H. Therefore, H is simple. The proof ends if we are able to prove that when H is simple and $|H| = 60$ then

$$H \cong A_5.$$

We will prove it through the following lemma.

□

Lemma 6.1.8. *Let H be a simple group (a group with no non-trivial normal subgroups) with $|H| = 60$. Then,*

$$H \cong A_5.$$

Proof. We will prove if following some steps.

- **Step 1**. First of all we will prove that H has a subgroup of order 12. By the Sylows theorems, using the previous notation,

$$n_2 = 3, 5 \ or \ 15,$$

$$n_3 = 4 \text{ or } 10,$$

$$n_5 = 6.$$

We have eliminated the cases when those numbers are one because H cannot have non-trivial normal subgroups.

- Suppose $n_2 = 5$. Then we would have finished because by Sylow theorems if T is a 2-Sylow group,

  $$5 = |H : N_H(T)|$$

  so $|N_H(T)| = 12$.
- Suppose $n_2 = 15$. At least two 2-Sylow subgroups must have non-trivial intersection that will be of order 2 because if not we would have 45 elements of order 2 or 4, and $45+24 > 60$. Let L_1 and L_2 be 2-subgroups such that

  $$L_1 \cap L_2 = \{e, g\}$$

  with $ord(g) = 2$. As all groups of order 4 are commutative, then $C_H(g)$, which are the elements of H that commute with g, will verify that

  $$L_1 \subset C_H(g)$$

  and

  $$L_2 \subset C_H(g).$$

  Since L_1 and L_2 are different, $|C_H(g)| > 4$ and

  $$4||C_H(g)|$$

  because it contains subgroups of order 4. Thus $|C_H(g)|$ can be either 12 or 20 because $C_H(g) \neq H$ as H is simple. If $|C_H(g)| = 20$, then g would have 3 conjugates:

  $$A = \left\{g, f_1 g f_1^{-1}, f_2 g f_2^{-1}\right\},$$

  with $f_1, f_2 \in H$ and $f_1, f_2 \notin C_H(g)$. Furthermore,

  $$C_H(f_1 g f_1^{-1}) = f_1 C_H(g) f_1^{-1}.$$

  Clearly, $f_1 C_H(g) f_1^{-1} \subset C_H(f_1 g f_1^{-1})$ because if $h \in C_H(g)$ then

  $$f_1 h f_1^{-1}(f_1 g f_1^{-1}) f_1 h^{-1} f_1^{-1} = f_1 h g h^{-1} f_1^{-1} = f_1 g f_1^{-1}.$$

  The equality follows from the fact that $|C_H(f_1 g f_1^{-1})|$ is bigger or equal than 20 but cannot be 60 since H is simple. It cannot be 30 because then

  $$|H : C_H(f_1 g f_1^{-1})| = 2,$$

so $C_H(f_1 g f_1^{-1})$ would be normal.
The conjugation of any of those three elements by an element of H induces a permutation of them because conjugation by g is an isomorphism. Therefore, there is a group homomorphism

$$\rho : H \to S_3.$$

The image is non-trivial because $\rho(f_1)$ sends g to $f_1 g f_1^{-1}$. The kernel is also non-trivial because if not we would have an inyection of H into a subgroup of S_3, but that is impossible since $|H| = 60 > |S_3| = 6$. Hence as the kernel is not the identity and is not H, we have

$$\ker(\rho) \triangleleft H.$$

Since $\ker(\rho)$ is always normal and is not trivial, we have a contradiction with the fact that H is simple.
Hence, $|C_H(g)| = 12$.

– Suppose $n_2 = 3$. Then by Sylow theorems, if T is a 2-group, then

$$|H : N_H(T)| = 3.$$

The normalizer of $G = N_H(T)$ contains G itself, so the order of that group must be divisible by 20, must divide 60 and cannot be 60 because H is simple, hence $|N_H(G)| = 20$ and hence

$$G = N_H(G).$$

In a similar way as before, G has three conjugates. Therefore,

$$B = \left\{ G, h_1 G h_1^{-1}, h_2 G h_2^{-1} \right\}$$

with $h_1, h_2 \notin N_H(G) = G$, and

$$N_H(h_1 G h_1^{-1}) = h_1 N_H(G) h_1^{-1}.$$

Clearly, $h_1 N_H(G) h_1^{-1} \subset N_H(h_1 G h_1^{-1})$ because if $h \in N_H(G)$ then

$$h_1 h h_1^{-1} (h_1 G h_1^{-1}) h_1 h^{-1} h_1^{-1} = h_1 h G h^{-1} h_1^{-1} = h_1 G h_1^{-1}.$$

Since $N_H(h_1 G h_1^{-1})$ contains $h_1 G h_1^{-1}$, which is a subgroup of order 20, then the order of $N_H(h_1 G h_1^{-1})$ must be divisible by 20 and a divisor of 60. As H is simple,

$$|N_H(h_1 G h_1^{-1})| = 20,$$

and then the equality follows. We have another group homomorphism

$$H \to S_3$$

that associates each element in H to the permutation of the elements of B induced by conjugation of that element. The image is non-trivial and the kernel is not the identity because of the size of H and S_3, so $\ker(H)$ is a non-trivial normal subgroup of H, which is a contradiction.

Sumarizing, we have proved that the only possibility is either $n_2 = 5$ or $n_2 = 15$, and for both of them there is always a subgroup A of order 12, as we wanted to prove.

- **Step 2**. The subgroup A has exactly 5 conjugates and there is an inyective homomorphism from H to S_5.

  Using a similar argument as before, let $N_H(A)$. Then $A \subset N_H(A)$, so the order of $N_H(A)$ must be divisible by 12 and must divide 60. Since H is simple, the order cannot be 60, hence $A = N_H(A)$ and therefore A has exactly 5 conjugates,

$$\left\{A, g_1 A g_1^{-1}, g_2 A g_2^{-1}, g_3 A g_3^{-1}, g_4 A g_4^{-1}\right\},$$

  where $e, g_1, ..., g_4 \in H$ and they all belong to a different equivalence class under the relation

$$x \sim y \Longleftrightarrow y^{-1}x \in N_H(A).$$

  Again, conjugation by an element of H induces a permutation of the five subgroups from above because

$$x g_i A g_i^{-1} x^{-1} = x g_j A g_j^{-1} x^{-1} \Longleftrightarrow g_i \sim g_j.$$

  Consequently, we have a group homomorphism

$$\rho : H \to S_5.$$

  Using the same argument as before, the image of that application is non-trivial. Therefore, the kernel must be the identity because if not it would be a normal group different from H and from the identity.

- **Step 3**. $\rho(H)$ and A_5 contain the 3-cycles and 5-cycles.

  First note that $[S_5 : \rho(H)] = 2$, so for all $g \in S_5$, $g^2 \in \rho(H)$. Furthermore, $g^2 \in A_5$ because it will be an even permutation. Let

$$\{a, b, c, d, e\} = \{1, 2, 3, 4, 5\}.$$

  Then,

$$(a\ b\ c\ d\ e) = (a\ d\ b\ e\ c)^2,$$

  and if

$$\{a, b, c\} = \{1, 2, 3\},$$

  then

$$(a\ b\ c) = (a\ c\ b)^2.$$

  This implies that all 3-cycles and 5-cycles can be written as the square of an element of S_5, hence all of them lie in A_5 and in $\rho(H)$.

- **Step 4**. $A_5 = \rho(H)$.

  There are exactly $\frac{5\times4\times3}{3} = 20$ 3-cycles and $\frac{5\times4\times3\times2}{5} = 24$ 5-cycles. Therefore,

  $$|\rho(H)\bigcap A_5| \geq 45,$$

  and as $\rho(H)\bigcap A_5$ is a subgroup of A_5, the order of $\rho(H)\bigcap A_5$ must divide $60 = |H|$, so

  $$|\rho(H)\bigcap A_5| = 60.$$

  Consequently,

  $$A_5 = \rho(H).$$

  Since ρ is inyective, this shows that $A_5 \cong H$, as we wished to prove.

□

The following corollary of this theorem will be used in the proof of an important theorem of Serre.

Corollary 6.1.9. *Suppose $p \geq 7$ and let G be a subgroup of $GL_2(\mathbb{F}_p)$ which contains either a half split Cartan subgroup, a split Cartan subgroup, a non-split Cartan subgroup, a half Borel subgroup or a quasi-half Borel subgroup. Then, there are only three possibilities for G:*

- *i) G is the whole space, so*

  $$G = GL_2(\mathbb{F}_p).$$

- *ii) G is contained in a Borel subgroup.*

- *iii) G is contained in the normalizer N_H of a Cartan subgroup H.*

Note that iii) includes the possibility that G is contained in a Cartan subgroup.

Proof. There are two possible cases:

- **Case** 1. The order of G is divisible by p.

  By Theorem 6.1.7, either G is contained in a Borel group, which is one of the possibilities of the corollary, or G contains $SL_2(\mathbb{F}_p)$. For the second case, suppose G contains $SL_2(\mathbb{F}_p)$. Then if we were able to prove that the application

  $$\det : G \to \mathbb{F}_p^*$$

  is surjective, $G = GL_2(\mathbb{F}_p)$ because for any matrix $A \in GL_2(\mathbb{F}_p)$, there exists $B \in G$ such that

  $$\det(A) = \det(B),$$

hence

$$\det(AB^{-1}) = 1.$$

Since $SL_2(\mathbb{F}_p) \subset G$,

$$C = AB^{-1} \in SL_2(\mathbb{F}_p) \subset G,$$

so

$$A = CB \in G.$$

The only thing that remains is to prove that under the hypothesis that one of the subgroups of the corollary is included in G, the application

$$\det : G \to \mathbb{F}_p^*$$

is surjective. But for all the cases it is obvious because the half split Cartan subgroup has the form

$$\left\{ P \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} P^{-1}, \quad a \in \mathbb{F}_p^* \right\}.$$

Since the determinat of each matrix is a and a is arbitrary, det is surjective. The split Cartan subgroup contains half spit Cartan subgroups, thus in particular the determinant application is surjective. A half Borel subgroup is of the form

$$\left\{ P \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} P^{-1}, \quad a, b \in \mathbb{F}_p, \quad a \neq 0 \right\}.$$

Therefore, the determinat of each matrix is again a, which can take any value on $\mathbb{F}_p^*$, hence det is again surjective. For the non-split Cartan subgroup, which is of the form

$$\left\{ P \begin{pmatrix} \lambda & 0 \\ 0 & \phi(\lambda) \end{pmatrix} P^{-1}, \quad \lambda \in \mathbb{F}_{p^2} : \lambda \neq 0 \right\},$$

consider $a \in \mathbb{F}_p^*$ such that there exists $x \in \mathbb{F}_p^*$ with

$$a = x^2.$$

Then, since $x \in \mathbb{F}_p^*$, $\phi(x) = x$, so taking $\lambda = x$,

$$\det \left(P \begin{pmatrix} \lambda & 0 \\ 0 & \phi(\lambda) \end{pmatrix} P^{-1} \right) = x^2 = a.$$

If $a \notin (\mathbb{F}_p^*)^2$, we take $x \in \overline{\mathbb{F}_p}$ such that $x^2 = a$. Then,

$$(x^2)^{p-1} = 1,$$

hence

$$(x^{p-1} - 1)(x^{p-1} + 1) = 0.$$

Since $x \notin \mathbb{F}_p^*$,

$$x^{p-1} = -1,$$

and as $p+1$ is even,

$$x^{p^2-1} = 1,$$

so $x \in \mathbb{F}_p^2$. Furthermore,

$$\phi(x)^2 - a = 0,$$

thus $\phi(x)x = a$, and taking $\lambda = x$,

$$\det\left(P \begin{pmatrix} \lambda & 0 \\ 0 & \phi(\lambda) \end{pmatrix} P^{-1}\right) = \phi(x)x = a.$$

This proves that det can take any value in a non-split subgroup, hence

$$\det : G \to \mathbb{F}_p^*$$

is surjective. For the case of the quasi-half Borel subgroup, det is also surjective since one of the members of the subgroup has determinant x, where $< x >= \mathbb{F}_p^*$.

- **Case** 2. p does not divide the order of G.

  Using Theorem 6.1.7, either G is contained in a Cartan subgroup, which would correspond to *iii*), G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself, which would correspond to *iii*) again, or the image H of G in $PGL_2(\mathbb{F}_p)$ is isomorphic to A_4, S_4 or A_5. Thus, we only have to show that this last situation cannot happen.

  The order of the image C_1 of a half split Cartan subgroup C is $p-1$ because $C \cong \mathbb{F}_p^*$ and there are no elements in C that are related (there is a one in the diagonal). The order of the image of a split Cartan subgroup is precisely $p-1$ because of a similar reasoning. The order of the image of a half Borel subgroup is $p(p-1)$ (because of the one in the diagonal) and it contains subgroups of the form

  $$\left\{P \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} P^{-1}, \quad a \in \mathbb{F}_p^*\right\},$$

  which have order $p-1$ (they are half split Cartan subgroups). The following quotient of abelian groups

  $$\mathbb{F}_{p^2}^*/\mathbb{F}_p^*$$

  has $p+1$ elements and is trivially isomorphic to the image of any non-split Cartan subgroup. In fact, it is cyclic because it is a quotient of cyclic subgroups. The order of the image of a quasi-half Borel subgroup is also $p-1$.

Summarizing, we have that the image H of G in $PGL_2(\mathbb{F}_p)$ contains elements of order either $p+1$ or $p-1$. As $p \geq 7$,

$$p+1 \geq 8, \quad p-1 \geq 6,$$

so H contains elements with order bigger than or equal to 6. Therefore, H cannot be isomorphic to A_4, A_5 or S_5 because the elements of those groups have order less than or equal to 5.

Thus, if p does not divide the order of G, G is contained in the normalizer of a Cartan subgroup, and when p divides the order of G, $G = GL_2(\mathbb{F}_p)$ or G is contained in a Borel subgroup, as we wanted to prove.

□

6.2 Some theorems about Galois representations.

Some of the most important theorems about Galois representations concerning the "size" of the possible image of $Gal(\overline{K}/K)$ are due to Serre. The proofs of most of them are very long and quite difficult to understand, mainly because they require a big background in algebraic number theory and algebraic geometry. In addition, most of the times the author omits a lot of previous steps. However, we are going to sketch the proof of one of them. Before that, we need some definitions and notations.

6.2.1 Semi-simplification representation.

Definition 6.2.1. Let V be a vector space, G a group and

$$\rho : G \to GL(V)$$

a representation. We say that (ρ, V) is an **irreducible representation** if there exists no subspace $W \subset V$ with $W \neq V$, $W \neq 0$, and such that for all $g \in G$,

$$\rho(g)W \subset W.$$

Definition 6.2.2. In the previous situation, we say that $W \subset V$ is ρ-invariant if for all $g \in G$,

$$\rho(g)W \subset W.$$

It is not very difficult to prove that there exists a chain of ρ-invariant subspaces

$$0 = V_q \subset V_{q-1} \subset ... \subset V_1 \subset V_0 = V,$$

such that V_i/V_{i+1} is irreducible (that is, there are no intermediate ρ-invariant subspaces between each of the subspaces of the chain). The action of G in V_i/V_{i+1} via ρ is well defined because V_{i+1} is ρ-invariant. The representation

$$\widetilde{\rho} : G \to GL(\bigoplus_{i=0}^{q-1} V_i/V_{i+1})$$

defined by the action of G on each component via ρ is called the **semi-simplification**.

6.2.2 The idele group

In this subsection we are going to define briefly some basic concepts about ideles that will be mentioned in some proofs.

Let K a number field, O_K the integer ring of K and $E = O_K^*$ the unit group of O_K. Let M_K the set of absolute values of K and M_K^∞ the set of archimedean absolute values, K_v the completion with respect to a non-archimedean value and U_v the unit group of K_v.

We define the **idele group** I as the group whose members are

$$(a_v)_{v \in M_K},$$

where $a_v \in K_v^*$ and $a_v \in U_v$ for all $v \in M_K$ except for a finite number of valuations. The operation in the group is just multiplication component by component. This group is a subset of the product of all K_v^*.

Of course K^* can be embedded in I because for each $a \in K^*$,

$$v(a) = 0$$

except for a finite number of $v \in M_K$. Therefore, $a \in U_v$ for almost all $v \in M_K$, so it can be seen as a subgroup of I.

Definition 6.2.3. In the same situation, $C = I/K^*$ is called the **group** of **idele classes** of K.

Let S be a finite subset of M_K and a collection of positive integers

$$m = (m_v)_{v \in S},$$

where $m_v \geq 1$. Define $U_{v,m}$ as 1 for $v \in M_K^\infty$, the group U_v if $v \in M_K - S$ and the subgroup of U_v formed by elements x for which

$$v(1 - x) \geq m_v$$

if $v \in S$. We also define

$$U_m = \prod_{v \in M_K} U_{v,m},$$

$$E_m = E \cap U_m$$

and

$$C_m = I/K^* U_m.$$

In fact, denoting K^{ab} as the maximal abelian extension of K, there is a surjective canonical homomorphism

$$Gal(K^{ab}/K) \to C_m$$

(see [6]).

6.2.3 Serre's theorem

Theorem 6.2.4. *Let K be a number field and E/K an elliptic curve over K without complex multiplication. Then there exists $N = N(E)$ for which for all prime $p \geq N$,*

$$\overline{\rho}_{E,p} : Gal(\overline{K}/K) \to GL_2(\mathbb{F}_p)$$

is surjective.

Proof. The following reasoning does not pretend to be a proof, it is just a summary of the main steps of it.

- **Step 1**.

  By Proposition 1.4.20, taking $N = N(E)$ big enough we can suppose that p is unramified in K. Let $v \in M_K$ a valuation such that $v|p$. If β is the prime in O_K associated to it, then

  $$pO_K|\beta$$

  and $k = O_K/\beta$ is a finite extension of $\mathbb{F}_p$. In particular it has characteristic p. Let Δ be the discriminant of E. Then there is a finite number of valuations $v \in M_K$ for which

  $$v(\Delta) > 0,$$

  and hence a finite number of prime numbers p for which $v|p$ and

  $$v(\Delta) > 0.$$

  Taking $N = N(E)$ big enough we can suppose that E has good reduction at all $v|p$. Note that the first election of $N = N(E)$ does not depend on the choice of the elliptic curve, it only depends on K. However, this second election of N depends on the discrimintant, and hence it depends on the elliptic curve E. Of course this does not mean that the analogous theorem eliminating the condition that N depends on the curve is false. We will discuss more about this later on.

Choose w a valuation in $\overline{K}$ such that $w|v$, let k the residual field and let K_{nr} the maximal unramified extension of $\overline{K}_\omega/K_v$, K_t the maximal tamely ramified extension, I the inertia subgroup of $Gal(\overline{K}/K) = G$, $I_p = Gal(\overline{K}/K_t)$ and

$$I_t = I/I_p = Gal(K_t/K_{nr}).$$

Let $x \in K_{nr}$ such that $v(x) = 1$, let $d \in \mathbb{N}$ with $(d, p) = 1$, and $K_d = K_{nr}(x^{1/d})$. The extension has ramification index d, so it is tamely ramified and $K_d \subset K_t$. For each $s \in Gal(K_d/K_{nr})$ there is an isomorphism θ_d

$$\theta_d : Gal(K_d/K_{nr}) \to \mu_d,$$

where μ_d are the d-unit roots, such that if $s \in Gal(K_t/K_{nr})$,

$$s(x^{1/d}) = \theta_d(s)x^{1/d}.$$

Thus there is a surjective homomorphism

$$\theta_{p-1} : K_t \to \mu_{p-1} \cong \mathbb{F}_p^*$$

- **Step 2**.

  Returning to the proof, as k has characteristic p, by Corollary 2.2.19 the group

  $$\widetilde{E}[p] = \left\{ \widetilde{P} \in E(\overline{k}) : [p]\widetilde{P} = O \right\}$$

  can either be O or isomorphic to $\mathbb{F}_p$.

  Case 1: The torsion subgroup of the reduced curve is non-trivial, hence

  $$\widetilde{E}[p] \cong \mathbb{F}_p.$$

  Then the surjective application

  $$E[p] \to \widetilde{E}[p]$$

  has (by the First Isomorphism Theorem) one dimensional kernel X_p. The subgroup G_ω of $Gal(\overline{K}, K)$ acts on $\widetilde{E}$, so if $\sigma \in G_\omega$ and $P \in X_p$,

  $$\widetilde{\sigma(P)} = \sigma(\widetilde{P}) = \sigma(\widetilde{O}) = \widetilde{O},$$

  which implies that

  $$\sigma(X_p) \subset X_p.$$

  If we take as a basis of $E[p]$ the pair (e_1, e_2) where $< e_1 >= X_p$ then the image of G_ω is contained in the Borel subgroup

  $$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Since the subgroup $I_p \subset G_\omega$ is a p-group, then its image should be contained in the subgroup

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

It can be proven that for each $s \in I_t$, its image is of the form

$$\begin{pmatrix} \theta_{p-1}^e(s) & * \\ 0 & 1 \end{pmatrix},$$

where e is the ramification index of $v|p$, or in other words,

$$v(p) = e$$

(the proof can be found in [35]). In the first step we supposed that p is unramified in K, so $e = 1$, and therefore we have two possibilities:

a) If I_p acts trivially over $E[p]$ then the image of I has order prime to p, and therefore

$$im(I) = im(I/I_p) = im(I_t).$$

In fact, as $e = 1$ and θ_{p-1} is surjective, we take $\sigma \in I_t$ such that

$$\theta_{p-1}(\sigma) = x$$

with $\mathbb{F}_p^* =< x >$. Let the image of σ be

$$A = \begin{pmatrix} x & b \\ 0 & 1 \end{pmatrix}.$$

Then

$$A^{p-1} = \begin{pmatrix} x^{p-1} & b(\sum_{n=0}^{n=p-2} a^n) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The order of A is $p-1$ because $\mathbb{F}_p^* =< x >$. Besides, we have seen that the image of I, which is the image of I_t, must be contained in the subgroup

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix},$$

which has order $p(p-1)$, and since the order of the image of I_t is prime to p, the image should be a subgroup of order less than or equal to $p-1$. Furthermore, as

$$\begin{pmatrix} x & b \\ 0 & 1 \end{pmatrix} \in im(I),$$

the image of I is the cyclic subgroup generated by

$$\begin{pmatrix} x & b \\ 0 & 1 \end{pmatrix}.$$

b) If I_p does not act trivially, then $im(I)$ is again contained in

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix},$$

but in this case $p||im(I_p)|$, so making the same computation as before, there is some $\sigma \in I_t$ such that $im(\sigma) = A$ and

$$A = \begin{pmatrix} x & b \\ 0 & 1 \end{pmatrix}.$$

By the same reason, $|A| = p-1$, because if not x would not be a generator of $\mathbb{F}_p^*$. This means that $p||im(I)|$ and $p-1||im(I)|$, and since $im(I)$ is contained in the previous half Borel subgroup, which has cardinality $p(p-1)$, then

$$im(I) = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}.$$

Note that in both cases, either $im(I)$ is a quasi-half Borel subgroup or a half Borel subgroup, so either $im(G)$ contains a quasi-half Borel subgroup or a half Borel subgroup.

Case 2. The p-torsion subgroup of the reduced curve is trivial.

This means that the map

$$E[p] \to \widetilde{E}[p]$$

is trivial and all the p-torsion elements are reduced to the origin. Then, if $e = 1$:

i) The action of I_p is trivial, and there exists a $\mathbb{F}_{p^2}$ structure in $E[p]$ such that the action of I_t over $E[p]$ is given by the character θ_{p^2-1}.

ii) Consequently, the image of I_t and therefore the image of I is a cyclic Cartan subgroup of order $p^2 - 1$.

The proof of this second case involves the use of the Neron model and the formal group. It can be found in [35].

Summarizing, we have that in both situations, the image of the inertia subgroup is either a quasi-half Borel subgroup, a half Borel subgroup or a non-split Cartan subgroup. Therefore the image of G contains either a quasi-half Borel subgroup, a half Borel subgroup or a non-split Cartan subgroup.

If the theorem does not hold, there is an infinite set of prime numbers L for which when $l \in L$,

$$\overline{\rho}_{E,l}(G) \neq GL_2(\mathbb{F}_p).$$

On the other hand, $im(G)$ is a subgroup of $GL_2(\mathbb{F}_p)$ that meets the conditions of Corollary 6.1.9, so either

- *i*) $im(G)$ is contained in a Borel or in a Cartan subgroup.

– *ii*) $im(G)$ is contained in the normalizer N_l of a Cartan subgroup C_l, but is not contained in the Cartan subgroup C_l.

- **Step 3**.

  If we are in case *ii*), the quotient N_l/C_l has order 2, hence the homomorphism

  $$\phi_l : G \to N_l \to N_l/C_l$$

  is clearly surjective because $\overline{\rho}_{E,l}(G)$ is not contained in C_l. Therefore,

  $$G/\ker(\phi_l)$$

  has order 2, and thus denoting

  $$K_l = \overline{K}^{\ker(\phi_l)} = \left\{ x \in \overline{K} : \quad \sigma(x) = x \ \forall \sigma \in \ker(\phi_l) \right\}$$

  then

  $$[K_l : K] = 2.$$

  It can be proven that for any number field K the number of unramified quadratic extensions is finite, and it can also be proven that for all primes $l \in L$ satisfying *ii*),

  $$K_l/K$$

  is unramified. Therefore, if K' is the composite of all the unramified quadratic extensions,

  $$[K' : K] < \infty,$$

  and

  $$K_l \subset K'.$$

  We replace K by K', which is a number field. If we are able to prove that

  $$\overline{\rho}_{E,l}(Gal(\overline{K}/K')) = \overline{\rho}_{E,l}(Gal(\overline{K'}/K')) = GL_2(\mathbb{F}_p)$$

  then we will have finished as

  $$Gal(\overline{K}/K') \subset Gal(\overline{K}/K).$$

  But now, $K_l = \overline{K}^{\ker(\phi_l)} \subset K'$, so $Gal(\overline{K}/K')$ fixes K_l and therefore

  $$Gal(\overline{K}/K') \subset Gal(\overline{K}/K_l) = \ker(\phi_l),$$

  which means that

  $$\overline{\rho}_{E,l}(Gal(\overline{K}/K')) \subset C_l.$$

  Hence with this new number field K' there are no primes in the case *ii*). Thus it suffices to show that *i*) cannot occur for an infinite number of primes.

- **Step 4**.

  We have now two possibilities:

  i) Suppose $\overline{\rho}_{E,l}(G)$ is contained in a Cartan subgroup C_l and the basis (e_1, e_2) of $GL_2(\mathbb{F}_p)$ verifies that C_l fixes $< e_1 >$ and $< e_2 >$. One of the possible chain of $\overline{\rho}_{E,l}(G)$-invariant spaces such that the quotients are irreducible is the following one:

  $$0 \subset < e_1 > \subset \mathbb{F}_p^2,$$

  because $\overline{\rho}_{E,l}(G)$ fixes $< e_1 >$, and because $GL_2(\mathbb{F}_p)/ < e_1 >$ and $< e_1 >$ are 1-dimensional spaces, so they are irreducible. In fact,

  $$< e_1 > \oplus \frac{\mathbb{F}_p^2}{< e_1 >} \cong < e_1 > \oplus < e_2 > = \mathbb{F}_p^2,$$

  hence the semi-simplification is exactly the same as the original representation. Anyway, we have that

  $$\overline{\rho}_{E,l}(G) \cong \widetilde{\rho}_{E,l}(G),$$

  which implies that $\widetilde{\rho}_{E,l}(G)$ is an abelian group.

  ii) Suppose $\overline{\rho}_{E,l}(G)$ is contained in a Borel subgroup B_l (for an infinite family of primes L) and the basis (e_1, e_2) of $GL_2(\mathbb{F}_p)$ verifies that B_l fixes $< e_1 >$. Then the only possible chain of $\overline{\rho}_{E,l}(G)$-invariant spaces such that the quotients are irreducible is the following one:

  $$0 \subset < e_1 > \subset \mathbb{F}_p^2,$$

  because again $\overline{\rho}_{E,l}(G)$ fixes $< e_1 >$, and because $GL_2(\mathbb{F}_p)/ < e_1 >$ and $< e_1 >$ are 1-dimensional spaces, so they are irreducible. The aim is to prove that the semi-simplification representation is abelian, i.e $\widetilde{\rho}_{E,l}(G)$ is abelian.

  Choose $g_1, g_2 \in G$ with

  $$\overline{\rho}_{E,l}(g_1) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

  and

  $$\overline{\rho}_{E,l}(g_2) = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}.$$

  Take $x \in < e_1 > \bigoplus \frac{\mathbb{F}_p^2}{< e_1 >}$, so $x = (a_1 e_1, \overline{a_2 e_2})$. Then

  $$\begin{aligned} \widetilde{\rho}_{E,l}(g_1)(x) &= \Big(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a_1 \\ 0 \end{pmatrix}, \overline{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 \\ a_2 \end{pmatrix}} \Big) \\ &= (a a_1 e_1, \overline{a_2 b e_1 + a_2 c e_2}) = (a a_1 e_1, \overline{a_2 c e_2}), \end{aligned}$$

so proceeding in a similar way,

$$\widetilde{\rho}_{E,l}(g_2)(\widetilde{\rho}_{E,l}(g_1)(x)) = \widetilde{\rho}_{E,l}(g_2)(aa_1e_1, \overline{a_2ce_2}) = (a'aa_1e_1, \overline{a_2cc'e_2}),$$

and in the same way,

$$\widetilde{\rho}_{E,l}(g_1)(\widetilde{\rho}_{E,l}(g_2)(x)) = (a'aa_1e_1, \overline{a_2cc'e_2}).$$

Therefore,

$$\widetilde{\rho}_{E,l}(g_1)(\widetilde{\rho}_{E,l}(g_2)(x)) = \widetilde{\rho}_{E,l}(g_2)(\widetilde{\rho}_{E,l}(g_1)(x))$$

for all $x \in \mathbb{F}_p^2$, which implies that $\widetilde{\rho}_{E,l}(G)$ is abelian, as we wished to prove. Till now we have explained quite in detail all the steps of the proof. For the rest of it we will just formulate the propositions involved.

- **Step 5**. Since the family of representations

  $$(\widetilde{\rho}_{E,l})_{l \in L}$$

  is abelian, we can think of the $\widetilde{\rho}_{E,l}$ as representations of the group of idele classes $C = I/K^*$ defined before. Studying the properties of this representations, it can be proven that the system of representations $(\overline{\rho}_{l,E})$ comes from a representation

  $$\rho_0 : S_m \to GL_2(\mathbb{F}_p),$$

  where S_m is a certain algebraic group defined in [36] that depends on m and K. Then using a theorem proved in [36], E has complex multiplication, which is a contradiction.

□

We have "proven" that given an elliptic curve E and a number field K, there is a number $N = N(E, K)$ that depends on E and K such that for all primes bigger than N, the representation is surjective. Some of the questions that arises naturally are the following ones:

a) Can we determine explicitly the smallest N, or at least any N for which that property holds given an elliptic curve and a number field?

b) If we fix K, does there exist a universal constant N that does not depend on the elliptic curve E?

c) Can N be a universal constant that does not depend on E and K?

The first question is known to be true. The second still remain open, but the third one is false. However, the second one has been partially answered.

Theorem 6.2.5. *Let $E/\mathbb{Q}$ an elliptic curve over the rational numbers without complex multiplication. Then there exist a number N which does not depend on E such that for all primes $p > N$,*

$$\overline{\rho}_{E,p} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_p)$$

is surjective.

This theorem proves question b) for the particular case of $K = \mathbb{Q}$. Let $G = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Doing something similar as we did in Theorem 6.2.4, it can be proven that either

- i) $\overline{\rho}_{E,p}(G) = GL_2(\mathbb{F}_p)$.
- ii) $\overline{\rho}_{E,p}(G)$ is contained in a Borel subgroup.
- iii) $\overline{\rho}_{E,p}$ is contained in the normalizer of a split Cartan subgroup.
- iv) $\overline{\rho}_{E,p}(G)$ is contained in the normalizer of a non-split Cartan subgroup.
- v) $\overline{\rho}_{E,p}(G)$ is contained in one of the 'exceptional' subgroups.

The exceptional subgroups are a collection of subgroups that we won't define here. However, Serre shows in [38] that these cases cannot occur for a large prime p. Case ii) is a consequence of the following theorem.

Theorem 6.2.6. *(Mazur) Let $E/\mathbb{Q}$ an elliptic curve withouth complex multiplication. Then if $p > 163$, $\overline{\rho}_{E,p}(G)$ cannot be contained in a Borel subgroup.*

The proof of this theorem can be found in [29].

For the case iv) it has also been proven that (assuming the Birch and Swinnerton-Dyer conjecture) there exists N such that for all $p > N$, $\overline{\rho}_{E,p}(G)$ cannot be contained in the normalizer of a non-spit Cartan subgroup. However, at the moment there is no proof that does not depend on a conjecture.

For the case iii),

Theorem 6.2.7. *(Bilu-Parent, 2009) Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. There exists p_0 such that if $p > p_0$, $\overline{\rho}_{E,p}(G)$ cannot be contained in the normalizer of a split Cartan subgroup.*

With this last theorem, we can deduce Theorem 6.2.5. In fact, Serre actually acts whether $N = 37$. This problem is also called Serre's uniformity problem (c.f. [38]). Of course we are not going to prove any of these theorems, but it is worth mentioning that some of them use analytic tools.

Till now, we have only spoken about the situation when the image of the representation is the whole $GL_2(\mathbb{F}_p)$. We are going to talk about the cases when the representation is not the whole space of matrices. Some of the relevant work that have been made can be found in [48]. There, Zywina characterize all the possible subgroups that can appear depending on the form of j_E[1]. He does it for the primes $p = 2, 3, 5, 7, 11, 13, 17$.

Now we are going to show with one theorem and one conjecture what is actually known and what is still not known about the possible images of the representations

[1]The number j_E denotes the $j-$invariant defined in Chapter 2.

of elliptic curves $E/\mathbb{Q}$ without complex multiplication. Define the following matrices in $GL_2(\mathbb{F}_p)$, for some $a, b \in \mathbb{F}_p$:

$$D(a,b) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad M_\epsilon(a,b) = \begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let p be an odd prime and $\varepsilon = -1$ if $p \equiv 3 \pmod 4$ and otherwise let $\varepsilon \geq 2$ be the smallest integer such that $\left(\frac{\varepsilon}{p}\right) = -1$. Define the following subgroups of $GL_2(\mathbb{F}_p)$:

$$C_s(p) = \left\{ D(a,b) : a, b \in \mathbb{F}_p^\times \right\},$$
$$C_{ns}(p) = \left\{ M_\varepsilon(a,b) : (a,b) \in \mathbb{F}_p^2,\ (a,b) \neq (0,0) \right\}.$$

For $C_{ns}(p)$, the characteristic polynomial of the matrix $\begin{pmatrix} a & b\varepsilon \\ b & a \end{pmatrix}$ is

$$p(x) = x^2 - 2ax + a^2 - b^2\varepsilon,$$

so the eigenvalues are $a \pm bi$, where $i^2 = \varepsilon$ and $i \notin \mathbb{F}_p$. The eigenspaces are the kernels of the matrices

$$\begin{pmatrix} -ib & \varepsilon b \\ b & -ib \end{pmatrix}$$

and

$$\begin{pmatrix} ib & \varepsilon b \\ b & ib \end{pmatrix},$$

which are generated by the vectors $(i, 1)$ and $(i, -1)$. These vectors don't depend on a and b. As the cardinality of $C_{ns}(p)$ is $p^2 - 1$, this proves that the subgroup $C_{ns}(p)$ is a non-split Cartan subgroup.

We also write $C_s^+(p)$ for the normalizer of $C_s(p)$ in $GL_2(\mathbb{F}_p)$ and $C_{ns}^+(p)$ for the normalizer of $C_{ns}(p)$ in $GL_2(\mathbb{F}_p)$.

Notation 6.2.8. *Let $E/\mathbb{Q}$ be an elliptic curve. From now on we will denote the subgroup $\overline{\rho}_{E,p}(Gal(\overline{\mathbb{Q}}/\mathbb{Q}))$ by $G_E(p)$.*

The following theorem, due to Mazur, Serre, Bilu, Parent, Rebolledo and Zywina (see [48],[2],[1] for more details) is a summary of what it is actually known about the possible images of the representations.

Theorem 6.2.9. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and p a prime. Then one the following possibilities occurs:*

- $G_E(p) = GL_2(\mathbb{F}_p)$.

- $p \in \{2, 3, 5, 7, 11, 13, 17, 37\}$, *and* $G_E(p)$ *is conjugate in* $GL_2(\mathbb{F}_p)$ *to one of the groups in Tables 6.1 and 6.2.*
- $p = 13$ *and* $G_E(13)$ *is conjugate in* $GL_2(\mathbb{F}_{13})$ *to a subgroup of* $C_s(13)$, $C_{ns}(13)$ *or* `13S4` *(see Table 6.2).*
- $p \geq 17$*:*
  - $p \equiv 1 \pmod 3$, *and* $G_E(p)$ *is conjugate in* $GL_2(\mathbb{F}_p)$ *to* $C_{ns}(p)$.
  - $p \equiv 2 \pmod 3$, *and* $G_E(p)$ *is conjugate in* $GL_2(\mathbb{F}_p)$ *to* $C_{ns}(p)$ *or to the subgroup*

    $$G_0(p) = \left\{ M_\epsilon(a,b)^3,\ J \cdot M_\epsilon(a,b)^3 \ :\ (a,b) \in \mathbb{F}_p^2,\ (a,b) \neq (0,0) \right\} \subseteq C_{ns}(p).$$

The following tables, which have been extracted from Table 3 of [45] and from [20] show all the possibilities for the images when $p \leq 11$ and all the known images for the cases $p = 13, 17$ and $p = 37$. The first and the second columns include the names of the subgroups. For the precise definition of those subgroups, check [45]. The numbers d and d_v, which appear on the tables, are defined as follows:

- $d_v = |G_E(p)v|$, for $v \in \mathbb{F}_p^2$ with $v \neq (0,0)$, where $G_E(p)v$ denotes the set of all possible images when the elements of $G_E(p)$ are applied to v. This is equivalent to the degrees of the extensions $\mathbb{Q}(P)$ over $\mathbb{Q}$ for points $P \in E$ of order[2] p.
- $d = |G_E(p)|$, or equivalently $d = [\mathbb{Q}(E[p]) : \mathbb{Q}]$.

[2]Note that the possible images when the elements of $G_E(p)$ are applied to v are precisely the number of embeddings of the extension $\mathbb{Q}(P)/\mathbb{Q}$.

Sutherland	Zywina	d_v	d
2Cs	G_1	1	1
2B	G_2	1 , 2	2
2Cn	G_3	3	3
3Cs.1.1	$H_{1,1}$	1 , 2	2
3Cs	G_1	2 , 4	4
3B.1.1	$H_{3,1}$	1 , 6	6
3B.1.2	$H_{3,2}$	2 , 3	6
3Ns	G_2	4	8
3B	G_3	2 , 6	12
3Nn	G_4	8	16
5Cs.1.1	$H_{1,1}$	1 , 4	4
5Cs.1.3	$H_{1,2}$	2 , 4	4
5Cs.4.1	G_1	2 , 4 , 8	8
5Ns.2.1	G_3	8 , 16	16
5Cs	G_2	4 , 4	16
5B.1.1	$H_{6,1}$	1 , 20	20
5B.1.2	$H_{5,1}$	4 , 5	20
5B.1.4	$H_{6,2}$	2 , 20	20
5B.1.3	$H_{5,2}$	4 , 10	20
5Ns	G_4	8 , 16	32
5B.4.1	G_6	2 , 20	40
5B.4.2	G_5	4 , 10	40
5Nn	G_7	24	48
5B	G_8	4 , 20	80
5S4	G_9	24	96

Sutherland	Zywina	d_v	d
7Ns.2.1	$H_{1,1}$	6 , 9 , 18	18
7Ns.3.1	G_1	12 , 18	36
7B.1.1	$H_{3,1}$	1 , 42	42
7B.1.3	$H_{4,1}$	6 , 7	42
7B.1.2	$H_{5,2}$	3 , 42	42
7B.1.5	$H_{5,1}$	6 , 21	42
7B.1.6	$H_{3,2}$	2 , 21	42
7B.1.4	$H_{4,2}$	3 , 14	42
7Ns	G_2	12 , 36	72
7B.6.1	G_3	2 , 42	84
7B.6.3	G_4	6 , 14	84
7B.6.2	G_5	6 , 42	84
7Nn	G_6	48	96
7B.2.1	$H_{7,2}$	3 , 42	126
7B.2.3	$H_{7,1}$	6 , 21	126
7B	G_7	6 , 42	252
11B.1.4	$H_{1,1}$	5 , 110	110
11B.1.5	$H_{2,1}$	5 , 110	110
11B.1.6	$H_{2,2}$	10 , 55	110
11B.1.7	$H_{1,2}$	10 , 55	110
11B.10.4	G_1	10 , 110	220
11B.10.5	G_2	10 , 110	220
11Nn	G_3	120	240

Table 6.1: Possible images $G_E(p) \neq GL_2(\mathbb{F}_p)$, for $p \leq 11$, for non-CM elliptic curves $E/\mathbb{Q}$.

Sutherland	Zywina	d_v	d
13S4	G_7	72 , 96	288
13B.3.1	$H_{5,1}$	3 , 156	468
13B.3.2	$H_{4,1}$	12 , 39	468
13B.3.4	$H_{5,2}$	6 , 156	468
13B.3.7	$H_{4,2}$	12 , 78	468
13B.5.1	G_2	4 , 156	624
13B.5.2	G_1	12 , 52	624
13B.5.4	G_3	12 , 156	624
13B.4.1	G_5	6 , 156	936
13B.4.2	G_4	12 , 78	936
13B	G_6	12 , 156	1872

Sutherland	Zywina	d_v	d
17B.4.2	G_1	8 , 272	1088
17B.4.6	G_2	16 , 136	1088
37B.8.1	G_1	12 , 1332	15984
37B.8.2	G_2	36 , 444	15984

Table 6.2: Known images $G_E(p) \in GL_2(\mathbb{F}_p)$, for $p = 13, 17$ or 37, for non-CM elliptic curves $E/\mathbb{Q}$.

The following conjecture, motivated by a question of Serre [38], is an improvement of the previous theorem.

Conjecture 6.2.10. *If E is an elliptic curve defined over $\mathbb{Q}$ without complex multiplication, $p \geq 17$ a prime and (p, j_E) is not in the set*

$$\left\{(17, -17 \cdot 373^3/2^{17}), (17, -17^2 \cdot 101^3/2), (37, -7 \cdot 11^3), (37, -7 \cdot 137^3 \cdot 2083^3)\right\},$$

then $G_E(p) = GL_2(\mathbb{F}_p)$.

This conjecture would answer Serre's uniformity problem.

In [43] there are more theorems which are quite similar to Theorem 6.2.4 and that we are just going to mention.

Theorem 6.2.11. *(Serre). Let K be a number field and E/K an elliptic curve without complex multiplication. Then, if $\rho_{E,l}$ denotes the l-adic representation*

$$\rho_{E,l} : Gal(\overline{K}/K) \to Aut(T_l(E)),$$

we have that:

a) $\rho_{E,l}(Gal(\overline{K}/K))$ is of finite index in $Aut(T_l(E))$.

b) $\rho_{E,l}(Gal(\overline{K}/K)) = Aut(T_l(E))$ for all but finitely many primes l.

The proof of a) can be found in [36].

6.3 Galois representations of curves with complex multiplication

Till now we had only spoken about Galois representations of elliptic curves without complex multiplication. In this section we are just going to mention some known results about the case when the elliptic curve has complex multiplication.

Up to isomorphism over $\overline{\mathbb{Q}}$, there are just thirteen elliptic curves defined over $\mathbb{Q}$ with complex multiplication, and they are uniquely determined by their endomorphism ring and thus by f and D, where

$$End(E) = \mathbb{Z} + f\mathcal{O},$$

with $\mathcal{O}$ the ring of integers of the imaginary quadratic field with discriminant $-D$. The complete table can be found in [48] or in [44]. In that table, D is always prime.

Proposition 6.3.1. *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication and $j_E \neq 0$. Then the ring $End(E)$ is an order in the ring of integers of an imaginary quadratic field of discriminant $-D$. Let $p \neq 2$ be a prime number. Then*

- *If* $\left(\frac{-D}{p}\right) = 1$ *(that is, if there exists* $x \in \mathbb{F}_p$, $x \neq 0$ *such that* $x^2 = -D$*) then* $\overline{\rho}_{E,p}(G)$ *is conjugate (in* $GL_2(\mathbb{F}_p)$*) to the normalizer of a split Cartan subgroup.*

- *If* $\left(\frac{-D}{p}\right) = -1$*, then* $\overline{\rho}_{E,p}(G)$ *is conjugate (in* $GL_2(\mathbb{F}_p)$*) to the normalizer of a non-split Cartan subgroup.*

- *If* $-D \equiv 0 \mod p$*, and so* $p = D$*, consider the groups*

$$G' = \left\{ \begin{pmatrix} a & b \\ 0 & \pm a \end{pmatrix} : a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\},$$

$$H_1 = \left\{ \begin{pmatrix} a & b \\ 0 & \pm a \end{pmatrix} : a \in (\mathbb{F}_p^\times)^2, b \in \mathbb{F}_p \right\}$$

and

$$H_2 = \left\{ \begin{pmatrix} \pm a & b \\ 0 & a \end{pmatrix} : a \in (\mathbb{F}_p^\times)^2, b \in \mathbb{F}_p \right\}.$$

Suppose E *is isomorphic to* $E_{D,f}$*, where* $E_{D,f}$ *is one of the thirteen elliptic curves of the table. Then* $\overline{\rho}_{E,p}(G)$ *is conjugate in* $GL_2(\mathbb{F}_p)$ *to* H_1*.*

If E *is isomorphic to the quadratic twist of* $E_{D,f}$ *by* $-p$ *then* $\overline{\rho}_{E,p}(G)$ *is conjugate in* $GL_2(\mathbb{F}_p)$ *to* H_2*.*

If E *is not isomorphic to* $E_{D,f}$ *or its quadratic twist by* $-p$*, then* $\overline{\rho}_{E,p}(G)$ *is conjugate in* $GL_2(\mathbb{F}_p)$ *to* G'*.*

The cases $p = 2$ and $j_E = 0$ can be found in [48].

6.4 Modular Galois representations and Fermat's Last Theorem

In this subsection we will give a brief survey about Fermat's Last Theorem and some of the tools that are involved.

6.4.1 Modular forms and Galois representations.

We begin first with some definitions.

Definition 6.4.1. Let A be a certain ring and $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Let

$$\rho : G_{\mathbb{Q}} \to GL_2(A)$$

be a representation, p a prime number and I_p its inertia subgroup. We say that ρ is **unramified** at a prime p if $I_p \subset \ker \rho$.

Recall that I_p is the kernel of the natural application

$$Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p),$$

and $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is generated by $Frob_p$, so when ρ is unramified at p,

$$\rho(Frob_p) \in GL_2(A)$$

makes sense.

Definition 6.4.2. We say that a representation ρ is **flat** at p if for every ideal $I \subset A$ such that A/I is finite, the induced representation

$$\rho : G_{\mathbb{Q}_p} \to GL_2(A/I)$$

extends to a finite flat group scheme over $\mathbb{Z}_p$ (for our purposes we don't need to know and understand the exact definition of flat).

Notation 6.4.3. *Let $\rho : G_{\mathbb{Q}} \to GL_2(A)$ and $\rho' : G_{\mathbb{Q}} \to GL_2(A)$ two representations. If there exists $M \in GL_2(A)$ such that*

$$\rho(\sigma) = M\rho'(\sigma)M^{-1}$$

for all $\sigma \in G_{\mathbb{Q}}$ then we will write

$$\rho \cong \rho'$$

and we will say that both representations are conjugate.

Definition 6.4.4. Let A be a ring with a maximal ideal m_A and let

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(A)$$

be a representation. We define the **residual representation** as

$$\overline{\rho} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(k_A),$$

where $k_A = A/m_A$ by composing with the natural application

$$GL_2(A) \to GL_2(k_A).$$

Let p be a prime number. Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a newform of conductor N with expression

$$f(q) = \sum_{n \geq 1} a_n q^n,$$

and let K_f be the number field generated by the coefficients a_n. Let λ be a prime ideal of the ring of integers $\mathcal{O}_f$ lying over p and $K_{f,\lambda}$ the completion of K_f with respect to λ. Let $\mathcal{O}_{f,\lambda}$ be the ring of integers in $K_{f,\lambda}$. Some theory made by

Eichler and Shimura (check [41], [42] or [12]) asserts that there is a two dimensional representation

$$\rho_f : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{f,\lambda})$$

such that for all sufficiently large primes l, ρ_f is unramified at l and

$$Tr(\rho_f(Frob_l)) = a_p \qquad and \qquad \det(\rho_f(Frob_l)) = l.$$

On some occasions we will write $\rho_{f,l}$ instead of ρ_f. The following theorem of Ribet ([34]) will be very useful for the Fermat's Theorem.

Theorem 6.4.5. *Let f be a newform of weight two and conductor lN where $l \nmid N$ and l is a prime number. Consider*

$$\overline{\rho}_f : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_{f,\lambda}/\lambda)$$

the residual representation, and suppose that $\overline{\rho}_f$ is absolutely irreducible and that either:

- *$\overline{\rho}_f$ is unramified at l; or*
- *$l = p$ and $\overline{\rho}_f$ is flat at p.*

Then there exists another newform $g \in \mathcal{S}_2(\Gamma_0(N))$ such that

$$\overline{\rho}_f \cong \overline{\rho}_g.$$

6.4.2 Another version of modularity.

Definition 6.4.6. Let $E/\mathbb{Q}$ be an elliptic curve with conductor N, and let l be a prime number. Then we say that $\rho_{E,l}$ is modular if there exists a newform $f \in \mathcal{S}_2(\Gamma_0(N))$ with number field $K_f = \mathbb{Q}$ such that

$$\rho_{f,l} \cong \rho_{E,l}.$$

The following theorem asserts that all definitions of modularity are equivalent. In fact,

Theorem 6.4.7. *Let $E/\mathbb{Q}$ be an elliptic curve. The following affirmations are equivalent.*

- *E is modular (as in Definition 5.3.3).*
- *For some prime p, $\rho_{E,p}$ is modular.*
- *For all primes, $\rho_{E,p}$ is modular.*

There are in fact two more equivalent assertions that we are not going to mention.

6.5 Fermat's Last Theorem

The original theorem, which was formulated by Fermat in 1637, was the following:

Theorem 6.5.1. *Let $n \geq 3$. Then there are no triples of positive integers $x, y, z \in \mathbb{N}$ such that*

$$x^n + y^n = z^n. \tag{6.5.1}$$

The case $n = 4$ and $n = 3$ were proven by Fermat. Therefore, it suffices to prove the theorem for all primes with $p \geq 5$. Indeed, if there was any compound number $n \geq 3$ such that there existed a triple (x, y, z) for which (6.5.1) held, then for $d|n$ with d either prime or $d = 4$,

$$(x^{\frac{n}{d}})^d + (y^{\frac{n}{d}})^d = (z^{\frac{n}{d}})^d,$$

which is a contradiction. Thus, it suffices to prove that for any $p \geq 5$,

$$a^p + b^p + c^p = 0 \Longrightarrow abc = 0.$$

Suppose that there existed a prime number $p \geq 5$ and a triple (a, b, c) with $abc \neq 0$. We can suppose that $(a, b, c) = 1$, so only one of them (say b) is even, and (without loss of generality),

$$a \equiv -1 \mod 4.$$

Let E_{a^p,b^p,c^p} the elliptic curve with Weiestrass model

$$y^2 = x(x - a^p)(x + b^p).$$

This elliptic curve have some remarkable properties.

Proposition 6.5.2. *The elliptic curve E_{a^p,b^p,c^p} is semistable. Its minimal discriminant and conductor are*

a) $\Delta_{a^p,b^p,c^p} = 2^{-8}(abc)^{2p}$.

b) $N_{a^p,b^p,c^p} = \prod_{l|abc} l$.

Let

$$\overline{\rho}_{a^p,b^p,c^p} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$$

the Galois represetation of the elliptic curve E_{a^p,b^p,c^p}. Frey and Serre proved some properties of this representation in [15], [16] and [38].

Theorem 6.5.3. *With the above hypothesis,*

- $\overline{\rho}_{a^p,b^p,c^p}$ *is absolute irreducible.*
- $\overline{\rho}_{a^p,b^p,c^p}$ *is unramified outside* $2p$ *and flat at* p.

Therefore, either by Theorem 5.3.4 or Theorem 5.3.5, which is more general, E_{a^p,b^p,c^p} is modular, so there exists a newform $f \in \mathcal{S}_2(\Gamma_0(N_{a^p,b^p,c^p}))$ such that

$$\rho_{a^p,b^p,c^p} \cong \rho_f.$$

Hence $\overline{\rho}_{a^p,b^p,c^p} \cong \overline{\rho}_f$. By the previous theorem $\overline{\rho}_f$ is absolute irreducible, and it is unramified outside $2p$ and flat at p. Next, choose $l | N_{a^p,b^p,c^p}$ with $l \neq 2, p$. Using Theorem 6.4.5, there exists another newform $g_l \in \mathcal{S}_2(\Gamma_0(\frac{N_{a^p,b^p,c^p}}{l}))$ such that

$$\overline{\rho}_f \cong \overline{\rho}_{g_l}.$$

Repeating this process, we obtain that there exists a newform $g \in \mathcal{S}_2(\Gamma_0(2))$ such that

$$\overline{\rho}_f \cong \overline{\rho}_g.$$

But the dimension of $\mathcal{S}_2(\Gamma_0)$ is equal to the genus of $X_0(2)$, which is zero (for the definition and the proof of this last statement, check [10]). On the other hand, $g \neq 0$ because $a_1(g) = 1$, so we have found a contradiction, and thus we have 'proved' Fermat's Last Theorem.

Bibliography

[1] Bilu, Y.; Parent, P.: Serre's Uniformity Problem in the Split Cartan Case. arXiv:0807.4954v5.

[2] Bilu, Y.; Parent, P.; Rebolledo, M.: Rational points on X+ 0 (pr)(Q), Ann. Inst. Fourier (Grenoble) 63 (2013), 957984. 3

[3] Birch, B.; Swinnerton-Dyer, H.P.F.: Notes on elliptic curves (I) and (II), J.Reine Angew. Math. 212 (1963), 7-25 and 218 (1965), 79-108.

[4] Breuil, C.; Conrad, B.; Diamond, F.; Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Amer. Math. Soc., 14(4):843-939, 2001.

[5] Brumer, A.: The average rank of elliptic curves I. Invent. math. 109, 445-472 (1992). Springer-Verlag 1992.

[6] Cassels, J.W.S.; Frohlich, A.: Algebraic Number Theory. Academic Press Inc. (London) 1967

[7] Coates, J.; Wiles, Andrew: On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39 (1977), 223-251.

[8] Derickx, M.; Kamienny, S.; Stein, W.; Stoll, M.: Torsion points on elliptic curves over number fields of small degree, in preparation (private communication).

[9] Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, I, II, III, IV, Gott. Nach., 1953, 1955, 1956, 1957.

[10] Diamond, F.; Shurman, J.: A First Course in Modular Forms. 2005 Springer.

[11] Dickson, L.E.: Linear groups with an exposition of Galois field theory. Cosimo Classics 2007 reprint of original publication by B.G. Teubner, Leipzig, 1901.

[12] Eichler, M: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. Math. 5 (1954), 355-366.

[13] Faltings, G.: The general case of S.Lang's conjecture, Barsotti Symposium in Algebraic Geometry (Abano Terme,1991), 175-182, Perspect. Math., 15, Academic Press, San Diego, CA, 1994.

[14] Fouvry, E.; Nair, M.; Tenenbaum, G.: L'ensemble Exceptionnel dans la Conjecture de Szpiro. Bull. Soc. Math. de France 120, (1992), 485506.

[15] Frey, G.: Links between solutions of $A - B = C$ and elliptic curves. In Number Theory, proceedings of the Journees arithmetiques, held in Ulm, 1987, H.P.Schlickewei, E. Wirsing, editors. Lecture notes in mathematics 1380. Springer-Verlag, Berlin, New York, 1989.

[16] Frey, G.: Links between stable elliptic curves and certain Diophantine equations. Ann. Univ. Saraviensis, Ser. Math. 1 (1986), 1-40.

[17] Frey, G.:Curves with infinitely many points of fixed degree, Israel J.Math. 85 (1994), no. 1-3, 79-83.

[18] Goldfeld, D.: Conjectures on elliptic curves over quadratic fields. Number Theory Carbondale 1979. Springer-Verlag 1979.

[19] Goldfeld, D.: Gauss class number problem for imaginary quadratic elds. Bulletin of the AMS 13 (1985), 23-37.

[20] González Jiménez, E.; Najman, F: Growth of torsion groups of elliptic curves upon base change. arXiv:1609.02515.

[21] Heath-Brown, D.R.: The Average Analytic Rank of Elliptic Curves. arXiv:math/0305114v1 (2003).

[22] Kamienny, S.; Mazur, B.: Rational torsion of prime order in elliptic curves over number fields. With an appendix by Andrew Granville. Columbia University Number Theory Seinar (New York, 1992). No. 228 (1995), 3, 81-100.

[23] Koblitz, N.: A course in Number Theory and Cryptography. SpringerVerlag. Graduate Texts in Math. 114. Second edition, 1994.

[24] Kuijk, W.; Serre, J.-P.; Swinnerton-Dyer H.P.F.; Dwork B.; Katz, N.; Cartier P.; Roy.Y: Modular Functions of One Variable III. Proceedings International Summer School University of Antwerp, RUCA July 17-August 3, 1972. Springer-Verlag Berlin Heidelberg 1973.

[25] Lang, S.: Algebraic Number Theory. Springer-Verlag New York Inc, 1986.

[26] Lang, S.: Algebra. Revised third edition. Springer-Verlag New York Inc, 2002.

[27] Manin, J.: The p-torsion of elliptic curves is uniformly bounded, Izv. Akad. Nauk SSSR 33 (1969), AMS Transl., 433-438.

[28] Mazur, B.: Modular curves and the Eisenstein ideal, IHES Publ. Math. 47 (1977), 33-186.

[29] Mazur, B.: Rational isogenies of prime degree, Invent. Math 44 (1978), 129-162.

[30] Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124 (1996), no. 1-3, 437-449.

[31] Neukirch, J.: Algebraic Number Theory. Springer-Verlag Berlin Heidelberg 1999 .

[32] Ogg, A.: Elliptic curves and wild ramification, Am. J. of Math. 89 (1967), 204-215.

[33] Parent, P.: No 17-torsion on ellitpic curves over cubic number fields, Journal de Théorie des Nombres de Bourdeaux 15 (2003), 831-838.

[34] Ribet, K.A.: On modular representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. Invent. math. 100 (1990), 431-476.

[35] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones math. 15, 259-331 (1972). Springer-Verlag 1972.

[36] Serre, J.-P.: Abelian l-adic representations and elliptic curves. New York: Benjamin 1968.

[37] Serre, J.-P.: Sur les représentations modulaires de degré 2 de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. (1987), 179-230.

[38] Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev, Publ. Math. IHES 54 (1981), pp. 123-201.

[39] Serre, J.-P.: A course in Arithmetic. Graduate Texts in Mathematics. 7. Springer-Verlag. 1973.

[40] Shafarevich, I.R.; Tate, J: The rank of elliptic curves, AMS Transl. 8 (1967), 917-920.

[41] Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton University Press, Princeton, 1971.

[42] Shimura, G.: Correspondances modulaires et les fonctions ζ de courbes algébriques, J. Math. Soc. Japan 10 (1958), 1-28.

[43] Silverman, J.: The Arithmetic of Elliptic Curves. Springer-Verlag New York Inc, 1986.

[44] Silverman, J.H.: Advanced topics in the arithmetic of elliptic curves, Second, Graduate Texts in Mathematics, vol 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[45] Sutherland, A.V.: Computing images of Galois representations attached to elliptic curves. Forum Math. Sigma 4 (2016), e4, 79 pp. 3, 3, 8.1.2.

[46] Weil, A.: Jacobi sums as Grssencharaktere, Trans. Amer. Math. Soc. (1952), 487-495.

[47] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. Annals of Math. 141 (1995), 443-551.

[48] Zywina, D.J.: On the possible images of the mod l representations associated to elliptic curves over $\mathbb{Q}$. arXiv:1508.07660. 3, 3, 3, 5, 7, 7.1, 8.1.2