Mazur's control theorem

Alberto Angurel Andrés

Máster en Matemáticas y Aplicaciones

MÁSTERES
DE LA UAM
2021-2022

Facultad de Ciencias

UAM Universidad Autónoma de Madrid

Universidad Autónoma de Madrid

Facultad de Ciencias, Departamento de Matemáticas

MAZUR'S CONTROL THEOREM

Master's Degree in Mathematics and Applications

Master's thesis

Author: **Alberto Angurel Andrés**

Supervisor: **Daniel Macías Castillo**

July 2022

Abstract

In this thesis, we expose a self-contained introduction to Iwasawa theory of elliptic curves, our main objective being to prove Mazur's control theorem concerning the Galois theoretic behaviour (at primes of good ordinary reduction) of Selmer groups of elliptic curves defined over a number field.

First, we cover some necessary algebraic preliminaries. They include the characterisation of Iwasawa modules up to pseudo-isomorphism, the basic theory of formal groups and the Pontryagin duality. We have also exposed the basic characterisation of profinite groups, as a preparation for generalising Galois theory to infinite field extensions. Finally, a detailed introduction to cohomological theory of finite and profinite groups has been included.

The second part of this thesis is related to local class field theory. Its goal is proving two deep results. The first one is the local reciprocity law, about an isomorphism between the Galois group of the maximal abelian extension of a local field and the profinite completion of the multiplicative group of that field. The other important result is the corank lemma, on the $\mathbb{Z}_p$-corank of a Galois cohomology group.

The final goal of this work is studying the arithmetic of elliptic curves. We do that when they are defined over a local field and over a number field. In the latter case, the Mordell-Weil theorem has been proven. We have delved into these issue by defining the Selmer and Tate-Shafarevich groups, as a preparation for Mazur's control theorem. After giving a proof, we have surveyed the different implications it has.

AMS Mathematics Subject Classification

- **11G05**: Arithmetic algebraic geometry. Elliptic curves over global fields.
- **11G07**: Arithmetic algebraic geometry. Elliptic curves over local fields.
- **11R23**: Algebraic number theory: global fields. Iwasawa theory.
- **11S25**: Algebraic number theory: local and p-adic fields. Galois cohomology.
- **11S31**: Algebraic number theory: local and p-adic fields. Class field theory.

Keywords

Iwasawa modules, formal groups, Galois cohomology, local reciprocity map, Mordell-Weil theorem, Selmer group, Tate-Shafarevich group, Mazur's Control Theorem.

Resumen

En este trabajo exponemos una introducción autocontenida de la teoría de Iwasawa de curvas elípticas, siendo nuestro principal objetivo demostrar el teorema de control de Mazur acerca del comportamiento teórico de la acción de Galois en los groups de Selmer de curvas elípticas definidas sobre un cuerpo de números.

En primer lugar, explicamos ciertos preliminares algebraicos. Entre ellos se encuentra la caracterización de módulos de Iwasawa salvo pseudo-isomorfismo, la teoría básica de grupos formales y la dualidad de Pontryagin. Además, hemos incluido una caracterización de los grupos profinitos, a modo de preparación para generalizar la teoría de Galois a extensiones infinitas. Por último, se ha expuesto una introducción detallada a la cohomología de grupos finitos y profinitos.

La segunda parte de este trabajo trata sobre la teoría de cuerpos de clase local y tiene como objetivo demostrar dos resultados profundos. En primer lugar, está la función de reciprocidad local, que da un isomofismo entre el grupo de Galois de la extensión maximal abeliana de un cuerpo local y la compleción profinita de el grupo multiplicativo de dicho cuerpo. Por otro lado, tenemos el lema del corango, sobre el corango como $\mathbb{Z}_p$-módulo de un grupo de cohomología de Galois.

El objetivo final de esta tesis es estudiar la aritmética de curvas elípticas, tanto cuando están definidas sobre un cuerpo local como cuando lo están sobre un cuerpo de números. En este último caso, se ha demostrado el teorema de Mordell-Weil. Posteriormente, se ha profundizado en este tema definiendo los grupos de Selmer y Tate-Shafarevich, a modo de preparación para el teorema de control de Mazur. Después de demostrar este resultado, hemos indagado en sus distintas implicaciones.

Clasificación Matemática por temas de la AMS

- **11G05**: Geometría algebraica aritmética. Curvas elípticas sobre cuerpos globales.
- **11G07**: Geometría algebraica aritmética. Curvas elípticas sobre cuerpos locales.
- **11R23**: Teoría algebraica de números: cuerpos globales. Teoría de Iwasawa.
- **11S25**: Teoría algebraica de números: cuerpos locales y p-ádicos. Cohomología de Galois.
- **11S31**: Teoría algebraica de números: cuerpos locales y p-ádicos. Teoría de cuerpos de clases.

Palabras Clave

Módulos de Iwasawa, grupos formales, cohomología de Galois, función de reciprocidad local, teorema de Mordell-Weil, grupo de Selmer, grupo de Tate-Shafarevich, teorema de control de Mazur.

Acknowledgements

Foremost, I want to thank my supervisor Daniel Macías, not only for sharing many mathematical ideas that guided me when I was stuck, but also for offering me invaluable advice for the next steps in my academic career.

I also appreciate the effort of the participants and organisers of the different study groups in which I have participated this year. In particular, I want to mention Daniel and Enrique, who have unselfishly shared with me their knowledge about Iwasawa theory and group cohomology and whose exciting observations have improved the quality of this thesis.

In another vein, I am grateful to ICMAT and CSIC for supporting this thesis through a JAE Intro Severo Ochoa-CSIC Master's grant.

Contents

Chapter 1

Introduction

1.1 About the Arithmetic of Elliptic Curves

The final goal of the content included in this thesis is to study the groups $E(K)$, where E is an elliptic curve defined over some field K.

An elliptic curve E is just a projective, smooth algebraic curve of genus 1 with a distinguished point $O \in E(K)$. They can be described by a Weierstrass equation. In other words, E can be studied as the points $(X : Y : Z)$ in the projective plane over the algebraic closure of K which satisfy the following equation:

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

for some coefficients $a_i \in K$. Elliptic curves are endowed with a natural abelian group structure, which can be defined algebraically or geometrically. This definition is the reason why O has a distinguished role. Moreover, imposing that O has coordinates belonging to K implies that the set of rational points $E(K)$ is a subgroup.

Computing the groups of rational points is the central problem that concerns the arithmetic of elliptic curves. In general, it is a difficult problem because, unlike conics, elliptic curves do not satisfy the local-global principle. It means that an elliptic curve may not have any rational point different from O although the curve always contains a non-trivial rational point when considered as curves defined over the completion via every valuation in K.

The situation when K is a number field, i.e., a finite extension of $\mathbb{Q}$, is related to Mordell-Weil theorem, which states that the group $E(K)$ is finitely generated under these hypothesis.

Theorem 1.1. (Mordell-Weil) Let E/K be an elliptic curve defined over a number field K. Then the group $E(K)$ is finitely generated.

Therefore, the structure theorem of finitely generated modules over the principal ideal domain $\mathbb{Z}$ can be applied and we have the existence of an integer $r \geq 0$ and a finite group T such that

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

Given an elliptic curve E/K, we want to know the rank r and the torsion subgroup T. The torsion is usually easily computable since there is a result which states that, under certain conditions, the torsion subgroup of some fixed order injects into the rational points of other elliptic curves, defined over finite fields. In fact, for every discrete valuation v defined on K but a finite amount of them, there is an injection

$$E(K)[m] \hookrightarrow \widetilde{E}(k_v)$$

where k_v is the residue field of the completion K_v and $\widetilde{E}$ is called the reduced curve. By checking some of these injections, one could compute $E(K)_{\text{tors}}$.

Even more, there is a result due to Mazur [18] that says there are just 15 possible torsion subgroups in an elliptic curve defined over $\mathbb{Q}$.

Theorem 1.2. (Mazur) Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following fifteen groups

$$\mathbb{Z}/N\mathbb{Z}, \text{ with } 1 \leq N \leq 10 \text{ or } N = 12; \quad \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \text{ with } 1 \leq N \leq 4.$$

The generalisation of this result to number fields is an active research issue. In this direction, there is a result due to Merel [19].

Theorem 1.3. (Merel, 1996) Let K be a number field such that $d = [K : \mathbb{Q}]$, let E/K be an elliptic curve and let $p > d^{3d^2}$ be a prime number. Then $E(K)$ does not contain torsion of order p.

The problem of computing the rank of a given elliptic curve is much more difficult and, up to now, there is no general method to compute it in an arbitrary curve. For a 'randomly chosen' elliptic curve defined over $\mathbb{Q}$, this rank is usually small, although it is conjectured that there are elliptic curves $E/\mathbb{Q}$ having arbitrarily large rank.

At the moment, the known elliptic curve E with the highest rank was found by N. Elkies [9] and has rank 28.

The way we approach this problem of computing the rank is purely cohomological and it is based in the following short exact sequence:

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \text{Sel}_E(K)_p \longrightarrow Ш_E(K)_p \longrightarrow 0$$

where p is an arbitrary prime number and $\text{Sel}_E(K)_p$ and $Ш_E(K)_p$ are the p-primary parts of the Selmer and Tate-Shafarevich groups. Those are subgroups of certain Galois cohomology groups which will be defined in chapter 11.

Since $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ and it injects into the Selmer group, the latter can establish an upper bound for the rank of Mordell-Weil. Moreover, there is an important conjecture related to this exact sequence:

Conjecture 1.1. Let E be an elliptic curve defined over a number field K. Then the Tate-Shafarevich group $Ш_E(K)$ is finite.

The interest of this conjecture resides on the fact that, under this assumption, the division subgroup of $\text{Sel}_E(K)$ will be isomorphic to $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, so the Selmer group will compute the rank of the Mordell-Weil group.

In this line of computing the rank of an elliptic curve there is one of the millenium-prize problems proposed by the Clay Mathematics Institute: Birch and Swinnerton-Dyer conjecture. It states that the rank of an elliptic curve defined over $\mathbb{Q}$ is the order of vanishing at certain complex function $L_{E|\mathbb{Q}}(s)$, called Hasse-Weil L-series (see [27]), whose definition involves only the number of points on the reduced curves $\widetilde{E}(k_v)$ for the finite places v in K. Moreover, it conjectures that the first non-vanishing coefficient in the Taylor expansion is related to the cardinality of the Tate-Shafarevich group.

The first general advance in proving this conjecture is a theorem from Coates and Wiles [8], that proves that the group $E(\mathbb{Q})$ must be finite in case that $L_{E|\mathbb{Q}}(s)$ does not vanish at $s = 1$ and E has complex multiplication. Gross and Zagier [12] proved the case when the Hasse-Weil L-series has a simple zero. They assume the elliptic curve was modular, but it was proved later that all elliptic curves defined over $\mathbb{Q}$ are. This result is known as modularity theorem

[3]. The situation for higher ranks is still open, although there are strong numerical evidences supporting it.

Next question that arises is whether Mordell-Weil theorem generalises to infinite algebraic extensions of $\mathbb{Q}$. The answer is clearly negative, since the torsion subgroup of an elliptic curve defined over an algebraically closed field is

$$E_{\text{tors}}(\overline{K}) \cong \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$$

which is not finitely generated. However, there might be infinite algebraic extensions $K|\mathbb{Q}$ such that $E(K)$ contains only finitely many torsion elements. Then checking whether the group $E(K)$ is finitely generated or not could be done using the following sufficient, and obviously necessary, conditions.

Theorem 1.4. Let K be a Galois extension of $\mathbb{Q}$. Then $E(K)$ is finitely generated if and only if the following conditions are satisfied.

1. The torsion subgroup $E(K)_{\text{tors}}$ is finite.
2. The rank of $E(L)$ is bounded when L runs through the finite subextensions of $K|\mathbb{Q}$.

Verifying the hypothesis of last theorem is usually hard, specially the one related to the boundedness of the rank.

A particular case in which these hypothesis has been done is when K is the maximal abelian extension $\mathbb{Q}_\Sigma^{\text{ab}}$ of the rationals which is unramified outside a certain finite set of primes Σ. The first hypothesis comes as consequence of some theorems due to K. Kato and D. Rohlich, since they deduced that $\text{rank}_{\mathbb{Z}} E(L)$ is bounded when E is a modular elliptic curve and L runs through the finite, abelian extensions of $\mathbb{Q}$ which are unramified outside a finite set of primes Σ. The assumption that the elliptic curve is modular does not suppose much problem, since the above mentioned modularity theorem [3] implies that every elliptic curve defined over $\mathbb{Q}$ is modular.

The situation regarding the torsion subgroup is not so difficult, even though it is still far out of the scope of this thesis. K. Ribet proved in [25] that $E(\mathbb{Q}_\Sigma^{\text{ab}})_{\text{tors}}$ is finite. As a consequence, we have the following result.

Theorem 1.5. Let $E/\mathbb{Q}$ be an elliptic curve and let Σ be a finite set of primes. Then $E(\mathbb{Q}_\Sigma^{\text{ab}})$ is finitely generated.

1.2 About Iwasawa Theory

Iwasawa theory was first introduced in 1959 by the Japanese mathematician Kenkichi Iwasawa. Its purpose was to examine the growth of the class number in a $\mathbb{Z}_p$-extension of a number field, that is, a Galois extension whose Galois group is isomorphic to the p-adic integers, where p is some fixed prime number. These extensions will be denoted by $F_\infty|F$, where F is a number field. Because of the Galois correspondence between subextensions and closed subgroups of $G_{F_\infty|F} \cong \mathbb{Z}_p$, we know that there is a unique subextension of degree p^n, which will be denoted by F_n.

For every number field F, there is a unique $\mathbb{Z}_p$-extension contained in $F(\mu_{p^\infty})$, where μ_{p^∞} are the roots of unity whose order is a power of p. It is known as the *cyclotomic* $\mathbb{Z}_p$-extension. If F is totally real, that is, every embedding from F into $\mathbb{C}$ is contained in $\mathbb{R}$, then it is conjectured that the only $\mathbb{Z}_p$-extension is the cyclotomic one. That is known as *Leopoldt's conjecture*. However, in case that F is an imaginary quadratic field, there is another important $\mathbb{Z}_p$-extension, known as the *anticyclotomic* $\mathbb{Z}_p$-extension. It is characterised by the isomorphism $G_{F_n|\mathbb{Q}} = \mathcal{D}_{2p^n}$, where $\mathcal{D}_{2p^n}$ represents the dihedral group whose order is $2p^n$.

The idea behind Iwasawa theory is the following one. The Galois group of the maximal abelian pro-p extension of F_∞ is a $\mathbb{Z}_p$-module over which there is an action of $\Gamma := G_{F_\infty|F}$ defined by

inner automorphisms. It can thus be understood as a module over the group algebra $Z_p[[\Gamma]]$, which is defined by an inverse limit over the group algebras of the finite quotients of Γ. It turns out that this group algebra is isomorphic to the power series ring $\Lambda := \mathbb{Z}_p[[T]]$ and finitely generated Λ-modules can be classified through the following structure theorem.

Theorem 1.6. Let M be an Iwasawa module. Then there are irreducible polynomials F_j, natural numbers r, m_i, n_j and a homomorphism with finite kernel and cokernel given by

$$M \xrightarrow{\approx} \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/F_j^{n_j}$$

The number r is called the rank of M and it vanishes if and only if M is a torsion Λ-module. Moreover, last theorem is the reason why we can define the following invariants:

$$\mu = \textstyle\sum_{i=1}^{s} m_i, \quad \lambda = \sum_{j=1}^{t} n_j \deg(F_j)$$

There is a theorem [21] from basic algebraic number theory which states that the ideal class group of a number field is always finite. However, computing its cardinality is not easy. The achievement of K. Iwasawa was finding that the growth of the class number in a $\mathbb{Z}_p$-extension of a number field follows some kind of regularity. In particular, Iwasawa proved in [15] the following result.

Theorem 1.7. In a $\mathbb{Z}_p$-extension, there are integers λ, μ and ν (where λ and μ come from theorem 1.6) such that, for n large enough

$$|Cl(F_n)_p| = p^{\lambda n + \mu p^n + \nu}$$

Remark 1.1. In case that $F_\infty|F$ is the cyclotomic $\mathbb{Z}_p$-extension of some number field, it is conjectured that $\mu = 0$.

The idea behind this proof is the following. By global class field theory, the class group of F_n is isomorphic to the Galois group of its maximal abelian extension unramified at every prime of F_n. That extension is known as Hilbert class field. Hence the p-primary part of this class group is the Galois group of the maximal p-subextension of the Hilbert class field. This new extension is called the p-Hilbert class field of F_n.

Iwasawa ideas can be applied to the maximal abelian, unramified at every prime, pro-p extension L_∞ of F_∞. Then the maximal abelian subextension $L_n|F_n$ of $L_\infty|F_n$ is thus the p-Hilbert class field of F_n, so $Cl(F_n)_p \cong G_{L_n|F_n}$. Moreover, $G_{L_n|F_n}$ can be computed as the abelianised group of $G_{L_\infty|F_n}$. Hence $X := G_{L_\infty|F_\infty}$ can be considered as Λ-module and $Cl(F_n)_p$ can be thus computed as the quotient X/w_n, where $w_n \in \mathbb{Z}_p[T]$ is some particular polynomial. The theorem follows thus from theorem 1.6.

Barry C. Mazur used in 1970 Iwasawa ideas for the study of elliptic curves. In particular, Mazur considered an elliptic curve E defined over a number field F and studied the growth of the group of rational points along a $\mathbb{Z}_p$-extension. His idea was to consider $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ as an Iwasawa module. One could thus deduce that $X/w_n = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)^{G_{F_\infty|F_n}}, \mathbb{Q}_p/\mathbb{Z}_p)$ and the growth of $\mathrm{Sel}_E(F_\infty)^{G_{F_\infty|F_n}}$ can be studied using theorem 1.6. This theorem also controls the growth of the Selmer group defined over the number fields in the tower due to the following result [17], whose proof is the main goal of this thesis.

Theorem 1.8. (Mazur, 1972) There are natural maps

$$\mathrm{Sel}_E(F_n)_p \to \mathrm{Sel}_E(F_\infty)_p^{G_{F_\infty|F_n}}$$

having finite kernels and cokernels whose orders are bounded as $n \to \infty$.

As a consequence, if an elliptic curve has rank 0 and finite Tate-Shafarevich group at the base field F, then $\mathrm{Sel}_E(F_\infty)$ will be a torsion Iwasawa module and, consequently, the rank of $E(F_n)$ is bounded as $n \to \infty$, which was one of the assumptions of theorem 1.4.

Under certain conditions, the growth of the Selmer and Tate-Shafarevich groups can be controlled by the invariants λ and μ defined after theorem 1.6.

Theorem 1.9. Assume that both $E(F_n)$ and $Ш_E(F_n)_p$ are finite for every $n \in \mathbb{Z}$. Then there are $\lambda, \mu \in \mathbb{N} \cup \{0\}$ depending only on E and $F_\infty | F$ such that

$$|\mathrm{Sel}_E(F_n)_p| = |Ш_E(F_n)_p| = p^{\lambda n + \mu p^n + O(1)}$$

Although it was conjectured that $\mu = 0$ in theorem 1.7 applied to the cyclotomic $\mathbb{Z}_p$-extension of the number field F, when working with elliptic curves we will show examples in which this invariant takes a positive value. The following result, which will not be proved on this thesis but appears in [10], gives a lower bound for this μ-invariant.

Theorem 1.10. Let $E/\mathbb{Q}$ be an elliptic curve and let p be an odd prime number such that E has good, ordinary reduction at p. Assume that $\mathrm{Hom}(\mathrm{Sel}_E(\mathbb{Q})_p, \mathbb{Q}_p/\mathbb{Z}_p)$ is a torsion Λ-module and that $E[p^\infty]$ contains a $G_\mathbb{Q}$-submodule of order p^m and ramified at p. Then $\mu \geq m$.

If the group of F-rational points of the elliptic curve is not torsion, it might happen that the rank remains unbounded in the $\mathbb{Z}_p$-extension. Nevertheless, that growth is in some way regular.

Theorem 1.11. Let E/F be an elliptic curve and assume it has good, ordinary reduction at all primes of F lying over p. If r is the rank of $\mathrm{Hom}(\mathrm{Sel}_E(\mathbb{Q})_p, \mathbb{Q}_p/\mathbb{Z}_p)$ as a Λ-module and $Ш_E(F_n)_p$ is finite for all $n \in \mathbb{N}$, then

$$\mathrm{rank}(E(F_n)) = rp^n + O(1) \ \forall n \in \mathbb{N}$$

We now state two theorems, whose proofs are out of the scope of this work and that shows that both situations (bounded or unbounded rank) may happen. For that purpose, we shall mention that basic theory of elliptic curves imply that the ring of endomorphisms of an elliptic curve satisfy that $\mathrm{End}(E) \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or a quadratic imaginary field, provided that the field over which the elliptic curve is defined has characteristic equal to 0. In the latter case, it is said that E has complex multiplication.

Theorem 1.12. Let $E/\mathbb{Q}$ be an elliptic curve and assume $F := \mathrm{End}(E) \otimes \mathbb{Q}$ is imaginary. Assume that F_∞ is a $\mathbb{Z}_p$-extension of F different from the anticyclotomic one. Then $\mathrm{rank}_\mathbb{Z} E(F_n)$ is bounded.

Theorem 1.13. In the conditions of last theorem, if either E has supersingular reduction at p or the Hasse-Weil L-series $L_{E/\mathbb{Q}}(s)$ has order zero at $s = 1$, then $\mathrm{rank}_\mathbb{Z}(E(F_n^{ac}))$ is unbounded.

1.3 About This Thesis

This thesis intends to be a fairly self contained introduction to Iwasawa theory of elliptic curves. The reader should also be warned that none of the results in these thesis are original, being the work done merely bibliographic.

However, a deep result regarding Poitou-Tate duality in Galois cohomology groups ([23], theorem 7.2.6) has had to be assumed while proving theorem 11.6, as a preparation for the main result in this thesis: Mazur's control theorem.

In another vein, it is assumed that the reader is familiar basic algebraic number theory and basic properties of local fields, appearing in [5] and chapters I and II of [21], basic homological algebra from the first chapter of [13] and, foremost, with some theory of elliptic curves included in chapter III of [27].

Now it will be briefly explained how the exposition is structured. First, it is divided into three parts. In part I we explain the algebraic preliminaries we will need for developing the remaining of the thesis. Part II shows an introduction to local class field theory, including some deep results over which we build the Iwasawa theory of elliptic curves. Finally, part III is related to the arithmetic of elliptic curves and completes the main goal of this thesis: proving Mazur's control theorem regarding the Galois theoretic behaviour of Selmer groups of an elliptic curve defined over a number field.

Each part is again subdivided in several chapters. We start in chapter 2 by showing different preliminaries related to commutative algebra which will be necessary for developing the Iwasawa theory of elliptic curves. Among them we highlight the structure theorem of Iwasawa modules up to pseudo-isomorphism, whose proof has been seen in [23]. This structure theorem will be applied later to some Galois and Selmer groups. Apart from that, different topics like Hensel's lemma and certain localisations in Dedekind domains, which generalise the finiteness theorems in algebraic number theory, are also covered in this chapter.

Chapter 3 is about formal groups, which appear in the theory of elliptic curves as a formal development of the sum operation in terms of a power series. Their study permits us to state very interesting properties about elliptic curves defined over local fields. In particular, the characterisation of the torsion points in the group associated to a formal group gives an algorithm to compute the torsion subgroup of an elliptic curve defined over a local field and, consequently, over a number field. Some properties of divisibility and the concepts of invariant differential and formal logarithm are also included in this chapter. The reference used for this chapter has been chapter IV. of [27].

In chapter 4 we expose the concept of Pontryagin duality in order to extend the structure theorem of finitely generated abelian groups to those groups having finite corank. For that purpose, we develop some theory of inverse and direct limits and then we introduce profinite groups, which will appear later in the exposition of infinite Galois theory. Then we detail the concept of duality and $\mathbb{Z}_p$-corank, which will be used to generalise the structure theorem of finitely generated modules over a principal ideal domain to those being cofinitely generated.

Chapter 5 is a mixture of topics related to Galois theory that will be required at some points of this thesis. First, we mention n-Kummer extensions, i.e., abelian extensions with exponent dividing n and describe them in terms of its generators. After that, we generalise Galois theory to infinite field extensions, where the profinite groups previously defined arise naturally. Finally, last section is dedicated to identify the absolute Galois group of a completion with the decomposition subgroup of the absolute Galois group of the original field.

Chapter 6 is dedicated to introduce the continuous cohomology of profinite groups. Apart from giving basic definitions, we show important properties like the long cohomological exact sequence and inflation-restriction sequence. We will also define Tate-cohomology groups, which are defined only for finite groups, and study them when the original group is cyclic. We conclude the chapter by showing an important theorem due to Tate and studying the cohomology groups for the p-adic numbers. This chapter plays a central role in this thesis, since the study of the arithmetic of the elliptic curves will be mainly cohomological. The references used for this chapter have been [4], [23] and [26].

Part II is dedicated to introduce local class field theory. Its main goal is to proof two deep results in this area: the local reciprocity law, in chapter 7 and the corank lemma, in chapter 8.

In chapter 7 we apply the cohomological results obtained in chapter 6 to a Galois group of a field extension. We particularise then to the case when the group is the absolute Galois group of a local field in order to prove one of the above mentioned results: the local reciprocity law, which establishes an isomorphism between the Galois group of the maximal abelian extension of a local filed and the profinite completion of the multiplicative group of that field. The reference used for this chapter has been [22].

The local reciprocity map will have a central role in the proof of the other result, the one concerning chapter 8. It is the corank lemma, which is proven in [11] and is related to the $\mathbb{Z}_p$-corank of certain Galois cohomology group It will be required in chapter 11 for describing the image of the Kummer map while proving the main result of this thesis: Mazur's control theorem.

The study of the arithmetic of elliptic curves is shown in part III. It includes the final goal of this thesis and uses all of the theory included in parts I and II. For this part, we have used [27] for chapters 9 and 10 and [11] for chapter 11.

First we expose a survey of the theory of elliptic curves defined over local and number fields. Chapter 9 is dedicated to the local case, first defining the reduction map and then deducing many interesting results about the torsion rational points. It provides a method for computing the torsion subgroup of an elliptic curve defined over a local field and it can be applied for number fields by considering different completions. In particular, it implies that the torsion subgroup of an elliptic curve defined over a local or a number field is finite, result that will be strengthened to Mordell-Weil theorem in chapter 10. Using the fact that the reduction map is surjective, even when restricted to the torsion subgroups, a description of the group of rational points of an elliptic curve defined over a local field has been given.

Like we have just mentioned, chapter 10 is dedicated to Mordell-Weil theorem, which states that the group $E(K)$ is finitely generated when K is a number field. Its proof is divided in two parts The first one is the weak Mordell-Weil theorem, which says that the factor group $E(K)/mE(K)$ is finite. The proof exposed uses some cohomological tools previously developed. After that, the weak Mordell-Weil theorem, together with the descent theorem and the definition of a height function on the elliptic curve, imply Mordell-Weil theorem.

Last chapter 11 is dedicated to the main theorem of this thesis: Mazur's Control theorem. Before stating it, we had to develop Kummer theory for elliptic curves and define Selmer and Tate-Shafatevich groups. After proving Mazur's control theorem, some consequences related to the growth of the rank of Mordell-Weil group and the cardinality of Tate-Shafarevich one in a $\mathbb{Z}_p$-extension have been mentioned.

Part I

Algebraic Preliminaries

Chapter 2

Commutative Algebra

In this chapter, we expose some preliminary results related to commutative algebra which will be needed for studying the arithmetic of elliptic curves. First section 2.1 is about one version of Hensel's lemma, which can be seen in [27] and is related to the existence of roots of polynomials in complete local rings.

In sections 2.2, 2.3 and 2.4 we show the properties of Iwasawa modules, which will take a very important role in the study of the growth of the Mordell-Weil group in $\mathbb{Z}_p$-extensions of certain number field. We start this exposition by considering a more general case: finitely generated modules over a complete discrete valuation ring. However, we will need to particularise to the case when the discrete valuation ring is also regular and has dimension 2, what will be the case we are going to be interested in, for the purpose of obtaining a complete structure theorem up to pseudo-isomorphism. For these sections, the main reference used has been [23].

Finally, section 2.5 studies the behaviour of certain localisations in Dedekind domains. It is used to extend two important theorems in algebraic number theory, Dirichlet's unit theorem and the finiteness of class number, to S-units and S-ideals, fact that will have a very important role in the proof of weak Mordell-Weil theorem. An interested reader should also check [21].

2.1 Hensel's Lemma

Throughout this section, we are going to show an important result, commonly known as Hensel's lemma, about lifting roots of polynomials in the residue field of a complete local ring.

Proposition 2.1. Let O be a ring that is complete with respect to its I-adic topology, where I is some ideal of O. Let $F \in O[T]$ be a polynomial and suppose there are a natural number $n \in \mathbb{N}$ and an element $a \in O$ satisfying

$$F(a) \in I^n, \quad F'(a) \in O^*$$

Then for any $\alpha \in O$ satisfying $\alpha = F'(a) \mod I$, the sequence

$$\omega_0 = a, \quad \omega_{m+1} = \omega_m - \frac{F(\omega_m)}{\alpha}$$

converges to an element $b \in O$ satisfying

$$F(b) = 0, \quad b \equiv a \mod I^n$$

Furthermore, those conditions determine b uniquely providing that R is an integral domain.

Proof. By replacing $F(w)$ by $\frac{F(w+a)}{\alpha}$, we can deal with the case $a = 0$ and $\alpha = 1$ without any loss of generality.

Since $F(0) \in I^n$, then $F(x) \in I^n \ \forall x \in I^n$, so it is easily seen by induction that $w_m \in I^n \ \forall m \in \mathbb{N}$.

Moreover, we will show by indiction that $w_m \equiv w_{m+1} \mod I^{n+m} \ \forall m \in \mathbb{N}$. The base case $m = 1$ is equivalent to the assumption $F(0) = I^n$. For the general case, write

$$F(X) - F(Y) = (X - Y)\left(F'(0) + XG(X, Y) + YH(X, Y)\right)$$

where $G, H \in O[X, Y]$. Then,

$$\begin{aligned} &w_{m+1} - w_m = (w_m - w_{m-1}) - (F(w_m) - F(w_{m-1})) = \\ &(w_m - w_{m-1})\left[1 - F'(0) - w_m G(w_m, w_{m-1}) - w_{m-1}H(w_m, w_{m-1})\right] \end{aligned}$$

The assumptions that $F'(0) \equiv 1 \mod I$ and $w_{m-1}, w_m \in I$, together the induction hypothesis $w_m - w_{m-1} \in I^{n+m-1}$, guarantees that $w_{m+1} - w_m \in I^{n+m}$.

Thus (w_n) is a Cauchy sequence in the I-adic topology, so it converges to an element $b \in O$ since O is complete. Since F is continuous with this topology, by taking limits we see that $b = b - F(b)$, so $F(b) = 0$.

To show uniqueness, let $c \in I^n \setminus \{b\}$ such that $F(c) = 0$. Then,

$$0 = F(b) - F(c) = (b - c)\left[F'(0) + bG(b, c) + cH(b, c)\right]$$

Since $b \neq c$, then $F'(0)+bG(b,c)+cH(b,c) = 0$, what is a contradiction because $F'(0) \notin I^n$. □

2.2 The Weierstrass Preparation Theorem

The main goal of this section is to show a structure appearing on the rings of power series over complete discrete valuation rings. It can be considered as a preparation for the study of Iwasawa modules, which are finitely generated ones over $\mathbb{Z}_p[[T]]$.

The above mentioned result is Weierstrass preparation theorem, which gives a description of every element in $O[[T]]$. For that purpose, we need to define what is the reduced degree of a power series.

Definition 2.1. Let O be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$ and residue field $\kappa = O/\mathfrak{m}$ and let $f = \sum_{n=0}^{\infty} a_n T^n \in O[[T]]$. The *reduced degree* of f is

$$s := \inf\{n \in \mathbb{N} : \ a_n \notin \mathfrak{m}\}$$

In the proof of Weierstrass preparation lemma, the following result, known as division lemma, plays an important role.

Lemma 2.1. Let O be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$ and whose residue field κ is finite and let $g \in O[[T]]$ be an element of reduced degree s. Then every $f \in O[[T]]$ can be written uniquely as

$$f(t) = g(t)h(t) + r(t)$$

with $h \in O[[T]]$ and a polynomial $r \in O[T]$ of degree less than $s-1$. In particular, $O[[T]]/fO[[T]]$ is a free O-module of rank s whose basis is $\{T^i + (f)O[[T]] : \ i = 0, \ldots, s-1\}$.

We will proof this lemma at the end of this section. The description given in Weierstrass preparation theorem is based on a special kind of polynomials, which are defined below.

Definition 2.2. Let O be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$. A polynomial $F \in O[T]$ is called *Weierstrass polynomial* or *distinguished polynomial* if it is of the form

$$F = T^s + a_{s-1}T^{s-1} + \cdots + a_1 T + a_0$$

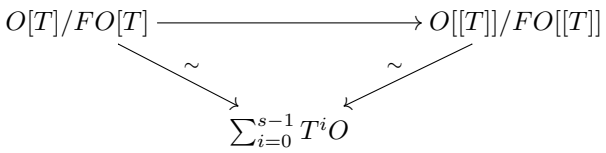
with $a_0, \ldots, a_{s-1} \in \mathfrak{m}$.

The importance of Weierstrass polynomials is that its residue ring is easily described due to the division lemma.

Corollary 2.1. Let O be a complete discrete valuation ring and let F be a Weierstrass polynomial. Then the injection $O[T] \hookrightarrow O[[T]]$ induces an isomorphism

$$O[T]/FO[T] \xrightarrow{\sim} O[[T]]/FO[[T]]$$

Proof. It comes from lemma 2.1 and the following commutative diagram:



□

Taking this background into account, we can state and proof the main result of this section.

Theorem 2.1. (Weierstrass Preparation Theorem) Let O be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$ and whose residue field is $\kappa = O/\mathfrak{m}$ and let $f \in O[[T]]$ have reduced degree s. Then there is a unique pair (u, g) such that $f(t) = u(t)g(t)$, $u \in O[[T]]^*$ and g is a Weierstrass polynomial of degree s.

Proof. By lemma 2.1, there is a unique $u \in O[[T]]$ and a unique polynomial $r(T) = \sum_{i=0}^{s-1} a_i T^i$ such that

$$T^s = f(T)u(T) - r(T)$$

Since f has reduced degree s then $\overline{a_i} = 0 \ \forall i = 0, \ldots, s-1$ and

$$T^s + \overline{a_{s-1}}T^{s-1} + \cdots + \overline{a_0} = \overline{f}(T) \cdot \overline{u}(T)$$

then the reduced degree of u is zero, so $u \in O[[T]]^*$. Then the existence is proven since $g(T) := T^s + r(T)$ is clearly a distinguished polynomial.

By corollary 2.1, $O[[T]]/(f(T)) \cong O[[T]]/(g(T)) \cong O[T]/(g(T))$ is a free $\mathbb{Z}_p$-module such that multiplication by T has minimal polynomial $g(T)$. This proves the uniqueness in the factorisation. □

Weierstrass preparation theorem can be understood as a structure theorem for the elements in $O[[T]]$.

Corollary 2.2. Let O be a complete discrete valuation ring and let π be a uniformizer. Then every $f \in O[[T]]$ can be written uniquely as

$$f(T) = \pi^m u(T) g(T)$$

where $m \in \mathbb{N}$, $u(T) \in O[[T]]^*$ and $g(T)$ is a Weierstrass polynomial.

Proof. It comes from theorem 2.1 after choosing

$$m = \min\{v(a_n) : n \in \mathbb{N}\}$$

where $f = \sum_{n=0}^{\infty} a_n T^n$. Thus $\pi^{-m} f$ has finite reduced degree and theorem 2.1 can be applied. □

As a consequence, we can show that $O[[T]]$ is a unique factorisation domain.

Corollary 2.3. Let O be a complete discrete valuation ring. Then power series ring $O[[T]]$ is a unique factorisation domain.

Proof. Since $O[T]$ is a unique factorisation domain, it is possible to express every distinguished polynomial as a product of monic irreducible elements in $O[T]$, being this decomposition unique. Since this decomposition reduces well to $k[[T]]$, the irreducible elements has to be Weierstrass polynomials. By theorem 2.1, they are also irreducible as elements of $O[[T]]$, so every element in $O[[T]]$ can be written as a product of irreducible ones because of corollary 2.2.

By corollary 2.2, we just need to check the uniqueness for distinguished polynomials. By theorem 2.1, we can assume that all decompositions consist of Weierstrass polynomials. Then the uniqueness of the factorisation in $O[T]$ guarantees the uniqueness in $O[[T]]$, so it is a unique factorisation domain.

□

We end this section by giving a proof of division lemma 2.1.

Proof of lemma 2.1. For the uniqueness, let $g(T)h(T) + r(T) = f(T) = g(T)h'(T) + r'(T)$. Then $s(T) = r'(T) - r(T)$ is divisible by $g(T)$ in $O[[T]]$. Let π be a prime element in O. If $s(T) \neq 0$, there are $m \in \mathbb{N}$ and $s_0(T) \in O[[T]] \setminus \pi O[[T]]$ such that $s(T) = \pi^m s_0(T)$. Since π is a prime element, and $g(T) \notin \pi(T)$, it is easy to see that $g(T)$ divides $s_0(T)$.

Consider the reduction map $O[[T]] \to \kappa[[T]] : \ f(T) \mapsto \widetilde{f}(T)$ consisting of reducing each coefficient modulo $\mathfrak{m}$. Since this reduction is a ring homomorphism, then $\widetilde{g}(T)$ divides $\widetilde{s_0}(T)$. However, this is imposible since the $\widetilde{s}_0(T)$ is a non-zero polynomial of degree less than the first non-vanishing coefficient of $\widetilde{g}(T)$. Hence, $s(T) = 0$, so $r(T) = r'(T)$ and, therefore, $h(T) = h'(T)$.

For the existence, we are going to use the fact that $\kappa[[T]]$ is a discrete valuation ring. For every $f \in O[[T]]$ we can write

$$\widetilde{f}(T) = T^s \left(\sum_{i=s}^{\infty} \widetilde{a_i} T^{s-i} \right) + \sum_{i=0}^{s-1} \widetilde{a_i} T^i$$

Since the reduced degree of $g(T)$ is s, then $\widetilde{g}(T)$ and T^s generate the same ideal, so $\widetilde{f}(t) = \widetilde{g}(t)\widetilde{h}(t) + \widetilde{r}(t)$, where $\widetilde{h}(T) \in \kappa[[T]]$ and $\widetilde{r}(T) \in \kappa[T]$ is a polynomial of degree less than s. We can lift this equation to $O[[T]]$ and obtain

$$f(T) = g(T)h_0(T) + r_0(T) + \pi f_1(T)$$

for some $f_1(T) \in O[[T]]$. We can do the same with $f_1(T)$ finding the existence of some $h_1(T), f_2(T) \in O[[T]]$ and $r_1(T) \in O[T]$ of degree less than s such that $f_1(T) = g(T)h_1(T) + r_1(T) + \pi f_2(T)$. Thus,

$$f(T) = g(T)\left(h_0(T) + \pi h_1(T)\right) + \left(r_0(T) + \pi r_1(T)\right) + \pi^2 f_2(T)$$

Doing that for every $n \in \mathbb{N}$ we get that

$$f(T) = g(T) \left(\sum_{i=0}^{n-1} \pi^i h_i(T) \right) + \left(\sum_{i=0}^{n-1} \pi^i r_i(T) \right) + \pi^n f_n(T)$$

The sequences of partial sums are Cauchy sequences, so we can define

$$h(t) = \sum_{i=0}^{\infty} \pi^i h_i(T), \quad r(T) = \sum_{i=0}^{\infty} r_i(T)$$

and they satisfy the equation $f(T) = g(T)h(T) + r(T)$. □

2.3 Modules up to Pseudo-Isomorphism

The main goal of this section is to prove the following structure theorem, which will be applied in next section to the case of Iwasawa modules, when $A = \mathbb{Z}_p[[T]]$.

Theorem 2.2. Let A be a Noetherian, integrally closed, 2-dimensional local ring whose maximal ideal has a minimal set of generators consisting of two elements. Then there exist finitely many prime ideals of height 1, $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\} \subset \mathcal{P}(A)$, nonnegative integers $r, r_i, n_{i_j} \in \mathbb{N} \cup \{0\}$ and a homomorphism with finite kernel and cokernel

$$f: \ M \xrightarrow{\approx} A^r \oplus \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{r_i} A/\mathfrak{p}_i^{n_{ij}}$$

The prime ideals $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ are determined by M since

$$r = \dim_K \ M \otimes_A K, \quad \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\} = \mathrm{supp}(M) \cap \mathcal{P}(A)$$

However, we are going develop the theory needed for the proof in a slightly more general version. From now on, let A be a commutative, noetherian and integrally closed local domain whose quotient field is K, but we will have to assume that A is regular of dimension 2 to complete the proof. First of all, it is useful to state a result from basic commutative algebra which is going to be needed.

Theorem 2.3. Let A be an integrally closed, noetherian domain and let $\mathcal{P}(A)$ be the set of prime ideals of height 1. Then

$$A = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} A_{\mathfrak{p}}$$

Proof. [16], Theorem 11.5 □

The notion of an homomorphism having finite kernel and cokernel is related to the concept of pseudo-isomorphism.

Definition 2.3. A finitely generated A-module M is called *pseudo-null* if $\mathrm{supp}(M) \cap \mathcal{P}(A) = \emptyset$ and $(0) \notin \mathrm{supp}(M)$.

Remark 2.1. If M is a finitely generated A-module, then

$$\mathrm{supp}(M) = V\left(\mathrm{Ann}_A(M)\right)$$

Remark 2.2. If A has Krull dimension equal to 2 then an A-module is pseudo-null if and only if it is finite. Indeed, providing that M is finite, then for each element $x \in M$, the quotient $A/\mathrm{Ann}_A(x)$ is finite, so it is also Artinian. Then there is some r_x such that $\mathfrak{m}^{r_x} \subset \mathrm{Ann}_A(x)$, where $\mathfrak{m}$ denotes the maximal ideal of A. Then there is some $r \in \mathbb{N}$ such that $\mathfrak{m}^r M = 0$. Since the only prime ideal in which $\mathfrak{m}^r$ is contained is $\mathfrak{m}$, then $M_{\mathfrak{p}} = \mathfrak{m}^r M_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$ of heigth 0 or 1. Therefore $\mathrm{supp}(M) \subset \{\mathfrak{m}\}$, so M is pseudo-null.

Conversely, if M is pseudo null then its support is contained in $\{\mathfrak{m}\}$ and, therefore, $\mathfrak{m} = \mathrm{rad}\left(\mathrm{Ann}_A(M)\right)$. Since $\mathfrak{m}$ is finitely generated, then $\mathfrak{m}^r \subset \mathrm{Ann}_A(M)$ for some $r \in \mathbb{N}$. Then M is a finitely generated $A/\mathfrak{m}^r$ module, so it is finite because so is $A/\mathfrak{m}^r$.

Definition 2.4. A homomorphism $f : M \to N$ of finitely generated A-modules is called a *pseudo-isomorphism* if $\ker(f)$ and $\operatorname{coker}(f)$ are pseudo-null A-modules. Equivalently, f is a pseudo-isomorphism if and only if

$$f_{\mathfrak{p}} : M_{\mathfrak{p}} \xrightarrow{\sim} N_{\mathfrak{p}}$$

is an isomorphism for every $\mathfrak{p} \in \mathcal{P}(A)$. We then write

$$f : M \xrightarrow{\approx} N$$

Lemma 2.2. Let M be a finitely generated A-torsion module and let $\alpha \in A$ be a non-zero element such that $\operatorname{supp}(A/\alpha A) \cap \operatorname{supp}(M) \cap \mathcal{P}(A) = \emptyset$. Then the multiplication on M by α is a pseudo-isomorphism.

Proof. For every $\mathfrak{p} \in \operatorname{supp}(M) \cap \mathcal{P}(A)$, then $\mathfrak{p} \notin \operatorname{supp}(A/\alpha A)$, so $A_{\mathfrak{p}}/\alpha A_{\mathfrak{p}} = (A/\alpha A)_{\mathfrak{p}} = 0$ and hence α is a unit in $A_{\mathfrak{p}}$. Therefore, multiplication by α induces an isomorphism in $A_{\mathfrak{p}}$.

For every $\mathfrak{p} \in \mathcal{P}(A) \backslash \operatorname{supp}(M)$, then $M_{\mathfrak{p}} = 0$, so multiplication by α also induces an isomorphism in $M_{\mathfrak{p}}$.

Finally, $M_{(0)} = M \otimes_A K = 0$ since M is A-torsion, so same argument applies. □

Now we want to classify the finitely generated A-modules up to pseudo-isomorphism. Due to next result, we can do that separately in the torsion and torsion-free parts.

Proposition 2.2. Let M be a finitely generated A-module, let $T_A(M)$ be the torsion submodule and let $F_A(M) = M/T_A(M)$ be the maximal torsion-free quotient of M. Then there is a pseudo-isomorphism

$$f : M \xrightarrow{\approx} T_A(M) \oplus F_A(M)$$

Proof. Since A is noetherian, then $T_A(M)$ is a finitely generated torsion module. Therefore, $\operatorname{Ann}_A(T_A(M)) \neq 0$. Then $\operatorname{supp}(T_A(M)) \cap \mathcal{P}(A)$ consits of some minimal primes of the set $V(\operatorname{Ann}_A(T_A(M)))$, so it is a finite set and we can write

$$\operatorname{supp}(T_A(M)) \cap \mathcal{P}(A) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$$

In case that $h = 0$, then $T_A(M)$ is pseudo-null, so the map

$$f : M \xrightarrow{\approx} T_A(M) \oplus F_A(m) : \ m \mapsto (0, \pi(m))$$

is a pseudo-isomorphism provided that π is the canonical projection.

If $h > 0$, consider the set $S = \bigcap_{i=1}^{h} \mathfrak{p}_i^c$. Then $S^{-1}A$ is a Dedekind domain with only finitely many prime ideals, so Chinese remainder theorem guarantees that it is a principal ideal domain.

The torsion part of $S^{-1}A$ is $S^{-1}T_A(M)$, so structure theorem for finitely generated modules over principal ideal domains says that it is a direct summand of $S^{-1}M$. Since M is finitely generated, we have that

$$\operatorname{Hom}_{S^{-1}A}\left(S^{-1}M, S^{-1}T_A(M)\right) = \operatorname{Hom}_A\left(M, S^{-1}T_A(M)\right) = S^{-1}\operatorname{Hom}_A\left(M, T_A(M)\right)$$

Thus there is a morphism $f_0 : \ M \to T_A(M)$ and $s_0 \in S$ such that

$$\frac{f_0}{s_0} : \ S^{-1}M \to S^{-1}T_A(M)$$

is the canonical projection. Then this map restricted to $S^{-1}T_A(M)$ is the identity, so there is some $s_1 \in S$ such that, defining $f_1 := s_1 f_0$, then

$$f_1\big|_{T_A(M)} = s_1 s_0 \ \mathrm{id}_{T_A(M)}$$

By lemma 2.2, $f_1\big|_{T_A(M)}$ is a pseudo-isomorphism. Considering

$$f = (f_1, \pi) : \ M \to T_A(M) \oplus F_A(M)$$

there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_A(M) & \longrightarrow & M & \longrightarrow & F_A(M) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1|_{T_A(M)}} & & \downarrow{\scriptstyle f} & & \downarrow & & \\ 0 & \longrightarrow & T_A(M) & \longrightarrow & T_A(M) \oplus F_A(M) & \longrightarrow & F_A(M) & \longrightarrow & 0 \end{array}$$

where the third vertical arrow is the identity. Snake's lemma, which is a well known result that will be detailed in lemma 6.3, shows that $\ker(f) \cong \ker(f_1)$ and $\operatorname{coker}(f) \cong \operatorname{coker}(f_1)$. Since f_1 is a pseudo-isomorphism from $T_A(M)$ to itself, both kernels and cokernels are pseudo-null and f is also an isomorphism. □

We can also use the structure theorem for finitely generated modules over a principal ideal domain in order to classify the A-torsion modules.

Proposition 2.3. Let M be a finitely generated torsion A-module. Then there exists a finite family of prime ideals $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\} \subset \mathcal{P}(A)$ and a pseudo-isomorphism

$$g : \ M \to \bigoplus_{i=1}^{h} \bigoplus^{r_i} A/\mathfrak{p}_i^{n_{ij}}$$

where n_{ij} are some natural numbers depending on M.

Proof. As in the proof of proposition 2.2, consider the finite set

$$\operatorname{supp}(M) \cap \mathcal{P}(A) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$$

In case $h = 0$, then the null map $M \to 0$ is a pseudo-isomorphism, so we can suppose that $h > 0$.

Again, let $S = \bigcap_{i=1}^{h} \mathfrak{p}_i^c$. Since $S^{-1}M$ is a torsion finitely generated module over the principal ideal domain $S^{-1}A$, whose prime ideals are $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$, then the structure theorem gives an isomorphism

$$g_0 : \ S^{-1}M \to \bigoplus_{i=1}^{h} \bigoplus^{r_i} S^{-1}A/S^{-1}\mathfrak{p}_i^{n_{ij}} = S^{-1}\left(\bigoplus_{i=1}^{h} \bigoplus^{r_i} A/\mathfrak{p}_i^{n_{ij}} \right)$$

where we have used that localisation is transitive. Since for every A-module E it is true that

$$\operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}E) = \operatorname{Hom}_A(M, S^{-1}E) = S^{-1}\operatorname{Hom}_A(M, E)$$

then there is an $s \in S$ and a morphism

$$g : M \to \bigoplus_{i=1}^{h} \bigoplus^{r_i} A/\mathfrak{p}_i^{n_{ij}}$$

such that $g = sg_0$. Then $S^{-1}g$ is an isomorphism, so it is easy to see that $\ker(g)$ and $\operatorname{coker}(g)$ are pseudo-null. In fact, given $\mathfrak{p} \in \operatorname{Supp}(M) \cap \mathcal{P}(A)$, $\ker(g)_{\mathfrak{p}} = \big(\ker(S^{-1}g)\big)_{S^{-1}\mathfrak{p}} = 0$ and $\operatorname{coker}(g)_{\mathfrak{p}} = \big(\operatorname{coker}(S^{-1}g)\big)_{S^{-1}\mathfrak{p}} = 0$. □

To study the torsion free parts, we need to introduce first the notion of reflexive module:

Definition 2.5. An A-module M is called *reflexive* if the canonical map

$$\varphi_M : M \to M^{**} = \mathrm{Hom}_A\left(\mathrm{Hom}_A\left(M, A\right), A\right) : \ m \mapsto \varphi_M(m) : \ \alpha \mapsto \alpha(m)$$

from M to its bidual is an isomorphism.

If M is a torsion-free finitely generated A-module, there are injections

$$M \hookrightarrow M_{\mathfrak{p}} \hookrightarrow M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K = M \otimes_A K =: V$$
$$M^* \hookrightarrow (M^*)_{\mathfrak{p}} \hookrightarrow (M^*)_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K = M^* \otimes_A K = \mathrm{Hom}_K(V, K) =: V^*$$

Then we can consider the dual spaces and its localisations as submodules of V^*. Moreover

$$(M^*)_{\mathfrak{p}} \cong \{\lambda \in V^* : \ \lambda(m) \in A_{\mathfrak{p}} \ \forall m \in M_{\mathfrak{p}}\} \cong (M_{\mathfrak{p}})^*$$

Lemma 2.3. Let M be a finitely generated torsion-free A-module. Then

1. $M^* = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M^*_{\mathfrak{p}}$
2. $M^{**} = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M_{\mathfrak{p}}$
3. $M = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M_{\mathfrak{p}}$ if and only if M is reflexive.

Proof. For the first part, let $\lambda \in \bigcap M^*_{\mathfrak{p}}$. Then for every $m \in M$ we get that $\lambda(m) \in A_{\mathfrak{p}}$ for every $\mathfrak{p} \in \mathcal{P}(A)$. Then, by theorem 2.3, $\lambda(M) \subset A$, so $\lambda \in M^*$.

For the second part, notice that $M_{\mathfrak{p}}$ is a torsion free finitely generated module over the principal ideal domain $A_{\mathfrak{p}}$, so the structure theorem states that it is free. Then it is clearly reflexive and the canonical map $M_{\mathfrak{p}} \to M^{**}_{\mathfrak{p}}$ is thus an isomorphism. Identifying $V = V^{**}$, due to the first part we have that

$$M^{**} = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M^{**}_{\mathfrak{p}} = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} M_{\mathfrak{p}}$$

The third part is clear from the second one. □

Corollary 2.4. If M is finitely generated, then M^* is reflexive.

Proposition 2.4. Let M be a finitely generated torsion-free A-module. Then there is an injective pseudo-isomorphism of M into a reflexive A-module.

Proof. The canonical map

$$\varphi_M : \ M \to M^{**}$$

is a pseudo-isomorphism because $M_{\mathfrak{p}}$ is a torsion-free finitely generated $A_{\mathfrak{p}}$-module for every $\mathfrak{p} \in \mathcal{P}(A) \cup \{0\}$. Since M is a quotient of A^r for some r, M^* is a subgroup of $(A^r)^* \cong A^r$, so it is finitely generated for being A^r Noetherian. Hence corollary 2.4 implies that M^{**} is reflexive.

Since $\ker(\varphi_M) \otimes_A K = 0$ for being φ_M a pseudo-isomorphism, then $\ker(\varphi_M)$ is torsion and therefore zero, because M is torsion-free. □

To complete the characterization of the torsion-free quotient we need to assume that A is regular of dimension 2.

Proposition 2.5. Let A be a Noetherian, integrally closed, 2-dimensional local domain whose maximal ideal has a minimal set of generators consisting of two elements, $m = p_1 A + p_2 A$. If M is a finitely generated A-module, the following statements are equivalent:

1. M is reflexive.
2. M is free.

Proof. In order to prove the non-trivial implication, assume M is reflexive. Since A/p_1A is an integral domain, $\mathrm{Hom}_A(M^*, A/p_1A)$ is a torsion-free A/p_1A module. The homomorphism

$$M^{**}/p_1M^{**} = \mathrm{Hom}_A(M^*, A) \otimes_A A/p_1A \hookrightarrow \mathrm{Hom}_A(M^*, A/p_1A)$$

is injective. Since M is reflexive then $M/p_1M \cong M^{**}/p_1M^{**}$ and it is a torsion free finitely generated module over the discrete valuation ring A/p_1A, so the structure theorem guarantees that M/p_1M is free.

Let $\varphi : A^r \twoheadrightarrow M$ be a minimal presentation of M and consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^r & \xrightarrow{p_1} & A^r & \longrightarrow & (A/p_1A)^r & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \overline{\varphi}} & & \\ 0 & \longrightarrow & M & \xrightarrow{p_1} & M & \longrightarrow & M/p_1M & \longrightarrow & 0 \end{array}$$

Since M/p_1M is free as an A/p_1A-module, Nakayama's lemma implies that its rank is r. Tensoring with the quotient field K_{p_1} of A/p_1A is an exact functor because it is also a localisation on the ideal (0).

$$0 \longrightarrow \ker(\overline{\varphi}) \otimes_{A/p_1} K_{p_1} \longrightarrow (A/p_1A)^r \otimes_{A/p_1} K_{p_1} \xrightarrow{\overline{\varphi}\otimes\mathrm{Id}} M/p_1M \otimes_{A/p_1} K_{p_1} \longrightarrow 0$$

Since $\overline{\varphi}\otimes\mathrm{Id}$ is a surjective linear map of K_{p_1} vector spaces of the same dimension, it is injective. It means that $\ker(\overline{\varphi})\otimes K_{p_1} = 0$. Since A/p_1A is a principal ideal domain, then $\ker(\varphi)$ is torsion free module of rank 0, so $\ker(\overline{\varphi}) = 0$.

Therefore, snake's lemma, which will be shown in lemma 6.3, implies that multiplication by p_1 is surjective in $\ker(\varphi)$, so $p_1 \ker(\varphi) = \ker(\varphi)$. Again, Nakayama's lemma implies that $\ker(\varphi) = 0$, so M is free. □

Taking all of these background into account, the proof of theorem 2.2 is complete.

Remark 2.3. The kernel of th pseudo-isomorphism of theorem 2.2 is the maximal finite submodule of M. In fact, elementary modules does not contain any non-trivial finite submodule, so every finite module of M has to be contained in the kernel.

2.4 The Structure Theorem of Iwasawa Modules

In this section we are going to particularise to the case we are interested in, which is $O = \mathbb{Z}_p$.

Definition 2.6. The group algebra $\Lambda = \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ is called the *Iwasawa algebra* and finitely generated Λ-module is called an *Iwasawa module.*

We want to apply theorem 2.2 to obtain the structure theorem for Iwasawa modules.

Theorem 2.4. Let M be an Iwasawa module. There are irreducible Weierstrass polynomials F_j, natural numbers r, m_i, n_j and a homomorphism

$$M \xrightarrow{\approx} \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/F_j^{n_j}$$

with finite kernel and cokernel. The numbers r, m_i, n_j and the Weierstrass polynomials are uniquely determined by M. A Λ-module of that form is called *elementary Iwasawa module.*

This theorem is the reason why we give the following definition. As we have mentioned in the introduction, these invariants can be used to control the growth of either the class number or the Tate-Shafarevich group in a $\mathbb{Z}_p$-extension.

Definition 2.7. Given a finitely generated Iwasawa module M, using notation of theorem 2.4 we define the following invariants:

- Λ-*rank of* M: $r(M) = \text{rank}_\Lambda(M) = r$.
- *Iwasawa* μ-*invariant*: $\mu(M) = \sum_{i=1}^{s} m_i$.
- *Iwasawa* λ-*invariant*: $\lambda(M) = \sum_{j=1}^{t} n_j \text{deg}(F_j)$.

Remark 2.4. The invariants r, μ and λ are additive functions since they are the can be computed using ranks of some localised modules over certain localised domains.

In order to proof theorem 2.4, we need to identify the prime ideals of $\mathbb{Z}_p[[T]]$.

Lemma 2.4. The prime ideals of heigth 1 of $\Lambda \cong \mathbb{Z}_p[[T]]$ are (p) and (F), where F is an irreducible Weierstrass polynomial over $\mathbb{Z}_p$.

Proof. Since Λ is a unique factorisation domain by corollary 2.3, the prime ideals of height one are those of the form $p = (f)$, where f is an irreducible element in Λ. Apart from (p), theorem 2.1 states that every prime ideal of height 1 can be written as $p = (F)$, where F is an irreducible Weierstrass polynomial. [1] □

With all of these background, theorem 2.2 implies theorem 2.4. Just the uniqueness part deserves a comment. However, two different Weierstrass polynomials cannot generate the same ideal because of the uniqueness part of theorem 2.1.

In order to apply theorem 2.4, we want to know when an Iwasawa module is finitely generated.

Proposition 2.6. Let M be an Iwasawa module. Then M is finitely generated if and only M/mM is a finitely generated $\mathbb{F}_p$-vector space. In that situation, the minimal number of generators of M as a Λ-module is $\dim_{\mathbb{F}_p}(M/mM)$.

Proof. If M is finitely generated, then $\dim_{\mathbb{F}_p}(M/mM)$ is clearly finite. Conversely, choose $m_1, \ldots, m_d \in M$ such that their images are a basis in M/mM and let $N = \Lambda m_1 + \cdots + \Lambda m_d$. Let X be a finitely generated sumbodule which contains N. Then

$$m\left(\frac{X}{N}\right) = \frac{mX + N}{N} = \frac{X}{N}$$

Thus Nakayama's lemma implies that $X/N = 0$, so $X = N$. Since that is true for every finitely generated submodule, then $M = N$. □

We can also use the structure theorem to study the growth of some relevant quotients of finitely generated Iwasawa modules. Before that, we need to consider a technical lemma.

Lemma 2.5. Let $f \in \mathbb{Z}_p[[T]]$ be a distinguished polynomial and let $M := \Lambda/(f(T))$. Then

$$\frac{w_{n+1}}{w_n} M = pM \quad \forall n > \frac{\lambda(\lambda - 1)}{2}$$

[1] Note that, by the proof of corollary 2.3, the irreducibility of a distinguished polynomial is equivalent in $\mathbb{Z}_p[T]$ and $\mathbb{Z}_p[[T]]$.

Proof. Consider the $\mathbb{F}_p$ vector space M/pM whose dimension is $\lambda = \deg(f)$. Multiplication by T is thus an endomorphism whose characteristic polynomial is X^λ and the endomorphism $T+1$ is represented by a matrix which is upper triangular and has 1 in every diagonal entry. Hence it belongs to a subgroup of order $p^{\frac{\lambda(\lambda-1)}{2}}$, so γ^{p^m} acts trivially on M/pM for $m \geq \frac{\lambda(\lambda-1)}{2}$. Now let $n > \frac{\lambda(\lambda-1)}{2}$ and let A be the matrix representing the action of γ on M as a $\mathbb{Z}_p$-module on the basis $\{1, T, \ldots, T^{\lambda-1}\}$. Then

$$A^{p^{n-1}} \equiv I \mod p \Rightarrow A^{p^n} \equiv I \mod p^2 \Rightarrow A^{p^n(p-1)} + \cdots + A^{p^n} + I \equiv pI \mod p^2$$

Hence there is some matrix $U \in GL_\lambda(\mathbb{Z}_p)$ such that

$$A^{p^n(p-1)} + \cdots + A^{p^n} + I = pU$$

Therefore,

$$\frac{w_{n+1}}{w_n} M = (\gamma^{p^n(p-1)} + \cdots + \gamma^{p^n} + 1)M = pM$$

□

Now we can control the growth certain quotients of some Iwasawa modules by using λ and μ invariants.

Proposition 2.7. Let M be a finitely generated torsion Λ-module with λ and μ the invariants given by the structure theorem. If M/w_nM if finite for all $n \in \mathbb{N}$, then

$$|M/w_nM| = p^{\mu p^n + \lambda n + O(1)}$$

Proof. Assume first that $M = E$ is a torsion elementary Λ-module. Hence

$$E \cong \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/F_j^{n_j}$$

For each factor, $E_i := \Lambda/p^{m_i}$, corollary 2.1 implies $E_i/w_nE_i = p^{m_i p^n}$. For the factors $E_j := \Lambda/F_j^{n_j}$, lemma 2.5 gives, for n large enough, an exact sequence

$$0 \longrightarrow E_j/w_n \xrightarrow{\frac{w_{n+1}}{w_n}} E_j/w_{n+1} \longrightarrow E_j/p \longrightarrow 0$$

Again corollary 2.1 implies that $|E_j/p| = p^{n_j \deg(F_j)}$, so for large enough n,

$$|E_j/w_{n+1}| = p^{n_j \deg(F_j)} |E_j/w_n|$$

Notice that E/w_n is a $\mathbb{Z}_p$ finite module, so its order has to be a power of p. Putting everything together, we have that

$$|E/w_n| = p^{\mu(E)p^n + \lambda(E)n + O(1)}$$

For the general case, let M_0 be the maximal finite submodule of M and let $N = M/M_0$. Then snake's lemma 6.3 below gives the following exact sequence

$$M_0/w_n \longrightarrow M/w_n \longrightarrow N/w_n \longrightarrow 0$$

Hence,

$$|N/w_n| \leq |M/w_n| \leq |N/w_n| \cdot |M_0|$$

Moreover, theorem 2.4 says there is an elementary Iwasawa module E and a finite Λ-module C such that the following sequence is exact:

$$0 \longrightarrow N \longrightarrow E \longrightarrow C \longrightarrow 0$$

Snake's lemma 6.3 gives thus an exact sequence

$$_{w_n}C \longrightarrow N/w_n \longrightarrow E/w_n \longrightarrow C/w_n \longrightarrow 0$$

where $_{w_n}C$ denotes the kernel of multiplication by w_n on C. Therefore,

$$\frac{1}{|C|} \leq \frac{1}{|C/w_n|} \leq \frac{|N/w_n|}{|E/w_n|} \leq |_{w_n}C| \leq |C|$$

Since the modules M_0 and C do not depend on n and taking into account that every finite $\mathbb{Z}_p$-module has an order which is a power of p, we get that

$$M/w_nM = p^{\mu(M)p^n+\lambda(M)n+O(1)}$$

□

Proposition 2.8. Let M be an Iwasawa module such that $M/w_0M = M/tM$ is a finitely generated $\mathbb{Z}_p$-module. Then M is a finitely generated Λ-module.

Moreover, if $\text{rank}_\Lambda M = r$, then $\text{rank}_{\mathbb{Z}_p} M/w_nM = rp^n + O(1)\ \forall n \in \mathbb{N}$, where $O(1)$ is always positive and bounded above by λ.

The converse is also true. If M is an Iwasawa module such that, for every $n \in \mathbb{N}$, M/w_n is a finitely generated $\mathbb{Z}_p$-module whose rank is $rp^n + O(1)$, then M is a Λ-module of rank r.

Proof. Clearly M/mM is finite, so proposition 2.6 implies that M is finitely generated. Assume first that $M = E$ is an elementary Iwasawa module. Then it is trivial that

$$E/w_nE \cong \mathbb{Z}_p^{rp^n} \oplus \bigoplus_{i=1}^{s} \left(\frac{\mathbb{Z}_p[[T]]}{p^{m_i}}\right)^{p^n} \oplus \bigoplus_{j=1}^{l} \frac{\mathbb{Z}_p[t]}{\left(F_j^{n_j}, w_n\right)}$$

Since every factor associated to the μ-invariant is $\mathbb{Z}_p$-torsion, they have no effect in the rank. Moreover, the factors associated to the λ-invariant have total rank bounded above by λ. Hence

$$\text{rank}_{\mathbb{Z}_p} E/w_nE = p^n \text{rank}_\Lambda E + O(1)$$

where $0 \leq O(1) \leq \lambda$.

For the general case, theorem 2.4 gives an exact sequence

$$0 \longrightarrow M_0 \longrightarrow M \longrightarrow E \longrightarrow C \longrightarrow 0$$

where M_0 and C are finite Λ-modules. Calling $N := M/M_0$, the exact sequence

$$M_0/w_n \longrightarrow M/w_n \longrightarrow N/n_w \longrightarrow 0$$

implies that $\text{rank}_{\mathbb{Z}_p}(M/w_n) = \text{rank}_{\mathbb{Z}_p}(N/w_n)$. Moreover, the exact sequence

$$_{w_n}C \longrightarrow N/w_n \longrightarrow E/w_n \longrightarrow C/w_n \longrightarrow 0$$

implies that $\text{rank}_{\mathbb{Z}_p}(N/w_n) = \text{rank}_{\mathbb{Z}_p}(E/w_n)$. Putting all together

$$\text{rank}_{\mathbb{Z}_p}(M/w_n) = \text{rank}_{\mathbb{Z}_p}(E/w_n) = rp^n + O(1)$$

where $0 \leq O(1) \leq \lambda$. □

The way we are going to encounter Iwasawa modules is as $\mathbb{Z}_p$-modules on which there is a continuous action by a group Γ, which is non-canonically isomorphic to $\mathbb{Z}_p$. This modules can be understood as $\mathbb{Z}_p[[\Gamma]]$-modules because of the following proposition.[2] However, we need to use the concept of inverse limit, which will be introduced rigorously in chapter 4,

Proposition 2.9. Assume that γ is a topological generator of $\Gamma \cong \mathbb{Z}_p$. Then the map

$$\mathbb{Z}_p[[T]] \xrightarrow{\sim} \mathbb{Z}_p[[\Gamma]] : \ T \mapsto \gamma - 1$$

Proof. Consider the distinguished polynomials

$$w_n = (T+1)^{p^n} - 1 = T^{p^n} + \sum_{i=1}^{p^n-1} \binom{p^n}{i} T^{p^n-i}$$

and let $\Gamma_n := \Gamma^{p^n} \subset \Gamma$ be the unique subgroup of index p^n. By corollary 2.1, we can consider the maps

$$\mathbb{Z}_p[[T]]/(w_n) \xrightarrow{\sim} \mathbb{Z}_p[T]/(w_n) \to \mathbb{Z}_p[\Gamma/\Gamma_n] : \ T + w_n\mathbb{Z}_p[[T]] \mapsto \gamma - 1 + \Gamma_n$$

which is an isomorphism of $\mathbb{Z}_p$-algebras, because its inverse is given by the map $\gamma + \Gamma_n \mapsto T + 1 + w_n\mathbb{Z}_p[[T]]$. Since $w_{n+1} \in w_n\mathbb{Z}_p[[T]]$, we can consider the following commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p[[T]]/(w_{n+1}) & \xrightarrow{\sim} & \mathbb{Z}_p[\Gamma/\Gamma_{n+1}] \\ \downarrow & & \downarrow \\ \mathbb{Z}_p[[T]]/(w_n) & \xrightarrow{\sim} & \mathbb{Z}_p[\Gamma/\Gamma_n] \end{array}$$

Then after taking limits we obtain the folllowing isomorphism

$$\varprojlim_n \mathbb{Z}_p[[T]]/(w_n) \xrightarrow{\sim} \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma_n] = \mathbb{Z}_p[[\Gamma]]$$

Then we just need to see that the natural homomorphism

$$\psi : \mathbb{Z}_p[[T]] \to \varprojlim_n \mathbb{Z}_p[[T]]/(w_n)$$

is an isomorphism. The injectivity comes from the fact that $w_n \in (p,T)^{n+1}$, so $\ker\psi = \bigcap_{n\in\mathbb{N}}(w_n) = \{0\}$. The surjectivity comes from the compactness of $\mathbb{Z}_p[[T]]$ with the (p,T)-adic topology, since each projection is surjective. Therefore, taking an element of the direct limit, the inverse image of each component by the projection is not empty and closed and finite intersections of them are also non-empty because the projections are compatible. Due to the compactness of $\mathbb{Z}_p[[T]]$, the intersection of the inverse images of all the projections is still not empty, so ψ is surjective. □

2.5 Localisation in Dedekind Domains

Throughout this section, let $\mathfrak{o}$ be a Dedekind domain and let K be its field of fractions. We want to study the localization of $\mathfrak{o}$ using a multiplicative S subset which will be the complement of a union $\bigcup_{\mathfrak{p}\in X}\mathfrak{p}$, where X is a set that contains every prime ideal of $\mathfrak{o}$ except a finite amount of them. In particular, our main goal will be tho show that the finiteness of the number of generators of the unit group and of the class number are conserved under this process.

[2] We consider these modules as $\mathbb{Z}_p[[\Gamma]]$-modules instead of $\mathbb{Z}_p[\Gamma]$-modules because of the compactness properties we obtain.

This process will be applied to the ring of integers of a number field and the localisation appears when we consider the elements having positive valuation for every prime but a finite amount of them. In this case, there are two important finiteness theorems from basic algebraic number theory and we will generalise them to the localised ring.

Theorem 2.5. (Dirichlet's Unit Theorem) Let $\mathfrak{o}$ be the ring of integers of a number field K. Then $\mathfrak{o}^*$ is a finitely generated group of rank $r+s-1$ and there is an isomorphism

$$\mathfrak{o}^* \cong \mathbb{Z}^{r+s-1} \times \mu_K$$

where μ_K is the finite subgroup formed by the roots of unity in K.

Proof. [21], Chap.I, Theorem 7.4. □

Theorem 2.6. Let K be a number field. Its class group is finite.

Proof. [21], Chap.I, Theorem 6.3. □

First of all, we need to see that the localised ring is still a Dedekind domain.

Proposition 2.10. If $\mathfrak{o}$ is a Dedekind domain and $S \subset \mathfrak{o} \setminus \{0\}$ is a multiplicative subset, then $S^{-1}\mathfrak{o}$ is also a Dedekind domain.

Proof. If $\mathfrak{a}$ is an ideal of $\mathfrak{o}$, then it has a finite set of generators, say $\{a_1, \dots, a_n\}$. Then, $\left\{\frac{a_1}{1}, \dots, \frac{a_n}{1}\right\}$ clearly generates $S^{-1}\mathfrak{a}$. Since every ideal of $S^{-1}\mathfrak{o}$ is an extended ideal, $S^{-1}\mathfrak{o}$ is Noetherian. Moreover, the bijection between prime ideals in $S^{-1}\mathfrak{o}$ and prime ideals in $\mathfrak{o}$ that does not meet S guarantees that every non-zero prime ideal in $S^{-1}\mathfrak{o}$ is maximal. Finally, $S^{-1}\mathfrak{o}$ is integrally closed. In fact, if some $x \in K$ satisfies the integral equation

$$x^n + \frac{a_1}{s_1}x^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

with coefficients $\frac{a_i}{s_i} \in S^{-1}\mathfrak{o}$, after multiplying by the n^{th} power of $s := s_1 \dots s_n \in S$, we would get an integral equation for sx with coefficients in $\mathfrak{o}$. That would mean that $sx \in \mathfrak{o}$, since it is integrally closed. It would be equivalent to $x = \frac{sx}{s} \in S^{-1}\mathfrak{o}$, so $S^{-1}\mathfrak{o}$ is integrally closed. □

As we stated above, we want to study the localization of a Dedekind domain under the complement of the union of almost every prime ideal in $\mathfrak{o}$. Since the Dedekind domains we are going to be interested in are the ring of integers of number fields, we are going to assume that the class number of $\mathfrak{o}$ is finite.

Proposition 2.11. Let $\mathfrak{o}$ be a Dedekind domain, let $X \subset \mathrm{Spec}(\mathfrak{o})$ be a set containing almost every prime ideal, and let $S = \bigcap_{\mathfrak{p} \in X} \mathfrak{p}^c$. If $Cl(\mathfrak{o})$ is a finite group, then there is a bijection

$$X \leftrightarrow \mathrm{Spec}\left(S^{-1}\mathfrak{o}\right) : \mathfrak{p} \mapsto S^{-1}\mathfrak{p}$$

Proof. From [1], proposition 3.11, the previous formula describes a bijection between prime ideals in $\mathrm{Spec}(\mathfrak{o})$ that does not meet S and prime ideal is $\mathrm{Spec}\left(S^{-1}\mathfrak{o}\right)$. Hence we just need to prove that the elements of X are precisely those prime ideals of $\mathfrak{o}$ that do not meet S.

It is clear that the elements of X does not meet S. Conversely, let $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{o})$ such that $\mathfrak{p} \cap S = \emptyset$. Then,

$$\mathfrak{p} \subset \bigcup_{\mathfrak{q} \in X} \mathfrak{q}$$

Let n be the class number of $\mathfrak{o}$. Thus $\mathfrak{p}^n$ is a principal ideal, which is generated by some $a \in \mathfrak{o}$. Then there is some $\mathfrak{q} \in X$ such that $a \in \mathfrak{q}$, so $\mathfrak{p}^n \subset \mathfrak{q}$. Since $\mathfrak{q}$ is a prime ideal, then $\mathfrak{p} \subset \mathfrak{q}$. Since $\mathfrak{o}$ is a Dedekind domain, both $\mathfrak{p}$ and $\mathfrak{q}$ are maximal ideals and $\mathfrak{p} = \mathfrak{q} \in X$. □

Remark 2.5. In the reference used [21], it is said that last result can be generalised to arbitrary Dedekind domains. However, that is not true because the finiteness of the class number is necessary.

There is a theorem due to Claborn, which is proven in [6], that states that every abelian is isomorphic to the class group of some Dedekind domain. Then there is a Dedekind domain $\mathfrak{o}$ and a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^n$ is not principal for any $n \in \mathbb{N}$.

For every $x \in \mathfrak{p}$, the ideal (x) has a factorisation containing some prime ideal different from $\mathfrak{p}$. Hence x is contained in some prime ideal different from p. Then we have a counter example to proposition 2.11 without assuming the finiteness of the class number, since

$$\mathfrak{p} \subset \bigcup_{\mathfrak{q} \in \mathrm{Spec}(\mathfrak{o}) \setminus \{\mathfrak{p}\}} \mathfrak{q}$$

Next statements we are going to show are the facts that the finiteness in the rank of the group of units and in the call number are conserved after localising. We will deduce its properties from the following exact sequence.

Proposition 2.12. Let $\mathfrak{o}$ be a Dedekind domain whose class number is finite. Then there is a canonical exact sequence

$$1 \longrightarrow \mathfrak{o}^* \longrightarrow \mathfrak{o}(X)^* \longrightarrow \bigoplus_{\mathfrak{p} \notin X} K^*/\mathfrak{o}_\mathfrak{p}^* \longrightarrow Cl(\mathfrak{o}) \longrightarrow Cl(\mathfrak{o}(X)) \longrightarrow 1$$

Proof. The first arrow is clearly an inclusion and the second one is induced by the maps $\mathfrak{o}(X)^* \hookrightarrow K^* \twoheadrightarrow K^*/\mathfrak{o}_\mathfrak{p}^*$. It is clear that every unit of $\mathfrak{o}$ is a unit in $\mathfrak{o}_\mathfrak{p}$ for every prime $\mathfrak{p}$, so it belongs to the kernel. Conversely, if $a \in \mathfrak{o}(X)^*$ belongs to the kernel, then $a \in \mathfrak{o}_\mathfrak{p}^* \ \forall \mathfrak{p} \notin X$. Since localisation is transitive, $a \in \mathfrak{o}(X)_{\mathfrak{p}_X}^* = \mathfrak{o}_\mathfrak{p}^*$, where $\mathfrak{p}_X$ is the extended ideal of $\mathfrak{p} \in X$. Then,

$$a, a^{-1} \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(\mathfrak{o})} \mathfrak{o}_\mathfrak{p} = \mathfrak{o} \Rightarrow a \in \mathfrak{o}^*$$

Thus the sequence is exact at $\mathfrak{o}(X)^*$. The third arrow is induced by the mapping

$$\bigoplus_{\mathfrak{p} \notin X} K^*/\mathfrak{o}_\mathfrak{p}^* \to Cl(\mathfrak{o}) : \ \bigoplus_{\mathfrak{p} \notin X} \alpha_\mathfrak{p} \mod o_\mathfrak{p}^* \mapsto \prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$$

where $v_\mathfrak{p}$ is the exponential valuation associated to the prime ideal $\mathfrak{p}$. Let $(\alpha_\mathfrak{p})_{\mathfrak{p} \notin X}$ be an element in the kernel, so it is mapped to a principal ideal. Then,

$$\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} = \alpha\mathfrak{o} = \prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha)}$$

Then $v_\mathfrak{p}(\alpha) = 0 \ \forall \mathfrak{p} \in X$ and $v_\mathfrak{p}(\alpha_\mathfrak{p}) = v_\mathfrak{p}(\alpha) \ \forall \mathfrak{p} \notin X$. It thus follows from proposition 2.5 that $\alpha \in \bigcap_{\mathfrak{p} \in X} \mathfrak{o}_\mathfrak{p}^* = \bigcap_{\mathfrak{p} \in X} \mathfrak{o}(X)_{\mathfrak{p}_X}^* = \mathfrak{o}(X)^*$. Furthermore, $\alpha \equiv \alpha_\mathfrak{p} \mod \mathfrak{o}_\mathfrak{p}^*$, which shows exactness at $\bigoplus_{\mathfrak{p} \notin X} K^*/\mathfrak{o}_\mathfrak{p}^*$, since the other inclusion is trivial.

Last arrow is defined by the map

$$Cl(\mathfrak{o}) \to Cl(\mathfrak{o}(X)) : \ \mathfrak{a} \mapsto \mathfrak{a} \cdot \mathfrak{o}(X)$$

which is clearly well defined because principal ideals are mapped to principal ideals. Due to proposition 2.5, the kernel of this map is the set of ideals whose factorisation into primes contains only elements out of X, which is clearly the image of the previous map, so the sequence is exact at $Cl(\mathfrak{o})$. Last arrow is also clearly surjective because every ideal in $\mathfrak{o}(X)$ is an extended ideal, so the exactness at $Cl(\mathfrak{o}(X))$ is satisfied. □

Corollary 2.5. Let $\mathfrak{o}$ be a Dedekind domain and let X be a set containing almost every prime ideal in $\mathfrak{o}$. If the class number of $\mathfrak{o}$ is finite, then the class number of $\mathfrak{o}(X)$ is also finite.

Corollary 2.6. Let $\mathfrak{o}$ be a Dedekind domain whose class number is finite and let $X \subset \mathrm{Spec}(\mathfrak{o})$ be such that $\mathrm{Spec}(\mathfrak{o}) \setminus X$ is a finite set containing a representative of every class of prime ideals in $\mathfrak{o}$, then $Cl\left(\mathfrak{o}(X)\right) = \{1\}$.

Proof. It follows from proposition 2.12 and the fact that the map

$$\bigoplus_{p \notin X} K^*/\mathfrak{o}_p^* \to Cl(\mathfrak{o})$$

is in this case surjective. □

Corollary 2.7. Let $\mathfrak{o}$ be a Dedekind domain whose class number is finite and let X be a set containing almost every prime ideal in $\mathfrak{o}$. Then the rank of $\mathfrak{o}(X)^*$ is finite and we have the equality

$$\mathrm{rank}\left(\mathfrak{o}(X)^*\right) = \mathrm{rank}\left(\mathfrak{o}^*\right) + \#\left(\mathrm{Spec}(\mathfrak{o}) \setminus X\right)$$

Proof. It follows from proposition 2.12 and the facts that rank is an additive function and that both class groups $Cl\left(\mathfrak{o}\right)$ and $Cl\left(\mathfrak{o}(X)\right)$ are finite. □

Chapter 3

Formal Groups

The content of this chapter is an introduction to the theory of formal groups. They arise naturally when studying the arithmetic of elliptic curves and one try to express the group operation as a power series of the coordinates.

The group operation defined on an elliptic curve is generally difficult to compute and the formulas usually consider several cases. A different approach to that computation is expressing the group operation as a power series of the coordinates. This is the content of section 3.5 and has the advantage that a single power series can be used to calculate every sum, having no necessity of considering several cases. However, one must be warned that this is just a formal expression, although convergence would be guaranteed in several cases, like sums in the kernel of the reduction map defined on an elliptic curve over a local field.

That is the reason why we define formal groups in section 3.1, which are a generalisation of the notion of a group in which we are just considering the operation but not the elements in the group. Some formal groups have associated groups, which are introduced in section 3.2. Section 3.3 is dedicated to the concept on invariant differential, which is an analogue to that concept in an elliptic curve. Finally, formal logarithm is considered in 3.4, which will be useful for studying the Mordell-Weil group in an elliptic curve defined over a local field.

Although this is a pretty technical chapter, its conclusions would imply interesting properties related to the arithmetic of elliptic curves defined over local fields. The reference used for this chapter has been chapter IV of [27].

3.1 The Definition of Formal Groups

Formal groups are a generalization of the definition of abelian groups in which we are just considering the operation and we are not considering the group elements.

Definition 3.1. Let R be a ring. A *formal group* $\mathcal{F}$ over R is a power series $F(X,Y) \in R[[X,Y]]$ with no constant term satisfying the following properties:

- Neutral element: $F(X,0) = X$; $F(0,Y) = Y$.
- Associativity: $F(X,F(Y,Z)) = F(F(X,Y),Z)$.
- Commutativity: $F(X,Y) = F(Y,X)$.
- Inverse element: $\exists!\ i(T) \in R[[T]]$ having no constant term such that $F(T,i(T)) = 0$.

Remark 3.1. The composition of two power series in $R[[t]]$ could not be well defined. However, the fact that the power series in the previous definition have no constant term ensures that

those compositions are well defined since the computation of each term in the composition involves only a finite sum.

Remark 3.2. The neutral element condition implies that

$$F(X,Y) = X + Y + \cdots$$

Now we show the most basic examples of formal groups. However, more interesting examples will appear in section 3.5 when talking about multiplication on elliptic curves.

Example 3.1. The *formal additive group*, denoted by $\mathcal{G}_a$, is defined by

$$G_a(X,Y) = X + Y$$

Example 3.2. The *formal multiplicative group*, denoted by $\mathcal{G}_m$, is defined by

$$G_m(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$$

We can also extend the definition of homomorphism between groups to the case of formal groups.

Definition 3.2. Let $(\mathcal{F}, F)$ and $(\mathcal{G}, G)$ be formal groups defined over R. A *homomorphism* from $\mathcal{F}$ to $\mathcal{G}$ defined over R is a power series $f \in R[[t]]$ such that

$$f\left(F(X,Y)\right) = G(f(X), f(Y))$$

Furthermore, two formal groups $(\mathcal{F}, F)$ and $(\mathcal{G}, G)$ are called *isomorphic* if there are formal group homomorphisms $f : \mathcal{F} \to \mathcal{G}$ and $g : \mathcal{G} \to \mathcal{F}$ such that

$$f(g(T)) = g(f(T)) = T$$

Definition 3.3. Let $(\mathcal{F}, F)$ be a formal group. We define the homomorphisms $[m] : \mathcal{F} \to \mathcal{F}$ inductively for $m \in \mathbb{Z}$ by

$$[0](T) = 0, \quad [m+1](T) := F([m](T), T), \quad [m-1](T) := F([m]T, i(T))$$

These induction is well defined since after doing a step up and another one down, and vice versa, we get the same power series since

$$F([m+1](T), i(T)) = F(F([m](T), T), i(T)) = F([m](T), F(T, i(T))) = F([m](T), 0) = [m](T)$$
$$F([m-1](T), T) = F(F([m](T), i(T)), T) = F([m](T), F(i(T), T)) = F([m](T), 0) = [m](T)$$

We will also use induction to prove that $[m]$ are formal group homomorphisms. For $m = 0$, that is clear. For $m > 0$, assuming that $[m-1]$ is a formal group homomorphism, we see that

$$[m](F(X,Y)) = F([m-1](F(X,Y)), F(X,Y)) = F(F([m-1](X), [m-1](Y)), F(X,Y)) =$$
$$F([m-1](X), F([m-1](Y), F(X,Y))) = F([m-1](X), F(X, F([m-1](Y), Y))) =$$
$$F([m-1](X), F(X, [m](Y))) = F(F([m-1](X), X), [m](Y)) = F([m](X), [m](Y))$$

so $[m]$ is a formal group homomorphism $\forall m \geq 0$ since it is clearly a power series without constant term.

Induction for negative numbers can be written as follows. Assuming that $[m+1]$ is a formal group homomorphism we get that

$$\begin{aligned}
&[m](F(X,Y)) = F([m+1](F(X,Y)), i(F(X,Y))) = \\
&F(F([m+1](X),[m+1](Y)), i(F(X,Y))) = \\
&F(F(F([m](X),X),F([m](Y),Y)), i(F(X,Y))) = \\
&F(F([m](X),F(X,F([m](Y),Y))), i(F(X,Y))) = \\
&F(F([m](X),F([m](Y),F(X,Y))), i(F(X,Y))) = \\
&F(F([m](X),[m](Y),F(X,Y)), i(F(X,Y))) = \\
&F(F([m](X),[m](Y)),F(F(X,Y),i(F(X,Y)))) = \\
&F(F([m](X),[m]Y),0) = F([m](X),[m](Y))
\end{aligned}$$

Remark 3.3. By induction, it is also easily proved that the first non-constant term in the power series of $[m]$ takes value m, i.e.,

$$[m]'(0) = m$$

Now we want to study in which cases multiplication by m is an isomorphism.

Lemma 3.1. Let $a \in R^*$ and let $f(T) \in R[[T]]$ be a power series such that $f(0) = 0$ and $f'(0) = a$. Then there is a unique power series $g(T) \in R[[T]]$ with no constant term satisfying that

$$f(g(T)) = T$$

This series $g(T)$ also satisfies that $g(f(T)) = T$.

Proof. We want to construct a sequence of polynomials $g_n(T) \in R[T]$ such that

$$f(g_n(T)) \equiv T \mod (T^{n+1}), \quad g_{n+1}(T) \equiv g_n(T) \mod (T^{n+1})$$

By induction, let $g_1(T) := a^{-1}T$. Assuming that $g_{n-1}(T)$ has been constructed there is some $b \in R$ such that $f(g_{n-1}(T)) = T + bT^n \mod (T^{n+1})$. Then, let $g_n(T) := g_{n-1}(T) - a^{-1}bT^n$. Then,

$$f(g_n(T)) = f(g_{n-1}(T) - a^{-1}bT^n) \equiv f(g_{n-1}(T)) - aa^{-1}bT^n \equiv T + bT^n - bT^n \equiv T \mod (T^{n+1})$$

Then $(g_n) \subset R[[T]]$ is a Cauchy sequence in the (T)-adic topology, so by completeness it converges to some $g(T)$. Left composition with f is a continuous function in that topology so

$$f(g(T)) = \lim_{n\to\infty} f(g_n(T)) = T$$

Clearly, $g(0) = 0$ and $g'(0) = a^{-1} \in R^*$, so we can apply to g what we have just proven and deduce the existence of some $h \in R[[T]]$ such that $g(h(T)) = T$. Then

$$g(f(T)) = g(f(g(h(T)))) = g(f \circ g(h(t))) = g(h(T)) = T$$

To see that $g(T)$ is unique, suppose that $G(T) \in R[[T]]$ is another power series satisfying that $f(G(T)) = T$. Then

$$g(T) = g(f(G(T))) = (g \circ f)(G(T)) = G(T)$$

□

Proposition 3.1. Let $(\mathcal{F}, F)$ and $(\mathcal{G}, G)$ formal groups over R and let $a \in R^*$. If $f : \mathcal{F} \to \mathcal{G}$ is an homomorphism such that $f'(0) = a$, then f is an isomorphism.

Proof. By lemma 3.1, there exists a power series $g \in R[[t]]$ such that $g(f(T)) = f(g(T))$. We just need to check that $g : \mathcal{G} \to \mathcal{F}$ is a homomorphism between these formal groups. Since f is a homomorphism,

$$F(g(X), g(Y)) = (g \circ f)(F(g(X), g(Y))) = g(G((f \circ g)(X), (f \circ g)(Y))) = g(G(X, Y))$$

so $g : \mathcal{G} \to \mathcal{F}$ is also a homomorphism. □

Corollary 3.1. Let $\mathcal{F}$ be a formal group over R. If $m \in R^*$, then $[m] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.

3.2 The Groups Associated to Formal Groups

In case R is a complete local ring, a formal group has associated a canonical group by considering the elements of the maximal ideal with the operation defined in definition 3.1.

Definition 3.4. Let $(\mathcal{F}, F)$ be a formal group over a local ring $(R, \mathfrak{m})$ which is complete with respect to the $\mathfrak{m}$-adic topology. Then the *group associated to* $\mathcal{F}/R$, which is denoted by $\mathcal{F}(\mathfrak{m})$, is the set $\mathfrak{m}$ endowed with the group operation

$$x \oplus_{\mathcal{F}} y := F(x, y) \quad [1]$$

With this operation, $0 \in \mathfrak{m}$ is the neutral element and given some $x \in \mathfrak{m}$, its inverse is

$$\ominus_{\mathcal{F}} x = i(x)$$

Remark 3.4. Given two formal groups $\mathcal{F}$ and $\mathcal{G}$ defined over R and a homomorphism $f : \mathcal{F} \to \mathcal{G}$, then map

$$\mathfrak{m} \to \mathfrak{m} : \ x \mapsto f(x)$$

is an homomorphism between their associated groups.

Remark 3.5. The associated group $\mathcal{F}(\mathfrak{m})$ has an important filtration of subgroups

$$\mathcal{F}(\mathfrak{m}) \supset \mathcal{F}(\mathfrak{m}^2) \supset \mathcal{F}(\mathfrak{m}^3) \cdots$$

Remark 3.2 implies that

$$\mathcal{F}(\mathfrak{m}^n)/\mathcal{F}(\mathfrak{m}^{n+1}) \cong \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

Example 3.3. The associated group $\mathcal{G}_a(\mathfrak{m})$ is just $\mathfrak{m}$ with the usual addition. On the other hand, $\mathcal{G}_m(\mathfrak{m})$ is the set $1 + \mathfrak{m}$ with the usual multiplication.

Proposition 3.2. Let $\mathcal{F}$ be a formal group defined over a complete local ring R and let p be the characteristic of the residue field $\kappa = R/\mathfrak{m}$. Then every element of finite order in $\mathcal{F}(\mathfrak{m})$ has an order that is a power of p.

Proof. Let $m \in \mathbb{N}$ such that $m \notin p\mathbb{Z}$ and let $x \in m$ such that $[m]x = 0$. By corollary 3.1, $[m]$ was an automorphism of the formal group, so its associated group homomorphism has to be an isomorphism of the associated group. Then, $\ker[m] = \{0\}$, so $\mathcal{F}(\mathfrak{m})$ has no non-trivial m-torsion elements.

Now let $n = p^r m$, where $r, m \in \mathbb{N}$, $m > 1$ and $p \nmid m$. If the associated group had an element x of order n, then $p^r x$ would have order m, which contradicts what was proven above. □

[1] This operation is well defined since F has no constant term and it converges because R is complete with the m-adic topology.

When we have defined the associated group of a formal group, we have chosen the elements of the maximal ideal $\mathfrak{m}$ of R to be the elements of the associated group. However, if R is the ring of integers of a complete field K with respect to a valuation and $L|K$ is a field extension, we can also consider the elements of the maximal ideal $\mathfrak{m}_L$ of the ring of integers R_L of L to be the elements of the associated group. In particular, when choosing $L = \overline{K}$ we get very interesting properties of divisibility.

Nevertheless, one should be careful to check that all the power series converge. However, that is not a problem in this case. For instance, given $x, y \in \overline{\mathfrak{m}}$, then $F(x, y)$ is a power series in the ring of integers of $K(x, y)$, which is a finite extension of K. Hence $K(x, y)$ is still a complete field, so convergence is guaranteed in this case.

Lemma 3.2. Let K be a complete field with respect to a discrete valuation, let R be its ring of integers, let $\overline{R}$ be the ring of integers in the algebraic closure $\overline{K}$ and let $\overline{\mathfrak{m}}$ be its maximal ideal. Assume that $\mathcal{F}$ has finite height, i.e., $[p] \notin \pi R[[T]]$, where $p = \mathrm{char}(R/\mathfrak{m})$ and π is a uniformizer in R. Then, given formal group $\mathcal{F}$ defined over R, $\mathcal{F}(\overline{\mathfrak{m}})$ is $[p]$-divisible, i.e., for every $x \in \mathcal{F}(\overline{\mathfrak{m}})$, there is some $y \in \mathcal{F}(\overline{\mathfrak{m}})$ such that $[p]y = x$.

Proof. Let $x \in \mathcal{F}(\overline{\mathfrak{m}})$, let $L = K(x)$ and let R_L be its ring of integers. Applying corollary 2.2 to $[p](T) - x \in R_L[[T]]$, we find some $u \in R_L[[T]]^*$ and a Weierstrass polynomial $g \in R_L[T]$ such that $[p](T) - x = \pi_L^m \cdot u \cdot g$ for some $m \geq 0$ and where π_L is a uniformizer in R_L. Since $[p] \notin \pi R[[T]]$ and $x \in \mathfrak{m}_L$, then $m = 0$ and g has positive degree. Let then $y \in \overline{K}$ be a root of g. Clearly, $y \in \overline{\mathfrak{m}}$ because, otherwise, the leading term in $g(y) = 0$ will have strictly less valuation than the others, which is not possible due to the ultrametric inequality. Then

$$[p]y - x = \pi^m \cdot u(y) \cdot g(y) = 0 \Rightarrow [p]y = x$$

□

Corollary 3.2. Let K be a complete field with respect to a discrete valuation, let R be its ring of integers, let $\overline{R}$ be the ring of integers in the algebraic closure $\overline{K}$ and let $\overline{\mathfrak{m}}$ be its maximal ideal. Given formal group $\mathcal{F}$ of finite height defined over R, then $\mathcal{F}(\overline{\mathfrak{m}})$ is divisible.

Proof. We just need to see that $\mathcal{F}(\overline{\mathfrak{m}})$ is $[l]$-divisible for every prime number $l \in \mathbb{Z}$. If $l = \mathrm{char}(k)$, then lemma 3.2 applies. On the other hand, if $l \neq \mathrm{char}(k)$, then $l \in R^*$, so corollary 3.1 states that $[l]$ is an isomorphism. □

3.3 The Invariant Differential

This section is dedicated to the notion of invariant differential in a formal group. It is just a formal expression of a differential form which has its name because of its analogy with the invariant differential ω of an elliptic curve. That differential satisfies the property

$$\omega(P + Q) = \omega(P) \ \forall P, Q \in E$$

and that is the reason why we give the following definition.

Definition 3.5. An *invariant differential* on a formal group $\mathcal{F}$ defined over R is a formal expression

$$w(T) = P(T)dT \in R[[t]]dT$$

satisfying that

$$P(F(T, S))F_X(T, S) = P(T) \tag{3.1}$$

where F_X denotes the formal derivative of F with respect to the first variable. Last identity will be sometimes written as $(\omega \circ F)(T, S) = \omega(T)$.

Moreover, we will say that an invariant differential is *normalised* if $P(0) = 1$.

Proposition 3.3. Given a formal group $(\mathcal{F}, F)$ over R, there is a unique normalised invariant differential, which is given by the formula

$$\omega = F_X(0,T)^{-1}\, dT$$

Proof. Let $\omega = P(T)dT$ be a normalized invariant differential. Substituting $T = 0$ in equation 3.1, we get that

$$P(S)F_X(0,S) = P(0) = 1 \Rightarrow P(T) = F_X(0,T)^{-1} \Rightarrow \omega = F_X(0,T)^{-1}\, dT$$

Then we have just seen the uniqueness. For the existence, we just need to see the previous formula describes an invariant differential. Considering the associative law and differentiating it with respect to U, we get that

$$F(U,F(T,S)) = F(F(U,T),S) \Rightarrow F_X(U,F(T,S)) = F_X(F(U,T),S)F_X(U,T)$$

Substituting $U = 0$,

$$F_X(0,F(T,S)) = F_X(T,S)F_X(0,T) \Rightarrow F_X(0,F(T,S))^{-1}F_X(T,S) = F_X(0,T)^{-1}$$

Hence $\omega = F_X(0,T)^{-1}dT$ is an invariant differential. □

Corollary 3.3. Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups defined over R and let ω_F and ω_G be their invariant differentials. Let $f : \mathcal{F} \to \mathcal{G}$ be a homomorphism. Then

$$\omega_G \circ f = f'(0)\omega_F$$

Proof. Since f is a homomorphism and ω_G is $\mathcal{G}$-invariant,

$$(\omega_G \circ f)(F(T,S)) = (\omega_G \circ G)(f(T), f(S)) = \omega_G(f(T)) = (\omega_G \circ f)(T)$$

Then $\omega_G \circ f$ is $\mathcal{F}$-invariant and, by proposition 3.3, $\omega_G \circ f$ and ω_F are proportional. Comparing the constant coefficients, $\omega_G \circ f = f'(0)\omega_F$. □

Last result is useful to describe as power series the multiplications by prime numbers in a formal group.

Corollary 3.4. Let $(\mathcal{F}, F)$ be a formal group over R and let $p \in \mathbb{Z}$ be a prime number. Then there are power series $f(T), g(T) \in R[[t]]$ with $f(0) = g(0) = 0$ such that

$$[p](T) = pf(T) + g(T^p)$$

Proof. Since $[p] : \mathcal{F} \to \mathcal{F}$ is a homomorphism, corollary 3.3 implies that

$$pP(T)dT = p\omega(T) = \omega \circ [p](T) = P([p](T))[p]'(T)dT$$

Because $P(0) = 1$, $P([p](T))$ is invertible in $R[[T]]$, so $[p]'(T) \in pR[[T]]$. Therefore every term aT^n in the series $[p](T)$ satisfies that $na \in pR$, so either $a \in pR$ or $p|n$. □

Now we can state a bound in the valuation of the torsion elements in the associated group. Notice that proposition 3.2 implies that the order of every torsion element is a power of the characteristic of the ring.

Theorem 3.1. Let R be a discrete valuation ring that is complete with respect to its maximal ideal $\mathfrak{m}$, let $p = \mathrm{char}(R/\mathfrak{m}) > 0$ and let v be the valuation on R. Let $\mathcal{F}/R$ be a formal group and suppose that $x \in \mathcal{F}(\mathfrak{m})$ has order p^n, for some $n \in \mathbb{N}$. Then,

$$v(x) \leq \frac{v(p)}{p^n - p^{n-1}}$$

Proof. We can assume that $\mathrm{char}(R) > 0$, since the other case is trivial by proposition 3.2. We are going to proceed by induction on n. For $n = 1$, corollary 3.4 implies that there are powers series $f(T), g(T) \in R[[T]]$ such that

$$0 = pf(x) + g(x^p)$$

By remark 3.3, the leading term of f is T, so the only possibility for the leading term of $pf(x)$ to be cancelled is that

$$v(px) \geq v(x^p) \Leftrightarrow v(p) \geq (p-1)v(x) \Leftrightarrow v(x) \leq \frac{v(p)}{p-1}$$

For the general case, assume the theorem is true for n and let $x \in \mathcal{F}(\mathfrak{m})$ be a torsion element whose order is p^{n+1}. Since $[p](x)$ has order p^n, induction hypothesis guarantees that

$$\frac{v(p)}{p^n - p^{n-1}} \geq v\left([p](x)\right) = v\left(pf(x) + g(x^p)\right) \geq \min\left\{v(px), v(x^p)\right\}$$

Since $v(x) > 0$, then $v(px) > v(p)$, so the only possibility is that

$$\frac{v(p)}{p^n - p^{n-1}} \geq v(x^p) = pv(x) \Leftrightarrow v(x) \leq \frac{v(p)}{p^{n+1} - p^n}$$

□

3.4 The Formal Logarithm

Another important property of the invariant differential is that its formal integral, which is commonly known as the formal logarithm, gives an isomorphism between our formal group and the additive formal group. Even though formal logarithm is not an isomorphism in the sense of definition 3.2, since the formal integral is a power series with coefficients in $R \otimes \mathbb{Q}$ instead of R, it is an isomorphism when considered the formal groups as defined over $R \otimes \mathbb{Q}$.

Last condition is not enough to be sure that the formal logarithm defines an isomorphism between the associated subgroups in case our formal group is defined over a discrete valuation ring. Nevertheless, we will see that $\log_{\mathcal{F}}(x)$ converges provided that $v(x)$ is large enough, so it defines an isomorphism between the associated subgroups $\mathcal{F}(\mathfrak{m}^r)$ and $\mathcal{G}_a(\mathfrak{m}^r) = (\mathfrak{m}^r, +)$ for some $r \in \mathbb{N}$.

Definition 3.6. Let R be a ring such that its additive group is torsion-free and let $K := R \otimes \mathbb{Q}$. Let $\mathcal{F}$ be a formal group defined over R and let

$$\omega(T) = (1 + c_1 T + c_2 T^2 + \cdots)\, dT$$

be its normalized invariant differential. The *formal logarithm* of $\mathcal{F}$ is the power series

$$\log_{\mathcal{F}}(T) = \int \omega(T) := T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \cdots \in K[[T]]$$

The *formal exponential* of $\mathcal{F}$ is the unique power series $\exp_{\mathcal{F}}(T) \in K[[T]]$ satisfying

$$\log_{\mathcal{F}} \circ \exp_{\mathcal{F}}(T) = \exp_{\mathcal{F}} \circ \log_{\mathcal{F}}(T) = T$$

Remark 3.6. The existence and uniqueness of the formal exponential are guaranteed by lemma 3.1.

Proposition 3.4. Let R be a torsion free ring and let $\mathcal{F}$ be a formal group defined over R. Then

$$\log_{\mathcal{F}} : \mathcal{F} \to \mathcal{G}_a$$

defines an isomorphism of formal groups over $K = R \otimes \mathbb{Q}$.

Proof. Let $\omega(T)$ the normalized invariant differential on $\mathcal{F}$, so $\omega(F(T,S)) = \omega(T)$. Integrating formally with respect to T gives the following identity.

$$\log_{\mathcal{F}} F(T,S) = \log_{\mathcal{F}} T + C(S)$$

where $C(S) \in K[[T]]$ is some constant of integration. After substituting $T = 0$, we see that $C(S) = \log_{\mathcal{F}}(S)$. Hence,

$$\log_{\mathcal{F}} F(T,S) = \log_{\mathcal{F}} T + \log_{\mathcal{F}} S = G_a\left(\log_{\mathcal{F}} T, \log_{\mathcal{F}} S\right)$$

Then $\log_{\mathcal{F}} : \mathcal{F} \to \mathcal{G}$ is a formal group homomorphism. By lemma 3.1, it is guaranteed the existence of an inverse homomorphism, which is the formal exponential, so $\log_{\mathcal{F}}$ is an isomorphism. □

We are going to see that logarithm can also define isomorphism between certain subgroups of the associated groups.

Theorem 3.2. Let K be a field of characteristic 0 that is complete with respect to a normalised discrete valuation, let R be its valuation ring and let $\mathfrak{m}$ its maximal ideal. Let $p \in \mathbb{Z}$ be a prime number such that $v(p) > 0$ and let $r > \frac{v(p)}{p-1}$. Then the formal logarithm induces an isomorphism

$$\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}^r) \to (\mathfrak{m}^r, +)$$

In order to proof this theorem, we need to consider some technical lemmas first.

Lemma 3.3. Let R be a torsion free ring and let $\mathcal{F}$ be a formal group over R. Then the formal exponential map can be written as

$$\exp_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{\lambda_n}{n!} T^n$$

where $\lambda_n \in R \ \forall n \in \mathbb{N}$ and $\lambda_1 = 1$.

Proof. Notice that $\log_{\mathcal{F}} \circ \exp_{\mathcal{F}}(T) = T$ and that

$$\log_{\mathcal{F}}(T) = T + \sum_{n=1}^{\infty} \frac{c_{n-1}}{n} T^n, \quad c_n \in R$$

Differentiating the first identity we get that

$$\log'_{\mathcal{F}}(\exp_{\mathcal{F}}(T)) \exp'_{\mathcal{F}}(T) = 1 \Rightarrow \lambda_1 = \exp'_{\mathcal{F}}(0) = \frac{1}{\log'_{\mathcal{F}}(\exp_{\mathcal{F}}(0))} = \frac{1}{\log'_{\mathcal{F}}(0)} = 1$$

By repeated differentiation, it is easily seen by induction that $\log'_{\mathcal{F}}(\exp_{\mathcal{F}}(T)) \exp^{(n)}_{\mathcal{F}}(T)$ can be expressed as a polynomial with integer coefficients in the variables $\log^{(i)}_{\mathcal{F}}(\exp_{\mathcal{F}}(T))$, where $i \in \{1, \ldots, n\}$ and $\exp^{(j)}_{\mathcal{F}}(T)$, where $j \in \{1, \ldots, n-1\}$.

Evaluating at $T = 0$, since $\log^{(i)}_{\mathcal{F}}(0) = (n-1)! c_n$ and $\exp^{(j)}_{\mathcal{F}}(0) = \lambda_j$, we see that $b_n = a_1 b_1$ is a polynomial expression, with coefficients in $\mathbb{Z}$, evaluated in the variables $c_1, \ldots, c_n, \lambda_1, \ldots, \lambda_{n-1}$. Then, it follows from an easy induction that $b_n \in R$. □

Lemma 3.4. Let $\mathcal{F}$ be a formal group defined over a discrete valuation ring R such that $\mathrm{char}(R) = 0$ and let $p \in \mathbb{Z}$ be a prime number such that $v(p) > 0$. If $v(x) > \frac{v(p)}{p-1}$, then $\log_{\mathcal{F}}(x)$ converges in R and

$$v\left(\log_{\mathcal{F}}(x)\right) = v(x)$$

Proof. Since $c_n \in R$, then $v(c_n) \geq 0$ and

$$v\left(\frac{c_{n-1}x^n}{n}\right) \geq nv(x) - v(n) \geq nv(x) - (\log_p n)v(p) \geq v(x) + \big((n-1) + \log_p(n)(p-1)\big)\, v(x)$$

For $n > p$, then $n - 1 > \log_p(n)(p-1)$, so $v\left(\frac{c_{n-1}x^n}{n}\right) > v(x)$. For $n \in \{2, \ldots, p-1\}$ then $v(n) = 0$, so $v(n) = 0$ and $v\left(\frac{c_{n-1}x^n}{n}\right) \geq v(x^n) > v(x)$. If $n = p$, then

$$v\left(\frac{c_{p-1}x^p}{p}\right) \geq pv(x) - v(p) = v(x) + (p-1)v(x) - v(p) > v(x)$$

By what we have just seen, $v\left(\frac{c_{n-1}x^n}{n}\right)$ goes to ∞ as $n \to \infty$, so $\log_{\mathcal{F}}(x)$ converges by the completeness of R. Since $v\left(\frac{c_{n-1}x^n}{n}\right) > v(x)$ for every $n \geq 2$ and the valuation of the leading term is equal to $v(x)$, then ultrametric inequality implies that

$$v\left(\log_{\mathcal{F}}(x)\right) = v(x)$$

□

We now want to see that $\exp_{\mathcal{F}}(x)$ also converges when $v(x)$ is large enough. However, we need to consider first a technical lemma.

Lemma 3.5. Let v be a valuation over a field K and let $p \in \mathbb{Z}$ a prime number such that $v(p) \in (0, \infty)$. Then

$$v(n!) \leq \frac{(n-1)v(p)}{p-1} \ \forall n \in \mathbb{N}$$

Proof. We can compute

$$v(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor v(p) \leq \sum_{i=1}^{\lfloor \log_p n \rfloor} \frac{nv(p)}{p^i} = \frac{nv(p)}{p-1}\left(1 - p^{-\lfloor \log_p n \rfloor}\right) \leq \frac{(n-1)v(p)}{p-1}$$

□

Lemma 3.6. Let $\mathcal{F}$ be a formal group defined over a discrete valuation ring R. Assume that the characteristic of R is 0. Let $p \in \mathbb{Z}$ be a prime number such that $v(p) > 0$ and let $x \in R$ such that $v(x) > \frac{v(p)}{p-1}$. Then $\exp_{\mathcal{F}}(x)$ converges in R and

$$v\left(\exp_{\mathcal{F}}(x)\right) = v(x)$$

Proof. For each term, lemma 3.5 implies that

$$v\left(\frac{\lambda_n x^n}{n!}\right) \geq nv(x) - v(n!) \geq nv(x) - (n-1)\frac{v(p)}{p-1} = v(x) + (n-1)\left(v(x) - \frac{v(p)}{p-1}\right)$$

If $v(x) > \frac{v(p)}{p-1}$ then $\lim_{n\to\infty} v\left(\frac{\lambda_n x^n}{n!}\right) = \infty$, so $\exp_{\mathcal{F}}(x)$ converges in R. Moreover, in that case $v\left(\frac{\lambda_n x^n}{n!}\right) \geq v(x)\ \forall n \in \mathbb{N}$ and the equality happens only for $n = 1$ since $\lambda_1 = 1$. Hence the ultrametric inequality implies that $v\left(\exp_{\mathcal{F}}(x)\right) = v(x)$. □

We can now conclude the proof of theorem 3.2. Provided that $v(x) \geq r$, lemmas 3.4 and 3.6 imply that the power series $\log_{\mathcal{F}}(x)$ and $\exp_{\mathcal{F}}(x)$ converges to an element having the same valuation as x. Thus

$$\log_{\mathcal{F}} :\ \mathcal{F}(\mathfrak{m}^r) \to (\mathfrak{m}^r, +), \quad \exp_{\mathcal{F}} :\ (\mathfrak{m}^r, +) \to \mathcal{F}(\mathfrak{m}^r)$$

are mutually inverse bijections. By proposition 3.4, $\log_{\mathcal{F}}$ is a group homomorphism, so it has to be an isomorphism.

3.5 Formal Groups and Elliptic Curves

We will end this section by ensuring that the group operation in an elliptic curve can be described by using a formal group. This description is in general just formal, being the convergence of the power series only guaranteed only in some particular cases. We will try to describe the group operation as a power series. For that purpose, consider an elliptic E/K curve whose Weierstrass equation is

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

With the change of coordinates

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}$$

the Weierstrass equation becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z, w) \tag{3.2}$$

Essentially, we have just change the order of the homogeneous coordinates, so the geometric group law is the same, with the subtle difference that now the origin is the point $(0, 0)$.

The curve can be considered as defined over $\overline{K((t))}$. We want to see that the there is a unique power series $w(t) \in K[[t]]$ without constant term such that $(t, w((t))) \in E$. This statement can be deduced from proposition 2.1 applied to the polynomial $w - f(z, w)$ and $a = 0$.

The group law of the curve can be also understood using a power series expansion. For that purpose, consider the elliptic curve defined over $\overline{K[[t_1, t_2]]}$. By proposition 2.1, there is a unique power series $w \in K[[t]]$ such that the points $(t_1, w(t_1)), (t_2, w(t_2)) \in E$. We wish to compute the sum of these two points. Then, the line containing $(t_1, w(t_1))$ and $(t_2, w(t_2))$ can be written as $w = \lambda z + \nu$, where

$$\lambda = \tfrac{w(t_2)-w(t_1)}{t_2-t_1} \in K[[t_1, t_2]], \quad \nu = w(t_1) - t_1\lambda \in K[[t_1, t_2]]$$

Substituting $w = \lambda z + \nu$ in equation 3.2, we get the following cubic equation in z.

$$\begin{aligned}&(1 + \lambda a_2 + \lambda^2 a_4 + \lambda^3 a_6)z^3 + (a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu)z^2 + \\ &(a_1\nu + 2a_3\lambda\nu + a_4\nu^2 + 3a_6\lambda\nu^2 - \lambda)z + (a_3\nu^2 + a_6\nu^3 - \nu) = 0\end{aligned}$$

Since t_1 and t_2 are roots of this equation for the appropiate values of $\lambda, \nu \in K[[t_1, t_2]]$, then the third root can be computed as

$$x = -t_1 - t_2 - \frac{a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu}{1 + \lambda a_2 + \lambda^2 a_4 + \lambda^3 a_6} \in K[[t_1, t_2]]$$

It can be easily checked that x is a power series with no constant term. The other coordinate of this third point of intersection can be computed as

$$y = \lambda x + \nu \in K[[t_1, t_2]]$$

It is again a power series with no constant term. Then, by the uniqueness part of proposition 2.1, $y = w(x)$.

A similar argument can be used to express the coordinates (t_3, w_3) of the third point of intersection of the line through (x, y) and $(0, 0)$ by a power series in $K[[t_1, t_2]]$ with no constant term. Then, the sum $(t_3, w_3) = (t_1, w_1) + (t_2, w_2)$ can be written as

$$(t_3, w_3) = \big(F(t_1, t_2), w(F(t_1, t_2))\big)$$

Analogously, there is a power series $i(t) \in K[[t]]$ with no constant term such that

$$-(t_1, w(t_1)) = (i(t_1), w(i(t_1)))$$

Remark 3.7. An important advantage of using this technique is that there is no necessity of distinguishing between summing different points of doubling one of them. That is because the line through a point $(z_1, w(z_1))$ has slope $\lambda = w'(z_1)$, where w' represents the formal derivative of the power series w is tangent to the curve. Then simplifying denominators in the expression of γ and substituting $z_1 = z_2$ would result in the same expression.

Proposition 3.5. Let $F \in R[[z_1, z_2]]$ be the power series given by the group law of the elliptic curve. Then, F defines a formal group.

Proof. Axioms of commutativity and the existence of neutral and inverse element comes from this properties in the group law of the curve. For the associative axiom, we just need to consider the curve to be defined over $\overline{K[[t_1, t_2, t_3]]}$. □

Chapter 4

The Pontryagin Duality

The main goal of this chapter is giving a tool for classifying some discrete p-primary groups which might not be finitely generated as groups. That tool is Pontryagin duality.

In order to develop it, we start by defining inverse and direct limits in section 4.1. Then we define profinite topological spaces in section 4.2, as a preparation for introducing profinite groups in section 4.3. The main references used have been [23] and [24]. We also characterise them in several ways and describe how their discrete continuous modules are.

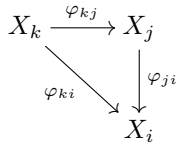
In section 4.4 the Pontryagin dual of a group is defined. It is also showed how the compact-open topology works and how duality behaves under taking direct and inverse limits. In section 4.5 we give a $\mathbb{Z}_p$-module structure to the Pontryagin dual, which will be used in section 4.6 to classify those discrete abelian groups being cofinitely generated. These sections are a personal development, guided by [11] and [24].

4.1 Direct and Inverse Limits

Definition 4.1. A *directed set* $(I, \leq)$ is a set I with a binary relation $\leq$ (possibly partial) satisfying the following axioms:

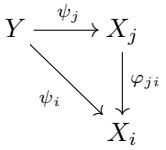
- $i \leq i \ \forall i \in I$.
- $i \leq j,\ j \leq k \Rightarrow i \leq k \ \forall i, j, k \in I$.
- $i \leq j,\ j \leq i \Rightarrow i = j \ \forall i, j \in I$.
- $\forall i, j \in I,\ \exists k \in I$ such that $i \leq k,\ j \leq k$.

Definition 4.2. An *inverse system* over a directed set I, is a collection of objects $\{X_i : i \in I\}$ in a category and a collection of morphisms $\{\varphi_{ji} : X_j \to X_i : i \leq j\}$ such that whenever $k \geq j \geq i$, the following diagram commutes

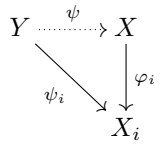


Definition 4.3. Let $\{X_i, \varphi_{ji}, I\}$ be an inverse system in some category $\mathcal{C}$ and let $Y \in \mathcal{C}$. A collection of maps $\{\psi_i : Y \to X_i : i \in I\}$ is said to be *compatible* if whenever $i \leq j$ the following

diagram commutes.

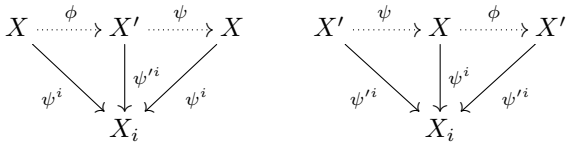


Definition 4.4. Given an inverse system $\{X_i, \varphi_{ji}, I\}$ in some category, an *inverse limit* is an object $X \in \mathcal{C}$ with compatible morphisms $\varphi_i : X \to X_i$ such that for every collection of compatible maps $\{\psi_i : Y \to X_i\}$ there is a unique morphism $\psi : Y \to X$ such that the following diagrams commute:



Proposition 4.1. Given an inverse system $\{X_i, \varphi_{ji}, I\}$ in any category, there is at most one inverse limit up to isomorphism.

Proof. Suppose there are two inverse limits X and X' with their respective collection of morphisms $\{\psi_i : \ i \in I\}$ and $\{\psi_i' : \ i \in I\}$. Then the universal property of inverse limits gives the following commutative diagram:

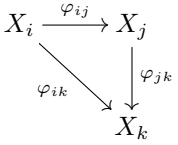


By the uniqueness part of the universal property of the direct limits, $\psi \circ \phi = Id_X$ and $\phi \circ \psi = Id_{X'}$, so $X \cong X'$. □

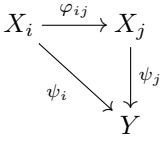
Remark 4.1. Let $\{X_i, \varphi_{ji}, I\}$ be an inverse system of topological spaces, groups or topological groups. Its inverse limit is the subset of their product space given by

$$\varprojlim_{i \in I} X_i = \left\{ (x_i) \in \prod_{i \in I} X_i : \varphi_{ji}(x_j) = x_i \ \forall (i,j) \in I^2 : \ j \geq i \right\}$$

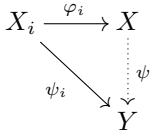
Definition 4.5. A *direct system* over a directed set I is a collection of objects $\{X_i : i \in I\}$ in a category and a collection of morphisms $\{\varphi_{ij} : X_i \to X_j : i \leq j\}$ such that whenever $k \geq j \geq i$, the following diagram commutes



Definition 4.6. Let $\{X_i, \varphi_{ij}, I\}$ be a direct system in some category $\mathcal{C}$ and let $Y \in \mathcal{C}$. A collection of maps $\{\psi_i : X_i \to Y : i \in I\}$ is said to be *compatible* if whenever $i \leq j$ the following diagram commutes.

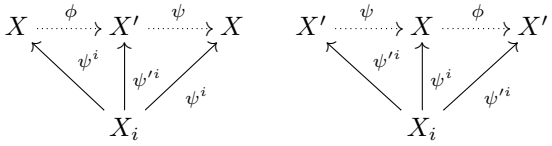


Definition 4.7. Given a direct system $\{X_i, \varphi_{ij}, I\}$ in some category, a *direct limit* is an object $X \in \mathcal{C}$ with compatible morphisms $\varphi_i : X_i \to X$ such that for every collection of compatible maps $\{\psi_i : X_i \to Y\}$ there is a unique morphism $\psi : X \to Y$ such that the following diagrams commute:



Proposition 4.2. Given a direct system $\{X_i : \varphi_{ij}, I\}$ in any category, there is at most one direct limit up to isomorphism.

Proof. It is analogous to the proof of proposition 4.1, just considering the following commutative diagrams:



□

Remark 4.2. Let $\{X_i, \varphi_{ij}, I\}$ be a system of topological spaces. Its direct limit is the quotient of their disjoint given by

$$\varprojlim_{i \in I} X_i = \left\{ (x_i) \in \bigsqcup_{i \in I} X_i : \varphi_{ij}(x_i) = x_j \ \forall (i,j) \in I^2 : \ i \geq j \right\}$$

In case the X_i are topological groups (or simply groups), the direct limit has a natural group operation which consist on multiplying componentwise.

We will end this section by showing some properties of the direct limit in certain categories.

Proposition 4.3. Let I be a directed set and let $\{A_i : i \in I\}$, $\{B_i : i \in I\}$ and $\{C_i : i \in I\}$ be direct system of R-modules such that, for every $i \in I$, the following sequence is exact:

$$0 \longrightarrow A_i \xrightarrow{\mu_i} B_i \xrightarrow{\varepsilon_i} C_i \longrightarrow 0$$

It the following diagrams are commutative for every $i \leq j$,

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_{ij}} & A_j \\ \downarrow{\scriptstyle \mu_i} & & \downarrow{\scriptstyle \mu_j} \\ B_i & \xrightarrow{\varphi_{ij}} & B_j \end{array} \qquad \begin{array}{ccc} B_i & \xrightarrow{\varphi_{ij}} & B_j \\ \downarrow{\scriptstyle \varepsilon_i} & & \downarrow{\scriptstyle \varepsilon_j} \\ C_i & \xrightarrow{\varphi_{ij}} & C_j \end{array}$$

then the direct limit induces another short exact sequence:

$$0 \longrightarrow \varinjlim_{i \in I} A_i \xrightarrow{\mu_*} \varinjlim_{i \in I} B_i \xrightarrow{\varepsilon_*} \varinjlim_{i \in I} C_i \longrightarrow 0$$

Proof. It is clear that the maps μ_* and ε_* are well defined.

Let a_i be a representative of an element in $\ker \mu_*$ and let $b_i := \mu_i(a_i)$. Since $[b_i] = 0$ there is some j such that $\varphi_{ij}(b_i) = 0$. Then $\varphi_{ij} \circ \mu_i(a_i) = \mu_j \circ \varphi_{ij}(a_i) = 0$. Since μ_j is injective, then $\varphi_{ij}(a_i) = 0$, so $[a_i] = 0$. The secuence is thus exact at $\varinjlim_{i \in I} A_i$.

It is clear that $\varepsilon_* \circ \mu_* = 0$. Conversely, given $[b_i] \in \ker \varepsilon_*$, there is some $j \in I$ such that $\varepsilon_j \circ \varphi_{ij}(b_i) = 0$, so $\varphi_{ij}(a_i) \in \mathrm{Im}(\mu_i)$ and, therefore, $[b_i] \in \mathrm{Im}(\mu_*)$.

Since ε_* is clearly surjective, the proof is complete. □

Proposition 4.4. Let $\{A_i : i \in I\}$ be a direct system of groups and let B another group. Then there is an isomorphism

$$\varinjlim_i (A_i \otimes B) \cong \left(\varinjlim_i A_i\right) \otimes B$$

Proof. The maps

$$\phi_i : A_i \otimes B \to \left(\varinjlim_i A_i\right) \otimes B : \ a_i \otimes b \mapsto [a_i] \otimes b$$

form a compatible system, so they induce a map

$$\phi : \varinjlim_i (A_i \otimes B) \to \left(\varinjlim_i A_i\right) \otimes B$$

Conversely, the map

$$\psi : \left(\varinjlim_i A_i\right) \times B \to \varinjlim_i (A_i \otimes B) : ([a_i], b) \mapsto [a_i \otimes b]$$

induces a map from the tensor product. It is easily seen that ψ and ψ are mutually inverse. □

4.2 Profinite Spaces

As a preparation to study the profinite groups, we will study first profinite topological spaces and its characterisation as compact, Hausdorff and totally disconnected spaces.

Definition 4.8. A topological space is called a *profinite space* if it is the inverse limit of finite discrete spaces.

Profinite Hausdorff topological spaces can be easily characterised as those being compact and totally disconnected.

Lemma 4.1. For a Hausdorff topological space T the following conditions are equivalent.

1. T is a profinite space.
2. T is compact and totally disconnected
3. T is compact and every point of T has a basis of neighbourhoods consisting of subsets which are both open and closed.

Before proving that equivalence, we need to consider some technical lemmas.

Lemma 4.2. If the transition maps are surjective, the inverse limit of compact, Hausdorff non-empty topological spaces $\{X_i : i \in I\}$ is non-empty, Hausdorff and compact.

Proof. Since the spaces X_i are compact, so is their product $\prod_{i \in I} X_i$, because of Tychonoff's theorem. The inverse limit $X := \varprojlim_i X_i$ can be expressed as follows

$$\varprojlim_i X_i = \bigcap_{i \leq j} X_{ji}$$

where $X_{ji} = \left\{ x \in \prod_{i \in I} X_i : \varphi_{ji} \circ \pi_j(x) = \pi_i(x) \right\}$. Since X_i is Hausdorff, then X_{ji} is closed whenever $i \leq j$, so X is closed too and thus compact. Clearly, it is also Hausdorff for being a subspace of a Hausdorff space.

Assume for the sake of contradiction that X is empty. Due to the compactness of the direct product, a finite amount of X_{j_k,i_k} would have empty intersection. However, let l be an upper bound for $\{j_1, \ldots, j_n\}$, which exists because of last axiom of definition 4.1 and an inductive argument. Given some $y_0 \in X_l$, by the axiom of choice there exist some $x_0 \in \prod_{i \in I} X_i$ such that $\pi_l(x_0) = y_0$ and

$$\pi_{i_k}(x_0) = \varphi_{l,i_k}(y_0) \ \forall k = 1, \ldots, n, \quad \pi_{j_k}(x_0) = \varphi_{l,j_k}(y_0) \ \forall k = 1, \ldots, n$$

Hence the compatibility of the transition maps implies that

$$x_0 \in \bigcap_{i=1}^{n} X_{j_k,i_k} \neq \emptyset$$

This contradiction proves that $X \neq \emptyset$. □

Lemma 4.3. Let T be a compact Hausdorff topological space and let $x \in T$. Then the connected component C of x is the intersection of all open and closed neighbourhoods of x.

Proof. Let $\{U_\alpha\}$ be the family of all open and closed neighbourhoods of x. Since C is connected, it is contained in every U_α, so

$$C \subset A := \bigcap U_\alpha$$

Then it is enough to show that A is connected. Assume that $A = U \cup V$, where $U \cap V = \emptyset$, and that U and V are closed in A, and so they are in T because A is closed too. Hence U and V are compact and there are open sets $U', V' \subset T$ containing U and V such that $U' \cap V' = \emptyset$.

Since $(T \setminus (U' \cup V')) \cap A = \emptyset$ and T is compact, there are a finite number $\alpha_1, \ldots, \alpha_n$ such that

$$(T \setminus (U' \cup V')) \cap U_{\alpha_1} \cap \cdots \cap U_{\alpha_n} = \emptyset$$

However, $B := U_{\alpha_1} \cap \cdots \cap U_{\alpha_n}$ is an open and closed neighbourhood of x and

$$x \in (B \cap U') \cup (B \cap V')$$

Without loss of generality, we can assume that $x \in B \cap U'$, which is clearly open and it is also closed because

$$B \cap U' = (T \setminus (B \cap V')) \cap B$$

By definition $A \subset B \cap U' \subset U'$, so $A \cap V \subset A \cap V' = \emptyset$, which implies that $V = \emptyset$. Thus A is connected. □

We can now complete the proof of lemma 4.1.

Proof of lemma 4.1. (1) ⇒ (2): T is compact by lemma 4.2. Since discrete spaces are totally disconnected, so is their direct product and their direct limit, as a subspace of the product, is totally disconnected too.

(2) ⇒ (3): Let $x \in T$ and let $\{U_\alpha\}$ be the family of open and closed neighbourhoods of x. According to lemma 4.3,

$$\{x\} = \bigcap U_\alpha$$

Let W be an open neighbourhood of T. Then $T \setminus W$ is compact and

$$(T \setminus W) \cap \left(\bigcap U_\alpha \right) = \emptyset$$

By compactness, there is a finite intersection of open and closed neighbourhood contained in W. Nevertheless, this finite intersection is itself an open and closed neighbourhood, so $\{U_\alpha\}$ is a basis of neighbourhoods.

(3) $\Rightarrow$ (1): Denote by $\mathcal{R}$ the set of equivalence relations in T such that the equivalence classes are open sets. Since T is compact, T/R is finite and discrete for every $R \in \mathcal{R}$. There is also a natural partial order relation in $\mathcal{R}$: we say $R \geq R'$ if and only if $xR \subset xR'$ $\forall x \in T$. This makes $\mathcal{R}$ a directed set because $R_1 \cap R_2$ is an upper bound for the pair R_1, R_2.[1]

If $R \geq R'$, we define the projection

$$\varphi_{RR'} : \ T/R \to T/R' : \ xR \mapsto xR'$$

Since the projections $\pi_R : X \to X/R : \ x \mapsto xR$ are clearly compatible, by the universal property of the inverse limit there is a canonical continuous mapping

$$\psi : T \to \varprojlim_{\mathcal{R}} T/R$$

We can see ψ is surjective because, given an element $\{x_R\}_{R \in \mathcal{R}} \in \varprojlim_{\mathcal{R}} T/R$, for each relation $R \in \mathcal{R}$, then $(\pi_R \circ \psi)^{-1}(x_R)$ is non-empty and compact. Since $\mathcal{R}$ is a directed set and the maps $\pi_R \circ \phi$ are compatible, finite intersecions of these preimages are also non-empty, which implies by compactness that

$$\psi^{-1}(\{x_R\}_{R \in \mathcal{R}}) = \bigcap_{R \in \mathcal{R}} (\pi_R \circ \psi)^{-1}(x_R) \neq \emptyset$$

Moreover, given some $x, y \in T$ such that $x \neq y$. By hypothesis, there is an open and closed set U such that $x \in U$ and $y \notin U$. Then, the equivalence relation defined by $(a, b) \in R$ if both are in U or if both are not in U satisfies that $(x, y) \notin R$. Then, $\psi(x) \neq \psi(y)$.

Since every equivalence class is open, the projection $\pi_R : T \to T/R$ is continuous provided that T/R is endowed with the discrete topology. Since all the projections are compatible, ψ is continuous by the universal property of the inverse limit. Further, ψ is an homeomorphism since T is compact and the inverse limit is Hausdorff. □

4.3 Profinite Groups

Now, we will focus in the category of profinite groups.

Definition 4.9. A *profinite group* is a topological group which is the inverse limit of finite discrete groups.

The situation regarding profinite groups is similar to profinite spaces. Hence profinite groups can be identified by their topological properties.

Proposition 4.5. Given a Hausdorff topological group, the following conditions are equivalent.

1. G is a profinite group.
2. G is compact and totally disconnected.

[1] Here we are understanding relations as subsets of $T \times T$ given by $(x, y) \in R \Leftrightarrow x \sim y$.

3. G is compact and the unit element has a basis of neighbourhoods consisting of open and closed normal subgroups.

Proof. (1) $\Rightarrow$ (2): By lemma 4.1.

(2) $\Rightarrow$ (3): By lemma 4.1, every point has a basis of neighbourhoods consisting of open and closed sets. Let U be an open and closed neighbourhood of the neutral element. Define

$$V := \{v \in U : Uv \subset U\}, \quad H = \{h \in V : h^{-1} \in V\}$$

Given some $v \in V$, then $uv \in U$ $\forall u \in U$. By the continuity of the group operation, there are open neighbourhoods U_u, V_u of u and v, respectively, such that $U_u V_u \in U$. Then $\{U_u : u \in U\}$ is an open cover of the compact subset U, so it is possible to find a finite subcover $\{U_{u_1}, \dots, U_{u_n}\}$. Define then

$$V_v := V_{u_1} \cap \cdots \cap V_{u_n}$$

which is clearly an open neighbourhood of v contained in V, Since $v \in V$ was arbitrary, V is open. Since the inversion map is an homeomorphism, $H = V \cap V^{-1}$ is open too.

Let's show that H is a subgroup. Trivially $e \in H$ and $H^{-1} = H$. Moreover given $x, y \in H$, since $Uxy \subset Uy \subset U$, then $xy \in V$. Similarly, since $x^{-1}, y^{-1} \in V$, then $y^{-1}x^{-1} \in V$, so $xy \in H$. Therefore, H is an open subgroup contained in U. H is also closed, since its complementary is a union of cosets of H, which are homeomorphic to H.

Since the cosets of H constitute an open cover of the compact group G, then $(G : H) < \infty$. Therefore, there are only finitely many conjugates of H. The finite intersection of all of them is an open and closed normal subgroup contained in U.

(3) $\Rightarrow$ (1): Assuming that U runs through the set of normal, open and closed subgroups, which is a directed set, there is a canonical continuous homomorphism

$$\psi : G \to \varprojlim_U G/U$$

Notice that the compactness imply that G/U is finite for every open normal subgroup. We will see that ψ is a group isomorphism and a homeomorphism. The injectivity is clear since G is Hausdorff and the normal, open and closed subgroups are a basis of neighbourhoods. For the surjectivity, let $x = \{x_U\} \in \varprojlim_U G/U$. Then

$$\psi^{-1}(x) = \bigcap_U (\pi_U \circ \psi)^{-1}(x_U)$$

Since the finite intersections of $(\pi_U \circ \psi)^{-1}(x_U)$ are nonempty, then $\psi^{-1}(x) \neq \emptyset$ due to the compactness of G.

The continuity on ψ comes from the universal property of the inverse limit. Since ψ is also bijective, G is compact and the inverse limit is Hausdorff, ψ is an homeomorphism. □

It is possible to characterise any closed subgroup of a profinite group as an inverse limit of open subgroups.

Proposition 4.6. Let G be a profinite group and let H be a closed subgroup. Then

$$H = \varprojlim_U HU$$

where U runs through the normal open subgroups and the transition maps are inclusions.

Proof. There is a canonical injection from H to the direct limit by considering the same element in the same coordinate. The surjectivity is equivalent to the following identity.

$$H = \bigcap_U HU$$

In fact, given $g \in G \setminus H$, by proposition 4.5 there is some open normal subgroup U such that $gU \cap H = \emptyset$ and hence $g \notin HU$.

□

In order to study the order of a profinite group, we need to introduce the concept of supernatural numbers.

Definition 4.10. A *supernatural number* is a formal product

$$\prod_p p^{n_p}$$

where p runs through all prime numbers and, for each p, the exponent is a non-negative integer or ∞.

Definition 4.11. Let G be a profinite group and let $H \subset G$ be a closed group. The *index* of H in G is the supernatural number

$$(G : H) = l.c.m.\,(G/U : H/(H \cap U))$$

where U ranges over all normal subgroups of G. The *order* of G is

$$\#G = (G : 1) = l.c.m.\,(|G/U|)$$

With that, the notion Sylow subgroup can be extended to profinite groups.

Definition 4.12. A profinite group G is said to be a pro-p group if it is the inverse limit of finite discrete p-group. Equivalently, a profinite group is pro-p if its order divides p^∞.

Definition 4.13. Let G be a profinite group and let p be a prime number. A subgroup G_p is a p-Sylow subgroup if it is a pro-p group and $(G : G_p)$ is prime to p.

Sylow theorems can be generalized to profinite groups.

Theorem 4.1. Let G be a profinite group and let p be a prime number.

1. There exists a p-Sylow subgroup G_p.
2. Every pro-p subgroup is contained in a p-Sylow subgroup.
3. The p-Sylow subgroups of G are conjugate.

Proof. Let U run through the open subgroups of G and denote by $\Sigma_p(U)$ to the set of p-Sylow subgroups of G/U, which is finite and non-empty by [14], theorem 1.7. If $V \subset U$, the canonical projection $G/V \to G/U$ induces a map

$$\Sigma_p(V) \to \Sigma_p(U)$$

If we endowed $\Sigma_p(U)$ with the discrete topology, then the inverse limit

$$\varprojlim_U \Sigma_p(U)$$

is not empty by lemma 4.2 and each element is a p-Sylow subgroup.

For the second part, let H be a pro-p group. By [14], theorem 1.14, the subset $\Sigma_p^H(U) \subset \Sigma_p(U)$ formed by the p-Sylow subgroups of G/U containing HU/U is not empty. Again, an element belonging to the inverse limit

$$\varprojlim_U \Sigma_P^H(U)$$

would be a Sylow subgroup containing H.

Finally, let G_p and G'_p be two p-Sylow subgroups of G and let S_U and S'_U be their images in G/U via the canonical projection. Let $C(U)$ be the set of elements $\sigma_U S_U \sigma_U^{-1} = S'_U$, which is not empty by [14], theorem 1.12. $C(U)$ is thus a projective system such that

$$\varprojlim_U C(U)$$

is not empty by lemma 4.2. Clearly, $\sigma G_p \sigma^{-1} G'_p$ for any $\sigma \in \varprojlim_U C(U)$. □

We will also be interested in continuous actions of a profinite group on different abelian groups.

Definition 4.14. Let G be a profinite group. A *(topological) G-module* M is an abelian Hausdorff topological group endowed with a continuous action

$$G \times M \to M : \ (g, m) \mapsto g(m)$$

such that for every $g, h \in G$ and $m, n \in M$ we have that

$$1(m) = m, \quad (gh)(m) = g(h(m)), \quad g(m+n) = g(m) + g(n)$$

Definition 4.15. Let G be a profinite group, let H be a subgroup and let M be a G-module. The *H-invariant* submodule is defined by

$$M^H = \{m \in M : h(m) = m \ \forall h \in H\}$$

Unless the contrary is stated, we will assume that M is endowed with the discrete topology. The continuity of the action of G in that case can be studied using the next proposition.

Proposition 4.7. Let G be a profinite group acting on an abelian discrete topological group M. Then the following conditions are equivalent:

1. The action is continuous.
2. For every $m \in M$ the subgroup $G_m := \{g \in G : g(m) = m\}$ is open.
3. $M = \bigcup_U M^U$, where U runs through the open normal subgroups of G.

Proof. (1) ⇒ (2): The continuous action restricts to a continuous function

$$\phi_m : G \to M : \ g \mapsto g(m)$$

Then $G_m = \phi_m^{-1}(\{m\})$ is open.

(2) ⇒ (3): Given $m \in M$, then $m \in M^{G_m} \subset \bigcup_U M^U$ because G_m is a normal subgroup for being the kernel of the homomorphism $G \to \mathrm{End(M)}$ induced by the action.

(3) ⇒ (1): Given $(g, m) \in G \times M$, there is an open subgroup such that $m \in M^U$. Then $gU \times m$ is an open neighbourhood of $(g, m) \in G \times M$ mapping to $g(m)$. Then the action is continuous at (g, m). □

4.4 The Dual Group

This section is dedicated to the Pontryagin duality. We will focus it as a preparation for defining in section 4.6 the notion of corank of a discrete p-primary module.

Throughout this section, let $p \in \mathbb{Z}$ be a fixed prime number. We are going to study the notion of dual group and then we will show that abelian pro-p groups and discrete p-primary abelian groups are mutually duals.

Definition 4.16. Let A be a topological group. Its *Pontryagin dual* is defined by

$$\widehat{A} = \mathrm{Hom}_{\mathrm{cts}}(A, \mathbb{Q}_p/\mathbb{Z}_p)$$

when $\mathbb{Q}_p/\mathbb{Z}_p$ is endowed with the discrete topology. The topology given to $\widehat{A}$ is the compact-open topology, i.e., the topology generated by the following subbase

$$V(K,U) = \left\{ f \in \widehat{A} : \ f(K) \subset U \right\}$$

where K runs through the compact subsets of A and U runs through the open sets in $\mathbb{Q}_p/\mathbb{Z}_p$.

Remark 4.3. The Pontryagin dual is sometimes defined as $\mathrm{Hom}_{\mathrm{cts}}(A, \mathbb{Q}/\mathbb{Z})$ (see [24]). However, we are going to be only interested in studying its p-primary parts and that is the reason we have given last definition.

In order to ensure that the Pontryagin dual of A is a topological group, we need to assume that A is locally compact. However, that does not arise any problem to our interests, since discrete and profinite groups are locally compact.

Proposition 4.8. Given a compact, Hausdorff and locally compact topological group A, its Pontryagin dual $\widehat{A}$ is a topological group with the compact-open topology.

Proof. The inverse map $i : x \mapsto -x$ is an homeomorphism because

$$-V(K,U) = V(K,-U)$$

and $-U$ is open since $\mathbb{Q}_p/\mathbb{Z}_p$ is a topological group.

Then we just need to see that the sum map is continuous. Let $f, g \in \widehat{A}$ and let $K \subset A$ compact and $U \subset \mathbb{Q}_p/\mathbb{Z}_p$ open be such that $f+g \in V(K,U)$. Since the sum operation is continuous in $\mathbb{Q}_p/\mathbb{Z}_p$, for each $x \in K$, there are open sets $\widetilde{V}_x, \widetilde{W}_x \subset \mathbb{Q}_p/\mathbb{Z}_p$ such that $f(x) \in \widetilde{V}_x$, $g(x) \in \widetilde{W}_x$ and $\widetilde{V}_x + \widetilde{W}_x \subset U$.

Since A is locally compact, we can find V_x and W_x precompact open neighbourhoods of x such that $\overline{V}_x \subset f^{-1}(\widetilde{V}_x)$ and $\overline{W}_x \subset g^{-1}(\widetilde{W}_x)$. By compactness, there is a finite number $x_1, \ldots, x_n$ such that

$$K \subset (V_{x_1} \cap W_{x_1}) \cup \cdots \cup (V_{x_n} \cap W_{x_n})$$

Therefore,

$$f \in V(V_{x_1}, \widetilde{V}_{x_1}) \cap \cdots \cap V(V_{x_n}, \widetilde{V}_{x_n}), \quad g \in V(W_{x_1}, \widetilde{W}_{x_1}) \cap \cdots \cap V(W_{x_n}, \widetilde{W}_{x_n})$$

By construction

$$\left[V(V_{x_1}, \widetilde{V}_{x_1}) \cap \cdots \cap V(V_{x_n}, \widetilde{V}_{x_n})\right] + \left[V(W_{x_1}, \widetilde{W}_{x_1}) \cap \cdots \cap V(W_{x_n}, \widetilde{W}_{x_n})\right] \subset f(K,U)$$

Hence, the sum operation is a continuous map and $\widehat{A}$ is a topological group. □

Corollary 4.1. If A is a compact Hausdorff group, then $\widehat{A}$ has de discrete topology.

Proof. Since A is compact and Hausdorff, it is locally compact, $\hat{A}$ is a topological group because of proposition 4.8. Hence we just need that the set $U = \{0\}$ is open. However, this is true by definition because it is $V(A, \{0\})$ □

From now on, we will assume that the homomorphisms are continuous without specifying it.

Proposition 4.9. Let $\{G_i : i \in I\}$ be an inverse system of finite discrete groups with transition maps $\{\psi_{ji} : j \geq i\}$, then

$$\mathrm{Hom}\left(\varprojlim_{i\in I} G_i, \mathbb{Q}_p/\mathbb{Z}_p\right) \cong \varinjlim_{i\in I} \mathrm{Hom}\left(G_i, \mathbb{Q}_p/\mathbb{Z}_p\right)$$

where the transition homomorphisms in the last direct limit are

$$\psi_{ij}^* : \mathrm{Hom}(G_i, \mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Hom}(G_j, \mathbb{Q}_p/\mathbb{Z}_p) : \ \phi \mapsto \phi \circ \psi_{ji}, \quad i > j$$

Proof. Let $G = \varprojlim_{i\in I} G_i$, let $\varphi \in \mathrm{Hom}\left(G, \mathbb{Q}_p/\mathbb{Z}_p\right)$ and let $U := \ker\varphi$. By continuity, U is an open normal subgroup of G, so there are some $j_1, \ldots, j_n \in I$ such that $\ker(\pi_{j_1}) \cap \cdots \cap \ker(\pi_{j_n}) \subset U$, where π_i is the canonical projection onto the i^{th} coordinate. If j is an upper bound of $\{j_1, \ldots, j_n\}$, then $\ker(\pi_j) \subset U$. Hence we identify φ with the equivalence class of the quotient map

$$\varphi_j = \overline{\varphi}_j : \ G_j \to \mathbb{Q}_p/\mathbb{Z}_p$$

If $i \in I$ was another index such that $\ker(\pi_i) \subset U$, then there is some upper bound $k \geq i, j$. Then we have that $\psi_{ki} \circ \pi_k = \pi_i$ and $\psi_{kj} \circ \pi_k = \pi_j$, so we have the following commutative diagrams:

$$\begin{array}{ccccc} G & \xrightarrow{\pi_k} & G_k & \xrightarrow{\psi_{ki}} & G_i \\ & & & \searrow^{\overline{\varphi}_k} & \downarrow{\scriptstyle \overline{\varphi}_i} \\ & & & & \mathbb{Q}_p/\mathbb{Z}_p \end{array} \qquad \begin{array}{ccccc} G & \xrightarrow{\pi_k} & G_k & \xrightarrow{\psi_{kj}} & G_i \\ & & & \searrow^{\overline{\varphi}_k} & \downarrow{\scriptstyle \overline{\varphi}_j} \\ & & & & \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

Thus $\overline{\varphi}_k = \overline{\varphi}_i \circ \psi_{ki} = \overline{\varphi}_j \circ \psi_{kj}$, so $\overline{\varphi}_i$, $\overline{\varphi}_j$ and $\overline{\varphi}_k$ belong to the same equivalence class in the direct limit. Hence we have defined a canonical map:

$$\Phi : \mathrm{Hom}\left(\varprojlim_{i\in I} G_i, \mathbb{Q}_p/\mathbb{Z}_p\right) \to \varinjlim_{i\in I} \mathrm{Hom}\left(G_i, \mathbb{Q}_p/\mathbb{Z}_p\right) : \ \varphi \mapsto [\varphi_i]$$

We want to see that this identification is a homomorphism. For that purpose, let $\alpha, \beta \in \mathrm{Hom}(G, \mathbb{Q}_p/\mathbb{Z}_p)$ and let $i, j \in I$ such that $\ker(\pi_i) \subset \ker(\alpha)$ and $\ker(\pi_j) \subset \ker(\beta)$. For every upper bound $k \geq i, j$,

$$\ker(\pi_k) \subset \ker(\pi_i) \cap \ker(\pi_j) \subset \ker(\alpha) \cap \ker(\beta) \subset \ker(\alpha + \beta)$$

and clearly $(\alpha + \beta)_k = \alpha_k + \beta_k$.

The inverse function is given as follows. If $\phi \in \mathrm{Hom}(G_i, \mathbb{Q}_p/\mathbb{Z}_p)$ for some $i \in I$ and $\pi_i : G \to G_i$ is the canonical projection, then

$$\Phi^{-1}(\phi) = \phi \circ \pi_i \in \mathrm{Hom}(G, \mathbb{Q}_p/\mathbb{Z}_p)$$

The inverse function is well defined. To see that, let $\varphi_1 \in \mathrm{Hom}(G_i, \mathbb{Q}_p/\mathbb{Z}_p)$ and $\varphi_2 \in \mathrm{Hom}(G_j, \mathbb{Q}_p/\mathbb{Z}_p)$ be two representatives of the same element in the direct product. Then

there is an upper bound $k \geq i, j$ such that the following diagram is commutative

$$\begin{array}{ccc} G_k & \xrightarrow{\psi_{ki}} & G_i \\ \downarrow{\scriptstyle \psi_{kj}} & & \downarrow{\scriptstyle \varphi_1} \\ G_j & \xrightarrow{\varphi_2} & \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

Hence,

$$\Phi^{-1}(\varphi_1) = \varphi_1 \circ \pi_i = \varphi_1 \circ \psi_{ki} \circ \pi_k = \varphi_2 \circ \psi_{kj} \circ \pi_k = \varphi_2 \circ \pi_j = \Phi^{-1}(\varphi_2)$$

then Φ^{-1} is well defined and thus Φ is an isomorphism. □

Proposition 4.10. Let $\{G_i : i \in I\}$ a direct system of finite discrete groups, being $\varphi_{ij} : G_i \to G_j$, for $i < j$, the transition maps. Then

$$\mathrm{Hom}\left(\varinjlim_I G_i, \mathbb{Q}_p/\mathbb{Z}_p\right) \cong \varprojlim_I \mathrm{Hom}\left(G_i, \mathbb{Q}_p, \mathbb{Z}_p\right)$$

where the transition homomorphisms in the last inverse limit are

$$\varphi_{ji}^* : \mathrm{Hom}(G_j, \mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Hom}(G_i, \mathbb{Q}_p/\mathbb{Z}_p) : \ \phi \mapsto \phi \circ \varphi_{ij}, \quad i < j$$

Proof. Let $i \in I$ and let $j_i : G_i \to \varinjlim_I G_i : \ x \mapsto [x]$ be the canonical map. Then consider the collection of maps

$$\psi_i : \mathrm{Hom}\left(\varinjlim_I G_i, \mathbb{Q}_p/\mathbb{Z}_p\right) \to \mathrm{Hom}\left(G_i, \mathbb{Q}_p, \mathbb{Z}_p\right) : \ \phi \mapsto \phi \circ j_i$$

Since $j_i = j_j \circ \varphi_{ij}$ $\forall i, j \in I$, the collection $\{\psi_i : i \in I\}$ is compatible. By the universal property of the inverse limit, it factors through a homomorphism

$$\psi : \mathrm{Hom}\left(\varinjlim_I G_i, \mathbb{Q}_p/\mathbb{Z}_p\right) \to \varprojlim_I \mathrm{Hom}\left(G_i, \mathbb{Q}_p, \mathbb{Z}_p\right)$$

Conversely, given $\phi \in \varprojlim_I \mathrm{Hom}(G_i, \mathbb{Q}_p, \mathbb{Z}_p)$, we see that for every $x \in G_i$, where $i \in I$, then

$$\psi^{-1}(\phi)([x]) = \pi_i^*(\phi)(x)$$

where π_i^* is the projection in the inverse limit associated to the coordinate $i \in I$. It is easy to see that ψ^{-1} is well defined since given two representatives $x \in G_i$ and $y \in G_j$ in the same equivalence class there is some upper bound $k \geq i, j$ and $z \in G_k$ in that equivalence class. Then

$$\pi_i^*(\phi)(x) = (\varphi_{ki}^* \circ \pi_k^*)(\phi)(x) = \pi_k^*(\phi)(\varphi_{ik}(x)) = \pi_k^*(\phi)(z) = (\varphi_{jk}^* \circ \pi_k^*)(\phi)(y) = \pi_j^*(\phi)(y)$$

Then ψ^{-1} is well defined, so ψ is an isomorphism. □

Remark 4.4. The topology in

$$\varprojlim_I \mathrm{Hom}\left(G_i, \mathbb{Q}_p, \mathbb{Z}_p\right)$$

given by the inverse limit is the compact open topology, since both of them are generated by the same subbasis.

Now we want to see that abelian pro-p groups and discrete p-primary abelian groups are mutually duals. For that purpose, we need to see that the duals of finite abelian p-groups are isomorphic to them.

Proposition 4.11. Let A be a discrete, finite cyclic p group. Then $\widehat{A}$ is non-canonically isomorphic to A.

Proof. Let $n \in \mathbb{N}$ be such that $|A| = p^n$ and let $\sigma \in A$ be a generator. Consider the map

$$\widehat{A} \to \mathbb{Q}_p/\mathbb{Z}_p[p^n] : \ \varphi \mapsto \varphi(\sigma)$$

It is well defined since $\operatorname{ord}(\varphi(\sigma))$ has to divide $\operatorname{ord}(\sigma) = p^n$. It is injective because σ generates A and surjective because A is discrete. Since $\mathbb{Q}_p/\mathbb{Z}_p[p^n]$ is cyclic of order p^n, it is isomorphic to A. By corollary 4.1, $\widehat{A}$ has the discrete topology, so it is also homeomorphic to A. □

Corollary 4.2. If A is an abelian finite discrete p-group, then $\widehat{A}$ is non-canonically isomorphic to A.

Proof. By structure theorem of finite abelian groups, we can write

$$A = C_1 \times \cdots \times C_r$$

where $C_1, \ldots, C_r$ are cyclic p-groups. Since A is also discrete, by proposition 4.11,

$$\widehat{A} = \operatorname{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p) = \operatorname{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p) \cong \operatorname{Hom}(C_1, \mathbb{Q}_p/\mathbb{Z}_p) \times \cdots \times \operatorname{Hom}(C_r, \mathbb{Q}_p/\mathbb{Z}_p) \cong C_1 \times \cdots \times C_r \cong A$$

By corollary 4.1, $\widehat{A}$ has the discrete topology, so it is homeomorphic to A. □

Corollary 4.3. If A is an abelian pro-p group, then $\widehat{A}$ is a discrete p-primary abelian group. Conversely, if A is a discrete, p-primary abelian group, then $\widehat{A}$ is an abelian pro-p group.

Proof. If A is an abelian pro-p group, it is an inverse limit of discrete abelian p-groups. Then proposition 4.9 and corollary 4.2 imply that A is a direct limit of finite discrete abelian groups, so $\widehat{A}$ is discrete, abelian and p-primary. By corollary 4.1, $\widehat{A}$ has also the discrete topology.

On the other hand, assume that A is an abelian, discrete, p-primary group. Since A is torsion, it can be understood as the direct limit of every finite subgroup, with the transition maps given by inclusions. Then proposition 4.10 and corollary 4.2 imply that $\widehat{A}$ is an inverse limit of finite, abelian p-groups. It can be seen, by remark 4.4, that the dual topology is the profinite topology, so $\widehat{A}$ is thus a pro-p group. □

We end this section by showing that in case A is either an abelian pro-p group or a discrete abelian p-primary group, then the Pontryagin bidual is canonically isomorphic to A.

Theorem 4.2. If A is either a p-primary discrete abelian group or an abelian pro-p group, then A is canonically isomorphic to $\hat{\widehat{A}}$.

Proof. If A is a finite, abelian, discrete group, then it is easily seen that the map

$$A \to \hat{\widehat{A}} = \operatorname{Hom}_{cts}(\operatorname{Hom}_{cts}(A, \mathbb{Q}_p/\mathbb{Z}_p)) : \ a \mapsto (\varphi \mapsto \varphi(a))$$

is an isomorphism, because it is clearly injective and both A and $\hat{\widehat{A}}$ are finite with same cardinality.

On the one hand, if A is p-primary, then

$$A = \varinjlim A_i$$

where A_i are the finite subgroups of A, which are finite, abelian, discrete p-groups. Then proposition 4.10 implies that

$$\widehat{A} = \varprojlim \widehat{A_i}$$

where the transition maps are given by

$$\widehat{\varphi_{ji}} : \widehat{A_j} \to \widehat{A_i} : \varphi \mapsto \varphi \circ \varphi_{ij}, \quad i < j$$

where φ_{ij} was the transition map in the direct limit. Then, the bidual group is given by

$$\hat{\hat{A}} = \varinjlim \hat{\hat{A}}_i$$

where the transition maps are given by

$$\hat{\hat{A}}_i \to \hat{\hat{A}}_j : \psi \mapsto \psi \circ \widehat{\varphi_{ji}}$$

Considering the identification $A_i \leftrightarrow \hat{\hat{A}}_i : a \mapsto \hat{\hat{a}}$ given in the first part of this proof and tracing through the definitions, we see that this transition maps are identified with the maps in the original direct limit, so $A \cong \hat{\hat{A}}$ canonically.

On the other hand, if A is a pro-p group then it is the inverse limit of finite discrete p-groups, so the theorem is proven similarly. □

4.5 The Dual $\mathbb{Z}_p$-module

We are going to work with $\mathbb{Z}_p$-modules instead of groups. To do that, notice there is a natural $\mathbb{Z}_p$-module structure in any p-primary abelian group.

Lemma 4.4. Let A be a discrete p-primary abelian group. Then there is a natural continuous action of $\mathbb{Z}_p$ on A.

Proof. Let $\alpha \in \mathbb{Z}_p$ and $a \in A$. Then there is a sequence $(\alpha_n) \subset \mathbb{Z}$ such that $(\alpha_n) \to \alpha$ with the natural topology in $\mathbb{Z}_p$. Since it is a Cauchy sequence, $\alpha_i - \alpha_j \in p^m\mathbb{Z}$ for i and j large enough, where p^m is the order of A. Then $\alpha_n a$ is eventually constant, so we can define αa to be this value. It is clear that this definition does not depend on the sequence chosen and that it really defines an action.

If we denote that action by $\psi : \mathbb{Z}_p \times A \to A$, it is clearly continuous since for every $a \in A$ we have that

$$\psi^{-1}(\{a\}) = \bigcup_{n\in\mathbb{Z}} \bigcup_{b\in A : nb=a} (n + \mathrm{ord}b\mathbb{Z}_p) \times \{b\}$$

which is an open set for being a union of open sets. □

Definition 4.17. Let A be a $\mathbb{Z}_p$-module. Then $\widehat{A}$ is a $\mathbb{Z}_p$-module with an operation defined by

$$\mathbb{Z}_p \times \widehat{A} \to \widehat{A} : (\alpha, \varphi(a)) \mapsto (\alpha\varphi)(a) := \varphi(\alpha a)$$

Remark 4.5. Notice that

$$\varphi(\alpha a) = \alpha\varphi(a)\ \forall \alpha \in \mathbb{Z}_p,\ \forall a \in A,\ \forall \varphi \in \widehat{A}$$

This is true for every $\alpha \in \mathbb{Z}$ because φ is a group homomorphism and then it has to be true for every $\alpha \in \mathbb{Z}_p$ since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and φ is continuous.

Remark 4.6. With the above definition, the natural map

$$A \to \hat{\hat{A}} = \mathrm{Hom}\left(\mathrm{Hom}\left(A, \mathbb{Q}_p/\mathbb{Z}_p\right), \mathbb{Q}_p/\mathbb{Z}_p\right) : \ a \mapsto \widetilde{a}(\varphi) := \varphi(a)$$

is a $\mathbb{Z}_p$-homomorphism. If A is a discrete p-primary group, it is an isomorphism by theorem 4.2.

Lemma 4.5. The natural action $\psi : \mathbb{Z}_p \times \widehat{A} \to \widehat{A}$ is continuous provided that A is locally compact.

Proof. Let $(\alpha, \varphi) \in \mathbb{Z}_p \times \widehat{A}$ and suppose that $\alpha\varphi \in V(K, U)$ for some compact set $K \subset A$ and some open set $U \subset \mathbb{Q}_p/\mathbb{Z}_p$.

Since the action $p : \mathbb{Z}_p \times \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}_p/\mathbb{Z}_p$ given by the usual product is continuous by lemma 4.4, then for every $x \in K$ we can find an open neighbourhood $V_x \subset \mathbb{Z}_p$ of α such that $p\left(V_x, \varphi(x)\right) \subset U$.

Since φ is continuous and A is a locally compact topological group, we can find for each $x \in K$ compact neighbourhood $W_x \subset \varphi^{-1}\left(\varphi(x)\right)$. $\{W_x : x \in K\}$ is a cover of K which has to admit a finite subcover $\{W_{x_1}, \ldots, W_{x_n}\}$ because each W_x contains an open neighbourhood of x which constitute an open cover of K. Therefore,

$$\psi\left[\left(V_{x_1} \times V(W_{x_1}, \varphi(x_1))\right) \cap \cdots \cap \left(V_{x_n} \times V(W_{x_n}, \varphi(x_n))\right)\right] \subset V(K, U)$$

so the action is continuous. □

Example 4.1. We are going to see that $\widehat{\mathbb{Z}_p} \cong \mathbb{Q}_p/\mathbb{Z}_p$. Notice that

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

Then, proposition 4.9 and proposition 4.11 states that

$$\widehat{\mathbb{Z}_p} = \varinjlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Q}_p/\mathbb{Z}_p$$

where the last isomorphism comes from the fact that all the transition maps has to be injective, because that maps were surjective in $\mathbb{Z}_p$.

Similarly, we have that

$$\left(\widehat{\mathbb{Q}_p/\mathbb{Z}_p}\right) \cong \widehat{\widehat{\mathbb{Z}_p}} \cong \mathbb{Z}_p$$

4.6 Corank

Pontryagin dual allow us to characterise some discrete p-primary groups which where not finitely generated as groups. The groups which are cofinitely generated are those whose Pontryagin dual is a finitely generated $\mathbb{Z}_p$-module. Then the structure theorem of finitely generated modules over the principal ideal domain $\mathbb{Z}_p$ classify these groups.

Definition 4.18. Let A be a discrete p-primary group. We say that A is cofinitely generated if $\widehat{A}$ is finitely generated as a $\mathbb{Z}_p$-module. We also say that A has corank r if $\widehat{A}$ has rank r as a $\mathbb{Z}_p$-module.

Remark 4.7. If A is a discrete p-primary group of corank k, then the structure theorem over principal ideal domains imply that $\widehat{A} \cong \mathbb{Z}_p^r \times T$, where T is a finite p-group. Hence theorem 4.2 and example 4.1imply that

$$A \cong \hat{\hat{A}} \cong \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^r \times \widehat{T}$$

Moreover, if A is divisible and cofinitely generated, then $A \cong \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^r$ for some $r \in \mathbb{N} \cup \{0\}$.

The Pontryagin duality also behaves well under taking short exact sequences.

Proposition 4.12. Let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of discrete p-primary abelian groups. Then there is another short exact sequence in the Pontryagin duals

$$0 \longrightarrow \widehat{C} \longrightarrow \widehat{B} \longrightarrow \widehat{A} \longrightarrow 0$$

Proof. Since A, B and C are p-primary discrete abelian groups, we can consider them as $\mathbb{Z}_p$-modules by lemma 4.4. Moreover, $\mathrm{Hom}_{\mathbb{Z}_p,cts}(A, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$.

Since $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible, then [13], Theorem I.7.1. implies that it is injective, so the following short sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(C, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Hom}(B, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow 0$$

□

Corollary 4.4. If A, B and C are p-primary discrete abelian groups such that there is a short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

then

$$\mathrm{corank}_{\mathbb{Z}_p}(B) = \mathrm{corank}_{\mathbb{Z}_p}(A) + \mathrm{corank}_{\mathbb{Z}_p}(C)$$

in the sense that if two of them are cofinitely generated, so is the third one.

Proof. It comes from proposition 4.12 and the fact that the rank is additive. □

Chapter 5

Galois Theory

In this chapter we cover some topics of Galois theory. First of all, we study the basic theory of Kummer extensions, which will appear on the proof of Mordell-Weil theorem. The references used have been [4] and [20]. After that, we expose the generalisation appearing in [21] of Galois theory to infinite field extensions. Finally, section 5.3 identifies the absolute Galois group of a completion with the decomposition subgroup of the absolute Galois group G_K. This fact will be used later to identify the absolute Galois group of p-adic fields as a subgroup of the Galois group of a number field. Last section generalises a result from [21] using theory from [23].

5.1 Kummer Field Extensions

In this section we study Galois extension $L|K$ whose Galois group $G_{L|K}$ is abelian. Denoting by n to the exponent of that group, then we are going to show that the extension is generated by n^{th} square roots of elements in K.

Definition 5.1. Let K be a field containing a primitive n^{th} root of unity. A Galois extension L of K is called an n-Kummer extension of K provided that $G_{L|K}$ is an abelian group whose exponent divides n.

Lemma 5.1. Let K be a field containing a primitive n^{th} root of unity ω, let $L|K$ be a cyclic extension of degree n and let σ be a generator of $G_{L|K}$. Then there is an $a \in L \setminus \{0\}$ with $\omega = \frac{\sigma(a)}{a}$.

Proof. σ can be considered as a K-linear transformation of the K-vector field L. Because σ has order n in $G_{L|K}$, it satisfies the polynomial equation $T^n - 1 = 0$. Furthermore, if there is a polynomial of degree $m < n$ vanishing σ, then the automorphisms $\mathrm{Id}, \sigma, \ldots, \sigma^m$ would be linearly dependent over K, contradicting basic Galois theory. Therefore, the minimal polynomial of σ has degree n and divides $T^n - 1$. Hence it is the minimal and the characteristical polynomial of σ, so ω is an eigenvalue of σ. Thus $\exists a \in L \setminus 0$ such that $\sigma(a) = \omega a$. □

Lemma 5.2. Let K be a field containing a primitive n^{th} root of unity ω and let $L|K$ be a cyclic Galois extension of degree n. Then there is an $a \in L$ such that $L = K(a)$ and $a^n \in K$.

Proof. Let σ be a generator of the Galois group. By lemma 5.1, there is an $a \in L \setminus \{0\}$ such that $\sigma(a) = \omega a$, where ω is a primitive n^{th} root of unity. Since $\sigma^i(a) = \omega^i a$, we see that a is fixed only by the identity automorphism, so $G_{L|K(a)} = \{\mathrm{Id}_L\}$. By the fundamental theorem of Galois theory, $L = K(a)$. Moreover,

$$\sigma(a^n) = \sigma(a)^n = (\omega a)^n = a^n$$

so a^n is fixed by $G_{L|K}$ and hence $a^n \in K$. □

Theorem 5.1. Let K be a field containing a primitive n^{th} root of unity ω and let L be a finite extension of K. Then $L|K$ is an n-Kummer extension if and only if $L = K\left(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r}\right)$.

Proof. Assume that $L = K(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i^n = a_i \in K$. If $\omega \in K$ is a primitive n^{th} root of unity, then the polynomial $f_i(x) = x^n - a_i$ is separable because the distinct elements $\alpha_i, \omega\alpha_i, \ldots, \omega^{n-1}\alpha_i$ are its roots. Hence $L|K$ is a separable extension and it is Galois because it is the splitting field of the polynomial

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

Let $\sigma, \tau \in G_{L|K}$. Given a generator α_i, there exists natural numbers $j, k \in \mathbb{N}$ such that $\sigma(\alpha_i) = \omega^j\alpha_i$ and $\tau(\alpha_i) = \omega^k\alpha_i$ because they have to be roots of the polynomial $x^n - a_i$. Then

$$(\sigma\tau)(\alpha_i) = \sigma(\omega^k\alpha_i) = \omega^k\omega^j\alpha_i = \omega^j\omega^k\alpha_i = \tau(\omega^j\alpha_i) = (\tau\sigma)(\alpha_i)$$

Therefore, $\sigma\tau$ and $\tau\sigma$ agree on the generators of L, so $\sigma\tau = \tau\sigma$. Thus $G_{L|K}$ is abelian.

Furthermore, $\sigma^n(\alpha_i) = \omega^{jn}(\alpha_i) = \alpha_i$ for every generator α_i. Then $\sigma^n = Id_L \ \forall\sigma \in G_{L|K}$, so the exponent of $G_{L|K}$ divides n.

Conversely, assume that $L|K$ is Galois and abelian with exponent dividing n. By the structure theorem of finite abelian groups, $G_{L|K}$ is a direct product of cyclic groups whose orders divide n, i.e. $G_{L|K} = C_1 \times \cdots \times C_r$. Define $H_i := C_1 \times \cdots C_{i-1} \times C_{i+1} \times \cdots \times C_r$, which satisfies that $G/H_i \cong C_i$. Let L_i be the fixed field of H_i, which is Galois over K, since $H_i \triangleleft G_{L|K}$, and $G_{L_i|K} \cong G_{L|K}/H_i \cong C_i$.

Thus, $L_i|K$ is a cyclic Galois extension whose order, say m_i, is the same as $|C_i|$. K contains the m_i^{th} primitive root ω^{n/m_i}, so lemma 5.2 says that $L_i = K(\alpha_i)$, where $\alpha_i^{m_i} \in K$. Since $m_i|n$, we have that $\alpha_i^n = a_i \in K$. Under Galois correspondence, the field $K(\alpha_1, \ldots, \alpha_r) = L_1 \cdots L_r$ corresponds to the group $H_1 \cap \cdots \cap H_r = \{\mathrm{Id}_L\}$, so $L = K(\alpha_1, \ldots, \alpha_r) = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$. □

Corollary 5.1. Let K be a field containing a primitive n^{th} root of unity. Its maximal n-Kummer extension is

$$K\left(\sqrt[n]{a} : a \in K\right)$$

Proof. The first part of the proof of theorem 5.1 does not assume that the number of generators has to be finite, so $K\left(\sqrt[n]{a} : a \in K\right)$ is an n-Kummer extension. Conversely, an n-Kummer extension $L|K$ is the composition of all of its finite Galois subextensions and they have to be contained in $K\left(\sqrt[n]{a} : a \in K\right)$, by theorem 5.1. Then, $L \subset K\left(\sqrt[n]{a} : a \in K\right)$, so the latter is the maximal n-Kummer extension of K. □

5.2 Infinite Galois theory

Galois theory of finite extensions has a generalisation to infinite ones. In this generalisation, profinite groups defined on section 4.3 arise naturally.

Definition 5.2. Let $L|K$ be a possibly infinite Galois extension and let $G_{L|K}$ be its Galois group. The *Krull topology* defined on $G_{L|K}$ is the one such that each automorphism $\sigma \in G_{L|K}$ has a basis of neighbourhoods formed by the cosets

$$\sigma G_{L|M}$$

where M runs through the finite Galois subextensions $M|K$.

Remark 5.1. If $L|K$ is a finite extension, the Krull topology is just the discrete topology on $G_{L|K}$.

Proposition 5.1. Let $L|K$ be a field extension. The Krull topology endows the Galois group $G_{L|K}$ with a topological group structure.

Proof. On the one hand, the map

$$p:\ G_{L|K}\times G_{L|K}\to G_{L|K}:\ (\sigma,\tau)\mapsto\sigma\tau$$

is continuous because

$$\sigma G_{L|M}\times\tau G_{L|M}\subset p^{-1}\left(\sigma\tau G_{L|M}\right)\ \forall\sigma,\tau\in G_{L|K}$$

for every finite Galois extension $M|K$.

On the other hand, the inversion map

$$i:\ G_{L|K}\to G_{L|K}:\ \sigma\mapsto\sigma^{-1}\ \forall\sigma\in G_{L|K}$$

is also continuous because

$$i^{-1}\left(\sigma^{-1}G_{L|M}\right)=\sigma G_{L|M}\ \forall\sigma\in G_{L|K}$$

for every finite Galois extension $M|K$. □

We now show that Galois groups are always profinite groups.

Proposition 5.2. Let $L|K$ be a Galois extension. Then $G_{L|K}$ is compact and Hausdorff with respect to the Krull topology.

Proof. Let σ,τ be distinct elements of $G_{L|K}$, let $x\in L$ be such that $\sigma(x)\neq\tau(x)$ and let $M|K$ the Galois closure of $K(x)$. Then $\sigma|_M\neq\tau|_M$, so $\sigma G_{L|M}\cap\tau G_{L|M}=\emptyset$. The Galois group $G_{L|K}$ is thus Hausdorff.

In order to prove the compactness, consider the map

$$h:\ G_{L|K}\to\prod_M G_{M|K},\ \sigma\mapsto\prod_M\sigma|_M$$

where M varies over the finite Galois subextensions. Since the groups $G_{M|K}$ are finite, its product is a compact topological space due to Tychonoff's theorem. Moreover, h is injective since $\sigma|_M=\mathrm{Id}_M$ for every finite Galois subextension is equivalent to $\sigma=\mathrm{Id}_L$.

The sets

$$U=\prod_{M\neq M_0}G_{L|M}\times\{\overline{\sigma}\}$$

where $\overline{\sigma}\in G_{M_0|K}$ form a subbasis of the product. Let σ be an extension of $\overline{\sigma}$ to L (which exists because of Zorn's lemma). Then

$$h^{-1}(U)=\sigma G_{L|M_0},\quad h(\sigma G_{L|M_0})=h(G_{L|K})\cap U$$

Thus h is an homeomorphism into its image, so we need to show that $h(G)$ is closed. For that purpose, let $F\subset F'$ be two finite Galois extensions and define

$$H_{F'|F}=\left\{\prod_M\sigma_M\in\prod_M G_{M|K}:\sigma_{F'}\big|_F=\sigma_F\right\}$$

The set $H_{F'|F}$ can be easily described. If $G_{F|K} = \{\sigma_1, \ldots, \sigma_n\}$, let $\Sigma_i \subset G_{F'|K}$ be the finite set of extensions of σ_i to F'. Then

$$H_{F'|F} = \bigcup_{i=1}^{n} \left(\prod_{M \neq F, F'} G_{M|K} \times \Sigma_i \times \{\sigma_i\} \right)$$

Hence $H_{F'|F}$ is clearly closed, so

$$h(G) = \bigcap_{F \subset F'} H_{F|F'}$$

is also closed. Therefore, $h(G)$ is compact and so is G. □

Corollary 5.2. Let $L|K$ be a Galois extension. Then $G_{L|K}$ is a profinite group providing that it is endowed with the Krull topology.

Proof. By construction, the identity has a basis of neighbourhoods consisting of open normal subgroups, which will be also closed because their complements are unions of its cosets. Since it is also compact and Hausdorff by proposition 5.2, proposition 4.5 applies. □

Remark 5.2. We can also describe explicitly the Galois group as the following inverse limit

$$G_{L|K} = \varprojlim_{M} G_{M|K}$$

where M runs through all finite Galois subextensions of $L|K$.

Remark 5.3. We have shown that every Galois group is profinite. The converse is also true, as it is shown in [29].

The main theorem of Galois theory can now be stated as follows.

Theorem 5.2. Let $L|K$ be a Galois extension. Then the assignment

$$M \to G_{L|M}$$

is a bijective correspondence between the subextensions $M|K$ of $L|K$ and the closed subgroups of $G_{L|K}$. In this identification, the open sugbroups correspond to the finite subextensions of $L|K$.

Proof. The assignment is well defined, since $G_{L|M}$ is clearly closed, and injective, since M is the fixed field of $G_{L|M}$. For the surjectivity, let H be a closed subgroup of $G_{L|K}$ and let M be its fixed field. Clearly, $H \subset G_{L|M}$. Conversely, let $\sigma \in G_{L|M}$ and let $F|M$ be a finite Galois subextension. The map $H \to G_{F|M}$ is clearly surjective because the fixed field of H is M and the main theorem of Galois theory for finite extensions applies. Then there is some $\tau \in H$ such that $\tau|_F = \sigma|_F$ or, equivalently, $\tau \in \sigma G_{F|M}$. Hence σ belongs to the closure of H in $G_{L|M}$ and, since H is closed, $\sigma \in H$.

Since $G_{L|K}$ is a compact topological group, the open subgroups are the closed ones having finite index. Hence every open subgroup H is of the form $H = G_{L|M}$, where $M|K$ is a subextension. Hence

$$G_{L|K} = \bigsqcup_{\sigma \in G_{M|K}} \sigma G_{L|M}$$

Since $(G_{L|K} : H) < \infty$, then $M|K$ is a finite extension. Conversely, let $M|K$ be a finite extension and let F be its Galois closure. Then for every $\sigma \in G_{L|M}$ then

$$\sigma G_{L|F} \subset G_{L|M}$$

so $G_{L|M}$ is an open subgroup. □

Remark 5.4. In last identification, normal subgroups are identified with Galois subextensions.

5.3 The Absolute Galois Group of a Completion

The goal of this section is to identify the absolute Galois group of a completion K_v of certain field K with respect to certain valuation v with the decomposition group of the absolute Galois group G_K.

Assume we have a Galois extension $L|K$ and let v be a valuation in K that extends to a valuation w in L. If K_v is the completion of K with respect to v and L_w is the direct limit of the completion with respect to the restriction of w to every finite subextension of $L|K$, then the following is a basic result from algebraic number theory.

Proposition 5.3. Let $L|K$ be a Galois extension, let $v \in M_K$ and let $w \in M_L$ be an extension to L. Then there is an isomorphism

$$\left(G_{L|K}\right)_w \cong G_{L_w|K_v}$$

where $\left(G_{L|K}\right)_w$ is the decomposition subgroup of $G_{L|K}$ with respect to the valuation w.

Proof. [21], proposition II. 9.6. □

The problem that appears when we are working with absolute Galois groups is that we do not know a priori whether, given a field K and a valuation v in K that extends to $\overline{v}$ in the algebraic closure, $\overline{K}_{\overline{v}}$ is the algebraic closure of K_v or not. However, that is true and can be seen using Krasner's lemma.

Lemma 5.3. (Krasner) Let K be a complete field with respect to a non-archimedean valuation v that extends to $\overline{K}$. Let $\alpha \in \overline{K}$ be separable over K and let $\alpha = \alpha_1, \dots, \alpha_n$ be its conjugates. Let $\beta \in \overline{K}$ satisfying that

$$|\alpha - \beta| < |\alpha - \alpha_i| \ \forall i = 2, \dots, n$$

Then $K(\alpha) \subset K(\beta)$.

Proof. Consider the extension $K(\alpha, \beta)|K(\beta)$ and let L be its Galois closure. By [21], theorem II. 4.8., the valuation extends uniquely to the algebraic closure, so $\overline{v} \circ \sigma = \overline{v}\ \forall \sigma \in G_K$. Hence for every $\sigma \in G_{L|K(\beta)}$

$$|\beta - \sigma(\alpha)| = |\beta - \alpha| < |\alpha - \alpha_i| \ \forall i = 2, \dots, n$$

Then,

$$|a - \sigma(a)| \leq \max\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\} < |\alpha - \alpha_i| \ \forall i = 2, \dots, n$$

Then $\sigma(\alpha) = \alpha\ \forall \sigma \in G_{L|K(\beta)}$, so $\alpha \in K(\beta)$. □

Proposition 5.4. Let K be a field and let $v \in M_K$ be a prime. Then

$$\overline{K_v} = (\overline{K})_v \ ^1$$

Proof. The result is clear if v is archimedean since both fields would be equal to $\mathbb{C}$ in that case. That is a consequence of Ostrwski's theorem, which is proven in [21], II.4.2. Hence we can assume without loss of generality that v is non-archimedean.

Since $(\overline{K})_v$ is the union of finite extensions of K_v, the inclusion $(\overline{K})_v \subset \overline{K_v}$ is clear. Conversely, let $\alpha \in \overline{K_v}$, let $f \in K_v[T]$ be its minimal polynomial and let

$$x := \min\{|\alpha - \alpha_i| : \ i = 2, \dots, n\}$$

Since K is dense in K_v, we can find a polynomial $g \in K[T]$ such that

$$|g(\alpha)| < |g(\alpha) - f(\alpha)| < x^n$$

[1] Notice the abuse of notation we are doing by denoting the extension of v to the algebraic closure indistinctly.

If $g(x) = \prod_{j=1}^{n}(x - \beta_j)$ there is some $\beta \in \{\beta_1, \ldots, \beta_n\}$ such that

$$|\alpha - \beta| < x$$

By lemma 5.3, we have that

$$\alpha \in K_v(\beta) = (K(\beta))_v \subset \left(\overline{K}\right)_v$$

□

We can thus identify the absolute Galois group of the completion K_v with a subgroup of G_K.

Corollary 5.3. Let K be a field and let K_v be its completion with respect to a certain prime. Then

$$G_{K_v} \cong (G_K)_v$$

Remark 5.5. Notice that the decomposition group $(G_K)_v$ depends on the extension of v to the algebraic closure. However, choosing a different extension would only give a conjugate subgroups since the Galois groups acts transitively on the different extensions by [21], proposition II.9.1.

Chapter 6

Group Cohomology

This chapter is dedicated to show an introduction to the cohomological theory of finite and profinite groups. We have developed first the continuous cohomology for profinite groups, which also applies to the finite case. After that, we have extended this definition to the Tate cohomology groups, which have only been defined for finite groups.

First of all, in section 6.1 are the cohomology groups introduced and described when its dimension is low. Coinduced modules also appear on this section and they are very important for the development of the cohomological theory because they are cohomologically trivial. Section 6.2 is dedicated to the most important result in this area: the long cohomological exact sequence. In particular, it is the base of the dimension-shifting technique.

Up to now, all changes studied are referred to the G-module. However, section 6.3 studies how a change in the group affects to the cohomology. This section has many interesting results for computing the cohomology groups. First of all, it is stated that the cohomology of profinite groups can be computed as a direct limit of the cohomology of finite ones. We have also defined inflation and restriction maps, which can be encapsulated in a really useful exact sequence. Finally, corestriction map gives some conditions of triviality of some cohomology groups. In particular, it implies that the cohomology of uniquely divisible modules always vanishes.

Tate-cohomology groups are defined in section 6.4. As we have mentioned above, we have only defined them for finite groups. They play an important role in the study of the cohomology of cyclic groups, in section 6.5. In this section, we have also stated the concept of Herbrand quotient.

Section 6.6 introduces the cup-product, which appear in the results of section 6.7. This results are the foundations of the local class field theory, that will be exposed in chapter 7.

Finally, section 6.8 studies some cohomology groups of the p-adic integers. These computations will be needed in chapters 8 and 11

6.1 The Cohomology Groups

Let G be a profinite group and let A be a topological G-module endowed with the discrete topology. Let $X^n = X^n(G, A) = \mathrm{Map}(G^{n+1}, A)$ be the abelian group consisting of all continuous maps from G^{n+1} to A. $X^n(G, A)$ is a G-module in the way given by

$$(\sigma x)(\sigma_0, \dots, \sigma_n) := \sigma x(\sigma^{-1}\sigma_0, \dots, \sigma^{-1}\sigma_n)$$

We also define the connecting homomorphisms by

$$\partial^n : X^{n-1} \to X^n : \ x \mapsto \partial x; \quad (\partial x)(\sigma_0, \ldots, \sigma_n) := \sum_{i=0}^{n} (-1)^i x(\sigma_0, \ldots, \widehat{\sigma_i}, \ldots, \sigma_n)$$

Furthermore, there is a G-homomorphism $\partial^0 : A \to X^0$ that associates every $a \in A$ to the constant function $x(\sigma_0) = a \ \forall \sigma_0 \in G$.

At this point, it is important to remark that given a continuous function $x : G^n \to A$, we get another continuous function by adding a new variable that plays no role, i.e., the function

$$G^{n+1} \to A : \ (\sigma_0, \ldots, \sigma_n) \mapsto x(\sigma_0, \ldots, \widehat{\sigma_i}, \ldots, \sigma_n)$$

is still a continuous function when considered as a function from G^{n+1}. Because A is a topological G-module, ∂x is also continuous. Therefore the connecting homomorphisms are well defined.

Proposition 6.1. The sequence

$$0 \longrightarrow A \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \xrightarrow{\partial^3} \cdots$$

is exact.

Proof. Clearly, it is a cochain complex, since $\partial\partial = 0$ (every term appears exactly twice with different sign). To see the exactness, consider the group homomorphisms $D^{-1} : X^0 \to A : x \mapsto x(1)$ and

$$D^n : X^{n+1} \to X^n : x \mapsto D^n x; \quad (D^n x)(\sigma_0, \ldots, \sigma_n) := x(1, \sigma_0, \ldots, \sigma_n) \ \forall n \geq 0$$

Similarly, D^n is well defined because it maps continuous functions to continuous maps. A simple calculation shows that

$$D^n \circ \partial^{n+1} + \partial^n \circ D^{n-1} = \mathrm{Id}_{X^n}$$

If $x \in \ker(\partial^{n+1})$, then $x = (\partial^n \circ D^{n-1})(x) \in \mathrm{Im}\,(\partial^n)$. As $\partial \circ \partial = 0$, then $\ker(\partial^{n+1}) = \mathrm{Im}\,(\partial^n)$, so the sequence is exact. □

The next step consists on changing the groups X^n by their subgroups of elements fixed by G, which will be denoted by

$$C^\bullet(G, A) := X^\bullet(G, A)^G$$

Therefore, $C^n(G, A)$ consists of the continuous functions $x : G^{n+1} \to A$ such that

$$x(\sigma\sigma_0, \ldots, \sigma\sigma_n) = \sigma x(\sigma_0, \ldots, \sigma_n)$$

From the exact sequence given by proposition 6.1, we obtain the sequence

$$C^0(G, A) \xrightarrow{\partial^1} C^1(G, A) \xrightarrow{\partial^2} C^2(G, A) \xrightarrow{\partial^3} \cdots$$

which in general is no longer exact but it is still a cochain complex.

Definition 6.1. In the exact sequence above mentioned, we will refer as *n-cocylces* to the elements of $Z^n(G, A) = \ker \partial^{n+1}$ and as *n-coboundaries* to the elements of $B^n(G, A) = \mathrm{Im}(\partial^n)$.

Since $\partial\partial = 0$, it is clear that $B^n(G, A) \subset Z^n(G, A)$. Therefore, it makes sense to give the following definition.

Definition 6.2. For $n \geq 0$, we define the *n-dimensional cohomology group* of G with coefficients in A as the factor group

$$H^n(G, A) := Z^n(G, A)/B^n(G, A)$$

where $B^0(G, A) := \{0\}$.

6.1.1 $H^0(G,A)$ and $H^1(G,A)$

For computational purposes, it is convenient to change the cochain complex $C^\bullet(G,A)$ via the isomorphism

$$C^n(G,A) \to X^{n-1}(G,A):\ x(\sigma_0,\dots,\sigma_n) \mapsto y(\sigma_1,\dots,\sigma_n) := x(1,\sigma_1,\sigma_1\sigma_2,\dots,\sigma_1\cdots\sigma_n)$$

It is clearly an isomorphism since its inverse map is given by

$$X^{n-1}(G,A) \to C^n(G,A) : y(\sigma_1,\dots,\sigma_n) \mapsto x(\sigma_0,\dots,\sigma_n) := \sigma_0 \cdot y(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \cdots, \sigma_{n-1}^{-1}\sigma_n)$$

Notice that these identification do not arise any problem related to continuity.

Under this identification, the first coboundary operators are given by

$$(\partial^1 a)(\sigma) = \sigma a - a, \qquad (\partial^2 y)(\sigma,\tau) = \sigma y(\tau) - y(\sigma\tau) + y(\sigma)$$

There is a natural identification of $C^0(G,A)$ with A by associating every G-invariant map $x:\ G \to A$ to its evaluation $x(1)$.[1] Under this identification, the elements $a \in Z^0(G,A)$ are such elements satisfying

$$\partial^1 a(\sigma) = \sigma a - a = 0\ \forall \sigma \in G$$

Hence, the 0-cocycles are the elements of A fixed by G. Because there are no 0-coboundaries, we have just proven that

$$H^0(G,A) = A^G$$

In order to study the first cohomology groups $H^1(G,A)$, we have to note that the 1-cocycles are the continuous functions $x: G \to A$ satisfying that

$$x(\sigma\tau) = x(\sigma) + \sigma x(\tau)\ \forall \sigma,\tau \in G \tag{6.1}$$

Nevertheless, to compute the first cohomology group $H^1(G,A)$, it is necessary to note that the coboundaries are the functions

$$x: G \to A:\ \sigma \mapsto \sigma a - a \quad [2]$$

It is interesting to consider the case where G acts trivially on A, i.e., $\sigma a = a\ \forall \sigma \in G,\ \forall a \in A$. In this case, the only 1-coboundary is the zero map, while 1-cocycles are exactly the same as the homomorphisms in $\mathrm{Hom}(G,A)$. Thus, the first homology group would be

$$H^1(G,A) = \mathrm{Hom}(G,A)$$

6.1.2 Coinduced Modules

One strength of cohomology lies on the fact that, given a profinite group G, there is a special kind of G-modules whose cohomology groups are trivial for every $n \geq 1$. These groups are called coinduced.

Definition 6.3. Given a profinite group G, a G-module A is said to be *coinduced* if $A = \mathrm{Map}(G,X)$ consists of all continuous functions from G to X, where X is an abelian group and its G-module structure is given by

$$(\sigma x)(\sigma_0) = \sigma x(\sigma^{-1}\sigma_0)$$

[1] For this identification, note that every map $G \to A:\ \sigma \mapsto \sigma a$ is continuous because A is a topological G-module.

[2] Note that these functions are continuous because A is a topological G-module.

From every G module A, we can build a coinduced module by considering

$$\mathrm{Ind}_G(A) := \mathrm{Map}(G, A)$$

Moreover, there is a canonical injection

$$i : A \hookrightarrow \mathrm{Ind}_G(A)$$

which maps an element $a \in A$ to the constant function onto this value. This injection induces the following short exact sequence:

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}_G(A) \longrightarrow A' \longrightarrow 1$$

The key fact for defining coinduced modules is that they have trivial cohomology groups for every $n \geq 1$.

Lemma 6.1. Coinduced G-modules are acyclic, i.e., its cohomology groups are null for every $n \geq 1$.

Proof. Since every group can be given a G-module structure (where G acts trivially), we can suppose that our coinduced module is $\mathrm{Ind}_G(A)$, where A is a G-module. Then, consider the map

$$\psi : C^n(G, \mathrm{Ind}_G(A)) \to X^n(G, A),\ x(\sigma_0, \ldots, \sigma_n) \mapsto y(\sigma_0, \ldots, \sigma_n) := x(\sigma_0, \ldots, \sigma_n)(1)$$

It is clear that it commutes with ∂ and it is an isomorphism since its inverse is given by

$$\phi : X^n(G, A) \to C^n(G, \mathrm{Ind}_G(A)) : y(\sigma_0, \ldots, \sigma_n) \mapsto x(\sigma_0, \ldots, \sigma_n)(\sigma) = \sigma y(\sigma^{-1}\sigma_0, \ldots, \sigma^{-1}\sigma_n)$$

By definition, $\psi \circ \phi = \mathrm{Id}_{X^n(G,A)}$. Furthermore, the definition says that

$$(\phi \circ \psi)(x)(\sigma_0, \ldots, \sigma_n)(1) = x(\sigma_0, \ldots, \sigma_n)(1)$$

Moreover, since $(\phi \circ \psi)(x)$ is G-invariant,

$$(\phi \circ \psi)(x)(\sigma_0, \ldots, \sigma_n)(\sigma) = \sigma \cdot \left(\sigma^{-1}(\phi \circ \psi)(x)\right)(\sigma_0, \ldots, \sigma_n)(1) =$$
$$\sigma \cdot (\phi \circ \psi)(x)(\sigma^{-1}\sigma_0, \ldots, \sigma^{-1}\sigma_n)(1) = \sigma \cdot (\sigma^{-1}x)(\sigma_0, \ldots, \sigma_n)(1) = x(\sigma_0, \ldots, \sigma_n)(\sigma)$$

Since this identification commutes with the boundary morphism, there is an isomorphism of cochain complexes

$$C^\bullet(G, \mathrm{Ind}_G(A)) \cong X^\bullet(G, A)$$

Nevertheless, $X^\bullet(G, A)$ is exact, so

$$H^n(G, \mathrm{Ind}_G(A)) = H^n(C^\bullet(G, \mathrm{Ind}_G(A))) = H^n(X^\bullet(G, A)) = 0\ \forall n \geq 1$$

□

Another important property of coinduced modules is that they behave well under taking subgroups or quotients. In order to see that, we need a technical lemma about the existence of continuous sections.

Lemma 6.2. Let G be a profinite group and let H be a subgroup. Let G/H the quotient space induced by right multiplication of elements in H and let

$$\pi : G \to G/H^3$$

be the canonical projection. Then there is a continuous section

$$\sigma : G/H \to G$$

such that $\sigma(1H) = 1$.

[3]Note that in case H is not a normal subgroup, then G/H has not got a canonical group structure. Indeed, by G/H we will refer to the set of right cosets.

Proof. Assume first that H is finite. Because G is Hausdorff and the identity element has a base of neighbourhoods consisting of normal open groups, we can find an open normal group such that $U \cap H = \{1\}$. Therefore the restriction $\pi|_U$ is injective. Since G is compact and $G \setminus U$ is a union of cosets of U, U is closed and, therefore, compact. Since G/H is Hausdorff, $\pi|_U$ is an homeomorphism onto its image. Call $\sigma : \pi(U) \to U$ to its inverse and let $\mathcal{R} = \{x_1 \ldots, x_n\}$ be a system of representatives of G/U. Given $i, j \in \{1, \ldots, n\}$ then either $\pi(Ux_i) = \pi(Ux_j)$ or $\pi(Ux_i) \cap \pi(Ux_j) = \emptyset$. Since this images are compact, then there is a cover of G/H consisting of a finite number of closed sets to which σ can be extended by translation. This extension will be continuous for being so when restricted to a finite closed cover. Clearly, $\sigma(1H) = 1$.

For the gereral case, let $\mathcal{P}$ the set of all pairs (L, η), where K is a closed subgroup of H and $\eta : G/H \to G/K$ is a continuous section of the canonical projection $G/K \to G/H$ such that $\eta(1H) = 1K$. We can define a partial order in P as follow: $(K_1, \eta_1) \geq (K_2, \eta_2)$ if $K_1 \subset K_2$ and the following diagram is commutative

$$\begin{array}{ccc} G/H & & \\ \downarrow{\scriptstyle \eta_1} & \searrow{\scriptstyle \eta_2} & \\ G/K_1 & \xrightarrow{\pi} & G/K_2 \end{array}$$

Let $\{(K_i, \eta_i) : i \in I\} \subset \mathcal{P}$ be a totally ordered subset, where I has been chosen to be a directed set. Define $K := \bigcap_{i \in I} K_i$. It can be seen that

$$G/K = \varprojlim_{i \in I} G/K_i$$

The condition of total order implies that $\{\eta_i : i \in I\}$ are compatible maps which induce, by the universal property of the inverse limit a continuous section

$$\eta : G/H \to G/K$$

By Zorn's lemma, $\mathcal{P}$ contains a maximal element (T, σ). If $T \neq \{1\}$, then there is a normal open group such that $T \cap U \subsetneq T$. Since $T/T \cap U$ is finite, then the first part of this proof implies that there is a continuous section

$$\xi : G/(T \cap U) \to G/T$$

Then the composition

$$\sigma \circ \xi : G/(T \cap U) \to G/H$$

is a continuous section, which contradicts the maximality of the pair (T, σ). □

Remark 6.1. Last section is not necessarily a group homomorphism, even though H is normal.

Corollary 6.1. Let G be a profinite group and let H be a closed subgroup. Then there is an homeomorphism

$$H \times G/H \to G$$

Proof. Consider the continuous map

$$\psi : H \times G/H \to G : \ (h, x) \mapsto \sigma(x)h$$

which it is bijective because its inverse is

$$G \to H \times G/H : g \mapsto \left(\left[\sigma(\pi(g))\right]^{-1} g, \pi(g) \right)$$

Since H is closed, then $H \times G/H$ is compact, so ψ has to be an homeomorphism because G is Hausdorff. □

Remark 6.2. Last homeomorphism is not necessarily a group homomorphism.

Proposition 6.2. Given a G-module A and a closed subgroup $H \subset G$, then $\mathrm{Ind}_G(A)$ is a coinduced H-module.

Proof. We can write

$$\mathrm{Ind}_G(A) = \mathrm{Map}(G, A) = \mathrm{Map}(H \times G/H, A) = \mathrm{Map}(H, \mathrm{Map}(G/H, A))$$

If we define the trivial action of H on G/H, then the previous identification is H-equivariant, so $\mathrm{Map}(G, A)$ is an H-induced module □

Proposition 6.3. Given a G-module A and a closed normal subgroup H, then $\mathrm{Ind}_G(A)^H$ is a coinduced G/H-module.

Proof. It comes from the fact that $\mathrm{Ind}_G(A) \cong \mathrm{Map}(G/H, \mathrm{Map}(H, A))$. Since H acts trivially on G/H, then $\mathrm{Ind}_G(A)^H = \mathrm{Map}\left(G/H, \mathrm{Map}(H, A)^H\right)$. Both modules can be considered as G/H modules and this identification is clearly equivariant with the action of G/H. □

6.2 The Long Cohomological Exact Sequence

In this section we prove the existence of the long cohomological exact sequence, which is the most powerful cohomological tool and has numerous consequences. It is based on the naturality of the well known snake's lemma. This lemma also appeared on chapter 2, but we feel this is the right place to proof it.

Lemma 6.3. Let R be a ring, let A, B, C, A', B' and C' be R-modules and let the following commutative diagram have exact rows.

$$\begin{array}{ccccccccc} & & A & \xrightarrow{\mu} & B & \xrightarrow{\varepsilon} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\mu'} & B' & \xrightarrow{\varepsilon'} & C' & & \end{array}$$

Then, there is a connecting homomorphism $\delta : \ker\gamma \to \mathrm{coker}\alpha$ such that the following sequence is exact:

$$\begin{array}{ccccccc} \ker\alpha & \xrightarrow{\mu_*} & \ker\beta & \xrightarrow{\varepsilon_*} & \ker\gamma & & \\ & & & \overset{\delta^n}{\searrow} & & & \\ \mathrm{coker}\alpha & \xrightarrow{\mu'_*} & \mathrm{coker}\beta & \xrightarrow{\varepsilon'_*} & \mathrm{coker}\gamma & & \end{array}$$

Moreover, if μ is a monomorphism, so is μ_* and ε'_* is an epimorphism provided that ε' is.

Proof. Last statement is clear. On the other hand, the commutative property of the diagram is responsible of the fact that the exact sequence on the first row could be restricted to the kernels:

$$\ker\alpha \xrightarrow{\mu_*} \ker\beta \xrightarrow{\varepsilon_*} \ker\gamma$$

It is clear that $\varepsilon_* \circ \mu_* = 0$. Furthermore, given $b \in \ker\varepsilon_*$, $\exists a \in A$ such that $\mu(a) = b$. Then, $\mu'\alpha(a) = \beta\mu(a) = \beta(b) = 0$. Since μ' is injective, $a \in \ker\alpha$ and, therefore, $b \in \mathrm{Im}(\mu_*)$. Hence, the restricted sequence is exact $\ker\beta$.

Furthermore, the exact sequence in the second row induce an exact sequence on the cokernels:

$$\mathrm{coker}\alpha \xrightarrow{\mu'_*} \mathrm{coker}\beta \xrightarrow{\varepsilon'_*} \mathrm{coker}\gamma$$

In fact, it is clear that $\varepsilon'_* \circ \mu'_* = 0$. Conversely, given $b' \in B'$ such that $b' + \mathrm{Im}(\beta) \in \ker \varepsilon'_*$, then $\varepsilon'(b') \in \mathrm{Im}(\gamma)$ and, since ε is surjective, $\varepsilon'(b) \in \mathrm{Im}(\gamma \circ \varepsilon)$, so $\exists b \in B$ such that $\gamma\varepsilon(b) = \varepsilon'(b') = \varepsilon'\beta(b)$. Thus $b' - \beta(b) \in \ker \varepsilon' = \mathrm{Im}\ \mu'$. Then $\exists a' \in A'$ such that $\mu'(a') = b' - \beta(b)$. Hence, $\mu'_*(a' + \mathrm{Im}\ \alpha) = b' + \mathrm{Im}\ \beta$.

The connecting homomorphism δ is defined as follows. Given $c \in \ker \gamma$, choose $b \in B$ such that $\varepsilon(b) = c$. Since $\varepsilon'\beta(b) = \gamma\varepsilon(b) = \gamma c = 0$, then $\beta(b) \in \ker(\varepsilon') = \mathrm{Im}\ \mu'$. Since μ' is injective, $\exists! a' \in A'$ such that $\mu'(a') = \beta(b)$. We define $\delta(c) := a' + \mathrm{Im}\ \alpha$. Providing that δ is well-defined, it is clear that it is an homomorphism.

We just need to check that the definition of δ is independent of the choice of b. Then, let $b' \in B$ be such that $\varepsilon(b') = c$. Then, $b' = b + \mu(a)$, for some $a \in A$, and $\beta(b') = \beta(b) + \beta\mu(a) = \beta(b) + \mu'\alpha(a)$. Therefore, the values of δ associated to b and b' differ in an element of the image of α, so they represent the same element in the cokernel.

Next step is to prove the exactness at $\ker \gamma$. If $c \in \mathrm{Im}\ \varepsilon_*$, then $\exists b \in \ker \beta$ such that $\varepsilon(b) = c$. Then, $\beta(b) = 0$, so $\delta(c) = 0$ too. Conversely, let $c \in \ker(\delta)$ and choose $b \in B$ such that $\varepsilon(b) = c$. Then there exists $a \in A$, such that $\beta(b) = \mu'\alpha(a) = \beta\mu(a)$. Defining $b' := \beta - \mu(a)$, then $\beta(b') = \beta(b) - \beta\mu(a) = c + 0 = c$, so $c \in \mathrm{Im}\ \varepsilon_*$.

Last step is to show the exactness at cokerα. Assume that $\delta(c) = a' + \mathrm{Im}\ \alpha$. That means that $\exists b \in B$ such that $\varepsilon(b) = c$ and $\beta(b) = \mu'(a')$. Then,

$$\mu'_*(a' + \mathrm{Im}\ \alpha) = \mu'(a') + \mathrm{Im}\ \beta = \beta(b) + \mathrm{Im}\ \beta = 0 + \mathrm{Im}\ \beta$$

Conversely, if $a' + \mathrm{Im}\ \alpha \in \ker \mu'_*$, then $\mu'(a') = \beta(b)$ for some $b \in B$. Clearly, $\delta\varepsilon(b) = a' + \mathrm{Im}\ \alpha \in \mathrm{Im}(\delta)$. □

Lemma 6.4. For every short exact sequence $0 \longrightarrow A \xrightarrow{\mu} B \xrightarrow{\varepsilon} C \longrightarrow 0$ of G-modules, there are homomorphisms

$$\delta^n : H^n(G, C) \to H^{n+1}(G, A)$$

such that the following sequence is exact:

$$\begin{array}{ccccccc}
0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G \\
 & & & \overset{\delta^0}{\searrow} & & & \\
 & & H^1(G,A) & \longrightarrow & H^1(G,B) & \longrightarrow & H^1(G,C) \\
 & & & \overset{\delta^1}{\searrow} & & & \\
 & & H^2(G,A) & \longrightarrow & H^2(G,B) & \longrightarrow & H^2(G,C) \\
 & & & \searrow & & & \\
 & & H^n(G,A) & \longrightarrow & H^n(G,B) & \longrightarrow & H^n(G,C)
\end{array}$$

Proof. Given that exact sequence, then

$$0 \longrightarrow X^{n-1}(G, A) \xrightarrow{\mu_*} X^{n-1}(G, B) \xrightarrow{\varepsilon_*} X^{n-1}(G, C) \longrightarrow 0$$

is well defined since the G-module homomorphisms μ and ε are continuous when A, B and C are endowed with the discrete topology.. The exactness at $X^{n-1}(G, A)$ and $\varepsilon_* \circ \mu_* = 0$ are clear facts. Given $\varphi \in \ker \varepsilon_*$, let $\psi = \mu^{-1} \circ \varphi(b)$, where μ^{-1} is a right inverse for μ. Notice that ψ is well defined and continuous since $\varphi(\sigma) \in \ker \varepsilon = \mathrm{Im}(\mu)\ \forall \sigma \in G^n$. It is clear that $\mu_*(\psi) = \varphi \in \mathrm{Im}(\mu_*)$ and the sequence is exact at $X^{n-1}(G, B)$.

On the other hand, we want to show that ε_* is surjective. Since ϵ is surjective, there is a section $\sigma : C \to B$ such that $\varepsilon \circ \sigma = \mathrm{Id}_C$. Then given $\varphi \in X^n(G, C)$, $\sigma \circ \varphi \in X^{n-1}(G, B)$ is a preimage of φ, so ε_* is surjective.

Using the inhomogeneous identification $C^n(G, A) \cong X^{n-1}(G, A)$ which commutes with the induced maps μ_* and ε_*, it is easy to see that the following sequence is exact.

$$0 \longrightarrow C^n(G, A) \longrightarrow C^n(G, B) \longrightarrow C^n(G, C) \longrightarrow 0$$

Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & C^n(G, A) & \longrightarrow & C^n(G, B) & \longrightarrow & C^n(G, C) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \partial_A} & & \downarrow{\scriptstyle \partial_B} & & \downarrow{\scriptstyle \partial_C} \\ 0 & \longrightarrow & C^{n+1}(G, A) & \longrightarrow & C^{n+1}(G, B) & \longrightarrow & C^{n+1}(G, C) \longrightarrow 0 \end{array}$$

The first part of the exact sequence given by the snake lemma 6.3 applied to this diagram could be understood as

$$0 \longrightarrow Z^n(G, A) \longrightarrow Z^n(G, B) \longrightarrow Z^n(G, C)$$

Alternatively, calling $\overline{C}^n(G, A) = C^n(G, A)/B^n(G, A)$, the second part of the exact sequence of lemma 6.3 is

$$\overline{C}^n(G, A) \longrightarrow \overline{C}^n(G, B) \longrightarrow \overline{C}^n(G, C) \longrightarrow 0$$

As the $C^\bullet(G, -)$ are cochain complexes, $B^n(G, -) \subset \ker \delta_n$, so the quotient maps induce the following commutative diagram

$$\begin{array}{ccccccc} & & \overline{C}^n(G, A) & \longrightarrow & \overline{C}^n(G, B) & \longrightarrow & \overline{C}^n(G, C) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \overline{\partial}_A} & & \downarrow{\scriptstyle \overline{\partial}_B} & & \downarrow{\scriptstyle \overline{\partial}_C} \\ 0 & \longrightarrow & Z^{n+1}(G, A) & \longrightarrow & Z^{n+1}(G, B) & \longrightarrow & Z^{n+1}(G, C) \end{array}$$

Noting that $H^n(G, A) = \ker \overline{\partial_A}$ and $H^{n+1}(G, A) = \operatorname{coker} \partial_A$, the snake lemma 6.3 gives the exact sequence

$$\begin{array}{ccccc} H^n(G, A) & \longrightarrow & H^n(G, B) & \longrightarrow & H^n(G, C) \\ & & \xrightarrow{\delta^n} & & \\ H^{n+1}(G, A) & \longrightarrow & H^{n+1}(G, B) & \longrightarrow & H^{n+1}(G, C) \end{array}$$

Gluing it for all $n \in \mathbb{N}$, we obtain the desired long exact sequence. □

That long exact sequence allows us to adopt a technique, called *dimension shifting* which let us study certain properties of higher dimensional cohomology groups by proving them on a single dimension. Consider the exact sequence

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}_G(A) \longrightarrow A' \longrightarrow 0$$

As $\mathrm{Ind}_G(A)$ is cohomologically trivial, the long exact sequence is written as

$$0 \longrightarrow A^G \longrightarrow \mathrm{Ind}_G(A)^G \cong A \longrightarrow A'^G \longrightarrow H^1(G, A) \longrightarrow 0$$

$$0 \longrightarrow H^{n-1}(G, A') \longrightarrow H^n(G, A) \longrightarrow 0$$

Last exact sequences means that there is an isomorphism $H^{n-1}(G, A) \cong H^n(G, A)$.

6.3 Change of Groups

We have just seen that a short exact sequence of G-modules induces a long sequence in the cohomology groups. However, we can also change the group G and it will have a consequence in the cohomology groups. These changes have interesting properties that will be useful for the purpose of computing cohomology groups.

Consider two profinite groups G and G', a G-module A, a G'-module A' and two continuous homomorphisms

$$\varphi : G' \to G, \quad f : A \to A'$$

such that $f(\varphi(\sigma')a) = \sigma'(f(a))\ \forall \sigma' \in G',\ \forall a \in A$. This condition ensures that $f \circ x \circ \varphi^k$ is G'-invariant for every $x \in C^n(G, A)$, so the following homomorphism is well defined

$$\psi : C^n(G, A) \to C^n(G', A') : x \mapsto f \circ x \circ \varphi^{n+1} \tag{6.2}$$

It clearly commutes with the connecting homomorphism ∂, so we have the following commutative diagram:

$$\begin{array}{ccc} C^n(G,A) & \xrightarrow{\psi} & C^n(G',A') \\ \downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle \partial} \\ C^{n+1}(G,A) & \xrightarrow{\psi} & C^{n+1}(G',A') \end{array}$$

Chasing at this diagram, it is clear that if $x \in Z^n(G, A) \subset C^n(G, A)$, then $(\partial \circ \psi)(x) = (\psi \circ \partial)(x) = 0$, so $\psi(x) \in Z^n(G', A')$.

On the other hand, if $y \in B^{n+1}(G, A)$, then $\exists x \in C^n(G, A)$ such that $y = \partial x$. Since $(\partial \circ \psi)(x) = (\psi \circ \partial)(x) = \psi(y)$, we have that $\psi(y) \in B^{n+1}(G', A')$.

Therefore, ψ maps cocycles to cocyles and coboundaries to coboundaries, so it induces a homomorphism in the cohomology groups:

$$H^n(G, A) \to H^n(G', A')$$

If we have two compatible pairs of homomorphisms

$$G'' \longrightarrow G' \longrightarrow G\ , \qquad A \longrightarrow A' \longrightarrow A''$$

then the homomorphism $H^n(G, A) \to H^n(G'', A'')$ is the composite of the homomorphism induced by each pair, i.e.,

$$H^n(G, A) \longrightarrow H^n(G', A') \longrightarrow H^n(G'', A'')$$

Hence the cohomology groups $H^n(G, A)$ are functorial in G and A simultaneously.

Now we can prove the relations of cohomology groups after taking direct and inverse limits.

Proposition 6.4. Let $(G_i)_{i\in I}$ be a projective system of profinite groups and let $(A_i)_{i\in I}$ be a direct system, where each A_i is a G_i-module and the transition maps

$$\varphi_{ji} : G_j \to G_i, \quad f_{ij} : A_i \to A_j$$

are compatible for every pair $i \leq j$. Then defining $G = \varprojlim_{i\in I} G_i$ and $A = \varinjlim_{i\in I} A_i$, we have

$$H^n(G, A) \cong \varinjlim_{i\in I} H^n(G_i, A_i)$$

where the transition maps in the direct limit are the induced homomorphisms

$$H^n(G_i, A_i) \to H^n(G_j, A_j),\ a \mapsto f_{ij} \circ a \circ \varphi_{ji}$$

Proof. Since the pairs $G_j \to G_i$ and $A_i \to A_j$ are compatible, the action

$$G \times A \to A : \ ((g_i)_{i\in I}, a_i) \mapsto g_i a_i$$

is well defined and makes A into a G-module. Moreover the pairs $G \to G_i$, $A_i \to A$ are compatible for every $i \in I$. Then there are canonical homomorphisms

$$\kappa_i : \ C^n(G_i, A_i) \to C^n(G, A)$$

This maps are compatible in the sense that they induce an homomorphism from the direct limit:

$$\kappa : \ \varinjlim_{i\in I} C^n(G_i, A_i) \to C^n(G, A)$$

We want to see that κ is an isomorphism. For the surjectivity, let $x \in C^n(G, A)$. Since G is compact and A is discrete, then x only takes a finite amount of values. By continuity, $x^{-1}(\{a\})$ is open for every $a \in A$, so by proposition 4.5 there is an open normal subgroup U such that x factors through

$$\overline{x} : \ (G/U)^{n+1} \to A$$

Since the profinite topology is induced from the product topology, there are some finite set of $\{i_1, \dots, i_h\} \subset I$ such that

$$\bigcap_{i=1}^{h} \ker(\pi_i) \subset U$$

If k is an upper bound of $\{i_1, \dots, i_h\}$, then $\ker(\pi_k) \subset U$, so x factors through

$$\overline{x} : \ G_k \to A$$

Since the image of x is finite, there is some $l \geq k$ such that every element in the image has a representative in A_l. Therefore, x factors through

$$\overline{x} : \ G_l \to A_l$$

and x is the image of the class generated by $\overline{x}$ in the direct limit.

To see the injectivity, let $x_i \in C^n(G_i, A_i)$ be a cochain that becomes zero in $C^n(G, A)$ when changing the group, i.e., the composition

$$G^{n+1} \longrightarrow G_i^{n+1} \xrightarrow{x_i} A_i \longrightarrow A$$

vanishes. However, since x_i takes only finitely many values, there exists some $j \geq i$ such that the composite

$$G_j^{n+1} \longrightarrow G_i^{n+1} \xrightarrow{x_i} A_i \longrightarrow A_j$$

vanishes. Then x_i has an equivalent cochain which is zero in $C^n(G_j, A_j)$, which shows the injectivity of κ.

Since κ clearly commutes with ∂, then it induces an isomorphism in the cohomology groups. □

The importance of this result resides in the fact that we can now compute the cohomology of profinite groups just by studying the cohomology of the finite ones.

Corollary 6.2. Let G be a profinite group and let A be a G-module. Then the cohomology groups can be described as follows.

$$H^n(G, A) = \varinjlim_{U} H^n(G/U, A^U)$$

where the direct limit is taken over the normal subgroups U of G.

Now we can consider some special changes of groups:

- **Conjugation**: For this case, let H be a closed subgroup of G, let A be a G-module and B an H-submodule of A. If we denote the conjugation by $\tau^\sigma := \sigma^{-1}\tau\sigma$ and ${}^\sigma H := \sigma H \sigma^{-1}$, we have the following pair of compatible homomorphisms for each $\sigma \in G$:

$$ {}^\sigma H \to H,\ \tau \mapsto \tau^\sigma, \quad B \to \sigma B,\ b \mapsto \sigma b $$

which induce the isomorphism in the cohomology groups, called the *conjugation isomorphisms*

$$ \sigma_* : H^n(H, B) \to H^n({}^\sigma H, \sigma B) $$

whose inverse is given by σ^{-1}. Moreover, this correspondence is functorial since

$$ 1_* = Id, \quad (\sigma\tau)_* = \sigma_*\tau_* $$

We are going to focus in the case in which H is a normal subgroup of G, so ${}^\sigma H = H$. Then, G acts by conjugation on $H^n(H, A)$. We are going to see that the restricted action to H is trivial, so $H^n(G, A)$ becomes a G/H module.

Proposition 6.5. Let G be a profinite group and let A be a G-module. Then the conjugation $\sigma_* : H^n(G, A) \to H^n(G, A)$ is the identity for every $\sigma \in G$.

Proof. We are going to proceed by induction, being the assertion trivial in $H^0(G, A) = A^G$. We assume it is also true for $n-1$ and consider the following exact sequence.

$$ 0 \longrightarrow A \longrightarrow \mathrm{Ind}_G(A) \longrightarrow A' \longrightarrow 0 $$

Then the long cohomological exact sequence induce the following commutative diagram.

$$ \begin{array}{ccc} H^{n-1}(G, A') & \xrightarrow{\delta} & H^n(G, A) \\ \downarrow{\scriptstyle \sigma_*} & & \downarrow{\scriptstyle \sigma^*} \\ H^{n-1}(G, A') & \xrightarrow{\delta} & H^n(G, A) \end{array} $$

By hypothesis the conjugation σ_* is the identity on $H^{n-1}(G, A')$. Since δ is an isomorphism for $n > 1$ and surjective for $n = 1$, it has to be the identity on $H^n(G, A)$ too. □

Corollary 6.3. Let G be a profinite group, let H be a closed normal subgroup and let A be a G module. Then $H^n(H, A)$ is a G/H module and the action is given by conjugation.

- **Inflation**: Let H be a normal closed subgroup of G and let A a be G-module. Then the submodule A^H consisting of the points in A which are fixed by H is clearly a G/H-module. The projection and injection

$$ G \to G/H, \quad A^H \hookrightarrow A $$

form a compatible pair of homomorphisms. Then, they induce the following homomorphism between cohomology groups, called inflation:

$$ \mathrm{Inf}\ {}_G^{G/H} : H^n(G/H, A^H) \to H^n(G, A) $$

Inflation is a transitive homomorphism. Suppose we have two closed normal subgroups subgroups satisfying that $H \subset K$. Then it is clear that we have the following commutative diagrams:

$$ \begin{array}{ccc} G & \longrightarrow & G/H \\ & \searrow & \downarrow \\ & & G/K \end{array} \qquad \begin{array}{ccc} A^K & \longrightarrow & A^H \\ & \searrow & \downarrow \\ & & A \end{array} $$

Hence, the way homomorphisms between cohomology groups are constructed, by the formula given in the equation 6.2, it is clear that we have the identity

$$\mathrm{Inf}\,{}_{G}^{G/H} \circ \mathrm{Inf}\,{}_{G/H}^{G/K} = \mathrm{Inf}\,{}_{G}^{G/K}$$

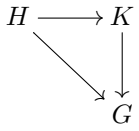
- **Restriction**: Similarly, if we have an arbitrary closed subgroup H of G and a G-module A, there is a pair of compatible homomorphisms given the inclusion and the identity:

$$H \hookrightarrow G, \quad A = A$$

which induces a homomorphism in the cohomology groups

$$\mathrm{Res}\,{}_{H}^{G} : H^n(G, A) \to H^n(H, A)$$

Similarly, restriction is transitive since, given the closed subgroups $H \subset K$, we have the following commutative diagram



so the induced homomorphisms between the cohomology groups satisfy the identity

$$\mathrm{Res}\,{}_{H}^{K} \circ \mathrm{Res}\,{}_{K}^{G} = \mathrm{Res}\,{}_{H}^{G}$$

When U is an open subgroup of G, then besides the restriction there is another map in the opposite direction, which is called corestriction. However, we need to consider some technical lemma before defining it.

Lemma 6.5. If

$$0 \longrightarrow A \longrightarrow Y^0 \xrightarrow{\partial_0} Y^1 \xrightarrow{\partial_1} Y^2 \xrightarrow{\partial_2} \cdots$$

is an acyclic resolution of A, i.e., $H^n(G, Y^n) = 0\ \forall n \geq 1$, then canonically

$$H^n(G, A) \cong H^n(H^0(G, Y^\bullet))$$

Proof. We can consider the exact sequences

$$0 \longrightarrow \quad A \quad \longrightarrow Y^0 \xrightarrow{\partial_0} \ker(\partial_1) \quad \longrightarrow 0$$

$$0 \longrightarrow \ker(\partial_n) \longrightarrow Y^n \xrightarrow{\partial_n} \ker(\partial_{n+1}) \longrightarrow 0$$

Since the modules Y^n are acyclic, lemma 6.4 gives the following isomorphisms:

$$H^1\left(G, \ker(\partial_{n-1})\right) \cong H^2\left(G, \ker(\partial_{n-1})\right) \cong \cdots \cong H^n(G, A)$$

Moreover, same lemma 6.4 gives another exact sequence

$$H^0\left(K, Y^{n-1}\right) \longrightarrow H^0\left(G, \ker(\partial_n)\right) \xrightarrow{\delta} H^1\left(G, \ker(\partial_{n-1})\right) \longrightarrow 0$$

Furthermore, we can compute

$$H^0\left(G, \ker(\partial_n)\right) = \ker\left(H^0\left(G, Y^n\right) \to H^0\left(G, \ker(\partial_{n+1})\right)\right) = \ker\left(H^0\left(G, Y^n\right) \to H^0\left(G, Y^{n+1}\right)\right)$$

$$\mathrm{Im}\left(H^0\left(G, Y^{n-1}\right) \to H^0\left(G, \ker(\partial_n)\right)\right) = \mathrm{Im}\left(H^0\left(G, Y^{n-1}\right) \to H^0\left(G, Y^n\right)\right)$$

Then there is an isomorphism

$$H^1\left(G, \ker(\partial_{n-1})\right) \cong \frac{H^0\left(G, \ker(\partial_n)\right)}{\mathrm{Im}\left(H^0\left(G, Y^{n-1}\right) \to H^0\left(G, \ker(\partial_n)\right)\right)} = \frac{\ker\left(H^0\left(G, Y^n\right) \to H^0\left(G, Y^{n+1}\right)\right)}{\mathrm{Im}\left(H^0\left(G, Y^{n-1}\right) \to H^0\left(G, Y^n\right)\right)}$$

Therefore there is a canonical isomorphism

$$H^n(G, A) \cong H^1\left(G, \ker(\partial_{n-1})\right) \cong H^n\left(H^0\left(G, Y^\bullet\right)\right)$$

□

Definition 6.4. Let G be a profinite group, let $U \subset G$ be an open subgroup and let A be a G-module. Since $X^n(G, A) = \mathrm{Ind}_G(X^{n-1}(G, A))$, then $X^n(G, A)$ are acyclic by lemma 6.1 and we can consider the acyclic resolution

$$0 \longrightarrow A \longrightarrow X^0(G, A) \xrightarrow{\partial} X^1(G, A) \xrightarrow{\partial} \cdots$$

By lemma 6.5, $H^n(U, A) = H^n\left(X^\bullet(G, A)^U\right)$. Moreover, there is a norm map

$$N_{G|U} : (X^n)^U \to (X^n)^G : \varphi \mapsto \sum_{\sigma \in R} \sigma \cdot \varphi$$

where R is a system of representatives of G/U, where the quotient is taken by right multiplication. Clearly, the norm map commutes with ∂, so taking cohomology groups of these cochain complexes we obtain a canonical homomorphism called *corestriction*.

$$\mathrm{Cor}\ {}^U_G : H^n(U, A) \to H^n(G, A)$$

Given two open subgroups $V \subset U \subset G$, it is easily seen that $N_{G/U} \circ N_{U/V} = N_{G/V}$. Therefore, corestriction is transitive:

$$\mathrm{Cor}\ {}^U_G \circ \mathrm{Cor}\ {}^V_U = \mathrm{Cor}\ {}^V_G$$

Proposition 6.6. If U is an open subgroup of G, then

$$\mathrm{Cor}\ {}^U_G \circ \mathrm{Res}\ {}^G_U = (G : U)$$

Proof. Let's proceed by induction. For $n = 0$, identifying $H^0(G, A) = A^G$ and $H^n(U, A) = A^U$, the restriction is the inclusion $A^G \hookrightarrow A^U$ and the corestriction is the norm map

$$N_{G|U} : \ A^U \to A^G : \ a \mapsto \sum_{\sigma \in R} \sigma a$$

It is thus clear that the composition is the multiplication in A^G by the index $(G : U)$.

For the general case, we are going to use dimension shifting. Assume the proposition is true for $n - 1$, when $n \geq 1$ and consider the exact sequence

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}_G(A) \longrightarrow A' \longrightarrow 0$$

Since $\mathrm{Ind}_G(A)$ is also a coinduced U-module by proposition 6.2, then there are surjective homomorphisms

$$\delta : H^{n-1}(G, A') \to H^n(G, A), \quad \delta : H^{n-1}(U, A') \to H^n(U, A)$$

These identifications are group homomorphisms, so they commute with the multiplication by $(G : U)$. Since $\mathrm{Cor}\ {}^{U}_{G} \circ \mathrm{Res}\ {}^{G}_{U} = (G : U)$ in $H^{n-1}(G, A')$ by the induction hypothesis and the boundary maps are surjective, then it suffices to check that the following diagram is commutative.

$$\begin{array}{ccccc} H^{n-1}(G, A') & \xrightarrow{\mathrm{Res}} & H^{n-1}(U, A') & \xrightarrow{\mathrm{Cor}} & H^{n-1}(G, A') \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\ H^{n}(G, A) & \xrightarrow{\mathrm{Res}} & H^{n}(U, A) & \xrightarrow{\mathrm{Cor}} & H^{n}(G, A) \end{array}$$

However, this is clear since both restriction and norm map commute with ∂. □

Proposition 6.7. Let G be a profinite group, let U be an open subgroup and let $n \in \mathbb{N} \cup \{0\}$. For every discrete G-module A such that $H^n(U, A) = 0$, we have

$$(G : U)H^n(G, A) = 0$$

Proof. Given $\varphi \in H^n(G, A)$, we have

$$\mathrm{Res}\ {}^{G}_{U}(\varphi) \in H^n(U, A) = 0 \Rightarrow \mathrm{Res}\ {}^{G}_{H}(\varphi) = 0$$

Then proposition 6.6 says that

$$(G : U)\varphi = \left(\mathrm{Cor}^{U}_{G} \circ \mathrm{Res}^{G}_{U}\right)(\varphi) = \mathrm{Cor}^{U}_{G}(0) = 0$$

Thus $(G : U)H^n(G, A) = 0$. □

Proposition 6.8. Let A be a G-module. Assume that multiplication by p is an automorphism of A for every prime number $p|\#G$. Then,

$$H^n(G, A) = 0$$

for every $n \geq 1$.

Proof. Assume first that G is finite of order $m = \#G$. Since multiplication by m is the composition of multiplication by prime numbers dividing it, then it is also an automorphism of A. Then, multiplication by m also induces automorphisms in the cohomology groups $H^n(G, A)$. However, proposition 6.7 applied to the subgroup $H = \{1_G\}$ implies that multiplication by m annihilates the cohomology group, since $n \geq 1$. Hence $H^n(G, A) = 0$.

Assume now that G is profinite and let $U \subset G$ be an open normal subgroup and let $m = \#G/U$. Again, multiplication by m is a composition of multiplications by prime $p|\#G$, which are automorphisms by hypothesis. Then multiplication by m is an automorphism so it is still an automorphism after taking U-invariants, i.e., $m : A^U \to A^U$ is still a well-defined isomorphism. Since G/U is finite, first part of the proof implies that $H^n(G/U, A^U) = 0$. By corollary 6.2,

$$H^n(G, A) = \varinjlim_{i \in I} H^n(G/U, A^U) = 0$$

□

Corollary 6.4. Let G be a profinite group and let A be a G-module. If A is a uniquely divisible group, i.e., for every $a \in A$ and $n \in \mathbb{N}$ there is a unique $b \in A$ such that $nb = a$, then A is cohomologically trivial, i.e.,

$$H^n(H, A) = 0\ \forall H \subset G$$

Another implication of proposition 6.7 is that cohomology groups are torsion.

Corollary 6.5. Let G be a profinite group and let A be a G-module. Then $H^n(G, A)$ is G-torsion for $n \geq 1$. Moreover, the prime decomposition of the order of every element in $H^n(G, A)$ contains only primes dividing $|G|$.

Proof. Let $\varphi \in H^n(G, A)$. By corollary 6.2, there is some open normal subgroup U such that φ has a representative in $H^n(G/U, A^U)$. By proposition 6.7, $(G : U)\varphi = 0$ □

Since cohomology groups are torsion, we can study their p-primary parts.

Proposition 6.9. Let G be a profinite group and let A be a torsion G-module. Then

$$H^n(G, A)_p = H^n(G, A_p)$$

Proof. Since A is torsion, then

$$A = \bigoplus_{p \text{ prime}} A_p$$

Since the boundary maps act independently on each factor, it is easily seen that

$$H^n(G, A) = \bigoplus_{p \text{ prime}} H^n(G, A_p)$$

Since $H^n(G, A_p)$ is p-primary and primary decomposition is unique, then

$$H^n(G, A)_p = H^n(G, A_p)$$

□

The restriction to Sylow subgroups has the important property of being injective, which will be very useful to compute certain cohomology groups.

Lemma 6.6. Let G be a profinite group, let A be a G-module and let G_p be a p-Sylow p-subgroup. Then

$$\text{Res} : \ H^n(G, A)_p \to H^n(G_p, A)$$

is injective for every $n \in \mathbb{N}$.

Proof. By proposition 4.3 and corollary 6.2, we can assume G is finite. Since $(G : G_p)$ is prime to p, by proposition 6.6, $\text{Cor} \circ \text{Res} = (G : G_p)$ is an automorphism of $\widehat{H}^n(G, A)_p$. It implies that the restriction map is injective. □

Corollary 6.6. Let G be a profinite group, let A be a G-module and let $n \in \mathbb{N}$. If for every prime p, $H^n(G_p, A)_p = 0$ for some p-Sylow subgroup, then $H^n(G, A) = 0$.

We now introduce a different change of group. One can define another cohomological operation, called transgression.

Proposition 6.10. Let H be a normal closed subgroup of G and let A be a G-module. Then there exists a canonical homomorphism, called *transgression*:

$$tg : \ H^1(H, A)^{G/H} \to H^2(G/H, A^H)$$

where $H^1(H, A)$ is understood as a G/H-module because of corollary 6.3. This homomorphism is defined as follows: given $x \in C^1(H, A)$ a representative of an element $[x] \in H^1(H, A)$, there is a cochain $y \in C^1(G, A)$ such that $y|_{H^2} = x$ and that ∂y is contained in A^H and depends only on the cosets of H, so may be regarded as a 2-cocycle in $H^2(G/H, A^H)$. Then we define

$$tg\,([x]) = [\partial y]$$

Proof. We will work with inhomogeneous cochains. Let $s : G/H \to G$ be a section of the canonical projection such that $s(1H) = 1$, given by lemma 6.2. Since x is invariant by conjugation under every $\gamma \in G/H$, then

$$\tau \mapsto s(\gamma)x\left(s(\gamma)^{-1}\tau s(\gamma)\right) - x(\tau)$$

has to be a 1-coboundary. Therefore, there is an element $y\left(s(\gamma)\right) \in A$ such that

$$s(\gamma)x\left(s(\gamma)^{-1}\tau s(\gamma)\right) - x(\tau) = \tau y\left(s(\gamma)\right) - y\left(s(\gamma)\right)$$

Since $s(1H) = 1$, we can assume that $y(1) = 0$. Moreover, the compactness of G implies that the left hand side takes only finitely many values, so proposition 4.7 says we can find an open subgroup $U \subset G$ such that all of these values belong to A^U and depends only on the cosets of G/U. This means that we can take for $y(s\gamma)$ the same value for every γ in a fixed coset of G/U, what will make $y : \ G/H \to A, \ \gamma \mapsto y\left(s(\gamma)\right)$ to be a continuous function.

Now, for an arbitrary $\sigma \in G$, there is a unique factorization $\sigma = s(\gamma)\tau$, where $\gamma \in G/H$ and $\tau \in H$. Then we define

$$y(\sigma) := y\left(s(\gamma)\right) + s(\gamma)x(\tau)$$

Hence it is clear that $y|_H = x$.

Now, let $\sigma = s(\gamma)\tau' = g\tau' \in G$, where $\tau' \in H$. Let also $\tau \in H$. Since x is a 1-cocycle,

$$y(\sigma\tau) = y(g\tau'\tau) = y(g)+gx(\tau'\tau) = y(g)+gx(\tau')+g\tau'x(\tau) = y(\sigma)+\sigma x(\tau) = y(\sigma)+\sigma y(\tau) \quad (6.3)$$

Furthermore, the definition of y gives that

$$y(\tau g) = y(g\tau^g) = y(g) + gx(\tau^g) = y(g) + x(\tau) + \tau y(g) - y(g) = x(\tau) + \tau y(g)$$

Hence, using equation 6.3 we obtain

$$y(\tau\sigma) = y(\tau g\tau') = y(\tau g) + \tau g x(\tau') = x(\tau) + \tau y(g) + \tau g x(\tau') = y(\tau) + \tau y(\sigma) \quad (6.4)$$

Now we can show that ∂y depends only on the right cosets of H. In fact, given $\sigma_1, \sigma_2 \in G$ and $\tau \in H$, using equation 6.3

$$\partial y(\sigma_1, \sigma_2\tau) = \sigma_1 y(\sigma_2\tau) - y(\sigma_1\sigma_2\tau) + y(\sigma_1) = \sigma_1 y(\sigma_2) + \sigma_1\sigma_2 y(\tau) - y(\sigma_1\sigma_2\tau) + y(\sigma_1) = \\ \sigma_1 y(\sigma_2) - y(\sigma_1\sigma_2) + y(\sigma_1) = \partial y(\sigma_1, \sigma_2)$$

For over, both equations 6.3 and 6.4 give us

$$\partial y(\sigma_1\tau, \sigma_2) = \sigma_1\tau y(\sigma_2) - y(\sigma_1\tau\sigma_2) + y(\sigma_1\tau) = \sigma_1 y(\tau\sigma_2) - \sigma_1 y(\tau) - y(\sigma_1\tau\sigma_2) + y(\sigma_1\tau) = \\ \sigma_1 y(\tau\sigma_2) - y(\sigma_1\tau\sigma_2) + y(\sigma_1) = \partial y(\sigma_1, \tau\sigma_2) = \partial y(\sigma_1, \sigma_2\tau^{\sigma_2}) = \partial y(\sigma_1, \sigma_2)$$

Using the fact that

$$\partial\partial y(\tau, \sigma_1, \sigma_2) = \tau\partial y(\sigma_1, \sigma_2) - \partial y(\tau\sigma_1, \sigma_2) + \partial y(\tau, \sigma_1\sigma_2) - \partial y(\sigma_1, \sigma_2) = 0$$

since $\partial y(\tau, \sigma_i) = \partial y(1, \sigma_i) = y(1) = 0$, we get that

$$\tau\partial y(\sigma_1, \sigma_2) = \partial y(\tau\sigma_1, \sigma_2) - \partial y(\tau, \sigma_1\sigma_2) + \partial y(\tau, \sigma_1) = \partial y(\sigma_1, \sigma_2)$$

so $\partial y(\sigma_1, \sigma_2) \in A^H$. Since it is a cocycle because $\partial\partial y = 0$, then it represents an element in $H^2(G/H, A^H)$.

The only step remaining is checking that transgression is well defined, since in that case it would be clearly an homomorphism. For that purpose, let $y' : \ G \to A$ be another cochain such that $y'|_H$ and $\partial y'(\sigma_1, \sigma_2)$ takes values in A^H which depend only on the cosets $\sigma_1 H$ and $\sigma_2 H$. Calling $z := y - y'$, we get that $z|_H = 0$. Then the fact that $\partial z(\sigma, \tau) = \partial z(\sigma, 1) = 0$ implies that $z(\sigma\tau) = z(\sigma)$, so $z(\sigma)$ depend only on the coset σH. Furthermore, since $\partial z(\tau, \sigma) = \partial z(1, \sigma) = 0$, then $\tau z(\sigma) = z(\tau\sigma) = z(\sigma\tau^\sigma) = z(\sigma)$, so $z(\sigma) \in A^H$. Therefore, z represents a cochain of G/H with values in A^H, so ∂z is a coboundary. Thus ∂y and $\partial y'$ represents the same element in $H^2(G/H, A^H)$. □

6.3.1 Inflation-Restriction Sequence

There is an important exact sequence that relates inflation, restriction and transgression.

Theorem 6.1. Let H be a closed normal subgroup of G, and let A be a G-module. Then, the sequence

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A)^{G/H} \xrightarrow{tg} H^2(G/H, A^H)$$

is exact.

Proof. To check the exactness at $H^1(G/H, A^H)$, let $f : G/H \to A^H$ be a 1-cocycle, which induces a 1-cocycle $\overline{f} \in H^1(G, A)$ via the composition

$$\overline{f} : \ G \longrightarrow G/H \xrightarrow{f} A^H \longrightarrow A$$

The fact that $f \in \ker(\text{Inf})$ means that $\overline{f}$ is a coboundary, i.e., there is an $a \in A$, such that $\overline{f}(\sigma) = \sigma a - a \ \forall \sigma \in G$. However, $\overline{f}$ has to be constant on the cosets of H in G, so

$$\sigma a - a = \sigma\tau a - a \ \forall \sigma \in G, \ \forall \tau \in H$$

Taking $\sigma = 1_G$, we get that $\tau a = a \ \forall \tau \in H$. Thus, $a \in A^H$, so f is a coboundary and inflation is injective.

The second step of the proof is to check that $\text{Res} \circ \text{Inf} = 0$. For that purpose, let $f \in H^1(G/H, A^H)$ be a cocycle and let $\overline{f}$ be as above. It is clear that $\overline{f}|_H$ is constant and it has to be equal to $f(1)$. Moreover, the condition of 1-cocycle given in equation 6.1 says that $f(1) = f(1) + f(1)$, so $f(1) = 0$. Hence, $\overline{f}|_H = 0$, which means that $\text{Res} \circ \text{Inf}(f) = 0$.

The next step is checking that $\ker(\text{Res}) \subset \text{Im}(\text{Inf})$. For that purpose, let $\phi \in \ker(\text{Res}) \subset H^1(G, A)$. Then, its restriction to H has to be a coboundary, i.e., $\varphi(\tau) = \tau a - a \ \forall \tau \in H$. Subtracting from φ the coboundary $G \to A : \ \sigma \mapsto \sigma a - a$, we get another representative $\tilde{\varphi}$ of the same element in the factor group $H^1(G, A)$ that satisfies that $\tilde{\varphi}|_H = 0$. Hence, consider the characterization of cocycles given by equation 6.1:

$$\tilde{\varphi}(\sigma\tau) = \tilde{\varphi}(\sigma) + \sigma\tilde{\varphi}(\tau) \ \forall \sigma, \tau \in G$$

Taking $\tau \in H$, we see that $\tilde{\varphi}(\sigma\tau) = \tilde{\varphi}(\sigma)$, so $\tilde{\varphi}$ is constant in the cosets of H in G. Moreover, taking $\sigma \in H$, we see that $\tilde{\varphi}(\tau) = \tilde{\varphi}(\sigma\tau) = \sigma\tilde{\varphi}(\tau)$, so the image of $\tilde{\varphi}$ is contained in A^H. Then, $\tilde{\varphi}$ can be considered as a map from G/H to A^H. Since G/H has the quotient topology and A^H inherits the subspace topology, that map would be continuous, so it would represent an element in $H^1(G/H, A^H)$. Therefore, $\varphi \in \text{Inf}\left(H^1(G/H, A^H)\right)$.

Moreover, corollary 6.3, implies that the image of the restriction map is invariant by G/H, so that arrow is well defined. To check the exactness at $H^1(H, A)^{G/H}$, suppose that $x = \text{Res}(y) \in H^1(H, A)^H$ for some $y \in H^1(G, A)$. Then y can be used to compute the transgression of x, so $tg([x]) = [\partial y] = 0$. Conversely, let $x \in \ker(tg)$. Then there is some $y \in C^1(G, A)$ such that $y|_{H^2} = x$ and that $[\partial y] = tg([x]) = 0$. Then ∂y is a 2-coboundary in $C^2(G/H, A^H)$, so there is some $z \in C^1(G/H, A^H)$ such that $\partial y = \partial z$. As a function in $C^1(G, A)$, $y - z$ is a 1-cocycle. Since $\text{Res}(y - z)$ and $\text{Res}(y) = x$ are cocycles in $C^1(H, A)$, so is $\text{Res}(z)$. Since z is constant in H, then it is clear that $\text{Res}(z) = 0$, so $[x] = \text{Res}([y - z]) \in \text{Im}(\text{Res})$. □

Theorem 6.2. Let $n \geq 1$, let G be a finite group and let H be a normal closed subgroup and assume that $H^q(H, A) = 0 \ \forall q \in \{1, \ldots, n-1\}$. Then the sequence

$$0 \longrightarrow H^n(G/H, A^H) \xrightarrow{\text{Inf}} H^n(G, A) \xrightarrow{\text{Res}} H^n(H, A)$$

is exact.

Proof. We will use the dimension shifting technique, being theorem 6.1 the base case. By induction, suppose that $n > 1$ and that the result is true for $n-1$. Consider the exact sequence

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}_G(A) \longrightarrow A' \longrightarrow 0$$

Since $\mathrm{Ind}_G(A)$ is also coinduced as an H-module because of proposition 6.2, we have seen that the long cohomology exact sequence imply that

$$H^q(H, A') \cong H^{q+1}(H, A) = 0 \ \forall q \in \{1, \dots, n-2\}$$

Hence A' satisfies the theorem hypothesis for $n-1$, so inductive hypothesis could be applied. Furthermore, since $H^1(H, A) = 0$, the first part of the long cohomological exact sequence reduces to

$$0 \longrightarrow A^H \longrightarrow \mathrm{Ind}_G(A)^H \longrightarrow (A')^H \longrightarrow 0$$

Moreover, $\mathrm{Ind}_G(A)^H$ is coinduced as a G/H module due to proposition 6.3. Consider then the following commutative diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{n-1}(G/H, A'^H) & \xrightarrow{\mathrm{Inf}} & H^n(G, A') & \xrightarrow{\mathrm{Res}} & H^n(H, A') \\
 & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\
0 & \longrightarrow & H^n(G/H, A^H) & \xrightarrow{\mathrm{Inf}} & H^n(G, A) & \xrightarrow{\mathrm{Res}} & H^n(H, A)
\end{array}$$

We knew that the vertical lines were isomorphisms due to the long cohomological sequence and the cohomological triviality of coinduced modules. Since the top row is exact by the inductive hypothesis, so is the bottom line. □

6.4 Cohomology of Finite Groups

In case G is a finite group, we can extend the standard resolution $X^n(G, A)$ to obtain the *complete standard resolution.* Hence we define

$$X^{-n-1}(G, A) := X^n(G, A) := \mathrm{Map}(G^{n+1}, A) \ \forall n \geq 0$$

For $n < 0$, the transition maps are defined as

$$\partial^n : \ X^{n-1} \to X^n : \ (\partial^n x)(\sigma_0, \dots, \sigma_{n-1}) = \sum_{\tau \in G} \sum_{i=0}^{n} (-1)^i x(\sigma_0, \dots, \sigma_{i-1}, \tau, \sigma_i, \dots, \sigma_{n-1})$$

For $n = 0$, the differential map is defined as

$$\partial^0 : \ X^{-1} \to X^0 : \ (\partial^0 x)(\sigma_0) = x\left(\sum_{\tau \in G} \tau\right)$$

Defining the maps $D^{-n} : \ X^{-n+1} \to X^{-n}$ as follows

$$(D^{-1}x)(\sigma_0) = \delta_{\sigma_0,1} x(1), \quad (D^{-n}x)(\sigma_0, \dots, \sigma_{n-1}) = \delta_{\sigma_0,1} x(\sigma_1, \dots, \sigma_{n-1}) \ \forall n > 1$$

where δ represents the Kronecker's delta function. The following identity is satisfied

$$D^n \circ \partial^{n+1} + \partial^n \circ D^{n-1} = \mathrm{Id}_{X^n(G,A)}$$

Hence we have an exact sequence

$$\cdots \longrightarrow X^{-2} \xrightarrow{\partial^{-1}} X^{-1} \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \longrightarrow \cdots$$

After considering the G-invariant elements, we can consider a cochain complex

$$\widehat{C}^\bullet(G,A) = (X^\bullet(G,A))^G$$

The *Tate cohomology groups* or *modified cohomology groups* are defined as the cohomology groups of this complex:

$$\widehat{H}^n(G,A) := H^n\left(\widehat{C}^\bullet(G,A)\right)$$

Remark 6.3. For $n \geq 1$ the cohomology group is the same as the Tate-cohomology group:

$$H^n(G,A) = \widehat{H}^n(G,A)\ \forall n \geq 1$$

It is possible to compute some cohomology groups using inhomogeneous cochains. Under the identification

$$\widehat{C}^n(G,A) \to X^{n-1}(G,A):\ x(\sigma_0,\ldots,\sigma_n) \mapsto y(\sigma_1,\ldots,\sigma_n) := x(1,\sigma_1,\sigma_1\sigma_2,\ldots,\sigma_1\cdots\sigma_n)$$

the 0^{th} boundary map is just the *norm map*:

$$\partial^0:\ A \to A:\ a \mapsto N_G(a) := \sum_{\sigma\in G} \sigma a$$

Hence, the 0^{th} Tate-cohomology group can be written as

$$\widehat{H}^0(G,A) \cong A^G/N_G(A)$$

Again under this identification, the boundary homomorphism has also a simple expression

$$\partial^{-1}:\ X^0(G,A) \to A:\ x \mapsto \sum_{\sigma\in G}\left(\sigma^{-1}x(\sigma) - x(\sigma)\right)$$

Hence, the -1-coboundaries are

$$\widehat{B}^{-1}(G,A) = I_G A = \{(\sigma-1)a:\ \sigma\in G,\ a\in A\}$$

The Tate Cohomology group is thus

$$\widehat{H}^{-1}(G,A) =_{N_G} A/I_G A$$

where ${}_{N_G}A$ represents the kernel of the norm map.

The cohomological triviality of coinduced modules and the long cohomological exact sequence also applies to modified cohomology groups, being their proofs similar.

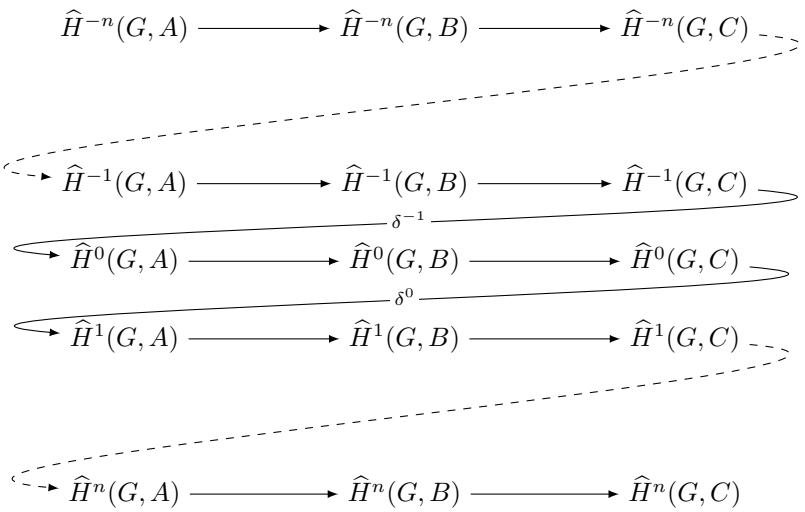
Proposition 6.11. Let G be a finite group and let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of G-modules. Then there are connecting homomorphisms

$$\delta^n : \widehat{H}^n(G,C) \to \widehat{H}^{n+1}(G,A)$$

such that the following sequence is exact:



Proposition 6.12. Let G be a finite group and let A be a coinduced G-module. Then

$$\widehat{H}^n(G,A) = 0 \ \forall n \in \mathbb{Z}$$

In case of finite groups, coinduced modules can be also identified as some tensor products.

Lemma 6.7. If G is a finite group and A is a G-module, there is an isomorphism

$$\mathrm{Ind}_G(A) \cong \mathbb{Z}[G] \otimes A$$

Proof. Consider the map:

$$\psi : \mathrm{Ind}_G(A) \to \mathbb{Z}[G] \otimes A : \ \varphi \mapsto \sum_{\sigma \in G} \sigma \otimes \varphi(\sigma)$$

It is a G-homomorphism since

$$\psi(\sigma\varphi) = \sum_{\tau \in G} \tau \otimes \sigma\varphi(\sigma^{-1}\tau) = \sum_{\tau \in G} \sigma\tau \otimes \sigma\varphi(\tau) = \sigma\left(\sum_{\tau \in G} \tau \otimes \varphi(\tau)\right) = \sigma\psi(\varphi)$$

On the other hand, the billinear map

$$\mathbb{Z}[G] \times A \to \mathrm{Ind}_G(A) : (\{n_\sigma\}_{\sigma \in G}, a) \mapsto \varphi; \ \varphi(\sigma) := n_\sigma a \ \forall \sigma \in G$$

induces an homomorphism $\mathbb{Z}[G] \otimes A \to \mathrm{Ind}_G(A)$ which is the inverse of ψ. □

Defining the G-modules

$$I_G := \langle (\sigma - 1) \in \mathbb{Z}[G] : \ \sigma \in G \rangle, \qquad J_G := \mathbb{Z}[G]/\mathbb{Z} \cdot N_G$$

there are exact sequences

$$0 \longrightarrow I_G \otimes A \longrightarrow \mathbb{Z}[G] \otimes A \xrightarrow{\varepsilon} A \longrightarrow 0$$
$$0 \longrightarrow A \xrightarrow{N_G} \mathbb{Z}[G] \otimes A \longrightarrow J_G \otimes A \longrightarrow 0$$

where ε is induced by the *augmentation map*, which is defined as

$$\varepsilon :\ \mathbb{Z}[G] \to \mathbb{Z} :\ \sum_{\sigma\in G} n_\sigma \sigma \mapsto \sum_{\sigma\in G} n_\sigma$$

If we define $A^0 = A$ and, inductively

$$A^m := J_G \otimes A^{m-1}\ \forall m \geq 0$$
$$A^m := I_G \otimes A^{m+1}\ \forall m \leq 0$$

then, by dimension-shifting, there are isomorphisms

$$\delta^m :\ \widehat{H}^{n-m}(G, A^m) \to \widehat{H}^n(G, A)\ \forall n, m \in \mathbb{Z}$$

We end this section giving a characterisation of the group $\widehat{H}^{-2}(G, \mathbb{Z})$.

Proposition 6.13. Let G be a finite group. Then there is a canonical isomorphism

$$\widehat{H}^{-2}(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$$

Proof. By lemma 6.7, $\mathbb{Z}[G]$ is a coinduced module. Define the ideal

$$I_G = \langle \sigma - 1 :\ \sigma \in G \rangle$$

Consider thus the following short exact sequence

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

By lemma 6.7, $\mathbb{Z}[G]$ is a coinduced module. Hence proposition 6.11 implies that there is an isomorphism

$$\delta :\ \widehat{H}^{-2}(G, \mathbb{Z}) \to \widehat{H}^{-1}(G, I_G) = I_G/I_G^2$$

For this, consider the map

$$G \to I_G/I_G^2,\ \sigma \mapsto (\sigma - 1) + I_G^2$$

It is a homomorphism since

$$\sigma\tau \mapsto \sigma\tau - 1 = (\sigma - 1) + (\tau - 1) + (\sigma - 1)(\tau - 1) \equiv (\sigma - 1) + (\tau - 1) \mod I_G^2$$

Since I_G/I_G^2 is abelian, the commutator of G is contained in the kernel of this map, so it induces a quotient map

$$\psi :\ G/G' \to I_G/I_G^2$$

In order to show that ψ is bijective, we have another map

$$I_G \to G/G' :\ \sigma - 1 \mapsto \sigma G'$$

This definition extends to all I_G by linearity, since I_G is the free abelian group generated by $\sigma - 1$, where σ varies over all elements of G.

It is easily seen that I_G^2 is contained in the kernel of this map since

$$(\sigma - 1)(\tau - 1) = (\sigma\tau - 1) - (\sigma - 1) - (\tau - 1) \mapsto \sigma\tau\sigma^{-1}\tau^{-1}$$

Hence the induced quotient map is ψ^{-1}, so ψ is an isomorphism. □

6.5 Cohomology of Cyclic Groups

When G is a cyclic group, its cohomology groups are easily computable.

Proposition 6.14. Let G be a cyclic group and let A be a G-module. Then there is an isomorphism

$$\widehat{H}^n(G,A) \cong \widehat{H}^{n+2}(G,A) \ \forall n \in \mathbb{Z}$$

Proof. Let $\sigma \in G$ be a generator and let $N = \#G$. Consider the following exact sequence.

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

where μ is the inclusion, $\sigma - 1$ is the multiplication and ε is the augmentation map given by

$$\sum_{i=0}^{n-1} a_i \sigma^i \mapsto \sum_{i=0}^{n-1} a_i$$

Writing $I = \ker \varepsilon$, we can split the previous sequence in two short exact sequences:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \xrightarrow{\sigma-1} I \longrightarrow 0$$

$$0 \longrightarrow I \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

Since all the previous $\mathbb{Z}$-modules are free, the previous sequences split and they remain exact after tensoring with A.

Since $\mathbb{Z}[G] \otimes A$ is coinduced by lemma 6.7, its cohomology groups are trivial and the long cohomological exact sequence appearing in proposition 6.11 gives the following isomorphisms:

$$\delta : \ \widehat{H}^n(G, I \otimes A) \to \widehat{H}^{n+1}(G,A), \quad \delta : \widehat{H}^n(G,A) \to \widehat{H}^{n+1}(G, I \otimes A)$$

The composite of this isomorphisms gives the desired isomorphisms:

$$\delta^2 : \ \widehat{H}^n(G,A) \to \widehat{H}^{n+2}(G,A)$$

□

Corollary 6.7. Let G be a finite cyclic group and let A be a G-module. Then for every even number n

$$\widehat{H}^n(G,A) \cong \widehat{H}^0(G,A) \cong A^G / N_G(A)$$

Corollary 6.8. Let G be a finite cyclic group generated by some $\sigma \in G$ and let A be a G-module. Then for every odd number n

$$\widehat{H}^n(G,A) \cong \widehat{H}^{-1}(G,A) \cong \ker N_G / (\sigma - 1)A$$

Remark 6.4. For $n = -1$, looking carefully at the isomorphism in proposition 6.14, one can find that every $a \in \ker N_G$ is associated to the coboundary given by

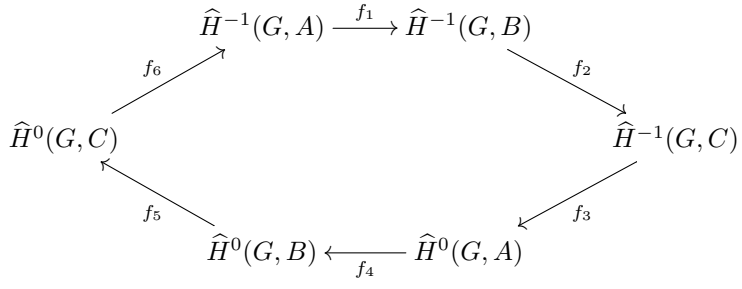
$$\sigma^k \mapsto \sum_{i=0}^{k-1} \sigma^i a$$

where σ is a generator of the group.

Proposition 6.15. Let G be a finite cyclic group and let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of G-modules. Then the long cohomology sequence form the following exact hexagon:



Proof. The only map that deserves a comment is the map $\widehat{H}^0(G,C) \to \widehat{H}^{-1}(G,A)$, which is just the composition of the map given in the long cohomological exact sequence and the isomorphism given in remark 6.4. However, since the following diagram is clearly commutative

$$\begin{array}{ccc} \widehat{H}^{-1}(G,A) & \longrightarrow & \widehat{H}^{-1}(G,B) \\ \downarrow \sim & & \downarrow \sim \\ H^1(G,A) & \longrightarrow & H^1(G,B) \end{array}$$

then the kernel of the map $H^1(G,A) \to H^1(G,B)$ is identified with the kernel of $\widehat{H}^{-1}(G,A) \to \widehat{H}^{-1}(G,B)$, so the hexagon is exact. □

In the study of cohomology of finite cyclic group it is very important the concept of Herbrand quotient. In its most general form, it can be defined as follows,

Definition 6.5. Let A be an abelian group and let $f, g \in \mathrm{End}(A)$ such that $f \circ g = g \circ f = 0$. Then the *Herbrand quotient* is defined as

$$q_{f,g}(A) = \frac{(\ker f : \mathrm{Im}\ g)}{(\ker g : \mathrm{Im}\ f)}$$

provided that both indices are finite.

Proposition 6.16. Let A be a finite abelian group and let $f, g \in \mathrm{End}(A)$ such that $f \circ g = g \circ f = 0$. Then

$$g_{f,g}(A) = 1$$

Proof. It comes from the fact that

$$|\ker(f)| \cdot |\mathrm{Im}(f)| = |A| = |\ker(g)| \cdot |\mathrm{Im}(g)|$$

□

In order to sutdy the cohomology groups of a G-module A, we will consider the endomorphisms

$$D = \sigma - 1, \qquad N = 1 + \sigma + \cdots + \sigma^{n-1}$$

This Herbrand quotient, called *special Herbrand quotient*, can be understood as

$$h(A) = q_{D,N}(A) = \frac{|\widehat{H}^0(G,A)|}{|\widehat{H}^{-1}(G,A)|} = \frac{|H^2(G,A)|}{|H^1(G,A)|}$$

Herbrand quotients have an interesting multiplicative property.

Proposition 6.17. Let G be a cyclic group and let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence. Then

$$h(B) = h(A)h(C)$$

in the sense that if two of these quotients are defined, so is the third and the equality holds.

Proof. It is clear from proposition 6.15 that the third Herbrand quotient is defined provided that the other two are defined too. Moreover, we can deduce from that result that

$$\begin{array}{ll} |\widehat{H}^{-1}(G,A)| = |\ker(f_6)||\ker(f_1)|, & |\widehat{H}^{-1}(G,B)| = |\ker(f_1)||\ker(f_2)|, \\ |\widehat{H}^{-1}(G,C)| = |\ker(f_2)||\ker(f_3)|, & |\widehat{H}^{0}(G,A)| = |\ker(f_3)||\ker(f_4)|, \\ |\widehat{H}^{0}(G,B)| = |\ker(f_4)||\ker(f_5)|, & |\widehat{H}^{0}(G,C)| = |\ker(f_5)||\ker(f_6)| \end{array}$$

Therefore,

$$|\widehat{H}^{-1}(G,A)||\widehat{H}^{-1}(G,C)||\widehat{H}^{0}(G,B)| = |\widehat{H}^{-1}(G,B)||\widehat{H}^{0}(G,A)||\widehat{H}^{0}(G,C)|$$

Hence the identity $h(B) = h(A)h(C)$ is clear. □

Corollary 6.9. Let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of abelian groups. If n denotes the multiplication by n, then

$$q_{0,n}(B) = q_{0,n}(A)q_{0,n}(C)$$

in the sense that if two of them are defined, so is the third one.

Proof. It comes from proposition 6.17 by considering a trivial action of a cyclic group of order n on A, B and C. □

Lemma 6.8. Let A be an abelian group and let $f, g \in \mathrm{End}(A)$ be two endomorphisms such that $f \circ g = g \circ f$. Assume that $q_{0,f}(A)$ and $q_{0,g}(A)$ are defined. Then $q_{0,gf}$ is defined too and

$$q_{0,gf}(A) = q_{0,g}(A) \cdot q_{0,f}(A)$$

Proof. Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & g(A) \cap \ker(f) & \longrightarrow & g(A) & \xrightarrow{f} & fg(A) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker(f) & \longrightarrow & A & \xrightarrow{f} & f(A) & \longrightarrow & 0 \end{array}$$

Snake's lemma gives an exact sequence

$$0 \longrightarrow \frac{\ker(f)}{g(A)\cap\ker(f)} \longrightarrow \frac{A}{g(A)} \longrightarrow \frac{f(A)}{fg(A)} \longrightarrow 0$$

Hence we have the equality

$$\frac{(A : fg(A))}{(A : f(A))} = \frac{(A : g(A)) \cdot |g(A) \cap \ker(f)|}{|\ker(f)|}$$

Since $\ker(fg)/\ker(g) = g^{-1}\left(g(A) \cap \ker(f)\right)/g^{-1}(0) \cong g(A) \cap \ker(f)$, we get that

$$\frac{(A : gf(A))}{|\ker(gf)|} = \frac{(A : g(A))}{|\ker(g)|}\frac{(A : f(A))}{|\ker(f)|}$$

Since $\ker(gf) \subset \ker(f)$, $q_{0,gf}$ is defined provided that $q_{0,f}$ and $q_{0,g}$ are. □

The following theorem is useful to prove the local reciprocity law in chapter 7.

Theorem 6.3. Let G be a cyclic group of prime order p and let A be a G-module. If $g_{0,p}(A)$ is defined, then $q_{0,p}(A^G)$ and $h(A)$ are also defined, and

$$h(A)^{p-1} = \frac{q_{0,p}\left(A^G\right)^p}{q_{0,p}(A)}$$

Proof. Let σ be a generator of G and let $D = \sigma - 1$. Then the following sequence is exact:

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{D} I_G A \longrightarrow 0$$

By lemma 6.3, $(I_G A : pI_G A) \leq (A : pA)$. Since $I_G(A)$ is also a subgroup of A, then $I_G A[p] \subset A[p]$. Hence $q_{0,p}(I_G A)$ is also defined. By corollary 6.9, $q_{0,p}(A^G)$ is also defined and

$$q_{0,p}(A) = q_{0,p}(A^G) \cdot q_{0,p}(I_G A)$$

Notice also that, since G acts trivially on A^G, then $q_{0,p}(A^G) = h(A)$.

Since the ideal $\mathbb{Z} \cdot N_G = \mathbb{Z}\left(\sum_{i=0}^{p-1} \sigma^i\right) \subset \mathbb{Z}[G]$ annihilates $I_G A$, we can consider $I_G A$ as a $\mathbb{Z}[G]/\mathbb{Z}N_G$-module. Moreover, the ring $\mathbb{Z}[G]/\mathbb{Z}N_G$ is isomorphic to $\mathbb{Z}[\zeta]$, where ζ is a p^{th}-primitive root of unity. Since $p = (\zeta - 1)^{p-1}\varepsilon$, where $\varepsilon \in \mathbb{Z}[\zeta]^*$, we have by applying lemma 6.8 repeatedly that

$$q_{0,p}(I_G A) = q_{0,D}(I_G A)^{p-1} q_{0,\varepsilon}(I_G A) = \frac{1}{q_{D,0}(I_G A)^{p-1}}$$

Since N_G is the 0-endomorphism on $I_G A$, we have that

$$q_{0,p}(I_G A) = \frac{1}{q_{D,0}(I_G A)^{p-1}} = \frac{1}{q_{D,N}(I_G A)^{p-1}} = \frac{1}{h(I_G A)^{p-1}}$$

Proposition 6.17 gives the identity $h(A)^{p-1} = h(A^G)^{p-1} h(I_G A)^{p-1}$. Thus the claim

$$h(A)^{p-1} = \frac{q_{0,p}(A^G)^p}{q_{0,p}(A)}$$

follows by substitution. □

6.6 The Cup Product

We can also extend the notion of tensor product to cohomology groups. For that purpose, given two G-modules A and B we can define a canonical action on $A \otimes B$ by the following formula:

$$G \times (A \otimes B) \to A \otimes B : \ (\sigma, a \otimes b) \mapsto \sigma a \otimes \sigma b$$

With there action, there is a canonical mapping

$$A^G \times B^G \mapsto (A \otimes B)^G : \ (a, b) \mapsto a \otimes b$$

It is easily seen that $N_G A \times N_G B$ is mapped to $N_G(A \otimes B)$, since

$$(N_G(a), N_G(b)) \mapsto \left(\sum_{\sigma \in G} \sigma a\right) \otimes \left(\sum_{\tau \in G} \tau b\right) = \sum_{\sigma \in G} \sigma \left(\sum_{\tau \in G} a \otimes \sigma^{-1}\tau b\right)$$

Hence it induces a quotient mapping in the 0^{th}-Tate-cohomology groups, which is called *cup-product*

$$\widehat{H}^0(G, A) \times \widehat{H}^0(G, B) \to \widehat{H}^0(G, A \otimes B) : \ (a + N_G A, b + N_G B) \mapsto (a \otimes b + N_G(A \otimes B))$$

Cup product can be extended to other dimensions by dimension-shifting.

Theorem 6.4. Let G br a finite group and let A and B be two G-modules. Then there is a unique family of bilinear maps, the *cup-product*

$$\cup : \ \widehat{H}^p(G, A) \times \widehat{H}^q(G, B) \to \widehat{H}^{p+q}(G, A \otimes B), \ p, q \in \mathbb{Z}$$

satisfying the following properties:

1. For $p = q = 0$, the cup product is given by

   $$\widehat{H}^0(G, A) \times \widehat{H}^0(G, B) \to \widehat{H}^0(G, A \otimes B) : \ (a + N_G A, b + N_G B) \mapsto (a \otimes b + N_G(A \otimes B))$$

2. If the sequences of G modules

   $$\begin{array}{c} 0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0 \\ 0 \longrightarrow A' \otimes B \longrightarrow A \otimes B \longrightarrow A'' \otimes B \longrightarrow 0 \end{array}$$

   are both exact, then the following diagram commutes

   $$\begin{array}{ccc} \widehat{H}^p(G, A'') \times \widehat{H}^q(G, B) & \xrightarrow{\cup} & \widehat{H}^{p+q}(G, A'' \otimes B) \\ \downarrow{\scriptstyle \delta \times \mathrm{Id}} & & \downarrow{\scriptstyle \delta} \\ \widehat{H}^{p+1}(G, A') \times \widehat{H}^q(G, B) & \xrightarrow{\cup} & \widehat{H}^{p+q+1}(G, A' \otimes B) \end{array}$$

3. If the sequences of G modules

   $$\begin{array}{c} 0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0 \\ 0 \longrightarrow A \otimes B' \longrightarrow A \otimes B \longrightarrow A \otimes B'' \longrightarrow 0 \end{array}$$

   are both exact, then the following diagram commutes

   $$\begin{array}{ccc} \widehat{H}^p(G, A) \times \widehat{H}^q(G, B'') & \xrightarrow{\cup} & \widehat{H}^{p+q}(G, A \otimes B'') \\ \downarrow{\scriptstyle \mathrm{Id} \times \delta} & & \downarrow{\scriptstyle (-1)^p \delta} \\ \widehat{H}^p(G, A) \times \widehat{H}^{q+1}(G, B') & \xrightarrow{\cup} & \widehat{H}^{p+q+1}(G, A \otimes B') \end{array}$$

Proof. By hypothesis 2 and 3, the following diagram is commutative:

$$\begin{array}{ccc}
\widehat{H}^0(G,A^p)\times\widehat{H}^0(G,B^q) & \xrightarrow{\cup} & \widehat{H}^0(G,A^p\otimes B^q) \\
\downarrow{\scriptstyle \delta^p\times 1} & & \downarrow{\scriptstyle \delta^p} \\
\widehat{H}^p(G,A)\times\widehat{H}^0(G,B^q) & \xrightarrow{\cup} & \widehat{H}^p(G,A\otimes B^q) \\
\downarrow{\scriptstyle 1\times\delta^q} & & \downarrow{\scriptstyle (-1)^{pq}\delta^q} \\
\widehat{H}^p(G,A)\times\widehat{H}^q(G,B) & \xrightarrow{\cup} & \widehat{H}^{p+q}(G,A\otimes B)
\end{array}$$

Hence it follows immediatly from condition 1 the uniqueness of the cup-product. The fact that this definition satisfies axioms 2 and 3 is a computation whose details can be checked in [23], proposition 1.4.7. □

Remark 6.5. If $p \geq 0$ and $q \geq 0$, then the cup-product is induced by the following application

$$\begin{aligned}
&\cup : C^p(G,A) \to C^q(G,B) \to C^{p+q}(G,A\otimes B) : \\
&\quad (a\cup b)(\sigma_0,\ldots,\sigma_{p+q}) = a(\sigma_0,\ldots,\sigma_p)\otimes b(\sigma_p,\ldots,\sigma_{p+q})
\end{aligned}$$

This definition also generalizes to the case when G is a profinite group.

Proposition 6.18. Let G be a finite group and let A and B be G-modules. Let also $\overline{a} = a + N_G A \in \widehat{H}^0(G,A)$ and $b \in \widehat{H}^p(G,B)$, where p is an integer. Then

$$\overline{a}\cup b = a\otimes b$$

Proof. For $p = 0$, it is just the definition of cup-product. For other integers p, it follows from dimension-shifting. □

Proposition 6.19. The cup product is anticommutative and associative, i.e., given $a \in \widehat{H}^p(G,A)$, $b \in \widehat{H}^q(G,B)$ and $c \in \widehat{H}^r(G,C)$, we have that

$$a\cup b = (-1)^{pq}(b\cup a), \quad (a\cup b)\cup c = a\cup(b\cup c)$$

Proof. It is trivial for $p = q = 0$. The general case follows from dimension-shifting. □

Again, dimension-shifting also gives the commutativity of the cup-product with the inflation and restriction.

We now show an important result for computing the cup product in a particular case which will be used in next chapter to study the properties of the reciprocity map.

Lemma 6.9. Let G be a finite group and let A and B be G-modules. Let also $a \in \widehat{H}^1(G,A)$ and let $b \in \widehat{H}^{-1}(G,B)$. Then

$$a\cup b = \sum_{\tau\in G} a(\tau)\otimes \tau b$$

Proof. Consider the exact sequences

$$\begin{aligned}
0 \longrightarrow A \longrightarrow A\otimes\mathbb{Z}[G] \longrightarrow A\otimes I_G \longrightarrow 0 \\
0 \longrightarrow A\otimes B \longrightarrow A\otimes\mathbb{Z}[G]\otimes B \longrightarrow A\otimes I_G\otimes B \longrightarrow 0
\end{aligned}$$

Let a' be the image of a in $H^1(G, A \otimes \mathbb{Z}[G])$. Since $A \otimes \mathbb{Z}[G]$ is a coinduced module by lemma 6.7, this cohomology group vanishes, so there is some $a_0 \in \widehat{H}^0(G, A \otimes \mathbb{Z}[G])$ such that $a' = \partial a_0$. This means that

$$a(\tau) = \tau a_0 - a_0 \ \forall \tau \in G^4$$

Moreover, if a_0' is the image of a_0 in the projection to $I_G \otimes A$, then the definition of the connecting homomorphism implies that $a = \delta(a_0')$. Then we obtain

$$a \cup b = \delta(a_0') \cup b = \delta(a_0' \cup b) = \delta(a_0 \otimes b) = N_G(a_0 \otimes b) = \sum_{\tau \in G} \tau a_0 \otimes \tau b = \sum_{\tau \in G} (a_1(\tau) + a_0) \otimes \tau b = \sum_{\tau \in G} a_1(\tau) \otimes \tau b$$

where we have used in the last equality that $N_G b = 0$. □

Lemma 6.10. Let G be a finite group and let A be a G-module. Let $\sigma \in G$ and $a \in H^1(G, A)$. If we denote by $\sigma G'$ the element that σ induces in $\widehat{H}^{-2}(G, \mathbb{Z}) \cong G^{ab}$, we have the following identity:

$$a \cup \sigma G' = a(\sigma) + I_G A \in \widehat{H}^{-1}(G, A)$$

Proof. Consider the exact sequence

$$0 \longrightarrow A \otimes I_G \longrightarrow A \otimes \mathbb{Z}[G] \longrightarrow A \longrightarrow 0$$

Then proposition 6.11 gives an isomorphism $\delta : \widehat{H}^{-1}(G, A) \to \widehat{H}^0(G, A \otimes I_G)$, so it is enough to proof that $\delta\left(a \cup \sigma G'\right) = \delta\left(a(\sigma) + I_G\right)$.

On the one hand, by the definition of δ we have that

$$\delta(a(\sigma)) = \sum_{\tau \in G} \tau a(\sigma) \otimes \tau + N_G(A \otimes I_G)$$

On the other hand, using the computations made in the proof of proposition 6.13, we get that

$$\delta(a \cup \sigma G') = -(a \cup \delta(\sigma G')) = -a \cup (\sigma - 1)$$

By lemma 6.9,

$$\delta(a \cup \sigma G') = -\sum_{\tau \in G} a(\tau) \otimes \tau(\sigma - 1) = \sum_{\tau \in G} a_1(\tau) \otimes \tau - \sum_{\tau \in G} a(\tau) \otimes \tau\sigma$$

Since a is a 1-cocycle, then $a(\tau\sigma) = a(\tau) + \tau a(\sigma)$. Then,

$$\delta(a \cup \sigma G') = \sum_{\tau \in G} (a(\tau\sigma) - a(\tau)) \otimes \tau\sigma = \sum_{\tau \in G} \tau a(\sigma) \otimes \tau\sigma$$

Hence,

$$\delta(a \cup \sigma G') - \delta(a(\sigma)) = \sum_{\tau \in G} \tau a(\sigma) \otimes \tau(\sigma - 1) = N_G\left(a(\sigma) \otimes (\sigma - 1)\right) \in N_G(A \otimes I_G)$$

□

[4] Notice the abuse of notation, since we are considering a_0 as an element of $A \otimes \mathbb{Z}[G]$ and $A \subset A \otimes \mathbb{Z}[G]$

6.7 Tate's Theorem

The goal of this section if proving a theorem about certain map defined as a cup-product map being an isomorphism. This isomorphism in some particular Galois cohomology groups will be understood as the reciprocity map in chapter 7.

We start proving a theorem of cohomological triviality.

Theorem 6.5. Let G be a finite group and let A be a G-module. If there is a dimension q such that

$$\widehat{H}^q(H,A) = \widehat{H}^{q+1}(H,A) = 0$$

for every subgroup $H \subset G$, then A has trivial cohomology.

Proof. It is clear that we just need to prove that $\widehat{H}^{q-1}(H,A) = \widehat{H}^{q+2}(H,A) = 0$. Moreover, we can assume by dimension-shifting that $q = 1$.

We are going to proceed by induction on $n = |G|$, being the case $n = 1$ trivial. Let thus G be a subgroup of order n. By the induction hypothesis, we can assume the statement is true for every proper subgroup of G.

If G is not a p-group, then the induction hypothesis would imply that $\widehat{H}^0(G_p,A) = \widehat{H}^3(G_p,A) = 0$ so, by corollary 6.6 and dimension-shifting, $\widehat{H}^0(G,A) = \widehat{H}^3(G,A) = 0$.

We can thus assume that G is a p-group, so there is a normal subgroup H such that G/H is cyclic of prime order. By induction,

$$\widehat{H}^0(H,A) = H^1(H,A) = H^2(H,A) = H^3(H,A) = 0$$

Hence theorem 6.2 gives isomorphisms

$$\mathrm{Inf}:\ H^q(G/H,A^H) \to H^q(G,A)\ \forall q = 1,2,3$$

The fact that $H^1(G,A) = 0$ implies then that $H^1(G/H,A^H) = 0$, so $H^3(G/H,A^H) = 0$ by proposition 6.14. Hence $H^3(G,A) = 0$.

Again, $H^2(G,A) = 0$ implies that $H^2(G/H,A^H) = \widehat{H}^0(G/H,A^H) = 0$. Taking into account that $\widehat{H}^0(H,A) = 0$, we have that

$$A^G = (A^H)^{G/H} = N_{G/H}(A^H) = N_{G/H}(N_H A) = N_G A \Rightarrow \widehat{H}^0(G,A) = 0$$

□

Theorem 6.6. Let G be a finite group and let A be a G-module satisfying that for each subgroup $H \subset G$ we have that

- $\widehat{H}^{-1}(H,A) = 0$
- $\widehat{H}^0(H,A)$ is cyclic of the same order as H.

If a generates the group $\widehat{H}^0(G,A)$, the cup product map

$$a\cup:\ \widehat{H}^n(G,\mathbb{Z}) \to \widehat{H}^n(G,A)$$

is an isomorphism for every $n \in \mathbb{Z}$.

Proof. Let $B = A \times \mathbb{Z}[G]$. Since the boundary morphisms acts independly on each factor and $\mathbb{Z}[G]$ is an induced module, we have that

$$\widehat{H}^n(H,B) = \widehat{H}^n(H,A) \times \widehat{H}^n(H,\mathbb{Z}[G]) = \widehat{H}^n(H,A)$$

Choose an $a_0 \in A^G$ such that $a_0 + N_G A$ generates $\widehat{H}^0(G, A)$ and consider the map

$$f : \mathbb{Z} \to B : \ n \mapsto n \cdot a_0 + n \cdot N_G$$

By proposition 6.18, it induces an isomorphism in the cohomology groups which fits into the following commutative diagram

$$\begin{array}{ccc} \widehat{H}^n(G,\mathbb{Z}) & \xrightarrow{a\cup} & \widehat{H}^n(G,A) \\ & \searrow^{\overline{f}} & \downarrow \sim \\ & & \widehat{H}^n(G,B) \end{array}$$

We just need to see that $\overline{f}$ is biyective. Since f was injective, the following sequence is exact:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} B \longrightarrow C \longrightarrow 0$$

where $C := \operatorname{coker}(f)$. By hypothesis, $\widehat{H}^{-1}(H, A) = \widehat{H}^{-1}(H, B) = 0$ for every subgroup $H \subset G$. Since G is finite, then $H^1(H, \mathbb{Z}) = \operatorname{Hom}(H, \mathbb{Z}) = 0$ for every subgroup $H \subset G$. By proposition 6.11, there is an exact sequence of the form

$$0 \longrightarrow \widehat{H}^{-1}(H, C) \longrightarrow \widehat{H}^0(H, \mathbb{Z}) \xrightarrow{\overline{f}} \widehat{H}^0(H, B) \longrightarrow \widehat{H}^0(H, C) \longrightarrow 0$$

Since $\overline{f}$ is clearly bijective for 0^{th} dimension, then $\widehat{H}^{-1}(H, C) = \widehat{H}^0(H, C)$ for every subgroup $H \subset G$. By theorem 6.5, $\widehat{H}^n(G, C) = 0 \ \forall n \in \mathbb{Z}$, so $\overline{f}$ is an isomorphism in every dimension. □

Theorem 6.7. Let G be a finite group and let A be a G-module satisfying the following properties

- For each subgroup $H \subset G$, we have $H^1(H, A) = 0$.
- For each subgroup $H \subset G$, $H^2(H, A)$ is cyclic of the same order as H. If a generates $H^2(G, A)$, the map
$$a \cup : \ \widehat{H}^n(G, \mathbb{Z}) \to \widehat{H}^{n+2}(G, A)$$
is an isomorphism.

Proof. The short exact sequences

$$0 \longrightarrow A \longrightarrow \operatorname{Ind}_G(A) \longrightarrow A' \longrightarrow 0$$
$$0 \longrightarrow A' \longrightarrow \operatorname{Ind}_G(A') \longrightarrow A''' \longrightarrow 0$$

induce isomorphisms $\delta^2 : \widehat{H}^n(H, A'') \to \widehat{H}^{n+2}(H, A)$, because of proposition 6.2. If $a \in H^2(G, A)$ is a generator of the group, then $\delta^{-2}a$ is a generator of $\widehat{H}^0(G, A)$. By the definition of cup-product, the following diagram is commutative:

$$\begin{array}{ccc} \widehat{H}^n(G,\mathbb{Z}) & \xrightarrow{\delta^{-2}a\cup} & \widehat{H}^n(G,A'') \\ \downarrow \mathrm{Id} & & \downarrow \delta^2 \\ \widehat{H}^n(G,\mathbb{Z}) & \xrightarrow{a\cup} & \widehat{H}^{n+2}(G,A) \end{array}$$

Since the map $\delta^{-2}\cup$ is bijective, then $a\cup$ is also bijective. □

6.8 Cohomology of the p-adic Integers

We end this chapter by describing some cohomology groups when G is isomorphic to the p-adic integers $\mathbb{Z}_p$. These results will be needed later in the study of the arithmetic of elliptic curves.

Proposition 6.20. Let p be a prime, let $G \cong \mathbb{Z}_p$ be generated by some $\gamma \in G$ and let A be a discrete, p-primary abelian group on which G acts continuously. Then

$$H^1(G, A) \cong A/(\gamma - 1)A$$

Proof. Defining $G_n := G^{p^n}$, proposition 6.4 and corollary 6.8 imply that

$$H^1(G, A) = \varinjlim_n H^1(G/G_n, A^{G^n}) = \varinjlim_n \ker N_n/(\gamma - 1)A^{G_n}$$

where $N_n : A^{G_n} \to A^{G_n}$ denotes the norm map associated to G/G_n. By remark 6.4, it is clear that direct limit homomorphisms are the maps induced by inclusions. Since direct limit is an exact functor by proposition 4.3,

$$H^1(G, A) = \frac{\varinjlim_n \ker N_n}{(\gamma - 1)\varinjlim_n A^{\Gamma_n}} = A'/(\gamma - 1)A$$

where $A' = \{a \in A : N_n(a) = 0 \text{ for some } n \in \mathbb{N}\}$. Just notice that δ-homomorphisms commute with the change of groups, so the transition maps in the direct product are the inclusions.

Fix some $a \in A$. Since A is p-primary, there is some $m \in \mathbb{N}$ such that $p^m a = 0$. Moreover, there is another $n \in \mathbb{N}$ such that $\gamma^{p^n} a = a$ because the action of Γ is continuous and proposition 4.7 is applied. Then

$$N_{n+m}(a) = \sum_{k=0}^{p^{n+m}-1} \gamma^k(a) = p^m \sum_{k=0}^{p^n-1} \gamma^k(a) = \sum_{k=0}^{p^n-1} \gamma^k(p^m a) = 0$$

Hence $a \in A'$ and

$$H^1(G, A) = A/(\gamma - 1)A$$

□

Proposition 6.21. Let p be a prime, let $G \cong \mathbb{Z}_p$ and let A be a discrete, p-primary G module. Then

$$H^2(G, A) = 0$$

Proof. Since inflation commutes with ∂ then the inflation maps

$$H^2\left(G/G^{p^n}, A^{G^{p^n}}\right) \to H^2\left(G/G^{p^m}, A^{G^{p^m}}\right)$$

where $m \geq n$, corresponds to the homormorphism

$$A^{G^{p^n}} / \left(N_{G/G^{p^n}} A\right) \to A^{G^{p^m}} / \left(N_{G/G^{p^m}} A\right)$$

induced by the norm map $N_{G^{p^n}/G^{p^m}}$. However, this is just the multiplication by p^{m-n}. Since A is p-primary then

$$H^2(G, A) = \varinjlim_{n \in \mathbb{N}} H^2\left(G/G^{p^n}, A^{G^{p^n}}\right) = 0$$

□

Proposition 6.22. Let G be a group and let A be a G-module such that $G \cong \mathbb{Z}_p$ and $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ as groups. Then $H^0(G, A)$ and $H^1(G, A)$ have the same $\mathbb{Z}_p$-corank. Furthermore, if $H^0(G, A)$ is finite, then $H^1(G, A) = 0$.

Proof. Let γ be a topological generator of G. By proposition 6.20, $H^1(G, A) \cong A/(\gamma - 1)A$. Then consider the exact sequence:

$$0 \longrightarrow H^0(G, A) \longrightarrow A \xrightarrow{\gamma-1} A \longrightarrow H^1(G, A) \longrightarrow 0$$

It can be split in two short exact sequences

$$0 \longrightarrow H^0(G, A) \longrightarrow A \longrightarrow (\gamma - 1)A \longrightarrow 0$$

$$0 \longrightarrow (\gamma - 1)A \longrightarrow A \longrightarrow H^1(G, A) \longrightarrow 0$$

Since A is cofinitely generated, corollary 4.4 thus implies that

$$\operatorname{corank}_{\mathbb{Z}_p} H^0(G, A) = \operatorname{corank}_{\mathbb{Z}_p} A - \operatorname{corank}_{\mathbb{Z}_p} (\gamma - 1)A = \operatorname{corank}_{\mathbb{Z}_p} H^1(G, A)$$

If $H^0(G, A)$ is finite, then $H^1(G, A) \cong A/(\gamma - 1)A$ is a divisible group of corank 0, so $H^1(G, A) = 0$. □

Part II

Local Class Field Theory

Chapter 7

The Local Reciprocity Law

In this chapter, we apply the cohomological theory of profinite groups to the case when G is a Galois group, which is the case we are going to be interested in while studying the arithmetic of elliptic curves. Then section 7.1 is dedicated to the main results about the cohomology of Galois groups.

After that, we particularise to the case when the base field is p-adic. In section 7.2 we study the cohomology of the unramified extensions while in section 7.3 we consider the ramified ones.

Finally, sections 7.4 and 7.5 expose a deep result, the local reciprocity law, which gives an isomorphism of the Galois group of the maximal abelian extension of a p-adic field and the profinite completion of the multiplicative group of that field. This isomorphism enable us to study the cohomology of the absolute Galois group and will play a central role in the proof of the corank lemma in chapter 8.

7.1 Galois Cohomology

Let $L|K$ be a Galois extension. Since we have already seen in corollary 5.2 that $G_{L|K}$ is a profinite group, we can apply the cohomological theory developed in chapter 6. From now on, given a $G_{L|K}$-module A, we will denote

$$H^n(L|K, A) := H^n(G_{L|K}, A), \quad H^n(K, A) := H^n(G_K, A) = H^n(G_{\overline{K}|K}, A)$$

The most natural modules in which the Galois group acts are the additive group L and the multiplicative group L^*. Notice that both actions are continuous since given $x \in L$, $G_{L|K(x)}$ is an open subgroup by theorem 5.2. The additive group is cohomologically trivial because of the existence of a normal basis.

Theorem 7.1. Let $L|K$ be a Galois extension. Then

$$\widehat{H}^n(L|K, L) = 0 \ \forall n \in \mathbb{Z}$$

Proof. By corollary 6.2 and remark 5.2, we can assume that $L|K$ is finite.

By the normal basis theorem, there exists some $a \in L$ such that $\{\sigma(a) : \sigma \in G_{L|K}\}$. Hence

$$L \cong \mathbb{Z}[G] \otimes K$$

is a coinduced module, so it is cohomologically trivial by proposition 6.12. □

The cohomology of the multiplicative group is slightly more interesting. However, the first cohomology group also vanishes. This result is usually known as Hilbert Theorem 90.

Theorem 7.2. Let $L|K$ be a Galois extension. Then

$$H^1(L|K, L^*) = 0$$

Proof. Again using corollary 6.2 and remark 5.2 we can assume that $L|K$ is finite.

Let $\varphi:\ G_{L|K} \to L^*$ be a 1-cocycle. Since the Galois automorphisms are linearly independent, we can find some $c \in L^*$ such that

$$b := \sum_{\sigma \in G_{L|K}} \varphi(\sigma)\sigma(c) \neq 0$$

Given some $\tau \in G_{L|K}$, using the characterisation of cocycles

$$\tau(b) = \sum_{\sigma \in G_{L|K}} \tau\left(\varphi(\sigma)\right)\tau(\sigma(c)) = \sum_{\sigma \in G_{L|K}} \varphi(\tau^{-1})\varphi(\tau\sigma)(\tau\sigma)(c) = \varphi(\tau)^{-1}b \Rightarrow \varphi(\tau) = \frac{\tau(b^{-1})}{b^{-1}}$$

Hence φ is a coboundary and, therefore, $H^1(L|K, L^*) = 0$. □

Hilbert Theorem 90 has an interesting consequence using the long cohomological sequence

Corollary 7.1. Let $L|K$ be a Galois extension and let $\mu_n \subset \overline{K}$ be the multiplicative subgroup of n^{th} roots of unity. Then there is a canonical isomorphism

$$\delta:\ K^*/(K^*)^n \to H^1(K, \mu_n)$$

where $(K^*)^n = \{x^n :\ x \in K\}$.

Proof. Consider the short exact sequence written in multiplicative notation

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^* \xrightarrow{\ n\ } \overline{K}^* \longrightarrow 1$$

where the last arrow is given by the exponentiation up to the n^{th} power. The long cohomological exact sequence given in lemma 6.4 says that the following sequence is exact:

$$K^* \xrightarrow{\ n\ } K^* \xrightarrow{\ \delta\ } H^1(K, \mu_n) \longrightarrow H^1\left(K, \overline{K}^*\right)$$

By theorem 7.2, $H^1(K, K^*) = 1$, so δ is surjective. Moreover, $\ker(\delta) = (K^*)^n$, so the quotient map is the desired isomorphism. □

Remark 7.1. The map δ can be computed as follows: given some $b \in K$, choose some $\beta \in \overline{K}$ such that $\beta^n = b$. Then the cocycle associated to b is

$$\sigma \mapsto \frac{\beta^\sigma}{\beta}$$

Corollary 7.2. If K is a finite field and $L|K$ is a finite Galois extension, then

$$\widehat{H}^n(L|K, L^*) = 0\ \forall n \in \mathbb{Z}$$

Proof. It comes form theorem 7.2 and proposition 6.16. □

7.2 Cohomology of Unramified Extensions

Let K be a local field and let $L|K$ be a finite unramified extension whose residue field extension is $l|k$. The main goal of this section is to show the existence of a canonical isomorphism

$$H^2(L|K, L^*) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

From now on, we will denote by $\varphi_{L|K}$ the element of $G_{L|K}$ which induces the Frobenius automorphism in $G_{l|k}$. We want to study the cohomology groups $H^2(L|K, L^*)$. For that purpose, the following theorem is important.

Theorem 7.3. Let $L|K$ be a finite unramified extension of p-adic fields and let U_L be the ring of integers of L. Then

$$\widehat{H}^n(L|K, U_L) = 0 \ \forall n \in \mathbb{Z}$$

Proof. Considering the exact sequence

$$1 \longrightarrow U_L^1 \longrightarrow U_L \longrightarrow l^* \longrightarrow 1$$

Where $U_L^k := 1 + \pi_L^k U_L$ and π_L is a uniformiser of L. Since $G_{L|K} = G_{l|k}$ and $\widehat{H}^n(l|k, l^*) = 0$ by corollary 7.2, then $\widehat{H}^n(L|K, U_L) \cong \widehat{H}^n(L|K, U_L^1)\ \forall n \in \mathbb{Z}$.

Moreover, the map

$$U_L^{k-1} \to l^+ :\ 1 + a\pi_L^{k-1} \mapsto a \mod (\pi_L)$$

induces an exact sequence

$$1 \longrightarrow U_L^k \longrightarrow U_L^{k-1} \longrightarrow l^+ \longrightarrow 0$$

By theorem 7.1, $\widehat{H}^n(L|K, l^+) = 0\ \forall n \in \mathbb{N}$, so lemma 6.4 gives isomorphisms $\widehat{H}^n(L|K, U_L^k) \cong \widehat{H}^n(L|K, U_L^{k-1})$. For large enough n, the p-adic logarithm implies that $U_L^n \cong R_L$ as $G_{L|K}$ modules, where R_L is the ring of integers of L. However, $R_L \cong R_K \otimes \mathbb{Z}[G_{L|K}]$ because $L|K$ is unramified. In fact, any lifting to U_L of some $a \in l$ that generates a normal basis of $l|k$ would generate R_L as a R_K module. Hence R_L is an induced module and, therefore, cohomologically trivial. □

Consider now the following short exact sequence

$$0 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v} \mathbb{Z} \longrightarrow 0$$

By theorem 7.3 and lemma 6.4, it induces an isomorphisms

$$v :\ H^2(L|K, L^*) \to H^2(L|K, \mathbb{Z})$$

Taking into account that $\mathbb{Q}$ is cohomologically trivial because of corollary 6.4, the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

induces an isomorphism

$$\delta :\ H^1(L|K, \mathbb{Q}/\mathbb{Z}) \to H^2(L|K, \mathbb{Z})$$

Taking it into account and the fact that the Galois group acts trivially on $\mathbb{Q}/\mathbb{Z}$, we have an isomorphism

$$\mathrm{inv}_{L|K} :\ H^2(L|K, L^*) \to \mathrm{Hom}(G_{L|K}, \mathbb{Q}/\mathbb{Z})$$

Since $G_{L|K}$ is cyclic of order $[L:K]$ and generated by $\varphi_{L|K}$, every homomorphism is determined by the image of this generator, which has to be an element whose order divides $[L:K]$. Hence we can consider the following isomorphism, which is called *invariant map*.

$$\mathrm{inv}_{L|K}: \ H^2(L|K, L^*) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \tag{7.1}$$

Taking that background into account, it is easy to compute the cohomology group of the maximal unramified extension by using corollary 6.2.

Corollary 7.3. Let K be a p-adic field and let K^{unr} be its maximal unramified extension. Then

$$H^2\left(K^{\mathrm{unr}}|K, (K^{\mathrm{unr}})^*\right) = \varinjlim_n \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}$$

7.3 Cohomology of Ramified Extensions

The goal of this section is to extend the previous one to ramified extensions. We are going to see that the image of the inflation of $H^2(L|K, L^*)$ to $H^2\left(K, \overline{K}^*\right)$ is the same for every Galois extension of the same degree. Hence we can use the unramified extension of the same degree to extend the invariant map to every finite Galois extension.

Lemma 7.1. Let K be a p-adic field and let $L|K$ be a finite Galois extension. Then the order of $H^2(L|K)$ divides $[L:K]$.

Proof. Assume first that $G_{L|K}$ is cyclic of prime degree $l = [L:K]$. By theorem 6.3, we have that

$$h(L^*)^{l-1} = \frac{q_{0,l}(K^*)^l}{q_{0,l}(L^*)}$$

Since we know the structure of p-adic fields, then

$$q_{0,l}(K^*) = \frac{(K^* : (K^*)^l)}{K^*[l]} = l \cdot q_K^{v_K(l)}$$

where q_K is the number of elements in the residue field of K. Hence

$$h(L^*)^{l-1} = \frac{l^l q_K^{lv_K(l)}}{l q_L^{v_L(l)}} = \frac{l^l q_K^{lv_K(l)}}{l q_K^{f\cdot e\cdot v_K(l)}} = l^{l-1} \Rightarrow h(L^*) = l$$

By theorem 7.2, $H^1(L|K, L^*) = 0$, so

$$|H^2(L|K, L^*)| = h(L^*) = l = [L:K]$$

For the general case, notice that the Galois group $G_{L|K}$ is solvable, so there is a subextension $M|K$ of prime degree. Since theorem 7.2 says that $H^1(L|M, L^*) = 0$, theorem 6.2 gives the following exact sequence:

$$0 \longrightarrow H^2(M|K, M^*) \xrightarrow{\mathrm{Inf}} H^2(L|K, L^*) \xrightarrow{\mathrm{Res}} H^2(L|M, L^*)$$

Hence $|H^2(L|K, L^*)|$ divides $|H^2(M|K, M^*)||H^2(L|M, L^*)| = [M:K] \cdot |H^2(L|M, L^*)|$. We can also assume by an inductive argument on the degree of the extension that $|H^2(L|M, L^*)|$ divides $[L:M]$. Hence the claim follows by the degree transitivity. □

Lemma 7.2. Let $L|K$ and $L'|K$ be finite Galois extensions such that $L'|K$ is unramified and let $N = L \cdot L'$. If $c \in H^2(L'|K)$, then

$$\mathrm{inv}_{N|L}(\mathrm{Res}^{N|K}_{N|L} \circ \mathrm{Inf}^{L'|K}_{N|K} c) = [L : K]\mathrm{inv}_{L'|K} c$$

Proof. Let f and e be the inertia and ramification degrees of $L|K$ and, since $N|L$ is unramified, consider the following diagram:

$$\begin{array}{ccccccc}
H^2(L'|K, L'^*) & \xrightarrow{v_{L*}} & H^2(L'|K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(L'|K, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle i} \\
H^2(N|K, N^*) & & H^2(N|K, \mathbb{Z}) & & H^1(N|K, \mathbb{Q}/\mathbb{Z}) & & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} & & \downarrow{\scriptstyle \cdot[L:K]} \\
H^2(N|L, N^*) & \xrightarrow{v_N} & H^2(N|L, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(N|L, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z}
\end{array}$$

To complete the proof we just need to show that this diagram is commutative. Commutativity of the left square is clear from the definitions, just taking into account that the inertia degrees of $N|L'$ and $L'|K$ are the same. Commutativity of the middle one is just the commutativity of the connecting homomorphism δ with restrictions and inflations. To see that the right square commutes, we have to take into account again that $N|L$ is unramified and that $\varphi_{N|L}|_{L'} = \varphi^f_{L'|K}$, fact that is true because this identity also happens with the Frobenius automorphisms of the residue fields. Then given $\chi \in H^1(L'|K, \mathbb{Q}/\mathbb{Z})$, we have that

$$[L : K]\chi(\varphi_{L'|K}) = ef\chi(\varphi_{L'|K}) = e\chi(\varphi_{N|L}|_{L'}) = e(\mathrm{Res}^{N|K}_{N|L} \circ \mathrm{Inf}^{L'|K}_{N|K})\chi(\varphi_{L'|K})$$

□

Theorem 7.4. Let K be a p-adic field and let $L|K$ be a finite Galois extension. Consider then the unramified extension $L'|K$ of the same degree. Then

$$\mathrm{Inf}_{L|K} H^2(L|K, L^*) = \mathrm{Inf}_{L'|K} H^2(L'|K, L'^*) \subset H^2\left(K, \overline{K}^*\right)$$

Proof. Since the inflation maps are injective by theorems 6.2 and 7.2, using the isomorphism $\mathrm{inv}_{L|K}$ appearing in equation 7.1 and lemma 7.1, we just need to prove that

$$\mathrm{Inf}^{L'|K}_K H^2(L'|K, L'^*) \subset \mathrm{Inf}^{L|K}_K H^2(L|K, L^*)$$

Since inflation is transitive, we can just prove it for inflations to the field extension $N|K$, where $N = LL'$. Consider then the following short exact sequence given by theorem 6.1:

$$1 \longrightarrow H^2(L|K, L^*) \xrightarrow{\mathrm{Inf}} H^2\left(N|K, N^*\right) \xrightarrow{\mathrm{Res}} H^2\left(N|L, N^*\right)$$

Hence the result is equivalent to

$$\mathrm{Res}^{N|K}_{N|L} \circ \mathrm{Inf}^{L'|K}_{N|K} = 0$$

However, by lemma 7.2, that is

$$\mathrm{inv}^{-1}_{N|L}([L : K] \cdot x) = 0 \ \forall x \in \frac{1}{[L' : K]}\mathbb{Z}/\mathbb{Z}$$

which is clearly true since both $L|K$ and $L'|K$ have the same degree. □

Last theorem and corollary 7.3 compute the Brauer group.

Corollary 7.4. Let K be a p-adic field and let K^{unr} be its maximal unramified extension. Then

$$H^2\left(K, \overline{K}^*\right) = H^2\left(K^{unr}|\,(K^{unr})^*\right) \cong \mathbb{Q}/\mathbb{Z}$$

We can also extend the invariant maps to ramified extensions using theorem 7.4

Corollary 7.5. Let K be a p-adic field and let $L|K$ and $L'|K$ be two finite Galois extensions of the same degree such that $L'|K$ is unramified. Then there is a canonical isomorphism

$$\psi_{L,L'}:\ H^2(L|K, L^*) \to H^2(L'|K, L'^*)$$

given by the condition $\mathrm{Inf}_K^{L'|K} \circ \psi_{L,L'} = \mathrm{Inf}_K^{L|K}$.

Definition 7.1. Let K be a p-adic field and let $L|K$ be a finite Galois extension. Then we define the invariant map of $L|K$ as the canonical homomorphism

$$\mathrm{inv}_{L|K} = \mathrm{inv}_{L'|K} \circ \psi_{L,L'}:\ H^2(L|K, L^*) \mapsto \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

where $L'|K$ is the unramified extension of degree $[L:K]$.

Proposition 7.1. Let K be a p-adic field and let $N \supset L \supset K$ be a tower of finite Galois extensions. Then

$$\mathrm{inv}_{L|K} = \mathrm{inv}_{N|K} \circ \mathrm{Inf}_{N|K}^{L|K}$$

Proof. By the definition of the invariant map for ramified extensions, we just need to prove it for unramified extensions. Then the statement is clear tracing through the definitions by taking into account the fact that $\varphi_{N|K}|_L = \varphi_{L|K}$. □

7.4 The Local Reciprocity Law

The local reciprocity law, which is an isomorphism between the abelianised group $G_{L|K}^{\mathrm{ab}}$ and certain quotient of K^*, now follows as a direct consequence of Tate's theorem.

Theorem 7.5. Let K be a p-adic field and let $L|K$ be a finite Galois extension. Then there is a canonical isomorphism

$$G_{L|K}^{\mathrm{ab}} \xrightarrow{u_{L|K}\cup} K^*/N_{L|K}L^*$$

Proof. By proposition 6.13, $G_{L|K}^{ab} \cong \widehat{H}^{-2}(L|K, \mathbb{Z})$ canonically. By definition, $K^*/N_{L|K}L^* = \widehat{H}^0(L|K, L^*)$, the canonical isomorphism is given by theorem 6.7 using the generator

$$u_{L|K} := (\mathrm{inv}_{L|K})^{-1}\left(\frac{1}{[L:K]} + \mathbb{Z}\right) \in H^2(L|K, L^*)$$

□

The inverse of these isomorphism is called *norm residue symbol* $(\ , L|K)$ and induces the exact sequence

$$0 \longrightarrow N_{L|K}L^* \longrightarrow K^* \xrightarrow{(\ ,L|K)} G_{L|K}^{\mathrm{ab}} \longrightarrow 1$$

The next step is showing that the norm residue symbol satisfy certain commutative property when considering towers of fields. It will be useful to generalise the reciprocity map to infinite extensions by taking the inverse limit. The following lemma establishes a relation between the norm residue symbol and the invariant map.

Lemma 7.3. Let K be a p-adic field, let $L|K$ be a Galois extension, let $a \in K^*$ and $\overline{a} := a \cdot N_{L|K}L^* \in \widehat{H}^0(L|K, L^*)$. Given a character $\chi \in H^1(L|K, \mathbb{Q}/\mathbb{Z})$, then

$$\chi\left((a, L|K)\right) = \mathrm{inv}_{L|K}\left(\overline{a} \cup \delta(\chi)\right) \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

where δ is the following isomorphism induced by the long cohomological exact sequence:

$$\delta: \ H^1(L|K, \mathbb{Q}/\mathbb{Z}) \to H^2(L|K, \mathbb{Z})$$

Proof. To simplify notation, we set $\sigma_a := (a, L|K)$. By proposition 6.19,

$$\overline{a} \cup \delta\chi = u_{L|K} \cup \sigma_a \cup \delta\chi = u_{L|K} \cup \delta(\sigma_a \cup \chi)$$

By lemma 6.10, we have that

$$\sigma_a \cup \chi = \chi(\sigma_a) = \frac{r}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \widehat{H}^{-1}(L|K, \mathbb{Q}/\mathbb{Z}) \Rightarrow \delta(\chi(\sigma_a)) = r + n\mathbb{Z} \in \widehat{H}^0(L|K, \mathbb{Z})$$

where $n := [L:K]$. Therefore

$$\overline{a} \cup \delta\chi = u_{L|K} \cup (r + n\mathbb{Z}) = u_{L|K}^r$$

Hence,

$$\mathrm{inv}_{L|K}(\overline{a} \cup \delta\chi) = r \cdot \mathrm{inv}_{L|K}(u_{L|K}) = \frac{r}{n} + \mathbb{Z} = \chi(\sigma_a)$$

□

Theorem 7.6. Let K be a p-adic field and let $N \supset L \supset K$ be a tower of finite Galois extensions. Then the following diagram is commutative

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,N|K)} & G_{N|K}^{\mathrm{ab}} \\ \Big\downarrow{\scriptstyle \mathrm{Id}} & & \Big\downarrow{\scriptstyle \pi} \\ K^* & \xrightarrow{(\ ,L|K)} & G_{L|K}^{\mathrm{ab}} \end{array}$$

where $\pi : G_{N|K} \to G_{L|K}$ is the canonical projection.

Proof. Let $\chi \in H^1(L|K, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L|K}, \mathbb{Q}/\mathbb{Z})$. By lemma 7.3 and proposition 7.1:

$$\chi(\pi(a, N|K)) = \mathrm{Inf}_{L|K}^{N|K}\chi(a, N|K) = \mathrm{inv}_{N|K}\left(\overline{a} \cup \delta\left(\mathrm{Inf}_{L|K}^{N|K}\chi\right)\right)$$
$$\mathrm{inv}_{N|K}\left(\mathrm{Inf}_{L|K}^{N|K}\left(\overline{a} \cup \delta\chi\right)\right) = \mathrm{inv}_{L|K}\left(\overline{a} \cup \delta\chi\right) = \chi(a, L|K)$$

That is true for every character $\chi \in \mathrm{Hom}(G_{L|K}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L|K}^{ab}, \mathbb{Q}/\mathbb{Z})$. Since the profinite group $G_{L|K}^{ab}$ is Hausdorff and the identity has a basis of neighbourhood formed by open normal subgroups by proposition 4.5, for every element $g \in G_{L|K}^{ab}$, there is a character $\chi \in \mathrm{Hom}(G_{L|K}^{ab}, \mathbb{Q}/\mathbb{Z})$ such that $\chi(g) \neq 0$. Hence we necessarily have that $\pi(a, N|K) = (a, L|K)$. □

Now we can identify the Galois group of the maximal abelian extension of a p-adic field with certain inverse limit. For that, we need to define the norm subgroups in K^*.

Definition 7.2. Let K be a p-adic field. A subgroup $H \subset K^*$ is said to be a *norm group* if there is an finite Galois extension $L|K$ such that

$$H = N_{L|K}(L^*)$$

Corollary 7.6. Let K be a p-adic field and let K^{ab} be its maximal abelian extension. Then there is an isomorphism

$$G_K^{\mathrm{ab}} = G_{K^{\mathrm{ab}}|K} = \varprojlim_H K^*/H$$

where H runs through the norm groups of K.

7.5 The Existence Theorem

Since the Galois group of the maximal abelian extension of a p-adic field is the inverse limit of all its finite abelian extensions, we want to know which subgroups of K are norm groups. We will see that they are those being open and having finite index. Hence we will have that G_K^{ab} is the profinite completion.

Theorem 7.7. Let K be a p-adic field, and let K^{ab} be its maximal abelian extension. Then there is a canonical isomorphism

$$G_{K^{\mathrm{ab}}|K} \cong \overleftarrow{K^*}$$

where $\overleftarrow{K^*}$ denotes the profinite completion of the multiplicative group K^*. This map is commonly known as *reciprocity map*.

For proving theorem 7.7, we need to consider some lemmas as a preparation for a result that states that the norm groups are exactly those being open and having finite index in K^*. However, the open condition is suporfluous. In fact, a group of finite index contains $(K^*)^m$, which is open. Hence our group is a union of cosets of $(K^*)^m$, so it is open.

Lemma 7.4. Let K be a p-adic field, let $L|K$ be a Galois extension and let $L^{\mathrm{ab}}|K$ be its maximal subextension. Then

$$N_{L|K}L^* = N_{L^{\mathrm{ab}}|K}\left(L^{\mathrm{ab}}\right)^*$$

Proof. By theorem 7.5,

$$K^*/N_{L|K}L^* \cong G_{L|K}^{\mathrm{ab}} = G_{L^{\mathrm{ab}}|K} = K^*/N_{L^{\mathrm{ab}}|K}\left(L^{\mathrm{ab}}\right)^*$$

Since these groups are finite and the inclusion $N_{L|K}L^* = N_{L|L^{\mathrm{ab}}}N_{L^{\mathrm{ab}}K}L^* \subset N_{L^{\mathrm{ab}}|K}\left(L^{\mathrm{ab}}\right)^*$ is clear, we have that $N_{L|K}L^* = N_{L^{\mathrm{ab}}|K}\left(L^{\mathrm{ab}}\right)^*$. □

Last lemma, together with theorem 7.5, implies the following corollary.

Corollary 7.7. Let K be a p-adic field and let $L|K$ be a finite Galois extension. Then $(K^* : N_{L|K}L^*)$ divides $[L : K]$ and the equality happens if and only if $L|K$ is abelian.

Lemma 7.5. Let K be a p-adic field, let $\{L_i|K : \ i \in I\}$ be abelian extensions and let N be the composition of all L_i. Then

$$N_{N|K}N^* = \bigcap_{i\in I} N_{L_i|K}L_i^*$$

Proof. The inclusion $N_{N|K}N^* \subset \bigcap_{i\in I} N_{L_i|K}L_i^*$ is clear since for every $i \in I$ we have that

$$N_{N|K}N^* = N_{L_i|K}\left(N_{N|L_i}N^*\right) \subset N_{L_i|K}L_i^*$$

Conversely, let $a \in \bigcap_{i\in I} N_{L_i|K}L_i^*$. Then $(a, L_i|K) = 1\ \forall i \in I$. Hence theorem 7.6 implies that $(a, N|K) = 1$, so $a \in N_{N|K}N^*$. □

Lemma 7.6. Let K be a p-adic field and let $L|K$ and $M|K$ be two abelian extensions. Then

$$L \subset M \Leftrightarrow N_{M|K}M^* \subset N_{L|K}L^*$$

Proof. The implication $\Rightarrow$ is clear since

$$N_{M|K}M^* = N_{L|K}\left(N_{M|L}M^*\right) \subset N_{L|K}L^*$$

Conversely, denote $N := LM$. Then we have by lemma 7.5 and corollary 7.7 that

$$N_{M|K}M^* \subset N_{L|K}L^* \Rightarrow N_{N|K}N^* = N_{M|K}M^* \Rightarrow [N : K] = [M : K] \Rightarrow N = M \Rightarrow L \subset M$$

□

Lemma 7.7. Let K be a p-adic field and let $H \subset K^*$ be a subgroup that contains a norm group. Then H is itself a norm group.

Proof. By hypothesis, there is a Galois extension $L|K$ such that $N_{L|K}L^* \subset H \subset K^*$. Moreover, we can assume without loss of generality, because of lemma 7.4, that $L|K$ is abelian.

By the isomorphism given in theorem 7.5, the finite set of subgroups of $K^*/N_{L|K}L^*$ is in bijection with the subextensions of $L|K$, so both finite sets have the same cardinality. Moreover, lemma 7.6 gives an injection $M \mapsto N_{M|K}M^*$ from the subextensions of $L|K$ to the subgroups of $K^*/N_{L|K}L^*$ and it will be a bijection by the cardinality argument. Hence there has to be an extension $M|K$ such that

$$H = N_{M|K}M^*$$

□

Theorem 7.8. Let K be a p-adic field. Then the norm groups of K^* are precisely the open subgroups of finite index in K^*.

Proof. By corollary 7.7, every norm group $N_{L|K}L^*$ has finite index, so there is some $m \in \mathbb{N}$ such that $(K^*)^m \subset N_{L|K}L^*$. Hence $N_{L|K}L^*$ is a union of open cosets of $(K^*)^m$, so it has to be itself open.

Conversely, let $H \subset K^*$ be an open subgroup of finite index m. Then $(K^*)^m \subset H$ and, by lemma 7.7, we just need to show that $(K^*)^m$ is a norm group.

We will assume first that K contains the m^{th} roots of unity. Then consider the composition L of every extension $K(\sqrt[m]{a})$, where a runs through the elements of K^*. Since $(K^* : (K^*)^m)$ is finite, then $L|K$ is also finite and, by lemma 7.5, we have that

$$N_{L|K}L^* = \bigcap_{a\in K^*} N_{K(\sqrt[m]{a})|K}K(\sqrt[m]{a})^*$$

Since $d = [K(\sqrt[m]{a}) : K]$ divides m, we have that

$$(K^*)^m \subset (K^*)^d \subset N_{K(\sqrt[m]{a})|K}K(\sqrt[m]{a})^* \Rightarrow (K^*)^m \subset N_{L|K}L^*$$

On the other hand, theorem 7.2 gives an isomorphism

$$K^*/(K^*)^m \cong \mathrm{Hom}(G_{L|K}, \mu_m)$$

Since $L|K$ is an abelian extension of exponent dividing m by theorem 5.1, then the structure theorem of finite abelian groups implies that $|G_{L|K}| = |\mathrm{Hom}(G_{L|K}, \mu_m)|$. Hence by theorem 7.5,

$$(K^* : (K^*)^m) = |G_{L|K}| = (K^* : N_{L|K}L^*) < \infty \Rightarrow (K^*)^m = N_{L|K}L^*$$

Assume now that K does not contain the m^{th} roots of unity. Let then K_1 be the extension obtained by adjoining the m^{th} roots of unity to K. By what we have just proven, we know that there is some extension $L|K_1$ such that

$$N_{L|K_1}L^* = (K_1^*)^m$$

Let L_1 be the Galois closure of $L|K$. Then we have that

$$N_{L_1|K}L_1^* = N_{K_1|K}\left(N_{L_1|K_1}L_1^*\right) \subset N_{K_1|K}\left(N_{L|K_1}L^*\right) = N_{K_1|K}((K_1^*)^m) = \left(N_{K_1|K}K_1^*\right)^m \subset (K^*)^m$$

By lemma 7.7, $(K^*)^m$ is itself a norm group. □

Remark 7.2. We have mentioned above that every subgroup of finite index is open, so every subgroup of finite index is a norm subgroup.

Now the proof of theorem 7.7 is complete. Moreover, we can see that the reciprocity map is an isomorphism of Galois modules.

Proposition 7.2. Let K be a p-adic field and let $L|K$ be a finite Galois extension. The reciprocity map

$$G_L^{\mathrm{ab}} \to \overleftarrow{L^*}$$

is an isomorphism of $G_{L|K}$-modules, where $G_{L|K}$ acts on G_L^{ab} by inner automorphisms.

Proof. It is clear since conjugation commutes with cup product by dimension shifting and it also commutes with the identification made in proposition 6.13. □

Chapter 8

Corank Lemma

This chapter is dedicated to a deep result about the rank of the Pontryagin dual of some cohomology groups as $\mathbb{Z}_p$-modules. This statement will play a central role in the proof of Mazur's control theorem.

The proof of this result is a good illustration of how can the theory of Iwasawa modules can be applied to arithmetic problems. In this problem, we consider a Galois group as an Iwasawa module. In fact, since the extension is abelian and pro-p, its Galois group is a $\mathbb{Z}_p$-module. Moreover, there is an action of another Galois group isomorphic to $\mathbb{Z}_p$, so it can be seen as an Iwasawa module due to proposition 2.9.

Theorem 8.1. Let K be a p-adic field. Suppose that A is a G_K-module and that $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ as a group. Then $H^1(K, A)$ is a cofinitely generated $\mathbb{Z}_p$-module whose corank is $[K : \mathbb{Q}_p]+\delta_A(K)$, where $\delta_A(K) = 1$ if $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ or $A \cong \mu_{p^\infty}$[1] as G_K modules and $\delta_A(K) = 0$ otherwise.

Proof. Assume first that G_K acts trivially on A. Hence

$$H^1(K, A) = \mathrm{Hom}(G_K, A) = \mathrm{Hom}(G_K^{\mathrm{ab}}, \mathbb{Q}_p/\mathbb{Z}_p)$$

where the last equality comes from the fact that A is abelian. Hence we can see that the pro-p completion of G_K^{ab} is the Pontryagin dual of $H^1(K, A)$.

By theorem 7.7 and [21], proposition II.5.7, there is an isomorphism

$$G_K^{\mathrm{ab}} \cong \overleftarrow{K} = \overleftarrow{\mathbb{Z}} \times \mathbb{Z}/(q-1) \times \mathbb{Z}/p^a \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]} = \mathbb{Z}_p^{[K:\mathbb{Q}_p]+1} \times \mathbb{Z}/(q-1) \times \mathbb{Z}/p^a \times \prod_{q \text{ prime}, q \neq p} \mathbb{Z}_q$$

where q is the cardinality of the residue field of K and $a \geq 0$ is an integer. Hence

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(K, A) = \mathrm{rank}_{\mathbb{Z}_p} G_K^{\mathrm{ab},p} = [K : \mathbb{Q}_p] + 1 = [K : \mathbb{Q}_p] + \delta_A(K)$$

Now assume that $A \cong \mu_{p^\infty}$ as G_{K_v}-modules. Then proposition 6.4 and theorem 7.2 imply that

$$H^1(K, A) \cong H^1\left(K, \varinjlim_n \mu_{p^n}\right) = \varinjlim_n H^1\left(K, \mu_{p^n}\right) \cong \varinjlim_n K^*/(K^*)^{p^n}$$

Since $K^* \cong \mathbb{Z} \times \mathbb{Z}/(q-1) \times \mathbb{Z}/p^a \times \mathbb{Z}_p^{[K_v:\mathbb{Q}_p]}$ by [21], proposition II.5.7, then

$$K^*/(K^*)^{p^n} \cong \begin{cases} (\mathbb{Z}/p^n)^{[K:\mathbb{Q}_p]+1} \times \dfrac{\mathbb{Z}/p^a}{\mathbb{Z}/p^{a-n}} & \text{if } n \leq a \\ (\mathbb{Z}/p^n)^{[K:\mathbb{Q}_p]+1} \times \mathbb{Z}/p^a & \text{if } n > a \end{cases}$$

[1] μ_{p^∞} represents the direct limit of the groups μ_{p^n} of p^n-roots of unity in $\overline{\mathbb{Q}_p}$.

The transition maps restrict well to each factor and they are injective except in the last factor, so

$$H^1(K,A) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K:\mathbb{Q}_p]+1} \times \mathbb{Z}/p^a \Rightarrow \text{corank}_{\mathbb{Z}_p} H^1(K,A) = [K:\mathbb{Q}_p] + \delta_A(K)$$

Now we will consider the case when $\delta_A(K) = 0$. We saw in example 4.1 that

$$\text{Hom}\,(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p \Rightarrow \text{Aut}\,(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p^*$$

Hence the action of the Galois group on A can be described with a character

$$\psi:\ G_K \to \mathbb{Z}_p^*$$

The map ψ is continuous. In fact, remember that $\text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$ was endowed with the compact-open topology, so consider a subbased open set $V(T,U)$, where $T \subset \mathbb{Q}_p/\mathbb{Z}_p$ is a compact set and $U \subset \mathbb{Q}_p/\mathbb{Z}_p$ is an open set. Since $\mathbb{Q}_p/\mathbb{Z}_p$ has the discrete topology, T is a finite set and

$$V(A,U) = \bigcap_{x\in A} \left(\bigcup_{y\in U} V(\{x\},\{y\}) \right)$$

Hence we just need to check that $\phi^{-1}\left(V(\{x\},\{y\})\right)$ is open for every $x, y \in \mathbb{Q}_p/\mathbb{Z}_p$. However, that is clear since it is the inverse image of $\{y\}$ via the continuous function

$$G_K \to \mathbb{Q}_p/\mathbb{Z}_p:\ \sigma \mapsto \sigma(x)$$

Assume first that $\text{Im}(\psi)$ is finite and $p > 2$. Using the p-adic logarithm, $\Delta := \text{Im}(\psi)$ has to be a cyclic group whose order divides $p-1$. Then $\ker(\psi)$ is a closed normal subgroup of finite index, so theorem 5.2 says that there is a finite extension $F|K$ such that $\ker(\psi) = G_F$. Then G_F acts trivially on A, so $H^1(F,A) = \text{Hom}(G_F, A)$. Then the exact sequence given in theorem 6.1 can be written as

$$0 \longrightarrow H^1(F|K,A) \xrightarrow{\text{Inf}} H^1(K,A) \xrightarrow{\text{Res}} \text{Hom}_{G_{F|K}}(G_F,A) \xrightarrow{tg} H^2(F|K,A)$$

By proposition 6.8, $H^n(F|K,A) = 0\ \forall n \geq 1$, so the restriction map is an isomorphism. Hence

$$\text{corank}_{\mathbb{Z}_p} H^1(K,A) = \text{corank}_{\mathbb{Z}_p} H^1(G_F,A)^{G_{F|K}} = \text{corank}_{\mathbb{Z}_p} \text{Hom}_{G_{F|K}}(G_F,A)$$

where $G_{F|K}$ acts on G_F by inner automorphisms. It is clear that

$$\text{Hom}_{G_{F|K}}(G_F,A) = \text{Hom}(G_F^{\psi},A)$$

where G_F^{ψ} is the maximal quotient of G_F on which $G_{F|K}$ acts by the character ψ. That is the quotient by the submodule generated by

$$\sigma(x) = \psi(\sigma)x\ \forall \sigma \in G_{F|K}\ \forall x \in G_F$$

By propositions 7.2 and 8.1 below,

$$\text{corank}_{\mathbb{Z}_p} H^1(K,A) = \text{rank}_{\mathbb{Z}_p}(G_F^{\psi}) = [K:\mathbb{Q}_p] = [K:\mathbb{Q}_p] + \delta_A(K)$$

In case $p = 2$, $|\Delta|$ is either 1 or 2. Since we are assuming that ψ is not the trivial character, then $\Delta = \{1,-1\} \subset \mathbb{Z}_2$, so by proposition 6.14, we have that

$$H^2(F|K,A) \cong \widehat{H}^0(F|K,A) \cong A^{\Delta}/N_{\Delta}(A) \cong \mathbb{Z}/2$$

Moreover, proposition 6.14. also implies that

$$H^1(F|K,A) \cong \widehat{H}^{-1}(F|K,A) =_{N_{\Delta}} A/I_G A = A/-2A \cong \mathbb{Z}/2$$

The restriction map has thus finite kernel and cokernel. Again we have that

$$\begin{aligned}\mathrm{corank}_{\mathbb{Z}_p} H^1(K,A) = \mathrm{corank}_{\mathbb{Z}_p} H^1(G_F,A)^{G_{F|K}} = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Hom}_{G_{F|K}}(G_F,A) = \\ \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Hom}(G_F^{\psi},A) = \mathrm{rank}_{\mathbb{Z}_p} G_F^{\psi} = [K:\mathbb{Q}_p] = [K:\mathbb{Q}_p] + \delta_A(K)\end{aligned}$$

Assume now that $\mathrm{Im}(\psi)$ is infinite and $p > 2$. Again using the p-adic logarithm, we find that $\mathrm{Im}(\psi) \cong \Delta \times \Gamma$, where Δ is still a cyclic group whose order divides $p-1$ and $\Gamma \cong \mathbb{Z}_p$. Again $\ker(\psi)$ is a closed subgroup, so there is a field extension $F_\infty|K$ such that $\ker(\psi) = G_{F_\infty}$. Hence $G := G_{F_\infty|K} \cong \Delta \times \Gamma$ and the inflation-restriction sequence can be written as

$$0 \longrightarrow H^1(G,A) \xrightarrow{\mathrm{Inf}} H^1(K,A) \xrightarrow{\mathrm{Res}} H^1(F_\infty,A)^G \xrightarrow{tg} H^2(G,A)$$

By proposition 6.21, we have that $H^2(\Gamma, A^\Delta) = 0$. Since $H^n(\Delta,A) = 0\ \forall n \geq 1$ by proposition 6.8, then theorem 6.2 implies that the following sequence is exact:

$$0 \longrightarrow H^2(\Gamma,A^\Delta) \xrightarrow{\mathrm{Inf}} H^2(G,A) \xrightarrow{\mathrm{Res}} H^2(\Delta,A)$$

Then $H^2(G,A) = 0$.

For the study of $H^1(G,A)$, we need to consider separately two cases. In case $|\Delta| = 1$, then $G = \Gamma$, so given a topological generator $\gamma \in \Gamma$,

$$H^1(G,A) = H^1(\Gamma,A) = A/(\gamma-1)A$$

However, $(\gamma-1)A$ is a division subgroup which does not vanish because Γ does not act trivially on A. Thus $(\gamma-1)A = A$, so $H^1(G,A) = 0$. In case $|\Delta| > 0$, then $A^\Delta = 0$ because $|\Delta|$ contains non-trivial roots of unity which do not fix any point. Then, inflation-restriction sequence

$$0 \longrightarrow H^1(\Gamma,A^\Delta) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(\Delta,A)$$

implies that $H^1(G,A) = 0$.

In case $p = 2$, then $|\Delta|$ can be 1 or 2. In case $|\Delta| = 1$, the preceding argument applies. However, in case $|\Delta| = 2$, subtle modifications are needed.

First of all, we have that

$$H^1(\Delta,A) \cong H^2(\Delta,A) \cong \mathbb{Z}/2$$

Moreover,

$$H^1(\Gamma,A^\Delta) = A^\Delta/(\gamma-1)A^\Delta, \quad H^2(\Gamma,A^\Delta) = 0$$

Since $A^\Delta \cong \mathbb{Z}/2$, then inflation-restriction sequence implies that both $H^1(G,A)$ and $H^2(G,A)$ are finite.

From now on, we will make no distinction between $p = 2$ and $p > 2$. In any case the restriction map $H^1(K,A) \to H^1(F_\infty,A)^G = \mathrm{Hom}_G(F_\infty,A)$ has finite kernel and cokernel, so

$$\mathrm{corank}_{\mathbb{Z}_p}\left(H^1(K,A)\right) = \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Hom}_G(F_\infty,A)\right) = \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Hom}_G(G_{F_\infty^{ab,p}},A)\right)$$

where we have used that A is abelian, so every homomorphism $G_{F_\infty} \to A$ vanish on the commutator subgroup. Moreover, since A is p-primary, we have used that every homomorphism has to factor through a pro-p quotient.

Let then $M_\infty|F_\infty$ be the maximal abelian extension pro-p of F_∞. Notice that $M_\infty|K$ is Galois since $\sigma(M_\infty)|F_\infty$ would be an abelian pro-p extension for every $\sigma \in K$, so $\sigma(M_\infty) \subset M_\infty$. Moreover, G acts on $X = G_{F_\infty}^{ab,p} = G_{M_\infty|F_\infty}$ by inner automorphisms. With this action, we

have that X is a $\mathbb{Z}_p$ module with a $\mathbb{Z}_p$-linear and continuous action of G. In particular, we can consider only the action of Γ on X, which makes X into an Iwasawa module.

By theorem 5.2, $\Gamma = G_{F_\infty|F_0}$ for some field extension $F_0|K$. Since $\Gamma \cong \mathbb{Z}_p$ it is topologically generated by some $\gamma \in \Gamma$. Then there is exactly one subextension $F_n|F_0$ of $F_\infty|F_0$ such that $[F_n : F_0] = p^n$, which will satisfy that $G_{F_\infty|F_n} = \overline{\langle \gamma^{p^n} \rangle}$. For each $n \geq 0$, define again M_n as the maximal abalian pro-p extension of F_n. It is clear that $F_\infty \subset M_n \subset M_\infty$ and that $M_n|F_n$ is the maximal abelian subextension of $M_\infty|F_n$. Hence $G_{M_\infty|M_n}$ is just the closure of the commutator subgroup $(G_{M_\infty|F_n})'$. Hence,

$$G_{M_\infty|M_n} = \{\gamma^{p^n} x \gamma^{-p^n} x^{-1} : x \in X\} = \{\gamma^{p^n}(x)x^{-1} : x \in X\}$$

because X is abelian and, therefore, the latter is a subgroup and it is closed since the map $x \mapsto \gamma^{p^n}(x)x^{-1}$ is a continuous map which sends the compact group X to a compact set. Using the notation used to study Iwasawa modules, we have that

$$G_{M_\infty|M_n} = \omega_n X \Rightarrow X/\omega_n X = G_{M_n|F_\infty}$$

By proposition 7.2, $G_{M_n|F_n}$ is a finitely generated $\mathbb{Z}_p$-module of rank

$$\text{rank}_{\mathbb{Z}_p} G_{M_n|F_n} = \text{rank}_{\mathbb{Z}_p} \overleftarrow{F_n^*} = [F_n : \mathbb{Q}_p] + 1 = p^n|\Delta|[K_v : \mathbb{Q}_p] + 1$$

Then, since $F_\infty|F_n$ is also a $\mathbb{Z}_p$-extension, we have that

$$\text{rank}_{\mathbb{Z}_p} G_{M_n|F_\infty} = \text{rank}_{\mathbb{Z}_p} X/w_n X = p^n|\Delta|[K_v : \mathbb{Q}_p]$$

Hence by proposition 2.8, X is a finitely generated Iwasawa module whose rank is

$$\text{rank}_\Lambda X = |\Delta|[K_v : \mathbb{Q}_p]$$

By proposition 8.2 below, $H^2(F_\infty, \mathbb{Z}/p) = 0$ and then multiplication by p induces a surjective endomorphism in the cohomology group

$$H^1(F_\infty, \mathbb{Q}_p/\mathbb{Z}_p) = \text{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p) = \widehat{X}$$

X will thus be a divisible group. It means that $\widehat{X}$ has not finite quotients, so X does not contain finite $\mathbb{Z}_p$-submodules and, therefore, X is $\mathbb{Z}_p$-torsion-free.

Let $Y = X_{\Lambda-tors}$ and let $W = X/Y$. Since W is torsion-free, snake's lemma 6.3 induces the following short exact sequence:

$$0 \longrightarrow Y/w_n \longrightarrow X/w_n \longrightarrow W/w_n \longrightarrow 0$$

Since proposition 2.2 implies that $\text{rank}_\Lambda X = \text{rank}_\Lambda W = [K_v : \mathbb{Q}_p]|\Delta|$, then proposition 2.8, together with the fact that W is Λ-torsion free, implies that

$$\text{rank}_{\mathbb{Z}_p} X/w_n X = \text{rank}_{\mathbb{Z}_p} W/w_n W = p^n[K_v : \mathbb{Q}_p]|\Delta|$$

Hence Y/w_n must be finite and isomorphic to a subgroup of X/w_n, what will be injected by 7.5 to μ_{F_n}, the p-primary part of the roots of unity contained in F_n.

Assume that $\mu_{p^\infty} \not\subset F_\infty$. Then μ_{F_n} has bounded order as $n \to \infty$. Then

$$Y = \varprojlim_n Y/(w_n)$$

would be finite. However, since X had not non-trivial finite submodules, $Y = 0$. Thus X is Λ-torsion-free.

In case that $\mu_{p^\infty} \subset F_\infty$, then $\mu_{F_n} = (X/w_n)_{\mathbb{Z}_p-tors}$ would be unbounded. Since W is Λ-torsion-free and has rank $r = |\Delta| \cdot [K_v : \mathbb{Q}_p]$, by theorem 2.4 it has to be pseudo-isomorphic to Λ^r and this pseudo-isomorphism has to be injective. In other words, there is a finite Λ-module C such that the following short exact sequence is exact:

$$0 \longrightarrow W \longrightarrow \Lambda^r \longrightarrow C \longrightarrow 0$$

By snake's lemma 6.3, there is another exact sequence

$$w_n C \longrightarrow W/w_n \longrightarrow (\Lambda/w_n)^r$$

Since $\Lambda/w_n \cong \mathbb{Z}_p^{p^n}$ has no $\mathbb{Z}_p$-torsion, then the $\mathbb{Z}_p$ torsion of W/w_n has order bounded by $|C|$. Hence Y/w_n is unbounded. Since Y/w_n is isomorphic to a subgroup of $\mu_{F_n} \subset \mu_{p^\infty}$, then

$$Y = \varinjlim_n Y/w_n = \varinjlim_n \mu_{F_n} = \varinjlim_m \mu_{p^n}{}^2$$

To complete the proof, notice that

$$\mathrm{Hom}_G(X, A) = \mathrm{Hom}(X^\psi, A) \Rightarrow \mathrm{corank}_{\mathbb{Z}_p} H^1(K, A) = \mathrm{rank}_{\mathbb{Z}_p} X^\psi$$

If we denote by ψ_Δ and ψ_Γ the restrictions of ψ to Δ and Γ, respectively, it is clear that

$$X^\psi = \left(X^{\psi_\Delta}\right)^{\psi_\Gamma}$$

By propositions 7.2 and 8.1 below, X^{ψ_Δ}/w_n has $\mathbb{Z}_p$-rank equal to $p^n[K : \mathbb{Q}_p]$, so proposition 2.8 implies that X^{ψ_Δ} is a finitely generated Λ-module of rank $[K : \mathbb{Q}_p]$.

Now we are going to study the character restricted to Γ. If $\gamma \in \Gamma$ is a topological generator, its image determines all the character ψ_Γ. Hence

$$X^\psi = \left(X^{\psi_\Delta}\right)^{\psi_\Gamma} = \frac{X^{\psi_\Delta}}{(\gamma - \psi(\gamma))} = \frac{X^{\psi_\Delta}}{(T + 1 - \psi(\gamma))}$$

The decomposition made using the p-adic logarithm says that $\psi(\Gamma) \in 1 + p\mathbb{Z}_p$, so $T + 1 - \psi(\gamma)$ is a distinguished polynomial.

In case $\mu_{p^\infty} \not\subset F_\infty$, then X^ψ is pseudo-isomorphic to $\Lambda^{[K:\mathbb{Q}_p]}$, being that pseudo-isomorphism injective. Hence,

$$\mathrm{rank}_{\mathbb{Z}_p} X^\psi = \mathrm{rank}_{\mathbb{Z}_p} \frac{X^{\psi_\Delta}}{(T + 1 - \psi(\gamma))} = [K : \mathbb{Q}_p] = [K : \mathbb{Q}_p] + \delta_A(K)$$

Otherwise, when $\mu_{p^\infty} \subset F_\infty$, then G acts on μ_{p^∞} by some character χ, which will be different from ψ by hypothesis. If $\psi_\Delta \neq \chi_\Delta$, then $Y \cap X^{\psi_\Delta} = \emptyset$, so the above mentioned argument applies. Otherwise, $\psi_\Gamma \neq \chi_\Gamma$ and, therefore,

$$\frac{Y}{(T + 1 - \psi(\gamma))}$$

would be finite. Thus,

$$\mathrm{rank}_{\mathbb{Z}_p} X^\psi = \mathrm{rank}_{\mathbb{Z}_p} \frac{X^{\psi_\Delta}}{(T + 1 - \psi(\gamma))} = [K : \mathbb{Q}_p] = [K : \mathbb{Q}_p] + \delta_A(K)$$

□

[2] Although μ_{F_n} does not necessarily coincide with μ_{p^n}, it is true that $\mu_{F_n} = \mu_{p^m}$ for some $m \in \mathbb{N}$. Since we have seen that μ_{F_n} has unbounded order as $n \to \infty$ and transition maps are the canonical projections, both inverse limits are the same.

Now we proof two facts used in the proof of the corank lemma. The first one is about the corank of local fields.

Proposition 8.1. Let K be a p-adic field and let $L|K$ be a finite extension such that $\Delta := G_{L|K}$ is a cyclic group of order n.

1. If R_K and R_L denote the ring of integers of K and L, respectively, then
$$\text{rank}_{\mathbb{Z}_p} R_L^\chi = \text{rank}_{\mathbb{Z}_p} R_K = [K : \mathbb{Q}_p] \ \forall \chi \in \widehat{\Delta}$$

2. Moreover,
$$\text{rank}_{\mathbb{Z}_p} \overleftarrow{L^*}^\chi = \begin{cases} [K : \mathbb{Q}_p] + 1 & \text{if } \chi \text{ is trivial.} \\ [K : \mathbb{Q}_p] & \text{if } \chi \text{ is not trivial.} \end{cases}$$
when we are understanding the ranks as the rank of their pro-p completions as $\mathbb{Z}_p$-modules.

Proof. 1. Let $\sigma \in \Delta$ be a generator of the group and let $a \in R_L$ be a generator of a normal basis. Then $R_K[\Delta][a] := R_K + aR_K + \sigma(a)R_K + \cdots + \sigma^{n-1}(a)R_K$ is a $\mathbb{Z}_p$-module of the same rank as R_L, so $(R_L : R_K[\Delta][a]) < \infty$. Since the rank is an additive function, it is clear that
$$\text{rank}_{\mathbb{Z}_p} R_L^\chi = \text{rank}_{\mathbb{Z}_p} R_K[\Delta][a]^\chi \ \forall \chi \in \widehat{\Delta}$$
The matrix that encodes the action of σ on $R_K[a]$ has each n^{th}-root of unit as aen eigenvalue of dimension 1. Hence it is easily seen that
$$\text{rank}_{\mathbb{Z}_p} R_K[\Delta][a]^\chi \cong R_K \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$$

2. Using p-adic logarithm one can see that L^* contains a subgroup H of finite index isomorphic to $\mathbb{Z} \times R_L$, where Δ acts trivially on $\mathbb{Z}$ and R_L is the ring of integers of L. Thus the statement is clear from what was proven on the first part.

□

The other unproven result used was about the p-cohomological dimension of the absolute Galois group G_K of an extension $K|\mathbb{Q}_p$ whose degree is divisible by p^∞.

Proposition 8.2. Let $K|\mathbb{Q}_p$ be a field extension whose degree is divisible by p^∞. Then
$$H^2(K, \mathbb{Z}/p) = 0$$

Proof. By proposition 4.6, we have that
$$H^2\left(K, \overline{K}^*\right) = \varinjlim_L H^2\left(L, \overline{K}^*\right) \tag{8.1}$$
where L runs through the finite Galois extensions of $\mathbb{Q}_p$ and transition maps are restrictions.

We will see that $H^2\left(K, \overline{K}^*\right)_p = 0$. Suppose for the sake of contradiction that it contains an element of p-torsion, so it has a representative in $H^2\left(L, \overline{K^*}\right)$, for some finite Galois extension $L|\mathbb{Q}_p$. Let $F|L$ be an extension of degree p such that $F \subset K$, whose existence is guaranteed because p^∞ divides $[K : L]$. Since $H^1\left(F, \overline{K}^*\right)$, theorem 6.2 gives an exact sequence
$$0 \longrightarrow H^2\left(F|L, F^*\right) \xrightarrow{\text{Inf}} H^2\left(L, \overline{K}^*\right) \xrightarrow{\text{Res}} H^2\left(L, \overline{K}^*\right)$$

By corollary 7.4, every element of order p is in the image of the inflation map, so it is restricted to zero and, therefore, it represents the zero class in the direct limit of equation 8.1.

The exact sequence of G_K modules

$$1 \longrightarrow \mu_p \longrightarrow \overline{K}^* \longrightarrow \overline{K}^* \longrightarrow 1$$

induces another exact sequence by lemma 6.4:

$$H^1\left(K, \overline{K}^*\right) \longrightarrow H^2\left(K, \mu_p\right) \longrightarrow H^2\left(K, \overline{K}^*\right)$$

By theorem 7.2, $H^1\left(K, \overline{K}^*\right) = 0$. Since $H^2\left(K, \mu_p\right)$ is p-primary, it has to vanish because the p-primary part of $H^2\left(K, \overline{K}^*\right)$ does.

The preceding argument applies to every extension of K, so $H^2(H, \mu_p) = 0$ for every subgroup $H \subset G_K$, in particular that is true when $H = G_p$ is a p-Sylow subgroup. Since G_p is a pro-p group and $\mathrm{Aut}(\mu_p)$ has $p - 1$ elements, then H acts trivially on μ_p, so

$$H^2(H_p, \mathbb{Z}/p) = H^2(H_p, \mu_p) = 0$$

If otherwise H_l is a l-Sylow subgroup, then $H^2(H_l, \mathbb{Z}/p) = 0$ by proposition 6.8.

By corollary 6.6, $H^2(K, \mathbb{Z}/p) = 0$. □

Part III

Arithmetic of Elliptic Curves

Chapter 9

Elliptic Curves over Local Fields

The goal of this chapter is exposing the basic theory of elliptic curves defined over local fields. We start in section 9.1 by defining the reduction map and stating some of its properties. In this section, we have work in a slightly more general case and we only assume that the field is complete with respect to a discrete valuation. In particular, we have studied some properties of the elements in the kernel of this map and we have proved that it is surjective in case E has good reduction. Even more, we have showed that, assuming we are working with fields of characteristic 0, it is still surjective when restricted to the torsion subgroups of the original and reduced curves.

In section 9.2 we state a precise characterisation of how the groups $E(K)$ can be. In this case, we do not try to be as general as possible and we will assume that K is a p-adic field. In particular, we have proven that

$$E(K) \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times T$$

where T is a finite group. After that, we have showed this behaviour under taking certain tensor products, that will appear on chapter 11.

9.1 The Reduction Modulo π

Let K be a complete field with respect to a discrete valuation, being R its ring of integers, $\mathfrak{m}$ its maximal ideal and $k = R/\mathfrak{m}$ its residue field of R. Let E/K be an elliptic curve whose Weierstrass equation can be written as

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

Since the change of coordinates $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ leads to a replacement in the coefficients of the preceding equation $a_i \mapsto u^i a_i$, we can assume these coefficients belong to R. Then, we will refer as a *minimal Weierstrass equation* to one of these equations having coefficients in R that minimises the valuation $v(\Delta)$ of its discriminant.

Proposition 9.1. A minimal Weierstrass equation is unique up to a change of coordinates

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

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

Proof. [27], Chap. VII. Prop. 1.3. □

Proposition 9.2. If (x, y) are coordinates of a Weierstrass equation whose coefficients are in R, then any change of coordinates

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

used to produce a minimal Weierstrass equation whose coordinates are (x', y') satisfies that $u, r, s, t \in R$.

Proof. [27], Chap. VII. Prop. 1.3. □

Consider a minimal Weierstrass equation for E and the surjective homomorphism $R \to k : t \mapsto \widetilde{t}$. Then the following equation defines an elliptic curve over k provided it is non-singular.

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

Proposition 9.1 tells us that the preceding equation is unique up to a standard change of coordinates in k.

Given a point $P \in E(K)$, we can find homogeneous coordinates $(x_0 : y_0 : z_0)$ such that $x_0, y_0, z_0 \in R$ and at least one of them belongs to R^*. Then we can define the reduction map

$$E(K) \to \widetilde{E}(k) : P = (x_0 : y_0 : z_0) \mapsto \widetilde{P} = (\widetilde{x_0} : \widetilde{y_0} : \widetilde{z_0})$$

It is also possible to define the reduction map for points the defined over the algebraic closure. In fact, if $P \in E(\overline{K})$, then P is defined over a finite extension L of K, which will be a complete field over the extension of the valuation v, by [21], theorem II. 4.8. Hence, we can define the reduction map in L, so the reduction map can be extended to the whole curve $E(\overline{K})$.

The main problem that arises in this reduction is that the reduced curve $\widetilde{E}$ might not be singular. In that case, we say that E has a *bad reduction*. Otherwise, we say that E has a *good reduction*. Nevertheless, non-singular points of the reduced curve form a subgroup.

Lemma 9.1. The subgroup E_{ns} of non-singular points of an elliptic curve E defined over a perfect field K form a subgroup of the curve.

Proof. Clearly $O \in E_{ns}$. On the other hand, let P, Q be two non-singular points of the curve and let R be a singular one. We will show that $P + Q \neq R$.

Let S be the third point of intersection of the curve with the line through P and Q. Since R is singular, then $R \neq O$ and every line through R has double or triple multiplicity at R, so $S \neq R$. By the same reason, the line through S and O cannot intersect R, so $P + Q \neq R$.

Similarly, the line through P and O cannot contain R, so $R \neq -P$. Therefore, non-singular points constitute a subgroup of the curve. □

We want to see that the reduction map is a group homomorphism onto non-singular points of the reduced curve. Consider the following subgroups.

$$E_0(K) := \{P \in E(K) : \widetilde{P} \in \widetilde{E}_{\text{ns}}(k)\}, \quad E_1(K) = \{P \in E(K) : \widetilde{P} = \widetilde{O}\}$$

Lemma 9.2. Let $P, Q \in E_0(K)$ (not necessarily distinct) and $L : ax + by + cz = 0$ be the line through them. Then $\widetilde{L} = \widetilde{a}\widetilde{x} + \widetilde{b}\widetilde{y} + \widetilde{c}\widetilde{z} = 0$ is the line through $\widetilde{P}$ and $\widetilde{Q}$.

Proof. Let $E : f(x, y, z) = 0$ be a minimal Weierstrass equation for the curve. If $\widetilde{P} \neq \widetilde{Q}$, the statement is clear. Moreover, if $P = Q$, then the tangent line through P has the equation

$$L = \frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y + \frac{\partial f}{\partial z}(P)z = 0$$

Then the tangent line of the reduced curve $\widetilde{E}$ through $\widetilde{P}$ has the desired form.

The only case remaining is $P \neq Q$ and $\widetilde{P} = \widetilde{Q}$. If $\widetilde{P} \neq \widetilde{O}$ we can write

$$P = (\alpha, \beta) \in E(K), \quad Q = (\alpha + \mu, \beta + \lambda) \in E(K)$$

where $\alpha, \beta, \lambda, \mu \in R$. The assumption $\widetilde{P} = \widetilde{Q}$ means that $\lambda, \mu \in \mathfrak{m}$. The fact that $\widetilde{P}$ is a non-singular point means that either $\dfrac{\partial \widetilde{f}}{\partial \widetilde{x}}(\widetilde{P}) \neq 0$ or $\dfrac{\partial \widetilde{f}}{\partial \widetilde{y}}(\widetilde{P}) \neq 0$. Assume the latter. Since $f(\alpha, \beta) = 0$, there are $a, b, c \in R$ such that

$$0 = f(\alpha + \mu, \beta + \lambda) = \frac{\partial f}{\partial x}(\alpha, \beta)\mu + \frac{\partial f}{\partial y}(\alpha, \beta)\lambda + a\mu^2 + b\mu\lambda + c\lambda^2$$

Since we are assuming that $\dfrac{\partial \widetilde{f}}{\partial \widetilde{y}}(\widetilde{P}) \neq 0$, then $v\left(\dfrac{\partial f}{\partial y}(\alpha, \beta)\right) = 0$, so

$$v(\lambda) = v\left(\frac{\partial f}{\partial y}(\alpha, \beta)\lambda\right) = v\left(\frac{\partial f}{\partial x}(\alpha, \beta)\mu + a\mu^2 + b\mu\lambda + c\lambda^2\right) \geq \min\{v(\mu), v(\lambda^2)\}$$

Since $v(\lambda) < v(\lambda^2)$ because $\lambda \in \mathfrak{m}$, then $v(\lambda) \geq v(\mu)$ so $\frac{\lambda}{\mu} \in R$. Then,

$$\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y}\frac{\lambda}{\mu} \equiv 0 \mod m$$

Then, tangent line through $\widetilde{P}$ has equation

$$y - \widetilde{\beta} = \frac{\widetilde{\lambda}}{\widetilde{\mu}}(x - \widetilde{\alpha})$$

which is clearly the reduced line $\widetilde{L}$ of the line through P and Q. The case when $\dfrac{\partial \widetilde{f}}{\partial \widetilde{x}} \neq 0$ is similar.

Finally, the case $\widetilde{P} = \widetilde{Q} = \widetilde{O}$ is analogous considering the inhomogeneous coordinates $\frac{x}{y}$ and $\frac{z}{y}$.

□

Corollary 9.1. The reduction map $E_0(K) \to \widetilde{E}_{\text{ns}}(k)$ is a group homomorphism.

Last group homomorphism can be understood as part of the following short exact sequence.

Proposition 9.3. The following exact sequence of abelian groups is exact.

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{\pi} \widetilde{E}_{\text{ns}}(k) \longrightarrow 0$$

Proof. The statement is clear except for the surjectivity of π. Since clearly $\widetilde{O} = \pi(O) \in \pi(E_0(K))$, let $\widetilde{P} = (\widetilde{\alpha}, \widetilde{\beta}) \in E_{\text{ns}}(k) \setminus \{\widetilde{O}\}$. Since it is non-singular, then either $\dfrac{\partial \widetilde{f}}{\partial \widetilde{x}} \neq 0$ or $\dfrac{\partial \widetilde{f}}{\partial \widetilde{y}} \neq 0$. Assume without lost of generality the latter and choose any $x_0 \in R$ such that $\widetilde{x}_0 = \widetilde{\alpha}$. Then the polynomial $\widetilde{f}(\widetilde{x}_0, y) \in k[[T]]$ has a simple root at $y = \widetilde{\beta}$. By Hensel's lemma, shown in proposition 2.1, there is some $y_0 \in R$ such that $\widetilde{y}_0 = \widetilde{\beta}$ and $f(x_0, y_0) = 0$. Then, $\pi((x_0, y_0)) = (\widetilde{\alpha}, \widetilde{\beta})$, so π is surjective. □

We can also study the kernel of the reduction map using the theory of formal groups. Let $F \in R[[X,Y]]$ be the power series describing its formal group law as in section 3.5. Given $z \in \mathfrak{m}$, lemma 2.1 implies that there is a unique $w = w(z) \in \mathfrak{m}$ such that $(z,w) \in E(K)$, provided that the change of coordinates described in section 3.5 has been made. If $\mathcal{F}(m)$ is the group associated to $(\mathcal{F}, F)$, then the map:

$$\mathcal{F}(m) \to E_1(K)$$

is a group isomorphism, since formal development of power series expansion can be done explicitly in this case because convergences are guaranteed. Thus next proposition comes from the general theory of formal groups.

Theory of formal groups enable us to compute some torsion points belonging to the kernel of the reduction map.

Proposition 9.4. Let $m \in \mathbb{N}$ which is not a power of $p = \mathrm{char}(k)$. Then the subgroup $E_1(K)$ has no non-trivial points of order m.

Proof. It comes from proposition 3.2. □

Proposition 9.5. Let E/K be an elliptic curve and let $m \in \mathbb{N}$ be prime to $\mathrm{char}(k)$. Assume further that the reduced curve is not singular. Then the reduction map

$$\pi : E(K)[m] \to \widetilde{E}(k)$$

is injective, where $E(K)[m]$ denotes the subgroup of m-torsion points of $E(K)$.

Proof. The kernel of this map has to be contained in $E_1(K)$. Since $E_1(K)$ contains no torsion points of order m by proposition 9.4, the kernel has to be trivial. □

Up to know, we have studied torsion elements whose orders are prime to $p = \mathrm{char}(k)$. For the general case, there are more difficulties but we have the following theorem.

Theorem 9.1. Let K be a complete field respect to a discrete valuation v and let R be its ring of integers. Let E/K be an elliptic curve given by a Weierstrass equation

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

with all $a_i \in R$. Let $P \in E(K)$ be a point of exact order $m \geq 2$.

- If m is not a power of p, then $x(P), y(P) \in R$.
- If $m = p^n$ and $r = \left\lfloor \dfrac{v(p)}{p^n - p^{n-1}} \right\rfloor$, then

  $$\pi^{2r}x(P), \pi^{3r}y(P) \in R$$

  where π is a uniformizer in K.

Proof. If (x', y') are coordinates of a minimal Weierstrass equation, proposition 9.2 implies that

$$v\left(x(P)\right) \geq v\left(x'(P)\right), \quad v\left(y(P)\right) \geq v\left(y'(P)\right)$$

Therefore, we can assume the given Weierstrass equation is minimal. If $x(P) \in R$, there is nothing to prove, so we will assume that $v\left(x(P)\right) < 0$. By the ultrametric inequality,

$$3v\left(x(P)\right) = 2v\left(y(P)\right) = -6s$$

for some $s \in \mathbb{N}$. Writing $P = \left(\dfrac{x(P)}{y(P)}, 1, \dfrac{1}{y(P)}\right) = (-z(P), 1 - w(P))$, we see that $P \in E_1(K)$. Then, the order of P has to be a prime power by proposition 3.2.

In that case, theorem 3.1 implies that

$$s = v\left(-\frac{x(P)}{y(P)}\right) = v\left(z(P)\right) \leq \frac{v(p)}{p^n - p^{n-1}} \Rightarrow s \leq r$$

Then, $\pi^{2r}x(P)$ and $\pi^{3r}y(P) \in R$. □

There is a slightly stronger result about the surjective of the reduction map which says that is is still surjective when restricted to the torsion points of the curve.

Theorem 9.2. Let E be an elliptic curve defined over K. Assume E has good or multiplicative reduction at K. Then the reduced map restricted to the torsion subgroup

$$\pi : \ E[m] \to \widetilde{E}_{\text{ns}}[m]$$

is surjective.

Proof. Call $\mathcal{F} := \ker(\pi)$. The operation in $\mathcal{F}$ can be described by a formal group defined over the ring of integers R of K and its associated group defined on the maximal ideal $\overline{\mathfrak{m}}$ of the ring of integers of the algebraic closure $\overline{K}$. Since $\widetilde{E}_{\text{ns}}$ has finite p-torsion, then $\mathcal{F}$ has finite height. Hence corollary 3.2 implies that $\mathcal{F}$ is divisible. Consider then the following commutative diagram in which the rows are exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{F} & \longrightarrow & E & \xrightarrow{\pi} & \widetilde{E}_{\text{ns}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \\ 0 & \longrightarrow & \mathcal{F} & \longrightarrow & E & \xrightarrow{\pi} & \widetilde{E}_{\text{ns}} & \longrightarrow & 0 \end{array}$$

Since $\mathcal{F}$ is $[m]$ divisible, then multiplication by m is surjective in $\mathcal{F}$, so snake lemma gives an exact sequence

$$0 \longrightarrow \mathcal{F}[m] \longrightarrow E[m] \xrightarrow{\pi} \widetilde{E}_{ns}[m] \longrightarrow 0$$

In particular, π remains surjective when restricted to $E[m]$. □

Corollary 9.2. The restricted map

$$\pi : \ E_{\text{tors}}(\overline{K}) \to \widetilde{E}(\overline{k})$$

is surjective.

Proof. It comes from theorem 9.2 and the fact that $\widetilde{E}(\overline{k})$ is torsion. □

Corollary 9.3. The restricted map

$$\pi : \ E[p^\infty] \to \widetilde{E}[p^\infty]$$

is surjective and $\ker \pi \cong \mathbb{Q}_p/\mathbb{Z}_p$.

9.2 The Structure of Mordell-Weil groups

The main goal of this section is to give a description of the group $E(K)$, when now K is a p-adic field. First we are going to see that the group $E_0(K)$ has finite index.

Theorem 9.3. Let E be an elliptic curve defined over a local field K. Then $E_0(K)$ has finite index in $E(K)$.

Proof. We can assume that the elliptic curve is given by a minimal Weierstrass equation in $\mathbb{P}^2(K)$, so we can give $E(K) \subset \mathbb{P}^2(K)$ the subspace topology, where the topology in $\mathbb{P}^2(K)$ is the quotient topology inherited from $K^3 \setminus \{0\}$.

Since K is compact, then K^2 is also compact by Tychonoff's theorem. Calling φ the quotient map, we find that

$$\mathbb{P}^2(K) := \varphi\big((K \times K \times \{1\}) \cup (K \times \{1\} \times K) \cup (\{1\} \times K \times K)\big)$$

Thus $\mathbb{P}^2(K)$ is a compact set.

Let $E(K)$ be given by the Weierstrass polynomial $f(x : y : z) = 0$. Since product and sum are clearly continuous functions $K \times K \to K$, then the polynomial

$$f : \ K^3 \to K : \ (x, y, z) \mapsto f(x, y, z)$$

defines a continuous function. Hence $f^{-1}(\{0\}) \subset K^3$ is a closed subset so

$$E(K) = \{(x : y : z) : f(x, y, z) = 0\}$$

is a closed in the compact space $\mathbb{P}^2(K)$ because $\varphi^{-1}\left(E(K)\right) = f^{-1}(\{0\})$ was also closed and it is the definition of quotient topology. Hence $E(K)$ is also compact.

It can also be seen that $E(K)$ is a topological group with the addition given by the group law. In fact, the sum is clearly a continuous function at every point different from

$$(P, P), \quad (P, -P), \quad (P, O), \quad (O, P) \ \forall P \in E(K)$$

since it is defined by polynomial functions of the coordinates. To see the continuity at a point (P, O) we just need to consider how a basis of neighbourhoods of O is. We can define them as

$$U^{(n)} = \{(a : 1 + b : c) : a, b, c \in \mathfrak{m}^n\} = \left\{ \left(\frac{a}{1+b} : 1 : \frac{c}{1+b} \right) : a, b, c \in \mathfrak{m}^n \right\} \cup \{O\} = \mathcal{F}(\mathfrak{m}^n)$$

If $P \in \mathcal{F}(\mathfrak{m})$, formal group law implies that the sum is continuous at (P, O). Otherwise, choose some $Q \in \mathcal{F}(\mathfrak{m})$, so the sum can be computed as

$$(A, B) \mapsto (A + Q, B - Q) \mapsto (A + Q) + (B - Q) = A + B \ \forall A, B \in E(K)$$

Then the sum map is continuous at (P, O) for being a composition of continuous functions.

To see the continuity at (P, P) and $(P, -P)$, we choose some $Q \in E(K) \setminus \{P, -P, O\}$ and sum $P + R = (P + Q) + (R - Q)$. The fact that the inversion is also a continuous function comes from its definition as polynomial functions in the coordinates. The extension to O is proven similarly using the formal law.

The reduction $\pi : E(K) \to \widetilde{E}(k)$ is clearly continuous provided that $\widetilde{E}(k)$ is endowed with the discrete topology. In fact, the reduction map $\pi : R^3 \setminus \mathfrak{m}^3 \to k^3 \setminus \{(0, 0, 0)\}$ is continuous and continuity behaves well after considering the quotient map. Hence $E_0(K)$ is an open subgroup of $E(K)$. Since the cosets is an open cover of $E(K)$, the compactness implies that $(E(K) : E_0(K)) < \infty$. □

Theorem 9.4. Let K be a finite extension of $\mathbb{Q}_p$ and let $n = [K : \mathbb{Q}_p]$. Then $E(K)$ contains a subgroup of finite index that is isomorphic to $\mathbb{Z}_p^n$ which is contained in $E_1(K)$.

Proof. By theorem 9.3 the factor group $E(K)/E_0(K)$ is finite. Moreover, $E_0(K)/E_1(K) \cong \widetilde{E}_{ns}(k)$ is also finite.

Since $E_1(K)$ is isomorphic to the associated group of some formal group $\mathcal{F}(\mathfrak{m})$, we just need to see that $\mathcal{F}(\mathfrak{m})$ has a group of finite index which is isomorphic to $\mathbb{Z}_p^n$. However, we know

that the factor groups $\mathcal{F}(\mathfrak{m}^i)/\mathcal{F}(\mathfrak{m}^{i+1}) \cong \mathfrak{m}_i/\mathfrak{m}_{i+1}$ are finite for every $i \in \mathbb{N}$ and that for large enough r, theorem 3.2 guarantees that the formal logarithm map

$$\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}^r) \to \mathcal{G}_a(\mathfrak{m}^r) = \pi^r R^+ \cong R^+$$

is an isomorphism, where R^+ is the additive group of the ring of integers R of K. Since $R^+ \cong \mathbb{Z}_p^n$, the proof is complete. □

Corollary 9.4. Let K be a finite extension of $\mathbb{Q}_p$. Then $E_1(K)$ is a $\mathbb{Z}_p$ module isomorphic to $\mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times T$, where T is a finite $\mathbb{Z}_p$-module.

Proof. First we will see that $E_1(K) \cong \mathcal{F}(\mathfrak{m})$ can be endowed with a structure of $\mathbb{Z}_p$-module. To define that structure, let $\alpha \in \mathbb{Z}_p$ and let $(a_n) \subset \mathbb{Z}$ a sequence converging to α. Then (a_n) is a Cauchy sequence in the p-adic topology, which means that for every $k \in \mathbb{N}$ there exists some $N \in \mathbb{N}$ such that $a_i \equiv a_j \mod p^k$ for every $i, j \geq N$.

Since corollary 3.4 implies that $[p](T) = pf(T) + g(T^p)$, then $[p^k](y) \in \mathcal{F}(\mathfrak{m}^k)\ \forall y \in \mathcal{F}(\mathfrak{m})$. Now fix some $x \in \mathcal{F}(\mathfrak{m})$. Then

$$[a_i](x) + \mathcal{F}(\mathfrak{m}^k) \equiv [a_j](x) + \mathcal{F}(\mathfrak{m}^k)\ \forall i, j \geq N$$

Hence $([a_i](x))$ is a Cauchy sequence in $\mathcal{F}(\mathfrak{m})$ and, by completeness, it will converge to some value, which will be by definition, $[\alpha]x \in \mathcal{F}(\mathfrak{m})$. One could check easily that this definition does not depend on the sequence (a_i) chosen and that it satisfies the axioms of the definition of $\mathbb{Z}_p$-module.

By theorem 9.4, $E_1(K)$ has a subgroup of finite index which is isomorphic to $\mathbb{Z}_p^{[K:\mathbb{Q}_p]}$. In particular, $E_1(K)$ is a finitely generated $\mathbb{Z}_p$-module and has rank $[K : \mathbb{Q}_p]$. Then the structure theorem of finitely generated modules over principal ideal domains states that

$$E_1(K) \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times T$$

where T is a finite torsion $\mathbb{Z}_p$-module. □

In case E has good reduction, it is possible to extend the direct product structure to the Mordell-Weil group.

Theorem 9.5. Let K be a finite extension of $\mathbb{Q}_p$ and let E be an elliptic curve having good reduction at K_v. Then $E(K) \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times T$ (as groups), where T is a finite group.

Proof. Since $\widetilde{E}(k)$ is a torsion group, we can split it into its p-primary and non p-primary parts:

$$\widetilde{E}(v) = E(k)_p \times \widetilde{E}(k)_{\sim p}$$

Then we define $E_{-1}(K)$ the subgroup of $E(K)$ consisting of points such that its reduction belongs to $E(k)_p$. Then for every $Q \in E_{-1}(K)$, $[p^n]Q \in E_1(K) \cong \mathcal{F}(\mathfrak{m})$ for n large enough. Then we can define a $\mathbb{Z}_p$-module structure like in corollary 9.4. To do that, given $\alpha \in \mathbb{Z}_p$ we can find some $a \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_p$ such that $\alpha = a + p^n\beta$. Hence we define

$$\alpha Q = aQ + \beta(p^n Q)$$

which is well defined because $p^n Q \in \mathcal{F}(m)$.

Since $E_{-1}(K)$ has a subgroup of finite index isomorphic to $\mathbb{Z}_p^{[K:\mathbb{Q}_p]}$, then structure theorem of finitely generated modules guarantees that there is a finite group S such that

$$E_{-1}(K) \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times S$$

Then consider the following short exact sequence:

$$0 \longrightarrow E_{-1}(K) \longrightarrow E(K) \longrightarrow \widetilde{E}(k)_{\sim p} \longrightarrow 0$$

This short exact sequence splits. In fact, $\widetilde{E}(k)$ is a finite abelian group, so the structure theorem gives an isomorphism

$$\widetilde{E}(k)_{\sim p} \cong C_1 \times \cdots \times C_r$$

where each C_i is a finite cyclic group whose order is called n_i and which are generated by some element Q_i. Notice that every n_i is prime to p because the order of $\widetilde{E}(k)_{\sim p}$ was prime to p too.

By theorem 9.2, there is some element $P_i \in E[n_i]$ such that $\widetilde{P}_i = Q_i$. Suppose by contradiction that $P_i \notin E(K)$. Then the orbit of P_i under the action of the Galois group would contain more than 1 element, so the reduction map $E[n_i] \to \widetilde{E}[n_i]$ would not be injective. Since n_i is prime to p, then the reduction map would not be either surjective, because it is a map between two finite sets having the same cardinality, which contradicts theorem 9.2.

Hence $P_i \in E(K)$ and the map

$$\widetilde{E}(k) \to E(K) : \ Q_i \mapsto P_i \ \forall i = 1, \ldots, n$$

is a splitting map. Then

$$E(K) \cong E_{-1}(K) \times \widetilde{E}(k)_{\sim p} = \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times S \times \widetilde{E}(k)_{\sim p}$$

□

We end up this section by showing how behaves the Mordell-Weil group when tensoring with $\mathbb{Q}_p/\mathbb{Z}_p$. It may seem meaningless, but it will be useful for studying the Selmer group and proving Mazur's control theorem.

Theorem 9.6. Let E be an elliptic curve defined over a finite extension K of $\mathbb{Q}_p$. Then $E(K) \otimes (\mathbb{Q}_l/\mathbb{Z}_l) = 0$, where $l \neq p$ is a prime.

Proof. By theorem 9.4, there is a finite group T and a short exact sequence

$$0 \longrightarrow \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \longrightarrow E(K) \longrightarrow T \longrightarrow 0$$

Since tensoring with $\mathbb{Q}_l/\mathbb{Z}_l$ is a right-exact functor, we have the following exact sequence

$$\mathbb{Z}_p^{[K:\mathbb{Q}_p]} \otimes \mathbb{Q}_l/\mathbb{Z}_l \longrightarrow E(K) \otimes \mathbb{Q}_l/\mathbb{Z}_l \longrightarrow T \otimes \mathbb{Q}_l/\mathbb{Z}_l \longrightarrow 0 \tag{9.1}$$

However, $\mathbb{Z}_p^{[K:\mathbb{Q}_p]} \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0$ since $\mathbb{Z}_p$ is a l-divisible group and $\mathbb{Q}_l/\mathbb{Z}_l$ is l-primary. In fact, given $a \times b \in \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \otimes \mathbb{Q}_l/\mathbb{Z}_l$, the order of b in $\mathbb{Q}_p/\mathbb{Z}_p$ is l^n for some $n \in \mathbb{N}$. Then there is some $x \in \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ such that $l^n x = a$ and

$$a \otimes b = l^n x \otimes b = x \otimes l^n b = x \otimes 0 = 0$$

Furthermore $T \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0$ too because T is finite and $\mathbb{Q}_l/\mathbb{Z}_l$ is divisible. In fact, let $n = |T|$ and let $a \in T$ and $b \in \mathbb{Q}_l/\mathbb{Z}_l$. Then there is some $x \in \mathbb{Q}_l/\mathbb{Z}_l$ such that $nx = b$ and

$$a \otimes b = a \otimes nx = na \otimes x = 0 \otimes x = x$$

Hence, by the exactness property appearing on equation 9.1, $E(K) \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0$. □

Last statement can be generalised to infinite extensions of $\mathbb{Q}_p$.

Corollary 9.5. Let E be an elliptic curve defined over an algebraic extension K of $\mathbb{Q}_p$. Then $E(K) \otimes (\mathbb{Q}_l/\mathbb{Z}_l) = 0$, where $l \neq p$ is a prime.

Proof. Since

$$E(K) = \varinjlim_{L} E(L)$$

where L runs through the finite subextensions of $K|\mathbb{Q}_p$. By proposition 4.4 and theorem 9.6,

$$E(K) \otimes \mathbb{Q}_l/\mathbb{Z}_l = \varinjlim E(L) \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0$$

□

Theorem 9.7. Let E be an elliptic curve defined ver $K = \mathbb{C}$ or $K = \mathbb{R}$. If l is a prime number, then

$$E(K) \otimes (\mathbb{Q}_l/\mathbb{Z}_l) = 0$$

Proof. If $K = \mathbb{R}$, then either $E(K) \cong \mathbb{R}/\mathbb{Z}$ or $E(K) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, because [28], corollary V.2.3.1. Otherwise, if $K = \mathbb{C}$, then $E(K) = (\mathbb{R}/\mathbb{Z})^2$ due to [27], proposition VI.3.6. In any case

$$\mathbb{R}/\mathbb{Z} \otimes \mathbb{Q}_l/\mathbb{Z}_l = \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0 \Rightarrow E(K) \otimes \mathbb{Q}_l/\mathbb{Z}_l = 0$$

□

Theorem 9.8. Let K be a finite extension of $\mathbb{Q}_p$. Then $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is cofinitely generated and has corank equal to $[K : \mathbb{Q}_p]$.

Proof. By lemma 9.5, $E(K) = \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times T$ as groups, where T is a finite group. Hence

$$E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K:\mathbb{Q}_p]}$$

□

Chapter 10

Mordell-Weil Theorem

The content of this chapter shows a proof for a central theorem in the study of the arithmetic of elliptic curves: the Mordell-Weil theorem. It states that the group $E(K)$, where K is a number field, is finitely generated. The proof is divided in two big steps.

We start proving, in section 10.1, the weak Mordell-Weil theorem, which says that the factor groups $E(K)/mE(K)$ are finite for every $m \in \mathbb{N}$. The proof procedure we have chosen is based on Galois cohomology. That is a really strong way to attack different related problems, since the strength of cohomological tools and Galois theory can be applied.

That condition does not imply a priori that a group is finitely generated, although it does for the group of rational points in an elliptic curve, as it is sketched in section 10.2. The proof uses descent theorem, which needs to define a height function on the elliptic curve.

The computation of a Mordell-Weil group can be divided in two steps: computing the torsion and computing the rank. Section 10.3 shows how to calculate the torsion in a process that requires few computational time. The situation for computing the rank is much harder and, although there is not known method to compute it in a general elliptic curve, this problem can be addressed with the content included in chapter 11.

Throughout this chapter, let K be a number field and let M_K the set of inequivalent valuations on K. Let further M_K^∞ be the subset of archimedean valuations and M_K^0 the subset of non-archimedean ones.

For every valuation v, let K_v the completion of K at v, let R_v be the ring of integers of K_v, let m_v be its maximal ideal and let k_v be its residue field.

10.1 The Weak Mordell-Weil Theorem

Our main goal in this section is to prove the weak Mordell-Weil theorem, which states that, in an elliptic curve E defined over a number field K, the factor group $E(K)/mE(K)$ is finite for every $m \geq 2$.

Theorem 10.1. (Weak Mordell-Weil theorem) Let K be a number field, let E/K be an elliptic curve defined over K and let $m \geq 2$ be an integer. Then

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

is a finite abelian group.

We will expose a prove that uses cohomological techniques. As $[m]$ is a non-constant isogeny,

it is surjective and we can consider the following short exact sequence of G_K-modules.

$$0 \longrightarrow E[m] \longrightarrow E\left(\overline{K}\right) \xrightarrow{[m]} E\left(\overline{K}\right) \longrightarrow 0$$

Since the Galois invariant points are those defined over K, the long cohomology sequence can be written as follows.

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)[m] & \longrightarrow & E(K) & \xrightarrow{[m]} & E(K) \\ & & & \overset{\delta}{\searrow} & & & \\ & & H^1(K, E[m]) & \longrightarrow & H^1(K, E) & \xrightarrow{[m]} & H^1(K, E) \end{array}$$

Here, we are denoting by $A[m]$ the m-torsion points of an abelian group A. From the middle part of this sequence, we can extract a short exact sequence, commonly known as *Kummer sequence for E/K*

$$0 \longrightarrow \tfrac{E(K)}{mE(K)} \longrightarrow H^1\left(K, E[m]\right) \longrightarrow H^1\left(K, E\right)[m] \longrightarrow 0$$

The connecting homomorphism δ given by lemma 6.3 could be described as follows. Given a point $P \in E(K)$ representative of an element in the factor group $E(K)/mE(K)$, choose an element $Q \in E\left(\overline{K}\right)$ such that $[m]Q = P$. Then, Q induces a cocycle in the cohomology group $H^1\left(K, E\right)$ given by the equation $\sigma \mapsto \sigma Q - Q$. This cocycle can be considered as a cocycle in $H^1(K, E[m])$, which will be the image of P via the connecting homomorphism.

At this point, we can make the first reduction of the proof of the weak Mordell-Weil theorem.

Lemma 10.1. Let $L|K$ be a finite Galois extension. Assume that $E(L)/mE(L)$ is finite. Then $E(K)/mE(K)$ is also finite.

Proof. On the one hand, there is a map

$$E(K)/mE(K) \to E(L)/mE(L) : \; P + mE(K) \mapsto P + mE(L)$$

which is clearly well defined. Being Φ its kernel, we can consider the following exact sequence:

$$0 \longrightarrow \Phi \longrightarrow E(K)/mE(K) \longrightarrow E(L)/mE(L)$$

On the other hand, we can consider the inflation-restriction exact sequence applied to the Galois groups

$$0 \longrightarrow H^1\left(L|K, E(L)[m]\right) \xrightarrow{\text{Inf}} H^1\left(K, E[m]\right) \xrightarrow{\text{Res}} H^1\left(L, E[m]\right)$$

The injections given in the Kummer sequence form the following commutative diagram.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Phi & \longrightarrow & E(K)/mE(K) & \longrightarrow & E(L)/mE(L) \\ & & \downarrow & \overset{\delta}{\searrow} & \downarrow \delta & & \downarrow \delta \\ 0 & \longrightarrow & H^1\left(L|K, E(L)[m]\right) & \xrightarrow{\text{Inf}} & H^1\left(K, E[m]\right) & \xrightarrow{\text{Res}} & H^1\left(L, E[m]\right) \end{array}$$

In this diagram, the map $\delta : \Phi \to H^1\left(K, E[m]\right)$ is obtained by restriction of the injection from $E(K)/mE(K)$. Since this diagram is clearly commutative, $\delta(\Phi) \subset \ker(\text{Res}) = \text{Im}(\text{Inf})$, so the δ homomorphism from Φ factors through $H^1\left(L|K, E(L)[m]\right)$. Moreover, $\delta|_\Phi$ is also injective because $\delta : \; E(K)/mE(K) \to H^1\left(K, E[m]\right)$ was.

Then, there is an injection $\Phi \hookrightarrow H^1(L|K, E[m])$. Since both $G_{L|K}$ and $E(L)[m]$ are finite, there is a finite number of 1-cocycles, so $H^1\left(G_{L|K}, E(L)[m]\right)$ is also finite. Thus, Φ is finite too.

Then, $(E(K)/mE(K))/\Phi$ is isomorphic to a subgroup of $E(L)/mE(L)$, so it has to be finite. Since Φ was finite, then $E(K)/mE(K)$ is also finite. □

In the weak Mordell-Weil theorem, we can consider the field

$$L = K(E[m])$$

formed by the composition of fields of the coordinates of the points $T \in E[m]$ over K. Since $E[m]$ is finite, then $L|K$ is finite too. Moreover, $L|K$ is Galois since G_K maps $E[m]$ to itself. Then, if we prove the weak Mordell-Weil theorem for L, it will be also true for K, so we can assume that $E[m] \subset E(K)$.

Under that assumption, G_K acts trivially on $E[m]$, so $H^1(K, E[m]) = \mathrm{Hom}(G_K, E[m])$. Hence there is an injection:

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G_K, E[m]) : P \mapsto \sigma Q - Q$$

where Q is some arbitrary element of $E\left(\overline{K}\right)$ such that $[m]Q = P$. This injection could be seen as a bilinear mapping, called *Kummer pairing*.

$$\kappa : E(K)/mE(K) \times G_K \to E[m] : (P, \sigma) \mapsto \sigma Q - Q$$

Lemma 10.2. When considering the Kummer pairing as an homomorphism

$$\psi : G_K \to \mathrm{Hom}\left(\frac{E(K)}{mE(K)}, E[m]\right),$$

its kernel is G_L, where $L = K([m]^{-1}E(K))$ is the composition of all fields $K(Q)$, the minimum field that contains K and the point Q is defined over $K(Q)$, as Q ranges over the points in $E\left(\overline{K}\right)$ satisfying that $[m]Q \in E(K)$.

Proof. Given $\sigma \in G_L$, then $\kappa(P+mE(K), \sigma) = \sigma Q - Q$, where Q is a point such that $[m]Q = P$. Since $Q \in E(L)$ by definition, then $\sigma Q = Q$, so $\psi(\sigma)$ maps every point $P \in E(K)$ to O.

Conversely, if $\sigma \in G_K$ satisfies that $\kappa(P + mE(K), \sigma) = O \ \forall P \in E(K)$, then every point $Q \in [m]^{-1}E(K)$ satisfies that $\sigma Q = Q$. Since L is the composition of $K(Q)$ over all $Q \in [m]^{-1}E(K)$, then σ fixes L, so $\sigma \in G_L$. □

Going backwards through this process, we can substitute G_K by $G_{L|K}$ in the Kummer pairing. Therefore, the injection stated above can be written as

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G_{L|K}, E[m]) : (P, \sigma) \mapsto \sigma Q - Q \tag{10.1}$$

Corollary 10.1. Let $L = K([m]^{-1}E(K))$. Then $L|K$ is an abelian extension of exponent dividing m.

Proof. $L|K$ is a Galois extension since G_K maps $[m]^{-1}E(K)$ to itself, because the Galois group fixes $E(K)$ and commutes with the group operation defined on the elliptic curve. Since $G_{L|K} = G_K/G_L$, lemma 10.2 gives an injection

$$G_{L|K} \hookrightarrow \mathrm{Hom}(E(K)/mE(K), E[m])$$

Then, $G_{L|K}$ is isomorphic to a subgroup of $\mathrm{Hom}(E(K)/mE(K), E[m])$. The latter is abelian and has exponent dividing m because these properties are inherited from $E[m]$. Therefore, $G_{L|K}$ is abelian and has exponent dividing m. □

Proposition 10.1. Let $L = K\left([m]^{-1}E(K)\right)$ and let

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

Then $L|K$ is unramified outside S, i.e., it is unramified for every valuation $v \in M_K$ such that $v \notin S$.

Proof. Let $v \in M_K \setminus S$, let $Q \in E\left(\overline{K}\right)$ be such that $[m]Q \in E(K)$ and let $K' = K(Q)$. Let v' be a place of K' that extends v. Since E has good reduction at v, reduction at v' is the same as reduction at v and $k_v \subset k'_{v'}$, non-singularity of $\widetilde{E}(k_v)$ implies non-singularity of $\widetilde{E}(k'_{v'})$. Hence $E_0(K') = E(K')$.

Let $I_{v'|v} \subset G_{K'|K}$ be the inertia group, i.e., the subgroup of Galois automorphisms that acts trivially on $k'_{v'}$. For every $\sigma \in I_{v'|v}$, corollary 9.1 implies that

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

However, the fact that $[m]Q \in E(K)$ implies that

$$[m](\sigma Q - Q) = \sigma([m]Q) - [m]Q = O$$

Hence $\sigma Q - Q$ is an m-torsion point which is in the kernel of the reduction map modulo v'. Since $v \notin S$, then $v(m) = 0$, so m is prime to $\mathrm{char}(k_v) = \mathrm{char}(k'_{v'})$ and proposition 9.5 implies that $\sigma Q = Q$.

Thus $I_{v'|v}$ fixes $K(Q)$, so $K(Q)|K$ is unramified at v. Since L is the composition of every $K(Q)$, as Q varies over $[m]^{-1}E(K)$, then L is unramified at v by [21], corollary II.7.3. □

Remark 10.1. In last proposition, the set of valuations $S \subset M_K$ is finite because, given a Weierstrass equation, E has good reduction at every valuation v such that $v(\Delta) = 0$ and $v(a_i) \geq 0\ \forall i = 1, 2, 3, 4, 6$.

Proposition 10.2. Let K be a number field, let $S \subset M_K$ be a finite set of valuations that contains M_K^∞ and let $m \geq 2$ be an integer. Let $L|K$ be the maximal abelian extension of K having exponent dividing m and unramified outside S. Then $L|K$ is a finite extension.

Proof. First, if the proposition is true for some finite extension K' of K, it has to be also true for K. In fact, the set S' of valuations lying above S is finite too and $LK'|K'$ is an abelian extension of exponent dividing m, because $G_{LK'|K'}$ is isomorphic by restriction to a subgroup of $G_{L|K}$, and it is unramified outside S' ([21], proposition II.7.2.). Then, $LK'|K'$ would be finite, so $L|K$ would be finite too. Thus we can assume without loss of generality that K contains the primitive m^{th} roots of unity μ_m.

Let $L|K$ be an extension satisfying all the hypothesis of the proposition and let R be the ring of integers of K. Let also $a_1, \ldots, a_h$ be representatives of the class group of K and $v_1, \ldots, v_h$ be their associated valuations. Define $\widetilde{S} := S \cup \{v_1, \ldots, v_h\}$ and the ring of $\widetilde{S}$-integers

$$R_{\widetilde{S}} = \left\{a \in K : v(a) \geq 0\ \forall v \in M_K \setminus \widetilde{S}\right\}$$

Since $R = \{a \in K : v(a) \geq 0\ \forall v \in M_K\}$ ([5], Theorem 10.3.1.) and there is a bijection between M_K^0 and $\mathrm{Spec}(R)$, considering $R_{\widetilde{S}}$ is the same as localising in the multiplicative set

$$Q = \bigcap_{p \in \mathrm{Spec}(R) \setminus \widetilde{S}} p^c$$

where, in an abuse of notation, we are identifying the valuations in $\widetilde{S}$ with their associate prime ideals. In both $R_{\widetilde{S}}$ and in $Q^{-1}R$, we are allowing denominators not belonging to any prime

ideal in $\mathrm{Spec}(R) \setminus \widetilde{S}$, i.e., elements which generate an ideal whose prime factorisation contains only elements of $\widetilde{S}$.

$R_{\widetilde{S}}$ is a principal ideal domain because, given an ideal b of $R_{\widetilde{S}}$, then $b \cap R$ is an ideal in R. Then, there is a representative of the class group a_i and some element $c \in K$ such that $b \cap R = c \cdot a_i$. Since every ideal in a localization is an extended ideal, $b = (b \cap R)R_{\widetilde{S}} = ca_i R_{\widetilde{S}} = cR_{\widetilde{S}}$ since the extended ideal of a_i is $R_{\widetilde{S}}$ because of proposition 2.11.

By corollary 5.1, L is the maximal subextension of $K(\sqrt[m]{a} : a \in K)$ unramified outside $\widetilde{S}$. Given some $a \in K$, if $K(\sqrt[m]{a})|K$ is unramified outside $\widetilde{S}$, then for every $v \in M_K \setminus \widetilde{S}$ and every $\widetilde{v} \in M_{K(\sqrt[m]{a})}$ lying above v, we get

$$\widetilde{v}(\sqrt[m]{a}) \in \mathbb{Z} \Rightarrow v(a) \in m\mathbb{Z}$$

When adjoining m^{th} roots to construct the maximal m-Kummer extension, we just need to consider one representative of each class of $K^*/(K^*)^m$, so we define the set

$$T_{\widetilde{S}} = \left\{ a \in K^*/(K^*)^m : v(a) \in m\mathbb{Z}\ \forall v \in M_K \setminus \widetilde{S} \right\} \quad [1]$$

Then, it is clear that

$$L \subset K\left(\sqrt[m]{a} : a \in T_S\right)$$

so $L|K$ would be finite provided that T_S is also finite.

Now consider the map

$$\psi : R^*_{\widetilde{S}}/\left(R^*_{\widetilde{S}}\right)^m \to T_{\widetilde{S}} :\ a\left(R^*_{\widetilde{S}}\right)^m \mapsto a\,(K^*)^m$$

which is clearly well defined since $v(a) = 0\ \forall a \in R^m_{\widetilde{S}}\ \forall v \in M_K \setminus S$. Furthermore, it is surjective. In fact, given $a \in K^*$, since $R_{\widetilde{S}}$ is a principal ideal domain, there is some $b \in K$ such that

$$aR_{\widetilde{S}} = \left(\prod_{p \in M_K \setminus \widetilde{S}} p^{v_p(a)/m}\right)^m = (bR_{\widetilde{S}})^m = b^m R_{\widetilde{S}}$$

Hence there is some $u \in R^*_{\widetilde{S}}$ such that $a = ub^m$, so $\psi(u) = a\,(K^*)^m$.

By corollary 2.7, $R_{\widetilde{S}}$ is a finitely generated group, so $R^*_{\widetilde{S}}/\left(R^*_{\widetilde{S}}\right)^m$ is finite. Since ψ is surjective, $T_{\widetilde{S}}$ is finite too. By what was commented above, $L|K$ is a finite extension. □

We can now complete the proof of theorem 10.1. Let $L = K\left([m]^{-1}E(K)\right)$. By corollary 10.1 and proposition 10.1, $L|K$ in an abelian extension of exponent dividing m which is unramified outside a certain finite set of valuations S, that contains M_K^∞, so it has to be contained in the maximal abelian extension of K having exponent dividing m and unramified outside S, which is finite by 10.2. Then, $L|K$ has to be finite too.

Since $E[m]$ is finite, then $\mathrm{Hom}(G_{L|K}, E[m])$ is a finite group too. Then, injection given in equation 10.1 implies that $E(K)/mE(K)$ is also finite.

10.2 The Mordell-Weil Theorem

This section is dedicated to sketch a proof for the Mordell-Weil theorem.

Theorem 10.2. (Mordell-Weil) Let E be an elliptic curve defined over a number field K. Then the group $E(K)$ is finitely generated.

[1] Note that the condition does not depend on the representative chosen because $v(a) \in m\mathbb{Z}\ \forall a \in (K^*)^m$, $\forall v \in M_K$.

The weak Mordell-Weil theorem states that the quotients $E(K)/mE(K)$ are finite. However, this condition is not enough to guarantee that an abelian group is finitely generated, being the additive group of $\mathbb{Q}$ a counter-example. To conclude that for the Mordell-Weil group, we need to use the theory of height functions.

Theorem 10.3. Let A be an abelian group. Suppose that there exists a height function

$$h : A \to \mathbb{R}$$

with the following properties:

1. For every $Q \in A$, there is a constant C_Q such that

$$h(P+Q) \leq 2h(P) + C_Q \ \forall P \in A$$

2. There are an integer $m \geq 2$ and a constant C_m such that

$$h(mP) \geq m^2 h(P) - C_m$$

3. For every constant D, the set

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

is finite.

If further the factor group A/mA is finite, then A/mA is finitely generated.

Proof. Let $\mathcal{R} = \{Q_1, \ldots, Q_r\}$ be a system of representatives of A/mA and let $P \in A$ be an arbitrary element. Define inductively $P_0 := P$ and S_{i+1} be the representative of $P_i + mA$ in $\mathcal{R}$. Hence we can define P_{i+1} as a solution of the equation

$$P_i = mP_{i+1} + S_{i+1}$$

For each $i \in \mathbb{N}$ we have that

$$h(P_i) \leq \frac{1}{m^2}\left(h(mP_{i-1}) + C_m\right) = \frac{1}{m^2}\left(h(P_{i-1} - S_{i+1}) + C_m\right) \leq \frac{1}{m^2}\left(2h(P_{i-1}) + C + C_m\right)$$

where $C := \max\{C_{-Q_1}, \ldots, C_{-Q_r}\}$. Using this inequality repeatedly,

$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \cdots \frac{2^{n-1}}{m^{2n}}\right)(C + C_m) < \left(\frac{2}{m^2}\right)^n h(P) + \frac{C + C_m}{m^2 - 2} \leq \frac{1}{2^n} h(P) + \frac{1}{2}(C + C_m)$$

If n is large enough, then $h(P_n) \leq 1 + \frac{1}{2}(C + C_m)$. Since

$$P = m^n P_n + \sum_{j=0}^{n-1} m^j S_{j+1}$$

and P was an arbitrary point, then A is generated by the finite set

$$\mathcal{R} \cup \left\{Q \in A : h(Q) \leq 1 + \frac{1}{2}(C + C_m)\right\}$$

□

In order to define a height function on the Mordell-Weil group $E(K)$, we start by defining it in the projective space $\mathbb{P}^n(K)$.

Definition 10.1. Let K be a number field and let $P = (x_0 : \cdots x_n) \in\in \mathbb{P}^n K$. Then the *height of P relative to K* is

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

where M_K is the set of inequivalent normalised valuations in K.

Proposition 10.3. Let $P \in \mathbb{P}^n K$. The height $H_K(P)$ does not depend on the choice of the homogeneous coordinates for P.

Proof. By [21], proposition III.1.3, we have the following identity

$$\prod_{v \in M_K} |\lambda|_v = 1$$

Hence,

$$\prod_{v \in M_K} \max\{|\lambda x_0|_v, \ldots, |\lambda x_n|_v\} = \prod_{v \in M_K} |\lambda|_v \max\{|x_0|_v, \ldots, |x_n|_v\} = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}$$

□

Proposition 10.4. Let K be a number field and let $L|K$ be a finite extension. Then for every $P \in \mathbb{P}^n K$, we have

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

Proof. From [21], proposition II.8.4, we have that

$$[L : K] = \sum_{w \in M_L, w|v} [L_w : K_v]$$

Hence

$$H_L(P) = \prod_{w \in M_L} \max\{|x_0|_w, \ldots, |x_n|_w\} = \prod_{v \in M_K} \prod_{w \in M_L, w|v} \max\{|x_0|_w, \ldots, |x_n|_w\} = \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_n|_v\}^{[L:K]} = H_K(P)^{[L:K]}$$

□

Last proposition gives us the possibility of extending the definition of our height function to the algebraic closure $\overline{\mathbb{Q}}$.

Definition 10.2. Let $P \in \mathbb{P}^n\left(\overline{\mathbb{Q}}\right)$. The *absolute height* of P is

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

where we take the positive root and where K is any number field over which P is defined.

Definition 10.3. Let E/K be an elliptic curve and let $f \in \overline{K}(E)$ be a rational function. The *height of E relative to f* is the function

$$h_f : E\left(\overline{K}\right) \to \mathbb{R} : \ P \mapsto \log(H(f(P)))$$

The fact that h_f satisfies the hypothesis of theorem 10.3 when $f \in K(E)$ is an even rational function, i.e., $f \circ [-1] = f$, is proven in [27], theorem VIII. 6.7. Hence the rational function $f(P) = x(P)$ can be used to proof Mordell-Weil theorem 10.2.

Remark 10.2. It is also important to analyse whether the Mordell-Weil theorem is effective. The main difficulty would be finding the generators of $E(K)/mE(K)$, which will be commented in next chapter.

Once we know them, the constants and the finite set of theorem 10.3 are effectively computable. Assuming we can now a system of generators of $E(K)/mE(K)$, the proof of theorem 10.3 provides a method for computing the generators of the Mordell-Weil group. Unfortunately, up to now there is any known general method for computing $E(K)/mE(K)$, although it can be done in some particular cases.

10.3 The Torsion Subgroup

Given an elliptic curve E/K, the torsion subgroup $E(K)_{\text{tors}}$ is easyly computable. First, theorem 9.1 can be restated as follows.

Theorem 10.4. Let E be an elliptic curve defined over a number field K whose Weierstrass equation is

$$y^2 + a_1xy + a3y = x^3 + a_2x^2 + a_4x + a_6$$

where a_1, a_2, a_3, a_4, a_6 are in the ring of integers R of K. Let $P \in E(K)$ be a torsion point of exact order $m \geq 2$.

1. If m is not a prime power, then $x(P), y(P) \in R$.
2. If $m = p^n$ is a prime power, then for each $v \in M_K^0$, defining

$$r_v := \left\lfloor \frac{v(P)}{p^n - p^{n-1}} \right\rfloor$$

Then,

$$v(x(P)) \geq -2r_v, \qquad v(y(P)) \geq -3r_v$$

This theorem has a corollary, which was proven independently by Lutz and Nagell, which reduces the calculation of the torsion of an elliptic curve over $\mathbb{Q}$ to a finite amount of computations.

Corollary 10.2. Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation

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

where $A, B \in \mathbb{Z}$. If $P \in E(\mathbb{Q})$ is a non-trivial torsion point whose order is m, then

1. $x(P), y(P) \in \mathbb{Z}$.
2. Either $[2]P = O$ or else $y(P)^2$ divides $4A^3 + 27B^2$.

Proof. If $m = 2$, then $y(P) = 0$ and hence $X(P)$ is the root of a monic polynomial with integer coefficients, so it is an integer. If $m > 2$, all the quantities r_v vanish, so $x(P)$ and $y(P)$ are integers.

For the second part, if $P \notin E[2]$, then $x(P)$, $y(P)$ and $x([2]P)$ are integers. Defining the polynomials

$$\phi(X) = X^4 + 2AX^2 - 8Bx + A^2, \quad \psi(X) = X^3 + AX + B$$

the duplication formula computed in [27] reads

$$x([2]P) = \frac{\phi(x(P))}{4\psi(x(P))}$$

Taking into account that $y(P)^2 = \psi(x(P))$, a computation shown in [27], corollary VIII.7.2 implies that

$$y(P)^2 \left(\left(12x(P)^2 + 16A\right) x([2](P)) - 3x(P)^3 - 5Ax(P) - 27B\right) = 4A^3 + 27B^2$$

□

Remark 10.3. Corollary 10.2 reduces to a finite number of candidates to be torsion elements of $E(\mathbb{Q})_{\text{tors}}$. Moreover, its possible orders can also be bounded by proposition 9.5. Hence $E(\mathbb{Q})_{\text{tors}}$ can be computed in finite time.

Moreover, there is a deeper result, whose proof is unfortunately out of the scope of this work, which reduces the possible torsion subgroups to one of the following fifteen possibilities.

Theorem 10.5. (Mazur) Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following fifteen groups

$$\mathbb{Z}/N\mathbb{Z}, \text{ with } 1 \leq N \leq 10 \text{ or } N = 12; \quad \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \text{ with } 1 \leq N \leq 4.$$

Proof. See [18]. □

We end this section by showing two examples of the computation of the torsion subgroup $E(\mathbb{Q})_{tors}$.

Example 10.1. Let $E/\mathbb{Q}$ be the elliptic curve defined by the Weierstrass equation

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

The discriminant of this curve is $\Delta = -64$. It can be easily computed that

$$\#\widetilde{E}(\mathbb{F}_3) = 4, \quad \#\widetilde{E}(\mathbb{F}_5) = 4, \quad \#\widetilde{E}(\mathbb{F}_7) = 4$$

Let $q \in \mathbb{Z}$ be a prime number greater than 2. By proposition 9.5, there is an injection

$$\pi : E(\mathbb{Q})[q] \hookrightarrow \mathbb{E}(\mathbb{F}_p)$$

where p is a prime different from 2 and q. In particular we can consider some $p \in \{3, 5, 7\}$, so $E(\mathbb{Q})[q]$ can be injected in a group of 4 elements. Since every non-trivial element in $E(\mathbb{Q})[q]$ has order q, then $E(\mathbb{Q})[q] = \{O\}$ $\forall q \geq 3$.

For $q = 2$, observe that

$$\widetilde{E}(\mathbb{F}_3) = \{O, (0,0), (2,1), (2,2)\} \cong \mathbb{Z}/4\mathbb{Z}$$
$$\widetilde{E}(\mathbb{F}_5) = \{O, (0,0), (2,0), (2,0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

Then for every $n \in \mathbb{N}$, there is are injections

$$E(\mathbb{Q})[2^n] \hookrightarrow \widetilde{E}(\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}, \quad E(\mathbb{Q})[2^n] \hookrightarrow \widetilde{E}(\mathbb{F}_5) \cong (\mathbb{Z}/2\mathbb{Z})^2$$

Then, it has to be an injection $E(\mathbb{Q})[2^n] \hookrightarrow \mathbb{Z}/2\mathbb{Z}$.

Hence it can be only one non-trivial torsion element, which is $(0, 0)$. Thus

$$E(\mathbb{Q})_{tors} = \{O, (0,0)\}$$

Example 10.2. (Mordell Curves) Let E be the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation

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

where $D \in \mathbb{Z}$. We can assume without loss of generality that D is sixth power free since otherwise we could make a change of coordinates in order to reduce the problem to that case.

Consider a prime number $p \in \mathbb{N}$ such that $p \equiv 2 \mod 3$ and such that E has a good reduction when considered as a curve defined over $\mathbb{Q}_p$. It is possible to find that prime because, given a Weierstrass equation with integer coefficients, $\Delta \notin p\mathbb{Z}$ for every prime but a finite amount of them and $E/\mathbb{Q}_p$ has good reduction for any of those primes at which $p \not| \Delta$.

The reduced curve $\widetilde{E}(\mathbb{F}_p)$ has $p+1$ points. In fact, since $\#(\mathbb{F}_p^*) \notin 3\mathbb{Z}$, the homomorphism $x \mapsto x^3$ is injective in the group of units, so it has to be an isomorphism. It can be extended to $0 \mapsto 0$ and thus the map

$$\mathbb{F}_p \to \mathbb{F}_p : \ x \mapsto x^3 + D$$

is a bijection. Then given some $y \in \mathbb{F}_p$ there is a unique $x \in \mathbb{F}_p$ such that $y^2 = x^3 + D$. Counting the point at infinity, $\widetilde{E}(\mathbb{F}_p)$ has exactly $p+1$ points.

Let $q \geq 5$ be another prime number. Since E has a good reduction at almost every prime number, it is posible to find, because of Dirichlet's theorem, a prime number $p \in 3\mathbb{Z}+2$ such that E has a good reduction at p and that $q \not| p+1$. By proposition 9.5, there is an injection

$$E(\mathbb{Q})[q] \to \widetilde{E}(\mathbb{F}_p)$$

In case that $E(\mathbb{Q})[q]$ is not the trivial group, it has by Lagrange's theorem an order which is a multiple of q, so it cannot be injected in a group of $p-1$ elements. Hence $E(\mathbb{Q})[q] = \{O\}$.

For $q = 3$ we can find a prime number p such that E has good reduction at p and that $p \equiv 2 \mod 9$. If we consider the injection $E(\mathbb{Q})[3] \hookrightarrow E(\mathbb{F}_p)$ and the fact that the latter has $p+1$ elements, we see that $E(\mathbb{Q})[3]$ has order at most 3. For $q = 2$, we can deduce that $E(\mathbb{Q})[2]$ has order 1 or 2 by looking for a prime $p \equiv 5 \mod 12$ at which E has good reduction.

Hence $E(\mathbb{Q})_{\text{tors}}$ is an abelian group of at most 6 elements, so it is isomorphic to one of the following.

$$E(\mathbb{Q})_{\text{tors}} = \{O\}, \quad E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}, \quad E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z}, \quad E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z}$$

For each value of D we want to see to which group is isomorphic $E(\mathbb{Q})_{\text{tors}}$. For that purpose we just need to see whether E has torsion points of order 2 and 3.

E has 2-torsion if and only if the equation $0 = x^3 + D$ has a solution in $\mathbb{Q}$ and this is equivalent to D being a cube. The fact that $E(\mathbb{Q})$ has a non-trivial 3-torsion group is equivalent to the existence of some $P \in E(\mathbb{Q})$ such that its tangent line intersects the curve at P with multiplicity 3. This happens if and only if one of the following identities is satisfied.

$$x(P) = 0, \quad 3x(P)^3 = 4y(P)^2$$

The first happens if and only if D is a square and the latter is equivalent to the following equations have rational solutions.

$$x^3(P) = 4D, \quad y^2(P) = -3D$$

This happens if and only if $D = -432n^6$, where $n \in \mathbb{Z}$. In conclusion

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/6\mathbb{Z}, & \text{if } D = 1 \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } D \neq 1 \text{ is a square.} \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } D = -432. \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } D \neq 1 \text{ is a cube.} \\ \{O\}, & \text{otherwise.} \end{cases}$$

Chapter 11

Mazur's Control Theorem

In chapter 10, we have proved that the group $E(K)$ is finitely generated and we have showed a method for computing the torsion. Moreover, there were another method for computing the rank of this group assuming we knew a system of generators of the group $E(K)/mE(K)$. A method for finding this generators is based on the Selmer groups defined in 11.1. However, the reader should be warned that it is difficult to compute this method in particular cases. This section also generalises the weak Mordell-Weil theorem to prove that the cokernel of an arbitrary isogeny defined over K in the group of rational points is finite.

In section 11.2, we give another definition of the Selmer group which also bounds the rank of Mordell-Weil group. Moreover, it is conjectured that this bound is exactly the rank. The study of this object will be the content of Mazur's Control theorem, in section 11.4. This result has interesting consequences, which are exposed in section 11.5. Among them, we highlight the control of the growth of the rank of the Mordell-Weil group in a $\mathbb{Z}_p$-extension.

11.1 Selmer Groups for Isogenies

In this section we are going to introduce the Selmer group for an isogeny between elliptic curves and the Tate-Shafarevich group. These concepts will generalise the weak Mordell-Weil theorem to arbitrary isogenies. It is important to notice we are going to define this objects in an abstract way, although we will be interested mainly in the case when K is a number field. The reason why we do that is because this objects will sometimes appear when studying the rational points defined over an infinite algebraic extension of $\mathbb{Q}$.

Throughout this section, let K be a perfect field. Let also E and E' be two elliptic curves defined over K and let $\phi: E \to E'$ be a non-zero isogeny defined over K. Since ϕ is surjective when considering the curves in the algebraic closure $\overline{K}$, we can consider the following short exact sequence of G_K-modules:

$$0 \longrightarrow E[\phi] \longrightarrow E \longrightarrow E' \longrightarrow 0$$

where $E[\phi]$ denotes the kernel of the isogeny ϕ.

It induces a long cohomological exact sequence:

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \longrightarrow H^1(K, E) \xrightarrow{\phi} H^1(K, E')$$

From this long exact sequence, we can obtain a short exact sequence, which is analogue to the Kummer sequence appearing in the proof of the weak Mordell-Weil theorem:

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(K, E[\phi]) \longrightarrow H^1(K, E)[\phi] \longrightarrow 0$$

where $H^1(K, E)[\phi]$ denotes the kernel of the map induced by the isogeny ϕ in the cohomology groups.

Let v be a valuation in K. Then the Kummer sequences for K and K_v can be adjoined in the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & H^1(K_v, E[\phi]) & \longrightarrow & H^1(K_v, E)[\phi] & \longrightarrow & 0 \end{array}$$

In this diagram, the first vertical arrow is induced by inclusion $E'(K) \subset E'(K_v)$, which factors through the quotient groups since $\phi(E(K)) \subset \phi(E(K_v))$, and the other two vertical arrows are defined as cohomological restrictions by identifying G_{K_v} as a fixed decomposition subgroup of G_K, because of corollary 5.3.

In order to show that this diagram is commutative, it is worthy to see how the Kummer map δ is defined. Let $P \in E'(K)$. Since ϕ is surjective, there is some $Q \in E$ such that $\phi(Q) = P$. Then the 1-coboundary

$$\psi : \ G_K \to E : \ \sigma \mapsto \sigma Q - Q$$

takes only values in $E[\phi]$. In fact, since ϕ is defined over K,

$$\phi(\sigma Q - Q) = \phi(\sigma Q) - \phi(Q) = \sigma(\phi(Q)) - \phi(Q) = \sigma P - P = O$$

As a cochain in $C^1(K, E)$, ψ is not a coboundary anymore, since Q does not necessarily belongs to $E[\phi]$, but it is still a cocycle, so it represents an element in $H^1(K, E)$. Hence tracing through the definitions the commutativity of the previous diagram is clear.

In the last row we can consider different valuations and we can also consider the direct product of some of them, since the exactness and the commutative property of the diagram remain true. In particular, we will consider the direct product over all the set of inequivalent valuations in K, which will be denoted by M_K. In that case, the commutative diagram can be written as follows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \displaystyle\prod_{v \in M_K} E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \displaystyle\prod_{v \in M_K} H^1(K_v, E[\phi]) & \longrightarrow & \displaystyle\prod_{v \in M_K} H^1(K_v, E)[\phi] & \longrightarrow & 0 \end{array} \tag{11.1}$$

Now we can define the Selmer group for the isogeny ϕ and the Tate-Shafarevich group.

Definition 11.1. Let E/K and E'/K be two elliptic curves and let $\phi : \ E \to E'$ be a non-zero isogeny defined over K. The ϕ-Selmer group of E/K is the kernel of the following diagonal map appearing in the diagram in equation 11.1:

$$S^{\phi}(E/K) := \ker \left\{ H^1(K, E[\phi]) \to \prod_{v \in M_k} H^1(K_v, E)[\phi] \right\}$$

Definition 11.2. Given an elliptic curve E/K, the *Tate-Shafarevich group* is defined as

$$Ш_E(K) := \ker\left\{\text{Res}:\ H^1(K,E) \to \prod_{v\in M_K} H^1(K_v,E)\right\}$$

Remark 11.1. The definition of Selmer and Tate-Shafarevich groups are independent of the inclusion $\overline{K} \hookrightarrow \overline{K}_v$ chosen, since a different one will give a conjugate subgroup $G_{K_v} = (G_K)_v \subset G_K$. However, proposition 6.5 states that conjugation induces the identity map in the cohomology groups, so the kernels $\text{Sel}_E(K)$ and $Ш_E(K)$ are independent of the chosen valuation.

Selmer and Tate-Shafarevich groups can be encapsulated in a short exact sequence with the cokernel of $\phi:\ E(K) \to E'(K)$.

Theorem 11.1. Let E/K and E'/K be two elliptic curves and let $\phi : E \to E'$ be an isogeny defined over a number field K. Then there is an exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} S^\phi(E/K) \xrightarrow{i} Ш_E(K)[\phi] \longrightarrow 0$$

where $Ш_E(K)[\phi]$ denotes the elements of the Tate-Shafarevich group which belong to the kernel of the induced map $\phi : H^1(K,E) \to H^1(K,E')$.

Proof. It is clear from the commutativity of the diagram in equation 11.3 that this maps are well defined, and the first one is clearly injective, so the sequence is exact at $E'(K)/\phi(E(K))$.

It is also clear that $i \circ \delta = 0$ because the maps in the original diagram satisfied that relation. Furthermore, $\ker(i) \subset \text{Im}(\delta)$ because the first row in the previous diagram was exact, so this sequence is also exact at $S^\phi(E/K)$.

Finally, given some $y \in Ш_E(K)[\phi]$, the exactness of the original diagram implies that there is some $x \in H^1(K, E[\phi])$ which can be identified with y as a cocycle in $H^1(K,E)$. However, commutativity property of the diagram and the definition of Tate-Shafarevich group imply that x is in the kernel of the diagonal map, so $x \in S^\phi(E/K)$. Hence, i is surjective and this sequence is also exact at $Ш_E(K)[\phi]$. □

There is an analogue result to the weak Mordell-Weil theorem which states the finiteness of the Selmer group providing K is a number field. The procedure of the proof will be the same, since we will first proof that the elements of a cohomology group which are unramified outside certain set of valuations is finite and then will proof that the Selmer group is contained in that unramified part of the cohomology group.

Lemma 11.1. Let K be a number field, let M be a finite abelian G_K-module and let $S \subset M_K$ be a finite set of places containing M_K^∞. Then

$$H^1(K,M;S) := \left\{\xi \in H^1(K,M):\ \xi \text{ is unramified outside } S\right\}$$

is finite.

Proof. Since the action of G_K in M is continuous, for every $m \in M$ there is an open subgroup that fixes M. Since M is finite, the intersection of all of these stabilizers is also an open subgroup, which is identified by infinite Galois theory with the absolute Galois group G_L of a finite extension $L|K$. Now inflation-restriction sequence appearing in theorem 6.1 gives an exact sequence as follows:

$$0 \longrightarrow H^1(L|K,M) \xrightarrow{\text{Inf}} H^1(K,M) \xrightarrow{\text{Res}} H^1(L,M)$$

Since $G_{L|K}$ and M are both finite and 1-cocycles of $L|K$ with values in M can be identified with functions $G_{L|K} \to M$ satisfying certain condition, then $H^1(L,K)$ is finite.

It is clear that restriction map sends cocycles unramified at certain valuation to cocycles unramified at every valuation dividing v. Hence

$$\mathrm{Res}\left(H^1(K,M;S)\right) \subset H^1\left(L,M;\widetilde{S}\right)$$

where $\widetilde{S}$ is the finite set of valuations in L lying over a valuation in S. Since the action of G_L on M is trivial,

$$H^1(L,M;S) = \mathrm{Hom}(G_L,M;S)$$

Let m be the exponent of M and let F be the maximal abelian extension of L having exponent dividing m and unramified outside S, which is finite by proposition 10.2. Calling $\pi : G_L \to G_{F|L}$ to the canonical projection, there is a natural map

$$\psi : \mathrm{Hom}(G_{F|L},M;S) \hookrightarrow \mathrm{Hom}(G_L,M;S),\ \phi \mapsto \phi \circ \pi$$

Moreover, ψ is also surjective because every homomorphism from G_L to M has to vanish in the conmutator of G_L, since M is abelian, and has to factor through a quotient of G_L having exponent dividing m. Taking that into account and noticing we are only considering homomorphisms vanishing on the invertia groups I_v for every valuation outside S, then factors through $G_{F|L}$. Hence ψ is an isomorphism and, since $F|L$ is finite, the proof is complete. □

Theorem 11.2. Let K be a number field and let E/K and E'/K be two elliptic curves and let $\phi : E \to E'$ be an isogeny defined over a number field K. The Selmer group $S^\phi(E/K)$ is finite.

Proof. Let $\xi \in S^\phi(E/K)$ and let $v \in M_K$ be a finite place of K such that $v(\deg(\phi)) = 0$ and such that E/K has good reduction at v. We are going to see that ξ is unramified at v.

Let $I_v \subset G_v$ be the inertia group of some extension of v to the algebraic closure. By definition, ξ is a coboundary when restricted to a cocycle in $H^1(K_v,E)$, so there is a point $P \in E\left(\overline{K_v}\right)$ such that

$$\xi_\sigma = \sigma P - P\ \forall \sigma \in G_v$$

Notice that $\sigma P - P$ has to be contained in $E[\phi]$ because ξ represents a cocycle in $H^1(K,E[\phi])$.

However, I_v acts trivially on the reduced curve $\widetilde{E}_v$, so

$$\widetilde{\sigma P - P} = \sigma\widetilde{P} - \widetilde{P} = \widetilde{O}\ \forall \sigma \in I_v$$

Then $\sigma P - P$ is in the kernel of the reduction map. However, it is also contained in $E[\phi]$ and the equation $[m] = \widehat{\phi} \circ \phi$ implies that $E[\phi] \subset E[m]$. Then $\xi_\sigma \in E[m]$, but we know from proposition 9.5 that $E(K)[m]$ injects into $\widetilde{E}_v$, so

$$\xi_\sigma = \sigma P - P = O\ \forall \sigma \in I_v$$

Hence $S^\phi(E/K)$ is unramified outside a finite set of places S, consisting of the archimedean ones, those at which E/K has bad reduction and those such that $v(\deg\phi) \neq 0$. The finiteness of the Selmer group comes thus from lemma 11.1. □

Last theorem implies that the weak Mordell-Weil theorem can be applied to arbitrary isogenies.

Corollary 11.1. Let K be a number field, let E/K and E'/K be two elliptic curves and let $\phi : E \to E'$ be an isogeny defined over K. Then the factor group

$$E'(K)/\phi(E(K))$$

is finite.

Proof. By theorem 11.1, $E'(K)/\phi(E(K))$ injects into $\mathrm{Sel}_E(K)$, which is finite by theorem 11.2. □

Remark 11.2. Corollary 11.1 applied to the isogeny $[m]$ proves the weak Mordell-Weil theorem.

11.2 The Selmer Group

In last section, we have introduced Selmer and Tate-Shafarevich groups. While Tate-Shafarevich group did not depend on the isogeny ϕ chosen for doing that construction, Selmer group did. In this section, we want to construct a Selmer group whose definition depends only on the elliptic curve E and the number field K over which it is defined. As we will see later, it is not a new object but it is a way of grouping the Selmer groups defined in the previous section for the isogenies $[m]$, when m runs through the natural numbers.

For that purpose, given an elliptic curve defined over a perfect field K, we can generalise the Kummer sequence used to prove the weak Mordell-Weil theorem in the following sense. Consider the Kummer homomorphism

$$\kappa : E(K) \otimes \mathbb{Q}/\mathbb{Z} \to H^1\left(K, E\left(\overline{K}\right)_{\mathrm{tors}}\right)$$

defined as follows. Given $P \otimes \frac{m}{n} \in E(K) \otimes \mathbb{Q}/\mathbb{Z}$, where $m, n \in \mathbb{Z}$, we choose some $Q \in E\left(\overline{K}\right)$ such that $[n]Q = [m]P$, which exists because the isogeny $[n]$ is surjective when defined over $E\left(\overline{K}\right)$. Then we define

$$\kappa\left(P \otimes \frac{m}{n}\right)(\sigma) := \sigma Q - Q \ \forall \sigma \in G_{\overline{K}|K}$$

It is well defined since it does not depend on the chosen Q. In fact, if we had chosen a different point Q', then $Q - Q'$ would be a torsion point and the result would differ in a coboundary. It does not depend either on the representative of the equivalence class in $\mathbb{Q}/\mathbb{Z}$ chosen, since in case we take an integer the chosen Q would be defined over K and it will induce the null cocycle. Moreover, the images are cocycles since

$$\kappa\left(P \otimes \frac{m}{n}\right)(\sigma\tau) = \sigma\tau Q - Q = \sigma\tau Q - \sigma Q + \sigma Q - Q =$$
$$\sigma(\tau Q - Q) + (\sigma Q - Q) = \sigma\left(\kappa\left(P \otimes \frac{m}{n}\right)(\tau)\right) + \kappa\left(P \otimes \frac{m}{n}\right)(\sigma)$$

so Kummer map is well defined.

Proposition 11.1. Given an elliptic curve defined over a perfect field K, the following sequence, which is called *Kummer sequence* is exact.

$$0 \longrightarrow E(K) \otimes \mathbb{Q}/\mathbb{Z} \xrightarrow{\kappa} H^1\left(K, E(\overline{K})_{\mathrm{tors}}\right) \xrightarrow{\lambda} H^1\left(K, E(\overline{K})\right) \longrightarrow 0$$

Proof. Let $x \in \ker\kappa$. It is easy to see that $x = P \otimes \frac{m}{n}$ for some $P \in E(K)$ and $m, n \in \mathbb{Z}$. Let $Q \in E(\overline{K})$ satisfying that $[n]Q = [m]P$, so

$$\kappa\left(P \otimes \frac{m}{n}\right)(\sigma) = \sigma Q - Q \ \forall \sigma \in G_{\overline{K}|K}$$

is a coboundary, so there is some $R \in E(\overline{K})_{\text{tors}}$ such that

$$\sigma R - R = \sigma Q - Q \ \forall \sigma \in G_K \Rightarrow \sigma(Q-R) = Q - R \ \forall \sigma \in G_K \Rightarrow Q - R \in E(K)$$

Let $l \in \mathbb{N}$ be the order of R. Then $[lm]P = [ln]Q = [ln](Q-R) \in E(K)$. Since $Q - R \in E(K)$,

$$x = P \otimes \frac{m}{n} = P \otimes \frac{lm}{ln} = [lm]P \otimes \frac{1}{ln} = [ln](Q-R) \otimes \frac{1}{ln} = (Q-R) \otimes 1 = 0$$

Then κ is injective, so the sequence is exact at $E(K) \otimes \mathbb{Q}/\mathbb{Z}$.

By construction, $\lambda \circ \kappa = 0$, since the result of the composition is the coboundary $\sigma \mapsto \sigma Q - Q$. Conversely, if $\varphi \in \ker \lambda$, then there is some $Q \in E(\overline{K})$ such that

$$\varphi(\sigma) = \sigma Q - Q \ \forall \sigma \in G_K$$

Since this cocycle takes values on $E\left(\overline{K}\right)_{tors}$ then for every $\sigma \in G_K$ there is some $n_\sigma \in \mathbb{N}$ such that

$$n_\sigma(\sigma Q - Q) = O \Rightarrow \sigma([n_\sigma]Q) = [n_\sigma]Q \tag{11.2}$$

Hence for every $n \in \mathbb{N}$ we can define the subgroup

$$G_n := \{\sigma \in G_K : \sigma([n]Q) = [n]Q\}$$

It is easy to see that G_n is the subgroup of Galois automorphisms that fix $K([n]Q)$ and, since $K([n]Q)|K$ is finite, then G_n is an open subgroup. By equation 11.2, $\{G_n : n \in \mathbb{N}\}$ is an open cover of the compact space G_K, so it has to admit a finite subcover $\{G_{n_1}, \ldots, G_{n_s}\}$. Define $N := lcm(n_1, \ldots, n_s)$. Then $G_{n_i} \subset G_N \ \forall i = 1, \ldots, s$, so $G = G_N$. Then $[N]Q \in E(K)$ and $\varphi = \kappa\left([N]Q \otimes \frac{1}{N}\right) \in \text{Im}(\kappa)$. Hence the sequence is exact at $H^1\left(K, E\left(\overline{K}\right)_{\text{tors}}\right)$.

Finally, the map λ appears in the long cohomological exact sequence given in lemma 6.4.

$$H^1\left(K, E\left(\overline{K}\right)_{tors}\right) \xrightarrow{\lambda} H^1\left(K, E\left(\overline{K}\right)\right) \longrightarrow H^1\left(K, E\left(\overline{K}\right)/E\left(\overline{K}\right)_{\text{tors}}\right)$$

However, $E\left(\overline{K}\right)/E\left(\overline{K}\right)_{\text{tors}}$ is a uniquely divisible group, so it is cohomologically trivial by corollary 6.4. Hence λ is surjective and the original sequence is also exact at $H^1\left(K, E\left(\overline{K}\right)\right)$. □

Now choose any valuation v of K and fix some inclusion $\overline{K} \hookrightarrow \overline{K_v}$, which determines an inclusion $G_{K_v} \subset G_K$ by corollary 5.3 and consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K) \otimes (\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa} & H^1\left(K, E\left(\overline{K}\right)_{\text{tors}}\right) & \xrightarrow{\lambda} & H^1\left(K, E\left(\overline{K}\right)\right) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a_v} & & \downarrow{\scriptstyle b_v} & & \downarrow{\scriptstyle c_v} & & \\ 0 & \longrightarrow & E(K_v) \otimes (\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa_v} & H^1\left(K_v, E\left(\overline{K_v}\right)_{\text{tors}}\right) & \xrightarrow{\lambda_v} & H^1\left(K_v, E\left(\overline{K_v}\right)\right) & \longrightarrow & 0 \end{array} \tag{11.3}$$

At this moment, we can define similarly the Selmer group by considering in the second exact row the direct product of all primes of K.

Definition 11.3. Given an elliptic curve E/K, its *Selmer group* is defined as follows.

$$\text{Sel}_E(K) = \bigcap_{v \in M_K} \ker(c_v \circ \lambda) \subset H^1\left(K, E\left(\overline{K}\right)_{\text{tors}}\right)$$

where the intersection is taken along all the primes v of K. Looking at diagram 11.3 it is also possible to reinterpret the Selmer group.

$$Sel_E(K) = \ker\left(\text{Res} : \ H^1\left(K, E\left(\overline{K}\right)_{\text{tors}}\right) \to \prod_v \left(H^1\left(K_v, E\left(\overline{K_v}\right)_{\text{tors}}\right)/\text{Im}(\kappa_v)\right)\right)$$

Again, remark 11.1 applies to this definition, so the Selmer group is also well defined.

The short exact sequence exposed for the ϕ-Selmer group and the kernel $Ш_E(K)[\phi]$ can be generalised to the Selmer group, but considering in this case the whole Tate-Shafarevich group.

Theorem 11.3. Let E/K be an elliptic curve. There is a short exact sequence

$$0 \longrightarrow E(K) \otimes (\mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa} \mathrm{Sel}_E(K) \xrightarrow{\lambda} Ш_E(K) \longrightarrow 0$$

Proof. From the diagram appearing in equation 11.3, it is clear that the maps κ and λ are well defined, that κ is injective and that $\mathrm{Im}(\kappa) = \ker(\lambda)$. Finally, given $\varphi \in Ш_E(K)$, there is some $\psi \in H^1(K, E_{\mathrm{tors}})$ such that $\lambda(\psi) = \phi$. It is also clear from the diagram that $\psi \in \mathrm{Sel}_E(K)$, so the sequence is exact. □

Taking into account the identity

$$\mathrm{corank}_{\mathbb{Z}_p} E(K) \otimes (\mathbb{Q}/\mathbb{Z}) = \mathrm{rank}_{\mathbb{Z}} E(K)$$

we see that $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_E(K)$ is an upper bound for this rank, because of corollary 4.4. It is conjectured that this upper bound is an equality when E is defined over a number field, which is equivalent to the following statement.

Conjecture 11.1. Let E be an elliptic curve defined over a number field K. Then the Tate-Shafarevich group $Ш_E(K)$ is finite.

The Selmer group can be expressed in terms of the Selmer groups of the isogenies $[n]$.

Proposition 11.2. Let E be an elliptic curve defined over a number field K. Then the following identity is satisfied:

$$\mathrm{Sel}_E(K) = \varinjlim_n S^n(E/K)$$

Proof. It is clear by proposition 6.4 that

$$H^1(K, E_{tors}) = H^1\left(K, \varinjlim_n E[n]\right) = \varinjlim_n H^1(K, E[n])$$

where the transition maps are induced by the inclusions $E[n] \subset E[m]$ whenever $n|m$. Since these transition maps commute with restrictions, they induce maps between the Selmer groups

$$S^n(E/K) \to S^m(E/K)$$

Hence it is not difficult to see that

$$\mathrm{Sel}_E(K) = \varinjlim_n S^n(E/K)$$

□

Another important property of Selmer groups is that, given a field extension $L|K$, the restriction map sends the Selmer group $\mathrm{Sel}_E(K)$ to $\mathrm{Sel}_E(L)$. Showing that this map has finite kernel and cokernel in case $L|K$ is a $\mathbb{Z}_p$-extension will be the content of Mazur's control theorem

Proposition 11.3. Let $L|K$ be a field extension and let E be an elliptic curve defined over K. Then the restriction $\mathrm{Res} : H^1(K, E_{\mathrm{tors}}) \to H^1(L, E_{\mathrm{tors}})$ induces a map in the Selmer groups:

$$\mathrm{Sel}_E(K) \to \mathrm{Sel}_E(L)^{G_{L|K}}$$

Proof. Let w be a prime of L lying over a certain prime v of K. Since the following diagram is clearly commutative

$$\begin{array}{ccc} E(K_v)\otimes(\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa_v} & H^1(K_v, E_{\text{tors}}) \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \text{Res}} \\ E(L_w)\otimes(\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa_w} & H^1(L_w, E_{\text{tors}}) \end{array}$$

Then $\text{Res}^{K_v}_{L_w}(\text{Im}(\kappa_v)) \subset \text{Im}(\kappa_w)$. Now consider another commutative diagram:

$$\begin{array}{ccc} H^1(K, E_{\text{tors}}) & \xrightarrow{\text{Res}} & H^1(K_v, E_{\text{tors}}) \\ \downarrow{\scriptstyle \text{Res}} & & \downarrow{\scriptstyle \text{Res}} \\ H^1(L, E_{\text{tors}}) & \xrightarrow{\text{Res}} & H^1(L_w, E_{\text{tors}}) \end{array}$$

Denoting by

$$S_v(K) = \ker\left(H^1(K, E_{\text{tors}}) \to H^1(K_v, E_{\text{tors}})/\text{Im}(\kappa_v)\right)$$

we see that if $\varphi \in S_v(K)$ then $\text{Res}^K_{K_v}(\varphi) \in \text{Im}(\kappa_v)$, so

$$\left(\text{Res}^L_{L_w} \circ \text{Res}^K_L\right)(\varphi) = \left(\text{Res}^{K_v}_{L_w} \circ \text{Res}^K_{K_v}\right)(\varphi) \in \text{Im}(\kappa_w)$$

Therefore, $\text{Res}^K_L(\varphi) \in S_w(L)$.

Let $\psi \in \text{Sel}_E(K) = \bigcap_v S_v(K)$. For any arbitrary prime w of L, there is a prime v of K such that w lie over v. Then $\text{Res}^K_L(\psi) \in S_w(L)$ for every prime w of L, so $\text{Res}^K_L(\psi) \in \text{Sel}_E(L)$ Moreover, $\text{Res}^K_L(\psi)$ is invariant by the Galois group because it is in the image of the restriction map. □

Since the Selmer group is torsion by corollary 6.5, we can study its p-primary parts separately.

Proposition 11.4. The p-primary part of $H^n(K, E_{\text{tors}})$ is $H^n(K, E[p^\infty])$.

Proof. It is proposition 6.9. □

Since $E(K)\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ is the p-primary part of $E(K)\otimes(\mathbb{Q}/\mathbb{Z})$ and the maps κ and κ_v can be restricted to the p-primary parts, we can consider the following commutative diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & E(K)\otimes(\mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{\kappa} & H^1\left(K, E[p^\infty]\right) \\ & & \downarrow{\scriptstyle a_v} & & \downarrow{\scriptstyle b_v} \\ 0 & \longrightarrow & E(k_v)\otimes(\mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{\kappa_v} & H^1(K_v, E[p^\infty]) \end{array}$$

Then the p-primary part of the Selmer group is

$$\text{Sel}_E(K)_p = \ker\left(H^1\left(K, E[p^\infty]\right) \to \prod_v H^1\left(K_v, E[p^\infty]\right)/\text{Im}(\kappa_v)\right)$$

because κ_v factors through the p-primary and not p-primary direct summands.

Remark 11.3. Given a field extension $K \subset L$, the canonical map $\text{Sel}_E(K) \to \text{Sel}_E(L)$ induces a natural map between the p-primary parts of the Selmer groups.

We end this section with a comment about Tate-Shafarevich conjecture 11.1. Although it is not known whether Tate-Shafarevich group is finite or not, there is a result due to Cassels that states that its order has to be a perfect square in case it is finite.

Theorem 11.4. Let E be an elliptic curve defined over a number field K. Then there is an alternate bilinear pairing

$$Ш_E(K) \times Ш_E(K) \to \mathbb{Q}/\mathbb{Z}$$

whose kernel is precisely $Ш_E(K)_{div}$.

Proof. See [2]. □

In case that $Ш_E(K)$ is finite, then $Ш_E(K)_{div} = 0$, so the above mentioned bilinear pairing is non-degenerate. In that case, $Ш_E(K)$ and $\mathrm{Hom}(Ш_E(K), \mathbb{Q}/\mathbb{Z})$ have the same number of elements, so the bilinear map induces an isomorphism between them.

By the structure theorem of finite abelian groups, there exists cyclic groups $C_1, \ldots, C_r$ such that

$$Ш_E(K) \cong C_1 \times \cdots C_r$$

If $\widehat{C}_i := \mathrm{Hom}(C_i, \mathbb{Q}/\mathbb{Z})$, then

$$\mathrm{Hom}(Ш_E(K), \mathbb{Q}/\mathbb{Z}) = \widehat{C}_1 \times \cdots \times \widehat{C}_r$$

The bilinear map pairs C_1 with a cyclic subgroup of $\mathrm{Hom}(Ш_E(K), \mathbb{Q}/\mathbb{Z})$ of order $|C_1|$ and disjoint of $\widehat{C}_1$. In the previous identification, it will correspond to a cyclic subgroup D_i of the same order and disjoint to C_i. Taking the quotients under $C_i \cdot D_1$ and applying an inductive argument, we deduce that $|Ш_E(K)|$ is a prefect square.

Corollary 11.2. Let E be an elliptic curve defined over a number field K. If $Ш_E(K)$ is finite, then its order is a perfect square. Similarly, given a prime number p, if $Ш_E(K)_p$ is finite, then its order is also a perfect square.

11.3 The Image of the Kummer Map

As a preparation for the proof of Mazur's control theorem, it is interesting to describe the images κ_v for each valuation $v \in M_K$.

If K is an algebraic extension of $\mathbb{Q}$, by theorems 9.6 and 9.7, $\mathrm{Im}(\kappa_v) = 0$ for every archimedean valuation and non-archimedean not dividing p. For valuations lying over p, the description is more subtle, but in case K is a number field we know that $\mathrm{Im}(\kappa_v)$ has corank $[K_v : \mathbb{Q}_p]$ by theorem 9.8.

Assume that E has good ordinary reduction at some prime v lying over p, i.e., the reduced curve $\widetilde{E}$ is non-singular and contains p-torsion defined over the algebraic closure $\overline{k}_v$.

By theorem 9.2, there is a short exact sequence

$$0 \longrightarrow \mathcal{F}[p^\infty] \longrightarrow E[p^\infty] \xrightarrow{\pi} \widetilde{E}[p^\infty] \longrightarrow 0$$

where $\mathcal{F}[p^\infty]$ is the p-primary part in the kernel of the reduction map and is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a group. It induces another exact sequence in the first cohomology groups

$$H^1\left(K_v, \mathcal{F}[p^\infty]\right) \xrightarrow{\varepsilon_v} H^1\left(K_v, E[p^\infty]\right) \xrightarrow{\pi_v} H^1\left(K_v, \widetilde{E}[p^\infty]\right)$$

Then, we will describe $\mathrm{Im}(\kappa_v)$ as the division subgroup of $\mathrm{Im}(\varepsilon_v)$. First we show that one is contained in the other.

Proposition 11.5. Let K_v be a p-adic field and let E/K_v be an elliptic curve having good reduction at v. Then

$$\mathrm{Im}(\kappa_v) \subset \mathrm{Im}(\varepsilon_v)$$

Proof. Since $\mathrm{Im}(\epsilon_v) = \ker(\pi_v)$, the preceding inclusion is equivalent to $\pi_v \circ \kappa_v = 0$. Let $P \otimes \frac{m}{n} \in E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Then

$$\kappa_v \left(P \otimes \frac{m}{n} \right) = \sigma Q - Q$$

where $Q \in E(\overline{K_v})$ is such that $[n]Q = [m]P$. Then

$$(\pi_v \circ \kappa_v) \left(P \otimes \frac{m}{n} \right) = \sigma \widetilde{Q} - \widetilde{Q} \in H^1 \left(K_v, \widetilde{E}[p^\infty] \right)$$

where $\widetilde{Q} := \pi(Q)$. It is clearly a coboundary in $H^1 \left(K_v, \widetilde{E} \right)$. However, $\widetilde{E}(\overline{k_v})$ is a torsion group, so its p-primary component $E[p^\infty]$ is a direct summand. By proposition 6.9, then $(\pi_v \circ \kappa_v) \left(P \otimes \frac{m}{n} \right)$ is also a coboundary in $H^1 \left(K_v, \widetilde{E}[p^\infty] \right)$. □

We want to identify $\mathrm{Im}(\kappa_v)$ with the divisible subgroup of $\mathrm{Im}(\varepsilon_v)$. To do that, we need to apply theorem 8.1.

Corollary 11.3. Assume that E has good, ordinary reduction when defined over K_v. The image subgroup $\mathrm{Im}(\epsilon_v)$ is cofinitely generated and has corank r.

Proof. We apply theorem 8.1 to $A = \mathcal{F}[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$. The action of G_{K_v} on A can be described by a character

$$\varphi : \ G_{K_v} \to \mathbb{Z}_p^*$$

because we have seen in example 4.1 that $\mathbb{Z}_p \cong \mathrm{Hom}\left(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p\right)$. Similarly, the action of G_{K_v} on μ_{p^∞} can be described by another character

$$\chi : \ G_{K_v} \to \mathbb{Z}_p^*$$

We can also consider the action of the Galois group on the quotient $E[p^\infty]/\mathcal{F}[p^\infty] \cong \widetilde{E}[p^\infty]$. It would be described by a character

$$\psi : \ G_{K_v} \to \mathbb{Z}_p^*$$

Using the Weil pairing shown in [27], proposition III. 8.1, we see that

$$\varphi\psi = \chi : \ G_{K_v} \to \mathbb{Z}_p^*$$

Since ψ describes the action of the Galois group on $\widetilde{E}[p^\infty]$, it is clearly non-trivial because $\widetilde{E}(k_v)$ is finite.

Hence $\varphi \neq \chi$ independently of the generators of $\mathcal{F}[p^\infty]$ and μ_{p^∞} chosen, so $\mathcal{F}[p^\infty]$ is not isomorphic to μ_{p^∞} as a G_{K_v}-module. Moreover, φ is not trivial either, since the torsion of $E(K_v)$ is finite by proposition 9.5, so it cannot contain $\mathcal{F}[p^\infty]$. Then theorem 8.1 implies that

$$\mathrm{corank}_{\mathbb{Z}_p} H^1\left(K_v, \mathcal{F}[p^\infty]\right) = [K_v : \mathbb{Q}_p]$$

However, we can consider the cohomological long exact sequence

$$H^0 \left(K_v, \widetilde{E}[p^\infty] \right) \xrightarrow{\delta} H^1\left(K_v, \mathcal{F}[p^\infty]\right) \xrightarrow{\varepsilon_v} H^1\left(K_v, E[p^\infty]\right)$$

However, $H^0 \left(K_v, \widetilde{E}[p^\infty] \right)$ is the p-primary part of $\widetilde{E}(k_v)$, so it is finite. Then $\ker(\varepsilon_v)$ is finite too and we can consider the following short exact sequence

$$0 \longrightarrow \ker(\varepsilon_v) \longrightarrow H^1\left(K_v, \mathcal{F}[p^\infty]\right) \xrightarrow{\varepsilon_v} \mathrm{Im}(\varepsilon_v) \longrightarrow 0$$

Since $\ker(\varepsilon_v)$ is finite, its Pontriagyn dual is finite too by 4.2, so $\operatorname{corank}_{\mathbb{Z}_p} = 0$. Then by corollary 4.4,

$$\operatorname{corank}_{\mathbb{Z}_p}\operatorname{Im}(\varepsilon_v) = \operatorname{corank}_{\mathbb{Z}_p} H^1\left(K_v, \mathcal{F}[p^\infty]\right) = [K_v : \mathbb{Q}_p]$$

□

Theorem 11.5. Assume K_v is a finite extension of $\mathbb{Q}_p$ and that E/K_v has good, ordinary reduction at K_v. Then $\operatorname{Im}(\kappa_v) = \operatorname{Im}(\epsilon_v)_{\text{div}}$.

Proof. By proposition 11.5, $\operatorname{Im}(\kappa_v) \subset \operatorname{Im}(\varepsilon_v)$. Since κ_v is injective, then $\operatorname{Im}(\kappa_v) \cong E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$

Since both $\operatorname{Im}(\kappa_v)$ and $\operatorname{Im}(\varepsilon_v)$ have the same corank. By corollary 4.4, the factor group $T = \operatorname{Im}(\varepsilon_v)/\operatorname{Im}(\kappa_v)$ has corank 0, so its Pontryagin dual $\widehat{T}$ is $\mathbb{Z}_p$-torsion and finitely generated, so it is finite and, therefore, T is finite too.

Since $\operatorname{Im}(\kappa_v) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]}$, then it is a division subgroup, so $\operatorname{Im}(\kappa_v) \subset \operatorname{Im}(\varepsilon_v)_{\text{div}}$. Then $\operatorname{Im}(\varepsilon_v)_{\text{div}}/\operatorname{Im}(\kappa_v)$ is a finite division group, so it only contains one element. Hence $\operatorname{Im}(\kappa_v) = \operatorname{Im}(\varepsilon_v)_{\text{div}}$. □

We have just seen that $\operatorname{Im}(\kappa_v)$ is a subgroup of finite index in $\operatorname{Im}(\varepsilon_v)$. Next theorem controls that index but this proof uses a result about Poitou-Tate duality which is out of the scope of this work.

Theorem 11.6. If K_v is a finite extension of $\mathbb{Q}_p$, and if E is an elliptic curve defined over K_v with good ordinary reduction, then $\operatorname{Im}(\kappa_v)$ has finite index in $\operatorname{Im}(\epsilon_v)$ and the quotient $\operatorname{Im}(\epsilon_v)/\operatorname{Im}(\kappa_v)$ is a cyclic group whose order divides $\left|\widetilde{E}(k_v)_p\right|$, where k_v is the residue field of v. In particular, if $p \not| \left|\widetilde{E}(k_v)\right|$, then $\operatorname{Im}(\kappa_v) = \operatorname{Im}(\epsilon_v)$.

Proof. We are going to use a result whose proof is out of the scope of this thesis (see [23], theorem 7.2.6). Given a finite G_{K_v} module M such that $|M| = p^n$ for some $n \in \mathbb{N}$, then $H^2(K_v, M)$ is the Pontryagin dual of $H^0\left(K_v, \operatorname{Hom}(M, \mu_{p^\infty})\right)$.

Since Weil pairing $E[p^m] \times E[p^m] \to \mu_{p^m}$ is alternating by [27], proposition III. 8.1, and because E has good ordinary reduction at K_v, it induces another non-degenerate pairing $\mathcal{F}[p^m] \times \widetilde{E}[p^m] \to \mu_{p^m}$, which means that there is an injection

$$\widetilde{E}[p^m] \hookrightarrow \operatorname{Hom}_{G_{K_v}}\left(\mathcal{F}[p^m], \mu_{p^m}\right) \hookrightarrow \operatorname{Hom}\left(\mathcal{F}[p^m], \mu_{p^m}\right)$$

Since both $\widetilde{E}[p^m]$ and $\operatorname{Hom}\left(\mathcal{F}[p^m], \mu_{p^m}\right)$ have p^m elements, then $\widetilde{E}[p^m] \cong \operatorname{Hom}\left(\mathcal{F}[p^m], \mu_{p^m}\right)$.

Since $\widetilde{E}(k_v)$ is finite, then $\widetilde{E}(k_v)[p^m] = \widetilde{E}(k_v)_p$ for large enough m. For this m, then

$$\widetilde{E}(k_v)_p \cong H^0\left(K_v, \operatorname{Hom}\left(\mathcal{F}[p^m], \mu_{p^m}\right)\right) \cong H^2(K_v, \mathcal{F}[p^m])$$

where the last isomorphism is not canonical and comes from proposition 4.11.

However, $H^1\left(K_v, \mathcal{F}[p^\infty]\right)$ has corank $[K_v : \mathbb{Q}_p]$ by theorem 8.1, so

$$H^1\left(K_v, \mathcal{F}[p^\infty]\right) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]} \times T$$

where T is a finite p-group. If $p^m \geq |T|$, then

$$H^1\left(K_v, \mathcal{F}[p^\infty]\right)_{\text{div}} = p^m H^1\left(K_v, \mathcal{F}[p^\infty]\right)$$

Now consider the exact sequence

$$0 \longrightarrow \mathcal{F}[p^m] \longrightarrow \mathcal{F}[p^\infty] \xrightarrow{\cdot p^m} \mathcal{F}[p^\infty] \longrightarrow 0$$

It induces an exact sequence in the cohomology groups

$$H^1\left(K_v, \mathcal{F}[p^\infty]\right) \xrightarrow{\cdot p^m} H^1\left(K_v, \mathcal{F}[p^\infty]\right) \longrightarrow H^2\left(K_v, \mathcal{F}[p^m]\right)$$

Then there is an injection

$$H^1\left(K_v, \mathcal{F}[p^\infty]\right)/H^1\left(K_v, \mathcal{F}[p^\infty]\right)_{\text{div}} = H^1\left(K_v, \mathcal{F}[p^\infty]\right)/p^m H^1\left(K_v, \mathcal{F}[p^\infty]\right) \hookrightarrow H^2\left(K_v, \mathcal{F}[p^m]\right)$$

Therefore, $H^1\left(K_v, \mathcal{F}[p^\infty]\right)/H^1\left(K_v, \mathcal{F}[p^\infty]\right)_{\text{div}}$ is a cyclic group whose order divides the one of $\widetilde{E}(k_v)_p$.

Moreover, the map ε_v induces a surjection

$$H^1\left(K_v, \mathcal{F}[p^\infty]\right)/H^1\left(K_v, \mathcal{F}[p^\infty]\right)_{\text{div}} \twoheadrightarrow \text{Im}(\varepsilon_v)/\text{Im}(\varepsilon_v)_{\text{div}} = \text{Im}(\varepsilon_v)/\text{Im}(\kappa_v)$$

It is thus clear that $\text{Im}(\varepsilon_v)/\text{Im}(\kappa_v)$ is cyclic and its order divides the order of $\widetilde{E}(k_v)_p$.

In case $\widetilde{E}(k_v)$ has no p-torsion or, equivalently, $p \nmid \widetilde{E}(k_v)$, then $\text{Im}(\varepsilon_v) = \text{Im}(\kappa_v)$. □

We can generalise last result to infinite extensions of $\mathbb{Q}_p$ whose profinite degree divides p^∞.

Theorem 11.7. Let E be an elliptic curve defined over an algebraic extension K_v of $\mathbb{Q}_p$ with finite residue field k_v. Assume that E has good ordinary reduction at K_v. Assume also that the profinite degree of $G_{K_v|\mathbb{Q}_p}$ is divisible by p^∞. Then $\text{Im}(\kappa_v) = \text{Im}(\epsilon_v)$. In particular, this is true if K_v is a ramified $\mathbb{Z}_p$-extension of F_v, where F_v is a finite extension of $\mathbb{Q}_p$.

Proof. We can write K_v as a union of finite extensions of $\mathbb{Q}_p$, i.e., $K_v := \bigcup_{i\in I} F_v^{(i)}$. Then proposition 4.6 implies that

$$H^1\left(K_v, E[p^\infty]\right) = \varinjlim_i H^1\left(F_v^{(i)}, E[p^\infty]\right)$$

where the transition maps are cohomological restrictions. Moreover, we can write

$$\text{Im}(\varepsilon_v) = \varinjlim_i \text{Im}(\varepsilon_v^{(i)}), \quad \text{Im}(\kappa_v) = \varinjlim_i \text{Im}(\kappa_v^{(i)})$$

By proposition 11.5, $\text{Im}\left(\kappa_v^{(i)}\right) \subset \text{Im}\left(\varepsilon_v^{(i)}\right)$ for every $i \in I$. Therefore, $\text{Im}(\kappa_v) \subset \text{Im}(\varepsilon_v)$. Furthermore, direct limit is an exact functor by proposition 4.3, so

$$\text{Im}(\varepsilon_v)/\text{Im}(\kappa_v) = \varinjlim_i \text{Im}(\varepsilon_v^{(i)})/\text{Im}(\kappa_v^{(i)})$$

Nevertheless, by theorem 11.6 the orders of the quotients $\text{Im}\left(\varepsilon_v^{(i)}\right)/\text{Im}\left(\kappa_v^{(i)}\right)$ are uniformly bounded by $|\widetilde{E}(k_v)_p|$, so the order of the direct limit has the same bound.

Now we are going to show that $\text{Im}(\varepsilon_v)$ is a divisible group. For that purpose, we just need to show that $H^1\left(K_v, \mathcal{F}[p^\infty]\right)$ is divisible. It is clearly divisible by every prime $q \neq p$, because multiplication by q is an isomorphism in $\mathcal{F}[p^\infty]$. For $q = p$, consider the short exact sequence

$$0 \longrightarrow \mathcal{F}[p] \longrightarrow \mathcal{F}[p^\infty] \xrightarrow{\cdot p} \mathcal{F}[p^\infty] \longrightarrow 0$$

It induces another exact sequence in the cohomology groups:

$$H^1\left(K_v, \mathcal{F}[p^\infty]\right) \xrightarrow{\cdot p} H^1\left(K_v, \mathcal{F}[p^\infty]\right) \xrightarrow{\delta} H^2\left(K_v, \mathcal{F}[p]\right)$$

Analogously to proposition 8.2, one can deduce $H^2\left(K_v, \mathcal{F}[p]\right) = 0$, so $H^1\left(K_v, \mathcal{F}[p^\infty]\right)$ is also p-divisible.

Therefore, $\text{Im}(\varepsilon_v)/\text{Im}(\kappa_v)$ is a finite division group, so it has to be trivial. □

11.4 Mazur's Control Theorem

Now we are able to prove the above mentioned Mazur's Control Theorem.

Theorem 11.8. (Mazur, 1972) Let F be a number field and let E be an elliptic curve defined over F. Assume that p is a rational prime such that E has good, ordinary reduction at all primes of F lying over p. Assume also that F_∞ is a $\mathbb{Z}_p$-extension of F and denote by F_n the unique subextension such that $[F_n : F] = p^n$. Then the natural maps

$$\mathrm{Sel}_E(F_n)_p \to \mathrm{Sel}_E(F_\infty)_p^{G_{F_\infty|F_n}}$$

have finite kernels and cokernels whose orders are bounded as $n \to \infty$.

As a matter of notation, we will write for every algebraic extension K of $\mathbb{Q}$ and every prime v of K

$$\mathcal{H}_E(K_v) = H^1(K_v, E[p^\infty])/\mathrm{Im}(\kappa_v)$$

where we have chosen any extension of every prime v to the algebraic closure. The product along every prime of K will be written as

$$\mathcal{P}_E(K) = \prod_v \mathcal{H}_E(K_v)$$

By definition, the p-primary part of the Selmer group is

$$\mathrm{Sel}_E(K)_p = \ker\left(H^1(K, E[p^\infty]) \to \mathcal{P}_E(K)\right)$$

Then defining

$$\mathcal{G}_E(K) := \mathrm{Im}\left(H^1\left(K, E[p^\infty]\right) \to \mathcal{P}_E(K)\right)$$

we can consider the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}_E(F_n)_p & \longrightarrow & H^1(F_n, E[p^\infty]) & \longrightarrow & \mathcal{G}_E(F_n) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle g_n} & & \\ 0 & \longrightarrow & \mathrm{Sel}_E(F_\infty)_p^{\Gamma_n} & \longrightarrow & H^1(F_\infty, E[p^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}_E(F_\infty)^{\Gamma_n} & & \end{array}$$

Here s_n is the natural maps between Selmer groups, which is well defined by proposition 11.3. Moreover, g_n is defined in each factor by:

$$r_{v_n} : \mathcal{H}_E((F_n)_{v_n}) \to \mathcal{H}_E((F_\infty)_\eta)$$

where η is any prime arbitrarily chosen among those lying above v_n and r_{v_n} is the cohomological restriction.

Snake's lemma 6.3 gives an exact sequence:

$$0 \longrightarrow \ker(s_n) \longrightarrow \ker(h_n) \longrightarrow \ker(g_n) \longrightarrow \mathrm{coker}(s_n) \longrightarrow \mathrm{coker}(h_n) \tag{11.4}$$

Lemma 11.2. $\ker(h_n)$ is finite and has bounded order as $n \to \infty$.

Proof. Consider the inflation-restriction sequence given by theorem 6.1

$$0 \longrightarrow H^1(\Gamma_n, E(F_\infty)_p) \longrightarrow H^1(F_n, E[p^\infty]) \xrightarrow{h_n} H^1(F_\infty, E[p^\infty])^{\Gamma_n}$$

where $\Gamma := G_{F_\infty|F} \cong \mathbb{Z}_p$ and $\Gamma_n := \Gamma^{p^n} = G_{F_\infty|F_n}$. Then $\ker(h_n) \cong H^1(\Gamma_n, E(F_\infty)_p)$. Let $A := E(F_\infty)_p$ be the p-primary subgroup of $E(F_\infty)$. If γ is a topological generator of Γ then proposition 6.20 implies that

$$H^1(\Gamma_n, A) = A/(\gamma^{p^n} - 1)A$$

Since $E(F_n)$ is finitely generated by Mordell-Weil theorem 10.2 and the kernel of $\gamma^{p^n} - 1$ acting on A is $E(F_n)_p$, then $H^0(\Gamma_n, A)$ is finite.

Since A is a subgroup of $E[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$, it is cofinitely generated. By remark 4.7 and proposition 6.22, $\left(\gamma^{p^n} - 1\right) A_{\text{div}} = A_{\text{div}}$. Then,

$$A_{\text{div}} \subset \left(\gamma^{p^n} - 1\right) A \subset A$$

Again, remark 4.7 says that A_{div} has finite index in A. Moreover, $H^1(\Gamma_n, A) \cong A/(\gamma^{p^n} - 1)A$ has order bounded by $[A : A_{\text{div}}]$, which does not depend on n. □

Lemma 11.3. $\text{coker}(h_n) = 0 \ \forall n \in \mathbb{N}$

Proof. Using inflation-restriction sequence given in theorem 6.1 applied to $G_{F_\infty} \subset G_{F_n}$, we see that the sequence

$$H^1(F_n, E[p^\infty]) \xrightarrow{h_n} H^1(F_\infty, E[p^\infty])^{\Gamma_n} \longrightarrow H^2(\Gamma_n, A)$$

where A is again $A = E(F_\infty)_p$. Since $\Gamma_n \cong \mathbb{Z}_p$, then proposition 6.21 implies that $H^2(\Gamma_n, A) = 0$, so h_n is surjective. □

In order to study $\ker(g_n)$ we can do it separately on each factor by studying $\ker(r_{v_n})$. In case v is archimedean, then v splits completely because $\mathbb{Z}_p$ has no subgroups of order 2, so $(F_\infty)_\eta = F_v$ for every $\eta|v$. Therefore, r_{v_n} is the identity map, so $\ker(r_{v_n}) = 0$.

For the non-archimedean case, we consider separately when $v \nmid p$ and $v|p$.

Lemma 11.4. Suppose that v is a non-arquimedean prime not dividing p. Then $\ker(r_{v_n})$ is finite and has bounded order as n tends to infinity. Moreover, if either E has good reduction at v or v splits completely in $F_\infty|F$, then $\ker(r_{v_n}) = 0$.

Proof. If v splits completely in $F_\infty|F$, then the lemma is clear since $(F_\infty)_\eta = F_v$, where η is any extension of v to F_∞.

Otherwise, Γ_v has finite index in Γ and $\Gamma_v \cong \mathbb{Z}_p$. Let M be the maximal abelian pro-p extension of F_v. By proposition 7.2, $G_{M|F_v} \cong \mathbb{Z}_p \times T$, where T is a finite group. Hence F_v has only one $\mathbb{Z}_p$-extension, which will be $(F_\infty)_\eta|F_v$. Therefore, $(F_\infty)_\eta|F_v$ will be the unramified $\mathbb{Z}_p$-extension of F_v.

Let $B_\eta := E((F_\infty)_\eta)[p^\infty]$, which is cofinitely generated, let $\Gamma_{v_n} := G_{(F_\infty)_\eta|(F_n)_{v_n}} \cong \mathbb{Z}_p$ and let γ_{v_n} be a topological generator of Γ_{v_n}. Since $\text{Im}(\kappa_{v_n}) = 0$ and $\text{Im}(\kappa_\eta) = 0$ by corollary 9.5, consider the inflation-restriction sequence given by theorem 6.1:

$$0 \longrightarrow H^1(\Gamma_{v_n}, B_\eta) \longrightarrow H^1\left((F_n)_{v_n}, E[p^\infty]\right) \xrightarrow{r_{v_n}} H^1\left((F_\infty)_\eta, E[p^\infty]\right)$$

Hence,

$$\ker(r_{v_n}) \cong H^1(\Gamma_{v_n}, B_v) \cong B_\eta/(\gamma_{v_n} - 1)B_\eta$$

Just as in the proof of lemma 11.2, $(B_v)_{\text{div}} \subset (\gamma_{v_n} - 1)B_v$, so

$$|\ker(r_{v_n})| \leq (B_v : (B_v)_{\text{div}})$$

and this bound does not depend on n.

Assume now that E has good reduction at v. We have seen that $(F_\infty)_\eta$ is the unramified $\mathbb{Z}_p$-extension of F_v. On the other hand, $F_v(E[p^\infty])$ is also unramified since the reduction map $E[p^\infty] \to \widetilde{E}[p^\infty]$ is a bijection because v does not divide p. Moreover,

$$F_v(E[p^\infty]) = \varinjlim_n F_v(E[p^n]) \subset \varinjlim_n F_v\left([p^n]^{-1}E(F_v)\right)$$

By corollary 10.1, whose proof does not require F_v to be a number field, $F_v\left([p^n]^{-1}E(F_v)\right)|F_v$ is an abelian extension of exponent dividing p^n and, therefore, its profinite degree divides p^∞. Moreover, $F_v(E[p^\infty])$ has to be an infinite extension since every finite extension of F_v contains only finitely many p-primary torsion points by proposition 9.5. Hence $F_v(E[p^\infty])$ is the unramified $\mathbb{Z}_p$-extension, so $F_v(E[p^\infty]) \cong (F_\infty)_\eta$.

Therefore, $B_v = E((F_\infty)_\eta)[p^\infty] = E[p^\infty]$ is divisible, so $\ker(r_{v_n}) = 0\ \forall n \in \mathbb{N}$. □

Lemma 11.5. Suppose that v is a prime dividing p. Assume that E has good ordinary reduction at v. Then $\ker(r_{v_n})$ is finite and has bounded order as n tends to ∞.

Proof. If v splits completely in $F_\infty|F$, then $(F_\infty)_\eta = F_v$ and $\ker(r_{v_n}) = 0\ \forall n \in \mathbb{N}$.

Otherwise, the decomposition subgroup of v has finite index in $\mathbb{Z}_p$. Assume first that v ramifies in $F_\infty|F$. The inertia group is thus a non-trivial closed subgroup of $\mathbb{Z}_p$, so it has finite index. Then the ramification degree of $(F_\infty)_\eta|F_v$ is finite, so the residue field f_η of $(F_\infty)_\eta$ is also finite. By theorem 11.7, r_{v_n} can be written as the composition of the following two maps:

$$\begin{aligned} a_n :&\ H^1\left((F_n)_{v_n}, E[p^\infty]\right)/\mathrm{Im}(\kappa_{v_n}) \to H^1\left((F_n)_{v_n}, E[p^\infty]\right)/\mathrm{Im}(\varepsilon_{v_n}) \\ b_n :&\ H^1\left((F_n)_{v_n}, E[p^\infty]\right)/\mathrm{Im}(\varepsilon_{v_n}) \to H^1\left((F_\infty)_\eta, E[p^\infty]\right)/\mathrm{Im}(\varepsilon_\eta) \end{aligned}$$

Since a_n is surjective,

$$|\ker(r_{v_n})| = |\ker(a_n)| \cdot |\ker(b_n)|$$

However, $\ker(a_n) = \mathrm{Im}(\varepsilon_{v_n})/\mathrm{Im}(\kappa_{v_n})$ has order bounded by $|\widetilde{E}(f_\eta)_p|$, due to theorem 11.6. On the other hand, we can consider the short exact sequence

$$0 \longrightarrow \mathcal{F}[p^\infty] \longrightarrow E[p^\infty] \longrightarrow \widetilde{E}[p^\infty] \longrightarrow 0$$

whose long cohomological exact sequence can be included the following commutative diagram:

$$\begin{array}{ccccc} 0 \longrightarrow H^1\left((F_n)_{v_n}, E[p^\infty]\right)/\mathrm{Im}(\varepsilon_{v_n}) & \xrightarrow{\pi_{v_n}} & H^1\left((F_n)_{v_n}, \widetilde{E}[p^\infty]\right) \\ \downarrow{\scriptstyle b_n} & & \downarrow{\scriptstyle c_n} \\ 0 \longrightarrow H^1\left((F_\infty)_\eta, E[p^\infty]\right)/\mathrm{Im}(\varepsilon_\eta) & \xrightarrow{\pi_\eta} & H^1\left((F_\infty)_\eta, \widetilde{E}[p^\infty]\right) \end{array}$$

where c_n is just the cohomological restriction. Then π_{v_n} injects $\ker(b_n)$ into $\ker(c_n)$, which means that $|\ker(b_n)| \leq |\ker(c_n)|$. However, inflation-restriction sequence given in theorem 6.1 says that

$$\ker(c_n) \cong H^1\left((F_\infty)_\eta|(F_n)_{v_n}, \widetilde{E}(f_\eta)_p\right) \cong \widetilde{E}(f_\eta)_p/(\gamma_{v_n} - 1)\widetilde{E}(f_\eta)_p$$

where γ_{v_n} is a topological generator of $G_{(F_\infty)_\eta|(F_n)_{v_n}}$. Here we have used that $G_{(F_\infty)_\eta|(F_n)_{v_n}} \cong \mathbb{Z}_p$ because v is finitely decomposed and therefore the Galois group is isomorphic to a subgroup of finite index in $\mathbb{Z}_p$. Then we have applied proposition 6.20.

Hence $|\ker(c_n)|$ is bounded above by $|\widetilde{E}(f_\eta)_p|$ and thus

$$|\ker(r_n)| \leq |\widetilde{E}(f_\eta)_p|^2$$

Finally, suppose that v is unramified in $F_\infty|F$ but it does not split completely. Then the decomposition group of v is a non-trivial closed subgroup of $\mathbb{Z}_p$, so it is also isomorphic to $\mathbb{Z}_p$. Therefore, $(F_\infty)_\eta$ is the unramified $\mathbb{Z}_p$-extension of F_v.

Denoting $F_{v_n} := (F_n)_{v_n}$, we claim that $H^1\left(F_{v_n}|F_{v_m}, E\left(F_{v_n}\right)\right) = 0$ for every natural numbers m and n. In fact, since E has good reduction at v, we can consider the exact sequence,

$$0 \longrightarrow \mathcal{F}(\mathfrak{m}_n) \longrightarrow E\left(F_{v_n}\right) \longrightarrow \widetilde{E}(f_n) \longrightarrow 0$$

where $\mathfrak{m}_n$ is the maximal ideal in the ring of integers of $(F_n)_{v_n}$ and f_n is the residue field of $(F_n)_{v_n}$. It induces an exact sequence in the cohomology groups

$$H^1\left(F_{v_n}|F_{v_m}, \mathcal{F}(\mathfrak{m}_n)\right) \longrightarrow H^1\left(F_{v_n}|F_{v_m}, E\left(F_{v_n}\right)\right) \longrightarrow H^1\left(F_{v_n}|F_{v_m}, \widetilde{E}(f_n)\right)$$

Then it is enough to prove that both $H^1\left(F_{v_n}|F_{v_m}, \mathcal{F}(\mathfrak{m}_n)\right)$ and $H^1\left(F_{v_n}|F_{v_m}, \widetilde{E}(f_n)\right)$ are trivial.

For the first one, we can consider the filtration $\mathcal{F}(\mathfrak{m}_n) \supset \mathcal{F}(\mathfrak{m}_n^2) \supset \mathcal{F}(\mathfrak{m}_n^3) \cdots$. By remark 3.5, $\mathcal{F}\left(\mathfrak{m}_n^i\right)/\mathcal{F}\left(\mathfrak{m}_n^{i+1}\right) \cong f_n$, so there is an exact sequence

$$H^1\left(F_{v_n}|F_{v_m}, \mathcal{F}\left(\mathfrak{m}_n^{i+1}\right)\right) \longrightarrow H^1\left(F_{v_n}|F_{v_m}, F\left(\mathfrak{m}_n^{i}\right)\right) \longrightarrow H^1\left(F_{v_n}|F_{v_m}, f_n\right)$$

However, since $F_{v_n}|F_{v_m}$ is unramified, then by theorem 7.2

$$H^1\left(F_{v_n}|F_{v_m}, f_n\right) \cong H^1(f_n|f_m, f_n) = 0$$

so the first arrow in the preceding exact sequence was surjective. Composing them, for each $i \in \mathbb{N}$ there is a surjection

$$H^1\left(F_{v_n}|F_{v_m}, \mathcal{F}\left(\mathfrak{m}_n^{i}\right)\right) \twoheadrightarrow H^1\left(F_{v_n}|F_{v_m}, \mathcal{F}\left(\mathfrak{m}_n\right)\right)$$

Then it is enough to prove that the comology group vannishes for some i. However, for large enough i, theorem 3.2 says that $\mathcal{F}(\mathfrak{m}^i) \cong R_n$, where R_n is the ring of integers of F_{v_n}. However, since $F_{v_n}|F_{v_m}$ is unramified, then $R_n = R_m \otimes \mathbb{Z}[G_{F_{v_n}|F_{v_m}}]$ is a coinduced module, so its cohomology vanishes. Therefore,

$$H^1\left(F_{v_n}|F_{v_m}, \mathcal{F}(\mathfrak{m})\right) = 0$$

On the other hand,

$$H^1\left(F_{v_n}|F_{v_m}, \widetilde{E}(f_n)\right) \cong H^1\left(f_n|f_m, \widetilde{E}(f_n)\right)$$

Theorem 6.1 says that $H^1\left(f_n|f_m, \widetilde{E}(f_n)\right)$ is isomorphic to a subgroup of $H^1\left(f_m, \widetilde{E}\left(\overline{f_m}\right)\right)$, we just need to see that the latter vanishes. Since $\widetilde{E}\left(\overline{f_m}\right)$ is torsion, we have that

$$\widetilde{E}\left(\overline{f_m}\right) = \prod_{q \text{ prime}} \widetilde{E}[q^\infty]$$

so it is enough to check that $H^1\left(f_m, \widetilde{E}[q^\infty]\right) = 0$ for every prime number q. Since f_m is finite,

$$G_{f_m} \cong \widehat{\mathbb{Z}} \cong \prod_{q \text{ prime}} \mathbb{Z}_q$$

Calling $H_q := \prod_{l \neq q} \mathbb{Z}_l$ and using theorem 6.1 again,

$$0 \longrightarrow H^1\left(\mathbb{Z}_q, \widetilde{E}[q^\infty]^{H_q}\right) \xrightarrow{\text{Inf}} H^1\left(\widehat{\mathbb{Z}}, \widetilde{E}[q^\infty]\right) \xrightarrow{\text{Res}} H^1\left(H_q, \widetilde{E}[q^\infty]\right)$$

By proposition 6.8, the latter cohomology group vanishes, so

$$H^1\left(\mathbb{Z}_q, \widetilde{E}[q^\infty]^{H_q}\right) \cong H^1\left(\widehat{\mathbb{Z}}, \widetilde{E}[q^\infty]\right)$$

In case $q \neq p$, we saw in the proof of lemma 11.4 that $f_m(\widetilde{E}[q^\infty])$ is the only $\mathbb{Z}_q$ extension of f_m, so $\widetilde{E}[q^\infty]^{H_q} = \widetilde{E}[q^\infty]$. In case $q = p$, one can also prove similarly that $F_{v_m}(E[p^\infty])|F_{v_m}$ has profinite degree dividing p^∞ and so does its residue extension $f_m(\widetilde{E}[p^\infty])|f_m$. Then $\widetilde{E}[p^\infty]^{H_p} = \widetilde{E}[p^\infty]$.

In any case, $H^0(\mathbb{Z}_q, \widetilde{E}[q^\infty]) = \widetilde{E}(f_m)_q$ is finite, so proposition 6.22 implies that

$$H^1\left(\widehat{\mathbb{Z}}, \widetilde{E}[q^\infty]\right) = H^1\left(\mathbb{Z}_q, \widetilde{E}[q^\infty]^{H_q}\right) = 0$$

Once we have proven the claim, denoting by $F_\eta := (F_\infty)_\eta$ we have by corollary 6.2 that

$$H^1\left(F_\eta|F_{v_m}, E\left(F_\eta\right)\right) = \varinjlim_n H^1\left(F_{v_n}|F_{v_m}, E\left(F_{v_n}\right)\right) = 0$$

Hence theorem 6.1 says that the following restriction map is injective.

$$\text{Res}: \ H^1\left(F_{v_n}, E\right) \to H^1\left(F_\eta, E\right) \tag{11.5}$$

We can use Kummer sequences to build the following commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E\left(F_{v_n}\right) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\kappa_n} & H^1\left(F_{v_n}, E[p^\infty]\right) & \xrightarrow{\lambda_n} & H^1\left(F_{v_n}, E\right) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow \text{Res} & & \downarrow \text{Res} & & \\
0 & \longrightarrow & E\left(F_\eta\right) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\kappa_\infty} & H^1\left(F_\eta, E[p^\infty]\right) & \xrightarrow{\lambda_\infty} & H^1\left(F_\eta, E\right) & \longrightarrow & 0
\end{array}$$

Then let $\varphi \in H^1\left(F_{v_n}, E[p^\infty]\right)$ be a representative of a class belonging to $\ker(r_{v_n}) \subset \mathcal{H}_E\left((F_n)_{v_n}\right)$. Then $\text{Res}(\varphi) \in \text{Im}(\kappa_\infty) = \ker(\lambda_\infty)$, so

$$\lambda_\infty \circ \text{Res}(\varphi) = 0 = \lambda_n \circ \text{Res}(\varphi)$$

By equation 11.5, $\lambda_n(\varphi) = 0$, so $\varphi \in \text{Im}(\kappa_n)$ and thus represents the zero class in $\mathcal{H}_E\left((F_n)_{v_n}\right)$. □

Now we can complete the proof of theorem 11.8.

Proof of theorem 11.8. Using the exact sequence given in equation 11.4, we get that

$$|\ker(s_n)| \leq |\ker(h_n)| \leq [E(F_\infty)_p : E(F_\infty)_{p,\text{div}}]$$

which is bounded for all $n \in \mathbb{N}$. Moreover, $\ker(g_n)$ is the direct product of $\ker(r_{v_n})$, where v_n runs through every valuation in F_n. Moreover, by lemma 11.4 $\ker(r_{v_n}) = 0$ for every valuation but those dividing p and being finitely decomposed in F_∞ or those finitely decomposed at which E has bad reduction. Hence the set of valuations in F_n such that $\ker(r_{v_n}) \neq \emptyset$ is bounded as $n \to \infty$. Furthermore, lemma 11.5 says that $\ker(r_{v_n})$ is bounded for every valuation, so $\ker(g_n)$ is also bounded. Using again the exact sequence of equation 11.4 and lemma 11.3, we get that

$$|\text{coker}(s_n)| \leq |\ker(g_n)|$$

is uniformly bounded. □

A natural question that arises is when the map s_n is injective and surjective. For the injectivity, a sufficient condition is that $E(F)$ does not contain p-torsion. In that case $E(F_\infty)$ will have no p-torsion. In fact, assume the contrary and let F_n be the minimal subextension containing $E(F_\infty)[p]$. If γ is a topological generator of $G_{F_\infty|F}$, then γ^{p^n} would act trivially on $E(F_\infty)[p]$. However, $E(F_\infty)[p]$ has to be isomorphic to $\mathbb{Z}/p$ or to $\mathbb{Z}/p \times \mathbb{Z}/p$.

In the first case γ can be identified with an element in $GL_1(\mathbb{F}_p) \cong \mathbb{F}_p^*$, so the only possibility for γ^{p^n} acts trivially on the p-torsion is that γ does the same.

In the latter case, $\gamma \in GL_2(\mathbb{F}_p)$ will have an eigenvalue $\alpha \in \overline{\mathbb{F}_p}$ which will satisfy that $\alpha^{p^n} = 1$. Hence $\alpha = 1$ and $\ker(\gamma - 1)$ will be non-trivial, which means that $E(F)[p] \neq \{O\}$.

Thus $E(F_\infty)_p = \{O\}$, so the proof of lemma 11.2 imply that

$$|\ker(s_n)| \leq |\ker(h_n)| \leq (E(F_\infty)_p : E(F_\infty)_{p,\mathrm{div}}) = 1$$

There is more subtle result about the injectivity of s_n whose proof is out of the scope of this thesis.

Proposition 11.6. Let E be an elliptic curve defined over a number field F and let F_∞ be a $\mathbb{Z}_p$-extension of F. Assume that E has good ordinary reduction at all primes lying over p and that there is at least one prime v of F lying over p satisfying that the ramification index $e(F_v : \mathbb{Q}_p) \leq p - 2$. Then the map

$$s_n : \ \mathrm{Sel}_E(F_n)_p \to \mathrm{Sel}_E(F_\infty)_p$$

is injective for every $n \in \mathbb{N} \cup \{0\}$.

Proof. [10], proposition 3.9. □

There is another result that characterises the surjectivity of the map s_n and states an implication about the vanishing of the Selmer group $\mathrm{Sel}_E(F_\infty)$. Before stating it, we need to define the anomalous primes for an elliptic curve as those satisfying that the reduced curve has the same cardinality as the residue field

Proposition 11.7. Let E be an elliptic curve defined over a number field F such that E has good, ordinary reduction at al primes of F lying over p. Assume that $\mathrm{Sel}_E(F)_p = 0$, that none of the primes of F over p are anomalous for E and that $E(F_v)_p = 0$ for all primes of F where E has bad reduction. Then $\mathrm{Sel}_E(F_\infty) = 0$.

Proof. We want to show first that the map s_n is surjective in this case. By lemma 11.3, we just need to show that $\ker(g_0) = 0$, which is equivalent to $\ker(r_v) = 0 \ \forall v \in M_F$.

Assume v does not divide p. If E has good reduction at v, then $\ker(r_v) = 0$ by lemma 11.4. Otherwise, $E(F_v)_p = \{O\}$ and the argument given while studying the injectivity of s_n implies that $E\left((F_\infty)_\eta\right)_p = \{O\}$, so the proof of lemma 11.4 also implies that $\ker(r_v) = 0$.

In case v divides p, we can assume that v ramifies since otherwise lemma 11.5 implies that $\ker(r_v) = 0$. In case v is ramified, then f_η is a finite p-extension of f_v. Again, the fact that $\widetilde{E}(f_v)_p = \left\{\widetilde{O}\right\}$ implies that $\widetilde{E}(f_\eta)_p = \left\{\widetilde{O}\right\}$. Hence the proof of lemma 11.5 shows that $\ker(r_v) = 0$.

Therefore, $\mathrm{Sel}_E(F) = 0$, implies that $\mathrm{Sel}_E(F_\infty)^\Gamma = 0$. Then its Pontryagin dual $X/TX = 0$, where $X = \mathrm{Hom}\left(\mathrm{Sel}_E(F_\infty), \mathbb{Q}_p/\mathbb{Z}_p\right)$. From proposition 2.6 one could deduce that $X = 0$, so $\mathrm{Sel}_E(F_\infty)_p = 0$. □

11.5 Consequences of Mazur's Theorem

Mazur's control theorem has interesting corollaries concerning the growth of the rank of the Mordell-Weil groups.

Corollary 11.4. Let E be an elliptic curve defined over a number field F and let p be a prime number such that E has good, ordinary reduction at all primes of F lying above p. Let also $F_\infty|F$ be a $\mathbb{Z}_p$-extension. If $\mathrm{Sel}_E(F)_p$ is finite, then $\mathrm{Sel}(F_\infty)_p$ is Λ-cotorsion. Consequently, $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ is bounded as $n \to \infty$.

Proof. Theorem 11.8 implies that $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is finite. Then $X := \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$ is a Λ-module and X/TX is the maximal quotient of X on which $\Gamma := G_{F_\infty|F}$ acts trivially. Hence the Pontryagin dual of X/TX is the maximal subgroup of $\mathrm{Sel}_E(F_\infty)_p$ on which Γ acts trivially, i.e., its dual is $\mathrm{Sel}_E(F_\infty)_p^\Gamma$. Thus X/TX is a finite quotient, so proposition 2.8 implies that X is a finitely generated torsion Λ-module.

Then $X/X_{\mathbb{Z}_p-\mathrm{tors}}$ is a finitely generated $\mathbb{Z}_p$-module, so the structure theorem states that $X/X_{\mathbb{Z}_p-\mathrm{tors}} \cong \mathbb{Z}_p^\lambda$ for some $\lambda \geq 0$. Hence $\mathrm{Sel}_E(F_\infty)_p$ is cofinitely generated, so remark 4.7 implies that

$$(\mathrm{Sel}_E(F_\infty)_p)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$$

Since $\mathrm{Sel}_E(F_\infty)^{\Gamma_n} \subset \mathrm{Sel}_E(F_\infty)$, then theorem 11.8 again implies that

$$(\mathrm{Sel}_E(F_n)_p)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n}, \text{ where } t_n \leq \lambda$$

Since

$$E(F_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rank}(E(F_n))}$$

injects into $(\mathrm{Sel}_E(F_n)_p)_{\mathrm{div}}$, we deduce that $\mathrm{rank}\,(E(F_n)) \leq \lambda\ \forall n \geq 0$. □

Under the conditions of last corollary, one could check the finiteness of the rank of Mordell-Weil group $E(F_\infty)$ just by checking whether its torsion subgroup is finite, which is usually easier.

Theorem 11.9. Let K be a Galois extension of a number field F and let E be an elliptic curve defined over F. Assume that $E(K)_{\mathrm{tors}}$ is finite and that $\mathrm{rank}_{\mathbb{Z}}E(L)$ is bounded as L varies over all finite subextensions of $K|F$. Then $E(K)$ is finitely generated.

Proof. Let $t := |E(K)_{\mathrm{tors}}| < \infty$. Choose a subextension $L|K$ such that $\mathrm{rank}_{\mathbb{Z}}E(K)$ is as large as possible. Since the rank is an additive function, $E(K)/E(L)$ must be a torsion group. Hence for each $P \in E(K)$ there is a natural number $n_P \in \mathbb{N}$ such that $n_P P \in E(L)$. Given $\sigma \in G_{K|L}$, then

$$[n_P](\sigma(P) - P) = \sigma([n_P]P) - [n_P](P) = O$$

Hence $\sigma(P) - P \in E(K)_{\mathrm{tors}}$, so $[t]\,(\sigma(P) - P) = O$. Thus,

$$\sigma\,([t]P) = [t]P\ \forall \sigma \in G_{K|L} \Rightarrow [t]P \in E(L)$$

We can thus define the following homomorphism

$$\varphi : E(K) \to E(L) :\ P \mapsto [t]P$$

Since $\ker(\varphi) = E(K)_{\mathrm{tors}}$, then $E(K)$ is finitely generated and $\mathrm{rank}_{\mathbb{Z}}E(K)$ is the maximum of $\mathrm{rank}_{\mathbb{Z}}E(L)$as L varies over all finite subextensions of $K|F$. □

All we have done can be summed up in the following result.

Corollary 11.5. Let E be an elliptic curve defined over a number field F and let p be a prime number such that E has good, ordinary reduction at all primes of F lying above p. Let also $F_\infty|F$ be a $\mathbb{Z}_p$-extension. If $\mathrm{Sel}_E(F)_p$ is finite and $E(F_\infty)_{\mathrm{tors}}$ is finite, then $E(F_\infty)$ is finitely generated.

Mazur's control theorem has an interesting result concerning the growth of Tate-Shafarevich group.

Corollary 11.6. Let E be an elliptic curve defined over a number field F such that E has good, ordinary reduction at all primes of F lying above p. Let $F_\infty|F$ be a $\mathbb{Z}_p$-extension and call F_n the unique subextension of degree p^n. If both $E(F_n)$ and $Ш_E(F_n)_p$ are finite for every $n \in \mathbb{Z}$, there are $\lambda, \mu \in \mathbb{N} \cup \{0\}$ depending only on E and $F_\infty|F$ such that

$$|Ш_E(F_n)_p| = p^{\lambda n + \mu p^n + O(1)}$$

Proof. Again let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$ the Pontryagin dual of the Selmer group. We have seen in the proof of corollary 11.4 that X is an Iwasawa module. X/w_nX is thus the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)^{\Gamma_n}$, since it is the maximal quotient on which Γ_n acts trivially. By theorem 11.8, we have that

$$\frac{|\mathrm{Sel}_E(F_n)_p|}{|X/w_nX|} = p^{e_n}$$

where $|e_n|$ is bounded as $n \to \infty$. By proposition 2.7, we have that $|X/w_nX| = p^{\mu p^n + \lambda n + O(1)}$. Using that $E(F_n)$ is finite, we have by theorem 11.3 that

$$|Ш_E(F_n)_p| = |\mathrm{Sel}_E(F_n)_p| = p^{\mu p^n + \lambda n + O(1)}$$

□

Remark 11.4. By corollary 11.2, $\mu p^n + \lambda n + O(1)$ has to be an even number for every $n \in \mathbb{N}$.

In the last corollary, the invariants λ and μ can be positive. Although under the conditions of proposition 11.7, $\lambda = \mu = 0$, there are elliptic curves in which that does not happen. Here we show an example where the constant μ is 1.

Example 11.1. We will now show an example where the μ-invariant is positive. Consider the prime number $p = 5$ and the elliptic curve $E = X_0(11)$ defined over the rationals $\mathbb{Q}$ and given by a Weierstrass equation

$$y^2 + y = x^3 - x^2 - 10x - 20$$

Its discriminant is $\Delta = -11^5$. One can find in Cremona tables [7] that $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$ and that $E[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mu_5$ as $G_\mathbb{Q}$-modules.

Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_5$-extension of $\mathbb{Q}$. Taking into account the Kummer isomorphism given in corollary 7.1, we can consider the following map

$$\mathcal{U}_\infty \to H^1(\mathbb{Q}_\infty, \mu_5) : \; b \mapsto \frac{\sigma(\beta)}{\beta}$$

where $\mathcal{U}_\infty$ is the group of units of the ring of integers of $\mathbb{Q}_\infty$ and $\beta \in \overline{\mathbb{Q}}$ is some element satisfying that $\beta^5 = b$. It is easy to see that the kernel of this map is $\mathcal{U}_\infty \cap (\mathbb{Q}_\infty)^5 = \mathcal{U}_\infty^5$. Hence $H^1(\mathbb{Q}_\infty, \mu_5)$ contains a subgroup isomorphic to

$$\frac{\mathcal{U}_\infty}{\mathcal{U}_\infty^5} = \varinjlim_n \frac{\mathcal{U}_n}{\mathcal{U}_n^5}$$

where $\mathcal{U}_n$ is the group of units in the ring of integers of $\mathbb{Q}_n := \mathbb{Q}(\mu_{5^n})$. Since $\mathbb{Q}_n$ is totally real and contains 5-torsion for $n \geq 1$, by Dirichlet's unit theorem 2.5 we have that

$$\frac{\mathcal{U}_n}{\mathcal{U}_n^5} \cong (\mathbb{Z}/5)^n$$

One could see that the Pontryagin dual of $\frac{\mathcal{U}_\infty}{\mathcal{U}_\infty^5}$ is isomorphic to

$$\varprojlim_n (\mathbb{Z}/5)^n \cong \varprojlim_n \frac{\mathbb{Z}_p[[T]]}{(w_n, 5)} \cong \mathbb{Z}_p[[T]]/(5)$$

which has μ-invariant $\mu = 1$. Since the μ-invariant is an additive function by remark 2.4, then $H^1(K_v, \mu_\infty)$ has positive μ-invariant.

The kernel of the reduction map $E[5] \to \widetilde{E}[5]$ must be a Galois module, so the only possibilities are $\mathbb{Z}/5$ and μ_5. It is just a computation to check $\widetilde{E}(\mathbb{F}_5)$ contains 5 torsion and that the reduction map is injective in $\mathbb{Z}/5$, so μ_5 must be contained in the kernel of the reduction map $E[5^\infty] \to \widetilde{E}[5^\infty]$. Hence the inclusion

$$\mu_5 \hookrightarrow E[5^\infty]$$

induces a cohomological map

$$\varepsilon : \frac{\mathcal{U}_\infty}{\mathcal{U}_\infty^5} \hookrightarrow H^1(\mathbb{Q}_\infty, \mu_5) \to H^1(\mathbb{Q}_\infty, E[5^\infty])$$

where $\mathbb{Q}_\infty$ is the cyclotomic extension of $\mathbb{Q}$.

The image of ε is contained in the Selmer group $\mathrm{Sel}_E(\mathbb{Q}_\infty)_5$. In fact, we have to check that the cohomological restriction belongs to $\mathrm{Im}(\kappa_v)$ for every valuation in $M_{\mathbb{Q}_\infty}$.

If v is archimedean, then $G_{(\mathbb{Q}_\infty)_v} = G_{\mathbb{R}}$ has two elements because $\mathbb{Q}_\infty$ is totally real. Then $H^1\left((\mathbb{Q}_\infty)_v, E[5^\infty]\right) = 0$ by proposition 6.8.

Assume now that v is non-archimedean and it is different from 5. By [23], Proposition 11.1.1, $(\mathbb{Q}_\infty)_v|\mathbb{Q}_v$ is the unramified $\mathbb{Z}_5$-extension of $\mathbb{Q}_v$. Let $b \in \mathcal{U}_\infty^* / \left(\mathcal{U}_\infty^*\right)^5$. If $\beta \in \overline{\mathbb{Q}}^*$ satisfies that $\beta^5 = b$, then $\mathbb{Q}_\infty(\beta)|\mathbb{Q}_\infty$ is an unramified extension of degree dividing 5, so the only possibility is that $\beta \in \mathbb{Q}_\infty$

$$\varphi(\sigma) = \frac{\sigma(\beta)}{\beta} = 1 \ \forall \sigma \in G_{\mathbb{Q}_\infty}$$

Finally, in case that $v = 5$, the cohomological restriction is contained in $\mathrm{Im}(\kappa_v)$ because of theorem 11.7.

The kernel $\ker(\varepsilon)$ is isomorphic to $H^0(\mathbb{Q}_\infty, E[5^\infty]/\mu_5)$, which is a subgroup of $E[5^\infty]/\mu_5$ and, therefore, is $\mathbb{Z}_p$-cofinitely generated, which means that the coinvariant is $\mu = 0$.

By remark 2.4, $\mathrm{Im}(\varepsilon)$ has coinvariant $\mu = 1$, so the Selmer group has positive μ-invariant. It is shown in [10] that the invariant μ takes the value 1 in this case.

The behaviour of these invariants λ and μ is still an active research issue. For instance, we state the following open problem concerning some cases when $\mu = 0$.

Conjecture 11.2. Let $E/\mathbb{Q}$ be an elliptic curve. Assume that $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is Λ-cotorsion. Then there exists a $\mathbb{Q}$-isogeneous elliptic curve E' such that $\mu = 0$. In particular, if $E[p]$ is irreducible as a $\mathbb{Z}/p$ representation of $G_{\mathbb{Q}}$, then $\mu = 0$.

Last conjecture would imply that there would be elliptic curves with arbitrary large values of the invariant λ.

Theorem 11.10. Let $p \in \mathbb{Z}$, then $\lambda + \mu$ is unbounded when E runs through the elliptic curves defined over $\mathbb{Q}$ with good, ordinary reduction at p. If furthermore conjecture 11.2 is true, then λ is unbounded.

Proof. [10], corollary 5.6. □

Is is also possible that the rank remains unbounded in the $\mathbb{Z}_p$-extension. In any case, assuming conjecture 11.1, there must be some regularity in the growth of the rank.

Corollary 11.7. Let E be an elliptic curve defined over a number field F having good, ordinary reduction at all primes of F lying over p. Let $F_\infty|F$ be a $\mathbb{Z}_p$-extension. Let $r = \text{corank}_\Lambda \text{Sel}_E(F_\infty)_p$. Then

$$\text{corank}_{\mathbb{Z}_p}(\text{Sel}_E(F_n)_p) = rp^n + O(1)\ \forall n \in \mathbb{N}$$

In particular, if $Ш_E(F_n)_p$ is finite for all $n \in \mathbb{N}$, then

$$\text{rank}(E(F_n)) = rp^n + O(1)\ \forall n \in \mathbb{N}$$

Proof. Let $X := \text{Hom}(\text{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Then by theorem 11.8 and proposition 2.8,

$$\text{corank}_{\mathbb{Z}_p}\left(\text{Sel}_E(F_n)p\right) = \text{corank}_{\mathbb{Z}_p}\left(\text{Sel}_E(F_\infty)_p^\Gamma\right) = \text{rank}_{\mathbb{Z}_p}(X/w_nX) = rp^n + O(1)$$

□

We will finish this work with a comment about the necessity of the hypothesis of good ordinary reduction in Mazur's control theorem 11.8 at the primes of F lying above p.

Assume first that E has good supersingular reduction at a prime of F lying over p. If $F_\infty|F$ is ramified at such prime, it can be shown that $\text{Sel}_E(F_\infty)_p = H^1(F_\infty, E[p^\infty])$ has positive corank. There are examples in which $E(F_n)$ and $Ш_E(F_n)_p$ are finite for every $n \in \mathbb{N}$, so corollary 11.4 would say that $\text{rank}_{\mathbb{Z}} E(F_n)$ would remain bounded, contrary to corollary 11.7. Therefore, theorem 11.8 does not hold in case there are primes of F lying over p which E has supersingular reduction at.

Otherwise, if we let E have multiplicative reduction at some primes of F lying above p, it is conjectured that the conclusion of theorem 11.8 remains true. It can be proved for $F = \mathbb{Q}$ and it is done, assuming certain condition, in [10].

Bibliography

[1] M. F. Atiyah, I. G. McDonald. *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company, 1969. 24

[2] J. W. S. Cassels. *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung.* Journal für die reine und angewandte Mathematik, **211** (1962), 95-112. 143

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor. *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises.* Journal of the American Mathematical Society **14** (2001), 843-939. 3

[4] J. W. S. Cassels, A. Fröhlich, (editors). *Algebraic Number Theory.* Thompson Book Company Inc. 1967. 6, 55

[5] J. W. S. Cassels. *Local Fields.* Cambridge University Press, 1986. 5, 128

[6] L. Claborn. *Every abelian group is a class group.* Pacific Journal of Mathematics, **18** (1966), 219-222. 25

[7] J. E. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1992. 154

[8] J. Coates, A. Wiles. *On the conjecture of Birch and Swinnerton-Dyer.* Inventiones Mathematicae **39** (1977), 223-251. 2

[9] N. Elkies. $\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$. Number Theory Listserver, 2006. 2

[10] R. Greenberg *Iwasawa Theory for Elliptic Curves.* Lecture Notes in Mathematics, **1716** (1999), 51-144. 5, 152, 155, 156

[11] R. Greenberg *Introduction to Iwasawa Theory for Elliptic Curves.* IAS/Park City Mathematical Series, **9** (2001), 407-464. 7, 39

[12] B.H. Gross, D. B. Zagier. *Heegner points and derivatives of L-series.* Inventiones Mathematicae **84** (1986), 225-320. 2

[13] P. J. Hilton, U. Stammbach. *A Course in Homological Algebra.* Springer-Verlag, 1971. 5, 54

[14] I. M. Isaacs. *Finite Group Theory.* American Mathematical Society, 2008. 46, 47

[15] K. Iwasawa. *On* Γ*-extensions of algebraic number fields.* Bulletin of the American Mathematical Society, **65** (1959), 183-226. 4

[16] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1989. 15

[17] B. Mazur. *Rational points of abelian varieties with values in towers of number fields.* Inventiones Mathematicae **18** (1972), 183-266. 4

[18] B. Mazur. *Modular Curves and the Eisenstein Ideal.* Publications Mathématiques de l'I.H.E.S. **47** (1977), 33-186. 2, 133

[19] L. B. Merel. *Bounds for the torsion of elliptic curves over number fields.* Invent. Math. **124** (1996), 437-449. 2

[20] P. Morandi. *Fields and Galois Theory.* Springer-Verlag, 1996. 55

[21] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, 1999. 4, 5, 11, 24, 25, 55, 59, 60, 105, 116, 128, 131

[22] J. Neukirch. *Class Field Theory.* Springer-Verlag, 2013. 6

[23] J. Neukirch, A. Schmidt, K.Wingberg. *Cohomology of Number Fields.* Springer-Verlag, 2000. 5, 6, 11, 39, 55, 87, 145, 155

[24] L. Ribes, P. Zaleski. *Profinite Groups.* Springer-Verlag, 2010. 39, 48

[25] K. Ribet. *Torsion Points of Abelian Varieties in Cyclotomic Extensions.* L'Enseignement Mathématique, **27** (1981), 315-319. 3

[26] J. P. Serre. *Local Fields.* Springer-Verlag, 1979. 6

[27] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1992. 2, 5, 6, 7, 11, 27, 115, 116, 123, 131, 132, 144, 145

[28] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, 1994. 123

[29] W. C. Waterhouse. *Profinite groups are Galois groups.* Proc. of the American Mathematical Society. **42** (1974), 639-640. 58