Universitat Politècnica de Catalunya

McGill University

The Golod-Shafarevich Inequality and the Class Field Tower Problem

Author:
Jordi Vilà Casadevall

Supervisors:
Henri Darmon
Víctor Rotger Cerdà

A thesis submitted in fulfilment of the requirements for the bachelor's degree in mathematics and the bachelor's degree in engineering physics

May 2022

Acknowledgements

I would like to start expressing my gratitude to my supervisors, Henri Darmon, for providing guidance and support throughout these months in Montreal, as well as for giving me the opportunity of coming to McGill University, and Víctor Rotger, for giving me the contact of Henri Darmon and for being willing to help me at any time.

I would like to thank Andrei Jaikin-Zapirain for providing me with my thesis topic, as well as for giving me the necessary support and references to carry out my thesis. I would also like to thank Martí Roset for dedicating so much time to helping me with the doubts that arose while carrying out my thesis, as well as for offering me guidance for my personal matters.

I am also very grateful to CFIS for giving me the opportunity to work on my undergraduate thesis abroad and for the financial support that made this possible.

Finally, I would like to thank my roommate and friend Jordi Rodríguez for all the good and bad days we have shared together, and all my friends here in Montreal for making this last year one of the best years of my life.

Abstract

In this thesis we will present explicit counterexamples for the class field tower problem, hence proving that there exist number fields K that cannot be embedded into a larger number field L with class number 1.

We will start by introducing profinite groups, which describe the Galois groups of infinite Galois extensions. Special emphasis is given to pro-p groups, which describe the Galois groups of p-extensions, as they appear in the solution of the class field tower problem. We will explain how to describe a pro-p group in terms of generators and relations, and prove the Golod-Shafarevich inequality, which establishes a criterion for a pro-p group to be infinite.

After introducing the necessary notions of algebraic number theory, we will apply the Golod-Shafarevich inequality to the class field tower problem via the Galois group of the maximal unramified pro-p extension. We will obtain a criterion for a number field K to have infinite class field tower, and give explicit examples of number fields satisfying this criterion.

Keywords: number theory, class field theory, class field tower problem, profinite groups, pro-p groups, Golod-Shafarevich inequality.

Resum

En aquesta tesi presentarem contraexemples explícit per al problema de la torre de cossos de classes, demostrant així que existeixen cossos de nombres K que no poden ser immergits dins un cos de nombres més gran L amb nombre de classes 1.

Començarem introduint els grups profinits, els quals descriuen els grups de Galois d'extensions de Galois infinites. Posarem un èmfasi especial als grups pro-p, els descriuen el grup de Galois de p-extensions, ja que apareixen en la solució del problema de la torre de cossos de classes. Explicarem com descriure un grup pro-p en termes de generadors i relacions, i demostrarem la desigualtat de Golod-Shafarevich, la qual estableix un criteri per a que un grup pro-p sigui infinit.

Després d'introduir les nocions necessàries de teoria algebraica de nombres, aplicarem la desigualtat de Golod-Shafarevich al problema de la torre de cossos de classes a través del grup de Galois de la extensió pro-p no ramificada maximal. Obtindrem un criteri per a que un cos de nombres K tingui una torre de cossos de classes infinita, i donarem exemples explícits de cossos de nombres satisfent aquest criteri.

Paraules clau: teoria de nombres, teoria de cossos de classes, problema de la torre de cossos de classes, grups profinits, grups pro-p, desigualtat de Golod-Shafarevich.

Resumen

En esta tesis presentaremos contraejemplos explícitos para el problema de la torre de cuerpos de clases, demostrando así que existen cuerpos de números K que no pueden ser inmergidos dentro de un cuerpo de números más grande L con número de clases 1.

Empezaremos introduciendo los grupos profinitos, los cuales describen los grupos de Galois de extensiones de Galois infinitas. Pondremos un énfasis especial a los grupos pro-p, los cuales describen los grupos de Galois de p-extensiones, ya que aparecen en la solución del problema de la torre de cuerpos de clases. Explicaremos como describir un grupo pro-p en términos de generadores y relaciones, y demostraremos de desigualdad de Golod-Shafarevich, la cual establece un criterio para que un grupo pro-p sea infinito.

Después de introducir las nociones necesarias de teoría de números, aplicaremos la desigualdad de Golod-Shafarevich al problema de la torre de cuerpos de clases a través del grupo de Galois de la extensión pro-p no ramificada maximal. Obtendremos un criterio para que un cuerpo de números K tenga una torre de cuerpos de clases infinita, y daremos ejemplos explícitos de cuerpos de números satisfaciendo este criterio.

Palabras clave: teoría de números, teoría de cuerpos de clases, problema de la torre de cuerpos de clases, grupos profinitos, grupo pro-p, desigualdad de Golod-Shafarevich.

MSC2020: 11R37, 14G32

Contents

Introduction

During the 19th century, class field theory developed around three main themes: relations between abelian extensions and ideal class groups, density theorems for primes using L-functions, and reciprocity laws. As explained in [Lem10], the need to study class field towers originated with the only conjecture of Hilbert concerning the Hilbert class field which turned out to be incorrect, namely the claim that the Hilbert class field of a number field with class number 4 has odd class number.

In fact, Hilbert's approach to proving the reciprocity law for fields with even class number was the following:

1. establishing the quadratic reciprocity law in fields with odd class number.
2. proving it in fields with even class number by applying the reciprocity law in its Hilbert class field which he conjectured implicitly to have odd class number.

In 1916, Philipp Furtwängler realized that the Hilbert 2-class field K_2^1 of a number field K with 2-class group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ need not have an odd class number. He observed that Hilbert's method to prove the quadratic reciprocity law in K would still work if the 2-class field K_2^2 of K_2^1 had odd class number. This made Furtwängler ask the following question: does the p-class field tower of a number field K always terminate?

A negative answer to that question would solve the class field tower problem, which asks whether the class field tower of any number field always terminate. This problem was posed by Furtwängler in 1925 and remained open for almost 40 years, with no clear indication whether the answer should be positive or negative. By class field theory, this problem is equivalent to the following question: *Given a number field K, does it always exist a finite extension L of K such that the ring of integers of L is a principal ideal domain?*.

The class field tower problem could be solved by finding a number field K whose maximal unramified prosolvable extension has infinite degree over K. A convenient way to construct such K would be to prove that for some prime p, the maximal unramified pro-p extension K_p^∞ of K has infinite degree, or equivalently, the Galois group $G_{K,p} = \mathrm{Gal}(K_p^\infty/K)$ is infinite.

A major evidence for the negative answer to the class field tower problem was given by Igor Shafarevich in 1963 (see [Sha63]), where the formula for the minimal number of generators $d(G_{K,p})$ of $G_{K,p}$ and an upper bound for the minimal number of relations $r(G_{K,p})$ were established. A year latter, in 1964, Golod and Shafarevich (see [GS64]) were able to produce counterexamples for the p-class field tower problem by showing that for any finite p-group G, the minimal numbers of generators $d(G)$ and relators $r(G)$ (where G is considered as a pro-p group) are related by the inequality $r(G) > (d(G) - 1)^2/4$. This was improved to $r(G) > d(G)^2/4$ in the subsequent works of Vinberg (see [Vin65]) and Roquette (see [Roq65]). This inequality is known as the Golod-Shafarevich Inequality. Golod and Shafarevich applied this inequality to $G_{K,p}$, that is by definition a pro-p group, and use this to obtain a criterion for the p-class field tower of K to be infinite.

The aim of the thesis is to present a proof of the class field tower problem, as well as provide the necessary framework to be able to formulate this problem and solve it. This thesis has three distinguished parts:

- The first four chapters introduce the group-theoretic base necessary for the class field tower problem. These chapters can be read by anyone who is familiar with the material covered in a regular bachelor's degree in mathematics, and it is mostly self-contained.

  In Chapter 1 we define and explain some properties of profinite groups. In Chapters 2 and 3 we introduce pro-p groups and explain how to present them in terms of generators and relators. Finally, in Chapter 4 we prove the inequality regarding the minimum number of generators and relators mentioned above.

  The main reference used for this part is [Koc02], and [Ers12] has also been an important reference in Chapter 4.

- Chapter 5 introduces the number-theoretic base of the thesis. It assumes some general knowledge about number fields and rings of integers, as well as valuations and completions. Ramification of primes are studied in this chapter, and the concept of Hilbert class field is presented. They main references used for this part are [Mar18] and [Jan96].

- Chapter 6 links the first two parts. The class field tower problem is stated and the theory developed in the first five chapters is used to solve it.

  Here, we will define the notion of p-Hilbert class field (although it will slightly differ from the notion most authors use). We show how the p-class field tower problem solves the class field tower problem, and use the Golod-Shafarevich inequality to give a criterion for K to have infinite class field tower problem. Finally, we will explicitly construct different number fields that satisfy this criterion. The work presented in this part is mostly taken from [Ers12].

Chapter 1

Profinite Groups

Profinite groups are objects of interest for mathematicians working in a variety of areas. They have an important role in number theory, as they are the groups which arise as Galois groups of algebraic field extensions. For this reason, we shall start by discussing the general properties of these groups.

1.1 Profinite Groups

Definition 1.1.1. Let I be a direct set, i.e., a partially ordered set such that, for every $i, j \in I$, there exists a $k \in I$ with $i \leq k$ and $j \leq k$. A *projective system* $P = \{I, G_i, \varphi_i^j\}$ is a collection of objects (groups, rings, topological groups, etc.) $\{G_i\}_{i\in I}$ and collection of morphisms $\varphi_i^j : G_j \to G_i$ for all $i \leq j$ satisfying that φ_i^i is the identity on G_i and $\varphi_i^j = \varphi_j^k \circ \varphi_i^j$ for every $i \leq j \leq k$.

We will mostly be interested in the category of compact topological groups, although we will also work with compact group algebras in Chapter 4. From now on, compact topological groups will be assumed to be Hausdorff. The inverse limit of a projective system can be define in any category using a universal property, although it does not always exist. In the category of compact topological groups, the inverse limit of a projective system always exists and it's unique up to isomorphism.

We can construct the inverse limit in the following way:

Theorem 1.1.2. *Let $P = \{I, G_i, \varphi_i^j\}$ be a projective system of compact topological groups. Then, the inverse limit of P is the group*

$$\varprojlim G_i = \left\{ \prod_{i\in I} g_i \in \prod_{i\in I} G_i \;\middle|\; \varphi_i^j(g_j) = g_i \ \forall\ i \leq j \right\}$$

with the topology induced by the product topology of $\prod G_i$.

Proof. First of all, we should verify that $\varprojlim G_i$ is an object in the category of compact (and Hausdorff) topological groups. $\prod_{i\in I} G_i$ is a topological group for being the product of topological groups, and it is both compact and Hausdorff for being the product of compact and Hausdorff spaces. Automatically, $\varprojlim G_i$ is a Hausdorff topological group and to verify that is compact, we just need to see that is closed in $\prod G_i$. Let $\pi_j : \prod G_i \to G_j$ be the projection morphisms, that are continuous by the definition of the product topology. Then, the functions $\left(\varphi_i^j \circ \pi_j\right) \cdot \pi_i^{-1}$ are also continuous and, since G_i are Hausdorff, $\{1\} \in G_i$ is closed and hence so is $\left(\left(\varphi_i^j \circ \pi_j\right) \cdot \pi_i^{-1}\right)^{-1}(\{1\})$. This implies that $\varprojlim G_i = \bigcap_{i\leq j} \left(\left(\varphi_i^j \circ \pi_j\right) \cdot \pi_i^{-1}\right)^{-1}(\{1\})$ is closed and thus compact.

Finally, one can easily check that the universal property of the inverse limit is fulfilled, taking as the natural projections of the inverse limit the restrictions of the morphisms π_i. □

Definition 1.1.3. Let $P = \{I, G_i, \varphi_i^j\}$ and $Q = \{J, H_i, \psi_i^j\}$ be projective systems of compact topological groups. A *morphism of projective systems of compact topological groups* $\varphi : P \to Q$ consists of a morphism of direct sets $\Phi : J \to I$ and morphisms of compact topological groups $\psi_i : G_{\Phi(i)} \to H_i$ for every $i \in J$ such that the diagram

$$\begin{tikzcd}
G_{\Phi(i)} \arrow[r, "\psi_i"] & H_i \\
G_{\Phi(j)} \arrow[u, "\varphi_{\Phi(i)}^{\Phi(j)}"] \arrow[r, "\psi_j"] & H_j \arrow[u, "\psi_i^j"']
\end{tikzcd}$$

commutes for all $i \leq j$.

A morphism φ of projective systems of compact topological groups induces a morphism $\varphi' : \varprojlim G_i \to \varprojlim H_i$ as follows:

$$\varphi\left(\prod_{i\in I} g_i\right) = \prod_{j\in J} \psi_j\left(g_{\Phi(j)}\right).$$

One can check that inductive limits behave well with exact sequences in the following way:

Theorem 1.1.4. *Let $P = \{I, F_i, \theta_i^j\}$, $Q = \{I, G_i, \varphi_i^j\}$ and $R = \{I, H_i, \psi_i^j\}$ be projective systems of compact topological groups. Let $\{\theta_i : F_i \to G_i \mid i \in I\}$ and $\{\psi_i : F_i \to H_i \mid i \in I\}$ be to families of compact topological group morphisms such that, for all $i \in I$,*

$$1 \longrightarrow F_i \xrightarrow{\theta_i} G_i \xrightarrow{\psi_i} H_i \longrightarrow 1$$

is an exact sequence. Then, if θ and ψ are the morphisms induced by $\{\theta_i\}$ and $\{\psi_i\}$ respectively, the sequence

$$1 \longrightarrow \varprojlim F_i \xrightarrow{\theta} \varprojlim G_i \xrightarrow{\psi} \varprojlim H_i \longrightarrow 1$$

is also exact.

Proof. The proof of this theorem can be found in page 6 in [Koc02]. □

Definition 1.1.5. A *profinite group* is a topological group that can be realized as a projective limit of discrete finite groups.

Remark. Since finite discrete groups are compact topological groups, so are profinite groups.

We now will state some properties of profinite groups. The following lemma holds not only for profinite groups, but for all compact topological groups:

Lemma 1.1.6. *Let G be a compact topological group and $H \subseteq G$ a subgroup. Then, the following properties hold:*

(i) H is open $\iff$ H is closed and $[G : H] < \infty$.

(ii) If H is an open normal subgroup of G, then G/H is a discrete group with the quotient topology.

Proof. Fix any $g \in G$. Since the multiplication map is continuous, so is the translation map defined by $a \mapsto ga$. Moreover, this map is an homeomorphism, and hence is both open and closed.

Suppose H is open and consider the cosets $\{g_iH \mid i \in I\}$ for some index set I. Suppose also that $g_1 = 1$. We can write G as a disjoint union of its cosets:

$$G = H \cup \left(\bigcup_{i \in I \setminus \{1\}} g_iH \right). \tag{1.1}$$

As the translation map is open, all cosets are open. Hence, Equation (1.1) defines an open covering of G and, since G is compact, there exist only a finite number of cosets. In addition, $\bigcup_{i \in I \setminus \{1\}} g_iH$ is open and hence H is closed.

Suppose now that G is closed and $[G : H] \leq \infty$. Again, write G as a disjoint union of cosets:

$$G = H \cup g_2H \cup \ldots \cup g_nH.$$

Since the translation map is closed, the different cosets are closed and $H = G \setminus (g_2H \cup \ldots \cup g_nH)$ is open.

To prove (ii), one just needs to realize that, since H is open, gH are also open and hence each point in the quotient G/H is open when G/H is given the quotient topology. □

Definition 1.1.7. Let G be a topological group. An *open normal neighbourhood basis* at $1 \in G$ is a neighbourhood basis at 1 consisting of open normal subgroups of G.

We can now prove the following theorem:

Theorem 1.1.8. *Let $\{I, G_i, \varphi_i^j\}$ be a projective system of finite discrete topological groups and $G = \varprojlim G_i$ a profinite group. Let $\pi_i : G \to G_i$ be the natural projections. Then, $\{\ker(\pi_i) \bigm| i \in I\}$ is an open normal neighbourhood basis at the unit element $1 \in G$.*

Proof. As G_i are discrete, $\{1\} \subseteq G_i$ are open subgroups. It follows that $\ker(\pi_i) = \pi_i^{-1}(\{1\})$ are open normal subgroups.

Let $U \subseteq G$ be an open set containing $1 \in G$. A base of the topology of $\prod G_i$ is given by the sets of the form

$$\prod_{i \in J} U_i \times \prod_{i \in I \setminus J} G_i,$$

where $U_i \subseteq G_i$ is any subset containing $1 \in G_i$ and $J \subseteq I$ is finite. This base on $\prod G_i$ induce a base of the topology of G. Take a basic open $V = \left(\prod_{i \in J} U_i \times \prod_{i \in I \setminus J} G_i\right) \cap G$ with $1 \in V \subseteq U$. Since I is a direct set and J is finite, there exists $m \in I$ with $i \leq m$ for all $i \in J$. Then, $\ker(\pi_m)$ must have a 1 in the m-th component and hence also in the i-th component for all $i \leq m$. So, $1 \in \ker(\pi_m) \subseteq V \subseteq U$. □

The following proposition gives a characterization of profinite groups:

Theorem 1.1.9. *Let G be a compact topological group. The following assertions are equivalent:*

(i) G is profinite.

(ii) There exist a set $\mathfrak{U}$ of open normal subgroups of G that form a basis at the unit element in G.

Proof. We have already seen that (i) implies (ii). Assume (ii) holds. First of all, we turn $\mathfrak{U}$ into a direct set by saying that $U \leq U' \iff U' \subseteq U$. This set is direct since, if $U, U' \in \mathfrak{U}$, then $U \cap U'$ is an open neighbourhood at 1, so it must contain an element of $\mathfrak{U}$. Now, we consider the projective systems $P = \{\mathfrak{U}, F_U = U, \theta_U^{U'}\}$, $Q = \{\mathfrak{U}, G_U = G, \mathrm{id}_G\}$ and $R = \{\mathfrak{U}, H_U = G/U, \psi_U^{U'}\}$, where $\theta_U^{U'}$ is the inclusion $U' \hookrightarrow U$ and and $\psi_U^{U'} : G/U' \twoheadrightarrow G/U$ is the morphism that maps $gU' \mapsto gU$ (this is well defined for $U \leq U'$). By Lemma 1.1.6, G/U are finite discrete topological groups and hence P, Q and R are projective systems of compact topological groups. Consider the inclusion morphisms $\theta_U : U \hookrightarrow G$ and the quotient morphisms $\psi_U : G \twoheadrightarrow G/U$. Then, for all $U \in \mathfrak{U}$, we have an exact sequence

$$1 \longrightarrow U \xrightarrow{\theta_U} G \xrightarrow{\psi_U} {}^{G}\!/\!{}_{U} \longrightarrow 1$$

that, by Theorem 1.1.4, induces an exact sequence

$$1 \longrightarrow \varprojlim_{U \in \mathfrak{U}} U \xrightarrow{\theta} \varprojlim_{U \in \mathfrak{U}} G \xrightarrow{\psi} \varprojlim_{U \in \mathfrak{U}} {}^{G}\!/\!{}_{U} \longrightarrow 1.$$

Clearly, $\varprojlim_{U \in \mathfrak{U}} G = G$. One can show that $\varprojlim_{U \in \mathfrak{U}} U = \{1\}$ as G is Hausdorff. With this, we obtain the exact sequence

$$1 \longrightarrow G \xrightarrow{\psi} \varprojlim_{U \in \mathfrak{U}} {}^{G}\!/\!{}_{U} \longrightarrow 1.$$

This implies that $G \cong \varprojlim_{U \in \mathfrak{U}} G/U$ and hence G is profinite. □

From the proof of this theorem we deduce the following statement:

Corollary 1.1.10. *Let G be a profinite group and let $\mathfrak{U}$ be a set of open normal subgroups of G that form a basis at 1. Then $G \cong \varprojlim_{U \in \mathfrak{U}} G/U$.*

Theorem 1.1.11. *Direct products and fibered products exist in the category of profinite groups.*

1.2 Subgroups and Quotient Groups

Let G be a profinite group. In the following, $\mathfrak{U}_G$ will denote the set of all open normal subgroups of G.

Lemma 1.2.1. *Let G be a profinite group and $V \subseteq G$ a closed subgroup. Then, V is a profinite group.*

Proof. Clearly, V is a Hausdorff topological group with the induced topology. Since V is closed and G is compact, V is compact. Consider the set $\mathfrak{U} = \{V \cap U \mid U \in \mathfrak{U}_G\}$. Since, $U \lhd G$, $V \cap U \lhd V$. The subgroups $V \cap U$ are open in V with the induce topology. Hence, $\mathfrak{U}$ is an open normal neighbourhood at $1 \in V$ and, by Theorem 1.1.9, V is a profinite group. □

Lemma 1.2.2. *Let G be a profinite group and N a closed normal subgroup. Then G/N is a profinite group.*

Proof. G/N is a topological group that is compact with the induced topology. Since, N is closed, G/N is also Hausdorff and thus it is a compact topological group (the proof of this last statement can be found on Proposition 1.27 in [Kra20]). Take $U \in \mathfrak{U}_G$. Then, $UN = \bigcup_{g \in N} Ug$ is open and hence UN/N is open in G/N. In addition, UN/N is normal in G/N. Therefore, $\{UN/N \mid U \in \mathfrak{U}_G\}$ is an open normal neighbourhood basis at $1 \in G/N$ and thus G/N is profinite. □

The following theorem guarantees the existence of a *continuous section*, that is, a continuous system of representatives of cosets with respect to a subgroup.

Theorem 1.2.3. *Let G be a profinite group and $H \subseteq G$ a subgroup. Then, there is a continuous section $\sigma : G/H \to G$ such that $\sigma(H) = 1$, that is, a continuous map $\sigma : G/H \to G$ between topological spaces such that the composition*

$$G/H \xrightarrow{\sigma} G \xrightarrow{\pi} G/H$$

is the identity map.

Proof. The proof of this theorem can be find in pages 9-10 in [Koc02]. □

This theorem will be used in the proof of Theorem 2.4.9.

Chapter 2

Free pro-p Groups

In the following, p will denote a prime number. We restrict our considerations on a special type of profinite groups called pro-p groups, which describe the Galois groups of p-extensions. We begin by studying free pro-p groups.

2.1 Construction of a Free pro-p Group

Definition 2.1.1. A *pro-p group* is a compact topological group that can be realized as a projective limit of discrete finite p-groups.

Definition 2.1.2. Let G be a pro-p group. A *system of generators* of G is a subset E of G with the following properties:

(i) G is the smallest closed subgroup containing E, i.e., $G = \overline{\langle E \rangle}$ is the topological closure of the group generated by E.

(ii) every neighbourhood of $1 \in G$ contains almost all (all except finitely many) elements of E.

Definition 2.1.3. A system of generators E of a pro-p group G is called *minimal* if no proper subset of E is a system of generators of G.

We shall see that systems of generators exist in any pro-p group. To do that, we begin by constructing a free pro-p group.

Lemma 2.1.4. *Let I be an index set and let F_I be the free group with generators $\{s_i \mid i \in I\}$. Let $\mathfrak{U}$ be the set of all normal subgroups N of F_I satisfying that:*

(i) $[F_I : N]$ is a power of p.

(ii) almost all elements of $\{s_i \mid i \in I\}$ are in N.

Then $\{F_I/N \mid N \in \mathfrak{U}\}$ is a projective system of finite p-groups.

Proof. We begin by showing that $\mathfrak{U}$ is closed by finite intersections. Take $N_1, N_2 \in \mathfrak{U}$. Clearly, $N_1 \cap N_2 \lhd F_I$ and satisfies the property (ii). It remains to see that the index of $N_1 \cap N_2$ in F_I is a power of p. By the third isomorphism theorem, we have

$$\frac{F_I \diagup N_1 \cap N_2}{N_1 \diagup N_1 \cap N_2} \cong F_I \diagup N_1,$$

so $\left|F_I/N_1 \cap N_2\right| = \left|F_I/N_1\right|\left|N_1/N_2 \cap N_2\right|$. By the second isomorphism theorem,

$$N_1 \diagup N_1 \cap N_2 \cong N_1N_2 \diagup N_2.$$

This implies that $\left|F_I/N_1 \cap N_2\right| = \left|F_I/N_1\right|\left|N_1N_2/N_2\right|$. By hypothesis, $\left|F_I/N_1\right|$ is a power of p and since $N_1N_2/N_2 \hookrightarrow F_I/N_2$ and $\left|F_I/N_1\right|$ is a power of p, we obtain that $\left|N_1N_2/N_2\right|$ is also a power of p. Hence, the index of $N_1 \cap N_2$ in F_I is a power of p.

Now, we turn $\mathfrak{U}$ into a direct set by saying that $N_1 \leq N_2$ if, and only if, $N_2 \subseteq N_1$ (this is indeed a direct set since $N_1, N_2 \leq N_1 \cap N_2$). The groups F_I/N are finite p-groups, and the natural projections $F_I/N_1 \twoheadrightarrow F_I/N_2$ for $N_2 \leq N_1$ make $\{F_I/N \mid N \in \mathfrak{U}\}$ a projective system. □

Definition 2.1.5. Let $\mathfrak{U}$ be as in Lemma 2.1.4. A *free pro-p group with system of generators* $\{s_i \mid i \in I\}$ is the pro-p group

$$F(I) := \varprojlim_{N \in \mathfrak{U}} F_I \diagup N,$$

where F_I/N are given the discrete topology.

To justify this name, we should see that $\{s_i \mid i \in I\}$ is indeed a system of generators of $F(I)$. We will do this later on. Let's now see that we can embed F_I into $F(I)$. Consider the following group morphism:

$$\begin{aligned} \varphi\colon F_I &\longrightarrow F(I) \\ g &\longmapsto \prod_{N \in \mathfrak{U}} gN \end{aligned}$$

We will see that φ is invective. First of all, let's prove the following lemma:

Lemma 2.1.6. *The image of F_I by φ is dense in $F(I)$.*

Proof. To prove this statement, we will see that the intersection of $\varphi(F_I)$ with any nonempty open set is nonempty. Let $U \subseteq F(I)$ be a nonempty open set. As we saw on Theorem 1.1.8, $\{\ker(\pi_N) \mid N \in \mathfrak{U}\}$ is an open neighbourhood basis at the unit element $1 \in F(I)$. Recall that in a topological group G, for any subset $X \subseteq G$ and any element $g \in G$, X is open (or closed) if and only if its translation gX is open (or closed). This fact implies that $\{\omega \ker(\pi_N) \mid \omega \in F(I), N \in \mathfrak{U}\}$ is a base for the topology of $F(I)$. Hence, there exist $\omega_0 \in F(I)$ and $N_0 \in \mathfrak{U}$ such that $\omega_0 \ker(\pi_{N_0}) \subseteq U$.

Write $\omega_0 = \prod_{N\in\mathfrak{U}} g_N N$ and let $g_0 \in F_I$ be a representative for the component of ω_0 corresponding to N_0. Then, $\varphi(g_0) = \prod_{N\in\mathfrak{U}} g_0 N$, and $\omega_0^{-1}\varphi(g_0) = \prod_{N\in\mathfrak{U}} g_N^{-1} g_0 N$ has a 1 in the component corresponding to N_0. This implies that $\omega_0^{-1}\varphi(g_0) \in \ker(\pi_{N_0})$ and hence $\varphi(g_0) \in \omega_0 \ker(\pi_{N_0}) \subseteq U$. As $\varphi(g_0) \in \varphi(F_I)$, we see that $U \cap \varphi(F_I) \neq \emptyset$. □

In the next section we will prove some auxiliary results in order to show that φ is injective.

2.2 The Magnus Group Algebra

In this section we will start by defining the concept of Magnus algebra and use it to prove the injectivity of the morphism φ defined in the previous section. This result will help us justify that $\{s_i \mid i \in I\}$ is a minimal system of generators of $F(I)$.

Definition 2.2.1. Let Λ be a ring with unity and let I be an index set. The *Magnus algebra* $\Lambda(I)$ is the Λ-algebra of formal power series in non-commutative variables x_i, $i \in I$, with coefficients in Λ.

Take $\Lambda = \mathbb{F}_p$ and define a morphism of groups ψ from the free group F_I generated by $\{s_i \mid i \in I\}$ to the the unit group of $\mathbb{F}_p(I)$ by putting

$$\psi(s_i) = 1 + x_i, \qquad \psi(s_i^{-1}) = (1+x_i)^{-1} = \sum_{\nu}^{\infty}(-x_i)^{\nu}.$$

Lemma 2.2.2. *The map ψ is injective.*

Proof. Let

$$g := s_{i_1}^{a_1} \cdots s_{i_k}^{a_k} \neq 1, \quad a_j \in \mathbb{Z},$$

be an element of F_I in a simplified presentation (that is, $i_j \neq i_{j+1}$ and $a_j \neq 0$). Since $g \neq 1$, we may assume that $k \geq 1$. We want to show that

$$\psi(g) = \psi(s_{i_1}^{a_1} \cdots s_{i_k}^{a_k}) = (1+x_{i_1})^{a_1} \cdots (1+x_{i_k})^{a_k} \neq 1.$$

Using the generalization of the binomial expression for integer powers, we get that

$$\psi(g) = \left(\sum_{b_1=0}^{\infty} \binom{a_1}{b_1} x_{i_1}^{b_1}\right) \cdots \left(\sum_{b_k=0}^{\infty} \binom{a_k}{b_k} x_{i_k}^{b_k}\right) = \sum_{b_1,\dots,b_k=0}^{\infty} \binom{a_1}{b_1} \cdots \binom{a_k}{b_k} x_{i_1}^{b_1} \cdots x_{i_k}^{b_k},$$

where $\binom{a_j}{b_j} \in \mathbb{F}_p$. For every $j = 1, \dots, k$, let b_j be the maximum power of p dividing a_j. Then, $\binom{a_j}{b_j} \neq 0$ and the coefficient of $x_{i_1}^{b_1} \cdots x_{i_k}^{b_k}$ does not vanish. Hence, $\psi(g) \neq 1$. □

Theorem 2.2.3. *The map $\varphi : F_I \to F(I)$ defined in the previous section is injective.*

Proof. From the definition of φ, it's easy to see that

$$g \in \ker(\varphi) \iff gN = 1N \ \ \forall\, N \in \mathfrak{U} \iff g \in N \ \ \forall\, N \in \mathfrak{U},$$

so $\ker(\varphi) = \bigcap_{N\in\mathfrak{U}} N$. Hence, proving that φ is injective is equivalent to proving that $\bigcap_{N\in\mathfrak{U}} = \{1\}$.

Let's suppose first that I is finite. Let $B^\nu \subset \mathbb{F}_p(I),\ \nu \geq 1$, be the ideal consisting of all power series all of whose terms have degree at least ν. Clearly, $\left|\mathbb{F}_p(I)/B^\nu\right|$ is finite and a power of p for all $\nu \geq 1$. Observe that $\bigcap_{\nu=1}^{\infty} B^\nu = \{0\}$. Now define $N_\nu := \{g \in F_I \mid \psi(g) - 1 \in B^\nu\}$. We claim that N_ν is a normal subgroup $F(I)$. This can be seen from the identity:

$$ab - 1 = (a-1)(b-1) + a - 1 + b - 1.$$

This identity clearly implies that if $g_1, g_2 \in N_\nu$, then g_1g_2 and g_1^{-1} are in N_ν. To see that N_ν is normal, take $g \in N_\nu$ and $h \in F_I$ and apply the previous identity two times:

$$\begin{gathered}\psi(hgh^{-1}) - 1 = (\psi(h)-1)(\psi(g)-1)(\psi(h)^{-1}-1) + (\psi(h)-1)(\psi(g)-1) + \\ +(\psi(h)-1)(\psi(h)^{-1}-1) + (\psi(g)-1)(\psi(h)^{-1}-1) + \psi(h) - 1 + \psi(g) - 1 + \\ +\psi(h)^{-1} - 1 = (\psi(h)-1)(\psi(g)-1)(\psi(h)^{-1}-1) + (\psi(h)-1)(\psi(g)-1) + \\ +(\psi(g)-1)(\psi(h)^{-1}-1) + \psi(g) - 1.\end{gathered}$$

From this expression see that $\psi(hgh^{-1}) - 1 \in B^\nu$ and so $hgh^{-1} \in N_\nu$. Applying Lemma 2.2.2, we see that $\bigcap_{\nu\geq 1} N_\nu = \{1\}$, as

$$\begin{gathered}g \in \bigcap_{\nu\geq 1} N_\nu \iff g \in N_\nu \ \ \forall\, \nu \geq 1 \iff \psi(g) - 1 \in B^\nu \ \ \forall\, \nu \geq 1 \iff \\ \iff \psi(g) - 1 \in \bigcap_{\nu\geq 1} B^\nu = \{0\} \iff \psi(g) = 1 \iff g = 1.\end{gathered}$$

Let's now show by induction on ν that the index of N_ν is a power of p. For $\nu = 1$, we have that $N_\nu = F_I$. Now observe that the morphism $\psi - 1$ induces a monomorphism $N_\nu/N_{\nu+1} \hookrightarrow B^\nu/B^{\nu+1}$. Since $B^\nu/B^{\nu+1}$ is a power of p, so is $N_\nu/N_{\nu+1}$.

We have seen that $\{N_\nu \mid \nu \geq 1\}$ is a set of normal subgroups of F_I with $[F_I : N_\nu]$ a power of p that satisfy that their intersection is trivial. Since $\{N_\nu \mid \nu \geq 1\} \subseteq \mathfrak{U}$, the intersection of the subgroups of $\mathfrak{U}$ is also trivial and hence φ is injective, as we wanted to show.

Finally, assume that I is infinite. Consider the set of all normal subgroups $N_{\nu,J}$ of F_I generated by the sets

$$N_\nu(J), \quad \{s_i \mid i \in I \setminus J\},$$

where $J \subset I$ is finite and $N_\nu(J) := \{g \in F_J \subset F_I \mid \psi(g) - 1 \in B^\nu\}$. Then, $N_{\nu,J} \in \mathfrak{U}$ and $\bigcap_{\nu,J} N_{\nu,J} = \{1\}$, which proves the claim. □

As φ is injective, we can identify F_I with it image inside $F(I)$. We will use the abuse of notation $g = \varphi(g)$ for the elements of F_I. With this identification, we can prove the following corollary:

Corollary 2.2.4. *The set* $\{s_i \in F_I \subseteq F(I) \mid i \in I\}$ *is a minimal system of generators of* $F(I)$.

Proof. As we showed in Lemma 2.1.6, F_I is dens in $F(I)$, so $F(I)$ is the topological closure of the group generated by $\{s_i \mid i \in I\}$. This shows that property (i) of Definition 2.1.2 holds. Lets see the property (ii) of Definition 2.1.2: take a neighbourhood U of 1. Since $\{\ker(\pi_N) \mid N \in \mathfrak{U}\}$ is a neighbourhood bais of 1, there exists $N_0 \in \mathfrak{U}$ with $N_0 \subseteq U$. Now remember that the subgroups $N \in \mathfrak{U}$ satisfy by construction that almost all elements of $\{s_i \mid i \in I\}$ are in N. Hence, all but finitely many $s_i \in N_0$. s_i is seen as an element of $F(I)$ though the embedding $\varphi(s_i) = \prod_{N \in \mathfrak{U}} s_i N$. So if $s_i \in N_0$, then $s_i \in \ker(\pi_{N_0}) \subseteq U$. This shows that almost all s_i are in U.

We have seen that $\{s_i \mid i \in I\}$ is a system of generators of $F(I)$. The minimality of this system is a consequence of the fact that F_I is a free group. □

2.3 Abelian pro-p Groups

In this section we will state some facts about abelian pro-p groups, although we will skip most of the proofs since we would required a deep study of the Pontryagin's duality. Abelian pro-p groups are used study some properties of arbitrary pro-p groups and will appear in the following sections. Moreover, they are used to describe the Galois group of abelian p-extensions, which will be used in Chapter 6.

Definition 2.3.1. Let G be an abelian profinite group. The *Pontryagin dual group* $\widehat{G}$ of G is the group of all morphisms of topological groups from G to the circle group $\mathbb{S}^1 \cong \mathbb{R}/\mathbb{Z}$ with the usual topology.

Lemma 2.3.2. *Let G be an abelian profinite group and $\chi \in \widehat{G}$. Then,* $\operatorname{Im}(\chi) \subseteq \mathbb{Q}/\mathbb{Z}$.

Proof. Let $U \subseteq \mathbb{S}^1$ be an open neighbourhood of $1 \in \mathbb{S}^1$ such that the only subgroup contained in U is $\{1\}$ (such a neighbourhood clearly exists). Then $\chi^{-1}(U)$ is an open neighbourhood of $1 \in G$ and, by Theorem 1.1.9, there exist an open normal subgroup $N \subseteq G$ such that $N \subseteq U$. Then, $\chi(N) \subseteq U$ is a subgroup, and hence is trivial. This implies that $N \subseteq \ker(\chi)$. By Lemma 1.1.6, G/N is finite and, since $[G : N] = [G : \ker(\chi)][\ker(\chi) : N]$, $G/\ker(\chi)$ is also finite. Since $\operatorname{Im}(\chi) \cong G/\ker(\chi)$, we have that $\operatorname{Im}(\chi) \subseteq \mathbb{S}^1$ is finite. $\operatorname{Im}(\chi)$ is a subgroup of the multiplicative group of $\mathbb{C}$. Thus, $\operatorname{Im}(\chi)$ is cyclic and therefore contained in $\mathbb{Q}/\mathbb{Z}$. □

This lemma tells us that $\widehat{G}$ is torsion. Normally, the Pontryagin dual of a locally compact abelian group is seen as a topological group with the topology of uniform convergence on compact sets. For an abelian profinite group, $\widehat{G}$ is an abelian discrete torsion group. More precisely, we have the following statement:

Theorem 2.3.3. *$G \to \widehat{G}$ is an exact contravariant functor from the category of abelian profinite groups to the category of abelian discrete torsion groups and vice versa.*

Theorem 2.3.4 (Pontryagin duality theorem)**.** *Let G be an abelian profinite group. Then, there is a canonical isomorphism $G \cong \widehat{\widehat{G}}$.*

In the case of pro-p groups, the Pontryagin dual of an abelian pro-p group is a discrete abelian p-primary torsion group, i.e., a discrete abelian group whose elements have order a power of p.

Suppose G is an abelian pro-p group with exponent p. Then, its dual Pontryagin group has a natural structure of an $\mathbb{F}_p$-vector space. If $a \in \mathbb{F}_p$ and $\chi \in \widehat{G}$, we define

$$(a \cdot \chi)(g) := (\chi(g))^a$$

Under this consideration, the following result holds:

Theorem 2.3.5. *Let G be an abelian pro-p group with exponent p. Let $\{\chi_i \mid i \in I\}$ be an $\mathbb{F}_p$-basis of $\widehat{G}$. The elements $s_i \in G$, $i \in I$, with*

$$\langle s_i, \chi_j \rangle := \chi_j(s_i) = e^{\frac{2\pi i}{p}} \delta_{ij}$$

form a minimal system of generators of G, and G is isomorphic to $\prod_I \mathbb{F}_p$.

2.4 First Characterization of Free pro-p Groups

In this section we will give a characterization of free pro-p groups and use it to prove that all pro-p groups have a system of generators. From now on, if not specified, a homomorphism will refer to a homomorphism of pro-p groups, i.e., a continuous group homomorphism. These morphisms have the following property:

Lemma 2.4.1. *Let F and G be pro-p groups and $\varphi : G \to F$ a bijective morphism. Then, φ is an isomorphism.*

Proof. We now that φ is an isomorphism of groups. Since F is compact and G is Hausdorff, φ is an homeomorphism and thus an isomorphism of pro-p groups. □

Lemma 2.4.2. *Let G be a pro-p group and N an open normal subgroup. Then G/N is a finite discrete p-group.*

Proof. We already know that G/N is a finite discrete group, so it suffices to prove that its cardinality is a power of p. Suppose $G = \varprojlim_{i \in I} G_i$, with G_i discrete finite p-groups. By Theorem 1.1.8, there exists $i \in I$ with $\ker(\pi_i) \subseteq N$, where $\pi_i : G \to G_i$ is the natural projection. Then, $[G : \ker(\pi_i)] = [G : N][N : \ker(\pi_i)]$. Since $G/\ker(\pi_i) \cong G_i$ is a finite p-group, $[G : N]$ must be a power of p. □

Theorem 2.4.3. *Let $F(I)$ be a free pro-p group with system of generators $\{s_i \bigm| i \in I\}$. Let G be a pro-p, and $\{t_i \bigm| i \in I\}$ a subset of G satisfying that every neighbourhood of $1 \in G$ contains almost all elements of $\{t_i \bigm| i \in I\}$.*

Then, there exists a unique homomorphism $\varphi : F(I) \to G$ such that

$$\varphi(s_i) = t_i \quad \forall\, i \in I. \tag{2.1}$$

Proof. Let's first prove the existence. Equation (2.1) can be extended uniquely to a group homomorphism $\psi : F_I \to G$, as F_I is the free group generated by the s_i. Let $\mathfrak{U}$ be the set defined in Lemma 2.1.4 and let $\mathfrak{U}_G$ be the set of all open normal subgroups of G. Take $U \in \mathfrak{U}_G$ and consider the induced group morphism

$$\overline{\psi}_U : F_I \to {}^{G}\!/_{U}.$$

Let $\Phi(U)$ be the kernel of this map. We claim that $\Phi(U) \in \mathfrak{U}$. First of all, it's clear that $\Phi(U) \lhd F_I$. By construction $\bigl|G/U\bigr|$ is a power of p, and hence so is $\bigl|F_I/\Phi(U)\bigr|$. Finally, by hypothesis, U contains almost all elements of $\{t_i \bigm| i \in I\}$ and, since ψ maps s_i to t_i, almost all $s_i \in \Phi(U)$. This proves the claim.

Consider the projective systems $\bigl\{\mathfrak{U}, F_I/N, \alpha_N^{N'}\bigr\}$ and $\bigl\{\mathfrak{U}_G, G/U, \beta_U^{U'}\bigr\}$, where the order of $\mathfrak{U}$ and $\mathfrak{U}_G$ is defined by $S \le S'$ if, and only if, $S' \subseteq S$, and the morphisms $\alpha_N^{N'}$ and $\beta_U^{U'}$ are the natural projections

$$\alpha_N^{N'} : {}^{F_I}\!/_{N'} \twoheadrightarrow {}^{F_I}\!/_{N}, \qquad \beta_U^{U'} : {}^{G}\!/_{U'} \twoheadrightarrow {}^{G}\!/_{U}.$$

As we have seen, G/U are finite discrete p-groups since U are open normal subgroups of G and we give F_I/N the discrete topology. Then, the morphism of direct sets

$$\begin{array}{rccc} \Phi\colon & \mathfrak{U}_G & \longrightarrow & \mathfrak{U} \\ & U & \longmapsto & \Phi(U) = \ker(\overline{\psi}_U) \end{array}$$

and the morphism of compact topological p-groups

$$\begin{array}{rccc} \tilde{\psi}_U\colon & {}^{F_I}\!/_{\Phi(U)} & \longrightarrow & {}^{G}\!/_{U} \\ & g\Phi(U) & \longmapsto & \psi(g)U \end{array}$$

define a morphism of projective systems. As we saw on Section 1.1, this defines a morphism of pro-p groups

$$F(I) = \varprojlim {}^{F_I}\!/_{N} \longrightarrow \varprojlim {}^{G}\!/_{U} \cong G$$

which maps $\prod_{N\in\mathfrak{U}} g_N N$ to $\prod_{U\in\mathfrak{U}_G} \psi(g_{\Phi(U)})U$. This morphism has the desired properties.

Let's now see the uniqueness of this morphism. Let φ and φ' be to different morphisms satisfying the property. We will obtain a contradiction. Since $\varphi \neq \varphi'$, there exist $g \in F(I)$ such that $\varphi(g) \neq \varphi'(g)$. Since G is Hausdorff, there exist two disjoint open subsets $U, U' \subseteq G$ with $\varphi(g) \in U$ and $\varphi'(g) \in U'$. Define $V = \varphi^{-1}(U)$ and $V' = \varphi'^{-1}(U')$, that are open since φ and φ' are continuous. Then, its intersection is open and nonempty because $g \in V \cap V'$. Using that F_I is dens in $F(I)$, we deduce that the intersection of $V \cap V'$ and F_I is nonempty. Let $h \in F_I \cap V \cap V'$. As both φ and φ' agree on $\{s_i \mid i \in I\}$, they also agree on F_I. Hence, $\varphi(h) = \varphi'(h)$. This is a contradiction because $\varphi(h) \in U$ and $\varphi'(h) \in U'$, but the sets U and U' are disjoint. □

Definition 2.4.4. Let G be a pro-p group. We define the *Frattini subgroup* of G, denoted by $\mathrm{Fr}(G)$, as the intersection of all maximal open subgroups of G. This group can be written as the close normal subgroup generated by the commutators and the p^{th}-powers, i.e., $\mathrm{Fr}(G) = \overline{G^p[G,G]}$.

The equivalence of these two ways to define the Frattini subgroups is proved on page 6 in [CT17].

Remark. The Frattini subgroup is the smallest closed normal subgroup N of G such that G/N is an elementary abelian p-group, i.e., is an abelian group with exponent p.

Before proving the next theorem, we will state a lemma that is a direct consequence of the first Sylow theorem. The proof of this lemma can be find in [Hal59].

Lemma 2.4.5. *Every subgroup of a p-group P of order p^m is contained in a maximal subgroup of order p^{m-1}, and all the maximal subgroups of P are normal subgroups.*

Theorem 2.4.6. *Let G_1 and G_2 be pro-p groups, and let $\varphi : G_1 \to G_2$ be homomorphism. Then, φ is surjective if, and only if, the induced map $\varphi_* : G_1/\mathrm{Fr}(G_1) \to G_2/\mathrm{Fr}(G_2)$ is surjective.*

Proof. Firs notice that φ_* is well defined since $\varphi(\mathrm{Fr}(G_1)) \subseteq \mathrm{Fr}(G_2)$. It is clear that if φ is surjective, so is φ_*.

Now suppose that φ is not surjective, i.e., $\varphi(G_1) \neq G_2$. For an open normal subgroup U of G_2, denote $\pi_U : G_2 \twoheadrightarrow G_2/U$ the natural projection. We claim that there exist $U \in \mathfrak{U}_{G_2}$ such that $\pi_U(\varphi(G_1)) \neq \pi_U(G_2) = G_2/U$. Recall that $G_2 = \varprojlim_{U \in \mathfrak{U}_{G_2}} G_2/U$. By the second isomorphism theorem,

$$\pi_U(\varphi(G_1)) = {\varphi(G_1)U}\big/{U} \cong {\varphi(G_1)}\big/{\varphi(G_1) \cap U}.$$

The set $\{\varphi(G_1) \cap U \mid U \in \mathfrak{U}_{G_2}\}$ is an open normal neighbourhood basis of $1 \in \varphi(G_1)$, so $\varphi(G_1)$ is profinite and equal to $\varprojlim_{U \in \mathfrak{U}_{G_2}} \varphi(G_1)/\varphi(G_1) \cap U$. Therefore, if $\pi_U(\varphi(G_1)) = \pi_U(G_2)$ for all $U \in \mathfrak{U}_{G_2}$, then

$$\varphi(G_1) = \varprojlim_{U \in \mathfrak{U}_{G_2}} {\varphi(G_1)}\big/{\varphi(G_1) \cap U} = \varprojlim_{U \in \mathfrak{U}_{G_2}} {G_2}\big/{U} = G_2,$$

which would contradict our hypothesis. Hence, there exist $U \in \mathfrak{U}_{G_2}$ with

$$\varphi(G_1)U\big/_U \neq G_2\big/_U.$$

Observe now that since U is a normal open subgroup, G_2/U is a finite p-group. By the Lemma 2.4.5, $\varphi(G_1)U/U$ is contained in a normal subgroup G'/U of index p of G_2/U. Therefore, $G' \lhd G_2$ and $[G_2 : G'] = p$. This implies that $\mathrm{Fr}(G_2) \subseteq G'$ and

$$\varphi_* \left(G_1\big/_{\mathrm{Fr}(G_1)} \right) \subseteq G'\big/_{\mathrm{Fr}(G_2)} \subsetneq G_2\big/_{\mathrm{Fr}(G_2)},$$

i.e., φ_* is not surjective. □

We know come to the characterization of free pro-p groups. Before, we will define the concept of group extension for a pro-p group.

Definition 2.4.7. Let G and H be pro-p groups. A *pro-p group extension* of G by H is given by a pro-p group $\overline{H}$ and an exact sequence

$$1 \longrightarrow H \longrightarrow \overline{H} \longrightarrow G \longrightarrow 1$$

in the category of pro-p groups. By Lemma 2.4.1, this allow us to identify (isomorphically) H as a subgroup of $\overline{H}$ such that $\overline{H}/H \cong G$.

Definition 2.4.8. We say that an extension of pro-p groups

$$1 \longrightarrow H \longrightarrow \overline{H} \xrightarrow{\varphi} G \longrightarrow 1$$

splits if there exist a morphism $\sigma : G \to \overline{H}$ such that $\varphi \circ \sigma = \mathrm{id}_G$.

Theorem 2.4.9. *Let G be a pro-p group. The following assertions are equivalent:*

(i) G is a free pro-p group.

(ii) every pro-p group extension of G by a pro-p group H splits.

(iii) G is a projective object in the category of pro-p groups.

Proof. (i) implies (ii): Let G be a free pro-p group with system of generators $\{s_i \mid i \in I\}$. Let

$$1 \longrightarrow H \longrightarrow \overline{H} \xrightarrow{\varphi} G \longrightarrow 1 \tag{2.2}$$

be a pro-p group extension. Since $G \cong \overline{H}/H$, by Theorem 1.2.3, there exist a continuous section $\sigma : G \to \overline{H}$. Now, we apply Theorem 2.4.3 to thee free pro-p group G, the pro-p group $\overline{H}$ and the subset $\{\sigma(s_i) \mid i \in I\} \subseteq \overline{H}$. We find that there exist a unique continuous morphism of groups $\sigma' : G \to \overline{H}$ such that $\sigma'(s_i) = \sigma(s_i)$ for all $i \in I$. The composition $\varphi \circ \sigma' : G \to G$ is also a continuous morphism of groups that lets s_i fixed and, by the uniqueness condition of Theorem 2.4.3, $\varphi \circ \sigma' = \mathrm{id}$ and hence the exact sequence (2.2) splits.

(ii) implies (iii): Let G, G_1, G_2 be pro-p groups, $f : G \to G_1$ a morphism and $e : G_2 \to G_1$ and epimorphism, as seen in the following diagram

$$\begin{tikzcd}
& G \arrow[d, "f"] \\
G_2 \arrow[r, two heads, "e"] & G_1
\end{tikzcd} \tag{2.3}$$

We wish to define a morphism $\overline{f} : G \to G_2$ such that $e \circ \overline{f} = f$. Consider the fibered product of G and G_2. This fibered product consists of the set $G_2 \times_{G_1} G = \{(g_2, g) \in G_2 \times G \mid e(g_2) = f(g)\}$ and the projection morphisms $\varphi_2 : G_2 \times_{G_1} G \to G_2$ and $\varphi : G_2 \times_{G_1} G \to G$. As e is surjective, so is φ, and we can complete the diagram (2.3) in the following way:

$$\begin{tikzcd}
1 \arrow[r] & \ker(\varphi) \arrow[r, "\mathrm{i}"] & G_2 \times_{G_1} G \arrow[r, "\varphi"] \arrow[d, "\varphi_2"] & G \arrow[r] \arrow[d, "f"] & 1 \\
& & G_2 \arrow[r, two heads, "e"] & G_1 &
\end{tikzcd}$$

By assumption, there exist a morphism $\psi : G \to G_2 \times_{G_1} G$ such that $\varphi \circ \psi = \mathrm{id}$. Then, $\overline{f} = \varphi_2 \circ \psi$ satisfies the desired condition.

(iii) implies (i): Assume G satisfies (iii). By Section 2.3, we know that $G/\mathrm{Fr}(G)$ is isomorphic to $\prod_{i \in I} \mathbb{F}_p$ for some index set I. By Theorem 2.4.3, there is a morphism $e : F(I) \to \prod_{i \in I} \mathbb{F}_p$. Clearly, this morphism is surjective and by how we constructed this morphism, one can see that $\ker(e) = \mathrm{Fr}(F(I))$. By hypothesis, there is a morphism $\varphi : G \to F(I)$ such that the diagram

$$\begin{tikzcd}
& G \arrow[dl, bend right, "\varphi"'] \arrow[d, "\pi"] \\
F(I) \arrow[r, two heads, "e"] & \prod_{i \in I} \mathbb{F}_p
\end{tikzcd}$$

commutes. We have that $F(I)/\mathrm{Fr}(F(I)) \cong \prod_{i \in I} \mathbb{F}_p$, so

$$\varphi_* : {}^{G}\!\big/_{\mathrm{Fr}(G)} \to {}^{F(I)}\!\big/_{\mathrm{Fr}(F(I))}$$

is an isomorphism. By Theorem 2.4.6, φ is surjective. Since $F(I)$ is free, (as we have already seen that (i) implies (ii)), there is a morphism $\psi : F(I) \to G$ such that $\varphi \circ \psi = \mathrm{id}$. Hence, ψ is injective and since ψ_* is surjective, so is ψ. By Lemma 2.4.1, ψ is an isomorphism of pro-p groups and thus $G \cong F(I)$ is free. □

We now will prove some consequences of Theorem 2.4.9.

Theorem 2.4.10. *Let G be a pro-p group, I some index set, and*

$$\theta : \prod_{i \in I} \mathbb{F}_p \to {}^{G}\!\big/_{\mathrm{Fr}(G)}$$

an epimorphism. Then, there exist an epimorphism $F(I) \to G$ that induces θ. Every system of generators of $G/\mathrm{Fr}(G)$ can be lifted to a system of generators of G.

Proof. Let $\pi_F : F(I) \to F(I)/\mathrm{Fr}(F(I)) \cong \prod_{i\in I} \mathbb{F}_p$ be the quotient morphism and consider the morphism $\theta\circ\pi_F : F(I) \to G/\mathrm{Fr}(G)$. Consider also the quotient morphism $\pi_G : G \twoheadrightarrow G/\mathrm{Fr}(G)$. By condition (iii) of Theorem 2.4.9, there exist a morphism $\varphi : F(I) \to G$ such that the diagram

$$\begin{tikzcd}
& F(I) \arrow[dl, bend right, "\varphi"] \arrow[d, "\pi\circ\theta_F"] \\
G \arrow[r, two heads, "\pi_G"] & {}^{G}\!/_{\mathrm{Fr}(G)}
\end{tikzcd}$$

commutes. By hypothesis, $\varphi_* = \theta$ is surjective. Therefore, by Theorem 2.4.6, φ is surjective, as we wanted to prove.

Now let $\{t_i \mid i \in I\}$ be a system of generators of $G/\mathrm{Fr}(G)$. By Theorem 2.4.3 there is a unique epimorphism $\overline{\theta} : F(I) \to G/\mathrm{Fr}(G)$ mapping the generators s_i of $F(I)$ to the t_i for all $i \in I$. Since $\overline{\theta}$ is surjective, so it is the morphism $\theta : \prod_{i\in I} \mathbb{F}_p \to G/\mathrm{Fr}(G)$. Therefore, there exist a epimorphism $\varphi : F(I) \to G$ that induces θ. Thus, the set $\{\varphi(s_i) \mid i \in I\}$ is a system of generators of G that corresponds to $\{t_i \mid i \in I\}$. □

Corollary 2.4.11. *Every pro-p group has a system of generators.*

Proof. This is a direct consequence of Theorems 2.3.5 and 2.4.10. □

Theorem 2.4.12 (Burnside's Basis Theorem)**.** *Let G be a pro-p group and $E = \{s_i \mid i \in I\}$ a subset of G such that every neighborhood of $1 \in G$ contains almost all elements of E. Then, E is a system of generators of G if, and only if, $\{s_i\mathrm{Fr}(G) \mid i \in I\}$ is a system of generators of $G/\mathrm{Fr}(G)$.*

Proof. The direct implication is clear. Assume $\{s_i\mathrm{Fr}(G) \mid i \in I\}$ generates $G/\mathrm{Fr}(G)$. There is a morphism $\varphi : F(I) \to G$ that maps the generators of $F(I)$ to the s_i respectively. The induced morphism $\varphi_* : F(I)/\mathrm{Fr}(F(I)) \to G/\mathrm{Fr}(G)$ is surjective since $s_i\mathrm{Fr}(G)$ are generators. This implies that the corresponding map φ is also surjective and hence E generates G. □

2.5 Cohomology of pro-p Groups

In this section we will introduce the basic notions of the cohomology of pro-p groups, although we will skip some of the proofs. These notions will be used in the following section to give another characterization of free pro-p groups. A further development of the cohomology of profinite groups can be found on Chapter 3 in [Hal59].

We will begin by defining the cohomology groups for any profinite group and then we will restrict to pro-p groups.

Let G be a profinite group and A a unitary G-module, i.e., A is an abelian group with a left action $G \times A \to A$ such that:

$$g \cdot (a+b) = g \cdot a + g \cdot b$$

for all $g \in G$ and $a, b \in A$. We make A into a topological space by giving it the discrete topology.

Definition 2.5.1. A is called a *discrete G-module* if the map $G \times A \to A$ induced by the action of G is continuous.

Definition 2.5.2. Let G be a profinite group and A a discrete G-module. For any $n \geq 1$, we define $K^n(G, A)$ to be the set of continuous maps from the n-fold product G^n to A. We put $K^0(G, A) := A$ and transfer the additive structure of A to $K^n(G, A)$.

As shown on page 11 on [Koc02] for the 1-dimensional case, the fact that $f \in K^n(G, A)$ is continuous is equivalent to say that the function $f(x_1, \ldots, x_n)$ only depends on cosets of x_i modulo some open normal subgroup of G.

Now consider the following group homomorphisms $d_n : K^n(G, A) \to K^{n+1}(G, A)$ defined by

$$\begin{aligned}(d_n f)(x_1, \ldots, x_{n+1}) = {} & x_1 \cdot f(x_2, \ldots, x_{n+1}) + \\ & + \sum_{m=1}^{n} (-1)^m f(x_1, \ldots, x_m x_{m+1}, \ldots, x_n) + (-1)^{m+1} f(x_1, \ldots, x_n).\end{aligned}$$

These morphisms satisfy the following property:

Theorem 2.5.3. *For $n \geq 1$, we have $d_n \circ d_{n-1} = 0$.*

This result tells us that the groups $K^n(G, A)$ together with the morphisms d_n is a cochain complex. This allow us to define the cohomology groups in the following way:

Definition 2.5.4. The *n-th cohomology group* of G with coefficients in A is:

$$\mathrm{H}^n(G, A) = \begin{cases} \ker(d_n) / \mathrm{Im}(d_{n-1}) & \text{if } n \geq 1, \\ \ker(d_n) & \text{if } n = 0. \end{cases}$$

Example 2.5.5. *Let's take a look at the case $n = 1$. Let $f \in K^1(G, A)$. The image of f by d_1 is the function:*

$$(d_1 f)(x_1, x_2) = x_1 \cdot f(x_2) - f(x_1 x_2) + f(x_1).$$

Then, a continuous function $f : G \to A$ is in $\ker(d_1)$ *if, and only if,*

$$f(g_1g_2) = f(g_1) + g_1 \cdot f(g_2)$$

for all $g_1, g_2 \in G$. These functions are called crossed homomorphisms.

Now take $a \in K^0(G, A) = A$. The image of a by d_0 is the function:

$$(d_0a)(x_1) = x_1 \cdot a - a.$$

Then, a continuous function $f : G \to A$ is in $\mathrm{Im}(d_0)$ *if, and only if, there exist $a \in A$ such that*

$$f(g) = g \cdot a - a$$

for all $g \in G$. These functions are called split crossed homomorphisms. The group $\mathrm{H}^1(G, A)$ *is the quotient of the group of all crossed homomorphisms by all the split crossed homomorphisms.*

We are interested in the case that $A = \mathbb{F}_p$ and G is a pro-p group acting trivially on G. In fact, it could be shown that this is the only possible way a pro-p group can act on $\mathbb{F}_p$. We introduce the following abbreviation:

$$\mathrm{H}^n(G) := \mathrm{H}^n(G, \mathbb{F}_p).$$

Let's take a look at the result described in Example 2.5.5 in this case. Since G acts trivially on $\mathbb{F}_p$, the crossed homomorphism from G to $\mathbb{F}_p$ are exactly the continuous groups homomorphisms, and the only split crossed homomorphism is the zero morphism. Hence, $\mathrm{H}^1(G)$ is the group of all continuous group homomorphism from G to $\mathbb{F}_p$. From this fact, we obtain the following result:

Lemma 2.5.6. *An abelian pro-p group G with exponent p has* $\mathrm{H}^1(G)$ *as its Pontryagin dual group.*

Proof. Since G has exponent p, for any $\chi \in \widehat{G}$, the image of χ will be contained in the set of all p-th roots of unity. The natural identification of $\mathbb{F}_p$ with the p-th roots of unity will give us an isomorphism between $\widehat{G}$ and $\mathrm{H}^1(G)$. □

Remark. Let G be a pro-p group. As $\mathbb{F}_p$ is abelian and has exponent p, any function $f \in \mathrm{H}^1(G)$ satisfies that $\mathrm{Fr}(G) \subseteq \ker(f)$. We have a correspondence between morphisms $f : G \to \mathbb{F}_p$ and morphism $f : G/\mathrm{Fr}(G) \to \mathbb{F}_p$. Hence, $\mathrm{H}^1(G) \cong \mathrm{H}^1(G/\mathrm{Fr}(G))$.

With this correspondence, and Theorems 2.3.3 and 2.3.4, one can state Theorem 2.4.6 in the following way:

Theorem 2.5.7. *Let G_1 and G_2 be pro-p group, and let $\varphi : G_1 \to G_2$ be a continuous group homomorphism. Then, φ is surjective, if, and only if, the induced map $\varphi^* :$* $\mathrm{H}^1(G_2) \to \mathrm{H}^1(G_1)$ *is injective.*

Remark. Since $K^n(G, \mathbb{F}_p)$ is an abelian group of exponent p, it has a natural structure of an $\mathbb{F}_p$-vector space. This structure translate well to the cohomology groups $\mathrm{H}^n(G)$.

2.6 Second Characterization of Free pro-p Groups

In this section we will give a second characterization of free pro-p groups using cohomology groups. To do so, we need a further study of extensions of pro-p groups.

Definition 2.6.1. Let G and H be pro-p groups and $\overline{H_1}, \overline{H_2}$ two pro-p group extensions of G by H. We say that they are *equivalent* if there exist an isomorphism $T : \overline{H_1} \to \overline{H_2}$ making the following diagram commutative:

$$\begin{tikzcd}
 & & \overline{H_1} \arrow[dd, "T"] \arrow[dr] & & \\
1 \arrow[r] & H \arrow[ur] \arrow[dr] & & G \arrow[r] & 1. \\
 & & \overline{H_2} \arrow[ur] & &
\end{tikzcd}$$

Remark. The equivalence of pro-p group extensions of G by H is an equivalence relation.

Definition 2.6.2. Let H and G be topological groups. Let $\mathrm{Aut}_{tg}(H)$ denote the group of all continuous group automorphisms of H. Let $\rho : G \to \mathrm{Aut}_{tg}(H)$ be a group homomorphism such that the induced map

$$\begin{array}{ccc} G \times H & \to & H \\ (g, h) & \mapsto & (\rho(g))(n) \end{array}$$

is continuous. We write $\rho_g(h) := (\rho(g))(h)$ for simplicity. We define the *semidirect product* of H and G with respect to ρ, denoted as $H \rtimes_\rho G$ as the the set $H \times G$ together with the group operation:

$$(h_1, g_1) * (h_2, g_2) := (h_1 \rho_{g_1}(h_2), g_1 g_2).$$

Lemma 2.6.3. *$(H \ltimes_\rho G, *)$ is a group with identity $(1, 1) \in H \ltimes_\rho G$. In fact, $H \ltimes_\rho G$ is a topological group with the product topology of $H \times G$.*

Theorem 2.6.4. *Let G and H be pro-p groups and let*

$$1 \longrightarrow H \longrightarrow \overline{H} \xrightarrow{\varphi} G \longrightarrow 1$$

be a pro-p group extension of G by H, where we identify H with its image inside $\overline{H}$. Suppose this extension splits, i.e. there exists a pro-p group homomorphism

$\sigma : G \to \overline{H}$ such that $\varphi \circ \sigma = \mathrm{id}_G$. Then, $\overline{H}$ is isomorphic as a topological group to the semidirect product $H \ltimes_\rho G$, where $\rho_g(h) = \sigma(g)h\sigma(g)^{-1}$.

Proof. Consider the map

$$\begin{array}{rccc} T: & H \ltimes_\rho G & \longrightarrow & \overline{H} \\ & (h,g) & \longmapsto & h \cdot \sigma(g). \end{array}$$

By construction, this map is continuous. This map is a group homomorphism with the product operation defined in $H \ltimes_\rho G$. Now consider the map

$$\begin{array}{rccc} \tilde{T}: & \overline{H} & \longrightarrow & H \ltimes_\rho G \\ & \overline{h} & \longmapsto & \left(\overline{h} \cdot \left(\sigma\left(\varphi(\overline{h})\right)\right)^{-1}, \varphi(\overline{h})\right), \end{array}$$

that is well defined because $\overline{h} \cdot \left(\sigma\left(\varphi(\overline{h})\right)\right)^{-1} \in \ker(\varphi) = H$. Again, by construction, this map is continuous. In addition, on can easily check that $T \circ \tilde{T} = \mathrm{id}_{\overline{H}}$ and $\tilde{T} \circ T = \mathrm{id}_{H \ltimes_\rho G}$. Thus, T is an isomorphism of topological groups. □

Remark. This theorem shows that, with these hypothesis, $H \ltimes_\rho G$ is a pro-p group.

Corollary 2.6.5. *If the pro-p group extension*

$$1 \longrightarrow H \longrightarrow \overline{H} \longrightarrow G \longrightarrow 1$$

splits, then it is equivalent to the pro-p group extension

$$1 \longrightarrow H \longrightarrow H \ltimes_\rho G \longrightarrow G \longrightarrow 1$$

where ρ is the automorphism defined in Theorem 2.6.4.

Now we come to the characterization of pro-p groups using cohomology groups. Before, we need the following lemmas:

Lemma 2.6.6. *Let $A \neq \{1\}$ be a finite p-group and G a subgroup of p-power order of the automorphism group of A. Then, the number of invariant elements $A^G := \{a \in A \mid g(a) = a \ \forall \ g \in G\} \neq \{1\}$*

Proof. We decompose A into disjoint orbits:

$$G \cdot a = \{g(a) \in A \mid g \in G\}.$$

If a is invariant, $|G \cdot a| = 1$. If a is not invariant, $|G \cdot a|$ is a multiple of p since the order of G is a power of p. This can be seen using that $|G_a||G \cdot a| = |G|$, where G_a is the stabilizer subgroup of G with respect to a. Now we write

$$|A| = \sum_{a \in A^G} 1 + \sum_{r=1}^{m} |G \cdot a_r| = |A^G| + \sum_{r=1}^{m} |G \cdot a_r|.$$

Since $|A|$ and $|G \cdot a_r|$ are multiples of p, so is $|A^G|$ and since $1 \in A^G$, $|A^G|$ has to be at least p. □

Lemma 2.6.7. *Let G be a pro-p group and let $H \neq 1$ be a closed normal subgroup of G. Then, there exist a closed normal subgroup H' of G such that $H' \subseteq H$ and $[H : H'] = p$.*

Proof. Since $H \neq 1$, we claim that there exist an proper subgroup H'' of H satisfying

1. H'' is open in H.
2. H'' is normal in G.
3. H'' is closed in G.

Indeed, take a nontrivial element $g \in H$. Since G is Hausdorff, there exist an open subset $U \subseteq G$ containing 1 with $g \notin U$. By Theorem 1.1.9, G has a neighbourhood basis at 1 consisting of open normal subgroups so, without loss of generality, we may assume that U is an open normal subgroup of G. Then $H'' = H \cap U$ is an open subgroup of H and, since both H and U are normal in G, so is H''. This group is proper in H because $g \in H$ but $g \notin H''$. Finally, since U is open in G, by Lemma 1.1.6, it is also closed. This implies that $H'' = H \cap U$ is closed in G. This proves the claim.

By Lemma 1.2.1, H is a pro-p group and, since H'' is open in H, by Lemma 1.1.6, $[H : H'']$ is finite. Let H' be a maximal proper subgroup of H containing H'' that is normal in G. We want to see that $[H : H'] = p$. If $[H : H'] > p$, there exist a subgroup $H_1/H' \subseteq H/H'$ of order p. G acts on H_1/H' by conjugation. By Lemma 2.6.6, the subgroup $H_2/H' \subseteq H_1/H'$ of all the invariant elements of the action of G/H' is nontrivial. So, H_2 satisfies that $H' \subsetneq H_2 \subsetneq H$ and is normal to G, contradicting the maximality of H'. We can see that H' is closed in G because we can write H' as a finite union of cosets gH''. □

Theorem 2.6.8. *A pro-p group G is free if, and only if,* $\mathrm{H}^2(G) = 0$.

Proof. In this proof we will use that there's a bijection between the equivalence classes of pro-p group extensions of G by a $\mathbb{F}_p$ and the second cohomology group $\mathrm{H}^2(G)$. This bijection is explained on Theorem 5.4.6 in [Wil21]

Suppose G is a free pro-p group. By Theorem 2.4.9, every extension $\overline{H}$ of G by $\mathbb{F}_p$ splits. Thus, by Corollary 2.6.5, $\overline{H}$ is equivalent to the extension

$$0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{F}_p \ltimes_\rho G \longrightarrow G \longrightarrow 1$$

for some $\rho \in \mathrm{Aut}_{tg}(\mathbb{F}_p) \cong \mathbb{F}_p^*$. We will see that $\rho = \mathrm{id}_{\mathbb{F}_p}$. We claim that ρ is continuous when we consider the discrete topology on $\mathrm{Aut}_{tg}(\mathbb{F}_p)$. By construction, the map

$$\begin{array}{rccc} \Phi : & G \times \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ & (g, a) & \longmapsto & \rho_g(a) \end{array}$$

is continuous. For any $a, b \in \mathbb{F}_p^*$, let $f_{a,b} \in \mathrm{Aut}_{tg}(\mathbb{F}_p)$ be the only automorphism that sends a to b. Fix $a, b \in \mathbb{F}_p$. Then,

$$\Phi^{-1}(b) = \bigsqcup_{c\in\mathbb{F}_p^*} \rho^{-1}(f_{c,b}) \times \{c\}$$

is open in $G\times\mathbb{F}_p$ and, intersecting with $G\times\{a\}$, we obtain that $\rho^{-1}(f_{a,b})\times\{a\} \subseteq G\times\mathbb{F}_p$ is open. Hence, $\rho^{-1}(f_{a,b})$ is open in G. This proves the claim.

Since ρ is continuous, $\ker(\rho) \subseteq G$ is an open normal subgroup. Thus, $G/\ker(\rho)$ is a finite p-group and we have an induced group morphism $G/\ker(\rho) \hookrightarrow \mathrm{Aut}_{tg}(\mathbb{F}_p) \cong \mathbb{F}_p^*$. Since $\mathbb{F}_p^*$ has order coprime to p, the only possibility is that this morphism is the trivial morphism. Hence $\ker(\rho) = G$, i.e., ρ is the constant function $\mathrm{id}_{\mathbb{F}_p} \in \mathrm{Aut}_{tg}(\mathbb{F}_p)$. This implies that $\mathbb{F}_p \ltimes_\rho G = \mathbb{F}_p \times G$. Consequently, all extensions of G by $\mathbb{F}_p$ are equivalent to the trivial extension

$$0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{F}_p \times G \longrightarrow G \longrightarrow 1.$$

Since there is only one equivalence class of extensions of G by $\mathbb{F}_p$, $\mathrm{H}^2(G) = 0$.

Now suppose that G is a pro-p group with $\mathrm{H}^2(G) = 0$. By Section 2.3, we have an isomorphism

$$\theta : \prod_I \mathbb{F}_p \to G/\mathrm{Fr}(G)$$

for some index set I. By Theorem 2.4.10, there exists an epimorphism $\varphi : F(I) \twoheadrightarrow G$ that induces θ. Denote $H = \ker(\varphi)$. If $H = \{1\}$, we obtain that φ is an isomorphism and hence G is free. Suppose $H \neq \{1\}$. We will obtain a contradiction. H is normal in $F(I)$ and since G is Hausdorff, H is closed. By Lemma 2.6.7, there exists a closed normal subgroup H' of G such that $H' \subseteq H$ and $[H : H'] = p$. By the third isomorphism theorem, $(F(I)/H') \,/\, (H/H') = F(I)/H$. Denote $G' = F(I)/H'$ and notice that $F(I)/H \cong G$ and $H/H' \cong \mathbb{F}_p$. Thus, φ induces the following pro-p group extension:

$$0 \longrightarrow \mathbb{F}_p \longrightarrow G' \longrightarrow G \longrightarrow 1.$$

Since $\mathrm{H}^2(G) = 0$, this extension is equivalent to the trivial extension, i.e., we have $G' \cong \mathbb{F}_p \times G$. Consider the following diagram:

$$\begin{tikzcd}
F(I) \arrow[r, "\alpha_1"] \arrow[d, "\beta_1"] & G' \cong \mathbb{F}_p \times G \arrow[r, "\alpha_2"] \arrow[d, "\beta_2"] & G \arrow[d, "\beta_3"] \\
\prod_I \mathbb{F}_p \arrow[r, "\gamma_1"] & G'/\mathrm{Fr}(G') \cong \mathbb{F}_p \times \prod_I \mathbb{F}_p \arrow[r, "\gamma_2"] & G/\mathrm{Fr}(G)
\end{tikzcd}$$

This diagram is commutative since the first row are just quotients of $F(I)$ by H' and H and the second rows are the induced morphisms. In addition, the second rows are isomorphisms since the composition is θ and both maps are surjective by Theorem

2.4.6. From this, we get a contradiction, as $(1, 0) \in G' \cong \mathbb{F}_p \times G$ is map to 0 thought $\beta_3 \circ \alpha_2$ but $\beta_2((1, 0)) = 1 \times (0, \ldots, 0)$, contradicting the injectivity of γ_2. □

Theorem 2.6.9. *Let G be a pro-p group. Suppose that $\mathrm{H}^n(G) = 0$ for some $n \in \mathbb{N}$. Then $\mathrm{H}^m(G) = 0$ for all $m > n$.*

Proof. The proof of this theorem can be found on page 49 in [Koc02]. □

The two previous theorems lead to the following result:

Corollary 2.6.10. *Let G be a free pro-p group. Then, $\mathrm{H}^n(G) = 0$ for all $n \geq 2$.*

Chapter 3

Presentation of pro-p Groups

On of the most important methods for constructing pro-p groups is the presentation by generators and relations. This will be used in Chapter 4 to introduce Golod-Shafarevich groups and to present the Golod-Shafarevich inequality.

3.1 The Generator Rank

Let G be a pro-p group. As we saw on Section 2.5, the first cohomology group $\mathrm{H}^1(G)$ can be seen as the group of all continuous group homomorphisms from G to $\mathbb{F}_p$. There is a natural way to regard $\mathrm{H}^1(G)$ as an $\mathbb{F}_p$-vector space.

Definition 3.1.1. The *generator rank* $d(G)$ of a pro-p group G is the dimension of $\mathrm{H}^1(G)$ as an $\mathbb{F}_p$-vector space.

This definition is motivated by the following statement:

Theorem 3.1.2. *Let G be a pro-p group. The cardinality of any minimal system of generators of G equals $d(G)$.*

Proof. Let $\{s_i \mid i \in I\}$ be a minimal system of generators of G. By Theorem 2.4.12, $\{s_i\mathrm{Fr}(G) \mid i \in I\}$ is a minimal system of generators of $G/\mathrm{Fr}(G)$. Then, by Theorem 2.3.5, we have an isomorphism

$$^{G}\!\diagup_{\mathrm{Fr}(G)} \cong \prod_I \mathbb{F}_p.$$

Taking into account Lemma 2.5.6 and dualizing this equivalence, we obtain

$$\mathrm{H}^1(G) \cong \mathrm{H}^1\left(^{G}\!\diagup_{\mathrm{Fr}(G)}\right) \cong \bigoplus_I \mathbb{F}_p,$$

and so $\dim\left(\mathrm{H}^1(G)\right) = \left|I\right|$. □

This theorem shows that all minimal systems of generators of a pro-p group have equal cardinality.

Remark. Notice that $d(G) = d(G/\mathrm{Fr}(G))$.

Lemma 3.1.3. *Let F be a finitely generated free pro-p group and $G \subseteq F$ pro-p subgroup of finite index. Then,*

$$d(G) = [F : G]\,(d(F) - 1) + 1.$$

Proof. The proof of this lemma uses the concept of Euler-Poincaré characteristic of a pro-p group. It is a consequence of Theorem 5.4 in [Koc02]. □

In general, any pro-p subgroup of finite index in a finitely generated pro-p group is finitely generated.

3.2 Relation Systems

Definition 3.2.1. Let G be a pro-p group. An exact sequence

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1 \tag{3.1}$$

of pro-p groups where F is a free pro-p group with system of generators $\{t_i \mid i \in I\}$ is called a *presentation* of G by F. We identify R with the corresponding subgroup of F. If $\{\varphi(t_i) \mid i \in I\}$ is a minimal system of generators of G, then the presentation is called *minimal*.

Definition 3.2.2. A subset $E \subseteq R$ is called a *(generating) system of relations* of G with respect to the presentation (3.1) if it satisfies:

(i) R is the smallest normal subgroup of F containing E.

(ii) every open normal subgroup of R contains almost all elements of E.

We say that E is *minimal* if no proper subset of E is a system of relations of G.

Definition 3.2.3. Let $\{G_i \mid i \in I\}$ be a family of pro-p groups and let $\{T_i \mid i \in I\}$ be a family of normal subgroups of the G_i such that the G_i/T_i are free pro-p groups. Let G be a pro-p group. A family of morphisms $\{\varphi_i : G_i \to G \mid i \in I\}$ is called *admissible* with respect to $\{T_i \mid i \in I\}$ if every open normal subgroup of G contains almost all $\varphi_i(T_i)$.

Theorem 3.2.4. *Let G be a pro-p group with a presentation as in Equation (3.1). Let the assumptions be as in Definition 3.2.3. Let $\{\varphi_i : G_i \to G \mid i \in I\}$ be admissible with respect to $\{T_i \mid i \in I\}$. For every $i \in I$, let*

$$1 \longrightarrow R_i \longrightarrow F_i \xrightarrow{\psi_i} G_i \longrightarrow 1 \tag{3.2}$$

be a presentation of G_i. Then, there exist morphisms $\chi_i : F_i \to F$ with restrictions $\overline{\chi} : R_i \to R$ such that the diagram

$$\begin{tikzcd}
R_i \arrow[r] \arrow[d, "\overline{\chi}_i"] & F_i \arrow[r, "\psi_i"] \arrow[d, "\chi_i"] & G_i \arrow[d, "\varphi_i"] \\
R \arrow[r] & F \arrow[r, "\psi"] & G
\end{tikzcd}$$

commutes and $\{\overline{\chi}_i \bigm| i \in I\}$ is admissible with respect to $\{R_i \bigm| i \in I\}$. In this case, we speak about an admissible presentation of $\{\varphi_i \bigm| i \in I\}$.

Proof. By Theorem 1.2.3, there exists a continuous section $\sigma : G \to F$ with $\sigma(1) = 1$. Let $\{t_k^i \bigm| k \in I_i\}$ be a system of generators of the free pro-p group F_i, where the images of t_k^i under the map $\theta_i : F_i \twoheadrightarrow G_i/T_i$ form a system of generators for some subset $I_i^1 \subseteq I_i$ and are mapped to 1 for $k \in I_i^2 := I_i \setminus I_i^1$. Then, by Theorem 2.4.3, we can define a morphism $\chi_i : F_i \to F$ by

$$\chi_i(t_k^i) = (\sigma \circ \varphi_i \circ \psi_i)\,(t_k^i), \quad k \in I_i.$$

This morphism satisfies that $\varphi_i \circ \psi_i = \psi \circ \chi_i$. Moreover, if $g \in \ker(\psi_i) = R_i$, then $\chi_i(g) \in \ker(\psi) = R$ and hence the restriction $\overline{\chi}_i$ is well define. Thus, the diagram (3.2) is commutative.

Notice that the quotient $R_i/R_i = \{1\}$ is a free pro-p group generated by 0 elements. Thus, to see that $\{\overline{\chi_i} \bigm| i \in I\}$ is admissible with respect to $\{R_i \bigm| i \in I\}$, we just need to see that every open normal subgroup of R contains almost all $\overline{\chi}_i(R_i)$.

Let N be an open normal subgroup of F. Then, $\sigma^{-1}(N)$ is an open neighbourhood of 1. Since G is profinite, there exists an open normal subgroup U of G with $U \subseteq N$. By assumption, we have

$$\varphi_i(T_i) \subseteq U \tag{3.3}$$

for almost all $i \in I$. Let i be an index for which (3.3) holds. Then, for all $k \in I_i^2$, $\psi(t_k^i) \in T_i$ and hence $\chi_i(t_k^i) \in \sigma(U) \subseteq N$. But this implies that $\chi_i(\ker \theta_i) \subseteq N$, and since $R_i \subseteq \ker(\theta_i)$, we have $\overline{\chi}_i(R_i) \subseteq R \cap N$. Since every neighborhood of $1 \in R$ contains a group $N \cap R$, this implies the claim. □

Lemma 3.2.5. *Assume the hypothesis of Theorem 3.2.4 and consider the family $\{\overline{\chi}_i : R_i \to R \bigm| i \in I\}$, that is admissible with respect to $\{R_i \bigm| i \in I\}$. Then, for any $\overline{f} \in \mathrm{H}^1(R)$ and for almost all $i \in I$, the image of $\overline{f}$, under the induced map $\mathrm{H}^1(R) \to \mathrm{H}^1(R_i)$ is 0.*

Proof. Let $f \in \ker(d_1) \subseteq K^1(R, \mathbb{F}_p)$ be a cocycle representing $\overline{f}$. Let U be a normal open subgroup of R on which f is constant. By assumption, for almost all $i \in I$, we have a factorization

$$R_i \longrightarrow U \longrightarrow R,$$

and therefore induced maps

$$\mathrm{H}^1(R_i) \longrightarrow \mathrm{H}^1(U) \longrightarrow \mathrm{H}^1(R).$$

Since f is constant in U, so is the image of $\overline{f}$ in $\mathrm{H}^1(U)$. As we saw on Section 2.5, $\mathrm{H}^1(U)$ is the group of all continuous group homomorphisms from U to $\mathbb{F}_p$, so the only possibility is that the image of $\overline{f}$ in $\mathrm{H}^1(U)$ is 0. □

This previous lemma guarantees that the map

$$\chi^* : \mathrm{H}^1(R) \longrightarrow \bigoplus_{i \in I} \mathrm{H}^1(R_i) \tag{3.4}$$

is well defined.

Since R is normal to F, F acts on R by conjugation. This action induces an action of F on $\mathrm{H}^1(R)$: if $f \in \mathrm{H}^1(R)$ and $h \in F$, we define

$$(h \cdot f)(r) := f(h^{-1}rh).$$

Since $\mathrm{H}^1(R)$ is the set of continuous group homomorphisms from R to $\mathbb{F}_p$ and $\mathbb{F}_p$ is abelian, it is clear that R acts trivially on $\mathrm{H}^1(R)$. Hence, we can regard this action as an action of G. Moreover, we can regard $\mathrm{H}^1(R)$ as a discrete G-module. With these considerations and the morphism defined in Equation (3.4), we have the following theorem:

Theorem 3.2.6. *The groups $\chi_i(R_i), i \in I$, generate R as a normal subgroup of F if, and only if, the restriction of χ^* to $\mathrm{H}^1(R)^G$ is injective.*

Recall that the normal subgroup of F generated by $\chi_i(R_i)$ is the subgroup generated by $\{g^{-1}rg \in F \mid g \in F,\, r \in \chi_i(R_i),\, i \in I\}$, i.e., is the smallest normal subgroup of F that contains $\chi_i(R_i)$. For the proof of Theorem 3.2.6 we need the following lemma:

Lemma 3.2.7. *Let G be a pro-p group and A a p-primary discrete G-module. Then, $A^G = 0$ implies $A = 0$.*

Proof. Using the same argument we used on the proof of Theorem 2.6.8, one can see that the fact that the action of G to A is continuous implies that the induced group morphism

$$\rho : G \to \mathrm{Aut}(A)$$

is continuous when we consider the discrete topology on $\mathrm{Aut}(A)$. Then, $\ker(\rho)$ is an open normal subgroup of G and we have an induced action of $G/\ker(\rho)$ on A. Since G is pro-p, $G/\ker(\rho)$ is a finite p-group. Then, each $a \in A$ generates a finite G-module A_0. If we had $A_0 \neq 0$, then Lemma 2.6.6 would imply that $A_0^G \neq 0$ contradicting our assumption. □

Now we come to the proof of Theorem 3.2.6:

Proof of Theorem 3.2.6. Suppose that $\chi_i(R_i), i \in I$, generate R as a normal subgroup of F and let $f \in \mathrm{H}^1(R)^G$ with $\chi^*(f) = 0$. We have that $f \circ \chi_i = 0$ for all $i \in I$ and hence $f(\chi_i(R_i)) = 0$. Since f is invariant under G (and invariant under F), for any $h \in F$ we have $f(h^{-1}\chi_i(R_i)h) = 0$. By assumption, the sets $h^{-1}\chi_i(R_i)h$ generate R. Therefore, $f(R) = 0$, i.e., $f = 0$.

Conversely, assume that the restriction of χ^* to $\mathrm{H}^1(R)^G$ is injective and let R' denote the normal subgroup of F generated by the $\chi_i(R_i)$. The inclusion $R' \hookrightarrow R$ induces a homeomorphism $\varphi : \mathrm{H}^1(R) \to \mathrm{H}^1(R')$ which factorizes the map (3.4):

$$\mathrm{H}^1(R) \xrightarrow{\varphi} \mathrm{H}^1(R') \longrightarrow \bigoplus\nolimits_{i\in I} \mathrm{H}^1(R_i).$$

By assumption, $\ker(\varphi)$ doesn't contain any nonzero elements invariant under the action of G. By Lemma 2.5.6,

$$\mathrm{H}^1(R) \cong \mathrm{H}^1\left({}^{R}\!/_{\mathrm{Fr}(R)}\right) \cong \widehat{{}^{R}\!/_{\mathrm{Fr}(R)}},$$

and so $\mathrm{H}^1(R)$ is a p-primary discrete G-module. Hence, $\ker(\varphi)$ is also a p-primary discrete G-module and, by Lemma 3.2.7, this implies that $\ker(\varphi) = 0$. Now, applying Theorem 2.5.7 we deduce that $R' = R$. □

Lemma 3.2.8. *Let the assumptions be as in Definition 3.2.3. Assume that* $\{\varphi_i \mid i \in I\}$ *is admissible with respect to* $\{T_i \mid i \in I\}$. *We consider the induced maps* $\varphi_i^* : \mathrm{H}^n(G) \to \mathrm{H}^n(G_i)$. *Then, for any* $\alpha \in \mathrm{H}^n(G)$, $n \geq 2$, *it holds that* $\varphi_i^*(\alpha) = 0$ *for almost all* $i \in I$.

Proof. Let $f \in \ker(d_n) \subseteq K^n(G, \mathbb{F}_p)$ be a cocycle representing α. Then f only depends on cosets of G modulo some open normal group U of G. Let i be an index such that $\varphi_i(T_i) \subseteq U$. Then , f induces a cocycle in $K^n(G_i, \mathbb{F}_p)$ that depends only on the cosets G_i/T_i, and which therefore must be induced from a cocycle in $K^n(G_i/T_i, \mathbb{F}_p)$. Since G_i/T_i is free, by the Corollary 2.6.10, $\mathrm{H}^n(G_i/T_i)$ vanishes for $n \geq 2$, hence so does $\varphi_i^*(\alpha)$. □

This lemma allow us to define the following map:

$$\varphi^* : \mathrm{H}^2(G) \to \bigoplus_{i\in I} \mathrm{H}^2(G_i). \tag{3.5}$$

Now we come to the main result of this section. To formulate it, we first define the notion of complementary set:

Definition 3.2.9. A subset $E \subseteq R$ is called a *complementary set* of $\{\chi_i \mid i \in I\}$ if:

(i) E and $\bigcup_{i\in I} \chi_i(R_i)$ generate R as a normal subgroup of F.

(ii) Each neighborhood of $1 \in R$ contains almost all elements of E.

The set E is called *minimal* if no proper subset of E is a complementary set.

Theorem 3.2.10. *Let G be a pro-p group and let $\{\varphi_i : G_i \to G \mid i \in I\}$ be a family of morphisms admissible with respect to $\{\, T_i \mid i \in I\,\}$. Assume we have an admissible presentation of $\{\varphi_i \mid i \in I\}$, where the presentations of G and G_i are minimal :*

$$\begin{tikzcd}
1 \arrow[r] & R_i \arrow[r] \arrow[d, "\overline{\chi}_i"] & F_i \arrow[r] \arrow[d, "\chi_i"] & G_i \arrow[r] \arrow[d, "\varphi_i"] & 1 \\
1 \arrow[r] & R \arrow[r] & F \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Moreover, let E be a minimal complementary set of $\{\chi_i \mid i \in I\}$ and consider the morphism φ^* defined in Equation (3.5). Then,

$$\dim_{\mathbb{F}_p}(\ker(\varphi^*)) = |E|$$

The proof of this theorem requires some more development of the cohomology of profinite groups. We will state the main ideas of the proof and cite [Koc02] for some needed results:

Proof. For every $j \in E$, let F_j be the smallest closed subgroup of F containing j, i.e., $F_j = \overline{\langle j \rangle}$, which is a pro-$p$ group. Let χ_j denote the inclusion $F_j \hookrightarrow F$. Consider the subgroups $R_j = F_j$. Note that $F_j \subseteq R$, and hence we can define the restriction $\overline{\chi_j} : R_j \to R$. We have a commutative diagram

$$\begin{tikzcd}
R_i \arrow[r] \arrow[d, "\overline{\chi}_j"] & F_j \arrow[r] \arrow[d, "\chi_j"] & G_j \arrow[d] \\
R \arrow[r] & F \arrow[r] & G
\end{tikzcd}$$

for $j \in I \cup E$. Condition (ii) in Definition 3.2.9 assures that the family $\{\overline{\chi}_j \mid j \in I \cup E\}$ is admissible with respect to $\{\, R_j \mid j \in I \cup E\,\}$ and we have an admissible presentation. In addition, by condition (i) in Definition 3.2.9,

$$\bigcup_{j\in I\cup E} \chi_j(R_j)$$

generate R as a normal subgroup of F. Hence, by Theorem 3.2.6, the induced map

$$\chi^* : \mathrm{H}^1(R)^G \longrightarrow \bigoplus_{j\in I\cup E} \mathrm{H}^1(R_j)$$

is injective. Consider the map

$$\psi^* : \mathrm{H}^1(R)^G \longrightarrow \bigoplus_{i\in I} \mathrm{H}^1(R_i)^{G_i}$$

and the commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1(R)^G \arrow[r] & \bigoplus_{j\in I\cup E} \mathrm{H}^1(R_j) \\
\ker(\psi^*) \arrow[u] \arrow[r] & \bigoplus_{j\in E} \mathrm{H}^1(R_j) \arrow[u]
\end{tikzcd} \tag{3.6}$$

Clearly, the second row in (3.6) is injective, and even an isomorphism since E is minimal. By Theorem 3.14 in [Koc02], we have the following exact commutative diagram:

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] \\
 & & \mathrm{H}^1(G) \arrow[r] \arrow[d, "\mathrm{inf}"] & \bigoplus_{i\in I} \mathrm{H}^1(G) \arrow[d, "\mathrm{inf}"] \\
 & & \mathrm{H}^1(F) \arrow[r] \arrow[d, "\mathrm{res}"] & \bigoplus_{i\in I} \mathrm{H}^1(F_i) \arrow[d, "\mathrm{res}"] \\
0 \arrow[r] & \ker(\psi^*) \arrow[r] & \mathrm{H}^1(R)^G \arrow[r, "\psi^*"] \arrow[d, "\mathrm{tra}"] & \bigoplus_{i\in I} \mathrm{H}^1(R_i)^{G_i} \arrow[d, "\mathrm{tra}"] \\
0 \arrow[r] & \ker(\varphi^*) \arrow[r] & \mathrm{H}^2(G) \arrow[r, "\varphi^*"] \arrow[d] & \bigoplus_{i\in I} \mathrm{H}^2(G_i) \arrow[d] \\
 & & 0 & 0
\end{tikzcd}$$

The morphisms inf, res and tra are called *inflation*, *restriction* and *transgression*. Its definition is not simple, and hence we will omit it. It can be found on pages 28 - 34 in [Koc02]. One can see that, since the presentation of G_i and G are minimal, the inflation maps and the transgression maps are isomorphisms. Thus, the induced map

$\ker(\psi^*) \to \ker(\varphi^*)$ is an isomorphism. Since,

$$\dim(\ker(\psi^*)) = \dim\left(\bigoplus_{j\in E} \mathrm{H}^1(R_j)\right) = \big|E\big|,$$

this implies the claim. □

We will give some consequences of this theorem. To this end, we introduce the notion of relation rank:

Definition 3.2.11. The *relation rank* of a pro-p group G, denoted by $r(G)$, is the $\mathbb{F}_p$-dimension of $\mathrm{H}^2(G)$.

Theorem 3.2.12. *The relation rank of a pro-p group G equals the cardinality of any minimal system of relations.*

Proof. Let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal presentation of G. Let I be a singleton and $G_i = G$. Take $T_i = G_i$. Then, $G_i/T_i = \{1\}$ is a free pro-p group. Define $\varphi : G_i \to G$ to be the trivial map. Then $\{\varphi_i \bigm| i \in I\}$ is admissible with respect to $\{T_i \bigm| i \in I\}$.

Consider for G_i the same presentation as G and apply Theorem 3.2.4 Then $\chi_i : F_i \to F$ is the trivial map and we have an admissible presentation of $\{\varphi_i \bigm| i \in I\}$.

Since $\chi_i(R_i) = \{1\}$, the notions of complementary set of $\{\chi_i \bigm| i \in I\}$ and generating system of relations coincide. Let $E \subseteq R$ be a minimal generating system of relations and consider the map

$$\varphi^* : \mathrm{H}^2(G) \longrightarrow \bigoplus_{i\in I} \mathrm{H}^2(G_i) = \mathrm{H}^2(G_i).$$

By Theorem 3.2.10,

$$\dim_{\mathbb{F}_p}(\ker(\varphi^*)) = \big|E\big|.$$

Since φ_i is the trivial map, so is φ^*. Thus, $\ker(\varphi^*) = \mathrm{H}^2(G)$. This implies the claim. □

Theorem 3.2.13. *Under the assumptions of Theorem 3.2.10, R is generated as a normal subgroup of F by the subgroups $\chi_i(R_i)$, $i \in I$, if, and only if, φ^* is injective.*

Chapter 4

The Golod-Shafarevich Inequality

In this chapter we will prove the famous Golod-Shafarevich inequality. To be able to state it, we need to define the concept of Golod-Shafarevich group. To do so, we shall begin by taking about the complete group algebra of a pro-p group.

4.1 Complete Group Algebra of a pro-p Group

For finite groups G, the additive group of the ring $\mathbb{F}_p[G]$ is isomorphic to the direct sum of $\left|G\right|$ copies of $\mathbb{F}_p$, and thus inherits the discrete topology, that makes $\mathbb{F}_p[G]$ into a compact group ring.

Let G be a pro-p group. For open normal subgroups $N, N' \subseteq G$ with $N' \subseteq N$, we can lift the natural map

$$G/N' \longrightarrow G/N$$

linearly to a homomorphism of group algebras

$$\mathbb{F}_p\left[G/N'\right] \longrightarrow \mathbb{F}_p\left[G/N\right].$$

This defines a projective system $\{\mathbb{F}_p[G/N] \mid N \in \mathfrak{U}_G\}$ of compact rings.

Definition 4.1.1. The *complete group algebra* $\mathbb{F}_p[[G]]$ of a pro-p group G over the compact field $\mathbb{F}_p$ is the projective limit of the system $\{\mathbb{F}_p[G/N] \mid N \in \mathfrak{U}_G\}$.

Remark. Since the algebras $\mathbb{F}_p[G/N]$ are compact, so is $\mathbb{F}_p[[G]]$.

We can embed G into $\mathbb{F}_p[[G]]$ via the following morphism

$$g \longmapsto \prod_{N \in \mathfrak{U}_G} [gN].$$

Lemma 4.1.2. *The subring $\mathbb{F}_p[G]$ (which is given the subspace topology) is dense in $\mathbb{F}_p[[G]]$.*

Proof. The proof of this lemma is analogous to the proof of Lemma 2.1.6. □

Other basic properties of $\mathbb{F}_p[[G]]$ are expressed in the following:

Theorem 4.1.3. *Let G be a pro-p group. The following properties hold:*

(i) The map $G \to \mathbb{F}_p[[G]]$ is a covariant functor from the category of profinite groups to the category of compact $\mathbb{F}_p$-algebras.

(ii) Let A be a compact $\mathbb{F}_p$-algebra. Every morphism $\varphi : G \to A^*$ from G to the unit group of A can be extended uniquely to a morphism $\mathbb{F}_p[[G]] \to A$.

(iii) Let $\varphi : G \to G'$ be a morphism of pro-p groups with kernel N. The kernel of the induced morphism $\varphi' : \mathbb{F}_p[[G]] \to \mathbb{F}_p[[G']]$ is the closed ideal $I(N)$ generated by the elements $h-1$, $h \in N$.

Proof. (ii) First, notice that φ can be lifted uniquely to a continuous homomorphism $\varphi' : \mathbb{F}_p[G] \to A$. By Lemma 4.1.2, $\mathbb{F}_p[G]$ is dense in $\mathbb{F}_p[[G]]$, and hence can be lifted uniquely to $\mathbb{F}_p[[G]]$.

(i) This is a consequence of (ii). Every map $G_1 \to G_2$ can be extended uniquely to a map $\mathbb{F}_p[[G_1]] \to \mathbb{F}_p[[G_2]]$.

(iii) Since the image of φ is closed in G', $\mathrm{Im}(\varphi)$ is also a pro-p group. Hence, without loss of generality, we may assume that φ is surjective. It is clear that $I(N) \subseteq \ker(\varphi')$. Thus, φ' induces a morphism

$$\tilde{\varphi} : {}^{\mathbb{F}_p[[G]]}\!\big/_{I(N)} \longrightarrow \mathbb{F}_p[[G']].$$

The restriction of $\tilde{\varphi}$ to the image of G in the quotient space $\mathbb{F}_p[[G]]/I(N)$

$$\psi : {}^{G+I(N)}\!\big/_{I(N)} \longrightarrow G'$$

is an isomorphism, since $I(N) \cap G = N$. By (ii), ψ^{-1} can be lifted to a morphism $\mathbb{F}_p[[G']] \to \mathbb{F}_p[[G]]/I(N)$, that turns out to be the inverse of $\tilde{\varphi}$. This implies that $I(N) = \ker(\varphi')$. □

Remark. Let G be a finite discrete p-group. Then $\{1\}$ is an open normal subgroup of G and $\mathfrak{U}_1 = \{1\}$ is cofinal in $\mathfrak{U}_G$. This shows that

$$\mathbb{F}_p[[G]] = \varprojlim_{N \in \mathfrak{U}_G} \mathbb{F}_p \left[{}^{G}\!\big/_{N}\right] \cong \varprojlim_{N \in \mathfrak{U}_1} \mathbb{F}_p \left[{}^{G}\!\big/_{N}\right] = \mathbb{F}_p[G]$$

Theorem 4.1.4. *Let G be a pro-p group. The system $\{I(N) \mid N \in \mathfrak{U}_G\}$ is an open neighborhood basis at $0 \in \mathbb{F}_p[[G]]$.*

Proof. Notice that, for every $N \in \mathfrak{U}_G$, $(\mathbb{F}_p[G/N], +)$ is a finite discrete topological group. Hence, $\mathbb{F}_p[[G]] = \varprojlim_{N \in \mathfrak{U}_G} \mathbb{F}_p[G]$ is a profinite group. Let π_N denote the map

$$\pi_N : \mathbb{F}_p[[G]] \longrightarrow \mathbb{F}_p\left[{}^{G}\!/_{N}\right].$$

By Theorem 1.1.8, $\{\ker(\pi_N) \mid N \in \mathfrak{U}_G\}$ is an open neighborhood basis at $0 \in \mathbb{F}_p[[G]]$.

Observe now that, for every $N \in \mathfrak{U}_G$, G/N is also a pro-p group. Thus, by 4.1.3, the morphism

$$\varphi_N : G \longrightarrow {}^{G}\!/_{N}$$

extends uniquely to a morphism

$$\varphi'_N : \mathbb{F}_p[[G]] \longrightarrow \mathbb{F}_p\left[\left[{}^{G}\!/_{N}\right]\right]$$

whose kernel is $I(N)$. Since N is open, G/N is a finite discrete p-group. Hence, $\mathbb{F}_p[[G/N]] \cong \mathbb{F}_p[G/N]$. This implies that $\ker(\pi_N) = I(N)$. □

In the following sections we will use this special case:

Lemma 4.1.5. *Let G be a pro-p group. Then, $\mathbb{F}_p[[G]]/I(G) \cong \mathbb{F}_p$.*

Proof. Consider the morphism $\varphi : G \to \{1\}$. By Theorem 4.1.3, we can extend φ to a morphism

$$\tilde{\varphi} : \mathbb{F}_p[[G]] \longrightarrow \mathbb{F}_p[\{1\}] \cong \mathbb{F}_p$$

with kernel $I(G)$. Hence, $\mathbb{F}_p[[G]]/I(G) \cong \mathbb{F}_p$. □

4.2 Filtrations

In this section we will start describing a special filtration of $\mathbb{F}_p[[G]]$, and use it to define a filtration of G known as Zassenhaus filtration. Remember that, for any open normal subset N of G, $I(N)$ denotes the closed ideal of $\mathbb{F}_p[[G]]$ generated by the elements $h - 1$, $h \in N$.

Definition 4.2.1. We denote by $I^n(G)$ the topological closure of the n-th power of $I(G)$ in $\mathbb{F}_p[[G]]$.

We will prove that the ideals $I^n(G)$ form an open neighbourhood basis at 0. First, we need the following two lemmas:

Lemma 4.2.2. *Let G be a finite p-group. Then $I^n(G) = 0$ for all sufficiently large n.*

Proof. If G is a finite p-group, so is $\mathbb{F}_p[[G]] \cong \mathbb{F}_p[G]$. For any $n \geq 0$, let

$$I^n(G) = A_0 \supset A_1 \supset \cdots \supset A_s = \{0\}$$

be a composition series of $I^n(G)$ as a G-module. If $s = 0$, we are done. Suppose $s > 0$. We claim that the factors A_k/A_{k-1} are isomorphic to $\mathbb{F}_p$. By Lemma 2.6.6, $(A_k/A_{k-1})^G$ is nonzero and hence A_k/A_{k-1} must have a submodule isomorphic to $\mathbb{F}_p$ where G acts trivially. Since A_k/A_{k-1} is irreducible, this submodule is A_k/A_{k-1}.

G acts trivially on $I^n(G)/A_1$, so

$$ga \equiv a \pmod{A_1}$$

for all $g \in G$ and all $a \in I^n(G)$. Thus, for all $g \in G$, $(g-1)I^n(G) \subseteq A_1$ and hence $I^{n+1}(G) \subseteq A_1$. This implies the claim. □

Lemma 4.2.3. *If G is a finitely generated pro-p group, then the index $[\mathbb{F}_p[[G]] : I^n(G)]$ is finite for all $n \geq 1$.*

Proof. By Lemma 4.1.5, $[\mathbb{F}_p[[G]] : I(G)]$ is finite, so it's enough to prove that $[I^n(G) : I^{n+1}(G)]$ is finite for all $n \geq 1$. We will use induction.

Let $s_1, \ldots, s_m$ denote the generators of G. We put

$$x_i = s_i - 1, \quad i = 1, \ldots, m, \qquad I^n = I^n(G).$$

I. $n = 1$. We define

$$A_1 = \mathbb{F}_p\, x_1 + \ldots + \mathbb{F}_p\, x_n.$$

Since A_1 is finite and I^2 is closed,

$$A_1 + I^2 = \bigcup_{a \in A_1} a + I^2$$

is also closed. Clearly, $A_1 + I^2 \subseteq I$. Let's see that $I \subseteq A_1 + I^2$. Note that $\{s_1, \ldots, s_m\} - 1 \subseteq A_1 + I_2$. Consider the following identity:

$$g_1 g_2 - 1 = (g_1 - 1)(g_2 - 1) + g_1 - 1 + g_2 - 1. \tag{4.1}$$

This shows that $\langle s_1, \ldots, s_m \rangle - 1 \subseteq A_1 + I^2$, where $\langle s_1, \ldots, s_m \rangle$ is the group generated by s_i. Since $A_1 + I^2$ is closed and $G \hookrightarrow \mathbb{F}_p[[G]]$, we have that $G - 1 \subseteq A_1 + I^2$, and thus $\mathrm{Span}_{\mathbb{F}_p}(G-1) \subseteq A_1 + I^2$. Now, for every $g - 1 \in G - 1$ and every $g' \in G$,

$$g'(g-1) = (g'g - 1) - (g' - 1) \in \mathrm{Span}_{\mathbb{F}_p}(G-1),$$

so $\mathrm{Span}_{\mathbb{F}_p}(G-1) = \mathrm{Span}_{\mathbb{F}_p[G]}(G-1)$. Since $\mathbb{F}_p[G]$ is dense in $\mathbb{F}_p[[G]]$,

$$I = \mathrm{Span}_{\mathbb{F}_p[[G]]}(G-1) \subseteq A_1 + I^2.$$

This proves the case $n = 1$.

II. Assume that I^{n-1}/I^n is finite. Let

$$I^{n-1} = A_{n-1} + I^n \tag{4.2}$$

be a decomposition of finite abelian groups with A_{n-1} finite. Multiplying by I, we see that

$$I^n \supseteq IA_{n-1} + I^{n+1} \supseteq A_1 A_{n-1} + I^{n+1}.$$

Again, since $A_1 A_{n-1}$ is finite and I^{n+1} is closed, $A_1 A_{n-1} + I^{n+1}$ is a closed subset of I^n. Now repeat the argument used in the first case to see that $A_1 A_{n-1} + I^{n+1} \subseteq I^n$: by Equation (4.2), we see that

$$(s_i - 1)I^{n-1} = (s_i - 1)A_{n-1} + (s_i - 1)I^n \subseteq A_{n-1}A_1 + I^{n+1}.$$

Using Equation (4.1) and a closure argument, we deduce that $(G-1)I^{n-1} \subseteq A_1 A_{n-1} + I^{n+1}$. As in the previous case, this implies that $\operatorname{Span}_{\mathbb{F}_p[G]}((G-1)I^{n-1}) \subseteq A_1 A_{n-1} + I^{n+1}$ and, since $\mathbb{F}_p[G]$ is dense in $\mathbb{F}_p[[G]]$,

$$\operatorname{Span}_{\mathbb{F}_p[[G]]}\left((G-1)I^{n-1}\right) \subseteq A_{n-1}A_1 + I^{n+1}.$$

Since $A_1 A_{n-1} + I^{n+1}$ is closed, we see that $I^n \subseteq A_1 A_{n-1} + I^{n+1}$. This implies that I^n/I^{n+1} is finite. □

Now, we can prove the following theorem:

Theorem 4.2.4. *Let G be a finitely generated pro-p group. Then $\{I^n(G) \mid n \in \mathbb{Z}^+\}$ is an open neighbourhood basis at $0 \in \mathbb{F}_p[[G]]$.*

Proof. By Lemma 4.2.3, the ideals $I^n(G)$ have finite index in $\mathbb{F}_p[[G]]$ and therefore are open. Consider the maps

$$\varphi_U : \mathbb{F}_p[[G]] \longrightarrow \mathbb{F}_p\left[{}^{G}\!/\!{}_{U}\right],$$

with $U \in \mathfrak{U}_G$. The set $\{\ker(\varphi_U) \mid U \in \mathfrak{U}_G\}$ is a neighbourhood basis at 0. Thus, it remains to show that for every $U \in \mathfrak{U}_G$, there is an $n \in \mathbb{Z}^+$ such that $I^n(G) \subseteq \ker(\varphi_U)$.

Take $g_1, \ldots, g_n \in G$ and $\lambda_0(g_1 - 1)\lambda_1 \cdots \lambda_{n-1}(g_n - 1)\lambda_n \in (I(G))^n$. Then,

$$\varphi_U\Big(\lambda_0(g_1 - 1)\lambda_1 \cdots \lambda_{n-1}(g_n - 1)\lambda_n\Big) = \overline{\lambda_0}(\overline{g_1} - 1)\overline{\lambda_1} \cdots \overline{\lambda_{n-1}}(\overline{g_n} - 1)\overline{\lambda_n} \in I^n(G/U)$$

Since $I^n(G/U)$ is a closed ideal and φ_U is continuous, $\varphi_U(I^n(G)) \subseteq I^n(G/U)$. By Lemma 4.2.2, $I^n(G/U) = 0$ for sufficiently large n. Therefore, $I^n(G) \subseteq \ker(\varphi_U)$ for sufficiently large n. □

The descending filtration $\{I^n(G) \mid n \in \mathbb{Z}^+\}$ induces a filtration in G defined in the following way:

Definition 4.2.5. The *Zassenhaus filtration* filtration of a pro-p group G is the descending filtration given by

$$G_n := \{g \in G \mid g - 1 \in I^n(G)\}$$

Remark. One can easily see using Equation (4.1) that G_n are normal subgroups of G.

In fact, it can be proved (Theorem 7.11 in [Koc02]) that this filtration is an open neighbourhood basis at 1. The Zassenhaus filtration will be used in the following section to introduce the Golod-Shafarevich groups. Now we will introduce another filtration that will be used on Chapter 6 in the solution of the class field tower problem.

Let G be a pro-p group. Write $\mathrm{Fr}^0(G) = G$ and $\mathrm{Fr}^n(G) = \mathrm{Fr}\left(\mathrm{Fr}^{n-1}(G)\right)$ for $n \geq 1$. Note that $\mathrm{Fr}^n(G)$ are pro-p since they are closed subgroups of a pro-p group. This is known as the *Frattini series*. One can show that G is finitely generated if, and only if, $\mathrm{Fr}^n(G)$ is open in G for all $n \geq 0$. In this case, $\bigcap_{n\geq 0} \mathrm{Fr}^n(G) = \{1\}$ and $\{\mathrm{Fr}^n(G) \mid n \geq 0\}$ is an open neighbourhood basis at 1. The proof of these facts can be found in [Lub82] and [Sem02].

4.3 The Golod-Shafarevich Inequality

In this section we will define Golod-Shafarevich groups using the Zassenhaus filtration introduced in Section 4.2. The Golod-Shafarevich inequality will give us a sufficient condition for a pro-p group to be Golod-Shafarevich, and hence infinite.

Assume that we have a finitely generated pro-p group G and a minimum presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1. \tag{4.3}$$

Recall that the generator rank $d(G) := \dim_{\mathbb{F}_p}(\mathrm{H}^1(G))$ equals the minimum number of generators of G. Since the presentation (4.3) is minimal, $d(G) = d(F)$. We write $d = d(G)$ for simplicity. Recall also that the relation rank $r(G) := \dim_{\mathbb{F}_p}(\mathrm{H}^2(G))$ equals the minimum number of relations of G. Again, for simplicity, we write $r = r(G)$.

Definition 4.3.1. The *level* of $r \in R$ is the unique positive integer m such that $r \in F_m \setminus F_{m+1}$, where $\{F_n \mid n \in \mathbb{Z}^+\}$ is the Zassenhaus filtration of F. We wite $\mathrm{lv}(r) = m$.

Let $E \subseteq R$ be a generating system of relations of G with respect to the presentation (4.3). We introduce the following notations:

$$a_n = \begin{cases} \dim_{\mathbb{F}_p} \left({}^{I^n(G)}\!\big/_{I^{n+1}(G)} \right) & \text{if } n \geq 1 \\ 1 & \text{if } n = 0. \end{cases}$$

$$E_n = \{r \in E \bigm| \operatorname{lv}(r) = n\}, \quad n \geq 1.$$

$$r_n = \begin{cases} |E_n| & \text{if } n \geq 1, \\ 1 & \text{if } n = 0. \end{cases}$$

Note that the definition of $a_n = \dim_{\mathbb{F}_p}(I^n(G)/I^{n+1}(G))$ also generalizes for $n = 0$ if we define $I^0(G) := \mathbb{F}_p[[G]]$, as Lemma 4.1.5 tells us that $\dim_{\mathbb{F}_p}(\mathbb{F}_p[[G]]/I(G)) = 1$. Note also that the sets E_n can be chosen to be finite because of our assumptions. We have the following lemma:

Lemma 4.3.2. *Assume the above setting and define*

$$b_n := \sum_{k=0}^{n} a_k.$$

Then,

$$-b_{n-1}d + \sum_{k=0}^{n} b_k r_{n-k} \geq 1$$

for all $n \geq 1$.

The proof of this lemma is rather long and complicate. The main idea is to establish an isomorphism between the complete group algebra $\mathbb{F}_p[[F]]$ of a free pro-p group F and the Magnus algebra $\mathbb{F}_p(I)$ defined in Section 2.2, consisting on the formal power series in non-commutative variables x_i with coefficients in $\mathbb{F}_p$. The explanation on how to construct this isomorphism, as well as the proof of this theorem, can be found on pages 68-71 in [Koc02].

A direct consequence of this lemma is the following theorem. To formulate it, we define the following Hilbert series:

$$\operatorname{Hilb}_A(t) = \sum_{n=0}^{\infty} a_n t^n, \qquad \operatorname{Hilb}_R(t) = \sum_{n=1}^{\infty} r_n t^n.$$

Theorem 4.3.3. *In the above setting, we have*

$$\frac{\big(1 - dt + \operatorname{Hilb}_R(t)\big) \cdot \operatorname{Hilb}_A(t)}{1-t} \geq \frac{1}{1-t},$$

where $\frac{1}{1-t} = \sum_{n \geq 0} t^n$.

Proof. Recall that given two formal series $F(t) = \sum_{n\geq 0} f_n t^n$ and $G(t) = \sum_{n\geq 0} g_n t^n$, we say that $F(t) \geq G(t)$ if $f_n \geq g_n$ for all $n \geq 0$. Computing the products of the formal series involved in the inequality we obtain that

$$\frac{\big(r_0 - dt + \mathrm{Hilb}_R(t)\big) \cdot \mathrm{Hilb}_A(t)}{1-t} = 1 + \sum_{n=1}^{\infty} \left(-b_{n-1}d + \sum_{k=0}^{n} b_k r_{n-k} \right) t^n.$$

The claim follows from Lemma 4.3.2. □

Definition 4.3.4. Let G be a finitely generated pro-p group with a presentation as in (4.3) and assume $E \subseteq R$ is a minimum generating system of relations with respect to that presentation. We say that G is a *Golod-Shafarevich group* if there exist a real number $\tau \in (0,1)$ such that $1 - d\tau + \mathrm{Hilb}_R(\tau) < 0$.

Remark. This definition can be generalized to any abstract group G saying that G is a Golod-Shafarevich group (with respect to p) if its pro-p completion $G_{\widehat{p}}$ is Golod-Shafarevich. However, we are only interested in pro-p groups. Hence, from now on, a Golod-Shafarevich group will refer to a Golod-Shafarevich pro-p group.

Lemma 4.3.5. *Let G be a Golod-Shafarevich group and $\tau \in (0,1)$ such that $1 - d\tau + \mathrm{Hilb}_R(\tau) < 0$. Then,*

(i) $\mathrm{Hilb}_A(\tau)$ *diverges.*

(ii) $\dim_{\mathbb{F}_p} \mathbb{F}_p[[G]] = \infty$.

Proof. (*i*) Observe that the series $\sum_{n\geq 0} t^n$ converges to $1/(1-\tau)$ when we evaluate it at τ. Suppose that $\mathrm{Hilb}_A(\tau)$ converges. Take the inequality in Theorem 4.3.3 and evaluate it at τ. Since $\tau > 0$ and all the series converge, the same inequality hols after evaluating at τ. Then

$$\big(1 - d\tau + \mathrm{Hilb}_R(\tau)\big) \cdot \mathrm{Hilb}_A(\tau) \geq 1.$$

Note that $a_0 = 1$ and $a_n \geq 0$ for all $n \geq 0$. Thus, $\mathrm{Hilb}_A(\tau) > 0$ and we get a contradiction.

(*ii*) Since $a_n = \dim_{\mathbb{F}_p}(I^n(G)/I^{n+1}(G))$ for all $n \geq 0$, $\sum_{n\geq 0} a_n = \dim_{\mathbb{F}_p}(\mathbb{F}_p[[G]])$. If $\mathbb{F}_p[[G]]$ was finite-dimensional, $\mathrm{Hilb}_A(t)$ would be a finite sum, and therefore would converge for any $t \in (0,1)$. From (*i*), $\mathrm{Hilb}_A(\tau)$ diverges, so $\mathbb{F}_p[[G]]$ must be infinite-dimensional. □

Corollary 4.3.6. *Golod-Shafarevich groups are infinite.*

Proof. Let G be a Golod-Shafarevich group. If G was finite, it would have finitely many open subsets and hence $\mathfrak{U}_G$ would be finite. But then,

$$\mathbb{F}_p[[G]] = \varprojlim_{U \in \mathfrak{U}_G} \mathbb{F}_p\left[{}^{G}\!/\!{}_{U}\right] \subseteq \prod_{U \in \mathfrak{U}_G} \mathbb{F}_p\left[{}^{G}\!/\!{}_{U}\right]$$

would be finite dimension, contradicting Lemma 4.3.5. Thus, G must be infinite □

Now we turn to the famous inequality $d^2/4 > r$ for Golod-Shafarevich pro-p groups that is used in the solution of the class field tower problem:

Theorem 4.3.7 (Golod-Shafarevich inequality)**.** *Let G be a finitely generated pro-p group with $d > 1$. If*

$$\frac{d^2}{4} > r,$$

then G is Golod-Shafarevich.

Proof. Suppose we have a minimum presentation of G as in (4.3). Let $E \subseteq R$ be a minimum generating system of relations with respect to that presentation. Then, $\sum_{n\geq 1} r_n = \left|E\right| = r$. Note first that $r_1 = 0$, that is, E has no relations of level 1. This could easily be seen by the isomorphism between $\mathbb{F}_p[[G]]$ and the Magnus algebra $\mathbb{F}_p(x_1, \ldots, x_d)$, as a level 1 relation would allow us to express one of the generators x_i as a linear combination of the others, contradicting the minimality of $\mathbb{F}_p(x_1, \ldots, x_d)$ and hence the minimality of F. Therefore, for any $\tau \in (0, 1)$, we have

$$1 - d\tau + \mathrm{Hilb}_R(\tau) \leq 1 - d\tau + r\tau^2. \tag{4.4}$$

If $d = 2$, necessary $r = 0$, and we see that any $\tau \in (1/2, 1)$ satisfies that $1-d\tau < 0$ and hence G is Golod-Shafarevich. Suppose so that $d \geq 3$. We proceed by contrapositive. If G is not Golod-Shafarevich, then $1 - d\tau + \mathrm{Hilb}_R(\tau) \geq 0$ for all $\tau \in (0, 1)$. In particular, this is true for $\tau = 2/d \in (0, 1)$ (note that we have treated separately the case $d = 2$). Combining this fact with Equation (4.4), we obtain that $d^2/4 \leq r$. □

Remark. Using a similar reasoning we could prove that if $d^2/4 \geq r$, then G must be infinite, but not necessary Golod-Shafarevich. This relies on the fact that if there exist $\tau \in (0, 1)$ such that $1 - d\tau + \mathrm{Hilb}_R(\tau) \leq 0$, then Lemma 4.3.5 also holds (we don't need the strict inequality as happens for Golod-Shafarevich groups). In this case, the theorem would also hold for $d = 1$ (for more details see [Ers12]).

Chapter 5

Results from Algebraic Number Theory

In the first four chapters we focused our study on profinite groups to be able to define a Golod-Shafarevich group and establish a criterion for a pro-p group to be Golod-Shafarevich in terms of its generators and relations. Now we change the subject completely. In this chapter we will give all the necessary results in algebraic number theory to be able to formulate and solve the class field tower problem. We will assume some basic knowledge of number fields and ring of integers. For instance, we will assume the theory given in the first three chapters in [Mar18] and in the first two chapters in [Jan96].

5.1 Splitting of Primes in Extensions

In this first section we will remind some of the general aspects of the splitting of primes in a finite extension of number fields. This will help us introduce the notation we will follow in the next sections.

Let K be a number field. We denote by $\mathcal{O}_K$ its ring of integers. For every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and any real constant $c \in (0,1)$, the function $|\alpha|_{\mathfrak{p}} = c^{\mathrm{ord}_{\mathfrak{p}}(\alpha)}$ for $\alpha \in K^*$ (and $|0|_{\mathfrak{p}} = 0$) defines a nonarchimedean valuation on K. We call this a $\mathfrak{p}$-*adic valuation*. For any two different primes ideals $\mathfrak{p}$ and $\mathfrak{q}$, a $\mathfrak{p}$-adic valuation and $\mathfrak{q}$-adic valuation are inequivalent.

On the other side, any embedding σ of K into $\mathbb{R}$ or $\mathbb{C}$ give rise to an archimedean valuation by putting $|\alpha|_\sigma = |\sigma(\alpha)|$, where $|\cdot|$ is the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$. Two embeddings give rise to equivalent valuations if, and only if, they are complex-conjugates.

Ostrowski's theorem tells us that any valuation on K is equivalent to a $\mathfrak{p}$-adic valuation or to a valuation coming from a real or complex embedding of K. An equivalence class of valuations on K is called a *prime* of K. By tradition, a prime is called an *infinite prime* if it contains an archimedean valuation, and a *finite prime* otherwise. We shall now describe how primes split when extended to a finite extension L of K. Let's begin with finite primes.

Every finite prime of K can be uniquely identified with a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. We can describe how a prime splits when extended in L by describing how $\mathfrak{p}$ splits when extended in $\mathcal{O}_L$. From now on, the term "prime ideal" will be used to mean "nonzero prime ideal".

Fix a prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$. We denote by $\mathfrak{p}O_L$ the ideal generated by $\mathfrak{p}$ in $\mathcal{O}_L$. If a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ divides $\mathfrak{p}\mathcal{O}_L$, we say that $\mathfrak{P}$ *lies over* $\mathfrak{p}$ or that $\mathfrak{p}$ *lies under* $\mathfrak{P}$. Every prime ideal of $\mathcal{O}_L$ lies over a unique prime ideal of $\mathcal{O}_K$ and every prime ideal of $\mathcal{O}_K$ lies under at least one prime ideal of $\mathcal{O}_L$.

The primes lying over $\mathfrak{p}$ are exactly the ones which occur in the prime decomposition of $\mathfrak{p}\mathcal{O}_L$. The exponent with which they occur are called the *ramification indices*. Thus, if $\mathfrak{P}^e$ is the exact power of $\mathfrak{P}$ dividing $\mathfrak{p}\mathcal{O}_L$, then e is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, denoted by $e(\mathfrak{P}|\mathfrak{p})$. We say that $\mathfrak{p}$ is *unramified* if $e(\mathfrak{P}|\mathfrak{p}) = 1$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$, and *ramified* otherwise.

If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$, the residue field $\mathcal{O}_K/\mathfrak{p}$ is canonically embedded into the residue field $\mathcal{O}_L/\mathfrak{P}$. The degree of this extension is called the *inertial degree* of $\mathfrak{P}$ over $\mathfrak{p}$, and it is denoted by $f(\mathfrak{P}|\mathfrak{p})$. The inertial degree is always finite, since it is bounded by $[L : K]$.

Notice that e and f are multiplicative in towers: if $\mathfrak{p}_K \subset \mathfrak{p}_L \subset \mathfrak{p}_E$ are prime ideals of the ring of integers of three number fields $K \subset L \subset E$, then

$$e(\mathfrak{p}_E|\mathfrak{p}_K) = e(\mathfrak{p}_E|\mathfrak{p}_L)e(\mathfrak{p}_L|\mathfrak{p}_K),$$
$$f(\mathfrak{p}_E|\mathfrak{p}_K) = f(\mathfrak{p}_E|\mathfrak{p}_L)f(\mathfrak{p}_L|\mathfrak{p}_K).$$

Ramification indices, inertial degrees and the degree of the extension L/K are related by the following formula:

Theorem 5.1.1. *Let n be the degree of L over K and let $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ be the prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Denote by $e_1, \dots, e_r$ and $f_1, \dots, f_r$ the corresponding ramification indices and inertial degrees. Then,*

$$\sum_{i=1}^{r} e_i f_i = n.$$

We say that $\mathfrak{p}$ *splits completely* if $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Theorem 5.1.1 tells us that this is equivalent to saying that there are exactly $[L : K]$ different primes ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$.

If L is a Galois extension of K, it is easy to see that the Galois group of L over K permutes the prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$ transitively. In other words, if $\mathfrak{P}$

is a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$ and $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\mathfrak{P})$ is also a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Moreover, those are all prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$. As a consequence, all prime ideals lying over $\mathfrak{p}$ have the same ramification index and inertial degree.

Let's now describe how infinite primes split when extended in a finite extension L of K. An infinite prime $\mathfrak{p}$ of K is called a *real prime* if the completion of K with respect to any valuation contained in $\mathfrak{p}$ is $\mathbb{R}$. Similarly, $\mathfrak{p}$ is called a *complex prime* if the completion of K with respect to any valuation contained in $\mathfrak{p}$ is $\mathbb{C}$. Thus, the real primes of K correspond to the distinct embeddings of K into $\mathbb{R}$ and the complex primes correspond to the conjugate pairs of embeddings of K into $\mathbb{C}$. We will describe how $\mathfrak{p}$ splits when extended in L by describing how its corresponding embedding can be extended to different embeddings of L into $\mathbb{R}$ or $\mathbb{C}$.

Consider first that $\mathfrak{p}$ is a complex prime of K and let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding of K into $\mathbb{C}$ such that $|\sigma(x)|$ is in $\mathfrak{p}$. As $\mathbb{C}$ is algebraically closed, we know from Galois theory that there are exactly $n = [L : K]$ different embeddings $\sigma_i : L \hookrightarrow \mathbb{C}$ such that $\sigma_i|_K = \sigma$. No two σ_i can be conjugates, as then they could not agree on K. Hence, they represent n distinct complex infinite primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ of L. We can write

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_n$$

to indicate that the $\mathfrak{P}_i$ are the primes of L extending $\mathfrak{p}$. In this case, we define the ramification indices $e(\mathfrak{P}_i|\mathfrak{p})$ and the inertial degrees $f(\mathfrak{P}_i|\mathfrak{p})$ to be one. We will say that the complex prime $\mathfrak{p}$ is unramified in L (because all ramification indices are one). Thus, in this case the formula $\sum_{i=1}^{n} e_i f_i = n$ holds.

Consider now that $\mathfrak{p}$ is a real prime of K and let $\sigma : K \hookrightarrow \mathbb{R}$ be the corresponding embedding. Regarding σ as an embedding from K into $\mathbb{C}$, we can apply Galois theory again to assure the existence of exactly $n = [L : K]$ different extensions of σ to L, some of which may have an image insider $\mathbb{R}$. List the extensions of σ as

$$\sigma_1, \ldots \sigma_r, \sigma_{r+1}, \overline{\sigma}_{r+1}, \ldots \sigma_{r+s}, \overline{\sigma}_{r+s},$$

where $\sigma_i(L) \subset \mathbb{R}$ for $1 \leq i \leq r$ and $\sigma_{r+j}, \overline{\sigma}_{r+j}$ give s pairs of complex conjugate embeddings of L into $\mathbb{C}$. Note that $r + 2s = n$. This give rise to r distinct real primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ and s distinct complex primes $\mathfrak{P}_{r+1}, \ldots, \mathfrak{P}_{r+s}$ of L extending $\mathfrak{p}$. We define the ramification indices as follows: if $\mathfrak{P}_i$ is a real prime of L lying over $\mathfrak{p}$, we set $e(\mathfrak{P}_i|\mathfrak{p}) = 1$. If $\mathfrak{P}_{r+j}$ is a complex primes, we set $e(\mathfrak{P}_{r+j}|\mathfrak{p}) = 2$. We define all inertial degrees to be one. Thus, we formally write

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r \mathfrak{P}_{r+1}^2 \cdots \mathfrak{P}_{r+s}^2.$$

Note that the we still have the formula $\sum_{i=1}^{r+s} e_i f_i = n$.

5.2 Galois Theory Applied to Prime Decomposition

In this section we will apply Galois theory to the general problem of determining how primes of a number field split in an extension field. We will find connections between the ramification indices and the inertial degrees introduced in the previous section with some subgroups of the Galois groups of this extension. Some parts of our discussion will be valid for both finite and infinite primes, although we will mostly restrict to finite primes, as the notions of Frobenius automorphism and Artin map are directly related to finite primes. In this section, all finite primes of a number field K may be identified with the corresponding prime ideal of $\mathcal{O}_K$.

Let K and L be number fields, and assume that L is a Galois extension of K. Let G be the Galois group of L over K and assume that the degree of the extension is $n = [L : K]$. Let $\mathfrak{p}$ be a finite prime of K. Recall that all primes $\mathfrak{P}$ of L lying over $\mathfrak{p}$ have the same ramification index e and inertial degree f. Thus, if there are r of such primes $\mathfrak{P}$, by Theorem 5.1.1, $ref = n$.

Definition 5.2.1. For each prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$, we define the *decomposition group* as

$$D = D(\mathfrak{P}|\mathfrak{p}) = \{\, \sigma \in G \;\big|\; \sigma(\mathfrak{P}) = \mathfrak{P} \,\}$$

and the *inertia group* as

$$E = E(\mathfrak{P}|\mathfrak{p}) = \{\, \sigma \in G \;\big|\; \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \;\; \forall\, \alpha \in \mathcal{O}_L \,\}.$$

Remark. D and E are subgroups of G with $E \subseteq D$, as the condition $\sigma(\mathfrak{P}) = \mathfrak{P}$ can be expressed as $\sigma(\alpha) \equiv 0 \pmod{\mathfrak{P}}$ if, and only if, $\alpha \equiv 0 \pmod{\mathfrak{P}}$.

The elements of D induce automorphisms of the field $\mathcal{O}_L/\mathfrak{P}$ in a natural way: Every $\sigma \in G$ restricts to an automorphism of $\mathcal{O}_L$ and, if $\sigma \in D$, the induced mapping $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$ has kernel $\mathfrak{P}$. Thus, each $\sigma \in D$ induces an automorphism $\overline{\sigma}$ of $\mathcal{O}_L/\mathfrak{P}$ that makes the following diagram commutative:

$$\begin{tikzcd}
\mathcal{O}_L \arrow[r, "\sigma"] \arrow[d] & \mathcal{O}_L \arrow[d] \\
\mathcal{O}_L/\mathfrak{P} \arrow[r, "\overline{\sigma}"] & \mathcal{O}_L/\mathfrak{P}
\end{tikzcd}$$

Moreover, it is clear that $\overline{\sigma}$ fixes the subfield $\mathcal{O}_k/\mathfrak{p}$ pointwise since σ fixes K. Thus, $\overline{\sigma}$ is an element of the Galois group $\overline{G}$ of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$. In other words, we have a mapping $D \to \overline{G}$, and it is easy to see that it is a group homomorphism. The kernel of this morphism is easily seen to be E. This information is summarized in the following lemma:

Lemma 5.2.2. *The mapping*

$$\begin{array}{ccc} D & \longrightarrow & \overline{G} \\ \sigma & \longmapsto & \overline{\sigma} \end{array}$$

is a group homomorphism with kernel E.

This shows that E is a normal subgroup of D. We will see that $D \to \overline{G}$ is actually onto, and hence $D/E \to \overline{G}$ is a group isomorphism.

Definition 5.2.3. The *decomposition field* L_D is the subfield of L fixed by D and the *inertia field* L_E is the subfield of L fixed by E.

In general, we adopt the following notation: For a subgroup H of G, L_H denotes the fixed field of H, and $\mathfrak{P}_H = \mathfrak{P} \cap L_H$ is the unique prime ideal of $\mathcal{O}_{L_H}$ lying under $\mathfrak{P}$. Clearly, $\mathfrak{P}_H$ lies over $\mathfrak{p}$ and $\mathcal{O}_{L_H}/\mathfrak{P}_H$ is an intermediate field between $O_L/\mathfrak{P}$ and $\mathcal{O}_K/\mathfrak{p}$.

We can now state the main result:

Theorem 5.2.4. *With the notations above, we have the following:*

DEGREES	L	$\mathfrak{P}$	RAMIFICATION INDICES	INERTIAL DEGREES
e	|	|	e	1
	L_E	$\mathfrak{P}_E$		
f	|	|	1	f
	L_D	$\mathfrak{P}_D$		
r	|	|	1	1
	K	$\mathfrak{p}$		

Proof. We begin by showing that $[L_D : K] = r$. By Galois theory we know that $[L_D : K]$ is the same as the index of D in G. As D fixes $\mathfrak{P}$, each coset σD, $\sigma \in G$, sends $\mathfrak{P}$ to $\sigma(\mathfrak{P})$. It is clear that $\sigma D = \tau D$ if, and only if $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$. This establishes a one-to-one correspondence between the left cosets σD and the prime ideals $\sigma(\mathfrak{P})$. As we explained in the previous section, G permutes the prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$ transitively. Hence, $\{\sigma(\mathfrak{P}) \mid \sigma \in G\}$ are exactly all the prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$. This shows what we wanted.

Next we show $e(\mathfrak{P}_D|\mathfrak{p}) = f(\mathfrak{P}_D|\mathfrak{p}) = 1$. Note first that $\mathfrak{P}$ is the only prime of $\mathcal{O}_L$ lying over $\mathfrak{P}_D$, since such primes are necessarily permuted transitively by the Galois group of L over L_D; this group is D, which fixes $\mathfrak{P}$. It follows by Theorem 5.1.1 that

$$[L : L_D] = e(\mathfrak{P}|\mathfrak{P}_D)f(\mathfrak{P}|\mathfrak{P}_D).$$

Since we have shown that $[L_D : K] = r$ and we know that $[L : K] = ref$, we have that $[L : L_D] = ef$. Moreover, since the ramification indices and inertial degrees are multiplicative in towers, $e(\mathfrak{P}|\mathfrak{P}_D)$ and $f(\mathfrak{P}|\mathfrak{P}_D)$ cannot exceed e and f respectively. Hence, $e(\mathfrak{P}|\mathfrak{P}_D) = e$, $f(\mathfrak{P}|\mathfrak{P}_D) = f$, and we obtain that

$$e(\mathfrak{P}_D|\mathfrak{p}) = f(\mathfrak{P}_D|\mathfrak{p}) = 1.$$

Next we show that $f(\mathfrak{P}|\mathfrak{P}_E) = 1$. By definition, this means showing that $\mathcal{O}_L/\mathfrak{P}$ is the trivial extension of $\mathcal{O}_{L_E}/\mathfrak{P}_E$. We will do this by showing that the Galois group of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_{L_E}/\mathfrak{P}_E$ is trivial. To do this, we will show that for each $\theta \in \mathcal{O}_L/\mathfrak{P}$, the polynomial $(x-\theta)^m$ has coefficients in $\mathcal{O}_{L_E}/\mathfrak{P}_E$ for some $m \geq 1$. It will follow that every member of the Galois group sends θ to another root of $(x-\theta)^m$, which can only be θ. This will prove what we want.

Fix any $\alpha \in \mathcal{O}_L$ corresponding to $\theta \in \mathcal{O}_L/\mathfrak{P}$. Clearly the polynomial

$$g(x) = \prod_{\sigma \in E}(x - \sigma(\alpha))$$

has coefficients in $\mathcal{O}_{L_E}$, as each element of $E = \mathrm{Gal}(L/L_E)$ fixes the coefficients of g. Reducing modulo $\mathfrak{P}$ we find that $\overline{g} \in (\mathcal{O}_L/\mathfrak{P})[x]$ actually has coefficients in $\mathcal{O}_{L_E}/\mathfrak{P}_E$. But, by the definition of E, all $\sigma(\alpha)$ are send to θ when reduced modulo $\mathfrak{P}$. Hence, $\overline{g}(x) = (x-\theta)^m$, where $m = |E|$. That completes the proof that $f(\mathfrak{P}|\mathfrak{P}_E) = 1$.

Using that $f(\mathfrak{P}_D|\mathfrak{p}) = 1$ and the multiplicativity in towers, we get that $f(\mathfrak{P}_E|\mathfrak{P}_D) = 1$. Thus, by Theorem 5.1.1 we must have that $[L_E : L_D] \geq f$. But by Lemma 5.2.2, D/E is embedded in $\overline{G}$, which is a group of order f, and hence $[L_E : L_D] = [D : E] \leq f$. Thus, $[L_E : L_D] = f$. Using Theorem 5.1.1 again, we obtain that $e(\mathfrak{P}_E|\mathfrak{P}_D) = 1$. Finally, we easily obtain that $[L : L_E] = e$ and $e(\mathfrak{P}|\mathfrak{P}_E) = e$ by considering the degrees and ramification indices already established. □

Corollary 5.2.5. *D is mapped onto $\overline{G}$ by the natural map $\sigma \mapsto \overline{\sigma}$. Hence, $D/E \cong \overline{G}$ is cyclic of order f.*

Proof. We have already seen that D/E is embedded in $\overline{G}$. Moreover, both groups have order f, since $[D : E] = [L_E : L_D]$. The fact that $\overline{G}$ is cyclic is a consequence of being a Galois group of a finite extension of finite fields. □

The following special case indicates a reason for the terms "decomposition field" and "inertia field". Even though this corollary won't be needed in Chapter 6, we still present it for completeness.

Corollary 5.2.6. *Suppose D is a normal subgroup of G. Then $\mathfrak{p}$ splits into r distinct primes in L_D. If E is also normal in G, then each of them remains prime (is "inert") in L_E. Finally, each one becomes an e^{th} power in L.*

Proof. If D is normal in G, then L_D is a Galois extension of K. We know that $\mathfrak{P}_D$ has ramification index and inertial degree 1, and hence so does any other prime $\mathfrak{P}'_D$ of L_D lying over $\mathfrak{p}$. By Theorem 5.1.1, there must be r primes of L_D lying over $\mathfrak{p}$. It follows that there must be exactly r primes in L_E lying over $\mathfrak{p}$, since this is true for both L_D and L. This implies that each prime $\mathfrak{P}'_D$ of L_D lying over $\mathfrak{p}$ lies under a unique prime $\mathfrak{P}'_E$ of L_E. If E is normal in G, then L_E is Galois over K, and hence $e(\mathfrak{P}'_E|\mathfrak{p}) = e(\mathfrak{P}_E|\mathfrak{p}) = 1$. This shows that $e(\mathfrak{P}'_E|\mathfrak{P}'_D) = 1$, and thus $\mathfrak{P}'_D$ is inert in L_E. Finally, by multiplicativity of the ramification index, we deduce that $\mathfrak{P}'_E$ becomes an e^{th} power in L. □

Corollary 5.2.7. *Let L/K be a Galois extension of number fields. A finite prime $\mathfrak{p}$ of K is unramified in L if, and only if, for all finite primes $\mathfrak{P}$ of L lying over $\mathfrak{p}$, $E(\mathfrak{P}|\mathfrak{p}) = \{\text{id}\}$.*

Proof. The finite prime $\mathfrak{p}$ is unramified in L if, and only if, $e(\mathfrak{P}|\mathfrak{p})$ for all finite primes $\mathfrak{P}$ of L lying over $\mathfrak{p}$. We have seen that $e(\mathfrak{P}|\mathfrak{p})$ is the degree of the extension L/L_E. Thus, this extension is trivial if, and only if, the inertia group $E(\mathfrak{P}|\mathfrak{p})$ is trivial. □

Definition 5.2.8. We say that an extension of number fields L/K is *unramified* if every prime of K (finite and infinite) is unramified in L. More generally, if S is a set of primes of K, we say that L/K is unramified outside S if all primes of K not belonging to S are unramified in L.

We will now prove two properties about the compositum and lifting of unramified Galois extensions of number fields. This property will be very useful in Chapter 6. First, we will need the following lemmas from Galois theory:

Lemma 5.2.9. *If L/K is Galois, then every lifting LF/F is Galois. In this case, the map*

$$\begin{array}{ccc} \mathrm{Gal}(LF/F) & \hookrightarrow & \mathrm{Gal}(L/K) \\ \sigma & \longmapsto & \sigma|_L \end{array}$$

is a well defined group monomorphism.

Lemma 5.2.10. *The compositum of Galois extensions L/K and F/K is Galois. In this case, the map*

$$\begin{array}{ccc} \mathrm{Gal}(LF/K) & \hookrightarrow & \mathrm{Gal}(L/K) \times \mathrm{Gal}(F/K) \\ \sigma & \longmapsto & (\sigma|_L \, , \, \sigma|_F) \end{array}$$

is a well defined group monomorphism.

Theorem 5.2.11. *Let L/K be an unramified Galois extension of number fields and F a finite extension of K. Then LF/F is unramified.*

Proof. Let's first see that any finite prime of F is unramified in LF. Let $\mathfrak{p}$ be a finite prime of F and $\mathfrak{P}$ a finite prime of LF lying over $\mathfrak{p}$. Note that $\mathfrak{P} \cap \mathcal{O}_L$ is a finite prime of L lying over the finite prime $\mathfrak{P} \cap \mathcal{O}_K$ of K, and that $e(\mathfrak{P} \cap \mathcal{O}_L | \mathfrak{P} \cap \mathcal{O}_K) = 1$. Take $\sigma \in E(\mathfrak{P}|\mathfrak{p})$. Then, for all $\alpha \in \mathcal{O}_L \subseteq \mathcal{O}_{LF}$, we have $\sigma(\alpha) = \sigma|_L(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$. As $\sigma|_L(\alpha) - \alpha \in \mathcal{O}_L$, we also have that $\sigma|_L(\alpha) \equiv \alpha \pmod{\mathfrak{P} \cap \mathcal{O}_L}$. Hence, $\sigma|_L \in E(\mathfrak{P} \cap \mathcal{O}_L | \mathfrak{P} \cap \mathcal{O}_K)$. By Corollary 5.2.7, $\sigma|_L = \mathrm{id}$ and by Lemma 5.2.9, $\sigma = \mathrm{id}$. This shows that $e(\mathfrak{P}|\mathfrak{p}) = 1$ and thus LF/F is unramified at the finite primes.

Let's now see that any infinite prime of F is unramified in LF. Let $\mathfrak{p}$ be an infinite prime of F and $\mathfrak{P}$ an infinite prime of LF lying over $\mathfrak{p}$. By Section 5.1, we know that $\mathfrak{p}$ correspond to an embedding σ of F into $\mathbb{C}$ and $\mathfrak{P}$ corresponds to an embedding τ of LF into $\mathbb{C}$ with $\tau|_F = \sigma$. If $\mathfrak{p}$ is a complex prime, $\mathfrak{p}$ is unramified, so suppose that $\mathfrak{p}$ is a real prime, i.e. $\sigma(F) \subset \mathbb{R}$. We must show that $\tau(LF) \subset \mathbb{R}$ to see that $e(\mathfrak{P}|\mathfrak{p}) = 1$. Note that $\tau|_L$ corresponds to an infinite prime of L lying over an infinite prime of K corresponding to $\tau|_K$. Note also that $\tau|_K = \sigma|_K$ is a real embedding and, since L/K is unramified, the image of $\tau|_L$ must also lie inside $\mathbb{R}$. Now take any $\alpha \in FL$ and write $\alpha = \sum_i \beta_i \gamma_i$ with $\beta_i \in L$ and $\gamma_i \in F$. Then

$$\tau(\alpha) = \sum_i \tau(\beta_i)\tau(\gamma_i) = \sum_i \tau|_L(\beta_i)\sigma(\gamma_i) \in \mathbb{R}.$$

This implies that $\tau(LF) \subset \mathbb{R}$ and hence $e(\mathfrak{P}|\mathfrak{p}) = 1$. □

Theorem 5.2.12. *Let L/K and F/K be Galois extensions of number fields. Let S be a set of primes of K. Suppose L/K and F/K are unramified outside S. Then, LF/K is also unramified outside S.*

Proof. For the case of finite primes, take a finite prime $\mathfrak{p} \notin S$ of K and let $\mathfrak{P}$ be a prime of LF lying over $\mathfrak{p}$. Then, $\mathfrak{P} \cap \mathcal{O}_L$ and $\mathfrak{P} \cap \mathcal{O}_F$ are finite primes of L and F lying over $\mathfrak{p}$ respectively. Take $\sigma \in E(\mathfrak{P}|\mathfrak{p})$. Using the same argument as in the previous proof, one can see that $\sigma|_L \in E(\mathfrak{P} \cap \mathcal{O}_L|\mathfrak{p})$ and $\sigma|_F \in E(\mathfrak{P} \cap \mathcal{O}_F|\mathfrak{p})$. Since L/K and F/K are unramified at $\mathfrak{p}$, we have that $\sigma|_L = \mathrm{id}_L$ and $\sigma|_F = \mathrm{id}_F$. Then, by Lemma 5.2.10, $\sigma = \mathrm{id}$ and $e(\mathfrak{P}|\mathfrak{p}) = 1$.

For the case of infinite primes, let $\mathfrak{P}$ be an infinite prime of LF lying over an infinite prime $\mathfrak{p} \notin S$ of K. $\mathfrak{p}$ corresponds to an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and $\mathfrak{P}$ corresponds to an embedding $\tau : LF \hookrightarrow \mathbb{C}$ with $\tau|_K = \sigma$. Suppose $\mathfrak{p}$ is a real prime (otherwise we already know it is unramified). The restriction of τ to L and F correspond to infinite primes of L and F lying over $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in L and F, $\tau(L), \tau(F) \subset \mathbb{R}$. Writing any element of LF in terms of elements of L and F we deduce that $\tau(FL) \subset \mathbb{R}$ and so $e(\mathfrak{P}|\mathfrak{p}) = 1$. □

Corollary 5.2.13. *Let L/K and F/K be unramified Galois extensions of number fields. Then, LF/K is unramified.*

Proof. Apply Theorem 5.2.12 with $S = \emptyset$. □

Assume L/K is a Galois extension of number fields and $\mathfrak{P}$ a finite prime of L lying over a finite prime $\mathfrak{p}$ of K. We are interested in knowing what happens to the groups $D(\mathfrak{P}|\mathfrak{p})$ and $E(\mathfrak{P}|\mathfrak{p})$ when we replace $\mathfrak{P}$ by another prime $\mathfrak{P}'$ of L lying over the same $\mathfrak{p}$. As explained in Section 5.1, $\mathfrak{P}' = \sigma(\mathfrak{P})$ for some $\sigma \in G = \mathrm{Gal}(L/K)$. It is easy to see that

$$D(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma D(\mathfrak{P}|\mathfrak{p})\sigma^{-1},$$
$$E(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma E(\mathfrak{P}|\mathfrak{p})\sigma^{-1}.$$

Thus, D and E are just replaced by conjugate subgroups of G. In particular, we see that when G is abelian, the groups $D(\mathfrak{P}|\mathfrak{p})$ and $E(\mathfrak{P}|\mathfrak{p})$ depend only on $\mathfrak{p}$, not on $\mathfrak{P}$.

5.3 The Frobenius Automorphism and the Artin Map

In this section we will introduce two notions that play an important role in class field theory: the Frobenius automorphism and the Artin map. This map will help us understand some important properties of the Hilbert class field, as we will explain in Section 5.4.

Assume that L/K is a Galois extension of number fields, and let $\mathfrak{P}$ be a finite prime of L lying over a finite prime $\mathfrak{p}$ of K. Assume that $\mathfrak{p}$ is unramified in L, so that $E(\mathfrak{P}|\mathfrak{p})$ is trivial. In this case, we have an isomorphism from the decomposition group $D = D(\mathfrak{P}|\mathfrak{p})$ to the Galois group $\overline{G}$ of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$. $\overline{G}$ is cyclic of order $f(\mathfrak{P}|\mathfrak{p})$, and has a special generator: the mapping which sends every $x \in \mathcal{O}_L/\mathfrak{P}$ to $x^{||\mathfrak{p}||}$, where $||\mathfrak{p}|| := \left|\mathcal{O}_K/\mathfrak{p}\right|$. The corresponding automorphism $\phi \in D$ satisfies that

$$\phi(\alpha) \equiv \alpha^{||\mathfrak{p}||} \pmod{\mathfrak{P}}$$

for every $\alpha \in \mathcal{O}_L$. Since $\mathfrak{p}$ is unramified, ϕ is the only element in D with this property, and in fact the only element in G (this property clearly implies that $\phi \in D$).

Definition 5.3.1. The described automorphism is called the *Frobenius automorphism.* We denote it by $\phi(\mathfrak{P}|\mathfrak{p})$ to indicate its dependence with $\mathfrak{P}$ and $\mathfrak{p}$.

Lemma 5.3.2. *Let $\sigma \in \mathrm{Gal}(L/K)$. Then $\sigma(\mathfrak{P})$ also lies over $\mathfrak{p}$ and*

$$\phi(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma\phi(\mathfrak{P}|\mathfrak{p})\sigma^{-1}.$$

Proof. For every $\alpha \in \mathcal{O}_L$, we have $\phi(\sigma(\mathfrak{P})|\mathfrak{p})(\alpha) - \alpha^{||\mathfrak{p}||} \in \sigma(\mathfrak{P})$. Substituting α by $\sigma(\alpha)$ and applying σ^{-1} we obtain that $(\sigma^{-1}\phi(\sigma(\mathfrak{P})|\mathfrak{p})\sigma)(\alpha) - \alpha^{||\mathfrak{p}||} \in \mathfrak{P}$ for every $\alpha \in O_L$, and hence $\phi(\mathfrak{P}|\mathfrak{p}) = \sigma^{-1}\phi(\sigma(\mathfrak{P})|\mathfrak{p})\sigma$. □

We have already seen that all primes over $\mathfrak{p}$ are of the form $\sigma(\mathfrak{P})$ for some $\sigma \in G = \mathrm{Gal}(L/K)$. Thus, the conjugacy class of $\phi(\mathfrak{P}|\mathfrak{p})$ is uniquely determined by $\mathfrak{p}$. In particular, when G is abelian, $\varphi(\mathfrak{P}|\mathfrak{p})$ itself is uniquely determined by the unramified prime $\mathfrak{p}$. This ϕ satisfies the same congruence for all primes lying over it, and hence it satisfies

$$\phi(\alpha) \equiv \alpha^{||\mathfrak{p}||} \pmod{\mathfrak{p}\mathcal{O}_L}.$$

Part of the significance of the Frobenius automorphism is that indicates how $\mathfrak{p}$ splits in L, as its order is the inertial degree. Thus, for example, an unramified prime $\mathfrak{p}$ splits completely in the Galois extension L if, and only if, $\phi(\mathfrak{P}|\mathfrak{p}) = \mathrm{id}$ for all $\mathfrak{P}$ lying over $\mathfrak{p}$.

Assume now that L is an abelian extension of K, that is, a Galois extension of K with abelian Galois group. The ideal group I_K is the group of fractional ideals of K, i.e., the group of O_K-submodules of K. As happens with the ideals of $\mathcal{O}_K$, any fractional ideal can be uniquely express as a product (with integer exponents) of prime ideals of $\mathcal{O}_K$. Hence, I_K is a free abelian group generated by the prime ideals of $\mathcal{O}_K$. Let P be the set of all (nonzero) prime ideals of $\mathcal{O}_K$ and S the subset of P of all primes that ramify in L. Denote by I_K^S the subgroup of I_K generated by $P \setminus S$. Then, an element of I_K^S has the form

$$\mathfrak{U} = \prod_{\mathfrak{p} \in P \setminus S} \mathfrak{p}^{a(\mathfrak{p})} \tag{5.1}$$

where almost all the exponents are zero.

Definition 5.3.3. We define the *Artin map* as the following group morphism:

$$\begin{array}{rccc} \Phi_{L/K}: & I_K^S & \longrightarrow & \mathrm{Gal}(L/K) \\ & \mathfrak{U} & \longmapsto & \displaystyle\prod_{\mathfrak{p} \in P \setminus S} \phi(\mathfrak{P}|\mathfrak{p})^{a(\mathfrak{p})} \end{array}$$

where $\mathfrak{U}$ has the form (5.1) and $\mathfrak{P}$ is any prime of L lying over $\mathfrak{p}$.

Of course, when $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, $\Phi(\mathfrak{p})$ is the Frobenius automorphism of $\mathfrak{p}$. One consequence of the Frobenius density theorem is stated in the following:

Theorem 5.3.4. *The Artin map carries I_K^S onto* $\mathrm{Gal}(L/K)$.

The statement and proof of the Frobenius density theorem, as well as the proof of this theorem can be found in Chapter IV in [Jan96].

5.4 The Hilbert Class Field

The aim of this section is to introduce the notion of the Hilbert class field of a given number field. This notion comes from a general theory know as class field theory, which studies the abelian extensions of global and local fields. The label "class field" refers to a field extension satisfying a technical property that is historically related to ideal class groups. One of the main theorems in class field theory is that class fields are the same as abelian extensions. The the Hilbert class field will be a particular class field of special interest.

We will not give a deep study of the notions and theorems of class field theory here, as this would be rather long and unnecessary. A more detailed study of class field theory is given in Chapter V in [Jan96]. We will just give a quick summary on the notion of Hilbert class field, some of its properties, and how is it related with the previous sections.

In 1898, Hilbert stated the following conjecture:

Conjecture 5.4.1. *For any number field K there is a unique finite extension L such that*

(i) *L/K is Galois and* $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K)$.

(ii) *L/K is unramified, and every abelian unramified extension of K is a subfield of L.*

(iii) *for every finite prime $\mathfrak{p}$ of K, the inertial degree $f(\mathfrak{P}|\mathfrak{p})$ (for any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$) is the order of $\mathfrak{p}$ in* $\mathrm{Cl}(K)$.

(iv) *every ideal of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_L$.*

Hilbert proved the existence of such extension when the class number (the cardinality of the class group $\mathrm{Cl}(K)$) was 2 and $[K : \mathbb{Q}] = 2$. In 1907, Philipp Furtwängler proved the first two parts of Hilbert's conjecture in general, and used this to prove the quadratic reciprocity law in all number fields in 1913. He proved the third part in 1911 and the fourth part in 1930, after Artin reduced it to a purely group-theoretic statement.

Property *(ii)* is normally used to characterize this extension:

Definition 5.4.2. Let K be a number field. The *Hilbert class field* of K, denoted by $\mathbb{H}(K)$, is the maximal unramified abelian extension of K.

Since all primes of K are unramified in $\mathbb{H}(K)$, property *(iii)* implies that a finite prime $\mathfrak{p}$ of K splits completely on $\mathbb{H}(K)$ if, and only if, its principal. Consider the Artin map associated to the extension $\mathbb{H}(K)/K$:

$$\begin{array}{rccc} \Phi_{\mathbb{H}(K)/K}: & I_K & \longrightarrow & \mathrm{Gal}(\mathbb{H}(K)/K) \\ & \displaystyle\prod_{\mathfrak{p}\in P} \mathfrak{p}^{a(\mathfrak{p})} & \longmapsto & \displaystyle\prod_{\mathfrak{p}\in P} \phi(\mathfrak{P}|\mathfrak{p})^{a(\mathfrak{p})} \end{array}$$

Note that, since no finite prime ramifies in K, the Artin map is defined for all nonzero fractional ideals of K (that is, $S = \emptyset$). As we saw in the previous section, the order of the Frobenius automorphism $\phi(\mathfrak{P}|\mathfrak{p})$ of a given finite prime $\mathfrak{p}$ of K is the inertial degree $f(\mathfrak{P}|\mathfrak{p})$. Hence, it is clear that $\mathfrak{p}$ is in $\ker(\Phi_{\mathbb{H}(K)/K})$ if, and only if, $\mathfrak{p}$ is a principal ideal. This property holds not only for the prime ideals of $\mathcal{O}_K$, but also for all nonzero fractional ideals of K. Thus, the kernel of the Artin map is precisely the set of nonzero principal fractional ideals of K. Since the Artin map is surjective, the induce map

$$\begin{array}{rccc} \overline{\Phi}_{\mathbb{H}(K)/K}: & \mathrm{Cl}(K) & \longrightarrow & \mathrm{Gal}(\mathbb{H}(K)/K) \\ & \overline{\mathfrak{U}} & \longmapsto & \Phi_{\mathbb{H}(K)/K}(\mathfrak{U}) \end{array}$$

establishes an isomorphism between the class group of K and the Galois group $\mathrm{Gal}(\mathbb{H}(K)/K)$. The notion of Hilbert class field and properties (i) and (ii) in Conjecture 5.4.1 will be widely used in the following chapter.

Chapter 6

The Class Field Tower Problem

In this finial chapter we will use all the theory developed in this thesis to formulate an solve the class field tower problem. We begin by formulating the following problem:

Problem 6.0.1 (Embeddability problem)**.** *Given a number field K, does it always exist a finite extension L of K such that the ring of integers of L is a principal ideal domain?*

If K is a number field, the extent to which $\mathcal{O}_K$ fails to be a PID is measured by the class group $\mathrm{Cl}(K)$. In particular, $\mathcal{O}_K$ is a PID if, and only if, $\mathrm{Cl}(K)$ is trivial. The class group of K is always finite and, by class filed theory, is isomorphic to the Galois group $\mathrm{Gal}(\mathbb{H}(K)/K)$. Thus, O_K is a PID if, and only if, its Hilbert class field of K is K itself. This brings us to consider another problem. To state it, we need the following definition:

Definition 6.0.2. Let K be a number field. Denote $\mathbb{H}^0(K) := K$ and $\mathbb{H}^n(K) := \mathbb{H}(\mathbb{H}^{n-1}(K))$ for $n \geq 1$. The *class field tower* of K is the following tower of extensions:

$$K = \mathbb{H}^0(K) \subseteq \mathbb{H}^1(K) \subseteq \mathbb{H}^2(K) \subseteq \dots$$

We say that the class field tower is *finite* if it stabilizes at some point, i.e., if there exists $m \in \mathbb{N}$ such that $\mathbb{H}^n(K) = \mathbb{H}^m(K)$ for all $n \geq m$. It is said to be *infinite* otherwise.

Problem 6.0.3 (Class field tower problem)**.** *Is the class field tower of any number field K always finite?*

Problems 6.0.1 and 6.0.3 are equivalent in the following sense:

Lemma 6.0.4. *Let K be a number field. Then, the class field tower of K is finite if, and only if, there exists a finite extension L/K with* $\mathrm{Cl}(L) = \{1\}$.

Proof. Assume that the class field tower is finite. Then, there exists $m \in \mathbb{N}$ with $\mathbb{H}(\mathbb{H}^m(K)) = \mathbb{H}^m(K)$ and hence $\mathrm{Cl}(\mathbb{H}^m(K)) = \{1\}$. Since the Hilbert class field of any number field is a finite extension of itself, $\mathbb{H}^m(K)/K$ is finite.

Assume now that L is a finite extension of K with trivial class group and consider the tower of fields

$$L = LK \subseteq L\mathbb{H}^1(K) \subseteq L\mathbb{H}^2(K) \subseteq \dots$$

For every $n \in \mathbb{N}$, we now that $\mathbb{H}^{n+1}(K)/\mathbb{H}^n(K)$ is an abelian unramified extension. Then, $L\mathbb{H}^{n+1}(K)/L\mathbb{H}^n(K)$ is abelian by Lemma 5.2.9 and unramified by Theorem 5.2.11. In particular, $L\mathbb{H}^1(K)$ is an abelian unramified extension of L. But $\mathrm{Cl}(L) = \{1\}$, so $\mathbb{H}(L) = L$ and L does not have nontrivial abelian unramified extensions. This implies that $L\mathbb{H}^1(K) = L$. Repeating this argument inductively we find that $L\mathbb{H}^n(K) = L$ for all $n \geq 0$. Since $\mathbb{H}^n(K) \subseteq L\mathbb{H}^n(K) = L$, every field in the class field tower of K is contained in L. L is a finite extension of K, so the class field tower of K must be finite. □

6.1 A Criterion for Infinite Class Field Towers

Our goal now is to prove that there exists number fields K with an infinite class field tower. Computing the class field of a given number is a rather difficult task. Its a bit easier to control the p-class field, defined in the following:

Definition 6.1.1. Let K be a number field and p a fixed prime number. The p-class field of K, denoted by $\mathbb{H}_p(K)$, is the maximal unramified Galois extension of K such that the Galois group $\mathrm{Gal}(\mathbb{H}_p(K)/K)$ is an elementary abelian p-group, i.e., an abelian group where every nontrivial element has order p.

Remark. Most authors define the p-class field of K to be the maximal unramified abelian p-extension of K (without the extra condition that the corresponding Galois group is elementary). We will use this alternative notion of p-class field, as this will allow us to apply some of the results seen in the previous chapters.

Theorem 6.1.2. *The p-class field of a given number field K always exists.*

Proof. Let K be a number field and let L_1 and L_2 be unramified Galois extensions of K with $\mathrm{Gal}(L_1/K), \mathrm{Gal}(L_2/K)$ elementary abelian p-groups. Then L_1L_2 is also a Galois extension of K. By Lemma 5.2.10, $\mathrm{Gal}(L_1L_2/K)$ is an elementary abelian p-group and by Corollary 5.2.13, L_1L_2/K is an unramified extension. In other words, the compositum of unramified elementary abelian p-extension is also an unramified elementary abelian p-extension. Thus, we define $\mathbb{H}_p(K)$ to be the compositum of all subextensions L of $\mathbb{H}(K)$ with $\mathrm{Gal}(L/K)$ an elementary abelian p-group. Clearly, $\mathbb{H}_p(K)$ satisfies the desired property. □

Definition 6.1.3. Let K be a number field. Denote $\mathbb{H}_p^0(K) := K$ and $\mathbb{H}_p^n(K) := \mathbb{H}_p(\mathbb{H}_p^{n-1}(K))$ for $n \geq 1$. The *p-class field tower* of K is the following tower of extensions:

$$K = \mathbb{H}_p^0(K) \subseteq \mathbb{H}_p^1(K) \subseteq \mathbb{H}_p^2(K) \subseteq \dots$$

As with the class field tower, we say that the p-class field tower is *finite* if it stabilizes at some point and *infinite* otherwise.

The following lemma will allow us to reduce the problem of proving that a certain class field tower is infinite to prove that the p-class field tower is infinite:

Lemma 6.1.4. *Let K be a number field and p a prime number. Then, $\mathbb{H}_p^n(K) \subseteq \mathbb{H}^n(K)$ for any $n \geq 1$.*

Proof. We will prove it by induction. By construction, $\mathbb{H}_p(K) \subseteq \mathbb{H}(K)$. Assume that $\mathbb{H}_p^n(K) \subseteq \mathbb{H}^n(K)$. Consider the following diagram of extensions:

$$\begin{tikzcd}
 & \mathbb{H}_p^{n+1}(K)\mathbb{H}^n(K) \arrow[dl, dash] \arrow[dd, dash] \\
\mathbb{H}_p^{n+1}(K) \arrow[dd, dash] & \\
 & \mathbb{H}^n(K) \\
\mathbb{H}_p^n(K) \arrow[ur, dash] &
\end{tikzcd}$$

Since $\mathbb{H}_p^{n+1}(K)/\mathbb{H}_p^n(K)$ is an unramified abelian extension, the same is true for the lifting $\mathbb{H}_p^{n+1}(K)\mathbb{H}^n(K)/\mathbb{H}^n(K)$. Then, by maximality of the Hilbert class field,

$$\mathbb{H}_p^{n+1}(K)\mathbb{H}^n(K) \subseteq \mathbb{H}(\mathbb{H}^n(K)) := \mathbb{H}^{n+1}(K).$$

This proves the statement. □

Corollary 6.1.5. *Let K be a number field. If the p-class field tower of K is infinite for some prime number p, then the class field tower of K must also be infinite.*

Definition 6.1.6. Let K be a number field and p a prime number. We define the following extension of K:

$$\mathbb{H}_p^\infty(K) := \bigcup_{n \geq 0} \mathbb{H}_p^n(K).$$

Clearly, the p-class field tower of K is finite if, and only if, $\mathbb{H}_p^\infty(K)$ is a finite extension of K. Our goal now will be to give sufficient conditions for $\mathbb{H}_p^\infty(K)$ to be infinite. In the following we will prove that $\mathbb{H}_p^\infty(K)$ is the maximal unramified pro-p extension of K (by pro-p extension we mean Galois extension with Galois group a pro-p group). This extension is not necessary abelian. If it was, it would be contained in the Hilbert class field of K and hence it would always be finite. For a possibly infinite extension L of K, we say that L/K is unramified if all of its finite subextensions are unramified. We begin with the following lemma:

Lemma 6.1.7. *Let K be a number field and p a prime number. Then, the extensions $\mathbb{H}_p^n(K)/K$ are Galois.*

Proof. We proceed by induction on n. Clearly, $\mathbb{H}_p(K)$ is Galois over K. Suppose $\mathbb{H}_p^n(K)/K$ is a Galois extension. We will see that for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $\sigma\left(\mathbb{H}_p^{n+1}(K)\right) = \mathbb{H}_p^{n+1}(K)$ and hence $\mathbb{H}_p^{n+1}(K)/K$ must be Galois.

Let $\sigma \in \mathrm{Gal}\left(\overline{K}/K\right)$. Since $\mathbb{H}_p^n(K)/K$ is Galois, $\sigma|_{\mathbb{H}_p^n(K)} \in \mathrm{Gal}(\mathbb{H}_p^n(K)/K)$. We have the following diagram of extensions:

$$\begin{tikzcd}
\mathbb{H}_p^{n+1}(K) \arrow[dr, no head] & & \sigma\left(\mathbb{H}_p^{n+1}(K)\right) \arrow[dl, no head] \\
& \mathbb{H}_p^n(K) \arrow[d, no head] & \\
& K &
\end{tikzcd}$$

We claim that $\sigma\left(\mathbb{H}_p^{n+1}(K)\right)/\mathbb{H}_p^n(K)$ is unramified. For the finite primes, notice that σ permutes the prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{H}_p^n(K)}$. Such prime ideals $\mathfrak{p}$ decompose as $\mathfrak{P}_1 \cdots \mathfrak{P}_r$ when extended in $\mathbb{H}_p^{n+1}(K)$, as they are unramified. Then, $\sigma(\mathfrak{p})$ decompose as $\sigma(\mathfrak{P}_1)\cdots\sigma(\mathfrak{P}_r)$ when extended in $\sigma\left(\mathbb{H}_p^{n+1}(K)\right)$, and hence finite primes of $\mathbb{H}_p^n(K)$ are unramified in $\sigma\left(\mathbb{H}_p^{n+1}(K)\right)$.

For the infinite primes, notice that σ permutes the embeddings of $\mathbb{H}_p^n(K)$ into $\mathbb{C}$ when acting by composition: if $\tau : \mathbb{H}_p^n(K) \hookrightarrow \mathbb{C}$ is one of these embeddings, so is $\tau\sigma^{-1} : \mathbb{H}_p^n(K) \hookrightarrow \mathbb{C}$. If τ extends to $r = [\mathbb{H}_p^{n+1}(K) : \mathbb{H}_p^n(K)]$ different embeddings of $\mathbb{H}_p^{n+1}(K)$ into $\mathbb{C}$ (where no two are complex conjugates), namely $\tau_1 \ldots, \tau_r$, then $\tau_1\sigma^{-1}, \ldots \tau_r\sigma^{-1}$ are the embeddings of $\sigma\left(\mathbb{H}_p^{n+1}(K)\right)$ into $\mathbb{C}$ extending $\tau\sigma^{-1}$ (again, no two embeddings are complex conjugates). This shown that infinite primes of $\mathbb{H}_p^n(K)$ are unramified in $\sigma\left(\mathbb{H}_p^{n+1}(K)\right)$.

Now recall that $\mathbb{H}_p^{n+1}(K)/\mathbb{H}_p^n(K)$ is Galois, and hence so is $\sigma\left(\mathbb{H}_p^{n+1}(K)\right)/\mathbb{H}_p^n(K)$. Sigma induces an isomorphism of groups between their Galois groups acting by conjugation:

$$\begin{array}{ccc}
\mathrm{Gal}\left(\mathbb{H}_p^{n+1}(K)/\mathbb{H}_p^n(K)\right) & \longrightarrow & \mathrm{Gal}\left(\sigma\left(\mathbb{H}_p^{n+1}(K)\right)/\mathbb{H}_p^n(K)\right) \\
\tau & \longmapsto & \sigma\tau\sigma^{-1}
\end{array}$$

This shows that $\mathrm{Gal}\left(\mathbb{H}_p^{n+1}(K)/\mathbb{H}_p^n(K)\right) \cong \mathrm{Gal}\left(\sigma\left(\mathbb{H}_p^{n+1}(K)\right)/\mathbb{H}_p^n(K)\right)$. Therefore, $\sigma\left(\mathbb{H}_p^{n+1}(K)\right)$ is a unramified Galois extension of $\mathbb{H}_p^n(K)$ such that the corresponding Galois group is an elementary abelian p-group. By maximality of the p-class field, we must have $\sigma\left(\mathbb{H}_p^{n+1}(K)\right) \subseteq \mathbb{H}_p^{n+1}(K)$ and, by injectivity of σ, this must be an equality. This proves the lemma. □

Lemma 6.1.8. *Let K be a number field and p a prime number. Then, $\mathbb{H}_p^\infty(K)/K$ is an unramified pro-p extension.*

Proof. First, notice that $\mathbb{H}_p^n(K)$ is a finite unramified extension of K. This is a consequence of the fact that ramification indices are multiplicative in towers. Let $L \subseteq \mathbb{H}_p^\infty(K)$ be a finite extension of K. Then, $L \subseteq \mathbb{H}_p^n(K)$ for some $n \in \mathbb{N}$ and hence L/K is unramified. This shows that $\mathbb{H}_p^\infty(K)/K$ is unramified.

By Lemma 6.1.7, the extensions $\mathbb{H}_p^n(K)/K$ are Galois and

$$\operatorname{Gal}\left(\mathbb{H}_p^{n+1}(K)/K\right) \Big/ \operatorname{Gal}\left(\mathbb{H}_p^{n+1}(K)/\mathbb{H}_p^n(K)\right) \cong \operatorname{Gal}\left(\mathbb{H}_p^n(K)/K\right),$$

so $\left|\operatorname{Gal}\left(\mathbb{H}_p^{n+1}(K)/K\right)\right| = \left|\operatorname{Gal}\left(\mathbb{H}_p^{n+1}(K)/\mathbb{H}_p^n(K)\right)\right|\left|\operatorname{Gal}\left(\mathbb{H}_p^n(K)/K\right)\right|$. Thus, applying induction we see that $\operatorname{Gal}\left(\mathbb{H}_p^{n+1}(K)/K\right)$ are finite p-groups. As $\mathbb{H}_p^\infty(K) = \bigcup_{n\geq 0} \mathbb{H}_p^n(K)$, by Galois theory, we have that $\mathbb{H}_p^\infty(K)/K$ is Galois and

$$\operatorname{Gal}\left(\mathbb{H}_p^\infty(K)/K\right) = \varprojlim_{n\geq 0} \operatorname{Gal}\left(\mathbb{H}_p^n(K)/K\right)$$

(for more details, see Chapter 2 in [Koc02]). This shows that $\mathbb{H}_p^\infty(K)/K$ is a pro-p extension. □

Now we can prove the following theorem:

Theorem 6.1.9. *Let K be a number field and p a prime number. Then, $\mathbb{H}_p^\infty(K)$ is the maximal unramified pro-p extension of K.*

Proof. We already know that $\mathbb{H}_p^\infty(K)$ is an unramified pro-p extension of K. Hence, we only need to prove that is maximal. Let L be an unramified Galois extension of K such that $G = \operatorname{Gal}(L/K)$ is a pro-p group. Let L_1 be the fixed field of $\operatorname{Fr}(G) \subseteq G$. Since $\operatorname{Fr}(G)$ is normal in G, L_1 is Galois over K and $\operatorname{Gal}(L_1/K) \cong \operatorname{Gal}(L/K)/\operatorname{Gal}(L/L_1)$. Since $\operatorname{Fr}(G)$ is closed in G, by the fundamental theorem of Galois theory for (possibly) infinite extension, $\operatorname{Gal}(L/L_1) = \operatorname{Fr}(G)$. Hence, $\operatorname{Gal}(L_1/K) \cong G/\operatorname{Fr}(G)$ is an elementary abelian p-group. Now note that L_1 is unramified over K. This implies that $L_1 \subseteq \mathbb{H}_p(K)$, that is a finite extension of K. In particular $G/\operatorname{Fr}(G)$ is finite and, since $d(G) = d\left(G/\operatorname{Fr}(G)\right)$, G is finitely generated. As we explained in the end of Section 4.2, in this case, the Frattini series $\{\operatorname{Fr}^n(G) \mid n \in \mathbb{N}\}$ form an open neighbourhood basis at $1 \in G$. Let L_n be the fixed field of $\operatorname{Fr}^n(G)$. We will prove by induction that $L_n \subseteq \mathbb{H}_p^n(K)$ for all $n \geq 1$.

We have already seen that $L_1 \subseteq \mathbb{H}_p^1(K)$. Suppose $L_n \subseteq \mathbb{H}_p^n(K)$. L/L_n is Galois with $\operatorname{Gal}(L/L_n) = \operatorname{Fr}^n(G)$. We have that $\operatorname{Fr}^{n+1}(G) := \operatorname{Fr}\left(\operatorname{Fr}^n(G)\right)$ is normal in $\operatorname{Fr}^n(G)$. Then, L_{n+1} is a Galois extension of L_n with Galois group $\operatorname{Gal}(L_{n+1}/L_n) \cong$

$\mathrm{Gal}(L/L_n)/\mathrm{Gal}(L/L_{n+1}) = \mathrm{Fr}^n(G)/\mathrm{Fr}^{n+1}(G)$, and thus L_{n+1} is an unramified elementary abelian p-extension of L_n. Consider the following diagram of extensions:

$$\begin{tikzcd}
& L_{n+1}\mathbb{H}_p^n(K) \arrow[dl, dash] \arrow[dd, dash] \\
L_{n+1} \arrow[dd, dash] & \\
& \mathbb{H}_p^n(K) \arrow[dl, dash] \\
L_n &
\end{tikzcd}$$

The lifting $L_{n+1}\mathbb{H}_p^n(K)/\mathbb{H}_p^n(K)$ of L_{n+1}/L_n is also an unramified elementary abelian p-extension, and hence $L_{n+1}\mathbb{H}_p^n(K) \subseteq \mathbb{H}_p^{n+1}(K)$. This shows that $L_{n+1} \subseteq \mathbb{H}_p^{n+1}(K)$.

Let's now see that $L = \bigcup_{n\geq 1} L_n$. Clearly, $\bigcup_{n\geq 1} L_n \subseteq L$. Take $\alpha \in L$. Then $K(\alpha)$ is a finite extension of K, and hence $\mathrm{Gal}(L/K(\alpha))$ is an open subgroup of $\mathrm{Gal}(L/K)$. Then, since the Frattini series form an open neighbourhood basis at 1, there exists $n \in \mathbb{N}$ with $\mathrm{Fr}^n(G) \subseteq \mathrm{Gal}(L/K(\alpha))$. The corresponding fields fixed by these subgroups satisfy the reverse inclusion, i.e., $K(\alpha) \subseteq L_n$. This shows that $L \subseteq \bigcup_{n\geq 1} L$.

Finally, since $L_n \subseteq \mathbb{H}_p^n(K)$ for all $n \geq 1$, we have that

$$L = \bigcup_{n\geq 1} L_n \subseteq \bigcup_{n\geq 1} \mathbb{H}_p^n(K) = \mathbb{H}_p^\infty(K).$$

This finishes the proof. □

Let $G_{K,p} := \mathrm{Gal}\left(\mathbb{H}_p^\infty(K)/K\right)$. Proving that $\mathbb{H}_p^\infty(K)/K$ is an infinite extension is equivalent to proving that $G_{K,p}$ is infinite.

We claim that Frattini quotient $G_{K,p}/\mathrm{Fr}(G_{K,p})$ is isomorphic to $\mathrm{Gal}\left(\mathbb{H}_p(K)/K\right)$. Indeed, let L be the fixed field of the subgroup $\mathrm{Fr}(G_{K,p})$. Since $G_{K,p}/\mathrm{Fr}(G_{K,p})$ is an elementary abelian p-group and L is unramified, $L \subseteq \mathbb{H}_p(K)$. On the other side, $\mathrm{Gal}\left(\mathbb{H}_p(K)/K\right) \cong \mathrm{Gal}\left(\mathbb{H}_p^\infty(K)/K\right)/\mathrm{Gal}\left(\mathbb{H}_p^\infty(K)/\mathbb{H}_p(K)\right)$ is an elementary abelian p-group. Since the Frattini subgroup $\mathrm{Fr}(G_{K,p})$ is the smallest normal subgroup of $G_{K,p}$ such that the quotient is elementary abelian, $\mathrm{Fr}(G_{K,p}) \subseteq \mathrm{Gal}\left(\mathbb{H}_p^\infty(K)/\mathbb{H}_p(K)\right)$, and hence $\mathbb{H}_p(K) \subseteq L$.

Recall that $\mathbb{H}_p(K)$ is the maximal subextension of the Hilbert class field of K such that its Galois group over K is an elementary abelian p-group. Thus, $\mathrm{Gal}(\mathbb{H}_p(K)/K)$ is the maximal elementary abelian quotient of $\mathrm{Gal}(\mathbb{H}(K)/K)$. Since the subgroup lattice and the quotient lattice of a finite abelian group are isomorphic, every quotient of $\mathrm{Gal}(\mathbb{H}(K)/K)$ is isomorphic to one of its subgroups. This implies that the

the maximum elementary quotient $\mathrm{Gal}(\mathbb{H}_p(K)/K)$ of $\mathrm{Gal}(\mathbb{H}(K)/K)$ is isomorphic to its maximal elementary subgroup: $\mathrm{Gal}(\mathbb{H}(K)/K)[p]$. Taking into account that $\mathrm{Gal}(\mathbb{H}(K)/K) \cong \mathrm{Cl}(K)$, we obtain that

$$\mathrm{Gal}(\mathbb{H}_p(K)/K) \cong \mathrm{Cl}(K)[p].$$

Let $\rho_p(K) := \dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p])$ be the p-rank of the class group of K. With all the considerations made above, and recalling that the generator rank of a pro-p group is the same as the generator rank of its Frattini quotient, we obtain that

$$d(G_{K,p}) = d\left({}^{G_{K,p}}\!\big/_{\mathrm{Fr}(G_{K,p})}\right) = d\left(\mathrm{Gal}\left(\mathbb{H}_p(K)/K\right)\right) = \rho_p(K). \tag{6.1}$$

The following theorem establishes a relation between the generator and relation ranks of $G_{K,p}$ and the number of infinite primes of K:

Theorem 6.1.10 (Shafarevich)**.** *Let K be a number field and $\nu(K)$ the number of infinite primes of K. Then, for any prime number p we have*

$$0 \le r(G_{K,p}) - d(G_{K,p}) \le \nu(K) - 1.$$

This theorem was originally proved by Shafarevich in [Sha63]. An proof in English of this inequality can be found in Section 11.3 in [Koc02] as a consequence of Theorems 11.5 and 11.8.

Combining Theorem 6.1.10 with Theorem 4.3.7, we obtain the following criterion for the group $G_{K,p}$ to be infinite:

Corollary 6.1.11 (Golod-Shafarevich)**.** *In the notations above, assume that*

$$\rho_p(K) > 2 + 2\sqrt{\nu(K) + 1}.$$

Then $G_{K,p}$ is Golod-Shafarevich and therefore infinite.

Proof. By Equation (6.1), $\rho_p(K) = d(G_{K,p})$. Rearranging the terms and squaring this inequality we obtain that

$$\frac{d(G_{K,p})^2}{4} - d(G_{K,p}) > \nu(K).$$

Using Theorem 6.1.10 we deduce that

$$\frac{d(G_{K,p})^2}{4} > r(G_{K,p}) + 1.$$

Hence $d(G_{K,p}) > 1$ and $d(G_{K,p})^2/4 > r(G_{K,p})$. Theorem 4.3.7 implies the claim. □

6.2 Particular Examples

To complete the negative solution to the class field tower problem it suffices to exhibit examples of number fields satisfying the inequality in Corollary 6.1.11. We will see that for any prime number p and any $n \in \mathbb{N}$, there exist a number field $K = K(p,n)$ such that $[K : \mathbb{Q}] = p$ and $\rho_p(K) \geq n$. Since $\nu(K) \leq [K : \mathbb{Q}]$ (because K has $[K : \mathbb{Q}]$ different embedding into $\mathbb{C}$), we can choose any $n > 2 + 2\sqrt{p+1}$. Then, $K(p,n)$ will satisfy the inequality in Corollary 6.1.11 and hence will have an infinite class field tower.

6.2.1 Number fields with infinite 2-class field tower

Let's start with the case $p = 2$. Take any $n+1$ distinct prime numbers $q_1, \dots, q_{n+1}$ congruent to 1 modulo 4 (the Dirichlet's theorem on arithmetic progressions assures us that there are infinitely many primes congruent to 1 modulo 4). Let $K = \mathbb{Q}(\sqrt{q_1 \cdots q_{n+1}})$ and $L = \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{n+1}})$. Note that $[K : \mathbb{Q}] = 2$.

Lemma 6.2.1. *The extension L/K is unramified.*

Proof. Note that L is a totally real number field, i.e., all its infinite primes are real. Therefore, L/K is unramified at the infinite primes. To see that is also unramified at the finite primes, we will first see that $L/\mathbb{Q}$ is unramified outside $\{q_1, \dots, q_{n+1}\}$. Then, we will see that the ramification indexes of the primes q_i in L are 2 and use this to deduce that L/K is unramified. Consider the following diagram:

$$\begin{tikzcd}
 & L = \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{n+1}}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{q_1}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{q_2}, \dots, \sqrt{q_{n+1}}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

By Theorem 5.2.12, if a prime number $q \in \mathbb{Z}$ ramifies in L, it must also ramify at $\mathbb{Q}(\sqrt{q_1})$ or at $\mathbb{Q}(\sqrt{q_2}, \dots, \sqrt{q_{n+1}})$. Thus, applying this reasoning repeatedly, q ramifies in L if, and only if, q ramifies in $\mathbb{Q}(\sqrt{q_i})$ for some i. The discriminant of $\mathbb{Q}(\sqrt{q_i})/\mathbb{Q}$ is q_i, and hence the only finite prime of $\mathbb{Q}$ that ramifies in $\mathbb{Q}(\sqrt{q_i})$ is q_i. This tells us that the only prime numbers that ramified at L are precisely $q_1, \dots, q_{n+1}$.

Let's now calculate the ramification indexes of q_i in L. Let $\mathfrak{Q}_i$ be a prime of L lying over q_i. Let $F = \mathbb{Q}(\sqrt{q_1}, \dots \sqrt{q_{i-1}}, \sqrt{q_{i+1}}, \dots \sqrt{q_{n+1}})$ and consider the group morphism given by Lemma 5.2.10:

$$\begin{array}{rccc} \Phi: & \mathrm{Gal}(L/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}\left(\mathbb{Q}(\sqrt{q_i})/\mathbb{Q}\right) \times \mathrm{Gal}\left(F/\mathbb{Q}\right) \\ & \sigma & \longmapsto & \left(\sigma|_{\mathbb{Q}(\sqrt{q_i})}, \sigma|_F\right) \end{array}$$

Let $\sigma \in E(\mathfrak{Q}_\mathfrak{i}|q_i)$. Then, using the same argument we used in the proof of Theorem 5.2.11, $\sigma|_{\mathbb{Q}(\sqrt{q_i})} \in E(\mathfrak{Q}_\mathfrak{i} \cap \mathbb{Q}(\sqrt{q_i})|q_i)$ and $\sigma|_F \in E(\mathfrak{Q}_\mathfrak{i} \cap F|q_i)$. In other words,

$$\Phi(E(\mathfrak{Q}_\mathfrak{i}|q_i)) \subseteq E(\mathfrak{Q}_\mathfrak{i} \cap \mathbb{Q}(\sqrt{q_i})|q_i) \times E(\mathfrak{Q}_\mathfrak{i} \cap F|q_i).$$

We know that the ramification index of q_i in $\mathbb{Q}(\sqrt{q_i})$ is 2 and, by the argument used in the beginning of the proof, $e(\mathfrak{Q}_\mathfrak{i} \cap F|q_i) = 1$. Using that the cardinality of the inertia subgroup is equal to the corresponding ramification index, and that Ψ is injective, we deduce that

$$\left|E(\mathfrak{Q}_\mathfrak{i}|q_i)\right| \leq \left|E(\mathfrak{Q}_\mathfrak{i} \cap \mathbb{Q}(\sqrt{q_i})|q_i)\right|\left|E(\mathfrak{Q}_\mathfrak{i} \cap F|q_i)\right| = 2 \cdot 1 = 2.$$

Since q_i ramifies in L, we must have $e(\mathfrak{Q}_\mathfrak{i}|q_i) = 2$.

Finally, note that the only possible finite primes of K that could ramify in L are those lying over the primes q_i. Let $\mathfrak{q}_\mathfrak{i}$ of be the unique prime of K lying under $\mathfrak{Q}_\mathfrak{i}$. The discriminant of $K/\mathbb{Q}$ is $q_1 \cdots q_{n+1}$, so q_i ramifies in K. We must have that $e(\mathfrak{q}_i|q_i) = 2$. By the multiplicativity of the ramification indexes, $e(\mathfrak{Q}_i|\mathfrak{q}_i) = 1$. This proves the statement. □

L is an abelian extension of K with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. Since L/K is unramified, we must have $L \subseteq \mathbb{H}(K)$. By the isomorphism between the subgroup lattice and the quotient lattice of a finite abelian group, $\mathrm{Gal}(\mathbb{H}(K)/K)$ must have a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. Hence, $\rho_2(K) = \dim_{\mathbb{F}_2}(G[2]) \geq \dim_{\mathbb{F}_2}((\mathbb{Z}/2\mathbb{Z})^n) = n$ (it can be shown that, in fact, $\rho_2(K) = n$). For any $n \geq 6 > 2 + 2\sqrt{3}$, by Corollary 6.1.11, $\mathbb{Q}(\sqrt{q_1 \cdots q_n})$ has an infinite class field tower.

6.2.2 Number fields with infinite *p*-class field tower for odd primes *p*

Now let's do the case where p is an arbitrary odd prime number. Take any $n+1$ distinct prime numbers $q_1, \ldots, q_{n+1}$ congruent to 1 modulo p. Let $L_i = \mathbb{Q}(\zeta_{q_i})$ be the q^{th} cyclotomic field and let K_i be the unique subfield of L_i that has index p over $\mathbb{Q}$. Let $L = L_1 \cdots L_{n+1}$ and $M = K_1 \ldots K_{n+1}$. Since $L_i \cap L_j = \mathbb{Q}$ for $i \neq j$, $\mathrm{Gal}(L/\mathbb{Q}) \cong \bigoplus \mathrm{Gal}(L_i/\mathbb{Q})$, and hence $\mathrm{Gal}(M/\mathbb{Q}) \cong \bigoplus \mathrm{Gal}(K_i/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^{n+1}$. Clearly, $\mathrm{Gal}(M/\mathbb{Q})$ has a subgroup of index p which does not contain $\mathrm{Gal}(K_i/\mathbb{Q})$ for any i (for instance, one could take the subgroup generated by $(1,0,\ldots,0,1), (0,1,0,\ldots,0,1), \ldots, (0,\ldots,0,1,1) \in (\mathbb{Z}/p\mathbb{Z})^{n+1}$). The field K fixed by this subgroup has index p over $\mathbb{Q}$ and is not contained in the compositum of any proper subset of $\{K_1, \ldots, K_{n+1}\}$.

Lemma 6.2.2. *The extensions KK_i/K are unramified.*

Proof. To see that infinite primes of K don't ramify in KK_i, note that both K and K_i are Galois over $\mathbb{Q}$ (since they are subextensions of an abelian Galois extension). Then, they must be either totally real or totally imaginary, but since they have odd degree over $\mathbb{Q}$ and the number of complex embedding is even, K and K_i must be totally real. Then, its compositum KK_i is also totally real, so infinite primes of K don't ramify in KK_i.

For the finite primes, note that the only finite prime of $\mathbb{Q}$ that ramifies in L_i is q_i. Then, by Theorem 5.2.12, $L/\mathbb{Q}$ is unramified outside $S = \{q_1, \ldots, q_{n+1}\}$, and hence so is any subextension of L. Therefore, KK_i/K may only be ramified a the finite primes $\mathfrak{q}_i$ of K laying over q_i. If KK_i/K was ramified at some prime $\mathfrak{q}_i$, then so would be M/K. This would be a contradiction since $M = K\prod_{j\neq i} K_j$, but KK_j/K are unramified at $\mathfrak{q}_i$ for $j \neq i$ and then so is their compositum M/K. □

The fields KK_i are unramified over K, so their compositum M is also unramified over K. In addition M/K is abelian with Galois $\mathrm{Gal}(M/K) \cong (\mathbb{Z}/p\mathbb{Z})^n$. Then, we must have $M \subseteq \mathbb{H}(K)$. Using again the correspondence between quotients and subgroups of a finite abelian group, we deduce that $\mathrm{Gal}(\mathbb{H}(K)/K)$ has a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$. This shows that $\rho_p(K) = \dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p]) \geq n$ (again, one could show that the equality holds). For any $n > 2 + 2\sqrt{p+1}$, the field K defined above has infinite p-class field tower and thus cannot be embedded in a greater number field with class number 1.

References

[CT17] Tim Clausen and Katrin Tent. *Some model theory of profinite groups.* May 2017.

[Cona] Keith Conrad. *History of Class Field Theory.*

[Conb] Keith Conrad. *Ostrowski for Number Fields.*

[Ers12] Mikhail Ershov. “Golod-Shafarevich groups: a survey”. In: *International Journal of Algebra and Computation* 22 (2012).

[GS64] Evgeny S. Golod and Igor R. Shafarevich. “On the class field tower”. Russian. In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 28.2 (1964), pp. 261–272.

[Hal59] Marshall Hall. *The Theory of Groups.* Macmillan, 1959.

[Jan96] Gerald J. Janusz. *Algebraic Number Fields.* Advances in the Mathematical Sciences. American Mathematical Society, 1996.

[Koc02] Helmut Koch. *Galois theory of p-extensions.* Springer monographs in mathematics. Springer, 2002.

[Kra20] Linus Kramer. *Locally Compact Groups and Lie Groups.* 2020, pp. 15–16.

[Lem10] Franz Lemmermeyer. *Class Field Towers.* 2010.

[Lub82] Alexander Lubotzky. “Combinatorial group theory for pro-p groups”. In: *Journal of Pure and Applied Algebra* 25 (Sept. 1982), pp. 311–325.

[Mar18] Daniel A. Marcus. *Number Fields.* Universitext. Springer International Publishing, 2018.

[Moo76] Calvin C. Moore. “Extensions and Low Dimensional Cohomology Theory of Locally Compact Groups Groups. III”. In: *Transactions of the American Mathematical Society* 221.1 (1976).

[Roq65] Peter Roquette. “Algebraic Number Theory”. In: Academic Press Inc. (London) Ltd, 1965. Chap. On class field towers, pp. 231–249.

[Sán03] Félix Cabello Sánchez. “Quasi-homomorphisms”. In: *Fundamenta Mathematicae* 178.3 (2003), pp. 255–270.

[Sem02] Darren Semmen. “The Frattini module and p’-automorphisms of free pro-p groups (Communications in Arithmetic Fundamental Groups)”. In: *RIMS Kokyuroku* 1267 (June 2002), pp. 177–188.

[Sha63] Igor R. Shafarevich. “Extensions with Prescribed Ramification Points”. Russian. In: *Publications Mathématiques de l’IHÉS* 18 (1963), pp. 71–95.

[Sha08] Romyar T. Sharifi. “On Galois groups of unramified pro-p extensions”. In: *Mathematische Annalen* 342.2 (2008), pp. 297–308.

[Vin65] Ernest B. Vinberg. “On the theorem concerning the infinite-dimensionality of an associative algebra”. Russian. In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 29 (1965), pp. 209–214.

[Wil21] Gareth Wilkes. *Profinite Groups and Group Cohomology*. 2021.

[Wil98] John S. Wilson. *Profinite groups*. London Mathematical Society Monographs. New Series, 19. Oxford University Press, 1998.