THE GOLOD-SHAFAREVICH THEOREM AND THE CLASS FIELD TOWER PROBLEM

Kathleen Zhou

A thesis submitted in partial fulfillment
of the requirements for the degree of
Bachelor of Arts in mathematics with honors.

Harvard College, 2017

Advisor: Barry Mazur

Contents

CHAPTER 1

Introduction

1. Historical Context and Motivation

The mid-19th century found number theorists tackling the mystery left by Fermat's marvelously offhand marginalia and developing the field of algebraic number theory. Of great importance to this theory was the ideal class group, since its structure indicates how far the ring of integers of a number field is from being a unique factorization domain, which occurs if and only if the ideal class group is trivial. As Gabriel "Fool's Gold" Lamé observed in 1847, Fermat's Last Theorem would be easily proven if the pth cyclotomic fields $\mathbb{Q}(\zeta_p)$ had class number 1 for odd primes p. However, sadly for Lamé, Ernst Kummer had shown three years earlier that this is in fact false for most p, with $p = 23$ being the famous first example. Though Kummer was able to eventually prove Fermat's Last Theorem for regular primes (primes p that do not divide the class number of $\mathbb{Q}(\zeta_p)$) by using the unique factorization of ideals of $\mathbb{Z}(\zeta_p)$, a general proof remained elusive.

While the failure of unique factorization in rings of integers is nonideal, it is reasonable to ask whether or not any number field K that does not have class number 1 can be embedded in a finite field extension L with class number 1. Though Kummer didn't have the tools to answer this embeddability question, his work laid the foundation for the 20th century development of class field theory, which sought to classify abelian extensions of arbitrary number fields. Earlier, the Kronecker-Weber theorem had shown that every finite abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field. However, this idea was not generalizable to algebraic number fields in general, necessitating the development of techniques specific to class field theory.

Of particular interest is the *Hilbert class field*, defined as the maximal unramified abelian extension of a number field, though this definition came about after Hilbert's initial conjecture. In 1902 Hilbert conjectured that for any number field K, there exists a unique finite extension H_K of K such that the principal prime ideals of $\mathcal{O}_K$ split completely in H_K/K. The existence and unicity of such an object was proved by Philipp Furtwängler, who proved various other properties, including completeness, i.e. the Hilbert class field is the maximal unramified abelian extension of K, giving us the definition we now use.

Note that the Hilbert class field H_K is Galois, since primes of a number field K are unramified in an extension L if and only if they are unramified in the normal closure of L. Therefore, by the maximality of H_K, it is a normal extension of K. Artin's reciprocity theorem of class field theory gives a canonical isomorphism $\mathrm{Gal}(H_K/K) \cong C_K$, where C_K denotes the ideal class group of K, and $[H_K : K] = h_K$, the class number of K. This isomorphism reduces the following theorem to a group-theoretic statement that was proved by Furtwängler.

THEOREM 1 (Principal Ideal Theorem, 1930). *Every fractional ideal $\mathfrak{a}$ of a number field K becomes principal (or* capitulates*) in the Hilbert class field H_K, i.e. for every ideal $\mathfrak{a}$ of the ring of integers $\mathcal{O}_K$, $\mathfrak{a}\mathcal{O}_{H_K}$ is principal in $\mathcal{O}_{H_K}$.*

This theorem is closely related to the class field tower problem, first proposed in 1925 by Furtwängler. A *class field tower* is formed by iteratively taking Hilbert class fields of a number field:

$$K = H_{K_0} \subseteq H_{K_1} \subseteq \dots,$$

where $H_{K_{i+1}}$ is the Hilbert class field of H_{K_i}. The class field tower problem asks whether the tower stabilizes within a finite number of steps. If so, then for some large n, H_{K_n} would be a finite extension of K and a principal ideal domain, so would have class number 1. In fact, the converse is also true. If L is a finite field extension of K such that $h_L = 1$, then for each i, $H_{K_i} \subset H_{L_i} = L$, so the class field tower over K must be finite. Thus, the class field tower problem is in fact equivalent to the embeddability problem.

For nearly 40 years, no counterexamples emerged, leading many to suppose that class field towers always terminated. It wasn't until 1964 that Evgeny Golod and Igor Shafarevich provided a definitive answer in the negative, producing counterexamples by using a group-theoretic statement. It is as follows.

THEOREM 2 (Golod and Shafarevich, 1964[1]). *For a finite p-group G, $r > d^2/4$, where $d = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$ and $r = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$.*

2. Infinite p-Class Field Towers

To answer the class field tower problem in the negative, we may consider p-class field towers instead, which are related to the embeddability of arbitrary number fields in finite field extensions with class number prime to p. A Hilbert p-class field H_K^p of number field K is simply defined as the maximal unramified abelian p-extension of K, where a p-extension refers to one whose Galois group is a p-group. The Hilbert p-class field tower over K is similarly defined. We also have an isomorphism between $\mathrm{Gal}(H_K^p/K)$ and the p-part C_K, denoted by C_K^p. We also denote the p-rank of C_K be $d_p C_K = \dim_{\mathbb{F}_p} C_K/pC_K$ (more generally we can take the p-rank of any abelian group A). Thus, as before, a number field K an be embedded into a finite field extension with class number prime to p if and only if the Hilbert p-class field tower terminates.

If any p-class field tower over K is infinite, then the class field tower is also infinite. Thus, to provide their negative result to the class field tower, Golod and Shafarevich needed only to verify that infinite p-class field towers exist. For any number field K, consider the union $\bigcup H_{K_i}^p$ of the elements in the p-class tower, which we shall denote as $H_{K_\infty}^p$. Note that if the tower terminates, $H_{K_\infty}^p$ must be a finite field extension, i.e. $\mathrm{Gal}(H_{K_\infty}^p/K)$ is a finite p-group.

REMARK 1. It is important to note that while the existence of an infinite p-class tower for a number field K implies that the class field tower of K does not terminate, the converse is not necessarily true [**Sch86, McL08**]. For example, the class field tower of $\mathbb{Q}(\sqrt{-239}, \sqrt{4049})$ is infinite, while all the p-class field towers are finite.

The first examples of number fields with infinite p-class field towers came from the 2-class field towers of quadratic imaginary number fields fields. One year prior to proving

[1]The original version of this inequality was $r > (d-1)^2/4$, and Vinberg and Gaschütz (1967) provided a refinement.

the Golod-Shafarevich inequality with Golod, Shafarevich proved a bound on the difference between relation and generator ranks of $G = \mathrm{Gal}(H^p_{K_\infty}/K)$ for K a quadratic imaginary number field.

THEOREM 3 (Shafarevich, 1963[2]). *Let $G = Gal(H^p_{K_\infty}/K)$ for a quadratic imaginary number field K. If G is finitely generated as a pro-p group, then*

$$r - d \leq 1.$$

For $p \neq 2$, then $r = d$.

This inequality, along with $r > d^2/4$ give us a contradiction for $d \geq 5$ if we assume all such G are finite p-groups. Thus, there must be infinite 2-class field towers, showing that not all number fields K have a finite field extension of class number 1.

The results of 2-genus theory for quadratic imaginary fields gives us a way to construct a number field with infinite 2-class field tower.

THEOREM 4. *If K is a quadratic imaginary field in which t odd primes ramify, then $d = d_2 C_K \geq t - 1$.*

Thus, the field $K = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17})$, in which 6 primes ramify, has an infinite 2-class field tower. The original counterexample given by Golod and Shafarevich in their 1964 paper is a number field in which 7 primes ramify, due to their slightly weaker original inequality $r > (d-1)^2/4$.

Note that this concept is generally true. If "too many" primes ramify in a number field, then it will have an infinite p-class field tower.

THEOREM 5 (Brumer, 1965). *If K is a number field of degree n over $\mathbb{Q}$, and p is a rational prime and t denotes the number of rational primes q such that p divides their ramification indices, then*

$$d_p C_K \geq t - n^2.$$

Further details will be given on the refinements made to Golod and Shafarevich's criterion for an infinite class field tower in Chapter 5.

[2]Iwasawa (1977) produced the more general inequality $r - d \leq c_1 + c_2$, where c_1 is the number of real embeddings of K and c_2 the number of complex embeddings.

CHAPTER 2

Preliminaries

1. Group Theory Reminders

DEFINITION 1. For a prime p, G is a *finite p-group* if $|G| = p^n$ from some $n \in \mathbb{N}$.

DEFINITION 2. Let G be a group. The *commutator* of two elements $x, y \in G$ is defined as $[x, y] = x^{-1}y^{-1}xy$. The *commutator subgroup of* G, denoted by $[G, G]$, is the set of all commutators of G, $\{[x, y] : x, y \in G\}$.

True to its name, the commutator is a measure of commutativity, and taking the quotient of G by the closure of $[G, G]$ gives the *abelianization of* G, denoted by G^{ab}. The abelianization is very important later when we use group cohomology to describe the generators of pro-p groups. Furthermore, the results of class field theory give us $G^{ab} \cong C_K^p$ for $G = \mathrm{Gal}(H_{K_\infty}^p/K)$. See the statement of Burnside's Basis Theorem in Chapter 3 for more information.

2. Group Algebras/Rings

DEFINITION 3. Let G be a (multiplicative) group and Λ a unitary commutative ring. The *group algebra* of G over Λ, also known as the *group ring*, denoted by $\Lambda[G]$, is defined to be the free Λ-module on the basis G, i.e. the set of all finite of all linear combinations

$$\alpha = \sum_{g \in G} a_g g$$

with $a_g \in \Lambda$ and $a_g = 0$ for all but finitely many $g \in G$. We define the sum

$$\left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} (a_g + b_g) g$$

and the product

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} c_g g$$

where $c_g = \sum_{x \in G} a_x b_{x^{-1}g}$.

DEFINITION 4. The group ring $\Lambda[G]$ has an *augmentation map* $\epsilon : \Lambda[G] \to \Lambda$ given by

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g.$$

The kernel $I(G)$ of this map is known as the *augmentation ideal* of $\Lambda[G]$.

PROPOSITION 1. *The set $\{g - 1 : g \neq 1, g \in G\}$ is a Λ-basis for $I(G)$.*

PROOF. For any $g \in G$, $\epsilon(g-1) = 1-1 = 0$, so the set is in $I(G)$. For any $\sum_{g\in G} a_g g \in I(G)$, we have that $\sum_{g\in G} a_g = 0$, so

$$\sum_{g\in G} a_g g = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g(g-1),$$

so the set spans $I(G)$.

Finally, suppose

$$0 = \sum_{g\in G} a_g(g-1).$$

Then

$$\sum_{g\in G} a_g = \sum_{g\in G} a_g g,$$

so the right hand side must be a constant, which can only happen if all $a_g = 0$ for $g \neq 1$. Thus, $\{g-1 : g \neq 1, g \in G\}$ is independent and spans, so is therefore a basis. □

Group algebras are useful in studying group representations.

3. Group Cohomology

From group rings, we get the concept of *G-modules*, which are in fact $\Lambda[G]$-modules, though we use the abbreviated terminology. A G-module M is acted on by a group G, and any such G-module has a submodule of G-invariant elements, denoted $M^G = \{m \in M : \forall g \in G : gm = m\}$. Furthermore, the collection of all G-modules forms a category, denoted C_G. The map that sends any module M to M^G yields a functor from $F : C_G \to \text{Ab}$. The cohomology groups of G with coefficients in M are the derived functors of F, i.e. they measure how far the cochain complex is from being exact. Though this is the simplest way to define cohomology groups, in the interest of avoiding category theory to keep this section as self-contained as possible, we introduce an alternative, though long-winded, definition of cohomology groups using cochains.

DEFINITION 5. Let G be a group and M a G-module, and suppose $n \geq 0$ is an integer. Then the *group of n-cochains*, is $C^n(G, M) = \{f : G^n \to M\}$, the group of continuous maps of G^n to M. These groups give us a cochain complex

$$\ldots \to C^n \xrightarrow{d^n} C^{n+1} \xrightarrow{d^n+1} C^{n+2} \to \ldots$$

with *coboundary homomorphisms* defined by

$$(d^n f)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}).$$

Note that $d^{n+1} \circ d^n = 0$.

DEFINITION 6. Let G, M, n be as in the previous definition. Then the set of n-cocycles of G with coefficients in M is defined $Z^n(G, M) = \ker d^n$. The group of n-coboundaries is$B^n(G, M) = \text{im } d^{n-1}$ for $n \geq 1$, with $B^0(G, M) = 0$.

With all of these definitions out of the way, we can finally define the nth cohomology group of G with coefficients in M to be

$$H^n(G, M) = Z^n(G, M)/B^n(G, M).$$

As an example, the 0th cohomology group of the G-module M, denoted $H^0(G, M) = \{m \in M : m^\sigma = m \ \forall \sigma \in G\}$. That is to say, $H^0(G, M)$ is the submodule of M containing all G-invariant elements. The 1st cohomology group $H^1(G, M)$ represents the set of crossed homomorphisms ($f : G \to M$ such that $\forall a, b \in G : f(ab) = f(a) + af(b)$ modulo the homomorphisms $f : G \to M$ such that $f(a) = am - m$ for some $m \in M$. Interpretations exist for cohomology groups of higher dimensions, though we omit them here.

REMARK 2. If the action of G on M is trivial, then we have that $H^0(G, M) = H^1(G, M) = \mathrm{Hom}(G, M)$.

CHAPTER 3

Pro-p Groups

1. Basic Definitions

Before we can discuss the Golod-Shafarevich theorem in much detail, we must first introduce pro-p groups, which were well-studied in the theory of p-adic analytic groups, particularly by Michel Lazard. Pro-p groups are a type of profinite group, which we can define in topological terms as follows:

DEFINITION 7. A *profinite group* is a compact, Hausdorff, totally disconnected topological group (a group G with a topology τ such that multiplication and taking inverses are continuous functions in the product topology and τ, respectively). Equivalently, a compact Haudorff topologically group is *profinite* if its open subgroups form a base for the neighborhoods of the identity, i.e. every open set containing the identity contains an open subgroup.

Note that the open subgroups of profinite groups are also closed due to compactness, so all open subgroups are also normal, and every closed subgroup of a profinite group is profinite. While the topological definition is concise, in our discussion, an equivalent algebraic definition is often more useful. Before introducing this alternate definition, we introduce the notion of inverse limits.

DEFINITION 8. A *directed partially ordered set* is a poset $(I, \leq)$ such that for every $i, j \in I$, there exists a $k \in I$ with $k \geq i, j$. An *inverse system*, also called a *projective system*, over I is a family of groups $(A_i)_{i \in I}$ with a family of homomorphisms $f_{i,j} : A_i \to A_j$ for all $i \geq j$ such that $f_{i,i}$ is the identity on A_i and $f_{ij} \circ f_{jk} = f_{ik}$ for all $i \geq j \geq k$. The *inverse limit*, also called *projective limit*, of the inverse system $((A_i)_{i \in I}, (f_{ij})_{i \geq j \in I})$, is the subgroup of the direct product of the A_i's defined as follows:

$$\varprojlim_{i \in I} A_i = \{\vec{a} \in \prod_{i \in I} A_i \mid a_j = f_{ij}(a_i), \forall i \geq j \in I\}.$$

PROPOSITION 2. *If G is a profinite group, then G is (topologically) isomorphic to $\varprojlim(G/N)$, where N ranges over the open normal subgroups of G. Furthermore, the inverse limit of an inverse system of discrete finite group is profinite. Thus, the topological definition and the definition of a profinite group as the inverse limit of an inverse system of finite groups are equivalent.*

We omit the proof of this proposition, but it can be found in chapter 1 of [**Dix99**].

1.1. Examples of Pro-p Groups. Galois groups of algebraic field extension are a natural example of profinite groups, since the Galois group $\mathrm{Gal}(L/K)$ for a Galois extension L/K is, by construction, the inverse limit of $\mathrm{Gal}(L_i/K)$ for all finite intermediary Galois extensions L_i/K. In fact, William Waterhouse (1974) proved that all profinite groups are the Galois groups of some field extension. The connection between profinite groups and class field theory is stated concisely by Waterhouse's title: "Profinite groups are Galois groups."

Another example of profinite groups is the profinite completion of an arbitrary group.

DEFINITION 9. Let G be an arbitrary topological group and $\mathfrak{N}$ the family of normal subgroups $N \lhd G$ of finite index in G that are closed under finite intersection and ordered by reverse inclusion. Then the *profinite completion* of G, denoted $\hat{G}$, is the inverse limit $\varprojlim (G/N)_{N\in\mathfrak{N}}$.

The profinite completion of G gives us a natural homomorphism

$$\iota : G \to \hat{G}, g \mapsto \prod_{N\in\mathfrak{N}} gN.$$

The image of G under ι is dense in $\hat{G}$ and the kernel of ι is $\bigcap_{N\in\mathfrak{N}} N$. Thus, ι is an injection if and only if G is residually finite, i.e. the intersection $\bigcap N = 1$. If p is a prime and $\mathfrak{N}_p$ consists of normal subgroups of p-power index, then $\varprojlim (G/N)_{N\in\mathfrak{N}_p}$ is known as the *pro-p completion* of G, often denoted as $\hat{G}_p$, which leads us to our definition of pro-p groups.

DEFINITION 10. For a fixed prime p, a *pro-p group* is a profinite group that is the projective limit of finite p-groups (groups in which the order every element is a power of p), or every open normal subgroup has index equal to some power of p. A finite group is pro-p if and only if its order is a power of p.

The most commonly cited example of pro-p groups are the p-adic integers $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ (the pro-p completion of the ring $\mathbb{Z}$) under the addition operation, and indeed the p-adic integers are the historical motivation for studying pro-p groups.

2. Presentations of Pro-p Groups

Because the Golod-Shafarevich theorem is really a group-theoretic statement regarding the minimal presentation of finite p-groups, it is necessary to include a discussion here about the presentations of pro-p groups. First, we will need to introduce the notion of generators of profinite/pro-p groups. *Please note that in the following section, we use "almost all" to mean all except finitely many, and p to refer to a fixed prime.* Here we provide a general definition of generating systems, but with respect to the Golod-Shafarevich theorem, we are primarily interested in finitely generated pro-p groups.

DEFINITION 11. Let G be a profinite group and $N \subset G$ be a closed normal subgroup of G. Let I be an index set and $E = \{s_i : i \in I\}$ be a convergent subset of N, i.e. every open subgroup of N contains almost all elements of E. Then the s_i *generate* N if N is the smallest closed normal subgroup of G containing E. Equivalently, the s_i *generate* N (as a normal subgroup of G) if the subgroup generated (algebraically) by conjugates of the s_i is dense in N, i.e. for every open normal subgroup $H \lhd G$, EH/H generates NH/H.

Taking G to be a normal subgroup of itself, we have a definition for the generators of a pro-p group.

DEFINITION 12. Let G be a profinite group, and let $E = \{s_i : i \in I\}$ be a convergent subset of G. Then E is a *system of generators* for G if G is the smallest closed subgroup containing E. We call E *minimal* if no proper subset of E generates G. The cardinality of a minimal system of generators is known as the *generator rank* of G, denoted by $d(G)$ or d.

Note that the concept of generators of a profinite group is basically same as that of standard group theory, though with a topological twist. Thus, it may not come as unexpected that free groups also have their analogue in free pro-p groups, which are constructed as the pro-p completions of the standard free groups.

DEFINITION 13. Let I be an index set and F_I be the (ordinary) free group on the generators $\{s_i \mid i \in I\}$, and let $\mathfrak{U}$ be the set of normal subgroups $N \lhd F_I$ of p-power index containing almost all of the generators. Then the inverse limit

$$F(I) = \varprojlim (F_I/N)_{N\in\mathfrak{U}}$$

is called the *free pro-p group with system of generators* $\{s_i \mid i \in I\}$.

DEFINITION 14. Suppose that E is a system of generators the pro-p group G. Let F be the free pro-p group on the system of generators E. Then, as with the presentation of ordinary groups, we have an exact sequence

$$1 \to R \to F \to G \to 1,$$

which is called a *presentation* of G by F, often denoted by $\langle E; R\rangle$.

DEFINITION 15. Let R, F, G, E be as above. A set $S \subseteq R$ is a *system of relations* with respect to E if S is a system of generators for R as a normal subgroup of F. A system of relations S is *minimal* if no proper subset of S generates R. The cardinality of S is known as the *relation rank* of G, denoted $r(G)$ or r.

3. Cohomological Interpretation of Generators and Relations

3.1. Computing $d(G)$. While the definitions of generators provided above are useful in giving the algebraic intuition behind systems of generators and systems of relations, they don't give us an easy way to calculate $r(G)$ and $d(G)$, which is why we would like to interpret generators and relations in terms of the cohomology groups of pro-p groups, allowing to use the tools like short exact sequences to simplify our calculations.

This is motivated by Pontryagin duality, which states that the category of discrete torsion abelian groups is dual to the category of profinite abelian groups, i.e. if G is a discrete torsion abelian group or profinite abelian group, its dual $G^* = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. In the context of pro-$p$ groups, Pontryagin duality gives us a correspondence between abelian pro-p groups and discrete abelian p-primary torsion groups.

Note: From now on, we abbreviate $H^n(G, \mathbb{F}_p)$ as $H^n(G)$. We are particularly interested in cohomology groups as vector spaces over $\mathbb{F}_p$, as any pro-p group G always acts trivially on $\mathbb{F}_p$, because every automorphism of the abelian group $\mathbb{F}_p$ has order coprime to p (by Fermat's Little Theorem). Therefore, $H^1(G) = \mathrm{Hom}(G, \mathbb{F}_p)$, suggesting that Pontryagin duality may be useful in elucidating the structure of $H^1(G)$.

DEFINITION 16. The *Frattini subgroup* $\Phi(G)$ of a group G is the intersection of all maximal closed subgroups of G.

REMARK 3. If G is a finite p-group, then $\Phi(G) = \overline{G^p[G, G]}$, i.e. the closure of the set of products of pth powers and commutators in G.

Thus, taking the quotient by $\Phi(G)$ should abelianize G, in addition to killing all pth powers, which makes $G/\Phi(G)$ the largest profinite abelian quotient of exponent p of G.

Furthermore, $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$. Taking the Pontryagin dual of $G/\Phi(G)$, we get

$$(G/\Phi(G))^* = \mathrm{Hom}(G/\Phi(G), \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{F}_p) = H^1(G).$$

This result, combined with the Burnside's Basis Theorem gives us a new way to interpret generator and relation rank.

THEOREM 6 (Burnside's Basis Theorem). *Let G be a pro-p group and let $E = \{s_i : i \in I\}$ be a convergent subset of G. Then E is a system of generators of G if and only if the subset $\overline{E}$ of residue classes modulo $\Phi(G)$ generates $G/\Phi(G)$.*

Considering G, $G/\Phi(G)$ and $(G/\Phi(G))^* = H^1(G)$ as vector spaces over $\mathbb{F}_p$, and noting that taking the dual doesn't change dimension, we have

$$d(G) = \dim_{\mathbb{F}_p}(G/\Phi(G)) = \dim_{\mathbb{F}_p}(G/\Phi(G))^* = \dim_{\mathbb{F}_p} H^1(G),$$

giving us a cohomological interpretation of the generator rank of a pro-p group.

3.2. Computing $r(G)$. To provide a cohomological interpretation of the relation rank, we note that the relation rank of G is $\dim_{\mathbb{F}_p} H^1(R)$, as given above, and that the presentation of G by the free pro-p group F gives the isomorphism $G \cong F/R$, with R a normal subgroup of F, which allows us to apply the Hochschild-Serre spectral sequence[1]. This spectral sequence induces an exact sequence known as an inflation-restriction exact sequence. Here, we gloss through the details and simply give the sequence:

$$0 \to H^1(G, \mathbb{F}_p^R) \to H^1(F, \mathbb{F}_p) \to H^1(R, \mathbb{F}_p)^G \to H^2(G, \mathbb{F}_p^R) \to H^2(F, \mathbb{F}_p).$$

Since F is free, the cohomological dimension[2] of F is ≤ 1, which implies that $H^2(F) = 0$, which allows us to sum dimensions (Hilbert's Syzygy Theorem), noting that $\mathbb{F}_p^R = \mathbb{F}_p$, which gives us

$$\dim_{\mathbb{F}_p} H^1(G) - \dim_{\mathbb{F}_p} H^1(F) + \dim_{\mathbb{F}_p} H^1(R)^G - \dim_{\mathbb{F}_p} H^2(G) = 0,$$

and since $\dim_{\mathbb{F}_p} H^1(G) = \dim_{\mathbb{F}_p} H^1(F)$,

$$\dim_{\mathbb{F}_p} H^1(R)^G = \dim_{\mathbb{F}_p} H^2(G).$$

We note that the action of any element $\overline{g} \in G$ on any $f \in H^1(R)$ is given by $(g \cdot f)(r) = g \cdot f(g^{-1}rg)$, where $g \in F$ is a representative of the residue class $\overline{g}$. Thus, the set of G-invariants of $H^1(R)$ is $\{f : R \to \mathbb{F}_p \mid f(r) = f(g^{-1}rg)\ \forall r \in R\}$. Thus, the $\mathbb{F}_p$-dimension of $H^1(R)^G$ counts the number of conjugacy classes of generators of R. However, the definition of a system of generators of R as a normal subgroup of F states that R is the smallest normal subgroup containing the generators of R, i.e. the system of relations for G, so we have $\dim_{\mathbb{F}_p} H^1(R) = \dim_{\mathbb{F}_p} H^1(R)^G$. Together with our previous result, this gives us the following proposition.

PROPOSITION 3. *For a pro-p group G,*

$$d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) \text{ and } r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p).$$

[1]Let G be a group, N be a normal subgroup, and A a G-module. Then there is a spectral sequence of cohomological type: $H^p(G/N, H^q(N, A)) \Rightarrow H^{p+q}(G, A)$.

[2]The cohomological dimension of G, denoted by $\mathrm{cd}(G)$, is defined as the least integer n such that $H^k(G) = 0$ for all $k > n$. A free group F has $\mathrm{cd}(F) \leq 1$. For details, see any general text on pro-p groups, such as [**Ser02**].

4. Completed Group Algebras

The cohomological interpretation of generators and ranks gives us a great deal of information about the presentation of a pro-p group. However, in order to prove the relationship between generators and relations given by the Golod-Shafarevich inequality, we need to give even more structure to pro-p groups. Specifically, we wish define an object with structure similar to that of a polynomial ring, allowing us to treat it as a graded algebra.

In essence, the completed group algebra is the profinite completion of group rings of the quotients of open normal subgroups. More precisely, let G be a pro-p group and let Λ be a compact unitary commutative ring. Let N, N' be open normal subgroups of G with $N \supseteq N'$. We can thus extend the map $G/N' \to G/N$ to the homomorphism $\Lambda[G/N'] \to \Lambda[G/N]$ of group rings. Note that if G is finite, then $\Lambda[G]$ is a compact group algebra.

Definition 17. The *completed group algebra* $\Lambda[[G]]$ of the pro-p group G is

$$\varprojlim(\Lambda[G/N])_{N\in\mathfrak{N}},$$

where $\mathfrak{N}$ is the set of all open normal subgroups of G.

There is an embedding $G \to \Lambda[[G]]$ given by $g \mapsto \prod_{N\in\mathfrak{N}} gN$. Furthermore, $\Lambda[G]$, viewed as a subring of $\Lambda[[G]]$ with the subspace topology is dense in $\Lambda[[G]]$. A key property of completed group algebras (by Brumer) is as follows.

Theorem 7. *If $\phi : G \to G'$ is a morphism of profinite groups with $N = \ker\phi$, we have that the kernel of the induced morphism $\phi' : \Lambda[[G]] \to \Lambda[[G']]$ is the closed ideal $I(N)$ generated by all $h - 1$ such that $h \in N$.*

We omit the details of the proof here, since they can be found in Theorem 7.3 (iii) [**Koc02**]. As a sketch, we have that $I(N) \subseteq \ker\phi$, so ϕ induces a morphism $\hat{\phi} : \Lambda[[G]]/I(N) \to \Lambda[[G']]$. To prove reverse inclusion, we restrict the morphism $\hat{\phi}$ to G (a subspace, using the embedding given above), which gives us an isomorphism $\{G + I(N)\}/I(N) \to G'$. Lifting the inverse map $G' \to \{G + I(N)\}/I(N)$ gives us an inverse to $\hat{\phi}$, so $I(N) = \ker\phi$.

This theorem is very useful in the proof of Golod-Shafarevich, since a minimal presentation of a pro-p group G gives us an epimorphism $F \to G$ of pro-p groups with kernel R. This allows us to apply what we know about free pro-p groups to more general pro-p groups. More specifically, free pro-p groups are easier to work with because their completed group algebras have the structure of a polynomial ring, as given by the Magnus algebra and related Magnus embedding.

Definition 18. Let Λ be a ring with identity and let m be a positive integer. The *Magnus algebra* $\Lambda(m)$ in the variables $x_1, \ldots, x_m$ over Λ is the algebra of formal noncommutative (associative) power series in the x_i with coefficients in Λ.

Theorem 8. *If F is a free pro-p group with system of generators $s_1, \ldots, s_m$, then the completed group ring $\Lambda[[F]]$ is isomorphic to the ring $\Lambda(m)$ by linearly extending the homomorphism $\psi(s_1) = 1 + x_i$.*

Again, we omit the details of the proof, since they are clearly presented in Theorem 7.16 of [**Koc02**]. Essentially, we establish that the powers of the augmentation ideal $\{I^n(G) : n \in \mathbb{N}\}$ form a basis of neighborhoods at $0 \in \Lambda[[G]]$. Recall that the augmentation ideal $I(G)$ is the kernel of the augmentation map $\Lambda[G] \to \Lambda$. In the context of completed group algebras, we use $I(G) \subset \Lambda[[G]]$ to refer to the closure of the augmentation ideal $I(G) \subset \Lambda[G]$ in $\Lambda[[G]]$.

The topology on the Magnus algebra $\Lambda(m)$ has a basis of open neighborhoods of 0 given by $\{D^n : n \in \mathbb{N}\}$, where D_n is the ideal of homogenous power series of $\Lambda(m)$ with degree n. We can use this topology to get an inverse map to ϕ, giving us an isomorphism $\Lambda[[F]] \to \Lambda(m)$.

From this point, we can identify $\Lambda[[F]]$ with $\Lambda(m)$, which we will often write as $\Lambda(x_1, \ldots, x_m)$ to explicitly reference the generators of $\Lambda(m)$. In the proof of the Golod-Shafarevich theorem, we will consider the specific case $\Lambda = \mathbb{F}_p$.

5. Filtrations

Definition 19. Let G be a finitely generated pro-p group, and let $\mathbb{F}_p[G]$ be its group ring over $\mathbb{F}_p$ with augmentation ideal $I(G) = (g-1)\mathbb{F}_p[G]$ (recall Proposition 1). For $n \in \mathbb{Z}^+$, let the ideal $I^n(G)$ in $\mathbb{F}_p[[G]]$ denote the closure of the nth power of $I(G)$ in $\mathbb{F}_p[[G]]$. Then define G_n, the *nth modular dimension subgroup of G* as

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

The descending chain of dimension subgroups

$$G = G_1 \supseteq G_2 \supseteq \ldots$$

forms what is called the *Zassenhaus filtration of G*.

Such a filtration allows us to divide the relations of any pro-p group into levels.

Definition 20. Let G be a pro-p group with minimal presentation $1 \to R \to F \to G \to 1$. The *level* of any $r \in R$ is given by the largest integer m such that $r \in F_m \setminus F_{m+1}$, where $\{F_m : m \in \mathbb{N}\}$ is the Zassenhaus filtration of F.

Zassenhaus filtrations can be generalized by filtrations induced by Lazard valuations, which are functions on monomials of a Magnus algebra. Note that if F is a free pro-p group with d generators, each element of $\mathbb{F}_p[[F]] = \mathbb{F}_p(d)$ can be uniquely represented as a linear combination $\sum_K \lambda_K M_K$, where $\lambda_K \in \mathbb{F}_p$ and M_K is a monomial of the variables $x_1, \ldots, x_d$. This allows us to define the Lazard valuation (essentially a modified degree/"logarithm" function) on $\mathbb{F}_p(d)$.

Definition 21. Let F be a d-generated free pro-p group, and let $\tau_1, \ldots, \tau_d \in \mathbb{Z}^+$. The *Lazard valuation of type* $(\tau_1, \ldots, \tau_d)$ on $\mathbb{F}_p(x_1, \ldots, x_d)$, is an additive function $v : \mathbb{F}_p(x_1, \ldots, x_d) \to \mathbb{Z} \cup \{\infty\}$, where $v(x_i) = \tau_i$ and the valuation on monomials is determined additively:

$$v(x_{i_1} x_{i_2} \ldots x_{i_d}) = \tau_{i_1} + \tau_{i_2} + \ldots + \tau_{i_d},$$
$$v(1) = 0, v(0) = \infty.$$

The valuation on an element $\sum_K \lambda_K M_K$ is defined as

$$v\left(\sum_K \lambda_K M_K\right) = \min\{v(M_K) : \lambda_K \neq 0\}.$$

Remark 4. Extending the definition above gives us, for all $a, b \in \mathbb{F}_p(x_1, \ldots, x_d)$, the properties

$$v(ab) = v(a) + v(b),$$
$$v(a + b) \geq \min\{v(a), v(b)\}.$$

Definition 22. We call $\sum_K \lambda_K M_K$ *homogenous of degree m* if $\lambda_K = 0$ for all $v(M_K) \neq m$.

If G is a pro-p group with a minimal presentation $1 \to R \to F \xrightarrow{\phi} G \to 1$, then the Lazard valuation on F induces a Lazard valuation on G. For any $\beta \in \mathbb{F}_p[[G]]$, define

$$v(\beta) = \max\{v(\alpha) \mid \alpha \in \mathbb{F}_p[[F]], \phi(\alpha) = \beta\}.$$

With a given Lazard valuation v on a pro-p group G, we can define a filtration

$$G_n^v = \{g \in G : v(g-1) \geq n\},$$

defining the *level* of any element in G to be the greatest n such that $g \in G_n^v$.

The Zassenhaus filtration is then the induced filtration given by the Lazard valuation of type $(1, \ldots, 1)$, where the valuation is analogous to taking the degree of a power series.

CHAPTER 4

Golod-Shafarevich Theorem

Now that we have introduced the major preliminary background concepts necessary for understanding the proof of the Golod-Shafarevich theorem, we can finally complete the proof. While all the proofs of Golod-Shafarevich in the literature are similar in concept, there are slight distinctions. For example, [**Ser02**] proves the weaker $r > d^2/4$ bound in a more general setting (finite-dimensional algebras) using Tor functors. The proofs of [**Roq67**] and [**Koc78**] are similar, with Roquette's proof being a dual of Koch's. Here, we present the proof of [**Koc78**], with the corrections made by [**McL08**]. Koch provided a revision of his 1978 proof in [**Koc02**], though it is perhaps it is a little less elegant and intuitive than McLeman's revision, so we merely note it here as a potential reference for curious readers.

1. Setup and Outline

Let G be a finitely-generated pro-p group with minimal presentation

$$1 \to R \to F \xrightarrow{\phi} G \to 1.$$

The map $\phi : F \to G$ induces a map $\mathbb{F}_p[[F]] \to \mathbb{F}_p[[G]]$, which we also denote as ϕ. For brevity's sake, let

$$A = \mathbb{F}_p[[F]] \text{ and } B = \mathbb{F}_p[[G]].$$

Let $\{s_1, \ldots, s_d\}$ be a lift of the generators of G to F, and let $\{\rho_1, \ldots, \rho_r\}$ be a system of relations for G, i.e. a system of generators for R. Then, using the results on Magnus algebras from the previous chapter, we have that

$$A \cong \mathbb{F}_p(x_1, \ldots, x_d),$$

with an isomorphism given by $s_1 \mapsto x_i + 1$. Then, since the kernel of $\phi : A \to B$ is given by $I(R)$, which is generated by $\rho_1 - 1, \ldots, \rho_r - 1$, we have, identifying A with $\mathbb{F}_p(x_1, \ldots, x_d)$,

$$B \cong A/I(R).$$

Denote the generators of the B by $y_i = \phi(s_i) - 1 = \phi(x_i)$.

Let v be a Lazard valuation of type $(\tau_1, \ldots, \tau_d)$ on A. We can suppose without loss of generality that $\tau_i \leq \tau_{i+1}$ for $1 \leq i \leq d-1$ (if not, just reorder the variables x_i. In addition, we can suppose that the relations are ordered so that their levels are monotonically increasing. The valuation v also induces a valuation on B (also denoted by v), giving us the filtration

$$I_n = \{b \in B \mid v(b) \geq n\}$$

for $n \in \mathbb{Z}$. For $n \leq 0$, we define $I_n = B$. In addition, we also introduce the sequence

$$c_n = \dim_{\mathbb{F}_p} B/I_n.$$

With this filtration, we can also count relations and generators by level, setting

$$r_n = |\{\rho_i \mid v(\rho_i - 1) = n\}| \text{ and } d_n = |\{x_i \mid \tau_i = n\}|.$$

Note that $r_0 = 1$, since the valuation on any constant is 0.

The proof centers around the exact sequence

$$B^r \xrightarrow{\phi_1} B^d \xrightarrow{\phi_0} B \xrightarrow{\epsilon} \mathbb{F}_p \to 0,$$

and its restriction (fixing n) to the exact sequence

$$\bigoplus_{i=1}^{r} I_{n-v(\rho_i-1)} \xrightarrow{\psi_1} \bigoplus_{i=1}^{d} I_{n-\tau_i} \xrightarrow{\psi_0} I_n \to 0.$$

We begin by proving these sequences are exact. Then, after some diagram-chasing and dimension counting, we will produce an inequality on the r_i and d_i that eventually gives us the Golod-Shafarevich inequality.

2. Proof

Consider the sequence

$$B^r \xrightarrow{\phi_1} B^d \xrightarrow{\phi_0} B \xrightarrow{\epsilon} \mathbb{F}_p \to 0, \tag{2.1}$$

where ϵ is the augmentation map of $B \to \mathbb{F}_p$. Another way to conceptualize ϵ is to consider B as $A/I(R)$ so that ϵ is the evaluation map at $(0, \ldots, 0)$.

We define ϕ_0

$$\phi_0(b_1, \ldots, b_d) = \sum_{i=1}^{d} b_i y_i.$$

To define ϕ_1, we first note that each $\rho_i - 1$ has a unique representation in the ring of (noncommutative) formal power series $\mathbb{F}_p(x_1, \ldots, x_d)$:

$$\rho_i - 1 = \sum_{j=1}^{d} z_{ij} x_j,$$

since we may collect the monomials based on their last free variable. Then we define

$$\phi_1(b_1, \ldots, b_r) = \left(\sum_{i=1}^{r} b_i \phi(z_{i1}), \ldots, \sum_{i=1}^{r} b_i \phi(z_{id}) \right).$$

PROPOSITION 4. *The sequence given in (2.1) is exact.*

PROOF. Since ϵ is surjective, then the sequence is exact at $\mathbb{F}_p$. For exactness at B, we note that the augmentation ideal of B is generated by the elements y_i, so $\operatorname{im}(\phi_0) = \ker(\epsilon)$.

Exactness at B^d is given by the fact that $\ker(\phi)$ is generated by the $\rho_i - 1$. More precisely, let $(b_1, \ldots, b_r) \in B^r$. Then

$$\begin{aligned}
\phi_0(\phi_1(b_1, \ldots, b_r)) &= \sum_{j=1}^{d} \sum_{i=1}^{r} b_i \phi(z_{ij}) y_j \\
&= \sum_{j=1}^{d} \sum_{i=1}^{r} b_i \phi(z_{ij} x_j) \\
&= \sum_{i=1}^{r} b_i \sum_{j=1}^{d} \phi(z_{ij} x_j) \\
&= \sum_{i=1}^{r} b_i \phi(\rho_i - 1) \\
&= 0.
\end{aligned}$$

Therefore, we have $\mathrm{im}(\phi_1) \subseteq \ker(\phi_0)$. To show inclusion in the other direction, let $b_1, \ldots, b_d \in B$ such that $\sum_{j=1}^{d} b_j y_j = 0$. We lift the b_j to $a_j \in A$, so that $\sum_{j=1}^{d} a_j x_j \in \ker(\phi)$, and since $\ker(\phi)$ is generated by the $\rho_i - 1 = \sum_{j=1}^{d} z_{ij} x_j$, we have that

$$\sum_{j=1}^{d} a_j x_j = \sum_{i=1}^{r} a'_i \sum_{j=1}^{d} z_{ij} x_j = \sum_{j=1}^{d} \sum_{i=1}^{r} a'_i z_{ij} x_j,$$

which gives us $a_j = \sum_{i=1}^{r} a'_i z_{ij}$. Thus, we have that

$$\begin{aligned}
\phi_1\big(\phi(a'_1), \ldots, \phi(a'_r)\big) &= \left(\sum_{i=1}^{r} \phi(a'_i z_{i1}), \ldots, \sum_{i=1}^{r} \phi(a'_i z_{id}) \right) \\
&= (\phi(a_1), \ldots, \phi(a_d)) \\
&= (b_1, \ldots, b_d),
\end{aligned}$$

so $(b_1, \ldots, b_d) \in \mathrm{im}(\phi_1)$. Thus, (2.1) is exact. □

For a fixed integer n, the restriction of (2.1) induces the sequence

$$\bigoplus_{i=1}^{r} I_{n - v(\rho_i - 1)} \xrightarrow{\psi_1} \bigoplus_{i=1}^{d} I_{n - \tau_i} \xrightarrow{\psi_0} I_n \to 0, \tag{2.2}$$

where ψ_1 and ψ_0 denote the restriction of ϕ_1 and ϕ_0 respectively.

First we verify that $\bigoplus_{i=1}^{r} I_{n - v(\rho_i - 1)}$ is indeed sent to $\bigoplus_{i=1}^{d} I_{n - \tau_i}$ under the map ϕ_1. Let $(h_1, \ldots, h_r) \in \bigoplus_{i=1}^{r} I_{n - v(\rho_i - 1)}$, which gives us

$$v(h_i) \geq n - v(\rho_i - 1). \tag{2.3}$$

Furthermore, since $\rho_i - 1 = \sum_{j=1}^{d} z_{ij} x_j$, we have that

$$v(\rho_i - 1) = \min\{v(z_{ij}) + \tau_j : 1 \leq j \leq d\}.$$

This gives us

$$v(z_{ij}) = v(\phi(z_{ij})) \geq v(\rho_i - 1) - \tau_j. \tag{2.4}$$

Combining (2.3) and (2.4), we have

$$v(h_j) + v(\phi(z_{ij}) \geq n - \tau_j.$$

We have that the jth term $\phi_1(h_1, \ldots, h_r)$ is

$$v\left(\sum_{i=1}^{r} h_j \phi(z_{ij})\right) = \min\{v(h_j) + v(\phi(z_{ij})\} \geq n - \tau_j,$$

so $\phi(h_1, \ldots, h_r) \in \bigoplus_{i=1}^{d} I_{n-\tau_i}$, as desired.

Similarly, ϕ_0 sends elements of $\bigoplus_{i=1}^{d} I_{n-\tau_i}$ to I_n. Now that we've verified that the restriction under the maps is correct, we show that (2.2) is exact at I_n.

PROPOSITION 5. *The map ψ_0 is surjective.*

PROOF. Let $h \in I_n$. Select a $g \in A$ such that $\phi(g) = h$ and $v(h) = v(g)$. Such a g exists, since ϕ is surjective and $v(h) = \max\{v(g) : \phi(g) = h\}$. This g has a unique representation $\sum_{i=1}^{d} g_i x_i$. Denoting the homogeneous components of g with degree m by $g^{(m)}$, we have

$$g^{(m)} = \sum_{i=1}^{d} g_i^{(m-\tau_i)} x_i.$$

Since g cannot have homogeneous components of less than degree n (since $\phi(g) \in I_n$), we have that $v(g_i) \geq n - \tau_i$, which means that $v(h_i) \geq n - \tau_i$, where $h_i = \phi(g_i)$, so $(h_1, \ldots, h_d) \in \bigoplus_{i=1}^{d} I_{n-v(x_i)}$, and

$$\psi_0(h_1, \ldots, h_d) = \sum_{i=1}^{d} h_i y_i = \sum_{i=1}^{d} \phi(g_i x_i) = \phi(g) = h.$$

□

Since (2.2) is exact in I_n and (2.1) is exact, then the factor sequence

$$\bigoplus_{i=1}^{r} B/I_{n-v(\rho_i - 1)} \to \bigoplus_{i=1}^{d} B/I_{n-\tau_i} \to B/I_n \to \mathbb{F}_p \to 0$$

is exact, which gives us

$$\sum_{i=1}^{n} r_i c_{n-i} - \sum_{i=1}^{n} d_i c_{n-i} + c_n \geq 1.$$

Noting that $r_0 = 1, d_0 = 0, c_0 = 1$, we can rewrite this as

$$\sum_{i=0}^{n} (r_i - d_i) c_{n-i} \geq 1. \tag{2.5}$$

With this, we make the following claim.

PROPOSITION 6. *Let G be a finite pro-p group, with d_i, r_i defined as above. Then*

$$\phi_v(t) = 1 + \sum_{n=1}^{\infty} (r_n - d_n) t^n$$

converges, and is greater than 0 for $0 < t < 1$.

PROOF. Multiplying each side of (2.5) by t^n and summing for all n, we have that

$$\sum_{n=0}^{\infty}\left(\sum_{i=0}^{n}(r_i-d_i)c_{n-i}\right)t^n \geq \sum_{n=0}^{\infty}t^n = \frac{1}{1-t}.$$

The Cauchy product of the two series gives us

$$\left(\sum_{n=0}^{\infty}(r_n-d_n)t^n\right)\left(\sum_{n=0}^{\infty}c_nt^n\right) = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n}(r_i-d_i)c_{n-i}\right)t^n.$$

Thus, we have that

$$\left(\sum_{n=0}^{\infty}(r_n-d_n)t^n\right)\left(\sum_{n=0}^{\infty}c_nt^n\right) \geq \frac{1}{1-t}.$$

We have that $\sum_{n=0}^{\infty}c_nt^n$ is convergent for $0<t<1$, since c_n is bounded above if G is finite[1]. Furthermore, since r is finite, we can assume without loss of generality that almost all the $r_n=0$. Because almost all the d_n and r_n are 0 and $\sum c_nt^n$ converges, the left hand side is a polynomial in t and therefore converges.

Dividing both sides by $\sum c_nt^n>0$, and noting that $\frac{1}{1-t}>0$, we get

$$\infty > \sum_{n=0}^{\infty}(r_n-d_n)t^n > 0.$$

Rewriting gives us

$$\phi_v(t) = 1+\sum_{n=1}^{\infty}(r_n-d_n)t^n > 0,$$

as desired. □

Note that for the Zassenhaus filtration, all the generators of a pro-p group are of level 1, so $d_1=d$ and $d_i=0$ for $i\neq 1$. Thus, the previous proposition is frequently presented in the literature as $\sum_{k=2}^{\infty}r_kt^k-dt+1>0$, which is sometimes known as the *Zassenhaus polynomial* of G. Note that $r_1=0$, because if a relation had level 1 (in the Zassenhaus filtration), then it would be a generator of F and contradict the minimality of the presentation of G.

COROLLARY 1. *Let G be a finite pro-p group with $d(G)=d$ and $r(G)=r$, and let $1\to R\to F\to G\to 1$ be a minimal presentation of G with $R\subset F_m$, where $\{F_n\}$ is the Zassenhaus filtration of G. Then,*

$$r > \frac{d^m}{m^m}(m-1)^{m-1}.$$

PROOF. Since $R\subset F_m$, we have $\phi_v(t)=1-dt+rt^m$. Suppose for the sake of contradiction that

$$r \leq \frac{d^m}{m^m}(m-1)^{m-1}.$$

This gives us

$$\sqrt[m-1]{\frac{d}{mr}} \geq \frac{m}{d(m-1)}.$$

[1]See Lemma 7.9 in [**Koc02**] for a proof of the fact that $I^n(G)=0$ for sufficiently large n using the composition series of $I^n(G)$.

Setting $t = \sqrt[m-1]{\frac{d}{mr}}$ gives

$$\begin{aligned}\phi_v\left(\sqrt[m-1]{\frac{d}{mr}}\right) &= 1 - d\cdot\sqrt[m-1]{\frac{d}{mr}} + r\cdot\frac{d}{mr}\cdot\sqrt[m-1]{\frac{d}{mr}} \\ &\leq 1 - \frac{m}{m-1} + \frac{1}{m-1} = 0,\end{aligned}$$

which contradicts Proposition 6. □

For $m = 2$, Corollary 1 gives us the Golod-Shafarevich theorem in the form given by Gaschütz and Vinberg's refinement.

THEOREM 9. *If G is a nontrivial finite p-group, with $d = d(G)$ denoting the generator rank and $r = r(G)$ denoting the relation rank, then $r > d^2/4$.*

Another statement of Vinberg/Gascütz's refinement is as follows:

THEOREM 10. *Let K be a number field and p a rational prime. If K has a finite p-tower, then*

$$d_p C_K < 2 + 2\sqrt{1 + d_p \mathcal{O}_K^\times},$$

where $\mathcal{O}_K^\times$ is the unit group of the ring of integers of K.

CHAPTER 5

Further Work & Ramifications

The Golod-Shafarevich inequality provides a definitive answer to the original class field tower problem by producing some number fields with infinite class field towers, but much work remains to be done in understanding the structure of class field towers, particularly since there does not exist a general method for computing class field towers. It is not even known how to categorize towers by whether they terminate or not. Even in more specific cases, such as 2-class towers of imaginary quadratic fields, a general method of classification does not yet exist.

Furthermore, most of the work done on the subject since 1964 involve the use of Golod and Shafarevich's original condition, or a variation of it, which might lead one to speculate whether producing an infinite p-class tower necessarily requires the application of Golod-Shafarevich at some step (whether applying to the number field itself, or to an unramified extension of the number field). Moreover, as far as we know currently, it seems "necessary" to approach the general class field tower question through p-class field towers. While the results of Schoof (1986) discussed in Chapter 1 produce number fields with infinite class towers but have finite p-class towers for all p, these number fields "depend on a *closely-related* q-class field tower being infinite for some prime q" [**Wan16**]. In addition to determining which number fields have finite (p-)class field towers and which have infinite ones, work has been done to determine the length of the tower if it is finite.

Definition 23. Let K be a number field and let $G = \mathrm{Gal}(H^p_{K_\infty}/K)$ be its p-tower group. Then the length of the p-tower, denoted by $\ell_p(K)$, is defined to be the minimal integer n such that $H^p_{K_n} = H^p_{K_{n+1}}$. Alternatively, the minimal integer n such that $\mathrm{Gal}(H^p_{K_n}/K) \cong G$. If no such integer exists, then $\ell_p(K) = \infty$.

Beyond determining the possible tower lengths of various p-ranks of C_K, much work has been done to determine the group structure of C^p_K. In the following section, we denote the group isomorphic to $\mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_t\mathbb{Z}$ by " a group of type $(m_1, \ldots, m_t)$."

In this section, we introduce several of the lingering questions that remain after Golod-Shafarevich's result, and attempt to give a broad outline of the methodology of mathematical work in this subject area.

1. Quadratic Imaginary Fields

While the Golod-Shafarevich inequality uses quadratic imaginary fields as a jumping off point for a negative answer for the general class field tower question, many open questions remain concerning the p-towers of quadratic imaginary fields. Generally, research in this subject area is splits the question into two cases: odd primes and even primes.

1.1. Odd p. The work of Koch and Venkov gives further insight to classifying quadratic imaginary number fields according to the length of their class towers.

THEOREM 11 (Koch-Venkov, 1975). *Let G be a p-tower group over a quadratic imaginary number field with a minimal presentation $1 \to R \to F \to G \to 1$. Then, $R \subset F_3$.*

Though we have not introduced the notion of cup products in this thesis, they are useful in the proof of this theorem. For details, see (3.9.13)(ii) and (10.10.10) in [**NSW13**]. Using Corollary 1, we get $r > 4d^3/27$, and by Theorem 3, we have that $r = d$ for $p \neq 2$, so $d \geq 3$ gives us a contradiction. As a result, we have the following corollary.

COROLLARY 2. *Let $p \neq 2$ be prime, and let K be a quadratic imaginary number field with $d_p C_K \geq 3$. Then the p-class field tower of K is infinite, i.e. $\ell_p(K) = \infty$.*

Examples include $\mathbb{Q}(\sqrt{-3321607})$ for $p = 3$ and $\mathbb{Q}(\sqrt{-22263549223})$ for $p = 5$.

Since $d_p\mathrm{C}_K = 0$ implies that $K = H^p_{K_1}$, we have that the length of the tower is 0. If $d_p\mathrm{C}_K = 1$, then if $G = \mathrm{Gal}(H^p_{K_\infty}/K)$, then $G^{ab} \cong C^p_K$ has 1 generator, so is cyclic and therefore abelian. Thus, $G^{ab} = G \cong C^p_K \cong \mathrm{Gal}(H^p_{K_1}/K)$, so the length of the tower is 1.

This leaves only one final case, $d_p\mathrm{C}_K = 2$. In fact, this case remains open, and Golod-Shafarevich does not tell us about whether the p-towers terminate or not, though no examples of infinite p-class towers have been found for K a quadratic imaginary number field and $p \neq 2$ have been found for $d_p\mathrm{C}_K$ have been found. Furthermore, it seemed from computations that p-towers of finite length must be very short. Only recently were the first examples of 3-towers of length 3 (e.g. $K = \mathbb{Q}(\sqrt{-9748})$) produced [**BM15**], and Bush and Mayer in fact produced a criterion for an imaginary quadratic field K to have $\ell_3(K) = 3$.

1.2. $\mathbf{p = 2}$. As stated in Chapter 1, the theorem of Golod and Shafarevich implies for quadratic imaginary number fields that if $d_2\mathrm{C}_K \geq 5$, then the tower does not terminate. However, the inequality does not give us information on for number fields with $d_2\mathrm{C}_K \leq 4$. Similar to the case with odd p, if $d_2\mathrm{C}_K = 0$, then $\ell_2(K) = 0$, and if $d_2\mathrm{C}_K = 1$, then $\ell_2(K) = 1$. For $d_2\mathrm{C}_K = 2, 3$ examples of finite and infinite 2-class field towers exist. Examples in the case of $d_2\mathrm{C}_K$ include $\mathbb{Q}(\sqrt{-2 \cdot 5 \cdot 31 \cdot 89})$, which has an infinite 2-tower[**Haj96**], while the tower of $\mathbb{Q}(\sqrt{-2379})$ has length 3 [**Bus03**]. In addition to studying number fields whose class groups have certain ranks, more specific cases have been studied, such as the case where $d_2\mathrm{C}_K = 3$ and $C_K \cong (2, 2, 2)$.

Thus, it is the case where $d_2\mathrm{C}_K = 4$ that remains mysterious. In 1978, Martinet conjectured that all 2-towers of number fields with 2-rank 4 are infinite. The problem remains open; no finite 2-towers for quadratic imaginary fields are known, and current examples of infinite 2-towers rely on some extension of Golod-Shafarevich in conjunction with genus theory.

While Corollary 2 does not hold for $p = 2$, in 1996, Hajir improved the earlier theorem of Koch.

THEOREM 12 (Hajir, 1996). *If K is an imaginary quadratic field and $d_4 C_K \geq 3$, i.e. C_K contains a subgroup of type $(4, 4, 4)$, then $\ell_2(K) = \infty$.*

Subsequent work on Martinet's conjecture has focused on cases where C_K has small 4-rank, with the results dependent on properties of the discriminant d_K of K. Genus theory gives us that for K such that $d_2\mathrm{C}_K = 4$, 5 prime discriminants divide d_K, so we can divide number fields into three cases: 1, 3, 5 negative prime discriminants divide d_K. Positive results to Martinet's question have been achieved through casework on Rédei matrices. A number field K has infinite 2-tower if:

- $d_4\mathrm{C}_K = 2$
  - 5 negative prime discriminants divide d_K [**Ben02**]
  - $4 \nmid d_K$ [**Ben15**]
  - 3 negative prime discriminants divide d_K, and d_K is congruent to 4 mod 8 in certain cases [**Ben02**]
  - 1 negative prime discriminant divides d_K [**Mou10**]
- $d_4\mathrm{C}_K = 1$
  - 5 negative prime discriminants divide d_K and d_K not congruent to 4 mod 8 [**Sue09**]
  - 1 negative prime discriminant divides d_K [**Mou10**]

Mouhib's 2010 improvement on Sueyoshi's 2004 result was significant because it applied generally to all 4-ranks.

Another branch of inquiry on the subject of 2-class towers of imaginary quadratic fields is inspired by the root discriminant bounds established by Odlyzko (1976). The root discriminant, $|d_K|^{1/[K:\mathbb{Q}]}$, remains constant throughout the class field tower, so is a useful invariant to study. A number field K will have infinite class field tower if its root discriminant is less than the lower bound on the root discriminant, so successfully finding an infinite p-class tower would improve this bound. Strategies to find infinite 2-class towers involve computation using what is known as the O'Brien tree (also known as descendant trees in the literature), constructed using the lower p-central series of G[1]. Extensive details on the methodology and some computations can be found in [**Bus03, Nov09**].

2. Other Fields

While imaginary quadratic fields have been a focal point for the author's review of literature, we wish to briefly mention that there are other results for different kinds of number fields. For example, many of the results for imaginary quadratic fields have analogues for real quadratic fields. In particular, an analogue for Theorem 12 for real quadratic number fields was established by Maire.

THEOREM 13. *Let K be a real quadratic number field with $d_4C_K \geq 4$. Then $\ell_2(K) = \infty$.*

A similar result exists for cyclic cubic extensions of $\mathbb{Q}$ for p-towers with $p \geq 5$. Finally, a great deal of work has been done for the p-class field towers of cyclotomic fields $\mathbb{Q}(\zeta_p)$. The author recommends Franz Lemmermeyer's comprehensive and detailed survey to interested readers [**Lem10**].

Hopefully this brief sampling of the work that has been done since Golod-Shafarevich gives a sense of how much remains to be learned about the structure of G.

3. Ramifications

Clearly, there remain many open questions regarding specifically the Galois groups of unramified p-extensions of number fields, but the implications of this area of study extend even further. Since a modification of the Golod-Shafarevich theorem holds for p-adic analytic groups, and because we can currently only produce infinite class towers using the inequality, there exists no method of producing potential counterexamples to the Fontaine-Mazur conjecture, as observed in [**NSW13**]. Lacking the background to say much more, we will leave it at that.

[1] closely related to dimension subgroups, by the work of Lazard and Jennings

References

[Ben01] Elliot Benjamin. On imaginary quadratic number fields with 2-class group of rank 4 and infinite 2-class field tower. *Pacific Journal of Mathematics*, 201:257–266, 2001.

[Ben02] Elliot Benjamin. On a question of martinet concerning the 2-class field tower of imaginary quadratic number fields. *Annales Mathématiques du Quebec*, 26(1):1–13, 2002.

[Ben15] Elliot Benjamin. On the 2-class field tower conjecture for imaginary quadratic number fields with 2-class group of rank 4. *Journal of Number Theory*, 154:118–143, 2015.

[BM15] Michael R. Bush and Daniel C. Mayer. 3-class field towers of exact length 3. *Journal of Number Theory*, 147:766–777, February 2015.

[Bus03] Michael R. Bush. Computation of galois groups associated to the 2-class towers of some quadratic fields. *Journal of Number Theory*, 100(2):313–325, June 2003.

[Chi09] Nancy Childress. *Class field theory*. Springer, 2009.

[Dix99] J. D. Dixon. *Analytic pro-p groups*. Cambridge Univ. Pr., 2 edition, 1999.

[Haj96] Farshid Hajir. On a theorem of koch. *Pacific Journal of Mathematics*, 176(1):15–18, 1996.

[Haj00] Farshid Hajir. Correction to "on a theorem of koch". *Pacific Journal of Mathematics*, 196(2):507–508, 2000.

[Koc78] Helmut Koch. *Helmut Koch*, chapter Appendix 1, pages 89–126. Deutscher Verlag der Wissenschaften, 1978.

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

[Lem10] Franz Lemmermeyer. Class field towers. 2010.

[McL08] Cameron McLeman. *A Golod-Shafarevich Equality and p-Tower Groups*. PhD thesis, University of Arizona, 2008.

[Mou10] Ali Mouhib. Infinite hilbert 2-class field towers of quadratic number fields. *Acta Aritmetica*, 145(3):267–272, 2010.

[Nov09] Harris Nover. *Computation of Galois Groups of 2-Class Towers*. PhD thesis, University of Wisconsin-Madison, 2009.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Springer, 2013.

[Roq67] Peter Roquette. *On Class Field Towers*, pages 231–249. Thompson Book Company, Inc., 1967.

[RZ00] Luis Ribes and Pavel Zalesskii. *Profinite groups*. Springer, 2000.

[Sch86] René Schoof. Infinite class field towers of quadratic fields. *Journal für die reine und angewandte Mathematik*, 1986(372):209–220, January 1986.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer, 2002.

[Sue04] Yutaka Sueyoshi. Infinite 2-class towers of some imginary quadratic number fields. *Acta Aritmetica*, 113(3):251–257, 2004.

[Sue09] Yutaka Sueyoshi. On 2-class field towers of imaginary quadratic fields. *Far East Journal of Mathematical Sciences*, 34(3):329–339, 2009.

[Sue10] Yutaka Sueyoshi. On the infinitude of 2-class field towers of some imaginary quadratic number fields. *Far East Journal of Mathematical Sciences*, 42(2):175–187, 2010.

[Wan16] Victor Y. Wang. On hilbert 2-class fields and 2-towers of imaginary quadratic number fields. *Journal of Number Theory*, 160:492–515, March 2016.