CLASS FIELD TOWERS AND A THEOREM OF GOLOD–ŠAFAREVIČ

JACOB SWENBERG

Abstract. In this short note, we discuss a theorem of Golod and Šafarevič, which gives some sufficient conditions for a number field to have an infinite class field tower. In particular, their theorem shows that infinite class field towers exist.

1. Introduction

A basic question in algebraic number theory is how class numbers grow in towers of number fields. One might first ask if there are infinite towers of class number 1 fields. Before that, we ask a more simple question:

Question 1.1. Let K be a number field. Does there exist a finite extension L of K such that L has class number 1?

Roquette [4] refers to this as the "imbedding problem for K."

Let H_K denote the Hilbert class field of K. The following proposition helps us answer this question:

Lemma 1.2. [4, Prop 1] *Let K be a number field and L a finite extension of K with class number 1. Then L contains the Hilbert class field of K.*

Proof. Let K_1 be the Hilbert class field of K. Let M be the normal closure of LK_1 over K, and let $I \leq \mathrm{Gal}(M/K)$ be the inertia subgroup for some place v of M. Then since K_1/K is unramified, we have $I \leq \mathrm{Gal}(M/K_1)$, so

$$I \cap \mathrm{Gal}(M/L) \subseteq \mathrm{Gal}(M/K_1) \cap \mathrm{Gal}(M/L) = \mathrm{Gal}(M/LK_1).$$

So the place of L under v is unramified in LK_1. So LK_1/L is unramified at all places. Furthermore, the kernel of the map $\mathrm{Gal}(M/L) \to \mathrm{Gal}(K_1/K)$ is exactly $\mathrm{Gal}(M/LK_1)$, so $\mathrm{Gal}(LK_1/L)$ is abelian. So LK_1/L is an unramified abelian extension.

On the other hand, L has class number 1. By Class Field Theory, we conclude that $LK_1 = L$. So $K_1 \subseteq L$. □

Corollary 1.3. *Let K be a number field. Let $K_0 = K$, and inductively define K_{n+1} to be the Hilbert class field of K_n. Then the tower of fields*

$$K_1 \subseteq K_2 \subseteq \cdots$$

terminates if and only if K is contained in some number field with class number 1.

Proof. Suppose that there exists a number field L with class number 1 such that $K \subseteq L$. Then $K_1 \subseteq L$ by Lemma 1.2. By induction, $K_n \subseteq L$ for all n. But L is a finite extension of K. So there exists some N such that for all $n \geq N$, we have $K_n = K_N$.

Date: Spring 2022.

Conversely, suppose that the tower above terminates. Then $K_n = K_{n+1}$ for some n, so K_n has class number 1 and contains K. □

We are then lead to the following question:

Question 1.4. Is there a number field K such that the tower $(K_n)_{n\geq 1}$ above does not terminate?

Golod and Šafarevič [1] provided a positive answer to this in their 1964 paper "On the Class Field Tower."

Theorem 1.5 (Golod–Šafarevič)**.** *There exists a number field K such that the tower*

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

is infinite (i.e. does not terminate).

The key part of the proof will be an inequality relating the *generator rank* and *relation rank* of finite p-groups.

The structure of this note is as follows. In Section 2, we establish some basic facts about class field towers. In Section 3, we discuss generators and relations for finite p-groups and pro-p groups. We use the concepts from this section to prove a sharpened version of the main inequality of Golod and Šafarevič in Section 4, following the proof given by Neukirch–Schmidt–Wingberg [3, Thm 3.9.7]. In Section 5, we use this inequality to prove that infinite class field towers exist, focusing on imaginary quadratic fields for brevity. In Section 6, we look at further work related to class field towers.

2. Class Field Towers

Let K be a number field throughout. As above, the ring of integers of K will be denoted by $\mathcal{O}_K$, and the class group of K will be denoted by Cl_K.

Definition 2.1. The *(Hilbert) class field tower* of K is the tower of fields

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

where $K_0 := K$ and K_{n+1} is the Hilbert class field of K_n.

Let

$$K_\infty := \bigcup_{n\geq 0} K_n.$$

Lemma 2.2. *The field K_∞ is the maximal unramified pro-solvable extension of K.*

Proof. (This is "obvious" according to some [3, p. 697], but I thought it was worth writing out.)

We see that K_∞ is a union of unramified extensions of K, so K_∞ is unramified over K. The Galois group $\mathrm{Gal}(K_\infty/K)$ is an inverse limit of solvable groups, since $\mathrm{Gal}(K_n/K)$ admits a subnormal series

$$\mathrm{Gal}(K_n/K) \rhd \mathrm{Gal}(K_n/K_1) \rhd \cdots \rhd \mathrm{Gal}(K_n/K_{n-1}) \rhd 1$$

with abelian factor groups $\mathrm{Gal}(K_i/K_{i-1}) \cong \mathrm{Cl}_{K_{i-1}}$.

Conversely, suppose L/K is a pro-solvable, unramified extension of K. Then there exists a tower of extensions

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L$$

with $\bigcup_n L_n = L$ and $\mathrm{Gal}(L_n/L_{n-1})$ abelian. Then L_1 is an unramfied abelian extension of K, so is contained in the Hilbert class field K_1 of K. Suppose that L_n is contained in K_n for some n. Then $L_{n+1}K_n$ is an unramified abelian extension of K_n, so is contained in K_{n+1}. By induction, this shows that L_n is contained in K_n for all n. So $L = \bigcup_n L_n \subseteq K_\infty$. □

Corollary 2.3. *The field K_∞ contains all unramified pro-p extensions of K.*

Proof. Recall that finite p-groups are solvable, since any p-group has nontrivial center and a quotient of a p-group is a p-group. □

Thus, in order to find a number field K with infinite class field tower, it suffices to find K that admits an infinite unramified pro-p extension.

Definition 2.4. The *(Hilbert) p-class field* $K_1^{(p)}$ of K is the maximal unramified abelian p-extension of K. The *(Hilbert) p-class field tower* of K is

$$K = K_0 \subseteq K_1^{(p)} \subseteq K_2^{(p)} \subseteq \cdots$$

where $K_{n+1}^{(p)}$ is the Hilbert p-class field of $K_n^{(p)}$.

Remark 2.5. We have that $\bigcup_n K_n^{(p)}$ is an unramified pro-p extension of K, so is contained in K_∞. In particular, if K has finite class field tower, than K has finite p-class field tower.

3. Facts about finite p groups

For this section, G is a pro-p group. For a 2-torsion abelian group A, we denote by $\dim_2 A$ the dimension of A over $\mathbb{F}_2$.

Definition 3.1. The *rank* of G, denoted $\mathrm{rk}\, G$, is the minimal cardinality of a topological generating set for G.

Definition 3.2. The *relation rank* of G, which we denote by $\mathrm{rel}\, G$, is the minimal cardinality of a topological generating set for the kernel of a surjective map $F \to G$, where F is a free p group of minimal rank.

Proposition 3.3.

$$\mathrm{rk}\, G = \dim_p H^1(G, \mathbb{F}_p) \qquad \textit{and} \qquad \mathrm{rel}\, G = \dim_p H^2(G, \mathbb{F}_p).$$

Proof. Omitted. □

The following lemma will also be useful when working with p-primary G-modules.

Lemma 3.4. *Let G be a finite p-group, and let A be a p-primary G-module (i.e. a finite G-module of p-power order). If $A^G = 0$, then $A = 0$.*

Proof. Suppose $A \neq 0$. As a G-set, we can decompose A into G-orbits. By the orbit-stabilizer theorem, if an orbit is not a singleton, it must have order divisible by p. Then the number of singleton orbits must be divisible by p. But there is always the singleton orbit $\{0\}$. So there must be some nonzero singleton orbit $\{a\}$. But then $a \in A^G - \{0\}$, a contradiction. So $A = 0$. □

Lemma 3.5. [3, Lem 3.9.8] *Let G be a finite p-group, let A be a finite $\mathbb{F}_p[G]$-module, and let $b_i = \dim H^i(G, \mathbb{F}_p)$. Then there is a resolution*

$$0 \to A \to \mathbb{F}_p[G]^{b_0} \to \mathbb{F}_p[G]^{b_1} \to \cdots$$

such that $(\mathbb{F}_p[G]^{b_i})^G$ is in the kernel of the respective boundary map.

Proof. Recall the isomorphism of G-modules $\mathbb{F}_p \to \mathbb{F}_p[G]^G$ given by $1 \mapsto \sum_{g \in G} g$. This extends to an isomorphism $\phi_i : \mathbb{F}_p^{b_i} \to (\mathbb{F}_p[G]^{b_i})^G$. Let $a_1, \ldots, a_{b_0}$ be an $\mathbb{F}_p$-basis of A^G (which makes sense because $b_0 = h^0(G, A) = \dim_{\mathbb{F}_p} A^G$).

We have an exact sequence of G-modules

$$A^G \to A \to A/A^G,$$

giving an exact sequence of $\mathbb{F}_p$-vector spaces

$$0 \to \mathrm{Hom}(A/A^G, \mathbb{F}_p[G]^{b_0}) \to \mathrm{Hom}(A, \mathbb{F}_p[G]^{b_0}) \to \mathrm{Hom}(A^G, \mathbb{F}_p[G]^{b_0}) \to 0.$$

Recall that for any G-modules A and B, we have $(\mathrm{Hom}(A, B))^G = \mathrm{Hom}_G(A, B)$, since the G-action on $\mathrm{Hom}(A, B)$ is given by

$$(gf)(a) = gf(g^{-1}a).$$

Then since $H^1(G, \mathrm{Hom}(A/A^G, \mathbb{F}_p[G]^{b_0})) = 0$, the long exact cohomology sequence gives that

$$\mathrm{Hom}_G(A, \mathbb{F}_p[G]^{b_0}) \to \mathrm{Hom}_G(A^G, \mathbb{F}_p[G]^{b_0})$$

is surjective. In particular, the map $A^G \to \mathbb{F}_p[G]^{b_0}$ given by $a_i \mapsto \phi(e_i)$ extends to a map $s : A \to \mathbb{F}_p[G]^{b_0}$.

We claim that s is injective. Indeed, $\ker s$ is a G-submodule of A, which is a finite G-module of p-power order. Since $(\ker s)^G = 0 \subseteq A^G$, Lemma 3.4 tells us that $\ker s = 0$. So s is injective.

Let $B = \mathbb{F}_p[G]^{b_0}/s(A)$, so that we have an exact sequence

$$0 \to A \to \mathbb{F}_p[G]^{b_0} \to B \to 0.$$

Note that $\mathbb{F}_p[G]^{b_0}$ is an induced module from $\mathbb{F}_p^{b_0}$, so is cohomologically trivial. Then by the long exact sequence on cohomology, the connect maps give isomorphisms

$$H^i(G, B) \cong H^{i+1}(G, A)$$

for $i \geq 1$. Looking near the beginning of the long exact sequence, we have

$$0 \to A^G \to (\mathbb{F}_p[G]^{b_0})^G \to B^G \to H^1(G, A) \to 0.$$

But the first map was defined as a bijection, so has trivial cokernel. So $B^G \cong H^1(G, A)$. By the same construction as above, we form a finite G-module C with an exact sequence

$$0 \to B \to \mathbb{F}_p[G]^{b_1} \to C \to 0$$

such that $B^G \to (\mathbb{F}_p[G]^{b_1})^G$ is bijective. We define $\partial : \mathbb{F}_p[G]^{b_0} \to \mathbb{F}_p[G]^{b_1}$ as the composite

$$\mathbb{F}_p[G]^{b_0} \to B \to \mathbb{F}_p[G]^{b_1}.$$

But then $(\mathbb{F}_p[G]^{b_0})^G$ is contained in the image of A, so is sent to 0 in B. By induction, we continue to build the resolution. $\square$

Definition 3.6. Let A be an $\mathbb{F}_p[G]$-module. The *ascending central series* for A is

$$A_0 = 0, \qquad A_{n+1}/A_n = (A/A_n)^G.$$

The *Poincaré polynomial* of A is

$$P_A(t) = \sum_n \dim(A_{n+1}/A_n)t^n.$$

Lemma 3.7.

$$P_A(t) = (1-t)\sum_n \dim(A_{n+1})t^n.$$

Proof. This follows immediately from $\dim(A_{n+1}/A_n) = \dim(A_{n+1}) - \dim(A_n)$. □

Lemma 3.8. *Let G be a finite p-group. Let $A \subseteq B$ be finite $\mathbb{F}_p[G]$-modules, and let $(A_n)_{n\geq 0}$ and $(B_n)_{n\geq 0}$ be their respective ascending central series. Then $A_n = B_n \cap A$.*

Proof. First, we have $A_1 = A^G = A \cap B^G = A \cap B_1$. So A/A_1 injects into B/B_1. By induction the ascending central filtrations on these modules agree, so the ascending central series for A agrees with that of B. □

4. The Main Inequality

Theorem 4.1 (Gaschütz, Vinberg, Neukirch–Schmidt–Wingberg)**.** [3, Thm 3.9.7] *If G is a finite p-group, then*

$$\dim H^1(G, \mathbb{F}_p) > \frac{1}{4}(\dim H^2(G, \mathbb{F}_p))^2.$$

Proof. Let $k = \dim H^1(G, \mathbb{F}_p)$, and $r = \dim H^2(G, \mathbb{F}_p)$. By Lemma 3.5 applied to $A = \mathbb{F}_p$, we have an exact sequence

$$0 \to \mathbb{F}_p \to \mathbb{F}_p[G] \to \mathbb{F}_p[G]^k \to \mathbb{F}_p[G]^r.$$

Let $A = \mathbb{F}_p[G]/\mathbb{F}_p$ be the cokernel of the first map, identified as a submodule of $\mathbb{F}_p[G]^k$. By Lemma 3.8, we know that $A_n = (\mathbb{F}_p[G]^k)_n \cap A$. Also, we observe that $\partial((\mathbb{F}_p[G]^k)^G) = 0 = (\mathbb{F}_p[G]^r)_0$ by construction of the sequence. By induction, $\partial((\mathbb{F}_p[G]^k)_n) \subseteq (\mathbb{F}_p[G]^r)_{n-1}$. So for each $n \geq 1$, we have a sequence

$$0 \to A_n \to (\mathbb{F}_p[G]^k)_n \to (\mathbb{F}_p[G]^r)_{n-1}.$$

Let $P(t) = P_{\mathbb{F}_p[G]}(t)$. Then $P_A(t) = (P(t)-1)/t$ by dimension shifting ($\mathbb{F}_p[G]$ is induced from $\mathbb{F}_p$). The above exact sequence implies that

$$s_n(\mathbb{F}_p[G]^k) \leq s_n(A) + s_{n-1}(\mathbb{F}_p[G]^r).$$

Then for $0 < t < 1$, by Lemma 3.7, we have

$$kP(t) \leq \frac{P(t)-1}{t} + rtP(t).$$

Rearranging, we get

$$(rt^2 - kt + 1)P(t) \geq 1.$$

As the coefficients for $P(t)$ are nonnegative, we get that $rt^2 - kt + 1 > 0$. On the other hand, the short exact sequence of G-modules

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{F}_p \to 0$$

induces a long exact sequence on cohomology:

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

But $H^1(G,\mathbb{Z}) = 0$, since there are no nontrivial homomorphisms $G \to \mathbb{Z}$ by finiteness of G. So $r \geq k$, so $0 < k/2r < 1$. Plugging in $t = k/2r$ above,

$$\frac{k^2}{4r} - \frac{k^2}{2r} + 1 > 0,$$

which finally gives $r > \frac{1}{4}k^2$, as desired. □

Remark 4.2. According to Neukirch–Schmidt–Wingberg [3, Rmk p. 230], this inequality was first proved independently by Gaschütz and Vinberg. Golod and Šafarevič made use of a slightly weaker inequality:

$$\operatorname{rk} G > \frac{1}{4}(\operatorname{rel} G - 1)^2.$$

5. The Main Theorem

We focus on the case where K is imaginary quadratic and $p = 2$ for simplicity. Let $G = G_K = \operatorname{Gal}(K^{sep}/K)$. We denote by G_{ur} the Galois group of the maximal unramified extension of K, and we denote by $G_{ur}^{(p)}$ its maximal pro-p quotient. In other words, $G_{ur}^{(p)}$ is the Galois group of the maximal unramified pro-p extension of K. We denote

$$h^i(-) := \dim_2 H^i(-,\mathbb{F}_2).$$

Lemma 5.1. [3, Cor 10.7.11] *Let K be a number field, p be a rational prime, and S a finite set of places of K. Let G_S be the Galois group of the maximal S-ramified (unramified outside of S) extension of K. Then for $0 \leq i \leq 2$, the groups $H^i(G_S,\mathbb{F}_p)$ are finite, and*

$$\sum_{i=0}^{2}(-1)^i h^i(G_S,\mathbb{F}_p) \leq \theta - \sum_{v\in S\cap S_p}[K_v:\mathbb{Q}_v] + \#S_\infty,$$

where

$$\theta = \begin{cases} 1, & \mu_p \subseteq K \text{ and } S \subseteq S_\infty \text{ if } p \neq 2 \text{ or } S \subseteq S_{\mathbb{C}} \text{ if } p = 2, \\ 0 & \text{else.} \end{cases}$$

Proof. Omitted. □

Lemma 5.2. *Let K be an imaginary quadratic field. Then*

$$h^2(G_{ur}^{(2)}) - h^1(G_{ur}^{(2)}) \leq 1.$$

Proof. Let $H \lhd G_{ur}$ be the kernel of the map $G_{ur} \to G_{ur}^{(2)}$ so that $G_{ur}^{(2)} = G_{ur}/H$. By inflation-restriction, we have an exact sequence

$$0 \to H^1(G_{ur}/H,\mathbb{F}_2) \to H^1(G_{ur},\mathbb{F}_2) \to H^1(H,\mathbb{F}_2)^{G_{ur}/H} \to H^2(G_{ur}/H,\mathbb{F}_2) \to H^2(G_{ur},\mathbb{F}_2).$$

Thus

$$h^2(G_{ur}/H) - h^1(G_{ur}/H) \leq h^2(G_{ur}) + \dim_2 H^1(H,\mathbb{F}_2)^{G_{ur}/H} - h^1(G_{ur}).$$

Since the fixed field of K^{ur} by H is, by definition of H, the maximal unramified pro-2 extension of K, it has no degree 2 extensions inside K^{ur}. So H cannot have any open index 2 subgroups. So there are no nontrivial continuous homomorphisms from H to $\mathbb{F}_2$. So

$$h^2(G_{ur}/H) - h^1(G_{ur}/H) \leq h^2(G_{ur}) - h^1(G_{ur}).$$

But by Lemma 5.1, we have

$$1 - h^1(G_{ur}) + h^2(G_{ur}) \leq 2.$$

So

$$h^2(G_{ur}^{(2)}) - h^1(G_{ur}^{(2)}) \leq h^2(G_{ur}) - h^1(G_{ur}) \leq 2 - 1 = 1. \qquad \square$$

Theorem 5.3. [3, Thm 10.10.5] *Let K be an imaginary quadratic field such that*

$$\dim_2 \mathrm{Cl}_K /2 \geq 2 + 2\sqrt{2}.$$

Then K has infinite class field tower.

Proof. Suppose for the sake of contradiction that K has finite class field tower. Then K has finite 2-class field tower. Let

$$h^i(K) := h^i(G_{ur}^{(2)}, \mathbb{F}_2).$$

By Theorem 4.1, we have

$$\frac{1}{4}h^1(K)^2 < h^2(K).$$

Rearranging, we have

$$(h^1(K) - 2)^2 < 4(h^2(K) - h^1(K) + 1).$$

But then by Lemma 5.2,

$$\begin{aligned} \dim_2 \mathrm{Cl}_K /2 &= h^1(G_{ur}^{(2)}, \mathbb{F}_2) \\ &< 2 + 2\sqrt{h^2(K) - h^1(K) + 1} \\ &\leq 2 + 2\sqrt{2}. \end{aligned}$$

This contradicts the assumption. So K has infinite class field tower. $\square$

Theorem 5.4. *Let K be an imaginary quadratic field extension of $\mathbb{Q}$ such that at least 6 rational primes are ramified in K. Then K has infinite class field tower.*

Proof. By Theorem 5.3, it suffices to show that $\dim_2 \mathrm{Cl}_K /2 \geq 5$. This follows from [3, Prop 10.10.3]. $\square$

Corollary 5.5. *The field*

$$K := \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$$

has infinite class field tower.

Proof. The primes 2, 3, 5, 7, 11, 13, 17, and 19 are ramified in K. By the above Theorem, K has infinite class field tower. $\square$

6. Further Work

In 2019, Farshid Hajir, Christian Maire, and Ravi Ramakrishna [2] proved the existence of number fields ramified only at p and ∞ with infinite p-class field tower for all p. Previously, only a handful of examples of this type were known.

References

[1] E. S. Golod and I. R. Šafarevič. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.

[2] Farshid Hajir, Christian Maire, and Ravi Ramakrishna. Infinite class field towers of number fields of prime power discriminant. *Advances in Mathematics*, 373:107318, 2020.

[3] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[4] Peter Roquette. On class field towers. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 231–249. Thompson, Washington, D.C., 1967.