REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

The Golod–Shafarevich inequality and the class field tower problem

*Jordi Vilà Casadevall
École Polytechnique Fédérale de Lausanne (EPFL)
jordi.vilacasadevall@epfl.ch

∗Corresponding author

Resum *(CAT)*
En aquest article presentem una demostració del problema de la torre de cossos de classes. Comencem introduint els grups pro-p, expliquem com descriure'ls en termes de generadors i relacions, i presentem la desigualtat de Golod–Shafarevich, la qual estableix un criteri perquè un grup pro-p sigui infinit. Després d'introduir algunes nocions de teoria algebraica de nombres, apliquem la desigualtat de Golod–Shafarevich al problema de la torre de cossos de classes. Obtenim un criteri perquè un cos de nombres tingui una torre de cossos de classes infinita, i donem exemples explícits de cossos de nombres satisfent aquest criteri.

Abstract *(ENG)*
In this article we present a proof of the class field tower problem. We begin by introducing pro-p groups, explain how to describe them in terms of generators and relations, and present the Golod–Shafarevich inequality, which establishes a criterion for a pro-p group to be infinite. After introducing some notions from algebraic number theory, we apply the Golod–Shafarevich inequality to the class field tower problem. We obtain a criterion for a number field to have an infinite class field tower, and give explicit examples of number fields satisfying this criterion.

Keywords: *number theory, class field tower problem, pro-p groups, Golod–Shafarevich inequality.*
MSC (2020): *11R37, 14G32.*

Received: *July 17, 2023.*
Accepted: *September 1, 2023.*

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

1. 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 [6], 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 1916, Philipp Furtwängler realized that the Hilbert 2-class field $\mathbb{H}_{(2)}(K)$ 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 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 $\mathbb{H}^2_{(2)}(K)$ of $\mathbb{H}_{(2)}(K)$ 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 terminates. 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 $\mathbb{H}_p^\infty(K)$ of K has infinite degree, or equivalently, that the Galois group $G_{K,p} := \mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$ is infinite.

A major evidence for the negative answer to the class field tower problem was given by Igor Shafarevich in 1963 (see [9]), 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 later, in 1964, Golod and Shafarevich (see [3]) 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 relations $r(G)$ (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 [10]) and Roquette (see [8]). 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 this article 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. We begin with a brief introduction to pro-p groups that lead to the formulation of the Golod–Shafarevich inequality, following [5] as the main reference. We then introduce some notions from algebraic number theory and class field theory, based on [7], [4] and [1]. We conclude by explaining the solution to the class field tower problem, giving some particular counterexamples of number fields with an infinite class field tower. Most of the results in this last part are taken from [2].

2. The Golod–Shafarevich inequality

Definition 2.1. A *profinite group* is a topological group that can be realized as a projective limit of discrete finite groups.

These groups have an important role in number theory, as Galois groups of algebraic field extensions are always profinite. We are interested in a particular type of profinite groups, called *pro-p groups*, which are those profinite groups that can be realized as an inverse limit of finite p-groups. These groups describe the Galois groups of p-extensions.

Definition 2.2. Let G be a pro-p group. A *system of generators* of G is a subset $E \subseteq G$ with the following properties:

(i) G is the smallest closed subgroup containing E,

(ii) every neighborhood of $1 \in G$ contains all but finitely many elements of E.

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

As when working with regular groups, we can define an analog of a free group and express a pro-p group in terms of generators and relations.

Definition 2.3. 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.

We define the *free pro-p group with system of generators* $\{s_i \mid i \in I\}$ as

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

The group F_I embeds into $F(I)$ by $g \mapsto \prod gN$, and the image of F_I is dense in $F(I)$. Through this embedding, the set $\{s_i \mid i \in I\}$ is in fact a minimal system of generators of $F(I)$.

Example 2.4. Let $I = \{1\}$. Then $F_I = \mathbb{Z}$ and the subgroups $N \in \mathfrak{U}$ in this case are precisely the subgroups $\mathbb{Z}/p^n\mathbb{Z}$. Thus, the free pro-p group generated by a singleton is

$$F(\{1\}) = \varprojlim_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

We say that 1 is a topological generator of $\mathbb{Z}_p$, since $\{1\}$ is a system of generators of this pro-p group as defined above. Nevertheless, observe that 1 does not generate $\mathbb{Z}_p$ as a group.

Definition 2.5. Let G be a pro-p group and let $F(I)$ be a free pro-p group with system of generators $\{s_i \mid i \in I\}$. A *presentation* of G by $F(I)$ is an exact sequence of of pro-p groups

$$1 \longrightarrow R \longrightarrow F(I) \xrightarrow{\varphi} G \longrightarrow 1.$$

We identify R with the corresponding subgroup of F. If $\{\varphi(s_i) \mid i \in I\}$ is a minimal system of generators of G, then the presentation is called *minimal*.

Definition 2.6. Given a presentation of G as in the previous definition, a subset $E \subseteq R$ is called a *system of relations* of G 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.

The first and second cohomology groups of a pro-p group G play a very important role since they allow us to define two very important invariants. If we consider the trivial action of G on $\mathbb{F}_p$, we can regard the cohomology groups $H_n(G, \mathbb{F}_p)$ as $\mathbb{F}_p$-vector spaces. Then, we define the *generator rank* of G as $d(G) := \dim_{\mathbb{F}_p}(H_1(G, \mathbb{F}_p))$ and the the *relation rank* of G as $r(G) := \dim_{\mathbb{F}_p}(H_2(G, \mathbb{F}_p))$. The name given to these invariants is justified by the following theorem:

Theorem 2.7. *The generator rank of a pro-p group G equals the cardinality of any minimal system of generators, and the relation rank equals the cardinality of any minimal system of relations.*

Observation 2.8. The previous theorem tells us, in particular, that any two minimal systems of generators have the same cardinality, and so do any two minimal system of relations. Moreover, this last number is independent of the chosen minimal presentation of G.

One would expect that if the generator rank of G is large compared to the relation rank, then G is infinite. Indeed, the following theorem establishes a sufficient condition for this to happen:

Theorem 2.9 (Golod–Shafarevich inequality)**.** *Let G be a finitely generated pro-p group with $d(G) > 1$. If*

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

then G is infinite.

3. Results from algebraic number theory

3.1 Places of a number field and ramification

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 $|\alpha|_{\mathfrak{p}} := c^{\operatorname{ord}_{\mathfrak{p}}(\alpha)}$ for $\alpha \in K^*$ (and $|0|_{\mathfrak{p}} = 0$) defines a non-Archimedean absolute value on K. We call this a $\mathfrak{p}$*-adic absolute value.* For any two different prime ideals $\mathfrak{p}$ and $\mathfrak{q}$, a $\mathfrak{p}$-adic and a $\mathfrak{q}$-adic absolute values are inequivalent, i.e., they generate different topologies.

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

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

Every finite place of K can be uniquely identified with a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. We can describe how a place 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 $\mathfrak{p}\mathcal{O}_L$ 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 $[L : K]$.

Let's now describe how infinite places split when extended in a finite extension L of K. An infinite place ν of K is called a *real place* if the completion of K with respect to any absolute value contained in ν is $\mathbb{R}$. Similarly, ν is called a *complex place* if the completion of K with respect to any absolute value contained in ν is $\mathbb{C}$. Thus, the real places of K correspond to the distinct embeddings of K into $\mathbb{R}$ and the complex places correspond to the conjugate pairs of embeddings of K into $\mathbb{C}$. We will describe how ν 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 ν is a complex place of K and let $\sigma\colon K \hookrightarrow \mathbb{C}$ be an embedding of K into $\mathbb{C}$ such that $|\sigma(x)|$ is in ν. As $\mathbb{C}$ is algebraically closed, we know from Galois theory that there are exactly $n = [L : K]$ different embeddings $\sigma_i\colon L \hookrightarrow \mathbb{C}$ such that $\sigma_i|_K = \sigma$. No two σ_i can be conjugates, as then they would not agree on K. Hence, they represent n distinct complex infinite places $\omega_1, \dots, \omega_n$ of L. We can write

$$\nu = \omega_1 \cdots \omega_n$$

to indicate that the ω_i are the places of L extending ν. In this case, we define the ramification indices $e(\omega_i|\nu)$ and the inertial degrees $f(\omega_i|\nu)$ to be one, and we say that the complex place ν is unramified in L.

Consider now that ν is a real place of K and let $\sigma\colon K \hookrightarrow \mathbb{R}$ 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 inside $\mathbb{R}$. List the extensions of σ as

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

where $\sigma_i(L) \subset \mathbb{R}$ for $1 \le i \le r$ and σ_{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 places $\omega_1, \dots, \omega_r$ and s distinct complex places $\omega_{r+1}, \dots, \omega_{r+s}$ of L extending ν. We define the ramification indices as follows: if ω_i is a real place of L lying over ν, we set $e(\omega_i|\nu) = 1$. If ω_{r+j} is a complex place, we set $e(\omega_{r+j}|\nu) = 2$. We define all inertial degrees to be one. Thus, we formally write

$$\nu = \omega_1 \cdots \omega_r \omega_{r+1}^2 \cdots \omega_{r+s}^2.$$

Definition 3.1. We say that an extension of number fields L/K is *unramified* if every place of K (finite and infinite) is unramified in L. More generally, if S is a set of places of K, we say that L/K is unramified outside S if all places of K not belonging to S are unramified in L.

Galois theory can be applied to the general problem of determining how places of a number field split in an extension field, as there are connections between the ramification indices and the inertial degrees introduced before with some subgroups of the Galois group of a given extension. The following theorem tells us that unramified Galois extensions remain unramified after lifting:

Theorem 3.2. *Let L/K be an unramified Galois extension of number fields and F a finite extension of K. Then LF/F is unramified.*

A similar property holds for the compositum of unramified Galois extensions:

Theorem 3.3. *Let L/K and F/K be Galois extensions of number fields. Let S be a set of places of K. Suppose L/K and F/K are unramified outside S. Then, LF/K is also unramified outside S.*

Applying this theorem to $S = \emptyset$ we obtain the following result:

Corollary 3.4. *Let L/K and F/K be unramified Galois extensions of number fields. Then, LF/K is unramified.*

3.2 The Hilbert class field

For a number field K, we denote by $\mathrm{Cl}(K)$ the *class group* of K, i.e., the quotient group of the fractional ideals of $\mathcal{O}_K$ by its subgroup of principal ideals. Its cardinality is known as the *class number* of K, and it is always finite.

In 1898, Hilbert stated the following conjecture:

Conjecture 3.5. *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 place $\mathfrak{p}$ of K, the inertial degree $f(\mathfrak{P}|\mathfrak{p})$ (for any place $\mathfrak{P}$ 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 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 3.6. 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.

4. The class field tower problem

We begin by formulating the following problem:

Problem 4.1 (Embeddability problem)**.** *Given a number field K, does it always exist a finite extension L of K such that the $\mathcal{O}_L$ 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. As explained in the previous section, the class group of K is isomorphic to the Galois group $\mathrm{Gal}(\mathbb{H}(K)/K)$. Thus, $\mathcal{O}_K$ is a PID if, and only if, the Hilbert class field of K is K itself. This brings us to consider another problem. To state it, we need the following definition:

Definition 4.2. The *class field tower* of K is the tower of extensions

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

where $\mathbb{H}^m(K)$ is the Hilbert class field of $\mathbb{H}^{m-1}(K)$. We say that the class field tower is *finite* if it stabilizes at some point.

Problem 4.3 (Class field tower problem)**.** *Is the class field tower of any number field K always finite?*

The two previous problems are equivalent in the following sense:

Lemma 4.4. *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 extensions

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

which is obtained by lifting the class field tower of K by L. By Theorem 3.2, $L\mathbb{H}^{n+1}(K)/L\mathbb{H}^n(K)$ is an abelian unramified extension for every $n \in \mathbb{N}$. 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. □

4.1 A criterion for infinite class field towers

In general, computing the class field of a given number is a rather difficult task. It's a bit easier to work with the p-class field, defined in the following:

Definition 4.5. Let p be 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.

Analogously to the class field tower, we define the *p-class field tower* of K as the tower

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

One has that $\mathbb{H}_p^n(K) \subseteq \mathbb{H}^n(K)$. Hence, if the p-class field tower of K is infinite for some prime number p, then so is its class field tower. For a given p, consider 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 $\mathbb{H}_p^\infty(K)/K$ to be infinite. The extension $\mathbb{H}_p^\infty(K)/K$ is unramified, since all its finite subextensions are. Moreover, it is Galois with Galois group

$$\mathrm{Gal}(\mathbb{H}_p^\infty(K)/K) = \varprojlim_{n\geq 0} \mathrm{Gal}(\mathbb{H}_p^n(K)/K).$$

As $\mathrm{Gal}(\mathbb{H}_p^n(K)/K)$ are finite p-groups, $\mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$ is pro-p. In fact, the following theorem holds:

Theorem 4.6. *$\mathbb{H}_p^\infty(K)$ is the maximal unramified pro-p extension of K.*

Let $G_{K,p} := \mathrm{Gal}(\mathbb{H}_p^\infty(K)/K)$. Proving that $\mathbb{H}_p^\infty(K)/K$ is an infinite extension is equivalent to proving that $G_{K,p}$ is infinite. Let $\mathrm{Fr}(G_{K,p})$ be the Frattini subgroup of $G_{K,p}$. Then, the quotient $G_{K,p}/\,\mathrm{Fr}(G_{K,p})$, known as the Frattini quotient, is isomorphic to $\mathrm{Gal}(\mathbb{H}_p(K)/K)$.

By the definition of the p-class field of K and Galois theory, $\mathrm{Gal}(\mathbb{H}_p(K)/K)$ is the maximal elementary abelian quotient of $\mathrm{Gal}(\mathbb{H}(K)/K)$. The correspondence between subgroups and quotients of a finite abelian group tells us that $\mathrm{Gal}(\mathbb{H}_p(K)/K)$ is isomorphic to the maximal elementary abelian subgroup of $\mathrm{Gal}(\mathbb{H}(K)/K)$, i.e., $\mathrm{Gal}(\mathbb{H}(K)/K)[p]$. Taking into account that $\mathrm{Gal}(\mathbb{H}(K)/K) \cong \mathrm{Cl}(K)$, we obtain that

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

The generator rank of a pro-p group is the same as the generator rank of its Frattini quotient, and thus

$$d(G_{K,p}) = d(G_{K,p}/\,\mathrm{Fr}(G_{K,p})) = d(\mathrm{Gal}(\mathbb{H}_p(K)/K)) = \dim_{\mathbb{F}_p}(\mathrm{H}^1(\mathrm{Cl}(K)[p])).$$

Since $\mathrm{Cl}(K)[p]$ is a finite elementary abelian p-group, $\mathrm{H}^1(\mathrm{Cl}(K)[p]) \cong \mathrm{Cl}(K)[p]$. Let $\rho_p(K) := \dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p])$ be the p-rank of the class group of K. Then,

$$d(G_{K,p}) = \dim_{\mathbb{F}_p}(\mathrm{H}^1(\mathrm{Cl}(K)[p])) = \dim_{\mathbb{F}_p}(\mathrm{Cl}(K)[p]) = \rho_p(K). \tag{1}$$

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

Theorem 4.7 (Shafarevich)**.** *Let K be a number field and $\nu_\infty(K)$ the number of infinite places of K. Then, for any prime number p we have*

$$0 \leq r(G_{K,p}) - d(G_{K,p}) \leq \nu_\infty(K) - 1.$$

Combining Theorem 4.7 with Theorem 2.9, we obtain the following criterion for the group $G_{K,p}$ to be infinite:

Corollary 4.8 (Golod–Shafarevich)**.** *In the notations above, assume that*

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

Then $G_{K,p}$ is infinite.

Proof. By Equation (1), $\rho_p(K) = d(G_{K,p})$. Rearranging the terms and squaring this inequality we obtain that

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

Using Theorem 4.7 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 2.9 implies the claim. □

4.2 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 4.8. 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 $\nu_\infty(K) \leq [K:\mathbb{Q}]$ (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 4.8 and hence will have an infinite class field tower.

For $p = 2$, take any $n+1$ distinct prime numbers $q_1, \dots, q_{n+1}$ congruent to 1 modulo 4. Let $K = \mathbb{Q}(\sqrt{q_1 \cdots q_{n+1}})$ and $L = \mathbb{Q}(\sqrt{q_1}, \dots, \sqrt{q_{n+1}})$. Notice that $[K:\mathbb{Q}] = 2$. One could see that the extension L/K is unramified, and hence $L \subseteq \mathbb{H}(K)$. Observe that L is an abelian extension of K with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. By the correspondence between subgroups and the quotients of a finite abelian group, $\mathrm{Gal}(\mathbb{H}(K)/K)$ must have a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. Thus, $\rho_2(K) = \dim_{\mathbb{F}_2}(\mathrm{Gal}(\mathbb{H}(K)/K)[2]) \geq \dim_{\mathbb{F}_2}((\mathbb{Z}/2\mathbb{Z})^n) = n$ (it can be shown that, in fact, $\rho_2(K) = n$). For any $n \geq 6 > 2 + 2\sqrt{3}$, by Corollary 4.8, K has an infinite class field tower.

For an odd prime p, take any $n+1$ distinct prime numbers $q_1, \dots, q_{n+1}$ congruent to 1 modulo p. Let $L_i = \mathbb{Q}(\zeta_{q_i})$ be the q_i-th cyclotomic field and let K_i be the unique subfield of L_i that has degree p over $\mathbb{Q}$. Let $L = L_1 \cdots L_{n+1}$ and $M = K_1 \cdots K_{n+1}$. 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. 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 $\{K_1, \dots, K_{n+1}\}$. One could see that the fields KK_i are unramified over K, and hence their compositum M is also unramified over K. In addition M/K is abelian with Galois group $\mathrm{Gal}(M/K) \cong (\mathbb{Z}/p\mathbb{Z})^n$. 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 an infinite p-class field tower and thus cannot be embedded in a greater number field with class number 1.

Acknowledgements

The author wants to thank his supervisors, Henri Darmon and Víctor Rotger, for their guidance during the development of his bachelor's thesis, on which this article is based.

References

[1] K. Conrad, History of class field theory, Expository paper, Available at `https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf`.

[2] M. Ershov, Golod–Shafarevich groups: a survey, *Internat. J. Algebra Comput.* **22(5)** (2012), 1230001, 68 pp.

[3] E.S. Golod, I.R. Shafarevich, On the class field tower (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **28(2)** (1964), 261–272.

[4] G.J. Janusz, *Algebraic Number Fields*, Second edition, Grad. Stud. Math. **7**, American Mathematical Society, Providence, RI, 1996.

[5] H. Koch, *Galois Theory of p-Extensions*, With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer, Springer Monogr. Math., Springer-Verlag, Berlin, 2002.

[6] F. Lemmermeyer, *Class Field Towers*, 2010.

[7] D.A. Marcus, *Number Fields*, Second edition, With a foreword by Barry Mazur, Universitext, Springer, Cham, 2018.

[8] P. Roquette, On class field towers, in: *Algebraic Number Theory* (Proc. Instructional Conf., Brighton, 1965), Academic Press, London, 1967, pp. 231–249.

[9] I.R. Shafarevich, Extensions with prescribed ramification points (Russian), *Inst. Hautes Études Sci. Publ. Math.* **18** (1963), 71–95.

[10] È.B. Vinberg, On the theorem concerning the infinite-dimensionality of an associative algebra (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **29** (1965), 209–214.