

PROFINITE GROUPS AND GALOIS COHOMOLOGY
STUDENT ALGEBRA SEMINAR
UNIVERSITY OF WASHINGTON
FEBRUARY 7, 2005

DAVID ROSOFF

0. INTRODUCTION

In this talk we will introduce profinite groups, their relation to Galois theory, their cohomology as topological groups, and give some applications. There are two ways to characterize profinite groups. One is as the inverse limit of a system of finite groups: given a directed set I , let G_i be a finite group for every $i \in I$. Then the inverse limit $G = \varprojlim G_i$ is a profinite group (by definition, a profinite group is one obtained in precisely this way). We regard each of the finite groups G_i as a discrete topological group, and then G is topologized as a subspace of $\prod_{i \in I} G_i$. The topology on G is always compact, Hausdorff, and totally disconnected; conversely, every such topological group is in fact profinite.

Let G be any group, and consider the normal subgroups N of finite index in G . The factor groups G/N comprise an inverse system in a canonical way; the inverse limit \widehat{G} is a profinite group called the profinite completion of G . For example, if $G = \mathbb{Z}$, the integers, then every subgroup of G is normal and of finite index; the quotients are the various groups $\mathbb{Z}/n\mathbb{Z}$. We have natural homomorphisms $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ whenever $m \mid n$, and the inverse limit $\widehat{\mathbb{Z}}$ is isomorphic to the direct product of \mathbb{Z}_p , the p -adic integers, over all p . This profinite group does arise as a Galois group, as we'll see below. Here are some examples.

- (1) Let $I = \mathbb{N}$ with the usual order and $G_i = \mathbb{Z}$ for all i , with $g_{j,k}$ multiplication by the prime p . Then $\varprojlim G_i = 0$.
- (2) Now let $I = \mathbb{N}$ ordered by division and $G_i = \mathbb{Z}/p^i\mathbb{Z}$ for all i , with $g_{j,k}$ the natural projection. Then $\varprojlim G_i = \mathbb{Z}_p$.
- (3) Let R be a ring and M an ideal of R . Then if $I = \mathbb{N}$ and $S_i = R/M^i$, again with $g_{j,k}$ the natural projection, $\varprojlim S_i$ is the M -adic completion of R .

Profinite groups arise naturally in Galois Theory.

Theorem (Krull). *Let K/F be a Galois extension of fields (i.e., it is normal and separable). Let $\text{Gal}(K/F)$ be the inverse limit of the groups $\text{Gal}(L/F)$, where L runs through all subfields of K Galois over F . Then there is an inclusion reversing correspondence between closed subgroups of $\text{Gal}(K/F)$ and intermediate fields L ; moreover, a subgroup H is normal precisely when the corresponding field L is Galois over F , and in this case $\text{Gal}(L/F) \cong G/H$.*

For an example that shows why we must restrict to closed subgroups, see the first section of Neukirch, *Class Field Theory*. But why do we care about infinite Galois extensions? The real reason is that every field comes with a canonical Galois extension that is usually of infinite degree. This is its separable closure, which coincides with the algebraic closure in characteristic 0. For a field k , we'll denote its separable closure by k^s and its algebraic closure by k^a . Here is an example. We can easily find the Galois group $\text{Gal}(\mathbb{F}_p^a/\mathbb{F}_p)$. The finite extensions of \mathbb{F}_p are, of course, the finite fields of characteristic p . If we arrange these in a poset, ordered by inclusion, we see that this poset is isomorphic to the natural numbers, ordered by divisibility, hence also isomorphic to the poset formed by the quotients of \mathbb{Z} . Thus the Galois group is isomorphic to $\widehat{\mathbb{Z}}$.

We'll need a few results from algebraic number theory to discuss the applications. Recall that a *number field* is a finite extension of the rational numbers \mathbb{Q} . Any such number field comes with a natural subring, analogous to the integers. Namely, the *ring of integers* in a number field K is the integral closure of \mathbb{Z} in K . The most important property these rings enjoy is that they are Dedekind domains. In the interest of brevity I will give you a crash course in the importance of these rings to number theory. If R is a Dedekind domain (Noetherian, integrally closed, Krull dimension 1) then it has an ideal class group. We say that ideals I and J of R are equivalent if there are elements $\alpha, \beta \in R$ such that $(\alpha)I = (\beta)J$. This is an equivalence relation and the equivalence classes form a group $C(R)$ or C_k under ideal multiplication, with the class of the principal ideals the trivial group element. Another way to regard this relation is that I and J are equivalent if and only if they are isomorphic as R -modules. Thus R is a PID just in case the ideal class group has order 1. It is one of the major theorems of algebraic number theory that if R is

the ring of integers of a number field, the ideal class group is always of finite order (the class number is finite). It is perhaps worth mentioning that for R a Dedekind domain, every ideal is a finitely generated projective R -module, and in fact we can say more:

$$K_0(R) \cong C(R) \times \mathbb{Z}.$$

Let K/k be an extension of number fields and write S/R for their rings of integers. Every ideal of R determines an ideal of S in an obvious way. Can we give necessary or sufficient conditions for this ideal to be principal, perhaps if we choose K in a clever way? This is a classic algebra homework problem (use the finiteness of the class number). We might also ask, given a number field k , does there exist a finite extension K such that *every* ideal of R becomes principal in S ? This is one of the motivating questions of class field theory. It turns out the answer is always yes, and the extension K is concisely characterized.

Definition. The Hilbert class field of a number field k is the unique maximal, unramified, abelian extension of k , where K/k is abelian if $\text{Gal}(K/k)$ is abelian.

The Hilbert class field always exists, and is always of finite degree over k . It is also well-known that the Galois group $\text{Gal}(K/k)$ is canonically isomorphic to the ideal class group of k , a fact which we will use later. So, every number field k admits a finite extension K such that every ideal of k principalizes in K . Of course the ring of integers of K need not be a PID either; there are in general ideals of S that do not come from ideals of R . However, R is a PID ($h_k = 1$) iff k is its own Hilbert class field. This leads to the famous class field tower question, namely: can every number field be embedded in a field whose ring of integers is a PID (equivalently, in a field of class number 1)? The question is equivalent to asking whether the process of forming iterated Hilbert class fields always terminates (exercise). Golod and Šafarevič proved the answer is no. A counterexample is the field $k = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17})$. We will develop the necessary machinery to sketch the proof.

1. PROFINITE GROUPS AND THEIR COHOMOLOGY

Some generalities on topological groups. Note first that if H is an open subgroup of G , then H is also closed, for its complement is the union of the other cosets of H . A partial converse is that if H is closed and of finite index, then H is open. Now specialize to the case that G is compact. Then certainly every quotient of G by a closed subgroup is compact. But if H is an open subgroup of the compact group G things are even better, for H is then necessarily of finite index in G : the cosets are an open cover of G by disjoint subsets, so there must be finitely many. This will help immensely when we try to make sense of the notion of order and index for profinite groups, even allowing us to formulate p -Sylow subgroups.

First, we show that inverse limits always exist in the category of groups. If G_i is an inverse system, we can certainly form the product $\prod_i G_i$. Let G be the subset of this product defined by

$$G = \{(x_i) : g_{j,k}(x_k) = x_j \text{ whenever } j \leq k\}.$$

It is easy to check that G satisfies the universal property, hence is the inverse limit of the G_i . We include this because the profinite topology of G coincides with the subspace topology of $G \subset \prod_i G_i$. It turns out that the collection of open normal subgroups of G forms a neighborhood basis at the identity, and since G is a topological group this determines the whole topology. I should also mention that there is an anti-equivalence of categories

$$\text{ProAb} \longleftrightarrow \text{TorAb}$$

where ProAb is the category of abelian profinite groups and TorAb is the category of torsion abelian groups. The equivalences are given by Pontrjagin duality; that is, if G is an abelian group then $\widehat{G} = \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$ is torsion if and only if G is profinite.

We would like to have a workable way to talk about the order of a profinite group, even though such groups are infinite in general. So define a *supernatural number* to be a formal product

$$\prod_p p^{n_p}$$

where the product is taken over all primes and $0 \leq n_p \leq \infty$ for each p (note that $n_p = \infty$ is permitted!). We define the gcd and lcm of supernatural numbers in the obvious fashion. A p -power is a supernatural number with $n_q = 0$ for all $q \neq p$, and a supernatural number is prime to p if $n_p = 0$.

Definition. Let G be a profinite group and H a closed subgroup. We define the index of H in G , denoted $[G:H]$, to be the supernatural number

$$[G : H] = \text{lcm}[G/U : H/H \cap U]$$

where U ranges over all open normal subgroups of G . (Recall that G is compact, so $|G/U|$ is a natural number.) The order of G itself is thus defined; it is

$$|G| = [G : 1] = \text{lcm}|G/U|.$$

Examples: the order of \mathbb{Z}_p is p^∞ , since the finite quotients are exactly the $\mathbb{Z}/p^n\mathbb{Z}$. The order of $\widehat{\mathbb{Z}}$ can then be computed:

$$|\widehat{\mathbb{Z}}| = \left| \prod_p \mathbb{Z}_p \right| = \prod_p |\mathbb{Z}_p| = \prod_p p^\infty.$$

Supernatural indeed.

In the category of finite groups, a p -group is a group whose order is a power of p , so we'll define a pro- p -group to be a profinite group whose order is a p -power, in the sense described above. (This agrees with the other possible definition, namely an inverse limit of finite p -groups.) All this is leading to

Definition. Let G be a profinite group and S a closed subgroup. We say that S is a p -Sylow subgroup of G if S is a pro- p -group and $[G : S]$ is prime to p .

Theorem. Let G be a profinite group. Then for any fixed prime number p , we have:

- (1) G possesses p -Sylow subgroups.
- (2) If T is any p -subgroup of G then T is contained in some p -Sylow subgroup of G .
- (3) Any two p -Sylow subgroups of G are conjugate.

Examples: \mathbb{Z}_p is a pro- p -group, so it is its own unique p -Sylow subgroup. Of course, it has countably many p -subgroups that are of index a power of p . What about $\widehat{\mathbb{Z}}$? It has a p -Sylow subgroup for each p , of course, each one isomorphic to some \mathbb{Z}_p .

Thus we have picked the right definition, because we got to prove the right theorem. We omit said proof (first due to J. Tate). Really, the reason I have gone through all this is to define what we will call *free profinite groups*. This is done in the following way. Let X be a set. Then we can form the free group $\langle X \rangle$ generated by the elements of X . The profinite completion of this group is the free profinite group on X . That is,

$$F(X) = \varprojlim_U \langle X \rangle / U,$$

where the limit is taken over all normal subgroups U with finite index in $\langle X \rangle$. If we restrict the limit to those normal, finite-index subgroups for which $[\langle X \rangle : U]$ is a p -power, we obtain the free pro- p -group on X . These will be denoted $F(X)$ and $F_p(X)$, respectively. For example, let X be a set with one element. Then the free group on X is of course just \mathbb{Z} , and so $F(X) = \widehat{\mathbb{Z}}$ and $F_p(X) = \mathbb{Z}_p$, the unique p -Sylow subgroup of $\widehat{\mathbb{Z}}$.

The point of this is that to give a counterexample to the class tower problem, we need to be able to discuss the rank of a profinite group, so we need some workable notion of free objects in these categories.

2. COHOMOLOGY OF PROFINITE GROUPS

Let G be a profinite group, and let A be a discrete G -module, by which we mean a discrete abelian group on which G acts continuously by automorphisms. That is, there is a homomorphism $G \rightarrow \text{Aut}(A)$ such that the natural map $G \times A \rightarrow A$ is continuous. Now let \mathcal{C} be the category of G -modules and G -maps (continuous G -equivariant homomorphisms). This is an abelian category. Define for each nonnegative integer n and each G -module A

$$C^n(G, A) = \{f : G^n \rightarrow A \text{ and } f \text{ is continuous}\}.$$

Note we do not require that f be a homomorphism. The $C^n(G, -)$ are all exact functors from \mathcal{C} to Ab . They also, for fixed A , form a cochain complex, with coboundary map defined by:

$$(d^n f)(x_1, \dots, x_{n+1}) = x_1 f(x_2, \dots, x_{n+1}) + \sum_{i=1}^n (-1)^i f(x_1, \dots, x_i x_{i+1}, \dots, x_{n+1}) + (-1)^{n+1} f(x_1, \dots, x_n).$$

Define also $Z^n(G, A)$, $B^n(G, A)$, and $H^n(G, A)$ in the usual way. We get all the usual bag of tricks for cohomology in more or less the usual way: cup product, inflation and restriction, transfer, and Bockstein exact sequences, for example.

Let S be a subgroup of G and A a G -module. Then A is an S -module in a natural way, and the inclusion map $S \rightarrow G$ is compatible with the identity $A \rightarrow A$, meaning that we obtain an induced map on cohomology

$$\text{res} : H^*(G, A) \rightarrow H^*(S, A).$$

This map is called restriction. Dually, if S is a closed normal subgroup of G , the natural projection $G \rightarrow G/S$ is compatible with the inclusion $A^S \rightarrow A$, meaning there is a natural map

$$\text{inf}: H^*(G/S, A^S) \rightarrow H^*(G, A).$$

Together these give a Hochschild-Serre spectral sequence:

$$H^p(G/S, H^q(S, A)) \Rightarrow H^*(G, A)$$

and we get an exact sequence of terms of low degree (transgression) called the inflation-restriction exact sequence:

$$0 \rightarrow H^1(G/S, A^S) \rightarrow H^1(G, A) \rightarrow H^1(S, A)^{G/S} \rightarrow H^2(G/S, A^S) \rightarrow H^2(G, A).$$

The first nonzero map and the last map are inflation, the second map is restriction, and the third map is the so-called transgression $d_2^{0,1}$, the edge map in the spectral sequence. Feel free to keep all this inside a black box.

Suppose f is an element of $Z^1(G, A)$. Then we have $df = 0$, or

$$xf(y) - f(xy) + f(x) = 0.$$

Thus for a 1-cocycle f , we have $f(xy) = xf(y) + f(x)$. Such a function is called a crossed homomorphism, because if A has only the trivial G -action, then it is a homomorphism. An element of $B^1(G, A)$ is called a principal crossed homomorphism; these are maps $G \rightarrow A$ having $f(x) = xa - a$ for some $a \in A$. We verify that $B^1 \leq Z^1$.

$$f(xy) = xya - a = x(ya) - xa + xa - a = x(ya - a) + (xa - a) = xf(y) + f(x).$$

As an aside, if G acts trivially on A , $H^1(G, A) = \text{Hom}_{\text{cont}}(G, A)$. It is perhaps worth mentioning that the $H^n(G, -)$ comprise a universal δ -functor from \mathcal{C} to Ab in the sense of Grothendieck. Among other things, this gives us that $H^n(G, -)$ is the n th right derived functor of the left exact functor $A \rightarrow A^G$, the fixed module functor. En route to this one proves that the category of discrete G -modules has enough injectives.

We also can relate profinite cohomology to ordinary group cohomology. Since G is profinite, there is an inverse system of finite groups G_i with $G \cong \varprojlim G_i$. Suppose in addition that we can express the G -module A as a direct limit (over the same index set) and that the two systems of maps thus obtained are compatible in the obvious way. Then

$$H^*(G, A) \cong H^*(\varprojlim G_i, \varinjlim A_i) \cong \varinjlim H^*(G_i, A_i).$$

All one needs to do to prove this is show that for all n , $C^n(G, A) \cong \varinjlim C^n(G_i, A_i)$ and in fact that cohomology commutes with direct limit. Note that all of the above assumes we are using continuous cochains only, and that many of these results will fail for discontinuous cochains.

Galois cohomology is a special case of profinite cohomology. Since every field k comes with a separable closure k^s , we have a canonical profinite group associated to k , that is, $G_k = \text{Gal}(k^s/k)$. It's common to write $H^n(k, A)$ for $H^n(G_k, A)$, to emphasize that this is an invariant of k . Similarly we would write $H^n(K/k, A)$ for $H^n(\text{Gal}(K/k), A)$. To prove the Golod-Šafarevič result, we'll be studying the cohomology of a certain p -extension, and so the Galois group in question will be a pro- p -group.

3. THE STRUCTURE OF PRO- p -GROUPS

The next proposition shows that for G a pro- p -group, we know all there is to know about the action of G on finite abelian p -groups.

Proposition. *Let G be a pro- p -group, and suppose A is a finite simple G -module of p -power order. Then A is isomorphic to the trivial G -module $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Consider the orbit relation on A , and write $O(x)$ for the orbit of $x \in A$ under G . Let G_x be the stabilizer of x in G . Then we have

$$|A| = |A^G| + \sum |O(x)|$$

where the sum is over a set of representatives for those equivalence classes with more than one element (compare the class equation). On the other hand the cardinality of $O(x)$ is $[G : G_x]$ (supernatural orbit-stabilizer theorem). Thus

$$|A| = |A^G| + \sum [G : G_x].$$

The indices occurring in the RHS are all p -powers, since G is a pro- p -group; they are all greater than 1, since we sum over only such classes. Since A is a p -group also, $p \mid |A|$. Hence $|A^G| > 1$. Since A is simple, $A = A^G$, so the action is the trivial one. But this means A is a simple abelian p -group, that is to say, $A \cong \mathbb{Z}/p\mathbb{Z}$. \square

Thus for G a pro- p -group, it is natural to study the cohomology groups $H^n(G, \mathbb{Z}/p\mathbb{Z})$. Since G acts trivially on $\mathbb{Z}/p\mathbb{Z}$ we have for $n = 1$

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \cong \text{Hom}_{\text{cont}}(G, \mathbb{Z}/p\mathbb{Z}).$$

We will identify these groups throughout the sequel. We also record one special case, which is proved by using the definition of $F_p(X)$ as the p -completion of $\langle X \rangle$.

Proposition. *Let X be any set. Then*

$$H^1(F_p(X), \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus |X|}.$$

Proof. We prove this in the case that $|X| < \infty$. Suppose that $\xi: F_p(X) \rightarrow \mathbb{Z}/p\mathbb{Z}$. Then $\xi^{-1}(0)$ is an open normal subgroup of $F_p(X)$, call it V . Let i be the inclusion $\langle X \rangle \rightarrow F_p(X)$. Then $U = V \cap i(\langle X \rangle)$ is a normal group of $\langle X \rangle$, and its index is p . Hence there is an induced map $\langle X \rangle/U \rightarrow \mathbb{Z}/p\mathbb{Z}$, thus by composition a map $\langle X \rangle \rightarrow \mathbb{Z}/p\mathbb{Z}$. The universal property of the free group then gives us a function $X \rightarrow \mathbb{Z}/p\mathbb{Z}$. Everything we have done is invertible, so this proves the converse also. \square

The goal of the rest of this section is to show that every pro- p -group is a quotient of some free pro- p -group $F_p(X)$, and to link the cardinality of X with the dimension of $H^1(G)$ as a $\mathbb{Z}/p\mathbb{Z}$ -vector space. We need a bit more Pontrjagin nonsense to get there, noting that since everything is in sight in a p -power, we can regard the duality functor as merely $\text{Hom}_{\text{cont}}(-, \mathbb{Z}/p\mathbb{Z})$. First, we define a pro- p -analogue of the Frattini subgroup of G , namely let $G^* = \bigcap \ker \chi$, where χ ranges over $H^1(G) = H^1(G, \mathbb{Z}/p\mathbb{Z})$. Then of course G^* is a closed normal subgroup of G .

Proposition. *The quotient G/G^* is Pontrjagin dual to $H^1(G)$.*

Proof. The discrete group $H^1(G)$ has a compact dual; in fact, the dual is simply

$$\text{Hom}_{\text{cont}}(\text{Hom}_{\text{cont}}(G, \mathbb{Z}/p\mathbb{Z}), \mathbb{Z}/p\mathbb{Z}).$$

The homomorphism $H^1(G) \rightarrow \mathbb{Z}/p\mathbb{Z}$ given by evaluation is continuous, giving a homomorphism $G \rightarrow H^1(G)^{\text{D}}$. The kernel of the latter is clearly G^* , so all we need to do is show it is onto. Suppose $\lambda \in H^1(G)^{\text{D}}$. Then λ represents a homomorphism $G \rightarrow \mathbb{Z}/p\mathbb{Z}$. Thus there is an induced homomorphism $G^{\text{ab}} \rightarrow \mathbb{Z}/p\mathbb{Z}$, and a corresponding element $\lambda \in H^1(G^{\text{ab}})^{\text{D}}$. By Pontrjagin duality, $\lambda \in G^{\text{ab}}$, so there is an element in G mapping to λ under the canonical abelianization map. \square

In particular, if $G = F_p(X)$, then

$$G/G^* \cong H^1(F_p(X))^{\text{D}} \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus |X|^{\text{D}}} \cong \prod_X \mathbb{Z}/p\mathbb{Z}.$$

Theorem. *Let G be a pro- p -group, and let X be a set. Suppose we have a vector space homomorphism $\theta: H^1(G) \rightarrow \bigoplus_X \mathbb{Z}/p\mathbb{Z}$. Then there is a group homomorphism $\pi: F_p(X) \rightarrow G$ such that θ is induced by π (on H^1). Moreover, if θ is injective then π is surjective.*

Proof. The dual map θ^{D} takes $\prod_X \mathbb{Z}/p\mathbb{Z}$ into $H^1(G)^{\text{D}} \cong G/G^*$. But $\prod_X \mathbb{Z}/p\mathbb{Z}$ is $F_p(X)/F_p(X)^*$, by the above example. General nonsense about free groups and p -groups and Sylow theory lets us lift our map $F_p(X) \rightarrow G/G^*$ to G . Roughly, what happens is the following. We have an extension

$$0 \rightarrow G^* \rightarrow G \rightarrow G/G^* \rightarrow 0$$

and a map $F_p(X) \rightarrow G/G^*$. We need to show that $F_p(X)$ satisfies a suitable lifting property for profinite groups. It turns out that our earlier argument shows that $F_p(X)$ has cohomological dimension ≤ 1 , which is equivalent to just such a property (compare projective dimension). \square

This shows in particular that every pro- p -group is the quotient of a free one. Of course what we might like to say is that G is then generated by $|X|$ elements, in the case where X is a finite set at least. So for G a profinite group and $\sigma_1, \dots, \sigma_n \in G$, say that the σ_j generate G topologically if and only if the closure of the normal subgroup generated by the σ_j is all of G . (So we look at the group generated by the conjugates of the σ_j , and take its closure.) Then the following proposition is immediate.

Proposition. *Let G be a pro- p -group and let $\sigma_1, \dots, \sigma_n$ be a subset of G . The following are equivalent:*

- (1) *The σ_j generate G topologically.*
- (2) *The homomorphism $F_p(\{n\}) \rightarrow G$ induced by the σ_j is surjective.*
- (3) *Every $\chi \in H^1(G)$ that vanishes on the σ_j is identically 0.*

Proof. Certainly 1 and 3 are equivalent. The remaining equivalences follow from the theorem above. \square

A corollary: The minimal number of generators of G is the dimension of $H^1(G)$. As one might expect, we are now going to relate the dimension of H^2 to the number of relations among this minimal generating set of a pro- p -group. Let G be a finitely generated pro- p -group, so that we have an exact sequence of continuous maps

$$0 \rightarrow N \rightarrow F_p(X) \rightarrow G \rightarrow 0$$

where X is a finite set. We can prove by similar arguments to those above that N is topologically generated by n elements as a normal subgroup of $F_p(X)$ if and only if $H^1(N, \mathbb{Z}/p\mathbb{Z})^G$ has dimension at most n . Therefore we will call the dimension of $H^1(N)^G$ the F_p -rank of n . To simplify notation from now on let $h_i(G) = \dim H^i(G, \mathbb{Z}/p\mathbb{Z})$ whenever G is a pro- p -group. Recall that we have a cohomology exact sequence, induced by the above (the so-called inflation-restriction sequence):

$$0 \rightarrow H^1(G) \rightarrow H^1(F_p(X)) \rightarrow H^1(N)^G \rightarrow H^2(G) \rightarrow 0.$$

This allows us to deduce the next proposition.

Proposition. *Let G be a finitely generated pro- p -group (so $h_1(G) < \infty$). More precisely suppose there is an exact sequence*

$$0 \rightarrow N \rightarrow F_p(X) \rightarrow G \rightarrow 0$$

where X has cardinality n . Then the F_p -rank of N is finite if and only if $h_2(G)$ is finite. In this case, we have the equality

$$\dim H^1(N)^G = n - h_1(G) + h_2(G).$$

Proof. The alternating sum of the dimensions is zero in the above cohomology exact sequence. □

4. SOLUTION OF THE CLASS TOWER PROBLEM

In this section we apply the foregoing to prove the following theorem.

Theorem. *The class tower problem has a negative solution. That is, there exist algebraic number fields whose class towers are infinite, hence admit no finite extension of class number one. The field $k = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17})$ is an imaginary quadratic example.*

Recall that what we are doing is constructing a sequence k_j of number fields. Each k_j is the Hilbert class field of k_{j-1} , so for each j , k_j/k_{j-1} is a finite unramified abelian extension. This implies that each k_j is unramified over $k_0 = k$ (though not abelian in general) and the union of the k_j is the maximal unramified extension Ω of k . Now let G be the Galois group of Ω over k . Then we know by the Galois correspondence that the maximal p -quotient of G corresponds to the maximal unramified p -extension of k . Denote this intermediate field by $k(p)$ and let $G(p) = \text{Gal}(k(p)/k)$. If $k(p)$ is of infinite degree over k , then so also is Ω . But this implies that the class tower is infinite, so we are reduced to finding such a k . We can do this using the stuff about generators and relations in pro- p -groups above and a bit of high powered number theory.

Recall that we can complete \mathbb{Q} in a variety of ways, either getting \mathbb{R} or \mathbb{Q}_p for some p . In fact Ostrowski's theorem says these are the only completions of \mathbb{Q} up to isomorphism. Now what if we complete a number field? It turns out we will either get \mathbb{R} , \mathbb{C} , or a finite extension of \mathbb{Q}_p for some p , and what's even better, it turns out there is exactly one isomorphism type of ultrametric completion for every prime ideal of the ring of integers of the number field, just like over \mathbb{Q} ! We call the completions "places", and in particular we are interested in the real and complex places. This just means the inequivalent ways of completing k so that the completed field embeds in \mathbb{R} and \mathbb{C} respectively. Let r_1 and $2r_2$ denote the number of such places. This is because the complex ones come in conjugate pairs. We require the following theorem, due to Iwasawa:

Theorem (Iwasawa). *Let K/k be an unramified p -extension with $G = \text{Gal}(K/k)$. If K admits no cyclic, unramified extension of degree p , then*

$$h_2(G) - h_1(G) \leq r_1 + r_2.$$

where again $h_i(G) = \dim H^i(G, \mathbb{Z}/p\mathbb{Z})$.

And finally, the key result of Golod-Šafarevič. There is a very beautiful proof using an ingenious idea of Tate. He splices together the profinite cohomology of a finite p -group and its ordinary group homology, obtaining a doubly-infinite sequence of groups. Denote these groups \tilde{H}^* . Then there are Tate cohomology cup-product isomorphisms, valid for all integer r and all finite groups G ,

$$\tilde{H}^{-r}(G, \mathbb{Z}) \cong \tilde{H}^r(G, \mathbb{Z})^D.$$

Together with a result of Rim that is a noncommutative analog of Nakayama's Lemma, Golod-Šafarevič proved the following amazing theorem.

Theorem (Golod-Šafarevič). *Let G be a finite p -group. Then*

$$h_2(G) > \frac{1}{4}h_1(G)^2, \text{ therefore } \lim_{h_1(G) \rightarrow \infty} (h_2(G) - h_1(G)) = \infty.$$

Using all this we can answer the class tower conjecture in the negative, even using just a degree 2 extension of \mathbb{Q} .

Solution of class tower problem. It follows from the remarks above that we may assume $\Omega = k(p)$ and $G = G(p)$. Suppose the theorem is false. Then $k(p)$ is a finite extension of k , so G is a finite p -group. By assumption, $k(p)$ admits no unramified p -extension, so applying the result of Iwasawa we obtain

$$h_2(G) - h_1(G) \leq r_1 + r_2 \leq [k : \mathbb{Q}] \leq \infty.$$

Now we specialize to the case $p = 2$. Let p_1, \dots, p_N be distinct odd primes satisfying $-\prod_{j=1}^N p_j \equiv 1 \pmod{4}$. Let k be the quadratic imaginary extension $\mathbb{Q}(\sqrt{-p_1 \cdots p_N})$, $K_j = k(\sqrt{\pm p_j})$, where we choose the plus or the minus sign according as $p_j \equiv 1$ or $-1 \pmod{4}$. Then each K_j is unramified over k , and further the K_j are independent. Let $G = G(2)$ be the Galois group of the maximal unramified 2-extension of k . Then $h_1(G) = h^1(G^{\text{ab}})$, since $\mathbb{Z}/p\mathbb{Z}$ is abelian. By the Galois correspondence, G^{ab} is the Galois group of the maximal abelian unramified 2-extension of k . Class field theory (Artin reciprocity) tells us that G^{ab} is isomorphic to the 2-primary part of the ideal class group of k ! In fact, we know even more: since each K_j is an unramified abelian quadratic extension of k , and since they are all independent, we know $Cl_k(2)$ has at least N generators, or $h_1(G) \geq N$. The field k is totally imaginary, so $r_1 = 0$ and $r_2 = 1$. Therefore, by Iwasawa's theorem again, $h_2(G) - h_1(G) \leq 1$. The theorem of Golod-Šafarevič says that $h_2(G) > h_1(G)^2/4$, so this is a contradiction if $N \geq 6$. \square