Class Field Tower Problem

MURILO CORATO ZANARELLA

January 16, 2018

1. Introduction

Definition 1.1. For a number field K, its *Class Field Tower* is

$$K = K^{(0)} \subseteq K^{(1)} \subseteq \cdots \subseteq K^{(n)} \subseteq \cdots,$$

where $K^{(i+1)}$ is the Hilbert Class field of $K^{(i)}$ for all $i \geq 0$. We denote $K^{(\infty)} = \bigcup_{i\geq 0} K^{(i)}$.

It is natural to ask whether this tower eventually stabilizes. This was first asked in 1925 by Furtwängler:

Question 1.2 (Class Field Tower Problem)**.** Does the Class Field Tower stabilizes for all number fields K?

In fact, this is an interesting question since it is equivalent to the following other question:

Question 1.3 (Embeddability Problem)**.** Does any number field K admit an extension L/K of number fields such that the class number of L is 1?

Proposition 1.4. The Class Field Tower problem and the Embeddability Problem are equivalent.

Proof. $(\Rightarrow):$ If the Class Field Tower of K stabilizes at $K^{(n)}$, then this means $|\mathrm{Cl}_{K^{(n)}}| = \left[K^{(n+1)} : K^{(n)}\right] = 1$, hence we can take $L = K^{(n)}$.

$(\Leftarrow):$ If we have L/K with $|\mathrm{Cl}_L| = 1$, then L is its own Hilbert Class Field. Inductively, we get $K^{(n)} \subseteq L^{(n)} = L$. Since $[L : K]$ is finite, we conclude that the Class Field Tower must stabilize. □

In 1964, these problems were solved in the negative by Evgeny Golod and Igor Shafarevich. Their proof, with some refinements, yields the following:

Theorem 1.5 (Golod-Shafarevich)**.** *If K is an imaginary quadratic field with at least 5 distinct odd primes dividing its discriminant, then K has an infinite Class Field Tower.*

This gives counter-examples such as $\mathbb{Q}(\sqrt{-3\cdot 5\cdot 7\cdot 11\cdot 13})$.
After this, several other counter-examples were constructed, such as by means of the following theorem.

Theorem 1.6 (Brumer)**.** *Let $K/\mathbb{Q}$ be Galois, of degree n. Let k be the number of infinite places of K, and p be a prime $p \mid n$. Let t_p be the number of primes ramified in K with the ramification index a multiple of p. Then K has an infinite Class Field Tower if*

$$t_p > \frac{k-1}{p-1} + \nu_p(n)\delta_p + 2 + 2\sqrt{k+\delta_p},$$

where $\delta_p = 1$ if the $p-$roots of unity are in K and 0 otherwise.

For instance, any quadratic real field with at least $7 > 4 + 2\sqrt{2}$ ramified primes has infinite Class Field Tower.
However, all the results currently known use the Golod-Shafarevich inequality 2.4 as one use its tools.

2. Outline of the Proof

Definition 2.1. We call an extension of number fields L/K a $p-$extension if it is Galois and $[L:K]$ is a power of p.

Lemma 2.2. *If K is a number field with finite Class Field Tower, there is a maximal unramified $p-$extension of K. We denote it by K^p. Moreover, K^p has no nontrivial unramified $p-$extension.*

Proof. Note $K^{(\infty)}$ is the maximal solvable unramified extension of K [1]. Since a $p-$group is solvable, we must have $L \subseteq K^{(\infty)}$ for any $p-$extension L/K. So if $G = \mathrm{Gal}\left(K^{(\infty)}/K\right)$, we need to prove there is a minimal normal subgroup $N \trianglelefteq G$ such that $[G\colon N]$ is a power of p. This is true for any finite group G, and follows once we prove that if N_1, N_2 are two such subgroups, then so is $N_1 \cap N_2$. If N_1, N_2 are two such subgroups, then $N_1 N_2$ is a subgroup of G of order $\frac{|N_1|\cdot|N_2|}{|N_1\cap N_2|}$, [2] we have that $N_1 \cap N_2$ is still normal, and

$$[G:N_1\cap N_2] = \frac{|G|\cdot|N_1N_2|}{|N_1|\cdot|N_2|} = \frac{[G:N_1]\cdot[G:N_2]}{[G:N_1N_2]} \mid [G:N_1]\cdot[G:N_2]$$

which is a power of p. Hence $N_1 \cap N_2$ also defines a $p-$extension. So K^p is well defined.

Suppose L/K^p is an unramified $p-$extension. Let M/K be the Galois closure of L/K. Then M/K is also unramified. If $L_1, \ldots, L_k$ are the conjugates of L, then we have $[M:K] \mid \prod_{i=1}^{k}[L_i:K] = [L:K]^k$, which is a power of p. Hence M/K is a $p-$extension, which implies $L \subseteq M \subseteq K^p$. Hence L/K^p is a trivial extension. □

So if we construct number fields K such that K^p/K is infinite, then its Class Field Tower is infinite. This is done by the two theorems that follow.

Notation. If G is a $p-$group, we denote $d(G) = |\mathrm{H}_1(G, \mathbb{F}_p)|$ and $r(G) = |\mathrm{H}_2(G, \mathbb{F}_p)|$ where the action of G in $\mathbb{F}_p$ is the trivial one.

Theorem 2.3 (Iwasawa)**.** *If we have an unramified $p-$extension L/K of number fields, such that L has no unramified Galois extension of degree p, then we have, for $G = \mathrm{Gal}(L/K)$,*

$$r(G) - d(G) \leq r + s.$$

Theorem 2.4 (Golod-Shafarevich)**.** *If G is a nontrivial finite $p-$group, then*

$$\frac{d(G)^2}{4} < r(G).$$

Now suppose for instance that K is a quadratic imaginary field, so that $r = 0$ and $s = 1$. Assume that K^2/K is finite. We let $G = \mathrm{Gal}\left(K^2/K\right)$. If N distinct odd primes divide D_K, then we can see that $d(G) \geq N$. Indeed, for any $p_i \mid D_K$ odd, we consider $L_i = \mathbb{Q}(\sqrt{p_i^\star})$. Then $L_i \subseteq K^2$, so it defines a map $\varphi_i\colon G \twoheadrightarrow G/\mathrm{Gal}\left(K^2/L_i\right) \xrightarrow{\sim} \mathbb{F}_2$ which we can see as an element of $\mathrm{H}^1(G, \mathbb{F}_2)$. They are linearly independent, since if $g_i \in G \setminus \mathrm{Gal}\left(K^2/L_i\right)$, then $\varphi_j(g_i) = \delta^i_j$. Since $\mathrm{H}^1(G,\mathbb{F}_2) \simeq \mathrm{H}_1(G,\mathbb{F}_2)$, [3] we conclude that $d(G) \geq N$.

Then $d(G)^2 < 4r(G) \leq 4(1 + d(G))$, so $d(G)^2 - 4d(G) - 4 < 0$, which is not true for $d(G) \geq 5$. Hence if $N \geq 5$ we have a contradiction, which forces the Class Field Tower of K to be infinite.

---

[1] To see that $K^{(\infty)}/K$ is Galois, we use that: If L/K is a Galois extension of number fields, and H is the Hilbert Class Field of L, then H/K is Galois. Indeed, if σ fixes K, then $\sigma L = L$ and so $\sigma H/L$ is an unramified abelian extension of L, hence $\sigma H \subseteq H \implies \sigma H = H$.

[2] That $|N_1N_2| = \frac{|N_1|\cdot|N_2|}{|N_1\cap N_2|}$ is a simple counting. If $n_i \in N_i$, then $n_2n_1 = n_1^{-1}(n_1n_2)n_1 \in n_1^{-1}N_1N_2n_1 \subseteq (n_1^{-1}N_1n_1)(n_1^{-1}N_2n_1)$, hence $N_2N_1 \subseteq N_1N_2$. Analogously, we have the other containment. Hence $N_1N_2 = N_2N_1$. Then it follows easily that N_1N_2 is a group.

[3] We have $\mathrm{H}_1(G,\mathbb{F}_2) \xrightarrow{\sim} G^{\mathrm{ab}} \otimes_{\mathbb{Z}} \mathbb{F}_2$ and $\mathrm{H}^1(G,\mathbb{F}_2) \xrightarrow{\sim} \mathrm{Hom}(G^{\mathrm{ab}}, \mathbb{F}_2)$, both counting the number of quotients of G^{ab} of size 2.

3. Proof of Iwasawa's Theorem

Notation. For any abelian group H, we denote $H_{(p)} = H/pH$.

Lemma 3.1.

$$\dim_{\mathbb{F}_p} \mathrm{H}_2(G,\mathbb{Z})_{(p)} = r(G) - d(G).$$

Proof. Consider the exact sequence $0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \to \mathbb{F}_p \to 0$ and its corresponding long exact sequence in homology

$$\mathrm{H}_2(G,\mathbb{Z})_{(2)} \to \mathrm{H}_2(G,\mathbb{F}_p) \to \mathrm{H}_1(G,\mathbb{Z}) \to \mathrm{H}_1(G,\mathbb{Z}) \to \mathrm{H}_1(G,\mathbb{F}_p) \to 0$$

where the 0 at the end is because the last three terms split. Since $\mathrm{H}_1(G,\mathbb{Z}) \simeq G^{\mathrm{ab}}$ is finite, we may compute dimensions and we obtain

$$\dim_{\mathbb{F}_p} \mathrm{H}_2(G,\mathbb{Z})_{(p)} = \dim_{\mathbb{F}_p} \mathrm{H}_2(G,\mathbb{F}_p) - \dim_{\mathbb{F}_p} \mathrm{H}_1(G,\mathbb{F}_p) = r(G) - d(G).$$

□

Notation. Denote $\mathbb{U}_K = \{(a_\mathfrak{p})_\mathfrak{p} \in \mathbb{I}_K : a_\mathfrak{p} \text{ is a unit for all } \mathfrak{p} \text{ finite}\} = \mathrm{Ker}(\mathbb{I}_K \to \mathrm{I}_K)$ and $U_K = \mathbb{U}_K \cap K^\times$, so that U_K is the group of units of K.

Then we have two exact sequences:

$$0 \to \mathbb{U}_L/U_L \to \mathbb{C}_L \to \mathrm{Cl}_L \to 0$$
$$0 \to U_L \to \mathbb{U}_L \to \mathbb{U}_L/U_L \to 0$$

By Class Field Theory, the fact that L has no unramified Galois extension of degree p is equivalent to the fact that $p \nmid |\mathrm{Cl}_L|$. As G is a $p-$group, we conclude that

$$\widehat{\mathrm{H}}^n(G,\mathrm{Cl}_L) = 0 \text{ for all } n \in \mathbb{Z}.^4$$

Since L/K is unramified, we have that the $\widehat{\mathrm{H}}^n(G,\mathbb{U}_L)$ all vanish[5]. Considering the long exact sequence induced by the two exact sequences above, we have for all r,

$$\widehat{\mathrm{H}}^r(G,\mathbb{U}_L/U_L) \xrightarrow{\sim} \widehat{\mathrm{H}}^r(G,\mathbb{C}_L)$$
$$\widehat{\mathrm{H}}^r(G,\mathbb{U}_L/U_L) \xrightarrow{\sim} \widehat{\mathrm{H}}^{r+1}(G,U_L)$$

and thus $\widehat{\mathrm{H}}^r(G,\mathbb{C}_L) \xrightarrow{\sim} \widehat{\mathrm{H}}^{r+1}(G,U_L)$ for all $r \in \mathbb{Z}$. The Main Theorem of Class Field Theory reads $\widehat{\mathrm{H}}^{r-2}(G,\mathbb{Z}) \xrightarrow{\sim} \widehat{\mathrm{H}}^r(G,\mathbb{C}_L)$ for all $r \in \mathbb{Z}$.[6] Hence we deduce

$$\widehat{\mathrm{H}}^{r-2}(G,\mathbb{Z}) \xrightarrow{\sim} \widehat{\mathrm{H}}^{r+1}(G,U_L) \text{ for all } r \in \mathbb{Z}.$$

In particular, for $r = -1$ we obtain

$$\mathrm{H}_2(G,\mathbb{Z}) \xrightarrow{\sim} \widehat{\mathrm{H}}^0(G,U_L) = U_K/\mathrm{Nm}_{L/K}(U_L),$$

and hence

$$\mathrm{H}_2(G,\mathbb{Z})_{(p)} \xrightarrow{\sim} \left(U_K/\mathrm{Nm}_{L/K}(U_L)\right)_{(p)}.$$

Taking dimensions, we get, by the lemma above,

$$r(G) - d(G) = \dim_{\mathbb{F}_p}(\left(U_K/\mathrm{Nm}_{L/K}(U_L)\right)_{(p)}) \le \dim_{\mathbb{F}_p}((U_K)_{(p)}).$$

Since by the Unit Theorem we have $U_K \simeq \mu_K \cdot \mathbb{Z}^{r+s-1}$, so we get $r(G) - d(G) \le r + s - 1 + \delta_K \le r + s$.

[4] This holds since we saw in class that $\widehat{\mathrm{H}}^n(G,\mathrm{Cl}_L)$ is $|G|-$torsion. Moreover, since Cl_L is $|\mathrm{Cl}_L|-$torsion, so is $\widehat{\mathrm{H}}^n(G,\mathrm{Cl}_L)$. So it is $\gcd(|G|,|\mathrm{Cl}_L|) = 1-$torsion. Hence $\widehat{\mathrm{H}}^n(G,\mathrm{Cl}_L) = 0$.

[5] Since $\widehat{\mathrm{H}}^n(G,\mathbb{U}_L) = \varinjlim \prod_{\mathfrak{p}\in S} \widehat{\mathrm{H}}^n\left(G_\mathfrak{P},\mathcal{O}_{L_\mathfrak{P}}^\times\right)$, it suffices to prove $\widehat{\mathrm{H}}^n\left(G_\mathfrak{P},\mathcal{O}_{L_\mathfrak{P}}^\times\right) = 0$. Since $G_\mathfrak{P}$ is cyclic, it suffices to prove for $n = 0$ and $n = 1$, which was done in class.

[6] We did not prove this in class, but it follows by Tate's theorem once one proves $\widehat{\mathrm{H}}^2(G,\mathbb{C}_L)$ is cyclic of order $[L:K]$. For example, for G cyclic, we have $\widehat{\mathrm{H}}^2(G,\mathbb{C}_L) \xrightarrow{\sim} \widehat{\mathrm{H}}^0(G,\mathbb{C}_L) \xrightarrow{\sim} G^{\mathrm{ab}} = G$ which is cyclic of the right order.

4. Proof of Golod-Shafarevich Inequality

For this entire section, G will denote a finite $p-$group. Remember that for a $G-$module A, we denote $A_G = \mathrm{H}_0(G, A) = A/I_G A$ where I_G is the augmentation ideal.

Lemma 4.1. *If A is a finite $G-$module with $pA = 0$, then $A_G = 0 \iff A^G = 0 \iff A = 0$.*

Proof. Let $A' = \mathrm{Hom}(A, \mathbb{F}_p)$. Then $(A')_G = \mathrm{Hom}(A^G, \mathbb{F}_p)$ and $(A')^G = \mathrm{Hom}(A_G, \mathbb{F}_p)$. So we only need to prove $A^G = 0 \implies A = 0$. Consider the action of G in A. Then $A^G = 0$ means that it has exactly one orbit of size 1. Since all other orbits are of size powers of p, we have $|A| \equiv 1 \mod p$. Since A is a $\mathbb{F}_p-$vector space, this implies $A = 0$. □

Lemma 4.2. *Let A be a finite $G-$module with $pA = 0$. Let $a_1, \dots a_r$ be a basis of A_G as a $\mathbb{F}_p-$vector space. Then they also generate A as a $G-$module.*

Proof. Let B be the submodule generated by the a_i. Then the sequence $0 \to B \to A \to A/B \to 0$ induces

$$\cdots \to B_G \to A_G \to (A/B)_G \to 0.$$

As $B_G \to A_G$ is a surjection, we get $(A/B)_G = 0$, so $A = B$ by the above lemma. □

Notation. We denote $\Lambda = \mathbb{F}_p[G]$.

Lemma 4.3. *Let A be a finite $G-$module with $pA = 0$. Then there is a resolution*

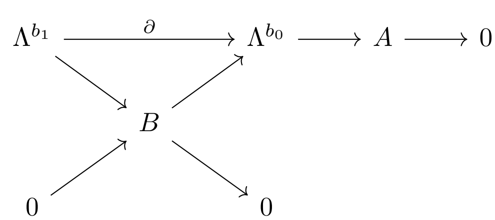
$$\cdots \xrightarrow{\partial} \Lambda^{b_2} \xrightarrow{\partial} \Lambda^{b_1} \xrightarrow{\partial} \Lambda^{b_0} \to A \to 0$$

such that $b_i = \dim_{\mathbb{F}_p}(\mathrm{H}_i(G, \mathbb{F}_p))$ and such that $\partial(\Lambda^{b_{n+1}}) \subseteq I_G \Lambda^{b_n}$.

Proof. By the above lemma, we have the epimorphism $\Lambda^{b_0} \twoheadrightarrow A$. Consider the exact sequence $0 \to B \to \Lambda^{b_0} \to A \to 0$. Since Λ^{b_0} is an induced $G-$module, all its homology groups for $i \geq 1$ vanish. The long exact sequence in homology then becomes

$$\cdots \to 0 \to \mathrm{H}_2(G, A) \to \mathrm{H}_1(G, B) \to 0 \to \mathrm{H}_1(G, A) \to \mathrm{H}_0(G, B) \to \mathrm{H}_0\left(G, \Lambda^{b_0}\right) \to \mathrm{H}_0(G, A) \to 0.$$

In fact, $\mathrm{H}_0\left(G, \Lambda^{b_0}\right) \to \mathrm{H}_0(G, A)$ is an isomorphism, since it is a surjection between $\mathbb{F}_p-$vector spaces of same dimension b_0. This implies that $\mathrm{H}_{i+1}(G, A) \xrightarrow{\sim} \mathrm{H}_i(G, B)$ for all $i \geq 0$ and also that $\mathrm{H}_0(G, B) \to \mathrm{H}_0\left(G, \Lambda^{b_0}\right)$ is the zero map. Repeating the above argument, we get a surjection $\Lambda^{b_1} \twoheadrightarrow B$. Then we can define $\Lambda^{b_1} \xrightarrow{\partial} \Lambda^{b_0}$ to be the composition $\Lambda^{b_1} \twoheadrightarrow B \to \Lambda^{b_0}$.



Note that $\partial(\Lambda^{b_1}) = \mathrm{Im}\left(B \to \Lambda^{b_0}\right) = \mathrm{Ker}\left(\Lambda^{b_0} \to A\right)$, so the top row is exact.

Moreover, since $\mathrm{H}_0(G, B) \to \mathrm{H}_0\left(G, \Lambda^{b_0}\right)$ is the zero map, we have $\mathrm{Im}\left(B \to \Lambda^{b_0}\right) \subseteq I_G \Lambda^{b_0}$. Hence $\partial(\Lambda^{b_1}) \subseteq I_G \Lambda^{b_0}$.

Continuing with this process in B, we get the desired resolution. □

Definition 4.4. Let A be a finite $G-$module such that $pA = 0$. Denote $c_i(A) = \dim_{\mathbb{F}_p} I_G^i A / I_G^{i+1} A$. Then the *Poincaré Polynomial* of A is $P_A(t) = \sum_{n\geq 0} c_n(A) t^n$. Note that since A is finite, this is indeed a polynomial.

Proof of Golod-Shafarevich. Let $d = d(G) = \dim_{\mathbb{F}_p} \mathrm{H}_1(G, \mathbb{F}_p)$ and $r = r(G) = \dim_{\mathbb{F}_p} \mathrm{H}_2(G, \mathbb{F}_p)$.

By the lemma above applied to $A = \mathbb{F}_p$, we have a resolution

$$\cdots \xrightarrow{\partial} \Lambda^r \xrightarrow{\partial} \Lambda^d \xrightarrow{\partial} \Lambda \to \mathbb{F}_p \to 0,$$

where we can take the map $\Lambda \to \mathbb{F}_p$ to be the augmentation map. By letting $E = I_G\Lambda, D = \Lambda^d, R = \Lambda^r$, we can write this sequence as

$$R \xrightarrow{\partial} D \to E \to 0.$$

Since $\partial(R) \subseteq I_G D$, this induces the sequence

$$I_G^n R \xrightarrow{\partial} I_G^{n+1} D \to I_G^{n+1} E \to 0$$

and hence induces

$$R/I_G^n R \xrightarrow{\partial} D/I_G^{n+1} D \to E/I_G^{n+1} E \to 0.$$

This last sequence is exact since we have

$$\mathrm{Ker}\left(D/I_G^{n+1}D \to E/I_G^{n+1}E\right) = \mathrm{Ker}\left(D \to E\right) \mod I_G^{n+1}D = \mathrm{Im}\left(R \xrightarrow{\partial} D\right) \mod I_G^{n+1}D = \mathrm{Im}\left(R/I_G^n R \xrightarrow{\partial} D/I_G^{n+1}D\right).$$

Note the first equality is true since $D \to E$ is surjective. From the exactness we obtain $s_n(D) \leq s_n(E) + s_{n-1}(R)$, where $s_n(A) = \sum_{0\leq i\leq n} c_i(A) = \dim_{\mathbb{F}_p}(A/I_G^{n+1}A)$ for a module A.

Since $I_G^i E/I_G^{i+1}E = I_G^{i+1}\Lambda/I_G^{i+2}\Lambda$, and $\Lambda/I_G\Lambda = \mathbb{F}_p$, we have that $P_E(t) = \frac{P(t)-1}{t}$ where $P(t) = P_\Lambda(t)$. Moreover, we clearly have $P_D(t) = dP(t)$ and $P_R(t) = rP(t)$. Using that for $0 < t < 1$ we have $\frac{1}{1-t}P_A(t) = \sum_{n\geq 0} s_n(A)$, the above inequality implies that

$$P_D(t) \leq P_E(t) + tP_R(t) \iff dP(t) \leq \frac{P(t)-1}{t} + rtP(t) \iff P(t)(1 - dt + rt^2) \geq 1.$$

Since $P(t)$ has positive coefficients, this implies that $1 - dt + rt^2 > 0$ for all $0 < t < 1$. By 3.1, we have $d \leq r < 2r$, so for $t = \frac{d}{2r}$ this reads $r > \frac{d^2}{4}$. $\square$

5. Sketch of Proof of Brumer's Theorem

As before, we assume that K has finite Class Field Tower and let $G = \mathrm{Gal}\left(K^{(\infty)}/K\right)$. Note that we have $\mathrm{Cl}_K \xrightarrow{\sim} \mathrm{Gal}\left(K^{(1)}/K\right) = G^{\mathrm{ab}}$ and

$$\mathrm{H}_1(G,\mathbb{F}_p) \simeq \mathrm{H}^1(G,\mathbb{F}_p) = \mathrm{Hom}(G,\mathbb{F}_p) = \mathrm{Hom}(G^{\mathrm{ab}},\mathbb{F}_p) \simeq \mathrm{Hom}(\mathrm{Cl}_K,\mathbb{F}_p) = \mathrm{Hom}((\mathrm{Cl}_K)_{(p)},\mathbb{F}_p),$$

which has the same size as $|(\mathrm{Cl}_K)_{(p)}|$, so in fact $d(G) = \dim_{\mathbb{F}_p}(\mathrm{Cl}_K)_{(p)}$.

So the theorem follows from Iwasawa's, Golod-Shafarevich's and the inequality

$$\dim_{\mathbb{F}_p}(\mathrm{Cl}_K)_{(p)} \geq t_p - \left(\frac{k-1}{p-1} + \nu_p(n)\delta_p\right).$$

Now let $G^\star = \mathrm{Gal}\left(K^{(1)}/\mathbb{Q}\right)$ and $G = \mathrm{Gal}(K/\mathbb{Q})$. We have the inflation-restriction exact sequence

$$0 \to \mathrm{H}^1(G^\star/G, U_{K^{(1)}}) \to \mathrm{H}^1(G^\star, U_{K^{(1)}}) \to \mathrm{H}^1(G, U_K).$$

By comparing dimensions in this formula, we are done if we prove that:

$$\mathrm{H}^1(G^\star/G, U_{K^{(1)}}) \simeq \mathrm{Cl}_K, \tag{5.1}$$

$$\dim_{\mathbb{F}_p}(\mathrm{H}^1(G^\star, U_{K^{(1)}}))_{(p)} = t_p, \tag{5.2}$$

$$\dim_{\mathbb{F}_p}(\mathrm{H}^1(G, U_K))_{(p)} \leq \frac{k-1}{p-1} + \nu_p(n)\delta_p. \tag{5.3}$$

Lemma 5.1. *Let L/K a Galois extension of number fields with Galois group G. If $I_L^G \subseteq P_L$, then we have a natural exact sequence*

$$0 \to \mathrm{Cl}_K \to \mathrm{H}^1(G, U_L) \to \mathrm{H}^1(G, \mathbb{U}_L) \to 0.$$

Proof. We have the following exact and commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_L & \longrightarrow & \mathbb{U}_L & \longrightarrow & \mathbb{U}_L/U_L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathbb{C}_L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_L & \longrightarrow & I_L & \longrightarrow & \mathrm{Cl}_L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

which induces the following exact commutative diagram in cohomology, where we use Hilbert 90

$$
\begin{array}{ccccccccccc}
 & & 0 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & U_K & \longrightarrow & \mathbb{U}_K & \longrightarrow & (\mathbb{U}_L/U_L)^G & \longrightarrow & \mathrm{H}^1(G, U_L) & \longrightarrow & \mathrm{H}^1(G, \mathbb{U}_L) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathbb{C}_K & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & P_L^G & \longrightarrow & I_L^G & \longrightarrow & \mathrm{Cl}_L^G & & & & \\
 & & \downarrow & & \downarrow & & & & & & \\
 & & \mathrm{H}^1(G, U_L) & \longrightarrow & \mathrm{H}^1(G, \mathbb{U}_L) & & & & & & \\
 & & \downarrow & & \downarrow & & & & & & \\
 & & 0 & & 0 & & & & & &
\end{array}
$$

We need to prove $\mathrm{H}^1(G, U_L) \xrightarrow{\varphi} \mathrm{H}^1(G, \mathbb{U}_L)$ is surjective with kernel Cl_K.

The hypothesis imply $P_L^G = I_L^G$, so that we get at once from the bottom of the diagram that the φ is surjective. Since the map $I_L^G \to \mathrm{Cl}_L^G$ is the zero map, a diagram chasing implies that $\mathbb{C}_K \to \mathrm{Cl}_L^G$ is also 0, so that $(\mathbb{U}_L/U_L)^G \to \mathbb{C}_K$ is an isomorphism. Then

$$
\mathrm{Ker}(\varphi) = \mathrm{Im}\left((\mathbb{U}_L/U_L)^G \to \mathrm{H}^1(G, U_L)\right) = (\mathbb{U}_L/U_L)^G/\mathrm{Im}\left(\mathbb{U}_K \to (\mathbb{U}_L/U_L)^G\right) \simeq
$$

$$
\simeq \mathbb{C}_K/\mathrm{Im}\left(\mathbb{U}_K \to (\mathbb{U}_L/U_L)^G \to \mathbb{C}_K\right) = \mathbb{C}_K/\mathrm{Im}(\mathbb{U}_K \to \mathbb{I}_K \to \mathbb{C}_K) = \mathbb{C}_K/\mathbb{U}_K = \mathbb{I}_K/(K^\times \cdot \mathbb{U}_K) = I_K/K^\times = \mathrm{Cl}_K.
$$

□

Proof of equation 5.1. Apply the lemma 5.1 above for the extension $K^{(1)}/K$ of Galois group $G' = \mathrm{Gal}\left(K^{(1)}/K\right)$. Note that $I_{K^{(1)}}^{G'} \subseteq P_{K^{(1)}}$ is the Principal Ideal theorem of the Hilbert Class Field. Since $K^{(1)}/K$ is unramified, we have that $\mathrm{H}^1(G', \mathbb{U}_{K^{(1)}}) = 0$. Then the lemma implies the equation we want since $G' = \mathrm{Gal}\left(K^{(1)}/K\right) = G^\star/G$. □

Proof of equation 5.2. We apply the lemma 5.1 for $K^{(1)}/\mathbb{Q}$. We have $I_{K^{(1)}}^{G^\star} \subseteq I_{K^{(1)}}^{G} \subseteq P_{K^{(1)}}$, so the theorem applies. The lemma gives us an isomorphism $\mathrm{H}^1(G^\star, U_{K^{(1)}}) \xrightarrow{\sim} \mathrm{H}^1(G^\star, \mathbb{U}_{K^{(1)}}) = \prod_p \mathbb{Z}/e_{K^{(1)}/\mathbb{Q}}(p)\mathbb{Z}$. Since $K^{(1)}/K$ is unramified, then $e_{K^{(1)}/\mathbb{Q}}(p) = e_{K/\mathbb{Q}}(p)$. Then the equation follows easily. □

Lemma 5.2. *Let G a finite group of order n and p a prime. Let A be a $G-$module which is a finitely generated abelian group. Then*

$$
\dim_{\mathbb{F}_p}(\mathrm{H}^1(G, A))_{(p)} \leq \nu_p(n) \dim_{\mathbb{F}_p} A_{(p)}.
$$

Sketch of Proof. Since the restriction map to a Sylow $p-$group P is injective on the $p-$primary components, we have that

$$
\dim_{\mathbb{F}_p}(\mathrm{H}^1(G, A))_{(p)} \leq \dim_{\mathbb{F}_p}(\mathrm{H}^1(P, A))_{(p)}.
$$

So it suffices to consider G a $p-$group.

Let $g_1, \ldots, g_d$ be a minimal generating set of G. Then we have $d \leq \nu_p(n)$ by Burnside Basis Theorem. Then every crossed homomorphism $f \in Z^1(G, A)$ is determined by the image in the g_i. Hence we have an injection $Z^1(G, A) \hookrightarrow A^d$.

Hence we have

$$\dim_{\mathbb{F}_p}(\mathrm{H}^1(G,A))_{(p)} \leq \dim_{\mathbb{F}_p}(A^d)_{(p)} \leq d \dim_{\mathbb{F}_p} A_{(p)} \leq \nu_p(n) \dim_{\mathbb{F}_p} A_{(p)}.$$

□

Remark 5.3. The stronger inequality

$$\dim_{\mathbb{F}_p}(\mathrm{H}^1(G,A))_{(p)} \leq \frac{r}{p-1} + \nu_p(n) \dim_{\mathbb{F}_p}(A^{\mathrm{tor}})_{(p)}$$

(where r is the rank of A) that we need for Brumer's theorem is proved by separating the cases of torsion and free modules, and proving a stronger inequality for the free module case.

Proof of equation 5.3. By Dirichlet's unit theorem, we have that $U_K \simeq \mu_K \cdot E$, where E is a free abelian group of k generators. Then the equation follows from the previous lemma 5.2 and the following remark for the full theorem. □

Without the improvements in 5.2, the bound we got implies the following weaker version of Brumer's theorem:

Theorem (Brumer)**.** *Let $K/\mathbb{Q}$ be Galois, of degree n. Let k be the number of infinite places of K, and p be a prime $p \mid n$. Let t_p be the number of primes ramified in K with the ramification index a multiple of p. Then K has an infinite Class Field Tower if*

$$t_p > \nu_p(n)(k+\delta_p) + 2 + 2\sqrt{k+\delta_p},$$

where $\delta_p = 1$ if the $p-$roots of unity are in K and 0 otherwise.

Corollary 5.4. There is a constant $c(n)$ such that, if $K/\mathbb{Q}$ is a Galois extension of number fields of degree n, then K has infinite Class Field Tower if the number of distinct primes ramified in $K/\mathbb{Q}$ is greater than $c(n)$. In fact, we can take

$$c(n) = \Omega(n)n + (2+2\sqrt{n})\omega(n)$$

by the weak form of Brumer's theorem we proved, or even

$$c'(n) = \sum_{p \mid n} \frac{n-1}{p-1} + \Omega(n) + (2+2\sqrt{n})\omega(n) < 3 \cdot n \cdot \ln\ln\ln n$$

for n sufficiently large by the stronger form of Brumer's theorem.