APPLICATIONS OF THE FIRST INEQUALITY

DAVID LIN AND JAE HYUNG SIM

Abstract. Our goal in these notes is to discuss some of the applications of the first inequality of class field theory.

1. Background

We begin by providing the necessary background on group cohomology. For reference with proofs, see chapter 4 of [?].

1.1. Cohomology.

Definition 1.1. Given an arbitrary group G and an arbitrary, abelian G-module A, we define the zeroth cohomology group by:

$$H^0(G, A) = A^G = \{a \in A \mid ga = a \text{ for all } g \in G\}$$

Definition 1.2. A cocycle is a map $f : G \to A$ such that $f(g_1 g_2) = f(g_1) \cdot g_1 f(g_2)$ for all $g_1, g_2 \in G$. Together the cocycles form a group under pointwise multiplication.
A coboundary is a map $f : G \to A$ such that $f(g) = ga/a$ for some $a \in A$ and all $g \in G$. These clearly form a subgroup of cocycles. So we define:

$$H^1(G, A) = \text{cocycles/coboundaries}$$

Note that when G is cyclic, we have that $H^1(G, A) = \ker(\text{Norm})/\text{Im}(\frac{g\cdot}{\cdot} : A \to A)$.

We can use cohomology to turn short exact sequences, such as the following:

$$1 \to A \to B \to C \to 1$$

into a long exact sequence:

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to \cdots$$

For now we only need the following statement about the $H^2(G, A)$.

Theorem 1.3. *If G is cyclic and A a G-module, $H^2(G, A) \cong A^G/Norm(A)$.*

Definition 1.4. The Tate cohomology groups are defined to be

$$\widehat{H}^r(G, A) = \begin{cases} A^G/\text{Norm}(A) & \text{if } r = 0 \\ H^r & r > 0 \end{cases}$$

Note that this directly implies that $H^2(G, A) \cong \widehat{H}^0(G, A)$, when G is cyclic.

Definition 1.5. The Herbrand quotient is $h_{2/1}(G, A) = |H^2(G, A)|/|H^1(G, A)|$, when the terms on the right are defined.

Lemma 1.6 (Shapiro's Lemma)**.** *Let G' be a subgroup of G. If A' is a G'-module, we can form the G-module $A = Hom_{G'}(\Lambda, A')$, where $\Lambda = \mathbb{Z}[G]$, the integral group ring of G. Then, for $q \geq 0$, we have:*

$$H^q(G, A) = H^q(G', A')$$

Proposition 1.7. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of G modules, where G is a cyclic group. Then, if at least two of $h_{2/1}(G, A), h_{2/1}(G, B), h_{2/1}(G, C)$ are defined, the third herbrand quotient is defined and $h_{2/1}(G, B) = h_{2/1}(G, A) \cdot h_{2/1}(G, C)$.*

Date: Mar 9, 2019.

Proposition 1.8. *Let A, B be G-modules, and $f : A \to B$ a G-homomorphism with finite kernel and cokernel. Then, if either $h_{2/1}(A)$ or $h_{2/1}(B)$ are defined, then the other is defined and $h_{2/1}(A) = h_{2/1}(B)$.*

Proposition 1.9. *Let E be a finite-dimensional $\mathbb{R}$-representation of G, and let L, M be two lattices of E which span E and are invariant under G. Then, if either $h_{2/1}(L)$ or $h_{2/1}(M)$ are defined, then the other is defined and $h_{2/1}(L) = h_{2/1}(M)$.*

1.2. **Ideles and Norms.**

Definitions 1.10. Let $L/K/\mathbb{Q}$ be abelian extensions.
We will use $N_{L/K}$ to denote the norm map for L/K.
K_p denotes the completion of K at some p a prime of K. Furthermore, U_p are the units of the ring of integers of K_p.
The ideles denoted as $\mathbb{A}_K^\times$ are equal to $\prod' K_p^\times \times (K \otimes \mathbb{R})^\times$ where $\prod'$ is a restricted product, meaning $\prod' K_p^\times$ is the subset of $\prod K_p^\times$ consisting of elements (a_p) where all but finitely many a_p lie in an open compact subgroup of $K_p^\times$, specifically U_p.
The idele class group denoted as C_K are equal to $K^\times \backslash \mathbb{A}_K^\times$.
The ideal class group denoted as Cl_K is I_K/Prin_K, where I_K is the set of fractional ideals in K and Prin_K is the set of principal ideals in K. A subgroup M of $K^\times$ is called a norm subgroup if there exists a finite abelian extension L/K with $M = N_{L/K} L^\times$.

From these definitions, the following proposition follows, though it will not be proven. For proofs and more background, see chapter 6 of [?].

Proposition 1.11. *For any number field K, the following sequence is exact.*

$$1 \longrightarrow \mathcal{O}_K^\times \diagdown \left((\mathbb{R} \otimes K)^\times \times \widehat{\mathcal{O}}_K^\times \right) \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 1$$

Proposition 1.12. *For some abelian extension L/K and finite set of primes S, we can define*

$$\mathbb{A}_{L,S}^\times = \prod_{v \in S} (\prod_{w|v} L_w^\times) \times \prod_{v \notin S} (\prod_{w|v} U_w)$$

Then, we have $h_{2/1}(G, \mathbb{A}_{L,S}^\times) = \prod_{v \in S} n_v$, where n_v are the degrees of the local extension, $[L_v : K_v]$.

Theorem 1.13. *A subgroup M of $K^\times$ is a norm subgroup if and only if it satisfies the following two conditions:*

(1) Its index $[K^\times : M]$ is finite.
(2) M is open in $K^\times$.

Theorem 1.14 (Weak Approximation)**.** *K is dense in a finite product of K_p.*

Corollary 1.15. *For S a finite set of primes, K surjects onto $\prod_S K_p/\mathcal{U}_p$, where $\mathcal{U}_p$ is some open subset of K_p.*

Proof. Because K is dense, the image of K intersects every open set. In particular, $x \cdot \prod_S(\mathcal{U}_p)$ is an open set for any x in $\prod_S K_p$, so there is an element, $\alpha \in K$ that maps into $x \cdot \prod_S(\mathcal{U}_p)$. Therefore, $\alpha \mapsto x$ in the quotient. □

2. The First Inequality

Theorem 2.1. *Let L/K be a cyclic extension of degree n. Then, $h_{2/1}(G, C_L) = n$.*

There is a proof of this on page 178 of [?]. Here, we restate and clarify this proof in the terminology used in this paper.

Proof. First, take a finite set S of primes large enough such that $\mathbb{A}_L^\times = L^\times \times \mathbb{A}_{L,S}^\times$. To be precise, S should contain the archimedean primes of K, the primes of K ramified in L, and primes of K that lie below primes whose classes generate Cl_L. Also, let T be the set of primes in L that lie above the primes in S. Because $\mathbb{A}_{L,S}^\times \to C_L$ is surjective by definition, we can write:

$$C_L = \mathbb{A}_L^\times / L^\times \simeq \mathbb{A}_{L,S}^\times / (L^\times \cap \mathbb{A}_{L,S}^\times)$$

Furthermore, we can denote $L_T = L^\times \cap \mathbb{A}_{L,S}^\times$ because it is easy to see that this is the set of $T-$units of L i.e. $L^\times \cap \prod_{w\in T}(L_w^\times) \times \prod_{w\notin T}(U_w)$. So, as $C_L = \mathbb{A}_{L,S}^\times / L_T$, we can see that:

$$h_{2/1}(G, C_L) = h_{2/1}(G, \mathbb{A}_{L,S}^\times)/h_{2/1}(G, L_T) \text{ by Proposition ??}$$

First, we calculate $h_{2/1}(G, \mathbb{A}_{L,S}^\times) = h_{2/1}(\prod_{v\in S}(\prod_{w|v} L_w^\times)) \cdot h_{2/1}(\prod_{v\notin S}(\prod_{w|v} U_w))$. Because S contains all ramified primes, we know from page 177 of [?] that $\prod_{v\notin S}(\prod_{w|v} U_w)$ has trivial cohomology, implying that $h_{2/1}(\prod_{v\notin S}(\prod_{w|v} U_w)) = 1$. So, we have:

$$h_{2/1}(G, \mathbb{A}_{L,S}^\times) = h_{2/1}(\prod_{v\in S}(\prod_{w|v} L_w^\times)) = (\prod_{v\in S} h_{2/1}(\prod_{w|v} L_w^\times))$$

By Proposition **??**, we see that $h_{2,1}(G, \mathbb{A}_{L,S}^\times) = \prod_{v\in S} n_v$, where n_v are the degrees of the local extensions. Now, we examine $h_{2/1}(L_T)$. We hope to show that $h_{2/1}(L_T) = n\prod_{v\in S} n_v$, as that will complete the proof. To do this, we construct two different lattices that span the same vector space, implying that they have the same Herbrand quotient, by Proposition **??**.

Let V be the real vector space of maps $f\colon T \to \mathbb{R}$, so we have that $V \simeq R^t$, where $t = [T]$, the cardinality of T. We define the action of G on V such that $(\sigma f)(w) = f(\sigma^{-1}w) \implies (\sigma f)(\sigma w) = f(w)$ for all $f \in V$, $\sigma \in G$, and $w \in T$. Now, we construct $N = \{f \in V | f(w) \in \mathbb{Z} \text{ for all } w \in T\}$. N spans V because we can multiply by any real number, and N is G-invariant because $\sigma^{-1}w$ is still an element of T and $f \in N$ maps any element of T to an integer. So, we have that $N \simeq \prod_{v\in S}(\prod_{w|v} \mathbb{Z}_w)$ where $\mathbb{Z}_w \simeq \mathbb{Z}$ for all w, and the action of G on N is to permute the $\mathbb{Z}_w$ for all w over a give $v \in S$. By applying Shapiro's lemma, again we get:

$$\widehat{H}^r(G, N) \simeq \prod_{v\in S} \widehat{H}^r(G, \prod_{w|v} \mathbb{Z}_w) \simeq \prod_{v\in S} \widehat{H}^r(G^v, \mathbb{Z})$$

Here, G^v is the decomposition group of v. So, we calculate:

$$h(N) = \prod_{v\in S}(|\widehat{H}^0(G^v, \mathbb{Z})|/|H^1(G^v, \mathbb{Z})|) = \prod_{v\in S}(|Z^{G^v}/N(Z)|/1) = \prod_{v\in S} n_v \text{ by Hilbert's Theorem 90}$$

Next, we define another lattice. Let $\lambda : L_T \to V$ such that $\lambda(a) \mapsto f_a$, where $f_a(w) = \log|a|_w$ for all $w \in T$. Dirichlet's Unit Theorem tells us that the kernel of this λ is finite and its image is a lattice M^0 of V spanning the subspace $V^0 = \{f \in V | \sum f(w) = 0\}$. From Proposition **??**, we have $h(L_T) = h(M^0)$ because the kernel of λ is finite. But, we can now write $V = V^0 + \mathbb{R}g$ where $g(w) = 1$ for all $w \in T$. We can construct $M = M^0 + \mathbb{Z}g$ to see that M spans V and both M^0 and $\mathbb{Z}g$ are invariant under G. Therefore, we get that $h_{2/1}(M) = h_{2/1}(M^0) \cdot h_{2/1}(\mathbb{Z}g) = nh_{2/1}(M^0) = nh_{2/1}(L_T)$. Furthermore, as M and N are lattices spanning the same vector space, we apply Proposition **??** and get that $h_{2/1}(M) = h_{2/1}(N)$. So, $\prod_v n_v = nh(L_T)$, as desired. □

Corollary 2.2 (First Inequality)**.** *Let L/K be a cyclic extension of degree n. Then, $\widehat{H}^0(G, C_L) \geq n$.*

Proof. This falls directly from Theorem **??**. □

3. Split Primes

Proposition 3.1. *If L/K is abelian and nontrivial, then there are infinitely many non-split primes.*

Proof. Suppose for contradiction that there are only finitely many non-split primes. Consider the following commutative diagram with exact rows and columns, resulting from the definition of C_K:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & L^\times & \longrightarrow & \mathbb{A}_L^\times & \longrightarrow & C_L & \longrightarrow & 1 \\
 & & \downarrow N & & \downarrow N & & \downarrow N & & \\
1 & \longrightarrow & K^\times & \longrightarrow & \mathbb{A}_K^\times & \longrightarrow & C_K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & K^\times/N_{L/K}(L^\times) & \longrightarrow & \mathbb{A}_K^\times/N_{L/K}(\mathbb{A}_L^\times) & \longrightarrow & C_K/N_{L/K}(C_L) & \longrightarrow & 1
\end{array}$$

First, we want to calculate $\mathbb{A}_K^\times/N_{L/K}(\mathbb{A}_L^\times)$. To do this, it suffices to examine the norm map. Suppose that $\mathfrak{p}$ is a totally split prime. Then, we can see that $N_{L/K}\colon (L\otimes K_\mathfrak{p}^\times)\to K_\mathfrak{p}^\times$ is surjective. This is because $L\otimes K_\mathfrak{p}^\times=\prod_n K_\mathfrak{p}^\times$, implying that for $\mathfrak{p}$ totally split

$$N_{L/K}\colon \prod_n K_\mathfrak{p}^\times \to K_\mathfrak{p}^\times$$
$$(a_1,...,a_n)\mapsto \prod_n a_i$$

This map is clearly surjective. But what happens at the non-split primes? Then, for some non-split prime $\mathfrak{p}$, we have $\mathfrak{p}=\mathfrak{p}_1\cdots\mathfrak{p}_r$ for some $r|n$ and $[L_{\mathfrak{p}_i}:K_\mathfrak{p}]=n/r$ where $L_{\mathfrak{p}_i}=L_{\mathfrak{p}_j}$ for $1\le i,j\le r$. Then, we have:

$$N_{L/K}\colon \prod_r L_\mathfrak{p}^\times \to K_\mathfrak{p}^\times$$
$$(a_1,...,a_r)\mapsto \prod_r N(a_i)$$

So, the image of $N_{L/K}$ is $N_{L_\mathfrak{p}/K_\mathfrak{p}}(L_\mathfrak{p}^\times)$. Together with our assumption that there are finitely many nonsplit primes, this implies that

$$\mathbb{A}_K^\times/N_{L/K}(\mathbb{A}_L^\times)=\prod_{\mathfrak{p}\text{ non-split}} K_\mathfrak{p}^\times/N_{L_\mathfrak{p}/K_\mathfrak{p}}(L_\mathfrak{p}^\times)$$

Now, we apply weak approximation to see that $K^\times$ is dense in $\prod_{\mathfrak{p}\text{ non-split}} K_\mathfrak{p}^\times$ because there are finitely many non-split primes. Theorem **??** gives us that $N_{L_\mathfrak{p}/K_\mathfrak{p}}(L_\mathfrak{p}^\times)$ is an open subgroup. Therefore, Corollary **??** tells us that $K^\times/N_{L/K}(L^\times)\to\mathbb{A}_K^\times/N_{L/K}(\mathbb{A}_L^\times)$ is surjective implying that $C_K/N_{L/K}(C_L)$ is trivial. However, Corollary **??** gives us a nontrivial lower bound on $\widehat{H}^0(G,C_L)$, so we have a contradiction. □

4. Dirichlet's Theorem on Arithmetic Progressions

Theorem 4.1. *If $(a,m)=1$, then there exists infinitely many primes of the form $a+mk$, where $k\in\mathbb{N}$.*

The most common proof of this theorem uses L-functions. However, we want to apply the first inequality to find some interesting facts.

Proposition 4.2. *There are infinitely primes p such that $p\not\equiv 1 \mod m$.*

Proof. Consider $K=\mathbb{Q}(\zeta_m)$. Then $G=\mathrm{Gal}(K/\mathbb{Q})=(\mathbb{Z}/m\mathbb{Z})^\times$. Now, consider $p\nmid m$. Then, from class field theory, we have that $\mathrm{Frob}_p\in Gal(K/\mathbb{Q})$ maps to $p\in(\mathbb{Z}/m\mathbb{Z})^\times$. Furthermore, we know that the decomposition group $\mathcal{D}_p=\{\sigma\in G:\sigma(p)=p\}=\langle\mathrm{Frob}_p\rangle$. Now, note that if p splits completely, then $\mathcal{D}_p=\{e\}$, which is equivalent to saying $\mathrm{Frob}_p=1$ and $p\equiv 1\mod m$. However, if you look at nonsplit primes, we previously showed that there are infinitely many nonsplit primes in Proposition 2.1. This implies that there must be infinitely many primes such that $p\not\equiv 1 \mod m$. □

This seems to be the limit of the first inequality without invoking stronger theorems. For example, we could use the Chebotarev Density Theorem to see that since G is abelian, the set of primes $p\equiv a\mod m$ has density $1/n$ in the set of all primes.

5. Hilbert Class Field

A consequence of class field theory is that for any given number field K, the class group Cl_K is isomorphic to the Galois group of M/K where M is the maximal extension of K that is abelian and unramified at all places of K. One immediate observation is that the class number $|Cl_K|$ is equal to the degree of the extension M/K. To explore how this consequence arises from class field theory, we will show that the first inequality implies that $[M:K]$ divides $|Cl_K|$.

We begin by first showing that if L/K is an abelian extension of prime degree p such that every prime of K is unramified in L, then p must divide $|Cl_K|$.

Proposition 5.1. *Let K be a number field and Cl_K its class group. If $p\in\mathbb{Z}$ is a prime such that p does not divide $|Cl_K|$, then there does not exist an finite abelian field extension L/K such that all primes of K are unramified in L and $p=[L:K]$.*

Proof. With the assumptions of the proposition, suppose for contradiction that there exists an abelian field extension L/K of degree p such that all primes of K are unramified in L. Let G denote the group $\mathrm{Gal}(L/K)$.

Let C_L and C_K be the idele class group of L and K, respectively. Then, we get the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_L^\times \diagdown \left((\mathbb{R} \otimes L)^\times \times \widehat{\mathcal{O}}_L^\times \right) & \longrightarrow & C_L & \longrightarrow & Cl_L & \longrightarrow & 1 \\ & & \downarrow N & & \downarrow N & & \downarrow N & & \\ 1 & \longrightarrow & \mathcal{O}_K^\times \diagdown \left((\mathbb{R} \otimes K)^\times \times \widehat{\mathcal{O}}_K^\times \right) & \longrightarrow & C_K & \longrightarrow & Cl_K & \longrightarrow & 1 \end{array}$$

where N on the quotient is the map taken at each place while N on C_L and Cl_L are the induced map (which facilitates commutativity). As a result, we get the following short exact sequence:

$$1 \longrightarrow \frac{\mathcal{O}_K^\times \diagdown (\mathbb{R}^\times \otimes K^\times) \times \widehat{\mathcal{O}}_K^\times)}{N(\mathcal{O}_L^\times \diagdown (\mathbb{R}^\times \otimes L^\times) \times \widehat{\mathcal{O}}_L^\times))} \longrightarrow C_K/N(C_L) \longrightarrow Cl_K/N(Cl_L) \longrightarrow 1$$

Recall that for any G-module M_L, $\widehat{H}^0(G, M_L)$ is defined to be $M_L^G/N(M_L)$. Thus, we can rewrite the above sequence as follows:

$$1 \longrightarrow \widehat{H}^0(G, \mathcal{O}_L^\times \diagdown (\mathbb{R} \otimes L)^\times \times \widehat{\mathcal{O}}_L^\times) \longrightarrow \widehat{H}^0(G, C_L) \longrightarrow \widehat{H}^0(G, Cl_L) \longrightarrow 1$$

By Theorem **??**, we know that $p = [L : K]$ divides $|\widehat{H}^0(G, C_L)|$. However, by assumption, p does not divide $|Cl_K|$, and since $\widehat{H}^0(G, Cl_L)$ is a quotient of Cl_K, p does not divide $|\widehat{H}^0(G, Cl_L)|$. Thus, it is sufficient to show that p does not divide $|\widehat{H}^0(G, \mathcal{O}_L^\times \diagdown (\mathbb{R} \otimes L)^\times \times \widehat{\mathcal{O}}_L^\times)|$ to arrive at a contradiction.

We take for granted from local class field theory that the norm map maps the component $\widehat{\mathcal{O}}_{L_v}^\times$ onto $\widehat{\mathcal{O}}_{K_v}^\times$ where L_v/K_v is unramified. For the infinite places, observe that the tensor-product $\mathbb{R} \otimes K$ (respectively $\mathbb{R} \otimes L$) decomposes into the product $\mathbb{C}^{c_K} \times \mathbb{R}^{r_K}$ (resp $\mathbb{C}^{c_L} \times \mathbb{R}^{r_L}$) where c_K (resp c_L) and r_K (resp r_L) are the number of complex embeddings and real embeddings of K (resp L), respectively. Since L is unramified everywhere, and therefore unramified at the infinite places, all real places of K cannot ramify as a complex place in L. Thus, each infinite place always splits which implies that the norm map is surjective at each complex place. As for the real places, the norm is clearly surjective. In conclusion, $\widehat{H}^0(G, \mathcal{O}_L^\times \diagdown (\mathbb{R} \otimes L)^\times \times \widehat{\mathcal{O}}_L^\times)$ is trivial and, in particular, its order is not divisible by p. ☐

The proof above actually provides a stronger statement than Proposition **??**. Since Theorem **??** states that $h_{2/1}(C_L)$ is precisely $[L : K]$, we can immediately extend the process to cyclic extensions of prime power. Precisely, we get the following corollary.

Corollary 5.2. *Let K be a number field and Cl_K its class group. If $p \in \mathbb{Z}$ is a prime such that p^n does not divide $|Cl_K|$ for some $n \in \mathbb{N}$, then there does not exist a cyclic field extension L/K such that all primes of K are unramified in L and $p^n = [L : K]$.*

Naturally, as we have broken down the cyclic extensions of prime power orders, we seek to extend this result to all abelian extensions of prime power orders. Specifically, we must extend our results to Galois extensions with Galois groups of the form $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$.

Proposition 5.3. *Let K be a number field and Cl_K its class group. If $p \in \mathbb{Z}$ is a prime such that p^n does not divide $|Cl_K|$, then there does not exist a finite abelian field extension L/K such that all primes of K are unramified in L and $p^n = [L : K]$.*

Proof. Suppose L/K is an abelian extension of degree p^n that is everywhere unramified. Prop **??** states that L/K cannot be a cyclic extension, so $\mathrm{Gal}(L/K)$ must be isomorphic to $\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$. Let $E_1, \ldots, E_r$ be the subextensions such that $\mathrm{Gal}(E_i/K) = \mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Gal}(E_1 \ldots E_r/K) = (\mathbb{Z}/p\mathbb{Z})^r$. Denote by E, the compositum of the subextensions $E_1, E_2, \ldots, E_r$.

Recall that the proof of surjection of the norm map $\mathcal{O}_L^\times \diagdown (\mathbb{R} \otimes L)^\times \times \widehat{\mathcal{O}}_L^\times \to \mathcal{O}_K^\times \diagdown (\mathbb{R} \otimes L)^\times \times \widehat{\mathcal{O}}_K^\times$ within the proof of Proposition **??** relies solely on L/K being an everywhere unramified extension, so the surjection still holds. Thus, it is sufficient to show that the order of the quotient $C_K/N(C_L)$ is divisible by p^n.

Since each E_i is a cyclic extension by construction, the first inequality tells us that $C_K/N(C_{E_i})$ has order p. Furthermore, each E_i is everywhere unramified since each E_i is a subextension of L. Note that since E, the compositum of all E_i, has Galois group $(\mathbb{Z}/p\mathbb{Z})^r$, the quotient $C_K/N_{E/K}(C_E)$ must have at least r factors of p-groups.

For each $1 \leq i \leq r$, define F_i as a subextension of L/K such that $\mathrm{Gal}(F_i/K) = \mathbb{Z}/p^{n_i}\mathbb{Z}$ and E_i is a subextension of F_i/K. By the proof of Proposition **??** and the proof of the first inequality, we know that $C_K/N_{F_i/K}(C_{F_i})$ has a cyclic component of degree p^{n_i}.

Finally, recall that norms compose nicely, i.e. $N_{E_i/K} \circ N_{F_i/E_i} = N_{F_i/K}$. Thus, $N_{F_i/K}(C_{F_i}) \subset N_{E_i/K}(C_{E_i})$. In fact, each F_i gives rise to a factor of $\mathbb{Z}/p^{n_i}\mathbb{Z}$ in $C_K/N_{L/K}(C_L)$. Since the norm of each F_i pass through $N_{E/K}(C_E)$, it follows that $C_K/N_{L/K}(C_L)$ contains a subgroup isomorphic to $\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$. It follows that p^n divides $|Cl_K/N_{L/K}(Cl_L)|$, so p^n divides $|Cl_K|$ which is a contradiction. □

In effect, Proposition **??** tells us that the maximal abelian everywhere unramified extension of a global field cannot have degree greater than the order of the class group. It remains to show that for any number field K, there exists an everywhere unramified abelian extension of K of degree $|Cl_K|$. However, once this "global" property (which is proven by the full force of class field thoery) is proven, one can conclude that the maximal everywhere unramified abelian extension of a number field K has Galois group isomorphic to its class group Cl_K.

Acknowledgments. It is a pleasure to thank our professor, Matthew Emerton, for teaching us about global class field theory. Also, we are very appreciative of PhD student Karl Schaefer for helping us work through computations and details.

References

[1] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory.* London Mathematical Society. 2010.