AN ABSTRACT APPROACH TO LOCAL CLASS FIELD THEORY

ACHYUT BHARADWAJ

Abstract. We prove the local reciprocity theorem, the central result of local class field theory, using Neukirch's approach. After introducing the necessary cohomological tools, we set up an abstract formulation of field theory and number theory. We then assume the Class Field Axiom, a minimal condition on the base field, and prove the reciprocity theorem. Finally, we verify the class field axiom in the case of local fields.

Contents

1. Introduction

Class Field Theory is the study of abelian Galois extensions of fields, motivated by the Kronecker Weber Theorems. The Global Kronecker Weber Theorem states that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$. Its local analogue asserts that every abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension of $\mathbb{Q}_p$.

Beyond these special cases, the central result is the Artin Reciprocity Theorem, which in the case of local fields is as follows:

Theorem 1.1 (Local Artin Reciprocity)**.** *If L/K is a finite Galois extension of local fields, there is an isomorphism $r_{L/K}\colon \mathrm{Gal}(L/K)^{ab} \to K^\times/N_{L/K}L^\times$.*

Indeed one may deduce the Kronecker Weber Theorems as corollaries of this theorem.

Our goal in this paper is to prove the local reciprocity theorem using an abstract approach due to Neukirch[1]. Earlier proofs had been given by Lubin-Tate, but Neukirch showed that the theorem can be deduced from a minimal set of assumptions, which he called the *Class Field Axiom*. Proving the Class Field Axiom for local fields then yields local reciprocity theorem. Although Neukirch avoids cohomological language, we take a slightly broader viewpoint and set up the arguments in terms of Tate cohomology. The paper proceeds by first developing this cohomological machinery, then setting up the abstract framework, proving the theorem abstractly and finally specializing to the local case. We also include a section on Kummer Theory as a toy model to illustrate the abstract method used. This also gives us Hilbert's Theorem 90 in passing.

2. Tate Cohomology

In this section, we set up some cohomological tools that we will use to state and prove the Class Field Axiom. Tate cohomology connects cohomology and homology groups into a single long exact sequence. Within this setting we introduce the Herbrand quotient, which is key to verifying the class field axiom, and collect a few miscellaneous results for later use.

Throughout this section, let G be a multiplicative abelian group and M be an additive left G-module. We write M^G to denote $\{m \in M \colon gm = m \forall g \in G\}$ and $M_G = M/I_G M$ where $I_G M$ denotes the subset of M generated by $\{gm - m \colon g \in G, m \in M\}$.

When G acts on M, we are often interested in the invariants M^G. However, the functor $M \mapsto M^G$ is only left exact. Group cohomology salvages this by extending the left exact sequence of invariants into a long exact sequence of so-called cohomology groups. In what follows, we mostly encounter the first two cohomology groups $H^0(G, M) = M^G$ and $H^1(G, M)$ which is the collection of crossed homomorphisms upto equivalence. For a full treatment of cohomology, see [5, Chapter 2]. Homology groups are defined dual to cohomology groups.

Tate cohomology ties in cohomology and homology groups into a single long exact sequence that extends infinitely on both sides. For finite G, it is based on the notion of a norm

Definition 2.1. If M is a G-module where G is a finite abelian group, the norm map $N_G \colon M \to M$ is defined so that $m \mapsto \sum_{g \in G} gm$.

If $g' \in G$, we have

$$g' N_G(m) = \sum_{g \in G} (gg')m = \sum_{h \in G} hm = N_G(m)$$

This shows that $N_G(M) \subset M^G$. This further implies that whenever $m \in I_G M$, $N_G(m) = 0$, i.e. $I_G M \subset \ker N_G$. Therefore, N_G induces a well defined map $\widetilde{N}_G \colon M/I_G M = M_G \to M^G$. The Tate groups are then defined as follows

Definition 2.2. For any $n \in \mathbb{Z}$, we define:

$$H_T^n(G, M) := \begin{cases} H_{-n-1}(G, M) & n \leq -2 \\ \ker \widetilde{N}_G & n = -1 \\ \operatorname{coker} \widetilde{N}_G & n = 0 \\ H^n(G, M) & n \geq 1 \end{cases}$$

We may equivalently write $H_T^{-1}(G, M) = \ker N_G / I_G M$ and $H_T^0(G, M) = M^G / N_G M$.

Proposition 2.3. *If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, it extends to a long exact sequence of Tate cohomologies as follows:*

$$\cdots \to H_T^n(A, M) \to H_T^n(B, M) \to H_T^n(C, M) \to H_T^{n+1}(A, M) \to \cdots$$

which extends over all integers n.

Proof. When $n < -2$, this is simply the long exact sequence of homology groups, and when $n > 1$, it is the long exact sequence of cohomology groups. We need to prove that the sequence remains exact for $-2 \leq n \leq 1$. To see this, consider the following commutative diagram where we know the rows to be exact.

$$\begin{array}{ccccccccc}
\cdots \longrightarrow H_1(G,C) & \longrightarrow & H_0(G,A) & \longrightarrow & H_0(G,B) & \longrightarrow & H_0(G,C) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \widetilde{N}_G} & & \downarrow{\scriptstyle \widetilde{N}_G} & & \downarrow{\scriptstyle \widetilde{N}_G} & & \\
0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) & \longrightarrow & H^1(G,A) \longrightarrow \cdots
\end{array}$$

Thus a direct application of the snake lemma implies that the sequence

$$H_T^{-1}(G,A) \to H_T^{-1}(G,B) \to H_T^{-1}(G,C) \to H_T^0(G,A) \to H_T^0(G,B) \to H_T^0(G,C)$$

is exact since H_T^{-1} is the kernel of $\widetilde{N}_G$ and H_T^0 is the cokernel. Now, the restriction of the map $H_1(G,C) \to H_0(G,A)$ to $\ker \widetilde{N}_G$ induces a map $H_1(G,C) \to H_T^{-1}(G,A)$. Since the map $H_T^{-1}(G,A) \to H_0(G,A)$ is injective the two maps have the same kernel. It therefore follows that the sequence $\cdots \to H_1(G,C) \to H_T^{-1}(G,A) \to \cdots \to H_T^0(G,C)$ is exact. Similarly, there is a map $H_T^0(G,C) \to H^1(G,A)$ whose image equals that of $H^0(G,C) \to H^1(G,A)$. This gives us the desired long exact sequence. □

We now turn to the periodicity of Tate cohomology in the case of cyclic groups.

Theorem 2.4. *If G is finite and cyclic, $H_T^n(G,M) = H_T^{n+2}(G,M)$ for all $n \in \mathbb{Z}$.*

Proof. For a full proof, see [5, Chapter II, Proposition 3.4.] We will give a sketch here.

The proof relies on the following lemma: If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \to 0$ is an exact sequence with $H_T^n(G,B) = H_T^n(G,C) = 0$ for all $n \in \mathbb{Z}$, then $H_T^{n+2}(G,A) \cong H_T^2(G,D)$. The proof is as follows: The exact sequence $0 \to A \to B \to C \to D \to 0$ gives rise to two exact sequences $0 \to A \to B \to B/\operatorname{Im} f \to 0$ and $0 \to B/\ker g \to C \to D \to 0$. Converting the first into a long exact sequence of Tate groups we get

$$\cdots \to H_T^{n+1}(A) \to H_T^{n+1}(B) \to H_T^{n+1}(B/\operatorname{Im} f) \to H_T^{n+2}(A) \to H_T^{n+2}(B) \to \cdots$$

However, $H_T^{n+1}(B) = 0$ and $H_T^{n+2}(B) = 0$ so that the map $H_T^{n+1}(B/\operatorname{Im} f) \to H_T^{n+2}(A)$ is an isomorphism. On repeating the process for the second sequence we see that $H_T^{n+1}(B/\ker g) \cong H_T^n(D)$. However, $B/\ker g = B/\operatorname{Im} f$ by exactness of the original sequence. This shows that $H_T^{n+2}(G,A) \cong H_T^n(G,D)$.

In order to apply this lemma to the theorem, we construct an exact sequence $0 \to M \to X \to X \to M \to 0$ where X has the property that $H_T^n(G,X) = 0$ for all n. In particular, the sequence used is

$$0 \to M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to M \to 0$$

To see why the middle term of the sequences has trivial tate cohomology and why the sequence is exact, see [5]. □

Thus, Tate cohomologies cycle back after two iterations. In particular, if $0 \to A \to B \to C \to 0$ is exact, we get the following exact hexagon:

$$\begin{tikzcd}
& H_T^{-1}(G,A) \arrow[r, "f_3"] & H_T^{-1}(G,B) \arrow[dr, "f_4"] & \\
H_T^0(G,C) \arrow[ur, "f_2"] & & & H_T^{-1}(G,C) \arrow[dl, "f_6"] \\
& H_T^0(G,B) \arrow[ul, "f_1"] & H_T^0(G,A) \arrow[l, "f_0"] &
\end{tikzcd}$$

This allows us to define the Herbrant quotient that plays a key role in the verification of the Class Field Axiom.

Definition 2.5. If G is cyclic and finite and M is a G-module, we define the Herbrand quotient to be $h(M) = \left|H_T^0(G,M)\right| / \left|H_T^{-1}(G,M)\right|$.

An important property of Herbrand quotients is that if $0 \to A \to B \to C \to 0$ is exact, $h(B) = h(A)h(C)$. To see why, let n_X^i denote the cardinality of $H_T^i(G,X)$ where X is one of A, B or C. We then have

$$\frac{n_B^0}{n_B^{-1}} = \frac{n_A^0}{n_A^{-1}} \cdot \frac{n_C^0}{n_C^{-1}} \cdot \left(\frac{n_B^0}{n_A^0} \cdot \frac{n_A^{-1}}{n_C^0} \cdot \frac{n_C^{-1}}{n_B^{-1}}\right)$$

Now, we have $H_T^0(G,A)/\ker f_0 \cong \operatorname{Im} f_0$ so that $n_A^0 = |\ker f_0|\,|\operatorname{Im} f_0|$. Doing the same for all terms, the term in the parentheses becomes

$$\frac{|\ker f_1|\,|\operatorname{Im} f_1|}{|\ker f_0|\,|\operatorname{Im} f_0|} \cdot \frac{|\ker g_0|\,|\operatorname{Im} g_0|}{|\ker f_2|\,|\operatorname{Im} f_2|} \cdot \frac{|\ker g_2|\,|\operatorname{Im} g_2|}{|\ker g_1|\,|\operatorname{Im} g_1|} = 1$$

which we get by applying exactness of the hexagon. This shows that $h(B) = h(A)h(C)$.

Below are a few other results that we will use later. The first two have applications in verifying the Class Field Axiom while the third is used in proving the Reciprocity Theorem from the axiom.

Proposition 2.6. *Shapiro's Lemma extends to the Tate cohomology H_T^0, i.e. if H is a subgroup of G, N is a H-module and M is a G-module, we have $H_T^0(G, \operatorname{Ind}_H^G N) \cong H_T^0(H,N)$.*

Proof. See [1, Chapter IV, Proposition 7.4.] □

Proposition 2.7. *If M is a finite G-module where G is cyclic then $h(M) = 1$.*

Proof. Let g be a generator of G and let $f\colon M \to M$ take $m \mapsto gm - m$. Then, the sequence $0 \to M^G \to M \xrightarrow{f} M \to M_G \to 0$ is exact. Now $|M| = |\ker f|\,|\operatorname{Im} f|$ and also $|M| = |\operatorname{Im} f|\,|M_G|$. This shows that $|M_G| = |\ker f| = \left|M^G\right|$. Next, we use the exact sequence $0 \to H_T^{-1}(M) \to M_G \xrightarrow{N_G} M^G \to H_T^0(M) \to 0$. Since $\left|M^G\right| = |M_G|$ we may repeat the above procedure to get $\left|H_T^{-1}(M)\right| |\operatorname{Im} N_G| = |\operatorname{Im} N_G| \left|H_T^0(M)\right|$ which gives the desired result. □

Proposition 2.8. *If G is a finite group with normal subgroup H and M is a G-module with $H^i(G, M) = 0$ for all $i = 1, 2, \ldots, n-1$, then the sequence*

$$0 \to H^n(G/H, M^H) \xrightarrow{\text{Inf}} H^n(G, M) \xrightarrow{\text{Res}} H^n(H, M)$$

is exact. We also deduce from this that

$$0 \to H^0_T(G/H, M^H) \xrightarrow{\text{Inf}} H^0_T(G, M) \xrightarrow{\text{Res}} H^0_T(H, M)$$

is exact.

Proof. See [3, Lemma 15.6 and Proposition 13.7.] □

3. Abstract Setup

We now reformulate the standard language of Galois theory and Number Theory in a purely group-theoretic framework, following Neukirch. This allows us to speak of fields, extensions, norms, and modules using only subgroups of a fixed profinite group.

3.1. Galois Groups and Fixed Fields.

Galois groups and fields are central to class field theory, for which we now provide an abstract framework.

If k is a field and $\overline{k}$ its separable closure, the abstract notion corresponding to $\text{Gal}(\overline{k}/k)$ is a profinite group, which is the projective limit of finite groups under the discrete topology. In particular $\text{Gal}(\overline{k}/k)$ is the projective limit of $\text{Gal}(K/k)$ where K is a finite extension of k. For more on profinite groups, see [6]. All our work moving forward will be in relation to a fixed profinite group G.

Since G is equipped with a topology, we index the closed subgroups of G as $\{G_K\}$. The index K of the closed subgroup G_K is called a fixed field. We will denote the index corresponding to a subgroup H as $\mathfrak{F}(H)$. In the case when $G = \text{Gal}(\overline{k}/k)$, closed subgroups correspond to intermediate fields and hence this definition of a fixed field makes intuitive sense.

We denote $k = \mathfrak{F}(G)$ and $\overline{k} = \mathfrak{F}(\{1\})$. If K and L are fields, we say $K \leq L$ or $K \subset L$ if $G_L \subset G_K$ and L will be called an extension of K (also denoted L/K). We write $\text{Gal}(L/K)$ to denote the quotient G_K/G_L and we will call L a Galois extension of K if $\text{Gal}(L/K)$ is a normal subgroup of G_K.

Another important notion is restrictions of field automorphisms, which we now abstractly define. Let $K \subset L \subset M$ with each extension normal and let $\sigma \in \text{Gal}(M/K) = G_K/G_M$. We map σ to its equivalence class in $(G_K/G_M)/(G_L/G_M)$ and use the identification $(G_K/G_M)/(G_L/G_M) \cong G_K/G_L$ to obtain $\sigma_L \in \text{Gal}(L/K)$. Once again, observe that all these definitions correspond to the usual definitions when G is a Galois group.

3.2. Modules and the Norm Map.

Class Field Theory also often studies multiplicative groups such as $L^\times$ as G-modules and hence incorporating modules into our formulation is important. In general, we fix a right multiplicative G-module A for which the action of G on A is continuous with respect to the topology on G. If L is an intermediate field, we write A_L to denote $A^{G_L} = \{a \in A \colon a^g = a \forall g \in G_L\}$. In particular, if we choose $A = \overline{k}^\times$, $L^\times = A_L$.

Notice the symbol $N_{L/K}$ in the statement of Theorem 1.1. This is called the norm map from A_L to A_K and it ties in to the cohomological definition of a norm. Given a finite extension L/K, we define the norm map $N_{L/K}\colon A_L \to A_K$ so that $N_{L/K}(a) = \prod_{\sigma\in S} a^\sigma$ where S is a collection of representatives of G_K/G_L.

Proposition 3.1. *The norm map $N_{L/K}$ is well defined.*

Proof. We first show that the product is independent of the choice of S. Suppose σ, τ are in the same equivalence class, i.e. $\sigma\tau^{-1} \in G_L$. For any $a \in A_L$, we then have $a^{\sigma\tau^{-1}} = a$. Applying the right action τ on both sides, $(a^{\sigma\tau^{-1}})^\tau = a^\sigma = a^\tau$ which shows the desired result. The preceding proof essentially shows that $\mathrm{Gal}(L/K)$ acts on A_L via a well defined group action. Next, we will show that the norm of a indeed lies in A_K. Suppose $\tau \in G_K$, we have

$$N_{L/K}(a)^\tau = \prod_{\sigma\in S} a^{\sigma\tau} = \prod_{\sigma\in S'} a^\sigma$$

where S' is the set τS, which is also a system of representatives. Since we showed that the product is independent of the system chosen, it follows that $N_{L/K}(a)^\tau = N_{L/K}(a)$ and we are done. $\square$

Therefore, we may write $N_{L/K}(a) = \prod_{\sigma\in G} a^\sigma$ where $G = \mathrm{Gal}(L/K)$ acts on A_L. This corresponds exactly to the norm map N_G acting on A_L.

We may therefore define Tate cohomologies of $\mathrm{Gal}(L/K)$. We have

$$H_T^{-1}(\mathrm{Gal}(L/K), A_L) = \ker N_G/I_G A_L = \ker N_{L/K}/Q$$

where $Q = I_{\mathrm{Gal}(L/K)}A_L$ is the set of all elements of A_L of the form $a^\sigma \cdot a^{-1}$ for some $a \in A_L$ and $\sigma \in \mathrm{Gal}(L/K)$. Similarly,

$$H_T^0(\mathrm{Gal}(L/K), A_L) = A^G/N_G A = A_L^{\mathrm{Gal}(L/K)}/N_{L/K}A_L = A_K/N_{L/K}A_L$$

The above two definitions are central to understanding the Class Field Axiom.

3.3. **Number Theory.** Proving Number Theoretic results involving extensions of fields often relies on simplifying the theorem statement to cases such as when the extension is unramified. We therefore need corresponding abstract notions.

Recall from Number Theory that an extension L/K is unramified if and only if L is contained in $\widetilde{K}$, which denotes the maximal unramified extension of K. In the abstract setting, we may take this as the definition of an unramified extension. However, we still need to define the maximal unramified extension of a field. Further recall that if L/K is an extension and $\mathfrak{P}$ is a prime ideal in L, the maximal extension of K for which $\mathfrak{p} = \mathfrak{P} \cap K$ remains unramified is the fixed field of the inertia group $I_{\mathfrak{P}}$ (see [7, Chapter 4, Theorem 28]).

We therefore first define the inertia group, from which other definitions naturally follow. In addition to the profinite group G, we assume the existence of a fixed surjection $d\colon G \to \widehat{\mathbb{Z}}$ which is the projective limit of $\mathbb{Z}/n\mathbb{Z}$. The inertia group I_k of the base field k is then defined as $\ker d$.

Now, for a field K, let $f_K = (\widehat{\mathbb{Z}} : d(G_K))$ so that the map $d_K = \frac{1}{f_K}d$ from G_K to $\widehat{\mathbb{Z}}$

is a surjection. We then define the inertia group of K, I_K by $\ker d_K$. Equivalently, $I_K = \ker d|_{G_K} = \ker d \cap G_K$. With this, we may define the maximal unramified extension:

Definition 3.2. For a field K, the maximal unramified extension of K is given by $\widetilde{K} := \mathfrak{F}(I_K)$. This is denoted as K^{unr} in many sources.

We equivalently have $G_{\widetilde{K}} = I_K$ and hence $I_K = G_K \cap G_{\widetilde{k}}$ which we will denote as $G_{K\widetilde{k}}$. Thus, the definition of an unramified extension now makes sense.

We will often want to make references to the inertia degree $f_{L/K}$ and ramification index $e_{L/K}$. We thus define $e_{L/K} := (I_K : I_L)$ and $f_{L/K} := (d(G_K) : d(G_L))$. Indeed, $f_K = f_{K/k}$ and when $L \subset \widetilde{K}$, $I_K \subset G_L$ so that $I_L = I_K$. Hence, $e_{L/K} = 1$ if L/K is unramified, which agrees with standard Number Theoretic notions. The corresponding notion of total ramification now follows simply:

Definition 3.3. We say L/K is totally ramified if $f_{L/K} = 1$.

Abstract Class Field Theory also relies heavily on the Frobenius automorphism that generates unramified Galois groups. We define it as follows:

Definition 3.4. If K is some field, we define ϕ_K to be the element of $\mathrm{Gal}(\widetilde{K}/K)$ such that $d_K(\phi_K) = 1$. We call ϕ_K the Frobenius element over K. This is well defined because $G_{\widetilde{K}}$ is the kernel of d_K, which makes the map $d_K\colon G_K/G_{\widetilde{K}}$ injective.

If L/K is an unramified extension of K, then there is a surjective homomorphism $\Psi\colon \mathrm{Gal}(\widetilde{K}/K) \to \mathrm{Gal}(L/K)$ since $L \subset K$. We then define the Frobenius automorphism $\phi_{L/K}$ to be $\Psi(\phi_K)$.

With all Number Theoretic notions now set in place, we explore a few basic results:

Proposition 3.5. *Some basic results are:*

(1) *If $K \subset L \subset M$, then $f_{M/K} = f_{M/L} f_{L/K}$ and $e_{M/K} = e_{M/L} e_{L/K}$.*
(2) *If L/K is Galois, then the sequence*
$$1 \to I_K/I_L \to \mathrm{Gal}(L/K) \to d(G_K)/d(G_L) \to 1$$
is exact
(3) $[L : K] = f_{L/K} e_{L/K}$
(4) *If f_L and f_K are finite, then $f_{L/K} = f_L/f_K$.*
(5) *With the same assumptions as in the previous proposition, the following diagram commutes*
$$\begin{tikzcd} G_L \arrow[r, "d_L"] \arrow[d, hook] & \widehat{\mathbb{Z}} \arrow[d, "f_{L/K}"] \\ G_K \arrow[r, "d_K"] & \widehat{\mathbb{Z}} \end{tikzcd}$$
where $f_{L/K}$ denotes multiplication by $f_{L/K}$.
(6) *With the same assumptions as above, $\phi_L|_{\widetilde{K}} = \phi_K^{f_{L/K}}$.*

Proof. Below are the proofs of the above propositions:

(1) Follows directly from Lagrange's theorem

(2) Clearly, the sequence $1 \to I_K \to G_K \to d(G_K) \to 1$ is an exact sequence as is the sequence $1 \to I_L \to G_L \to d(G_L) \to 1$. If L/K is Galois, G_L is a normal subgroup of G_K. Therefore, G_K/G_L is well defined and there is a canonical injection $i : I_K/I_L \hookrightarrow G_K/G_L$. Next, define $\tilde{d}\colon G_K/G_L \to d(G_K)/d(G_L)$ by $\tilde{d}([x]) = [d(x)]$. This map is clearly surjective. Moreover, $\tilde{d}[x] = 0$ if and only if $d(x) \in d(G_L)$. Now, $d(x) \in d(G_L)$ if and only if $[x] \in \operatorname{Im} i$. This is because if $[y] \in \operatorname{Im} i$, there is some $x \in I_K$ such that $y \in [x] = xG_L$ or $y = xz$ for $z \in G_L$. Hence, $d(y) = d(x) + d(z) = d(z) \in d(G_L)$ and the converse is obvious. This shows that $\tilde{d}[x] = 0$ iff $[x] \in \operatorname{Im} i$, or $\ker \tilde{d} = \operatorname{Im} i$ and completes the proof of exactness.

(3) If L/K is Galois, part (2) directly gives the desired result. If L/K is not Galois, let M be the smallest Galois extension containing L and use part (1) along with the fact that M/L is Galois.

(4) This follows from $(\widehat{\mathbb{Z}}/d(G_L))/(\widehat{\mathbb{Z}}/d(G_K)) \cong d(G_K)/d(G_L)$.

(5) Since $f_{L/K} = f_L/f_K$, we have $f_L/f_K d_L(x) = 1/f_K d(x) = d_K(x)$.

(6) We have $d_L(\phi_L) = 1$ so that $d_K(\phi_L) = f_{L/K} = f_{L/K} d_K(\phi_K) = d_K(\phi_K^{f_{L/K}})$. Thus, $\phi_L^{-1}\phi_K^{f_{L/K}} \in \ker d_K = I_K = G_{\widetilde{K}}$ which proves the desired result.

□

We now fix some field K and some Galois extension L of K. Suppose that f_K is finite. Consider the map $d_K \colon G_K \to \widehat{\mathbb{Z}}$. As we have seen before, this induces a bijection $d_K \colon G_K/I_K \to \widehat{\mathbb{Z}}$. Now, since $L \supset K$, $I_L \subset I_K$ and therefore d_K acts on $G_K/I_L = G_K/G_{\widetilde{L}} = \operatorname{Gal}(\widetilde{L}/K)$. We may therefore define:

Definition 3.6. The frobenius semigroup of $\widetilde{L}$ over K,

$$\operatorname{Frob}(\widetilde{L}/K) := \{\sigma \in \operatorname{Gal}(\widetilde{L}/K) \colon d_K(\sigma) \in \mathbb{N}\}$$

The Frobenius semigroup is important since we construct the reciprocity map by first defining it on the Frobenius semigroup and using this to induce a map on $\operatorname{Gal}(L/K)$.

Proposition 3.7. *If L/K is finite, the canonical map $\Psi\colon \operatorname{Frob}(\widetilde{L}/K) \to \operatorname{Gal}(L/K)$, $\sigma \mapsto \sigma|_L$ is a surjection.*

Proof. Fix $\sigma \in \operatorname{Gal}(L/K)$. We will find $\tilde{\sigma} \in \operatorname{Frob}(\widetilde{L}/K)$ such that $\tilde{\sigma}|_L = \sigma$. Fix some $\phi \in \operatorname{Gal}(\widetilde{L}/K)$ such that $d_K(\phi) = 1$. Therefore, $\phi|_{\widetilde{K}} = \phi_K$ which implies that $\phi|_{L\cap\widetilde{K}} = \phi_K|_{L\cap\widetilde{K}} = \phi_{L\cap\widetilde{K}/K}$. So, the restriction of ϕ to $L \cap \widetilde{K}$ is the frobenius automorphism of $L \cap \widetilde{K}/K$, which shows that it generates $\operatorname{Gal}(L/K)$. Hence, $\sigma|_{L\cap\widetilde{K}} = \phi|^n_{L\cap\widetilde{K}}$ for some positive integer n. If $n = 0$, then σ is 1 and is mapped onto trivially.

Next, we make use of the isomorphism from $\operatorname{Gal}(\widetilde{L}/\widetilde{K}) \to \operatorname{Gal}(L/(L \cap \widetilde{K}))$ that takes $\tau \in \operatorname{Gal}(\widetilde{L}/\widetilde{K})$ and maps it to $\tau|_L$. Now, we know that $\sigma\phi^{-n}_{L\cap\widetilde{K}}$ is 1 and that $\sigma\phi^{-n}|_L \in \operatorname{Gal}(L/K)$. Therefore, $\sigma\phi^{-n} \in \operatorname{Gal}(L/L \cap \widetilde{K})$. Thus, there exists some $\tau \in \operatorname{Gal}(\widetilde{L}/\widetilde{K})$ such that $\tau|_L = \sigma\phi^{-n}|_L$. Now, let $\tilde{\sigma} = \tau\phi^n$. We have $\tau \in \operatorname{Gal}(\widetilde{L}/\widetilde{K}) \subset \operatorname{Gal}(\widetilde{L}/K)$ and $\phi \in \operatorname{Gal}(\widetilde{L}/K)$ so that $\tilde{\sigma} \in \operatorname{Gal}(\widetilde{L}/K)$. Clearly,

$$\tilde{\sigma}|_L = \tau\phi^n|_L = \tau|_L\phi|^n_L = \sigma\phi^{-n}|_L\phi^n|_L = \sigma|_L = \sigma$$

We are left to show that $\tilde{\sigma} \in \mathrm{Frob}(\widetilde{L}/K)$, i.e. that $d_K(\widetilde{\sigma}) \in \mathbb{N}$. We know that $d_K(\tilde{\sigma}) = d_K(\tilde{\sigma}|_{\widetilde{K}})$. But $\tilde{\sigma}|_{\widetilde{K}} = \phi_K^n$. This is because τ fixes $\widetilde{K}$ which implies that $\tau\phi^n|_{\widetilde{K}} = \phi^n|_{\widetilde{K}}$ which is exactly ϕ_K^n. Since n is positive, it follows that $d_K(\tilde{\sigma}) \in \mathbb{N}$ and we are done. □

Proposition 3.8. *If $\sigma \in \mathrm{Frob}(\widetilde{L}/K)$ and M is the fixed field of σ (defined to be the fixed field of the subgroup generated by σ), then: $f_{M/K} = d_K(\sigma)$; $[M : K]$ is finite; $\widetilde{M} = \widetilde{L}$; and $\sigma = \phi_M$.*

Proof. See [1, Chapter IV, Proposition 4.5.] □

3.4. **Abstract Valuation Theory.** When working with local fields, valutions are central. If K is a local field, a valuation v maps K to $\mathbb{R} \cup \{\infty\}$ with $0 \mapsto \infty$. We restrict valuations to $K^\times$ to avoid carrying the infinity case. This is a G-module and hence we define the valuation as a map on G-modules.

Fix a continuous G-module A as before and let $v\colon A^G = A_k \to \widehat{\mathbb{Z}}$ satisfying:

- Let $Z = \mathrm{Im}\, v$. Then, $\mathbb{Z} \subset Z$ and $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$, i.e. the inverse limit of Z/nZ equals that of $\mathbb{Z}/n\mathbb{Z}$.
- $v(N_{K/k}A_K) = f_K Z$ whenever K is finite over k (as before, k is the fixed field of G).

Such a map is called a Henselian valuation. Given the map v, we may define $v_K := \frac{1}{f_K} v \circ N_{K/k}\colon A_K \to \widehat{\mathbb{Z}}$. The following proposition allows us to easily navigate between valuations on different fields:

Proposition 3.9. *If L/K is a finite extension and $a \in A_L$, we have $v_K(N_{L/K}(a)) = f_{L/K} v_L(a)$.*

Proof. We have by definition

$$\begin{aligned} v_K(N_{L/K}(a)) &= \frac{1}{f_K} v(N_{K/k}(N_{L/K}(a))) = \frac{1}{f_K} v(N_{L/k}(a)) \\ &= \frac{f_L}{f_K} \cdot \frac{1}{f_L} v(N_{L/k}(a)) = f_{L/K} v_L(a) \end{aligned}$$

which proves the desired result. □

The following definitions prove important in defining the reciprocity map:

Definition 3.10. We say $u \in A_K$ is a unit of A_K if $v_K(u) = 0$. We say $\pi \in A_K$ is a uniformizer or prime if $v_K(\pi) = 1$. We denote the group of units by U_K.

Now consider any $a \in A_K$ and let $v(a) = n$. Let π be a uniformizer of A_K and let $u = \pi^{-n}a$ so that $v(u) = 0$. Thus, we have $a = \pi^n u$ where π is a uniformizer and u is a unit. In other words, every element of A_K can be expressed as a product of a unit and the power of a uniformizer.

4. Abstract Class Field Theory

In this section, we dive right into stating the Class Field Axiom and proving the local reciprocity theorem assuming it. For a concrete toy model illustrating these ideas, the reader may consult the Appendix on Kummer Theory, where one sees how a statement similar to the Class Field Axiom arises naturally in that setting.

Fix a profinite group G and a G-module A. A Class Field Theory is a pair of maps (d, v) where $d\colon G \to \widehat{\mathbb{Z}}$ is a continuous surjection and v is a Henselian valuation[1, p. 300]. The class field axiom states[1]:

Axiom 4.1. For every cyclic extension L/K,

$$\left|H^0_T(\mathrm{Gal}(L/K), A_L)\right| = [L:K] \quad \text{and} \quad \left|H^{-1}_T(\mathrm{Gal}(L/K), A_L)\right| = 1$$

Our goal in this section is to use this axiom to prove the reciprocity theorem. Once we have done so, local class field theory reduces to proving the axiom for the case when k is a local field and $A = \overline{k}^\times$. We show the reciprocity theorem by explicitly constructing the map. We first construct a map r' on the Frobenius semigroup $\mathrm{Frob}(\widetilde{L}/K)$ and then use the surjection $\mathrm{Frob}(\widetilde{L}/K) \to \mathrm{Gal}(L/K)$ to define $r(\sigma) = r'(\tilde{\sigma})$ where $\tilde{\sigma} \mapsto \sigma$ under the surjection. We will show that r' is multiplicative so that r is a homomorphism. We then proceed to prove that r is a bijection thus proving Theorem 1.1.

Proposition 4.2. *If L/K is an unramified extension where L and K are both finite over k, then $H^i_T(\mathrm{Gal}(L/K), U_L) = 1$ for $i = 0, -1$. Moreover, $H^1_T(\mathrm{Gal}(L/K), A_L)$ is cyclic and generated by any uniformizer L.*

Proof. Let $G = \mathrm{Gal}(L/K)$. Suppose $u \in U_L$. We want to show that $H^{-1}_T(G, U_L)$ is trivial, i.e. whenever $N_{L/K}(u) = 1$ $u = v^\sigma v^{-1} = v^{\sigma - 1}$ for some $v \in U_L$. Since $H^{-1}_T(G, A_L)$ is trivial, we already have $u = a^{\sigma-1}$ for some $\sigma \in G$ and $a \in A_L$. But since L/K is unramified, $\phi_{L/K}$ generates G which implies that $I_G = \langle \sigma - 1\colon \sigma \in G\rangle = \left\langle \phi_{L/K} - 1\right\rangle$. Therefore, we have $u = a^{\phi_{L/K}-1}$. Pick a uniformizer π of A_K. We claim that π is also a uniformizer of A_L. To see this, we have

$$v_K(N_{L/K}(\pi)) = v_K(\pi \cdot \pi^\phi \cdots \pi^{\phi^{n-1}})$$

since $\phi = \phi_{L/K}$ generates G and moreover $\pi \in A_K$ implies that ϕ acts trivially on π and therefore the above product becomes $nv_K(\pi)$ where $n = |G|$. But we have $v_K(N_{L/K}(\pi)) = f_{L/K} v_L(\pi) = nv_L(\pi)$ since $e_{L/K} = 1$ which shows that $v_L(\pi) = v_K(\pi) = 1$. Thus, π is a uniformizer of A_L. Let $v = a\pi^{-m}$ where $m = v(a)$ so that v is a unit with $a = \pi^m v$. We then have $a^{\phi-1} = (\pi^m v)^\phi (\pi^m v)^{-1}$ but ϕ acts trivially on $\pi^m \in A_K$ so that $u = a^{\phi-1} = v^{\phi-1}$. This shows that $H^{-1}_T(G, U_L) = 1$.

Next, we show that if $u \in U_K$, then $u \in N_{L/K}U_L$. Suppose that $u = N_{L/K}(a)$ for some $a \in A_L$. We then have $v_K(u) = v_K(N_{L/K}(a)) = nv_L(a)$ since L/K is unramified. But $v_K(u) = 0$ which implies that $v_L(a) = 0$ so $a \in U_L$. Therefore, we only need to show that $u \in N_{L/K}A_L$. To see this, we observe that $v_K\colon A_K \to Z$ induces a homomorphism $\tilde{v}_K\colon A_K/N_{L/K}A_L \to Z/nZ$ (this is well defined because whenever $x = N_{L/K}(y)$ for some y we have $v_K(x) = nv_L(y) \in nZ$). This homomorphism is surjective since $\tilde{v}_K([\pi_K]) = [1]$ if π_K is a uniformizer and 1 generates $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$. Moreover, by the Class Field Axiom, we have $\left|A_K/N_{L/K}A_L\right| = n$ and since $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$, the image has cardinality n. This implies that v_K is an isomorphism. Now, if $u \in U_K$, $\tilde{v}_K(u) = 0$ which implies that $[u] = 0$, i.e. $u \in N_{L/K}A_L$ and we are done. ∎

As a consequence, if L/K is unramified, then $N_{L/K}U_L = U_K$.

Definition 4.3. Let $K \subset L$. We define the reciprocity map $r'\colon \operatorname{Frob}(\tilde{L}/K) \to A_K/N_{\tilde{L}/K}A_{\tilde{L}}$ to be such that $r'(\sigma) = [N_{M/K}(\pi)]$ where M is the fixed field of σ and π is a uniformizer of M.

Proposition 4.4. *The map r' is well defined*

Proof. We need to show that the value of $N_{M/K}(\pi)$ is independent of the choice of π. Suppose π and π' are both uniformizers of M. We need to show that $N_{M/K}(\pi) \equiv N_{M/K}(\pi') \pmod{N_{\tilde{L}/K}A_{\tilde{L}}}$ or equivalently,

$$N_{M/K}(\pi)/N_{M/K}(\pi') = N_{M/K}(\pi/\pi') \in N_{\tilde{L}/K}A_{\tilde{L}}$$

Clearly, $u = \pi/\pi' \in U_M$. We know that $\widetilde{M} = \widetilde{L}$ so that $\widetilde{L}/M$ is unramified. Therefore, $U_M = N_{\widetilde{L}/M}U_{\widetilde{L}}$ so that $u \in N_{\widetilde{L}/M}U_{\widetilde{L}}$. Hence, there is some $x \in U_{\widetilde{L}}$ such that $u = N_{\widetilde{L}/M}(x)$ which implies $N_{M/K}(u) = N_{M/K}(N_{\widetilde{L}/M}(x)) = N_{\widetilde{L}/K}(x)$ which shows the desired result. □

Next, we focus on showing that r' is multiplicative. Here, we deviate from Neukirch and follow the approach used in [3]. The following two lemmas will prove useful:

Lemma 4.5. *Let $\sigma, \phi \in \operatorname{Frob}(\widetilde{L}/K)$ such that $d_K(\phi) = 1$ and let $n = d_K(\sigma)$. Let M be the fixed field of σ and let $a \in A_M$. Then, $N_{M/K}(a) = N_{\widetilde{L}/\widetilde{K}}(\psi)$ where $\psi = a \cdot a^{\phi} \cdots a^{\phi^{n-1}}$.*

Proof. Let $M' = M \cap \widetilde{K}$ so that M' is unramified. Therefore, $f_{M/K} = f_{M'/K} = n$ and $e_{M'/K} = 1$ so that $[M' : K] = n$. Now, since $\operatorname{Gal}(M'/K)$ is generated by $\phi_{M'/K}$, we get that $N_{M'/K}(x) = x \cdot x^{\phi_{M'/K}} \cdots x^{\phi_{M'/K}^{n-1}}$. Now, by definition, $\phi_{M'/K} = \phi_K|_{M'}$. Moreover, $d_K(\phi) = 1$ implies $\phi|_{\widetilde{K}} = \phi_K$. Thus, $\phi_{M'/K} = \phi|_{M'}$ because $M' \subset \widetilde{K}$. So, whenever $x \in A_{M'}$, we have $N_{M'/K}(x) = x \cdot x^{\phi} \cdots x^{\phi^{n-1}}$.

For any $a \in A_M$, we therefore have

$$N_{M/K}(a) = N_{M'/K}(N_{M/M'}(a)) = N_{M/M'}(a) \cdot N_{M/M'}(a)^{\phi} \cdots N_{M/M'}(a)^{\phi^{n-1}}$$

This looks similar to the desired result except that we want $N_{\widetilde{L}/\widetilde{K}}$ instead of $N_{M/M'}$. However,

$$N_{\widetilde{L}/\widetilde{K}}|_{A_M} = N_{M\cap\widetilde{L}/M\cap\widetilde{K}} = N_{M/M'}$$

since $M \subset \widetilde{L}$. Thus,

$$N_{M/K}(a) = N_{\widetilde{L}/\widetilde{K}}(a) \cdot N_{\widetilde{L}/\widetilde{K}}(a)^{\phi} \cdots N_{\widetilde{L}/\widetilde{K}}(a)^{\phi^{n-1}} = N_{\widetilde{L}/\widetilde{K}}(a \cdots a^{\phi^{n-1}})$$

which shows the desired result □

Lemma 4.6. *Let M/L and L/K be finite with M/K Galois and L/K unramified. If $u \in U_M$ such that $N_{M/L}(u) \in U_K$, then $N_{M/L}(u) \in N_{M/K}U_M$.*

Proof. We use the inflation restriction exact sequence. The following sequence is exact:

$$0 \to H^0_T(G/H, M^H) \xrightarrow{\text{Inf}} H^0_T(G, M) \xrightarrow{\text{Res}} H^0_T(H, M)$$

Letting $G = \operatorname{Gal}(M/K)$ and $H = \operatorname{Gal}(M/L)$, we get the sequence

$$0 \to H^0_T(\operatorname{Gal}(L/K), U_L) \xrightarrow{\text{Inf}} H^0_T(\operatorname{Gal}(M/K), U_M) \xrightarrow{\text{Res}} H^0_T(\operatorname{Gal}(M/L), U_M)$$

Since $H_T^0(G,M) = M^G/N_G M$, the sequence then becomes

$$0 \to U_K/N_{L/K}U_L \xrightarrow{\text{Inf}} U_K/N_{M/K}U_M \xrightarrow{\text{Res}} U_L/N_{M/L}U_M$$

Now, if $v = N_{M/L}(u) \in U_K$, it defines an element $[v] \in U_K/N_{M/K}U_M$. Moreover, $\text{Res}(v) = 0$ since $v \in N_{M/L}U_M$. Therefore $v \in \ker(\text{Res}) = \text{Im}(\text{Inf})$. But since L/K is unramified, $N_{L/K}U_L = U_K$, which shows that $U_K/N_{L/K}U_L$ is trivial. So, the image of Inf is trivial, which shows that $v \in N_{M/K}U_M$ and we are done. □

Proposition 4.7. *The map r' is multiplicative*

Proof. Let $\sigma_1, \sigma_2, \sigma_3 \in \text{Frob}(\widetilde{L}/K)$ such that $\sigma_3 = \sigma_1\sigma_2$. Let M_i be their respective fixed fields and $\pi_i \in M_i$ be uniformizers so that $r'(\sigma_i) = [N_{M_i/K}(\pi_i)] = [\rho_i]$ where $\rho_i = N_{M_i/K}(\pi_i)$. We need to show that $r'(\sigma_3) = r'(\sigma_1)r'(\sigma_2)$. This can be achieved by showing that $\rho_3 \equiv \rho_1\rho_2 \pmod{N_{\widetilde{L}/K}(A_{\widetilde{L}})}$. Equivalently, we need to show that $\rho = \rho_1\rho_2/\rho_3 \in N_{\widetilde{L}/K}A_{\widetilde{L}}$.

Further we observe that $v_K(\rho) = 0$: We have

$$v_K(N_{M_i/K}(\pi_i)) = f_{M_i/K}v_{M_i}(\pi_i) = f_{M_i/K}$$

since π_i is a uniformizer. Since M_i is the fixed field of σ_i, we have $d_K(\sigma_i) = f_{M_i/K}$, which shows that $v_K(\rho_i) = d_K(\sigma_i)$. Hence, $v_K(\rho) = d_K(\sigma_1\sigma_2/\sigma_3) = d_K(1) = 0$ so that $\rho \in U_K$.

Now, each ρ_i is obtained by applying a different norm map, which makes it difficult to use the multiplicativity of the norm. Thus, we transfer to a common field as follows: Let $\phi \in \text{Gal}(\widetilde{L}/K)$ such that $d_K(\phi) = 1$ and let $d_i = d_K(\sigma_i)$. Let $\psi_i = \pi_i\pi_i^{\phi}\cdots\pi_i^{\phi^{d_i-1}}$ so that Lemma 4.5 implies that $\rho_i = N_{M_i/K}(\pi_i) = N_{\widetilde{L}/\widetilde{K}}(\psi_i)$. For the sake of brevity, we will write N without subscript to denote $N_{\widetilde{L}/\widetilde{K}}$. Therefore, $\rho = N(\psi_1)N(\psi_2)/N(\psi_3) = N(\psi_1\psi_2/\psi_3) = N(u)$ where $u = \psi_1\psi_2/\psi_3$. Therefore, it suffices to show that $N(u) \in N_{\widetilde{L}/K}(A_{\widetilde{L}})$. In particular, we will show the stronger statement that $N(u) = N_{\widetilde{L}/K}U_{\tilde{L}}$. This looks like we could apply Lemma 4.6. However, we need to set up M, L and K appropriately so that all extensions are finite, M/K is Galois and L/K is unramified.

We know that $u \in U_{\widetilde{L}}$ since $\rho = N(u) \in U_K$. Now, $\widetilde{L}$ is the union of finite unramified extensions of L. Therefore, there is some finite unramified extension M of L such that $u \in U_M$. Let $L' = M \cap \widetilde{K}$. Thus, upon restricting the norm map to M, we get $N(u) = N_{M/(M\cap\widetilde{K})}(u) = N_{M/L'}(u)$. Here, M/L' and L'/K are both finite with M/K Galois and L'/K unramified over K, since $L' \subset \widetilde{K}$. Moreover,

$$N_{M/L'}(u) = N(u) = N_{M_1/K}(\pi_1)N_{M_2/K}(\pi_2)/N_{M_3/K}(\pi_3)$$

which is in U_K, since each component of the product lies in A_K and $v(N(u)) = 0$.

It follows by Lemma 4.6 that $N(u) = N_{M/L'}(u) \in N_{M/K}U_M \subset N_{\widetilde{L}/K}U_{\widetilde{L}}$, which shows the desired result. □

Note that r' also acts as a map $\text{Frob}(\widetilde{L}/K) \to A_K/N_{L/K}A_L$ since $N_{\widetilde{L}/K}A_{\widetilde{L}} \subset N_{L/K}A_L$.

We now use the map r' to construct a map $r\colon \mathrm{Gal}(L/K) \to A_K/N_{L/K}A_K$. To do so, we use the surjection $\mathrm{Frob}(\tilde{L}/K) \to \mathrm{Gal}(L/K)$. Given $\sigma \in \mathrm{Gal}(L/K)$, let $\tilde{\sigma} \in \mathrm{Frob}(\tilde{L}/K)$ that maps to σ. We then define $r(\sigma) = [N_{M/K}(\pi)]$ where M is the fixed field of $\tilde{\sigma}$ and π is a uniformizer of M. That is, $r(\sigma) = r'(\tilde{\sigma})$ where $r'\colon \mathrm{Frob}(\widetilde{L}/K) \to A_K/N_{L/K}A_L$. This is called the reciprocity map and is often denoted $r_{L/K}$.

Proposition 4.8. *The reciprocity map* $r\colon \mathrm{Gal}(L/K) \to A_K/N_{L/K}A_L$ *is well defined.*

Proof. We need to show that if $\tilde{\sigma}$ and $\tilde{\sigma}'$ are two elements of $\mathrm{Frob}(\widetilde{L}/K)$ that map to σ, then $r'(\widetilde{\sigma}) = r'(\widetilde{\sigma}')$. Let $\tilde{\sigma}' = \tilde{\sigma}\tilde{\tau}$ where $\tilde{\tau} \in \mathrm{Gal}(\widetilde{L}/K)$. If $d_K(\widetilde{\sigma}') < d_K(\widetilde{\sigma})$, $\widetilde{\tau} \in \mathrm{Frob}(\widetilde{L}/K)$. In this case, we will be done if we can prove that $r'(\tilde{\tau}) = 1$ because $r'(\tilde{\sigma}') = r'(\tilde{\sigma}\tilde{\tau}) = r'(\tilde{\sigma})r'(\tilde{\tau}) = 1$.

Let N be the fixed field of $\tilde{\tau}$ and let π_N be a uniformizer in A_N. Further, since $\tilde{\sigma}$ and $\tilde{\sigma}'$ have the same restriction to L, $\tilde{\tau}|_L = 1$. Thus, N contains L which implies that $A_L \subset A_N$. So, $r'(\tilde{\tau}) = N_{N/K}(\pi_N) = N_{L/K}(N_{N/L}(\pi_N)) \in N_{L/K}A_L$. Hence, $r'(\tilde{\tau}) = 1$ which shows the desired result.

The only case we are now left to consider is the case when $d_K(\tilde{\sigma}) = d_K(\tilde{\sigma}')$. In this case, $\tilde{\tau} \in \ker d_K = G_{\widetilde{K}}$, i.e. $\tilde{\tau}|_{\widetilde{K}} = 1$. We also know that $\tilde{\tau}|_L = 1$. Since $\widetilde{L} = L\widetilde{K}$, it follows that $\tilde{\tau} = 1$ and hence $\tilde{\sigma} = \tilde{\sigma}'$ and we are done. □

Until now, we have showed that r exists and is a homomorphism because r' is multiplicative. In order to show that r induces an isomorphism $\mathrm{Gal}(L/K)^{ab} \to A_K/N_{L/K}A_L$, we will need to simplify to specific cases and show that each case implies the next. In particular, we will need to show that if the theorem holds for the unramified and abelian, cyclic, totally ramified cases, then it also holds for the abelian cyclic case. The following proposition is useful for transitioning between these cases:

Proposition 4.9. *If* L/K *and* L'/K' *are extensions with* $K \subset K'$ *and* $L \subset L'$, *then the diagrams*

$$\begin{array}{ccc} \mathrm{Gal}(L'/K') & \xrightarrow{r_{L'/K'}} & A_{K'}/N_{L'/K'}A_{L'} \\ \downarrow & & \downarrow N_{K'/K} \\ \mathrm{Gal}(L'/K') & \xrightarrow{r_{L'/K'}} & A_{K'}/N_{L'/K'}A_{L'} \end{array} \qquad \begin{array}{ccc} \mathrm{Gal}(L/K)^{ab} & \xrightarrow{r_{L/K}} & A_K/N_{L/K}A_L \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L/K')^{ab} & \xrightarrow{r_{L/K'}} & A_{K'}/N_{L/K'}A_L \end{array}$$

both commute.

Proof. See [1, Chapter IV, Proposition 5.8 and 5.9.] □

We now move on to showing the reciprocity theorem. Recall that it states that $r_{L/K}\colon \mathrm{Gal}(L/K)^{ab} \to A_K/N_{L/K}A_L$ is an isomorphism when L/K is a finite Galois extension. Our approach will be as follows: We first show the result when L/K is unramified. Combining this with the case when L/K is cyclic and totally ramified will show the result for L/K abelian and cyclic. We then drop the cyclic assumption before we finally drop the abelian assumption to complete the proof.

We start by showing that $r_{L/K}$ is an isomorphism when L/K is unramified. Moving forward, we will assume that L/K is finite, Galois.

Proposition 4.10. *If L/K is an unramified extension, r is an isomorphism that takes the frobenius automorphism $\phi = \phi_{L/K}$ to a uniformizer π of K.*

Proof. It will suffice to show that ϕ maps to a uniformizer of K, say π. Once this is known, the map is obviously bijective. This is because $\mathrm{Gal}(L/K)$ and $A_K/N_{L/K}A_L$ have equal order by the class field axiom and a generator ϕ of $\mathrm{Gal}(L/K)$ maps to a generator π of $A_K/N_{L/K}A_L = H_T^0(\mathrm{Gal}(L/K), A_L)$.

Let $\phi_K \in \mathrm{Gal}(\widetilde{K}/K)$ such that $\phi_K|_L = \phi$. Since $L \subset \widetilde{K}$, it follows that $\widetilde{L} = \widetilde{K}$ so that $\phi_K \in \mathrm{Gal}(\widetilde{L}/K)$ with $\phi_K|_L = \phi$. Therefore, by definition, $r(\phi) = r'(\phi_K)$. Moreover, the fixed field of ϕ_K is K itself since it is the Frobenius element. Thus, $r(\phi) = [N_{K/K}(\pi)] = [\pi]$ where π is some uniformizer of K. $\square$

Now, we assume that L/K is abelian, cyclic and totally ramified. We prove the theorem for this case.

Proposition 4.11. *The reciprocity theorem holds when L/K is abelian, cyclic and totally ramified*

Proof. We will show that the map is injective. Bijectivity will then follow naturally since the domain and range have equal group order. Since $\mathrm{Gal}(L/K)$ is cyclic, let σ be a generator. If $\mathrm{Gal}(L/K)$ has order n, then we only need to show that whenever $r(\sigma^k) = 1$ for $0 \leq k < n$, we have $k = 0$. The most natural way to show this would be to show that $n \mid k$ and this would force $k = 0$ if $0 \leq k < n$. We need some setup before moving to this step. To start off, suppose that σ is a generator and k is such that $r(\sigma^k) = 1$.

Recall the definition of $r(\sigma)$. We choose some $\tilde{\sigma} \in \mathrm{Frob}(\widetilde{L}/K)$ that lifts σ. Since L/K is totally ramified, we can choose $\tilde{\sigma}$ such that its fixed field M is totally ramified over K. We will prove this later. However, the reason this choice of M is important is as follows: Let F be a finite subextension of $\widetilde{L}/K$ that contains both M and L and let $F' = F \cap \widetilde{K}$. Then, it is easy to see that $N_{F/F'}|_{A_M} = N_{M/K}$ and also that $N_{F/F'}|_{A_L} = N_{L/K}$ since L is totally ramified. The former is because $M \cap F = M$ and $M \cap F' = M \cap F \cap \widetilde{K} = M \cap \widetilde{K}$ which equals K since M is totally ramified.

Moreover, F/F' is cyclic with degree n because it is isomorphic to $\mathrm{Gal}(L/K)$. To see why, note that $d(G_{F'})/d(G_F) = 1$ since F/F' is totally ramified. Therefore, the sequence $1 \to I_{F'}/I_F \to G_{F'}/G_F \to 1$ is exact, which shows that $I_{F'}/I_F \cong G_{F'}/G_F$. So, $G_{F'}/G_F \cong G_{\widetilde{F'}/\widetilde{F}}/G_{\widetilde{F}} = G_{\widetilde{K}}/G_{\widetilde{L}} \cong G_K/G_L$.

Let π_M and π_L be uniformizers of M and L respectively so that they are both uniformizers of F (since it contains both M and L). So, there is some $u \in U_F$ such that $\pi_M^k = u\pi_L^k$. Now, by definition $r(\sigma^k) = [N_{M/K}(\pi_M^k)] = [N_{F/F'}(\pi_M^k)]$ since $\pi_M \in A_M$ which can then further be expanded as

$$r(\sigma^k) = [N_{F/F'}(u\pi_L^k)] = [N_{F/F'}(u)][N_{F/F'}(\pi_L)]^k$$

However, $\pi_L \in A_L$ implies $N_{F/F'}(\pi_L) = N_{L/K}(\pi_L) \in N_{L/K}A_L$ and therefore $[N_{F/F'}(\pi_L)]^k = [1]$. Hence, $r(\sigma^k) = [N_{F/F'}(u)]$. Since we are assuming $r(\sigma^k) = 1$, it follows that $N_{F/F'}(u) \in N_{L/K}A_L$. In particular, since u is a unit, $N_{F/F'} \in N_{L/K}U_L$ so that $N_{F/F'}(u) = N_{L/K}(v)$ for some $v \in U_L$. But if $v \in U_L$, we have $N_{L/K}(v) = N_{F/F'}(v)$. Hence, $N_{F/F'}(u^{-1}v) = 1$.

Since F/F' is a finite, cyclic extension generated by the same generator σ, we have $H_T^{-1}(\mathrm{Gal}(F/F'), A_F) = 1$. In other words, every element of $\ker N_{F/F'}$ may be written as $a^\tau a^{-1}$ for some $a \in A_F$ and $\tau \in \mathrm{Gal}(F/F')$, which is in turn a power of σ. Therefore, every element of the kernel may be written as $a^\sigma a^{-1}$ for some $a \in A_F$. Since $N_{F/F'}(u^{-1}v) = 1$, it follows that $u^{-1}v = a^\sigma a^{-1}$ for some $a \in A_F$. So, we have $\pi_L^k v = \pi_F^k u^{-1} v = \pi_F^k a^{\sigma - 1}$. Now, since $\tilde{\sigma}|_L = \sigma$, we have

$$(\pi_L^k v)^{\sigma-1} = (\pi_L^k v)^{\tilde{\sigma}-1} = (\pi_F^k a^{\sigma-1})^{\tilde{\sigma}-1}$$

Since $\pi_F \in A_F$ and $\tilde{\sigma} \in G_F$ we have $\pi_F^{\tilde{\sigma}} = \pi_F$ so that

$$(\pi_L^k v)^{\sigma-1} = (a^{\sigma-1})^{\tilde{\sigma}-1} = (a^{\tilde{\sigma}-1})^{\sigma-1}$$

Let $x = \pi_L^k v a^{1-\tilde{\sigma}}$. Then, $x^\sigma = x$ and hence $x \in A_{F'}$. Now, we have

$$f_{F/F'} v_F(x) = v_{F'}(N_{F/F'}(x)) = v_{F'}(x \cdot x^\sigma \cdots x^{\sigma^{n-1}}) = \sum_{i=0}^{n-1} v_{F'}(x^{\sigma^i})$$

However, $x^\sigma = x$ and so $x^{\sigma^i} = x$ which shows that $f_{F/F'} v_F(x) = n v_{F'}(x)$. But F/F' is totally ramified, which implies that $v_F(x) = n v_{F'}(x)$.

Now, $v_F(x) = v_F(\pi_L^k v a^{1-\tilde{\sigma}}) = k + v_F(v) + v_F(a^{1-\tilde{\sigma}})$. Clearly v is a unit and $a^{1-\sigma} = u^{-1}v$ is also a unit. Therefore, both terms cancel out and we get $v_F(x) = k$. Therefore, $n v_{F'}(x) = k$ which shows that $n \mid k$ and we are done.

We are left to show that there exists some $\tilde{\sigma} \in \mathrm{Gal}(\widetilde{L}/K)$ with fixed field totally ramified over K. We make use of the isomorphism $\mathrm{Gal}(\widetilde{L}/\widetilde{K}) \to \mathrm{Gal}(L/K)$. One can see this by plugging in $d(G_K)/d(G_L) = 1$ in the exact sequence $1 \to I_K/I_L \to \mathrm{Gal}(L/K) \to d(G_K)/d(G_L) \to 1$. We have $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Gal}(\widetilde{L}/\widetilde{K}) \subset \mathrm{Gal}(\widetilde{L}/K)$ and also $\phi_L \in \mathrm{Gal}(\widetilde{L}/L) \subset \mathrm{Gal}(\widetilde{L}/K)$. Therefore, $\tilde{\sigma} = \sigma\phi_L \in \mathrm{Gal}(\widetilde{L}/K)$ and we clearly have $(\sigma\phi_L)|_L = \sigma_L = \sigma$. Therefore, $\tilde{\sigma}$ lifts σ. We will show that the fixed field M of $\tilde{\sigma}$ satisfies the desired property. Note that $d_K(\tilde{\sigma}) = d_K(\sigma\phi_L) = d_K(\phi_L)$ since $d_K(\sigma) = 0$ because $\sigma \in G_{\widetilde{K}} = I_K$. But $d_K(\phi_L) = f_{L/K} = 1$. If M is the fixed field of $\tilde{\sigma}$, then $f_{M/K} = d_K(\tilde{\sigma}) = 1$. Therefore, M/K is unramified and we are done. ∎

Next, we drop the totally ramified assumption and prove the theorem when L/K is abelian and cyclic.

Proposition 4.12. *The reciprocity theorem holds when L/K is abelian and cyclic.*

Proof. As before, we are done if L/K is unramified. Otherwise, let M be the maximal unramified subextension of K. We then have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Gal}(L/M) \arrow[r, "r_{L/M}"] \arrow[d, hook] & A_M/N_{L/M}A_L \arrow[d, "N_{M/K}"] \\
\mathrm{Gal}(L/K) \arrow[r, "r_{L/K}"] & A_K/N_{L/K}A_L
\end{tikzcd}$$

We know $r_{L/M}$ is an isomorphism since M is unramified. Now, by the class field axiom, since L/K is finite and cyclic, $\left|A_K/N_{L/K}A_L\right| = [L : K]$ and similarly $\left|A_M/N_{L/M}A_L\right| = [L : M] < [L : K]$. Therefore, $N_{M/K}$ must be injective and since the diagram commutes $r_{L/K}$ must be injective. The fact that $\left|(A_K/N_{L/K}A_L)\right| = |\mathrm{Gal}(L/K)|$ then shows that $r_{L/K}$ is a bijection. □

Next, we drop the cyclic assumption

Proposition 4.13. *The reciprocity theorem holds when L/K is abelian.*

Proof. Suppose M is a cyclic subextension of L. Since the map $r_{M/K}$ is an isomorphism, the commutative diagram shows that $\ker r_{L/K}$ is a subset of the kernel of the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. This holds for every cyclic subextension M, i.e. $\ker r_{L/K}$ lies in the intersection of all cyclic normal subgroups of $\mathrm{Gal}(L/K)$ (the kernel of the map from $G \to H$ corresponds to the coset of 0 which is H itself). If L/K is abelian, the trivial group is cyclic and normal which shows that $\ker r_{L/K}$ is trivial. We are left to show surjectivity.

To show surjectivity, we use induction on $n = [L : K]$. The base case is obvious. If n is prime, then L/K is cyclic and we are done. Otherwise, there exists some cyclic subextension $M \subset L$ with degree less than n. Hence, by our inductive hypothesis, $r_{L/M}$ is an isomorphism as is $r_{M/K}$. Since $r_{L/M}$ is injective so is $N_{M/K} \colon A_M/N_{L/M}A_L \to A_k/N_{L/K}A_L$. We therefore obtain the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(L/M) \arrow[r, hook] \arrow[d, hook, two heads, "r_{L/M}"] & \mathrm{Gal}(L/K) \arrow[r, two heads] \arrow[d, hook, two heads, "r_{L/K}"] & \mathrm{Gal}(M/K) \arrow[r] \arrow[d, hook, two heads, "r_{M/K}"] & 1 \\
& A_M/N_{L/M}A_L \arrow[r, hook] & A_K/N_{L/K}A_L \arrow[r, two heads] & A_K/N_{M/K}A_M \arrow[r] & 1
\end{tikzcd}$$

where the rows are exact. Since $r_{L/M}$ and $r_{M/K}$ are known to be isomorphisms, we may redraw the diagram as

$$\begin{tikzcd}
& \mathrm{Gal}(L/K) \arrow[dr, two heads, "s_1"] \arrow[dd, hook, "r_{L/K}"] & \\
X \arrow[ur, hook, "i_1"] \arrow[dr, hook, "i_2"'] & & Y \\
& A_K/N_{L/K}A_L \arrow[ur, two heads, "s_2"'] &
\end{tikzcd}$$

where X is isomorphic to $\mathrm{Gal}(L/M)$ and Y isomorphic to $\mathrm{Gal}(M/K)$. Suppose $x \in A_K/N_{L/K}A_L$. We aim to show that $x \in \mathrm{Im}\, r_{L/K}$. Let $y = s_2(x)$ and let $z \in \mathrm{Gal}(L/K)$ such that $s_1(z) = y$. Let $x' = r_{L/K}(z) \in \mathrm{Im}\, r_{L/K}$. Then clearly $s_2(x) = s_2(x')$ and therefore $s_2(x'x^{-1}) = 1$, i.e $x'x^{-1} \in \ker s_2$. Since the bottom sequence is exact, it follows that $x'x^{-1} \in \mathrm{Im}\, i_2$ which implies that $x'x^{-1} \in \mathrm{Im}\, r_{L/K}$

because the left triangle commutes. Thus $x' \in \operatorname{Im} r_{L/K}$ then implies that $x \in \operatorname{Im} r_{L/K}$. This shows that $r_{L/K}$ is surjective and completes the proof. $\square$

Proposition 4.14. *If L/K is finite and Galois, the reciprocity map $r_{L/K}\colon \operatorname{Gal}(L/K) \to A_K/N_{L/K}A_L$ induces an injective map $r_{L/K}\colon \operatorname{Gal}(L/K)^{ab} \to A_K/N_{L/K}A_L$.*

Proof. Let $G = \operatorname{Gal}(L/K)$ and let $H = A_K/N_{L/K}A_L$. Since $r_{L/K}$ is a homomorphism, the commutator subgroup $[G,G]$ gets mapped to $[H,H]$. However, since H is abelian, its commutator subgroup is trivial, which implies that $[G,G] \subset \ker r_{L/K}$. This shows that the induced map $r_{L/K}\colon \operatorname{Gal}(L/K)^{ab} \to A_K/N_{L/K}A_L$ is well defined. To show injectivity, let M be the maximal abelian subextension of L/K. Then, $\operatorname{Gal}(M/K) \cong \operatorname{Gal}(L/K)^{ab}$. We use the following commutative diagram:

$$\begin{tikzcd}
\operatorname{Gal}(L/K)^{ab} \arrow[r, "r_{L/K}"] \arrow[d] & A_K/N_{L/K}A_L \arrow[d] \\
\operatorname{Gal}(M/K) \arrow[r, "r_{M/K}"] & A_K/N_{M/K}A_M
\end{tikzcd}$$

Since $\operatorname{Gal}(L/K)^{ab} \cong \operatorname{Gal}(M/K)$ and $\operatorname{Gal}(M/K) \cong A_K/N_{M/K}A_M$ (since M is abelian), it follows that $r_{L/K}$ must be injective. $\square$

Finally, we show that $r_{L/K}\colon \operatorname{Gal}(L/K) \to A_K/N_{L/K}A_L$ is surjective to complete the proof of the theorem. Note that showing this will automatically show that the induced map $\operatorname{Gal}(L/K)^{ab} \to A_K/N_{L/K}A_L$ is also surjective. We restate Theorem 1.1 for reference:

Theorem 4.15. *Assume the class field axiom. If L/K is a finite Galois extension, there is an isomorphism $r_{L/K}\colon \operatorname{Gal}(L/K)^{ab} \to A_K/N_{L/K}A_L$.*

Proof. First, we assume $\operatorname{Gal}(L/K)$ is solvable and use induction on $n = [L:K]$. Once again, the base case is obvious. Now, since $G = \operatorname{Gal}(L/K)$ is solvable, the commutator subgroup $H = [G,G]$ is a strict subset of G. Therefore, $M = \mathfrak{F}(H) \cap L$ cannot be K, which implies that either $M = L$ or M is a proper intermediate extension in which case we have $[L:M] < [L:K]$ which shows that $r_{L/M}$ is surjective and hence an isomorphism. This leads to the commutative diagram resembling that in proposition 4.14 and by following the same steps, we may prove that $r_{L/K}$ is surjective. If $M = L$, L/K is abelian and we are done. Thus, the theorem is true in the solvable case.

Next, the general case. We use induction again with the result being obvious for the base case. Suppose it holds whenever $[L:K] < n$ for some n. We aim to show that $r_{L/K}$ is surjective for $[L:K] = n$. We do so by showing that for every prime $p \mid \left|A_K/N_{L/K}A_L\right|$, S_p is contained in the image of $r_{L/K}$ where S_p denotes the p-Sylow subgroup and p is a prime. Fix a prime p and let M be the fixed field of the p-Sylow subgroup of $\operatorname{Gal}(L/K)$. Now, since S_p is a proper subgroup of $\operatorname{Gal}(L/K)$, which implies that M properly contains K and hence $[L:M] < n$. Therefore $r_{L/M}$ is surjective. Therefore, if we show that S_p is contained in the image of $N_{M/K}$ we will be done since the diagram as in Proposition 4.9 commutes. To this end, let $i\colon A_K/N_{L/K}A_L \to A_M/N_{L/M}A_L$ be the canonical injection so that $N_{M/K}(i(x)) = x^{\sigma_1} \cdots x^{\sigma_{[M:K]}} = x^{[M:K]}$ since $i(x) \in A_K$ is fixed by σ_i. Now, by definition of the p-Sylow subgroup, $[M : K]$ is coprime with p. Thus, $N_{M/K} \circ i$ is a surjection from S_p to itself. This shows that $S_p \subset \operatorname{Im} N_{M/K}$ and we are done. □

This completes the proof of Theorem 1.1 assuming the Class Field Axiom.

5. Local Class Field Theory

Now that we have completed the proof of Theorem 1.1 assuming the Class Field Axiom, we verify the axiom in the local case. We begin by reviewing local fields. See [8, Chapter 7] for a full treatment.

Definition 5.1. A discrete valuation on a field K is a map $v\colon K \to \mathbb{Z} \cup \{\infty\}$ satisfying $v(xy) = v(x) + v(y)$, $v(x) = \infty$ iff $x = 0$ and $v(x + y) \geq \min\{v(x), v(y)\}$.

We say that K is a discrete valuation field if it has a non-trivial discrete valuation. We define ring $\mathcal{O}_K := \{x \in K : v(x) \geq 0\}$. This ring is a discrete valuation ring, which means it is a principal ideal domain that has exactly one nonzero prime ideal. We denote this ideal by $\mathfrak{p}_K$. We define the residue class field of K as $\kappa = \mathcal{O}_K/\mathfrak{p}_L$. The discrete valuation induces a metric on K via an absolute value given by $|x|_v = q^{-v(x)}$ where $q > 1$ is some fixed real number.

Definition 5.2. A local field is a discrete valuation field that is complete with respect to the metric induced by its valuation and has finite residue class field.

Example 5.3. Fix a prime p and let v_p be the function which takes n to the highest power of p in the prime factorization of n when n is an integer. We can extend this definition to $\mathbb{Q}$ by letting $v_p(1/n) = -v_p(n)$. Thus, v_p defines a valuation on $\mathbb{Q}$ called the p-adic valuation. This induces a metric given by $\|x\|_p = p^{-v_p(x)}$. The p-adic number field $\mathbb{Q}_p$ is then defined as the completion of $\mathbb{Q}$ with respect to this metric. We can then extend the definition of v_p to $\mathbb{Q}_p$ so that we get a metric on $\mathbb{Q}_p$ given by the same formula. It turns out that $\mathbb{Q}_p$ is complete with respect to this metric and is therefore a local field. The p-adic valuation also has the property that $v_p(x + y) = \min\{v_p(x), v_p(y)\}$ when $x \neq y$. This is called the ultrametric property.

In fact, every local field is either p-adic for some prime p or the field $\mathbb{F}_q((T))$ of formal Laurent series in T over the finite field $\mathbb{F}_q$. Moving forward, we will assume that the field we are working with is $\mathbb{Q}_p$ for some prime p, though everything done can be easily generalized to all local fields.

The main goal of this section is to prove the reciprocity theorem for local fields. To this end, we first set up the local Class Field Theory by fixing a profinite group G, fixing a G-module A and defining maps d and a Henselian valuation v.

Let k be a local field. Fix $G = \operatorname{Gal}(\overline{k}/k)$ where $\overline{k}$ denotes the separable closure of k. Let A be the G-module $k^\times$. If k is a local field, then $\operatorname{Gal}(\overline{\kappa}/\kappa)$ is isomorphic to $\widehat{\mathbb{Z}}$ so that there is a surjection $d\colon G \to \widehat{\mathbb{Z}}$ (See [1] Ch II Proposition 9.9). Next, since v is a homomorphism on $k^\times$, $v(k^\times) = m\mathbb{Z}$ for some m. So, we can define $v_k\colon k^\times \to \mathbb{Z}$ to take $x \mapsto v(x)/m$ so that v_k is surjective onto $\mathbb{Z}$. If $Z = \operatorname{Im} v_k$ we clearly have $\mathbb{Z} \subset Z$ and $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$ for all n. Moreover, by [1] Ch II Proposition 4.8, v_k satisfies $v_k(N_{K/k}k^\times) = f_K\mathbb{Z}$ for any K is finite over K. Thus, v_k is a Henselian valuation. We may therefore apply the results of Abstract Class Field Theory. We now prove the class field axiom using the approach in [4].

Theorem 5.4. *If $k = \mathbb{Q}_p$ is a local field with v, d and A as above, then for any finite cyclic extension L/K, we have $\left|H_T^{-1}(G, L^\times)\right| = 1$ and $\left|H_T^0(G, L^\times)\right| = [L : K]$, where $G = \mathrm{Gal}(L/K)$ (not to be confused with $\mathrm{Gal}(\bar{k}/k)$).*

Proof. The fact that $H_T^{-1}(G, L^\times) = 1$ follows from Hilbert's Theorem 90 (see appendix) along with the fact that $H_T^1 = H_T^{-1}$ for cyclic groups. We are left to show that $\left|H_T^0(G, L^\times)\right| = [L : K]$. The method we will use to show this will be to show that the Herbrand quotient $h(L^\times) = [L : K]$, which along with the fact that $H_T^{-1}(G, L^\times)$ yields the desired result. We further simplify by noting that the sequence $1 \to U_L \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$ is exact so that $h(L^\times) = h(U_L)h(\mathbb{Z})$. Since we are considering $\mathbb{Z}$ as a G-module with trivial action, $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/[L : K]\mathbb{Z}$ and $H_T^{-1}(G, \mathbb{Z}) = 0$ since $a^g - a = 0$ for all $g \in G, a \in \mathbb{Z}$. Thus, $h(\mathbb{Z}) = [L : K]$ and it now suffices to show that $h(U_L) = 1$. We will further reduce the problem by finding $W \subset U_L$ with finite index such that $h(W) = 1$. Then, $h(U_L) = h(U_L/W)h(W) = h(W) = 1$ by Proposition 2.7. We find W as follows.

First, consider $\mathcal{O}_K$ as an additive G-module. By the normal basis theorem, there is a basis of L as a vector space over K of the form $\{\alpha^\sigma : \sigma \in G\}$ where $\alpha \in \mathcal{O}_K$ (we can scale α so that it lies in $\mathcal{O}_K$). We then let $V = \sum_{\sigma \in G} \alpha^\sigma \mathcal{O}_K \subset \mathcal{O}_L$. Note that we can choose α with valuation as large as we want by simply multiplying by the required power of p. Since $p \in K$, σ fixes p and the sum is unchanged. Moreover, $V \cong \mathrm{Ind}_1^G \mathcal{O}_K$ via the isomorphism that takes $f \colon G \to \mathcal{O}_K$ to $\sum a^\sigma f(\sigma)$. This tells us by Shapiro's Lemma and its extension to H_T^0 (Proposition 2.6) that $H_T^i(G, V) = 0$ so that $h(V) = 0$, where V is viewed as an additive G-module. However, we need $W \subset U_L$ to be multiplicative. We therefore try to convert V to a multiplicative module via an isomorphism that preserves H_T^i. This will give us our desired module W.

The most natural way to convert addition to multiplication is using exponentiation $\exp(x) = \sum x^k/k!$. This is a formal power series which has radius of convergence $R = p^{-1/(p-1)}$, i.e. the series converges whenever $v_p(x) > 1/(p-1)$. Since we can choose α to have arbitrarily large valuation, we can choose it so that $v_p(\alpha) > 1/(p-1)$, which will ensure that $V \subset B_R(0)$ (this denotes the ball of radius R centered at 0). Now, let $W = \exp(V)$. It is easy to see that $\exp \colon V \to W$ is injective since when $x \neq 0$ we have $v_p(x) < \infty$ which implies that $v_p(x^k)$ is a strictly decreasing sequence and hence by the ultrametric property, we have $v_p(\exp(x) - 1) = v_p(x) < \infty$. So, if $x \neq 0$, $\exp(x) \neq 1$. Since exp takes addition to multiplication, W is now a multiplicative G-module with $h(W) = 1$ since it is isomorphic to V. Moreover, $v_p(\exp(x) - 1) = v_p(x) > 1/(p-1) > 0$ implies that $p \mid \exp(x) - 1$, i.e. $\exp(x) = 1 + p\beta \subset \mathcal{O}_L$ where $\beta \in \mathcal{O}_L$. Since 1 is a unit in k, it therefore follows that $\exp(x)$ is also a unit so that $W \subset U_L$.

We are still left to show that U_L/W is finite. This can be seen with some topology. First, note that V is open as follows. Let $r = v_p(\alpha)$ and let $x \in L$ with $v_p(x) = R > r$. We then have $x = p^R u$ where u is a unit. Since u is a unit, $u \in V$ and since $R > r$, $p^R \in V$ and hence $x \in V$. Therefore, $B_{p^{-R}}(0) \subset V$. We can do this at any point and not just 0 so V is open. This shows that W is open since exp is a homeomorphism (its inverse is the logarithm which is again continuous).

Moreover, U_L is compact since it a closed subset of a compact set $\mathcal{O}_L$. An open subgroup of a compact group has finite index. Therefore, W has finite index in U_L. This shows the desired result. ☐

Appendix: Kummer Theory

We turn to Kummer Theory, which serves as a model case for the abstract approach to Theorem 1.1. Our aim is to prove Theorem 5.5. We give two proofs: first via cohomology, then via an abstract reformulation that isolates the minimal assumptions needed. Following [1, IV.3], we call this the Kummer Theory Axiom. Verifying this axiom recovers Theorem 5.5, analogous to how Neukirch derives the main reciprocity law. This prepares the ground for abstract class field theory. We begin by explaining the theorem of interest.

In most standard treatments, the main goal of Kummer Theory is to prove that there is a correspondence between cyclic Galois extensions of a field K and cyclic subgroups of the multiplicative group $K^\times/(K^\times)^n$ where $(K^\times)^n$ denotes the image power map that takes $x \mapsto x^n$. The set of nth roots of unity, denoted μ_n, is the kernel of this map. Note that n is any integer that is not divisible by the characteristic of K. This is proved as a corollary of the following theorem

Theorem 5.5. *Let L/K be a finite cyclic Galois extension of fields where K is a field that contains the nth roots of unity μ_n where n is some integer not divisible by the characteristic of K. Then, the group $(K^\times \cap (L^\times)^n)/(K^\times)^n$ is isomorphic to $\mathrm{Hom}(G, \mu_n)$, the set of homomorphisms from G to μ_n, where $G = \mathrm{Gal}(L/K)$.*

By taking the projective limit, the above theorem can be extended to infinite field extensions L/K. Then, letting $L = \overline{K}$, we see that $K^\times \cap (\overline{K}^\times)^n = K^\times$. This is because the power map is surjective by virtue of $\overline{K}$ being algebraically closed. Hence, $K^\times/(K^\times)^n \cong \mathrm{Hom}(G, \mu_n)$. With a little more work this can be shown to imply the correspondence between cyclic extensions and cyclic subgroups. The rest of the section will focus on proving Theorem 5.5.

We begin with the cohomological approach by viewing $L^\times$ and $K^\times$ as multiplicative, right G-modules. The following lemma is by Emmy Noether:

Theorem 5.6 (Hilbert's Theorem 90)**.** *If L/K is a finite Galois extension, then $H^1(\mathrm{Gal}(L/K), L^\times)$ is trivial.*

The proof relies on the following lemma

Lemma 5.7. *View L as a vector space over K. Consider the space V of all K-linear maps from L to itself. The space of K-linear maps on L is a vector space over L. The K-fixing automorphisms on L are linearly independent over L in V.*

Proof. Let $\sigma_1, \dots, \sigma_n$ denote the K-fixing automorphisms over L. Suppose that they are not linearly independent. Then, there exists a smallest natural number m such that $a_1\sigma_1 + \cdots + a_m\sigma_m = 0$ where a_i are all nonzero. Then, suppose that

$x_0 \in L$ such that $\sigma_1(x_0) \neq \sigma_2(x_0)$. Let $b_i = (\sigma_1(x_0) - \sigma_i(x_0))a_i$ so that

$$\sum b_i\sigma_i(x) = \sum_{i=2}^{m}(\sigma_1(x_0) - \sigma_i(x_0))a_i\sigma_i(x) = \sum_{i=1}^{m} a_i\sigma_1(x_0)\sigma_i(x_0) - \sum_{i=1}^{m} a_i\sigma_i(x_0)\sigma_i(x)$$
$$= 0 - \sum_{i=1}^{m} a_i\sigma_i(x_0x) = 0$$

for any $x \in L$, since $\sum a_i\sigma_i(x) = 0$ for every $x \in L$. However, this gives us only $m-1$ distinct non-zero coefficients since $b_1 = 0$, contradicting the minimality of m. Thus, σ_i must be linearly independent. □

Proof of Theorem 5.6. Upon explicitly computing $H^1(\mathrm{Gal}(L/K), L^\times)$, we see that this is equal to Z/B where Z the set of maps $f\colon G \to M$ satisfying $f(gh) = f(h)^g f(g)$ and B is the set of maps of the form $f(g) = m^g m^{-1}$. Let $f \in Z$. We know that $G = \mathrm{Gal}(L/K)$ is the set of automorphisms on L fixing K and therefore G as a set of vectors in V is linearly independent. Thus there exists some $x \in L^\times$ such that

$$t = \sum_{\sigma\in G} f(\sigma)\cdot\sigma(x) = \sum_{\sigma\in G} f(\sigma)x^\sigma \neq 0$$

If $\tau \in G$,

$$\tau(t) = \sum_{\sigma\in G} \tau(f(\sigma))\tau(\sigma(x)) = \sum_{\sigma\in G} f(\sigma)^\tau x^{\sigma\tau}$$

Since $f \in \ker d^1$, $f(\sigma)^\tau = f(\tau)^{-1}f(\sigma\tau)$ so that

$$\tau(t) = \sum_{\sigma\in G} f(\tau)^{-1}f(\sigma\tau)x^{\sigma\tau} = f(\tau)^{-1}\sum_{\sigma\in G} f(\sigma\tau)x^{\sigma\tau} = f(\tau)^{-1}t$$

Therefore, we get $f(\tau) = t\tau(t)^{-1} = (t^{-1}t^\tau)^{-1}$ and hence $f \in B$, which shows the desired result. □

Proof of Theorem 5.5. We first start with the short exact sequence

$$1 \to \mu_n \to L^\times \xrightarrow{\mathcal{P}_n} (L^\times)^n \to 1$$

where $\mathcal{P}_n$ denotes the power map. Applying group cohomology to this short exact sequence, we get a long exact sequence

$$1 \to H^0(G,\mu_n) \to H^0(G,L^\times) \to H^0(G,(L^\times)^n) \to H^1(G,\mu_n) \to H^1(G,L^\times) \to \cdots$$

Here, $G = \mathrm{Gal}(L/K)$. However, by Hilbert's Theorem 90, $H^1(G,L^\times) = 1$ so that the sequence terminates at $H^1(G,L^\times)$. We now compute the rest of the terms. We have $H^0(G,M) = M^G$ and $\mu_n \subset K$ so that it is fixed by G. Hence, $\mu_n^G = \mu_n$. Similarly, $H^0(G,L^\times) = (L^\times)^G$ which can be written as $L^G \setminus 0 = K^\times$. Similarly, $H^0(G,(L^\times)^n) = K^\times \cap (L^\times)^n$. We are now left to compute $H^1(G,\mu_n)$.

Write $H^1(G,\mu_n) = Z/B$. Since μ_n is fixed by G, B is trivial. Moreover if $f \in Z$, $f(\sigma)$ is fixed by G so that $f(\sigma\tau) = f(\sigma)f(\tau)^\sigma = f(\sigma)f(\tau)$ which shows that f is a homomorphism. Hence, $H^1(G,\mu_n) \cong \mathrm{Hom}(G,\mu_n)$. We therefore get the exact sequence

$$1 \to \mu_n \to K^\times \xrightarrow{\mathcal{P}_n} K^\times \cap (L^\times)^n \to \mathrm{Hom}(G,\mu_n) \to 1$$

which shows that $\mathrm{Hom}(G,\mu_n) \cong (K^\times \cap (L^\times)^n)/(K^\times)^n$ and we are done. □

To prove the result abstractly, we use the formulation developed in Section 3. We fix a profinite group G and a continuous G-module A, which in the concrete case gives rise to $L^\times$ and $K^\times$.

In addition, the two most important facts in our proof of Theorem 1.1 were $\mu_n \subset K$ and $H^1(G, L^\times) = 1$. Therefore, our abstract formulation must encompass these facts. To this end, fix a surjective homomorphism $\mathcal{P}\colon A \to A$ with finite cyclic kernel $\mu_{\mathcal{P}}$ and fix some field K so that $\mu_{\mathcal{P}} \subset A_K$. This corresponds to the power map that takes a to a^n. The axiom is as follows:

Axiom 5.8. For all finite cyclic extensions L/K, $H^1(\mathrm{Gal}(L/K), A_L)$ is trivial.[1]

Now, to prove Theorem 5.5, we fix a field k and let $G = \mathrm{Gal}(\overline{k}/k)$. We choose $A = \overline{k}^\times$. Fix some integer n and let $\mu_{\mathcal{P}}\colon a \mapsto a^n$. Choose a field $K \supset k$ that contains $\mu_{\mathcal{P}}$. For any finite cyclic extension L of K we then have $H^1(\mathrm{Gal}(L/K), A_L) = H^1(\mathrm{Gal}(L/K), L^\times) = 1$. This gives us everything we need to continue the proof the same way as before. In essence, rather than directly using Hilbert's Theorem 90, we are given the same result as an axiom. For any system in which this axiom is true, Theorem 5.5 holds.

The latter approach illustrates how Neukirch proved Theorem 1.1. If we were to do it from scratch, we would: first set up an abstract formulation and assume the Kummer Theory Axiom. Then, prove Theorem 5.5 assuming this and finally prove the Kummer Theory Axiom itself. The last step is the proof of Theorem 5.6 and the previous step is exactly the same as our concrete proof of Theorem 5.5.

Acknowledgements

I would like to express my gratitude to my mentor, Shubhrajit Bhattacharya, for his constant guidance and support throughout my readings and the preparation of this paper. His explanations and insights provided valuable motivation for many concepts that might otherwise have remained too abstract, and his perspective on related areas helped me appreciate the broader context and stay engaged.

I am also deeply thankful to Professor Peter May for organizing the UChicago Mathematics REU, providing me with the opportunity to pursue my mathematical interests in such a stimulating environment, and for offering valuable feedback on the initial draft of this paper.

References

[1] J. Neukirch, *Algebraic number theory*, translated from the 1992 German original and with a note by Norbert Schappacher, Grundlehren der mathematischen Wissenschaften, 322, Springer, Berlin, 1999; MR1697859

[2] K. S. Brown, *Cohomology of groups*, corrected reprint of the 1982 original, Graduate Texts in Mathematics, 87, Springer, New York, 1994; MR1324339

[3] K. S. Kedlaya, *Notes on Class Field Theory*, AMS Open Math Notes, Works in Progress, Ref.# OMN:201710.110715, last revised 2017-10-24.

[4] K. S. Kedlaya, *Notes on Class Field Theory*, AMS Open Math Notes, Works in Progress, Ref.# OMN:201710.110715, last revised 2021-03-15.

[1] Neukirch uses $H_T^{-1}(\mathrm{Gal}(L/K), A_L) = 1$ but these are equivalent since Tate groups are periodic.

[5] J. S. Milne, *Class Field Theory* (v4.03), 2020, available at `www.jmilne.org/math/`, viii+287 pp.
[6] J.-P. Serre, *Galois cohomology*, translated from the French by Patrick Ion and revised by the author Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer, Berlin, 2002; MR1867431
[7] D. A. Marcus, *Number fields*, second edition of [MR0457396],
[8] J. S. Milne, *Algebraic Number Theory* (v3.08), 2020, p. 166. Available at `www.jmilne.org/math/`.