ARTIN RECIPROCITY

ADAM EARNST

Abstract. Reciprocity laws have long been considered some of the most beautiful results in number theory. These reciprocity laws can be interpreted in terms of finite extensions of number fields. Artin reciprocity generalizes the early reciprocity laws of Gauss, Jacobi, and Eisenstein into a statement that holds for all finite extensions of number fields. This paper presents a proof of Artin reciprocity and discusses its relation to the much more elementary quadratic reciprocity.

Contents

1. Introduction

In 1801, Gauss published the first proof of quadratic reciprocity. This theorem, formally stated in Section 9, asserts that given two odd primes p and q, where at least one is congruent to 1 mod 4, p is a square mod q if and only if q is a square mod p. Fittingly, this theorem uncovers a reciprocal relationship between the behavior of squares mod p and mod q. Following Gauss' proof of quadratic reciprocity, many reciprocity laws of a similar flavor were proved. These include, but are not limited to, cubic reciprocity and biquadratic reciprocity.

A century later, number theorists began laying the grounds for one of the largest projects in the field: class field theory. In essence, this project was designed to study finite abelian extensions of number fields. One particular goal of class field theory was to relate the Galois group of a finite abelian extension L/K to the structure of the field K [3]. This is precisely what the theorem of Artin reciprocity, proved in 1927, accomplished. But why is this goal important? In fact, all of the earlier reciprocity laws can be reframed as a relationship between the splitting of prime ideals in a finite extension of number fields and some modularity condition. As will

be developed in this paper, the Galois group of L/K encodes information about the splitting of prime ideals, and the structure of K, interpreted through generalized ideal class groups, gives a modularity condition.

In this paper, we present a proof of the theorem of Artin reciprocity. Sections 2-4 present an assortment of tools needed to understand and prove Artin reciprocity. These sections are written to convey the necessary propositions and theorems to a reader who has minimal experience in algebraic number theory; if interested, one can consult any of the excellent textbooks cited in these sections to delve deeper into any particular area. Sections 5-8 are devoted to proving Artin reciprocity, following the approach of [5]. Section 8 is much more technical than the others in the paper, so a reader may decide to first skip ahead to Section 9 to see how the cyclotomic case of Artin reciprocity can be used to prove quadratic reciprocity.

2. Algebraic Number Theory Preliminaries

Let K be a number field, i.e. a finite extension of $\mathbb{Q}$. We use $\mathcal{O}_K$ to denote the ring of integers of K, which consists of the elements $a \in K$ that satisfy a monic polynomial $f(x) \in \mathbb{Z}[x]$. We also introduce the concept of a fractional ideal of $\mathcal{O}_K$ in K:

Definition 2.1. A *fractional ideal* $\mathfrak{a}$ of $\mathcal{O}_K$ in K (often just called a fractional ideal of K) is an $\mathcal{O}_K$-module contained in K such that $c\mathfrak{a} \subset \mathcal{O}_K$ for some $c \in K^\times$.

We note that if $\mathfrak{a}$ is a nonzero fractional ideal and $c\mathfrak{a} \subset \mathcal{O}_K$, then $\mathfrak{b} := c\mathfrak{a}$ is an ideal in $\mathcal{O}_K$. The ring of integers of any number field is a Dedekind domain, so ideals factor uniquely into prime ideals. Therefore, we can simplify our description of fractional ideals of K. We have that $\mathfrak{a} = (c)^{-1}\mathfrak{b}$, and by unique factorization of (c) and $\mathfrak{b}$,

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})},$$

where $\mathfrak{p}$ ranges over the prime ideals of $\mathcal{O}_K$, and $a(\mathfrak{p}) \in \mathbb{Z}$, with $a(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$.

Let $K \subset L$ be two number fields, and set $n = [L : K]$. Let $I(\mathcal{O}_K)$ and $I(\mathcal{O}_L)$ be the groups of fractional ideals of K and L, respectively, excluding the zero ideal. Throughout this paper, when we say fractional ideal, or ideal, we exclude the zero ideal in this terminology. There is an injection from $I(\mathcal{O}_K)$ to $I(\mathcal{O}_L)$ defined by sending $\mathfrak{a}$ to $\mathfrak{a}\mathcal{O}_L$. Using this, we can see how prime ideals in $\mathcal{O}_K$ split, or factor, in $\mathcal{O}_L$. By unique factorization of ideals, if $\mathfrak{p}$ is a prime ideal of K, then we can factor the corresponding ideal $\mathfrak{p}\mathcal{O}_L$ of L as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}.$$

Here, the $\mathfrak{P}_i$ represent prime ideals of $\mathcal{O}_L$ and each e_i is a positive integer. The quantity e_i is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$. In this scenario, we often say that $\mathfrak{P}_i$ is a prime ideal lying above $\mathfrak{p}$.

In this context, we can introduce the idea of *residue class fields*. A residue class field is the quotient field formed by quotienting out the ring of integers $\mathcal{O}_K$ of some number field K by a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. For each prime $\mathfrak{P}_i$ lying above $\mathfrak{p}$, we have an induced inclusion of residue fields,

$$\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i.$$

The reader can check that the natural inclusion, induced by the inclusion of rings of integers $\mathcal{O}_K \subset \mathcal{O}_L$, is in fact well-defined because $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$. It can also be verified that the field inclusion is a finite field extension, bounded by $[L : K]$. As a corollary to this fact, we can take $K = \mathbb{Q}$, and let L be an arbitrary number field. If we let p be a prime number, and $\mathfrak{p}$ be a prime ideal of L lying above (p), then the residue class field $\mathcal{O}_L/\mathfrak{p}$ is a finite extension of the finite field $\mathbb{F}_p$. Therefore, all residue class fields are finite fields.

Another important quantity that often appears in tandem with the ramification index e_i is the *residue class degree* of a prime ideal lying above another. We define the *residue class degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$ to be $f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$. A prime ideal $\mathfrak{p}$ is said to split completely if all of the e_i and f_i are equal to 1.

So far, we have a map from $I(\mathcal{O}_K)$ to $I(\mathcal{O}_L)$.We can use the definition of residue class degree to define a map in the other direction, from $I(\mathcal{O}_L)$ to $I(\mathcal{O}_K)$. If $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_L$, then $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. Then, we can define a *norm map* as follows:

Definition 2.2. The *norm map* $N_K^L : I(\mathcal{O}_L) \to I(\mathcal{O}_K)$ is the unique homomorphism induced by $N_K^L(\mathfrak{P}) = \mathfrak{p}^f$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ and $f = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ is the residue class degree of $\mathfrak{P}$ over $\mathfrak{p}$.

We will often use the norm map without the subscript and superscript. In this case, if $\mathfrak{a}$ is a fractional ideal in K, $N\mathfrak{a}$ denotes the norm with respect to $\mathbb{Q}$, that is $N_{\mathbb{Q}}^K(\mathfrak{a})$. As a critical note, the inclusion homomorphism from $I(\mathcal{O}_K)$ to $I(\mathcal{O}_L)$ is not surjective, so it and the norm map are not inverses.

In the case that L/K is a Galois extension, the norm map has an alternative formulation.

Proposition 2.3. *If the extension L/K is Galois, we can equivalently define the norm of a fractional ideal $\mathfrak{a}$ as follows:*

$$N_K^L(\mathfrak{a}) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\mathfrak{a}.$$

The ramification indices and residue class degrees of primes $\mathfrak{P}_i$ above $\mathfrak{p}$ also have important numerical significance, which is laid out in the following proposition:

Proposition 2.4. *Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, where the $\mathfrak{P}_i$ are prime ideals in $\mathcal{O}_L$. Then,*

$$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

Corollary 2.5. *If L/K is Galois, then the e_i are all equal to the same number e and the f_i are all equal to the same number f. Thus, $[L : K] = efg$.*

Now, we focus specifically on Galois extensions L/K. Fix a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. By Corollary 2.5, $\mathfrak{p}$ factors as

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e.$$

Any Galois automorphism $\sigma \in \mathrm{Gal}(L/K)$ permutes the prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ that lie above $\mathfrak{p}$. This group action of $\mathrm{Gal}(L/K)$ on the prime ideals above $\mathfrak{p}$ is in fact transitive. For each ideal $\mathfrak{P}$ lying above $\mathfrak{p}$, we can define a subgroup of the Galois group as follows:

Definition 2.6. The *decomposition group* of $\mathfrak{P}$ is the subgroup of $\mathrm{Gal}(L/K)$ given by $G_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\mathfrak{P} = \mathfrak{P}\}$.

If $\sigma \in G_{\mathfrak{P}}$, then σ induces an automorphism of $\mathcal{O}_L/\mathfrak{P}$ that fixes $\mathcal{O}_K/\mathfrak{p}$. This gives us a homomorphism from the decomposition group $G_{\mathfrak{P}}$ to the Galois group of the residue class field extension $\overline{G}_{\mathfrak{P}} := \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. The residue class field extension is Galois because both fields are finite. We call the kernel of this homomorphism, $T_{\mathfrak{P}}$, the *inertia group* of $\mathfrak{P}$. This homomorphism is in fact surjective, and a thorough proof can be found in [6].

By the orbit-stabilizer theorem, $|G_{\mathfrak{P}}| = n/g$. Additionally, $|\overline{G}_{\mathfrak{P}}| = f$. By the first isomorphism theorem and Corollary 2.5, we have that $|T_{\mathfrak{P}}| = e$. Therefore, if $\mathfrak{p}$ is *unramified* in L, meaning that the common ramification index of all $\mathfrak{P}_i$ above $\mathfrak{p}$ is $e = 1$, the map from $G_{\mathfrak{P}}$ to $\overline{G}_{\mathfrak{P}}$ is an isomorphism. Thus, there is a unique element of $G_{\mathfrak{P}}$ that maps to the Frobenius element of $\overline{G}_{\mathfrak{P}}$. In the case that L/K is abelian, meaning that its Galois group is abelian, $G_{\mathfrak{P}}$ and the aforementioned unique element of $G_{\mathfrak{P}}$ are independent of the choice of prime $\mathfrak{P}$ above $\mathfrak{p}$.

Now, we define a tool that is incredibly useful for computation, the *discriminant*. Suppose that $\alpha_1, \ldots, \alpha_n$ is a field basis for L over K. Then, we can define the discriminant of this basis.

Definition 2.7. The discriminant of the basis $\alpha_1, \ldots, \alpha_n$ of the extension of number fields L/K is given by the following matrix determinant:

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{tr}_{L/K}\, \alpha_i\alpha_j).$$

There are many helpful tricks that can be used to calculate the discriminants of certain bases. We will state one that will be useful for our purposes.

Proposition 2.8. *Suppose that $L = K(\alpha)$. Then, if $n = [L : K]$, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a basis for L over K. Let $f(x) \in K[x]$ be the minimal polynomial of α. Then,*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N(f'(\alpha))$$

Proof. A proof of this proposition, along with other propositions related to discriminant calculations, is given in [4]. □

The idea of a discriminant can be made independent of the choice of basis.

Definition 2.9. The discriminant of L/K is the ideal in $\mathcal{O}_K$ generated by the discriminants of all field bases of L/K which are contained in $\mathcal{O}_L$.

For clarity, we will use the term "discriminant" to refer to the ideal described in Definition 2.9. We will use the exact wording "discriminant of a basis" if we need to refer to the number discriminant as described in Definition 2.7.

The discriminant of an extension of number fields encodes a great amount of information about the extension itself. One particularly useful fact relates the discriminant to ramified primes.

Theorem 2.10. *A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ ramifies in L if and only if it divides the discriminant of L/K.*

Proof. A full proof of this theorem is provided in [7]. □

Due to the prime factorization of ideals, this theorem has an immediate corollary.

Corollary 2.11. *Only finitely many primes of $\mathcal{O}_K$ ramify in $\mathcal{O}_L$.*

3. Local Fields

The main theorem of this paper, Artin reciprocity, is a statement concerning number fields, which are examples of *global fields*. However, to understand the class field theory of global fields, one must also understand the theory of *local fields*. The completion of a number field K with respect to an absolute value on K is an example of a local field, and this is the only type of local field that we will consider in this paper. To formalize this, we first introduce the definition of an absolute value on K.

Definition 3.1. An *absolute value* on K is a function $|\cdot|_v$ from K to the nonnegative real numbers satisfying the following properties:

(i) $|x|_v = 0$ if and only if $x = 0$.
(ii) For all $x, y \in K$, $|xy|_v = |x|_v|y|_v$.
(iii) For all $x, y \in K$, $|x + y|_v \leq |x|_v + |y|_v$.

The simplest way to define an absolute value on K is by embedding the number field in either the real or complex numbers. Such absolute values are called *archimedean*. Furthermore, if the absolute value is induced by an embedding in $\mathbb{R}$, we say that it is *real archimedean*. If the absolute value is induced by an embedding in $\mathbb{C}$ whose image is not contained in $\mathbb{R}$, we say that it is *complex archimedean*. As an example of an archimedean absolute value, in $\mathbb{Q}(i)$, embedding in the complex numbers gives the absolute value $|a + bi| = \sqrt{a^2 + b^2}$. However, we can also introduce some non-trivial absolute values corresponding to the prime ideals of $\mathcal{O}_K$. Fix a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. For an element $a \in \mathcal{O}_K$, we define the order of a at $\mathfrak{p}$ to be the unique nonnegative integer i such that $a \in \mathfrak{p}^i$ but $a \notin \mathfrak{p}^{i+1}$ (here, $\mathfrak{p}^0$ is taken to be $\mathcal{O}_K$). We denote this by $i = \mathrm{ord}_{\mathfrak{p}}(a)$. This notion of order can be extended to K by expressing any element $a \in K$ as $a = b/c$, where $b, c \in \mathcal{O}_K$. We then take $\mathrm{ord}_{\mathfrak{p}}(a) = \mathrm{ord}_{\mathfrak{p}}(b) - \mathrm{ord}_{\mathfrak{p}}(c)$. Take $(p) = \mathfrak{p} \cap \mathbb{Q}$. Let e be the ramification index of $\mathfrak{p}$ over p. Then, we get the following absolute value:

$$|a|_{\mathfrak{p}} = \frac{1}{p^{\mathrm{ord}_{\mathfrak{p}}(a)/e}}.$$

We call $|\cdot|_{\mathfrak{p}}$ a $\mathfrak{p}$-*adic absolute value*. Alternatively, the $\mathfrak{p}$-adic absolute values are often called *non-archimedean*. If $K = \mathbb{Q}$, the absolute value corresponding to (p) is precisely the p-adic absolute value. Suppose L/K is a finite extension of number fields, and $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$, a prime ideal of $\mathcal{O}_K$. Then, the absolute value $|\cdot|_{\mathfrak{P}}$ agrees with $|\cdot|_{\mathfrak{p}}$ on K.

We will denote the set of these $\mathfrak{p}$-adic absolute values and the archimedean absolute values induced by an embedding in $\mathbb{R}$ or $\mathbb{C}$ by M_K. We call this the set of *canonical absolute values*. Surprisingly, these are the only possible absolute values on K, up to exponentiation by a constant. A proof of this fact is given in [2].

We obtain local fields by constructing the completion of a number field K with respect to one of its canonical absolute values v. For $K = \mathbb{Q}$, this is a familiar concept, at least for the archimedean absolute value on $\mathbb{Q}$, which corresponds to Euclidean distance. In this case, we construct $\mathbb{R}$ by taking the ring of all Cauchy sequences in $\mathbb{Q}$, and quotienting out by all Cauchy sequences which converge to 1. We can do the same for the non-archimedean absolute values of $\mathbb{Q}$, where convergence is interpreted using these new absolute values, and this construction yields the p-adic numbers $\mathbb{Q}_p$. This construction can be done for any number field K and

any absolute value v. We denote this new field by K_v, and call it the completion of K with respect to v.

Local fields are an incredibly useful tool that will be used to prove Artin reciprocity. Much of this is because of the convenient algebraic and topological properties of these fields. Let K be a number field and v a non-archimedean absolute value. We then consider the local field K_v. We define the ring of integers of K_v to be the set of elements of K_v with an absolute value less than or equal to 1. As with number fields, we will use the notation $\mathcal{O}_{K_v}$ to refer to the ring of integers of a local field K_v. This ring of integers is a local ring, meaning that it has a unique maximal ideal $\mathfrak{m}$. We often refer to $\mathfrak{m}$ as the maximal ideal of K_v.

This maximal ideal is very important to the topology of K_v. If we imbue K_v with the metric topology induced by the absolute value $|\cdot|_v$, then the subgroups $\mathfrak{m}^i$ are open. Moreover, for $i > 0$, they form a neighborhood basis at 0. By the translational invariance of the metric topology on K_v, we have a neighborhood basis for any point $a \in K_v$ by taking the subgroups $a + \mathfrak{m}^i$. We now state two useful propositions.

Proposition 3.2. *Let L/K be a finite extension of number fields. Let $v \in M_K$ be an absolute value on K. Then, if we let w range over all absolute values extending v to L, we have that*

$$N_K^L(a) = \prod_w N_{K_v}^{L_w}(a).$$

Proof. A proof can be found in [5]. □

Proposition 3.3. *Suppose L/K is a finite extension of number fields. Let v be an absolute value on K, and let w be an extension of that absolute value to L. Then, the local norm $N_{K_v}^{L_w}$ is a continuous map.*

Proof. Let E be the Galois closure of L_w over K_v. Then, any embedding of L_w into its algebraic closure that fixes K_v has an image which lies within E. Thus, these injective homomorphisms can be thought of as maps from L_w to E. The norm map can be expressed as a product varying over all of the K_v-embeddings σ of L_w into E:

$$N_{K_v}^{L_w}(\alpha) = \prod_\sigma \sigma\alpha.$$

We claim that each σ is continuous as a map from L_w to E. Each embedding σ commutes with addition, so it suffices to show continuity at 0.

First assume that v is a non-archimedean absolute value. Then all of our fields are non-archimedean local fields. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}_{K_v}$, and let $\mathfrak{M}$ be the maximal ideal of $\mathcal{O}_E$. Let's denote the image of L_w under σ by L'_w. This is a field, and the image of $\mathfrak{m}$ is the maximal ideal of L'_w; let's call this $\mathfrak{m}'$. Since $\mathfrak{m}'\mathcal{O}_E$ is a non-unit ideal in $\mathcal{O}_E$, it must be of the form $\mathfrak{M}^d$ for some $d > 0$. So, the image of $\mathfrak{m}$ is contained in $\mathfrak{M}^d$.

Since the topology on E is a discrete metric topology, the open sets $\mathfrak{M}^m$, $m > 0$, form a neighborhood basis of 0. By the division algorithm, $m = dq - r$ for $q > 0$ and $0 \leq r < d$. Therefore,

$$\mathfrak{m}^q \subset \sigma^{-1}(\mathfrak{M}^{dq}) \subset \sigma^{-1}(\mathfrak{M}^m).$$

So $\sigma : L_w \to E$ is continuous, thus the norm map, viewed as a function from L_w to E, is also continuous. We know that the image of the norm map is in fact K_v.

The topology on K_v is the subspace topology, so the norm map is also continuous as a map from L_w to K_v.

In the case that v is archimedean, the fields K_v and L_w are either $\mathbb{R}$ or $\mathbb{C}$. If $[L_w : K_v] = 1$, the norm map is the identity and thus continuous. If $K_v = \mathbb{R}$ and $L_w = \mathbb{C}$, the norm map is given by $N_{\mathbb{R}}^{\mathbb{C}}(\alpha) = \alpha\overline{\alpha}$, which is continuous as a map from $\mathbb{C}$ to $\mathbb{R}$. □

These two propositions can be used together to extract some notion of continuity from the global norm map, which is central to the main result of Section 7.

4. Generalized Ideal Classes

Let K be a number field, and let I denote the group of fractional ideals of $\mathcal{O}_K$ in K. Identify two fractional ideals if they are the same up to scaling, that is, $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a} = \alpha\mathfrak{b}$ for some $\alpha \in K^\times$. This forms an equivalence relation, and we can denote the quotient group by I/P, where P is the subgroup of I consisting of principal fractional ideals. We call I/P the *ideal class group* of K. The *class number* of K is defined to be the size of I/P. The class number of any number field is in fact finite, and an elementary proof can be found in [4]. In essence, the ideal class number is a measure of how close the ring of integers of a field is to being a principal ideal domain (PID): the smaller the ideal class number, the more like a PID. For a field K where $\mathcal{O}_K$ is a PID, I/P is the trivial group, giving the smallest possible class number of 1. One example of a field whose ring of integers is not a PID is $\mathbb{Q}(\sqrt{-5})$. However, the ideal class number of this field is 2, suggesting that it is in some sense almost a PID.

We are interested in generalizing the notion of an ideal class group. To motivate this new definition, recall the discussion in Section 2 about the decomposition group. In this scenario, the finite set of ramified primes behaves differently than all other prime ideals in that they do not induce an isomorphism from $G_{\mathfrak{P}}$ to $\overline{G}_{\mathfrak{P}}$. Thus, we may sometimes want to consider fractional ideals that have no ramified primes in their factorization. We will formalize this idea through the notion of a *cycle*, which is a generalization of an ideal.

Definition 4.1. A cycle $\mathfrak{c}$ of K is a formal product over all canonical absolute values

$$\mathfrak{c} = \prod_{v \in M_K} v^{m(v)},$$

where $m(v)$ is a nonnegative integer that is zero for all but finitely many v.

Since many of the absolute values on K correspond to a prime ideal of $\mathcal{O}_K$, we will often use the notation $\mathfrak{p}$ instead of v for these absolute values. Each cycle has a finite part, taken by ignoring any archimedean absolute values in its product form. Formally, the finite part of a cycle, denoted $\mathfrak{c}_0$ is given by

$$\mathfrak{c}_0 = \prod_{\mathfrak{p} \in M_K \setminus \infty} \mathfrak{p}^{m(\mathfrak{p})},$$

where the ∞ in the product above denotes the set of archimedean absolute values on K. Finite cycles of K, or cycles that contain no archimedean absolute values, are in bijection with ideals of $\mathcal{O}_K$.

For any cycle $\mathfrak{c}$ of K, we let $I(\mathfrak{c})$ denote the set of fractional ideals in K relatively prime to $\mathfrak{c}$. In other words, $I(\mathfrak{c})$ is the subgroup of I generated by all prime ideals

in $\mathcal{O}_K$ that have multiplicity 0 in $\mathfrak{c}$. Like I, the set of all fractional ideals, $I(\mathfrak{c})$ forms a group under multiplication.

To create generalized ideal class groups, we want to consider the quotient of $I(\mathfrak{c})$ with respect to some subgroup of $I(\mathfrak{c})$. The immediate choice is $P(\mathfrak{c})$, the set of principal fractional ideals prime to $\mathfrak{c}$. However, for any cycle $\mathfrak{c}$, one can verify that $I(\mathfrak{c})/P(\mathfrak{c}) \cong I/P$. To obtain generalized ideal class groups that are actually different from the ideal class group, we will instead take the quotient of $I(\mathfrak{c})$ with respect to a subgroup of $P(\mathfrak{c})$. To define this subgroup, we need the following definition.

Definition 4.2. Let $a \in K^\times$. For a cycle $\mathfrak{c}$ of K, we say that $a \equiv 1 \pmod^\times \mathfrak{c}$ if:

(i) For each prime ideal $\mathfrak{p}$ with positive multiplicity in $\mathfrak{c}_0$, a lies in the localization of $\mathcal{O}_K$ at the prime $\mathfrak{p}$. If we denote its unique maximal ideal as $\mathfrak{m}_\mathfrak{p}$, then we must also have
$$a \equiv 1 \pmod{\mathfrak{m}_\mathfrak{p}^{m(\mathfrak{p})}}.$$
(ii) For each real absolute value v with positive multiplicity in $\mathfrak{c}$, let σ_v represent the corresponding embedding from K into $\mathbb{R}$. We then enforce that $\sigma_v(a) > 0$.

An equivalent way to interpret (i) in the preceding definition is as follows. An element $a \in K^\times$ satisfies (i) if and only if:

- For each prime ideal $\mathfrak{p}$ with positive multiplicity in $\mathfrak{c}_0$, $\operatorname{ord}_\mathfrak{p}(a) = 0$.
- $a = \alpha/\beta$, where α and β both lie in $\mathcal{O}_K$, have order 0 at $\mathfrak{p}$, and satisfy $\alpha \equiv \beta \pmod{\mathfrak{p}^{m(p)}}$.

Using this equivalent definition, we can produce some simple examples for $K = \mathbb{Q}$. If we have $\mathfrak{c} = 2^2 \cdot 5$, then $23/3 \equiv 1 \pmod^\times \mathfrak{c}$, but $26/6 = 13/3 \not\equiv 1 \pmod^\times \mathfrak{c}$.

One can check that the subset of $K^\times$ consisting of elements a such that $a \equiv 1 \pmod^\times \mathfrak{c}$ is a group, which we will denote by $K_\mathfrak{c}$. We then define $P_\mathfrak{c}$ to be the group of fractional ideals that are principal, and generated by an element of $K_\mathfrak{c}$. The quotient group $I(\mathfrak{c})/P_\mathfrak{c}$ is called the $\mathfrak{c}$-*ideal class group*.

In the context of class field theory, we wish to study certain quotients of $I(\mathfrak{c})$. While $I(\mathfrak{c})/P_\mathfrak{c}$ is solely dependent on K, we wish to define another quotient of $I(\mathfrak{c})$ that depends also upon a finite extension L of K. For this, we introduce a new subgroup $\mathfrak{N}(\mathfrak{c}, L/K)$. We define $\mathfrak{N}(\mathfrak{c}, L/K)$ to be the subgroup of fractional ideals in $I(\mathfrak{c})$ which can be written in the form $N_K^L(\mathfrak{A})$, where $\mathfrak{A}$ is a fractional ideal of L. The quotient group $I(\mathfrak{c})/P_\mathfrak{c}\mathfrak{N}(\mathfrak{c}, L/K)$ will be of critical importance in the statement of Artin reciprocity.

The final idea that we need to develop regarding cycles uses the idea of completions developed in Section 3, and is called *admissibility*. Let L/K be a finite extension of number fields, and $\mathfrak{c}$ a cycle of K. Let v be an absolute value on K. For an element $\alpha \in K_v^\times$, we can define its residue modulo a cycle locally. That is, we only consider the v-component $v^{m(v)}$ of $\mathfrak{c}$, which we will denote $\mathfrak{c}_v$. Then, we have the following definition:

Definition 4.3. Let $\alpha \in K_v^\times$. Then, we say that $\alpha \equiv 1 \pmod^\times \mathfrak{c}_v$ if one of the following conditions is met.

(i) The absolute value v corresponds to a prime ideal of K, and
$$\alpha \equiv 1 \pmod{\mathfrak{m}_\mathfrak{p}^{m(\mathfrak{p})}},$$
where $\mathfrak{m}_\mathfrak{p}$ denotes the maximal ideal of K_v.

(ii) The absolute value v is real archimedean and $\alpha > 0$.
(iii) The absolute value v is complex archimedean.

We let $W_{\mathfrak{c}}(v)$ be the subgroup of $K_v^\times$ consisting of all $\alpha \in K_v^\times$ such that $\alpha \equiv 1 \pmod^\times \mathfrak{c}_v$. The similarity between the two notions of $\mathrm{mod}^\times$ given in Definitions 4.2 and 4.3 can be seen through the following equation:

$$\bigcap_{v \in M_K} \Big(K^\times \cap W_c(v)\Big) = K_c$$

A cycle $\mathfrak{c}$ of K is said to be *admissible* for L/K if for each absolute value v of K and each absolute value w extending v to L, $W_{\mathfrak{c}}(v)$ is contained in the group of local norms $N_{K_v}^{L_w} L_w^\times$. It is a fact that there exists some admissible cycle for all finite extensions of number fields L/K. As $\mathfrak{c}$ is made larger, the sets $W_{\mathfrak{c}}(v)$ shrink, meaning that if an admissible cycle divides some other cycle, that other cycle is admissible too. Thus, there is always a minimal admissible cycle for the extension L/K, which we will often denote by $\mathfrak{f}$.

5. Statement of the Main Theorem

In this section, we let L/K be a finite abelian extension of number fields. Let $G = \mathrm{Gal}(L/K)$. Recall from Section 2 that for any unramified prime $\mathfrak{p}$ of $\mathcal{O}_K$, there exists a unique element $\sigma \in G_{\mathfrak{P}} \subset G$ such that σ maps to the Frobenius element of $\overline{G}_{\mathfrak{P}}$, i.e.

$$\sigma(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}}, \quad \forall \alpha \in \mathcal{O}_L. \tag{5.1}$$

Since L/K is abelian, this element is independent of the prime $\mathfrak{P}$ above $\mathfrak{p}$. We denote σ by $(\mathfrak{p}, L/K)$, and call it the *Artin symbol* of $\mathfrak{p}$ in G.

We now note that we can extend the Artin symbol to fractional ideals generated by unramified prime ideals of $\mathcal{O}_K$ by multiplicativity. Suppose that

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n},$$

for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ unramified in L. Then, we define the Artin symbol of $\mathfrak{a}$ to be

$$(\mathfrak{a}, L/K) = \prod_{i=1}^{n} (\mathfrak{p}_i, L/K)^{r_i}.$$

By Theorem 2.10, the subgroup of fractional ideals generated by unramified prime ideals of $\mathcal{O}_K$ is precisely $I(\mathfrak{d})$, where $\mathfrak{d}$ is the discriminant of L/K, and $I(\mathfrak{d})$ represents the subgroup of fractional ideals relatively prime to $\mathfrak{d}$. So the Artin symbol gives us a homomorphism:

$$\begin{aligned} \omega : I(\mathfrak{d}) &\to G \\ \mathfrak{a} &\mapsto (\mathfrak{a}, L/K). \end{aligned}$$

Take an arbitrary cycle $\mathfrak{c}$ divisible by all ramified primes. Then, $I(\mathfrak{c}) \subset I(\mathfrak{d})$, so we can define the Artin map on the group of $\mathfrak{c}$-ideals as a restriction of the Artin map on $I(\mathfrak{d})$:

$$\begin{aligned} \omega_{\mathfrak{c}} : I(\mathfrak{c}) &\to G \\ \mathfrak{a} &\mapsto (\mathfrak{a}, L/K). \end{aligned}$$

Now, we are ready to state the law of Artin reciprocity.

Theorem 5.2. (Artin Reciprocity) *There exists some cycle $\mathfrak{c}$ of K, divisible by all primes ramified in L, such that:*

(1) The Artin map $\omega_{\mathfrak{c}}$ is surjective.
(2) The kernel of the Artin map is precisely $P_c\mathfrak{N}(\mathfrak{c}, L/K)$.

Alternatively, we can say that the law of Artin reciprocity is the assertion that there exists some cycle $\mathfrak{c}$ such that there is a canonical isomorphism

$$\frac{I(\mathfrak{c})}{P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)} \cong \mathrm{Gal}(L/K).$$

Before proceeding to a proof, we provide a few remarks about different ways to interpret Artin reciprocity. Since $I(\mathfrak{c})$ is an abelian group, so is the quotient $I(\mathfrak{c})/P_{\mathfrak{c}}$. Therefore, the image of $\mathfrak{N}(\mathfrak{c}, L/K)$ under this quotient map is a normal subgroup, and we have a natural isomorphism

$$\frac{I(\mathfrak{c})}{P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)} \cong \frac{I(\mathfrak{c})/P_{\mathfrak{c}}}{\mathfrak{N}(\mathfrak{c}, L/K)/P_{\mathfrak{c}}}.$$

Therefore, we can regard $I(\mathfrak{c})/P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)$ as a quotient of $I(\mathfrak{c})/P_{\mathfrak{c}}$. This means that the Artin map induces a surjection from $I(\mathfrak{c})/P_{\mathfrak{c}}$ onto $\mathrm{Gal}(L/K)$. In Section 9, this viewpoint will be especially useful for explicit computations, as it is easier to compute P_c than $\mathfrak{N}(\mathfrak{c}, L/K)$.

6. Surjectivity of the Artin Map

We will begin by proving the easier of the two assertions in Theorem 5.2, the surjectivity of the Artin map. To start, we state some properties of the Artin symbol that will be integral to the proofs in this section as well as Sections 7 and 8.

Proposition 6.1.

(i) Let L'/K be a finite abelian extension such that $L' \supset L \supset K$. Suppose $\mathfrak{a}$ is a fractional ideal of K whose factorization contains no primes that are ramified in L'. Then,

$$res_L(\mathfrak{a}, L'/K) = (\mathfrak{a}, L/K).$$

This property is often called consistency*.*

(ii) Let E/K be an arbitrary finite extension of K. Suppose $\mathfrak{p}$ is a prime in K unramified in L, and $\mathfrak{q}$ is a prime of E lying above $\mathfrak{p}$. Then,

$$res_L(\mathfrak{q}, LE/E) = (\mathfrak{p}, L/K)^f,$$

where f is the residue class degree, i.e. $f = [\mathcal{O}_E/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$.

(iii) Let E be as above. Let $\mathfrak{b}$ be a fractional ideal of E such that if $\mathfrak{q}$ is a prime ideal in its factorization, and $\mathfrak{q}$ lies above $\mathfrak{p}$ in K, then $\mathfrak{p}$ is unramified in L. Then,

$$res_L(\mathfrak{b}, LE/E) = (N_K^E\mathfrak{b}, L/K).$$

Proof.

(i) Take $\mathfrak{p}$ to be a prime unramified in L', and let $\mathfrak{P}'$ be a prime in L' lying above $\mathfrak{p}$. Let $\sigma = (\mathfrak{p}, L'/K)$. Then, $\sigma\alpha - \alpha^{N\mathfrak{p}} \in \mathfrak{P}'$ for all $\alpha \in \mathcal{O}_{L'}$. For all $\alpha \in \mathcal{O}_L$, we have that $\sigma\alpha - \alpha^{N\mathfrak{p}} \in \mathcal{O}_L$. Since $\mathfrak{P}' \cap \mathcal{O}_L = \mathfrak{P}$ for some prime ideal $\mathfrak{P}$ of L lying above $\mathfrak{p}$, the restriction of σ to L satisfies (5.1), and is thus the Artin symbol $(\mathfrak{p}, L/K)$. The result thus holds for all fractional ideals satisfying the given conditions by multiplicativity.

(ii) Let $\sigma = (\mathfrak{q}, LE/E)$. Select a prime ideal $\mathfrak{Q}$ of $\mathcal{O}_{LE}$ lying above $\mathfrak{q}$. Then, for $\alpha \in \mathcal{O}_{LE}$,
$$\sigma\alpha \equiv \alpha^{N\mathfrak{q}} \pmod{\mathfrak{Q}}.$$
We also know that $\mathfrak{Q} \cap \mathcal{O}_L$ will be a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Let's call this $\mathfrak{P}$. So, if $\alpha \in \mathcal{O}_L$, then
$$\sigma\alpha \equiv \alpha^{N\mathfrak{q}} \pmod{\mathfrak{P}}.$$
Therefore, $\overline{\sigma}$ is the automorphism sending α to $\alpha^{N\mathfrak{q}}$. Since $N\mathfrak{q} = N\mathfrak{p}^f$, $\overline{\sigma}$ is the fth power of the Frobenius element. After mapping back into $G_{\mathfrak{P}}$, we get the statement of the proposition.

(iii) This statement is obtained from (ii) by applying the multiplicativity of the Artin symbol, using the fact that $N(\mathfrak{q}) = \mathfrak{p}^f$.

□

We now state two technical lemmas that will help us prove the surjectivity of the Artin map. These fall outside of the scope of this paper, and are not at all trivial.

Lemma 6.2. *Suppose that $\mathfrak{c}$ is a cycle in K that is divisible by all primes that ramify in L. Then,*
$$[I(\mathfrak{c}) : P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)] \leq [L : K].$$

Lemma 6.3. *Suppose that L/K is a finite cyclic extension, and $\mathfrak{c}$ is an admissible cycle for L/K. Then,*
$$[I(\mathfrak{c}) : P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K) = [L : K].$$

Proof. Proofs of these two lemmas can be found in chapters 8 and 9 of [5], respectively. □

This lemma has an important corollary, which is also proved using ideles in [5].

Corollary 6.4. *Suppose L/K is a nontrivial finite cyclic field extension. Then, there are infinitely many prime ideals of K which do not split completely in L.*

Now, we can prove the surjectivity of the Artin map.

Theorem 6.5. *Suppose that $\mathfrak{c}$ is a cycle in K that is divisible by all primes that ramify in L. Then, the Artin map $\omega_{\mathfrak{c}}$ is surjective.*

Proof. Let $\mathfrak{c}$ be a cycle of K divisible by all ramified primes. Let H be the image of the Artin map $\omega_{\mathfrak{c}}$. Let E be the fixed field of H, so we have $K \subset E \subset L$. By consistency, we have that for any prime ideal $\mathfrak{p} \in I(\mathfrak{c})$,
$$(\mathfrak{p}, E/K) = \mathrm{res}_E(\mathfrak{p}, L/K) = 1,$$
since $(\mathfrak{p}, L/K)$ is an automorphism that fixes E. By the definition of the Artin symbol, $(\mathfrak{p}, E/K) = 1$ if and only if the Galois group of the residue fields is trivial, that is, the ramification index f of $\mathfrak{p}$ is equal to 1. Since $\mathfrak{p}$ is unramified in L and therefore also in E, this is exactly what it means for $\mathfrak{p}$ to split completely in E.

Suppose that $H \neq G$. Then, $E \neq K$. Since E/K is a nontrivial finite abelian extension, it is a consequence of the structure theorem for finite abelian groups that there exists some intermediate field $K \subset F \subset E$ such that F/K is a nontrivial cyclic field extension. Because all primes $\mathfrak{p} \in I(\mathfrak{c})$ split completely in E, they split completely in F too. This leaves only finitely many prime ideals which do not split completely in F, contradicting Corollary 6.4. So $H = G$, meaning the Artin map is surjective. □

Now it remains to prove the second part of Theorem 5.2. That is, we must find some cycle $\mathfrak{c}$ such that the kernel of the Artin map $\omega_{\mathfrak{c}}$ from $I(\mathfrak{c})$ to $\mathrm{Gal}(L/K)$ is equal to $P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)$. To do this, we claim that it suffices to find some cycle $\mathfrak{c}$, divisible by all ramified primes, such that $P_{\mathfrak{c}} \subset \ker(\omega_{\mathfrak{c}})$. Such a cycle is called a *conductor* of the Artin map. We now argue why finding a conductor is sufficient to prove that the kernel of the Artin map is $P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)$.

Suppose $\mathfrak{c}$ is a conductor of the Artin map. Then, any element of $\mathfrak{N}(\mathfrak{c}, L/K)$ can be written as $N_K^L(\mathfrak{A})$ for some fractional ideal $\mathfrak{A}$ in L. Then, $(N_K^L(\mathfrak{A}), L/K) = 1$ by Proposition 6.1iii. So $\mathfrak{N}(\mathfrak{c}, L/K) \subset \ker(\omega_f c)$, and $P_{\mathfrak{c}} \subset \ker(\omega_{\mathfrak{c}})$ by the definition of a conductor. So, $P_c\mathfrak{N}(\mathfrak{c}, L/K) \subset \ker(\omega_{\mathfrak{c}})$. Therefore,

$$[I(\mathfrak{c}) : \ker(\omega_{\mathfrak{c}})] \leq [I(\mathfrak{c}) : P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)].$$

By the surjectivity of the Artin map, $[I(\mathfrak{c}) : \ker(\omega_{\mathfrak{c}})] = [L : K]$. By Lemma 6.2, $[I(\mathfrak{c}) : P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, L/K)] \leq [L : K]$. So the inequality must in fact be an equality, and we must have

$$P_c\mathfrak{N}(\mathfrak{c}, L/K) = \ker(\omega_{\mathfrak{c}}).$$

As a note, if $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are cycles such that $\mathfrak{c}_1$ divides $\mathfrak{c}_2$, and $\mathfrak{c}_1$ is a conductor, then $\mathfrak{c}_2$ is a conductor. This is because $P_{\mathfrak{c}_2} \subset P_{\mathfrak{c}_1}$, which is contained in the kernel of the Artin map.

7. The Cyclotomic Case

We first assert the existence of a conductor for cyclotomic extensions of $\mathbb{Q}$. We begin with a small lemma about cyclotomic extensions.

Lemma 7.1. *If p ramifies in $\mathbb{Q}(\zeta_m)$, then $p \mid m$.*

Proof. Let $\Phi \in \mathbb{Z}[x]$ be the minimal polynomial of ζ_m. Since ζ_m also satisfies $x^m - 1 = 0$, we have that $x^m - 1 = \Phi(x)g(x)$ for some $g \in \mathbb{Z}[x]$. Taking derivatives, we get

$$mx^{m-1} = \Phi'(x)g(x) + \Phi(x)g'(x).$$

Plugging in ζ_m, we get $m\zeta_m^{m-1} = \Phi'(\zeta_m)g(\zeta_m)$. Now, take the norm of both sides. Since ζ_m has absolute value 1, its norm will be one of ± 1. Let $\Delta = \Delta(1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1})$ be the discriminant of the basis $\{1, \zeta, \ldots, \zeta^{\phi(m)-1}\}$. Using Proposition 2.8 to relate these norms to the discriminant , we get

$$N(m\zeta_m^{m-1}) = \pm N(m) = \pm m^{\phi(m)} = N(\Phi'(\zeta_m))N(g(\zeta_m)) = \pm \Delta N(g(\zeta_m)).$$

Thus, the discriminant of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, divides Δ, which divides $m^{\phi(m)}$. A prime ramifies if and only if it divides the discriminant, so only primes that divide m can ramify in $\mathbb{Q}(\zeta_m)$. □

Theorem 7.2. *Let $K = \mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{N}$. Then, $m\infty$ is a conductor of the Artin map.*

Proof. It suffices to prove the above statement for $L = \mathbb{Q}(\zeta_m)$. Suppose $\mathfrak{c}$ is a conductor for the Artin map on L/K, and L' is an intermediate field. By consistency, any fractional ideal in the kernel of the Artin map on L/K is also in the kernel of the Artin map on L'/K. So we will also have that $P_{\mathfrak{c}}$ is contained in the kernel of the Artin map on L'/K, meaning that $\mathfrak{c}$ is also a conductor.

The cycle $\mathfrak{c} = m\infty$ divides all ramified primes by Lemma 7.1. The Artin map from $I(\mathfrak{c})$ to $\mathrm{Gal}(L/K)$ is determined by its action on the primes not dividing m. Let

p be a prime not dividing m. By (5.1), $((p), \mathbb{Q}(\zeta_m)/\mathbb{Q})$ is the Galois automorphism sending ζ_m to ζ_m^p. Therefore, $((a), \mathbb{Q}(\zeta_m)/\mathbb{Q}) = 1$ if and only if $a \equiv 1 \pmod^\times \mathfrak{c}$. Note that the positivity of a implied by $a \equiv 1 \pmod^\times \mathfrak{c}$ is essential here since our description of the Artin symbol of (p) is only valid when p is a positive prime. □

Corollary 7.3. *Suppose p is an odd prime. Let $L = \mathbb{Q}(\sqrt{p})$ and $K = \mathbb{Q}$, and consider the Artin map for this abelian field extension. Then,*

$$p \equiv 1 \pmod 4 \implies p\infty \text{ is a conductor of the Artin map.}$$
$$p \equiv 3 \pmod 4 \implies 4p\infty \text{ is a conductor of the Artin map.}$$

Proof. By Gauss sums, one can deduce that $i^{(p-1)/2}\sqrt{p} \in \mathbb{Q}(\zeta_p)$. This approach is outlined in chapter 6 of [4]. Therefore, if $p \equiv 1 \pmod 4$, then $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$, and by Theorem 7.2, $p\infty$ is a conductor of the Artin map. If $p \equiv 3 \pmod 4$, we have that $i\sqrt{p} \in \mathbb{Q}(\zeta_p)$. Since $i \in \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$, $\sqrt{p}$ is in the compositum of those fields, which is $\mathbb{Q}(\zeta_{4p})$. So in this case, $4p\infty$ is a conductor of the Artin map. □

We can extend Theorem 7.2 to arbitrary cyclotomic extensions. That is, we may consider extensions of an arbitrary number field obtained by adjoining a root of unity.

Theorem 7.4. *Let $K \subset L \subset K(\zeta_m)$ for some $m \in \mathbb{N}$. Then, there exists a conductor of the Artin map divisible only by primes $\mathfrak{p}$ which divide m and real archimedean absolute values.*

Proof. By the same argument as before, it suffices to take $L = K(\zeta_m)$. Suppose $m = p_1^{a_1} \cdots p_\ell^{a_\ell}$. For each p_i, let $\mathfrak{p}_j$ be a prime ideal of K lying above p_i. By Proposition 3.3, the continuity of local norms, there exists some integer r such that $\alpha \in 1 + \mathfrak{m}_{\mathfrak{p}_j}^r$ implies that $N_{\mathbb{Q}_{p_i}}^{K_{\mathfrak{p}_j}} \alpha \in 1 + \mathfrak{m}_{p_i}^{a_i}$. If $\alpha \in K$, the former condition is equivalent to saying that $\alpha \equiv 1 \pmod^\times \mathfrak{p}_j^r$. This implies that all of the local norms are contained within $1 + \mathfrak{m}_{p_i}^{a_i}$. Since the product of the local norms is the global norm N from K to $\mathbb{Q}$ by Proposition 3.2, we also have the containment

$$N\alpha \in \left(1 + \mathfrak{m}_{p_i}^{a_i}\right) \cap \mathbb{Q}.$$

Therefore, $N\alpha \equiv 1 \pmod^\times p_i^{a_i}$. Applying this to all primes p_i, we can find some cycle $\mathfrak{c}'$ such that $\alpha \equiv 1 \pmod^\times \mathfrak{c}'$ implies $N\alpha \equiv 1 \pmod^\times m$. Let $\mathfrak{c}$ be the product of $\mathfrak{c}'$ with all real archimedean values on K. Then, if $\alpha \equiv 1 \pmod^\times \mathfrak{c}$, the norm $N\alpha$ will be positive.

Now, by consistency, we have that for such α,

$$\mathrm{res}_{\mathbb{Q}(\zeta_m)}((\alpha), L/K) = (N_{\mathbb{Q}}^K(\alpha), \mathbb{Q}(\zeta_m)/\mathbb{Q}) = 1.$$

So $P_{\mathfrak{c}} \subset \ker \omega_{\mathfrak{c}}$, and thus $\mathfrak{c}$ is a conductor of the Artin map. □

8. The General Case

We are now ready to prove the general theorem of Artin reciprocity. We follow the approach of chapter 10 in [5], providing some extra details and commentary where desired. As the first step of our proof, we present the following lemma.

Lemma 8.1. *Suppose K is a number field, L/K is a finite cyclic extension, and S is a finite set of prime numbers. Let $\mathfrak{p}$ be a prime ideal of K unramified in L. Then there exists an integer m relatively prime to S and a finite extension E/K such that:*

(i) $L \cap E = K$.
(ii) $L(\zeta_m) = E(\zeta_m)$ *and* $L \cap K(\zeta_m) = K$.
(iii) $\mathfrak{p}$ *splits completely in* E.
(iv) There exists an automorphism $\tau \in \mathrm{Gal}(K(\zeta_m)/K)$, *such that* τ *and* $(\mathfrak{p}, K(\zeta_m)/K)$ *generate cyclic subgroups of* $\mathrm{Gal}(K(\zeta_m)/K)$ *with trivial intersection.*

In this lemma, m *can be chosen such that it is only divisible by arbitrarily large primes.*

Proof. To prove this lemma, one essentially "translates" a statement about modular arithmetic to one about cyclotomic extensions. This process is explained in full in section 2 of chapter 10 in [5]. □

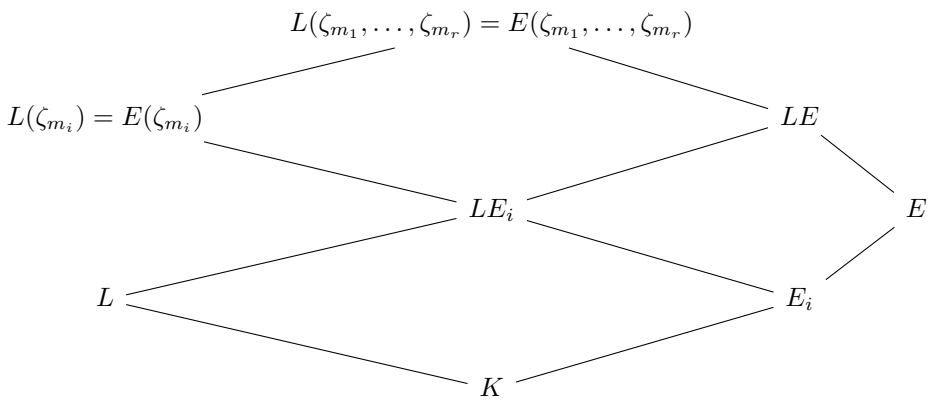
To construct a conductor, we will recursively apply Lemma 8.1 to a finite set of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of K. By the lemma, there exist fields E_i with associated integers m_i for each i. Recall that from Lemma 8.1, we can take the primes in the factorization of m_i to be arbitrarily large. By doing this, we can choose m_i that are all relatively prime. We can also ensure that $L(\zeta_{m_1}, \ldots, \zeta_{m_{i-1}}) \cap \mathbb{Q}(\zeta_{m_i}) = \mathbb{Q}$ for all i. We let E be the compositum of all of the fields E_i. Then, $L(\zeta_{m_1}, \ldots, \zeta_{m_r}) = E(\zeta_{m_1}, \ldots, \zeta_{m_r})$. Let G denote the Galois group of L/K, and G_i denote the Galois group of $\mathbb{Q}(\zeta_{m_i})/\mathbb{Q}$. The Galois group of $L(\zeta_{m_1}, \ldots, \zeta_{m_r})/K$ is thus isomorphic to

$$G \times G_1 \times \cdots \times G_r.$$

From the proof of Lemma 8.1, each field E_i is the fixed field of the subgroup

$$H_i \times G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_r. \tag{8.2}$$

Here, H_i is a subgroup of $G \times G_i$. To describe H_i, let σ be an some fixed generator of G, and τ_i be the automorphism from Lemma 8.1 that generates a cyclic subgroup of $\mathrm{Gal}(K(\zeta_{m_i})/K)$. Then, H_i is the subgroup of $G \times G_i$ generated by $(\mathfrak{p}_i, L/K) \times (\mathfrak{p}_i, K(\zeta_{m_i})/K)$ and $\sigma \times \tau_i$. To illustrate everything we have done so far, we have the following field extension diagram.



Now, I claim that $\mathrm{Gal}(LE/E) \cong \mathrm{Gal}(L/K)$. In fact, this isomorphism is given by restriction to L. This is true if and only if $L \cap E = K$. E is the fixed field of the intersection of the subgroups in (8.2). Therefore, $\sigma \times \tau_1 \times \cdots \times \tau_r$ fixes E. The fixed field of L is $1 \times G_1 \times \cdots \times G_r$, so $1 \times \tau_1 \times \cdots \times \tau_r$ fixes L. Thus, both automorphisms fix $L \cap E$, meaning that the automorphism $\sigma \times 1 \times \cdots \times 1$ fixes $L \cap E$. We can self-compose this automorphism and multiply by an automorphism

that fixes L to get an arbitrary element of $G \times G_1 \times \cdots \times G_r$, all of which fix $L \cap E$. Therefore, we must have $L \cap E = K$.

Theorem 8.3. *Let L/K be a finite cyclic extension. Then, if $\mathfrak{c}$ is an admissible cycle for L/K, then $\mathfrak{c}$ is a conductor of the Artin map for L/K.*

Proof. Following our discussion from Section 6, $\mathfrak{c}$ is a conductor if and only if $\ker(\omega_\mathfrak{c}) = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c}, L/K)$. In the cyclic case, it is easier to prove the latter condition. Later, we will use the definition of a conductor to extend this theorem to arbitrary finite abelian extensions.

We first note that it suffices to prove that $\ker(\omega_\mathfrak{c}) \subset P_\mathfrak{c}\mathfrak{N}(\mathfrak{c}, L/K)$. Since we are in the cyclic case, Lemma 6.3 gives that

$$[I(\mathfrak{c}) : P_\mathfrak{c}\mathfrak{N}(\mathfrak{c}, L/K)] = [L : K],$$

and the surjectivity of the Artin map, Theorem 6.5, gives that

$$[I(\mathfrak{c}) : \ker(\omega_\mathfrak{c})] = [L : K],$$

meaning that $\ker(\omega_\mathfrak{c}) = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c}, L/K)$, as desired.

Additionally, it is sufficient to prove the statement of our theorem for the minimal admissible cycle $\mathfrak{f}$, which follows from the discussion in the last paragraph of Section 6.

Let $\mathfrak{f}$ be the minimal admissible cycle for L/K, and consider a fractional ideal $\mathfrak{a} \in I(\mathfrak{f})$ that is in the kernel of the Artin map, i.e. $(\mathfrak{a}, L/K) = 1$. We may write $\mathfrak{a}$ as a product of prime ideals in K:

$$\mathfrak{a} = \prod_i^r \mathfrak{p}_i^{a_i}.$$

As described earlier, we construct fields E_i, corresponding to roots of unity ζ_{m_i}, satisfying Lemma 8.1 for each prime $\mathfrak{p}_i$ in the factorization of $\mathfrak{a}$. Let E be the compositum of the E_i.

Let σ be a generator of $\mathrm{Gal}(L/K)$. For each prime $\mathfrak{p}_i$, we must have that

$$(\mathfrak{p}_i^{a_i}, L/K) = \sigma^{d_i},$$

for some $0 \leq d_i < \#\,\mathrm{Gal}(L/K)$.

Recall that $\mathrm{Gal}(LE/E) \cong \mathrm{Gal}(L/K)$. By Theorem 6.5, we can select a fractional ideal $\mathfrak{b}_E$ of E that is relatively prime to $\mathfrak{f}$ and all the m_i, such that

$$(\mathfrak{b}_E, LE/E) = \sigma.$$

Using Proposition 6.1iii, if we let $\mathfrak{b}_K = N_K^E \mathfrak{b}_E$, then we have that

$$(\mathfrak{b}_K, L/K) = \sigma.$$

We now note that $\mathfrak{p}_i$ is a norm from E_i to K, since $\mathfrak{p}_i$ splits completely in E_i by 8.1, and is thus the image of any prime lying above $\mathfrak{p}_i$ via the norm map. $\mathfrak{b}_K$ is a norm from E_i to K, since the norm map is transitive, meaning that

$$\mathfrak{b}_K = N_K^E \mathfrak{b}_E = N_K^{E_i}(N_{E_i}^E \mathfrak{b}_E).$$

By the multiplicativity of the norm, the fractional ideal $\mathfrak{p}_i^{a_i}\mathfrak{b}_K^{-d_i}$ is a norm from E_i to K. We write this as $\mathfrak{p}_i^{a_i}\mathfrak{b}_K^{-d_i} = N_K^{E_i}\mathfrak{A}$, for a fractional ideal $\mathfrak{A}_i$ in E_i. By the multiplicativity of the Artin symbol, we can deduce that $(\mathfrak{p}_i^{a_i}\mathfrak{b}_K^{-d_i}, L/K) = 1$. Proposition 6.1iii, along with the fact that $\mathrm{Gal}(LE_i/E_i) \cong \mathrm{Gal}(L/K)$ via restriction to L, implies that $(\mathfrak{A}_i, LE_i/E_i) = 1$.

Notice that $LE_i \subset E_i(\zeta_{m_i})$ by Lemma 8.1, so we can apply 7.4 to find a conductor $\mathfrak{c}_i$ of the extension. Note that we may take $\mathfrak{c}_i$ highly divisible by the factors of $\mathfrak{f}$ and all integers m_i. Then, we have that

$$\mathfrak{A}_i = (\beta_i) N_{E_i}^{LE_i} \mathfrak{B}_i,$$

where $\beta_i \equiv 1 \pmod^{\times} \mathfrak{c}_i$, and $\mathfrak{B}_i$ is a fractional ideal in LE_i prime to $\mathfrak{c}_i$. If we apply the norm from E_i to K and use the continuity of norms, we get

$$\mathfrak{p}_i^{a_i} \mathfrak{b}_K^{-d_i} = (N_K^{E_i} \beta_i) N_K^{E_i} N_{E_i}^{LE_i} \mathfrak{B}_i = (N_K^{E_i} \beta_i) N_K^L N_L^{LE_i} \mathfrak{B}_i.$$

By the continuity of local norms, taking $\mathfrak{c}_i$ to be large enough ensures that $N_K^{E_i} \beta_i \equiv 1 \pmod^{\times} \mathfrak{f}$. Taking the product of the above equation for all i gives

$$\mathfrak{a} \mathfrak{b}_K^{-\sum d_i} = \Big(\prod N_K^{E_i} \beta_i \Big) N_K^L \Big(\prod N_L^{LE_i} \mathfrak{B}_i \Big). \tag{8.4}$$

Our initial hypothesis tells us that $\prod (\mathfrak{p}_i^{a_i}, L/K) = \sigma^{\sum d_i} = 1$. Therefore $[L : K]$ divides $\sum d_i$, as σ is a generator of a cyclic group of order $[L : K]$. Let $n = [L : K]$, and take a prime ideal $\mathfrak{p}$ of K. The ideal $\mathfrak{p}^{dn}$ is a norm from L to K for any integer by the following argument. Take a prime ideal $\mathfrak{P}$ of L lying above $\mathfrak{p}$. By 2.5, $N_K^L \mathfrak{P} = \mathfrak{p}^f$, where f divides n. Therefore, there exists some integer $j = dn/f$ such that the norm of $\mathfrak{P}^j$ is equal to $\mathfrak{p}^{dn}$. Applying multiplicativity, any nth power of a fractional ideal in K is a norm from L to K. Thus, $\mathfrak{b}_K^{\sum d_i} \in \mathfrak{N}(\mathfrak{f}, L/K)$, and multiplying this to both sides of (8.4) shows that $\mathfrak{a} \in P_{\mathfrak{f}} \mathfrak{N}(\mathfrak{f}, L/K)$. We now have our desired containment, and we are done. □

Corollary 8.5. *Let L/K be a finite abelian extension of number fields. Then, if $\mathfrak{c}$ is an admissible cycle for L/K, it is a conductor of the Artin map for L/K.*

Proof. Using Galois theory, we can associate intermediate fields of L/K with subgroups of $G = \mathrm{Gal}(L/K)$. Due to the structure theorem, a finite abelian group is the direct product of finitely many finite cyclic groups. We can thus take finitely many subgroups of G, call them H_i, such that G/H_i is cyclic and the intersection of the H_i is 1. These correspond to intermediate fields F_i which have compositum L. An element of $\mathrm{Gal}(L/K)$ is equal to 1 if and only if its restriction to each of the F_i is 1.

Let $\mathfrak{f}$ be the minimal admissible cycle of L/K. By Theorem 8.3, any admissible cycle of F_i/K is a conductor for the Artin map for F_i/K. Since $\mathfrak{f}$ is an admissible cycle for L/K, it is also an admissible cycle for all of the F_i/K, since taking a smaller field extension results in a larger group of norms. Therefore, $\mathfrak{f}$ is a conductor for the Artin maps on each F_i/K, meaning that $P_{\mathfrak{f}}$ is contained in the kernel of each Artin map. This means that $P_{\mathfrak{f}}$ is also contained in the kernel of the Artin map for L/K. Therefore, $\mathfrak{f}$ is a conductor of the Artin map for L/K. □

9. Quadratic Reciprocity

As mentioned in the introduction to this paper, one of the motivations to study Artin reciprocity is to generalize many classical reciprocity laws, including quadratic reciprocity. In this section, I will explain how quadratic reciprocity arises as a consequence of Artin reciprocity. To formulate the standard statement of quadratic reciprocity, we need the following definition of the Legendre symbol.

Definition 9.1. Let p be a prime and $a \in \mathbb{Z}$ such that $p \nmid a$. The *Legendre symbol* is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1, & \text{if } x^2 \equiv a \pmod{p} \text{ has no solution.} \end{cases}$$

The statement of quadratic reciprocity is as follows:

Theorem 9.2. *Let p and q be distinct odd primes. Then,*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Although there are many more elementary ways to prove quadratic reciprocity (an exercise in [4] jokingly asks the reader to count the proofs of the theorem stated in the textbook before coming up with a new proof), we will prove it as a consequence of Artin reciprocity.

We first state a useful theorem by Dedekind and Kummer that we will use to rephrase quadratic reciprocity in terms of the splitting of prime ideals in quadratic extensions of $\mathbb{Q}$.

Theorem 9.3. *Let $K = \mathbb{Q}(\alpha)$ be a number field, where $\alpha \in \mathcal{O}_K$. Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α. Then, for any prime p that does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, we let $\overline{f}$ denote the reduction of f mod p, which is a polynomial in $\mathbb{F}_p[T]$. Suppose that $\overline{f}$ factors as*

$$\overline{f}(T) = \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g},$$

where the π_i are distinct monic irreducibles in $\mathbb{F}_p[T]$. Then, $p\mathcal{O}_K$ factors into prime ideals in $\mathcal{O}_K$ as

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where the $\mathfrak{p}_i$ are all distinct. Furthermore, for all i, $f_i = [(\mathcal{O}_K/\mathfrak{p}_i) : \mathbb{Z}/p] = \deg(\pi_i)$.

Proof. A proof this theorem is tangential to the focus of this paper, so I will not provide one here. An excellent proof is provided in [1]. □

.

Corollary 9.4. *Let p and q be distinct primes. p is a square mod q if and only if q splits completely in $K = \mathbb{Q}(\sqrt{p})$.*

Proof. Since K is a quadratic extension of $\mathbb{Q}$, we have an explicit description of $\mathcal{O}_K$, which is proved in [4]:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{p}], & p \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right], & p \equiv 1 \pmod{4}. \end{cases}$$

In the first case, $[\mathcal{O}_K : \mathbb{Z}[\sqrt{p}]] = 1$, and in the second, $[\mathcal{O}_K : \mathbb{Z}[\sqrt{p}]] = 2$. Since q is an odd prime, Theorem 9.3 applies with $\alpha = \sqrt{p}$ and $f(T) = T^2 - p$. So q splits completely in K if and only if f factors as the product of two linear polynomials mod q. This is equivalent to p being a square mod q. □

Now, we can prove Theorem 9.2 using Artin Reciprocity.

Proof. Let $p^* = (-1)^{(p-1)/2}p$. Then, $p^* \equiv 1 \pmod 4$. By Corollary 9.4, p^* is a square mod q if and only if q splits completely in $L = \mathbb{Q}(\sqrt{p^*})$. Additionally, $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$, and this can be proved using Gauss sums. This is shown in Proposition 6.3.2 of [4]. Therefore, as a consequence of Lemma 7.1, q does not ramify in L, so we can use the Artin symbol.

Now, note that the Artin symbol $(q, \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = 1$ if and only if the Frobenius of the residue class field extension is the identity, which occurs when the residue class degree is equal to 1. Since q does not ramify in $\mathbb{Q}(\sqrt{p^*})$, this is equivalent to q splitting completely in $\mathbb{Q}(\sqrt{p^*})$.

By Theorem 7.2, $p\infty$ is a conductor for $L/\mathbb{Q}$. By Artin reciprocity, $P_{p\infty}$ is contained in the kernel of the Artin map, and thus

$$\frac{I(p\infty)}{P_{p\infty}} \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \cong \{\pm 1\}.$$

Note that the representatives of $\frac{I(p\infty)}{P_{p\infty}} \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ are simply the ideals (a) with $a \in \mathbb{Z}$ and $1 \le a \le p-1$.

So q being in the kernel of the Artin map is equivalent to q (thought of as an element of $(\mathbb{Z}/p\mathbb{Z})^\times$) mapping to $1 \in \mathrm{Gal}(K/\mathbb{Q})$. But there is only one surjection from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\{\pm 1\}$, namely the one that sends the squares to 1 and non-squares to -1. Therefore, p^* is a square mod q if and only if q is a square mod p. That is,

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Using the fact that $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$ and the multiplicativity of the Legendre symbol,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

□

Acknowledgments

I would like to thank my mentor, Katie Gallagher, for her guidance and support throughout this program. I also owe a great deal of thanks to Peter May for organizing a wonderful REU this summer.

References

[1] Keith Conrad. Factoring after Dedekind. https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf. Accessed: 2023-07-26.

[2] Keith Conrad. Ostrowski for number fields. https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf. Accessed: 2023-07-26.

[3] Dennis Garbanati. Class field theory summarized. *Rocky Mountain J. Math.*, 11(2):195–225, 1981.

[4] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[5] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[6] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, second edition, 2018. With a foreword by Barry Mazur.

[7] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.