Higher Power Reciprocity Laws

James Rickards

12 October 2015

Contents

1 Introduction

1.1 What is a Reciprocity Law?

The Legendre symbol for quadratic residues is defined as

Definition 1.1.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a nonzero quadratic residue modulo } p, \\ 0, & \text{if } p \mid a, \\ -1, & \text{otherwise.} \end{cases}$$

where a is an integer and p and odd prime.

It can be extended to the Jacobi Symbol, where the denominator is any odd positive integer by defining

Definition 1.2. $\left(\frac{a}{p_1 p_2 \cdots p_r}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$ where the p_i are odd primes.

Theorem 1.3 (Law of Quadratic Reciprocity)**.**

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$$

where m, n are coprime odd positive integers.

When p, q are distinct odd primes, the residue class of p modulo q determines whether p is a square modulo q. What the Law of Quadratic Reciprocity implies is that this can *also* be determined by the residue class of q modulo $4p$ (or q modulo p when $p \equiv 1 \pmod 4$).

We will now deal with attempts to generalize this result: instead of looking at quadratic residues, you can consider higher powers. Generalizing results and methods from $\mathbb{Q}$ to larger number fields will not only be interesting, but necessary to deal with higher cases.

1.2 A Brief Summary

This essay begins by defining the power residue symbol in general, and exploring its basic properties. Sections 3-5 deal mostly with Eisenstein Reciprocity, and specific cases of it (or slight variations in the case of quartic reciprocity). To motivate the introduction of Gauss and Jacobi sums, we give a proof of quadratic reciprocity involving them. After investigating their properties, we present a full exposition on cubic reciprocity, which will help motivate the section on Eisenstein reciprocity. Before that, we present only the results from quartic reciprocity: they are not a consequence of Eisenstein reciprocity, but the methods involved are very similar to the cubic case, so it would not add much to present proofs. We then move on to Eisenstein reciprocity: this is a reciprocity law in $\mathbb{Q}(\zeta_n)$ where n is an odd prime. Its statement is simple and elegant, and it is one of the most general reciprocity laws that you can obtain without class field theory. The bulk of its proof is factorizing the Gauss sum in general; the rest of the proof is applying a few tricks to deduce the law.

With the development of class field theory came the statement and proof of Artin's Reciprocity Law. As mentioned by Peter Swinnerton-Dyer on page 100 in [4], as well as by Franz Lemmermeyer on page ix in [3], this law could be used to deduce all previously known reciprocity laws. However, this deduction is not obvious from a first glance! In section 6, we will start off by defining the Artin symbol, and linking it to the power residue symbol. We will then state several results of global class field theory, leading to Artin's Law. Deduction of reciprocity laws from Artin is not immediate; instead we will first introduce the Hilbert symbol and a few key results. The essay ends with the examples of deducing quadratic reciprocity, as well as cubic reciprocity. While most proofs are given, in the last 2 sections we will not provide proofs of a few key results which require more involved class field theory. These results are either common and included in any good book on class field theory, or we will give a reference to where to find a proof.

Most of the theorems/propositions/lemmas and the method of their proofs for sections 3-5 came from [3], Franz Lemmermeyer's fantastic book about reciprocity laws. It is a great place to look for those who want to find out more; the full list of references at the end totals 885, so it is also an excellent place to find references to other books and articles dealing with similar topics. The material after section 6.1 mostly derives from chapter 5 of [4], Peter Swinnerton-Dyer's short book on Algebraic Number Theory.

1.3 Notation

One caveat of working in extensions of $\mathbb{Q}$ is that primes in $\mathbb{Z}^+$ may no longer be prime. When we refer to a prime, it will typically be obvious from context whether we mean a prime ideal, a prime in the number field, or a prime in $\mathbb{Z}^+$. However for added measure, when we are not working over $\mathbb{Z}$ or $\mathbb{Q}$, we will refer to primes in $\mathbb{Z}^+$ as "integer primes". They will typically be labeled with regular letters, like p, q. Prime ideals will normally be assigned curly letters or Greek characters, like $\mathfrak{p}, \mathfrak{q}, \Lambda$. An automorphism σ acting on an element α is written both as $\sigma(\alpha)$ and α^σ.

2 Generalized Power Residue Symbol

2.1 Generalized Power Residue Symbol

In defining the generalized power residue symbol, it is good to keep in mind the Legendre symbol, as we want this to be a special case of the new symbol. The Legendre symbol is multiplicative on top, so to retain this feature, it will be necessary for the symbol to take more values than ±1 (there is some theory where power residue symbols only take ±1: rational reciprocity. The theory is fairly limited and will not be covered in this essay).

Let $n > 1$ be a positive integer, and k be a number field which contains a primitive n^{th} root of unity ζ_n. Suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_k$ coprime to n (i.e. $\mathfrak{p} \nmid n\mathcal{O}_k$) lying above the integer prime p. Then $N\mathfrak{p} = \left|\frac{\mathcal{O}_k}{\mathfrak{p}}\right| = p^f = q$ some positive integer f, and $\mathfrak{p}$ is coprime to n if and only if $p \nmid n$. For all $x \in \mathcal{O}_k$ coprime to $\mathfrak{p}$, we have:

$$x^{q-1} \equiv 1 \pmod{\mathfrak{p}}. \tag{2.1}$$

I claim that the reduction of ζ_n modulo $\mathfrak{p}$ still has order n in $\frac{\mathcal{O}_k}{\mathfrak{p}}$, hence $n \mid q-1$. Indeed, the n^{th} roots of unity in $\mathbb{F}_{p^f}$ satisfy $x^n - 1 = 0$, and this is separable since $p \nmid n$. So we do get n distinct n^{th} roots of unity, which form the group generated by $\overline{\zeta_n}$ (the reduction of ζ_n), which is what we desire. This allows us to now define the power residue symbol:

Definition 2.1. For $\alpha \in \mathcal{O}_k$ coprime to $\mathfrak{p}$, define $(\frac{\alpha}{\mathfrak{p}})_n$ to be the unique n^{th} root of unity in $\mathcal{O}_k$ such that:

$$\alpha^{\frac{q-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}. \tag{2.2}$$

Extend this definition multiplicatively in the denominator to all ideals coprime to α and n.

2.2 Properties of the Power Residue Symbol

Proposition 2.2. *The power residue symbol for $n = 2$ and $k = \mathbb{Q}$ agrees with the definition of the Legendre (and hence Jacobi) symbol where defined.*

Proof. It suffices to show

$$x^{\frac{p-1}{2}} \equiv \left(\frac{x}{p}\right) \pmod{p}, \tag{2.3}$$

for integers x coprime to p. If $x \equiv y^2 \pmod{p}$ then $x^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1 \equiv \left(\frac{x}{p}\right) \pmod{p}$, and if x is not a quadratic residue, let r be a generator for the multiplicative group modulo p (this is cyclic). Then $x \equiv r^e \pmod{p}$ with e odd, so $x^{\frac{p-1}{2}} \equiv r^{\frac{(p-1)e}{2}} \equiv -1 \equiv \left(\frac{x}{p}\right) \pmod{p}$ since $r^{\frac{(p-1)e}{2}}$ squares to give 1, but cannot be 1 as $p - 1 \nmid \frac{(p-1)e}{2}$ since e is odd. □

Proposition 2.3. *Let $n > 1$ be a positive integer, and let p be an integer prime such that $p - 1$ is coprime to n. Then all integers x coprime to p are n^{th} powers modulo p*

Proof. Let r be a primitive root modulo p, and let $x \equiv r^e \pmod{p}$. Then, as $p - 1, n$ are coprime, choose integers a, b such that $a(p - 1) + bn = e$. Then we let $y \equiv r^b \pmod{p}$, and $y^n \equiv r^{nb} \equiv r^{nb+a(p-1)} \equiv r^e \equiv x \pmod{p}$ as required. □

Proposition 2.3 tells us that the only interesting cases are when $p \equiv 1 \pmod{n}$: we only care about the equivalence class of n modulo $p - 1$, and can factor out coprime factors to reduce to the above.
It is worth checking how our definition captures elements being n^{th} powers modulo prime ideals, and how we can find the n^{th} power residue classes modulo p when $p \equiv 1 \pmod{n}$. This second question is not obvious, as we are forced to use n^{th} roots of unity, which do not occur in $\mathbb{Q}$ (for $n > 2$), and so the prime ideals in the number field are not necessarily generated by the integer primes. We will answer this question after a useful lemma and proposition.

Lemma 2.4. *Let L/K be a Galois extension of number fields such that $\zeta_n \in L$. Then for all $\sigma \in Gal(L/K)$ we have*

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n^{\sigma} = \left(\frac{\alpha^\sigma}{\mathfrak{a}^\sigma}\right)_n$$

for all $\alpha \in \mathcal{O}_L/\{0\}$ and ideals $\mathfrak{a}$ coprime to $n\alpha$.

Proof. By definition, if $\mathfrak{p}$ is a prime ideal with norm q, we have

$$\alpha^{\frac{q-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}} \qquad \text{and} \qquad (\alpha^\sigma)^{\frac{q-1}{n}} \equiv \left(\frac{\alpha^\sigma}{\mathfrak{p}^\sigma}\right)_n \pmod{\mathfrak{p}^\sigma}.$$

Apply σ to the first equation and equating them gives the result when $\mathfrak{p}$ is prime. The multiplicativity of the power residue symbol implies the result in general.

□

Note that complex conjugation is an automorphism of any number field over $\mathbb{Q}$, so the above lemma applies to it (we will need this fact later on).

Proposition 2.5. *Let $n \geq 3$, let p be an integer prime such that $p \nmid n$, let f denote the order of p modulo n, and let $K = \mathbb{Q}(\zeta_n)$. Then $p\mathcal{O}_K$ is a product of $\dfrac{\phi(n)}{f}$ distinct prime ideals, each with inertia degree f.*

Proof. Let $\mathfrak{p}$ be any prime ideal lying above p. The residue field $\dfrac{\mathcal{O}_k}{\mathfrak{p}}$ is just $\mathbb{F}_p(\zeta_n)$. Now, $n \mid p^f - 1$ hence $\zeta_n \in \mathbb{F}_{p^f}$. If $0 < r < f$, then $n \nmid p^r - 1$ whence $\zeta_n \notin \mathbb{F}_{p^r}$ (the multiplication group of finite fields is cyclic). Therefore $\dfrac{\mathcal{O}_k}{\mathfrak{p}} = \mathbb{F}_{p^f}$, i.e. the inertia degree of $\mathfrak{p}$ is f. Since $p \nmid n$, p does not ramify, and as $\mathfrak{p}$ was arbitrary and $[K : \mathbb{Q}] = \phi(n)$, the proposition follows.

□

Proposition 2.6. *Let k be a number field containing a primitive n^{th} root of unity ζ_n, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$, coprime to $x \in \mathcal{O}_k$. Then:*
i) $\left(\dfrac{x}{\mathfrak{p}}\right)_n = 1$ iff x is an n^{th} power modulo $\mathfrak{p}$.
ii) $x \in \mathbb{Z}$ is an n^{th} power in $\frac{\mathbb{Z}}{p\mathbb{Z}}$, where $p \equiv 1 \pmod{n}$ is an integer prime, if and only if $\left(\dfrac{x}{\mathfrak{p}}\right)_n = 1$, where $\mathfrak{p}$ is any prime ideal lying above p in $\mathbb{Q}(\zeta_n)$.

Proof. i) If x is an n^{th} power modulo $\mathfrak{p}$, then $x \equiv \alpha^n \pmod{\mathfrak{p}}$. Then $\left(\dfrac{x}{\mathfrak{p}}\right)_n \equiv x^{\frac{q-1}{n}} \equiv \alpha^{q-1} \equiv 1 \pmod{\mathfrak{p}}$ so this direction is proved. If $\left(\dfrac{x}{\mathfrak{p}}\right)_n \equiv 1 \pmod{p}$, then as $\left(\dfrac{\mathcal{O}_k}{\mathfrak{p}}\right)^\times$ is cyclic (multiplication group of a finite field), let it be generated by r. So $x \equiv r^s \pmod{\mathfrak{p}}$. Then $1 \equiv \left(\dfrac{x}{\mathfrak{p}}\right)_n \equiv x^{\frac{q-1}{n}} \equiv r^{\frac{s(q-1)}{n}} \pmod{p}$ implies that $q - 1 \mid \dfrac{s(q-1)}{n}$, i.e. $n \mid s$, so x is indeed an n^{th} power modulo $\mathfrak{p}$.

ii) By Proposition 2.5, the residue field of $\mathfrak{p}$ is just $\mathbb{F}_p$. Therefore $\left(\dfrac{x}{\mathfrak{p}}\right)_n = 1$ if and only if x is an n^{th} power in $\dfrac{\mathcal{O}_k}{\mathfrak{p}} = \mathbb{F}_p$, which is the result we desire.

□

3 Gauss and Jacobi Sums

3.1 A Quadratic Example

When considering quadratic reciprocity, a natural sum to consider is $\tau = \sum\limits_{n=1}^{p-1} \left(\dfrac{n}{p}\right) \zeta_p^n \in \mathbb{Z}[\zeta_p]$ where $\zeta_p = \exp(\dfrac{2\pi i}{p})$ and p is an odd integer prime.

Lemma 3.1. *If p is an odd prime, then $S = \sum\limits_{n=1}^{p-1} \left(\dfrac{n}{p}\right) = 0$*

Proof. Let x be any quadratic non-residue modulo p (which exists as $p > 2$). Then:

$$-S = \left(\frac{x}{p}\right) \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = \sum_{n=1}^{p-1} \left(\frac{nx}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) = S,$$

since $y = nx$ runs through $1, 2, \ldots, p-1$ when n does. Hence $S = 0$. □

Proposition 3.2. *Let τ be defined as above. then:*

i) $\tau^2 = (-1)^{\frac{p-1}{2}} p = p^*$.

ii) $\tau^{q-1} \equiv \left(\dfrac{q}{p}\right) \pmod{q}$ for any odd prime $q \neq p$.

Proof. i) We calculate

$$\tau^2 = \sum_{m=1}^{p-1}\left(\frac{m}{p}\right)\zeta_p^m \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta_p^n = \sum_{m,n}\left(\frac{mn}{p}\right)\zeta_p^{m+n}.$$

Using $x = n/m$, and $\sum_{i=1}^{p} \zeta_p^i = 0$ we thus get:

$$\tau^2 = \sum_{m,x}\left(\frac{m^2x}{p}\right)\zeta_p^{m(1+x)} = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{m=1}^{p-1}(\zeta_p^{1+x})^m.$$

For $x \neq p-1$, ζ_p^{1+x} is a primitive p^{th} root of unity, so this sum is $\sum_{i=1}^{p-1} \zeta_p^i = 0 - \zeta_p^p = -1$. For $x = p-1$, this sum evaluates to $p-1$. Therefore we see that:

$$\tau^2 = -\sum_{x=1}^{p-2}\left(\frac{x}{p}\right) + \left(\frac{-1}{p}\right)(p-1) = p\left(\frac{-1}{p}\right) = p^*,$$

where we used the previous lemma for the second last equality.

ii) Note $\tau = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta_p^n = \sum_{n=1}^{p-1}\left(\frac{nq^2}{p}\right)\zeta_p^n$. Therefore we calculate:

$$\tau^q = \left(\sum_{n=1}^{p-1}\left(\frac{nq^2}{p}\right)\zeta_p^n\right)^q \equiv \sum_{n=1}^{p-1}\left(\frac{nq^2}{p}\right)\zeta_p^{qn} \equiv \left(\frac{q}{p}\right)\tau \pmod{q}.,$$

since nq runs through $1, 2, \ldots, p-1$ modulo p as n does. □

The law of quadratic reciprocity for primes now follows almost immediately (this is easily generalized to the corresponding law for all odd positive integers).

Corollary 3.3 (Law of Quadratic Reciprocity)**.**

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

where p, q are distinct odd positive primes.

Proof. We have

$$\left(\frac{p^*}{q}\right) \equiv (p^*)^{\frac{q-1}{2}} = \tau^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q}, \tag{3.1}$$

and hence equality as $-1 \not\equiv 1 \pmod{q}$. The law now follows from Equation 3.1 and $\left(\frac{-1}{q}\right) = -1$ for $q \equiv 3 \pmod{4}$ (which can be proved by using $(\frac{\mathbb{Z}}{q\mathbb{Z}})^\times$ is cyclic). □

3.2 Gauss and Jacobi Sums

The general version of a Gauss sum is as follows: we have a number field K, and a prime ideal $\mathfrak{p}$. The quotient field is $\frac{\mathcal{O}_k}{\mathfrak{p}} \simeq \mathbb{F}_q$ which is a finite extension of $\mathbb{F}_p$, and $q = p^f$. Let χ be a multiplicative character $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$, and let ψ be an additive character $\psi : \mathbb{F}_q \to \mathbb{C}^\times$.

Definition 3.4. The Gauss sum associated with χ,ψ, and $\alpha \in \mathbb{F}_q^\times$ is

$$G_\alpha(\chi, \psi) = -\sum_{t \in \mathbb{F}_q^\times} \chi(t)\psi(\alpha t). \tag{3.2}$$

Remark. Let $Tr : \mathbb{F}_q \to \mathbb{F}_p$ be the trace map. We will always be taking $\psi(t) = \zeta_p^{Tr(t)}$, so we will drop the ψ in the input. We will also typically take χ to be the n^{th} power residue symbol, or a power of it.

Remark. Let $\mathbb{1}$ be the trivial character, i.e. $\mathbb{1}(t) = 1$ for all $t \in \mathbb{F}_q$. It is convenient to set $\mathbb{1}(0) = 1$ and $\chi(0) = 0$ for all multiplicative characters $\chi \neq \mathbb{1}$. However now, $\chi\chi^{-1} \neq \mathbb{1}$ if multiplication is defined pointwise. Therefore we alter it slightly to the following:

$$(\chi\theta)(t) := \begin{cases} \chi(t)\theta(t) & \text{if } t \neq 0, \\ 0 & \text{if } t = 0 \text{ and } \chi \neq \theta^{-1}, \\ 1 & \text{if } t = 1 \text{ and } \chi = \theta^{-1}. \end{cases} \tag{3.3}$$

We now present some simple results about Gauss sums which will be of use in proving reciprocity laws. First off, we drop the need for the α in the input.

Proposition 3.5. *Define $G(\chi) = G_1(\chi)$. Then $G_\alpha(\chi) = \chi(\alpha)^{-1}G(\chi)$.*

Proof. This is a simple calculation:

$$G_\alpha(\chi) = -\sum_{t \in \mathbb{F}_q^\times} \chi(t)\psi(\alpha t) = -\chi(\alpha)^{-1} \sum_{t \in \mathbb{F}_q^\times} \chi(\alpha t)\psi(\alpha t) = \chi(\alpha)^{-1}G(\chi).$$

□

The introduction of the Jacobi sum comes naturally when attempting to multiply two Gauss sums. First, note that $G(\mathbb{1}) = 1$, which can be derived similarly to the proof of lemma 3.1. So we let $\chi_1, \chi_2 \neq \mathbb{1}$ be nontrivial characters on $\mathbb{F}_q^\times$:

$$G(\chi_1)G(\chi_2) = \sum_{x,y \in \mathbb{F}_q} \chi_1(x)\chi_2(y)\psi(x+y) = \sum_{x,z \in \mathbb{F}_q} \chi_1(x)\chi_2(z-x)\psi(z).$$

Note that we have extended the sum to all of $\mathbb{F}_q$ with reference to the previous remark, and have introduced $z = x + y$. We next split the sum into cases of $z = 0$ and $z \neq 0$:

$$G(\chi_1)G(\chi_2) = \sum_{x \in \mathbb{F}_q, z \in \mathbb{F}_q^\times} \chi_1(x)\chi_2(z-x)\psi(z) + \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(-x).$$

As $\chi_1 \neq \mathbb{1}$, $\chi_1(0) = 0$, and so the second sum is $\chi_1(-1) \sum_{x \in \mathbb{F}_q^\times} \chi_1\chi_2(-x)$. So if $\chi_1\chi_2 \neq \mathbb{1}$, then just as in lemma 3.1 we get the sum being 0. Otherwise, the sum is $\chi_1(-1)(q-1)$.

For the first sum, we make the change of variable of removing x and introducing $r = x/z$ (as $z \neq 0$), and we calculate:

$$\begin{aligned} \sum_{x, z \neq 0 \in \mathbb{F}_q} \chi_1(x)\chi_2(z-x)\psi(z) &= \sum_{r \in \mathbb{F}_q, z \in \mathbb{F}_q^\times} \chi_1(z)\chi_2(z)\psi(z)\chi_1(r)\chi_2(1-r) \\ &= \Big(\sum_{z \in \mathbb{F}_q^\times} \chi_1\chi_2(z)\psi(z)\Big)\Big(\sum_{r \in \mathbb{F}_q} \chi_1(r)\chi_2(1-r)\Big) \\ &= G(\chi_1\chi_2)\Big(-\sum_{r \in \mathbb{F}_q} \chi_1(r)\chi_2(1-r)\Big). \end{aligned}$$

Definition 3.6. For nontrivial multiplicative characters $\chi_1, \chi_2 \neq \mathbb{1}$ on $\mathbb{F}_q^\times$, the *Jacobi sum* of χ_1 and χ_2 is $J(\chi_1, \chi_2) = -\sum_{r \in \mathbb{F}_q} \chi_1(r)\chi_2(1-r)$.

The above calculations give us:

$$G(\chi_1)G(\chi_2) = G(\chi_1\chi_2)J(\chi_1, \chi_2), \tag{3.4}$$

as long as none of $\chi_1, \chi_2, \chi_1\chi_2$ are $\mathbb{1}$.

When $\chi = \chi_1 = \chi_2^{-1}$, we get $G(\chi, \chi^{-1}) = \chi(-1)(q-1) + G(\mathbb{1})J(\chi, \chi^{-1})$. So we calculate the Jacobi sum:

$$J(\chi, \chi^{-1}) = -\sum_{r\in\mathbb{F}_q} \chi(r)\chi^{-1}(1-r) = -\sum_{r\in\mathbb{F}_q\setminus\{1\}} \chi(\frac{r}{1-r}).$$

Now, $\mathbb{F}\setminus\{1\} \to \mathbb{F}\setminus\{-1\} : r \to \frac{r}{1-r} = -1 + \frac{1}{1-r}$ is a bijection, hence this sum is just $-\sum_{t\in\mathbb{F}_q\setminus\{-1\}} \chi(t) = \chi(-1)$. Therefore $G(\chi)G(\chi^{-1}) = \chi(-1)q$. We collect the above results (and a couple of new ones) into a proposition.

Proposition 3.7. *For all $\alpha \in \mathbb{F}_q^\times$ and nontrivial characters $\chi, \chi_1, \chi_2 \neq \mathbb{1}$ such that $\chi_1\chi_2 \neq \mathbb{1}$, where χ has order n, we have:*

$i) G_\alpha(\chi) \in \mathbb{Z}[\zeta_p, \zeta_n]$;	$iv) G(\chi_1)G(\chi_2) = G(\chi_1\chi_2)J(\chi_1, \chi_2)$;
$ii) G_\alpha(\chi) = \chi(\alpha)^{-1}G(\chi)$;	$v) \chi(-1)G(\chi^{-1}) = \overline{G(\chi)}$;
$iii) G(\chi)G(\chi^{-1}) = \chi(-1)q$;	$vi) G(\chi)\overline{G(\chi)} = q$.

Proof. i) is clear, we have already proved $ii) - iv)$, and $vi)$ follows from $v)$ and $iii)$ (noting $\chi(-1)^2 = 1$). For $v)$, we calculate:

$$\overline{G(\chi)} = -\sum_{t\in\mathbb{F}_q^\times} \chi(t)^{-1}\psi(t)^{-1} = -\chi(-1)^{-1}\sum_{t\in\mathbb{F}_q^\times} \chi(-t)^{-1}\psi(-t) = \chi(-1)G(\chi^{-1}),$$

where we have used that the complex conjugate of a root of unity is its inverse. □

Recall that in the previous section we showed $\tau^2 = \pm p$; here $\tau = -G(\chi)$ when χ is the quadratic residue symbol in $\mathbb{Z}$. The result that generalizes this is the following corollary.

Corollary 3.8. *Let χ be a character of order n on $\mathbb{F}_q$. Then:*

$$G(\chi)^r = G(\chi^r)J(\chi, \chi)J(\chi, \chi^2)\cdots J(\chi, \chi^{r-1})$$

for all $1 \leq r \leq n-1$. Furthermore,

$$G(\chi)^n = \chi(-1)qJ(\chi, \chi)J(\chi, \chi^2)\cdots J(\chi, \chi^{n-2}) \in \mathbb{Z}[\zeta_n]. \tag{3.5}$$

Proof. The first part is derived by repeatedly applying property iv) of proposition 3.7. For the second equation, take $r = n-1$, multiply each side by $G(\chi)$, and simplify using $\chi^{n-1} = \chi^{-1}$ (χ has order n) and $G(\chi)G(\chi^{-1}) = \chi(-1)q$. □

We have derived some interesting results so far, however it is not immediately clear how they relate to reciprocity. We will require the prime ideal factorizations of Gauss and Jacobi sums, as well as a result analogous to Proposition 3.2ii).

Proposition 3.9. *Let $p \equiv 1 \pmod{n}$ be an integer prime, let $\mathfrak{p}$ be any prime ideal lying above p in $K = \mathbb{Q}(\zeta_n)$, and let $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_n$ be the power residue symbol. If $r \equiv 1 \pmod{n}$ is any integer prime not equal to p, then*

$$G(\chi)^{r-1} \equiv \chi(r)^{-1} \pmod{r}. \tag{3.6}$$

Proof. By proposition 2.5, p splits into a product of $\phi(n)$ primes, all with inertia degree 1 (note that similarly if $\mathfrak{p}$ has inertia degree 1, then the integer prime it lies above is also $1 \pmod{n}$). The inertia degree being 1 implies that $G(\chi) = -\sum_{t=1}^{p-1} \chi(t)\zeta_p^t$. Now we calculate (noting that r is odd as $n \mid r-1$, and r is prime):

$$G(\chi)^r \equiv -\sum_{t=1}^{p-1} \chi(t)^r \zeta_p^{rt} = -\sum_{t=1}^{p-1} \chi(t)\zeta_p^{rt} = \chi(r)^{-1}G(\chi) \pmod{r}.$$

Multiply each side by $\overline{G(\chi)}$, use $G(\chi)\overline{G(\chi)} = p$, and divide out by p (which is coprime to r) and we get the result. □

To obtain the factorizations of the sums for small powers, the following lemma and proposition will suffice.

Lemma 3.10. *Let p be an integer prime. Then:*

$$\sum_{a=1}^{p-1} a^k \equiv \begin{cases} 0 \pmod{p}, & \text{if } 0 < k < p-1; \\ -1 \pmod{p}, & \text{if } k = p-1. \end{cases}$$

Proof. For $k = p-1$ this is trivial by Fermat's Little Theorem, and otherwise the proof follows exactly as the proof of lemma 3.1. □

Proposition 3.11. *Adopting the notation of Proposition 3.9, we have $J(\chi^a, \chi^b) \equiv 0 \pmod{\mathfrak{p}}$ for all integers $a, b \geq 1$ such that $a + b \leq n-1$.*

Proof. As $\mathfrak{p}$ has degree 1, we can write the Jacobi sum as $J(\chi^a, \chi^b) = -\sum\limits_{t=0}^{p-1} \chi^a(t)\chi^b(1-t)$. Since by definition we have $\chi(t) \equiv t^{\frac{p-1}{n}} \pmod{\mathfrak{p}}$ for all t, and $\chi(0) = 0$, we can write this sum as:

$$J(\chi^a, \chi^b) \equiv -\sum_{t=1}^{p-1} t^{\frac{a(p-1)}{n}}(1-t)^{\frac{b(p-1)}{n}} \pmod{\mathfrak{p}}.$$

Upon expansion, the exponent of the t's are at most $\dfrac{a(p-1)}{n} + \dfrac{b(p-1)}{n} = (p-1)\dfrac{a+b}{n} < p-1$ as $a+b \leq n-1$. So by the previous lemma, the sum over t of these is 0 modulo $\mathfrak{p}$, and hence the entire sum is 0 modulo $\mathfrak{p}$. □

4 Cubic and Quartic Reciprocity

4.1 Cubic Reciprocity

The cubic case is fairly simple, as we can find the prime ideal factorization of $G(\chi)$ fairly easily. Throughout this section, we will let $\omega = \zeta_3 = \dfrac{-1+\sqrt{-3}}{2}$. Recall that $K = \mathbb{Q}(\omega)$ has class number 1, so $\mathbb{Z}[\omega]$ is a PID and a UFD (and thus the primes coincide with the prime ideals). Since K is an imaginary quadratic field, the norm on K is just the typical modulus on $\mathbb{C}$, i.e. $|\cdot|$. We begin with some quick propositions dealing with the units in $\mathbb{Z}[\omega]$, and their ramifications (the non-mathematical sense of the word).

Proposition 4.1. *The units of $\mathbb{Z}[\omega]$ are $\pm\omega^r$ for $r = 1, 2, 3$.*

Proof. Recall $a + b\omega$ $(a, b \in \mathbb{Z})$ is a unit if and only if $\pm 1 = |a + b\omega|$ (as this is the norm over $\mathbb{Q}$). Well, we calculate:

$$|a + b\omega| = \left|\frac{2a - b + b\sqrt{-3}}{2}\right| = \frac{1}{4}\sqrt{(2a-b)^2 + 3b^2} = \sqrt{a^2 - ab + b^2}.$$

Therefore this amounts to solving $a^2 - ab + b^2 = 1$. If $ab > 0$, then $(a-b)^2 < a^2 - ab + b^2$ hence $a - b = 0$, and then $a = b = \pm 1$. If $ab < 0$, then $(a+b)^2 < a^2 - ab + b^2$ so now $a = -b$ and we get no solutions. Finally, $ab = 0$ gives us $(a, b) = (\pm 1, 0), (0, \pm 1)$, so all together there are precisely 6 distinct units. Since $\pm\omega^r$ for $r = 1, 2, 3$ are 6 distinct units, this is the entire set. □

Definition 4.2. In the ring of integers of a number field, nonzero numbers x and y are called *associates* if their ratio is a unit.

Proposition 4.3. *If $x \in \mathbb{Z}[\omega]$ is coprime to* 3*, then exactly one associate of x is equivalent to* 1 *modulo* 3*.*

Proof. Since $3 = (\sqrt{-3})^2 = (1+2\omega)^2$, we see that $\dfrac{\mathcal{O}_K}{3} \simeq \dfrac{\mathbb{Z}}{9\mathbb{Z}}$. Since precisely one unit is equivalent to 1 (mod 3), they are all distinct modulo 3, and hence form the 6 residue classes modulo 3 which are coprime to 3. So if x is coprime to 3, it falls into exactly one of these classes, and thus the result follows. □

It is worth explicitly pointing out that modulo 3 has a slightly different meaning than normal here: typically the residue classes are $0, 1, 2$. However, when working in $\mathbb{Q}(\omega)$, the residue classes are now $a + b\omega$ where $a, b \in \{0, 1, 2\}$. As 3 is no longer a prime, this is no longer an integral domain either.

Proposition 4.4. *Let $p \equiv 1 \pmod 3$ be an integer prime, and χ a character of order* 3 *on $\mathbb{F}_p$. Since $J(\chi,\chi) \in \mathbb{Z}[\omega]$, let $J(\chi,\chi) = a + b\omega$ with $a, b \in \mathbb{Z}$. Then we have $p = a^2 - ab + b^2$, $a \equiv 1 \pmod 3$, and $b \equiv 0 \pmod 3$.*

Proof. Proposition 3.7 showed that $G(\chi)\overline{G(\chi)} = p$, and Corollary 3.8 gives us $G(\chi)^3 = pJ(\chi,\chi)$ (since χ has order 3, $\chi(-1) = \chi(-1)^3 = 1$). Thus $|G(\chi)| = \sqrt{p}$, and so $|J(\chi,\chi)| = \dfrac{1}{p}|G(\chi)^3| = \sqrt{p}$. But we have $J(\chi,\chi)| = |a + b\omega| = \sqrt{a^2 - ab + b^2}$, whence we get $p = a^2 - ab + b^2$.

To finish, we need to show that $J(\chi,\chi) \equiv 1 \pmod 3$. Well, we calculate:

$$G(\chi)^3 \equiv -\sum_{t=0}^{p-1} \chi^3(t)\zeta_p^{3t} = -\sum_{t=1}^{p-1} \zeta_p^t = 1 \pmod 3.$$

We now get: $J(\chi,\chi) \equiv pJ(\chi,\chi) = G(\chi)^3 \equiv 1 \pmod 3$, finishing the proposition. □

Corollary 4.5. *Let π be a prime in $\mathbb{Z}[\omega]$ such that $\pi \equiv 1 \pmod 3$, and π lies above an integral prime $p \equiv 1 \pmod 3$. Letting $\chi = \left(\frac{\cdot}{\pi}\right)_3$, then:*

$$J(\chi,\chi) = \pi,\ G(\chi)^3 = \pi^2\overline{\pi}. \tag{4.1}$$

Proof. Proposition 3.11 tells us that $\pi \mid J(\chi,\chi)$. But $|J(\chi,\chi)| = \sqrt{p} = \pi$ from the preceding proposition, so π and $J(\chi,\chi)$ differ by a unit. As $J(\chi,\chi) \equiv 1 \equiv \pi \pmod 3$, we get $J(\chi,\chi) = \pi$. The second part follows from $p = |\pi|^2 = \pi\overline{\pi}$. □

Definition 4.6. A number in $\mathbb{Z}[\omega]$ is called *primary* if it is equivalent to a nonzero integer modulo $(1-\omega)^2$. This is equivalent to it being $\pm 1 \pmod 3$.

Remark. We have to be a bit careful: as we are in a PID, we can and will refer to ideals by any generator. So when $\left(\frac{\alpha}{\beta}\right)_3$ is written, β is in fact the *ideal* generated by β and not the elements β. Hence this value does not change when multiplying β by a unit. However, multiplying the α by a unit can in fact change the value of the symbol! Thus, for reciprocity laws, we will often need assumed conditions about the inputs, and this does not lose us any generality.

Proposition 4.7. *Let $\alpha \in \mathbb{Z}[\omega]$ be primary, and $a \in \mathbb{Z}$ be such that α, a are relatively prime. Then:*

$$\left(\frac{\alpha}{a}\right)_3 = \left(\frac{a}{\alpha}\right)_3.$$

Furthermore, $\left(\frac{a}{b}\right)_3 = 1$ for all relatively prime $a, b \in \mathbb{Z}$ with $3 \nmid b$.

Proof. Since the cubic reciprocity symbol is multiplicative, it will suffice to prove $\left(\frac{\alpha}{a}\right)_3 = \left(\frac{a}{\alpha}\right)_3$ when $\alpha \in \mathbb{Z}[\omega]$ is prime and $a \in \mathbb{Z}^+$ is an integer prime (also noting that $\left(\frac{-1}{x}\right)_3 = 1$ for all x). We split into three cases:

Case 1: $p = \alpha\overline{\alpha} \equiv 1 \pmod 3$ is an integer prime, and $a = q = \lambda\overline{\lambda} \equiv 1 \pmod 3$.

Let $\chi = \left(\frac{\cdot}{\alpha}\right)_3$, Proposition 3.9 tells us that $G(\chi)^{q-1} \equiv \chi(q)^{-1} \equiv \chi(q)^2 \pmod q$. Using the Gauss sum factorization, we get:

$$\left(\frac{q}{\alpha}\right)_3^2 \equiv G(\chi)^{q-1} = (\alpha^2\overline{\alpha})^{\frac{q-1}{3}} \equiv \left(\frac{\alpha^2\overline{\alpha}}{\lambda}\right)_3 \pmod \lambda,$$

hence

$$\left(\frac{q}{\alpha}\right)_3^2 = \left(\frac{\alpha^2\overline{\alpha}}{\lambda}\right)_3. \tag{4.2}$$

Observe that

$$\left(\frac{\overline{\alpha}}{\lambda}\right)_3 = \overline{\left(\frac{\alpha}{\overline{\lambda}}\right)_3} = \left(\frac{\alpha}{\overline{\lambda}}\right)_3^{-1} = \left(\frac{\alpha}{\overline{\lambda}}\right)_3^2.$$

Simplifying the right hand side of 4.2 gives us:

$$\left(\frac{\alpha^2\overline{\alpha}}{\lambda}\right)_3 = \left(\frac{\alpha}{\lambda\overline{\lambda}}\right)_3^2 = \left(\frac{\alpha}{q}\right)_3^2.$$

Squaring yields the equation $\left(\frac{q}{\alpha}\right)_3 = \left(\frac{\alpha}{q}\right)_3$, as desired.

Case 2: $p = \alpha\overline{\alpha} \equiv 1 \pmod 3$ is an integer prime, and $a = q \equiv 2 \pmod 3$.

In this case, we modify 3.9:

$$G(\chi)^q \equiv -\sum_{t=1}^{p-1} \chi(t)^q \zeta_p^{qt} = -\sum_{t=1}^{p-1} \chi(t)^2 \zeta_p^{qt} = \chi(q^2)^2 G(\chi^2) = \chi(q) G(\chi^{-1}) \pmod q.$$

Thus we have

$$G(\chi)^{q+1} \equiv \chi(q) G(\chi^{-1}) G(\chi) = \chi(q) p \pmod q.$$

Therefore

$$\alpha\overline{\alpha}\chi(q) \equiv G(\chi)^{q+1} = (\alpha^2\overline{\alpha})^{\frac{q+1}{3}} \pmod q. \tag{4.3}$$

Writing $\alpha = x + y\omega$, we get

$$\alpha^q \equiv x^q + y^q\omega^q \equiv x + y\omega^{-1} = \overline{\alpha} \pmod q.$$

Using this in Equation 4.3 gives us

$$\alpha^{q+1}\left(\frac{q}{\alpha}\right)_3 \equiv (\alpha^{q+2})^{\frac{q+1}{3}} \pmod q.$$

Finally, this yields

$$\left(\frac{q}{\alpha}\right)_3 \equiv \alpha^{\frac{q^2-1}{3}} \equiv \left(\frac{\alpha}{q}\right)_3 \pmod q.$$

We can drop the modulo q, yielding the desired equality.

Case 3: $\alpha = p \equiv 2 \pmod 3$ and $a = q \equiv 2 \pmod 3$ are integer primes.

First, note that this is the last case, since $\alpha = p \equiv 2 \pmod 3$ and $a = q \equiv 1 \pmod 3$ is a consequence of case 2 (switch a, α, repeat with $\overline{\alpha}$ instead of α, and multiply). Case 3 is in fact trivial; Proposition 2.3 tells us that $\left(\frac{q}{p}\right)_3 = 1 = \left(\frac{p}{q}\right)_3$

For the last part of the proposition, it suffices to show the result when b is an integer prime. If $b \equiv 2 \pmod 3$, then we are done by Proposition 2.3. Otherwise, $b = \lambda\overline{\lambda} \equiv 1 \pmod 3$, and:

$$\left(\frac{a}{b}\right)_3 = \left(\frac{a}{\lambda\overline{\lambda}}\right)_3 = \left(\frac{a}{\lambda}\right)_3 \left(\frac{a}{\overline{\lambda}}\right)_3 = \left(\frac{a}{\lambda}\right)_3 \overline{\left(\frac{a}{\lambda}\right)_3} = \left(\frac{a}{\lambda}\right)_3 \left(\frac{a}{\lambda}\right)_3^2 = 1,$$

as claimed. □

Proposition 4.8. *Let p, q be integers with $p \equiv 1 \pmod 3$ and $q \equiv 2 \pmod 3$. Then the following supplementary laws hold:*

$$\left(\frac{\omega}{p}\right)_3 = \omega^{\frac{1-p}{3}}; \qquad \left(\frac{\omega}{q}\right)_3 = \omega^{\frac{1+q}{3}};$$

$$\left(\frac{1-\omega}{p}\right)_3 = \omega^{\frac{p-1}{3}}; \qquad \left(\frac{1-\omega}{q}\right)_3 = \omega^{\frac{-1-q}{3}}.$$

Proof. First, assume p, q are integer primes. If $p = \alpha\overline{\alpha} \equiv 1 \pmod 3$, then

$$\left(\frac{\omega}{p}\right)_3 = \left(\frac{\omega}{\alpha}\right)_3 \left(\frac{\omega}{\overline{\alpha}}\right)_3 = \left(\frac{\omega}{\alpha}\right)_3 \left(\frac{\omega^2}{\alpha}\right)_3^2 = \left(\frac{\omega}{\alpha}\right)_3^2 = \omega^{\frac{2(p-1)}{3}} = \omega^{\frac{1-p}{3}}.$$

Next,

$$\left(\frac{\omega}{q}\right)_3 = \omega^{\frac{q^2-1}{3}} = (\omega^{\frac{q+1}{3}})^{q-1} = \omega^{\frac{q+1}{3}}.$$

The extension to all composite integers comes from the following sequence of calculations:
If $x = 3m+1$, $y = 3n+1$ then

$$\frac{1-xy}{3} \equiv -m-n \equiv \frac{1-x}{3} + \frac{1-y}{3} \pmod 3.$$

If $x = 3m+1$, $y = 3n+2$ then

$$\frac{1+xy}{3} \equiv n+2m+1 \equiv -m+n+1 \equiv \frac{1-x}{3} + \frac{1+y}{3} \pmod 3.$$

If $x = 3m+2$, $y = 3n+2$ then

$$\frac{1-xy}{3} \equiv -2m-2n-1 \equiv m+1+n+1 \equiv \frac{1+x}{3} + \frac{1+y}{3} \pmod 3.$$

From the preceding proposition, if $x \in \mathbb{Z}$ is coprime to 3, then we have $\left(\frac{3}{x}\right)_3 = 1$. Thus

$$\left(\frac{1-\omega}{x}\right)_3 = \left(\frac{1-\omega}{x}\right)_3^4 = \left(\frac{-3\omega}{x}\right)_3^2 = \left(\frac{\omega}{x}\right)_3^2, \tag{4.4}$$

from which the last two equations follow. □

We are now ready for the main result of this subsection: the cubic reciprocity law in $\mathbb{Q}(\omega)$!

Theorem 4.9. *[Eisenstein's Law of Cubic Reciprocity] Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be primary and relatively prime. Then*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3$$

Furthermore, if $\alpha = a + b\omega$ with $a = 3m+1$ and $b = 3n$, then

$$\left(\frac{\omega}{\alpha}\right)_3 = \omega^{\frac{1-a-b}{3}} = \omega^{-m-n}; \qquad \left(\frac{1-\omega}{\alpha}\right)_3 = \omega^{\frac{a-1}{3}} = \omega^m.$$

Proof. As always, we can assume α, β are prime and primary. If one of them is an integer prime, then it is equivalent to 2 modulo 3 and this case is covered in 4.7. Thus assume $\alpha\overline{\alpha} = p \equiv 1 \pmod 3$ and $\beta\overline{\beta} = q \equiv 1 \pmod 3$ are integer primes.

Case 1: p, q are distinct

Equation 4.2 applied to (p, q) and (q, p) gives us:

$$\left(\frac{q}{\alpha}\right)_3^2 = \left(\frac{\alpha^2\overline{\alpha}}{\beta}\right)_3; \qquad\qquad \left(\frac{\beta^2\overline{\beta}}{\alpha}\right)_3 = \left(\frac{p}{\beta}\right)_3^2.$$

Multiply these equations, substitute the factorizations for p, q, and cancel out cubes to get $\left(\frac{\beta}{\alpha}\right)_3 = \left(\frac{\alpha}{\beta}\right)_3$ as we desire.

Case 2: $p = q$

This case is made easy by a clever manipulation:

$$\left(\frac{\overline{\alpha}}{\alpha}\right)_3 = \left(\frac{\overline{\alpha}+\alpha}{\alpha}\right)_3 = \left(\frac{\alpha}{\overline{\alpha}+\alpha}\right)_3 = \left(\frac{-\overline{\alpha}}{\overline{\alpha}+\alpha}\right)_3 = \left(\frac{\overline{\alpha}+\alpha}{\overline{\alpha}}\right)_3 = \left(\frac{\alpha}{\overline{\alpha}}\right)_3.$$

The second equality is valid since $\alpha, \overline{\alpha}+\alpha$ are relatively prime and primary, and so case 1 applies (the fourth equality is similar).

For the first supplementary law, we first note that

$$\left(\frac{\omega}{\overline{\alpha}}\right)_3 = \left(\frac{\overline{\omega^2}}{\overline{\alpha}}\right)_3 = \overline{\left(\frac{\omega}{\alpha}\right)_3^2} = \left(\frac{\omega}{\alpha}\right)_3.$$

Multiplying each side by $\left(\frac{\omega}{\alpha}\right)_3$ gives

$$\left(\frac{\omega}{\alpha}\right)_3^2 = \left(\frac{\omega}{p}\right)_3 = \omega^{\frac{1-p}{3}} = \omega^{\frac{1-a^2+ab-b^2}{3}},$$

where we used Proposition 4.8 for the second equality. Since $a \equiv 1 \pmod 3$ and $b \equiv 0 \pmod 3$, we get $(a-1)^2 \equiv b^2 \equiv (a-1)b \equiv 0 \pmod 9$, and therefore $1 - a^2 + ab - b^2 \equiv 1 - (2a-1) + b - 0 \equiv -1 + a + b \pmod 9$. Hence

$$\left(\frac{\omega}{\alpha}\right)_3^2 = \omega^{-\frac{1-a-b}{3}}.$$

Squaring this equation yields the first supplementary law.

For the second supplementary law, consider the following:

$$\left(\frac{3\omega}{\alpha}\right)_3 = \left(\frac{-3\omega}{\alpha}\right)_3 = \left(\frac{\alpha-3\omega}{\alpha}\right)_3 = \left(\frac{\alpha}{\alpha-3\omega}\right)_3 = \left(\frac{3\omega}{\alpha-3\omega}\right)_3.$$

Apply this n times, and use the first law to get

$$\left(\frac{3\omega}{\alpha}\right)_3 = \left(\frac{3\omega}{a}\right)_3 = \left(\frac{\omega}{a}\right)_3 = \omega^{\frac{1-a}{3}}.$$

The second supplementary now follows easily from

$$\left(\frac{1-\omega}{\alpha}\right)_3 = \left(\frac{1-\omega}{\alpha}\right)_3^4 = \left(\frac{-3\omega}{\alpha}\right)_3^2 = \omega^{\frac{a-1}{3}}.$$

□

We shall end this subsection with a warning: if $\left(\frac{\alpha}{\beta}\right)_3 = 1$ then it does *not* necessarily mean that α is a cube modulo β (just as it is for the Jacobi symbol). This mistake is easier to make now because integer primes equivalent to 1 modulo 3 are no longer prime! As an example, $13 \equiv -1 \pmod 7$ hence $\left(\frac{13}{7}\right)_3 = 1$, and so we conclude that $\left(\frac{7}{13}\right)_3 = 1$. Letting $13 = \alpha\overline{\alpha}$, Proposition 2.6ii told us that 7 is a cube modulo 13 if and only if $\left(\frac{7}{\alpha}\right)_3 = 1$, *not* if $\left(\frac{7}{13}\right)_3 = 1$. In fact, 7 is not a square modulo 13.

4.2 Quartic Reciprocity

The quartic reciprocity law is similar to the cubic law, but it is not a consequence of the Eisenstein reciprocity law proved in the next section. Thus the result is of interest, but the methods involved are very similar to what we have already seen, so we will present the key steps only. For a full breakdown, see sections 6.2 and 6.3 of [3].

We are working in $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, which has $\mathbb{Z}[i]$ as the ring of integers.

Definition 4.10. Call $x \in \mathbb{Z}[i]$ *primary* if $x \equiv 1 \pmod{2+2i}$.

Proposition 4.11. *Let $p \equiv 1 \pmod 4$ be an integer prime, let χ be a character of order 4 on $\mathbb{F}_p$, and let $J(\chi,\chi) = a + bi$ with $a, b \in \mathbb{Z}$. Then $a \equiv 1 \pmod 4$, $p = a^2 + b^2$, and*

$$J(\chi,\chi^2) = \chi(-1)J(\chi,\chi), \qquad\qquad G(\chi)^4 = p \cdot J(\chi,\chi)^2.$$

Proposition 4.12. *Let $\pi \equiv 1 \pmod{(1+i)^3}$ be prime in $\mathbb{Z}[i]$, and let $\chi = \left(\frac{\cdot}{\pi}\right)_4$ be the power residue symbol. Then*

$$J(\chi,\chi) = \chi(-1)\pi, \qquad\qquad J(\chi,\chi^2) = \pi, \qquad\qquad G(\chi)^4 = \pi^3\overline{\pi}.$$

Theorem 4.13 (Quartic Reciprocity Law). *Let $\alpha = a + bi, \beta = c + di$ be relatively prime and primary Gaussian integers. Then we have*

$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\beta}{\alpha}\right)_4^{-1} = (-1)^{\frac{N\alpha-1}{4}\frac{N\beta-1}{4}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}} = (-1)^{\frac{bd}{4}}$$

Furthermore, there are supplementary laws

$$\left(\frac{i}{\alpha}\right)_4 = i^{\frac{1-a}{2}}, \qquad\qquad \left(\frac{1+i}{\alpha}\right)_4 = i^{\frac{a-b-b^2-1}{4}}, \qquad\qquad \left(\frac{2}{\alpha}\right)_4 = i^{\frac{-b}{2}}$$

5 Eisenstein Reciprocity

5.1 Gauss Sum Factorization

Before we start off, we should recall a few useful facts. Let $K = \mathbb{Q}(\zeta_n)$, and $\mathfrak{p}$ be a prime ideal of K above $p \equiv 1 \pmod n$. Proposition 2.5 tells us that $\mathfrak{p}$ has inertia degree 1, so p splits completely. Let χ be a multiplicative character on $\mathbb{F}_p$, then Proposition 3.7 says $G(\chi)\overline{G(\chi)} = p$, and Corollary 3.8 gives $G(\chi)^n \in \mathbb{Z}[\zeta_n]$. Hence the only prime ideals that can occur in the prime factorization of $G(\chi)^n$ in $\mathbb{Z}[\zeta_n]$ all lie above p.

The Galois group $G = Gal(K/\mathbb{Q})$ acts transitively on the prime ideals above p, hence letting $\mu = G(\chi)^n$ we can write $\mu\mathcal{O}_K = \mathfrak{p}^\gamma$, where $\gamma = \sum\limits_{\sigma} b_\sigma \sigma \in \mathbb{Z}[G]$ (note that γ depends on the choice of $\mathfrak{p}$ lying above p). Thus to determine the factorization, it suffices to determine γ. We will do so with a series of lemmas.

Lemma 5.1. *Let $\gamma = \sum\limits_{\sigma} b_\sigma \sigma$ be defined as above. Then*

$$\sum_{\sigma \in G} b_\sigma = \frac{1}{2}n\phi(n),$$

and $0 \leq b_\sigma \leq n$,

Proof. Taking norms, we find that

$$N_{K/\mathbb{Q}}\mu = N_{K/\mathbb{Q}}\mathfrak{p}^{\gamma} = p^{\sum_{\sigma \in G} b_\sigma}, \text{ and}$$

$$N_{K/\mathbb{Q}}\mu^2 = N_{K/\mathbb{Q}}(\mu\overline{\mu}) = N_{K/\mathbb{Q}}(p^n) = p^{n\phi(n)}.$$

Squaring the first equation and equating to the second gives the equality. The first half of the inequality is from $G(\chi)^n = \mu \in \mathbb{Z}[\zeta_n]$ (it is integral over $\mathbb{Z}$), and the second half is from $\mu\overline{\mu} = p^n$. □

Note that if $S = \{x | 1 \leq x \leq n, \ \gcd(n, x) = 1\}$ then the size of S is $\phi(n)$ and the sum of the elements of S is $\frac{1}{2}n\phi(n)$ (pair up x with $n - x$). As the Galois group has size $\phi(n)$, this suggests that S and $\{b_\sigma\}$ are the same set.

Lemma 5.2. *Let χ be a character with order n on $\mathbb{F}_p$ where $p \equiv 1 \pmod{n}$. Let $G(\chi)$ be the Gauss sum associated to χ, and put $L = \mathbb{Q}(\zeta_n, G(\chi))$. Then $L \subset \mathbb{Q}(\zeta_{np})$ and $[L : \mathbb{Q}(\zeta_n)] = n$.*

Proof. The inclusion $\mathbb{Q}(\zeta_n) \subset L \subset \mathbb{Q}(\zeta_{np})$ is clear. All extensions here are abelian, so $\mathrm{Gal}(L/\mathbb{Q}(\zeta_n))$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{np})/\mathbb{Q}(\zeta_n)) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (the inclusion is clear, and the groups are isomorphic since both have the size $\phi(p) = p - 1$ as n, p are coprime). Therefore this Galois group is cyclic.

Take g to be a primitive root in $\mathbb{F}_p$, and let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{np})/\mathbb{Q})$ be $\sigma : \zeta_p \to \zeta_p^g$ and $\zeta_n \to \zeta_n$. As χ has order n, and g is a primitive root, we see that $\chi(g)$ must be a primitive n^{th} root of unity. Now, σ is a generator for $\mathrm{Gal}(\mathbb{Q}(\zeta_{np})/\mathbb{Q}(\zeta_n)$, hence $\sigma|_L$ generates $\mathrm{Gal}(L/\mathbb{Q}(\zeta_n)$. We have

$$G(\chi)^\sigma = -\sum_{t=1}^{p-1} \chi(t)\zeta_p^{gt} = \chi(g)^{-1}G(\chi),$$

whence σ^n is the smallest power of σ which fixes L. Thus $\mathrm{Gal}(L/\mathbb{Q}(\zeta_n))$ is cyclic of order n, generated by $\sigma|_L$, and the conclusion follows. □

Lemma 5.3. *Let $\gamma = \sum_\sigma b_\sigma \sigma$ be defined as before. Then* $\gcd(b_\sigma, n) = 1$.

Proof. Let $\mathfrak{p}$ be a prime above p in K with $\mathfrak{p}^a || G(\chi)^n = \mu$; we need to show $\gcd(a, n) = 1$. Since $G(\chi)$ satisfies $f(x) = x^n - \mu$ in $K[x]$, and $[L : K] = n$ from the above lemma, $f(x)$ is the minimal polynomial of $G(\chi)$ over $K[x]$.

Recall that $K \subset L \subset \mathbb{Q}(\zeta_n, \zeta_p)$, p ramifies completely in $\mathbb{Q}(\zeta_p)$ and splits completely in $\mathbb{Q}(\zeta_n)$. Hence K is the decomposition field of p inside $\mathbb{Q}(\zeta_n, \zeta_p)$, and $\mathfrak{p}$ ramifies completely in any field between K and $\mathbb{Q}(\zeta_n, \zeta_p)$. Thus there is exactly one prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ that lies above $\mathfrak{p}$, and $\mathfrak{p} = \mathfrak{q}^n$. We have

$$\frac{K_\mathfrak{p}[x]}{f(x)} = L \oplus K_\mathfrak{p} \cong \oplus_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P} = L_\mathfrak{q}.$$

In particular, this implies that $f(x)$ is irreducible in $K_\mathfrak{p}[x]$.

Let $w = \gcd(n, a)$, and since $\mathfrak{q}^{na} = \mathfrak{p}^a || G(\chi)^n$, we get $\mathfrak{q}^a || G(\chi)$. In $L_\mathfrak{q}$, we have $G(\chi) = \mathfrak{q}^a u$ where u is a unit (recall that complete fields are PIDs, so we can work with our prime ideal as being an actual element). So $\mu = \mathfrak{p}^a u^n$ in $K_\mathfrak{p}$ and $v = u^n$ must be a unit of $K_\mathfrak{p}$. Now, $g(x) = x^n - v$ has a solution in $L_\mathfrak{q}$, so this descends to a solution of $\overline{g}(x)$ in the residue field, which is $\mathbb{F}_p$ ($\mathfrak{q}$ has inertia degree 1). As v is a unit, $v \neq 0$ in $\mathbb{F}_p$, and so the root in $\mathbb{F}_p$ is nonzero. But $\mathbb{F}_p$ contains all n^{th} roots of unity, hence $\overline{g}(x)$ is separable and splits in $\mathbb{F}_p$! The residue field of $K_\mathfrak{p}$ is also $\mathbb{F}_p$, whence as $g(x) \in K_\mathfrak{p}[x]$, we see that its reduction is separable and splits in the residue field of $K_\mathfrak{p}$, so by Hensel's lemma all roots of $g(x)$ are in $K_\mathfrak{p}$. So $u \in K_\mathfrak{p}$, and $\mu = u^n \mathfrak{p}^a$ is true in $K_\mathfrak{p}$.

Take $f(x) = x^n - \mu$, and then $x^{\frac{n}{w}} - u^{\frac{n}{w}} \mathfrak{p}^{\frac{a}{w}} | f(x)$ in $K_\mathfrak{p}[x]$. Since $f(x)$ is irreducible in $K_\mathfrak{p}[x]$, this immediately implies that $w = 1$, hence the lemma is proven. □

For $1 \leq a \leq n$ coprime to n, let $\sigma_a \in \mathrm{Gal}(K/\mathbb{Q})$ denote the automorphism of K given by $\zeta_n \to \zeta_n^a$. Write $\gamma = \sum\limits_{(a,n)=1} b_a \sigma_a$. For $\theta \in \mathrm{Gal}(L/\mathbb{Q})$, let $e(\theta) \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ be defined by $\theta : \zeta_n \to \zeta_n^{e(\theta)}$. Thus we see that $\theta|_K = \sigma_{e(\theta)}$.

Lemma 5.4. *With the notation above, we have $\theta\gamma \equiv e(\theta)\gamma \pmod{n}$.*

Proof. Let $A = G(\chi)^{\theta - e(\theta)} \in L$; I claim that $A \in K$. Let $\alpha \in \mathrm{Gal}(L/K)$ be a generator of this cyclic group, where we associate $\mathrm{Gal}(L/K)$ with a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, and we may also think of α as the restriction of an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{np})/\mathbb{Q})$ (this was explored in Lemma 5.2). So, $\alpha : \zeta_n \to \zeta_n$ and $\alpha : \zeta_p \to \zeta_p^g$ for some g coprime to p. In Lemma 5.2, we showed that $G(\chi)^\alpha = \chi(g)^{-1}G(\chi)$. Since $\mathrm{Gal}(L/\mathbb{Q})$ is abelian, we have

$$A^\alpha = \frac{\alpha(\theta(G(\chi)))}{\alpha(G(\chi)^{e(\theta)})} = \frac{\theta(\alpha(G(\chi)))}{\alpha(G(\chi))^{e(\theta)}} = \frac{\theta(\chi(g)^{-1}G(\chi))}{(\chi(g)^{-1}G(\chi))^{e(\theta)}} = \frac{1}{\chi(g)^{\theta - e(\theta)}} A.$$

But $\chi(g)$ is an n^{th} root of unity, so $\chi(g)^{e(\theta)} = \sigma_{e(\theta)}(\chi(g))$. As $\theta|_K = \sigma_{e(\theta)}$, we get $A^\alpha = A$. Since α generates $\mathrm{Gal}(L/K)$, this implies that $A \in K$ as claimed.

We now get $A^n = \mu^{\theta - \sigma_{e(\theta)}}$ in $\mathcal{O}_K$, so all exponents of prime powers on the right hand side are multiples of n. Pluging in $\mu = \mathfrak{p}^\gamma$ yields the claim. □

Note that the above implies that $\sigma_{e(\theta)}\gamma = \theta\gamma \equiv e(\theta)\gamma \pmod{n}$, or more simply, $\sigma_c\gamma \equiv c\gamma \pmod{n}$. So

$$\sigma_c\gamma = \sum \sigma_c b_a \sigma_a = \sum b_a \sigma_{ac},$$

and

$$\sigma_c\gamma \equiv c\gamma = \sum c b_a \sigma_a = \sum c b_{ac} \sigma_{ac} \pmod{n}.$$

Equating coefficients gives us $cb_{ac} \equiv b_a \pmod{n}$, or $b_{ac} \equiv c^{-1}b_a \pmod{n}$ for all $a, c \in (\mathbb{Z}/n\mathbb{Z})^\times$. In particular, $b_c \equiv c^{-1}b_1 \pmod{n}$, so since b_1 is coprime to n, we see that the set of b_c forms a complete residue set modulo n as we suspected. As $1 \leq b_i \leq n$, we in fact get that $b_c \equiv c^{-1}b_1 \pmod{n}$ defines b_c uniquely, and $\{b_1, \ldots, b_{\phi(n)}\} = \{x | 1 \leq x \leq n,\ \gcd(x, n) = 1\}$. Thus $b_i = 1$ for some i, and we can change which $\mathfrak{p}$ we choose so that $b_1 = 1$. We summarize our result in the following proposition.

Proposition 5.5. *Let χ be a character on $\mathbb{F}_p$ of order n, where $p \equiv 1 \pmod{n}$ is an integer prime, and take $G(\chi)$ to be the corresponding Gauss sum. Let $K = \mathbb{Q}(\zeta_n)$, and $\sigma_t \in Gal(K/\mathbb{Q})$ be $\sigma_t : \zeta_n \to \zeta_n^t$ for $1 \leq t \leq n$ and $\gcd(t, n) = 1$. Then there exists a prime ideal $\mathfrak{p}$ above p in K such that*

$$G(\chi)^n \mathcal{O}_K = \mathfrak{p}^\gamma, \qquad \gamma = \sum_{\substack{1 \leq t \leq n \\ \gcd(t,n)=1}} t^{-1}\sigma_t, \tag{5.1}$$

where t^{-1} is the smallest positive integer such that $t^{-1}t \equiv 1 \pmod{n}$.

An amazing part of the above proposition is it is true for any character of order n on $\mathbb{F}_p$! However we still have a small hole: with $\left(\frac{\cdot}{\mathfrak{p}}\right)_n$, we do not know which prime ideal to choose! Let $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_n^{-1}$ (note we take the inverse), and we claim that $\mathfrak{p} || G(\chi)^n$. Now, $\mathfrak{p} = \mathfrak{P}^{p-1}$ in $\mathbb{Q}(\zeta_{pn})$, so we get

$$\mathfrak{p} || G(\chi)^n \Longleftrightarrow \mathfrak{P}^{p-1} || G(\chi)^n \Longleftrightarrow \mathfrak{P}^{\frac{p-1}{n}} || G(\chi).$$

Let $m = \frac{p-1}{n}$ and $\Pi = \zeta_p - 1$; note that since Π generates the unique prime ideal above p in $\mathbb{Q}(\zeta_p)$, then $\mathfrak{P} || \Pi$. The result of $\mathfrak{P}^m || G(\chi)$ follows immediately from the following proposition.

Proposition 5.6. *Inheriting the above notation, the following congruence holds*

$$G(\chi) \equiv \frac{\Pi^m}{m!} \pmod{\mathfrak{P}^{m+1}}.$$

Proof. The following computation yields our result:

$$\begin{aligned}
-G(\chi) &= \sum_{t=1}^{p-1} \chi(t)\zeta_p^t = \sum_{t=1}^{p-1} \chi(t)(1+\Pi)^t = \sum_{t=1}^{p-1} \chi(t) \sum_{j=0}^{t} \binom{t}{j} \Pi^j \\
&\equiv^{1,2} \sum_{j=0}^{m} \sum_{t=1}^{p-1} t^{p-1-m} \binom{t}{j} \Pi^j =^{3,4} \sum_{t=1}^{p-1} t^{p-1-m} \binom{t}{m} \Pi^m \\
&=^4 \sum_{t=1}^{p-1} t^{p-1-m} \frac{t^m}{m!} \Pi^m \equiv (p-1)\frac{\Pi^m}{m!} \equiv -\frac{\Pi^m}{m!} \pmod{\Pi^m \mathfrak{P}}
\end{aligned}$$

We have used the following:
1. $\chi(t) \equiv t^{p-1-m} \pmod{\mathfrak{p}}$;
2. $\Pi^j \equiv 0 \pmod{\Pi^n \mathfrak{P}}$ for $j > n$;
3. $\binom{t}{j}$ is a polynomial of degree j in t; so when $j \le m$, $t^{p-1-m}\binom{t}{j}$ contains a monomial of degree divisible by $p-1$ if and only if $j = m$;
4. $\sum_{t=1}^{p-1} t^k \equiv 0 \pmod{p}$ if $p-1$ does not divide k (see Proposition 3.10);
5. $\Pi^m \mathfrak{P} \mid p$;

□

This proposition says that when we take χ to be the inverse of the power residue symbol, then the $\mathfrak{p}$ in Proposition 5.5 is the $\mathfrak{p}$ in the denominator of the power residue symbol. From $G(\chi^{-1})G(\chi) = \pm p$, we can get the factorization of the $G(\left(\frac{\cdot}{\mathfrak{p}}\right)_n)$. We collect our conclusion into the following theorem.

Theorem 5.7 (Stickelberger's Relation). *Let $K = \mathbb{Q}(\zeta_n)$, $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_n^{-1}$, where $\mathfrak{p}$ is a prime ideal lying above the integer prime $p \equiv 1 \pmod{n}$. Take $G(\chi)$ to be the corresponding Gauss sum, and $\sigma_t \in Gal(K/\mathbb{Q})$ be $\sigma_t : \zeta_n \to \zeta_n^t$ for $1 \le t \le n$ and $\gcd(t,n) = 1$. Then*

$$G(\chi)^n \mathcal{O}_K = \mathfrak{p}^\gamma, \qquad \gamma = \sum_{\substack{1\le t\le n \\ \gcd(t,n)=1}} t^{-1}\sigma_t, \tag{5.2}$$

where t^{-1} is the smallest positive integer such that $t^{-1}t \equiv 1 \pmod{n}$.

5.2 Eisenstein Reciprocity

Let's start off with a proposition similar to Proposition 3.9.

Proposition 5.8. *Let $p \equiv 1 \pmod{n}$ be an integer prime, let $\mathfrak{p}$ be a prime ideal above p in $K = \mathbb{Q}(\zeta_n)$, and let $\mu = G(\chi)^n$ where $G(\chi)$ is the Gauss sum corresponding to $\chi = \left(\frac{\cdot}{\mathfrak{p}}\right)_n^{-1}$ (note the inverse). Then for all prime ideals $\mathfrak{q}$ in $\mathcal{O}_K$ coprime to pn we have*

$$\left(\frac{\mu}{\mathfrak{q}}\right)_n = \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_n, \tag{5.3}$$

where $N\mathfrak{q} = q^f$ is the norm of $\mathfrak{q}$ over $\mathbb{Q}$.

Proof. As $\mathfrak{q} \nmid n$, the equation $x^n - 1$ is separable in $\mathbb{F}_q$, and as K contains all n^{th} roots of unity, their reductions modulo $\mathfrak{q}$ form a subgroup of $\mathbb{F}_{q^f}^\times$ of order n, hence $q^f \equiv 1 \pmod{n}$. Thus

$$\begin{aligned}
(-G(\chi))^{q^f} &\equiv \sum_t \chi(t)^{q^f} \zeta_p^{tq^f} = \sum_t \chi(t)\zeta_p^{tq^f} \\
&= -\chi(q^f)^{-1} G(\chi) = \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_n (-G(\chi)) \pmod{q\mathcal{O}_K}.
\end{aligned}$$

Therefore $(-G(\chi))^{q^f-1} \equiv \left(\frac{N\mathfrak{q}}{\mathfrak{p}}\right)_n \pmod{q}$. We also have

$$(-G(\chi))^{q^f-1} = ((-1)^n\mu)^{\frac{q^f-1}{n}} \equiv \left(\frac{\mu}{\mathfrak{q}}\right)_n \pmod{\mathfrak{q}},$$

and equating the two expressions gives us the result (as normal, we can drop the modulo q). □

Definition 5.9. For each prime ideal $\mathfrak{p} \nmid n$ in $\mathbb{Z}[\zeta_n]$ define $\Phi(\mathfrak{p}) = G(\chi_{\mathfrak{p}})^n$ where $\chi_{\mathfrak{p}} = \left(\frac{\cdot}{\mathfrak{p}}\right)_n^{-1}$. Extend Φ multiplicatively to all ideals coprime to n.

From the multiplicativity of Φ, the power residue symbol, the norm, and Proposition 5.8 we get

$$\left(\frac{\Phi(\mathfrak{a})}{\mathfrak{q}}\right)_n = \left(\frac{N\mathfrak{q}}{\mathfrak{a}}\right)_n, \tag{5.4}$$

for all ideals $\mathfrak{a}$ which are products of prime ideals of degree 1 not dividing n.
Now, if $\mathfrak{a} = \alpha\mathcal{O}_K$ is principal and a product of prime ideals with inertia degree 1, then there is a unit $\epsilon(\alpha) \in \mathcal{O}_K^\times$ such that

$$\Phi(\mathfrak{a}) = \epsilon(\alpha)\alpha^\gamma, \tag{5.5}$$

where γ is defined in Equation 5.2. Note that all results in this section have not required n to be an odd prime; we will finally introduce that restriction. Let $n = \ell$ be an odd prime, and then

$$\left(\frac{\sigma_t^{-1}(\alpha^t)}{\mathfrak{q}}\right)_\ell = \left(\frac{\sigma_t^{-1}(\alpha)}{\mathfrak{q}}\right)_\ell^t = \left(\frac{\sigma_t^{-1}(\alpha)}{\mathfrak{q}}\right)_\ell^{\sigma_t} = \left(\frac{\alpha}{\mathfrak{q}^{\sigma_t}}\right)_\ell.$$

Upon multiplying this over t, we get

$$\left(\frac{\alpha^\gamma}{\mathfrak{q}}\right)_\ell = \prod_t \left(\frac{\alpha}{\mathfrak{q}^{\sigma_t}}\right)_\ell = \left(\frac{\alpha}{N\mathfrak{q}}\right)_\ell. \tag{5.6}$$

This looks very promising: combining 5.4 and this last equality gets us something that starts to approach a reciprocity law. However, at the moment there are two major problems: we have the factor of $\epsilon(\alpha)$ to deal with, and the equations are only valid when the primes dividing α have inertia degree 1. Before dealing with those problems, we will introduce the concept of *semi−primary* numbers (similarly to in the cubic case).

Definition 5.10. Let ℓ be an odd integer prime, and call $\alpha \in \mathbb{Z}[\zeta_\ell]$ *semi-primary* if α and ℓ are coprime, and $\alpha \equiv a \pmod{(1-\zeta_l)^2}$ for some $a \in \mathbb{Z}$ (note that a is necessarily nonzero).

To familiarize ourselves with working with semi-primary numbers, the following proposition suffices.

Proposition 5.11. *Let ℓ be an odd prime, and assume that* $\gcd(\alpha, \ell) = 1$ *for some $\alpha \in \mathbb{Z}[\zeta_\ell]$. Then there is a unique $c \in \frac{\mathbb{Z}}{l\mathbb{Z}}$ such that $\zeta_\ell^c\alpha$ is semi-primary;*

Proof. Let $\lambda = 1-\zeta_\ell$; then (λ) is the unique prime ideal in $\mathbb{Q}(\zeta_\ell)$ above ℓ. Since powers of ζ_ℓ form an integral basis for $\mathcal{O}_{\mathbb{Q}(\zeta_\ell)}$, powers of $\lambda = 1-\zeta_\ell$ do as well, and thus $\alpha \equiv a + b\lambda \pmod{\lambda^2}$ for some $a, b \in \mathbb{Z}$. As α, ℓ are coprime, we see $\ell \nmid a$, so choose $c \in \mathbb{Z}$ by $c \equiv ba^{-1} \pmod{\ell}$. Since $\zeta_\ell^c = (1-\lambda)^c \equiv 1 - c\lambda \pmod{\lambda^2}$, we see $\zeta_\ell^c\alpha \equiv (a+b\lambda)(1-c\lambda) \equiv a + (b-ac)\lambda \equiv a \pmod{\lambda^2}$ as required. Clearly the implications hold in reverse, i.e. c is uniquely defined modulo ℓ.

□

The first use of semi-primary numbers comes now: if α is semi-primary, then $\epsilon(\alpha)$ is an ℓ^{th} power!

Lemma 5.12. *The unit $\epsilon(\alpha)$ defined in Equation 5.5 has the following properties:*
i) $\epsilon(\alpha)$ is a root of unity.
ii) If α is an semi-primary and $n = \ell$ is an odd integer prime, then $\epsilon(\alpha) = \pm 1$.

Proof. i) Let $K = \mathbb{Q}(\zeta_n)$; I claim it is sufficient to show that $|\epsilon(\alpha)| = 1$. Indeed, assuming this, then as complex conjugation is in the *abelian* Galois group $\mathrm{Gal}(K/\mathbb{Q})$, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $1 = \sigma(1) = (\epsilon(\alpha)\overline{\epsilon(\alpha)})^\sigma = \epsilon(\alpha)^\sigma\overline{\epsilon(\alpha)^\sigma} = |\epsilon(\alpha)^\sigma|^2$. But $|\epsilon(\alpha)^\sigma| = 1$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ implies that α is an n^{th} root of unity by a theorem of Kronecker (Here's a summarized proof: let $\epsilon(\alpha)$ and its conjugates be $r_1, \dots, r_k$. Let $f_i(x) \in K[x]$ be the polynomial with roots $\{r_j^i\}_{j=1}^k$; simple Galois theory shows that this is in fact a polynomial in $\mathbb{Z}[x]$. The condition now gives us that the coefficients are bounded in $\mathbb{Z}$, hence for some powers we get the roots being the same and in the same order, and thus equating them shows that they are roots of unity).
Hence we need to show that $|\epsilon(\alpha)| = 1$. First, $|\Phi(\mathfrak{p})|^2 = p^n = (N\mathfrak{p})^n$ for all prime ideals of inertia degree 1, hence $|\Phi(\alpha)|^2 = |N(\alpha)|^n$. Note that σ_{-1} is complex conjugation, and so $|\alpha^\gamma|^2 = \alpha^\gamma\alpha^{\gamma\sigma_{-1}}$. We calculate

$$\begin{aligned}\gamma(1+\sigma_{-1}) &= \sum_t t^{-1}\sigma_t + \sum_t t^{-1}\sigma_t\sigma_{-1} = \sum_t t^{-1}\sigma_t + \sum_t t^{-1}\sigma_{-t} \\ &= \sum_t t^{-1}\sigma_t + \sum_t (n-t^{-1})\sigma_t = n\sum_t \sigma_t,\end{aligned}$$

whence $|\alpha^\gamma|^2 = |N(\alpha)|^n$ yielding the claim (recall the equation $\Phi(\alpha) = \epsilon(\alpha)\alpha^\gamma$).

ii) Let $\alpha \equiv z \pmod{\Lambda^2}$, where $\Lambda = (1-\zeta_\ell)\mathcal{O}_K$ is the prime ideal above the integer prime ℓ, and $z \in \mathbb{Z}$. For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\Lambda^\sigma = \Lambda$ (the Galois group acts transitively on the primes above ℓ, which is only Λ). Applying σ to our equation yields $\alpha^\sigma \equiv z \pmod{\Lambda^2}$. Thus

$$\alpha^\gamma \equiv z^{1+2+\cdots+(\ell-1)} \equiv z^{\frac{\ell(\ell-1)}{2}} \equiv \left(\frac{z}{\ell}\right)_2^\ell \equiv \pm 1 \pmod{\Lambda^2}.$$

If we can show that $\Phi(\alpha) \equiv \pm 1 \pmod{\Lambda^2}$, then $\epsilon(\alpha) \equiv \pm 1 \pmod{\Lambda^2}$ and so $\epsilon(\alpha)$ is a semi-primary root of unity, whence it is ± 1.
As per normal, we only need to check this when $\alpha = \mathfrak{p}$ is a prime ideal. We calculate

$$\begin{aligned}\Phi(\alpha) = G(\chi_\mathfrak{p})^\ell = (-\sum_{t\neq 0}\chi_\mathfrak{p}(t)\psi(t))^\ell \equiv -\sum_{t\neq 0}\chi_\mathfrak{p}(t)^\ell\psi(t)^\ell &= -\sum_{t\neq 0}\psi(\ell t) \\ &= \psi(0) = 1 \pmod{\ell},\end{aligned}$$

and we are done since $\Lambda^2 \mid \ell$ as $\ell > 2$. □

Let $\alpha \in \mathbb{Z}[\zeta_\ell]$ be semi-primary, let $\sigma : \zeta_\ell \to \zeta_\ell^r$ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$, and define

$$\beta = \alpha^S, \qquad\qquad S = \prod_{\substack{e\mid\ell-1 \\ e\neq\ell-1}} (1-\sigma^e).$$

Let $\mathfrak{p}$ be a prime ideal of degree $f > 1$ that divides β, and let the integer prime p above $\mathfrak{p}$ split into a product of e prime ideals; then $ef = \ell - 1$. As $f > 1$, $1-\sigma^e$ occurs in the product, and so we can write $S = h(\sigma)(1-\sigma^e)$ for some integer polynomial $h(x)$. But σ^e fixes $\mathfrak{p}$, so $\mathfrak{p}$ occurs equally often in the numerator and denominator of $\beta = (\alpha^{h(\sigma)})^{1-\sigma^e}$, whence $\mathfrak{p}$ does not occur in the factorization of $\beta\mathcal{O}_K$! Thus $\beta\mathcal{O}_K$ is a product of prime ideals of inertia degree 1.

Let $\mathfrak{q}$ be any prime ideal coprime to $\alpha\ell$, and then from Equations 5.4-5.6 and Lemma 5.12, we know that $\left(\frac{\beta}{N\mathfrak{q}}\right)_\ell = \left(\frac{N\mathfrak{q}}{\beta}\right)_\ell$. Let $N\mathfrak{q} = q^f$ where q is an integer prime; then $f \mid \ell - 1$, so f is coprime to ℓ. So we get $\left(\frac{\beta}{q}\right)_\ell^f = \left(\frac{q}{\beta}\right)_\ell^f$ and so $\left(\frac{\beta}{q}\right)_\ell = \left(\frac{q}{\beta}\right)_\ell$. We also have $\left(\frac{\alpha^\sigma}{q}\right)_\ell = \left(\frac{\alpha}{q}\right)_\ell^\sigma = \left(\frac{\alpha}{q}\right)_\ell^r$, and we calculate (the products are taken over the same range as for S, namely $e \mid \ell - 1$ and $e \neq \ell - 1$)

$$\begin{aligned}\left(\frac{\alpha}{q}\right)_\ell^{\prod(1-r^e)} &= \left(\frac{\alpha}{q}\right)_\ell^{\prod(1-\sigma^e)} = \left(\frac{\beta}{q}\right)_\ell = \left(\frac{q}{\beta}\right)_\ell \\ &= \left(\frac{q}{\alpha}\right)_\ell^{\prod(1-\sigma^e)} = \left(\frac{q}{\alpha}\right)_\ell^{\prod(1-r^e)}.\end{aligned}$$

The product $\prod(1 - r^e)$ is not divisible by ℓ, hence we conclude that $(\frac{\alpha}{q})_\ell = (\frac{q}{\alpha})_\ell$ for all semi-primary $\alpha \in \mathcal{O}_K$ and integer primes q coprime to $\alpha\ell$. As the power residue symbol is multiplicative, we can replace q by $a \in \mathbb{Z}$ coprime to $\alpha\ell$. We record this result, some supplementary laws, and a couple corollaries in the following theorem.

Theorem 5.13 (Eisenstein's Reciprocity Law for l-th Powers)**.** *Let ℓ be an odd integer prime, and suppose that $a \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}[\zeta_\ell]$ are semi-primary and relatively prime to each other. Then*

$$\left(\frac{a}{\alpha}\right)_\ell = \left(\frac{\alpha}{a}\right)_\ell.$$

Furthermore, the following also hold
i) $(\frac{\alpha}{a})_\ell = 1$ if $\alpha \in \mathbb{Z}[\zeta_\ell + \zeta_\ell^{-1}]$ (i.e. α is real);
ii) $(\frac{a}{b})_\ell = 1$ for all $a, b \in \mathbb{Z}$ with $\gcd(a, b) = \gcd(b, \ell) = 1$;
iii) The two supplementary laws:

$$\left(\frac{\zeta_\ell}{a}\right)_\ell = \zeta_\ell^{(a^{\ell-1}-1)/\ell}, \qquad \left(\frac{1-\zeta_\ell}{a}\right)_\ell = \left(\frac{\zeta_\ell}{a}\right)_\ell^{\frac{\ell+1}{2}}$$

[the second supplementary law is incorrect in [3]; they have the exponent as $\frac{\ell-1}{2}$ instead of $\frac{\ell+1}{2}$].

Proof. Only assertions i)-iii) remain.
i) Let $G = \mathrm{Gal}(K/\mathbb{Q})$ with $K = \mathbb{Q}(\zeta_\ell)$, and let $\tau \in G$ be complex conjugation. Then $H = \langle\tau\rangle$ is a normal subgroup of G with order 2. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ above the integer prime p with inertia degree $f \mid \ell - 1$. We have

$$\left(\frac{\alpha}{\mathfrak{p}^\tau}\right) = \left(\frac{\alpha^\tau}{\mathfrak{p}^\tau}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)^\tau = \left(\frac{\alpha}{\mathfrak{p}}\right)^{-1}.$$

Since $p^f = \prod_{\sigma\in G} \mathfrak{p}^\sigma$, we get

$$\left(\frac{\alpha}{p}\right)_\ell^f = \prod_{\sigma\in G/H} \left(\frac{\alpha}{\mathfrak{p}^\sigma\mathfrak{p}^{\sigma\tau}}\right)_\ell = 1,$$

and so the result follows as $\gcd(f, \ell) = 1$.

ii) This is a special case of i) for $\ell \nmid a$, and otherwise, $(\frac{a}{b})_\ell = (\frac{a+b}{b})_\ell = 1$.

iii) First, take $a = p$ to be an integer prime, and let $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g$. Suppose the inertia degree of the p_i's is f; then $\ell - 1 = fg$. We have

$$\left(\frac{\zeta_\ell}{p}\right)_\ell = \prod_{j=1}^{g} \left(\frac{\zeta_\ell}{\mathfrak{p}_j}\right)_\ell = \prod_{j=1}^{g} \zeta_\ell^{\frac{p^f-1}{\ell}} = \zeta_\ell^{g\frac{p^f-1}{\ell}}.$$

Since

$$\frac{p^{fg}-1}{\ell} = \frac{p^f-1}{\ell}(p^{f(g-1)} + \cdots + p^f + 1) \equiv g\frac{p^f-1}{\ell} \pmod{\ell}$$

the first supplementary law holds for integer primes $a = p$. Now,

$$\begin{aligned}\frac{(mn)^{\ell-1}-1}{\ell} &= \frac{m^{\ell-1}-1}{\ell}n^{\ell-1} + \frac{n^{\ell-1}-1}{\ell} \\ &\equiv \frac{m^{\ell-1}-1}{\ell} + \frac{n^{\ell-1}-1}{\ell} \pmod{\ell}\end{aligned}$$

shows the first law holds for all a (by repeated applications of the above equation).
The second law holds from the first law, i), and that $(1-\zeta_\ell)^2\zeta_\ell^{-1}$ is real.

□

Remark. Takagi extended Eisenstein's result to arbitrary number fields K containing ζ_ℓ (page 393 of [3]).

6 Artin's Reciprocity Law

6.1 The Artin Symbol

Let L/K be a finite Galois extension of number fields, and let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ which is unramified in L/K.

Definition 6.1. The *Frobenius automorphism* ϕ of $\mathfrak{P}$ is the unique automorphism $\phi \in \mathrm{Gal}(L/K)$ such that

$$\phi(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}} \tag{6.1}$$

for all $\alpha \in \mathcal{O}_L \backslash \mathfrak{P}$, where $\mathfrak{p}$ is the prime ideal in $\mathcal{O}_K$ below $\mathfrak{P}$, and $N\mathfrak{p}$ is the norm of $\mathfrak{p}$.

The existence and uniqueness of ϕ is easily seen when looking at the local picture. Indeed, let $N\mathfrak{p} = q$, and let $f = [L_\mathfrak{P} : K_\mathfrak{p}] = |\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})|$. As $\mathfrak{p}$ is unramified, we recall that the residue field of $L_\mathfrak{P}$ is $\mathbb{F}_{q^f}$, and that $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \simeq \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ (pg30 of [2]). Thus the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$, which sends $\alpha \to \alpha^q$, corresponds to a unique automorphism of $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. This group injects into $\mathrm{Gal}(L/K)$, with image being the decomposition group of $\mathfrak{P}$ (pg24 of [2]). Translating the original action on $\mathbb{F}_{q^f}$ to L gives Equation 6.1. Given a ϕ satisfying Equation 6.1, we see that if $\alpha \in \mathcal{O}_L\backslash\mathfrak{P}$ then $\phi(\alpha) \in \mathcal{O}_L\backslash\mathfrak{P}$, whence $\phi(\mathfrak{P}) = \mathfrak{P}$, and so ϕ is in the decomposition group of $\mathfrak{P}$. Therefore we can work backwards and see that ϕ must be unique, as claimed.

Definition 6.2. The *Frobenius symbol* is

$$\phi = \left[\frac{L/K}{\mathfrak{P}}\right]$$

where ϕ is the Frobenius automorphism defined above.

Lemma 6.3. *Let $\sigma \in Gal(L/K)$. Then*

$$\left[\frac{L/K}{\mathfrak{P}^\sigma}\right] = \sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}.$$

Proof. First, note that $\mathfrak{P}$ being unramified implies $\mathfrak{P}^\sigma$ is also unramified, so our expression is defined. Now, apply σ to Equation 6.1, and we get

$$\sigma(\alpha)^{N\mathfrak{p}} = \sigma(\alpha^{N\mathfrak{p}}) \equiv (\sigma\left[\frac{L/K}{\mathfrak{P}}\right])\alpha = (\sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1})\sigma(\alpha) \pmod{\mathfrak{P}^\sigma},$$

for all $\sigma(\alpha)$ with $\alpha \in \mathcal{O}_L\backslash\mathfrak{P}$. Letting $\beta = \sigma(\alpha)$, this is the same as saying

$$\beta^{N\mathfrak{p}} \equiv (\sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1})\beta \pmod{\mathfrak{P}^\sigma}$$

for all $\beta \in \mathcal{O}_L\backslash\mathfrak{P}^\sigma$, and we deduce the result. □

Now assume L/K is *abelian.* Then for any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\left[\frac{L/K}{\mathfrak{P}^{\sigma}}\right] = \sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1} = \left[\frac{L/K}{\mathfrak{P}}\right].$$

Recalling that the Galois group acts transitively on the primes above $\mathfrak{p}$, we thus see that the Frobenius symbol does not depend on the prime above $\mathfrak{p}$. This knowledge allows us to now define the Artin symbol.

Definition 6.4. Let L/K be a finite *abelian* extension of number fields, and let $\mathfrak{p} \in \mathcal{O}_K$ be an unramified prime ideal. Let $\mathfrak{P}$ be any prime ideal of L lying above $\mathfrak{p}$, and then define the *Artin symbol* $\left(\frac{L/K}{\mathfrak{p}}\right)$ as

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left[\frac{L/K}{\mathfrak{P}}\right].$$

Extend this multiplicatively on the bottom to all ideals α of $\mathcal{O}_K$ coprime to $\mathrm{disc}(L/K)$ (i.e. the unramified ideals).

It is important to remember that the Artin symbol is not an element of L, but an automorphism in the Galois group of L/K. Furthermore, it is only defined for products of unramified primes. We now can record the connection to the power residue symbol.

Proposition 6.5. *Let K be a number field that contains a primitive n^{th} root of unity, ζ_n. For any $\alpha \in K^{\times}$, put $L = K(\sqrt[n]{\alpha})$, and let $\mathfrak{p}$ be any prime ideal of $\mathcal{O}_K$ which is unramified in L/K ($\mathfrak{p} \nmid n\alpha$ suffices). Then the following identity holds:*

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha} \tag{6.2}$$

Proof. By definition, the left hand side is congruent to $(\sqrt[n]{\alpha})^{N\mathfrak{p}} \pmod{\mathfrak{P}}$ for any prime $\mathfrak{P}$ lying above $\mathfrak{p}$. But $\mathfrak{p}$ is unramified, so combining these congruences shows that the left hand side is congruent to $(\sqrt[n]{\alpha})^{N\mathfrak{p}}$ $\pmod{\mathfrak{p}}$. The right hand side is congruent to $\alpha^{(N\mathfrak{p}-1)/n}\sqrt[n]{\alpha} = \alpha^{N\mathfrak{p}/n} \pmod{\mathfrak{p}}$, whence the Equation 6.2 is true modulo $\mathfrak{p}$. The left hand side is a Galois conjugate of $\sqrt[n]{\alpha}$; they are $\zeta_n^j\sqrt[n]{\alpha}$ for $1 \leq j \leq n$, which is the form the right hand side takes. But these n possibilities are distinct modulo $\mathfrak{p}$, and so the result follows. □

6.2 Artin's Reciprocity Law

Let k be a number field; recall a *place* on k is an equivalence class of absolute values. Non-archimedean/finite places correspond to completing with respect to a prime ideal, and archimedean/infinite places correspond to embedding k into $\mathbb{C}$ and taking the regular absolute value. As such, a real infinite place is an embedding $\sigma : k \to \mathbb{R}$.

Definition 6.6. A *divisor* $\mathfrak{m}$ is the formal product of finite or infinite real places of K. We write $\mathfrak{m} = \prod \mathfrak{p}_i^{n_i}$, where the $\mathfrak{p}_i$ are either prime ideals (representing completion with respect to that prime ideal) or infinite real places.

Let I_K be the group of fractional ideals of K, and take $A_{\mathfrak{m}}$ to be the subgroup consisting of the fractional ideals whose prime ideal factorization contains no prime ideal dividing $\mathfrak{m}$ (clearly, the infinite places which may form a part of $\mathfrak{m}$ have no effect on $A_{\mathfrak{m}}$). Let $H_{\mathfrak{m}}^0$ be the subgroup of $A_{\mathfrak{m}}$ consisting of the principal ideals which can be written as (α), where $\alpha \equiv 1 \pmod{\mathfrak{m}}$. That is, if $\mathfrak{p}_i$ is a prime ideal, $\alpha \equiv 1 \pmod{\mathfrak{p}_i^{n_i}}$, and if $\mathfrak{p}_i$ is an infinite real place $\sigma : K \to \mathbb{R}$, we have $\sigma(\alpha) > 0$. It is clear that $H_{\mathfrak{m}}^0$ has finite index in the group of principal ideals of $A_{\mathfrak{m}}$, which has finite index in $A_{\mathfrak{m}}$. Thus for any $\mathfrak{m}$ we get a finite group $A_{\mathfrak{m}}/H_{\mathfrak{m}}^0$.

Let $H_{\mathfrak{m}}$ be any subgroup of $A_{\mathfrak{m}}$ containing $H_{\mathfrak{m}}^0$. Suppose that $\mathfrak{m} \mid \mathfrak{n}$; note we have $A_{\mathfrak{m}} \supset A_{\mathfrak{n}}$ and $H_{\mathfrak{m}}^0 \supset H_{\mathfrak{n}}^0$. Take $H_{\mathfrak{n}} = H_{\mathfrak{m}} \cap A_{\mathfrak{n}} \supset H_{\mathfrak{n}}^0$, then there is a canonical injection $A_{\mathfrak{n}}/H_{\mathfrak{n}} \hookrightarrow A_{\mathfrak{m}}/H_{\mathfrak{m}}$. Recalling our definition of

$H^0_\mathfrak{m}$, we see that for every coset $\alpha H^0_\mathfrak{m}$ in $A_\mathfrak{m}$, we can take $\alpha \in A_\mathfrak{n}$ (a coset is just a residue class modulo $\mathfrak{m}$, and since $\mathfrak{m} \mid \mathfrak{n}$, we can ensure the extra conditions of being coprime to n are met). As $H_\mathfrak{m} \supset H^0_\mathfrak{m}$, the same is true for $H_\mathfrak{m}$, and therefore our injection is a bijection, that is

$$\frac{A_\mathfrak{n}}{H_\mathfrak{n}} \simeq \frac{A_\mathfrak{m}}{H_\mathfrak{m}}$$

canonically.

Let $\mathfrak{m}_1, \mathfrak{m}_2$ be two divisors with respective associated groups $H_{\mathfrak{m}_1}, H_{\mathfrak{m}_2}$. Call these groups equivalent if for some (hence all) common multiples $\mathfrak{m}$ of $\mathfrak{m}_1, \mathfrak{m}_2$ we have

$$A_\mathfrak{m} \cap H_{\mathfrak{m}_1} = A_\mathfrak{m} \cap H_{\mathfrak{m}_2}.$$

It is clear that this is an equivalence relation, and the canonical isomorphism shows that the quotient group $A_\mathfrak{m}/H_\mathfrak{m}$ is independant of the choice of $\mathfrak{m}$ (within an equivalence class).

Definition 6.7. The equivalence class of the above quotient groups is called the *congruence divisor class group A/H*. The least divisor $\mathfrak{m}$ for which this can be realized is called the conductor $\mathfrak{f}$ of A/H (where A/H of course refers to $A_\mathfrak{m}/H_\mathfrak{m}$ for any multiple $\mathfrak{m}$ of $\mathfrak{f}$).

Definition 6.8. A finite extension L of K is called a *class field* for A/H if the prime ideals $\mathfrak{p}$ of K which split completely in L are precisely the ones belonging to H. For the infinite real places of K, this means that we require that all extensions to L are complex if the place was in $\mathfrak{f}$, and all extensions are real otherwise.

We can now state a classical theorem in class field theory, and Artin's reciprocity law (note that there are several equivalent formulations of the law, we will only state one version).

Theorem 6.9. *Let L/K be a finite abelian extension of number fields. Then it is a class field for some A/H. Moreover, for each congruence divisor class group A/H in K, there is a unique class field L/K; L is abelian over K.*

Theorem 6.10 (Artin's Reciprocity Law)**.** *The Galois group of L/K is isomorphic to A/H. This isomorphism is in fact canonical, realized by the map $\mathfrak{a} \to \left(\frac{L/K}{\mathfrak{a}}\right)$, which is a surjective homomorphism $A \to$ Gal(L/K) with kernel H.*

6.3 The Hilbert Symbol

Before deducing reciprocity laws, we need to introduce the local Artin map, as well as the Hilbert symbol. Let K be a number field containing a primitive n^{th} root of unity ζ_n, and assume L is a finite abelian extension of K. If $\mathfrak{p}$ is a prime ideal of K, then completing L with respect to any prime ideal of L above $\mathfrak{p}$ gives isomorphic fields (as L/K is abelian). We will call this field $L_\mathfrak{p}$ for simplicity.

Definition 6.11. Let v be a place of K. The *local Artin map* is a map $\psi_v : K_v^\times \to \mathrm{Gal}(L/K)$. If $v = \mathfrak{p}$ is finite and $L_\mathfrak{p}/K_\mathfrak{p}$ is unramified, then $\psi_\mathfrak{p}$ is given by

$$\beta \to \left(\frac{L/K}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\beta)}$$

To define ψ_v in general, it involves giving a map $K_v^\times \to A/H$ (see page 107 of [4]), where A/H is the congruence divisor class group corresponding to L/K, and then mapping A/H isomorphically to $\mathrm{Gal}(L/K)$ via Artin's reciprocity law.

Remark. The local Artin map is defined on $K_v^\times$, so when we use it on $K^\times$ we really mean the restriction of it to $K^\times$.

Definition 6.12. Let v be a place of k. The *Hilbert symbol* is a function $(-,-)_v : K^\times \times K^\times \to \langle \zeta_n \rangle \subset \mathbb{C}^\times$ given by

$$(\alpha,\beta)_v(\sqrt[n]{\alpha}) = (\psi_v(\beta))(\sqrt[n]{\alpha}),$$

where ψ_v is the local Artin map corresponding to the abelian extension $K(\sqrt[n]{\alpha})/K$.

Lemma 6.13. *The following simple properties of the Hilbert symbol hold:*
i) $(\alpha,\beta\beta')_v = (\alpha,\beta)_v(\alpha,\beta')_v$*;*
ii) $(\alpha\alpha',\beta)_v = (\alpha,\beta)_v(\alpha',\beta)_v$*;*
iii) $(\alpha,-\alpha)_v = (\alpha,1-\alpha)_v = 1$*;*
iv) $(\alpha,\beta)_v(\beta,\alpha)_v = 1$*;*
v) If either α *or* β *is an* n^{th} *power, then* $(\alpha,\beta)_v = 1$*. Thus the Hilbert symbol descends to a map* $\frac{K^\times}{(K^\times)^n} \times \frac{K^\times}{(K^\times)^n} \to \langle \zeta_n \rangle$*.*

Proof. i)-iii) are relatively simple manipulations; see page 108 of [4].
iv) Using bilinearity and iii) give

$$1 = (\alpha\beta,-\alpha\beta)_v = (\alpha,-\alpha)_v(\alpha,\beta)_v(\beta,\alpha)_v(\beta,-\beta)_v = (\alpha,\beta)_v(\beta,\alpha)_v$$

v) If $\alpha = \gamma^n$, then $K(\sqrt[n]{\alpha}) = K$ so the local Artin map is trivial. If $\beta = \gamma^n$, then as $K(\sqrt[n]{\alpha})/K$ is cyclic of order dividing n, we have $\psi_v(\beta) = \psi_v(\gamma)^n = id$ so the local Artin map is again trivial. The local Artin map being trivial then implies that $(\alpha,\beta)_v = 1$. □

Remark. The Hilbert symbol can be extended continuously to a map on $K_v^\times \times K_v^\times$ with analogous properties; see page 109 of [4].

Definition 6.14. Let S denote the set of infinite places of K, unioned with the set of prime ideals dividing n. For any $\alpha_1,\alpha_2,\ldots,\alpha_i \in K^\times$, let $S(\alpha_1,\alpha_2,\ldots,\alpha_i)$ be the union of S with the set of primes for which $\alpha_1,\alpha_2,\ldots,\alpha_i$ are not units (i.e. the set of primes dividing the numerator or denominator of at least one of the α_j's). Note that S and $S(\alpha_1,\alpha_2,\ldots,\alpha_i)$ are always finite.

Proposition 6.15. *Let* $\alpha,\beta \in K^\times$*. Then*

$$\prod_v (\alpha,\beta)_v = 1.$$

Proof. This follows from properties of the local Artin map; see page 109 of [4]. □

Note that this is a finite product: if $v = \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal not in $S(\alpha,\beta)$, then $K(\sqrt[n]{\alpha})/K$ is unramified at $\mathfrak{p}$ and $v_\mathfrak{p}(\beta) = 0$, whence $\psi_\mathfrak{p}(\beta) = id$, the identity map. Thus $(\alpha,\beta)_\mathfrak{p} = 1$ for all such $\mathfrak{p}$, and only finitely many prime ideals are in $S(\alpha,\beta)$, completing the claim.

Proposition 6.16. *If* $\mathfrak{p} \notin S$*, then for* $\alpha,\beta \in K^\times$ *we have*

$$(\alpha,\beta)_\mathfrak{p} = \left(\frac{\gamma}{\mathfrak{p}}\right)_n \text{ where } \gamma = (-1)^{v_\mathfrak{p}(\alpha)v_\mathfrak{p}(\beta)}\alpha^{v_\mathfrak{p}(\beta)}\beta^{-v_\mathfrak{p}(\alpha)}.$$

Proof. First, assume $\alpha \in \mathcal{O}_K$ is coprime to $\mathfrak{p}$, and let $\pi \in K^\times$ be so that $\mathfrak{p}||\pi$. Then

$$(\alpha,\pi)_\mathfrak{p}(\sqrt[n]{\alpha}) = \left(\frac{K(\sqrt[n]{\alpha})/K}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\pi)}(\sqrt[n]{\alpha}) = \left(\frac{K(\sqrt[n]{\alpha})/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha},$$

where the last equality is by Proposition 6.5. Therefore we get $(\alpha, \pi)_\mathfrak{p} = \left(\frac{\alpha}{\mathfrak{p}}\right)_n$.
Now for $\alpha, \beta \in K^\times$, write $\alpha = \pi^{v_\mathfrak{p}(\alpha)}\alpha_0$ and $\beta = \pi^{v_\mathfrak{p}(\beta)}\beta_0$. Using bilinearity and $(-\pi, \pi)_\mathfrak{p} = 1$ we obtain

$$(\alpha, \beta)_\mathfrak{p} = (-1, \pi)_\mathfrak{p}^{v_\mathfrak{p}(\alpha)v_\mathfrak{p}(\beta)}(\pi, \beta_0)_\mathfrak{p}^{v_\mathfrak{p}(\alpha)}(\pi, \alpha_0)_\mathfrak{p}^{-v_\mathfrak{p}(\beta)} = ((-1)^{v_\mathfrak{p}(\alpha)v_\mathfrak{p}(\beta)}\alpha_0^{v_\mathfrak{p}(\beta)}\beta_0^{-v_\mathfrak{p}(\alpha)}, \pi)_\mathfrak{p} = (\gamma, \pi)_\mathfrak{p},$$

from which the result follows (the $\mathfrak{p}$'s cancel to give the last equality). □

Corollary 6.17. *If $\alpha, \beta \in K^\times$ and $\mathfrak{p} \notin S(\alpha)$, then*

$$(\alpha, \beta)_\mathfrak{p} = \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{v_\mathfrak{p}(\beta)}.$$

Proof. Use $v_\mathfrak{p}(\alpha) = 0$ in the above proposition. □

Definition 6.18. For $\alpha, \beta \in K^\times$, let $(\beta)^{S(\alpha)}$ denote the ideal obtained from starting with (β), and removing all prime factors which are in $S(\alpha)$. Also, define

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{(\beta)^{S(\alpha)}}\right)_n.$$

If $S(\alpha) = \mathcal{O}_k$ (this happens when β is a unit), define $\left(\frac{\alpha}{\beta}\right) = 1$.

Proposition 6.19. *For $\alpha, \beta \in K^\times$ we have*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{v \in S(\alpha) \cap S(\beta)} (\beta, \alpha)_v.$$

Proof. Using Corollary 6.17, we see that

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{(\beta)^{S(\alpha)}}\right)_n = \prod_{\mathfrak{p} \notin S(\alpha)} \left(\frac{\alpha}{\mathfrak{p}^{v_\mathfrak{p}((\beta)^{S(\alpha)})}}\right)_n = \prod_{\mathfrak{p} \notin S(\alpha)} \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{v_\mathfrak{p}(\beta)} = \prod_{\mathfrak{p} \notin S(\alpha)} (\alpha, \beta)_\mathfrak{p},$$

noting that $v_\mathfrak{p}(\beta) = v_\mathfrak{p}((\beta)^{S(\alpha)})$ when $\mathfrak{p} \notin S(\alpha)$. Using this and Lemma 6.13iv, we calculate

$$\begin{aligned}
\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} &= \left\{\prod_{\mathfrak{p} \notin S(\alpha)} (\alpha, \beta)_\mathfrak{p}\right\}\left\{\prod_{\mathfrak{p} \notin S(\beta)} (\beta, \alpha)_\mathfrak{p}^{-1}\right\} \\
&= \left\{\prod_{\mathfrak{p} \notin S(\alpha)} (\alpha, \beta)_\mathfrak{p}\right\}\left\{\prod_{\mathfrak{p} \notin S(\beta)} (\alpha, \beta)_\mathfrak{p}\right\} \\
&= \prod_{\mathfrak{p} \notin S(\alpha) \cap S(\beta)} (\alpha, \beta)_\mathfrak{p},
\end{aligned}$$

since the terms appearing in both products correspond to $\mathfrak{p} \notin S(\alpha, \beta)$; but $(\alpha, \beta)_\mathfrak{p} = 1$ for such $\mathfrak{p}$ (noted after Proposition 6.15), so they have no effect on the product. To finish, apply Proposition 6.15, and use Lemma 6.13iv to finish. □

Now we have an expression which looks more like a reciprocity law than Artin's law! Note that if $\alpha, \beta \in \mathcal{O}_K$ are coprime to each other and to n, then $\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{\beta}\right)_n$, so to deduce reciprocity laws we just need to calculate $(\beta, \alpha)_v$ for $v \in S(\alpha) \cap S(\beta)$.

7 Deducing Reciprocity Laws

7.1 Quadratic Reciprocity Revisited

Take $n = 2$, and note that $(\alpha, \beta)_v = \pm 1$ as it must be a square root of 1. So we just need to find a condition on α, β, v that is equivalent to $(\alpha, \beta)_v = 1$. From page 111 of [4], this condition is simply

$$(\alpha, \beta)_v = \begin{cases} 1 & \text{if } \alpha x^2 + \beta y^2 = 1 \text{ has a solution in } K_v, \\ -1 & \text{otherwise.} \end{cases}$$

Take $K = \mathbb{Q}$, then $S = \{2, \infty\}$ and $\mathbb{Q}_\infty = \mathbb{R}$. Let a, b be coprime odd positive integers, then $ax^2 + by^2 = 1$ has a solution in $\mathbb{R}$, for example $(x, y) = (0, \sqrt{\frac{1}{b}})$. Therefore we get

$$\left(\frac{a}{b}\right)_2 \left(\frac{b}{a}\right)_2^{-1} = (b, a)_2 \tag{7.1}$$

Lemma 7.1. *If $a, b \in \mathbb{Z}^+$ are coprime odd positive integers, then*

$$(b, a)_2 = \begin{cases} -1 & \text{if } a \equiv b \equiv 3 \pmod 4, \\ 1 & \text{else.} \end{cases}$$

Proof. It suffices to see whether $ax^2 + by^2 = 1$ has a solution in $\mathbb{Q}_2$ or not. We will divide into cases.

Case 1: Either $a \equiv 1 \pmod 8$ or $b \equiv 1 \pmod 8$.
Wlog we can assume $a \equiv 1 \pmod 8$. Then letting $f(x) = ax^2 - 1$, we have $|f(1)| = |a - 1| \leq 2^{-3}$ whereas $|f'(1)|^2 = |2a|^2 = 2^{-2} > |f(1)|$, so there is a solution r to $f(x) = 0$ by Hensel's Lemma. Then $(r, 0)$ is a solution to $ax^2 + by^2 = 1$ as required.

Case 2: We have $a \equiv 5 \pmod 8$ or $b \equiv 5 \pmod 8$.
Wlog we have $a \equiv 5 \pmod 8$, and as b is odd we get $4b \equiv 4 \pmod 8$. Let $f(x) = ax^2 + 4b - 1$, and proceed exactly as in case 1, except the solution to $ax^2 + by^2 = 1$ is now $(r, 2)$ where $f(r) = 0$.

Case 3: We have $a \equiv b \equiv 3 \pmod 4$.
If we have a solution, then by multiplying through by a suitable power of 2, we can get a solution to $ax^2 + by^2 = 2^{2m}$ for some $m \geq 0$ with $x, y \in \mathbb{Z}_2$. Wlog one of x, y is odd, as otherwise we either have a contradiction if $m = 0$, or we can divide through by 4. Now, $z^2 \equiv 0, 1 \pmod 4$ for $z \in \mathbb{Z}_2$, so $ax^2 + by^2 \equiv 2, 3 \pmod 4$. But $2^{2m} \equiv 0, 1 \pmod 4$ so this is a contradiction, and thus we cannot have a solution.

□

As a corollary of the above lemma and Equation 7.1, we immediately get the full law of quadratic reciprocity! Note that we proved it for all odd coprime a, b and not just for primes. It is also clear how one can go about generalizing the law to number fields other than $\mathbb{Q}$, something which isn't necessarily clear in more elementary proofs. We will always have a solution to $ax^2 + by^2 = 1$ in the infinite places, so we just need to factorize 2 in $\mathcal{O}_K$, and use Hensel's lemma on appropriate polynomials in the corresponding complete fields.

7.2 Towards Eisenstein Reciprocity

As the Hilbert symbol is fairly difficult to define, one would expect some difficulty in calculating $(\alpha, \beta)_v$ in general. While $n = 2$ was fairly straightforward, $n = 3$ already becomes a bit tricky. We will follow the programme set forth in exercise 5.6 of [4], which is quite similar to the approach found in exercise 2 of [1].

For this section, let $n = p$ be an odd prime, let ζ_p be a p^{th} primitive root of unity, and let $K = \mathbb{Q}_p$. Let $\pi = 1 - \zeta_p$, so that $\mathfrak{p} = (\pi)$ is the unique prime above p, hence this is the only finite place in S.

Proposition 7.2. *Let $\alpha, \beta \in \mathbb{Z}[\zeta_p]$ be coprime to each other and to p. Then we have*

$$\left(\frac{\alpha}{\beta}\right)_p \left(\frac{\beta}{\alpha}\right)_p^{-1} = (\beta, \alpha)_{\mathfrak{p}}.$$

Proof. As noted just below Proposition 6.19, we have $\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{\beta}\right)_n$ and $\left(\frac{\beta}{\alpha}\right) = \left(\frac{\beta}{\alpha}\right)_n$. Next, all infinite places v of K have $\mathbb{C}$ as their completion, hence the corresponding local Artin maps are all trivial (the Galois group in question has one element!) and thus $(\alpha, \beta)_v = 1$. Therefore using Proposition 6.19 and that $\mathfrak{p}$ is the only finite element of S gives us the result. □

Let $o_{\mathfrak{p}}^{\times} = \{\alpha \in K_{\mathfrak{p}}^{\times} | v_{\mathfrak{p}}(\alpha) = 0\}$ be the group of units of $\mathcal{O}_{K_{\mathfrak{p}}}$, and let $U_0 = o_{\mathfrak{p}}^{\times}$. Take $\eta_r = 1 - \pi^r$ for $r \geq 1$, and let $U_r = \{\alpha \in K_{\mathfrak{p}}^{\times} | \alpha \equiv 1 \pmod{\pi^r}\}$, a group under multiplication.

Lemma 7.3. *The following four results hold:*
i) The image of π generates $K_{\mathfrak{p}}^{\times}/o_{\mathfrak{p}}^{\times}$.
ii) $o_{\mathfrak{p}}^{\times} = (o_{\mathfrak{p}}^{\times})^p U_1$.
iii) For each $r \geq 1$, the image of η_r generates U_r/U_{r+1}.
iv) $U_{p+1} \subset U_1^p$

Proof. i) Recall that $\mathfrak{p} = (\pi)$; the result is now obvious.

ii) If $\alpha \in o_{\mathfrak{p}}^{\times}$, then as $N\mathfrak{p} = N(\pi) = p$ we have

$$\alpha^{1-p} = (\alpha^{p-1})^{-1} \equiv 1^{-1} \equiv 1 \pmod{\pi}.$$

Letting $\alpha^{1-p} = \gamma$, we see that $\gamma \in U_1$ and $\alpha = \alpha^p\gamma \in (o_{\mathfrak{p}}^{\times})^p U_1$ as required.

iii) Since $\frac{K_{\mathfrak{p}}}{\pi} \simeq \mathbb{F}_p$, $\alpha \in K_{\mathfrak{p}}^{\times}$ can be written uniquely as $\alpha = \sum_{i=m}^{\infty} a_i \pi^i$ where $0 \leq a_i \leq p-1$, $m \in \mathbb{Z}$, and $a_m \neq 0$ (hence $v_{\mathfrak{p}}(\alpha) = m$). Therefore we can take $\{1, 1+\pi^r, 1+2\pi^r, \ldots, 1+(p-1)\pi^r\}$ as representatives for the cosets of U_r/U_{r+1}. Since $\eta_r^i \equiv 1 - i\pi^r \pmod{\pi^{r+1}}$, we see that the image of η_r generates U_r/U_{r+1}.

iv) We will use an idea similar to Hensel's lemma here; start with $\alpha \in U_{p+1}$. Write $\pi^{p-1} = up$ for some unit $u \in \mathcal{O}_{K_{\mathfrak{p}}}$, and let $b_0 = 1$. We construct a sequence $b_0, b_1, \ldots$ such that

$$\alpha \equiv b_j^p \pmod{\pi^{j+p+1}} \qquad\qquad b_{j+1} \equiv b_j \pmod{\pi^{j+2}}.$$

First, note that b_0 satisfies the first equivalence. Given b_j, let $\alpha \equiv b_j^p + x\pi^{j+p+1} \pmod{\pi^{p+j+2}}$, and write $b_{j+1} = b_j + y\pi^{j+2}$, where y must be in $\mathcal{O}_{K_{\mathfrak{p}}}$. To satisfy the first equivalence we thus need

$$b_j^p + x\pi^{j+p+1} \equiv (b_j + y\pi^{j+2})^p \equiv b_j^p + py\pi^{j+2}b_j^{p-1} \equiv b_j^p + \frac{yb_j^{p-1}}{u}\pi^{p+j+1} \pmod{\pi^{j+p+2}}.$$

Taking $y = \dfrac{xu}{b_j^{p-1}}$ works (noting that b_j is a unit as $b_j \equiv b_0 \equiv 1 \pmod{\pi}$), so we define b_{j+1} using this value of y. Now, the second equivalence guarantees us that $\beta = \lim_{j\to\infty} b_j$ exists in $K_{\mathfrak{p}}$, and the first equivalence gives us $\alpha = \beta^p$. Since $b_j \equiv 1 \pmod{\pi}$, we have $\beta \in U_1$ and the result follows.

□

Corollary 7.4. *The set $\{\pi, \eta_1, \eta_2, \ldots, \eta_p\}$ generate $K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^p$*

Proof. For $\alpha \in K_{\mathfrak{p}}^{\times}$, using Lemma 7.3i and ii, we can write $\alpha = \pi^e \gamma^p u_1$ where $e \in \mathbb{Z}$, $\gamma \in o_{\mathfrak{p}}^{\times}$, and $u_1 \in U_1$. Using part iii repeatedly, we get

$$\alpha = \pi^e \gamma^p \eta_1^{e_1} \eta_2^{e_2} \cdots \eta_p^{e_p} u_{p+1},$$

where $e_1, e_2, \ldots, e_p \in \mathbb{Z}$ and $u_{p+1} \in U_{p+1}$. But part iv shows that $u_{p+1} \in U_1^p \subset (K_{\mathfrak{p}}^{\times})^p$ whence

$$\alpha \in \pi^e \eta_1^{e_1} \eta_2^{e_2} \cdots \eta_p^{e_p} \frac{K_{\mathfrak{p}}^{\times}}{(K_{\mathfrak{p}}^{\times})^p}.$$

As α was arbitrary, the corollary follows. □

Thus to calculate $(\alpha, \beta)_{\mathfrak{p}}$ we only need to consider when α, β lie in the set $\{\pi, \eta_1, \eta_2, \ldots, \eta_p\}$. This is accomplished in the next lemma.

Proposition 7.5. *If $u, v \geq 1$, then*

$$(\eta_u, \eta_v)_{\mathfrak{p}} = (\eta_u, \eta_{u+v})_{\mathfrak{p}} (\eta_{u+v}, \eta_v)_{\mathfrak{p}} (\pi, \eta_{u+v})_{\mathfrak{p}}^v (\eta_v, \pi)_{\mathfrak{p}}^v, \tag{7.2}$$

and in particular, $(\eta_u, \eta_v)_{\mathfrak{p}} = 1$ if $u + v > p$. Moreover, $(\pi, \pi)_{\mathfrak{p}} = 1$ and

$$(\eta_u, \pi)_{\mathfrak{p}} = \begin{cases} 1 & \text{if } 1 \leq u < p, \\ \zeta_p & \text{if } u{=}p. \end{cases} \tag{7.3}$$

Proof. Since p is odd, -1 is a p^{th} power, so using Lemma 6.13 we get

$$(\alpha, \alpha)_{\mathfrak{p}} = (\alpha, -1)_{\mathfrak{p}} (\alpha, -\alpha)_{\mathfrak{p}} = 1$$

for all $\alpha \in K_{\mathfrak{p}}^{\times}$. For Equation 7.2, let $\beta = \frac{\eta_v}{\eta_{u+v}} = \frac{1-\pi^v}{1-\pi^{u+v}}$, and note that

$$1 - \beta = \frac{\pi^v - \pi^{u+v}}{1 - \pi^{u+v}} = \pi^v \frac{\eta_u}{\eta_{u+v}}.$$

Lemma 6.13 gives $1 = (\beta, 1-\beta)_{\mathfrak{p}}$, so using the bilinearity of the Hilbert symbol, and $1 = (1, \alpha)_{\mathfrak{p}} = (\alpha, \alpha)_{\mathfrak{p}}$, we can get rid of the denominators and factorize the π out to get

$$\begin{aligned} 1 = \Big(\frac{\eta_v}{\eta_{u+v}}, 1 - \beta\Big)_{\mathfrak{p}} &= \Big(\eta_v, \pi^v \frac{\eta_u}{\eta_{u+v}}\Big)_{\mathfrak{p}} \Big(\eta_{u+v}, \pi^v \frac{\eta_u}{\eta_{u+v}}\Big)_{\mathfrak{p}}^{-1} \\ &= (\eta_v, \pi)_{\mathfrak{p}}^v (\eta_v, \eta_u)_{\mathfrak{p}} (\eta_v, \eta_{u+v})_{\mathfrak{p}}^{-1} [(\eta_{u+v}, \pi)_{\mathfrak{p}}^v (\eta_{u+v}, \eta_u)_{\mathfrak{p}} (\eta_{u+v}, \eta_{u+v})_{\mathfrak{p}}^{-1}]^{-1}, \end{aligned}$$

from which Equation 7.2 follows.

If $1 \leq u < p$, then

$$(\eta_u, \pi)_{\mathfrak{p}}^u = (\eta_u, \pi^u)_{\mathfrak{p}} = (\eta_u, 1 - \eta_u)_{\mathfrak{p}} = 1$$

Thus $(\eta_u, \pi)_{\mathfrak{p}}$ is both a p^{th} and a u^{th} root of unity. But p, u are coprime, so $(\eta_u, \pi)_{\mathfrak{p}} = 1$ as claimed.

If $u + v > p$, then from Lemma 7.3iv we have $\eta_{u+v} \in (K_{\mathfrak{p}}^{\times})^p$, so expressions involving it evaluate to 1. Thus applying Equation 7.2 along with the proven part of Equation 7.3 gives us $(\eta_u, \eta_v)_{\mathfrak{p}} = 1$ when $u + v > p$ and $v \neq p$. If $v = p$, then

$$(\eta_u, \eta_v)_{\mathfrak{p}} = (\eta_p, \pi)_{\mathfrak{p}}^p = (\eta_p, \pi^p)_{\mathfrak{p}} = (\eta_p, 1 - \eta_p)_{\mathfrak{p}} = 1,$$

as required.

We are finally left with calculating $(\eta_p, \pi)_{\mathfrak{p}}$. Take $(u, v) = (1, p-1)$ in Equation 7.2, and we get

$$(\zeta_p, \eta_{p-1})_{\mathfrak{p}} = (\pi, \eta_p)_{\mathfrak{p}}^{p-1} = (\pi, \eta_p)_{\mathfrak{p}}^{-1} = (\eta_p, \pi)_{\mathfrak{p}} \tag{7.4}$$

as the other factors are 1 (and we are working with p^{th} roots of unity). Let $\beta \in \mathcal{O}_K^\times$ have $v_{\mathfrak{p}}(\beta) = 0$, and note that $S(\zeta_p) = S = \{\mathfrak{p}\}$. For finite places $\mathfrak{q} \neq \mathfrak{p}$, we have

$$(\zeta_p, \beta)_{\mathfrak{q}} = \left(\frac{\zeta_p}{\mathfrak{q}}\right)_p^{v_{\mathfrak{q}}(\beta)} = \zeta_p^{v_{\mathfrak{q}}(\beta)\frac{N\mathfrak{q}-1}{p}},$$

where we used corollary 6.17 for the first equality, and the second equality is true modulo p by definition; the only way this can be satisfied is if it is in fact an equality. We have

$$(\zeta_p, \beta)_{\mathfrak{p}} = \big(\prod_{\mathfrak{q}\neq\mathfrak{p}} (\zeta_p, \beta)_{\mathfrak{p}}\big)^{-1} = \big(\prod_{\mathfrak{q}\neq\mathfrak{p}} \zeta_p^{v_{\mathfrak{q}}(\beta)\frac{N\mathfrak{q}-1}{p}}\big)^{-1} \tag{7.5}$$

where the first equality is Proposition 6.15. Thus we need to calculate $\sum v_{\mathfrak{q}}(\beta)(N\mathfrak{q} - 1) \pmod{p^2}$; we can thus restrict the sum to prime ideals dividing β. We claim that

$$\sum_{\mathfrak{q}|\beta} v_{\mathfrak{q}}(\beta)(N\mathfrak{q} - 1) \equiv N(\beta) - 1 \pmod{p^2}. \tag{7.6}$$

Indeed, write $\beta = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$; as $p \mid N\mathfrak{q}_i - 1$ write $N\mathfrak{q}_i = px_i + 1$ for some $x_i \in \mathbb{Z}$. Then the left hand side of the equation is $\sum\limits_{i=1}^{r} e_i x_i p$. Using binomial expansion, $N(\mathfrak{q}_i^{e_i}) = (1 + px_i)^{e_i} \equiv 1 + px_i e_i \pmod{p^2}$, hence the right hand side is $N(\beta) - 1 \equiv \prod\limits_{i=1}^{r}(1 + px_i e_i) - 1 \equiv \sum\limits_{i=1}^{r} e_i x_i p \pmod{p^2}$, so the claim is proven.
Now,

$$N(\eta_{p-1}) = N_{K/\mathbb{Q}}(1 - \pi^{p-1}) = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} (1 - \sigma(1 - \zeta_p)^{p-1}) = \prod_{i=1}^{p-1}(1 - (1 - \zeta_p^i)^{p-1}).$$

As $p \mid \pi^{p-1}$ and $\pi \mid 1 - \zeta_p^i$, upon expansion we see that

$$\prod_{i=1}^{p-1}(1-(1-\zeta_p^i)^{p-1}) \equiv 1-\sum_{i=1}^{p-1}(1-\zeta_p^i)^{p-1} = 1-Tr_{K/\mathbb{Q}}((1-\zeta_p)^{p-1}) = 1-Tr_{K/\mathbb{Q}}\left(\sum_{i=0}^{p-1}\binom{p-1}{i}(-1)^i\zeta_p^i\right) \pmod{p^2}.$$

Now, $Tr_{K/\mathbb{Q}}(\zeta_p^0) = p - 1$, and for $1 \le i \le p-1$, ζ_p^i has minimal polynomial $\dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$, whence $Tr_{K/\mathbb{Q}}(\zeta_p^i) = -1$. Therefore

$$1 - Tr_{K/\mathbb{Q}}\left(\sum_{i=0}^{p-1}\binom{p-1}{i}(-1)^i\zeta_p^i\right) = 1 - \sum_{i=0}^{p-1}\binom{p-1}{i}(-1)^i Tr_{K/\mathbb{Q}}(\zeta_p^i) = 1 - (p-1) - \sum_{i=1}^{p-1}\binom{p-1}{i}(-1)^{i+1}.$$

For all $N \in \mathbb{Z}^+$ we have

$$\binom{N}{0} + \binom{N}{2} + \cdots = \binom{N}{1} + \binom{N}{3} + \cdots.$$

Therefore

$$N(\eta_{p-1}) \equiv 1 - (p-1) - 1 \equiv 1 - p \pmod{p^2},$$

hence by Equation 7.6

$$\sum_{\mathfrak{q}|\eta_{p-1}} v_{\mathfrak{q}}(\eta_{p-1})(N\mathfrak{q} - 1) \equiv -p \pmod{p^2},$$

and combining Equations 7.4, 7.5 with this gives us

$$(\eta_p, \pi)_{\mathfrak{p}} = (\zeta_p, \eta_{p-1})_{\mathfrak{p}} = (\zeta_p^{-1})^{-1} = \zeta_p$$

as required. □

7.3 Cubic Reciprocity Revisited

Proving Eisenstein's reciprocity law is now fairly straightforward, however we will just stick to the cubic case for simplicity. Originally Theorem 4.9, Eisenstein's law of cubic reciprocity is:

Theorem. *Let $\alpha, \beta \in \mathbb{Z}[\omega]$ be primary and relatively prime. Then*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3$$

Furthermore, if $\alpha = a + b\omega$ with $a = 3m + 1$ and $b = 3n$, then

$$\left(\frac{\omega}{\alpha}\right)_3 = \omega^{\frac{1-a-b}{3}} = \omega^{-m-n}; \qquad \left(\frac{1-\omega}{\alpha}\right)_3 = \omega^{\frac{a-1}{3}} = \omega^m.$$

Proof. For the main law, since $\left(\frac{-1}{\gamma}\right)_3 = 1$ for all $\gamma \in \mathbb{Z}$ coprime to π, we can assume $\alpha \equiv \beta \equiv 1 \pmod 3$. Thus $\alpha, \beta \in U_2$, and so we can write

$$\alpha = \eta_2^e \eta_3^f u_4, \qquad \beta = \eta_2^{e'} \eta_3^{f'} u_4'.$$

for $e, e', f, f' \in \mathbb{Z}$ and $u_4, u_4' \in U_4 \subset U_1^3$. Thus when we bilinearly expand $(\beta, \alpha)_{\mathfrak{p}}$, we get terms involving one of u_4, u_4' which evaluate to 1 as they are cubes, and terms of the form $(\eta_x, \eta_y)_{\mathfrak{p}}$ with $x, y \geq 2$. But then $x + y \geq 4 > 3$ so by Proposition 7.5 they too evaluate to 1, whence $(\beta, \alpha)_{\mathfrak{p}} = 1$. Therefore Proposition 7.2 implies the result.

For the first supplementary law, we note that $(\omega)^{S(\alpha)} = \mathcal{O}_K$. Thus Proposition 7.2 gives

$$\left(\frac{\omega}{\alpha}\right)_3 = (\alpha, \omega)_{\mathfrak{p}} = (\alpha, \eta_1)_{\mathfrak{p}}.$$

Note that $\pi^2 = -3\omega$, so $3 = -(1-\pi)^2\pi^2$, and so we can expand α as

$$\alpha = 1 + 3m + 3n\omega = 1 - (1-\pi)^2\pi^2(m + (1-\pi)n) \equiv 1 - (m+n)\pi^2 + (2m+3n)\pi^3 \pmod{\pi^4}.$$

Since $\eta_2^i \equiv 1 - i\pi^2 \pmod{\pi^3}$, we see that $\alpha \equiv \eta_2^{m+n} \pmod{\pi^3}$. Next,

$$\alpha\eta_2^{-m-n} \equiv (1 - (m+n)\pi^2 + (2m+3n)\pi^3)(1 + (m+n)\pi^2) \equiv 1 + (2m+3n)\pi^3 \pmod{\pi^4}.$$

As $\eta_3^i \equiv 1 - i\pi^3 \pmod{\pi^4}$, we get that $\alpha = \eta_2^{m+n}\eta_3^{-2m-3n}u_4$ with $u_4 \in U_4$ (hence it is a cube). Therefore we get

$$\left(\frac{\omega}{\alpha}\right)_3 = (\alpha, \eta_1)_{\mathfrak{p}} = (\eta_2, \eta_1)_{\mathfrak{p}}^{m+n}(\eta_3, \eta_1)_{\mathfrak{p}}^{-2m-3n}.$$

Proposition 7.5 gives us $(\eta_3, \eta_1)_{\mathfrak{p}} = 1$, and

$$(\eta_2, \eta_1)_{\mathfrak{p}} = (\eta_2, \eta_3)_{\mathfrak{p}}(\eta_3, \eta_1)_{\mathfrak{p}}(\pi, \eta_3)_{\mathfrak{p}}(\eta_1, \pi)_{\mathfrak{p}} = (\eta_3, \pi)_{\mathfrak{p}}^{-1} = \omega^2.$$

Therefore

$$\left(\frac{\omega}{\alpha}\right)_3 = \omega^{2m+2n} = \omega^{-m-n},$$

which is the first supplementary law.

For the second supplementary law, note that $(\pi)^S(\alpha) = \mathcal{O}_K$. Therefore by Propositions 6.19, 7.5 we have

$$\left(\frac{1-\omega}{\alpha}\right)_3 = \left(\frac{\pi}{\alpha}\right)_3 = (\alpha, \pi)_{\mathfrak{p}} = (\eta_2, \pi)_{\mathfrak{p}}^{m+n}(\eta_3, \pi)_{\mathfrak{p}}^{-2m-3n} = \omega^{-2m-3n} = \omega^m,$$

which is the second supplementary law. □

References

[1] Cassels, J.W.S. and Fröhlich A. *Algebraic Number Theory.* Academic Press, 1967.

[2] Fisher, T. Local Fields (Michaelmas Term 2011) [pdf]. Retrieved from `http://tartarus.org/gareth/maths/notes/iii/Local_Fields_2011.pdf`

[3] Lemmermeyer, Franz. *Reciprocity Laws: From Euler to Eisenstein.* Springer, 2000.

[4] Swinnerton-Dyer, H.P.F. *A Brief Guide to Algebraic Number Theory.* Cambridge University Press, 2001.