RECIPROCITY LAWS

NANCY XU

ABSTRACT. This paper surveys four of the early reciprocity laws. We start with a discussion of quadratic reciprocity, which we will prove using the splitting of primes in algebraic number fields. We then introduce Gauss and Jacobi sums before using them to prove cubic, biquadratic, and Eisenstein reciprocity.

CONTENTS

1. INTRODUCTION

For distinct primes p, q, reciprocity laws turn the question of whether q is an nth power modulo p into the question of whether p is an nth power modulo q, hence the name "reciprocity." The case $n = 2$ is quadratic reciprocity. The cases $n = 3$ and $n = 4$ are cubic and biquadratic reciprocity, respectively, where we move from the familiar $\mathbb{Z}$ to $\mathbb{Z}[\zeta_3]$ or $\mathbb{Z}[i]$. The Eisenstein reciprocity covers the case $n = l$ for an odd prime l in the cyclotomic field $\mathbb{Z}[\zeta_l]$.

Quadratc reciprocity can be used to solve the problem of whether a prime can be expressed in the form $x^2 + ny^2$, where $x, y \in \mathbb{Z}$ and n is a fixed integer. In particular, if $x^2 + ny^2 \equiv 0 \pmod{p}$ and $(x, y) = 1$, then $x^2 \equiv -ny^2 \pmod{p}$, so n must be a square modulo p. Conversely, if n is a square modulo p then $p|(x^2+ny^2)$. When $n = 1, 2, 3$, if $p|(x^2 + ny^2)$ for x, y relatively prime, then p can be written as $p = x^2 + ny^2$, thus in these cases of n quadratic reciprocity provides a complete characterization of primes expressable as $x^2 + ny^2$. Reciprocity laws also have applications in cryptography; for example, biquadratic reciprocity can be used to identify the encrypted message in the Rabin public-key cryptosystem.

We begin with the discussion of quadratic reciprocity in Section 2, where we first introduce prime splitting in number fields before proceeding to a proof. We then proceed to establishing preliminaries for higher reciprocity with a brief introduction of characters, Gauss sums, and Jacobi sums in Section 3, before diving into cubic, biquadratic, and Eisenstein reciprocity in Sections 4, 5, and 6, respectively.

For this paper, we will assume basic knowledge of abstract algebra and Galois Theory.

2. Quadratic Reciprocity

To formulate quadratic reciprocity we will introduce the Legendre symbol, an indicator function whose output is determined by whether the input integer is a square modulo a prime p. While quadratic reciprocity has many equivalent formulations, its symmetry is the most apparent when presented using the Legendre symbol.

Definition 2.1. For $a, p \in \mathbb{Z}$, p a prime, define the *Legendre symbol* as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p \text{ and } p \nmid a \\ -1 & \text{if } a \text{ is not a square modulo } p \\ 0 & \text{if } p|a. \end{cases}$$

Proposition 2.2. *Let $a, b, p \in \mathbb{Z}$, where p is a prime. We have the following properties:*

1. *(Euler's Criterion) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.*
2. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*
3. *If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

Proof. (2) and (3) are clear from definition, so we will only prove (1).

Let γ be a generator of $\mathbb{F}_p$, $\alpha \equiv \gamma^a \pmod p$, and $x \equiv \gamma^n \pmod p$ for positive integers a, n. Then $x^2 \equiv \alpha \pmod p$ is solvable if and only if $2n \equiv a \pmod{p-1}$ is solvable, where the latter is true when $2|a$, as $(2, p-1) = 2$. Since γ is a generator, this condition holds if and only if $\gamma^{\frac{a(p-1)}{2}} \equiv 1 \pmod p$. □

Proposition 2.2 (2) is a particularly nice property, since using quadratic reciprocity it is possible to determine when an arbitrary integer is a square modulo p by decomposing it into primes and using this multiplicative property. The law of quadratic reciprocity is as follows:

Theorem 2.3. *For odd primes $p, q \in \mathbb{Z}$,*

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

Moreover, we have the following supplements:

- *(First Supplement) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.*
- *(Second Supplement) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

The first supplement follows directly from Proposition 2.2 (1). We will present a proof of the second supplement using prime splitting; it is not the simplest known proof but motivates some of the ideas in higher reciprocity laws. Our strategy is as follows: In Section 2.1, we will show that $\mathbb{Q}[p*]$, where $p* = (-1)^{\frac{p-1}{2}} p$, is the unique quadratic subfield of $\mathbb{Q}[\zeta_p]$. Section 2.2 shows that a prime q splits completely in an intermediate field if and only if this field contains the decomposition field, and we will show that $\mathbb{Q}[p*]$ satisfies this property in Section 2.4. Section 2.3 shows that q splits completely in $\mathbb{Q}[p*]$ if and only if $p*$ is a square modulo q, and finally Section 2.4 will show that q is a square modulo p if and only if q splits completely in $\mathbb{Q}[p*]$

and tie together the pieces from the previous sections. Relevant terminology will be defined in the next few sections.

2.1. **Quadratic Subfield.** In this section, we will determine the unique quadratic subfield of $\mathbb{Q}[\zeta_p]$ by computing the *discriminant* of the pth roots of unity using *norms.* Consider a number field $K/\mathbb{Q}$ of degree n with $\sigma_1, \dots, \sigma_n$ as the n embeddings of $K \in \mathbb{C}$.

Definition 2.4. The *norm* of an element $\alpha \in K$ is given by

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\dots\sigma_n(\alpha).$$

Definition 2.5. For any n-tuple $\alpha_1, \dots, \alpha_n \in K$, the discriminant of $\alpha_1, \dots, \alpha_n$ is given by

$$\Delta(\alpha_1, \dots, \alpha_n) = |\sigma_i(\alpha_j)|^2,$$

i.e. the square of the determinant of the matrix with $\sigma_i(\alpha_j)$ in the ith row and jth column.

As defined, the discriminant is quite difficult to calculate, but interpreting it as the norm of a polynomial can simplify computations.

Proposition 2.6. *For a ring $\mathbb{Q}[\alpha]$, let f be the monic irreducible polynomial for α over $\mathbb{Q}$ and $\alpha_1, \dots, \alpha_n$ be the conjugates of α. Then*

$$\Delta(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \le r < s \le n} (\alpha_s - \alpha_r)^2 = \pm N(f'(\alpha),$$

where the $+$ sign holds if and only if $n \equiv 0, 1 \pmod 4$.

Proof. Let σ_i be the automorphism such that $\sigma_i(\alpha) = \alpha_i$, where $1 \le i \le n$. To show the first equality, we have

$$|\sigma_i(\alpha_j)| = |\sigma_i(\alpha)^j| = |\alpha_i^j|,$$

where $|\alpha_i^j|$ is a Vandermonde determinant. Thus

$$|a_i^j|^2 = \left(\prod_{1 \le r < s \le n} (\alpha_s - \alpha_r) \right)^2 = \prod_{1 \le r < s \le n} (\alpha_s - \alpha_r)^2.$$

Now

$$\Delta(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s),$$

so $(-1)^{\frac{n(n-1)}{2}} = 1$ if and only if $n \equiv 0, 1 \pmod 4$. Since f' has rational coefficients, it follows that

$$N(f'(\alpha)) = \prod_{r=1}^{n} \sigma_r(f'(\alpha)) = \prod_{r=1}^{n} f'(\sigma_r(\alpha)) = \prod_{r=1}^{n} f'(\alpha_r).$$

Since $f(x) = \prod_i (x - \alpha_i)$, for each r, we have $f'(\alpha_r) = \prod_{i \ne r} (\alpha_r - \alpha_i)$, which shows the second equality. □

Proposition 2.7. *Let $p \in \mathbb{Z}$ be a prime, and define $p* = (-1)^{\frac{p-1}{2}} p$. Then $\sqrt{p*} \in \mathbb{Q}[\zeta_p]$.*

Proof. We will first apply Proposition 2.6 to compute $\Delta(1, \zeta_p, \ldots, \zeta_p^{p-2})$ in $\mathbb{Q}[\zeta_p]$.

The irreducible polynomial of ζ_p is given by $f(x) = 1 + x + \ldots + x^{p-1}$, which can be rewritten as $x^p - 1 = (x-1)f(x)$. We differentiate the equation to get $px^{p-1} = f(x) + (x-1)f'(x)$, and substituting $x = \zeta_p$ gives us $f'(\zeta_p) = p/(\zeta_p(\zeta_p - 1))$. We take the norm to get

$$N(f'(\zeta_p)) = \frac{N(p)}{N(\zeta_p)N(\zeta_p - 1)}.$$

Since $\mathbb{Q}[\zeta_p]$ is a Galois extension over $\mathbb{Q}$, the embeddings of $\mathbb{Q}[\zeta_p]$ into $\mathbb{C}$ are precisely the elements in the Galois group of $\mathbb{Q}[\zeta_p]$ over $\mathbb{Q}$. We have

$$N(p) = p^{p-1}$$
$$N(\zeta_p) = \prod_{i=1}^{p-1} \zeta_p^i = \zeta_p^{\frac{p(p-1)}{2}} = 1$$
$$N(\zeta_p - 1) = N(-1)N(1 - \zeta_p) = (-1)^{p-1} \prod_{i=1}^{p-1} (1 - \zeta_p^i) = p.$$

Then $N(f'(\zeta_p)) = \pm p^{p-2}$, where the + sign holds if and only if $p \equiv 1 \pmod 4$ by Proposition 2.6. From the definition of the discriminant, its square root must be in $\mathbb{Q}[\zeta_p]$, which we find to be $\sqrt{\pm p^{p-2}} = p^{\frac{p-3}{2}}\sqrt{p*}$, so $\sqrt{p*} \in \mathbb{Q}[\zeta_p]$ as desired. □

Corollary 2.8. *The unique quadratic subfield of* $\mathbb{Q}[\zeta_p]$ *is* $\mathbb{Q}[\sqrt{p*}]$.

Proof. The Galois group G of $\mathbb{Q}[\zeta_p]$ over $\mathbb{Q}$ is cyclic of order $p-1$, so it has a unique subgroup of order 2. By the Main Theorem of Galois Theory, there exists a unique quadratic subfield of $\mathbb{Q}[\zeta_p]$, which by Proposition 2.7 is $\mathbb{Q}[\sqrt{p*}]$. □

2.2. Prime Splitting.

Prime elements often do not remain irreducible in a larger ring; for example, while 2 is prime in $\mathbb{Z}$, it *splits* in $\mathbb{Z}[i]$ as $2 = (1+i)(1-i)$. Splitting becomes complicated in rings that are not unique factorization domains, thus we will instead work with prime *ideals* instead of prime elements, since prime ideals can be decomposed uniquely in Dedekind domains.

We begin by establishing notation for this subsection. Let K, L be field extensions of $\mathbb{Q}$ such that $K \subset L$. For an arbitrary field F, let $\mathcal{O}_F$ be the ring of integers associated to F. Let $P \subset \mathcal{O}_K$ and $Q \subset \mathcal{O}_L$ be prime ideals in their respective number rings. The goal of this section is to determine the fields K' such that $K \subset K' \subset L$ in which every prime ideal $P \subset \mathcal{O}_K$ *splits completely* in K'.

Definition 2.9. A prime $P \subset \mathcal{O}_K$ *splits completely* in $\mathcal{O}_L$ if and only if P splits into $[L : K]$ distinct primes.

We do so by showing that every prime in $\mathcal{O}_K$ splits completely in what we will call the *decomposition field*, and that all intermediate fields satisfying this property contain this field. Before we proceed, it is important to establish some preliminary definitions to describe a prime decomposition:

Definition 2.10. *Q lies over P*, or *P lies under Q*, if $Q|P\mathcal{O}_L$. Equivalently, $P \subset Q$, or alternatively $Q \cap \mathcal{O}_K = P$.

Every prime $Q \subset \mathcal{O}_L$ lies over a unique prime $P \subset \mathcal{O}_K$, and the argument goes as follows: for a nonzero $\alpha \in Q$, there exists an $a_i \in \mathcal{O}_K$ such that $\alpha^m + a_1\alpha^{m-1} + \ldots + a_m = 0$, where we can assume that $a_m \neq 0$ since we're working in the field L, so $a_m \in Q \cap \mathcal{O}_K$ and $Q \cap \mathcal{O}_K$ is nonempty. Since $1 \notin Q$, it follows that $Q \cap \mathcal{O}_K$ is prime.

Definition 2.11. The ramification index e is the unique nonnegative integer such that $P \subset Q^e$ and $P \not\subset Q^{e+1}$, denoted as $e(Q|P)$.

In other words, if we decompose $P \subset \mathcal{O}_K$ in $\mathcal{O}_L$ as $P = Q_1^{e_1} Q_2^{e_2} \dots Q_g^{e_g}$, then $Q_1, Q_2, \dots, Q_g$ lie over P and have ramification indices $e_1, e_2, \dots, e_g$, respectively.

The containment of $\mathcal{O}_K$ in $\mathcal{O}_L$ induces a ring homomorphism $\mathcal{O}_K \longrightarrow \mathcal{O}_L/Q$ with kernel $\mathcal{O}_K \cap Q = P$, thus $\mathcal{O}_K/P$ embeds in $\mathcal{O}_L/Q$, and $\mathcal{O}_L/Q$ is a finite field extension of $\mathcal{O}_K/P$.

Definition 2.12. The degree of the field extension f of $\mathcal{O}_L/Q$ over $\mathcal{O}_K/P$ is the *inertial degree* of Q over P, denoted as $f(Q|P)$.

One useful property regarding ramification degrees and inertial fields is that they are multiplicative in towers, i.e. if $P \subset Q \subset U$ are prime ideals in the ring of integers of the field extension $F \subset L \subset K$, then

$$e(U|P) = e(U|Q)e(Q|P)$$
$$f(U|P) = f(U|Q)f(Q|P).$$

The next two Propositions will relate the ramification index, inertial degree, and the degree of the extension $K \subset L$ for when the extension L/K is Galois.

Proposition 2.13. *Let $Q, Q' \subset \mathcal{O}_L$ be prime ideals lying over the prime ideal $P \subset \mathcal{O}_K$. Then $\sigma(Q) = Q'$ for some $\sigma \in G(L/K)$.*

Proof. See Section 3, Theorem 23 of Marcus [5]. □

In other words, the Galois group of L/K permutes the prime ideals lying over P transitively.

Proposition 2.14. *Let $n = [L : K]$, and write $P\mathcal{O}_L = Q_1^{e_1} Q_2^{e_2} \dots Q_g^{e_g}$, where $Q_i \in \mathcal{O}_L$ is a prime ideal for $1 \leq i \leq g$ and $Q_i = Q_j$ if and only if $i = j$. Then $e_1 = e_2 = \dots = e_g$ and $f_1 = f_2 = \dots = f_g$. Let e and f denote these common values. Then $gef = n$.*

Proof. See Section 3 of Marcus [5] or Section 12.3, Theorem 3' of Ireland and Rosen [3]. □

Proposition 2.14 is particularly useful in characterizing primes when n is small, as we will see in Sections 4 and 5. For now, if we want to show that every prime splits completely in an intermediate field K', it is enough for us to prove that $[K : K'] = g$ and $e = f = 1$.

For groups H, G, we write $H \subset G$ if H is an arbitrary subgroup of G and $H \triangleleft G$ if H is a normal subgroup of G.

Definition 2.15. Let G be the Galois group of L/K, and suppose that Q lies over P. The *decomposition group* $D \subset G$ is given by $D = D(Q|P) = \{\sigma \in G : \sigma Q = Q\}$. The fixed field L_D of of D is called the *decomposition field*.

It follows that $D = G(L/L_D)$. It can also be checked that D is indeed a subgroup of G.

Proposition 2.16. *Let g be the number of distinct prime ideals in the decomposition of P in $\mathcal{O}_L$. Let $Q_D \in D(Q|P)$ be a prime ideal over P. Then $[L_D : K] = g$ and $e(Q_D|P) = f(Q_D|P) = 1$.*

Proof. We know from Galois Theory that $[L_D : K] = [G : D]$, so it is enough to compute the latter. Every left coset σD, $\sigma \in G$, sends Q to σQ. We know that $\sigma D = \tau D$ if and only if $\sigma Q = \tau Q$, for any $\sigma, \tau \in G$, so there exists a bijection between the set of left cosets σD and set of primes σQ. But by Proposition 2.13, primes of the form σQ are precisely those lying over P, hence there are g of them and $[L_D : K] = g$.

To show $e(Q_D|P) = f(Q_D|P) = 1$, notice that Q is the only prime in S lying over P, since primes lying over P are permuted transitively by $D = G(L/L_D)$. By Proposition 2.14, we have $[L : L_D] = e(Q|Q_D)f(Q|Q_D)$. Our previous results shows that $[L_D : K] = g$, hence again by Proposition 2.14, it follows that $[L : L_D] = e(Q|P)f(Q|P)$. But $e(Q|Q_D) \leq e(Q|P)$ and $f(Q|Q_D) \leq f(Q|P)$, so $e(Q|Q_D) = e(Q|P)$ and $f(Q|Q_D) = f(Q|P)$. Since ramification indices and inertial degrees are multiplicative in towers, we get $e(Q_D|P) = f(Q_D|P) = 1$, as desired. □

Corollary 2.17. *If $D \triangleleft G$, P splits into g distinct primes in $\mathcal{O}_{L_D}$.*

Proof. Since D is a normal subgroup of G, L_D/K is a Galois extension, so the primes lying over P are transitive. Thus from proposition 2.16, it follows that for any $P' \subset L_D$ lying over P, we have $e(P'|P) = f(P'|P) = 1$. Since $[L_D : K] = g$, it follows again from Proposition 2.14 that P splits into g distinct primes in L_D. □

Proposition 2.18. *Let $P' \subset \mathcal{O}_K$ be a prime lying over P. Then L_D is the largest intermediate field K' such that $e(P'|P) = f(P'|P) = 1$.*

$$\begin{tikzcd}
L \arrow[r, dash, "e'f'"] \arrow[dr, dash, "ef"] & L_D K' \arrow[r, dash, "r'"] \arrow[d, dash] & K' \arrow[d, dash] \\
 & L_D \arrow[r, dash, "r"] & K
\end{tikzcd}$$

Proof. Suppose that K' is the fixed field of some $H \subset G$. We know L is a Galois extension of K', thus the decomposition group of Q over $P' \subset K$ is given by $D(Q|P') = D \cap H$. Therefore, from Galois Theory it follows that $L_D K'$ is the decomposition field for Q over P. By Theorem 2.16 and the multiplicativity of the degree of field extensions, we get $[L : L_D] = e(Q|P)f(Q|P)$ and $[L : L_D K'] = e(Q|P')f(Q|P')$. But by multiplicativity $e(Q|P')e(P'|P) = e(Q|P)$ and $f(Q|P')f(P'|P) = f(Q|P)$, so since $e(P'|P) = f(P'|P) = 1$, we have $[L : L_D] = [L : L_D K']$. Thus $[L_D K' : L_D] = 1$ and $K' \subset L_D$, as desired. □

Corollary 2.19. *Let K' be a field such that $K \subset K' \subset L$. If $D \triangleleft G$, then P splits completely in K if and only if $K' \subset L_D$.*

Proof. First, by Proposition 2.14, P splits completely in K' if and only if $e(P'|P) = f(P'|P) = 1$ for a prime $P' \subset \mathcal{O}_{K'}$ lying over P. Thus Proposition 2.18 tell us that $K' \subset L_D$ if P splits completely in K', and conversely if $K' \subset L_D$, Corollary 2.17 tells us that P splits completely in K'. □

2.3. **Prime Splitting in Quadratic Fields.** Our next task is to show that a prime q splits completely in $\mathbb{Q}[p*]$ if and only if it is a square modulo p. To determine the decomposition of prime ideals in quadratic fields, first notice that by Proposition 2.14 there are only three ways a prime can decompose in a quadratic field; since $gef = 2$, either $(e, f, g) = (2, 1, 1)$, $(1, 1, 2)$ or $(1, 2, 1)$. The prime splits completely only in the second case. For this subsection, let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic field with $d \in \mathbb{Z}$ square-free.

Proposition 2.20. *Let $p \in \mathbb{Z}$ be an odd prime. The splitting behavior of p in K is as follows:*

1. *If $p \nmid d$ and d is a square modulo p, then $(p) = PP'$, where $P \neq P'$.*
2. *If $p \nmid d$ and d is not a square modulo p, then $(p) = P$.*
3. *If $p|d$, then $(p) = P^2$.*

Here P and P' are prime ideals in $\mathcal{O}_K$.

Proof. For (1), suppose that $p \nmid d$ and $a^2 \equiv d \pmod p$ for some $a \in \mathbb{F}_p$. We have $(p, a + \sqrt{d})(q, a - \sqrt{d}) = (p)(p, a + \sqrt{d}, a - \sqrt{d}, (a^2 - d)/p)$, where the latter ideal contains $2a = (a + \sqrt{d}) + (a - \sqrt{d})$ and p, which are relatively prime, so $\mathcal{O}_K = (p, a + \sqrt{d}, a - \sqrt{d}, (a^2 - d)/p)$. Let $P = (p, a + \sqrt{d})$ and $P' = (p, a - \sqrt{d})$. If $P = P'$, then $2a, p \in P$ and $P = \mathcal{O}_K$, so $P \neq P'$.

For (2), suppose that $p \nmid d$ and d is not a square modulo p, and let $P \subset \mathcal{O}_K$ be a prime ideal lying over p. If $f(P|p) = 1$, then $\mathbb{F}_p \cong \mathcal{O}_K/P$, so there exists some $a \in \mathbb{F}_p$ such that $a \equiv \sqrt{d} \pmod p$. But then $a^2 \equiv d \pmod p$, which contradicts our assumption, so $f(P|p) = 2$ and P is the only prime lying over p.

For (3), suppose that $p|d$. Then $(p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = (p)(p, (d/p)\sqrt{d})$. We know p and d/p are relatively prime since d is square-free, so $\mathcal{O}_K = (p, (d/p)\sqrt{d})$. Setting $P = (p, \sqrt{d})^2$ gives us what we want. □

The prime decomposition of $p = 2$ can be found in a similar manner.

Proposition 2.21. *Suppose $p = 2$.*

1. *If $m \equiv 1 \pmod 8$, then $(2) = PP'$, where $P \neq P'$.*
2. *If $m \equiv 5 \pmod 8$, then $(2) = P$.*
3. *If $m \equiv 3 \pmod 4$, Then $(2) = P^2$.*

Proof. The same argument as in Proposition 2.20 shows that

- If $m \equiv 1 \pmod 8$, then $(2) = (2, \frac{1+\sqrt{m}}{2})(2, \frac{1-\sqrt{m}}{2})$.
- If $m \equiv 3 \pmod 4$, then $(2) = (2, 1 + \sqrt{m})^2$.

This will show (1) and (3). For (2), if we suppose the contrary, then as in Proposition 2.20 there exists an integer $a \in \mathbb{Z}$ such that $a \equiv (1 + \sqrt{m})/2 \pmod P$. But since $(1+\sqrt{m})/2$ satisfies $x^2 - x + (1-d)/4$, it follows that $a^2 - a + (1-d)/4 \equiv 0 \pmod 2$. However, $2|(a^2 - a)$ for all $a \in \mathbb{Z}$, so it follows that $(1 - d)/4 \equiv 0 \pmod 2$ and $d \equiv 1 \pmod 8$, giving us a contradiction. □

2.4. **Proof.** We are now ready to assemble the proof of quadratic reciprocity. Before we do so, we need one more result concerning the splitting behavior in cyclotomic fields.

Proposition 2.22. *Let $p, m \in \mathbb{Z}$ be such that p is a prime and and $p \nmid m$. Let f be the order of p modulo m. Then $(p) = P_1 P_2 \dots P_g$ in $\mathcal{O}_{\mathbb{Q}[\zeta_p]}$, where the P_is are distinct prime ideals with $f(P_i|P) = f$ and $g = \phi(m)/f$.*

Proof. See Section 13.2, Theorem 2 of Ireland and Rosen [3]. □

Let $F_d \subset \mathbb{Q}[\zeta_p]$ be the unique subfield of degree d over $\mathbb{Q}$ for each divisor d of $p-1$. The next proposition will use Proposition 2.22 to relate prime splitting and being a square modulo p.

Proposition 2.23. *Let $p, q \in \mathbb{Z}$ be odd primes such that $p \neq q$. For a divisor d of $p-1$, q is a dth power modulo p if and only if q splits completely in F_d.*

Proof. By Proposition 2.22, q splits into g distinct primes in $\mathbb{Q}[\zeta_p]$, where each prime has order $f = (p-1)/r$, where f is the order of q in $\mathbb{F}_p^\times$. Let $\gamma \in \mathbb{F}_p^\times$ generate the field. Then the dth powers $\{\gamma^d, \gamma^{d^2}, \ldots, \gamma^{d^{p-1}}\}$ form the unique subgroup of order $(p-1)/d$. Since f is the order of q, we know that q is a dth power modulo p if and only $f|(p-1)/d$, which is true if and only if $F_d \subset F_r$. We know that the decomposition field has degree r over $\mathbb{Q}$ and F_r is the only such field, thus F_r is the decomposition field. By Corollary 2.19, the condition $F_d \subset F_r$ is equivalent to q splitting completely in F_d. □

All that is left of the proof is tying together the results established thus far.

Proof. Proposition 2.23 tells us that $\left(\frac{q}{p}\right) = 1$ if and only if q splits completely in F_2, which we found to be $\mathbb{Q}[\sqrt{p*}]$ in Corollary 2.8. By Proposition 2.20, q splits completely in $\mathbb{Q}[\sqrt{p*}]$ if and only if $\left(\frac{p*}{q}\right) = 1$, thus

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

so

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

as desired.

The same argument and Proposition 2.21 proves the second supplement. □

3. Gauss and Jacobi Sums

To prove the cubic, biquadratic, and Eisenstein reciprocity laws, it is necessary to introduce Gauss and Jacobi sums as well as their essential properties. These sums are defined in terms of *characters*.

Definition 3.1. A *multiplicative character* on $\mathbb{F}_p$ is a map $\chi : \mathbb{F}_p^\times \longrightarrow \mathbb{C}^\times$ satisfying $\chi(a)\chi(b) = \chi(ab)$ for all $a, b \in \mathbb{F}_p^\times$.

Let $a \in \mathbb{F}_p^\times$. The multiplicative character satisfies the following properties:

(1) $\chi(1) = 1$.
(2) $\chi(a)$ is a $(p-1)$th root of unity.
(3) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

The Legendre symbol is an example of a multiplicative character, and so are its analogs for higher reciprocity laws. Another example is the trivial character $\epsilon(a) = 1$ for all $a \in \mathbb{F}_p^\times$. It is sometimes useful to extend the definition of χ to all of $\mathbb{F}_p$ by letting $\epsilon(0) = 0$ and $\chi(0) = 1$ for all $\chi \neq \epsilon$.

The following will be useful in proving certain properties of Gauss and Jacobi sums.

Proposition 3.2. *Let χ be a character on $\mathbb{F}_p$. Then*

$$\sum_{t\in\mathbb{F}_p} \chi(t) = \begin{cases} 0 & \text{if } \chi \neq \epsilon \\ p & \text{if } \chi = \epsilon. \end{cases}$$

Proof. If $\chi = \epsilon$, then $\epsilon(t) = 1$ for all $t \in \mathbb{F}_p$, so the sum equals p. Otherwise, fix an $a \in \mathbb{F}_p^\times$. Then

$$\chi(a) \sum_{t\in\mathbb{F}_p} \chi(t) = \sum_{t\in\mathbb{F}_p} \chi(at) = \sum_{t\in\mathbb{F}_p} \chi(t),$$

since multiplication by a permutes the elements in $\mathbb{F}_p$. Since $\chi(a) \neq 1$, it follows that $\sum_{t\in\mathbb{F}_p} \chi(t) = 0$. □

We will now introduce Gauss and Jacobi sums.

Definition 3.3. Let χ be a character on $\mathbb{F}_p$. The *Gauss sum* on $\mathbb{F}_p$ belonging to χ is defined as $g_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t)\zeta_p^{at}$.

For simplicity of notation, let $g_1(\chi) = g(\chi)$. For $a \in \mathbb{F}_p^\times$ and χ a nontrivial character on $\mathbb{F}_p$, we have:

$$\chi(a)g_a(\chi) = \chi(a) \sum_{t\in\mathbb{F}_p} \chi(t)\zeta_p^{at} = \sum_{t\in\mathbb{F}_p} \chi(at)\zeta_p^{at} = g(\chi),$$

which gives us the identity $g_a(\chi) = \chi(a^{-1})g(\chi)$.

Proposition 3.4. *Let $\chi \neq \epsilon$ be a character on $\mathbb{F}_p$. Then $|g(\chi)|^2 = p$.*

Proof. The strategy is to compute $\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)}$ in two different ways.

First, if $a \neq 0$ we can write $g_a(\chi) = \chi(a^{-1})g(\chi)$ and $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$, so taking the sum over $\mathbb{F}_p$ gives us

$$\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} = \sum_{a\in\mathbb{F}_p} \chi(a)\chi(a^{-1})g(\chi)\overline{g(\chi)} = (p-1)g(\chi)\overline{g(\chi)},$$

since $\chi(a)\chi(a^{-1}) = 1$ for $a \neq 0$ and $\chi(0)\overline{\chi(0)} = 0$.

Next, using the definition of Gauss sums, we have

$$\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} = \sum_{a\in\mathbb{F}_p} \sum_{x,y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta_p^{a(x-y)} = \sum_{x,y\in\mathbb{F}_p} \chi(x)\overline{\chi(y)} \sum_{a\in\mathbb{F}_p} \zeta_p^{a(x-y)}. \quad (*)$$

When $x \neq y$, the inner expression sums over all pth roots of unity, which equals zero since $\sum_{i\in\mathbb{F}_p} \zeta_p^i = (\zeta_p^p - 1)/(\zeta_p - 1) = 0$. When $x = y$, the inner expression sums to p. We know that $\chi(x)\overline{\chi(x)} = 1$ if $x \neq 0$ and $\chi(0)\overline{\chi(0)} = 0$, so $(*)$ reduces to

$$\sum_{x\in\mathbb{F}_p} \chi(x)\overline{\chi(x)}p = (p-1)p.$$

Equating the two expressions gives us $|g(\chi)|^2 = p$. □

There is also a nice relationship between $\overline{g(\chi)}$ and $g(\overline{\chi})$:

$$\overline{g(\chi)} = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\zeta_p^{-t} = \chi(-1) \sum_{t\in\mathbb{F}_p} \overline{\chi(-t)}\zeta_p^{-t} = \chi(-1)g(\overline{\chi}),$$

so the result from Proposition 3.4 can also be expressed as

$$g(\chi)g(\overline{\chi}) = \chi(-1)p.$$

The Jacobi sum is very similar to the Gauss sum and the two sums are very much related, as we'll see in the next proposition. We will primarily use Jacobi sums to decompose certain Gauss sums into primes.

Definition 3.5. For characters χ, λ of $\mathbb{F}_p$, the *Jacobi sum* is defined to be $J(\chi, \lambda) = \sum_{x+y=1} \chi(x)\lambda(y)$.

Proposition 3.6. *Let χ, λ be nontrivial characters of $\mathbb{F}_p$ such that $\chi\lambda \neq \epsilon$. Then $J(\chi, \lambda) = g(\chi)g(\lambda)/g(\chi\lambda)$.*

Proof. Note that

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_{x\in\mathbb{F}_p} \chi(x)\zeta_p^x\right)\left(\sum_{y\in\mathbb{F}_p} \lambda(y)\zeta_p^y\right) \\ &= \sum_{x,y\in\mathbb{F}_p} \chi(x)\lambda(y)\zeta_p^{x+y} \\ &= \sum_{t\in\mathbb{F}_p}\left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta_p^t. \end{aligned}$$

Since χ, λ are characters, $\chi\lambda$ must also be a character. If $t = 0$, by Proposition 3.2 we have

$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_{x\in\mathbb{F}_p} \chi(x)\lambda(-x) = \lambda(-1)\sum_{x\in\mathbb{F}_p} \chi(x)\lambda(x) = 0.$$

If $t \neq 0$, let x', y' be such that $x = tx'$ and $y = ty'$, so the condition $x + y = t$ becomes $x' + y' = 1$. Then

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi(t)\lambda(t)J(\chi, \lambda),$$

so

$$g(\chi)g(\lambda) = \sum_{t\in\mathbb{F}_p} \chi(t)\lambda(t)J(\chi, \lambda)\zeta_p^t = J(\chi, \lambda)g(\chi\lambda),$$

as desired. □

4. Cubic Reciprocity

Cubic reciprocity answers the question of when a prime is a perfect cube modulo another prime. Similar to in quadratic reciprocity, we will formulate cubic reciprocity in terms of the *cubic residue character*, which will best display the underlying symmetry. We will see that the cubic residue character is either 0 or a third root of unity, so it makes sense for us to work in $\mathbb{Z}[\zeta_3]$ instead of $\mathbb{Z}$ for cubic reciprocity.

Our first step is to determine the prime elements in $\mathbb{Z}[\zeta_3]$. Every prime in $\mathbb{Z}[\zeta_3]$ lies over a unique prime in $\mathbb{Z}$, so the primes in $\mathbb{Z}[\zeta_3]$ can be completely characterized using Proposition 2.22:

Proposition 4.1. *Let $p \in \mathbb{Z}$ be a rational prime.*

(1) *If $p \equiv 1 \pmod 3$, then $p = \pi\overline{\pi}$, where π is prime in $\mathbb{Z}[\zeta_3]$.*
(2) *If $p \equiv 2 \pmod 3$, then p is prime in $\mathbb{Z}[\zeta_3]$.*
(3) *If $p = 3$, then $p = -\zeta_3^2(1 - \zeta_3)^2$, where $1 - \zeta_3$ is prime in $\mathbb{Z}[\zeta_3]$.*

Let $\pi \in \mathbb{Z}[\zeta_3]$ be a prime such that $N\pi \neq 3$. For any α relatively prime to π, the analog of Fermat's Little Theorem states that $\alpha^{N\pi - 1} \equiv 1 \pmod{\pi}$. The residue classes of 1, ζ_3, ζ_3^2 are distinct modulo π and $\alpha^{\frac{N\pi-1}{3}}$ is a third root of unity, thus there must be a unique m modulo 3 such that $\alpha^{\frac{N\pi-1}{3}} \equiv \zeta_3^m \pmod{\pi}$.

Definition 4.2. If $N\pi \neq 3$, the *cubic residue character* of α modulo π is given by

(1) $\left(\frac{\alpha}{\pi}\right)_3 = 0$ if $\pi | \alpha$.

(2) $\left(\frac{\alpha}{\pi}\right)_3 = \zeta_3^m$ where m is the unique integer modulo 3 such that $\alpha^{\frac{N\pi-1}{3}} \equiv \zeta_3^m$ $\pmod{\pi}$, if $\pi \nmid \alpha$.

The cubic residue character is also a multiplicative character, and it satisfies similar properties to the Legendre symbol:

Proposition 4.3. *For $\pi, \alpha \in \mathbb{Z}[\zeta_3]$ where π is prime,*

(1) $\left(\frac{\alpha}{\pi}\right)_3 = 1$ if and only if $x^3 \equiv \alpha \pmod{\pi}$ is solvable, i.e. if and only if α is a cubic residue.

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

(3) If $\alpha \equiv \beta \pmod{\pi}$, then $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Proof. (2) and (3) are clear from definition, and the proof of (1) is similar to that of Proposition 2.2, but instead we work in $[\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]]$.

As before, the multiplicative property will allow us to determine whether any $\alpha \in \mathbb{Z}[\zeta_3]$ is a perfect cubic modulo a prime, since we can factor α into primes and use multiplicativity. □

Every element in $\mathbb{Z}[\zeta_3]$ has 6 associates, including itself, so it is enough to determine the reciprocity law for one of its associates and the units in $\mathbb{Z}_3$. We will state cubic reciprocity for one such associate – which we will designate *primary* – and the units will be taken care of in the supplementary laws. See Section 9.3, Theorem 1 of Ireland and Rosen [3] for the supplements.

Definition 4.4. A prime $\pi \in \mathbb{Z}[\zeta_3]$ is *primary* if $\pi \equiv 2 \pmod{3}$.

Proposition 4.5. *Let $N\pi = p \equiv 1 \pmod{3}$. Then exactly one of the associates of π is primary.*

Proof. Write $\pi = a + b\zeta_3$. We will first prove existence. The associates of π are

$$a+b\zeta_3, \quad -b+(a-b)\zeta_3, \quad (b-a)-a\zeta_3, \quad -a-b\zeta_3, \quad b+(b-a)\zeta_3, \quad (a-b)+a\zeta_3.$$

Since $p = a^2 - ab + b^2 \equiv 1 \pmod{3}$, either $3 \nmid a$ or $3 \nmid b$. Thus the first term of either the first or second associate is not divisible by 3, so suppose $3 \nmid a$. Similarly, from the first and fourth associates, we can further assume that $a \equiv 2 \pmod{3}$. Now $1 \equiv 4 - 2b + b^2 \pmod{3}$, so $b(b-2) \equiv 0 \pmod{3}$. If $3|b$, the $a + b\zeta_3$ is primary, and if $b \equiv 2 \pmod{3}$, then $b + (b-a)\zeta_3$ is primary.

To prove uniqueness, suppose that $a + b\zeta_3$ is primary. It is clear from taking congruences modulo 3 that no other associate is primary. □

We are now in a position to state the law of cubic reciprocity.

Theorem 4.6 (Cubic Reciprocity)**.** *Let $\pi_1, \pi_2 \in \mathbb{Z}[i]$ be primary primes with $N\pi_1, N\pi_2 \neq 3$ and $N\pi_1 \neq N\pi_2$. Then*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

For simplicity of notation, let $\chi_\pi = \left(\frac{\cdot}{\pi}\right)_3$ for the remainder of this section. Let $\pi \in \mathbb{Z}[\zeta_3]$ be a complex prime. Then $N\pi = p \equiv 1 \pmod 3$ for an odd rational prime p. We know $\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]$ is a finite field of characteristic p, so $\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]$ is isomorphic to $\mathbb{F}_p$. Then we can consider χ_π as a character on $\mathbb{F}_p$, which allows us to work with $G(\chi_\pi)$ and $J(\chi_\pi, \chi_\pi)$.

The proof will proceed as follows: We will first find the prime factorization of $g(\chi_\pi)^3$ in $\mathbb{Z}[\zeta_3]$ by writing it in terms of a Jacobi sum, which is easier to compute. We will then separate into cases based on whether π_1, π_2 are complex or rational primes, but the general procedure will be to deduce reciprocity by rewriting a Gauss sum in two different ways.

The following propositions will lead us to the prime factorization of $g(\chi_\pi)^3$.

Proposition 4.7. *Let χ_π be the cubic residue character, where π is primary. Then $g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi)$.*

Proof. Proposition 3.6 tells us that

$$g(\chi_\pi)^3 = g(\chi_\pi)g(\chi_\pi^2)J(\chi_\pi, \chi_\pi) = g(\chi_\pi)g(\overline{\chi_\pi})J(\chi_\pi, \chi_\pi).$$

Using Proposition 3.4 and observing that $\chi_\pi(-1) = \chi_\pi((-1)^3) = 1$, we get $g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi)$. □

Proposition 4.8. *Let χ_π be as before. Then $J(\chi_\pi, \chi_\pi) = \pi$.*

Proof. Proposition 3.4 and Proposition 3.6 tells us that $J(\chi_\pi, \chi_\pi)\overline{J(\chi_\pi, \chi_\pi)} = p$, where we recall that $N\pi = p \equiv 1 \pmod 3$ and p is a rational prime. Thus $J(\chi_\pi, \chi_\pi)$ is a prime in $\mathbb{Z}[\zeta_3]$ with norm p. Reducing modulo 3 gives us:

$$g(\chi_\pi) = \left(\sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta_p^{3t}\right)^3 \equiv \sum_{t\in\mathbb{F}_p} \chi_\pi(t)^3\zeta_p^{3t} \pmod 3.$$

Since χ_π is cubic, we have $\chi(0) = 0$ and $\chi(t)^3 = 1$ for $t \neq 0$, so $\sum_{t\in\mathbb{F}_p} \chi_\pi(t)^3\zeta_p^{3t} = -1$. Then

$$pJ(\chi_\pi, \chi_\pi) = g(\chi_\pi)^3 \equiv -1 \pmod 3,$$

and since $p \equiv 1 \pmod 3$, we have $J(\chi_\pi, \chi_\pi) \equiv -1 + 0 \cdot \zeta_3 \pmod 3$. Thus $J(\chi_\pi, \chi_\pi)$ is in fact a primary prime.

Let $J(\chi_\pi, \chi_\pi) = \pi'$. We know $p = \pi\overline{\pi} = \pi'\overline{\pi}'$, so either $\pi|\pi'$ or $\pi|\overline{\pi}'$, and since the primes are primary, either $\pi = \pi'$ or $\pi = \overline{\pi}'$. We want to show the former. We have

$$J(\chi_\pi, \chi_\pi) = \sum_{t\in\mathbb{F}_p} \chi_\pi(t)\chi_\pi(1-t) = \sum_{t\in\mathbb{F}_p} t^{\frac{p-1}{3}}(1-t)^{\frac{p-1}{3}} \pmod \pi$$

by definition. The coefficients in the polynomial are of the form $a\sum_{c\in\mathbb{F}_p} c^k$ for some a and $(p-1)/3 \leq k < 2(p-1)/3$, so if γ is a generator of $\mathbb{F}_p$, the sum reduces as

$$a\sum_{c\in\mathbb{F}_p} c^k = a\sum_{i=1}^{p-1} \gamma^{ik} = a\frac{\gamma^{(p-1)k} - 1}{\gamma^k - 1} \equiv 0 \pmod p,$$

since $(k, p-1) = 1$. Thus $J(\chi_\pi, \chi_\pi) \equiv 0 \pmod \pi$ and $\pi = \pi'$, as desired. □

Corollary 4.9. *With definitions as above, we have $g(\chi_\pi)^3 = \pi^2\overline{\pi} = p\pi$.*

Proof. This follows directly from Propositions 4.7 and 4.8. □

We can now present the proof of cubic reciprocity.

Proof. We will consider three cases: if π_1, π_2 are both rational primes, one is rational and one is complex, and both are complex.

Case 1. Suppose that $\pi_1 = q$ and $\pi_2 = p$, where p, q are rational primes. We need a few preliminary results:

(1) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.
(2) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.
(3) $\chi_p(n) = 1$ if n is a rational integer relatively prime to p.

For (1), $\chi_\pi(\alpha)$ equals $1, \zeta_3$, or ζ_3^2, and in each case its square is equal to its conjugate. For (2), by definition we have

$$\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi},$$

and taking the conjugate gives us

$$\overline{\alpha}^{\frac{N\pi-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}.$$

Since $N\pi = N\overline{\pi}$, we have $\chi_{\overline{\pi}}(\overline{\alpha}) \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$, thus $\chi_{\overline{\pi}}(\overline{\alpha}) \equiv \overline{\chi_\pi(\alpha)}$. To show (3), we have from (1) and (2) that

$$\chi_p(n) = \overline{\chi_p(n)} = \chi_p(n)^2,$$

so $\chi_p(n) = 1$. From (3), $\chi_q(p), \chi_p(q) = 1$, so $\chi_q(p) = \chi_p(q)$ trivially.

Case 2. Suppose that $\pi_1 = q \equiv 2 \pmod 3$ is a rational prime and π_2 is a complex prime with norm $p \equiv 1 \pmod 3$. Raising both side of $g(\chi_{\pi_2}) = p\pi$ to the $(q^2-1)/3$th power and reducing modulo q gives us

$$g(\chi_{\pi_2})^{q^2-1} = (p\pi_2)^{\frac{q^2-1}{3}} \equiv \chi_q(p\pi_2) \pmod{q}.$$

But $\chi_q(p) = 1$ by Case 1, so

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi_2) g(\chi_{\pi_2}) \pmod{q}.$$

Expanding $g(\chi_{\pi_2})^{q^2}$ using the definition of Gauss sums gives us

$$g(\chi_{\pi_2})^{q^2} = \left(\sum_{t\in\mathbb{F}_p} (t)\zeta_p^t\right)^{q^2} \equiv \sum_{t\in\mathbb{F}_p} \chi_{\pi_2}(t)^{q^2}\zeta_p^{q^2 t} \pmod{q}.$$

Since $q^2 \equiv 1 \pmod 3$ and χ_{π_2} is a cubic residue, the expression simplifies as

$$g(\chi_{\pi_2})^{q^2} \equiv \chi_{q^2}(\chi_{\pi_2}) \equiv \chi_{\pi_2}(q^{-2}) g(\chi_{\pi_2}) \equiv \chi_\pi(q) g(\chi_{\pi_2}) \pmod{q}.$$

Putting everything together, we have $\chi_{\pi_2}(q) g(\chi_{\pi_2}) \equiv \chi_q(\pi_2) g(\chi_{\pi_2}) \pmod{q}$, so multiplying both sides by $g(\overline{\chi}_\pi)$ and then by p^{-1} gives us $\chi_{\pi_2}(q) \equiv \chi_q(\pi_2) \pmod{q}$, so it follows that $\chi_{\pi_2}(q) = \chi_q(\pi)$.

Case 3. Suppose that π_1, π_2 are complex primes with $N\pi_1 = p_1$ and $N\pi_2 = p_2$ such that $p_1, p_2 \equiv 1 \pmod 3$. From $g(\chi_{\overline{\pi}_1})^3 = p_1\overline{\pi}_1$, raising both sides to the $(N\pi_2 - 1)/3 = (p_2-1)/3$th power, taking the congruence modulo π_2, and applying the same argument as in the second case gives us

$$\chi_{\overline{\pi}_1}(p_2^2) = \chi_{\pi_2}(p_1\overline{\pi}_1).$$

Similarly, raising both sides of $g(\chi_{\pi_2})^3 = p_2\pi_2$ to the $(p_1-1)/3$th power and reducing modulo π_1 gives us

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2).$$

It follows from Case 1 (2) that $\chi_{\overline{\pi}_1}(p_2^2) = \chi_{\pi_1}(p_2)$. Then

$$\begin{aligned}\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi}_1) &= \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi}_1}(p_2^2)\\ &= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2)\\ &= \chi_{\pi_2}(p_1^2)\\ &= \chi_{\pi_2}(\pi_1)\chi(p_1\overline{\pi}_1),\end{aligned}$$

so it follows that $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$. □

5. Biquadratic Reciprocity

Biquadratic reciprocity addresses the question of when an element is a perfect fourth power modulo another element relatively prime to it. The major distinction between this and the previous two reciprocity laws is that it is no longer stated for primes, but for elements that are relatively prime, thus new notation is needed. However, much of the proof techniques will be similar to in cubic reciprocity, hence some details in this section will be omitted. The *biquadratic residue character* will either be 0 or a fourth root of unity, hence we will work in $\mathbb{Z}[i]$. We can characterize the primes in $\mathbb{Z}[i]$ by decomposing primes in $\mathbb{Z}$ using Proposition 2.22.

Proposition 5.1. *Let $p \in \mathbb{Z}$ be a rational prime.*

(1) If $p \equiv 1 \pmod 4$, then $p = \pi\overline{\pi}$, where π is prime in $\mathbb{Z}[i]$.
(2) If $p \equiv 3 \pmod 4$, then p is prime in $\mathbb{Z}[i]$.
(3) If $p = 2$, then $p = -i(1+i)^2$ where $(1+i)$ is prime in $\mathbb{Z}[i]$.

For any prime $\pi \in \mathbb{Z}[i]$ such that $N\pi \neq 2$, we know that the residue classes of $1, -1, i, -i$ are distinct modulo π, so as before there exists a unique j modulo 4 such that $\alpha^{(N\pi-1)/4} \equiv i^j \pmod{\pi}$.

Definition 5.2. Let $\pi \in \mathbb{Z}[i]$ be an irreducible element such that $N\pi \neq 2$. The *biquadratic (or quartic) residue character* of α over π is given by

(1) $\left(\frac{\alpha}{\pi}\right)_4 = 0$ if $\pi|\alpha$.
(2) $\left(\frac{\alpha}{\pi}\right)_4 = i^j$, where $\alpha^{\frac{N\pi-1}{4}} \equiv i^j \pmod{\pi}$ for a unique j modulo 4, when $\pi \nmid \alpha$.

The biquadratic residue character satisfies the same properties as listed in Proposition 4.3, with the modification in (1) that $\left(\frac{\alpha}{\pi}\right)_4 = 1$ if and only if α is a perfect fourth power in $\mathbb{Z}[i]$. The proof proceeds in a similar manner.

We can extend Definition 5.2 so that the residue character is defined for any pair of relatively prime elements:

Definition 5.3. For a nonunit $\alpha \in \mathbb{Z}[i]$ such that $(1+i) \nmid \alpha$, write $\alpha = \prod_i \lambda_i$, where λ_i is irreducible. Let $\beta \in \mathbb{Z}[i]$ be such that β is relatively prime to α. Define

$$\left(\frac{\beta}{\alpha}\right)_4 = \prod_i \left(\frac{\beta}{\lambda_i}\right)_4.$$

This symbol is well-defined since $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\lambda}\right)_4$ if $(\pi) = (\lambda)$.

Like in the cubic case, it is convenient to introduce the notion of "primary." However, here primary elements in $\mathbb{Z}[i]$ need not be prime.

Definition 5.4. A nonunit $\alpha \in \mathbb{Z}[i]$ is primary if $\alpha \equiv 1 \pmod{(1+i)^3}$.

Proposition 5.5. *A nonunit $\alpha \in \mathbb{Z}[i]$ is primary iff either $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$, or $a \equiv 3 \pmod 4$.*

Proof. See Section 9.7, Lemma 6 of Ireland and Rosen [3]. □

Proposition 5.6. *For a nonunit $\alpha \in \mathbb{Z}[i]$ such that $(1+i) \nmid \alpha$, there exists a unique unit u such that $u\alpha$ is primary.*

Proof. See Section 9.7, Lemma 7 of Ireland and Rosen [3]. □

It can be shown that a primary element can be written as the product of primary irreducibles. Observe that for the biquadratic case, it is no longer necessary for a primary element to be prime in $\mathbb{Z}[i]$; in fact biquadratic reciprocity will be stated for two relatively prime elements rather than two primes.

We will first prove a supplemental case that will be useful in the proof of biquadratic reciprocity.

Proposition 5.7. *Given $n \in \mathbb{Z}$ such that $n \equiv 1 \pmod 4$, we have $\chi_n(i) = (-1)^{\frac{n-1}{4}}$.*

Proof. If $n = p \equiv 1 \pmod 4$ for p a positive prime, then $p = \pi\overline{\pi}$ for an irreducible π and

$$\left(\frac{i}{p}\right)_4 = \left(\frac{i}{\pi}\right)_4 \left(\frac{i}{\overline{\pi}}\right)_4 = (i^{\frac{p-1}{4}})^2 = (-1)^{\frac{p-1}{4}}.$$

If $n = -q$ for an odd prime $q \equiv 3 \pmod 4$, then

$$\left(\frac{i}{-q}\right)_4 = i^{\frac{q^2-1}{4}} = (i^{q-1})^{\frac{q+1}{4}} = (-1)^{\frac{-q-1}{4}}.$$

An arbitrary n can be written as a product of primes of the form p and $-q$, so it is enough to show that for $n = st$ we have $(n-1)/4 \equiv (s-1)/4 + (t-1)/4 \pmod 2$, since the general case will follow by induction. This can be shown by doing casework on whether s, t are congruent to 1 or 5 $\pmod 8$. □

We will now state biquadratic reciprocity.

Theorem 5.8 (Biquadratic Reciprocity)**.** *Let λ, π be relatively prime primary elements of $\mathbb{Z}[i]$. Then*

$$\left(\frac{\lambda}{\pi}\right)_4 = \left(\frac{\pi}{\lambda}\right)_4 (-1)^{\frac{N\lambda-1}{4}\cdot\frac{N\pi-1}{4}}.$$

For simplicity of notation, let $\chi_\pi = \left(\frac{\cdot}{\pi}\right)_4$ for the remainder of the section. As in the cubic case, let $\pi \in \mathbb{Z}[i]$ be a complex primary irreducible so that $N\pi = p \equiv 1 \pmod 4$. Since $\mathbb{Z}[i]/\pi\mathbb{Z}[i] \simeq \mathbb{F}_p$, we can consider χ_π as a biquadratic character on $\mathbb{F}_p$. The structure of the proof will be similar to in cubic reciprocity: we will first find the prime factorization of $g(\chi_\pi)^4$, then prove special cases of the theorem to build up to the general case.

Proposition 5.9. *For $p \equiv 1 \pmod 4$ an odd prime, $g(\chi_\pi)^4 = pJ(\chi_p, \chi_p)^2$. Also, we have $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) = \pi$, so consequently $g(\chi_\pi)^4 = \pi^3\overline{\pi}$.*

Proof. See Section 9.9 of Ireland and Rosen [3]. □

We will begin the proof by considering special cases. When λ, π are rational integers, the case is similar to in cubic reciprocity.

Proposition 5.10. *Let $\alpha, a \in \mathbb{Z}$ be such that $\alpha \neq 0$, a is an odd nonunit, and α and a are relatively prime. Then $\chi_a(\alpha) = 1$.*

Proof. Without loss of generality, suppose $a > 0$ and write $a = \Pi p_i \Pi q_i$, where p_i, q_i are primes such that $p_i \equiv 1 \pmod 4$ and $q_i \equiv 3 \pmod 4$. It follows from definition that for $\pi, \alpha \in \mathbb{Z}[i]$ where π is irreducible with $N\pi \neq 2$ and $\pi \nmid \alpha$, we have $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$. Therefore, if $p_i = \pi\overline{\pi}$ for an irreducible element π, we have

$$\chi_\alpha(p_i) = \chi_\alpha(\pi)\chi_\alpha(\overline{\pi}) = \chi_\alpha(\pi)\overline{\chi_\alpha(\pi)} = 1.$$

On the other hand, since $Nq_i = q_i^2$,

$$\chi_a(q_i) \equiv a^{\frac{q_i^2-1}{4}} \equiv (a^{q_i-1})^{\frac{q_i+1}{4}} \equiv 1 \pmod q)_i.$$

From multiplicativity it follows that $\chi_a(\alpha) = 1$. □

From the preceding proposition, if $\lambda = a$, $\pi = \alpha$ for relatively prime nonunits $a, \alpha \in \mathbb{Z}$, we have trivially that $\chi_\alpha(a) = \chi_a(\alpha) = 1$. This settles the case of when λ, π are relatively prime rational integers.

We will now consider the case of when one element is complex and the other a rational integer, starting with when λ, π are irreducibles.

Proposition 5.11. *For an odd prime $q \in \mathbb{Z}$, $\chi_\pi((-1)^{\frac{q-1}{2}}q) = \chi_q(\pi)$.*

Proof. First, notice that what we have is indeed a special case of biquadratic reciprocity since $(-1)^{\frac{q-1}{2}}q$ is primary for any odd prime $q \in \mathbb{Z}$. We can consider separately when $q \equiv 1$ or $3 \pmod 4$, but in both cases the strategy is to write $g(\chi_\pi)^{q+1}$ (resp. $g(\chi_\pi)^{q+3}$) in two different ways, one by using the definition of Gauss sums to simplify $g(\chi_\pi)^q$, and the other by raising $g(\chi_\pi)^4 = \pi^3\overline{\pi}$ to the $(q+1)/4$th (resp. $(q+3)/4$th) power. Details can be found in Section 9.9 of Ireland and Rosen [3]. □

The previous result can be generalized as follows:

Proposition 5.12. *Let $a \in \mathbb{Z}$ be such that $a \equiv 1 \pmod 4$ and let $\lambda \in \mathbb{Z}[i]$ be primary, where λ is relatively prime to a. Then $\chi_a(\lambda) = \chi_\lambda(a)$.*

Proof. By assumption a is primary, so we can write it as a product of primary primes $p_1, \dots, p_n$ and $q_1, \dots, q_m$, where $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$, for $1 \leq i \leq n$ and $1 \leq j \leq m$. Since $a \equiv 1 \pmod 4$, it follows that $a = p_1 \dots p_n(-q_1)\dots(-q_m)$. Applying Proposition 5.11 gives us

$$\chi_a(\lambda) = \prod_i \chi_{p_i}(\lambda) \prod_j \chi_{q_j}(\lambda) = \chi_\lambda(p_i)\chi_\lambda(-q_j) = \chi_\lambda(a).$$

□

For the next case, suppose that $\pi = a + bi$ and $\lambda = c + di$ are primary and relatively prime.

Proposition 5.13. *If $(a, b) = 1$, $(c, d) = 1$, then $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}$.*

Proof. From the hypothesis, we have $(a, \pi) = (b, \pi) = (c, \lambda) = (d, \lambda)$. From $ci \equiv d \pmod \lambda$, multiplying both sides by b and simplifying gives us $c\pi \equiv ac + bd \pmod \lambda$, so $(ac + bd, \lambda) = (ac + bd, \pi) = 1$ and

$$\chi_\lambda(c)\chi_\lambda(\pi) = \chi_\lambda(ac + bd). \quad (1)$$

Similarly, $a\lambda \equiv ac + bd \pmod{\pi}$, so

$$\chi_\pi(a)\chi_\pi(\lambda) = \chi_\pi(ac+bd). \quad (2)$$

Multiplying the conjugate of (2) by (1) gives us:

$$\chi_\lambda(c)\chi_{\overline{\pi}}(a)\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\lambda\overline{\pi}}(ac+bd),$$

or

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_\lambda(c)\chi_{\overline{\pi}}(a)\chi_{\lambda\overline{\pi}}(ac+bd).$$

Suppose first that c, a, and $ac+bd$ are nonunits. For each odd integer n, let $\epsilon(n) = (-1)^{\frac{n-1}{2}}$. Then $\epsilon(n)n \equiv 1 \pmod 4$ is primary, so working in terms of $\epsilon(n)n$ and using Proposition 5.12 gives us:

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_c(\overline{\lambda})\chi_a(\pi)\chi_{ac+bd}(\lambda\overline{\pi}).$$

From Proposition 5.10, it follows that

$$\begin{aligned}
\chi_c(\overline{\lambda}) &= \chi_c(c-di) = \chi_c(-di) = \chi_c(i)\\
\chi_a(\pi) &= \chi_a(a+bi) = \chi_a(bi) = \chi_a(i)\\
\chi_{ac+bd}(\overline{\pi}\lambda) &= \chi_{ac+bd}((ad-bc)i) = \chi_{ac+bd}(i).
\end{aligned}$$

Thus

$$\begin{aligned}
\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} &= \chi_{(ac+bd)ac}(i)\\
&= (-1)^{\frac{(ac+bd)ac-1}{4}}\\
&= (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}.
\end{aligned}$$

We get the first equality from Proposition 5.7, and the second can be shown using Proposition 5.5 and casework.

When a, c, or $ac+bd$ equals ±1, we have $\chi_\pi(\pm 1) = \chi_{\pm 1}(\pi) = 1$, and a similar strategy as the one illustrated will suffice. □

Most of the work has already been done, and to prove the general case of biquadratic reciprocity, all that is left is to put together the special cases.

Proof. Write $\pi = m(a+bi)$ and $\lambda = n(c+di)$, where $(a,b) = (c,d) = 1$ and $m \equiv n \equiv 1 \pmod 4$, so $a+bi$ and $c+di$ are primary. It follows from Proposition 5.11 that $\chi_\pi(n) = \chi_n(\pi)$ and $\chi_\lambda(m) = \chi_m(\lambda)$, and from Proposition 5.10 that $\chi_m(n) = \chi_n(m) = 1$. Thus

$$\begin{aligned}
\chi_\lambda(\pi) &= \chi_\lambda(m)\chi_\lambda(a+bi)\\
&= \chi_m(\lambda)\chi_n(a+bi)\chi_{c+di}(a+bi)\\
&= \chi_m(\lambda)\chi_{a+bi}(n)\chi_{a+bi}(c+di)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}\\
&= \chi_\pi(\lambda)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}\\
&= \chi_\pi(\lambda)(-1)^{\frac{N\pi-1}{4}\cdot\frac{N\lambda-1}{4}},
\end{aligned}$$

where the last equality follows from $m \equiv n \equiv 1 \pmod 4$. □

6. Eisenstein Reciprocity

Eisenstein's reciprocity generalizes some of the previous reciprocity laws for perfect odd powers. We will work in the ring of integers of the cyclotomic field $K = \mathbb{Q}[\zeta_m]$, denoted $\mathcal{O}_K$. To take advantage of unique prime factorization, we will consider prime ideals rather than prime elements in K, so it is necessary for us to extend the notion of a norm to ideals.

Definition 6.1. For an ideal $A \subset \mathcal{O}_K$, we define the *norm of* A, $N(A)$, to be the number of elements in $\mathcal{O}_K/A$.

The norm is well-defined since $\mathcal{O}_K/A$ is always finite, and it can be checked that the norm is multiplicative (see Section 14.1, Proposition 14.1.1 of Ireland and Rosen [3] for details).

Proposition 6.2. *Let $K/\mathbb{Q}$ be a Galois extension with G its Galois group. Then*

$$\prod_{\sigma \in G} \sigma(A) = (N(A)).$$

Proof. See Section 14.1, Propositon 14.1.2 of Ireland and Rosen [3]. □

Let $P \subset \mathcal{O}_K$ be a prime ideal not containing m, and let $q = N(P) = |\mathcal{O}_K/P|$. For simplicity, for any $w \in \mathcal{O}_K$, we will denote as $\overline{w}$ its coset in $\mathcal{O}_K/P$.

We know $x^m - 1 = \sum_{i=0}^{m-1}(x - \zeta_m^i)$, so dividing both sides by $x - 1$ gives us

$$1 + x + \ldots + x^{m-1} = \prod_{i=1}^{m-1}(x - \zeta_m^i).$$

Let $x = 1$. Then $m = \prod_{i=1}^{m-1}(1 - \zeta_m^i)$, so reducing modulo $\mathcal{O}_K/P$ gives us $\overline{m} = \prod_{i=1}^{m-1} \overline{(1 - \zeta_m^i)}$. We know $\overline{m} \neq \overline{0}$, so it follows that $\overline{\zeta}_m^i \neq 1$ for $1 \leq i \leq m-1$. Therefore $\overline{\zeta}_m^i = \overline{\zeta}_m^j$ if and only if $i = j$ for $0 \leq i, j \leq m-1$, so the cosets of $1, \zeta_m, \ldots, \zeta_m^{m-1}$ are distinct in $\mathcal{O}_K/P$. From the analog of Fermat's Little Theorem, we have $\alpha^{q-1} \equiv 1 \pmod{P}$ for $\alpha \in \mathcal{O}_K$, $\alpha \notin P$, so

$$\sum_{i=0}^{m-1}(\alpha^{\frac{q-1}{m}} - \zeta_m^i) \equiv 0 \pmod{P}.$$

Since P is prime it follows that there exists a unique i modulo m such that $\alpha^{\frac{q-1}{m}} \equiv \zeta_m^i \pmod{P}$.

Definition 6.3. For $\alpha \in \mathcal{O}_K$ and P a prime ideal such that $m \notin P$, define the *mth power residue symbol*, $\left(\frac{\alpha}{P}\right)_m$, as:

1. $\left(\frac{\alpha}{P}\right)_m = 0$ if $\alpha \in P$.
2. $\left(\frac{\alpha}{P}\right)_m = \zeta_m^i$, where i is the unique integer modulo m such that $\alpha^{\frac{NP-1}{m}} \equiv \zeta_m^i \pmod{P}$, if $\alpha \notin P$.

The power residue symbol generalizes the quadratic, cubic, and quartic residue characters and satisfies the same properties, specifically those listed in Proposition 4.3 with the modification in (1) that $\left(\frac{\alpha}{P}\right)_m = 1$ if and only if $x^m \equiv \alpha \pmod{P}$ is solvable in $\mathcal{O}_K$.

As in the quartic case, we can extend this definition to an arbitrary ideal:

Definition 6.4. Let $A \subset \mathcal{O}_K$ be an ideal prime to m with prime decomposition $A = P_1 P_2 \dots P_n$. For $\alpha \in \mathcal{O}_K$, define $\left(\frac{\alpha}{A}\right)_m = \prod_{i=1}^n \left(\frac{\alpha}{P_i}\right)_m$. If $\beta \in \mathcal{O}_K$ is relatively prime to m, define $\left(\frac{\alpha}{\beta}\right)_m = \left(\frac{\alpha}{(\beta)}\right)_m$.

The purpose of this definition is so that we can express the power residue symbol in terms of two elements in $\mathcal{O}_K$ rather than an element and an ideal. Eisenstein's Reciprocity law will also be stated using this refined definition.

Proposition 6.5. *Let $A, B \subset \mathcal{O}_K$ be ideals relatively prime to m. Then*

(1) $\left(\frac{\alpha\beta}{A}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\beta}{A}\right)_m$.
(2) $\left(\frac{\alpha}{AB}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\alpha}{B}\right)_m$.
(3) If α is relatively prime to A and $x^m \equiv \alpha \pmod{A}$ is solvable in $\mathcal{O}_K$, then $\left(\frac{\alpha}{A}\right)_m = 1$.

Proof. All three properties follow from definition. □

The multiplicativity properties will be particularly useful, since it would mean that for statements concerning general ideals, we only need to prove them for prime ideals, and the general case will follow. One point to note is that the converse of (3) is not necessarily true; to determine whether α is an mth power modulo A, it is necessary to decompose A into prime ideals.

As before, an integral part of the proof of the reciprocity law involves decomposing a Gauss sum into primes, and our case the primes lying over the Gauss sum will be transitive and hence can be described in terms of a single prime and automorphisms in $G = G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. It is therefore necessary for us to consider how these automorphisms will behave with respect to $\left(\frac{\alpha}{A}\right)_m$. For $\sigma \in G$ and $\alpha \in \mathbb{Q}(\zeta_m)$, it will be convenient for us to use the exponential notation and write α^σ instead of $\sigma(\alpha)$, which we will do for the rest of the paper.

Proposition 6.6. *Let $A \subset \mathcal{O}_K$ be an ideal prime to m, and let $\sigma \in G$. Then*

$$\left(\frac{\alpha}{A}\right)_m = \left(\frac{\alpha^\sigma}{A^\sigma}\right)_m.$$

Proof. It is enough for us to prove the proposition for the prime ideal $A = P$, as the general case will follow from multiplicativity. By definition

$$\alpha^{\frac{NP-1}{m}} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P},$$

so applying σ gives us

$$(\alpha^\sigma)^{\frac{NP-1}{m}} \equiv \left(\frac{\alpha}{P}\right)_m^\sigma \pmod{P^\sigma}.$$

Since P is prime to m, it follows that P^σ is also prime to m. We also know $NP = NP^\sigma$, so $\left(\frac{\alpha^\sigma}{P^\sigma}\right)_m = \left(\frac{\alpha}{P}\right)_m^\sigma$. □

Similar to the cubic and biquadratic cases, we will state reciprocity in terms of *primary* elements:

Definition 6.7. Let $m = l$ be an odd prime. A nonzero element $\alpha \in \mathcal{O}_K$ is *primary* if it is not a unit, is relatively prime to l, and is congruent to an integer modulo $(1-\zeta_l)^2$.

Proposition 6.8. *Let $\alpha \in \mathcal{O}_K$, where α is relatively prime to l. Then there exists an integer c unique modulo l such that $\zeta_l^c \alpha$ is primary.*

Proof. Let $\lambda = 1 - \zeta_l$. It can be shown that $\lambda^{l-1} = l$ (see Section 13.2, Proposition 13.2.7 of Ireland and Rosen [3]), thus from Proposition 2.14 it follows that (λ) is a prime ideal of inertial degree 1, so there exists an $a \in \mathbb{Z}$ such that $\alpha \equiv a \pmod{\lambda}$. Then $(\alpha - a)/\lambda \in \mathcal{O}_K$, so there exists a $b \in \mathbb{Z}$ such that $(\alpha - a)/\lambda \equiv b \pmod{\lambda^2}$, thus $\alpha \equiv a + b\lambda \pmod{\lambda^2}$. Since $\zeta_l = 1 - \lambda$, we have $\zeta_l^c \equiv 1 - c\lambda \pmod{\lambda^2}$ and thus $\zeta_l^c \alpha \equiv a + (b - ac)\lambda \pmod{\lambda^2}$. By assumption $l \nmid \alpha$, so $l \nmid a$. Then we can choose a unique c modulo l such that $ac \equiv b \pmod{l}$, so $\zeta_l^c \alpha \equiv a \pmod{\lambda^2}$ and thus $\zeta_l^c \alpha$ is primary. □

This definition of primary is slightly weaker than the ones in the cubic and biquadratic case, since we only have uniqueness up to multiplication by roots of unity, but for our purposes this will suffice.

We can now state the reciprocity law.

Theorem 6.9 (Eisenstein Reciprocity)**.** *Let $l, a \in \mathbb{Z}$ be such that l is an odd prime and $(l, a) = 1$, and let $\alpha \in \mathcal{O}_K$ be a primary element such that a and α are relatively prime. Then*

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

The remainder of this section will be dedicated to a proof of this theorem. Some results we present below will hold in $\mathbb{Z}[\zeta_m]$ for an arbitrary m while others hold only if $m = l$, where l is an odd prime, and we will use m or l accordingly.

We begin with a discussion of the Stickelberger relation, a result which provides a prime decomposition for certain powers of Gauss sums. We have seen the utility of analogous statements in the cubic and biquadratic cases in Corollary 4.9 and Proposition 5.9.

Let F be a finite field with $q = p^f$ elements, χ a multiplicative character of order m, and ψ a nontrivial additive character. Then χ is an mth root of unity while ψ is a pth root of unity since p is the characteristic of F, so $g(\chi, \psi) = \sum_{t \in F} \chi(t)\psi(t) \subset \mathbb{Q}[\zeta_m, \zeta_p]$. It will be convenient for us to specify χ and ψ.

Let $P \subset \mathcal{O}_K$ be a prime ideal such that $m \notin P$, and with this define $\chi_P(t) = \left(\frac{t}{P}\right)_m^{-1}$. Let $p \in \mathbb{Z}$ be the unique prime under P, so that $NP = q = p^f$, where f is the order of p modulo m by Proposition 2.22. Let $F = \mathcal{O}_K/P$. Now let $\psi(t) = \zeta_p^{tr(t)}$, where $tr : F \longrightarrow \mathbb{F}_p$ is defined as $tr(t) = t + t^p + \ldots + t^{p^{f-1}}$. Define $g(P) = g(\chi_P, \psi)$ and $\Phi(P) = g(P)^m$.

We will formulate the Stickelberger relation using "symbolic powers." For a Galois extension K over $\mathbb{Q}$ with Galois group $G = G(K/\mathbb{Q})$, define $\mathbb{Z}[G]$ to be the set of formal expressions $\sum_{\sigma \in G} a(\sigma)\sigma$ with coefficients $a(\sigma) \in \mathbb{Z}$. For an ideal $A \subset K$, define

$$A^{\sum a(\sigma)\sigma} \prod_{\sigma} (A^{\sigma})^{a(\sigma)}.$$

For the remainder of the paper, let σ_t be the automorphism defined as $\sigma_t(x) = xt$, where $x \in \mathbb{Q}[\zeta_m]/\mathbb{Q}$ and t is a fixed integer such that $(t, m) = 1$.

Theorem 6.10 (The Stickelberger Relation)**.** *Let $P \subset \mathcal{O}_K$ be a prime ideal not containing m. Then*

$$(\Phi(P)) = P^{\sum t \sigma_t^{-1}},$$

where the sum is over all $1 \leq t < m$ *such that* $(t, m) = 1$.

Proof. See Section 14.4, Theorem 2 of Ireland and Rosen [3]. □

As an example, when $m = 3$, we proved using Jacobi sums in Corollary 4.9 that $g(P)^3 = \Phi(P) = \pi\overline{\pi}^2$. If $\sigma \in G(\mathbb{Q}[\zeta_3]/\mathbb{Q})$ is the nontrivial automorphism, then $\Phi(P) = \pi^{1+2\sigma}$ since $\sigma = \sigma^{-1}$. The prime factorization of $g(P)^3$ played a vital role in the proof of cubic reciprocity, and the generalized result will be equally important here. For simplicity, let $\gamma = \sum t\sigma_t^{-1}$ for $1 \leq t < m$ and $(t, m) = 1$.

Since we will work with ideals that are not prime, it is necessary to extend the definition of Φ.

Definition 6.11. Let $A \subset \mathcal{O}_K$ be an ideal prime to m with prime decomposition $A = P_1 \dots P_n$. Define

$$\Phi(A) = \Phi(P_1)\Phi(P_2)\dots\Phi(P_n).$$

It is clear by definition that Φ is multiplicative. For simplicity we will write $\Phi((\alpha))$ as $\Phi(\alpha)$.

For the first step of the proof, we will take a similar approach as in cubic and biquadratic reciprocity by computing a power of $g(P)$ in two different ways.

Proposition 6.12. *Let* $P, P' \subset \mathcal{O}_K$ *be prime ideals relatively prime to* m *such that* NP *and* NP' *are relatively prime. Then*

$$\left(\frac{\Phi(P)}{P'}\right)_m = \left(\frac{NP'}{P}\right)_m.$$

Proof. Let $q' = p'^{f'} = NP'$. By Proposition 2.22, it follows that $q' \equiv 1 \pmod{m}$. We will compute $g(P)^{q'-1}$ in two ways. First,

$$\begin{aligned} g(P)^{q'} &\equiv \sum_{t \in \mathbb{F}_{q'}} \chi_P(t)^{q'}\psi(t)^{q'} \pmod{p'} \\ &\equiv \sum_{t \in \mathbb{F}_{q'}} \chi_P(t)\psi(q't) \pmod{p'} \\ &\equiv \left(\frac{q'}{P}\right)_m g(P) \pmod{p'}. \end{aligned}$$

Next,

$$g(P')^{q'-1} = \Phi(P)^{\frac{q'-1}{m}} \equiv \left(\frac{\Phi(P)}{P'}\right) \pmod{P'},$$

so it follows that $\left(\frac{\Phi(P)}{P'}\right)_m = \left(\frac{NP'}{P}\right)_m$. □

Corollary 6.13. *Let* $A, P \in \mathcal{O}_K$ *be such that* $A = (\alpha)$ *is principal and relatively prime to* m, P *is a prime ideal, and* NA *and* NP *are relatively prime. Then*

$$\left(\frac{\epsilon(\alpha)}{P}\right)_m \left(\frac{\alpha}{NP}\right)_m = \left(\frac{NP}{\alpha}\right)_m.$$

Proof. From Stickelberger's relation and using multiplicativity, it follows that $(\Phi(\alpha)) = (\alpha)^\gamma = (\alpha^\gamma)$, and thus

$$\left(\frac{\Phi(\alpha)}{P}\right)_m = \left(\frac{\epsilon(\alpha)}{P}\right)_m \left(\frac{\alpha^\gamma}{P}\right)_m,$$

where $\epsilon(\alpha)$ is a unit in $\mathcal{O}_K$. We have

$$\left(\frac{\alpha^{t\sigma_t^{-1}}}{P}\right)_m = \left(\frac{\alpha^{\sigma_t^{-1}}}{P}\right)_m^t = \left(\frac{\alpha^{\sigma_t^{-1}}}{P}\right)_m^{\sigma_t} = \left(\frac{\alpha}{P^{\sigma^t}}\right)_m,$$

so

$$\left(\frac{\alpha^\gamma}{P}\right)_m = \prod_t \left(\frac{\alpha^{t\sigma_t^{-1}}}{P}\right)_m = \prod_t \left(\frac{\alpha}{P^{\sigma_t}}\right)_m = \left(\frac{\alpha}{NP}\right)_m,$$

where the product is over $1 \le t < m$ for $(t, m) = 1$. Decomposing (α) into primes and use multiplicativity gives us $\left(\frac{NP}{\alpha}\right)_m = \left(\frac{\Phi(\alpha)}{P}\right)_m$ by Proposition 6.12, and the result follows. □

Notice that for $m = l$ an odd prime, we would be done if $\left(\frac{\epsilon(\alpha)}{P}\right)_l = 1$ for α primary, and the argument proceeds as follows: Let $p \in \mathbb{Z}$ be a prime such that $(p, l) = 1$ and p is relatively prime to α in $\mathcal{O}_K$. Let $P \subset \mathcal{O}_K$ be a prime ideal containing p. Then $NP = p^f$ and

$$\left(\frac{\alpha}{p}\right)_l = \left(\frac{p}{\alpha}\right)_l^f.$$

From Proposition 2.22 it follows that $f|(l-1)$, thus $(f, l) = 1$ and so $\left(\frac{\alpha}{p}\right)_l = \left(\frac{p}{\alpha}\right)_l$. By multiplicativity, for any $a \in \mathbb{Z}$ relatively prime to l and α, we have $\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l$. To show $\left(\frac{\epsilon(\alpha)}{P}\right)_l = 1$, we will begin by determining $\epsilon(\alpha)$. We first need two results concerning roots of unity and another concerning automorphisms:

Lemma 6.14. *The only roots of unity in $\mathbb{Q}[\zeta_m]$ are $\pm\zeta_m^i$ for $1 \le i < m$.*

Lemma 6.15. *Let $K/\mathbb{Q}$ be a number field, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the $n = [K : \mathbb{Q}]$ be the isomorphisms of K into $\mathbb{Q}$. If $\alpha \in K$ satisfies $|\alpha^{\sigma_i}| \le 1$ for $1 \le i \le n$, then α is a root of unity.*

The proofs to both lemmas can be found in Section 14.5 of Ireland and Rosen [3].

Lemma 6.16. *Let $A \subset \mathcal{O}_K$ be an ideal relatively prime to m, and let σ be an automorphism of $\mathbb{Q}[\zeta_m]/\mathbb{Q}$. Then $\Phi(A)^\sigma = \Phi(A^\sigma)$.*

Proof. It is enough to prove the result for $A = P$ a prime ideal, as the general case follows from multiplicativity.

Let $\overline{\sigma}$ be an automorphism of $\mathbb{Q}[\zeta_m, \zeta_p]/\mathbb{Q}$ that restricts to σ on $\mathbb{Q}[\zeta_m]$ and the identity on $\mathbb{Q}[\zeta_p]$. It follows from Proposition 6.6 that

$$g(P)^{\overline{\sigma}} = \sum_{t \in \mathbb{F}_{NP}} \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m^{-1} \zeta_p^{tr(\overline{\alpha})},$$

since $tr(\overline{\alpha}^\sigma) = tr(\overline{\alpha})$ as $tr(\overline{\alpha}) \in \mathbb{F}_p$. Thus $g(P)^{\overline{\sigma}} = g(P^\sigma)$, and raising both sides to the mth power gives our result. □

Proposition 6.17. *Let $\alpha \in \mathcal{O}_K$, where α is relatively prime to m. Then $\Phi(\alpha) = \epsilon(\alpha)\alpha^\gamma$, where $\epsilon(\alpha) = \pm\zeta_m^i$ for some i.*

Proof. We first need three results:

(1) $|\Phi(\alpha)|^2 = (N(\alpha))^m$.
(2) $|\alpha^\gamma|^2 = |N\alpha|^m$.

(3) $N(\alpha) = |N\alpha|$.

For (1), it is enough to show the identity for a prime ideal P by multiplicativity. An argument similar to the proof of Proposition 3.4 shows that $|g(P)|^2 = q$, so $|\Phi(P)|^2 = |g(P)|^{2m} = (NP)^m$ and the result follows.

For (2), we have

$$|\alpha^\gamma|^2 = \alpha^\gamma \alpha^{\gamma\sigma_{-1}} = \alpha^{\gamma(1+\sigma_{-1})}$$

since σ_{-1} acts as complex conjugation on $\mathbb{Q}[\zeta_m]$. We know $\sigma_{-1}\gamma = \sigma_{-1}\sum t\sigma_t^{-1} = \sum t\sigma_{-t}^{-1}$, and we can rewrite γ as $\gamma = \sum(m-t)\sigma_{-t}^{-1}$, so

$$(1+\sigma_{-1})\gamma = \sum t\sigma_t^{-1} + \sigma_{-1}\sum t\sigma_t^{-1} = m\sum \sigma_t^{-1},$$

and the result follows since $N\alpha = \alpha^{\sum \sigma_t^{-1}}$. To show (3), it follows from Proposition 6.2 that for a principal ideal (α)

$$(N((\alpha))) = \Pi\sigma((\alpha)) = \Pi(\alpha^\sigma) = (\Pi(\alpha^\sigma)) = (N(\alpha)).$$

From Proposition 6.2 and Definition 2.4, it follows that $N((\alpha))$ and $N(\alpha)$ are fixed under automorphisms of $\mathbb{Q}[\zeta_m]$ over $\mathbb{Q}$, so $N((\alpha)), N(\alpha) \in \mathbb{Q}$ and thus $N(\alpha) = |N(\alpha)|$.

Putting together $(1), (2)$, and (3) gives us that $|\epsilon(\alpha)| = 1$. A similar argument will show that $|\epsilon(\alpha^\sigma)| = 1$ for any $\sigma \in G(\mathbb{Q}[\zeta_m]/\mathbb{Q})$, and it follows from Lemma 6.16 that $|\epsilon(\alpha)^\sigma| = 1$. Thus by Lemma 6.15 $\epsilon(\alpha)$ must be a root of unity, and by Lemma 6.14, we have $\epsilon(\alpha) = \pm\zeta_m^i$. □

Lemma 6.18. *If $A \subset \mathcal{O}_K$ is an ideal prime to l then $\Phi(A) \equiv \pm 1 \pmod{l}$.*

Proof. It is enough to show that $\Phi(P) \equiv -1 \pmod{l}$ for a prime ideal $P \subset \mathcal{O}_K$ relatively prime to l. Let $q = p^f = NP$, where p is an odd prime. We have:

$$\begin{aligned}\Phi(P) = g(P)^l &\equiv \sum_{t \in \mathbb{F}_q} \chi_P(t)^l \psi(t)^l \pmod{l} \\ &\equiv \sum_{t \in \mathbb{F}_q, t \neq 0} \psi(lt) \equiv -1 \pmod{l}.\end{aligned}$$

□

The next proposition is where the assumption that α is primary becomes important.

Proposition 6.19. *If $\alpha \in \mathcal{O}_K$ is primary, then $\epsilon(\alpha) = \pm 1$.*

Proof. It follows from Lemma 6.18 that $(\alpha)^\gamma \equiv \pm 1 \pmod{l}$. Since α is primary, we have $\alpha \equiv x \pmod{(1-\zeta_l)^2}$ and

$$\alpha^\gamma \equiv x^\gamma \equiv x^{1+2+\ldots+(l-1)} \pmod{(1-\zeta_l)^2}.$$

Since $x^{\frac{l-1}{2}} \equiv \pm 1 \pmod{l}$, we get

$$\alpha^\gamma \equiv (\pm 1)^l \equiv \pm 1 \pmod{(1-\zeta_l)^2},$$

so $\epsilon(\alpha) \equiv \pm 1 \pmod{(1-\zeta_l)^2}$. By Proposition 6.17, we know $\epsilon(\alpha) = \pm\zeta_l^i$. By the uniqueness criterion in Proposition 6.8, it follows that $\epsilon(\alpha) = \pm 1$. □

Thus if α is primary, we have

$$\left(\frac{\epsilon(\alpha)}{B}\right)_l = \left(\frac{\pm 1}{B}\right)_l = \left(\frac{\pm 1}{B}\right)_l^l$$

since l is odd, thus $\left(\frac{\epsilon(\alpha)}{B}\right)_l = 1$, which completes the proof.

The discussion of reciprocity laws does not end here. In fact, much of the results presented in this paper are consequences of Artin's reciprocity law, a central result in class field theory that, in simplistic terms, shows that the power residue symbol $\left(\frac{\alpha}{P}\right)_m$ only depends on the residue class of α modulo some multiple of P. An introduction to this topic is presented in Cox [2].

Acknowledgments

I would like to thank my mentors Eric Chen and Wei Yao for their general guidance, patience and thoughtfulness in answering my questions, recommendations of resources, and feedback for this paper. I would also like to thank Peter May for his efforts in organizing this REU program.

References

[1] Michael Artin, *Algebra*, Pearson, Second edition, 2010.

[2] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, Inc., 1989.

[3] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, Inc., New York, NY, Second edition, 1990.

[4] Franz Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein.* Springer-Verlag, Inc., Berlin, 2000.

[5] Daniel A. Marcus. *Number Fields.* Springer International Publishing AG, New York, NY, Second edition, 2018.