Quadratic & Cubic Reciprocity Laws

Additi Pandey
02119403

Supervisor: Jack Sempliner
September 2022

Abstract

In this thesis, we provide proofs to the law of quadratic and cubic reciprocity using Gauss sums and Artin reciprocity. As an application of our work in this thesis, we study the primes of the forms $x^2 + 5y^2$, $x^2 + 26y^2$ and $x^2 + 27y^2$. We also aim to build the intuition to tackle the problem of finding solutions to the primes of the form $x^2 + ny^2$ for all $n > 0$. Our work serves as a preliminary set-up to study Artin reciprocity and search for a general reciprocity law.

Contents

1 Introduction

The genealogy of the law of quadratic reciprocity dates back to Fermat and Euler when former proposed conjectures related to primes to be written as sum of two squares, for instance,

$p = x^2 + y^2 \iff p \equiv 1 \pmod 4$, and latter proved them using descent[1] and reciprocity[2] steps. Ever since then, the law of quadratic reciprocity has been an indispensable tool in algebraic number theory. From finding solutions to the Diophantine equation $x^2 - dy^2 = p$, where d is an integer and p is a prime, by reducing them modulo p, a prime[3] to its usage in public-key cryptography[4], it is one of the most fundamental theorems that lies in the realms of algebraic number theory. A detailed historical account of the law of quadratic reciprocity can be found in [16, 17].

There is a significant corpus of literature on the proof of the law of quadratic reciprocity. The most recent proof was published this year based on Gauss's Lemma and Hermite's identity by Lemmermeyer [24]. A collection of all the proofs can be found in [23]. In this thesis, however, we will prove the law of quadratic reciprocity using Gauss sums[5] as it provides a general framework to prove the higher reciprocity laws (see [9]). Moreover, there are two great ways to motivate the Gauss sums:

- Since these are the discrete Fourier transform of a multiplicative character χ at a, proving the law of quadratic reciprocity or evaluating the sign of the Gauss sums becomes a lot more intuitive (see [4]).
- A more Galois theoretic approach, which we will cover in thesis, where the Gauss sums generate a unique quadratic subextension which is the fixed field of a unique subgroup of index 2 (see section 4.5).

Naturally, once we know how to prove the law of quadratic reciprocity, we want to generalise it to the higher reciprocity laws. We use the Gauss sums and prove the law of cubic reciprocity with the argument that we used to prove the law of quadratic reciprocity. This proof was given by Eisenstein [9, p. 108]. The law of bi-quadratic reciprocity also follows the same outline, however, we will restrict ourselves to the quadratic and cubic reciprocity laws.

In the second part of this thesis, we aim to provide a thorough explanation of the Gauss sums and our reciprocity laws using Galois theory. To do this, we study Artin reciprocity, which can be stated as follows:

Theorem 1.1 (Artin Reciprocity Theorem)**.** *[7, p. 62] Let L/K be an abelian extension, and $\mathfrak{f}$ be the conductor[6] of the extension divisible by all primes, finite or infinite, that ramify in L. Let $I_K^{\mathfrak{f}}$ be the set of all fractional ideals[7] of K, relatively prime to $\mathfrak{f}$ and $P_K^{\mathfrak{f}}$ be the set of all principal fractional ideals[8] of K, relatively prime to $\mathfrak{f}$. Then:*

- *The Artin map $\phi_{L/K} : I_K^{\mathfrak{f}} \longrightarrow Gal(L/K)$ is surjective.*

[1] In this case, the descent step corresponds to the following: Let p be an odd prime, $p|(x^2 + y^2)$ for $x, y \in \mathbb{Z}$ then p can be represented by $x^2 + y^2$

[2] In this case, the reciprocity step is: Let p be an odd prime, $p \equiv 1 \pmod 4$ then $p|x^2 + y^2$ for x, y integers.

[3] reduction modulo p on $x^2 - dy^2 = p$ gives a necessary condition that $\left(\frac{d}{p}\right) = 1$.

[4] To decrypt a message we find quadratic residues modulo N, where $N = pq$ and p, q are primes that encrypt a message in their product.

[5] Gauss sum is defined as $\sum_{t=0}^{p-1} \chi(t)\zeta^{at}$, where a an integer.

[6] The smallest n such that the quadratic number field $K \subset \mathbb{Q}(\zeta_n)$ [12].

[7] A fractional ideal of an integral domain A is a non-zero ideal I of A rescaled by a non-zero element $\alpha \in K$ such that $\alpha I \subset A$ [11].

[8] A principal fractional ideal generated by α, is an ideal αA, where $\alpha \in K^\times$ and A, K are same as above.

- $P_K^{\mathfrak{f}} \subset ker(\phi_{L/K})$ *so there is an explicit isomorphism* $\frac{Cl_K^{\mathfrak{f}}}{ker(\phi_{L/K})} \cong Gal(L/K)$.

The proof of Artin reciprocity requires extensive class field theory and will not be covered in this thesis. However, we direct our readers to [12, 14, 18] for an intuitive treatment on the subject.

Using Artin reciprocity and the Kronecker Weber theorem[9] we will prove the law of quadratic reciprocity. The outline of the proof is as follows:

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_q)$. Let p be a prime such that it is unramified in the abelian extension L/K, then p splits in the maximal quadratic subextension of $L \iff \phi_{L/K} = 1 \iff p$ belongs to the subgroup of index 2 in $Gal(L/K)$ [7, 12, 15].

We will then apply the same argument to prove the law of cubic reciprocity. This tells us that Artin reciprocity establishes a one-to-one correspondence between some prime numbers and the abelian field extensions L/K[19].

Artin reciprocity plays a key role in class field theory and in generalising the reciprocity law. Insights into this can be found in Langlands' conjectures [20], which is a grand web of conjectures unifying number theory with other areas of mathematics[21].

As an application of our work done in the first two section, we devote the last section to study the primes represented by $x^2 + 5y^2$, $x^2 + 27y^2$ and $x^2 + 26y^2$ and outline directions of further advancement (see [8]).

2 Preliminaries

In this section, we will provide the necessary background to some concepts that are used in this thesis. We suggest our readers to [8, 29, 35] for a broader treatment of these concepts.

Number Field:

A number field K is a field extension of $\mathbb{Q}$ such that the degree of K over $\mathbb{Q}$ is finite.

The Ring of Integers:

The set of algebraic integers in a number field K forms a ring called the ring of integers of K. The ring of integers corresponding to a number field K is denoted by $\mathcal{O}_K$. Some algebraic properties of $\mathcal{O}_K$ to keep in mind:

- If I is a non-zero ideal of $\mathcal{O}_K$ then $\mathcal{O}_K/I$ is finite[10].
- The ring of integers $\mathcal{O}_K$ is a Dedekind domain[11].
- A non-zero prime ideal $I \subset \mathcal{O}_K$ is a maximal ideal[12].

Quadratic Field and Quadratic Ring:

[9] A consequence of Artin reciprocity- states that all abelian extensions are contained in cyclotomic extensions.

[10] see 2

[11] An integral domain is a Dedekind domain if it is integrally closed, Noetherian and every non-zero prime ideal is maximal.

[12] If I is not maximal then, $\exists I_1$ such that $I \subset I_1 \subset \mathcal{O}_K$. If I_1 is not maximal then we repeat this process. Since, $\mathcal{O}_K$ is Noetherian, therefore, this ascending chain terminates, proving that there is a maximal ideal.

Let d be the discriminant of the quadratic number field $\mathbb{Q}(\sqrt{d})$, and $\mathcal{O}_K$ be the quadratic ring given by:

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\} \text{ if } d \not\equiv 1 \pmod 4$$

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2} \,|a, b \in \mathbb{Z}\right\} \text{ if } d \equiv 1 \pmod 4$$

Fractional Ideals

- Let K be a number field. A fractional ideal of $\mathcal{O}_K$ is an additive subgroup I of K such that $\alpha I \subset \mathcal{O}_K$ is a non-zero ideal for some $\alpha \in K^\times$.
- A principal fractional ideal is an ideal $\alpha\mathcal{O}_K$ for $\alpha \in K^\times$, where K is a number field.
- Integral ideals are the fractional ideals with $\alpha = 1$.
- If I, J are fractional ideals then $IJ = \{\sum_{i\in I, j\in J} ij\} \subset K$ is a fractional ideal.
- Let K be a quadratic field and $\mathcal{O}_K$ be the quadratic ring, and let I be a non-zero ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/I$ is finite since if $0 \neq \alpha \in I$ be an element of I then $N(\alpha) = \alpha\alpha' \in I$. This shows that $\mathcal{O}_K/I$ is finite as $\mathcal{O}_K/(N(\alpha))$ is finite[13].

  From this point till the end of the section, we assume K to be the quadratic number field.

- The norm of a fractional ideal I of $\mathcal{O}_K$ is given by

  $$\frac{[\mathcal{O}_K : kI]}{k^2}$$

  where $k \in \mathbb{Z}$ such that $kI \subset \mathcal{O}_K$ is a non-zero ideal. Here, the power of k is 2 in the denominator because $[K : \mathbb{Q}] = 2$.
- Let $\alpha \in K^\times$, then $N(\alpha\mathcal{O}_K) = [\mathcal{O}_K : \alpha\mathcal{O}_K]$. Since $\mathcal{O}_K$ is a free abelian group of rank 2, therefore, $[\mathcal{O}_K : \alpha\mathcal{O}_K] = |\det(m_\alpha)|$, where m_α is the $\mathbb{Z}$ linear map that takes $x \mapsto \alpha x$. Moreover, the trace $Tr(\alpha) = tr(m_\alpha)$.
- Let $d \equiv 0, 1 \pmod 4$ be the discriminant of K. Let $a_1, a_2 \in K$ be linearly independent over $\mathbb{Q}$. If $[a_1, a_2] = A \cdot [1, \sqrt{d}]$, where $A = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$ with $\det(A) > 0$, then $[a_1, a_2]$ form a positive basis of K.

Binary Quadratic Forms

- A binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is a degree 2 homogenous polynomial in two variables with integer coefficients.
- A binary quadratic form $f(x, y)$ is primitive if $gcd(a, b, c) = 1$.
- Discriminant of $f(x, y) = b^2 - 4ac \equiv 0, 1 \pmod 4$.

[13] Viewing $(N(\alpha))$ as a subgroup of a free abelian group of rank 2, $(N(\alpha))$ also has rank 2. Hence, $[\mathcal{O}_K : (N(\alpha))]$ is finite. For details, we refer our readers to [11, pp. 58–59]

- Corresponding to $d \equiv 0, 1 \pmod 4$, the discriminant of a quadratic number field K, $\exists f(x, y)$ with same discriminant such that

$$x^2 - \frac{d}{4}y^2 \text{ if } d \equiv 0 \pmod 4$$

$$x^2 + xy + \frac{1-d}{4}y^2 \text{ if } d \equiv 1 \pmod 4$$

- We say $f(x, y)$ represents n if $f(x, y) = n$ has integral solutions.

- If $f(x, y) = n$ has integral solutions such that $(x, y) = 1$, then $f(x, y)$ properly represents n.

- Let $Q(d)$ be the set of binary quadratic forms of discriminant d. We define an action of $GL(2, \mathbb{Z})$ on $Q(d)$ by a linear change of variables as follows:

  Let $f(x, y) = ax^2 + bxy + cy^2$, then $f(x, y) = (x, y) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$.

  If $A = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in GL_2(\mathbb{Z})$ for integers p, q, r, s then,

  $f_{|A} = (x, y)A^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix}$.

- Two binary forms $\exists\ A \in SL(2, \mathbb{Z})$, such that $f(x, y)$ and $g(x, y)$ are equivalent if $f_{|A} = g$.

- A positive definite binary quadratic form $f = [a, b, c]$ is said to be *reduced* if $|b| \leq a \leq c$ and, if $a = c$ or $|b| = a$, $\implies b \geq 0$.

  Theorem 2.1 ([8, pp. 27–28])**.** *Every primitive positive definite form is equivalent to a unique reduced form.*

  Proof of Theorem 2.1. To show that any primitive positive definite form is equivalent to a reduced form, we will first show that every primitive positive definite quadratic form of discriminant d is properly equivalent to a reduced form and we shall then show that there is a unique reduced form, corresponding to an equivalence class.

  Let us pick up a form $f(x, y) = ax^2 + bxy + cy^2$ from the equivalence class of positive definite forms f such that $|b|$ is minimal. Suppose $|b| > a$. To make it a reduce form, we need $|b| \leq a$. Consider $\sigma \in SL_2(\mathbb{Z})$ such that

$$\sigma = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$

  Let us define $f_{|\sigma} = (x, y)\ \sigma^T \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \sigma \begin{pmatrix} x \\ y \end{pmatrix}$

  So, we get $f_{|\sigma} = ax^2 + (2am + b)xy + c'y^2$, where $c' = am^2 + mb + c$. Since, $a < |b|$ in $f(x, y)$, we can choose $m \in \mathbb{Z}$ such that $|(2am + b)| < |b|$. This contradicts the fact that

$|b|$ is minimal. So, we have $|b| \leq a$. By symmetry, this implies that $|b| \leq c$. Consider $\tau = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$. If $a > c$ then we apply τ. This interchanges a and c. This form is reduced except for when $b < 0$. In that case and $a = -b$ or $a = c$. In the former case, we change basis of f to σ with $m = 1$ such that $ax^2 - axy + cy^2$ changes to $ax^2 + axy + cy^2$. In the latter case, we change basis of f to that of τ and that gives us $ax^2 + bxy + ay^2 \longrightarrow ax^2 - bxy + ay^2$.

We shall now show that corresponding to an equivalence class, there is a unique reduced form. Let $a'x^2 + b'xy + c'y^2$ be a form equivalent to $f(x, y) = ax^2 + bxy + cy^2$. Let $\kappa = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ such that $p, r \neq 0$. Then $f_{|\kappa} = a'x^2 + b'xy + c'y^2$. Comparing coefficients of x^2, we get: $a' = p^2a + prb + rc^2$. We check when a' $geqa, a' \leq a, a = a'$ depending on whether $p > r$ or $r > p, p = 0$ or $r = 0$. If $a'x^2 + b'xy + c'y^2$ is equivalent to $f(x, y)$ then $a' = a$, which gives us $r = 0$ and $p = \pm 1$, finally leading to $a'x^2 + b'xy + c'y^2 = f(x, y)$. □

- Relationship between a discriminant D and an integer represented by a binary quadratic form of discriminant D is given by:

  Theorem 2.2 ([3, p. 26])**.** *Let $d \equiv 0, 1 \pmod 4$ and m be odd integer that does not divide d, then d is a quadratic residue modulo $m \iff$ there exists a primitive quadratic form $f(x, y) = ax^2 + bxy + cy^2$ of discriminant d and integers x, y such that m is properly represented by $f(x, y)$.*

  Proof of Theorem 2.2. [[3, p. 26]] Let $m = f(x, y)$ such that $f(x, y) = ax^2 + bxy + cy^2$. Changing basis to that of A, where $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$ and p, q, r, s are integers such that $ps - qr = 1$. The resulting form $f_{|A} = (x, y)A^T A \begin{pmatrix} x \\ y \end{pmatrix}$ we get that $f_{|A} = mx^2 + (2apq + bps + bqr + 2crs)xy + cy^2 = mx^2 + bxy + cy^2$ for $b = (2apq + bps + bqr + 2crs)$. Now, discriminant d of $f_{|A} = b^2 - 4mc \implies d \equiv b^2 \pmod m$. Conversely, suppose that d is a quadratic residue modulo m. Then $d = b^2 - 4mc \implies d$ is the discriminant of the quadratic form $mx^2 + bxy + cy^2$. If $x = 1, y = 0$ then it properly represents m. □

Correspondence between Oriented Ideals and Quadratic Forms

Let I_K, P_K denote the set of fractional ideals and principal fractional ideals of $\mathcal{O}_K$, respectively. Let $[a_1, a_2]$ be the positive basis of I as $\mathbb{Z}$ module, then $(I, (a_1, a_2))$ are called oriented fractional ideals, denoted by I_K^+.

Definition 2.3 ([11, p. 67])**.** Let $(I, (a_1, a_2))$ be an oriented fractional ideal of $\mathcal{O}_K$. Then the binary quadratic form attached to it is given by:

$$f_{I,(a_1,a_2)}(x, y) = \frac{N(a_1x + a_2y)}{N(I)} \in \mathbb{Z}[x, y]$$

Let $K^{\times}_{N>0}$ denote the multiplicative group $\{\beta \in K^{\times} | N(\beta) > 0\}$. The action of this β maps the oriented fractional ideal $(I, (a_1, a_2)) \in I_K^+$ to $(\beta I, (\beta a_1, \beta a_2)) \in I_K^+$. If $N(\beta) < 0$, then $(\beta I, (\beta a_1, -\beta a_2)) \in I_K^+$ for the oriented fractional ideal $(I, (a_1, a_2)) \in I_K^+$ and $-f_{I,(a_1,a_2)}(X, -Y) = f_{\beta I,(\beta a_1,-\beta a_2)}(X, Y)$, where $f_{I,(a_1,a_2)}$ is the binary quadratic form corresponding to the oriented ideal$(I, (a_1, a_2))$. However, note that β corresponding to $N(\beta) < 0$ does not belong to $K^{\times}_{N>0}$.

Let us now prove the theorem that prove the correspondence between ideals in $\mathcal{O}_K$, where K is a quadratic number field of discriminant d, and the primitive quadratic forms of discriminant d.

Theorem 2.4 ([11, pp. 67–69])**.** *1. The map $\psi : I_K^+/SL(2,\mathbb{Z}) \longrightarrow I_K$ that sends $(I, (a_1, a_2)) \mapsto I$ is bijective.*

2. The map $\phi : K^{\times}_{N>0} \setminus I_K^+ \longrightarrow Q(d)$ that sends $(I, (a_1, a_2)) \mapsto f_{I,(a_1,a_2)}$ is bijective.

Proof of Theorem 2.4. 1. Two elements in I_K^+ that map to same element in I, differ by a change of basis transformation and these bases are such that the action of $SL_2(\mathbb{Z})$ on I_K^+ makes these bases equivalent. This shows that the map is well defined and bijective.

2. This proof requires some non-trivial work. We will first show that the map is well-defined.

   Let a_1^{-1} act on I_K^+ such that $(I, (a_1, a_2)) \mapsto (a_1^{-1}I, (1, \pm a_1^{-1}a_2))$, where the sign depends on $N(a_1^{-1})$. Let $[1, \pm a_1^{-1}a_2] = [1, \alpha]$ be a positive I basis, then I can written as $I = \mathbb{Z} \oplus \alpha\mathbb{Z}$. For convenience, we shall denote $f_{I,(a_1,a_2)}$ as f. Let us find the discriminant of $f(x, y)$. By definition 2.3, we have $f(x, y) = \frac{N(x+\alpha y)}{N(I)} = \frac{x^2+(\alpha+\alpha')xy+\alpha\alpha' y^2}{N(I)}$. Set $\alpha = a + b\frac{\sqrt{d}}{2}$. Notice that $(\alpha + \alpha')^2 - 4\alpha\alpha' = (\alpha - \alpha)^2 = db^2$.

   Choose $k \in \mathbb{Z}$ such that $k \neq 0$ and $\alpha k \in \mathcal{O}_K$. Let us find the norm of I: $N(I) = \frac{[\mathcal{O}_K : kI]}{k^2} = \frac{[\mathcal{O}_K : k(1,\alpha)]}{k^2} = \frac{|k \cdot kb|}{k^2} = |b|$.

   We have that the discriminant of f is $d_f = db^2/b^2 = d$. Hence, the map is well-defined.

   Let us now show that the map is one-to-one.

   Let $f_{I,(a_1,a_2)} = f_{J,(b_1,b_2)}$, then by definition 2.3, we have

$$\frac{N(a_1x + a_2y)}{N(I)} = \frac{N(b_1x + b_2y)}{N(J)} \tag{1}$$

   Let $(x, y) = (1, 0)$, then $N(a_1)/N(I) = N(b_1)/N(K + J)$. Set $a_2 = a_1\alpha$ and $b_2 = b_1\beta$, then by equation 1, we have that

$$N(x + \alpha y) = N(x + \beta y)$$

   Let $y = -1$, this gives us $N(x-\alpha) = N(x-\beta)$. Thus we have, $\alpha = \beta$ since $[a_1, a_2], [b_1, b_2]$ are positive basis of I, J respectively and $N(\alpha), N(\beta)$ will have same sign. This means that $[1, \alpha], [1, \beta]$ are both positive basis or negative basis. Since $[1, \alpha]$ and $[1, \alpha']$ have opposite orientation as $\sqrt{d} \mapsto -\sqrt{d}$ from $\alpha \longrightarrow \alpha'$, therefore, $\alpha = \beta \implies [a_1, a_2] = \lambda[b_1, b_2]$, where $\lambda \in K^{\times}$. Since, these are both positive basis, hence $N(\lambda) > 0$, hence

it belongs to $K^{\times}_{N>0}$. So the preimage of ϕ is $K^{\times}_{N>0}$ orbit in I_K^+, hence, $(I,(a_1,a_2)) = (\lambda J,(\lambda b_1,\lambda b_2))$.

We shall now show that the map is surjective. We will only consider the case when $d<0$ and $a>0$, since this will be the only case we will need in this thesis. In case of $d>0$, $\beta \in K^{\times}$ has norm >0 but that case can be handled by taking $-f_{I,(a_1,a_2)}(X,-Y) = f_{\beta I,(\beta a_1,-\beta a_2)}(X,Y)$, where $f_{I,(a_1,a_2)}$ is the binary quadratic form corresponding to the oriented ideal $(I,(a_1,a_2))$.

So, we shall show that corresponding to a binary quadratic form (positive definite, here), there exists a fractional ideal in I_K^+. Let $f(x,y) = ax^2+bxy+cy^2$. Let $y=1$, then ax^2+bx+c has complex roots since $d<0$. Let α be a unique root such that it has positive imaginary part. Since $a>0$, so let $\alpha = \frac{-b+\sqrt{d}}{2a}$. Notice that $\alpha \in K$. Let $\beta = a\alpha$ so we have, $\beta = \frac{-b+\sqrt{d}}{2}$. Let us take the basis of $\mathcal{O}_K = \left(1, \frac{d+\sqrt{d}}{2}\right)$. Consider $\beta = \left(\frac{-b+d}{2}\right) - \left(\frac{d+\sqrt{d}}{2}\right) \in \mathcal{O}_K$. So we have $\mathcal{O}_K = [1,\beta]$. Consider $[a,\beta]\mathcal{O}_K = [a,\beta][1,\beta] = [a,\beta,a\beta,\beta^2]$. On computing β^2, one may find that it is equal to $-ac+b\beta$. Certainly $\beta^2 \in [a,\beta]$. Observe that determinant of $[a,\beta]>0$, so the basis is positively oriented.

Let us find the quadratic form associated to $(I,(a,\beta))$ by definition 2.3, we have:

$$f_{I,(a,\beta)} = \frac{N(ax+\beta y)}{N(I)} = \frac{a^2x^2+abxy+\left(\frac{b^2-d}{4}\right)y^2}{a} = ax^2+bxy+cy^2 = f(x,y)$$

This quadratic form is primitive. We shall now let $\alpha = \beta/a$. We will use lemma 7.5 [14] in [8, pp. 135–136], to show that the fractional ideal I is proper ideal in $\mathcal{O}_K$. We shall show that $\beta[1,\alpha] \subset [1,\alpha]$, i.e. $\beta \in [1,\alpha]$ and $\beta\alpha \in [1,\alpha]$. So, we have, $\beta = x+y\alpha$, where $x,y \in \mathbb{Z}$. Notice that this holds true when $x=0, y=a$. We also need to show that $\beta\alpha \in [1,\alpha]$. Note that, $\beta\alpha = x\alpha+y\alpha^2 = x\alpha + y\left(\frac{b^2+d-2b\sqrt{d}}{4a^2}\right) = x\alpha + \frac{y}{a}(-b\alpha-c) = \frac{-cy}{a} + \left(\frac{-by}{a}+x\right)\alpha$. Since $y=a$, we have $\beta\alpha \in [1,\alpha]$. This leads us to $\{\beta \in K | \beta[1,\alpha] \subset [1,\alpha]\} = [1,a\alpha] = [1,\beta] = \mathcal{O}_K$. This implies that since $[1,\alpha]$ is a proper fractional ideal of $\mathcal{O}_K$, therefore, $I = [a,\beta] = a[1,\alpha] \subset [1,a\alpha]$. That is $a\mathbb{Z}\oplus\beta\mathbb{Z} \subset \mathcal{O}_K$.

We have therefore shown that the map ϕ is well-defined, injective and surjective. Hence, ϕ is bijective.

□

Corollary 2.5 ([11]). *The map $\phi : I_K^+ \longrightarrow Q(d)$ induces a bijection $P_K^+\backslash I_K \longrightarrow Q(d)/SL_2(\mathbb{Z})$.*

Proof. By definition of P_K^+, we have that $K^{\times}_{N>0} \setminus I_K = K^{\times}_{N>0} \setminus I_K^+/SL_2(\mathbb{Z}) = Q(d)/SL_2(\mathbb{Z})$ by theorem 2.4. □

Ideal Class Group

Let d be a fundamental discriminant, that is, the discriminant of $K = \mathbb{Q}(\sqrt{-d})$. For fundamental discriminants, $Q(d)$ is the set of primitive quadratic forms and we get: $Cl(\mathcal{O}_K) =$

[14] Let $K = \mathbb{Q}(\tau)$ be a quadratic number field and $ax^2+bxy+cy^2$ be the minimal polynomial of τ such that a,b,c are coprime. Then $[1,\tau]$ is a proper fractional ideal of $[1,a\tau]$ of K.

$Q(d)/SL_2(\mathbb{Z})$. Recall from theorem 2.4 that $Q(d)/SL_2(\mathbb{Z}) = P_K^+ \setminus I_K$. If $d < 0$, then the norm of $\alpha \in K^\times > 0$, so $P_K^+ = P_K$, hence we have, $Cl(\mathcal{O}_K) = P_K \setminus I_K$.

The composition law of fractional ideals $I \cdot J = IJ$ induces group structure on $Cl(\mathcal{O}_K) = I_K/P_K$ with identity element the class of principal fractional ideals. This group is abelian and is called the class group. The composition law of fractional ideals corresponds to the Dirichlet's composition of forms. A detailed description of this can be found in [8, 35].

The order of the class group is called the class number. It is denoted by $h(d)$ corresponding to the discriminant d of the number field K. Class number is equal to the number of classes present in the class group. The following theorem provides a way to calculate it and shows that it is finite.

Theorem 2.6 ([3, p. 29])**.** *Let $d < 0$. The number of classes of primitive positive definite forms of discriminant d is finite and equal to the number of reduced forms of discriminant d.*

Proof of Theorem 2.6. Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced form of discriminant $D < 0$, then $b^2 \leq a^2$ and $a \leq c$

Since $d < 0 \implies -d > 0$ and $-d = -b^2 + 4ac \geq 4a^2 - a^2 = 3a^2$

Hence, $a \leq \sqrt{(-d)/3}$. If d is fixed then $|b| \leq a \implies$ finite choices for a, b, c, hence, there are only finite number of reduced forms of discriminant d, so the class number $h(d)$ is finite.

Since every primitive positive definite form is properly equivalent to a reduced form[15], therefore, the number of proper equivalence classes is also finite, hence, $h(d)$ is finite and equal to the number of reduced forms of d. □

3 Reciprocity Laws before Artin

The proof of the law of quadratic reciprocity was a crowning achievement by Gauss. Later many mathematicians came up with their proofs. In this section, we prove the law of quadratic and cubic reciprocity using the Gauss sum. As mentioned earlier, the Gauss sum $g_a = \sum_t \chi(t)\zeta^{at}$, where χ is the Legendre symbol or $\left(\frac{t}{p}\right)$. We will see that the value of the Gauss sum comes to be $\pm\sqrt{\pm p}$. To find out what the sign is going to be is a difficult problem. Gauss conjectured that the value of the Gauss sum is $\sqrt{\pm p}$, however, it took him a long time to prove it. A more linear algebra-based treatment of this problem is in [4]. In this section, we use these Gauss sums along with the notion of Jacobi sums to prove the law of cubic reciprocity.

3.1 Quadratic Reciprocity

Let us start this section with the study of the quadratic residues modulo p, where p is an odd prime. Recall, the problem of solving a quadratic polynomial $f(x) \equiv 0$ modulo n, where $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, by Chinese remainder theorem, reduces to a problem of solving individual congruences $f(x) \equiv 0 \pmod{p_1}$, $f(x) \equiv 0 \pmod{p_2}$, $\dots$,$f(x) \equiv 0 \pmod{p_k}$.

So, let us consider solving the following quadratic congruence:

$$f(x) = ax^2 + bx + c \equiv 0 \pmod{p} \tag{2}$$

[15] see Theorem 2.1.

If $a \equiv 0 \pmod{p}$, then equation (2) reduces to a linear congruence which can be easily solved. So, let $a \not\equiv 0 \pmod{p}$. Similarly, if $p = 2$, then the case is trivial, so we assume p to be an odd prime.

Multiply equation (2) by $4a$, then the equation reduces to finding solutions to $(2ax+b)^2 \equiv (b^2-4ac) \pmod{p}$. Let $(2ax+b) = y$ and $b^2-ac = D$, then equation (2) becomes the problem of finding when $y^2 \equiv D \pmod{p}$ is solvable. We say that $y^2 \equiv D \pmod{p}$ is solvable $\iff D$ is a quadratic residue modulo p.

Definition 3.1. Let $p \nmid y$ be a prime, then if $\exists\ d$ such that $d^2 \equiv y$ modulo p for some d, then y is a quadratic residue modulo p, otherwise it is a quadratic non-residue modulo p.

To distinguish between the quadratic residues and quadratic non-residues, we define the Legendre symbol.

Definition 3.2. For any integer a and an odd prime p, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be a unique homomorphism $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ such that $[a]_p \mapsto \chi(a) = \left(\frac{a}{p}\right)$. It takes values as follows:

- 0 if $p|a$
- 1 if a is a quadratic residue modulo p
- -1 if a is a quadratic non-residue modulo p

The Legendre symbol is a multiplicative character[16] on $\mathbb{F}_p$. Therefore, many of its properties are the properties of these characters[17]. We shall now list some of these properties.

Proposition 3.3 ([9, p. 51])**.** *Let p be an odd prime, and a, b are integers such that $p \nmid a$ and $p \nmid b$, then:*

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

Before proving these properties, let us first draw our attention to the first property. It is called Euler's criterion and provides an easy way to calculate the Legendre symbol. Let us state it mathematically and prove it.

Proposition 3.4 (Euler's criterion)**.** *[26] Let p be an odd prime, and a is an integer such that $p \nmid a$, then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.*

Proof of Proposition 3.4. By Fermat's little theorem, $a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, so $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. If a is a quadratic residue modulo p, then $\exists\ d$ such that $a \equiv d^2 \pmod{p}$. Then, $(d^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ is true by Fermat's little theorem.

[16] A multiplicative character χ is a homomorphism $\mathbb{F}_p^\times \longrightarrow \mathbb{C}$ such that $\chi(a) \cdot \chi(b) = \chi(ab)$, where $a, b \in \mathbb{F}_p^\times$.
[17] Section 3.3 provides a list of the properties of the multiplicative characters.

If a is a quadratic non-residue modulo p, then $a = g^r$, where g is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and r is an odd integer (if r was even then a would be a residue modulo p).

Recall, if g is a generator of $\mathbb{F}_p^\times$, then every residue class in this group is a power of g and g generates the cyclic group of order $p-1$. Suppose $1 = a^{\frac{p-1}{2}} = g^{\frac{r(p-1)}{2}}$. Since, g generates the group $\mathbb{F}_p$, it has order $p-1$, so $(p-1)|\frac{r(p-1)}{2}$ but r is odd so this is not possible. Hence, $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

We have proved the first property of the Legendre symbol. Let us try to prove the other two:

Proof of Proposition 3.3.

1. We have proved this in Proposition 3.4.
2. Let us use the first property to prove this:
   We have: $ab^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}b^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$. We know that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ and $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}$, so this gives us: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
3. The proof again follows from the first property. $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

□

Corollary 3.5 ([9, pp. 51–52])**.** *There are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p.*

Proof of Corollary 3.5. By Fermat's little theorem, we know that there are $p-1$ solutions to the equation $a^{p-1} \equiv 1 \pmod{p}$, where a is an integer and p an odd prime that does not divide a. We also know that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ has $\frac{p-1}{2}$ solutions. So, there are $\frac{p-1}{2}$ quadratic residues and $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic non-residues modulo p. □

Euler's criterion tells us that given an odd prime p and an integer a coprime to p if a is a quadratic residue or a non-residue modulo p. However, given an integer a, what are the primes such that a is a quadratic residue modulo p? This question is answered by the law of quadratic reciprocity. But before we mathematically formulate the law of quadratic reciprocity, let us prove the following results.

In what follows, we will compute the value of the Legendre symbol for $a = -1, 2$ over an odd prime p.

Proposition 3.6. *The Legendre symbol for -1 over an odd prime p is given by: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, and for 2 over an odd prime p is given by: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

Proof of Proposition 3.6. The proof of the first part of the proposition is easy to prove and follows Euler's criterion by substituting $a = -1$ and the definitions stated above. Let us prove the second part [26].

Let $q = \frac{p-1}{2}$, and consider the following set of equation:

$1 = (-1)(-1)$

$2 = 2(-1)^2$

$3 = (-3)(-1)^3$

$4 = 4(-1)^4$

$\vdots$

$q = (\pm q)(-1)^q$

Multiplying these equations yields $q!$ on the LHS and some product of odd and even numbers on the RHS. Notice that the even numbers on RHS are $2(4)(6)(8)\ldots$. Since, $q = \frac{p-1}{2}$, $2q = p-1 \equiv (-1) \pmod{p}$ and $2(q-1) \equiv -3 \pmod{p}$, so we have, $2(4)(6)\ldots(-3)(-1)$. The RHS contains $(2)(4)(6)\ldots(p-1) = 2^q q!$. We have the powers of (-1) still left to be accounted for and that is $(-1)^{1+2+\ldots q} = (-1)^{\frac{(q+1)q}{2}}$. We thus have $2^q q! \equiv (-1)^{\frac{(q+1)q}{2}} q! \pmod{p}$.
$2^q \equiv (-1)^{\frac{(q+1)q}{2}} \pmod{p}$, and $\frac{(q+1)q}{2}$ is even when $p \equiv 1, 7 \pmod{9}$, and hence, $\frac{(q+1)q}{2} = \frac{p^2-1}{8}$. □

Thus far, we computed the congruence conditions for -1 and 2 to be quadratic residue modulo p, where p is an odd prime. However, what if p, q are two odd primes? If p, q are two odd primes then the law of quadratic reciprocity tells us that p is a quadratic residue modulo $q \iff q$ is a quadratic residue modulo p. Thus, there is some sort of a "reciprocal" relation established. Gauss has referred to this theorem as the "Fundamental theorem" in *Disquisitiones Arithmeticae* and gave 8 proofs of this in his lifetime.

Theorem 3.7 (The Law of Quadratic Reciprocity)**.** *Let p, q be distinct odd primes, then:*

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
- *If p, q are odd primes, then* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proof of Theorem 3.7. We have already dealt with the first two cases. Using the primitive roots of unity gives a more elegant proof of the second case. We will discuss this proof as well as the proof of the last case in the next section 3.2. □

3.2 Proof of the Law of Quadratic Reciprocity

In this section, we will introduce the quadratic Gauss sums. The Gauss sums form the crux of our argument for proving the law of quadratic reciprocity and cubic reciprocity law. The Gauss sum corresponding to some integer a is defined as $g_a = \sum_{t=0}^{p-1} \chi(t)\zeta^{at}$, where χ is a multiplicative character in $\mathbb{F}_p^\times$ which can be extended to $\mathbb{F}_p$ by defining $\chi(0) = 0$. Since the Gauss sum is a discrete Fourier transform[18] at a of the function χ, if F is a $p \times p$ matrix with its (i, j)-th entry as ζ^{ij}, then the trace of F is the Gauss sum corresponding to an integer a. A more detailed discussion of this can be found in [4, 44]. The law of quadratic reciprocity is proved by evaluating the Gauss sum at p, an odd prime, with the Legendre symbol as the multiplicative character. Let us discuss this in more detail.

[18]Let $\mathcal{F}$ be the set of functions $f : (\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathbb{C}$, then the discrete Fourier transform of f is $\hat{f}(x) = \sum_t f(t)e^{\frac{2\pi i t}{n}x}$, $\forall\, y \in (\mathbb{Z}/n\mathbb{Z})$

3.2.1 Quadratic Character of 2

The quadratic character of a prime p refers to the Legendre symbol of p over some other odd prime. Recall from section 3.1, where we found the quadratic character of 2, which was $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

We shall now prove the same result using the 8-th root of unity.

Let ζ be the primitive eighth root of unity, then $\zeta^8 = 1$. We have, $\zeta^4 = -1$, and $\zeta^2 = -\zeta^{-2}$. Taking square roots on both sides of $\zeta^4 = -1$, gives us $\zeta^2 = \pm i$. If $\zeta^2 = i$, then $\zeta^{-2} = -i$. So we have, $\zeta^2 + \zeta^{-2} = 0 \implies (\zeta + \zeta^{-1})^2 = 2$. Let $\tau = \zeta + \zeta^{-1}$, then $\tau^2 = 2$. By Euler's criterion, we have $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$, where p is an odd prime. Since $2 = \tau^2$, we have $(\tau^2)^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p} \implies \tau^{p-1} \equiv \left(\frac{2}{p}\right) \pmod{p} \implies \tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p}$. We know, $\tau = \zeta + \zeta^{-1}$, so $\tau^p = \zeta^p + \zeta^{-p}$. Clearly, $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ when $p \equiv \pm 1 \pmod 8$ and $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$ when $p \equiv \pm 3 \pmod 8$. $\zeta^4 = \zeta^3\zeta = -1 \implies \zeta^3 = -\zeta^{-1}$. So, we have:

$$\zeta^p + \zeta^{-p} = \begin{cases} \tau & p \equiv \pm 1(8) \\ -\tau & p \equiv \pm 3(8) \end{cases}$$

Substituting this in the relation $\tau^p \equiv \left(\frac{2}{p}\right)\tau(p)$, we get:

$$(-1)^{\frac{p^2-1}{8}}\tau \equiv \left(\frac{2}{p}\right)\tau \pmod{p} \implies (-1)^{\frac{p^2-1}{8}} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

At this point, one might wonder why we performed computations on the primitive eighth root of unity to find the quadratic character of 2? The answer to this is that $\tau = \sqrt{2} \in \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8) \implies \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$. This is a special case of Kronecker-Weber theorem[19] which assists in studying the splitting of a prime p in the extension $\mathbb{Q}(\sqrt{2})$, thereby, determining the value of the quadratic character of 2. We will learn more about this in section 3.2.2 and will elucidate it further in section 4.4.1.

3.2.2 Quadratic Gauss Sum

We shall now proceed to find the quadratic character of an odd prime p, and prove the law of quadratic reciprocity. However, let us first define the Gauss sum formally. Let ζ_p be the p^{th} root of unity.

Definition 3.8. $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta_p^{at}$ is called the quadratic Gauss sum.

Note: In this section, the summation is always from $t = 0$ to $p - 1$.

The Gauss sum at $a = 1$ is $g_1 = \sum_t \left(\frac{t}{p}\right) \zeta_p^t$. We will denote this by g.

Proposition 3.9. $g_a = \left(\frac{a}{p}\right) g_1$

Proof of Proposition 3.9. If $a \equiv 0 \pmod{p}$ then $\zeta_p^a = 1$ so $\sum_t \left(\frac{t}{p}\right) \zeta_p^{at} = 0$ as $\sum_t \left(\frac{t}{p}\right) = 0$ since we are taking the sum of all quadratic residues and quadratic non-residues modulo p.

[19] see footnote 9

If $a \not\equiv 0 \pmod{p}$ then, $g_a = \sum_t \left(\frac{t}{p}\right) \zeta_p^{at}$ and $\left(\frac{a}{p}\right) g_a = \sum_t \left(\frac{at}{p}\right) \zeta_p^{at} = g_1$. Multiplying the equation by $\left(\frac{a}{p}\right)$ again, gives: $\left(\frac{a}{p}\right)^2 g_a = \left(\frac{a}{p}\right) g_1 \implies g_a = \left(\frac{t}{p}\right) g_1$. □

Once we have obtained this result, we now proceed to prove $g^2 = (-1)^{\frac{p-1}{2}} p$, which is analogous to $\tau^2 = 2$ (see section 3.2.1).

Proposition 3.10. $g^2 = (-1)^{\frac{p-1}{2}} p$

To be able to prove this proposition, we will need the following lemma:

Lemma 3.11. $\sum_t \zeta_p^{t(x-y)} = p$ *if* $x \equiv y \pmod{p}$, *else it is* 0.

Proof of Lemma 3.11. If $x \equiv y \pmod{p}$ then $p|(x-y)$, so $\zeta_p^{x-y} = 1 \implies \sum_t \zeta_p^{t(x-y)} = p$ and if $x \not\equiv y \pmod{p}$, that is, $p \nmid (x-y)$, then $\zeta_p^{x-y} \neq 1$, and by geometric progression $\sum_t \zeta_p^{t(x-y)} = \frac{\zeta_p^{(x-y)p}-1}{\zeta_p^{x-y}-1} = 0$. □

Proof of Proposition 3.10. Let us evaluate the sum of $g_a g_{-a}$ over a. From proposition 3.9, we know that $g_a = \left(\frac{a}{p}\right) g$, so $g_{-a} = \left(\frac{a}{p}\right) g$, hence $g_a g_{-a} = \left(\frac{-1}{p}\right) g^2$. Applying summation over a on both sides, we get:

$$\sum_a g_a g_{-a} = \sum_a \left(\frac{-1}{p}\right) g^2 = (p-1)\left(\frac{-1}{p}\right) g^2$$

. Now, we know that g_a is the Gauss sum corresponding to a, so

$$g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta_p^{a(x-y)}$$

By lemma 3.11, applying summation over a in the equation will give:

$$\sum_a g_a g_{-a} = \sum_a \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta_p^{a(x-y)} = (p-1)p$$

.Comparing the two results we got from evaluating $\sum_a g_a g_{-a}$, we get:

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

□

Let us now prove the law of quadratic reciprocity. To ease our calculation, we let $p^* = (-1)^{\frac{p-1}{2}} p$. Observe that g^2 analogous to τ^2, where $\tau^2 = 2$ (see section 3.2.1). Also note that $g_a \in \mathbb{Z}[\zeta_p]$ and $g \in \mathbb{Z}[\zeta_p]$. If $L = \mathbb{Q}(\zeta_p)$ then $\mathbb{Q}(g) \subset L$ (again a special case of Kronecker Weber theorem). Therefore whatever we have done so far, is very similar to our work in section 3.2.1.

Let q be an odd prime, distinct from p. We shall work in the ring $(\mathcal{O}_L)/(q)$, where $L = \mathbb{Q}(\zeta_p)$.

Raising g to the power $q-1$ and applying Euler's criterion, we get:

$$g^{q-1} = (g^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod{q} \tag{3}$$

This can be written as:

$$g^q \equiv \left(\frac{p^*}{q}\right) g \pmod{q} \tag{4}$$

Recall, this looks similar to $\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p}$, where p is an odd prime. On raising $g = \sum_t \left(\frac{t}{p}\right)\zeta_p^t$ to the power of q, where q is an odd prime, we get:

$$g^q = \left(\sum_t \left(\frac{t}{p}\right)\zeta_p^t\right)^q = \left(\sum_t \left(\frac{t}{p}\right)^q \zeta_p^{qt}\right) = \left(\sum_t \left(\frac{t}{p}\right)\zeta_p^{qt}\right) \equiv g_q \tag{5}$$

We know from 3.10 that $g_q \equiv \left(\frac{q}{p}\right) g$, so, our equation 5 can be rewritten as:

$$g^q \equiv \left(\frac{q}{p}\right) g \pmod{q} \tag{6}$$

Comparing equation 4 and equation 6, we get:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right) \tag{7}$$

Substituting $p^* = (-1)^{\frac{p-1}{2}} p$, we get:

$$\left(\frac{p^*}{q}\right) = \frac{(-1)^{\frac{p-1}{2}}}{q}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \tag{8}$$

Substituting $\left(\frac{p^*}{q}\right)$ in equation 7 by RHS of equation 8, gives us the law of quadratic reciprocity:

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

Thus far, we introduced the quadratic Gauss sum and proved the law of quadratic reciprocity. Notice that the key ingredient in our proof of quadratic reciprocity is $g^2 = p^*$ or rather $g = \sqrt{p^*}$. Observe that if $p \equiv 1 \pmod 4 = 4k+1$ for some integer k, then $g = \sqrt{(-1)^{2k}p} = \sqrt{p}$, and if $p = 4k+3$, then $g = \sqrt{-p}$. So, the sign of g, depends on whether p is congruent to 1 (mod 4) or 3 (mod 4) and affects the Legendre symbol as follows:

Let $p \equiv 1 \pmod 4$, then

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

which is ± 1 depending on the value of $q \pmod p$, while if $p \equiv 3 \pmod 4$, then

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

which is ± 1 depending on the value of $q \pmod{4p}$.

This is due to the ramification of primes in the quadratic number field. We have been pressing the fact that $\mathbb{Q}(g) \subset \mathbb{Q}(\zeta_p)$ by Kronecker-Weber theorem. Our intent is to convey that other than p, we have $2, \infty$ ramified in $\mathbb{Q}(\sqrt{-p})$, when $-p \equiv 3 \pmod 4$. The reason we work with $p^* \equiv 1 \pmod 4$ when proving the quadratic reciprocity law was that even if $p \equiv 3 \pmod 4$, $p^* = -p \equiv 1 \pmod 4$ and p is the only prime ramified in $\mathbb{Q}(\sqrt{p^*})$. In general, it is important to bear in mind that whether q splits in $\mathcal{O}_K$ or not depends upon what the congruence condition is, which is determined by whether only p or both $2, p$ are ramified in the quadratic extension. We shall discuss this in more detail in section 4.4.2.

3.3 Gauss and Jacobi Sums

In section 3.2, for odd primes p, q, computations on the expression $g(\chi)^2 = p^*$ gave us a quadratic number field in which q splits completely to be a quadratic residue modulo p, with χ being the Legendre symbol. Analogous to this, for cubic reciprocity, we talk about splitting of q in $L = K(p^{1/3})$, where K is quadratic number field $\mathbb{Q}(\sqrt{-3})$. So, based on the argument we drew in the proof of the law of quadratic reciprocity, we need $g(\chi)^3$ to prove the law of cubic reciprocity. The Jacobi sums, which are products of powers of the Gauss sums, give us a simpler expression for $g(\chi)^3$ which is $pJ(\chi, \chi) = p\pi$, with χ denoting the cubic residue character.

In general, to prove any n^{th} reciprocity law, the Jacobi sum furnishes us with a simpler expression for $g(\chi)^n$, where χ denotes the n^{th} residue symbol.

We were able to get $g(\chi)^2 = p^*$ in the proof of the quadratic reciprocity law in section 3.2.2 using the properties $\chi^2 = \epsilon$ and $\chi(-1) = (-1)^{\frac{p-1}{2}}$, where χ was the Legendre symbol (a multiplicative character[20]). Clearly, the properties of these multiplicative characters influence the equations involving the Gauss and Jacobi sums. Therefore, it is vital to explore their properties, before delving deeper into the study of these sums.

Definition 3.12 ([9, p. 88])**.** A multiplicative character on $\mathbb{F}_p$ is a homomorphism from $\mathbb{F}_p^\times \longrightarrow \mathbb{C}$ such that $\chi(a)\chi(b) = \chi(ab)$, for $a, b \in \mathbb{F}_p^\times$.

The identity multiplicative character is denoted by ϵ, and it maps all $a \in \mathbb{F}_p^\times$ to 1. Recall that $\chi^2(a) = \epsilon$ if χ is the Legendre symbol. In section 3.1, we talked about the properties of the Legendre symbol. Multiplicative characters in general also have some properties, which will further elucidate the properties of the Legendre symbol. We shall now list these properties:

Proposition 3.13 ([9, p. 88])**.** *Let χ be a multiplicative character and $a \in \mathbb{F}_|^\times$, then:*

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

[20] see definition 3.2

Proof of Proposition 3.13. 1. $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$.

So, either $\chi(1) = 0$ or $\chi(1) = 1$. Since $\chi(1) \neq 0$ as $\chi(0) = 0$ and $0 \neq 1$, so $\chi(1) = 1$.

2. $a^{p-1} \equiv 1(p)$ by Fermat's Little Theorem. $\chi(a^{p-1}) = \chi(a)^{p-1} = \chi(1) = 1$, so $\chi(a)$ is $(p-1)^{st}$ root of unity.

3. $\chi(1) = \chi(a \cdot a^{-1}) = \chi(a) \cdot \chi(a^{-1}) = 1$.

$$\chi(a^{-1}) = \frac{1}{\chi(a)} = \chi(a)^{-1}$$

Also, $\chi(a)$ is a complex root of unity. So, $\chi(a)\overline{\chi(a)} = |\chi(a)|^2 = 1 \implies \chi(a)^{-1} = \overline{\chi(a)}$.

□

Remark ([9, p. 89]). The summation over $t \in \mathbb{F}_p^*$ of all the non-trivial multiplicative characters is 0. While, if the characters are trivial, then the summation over t is p.

Let us see if these properties hold in case of the Legendre symbol.

- The first property is clear as $\left(\frac{1}{p}\right) = 1$ as 1 is always a quadratic residue modulo p.
- The second property follows from $\left(\frac{a}{p}\right)^{p-1} = 1$ as $p-1$ is always even.
- For property 3, let $ab \equiv 1 \pmod{p}$ for some integers a, b not divisible by p, then $\left(\frac{ab}{p}\right) = 1 \iff \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

  Proof. This proof follows from the following equations:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1$$
$$\left(\frac{b}{p}\right)^2 = 1 \implies \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)^{-1}$$

  □

- Summation of all Legendre symbol over $t \in \mathbb{F}_p$ is 0 since there are as many quadratic residues as there are quadratic non-residues.

  Since the Legendre symbol $\left(\frac{1}{p}\right) = 1$, hence, summation over all $t \in \mathbb{F}_p$ means p times summation of 1 which is p.

The multiplicative characters form a cyclic group under multiplication with the identity element ϵ such that $\chi^{p-1} = \epsilon$.

We now have a thorough knowledge of the multiplicative characters. We shall now delve deeper into the discussion of the Gauss and Jacobi sums to be equipped to prove the law of cubic reciprocity.

3.3.1 The Gauss Sums

We aim to generalise the results we proved in the section 3.2 for an arbitrary multiplicative character χ.

Definition 3.14. Let χ be a character defined on $\mathbb{F}_p$ and $a \in \mathbb{F}_p$, where p is an odd prime. Let ζ be the p-th root of unity. Then $g_a = \sum_{t=0}^{p-1} \chi(t)\zeta^{at}$ is called the Gauss sum.

Recall, in proposition 3.9, we proved that $g_a = \left(\frac{a}{p}\right) g_1$. This proposition was extremely helpful in proving the law of quadratic reciprocity and it also gave us the important relation $g^2 = (-1)^{\frac{p-1}{2}} p$ for an odd prime p, which we outlined in section 3.1. Given the pivot role it has played in the proving the quadratic reciprocity law, it is important that we generalise it, in order to extend its usage in proving higher reciprocity laws.

Proposition 3.15 ([9, p. 91])**.** *If $a \neq 0$ and $\chi \neq \epsilon$, then $g_a = \chi(a^{-1})g_1(\chi)$. If $a \neq 0$ and $\chi = \epsilon$ then $g_a(\epsilon) = 0$, while if $a = 0$ and $\chi = \epsilon$, then $g_0(\epsilon) = p$.*

Proof of Proposition 3.15. Suppose $a \neq 0$ and $\chi \neq \epsilon$, then

$$\chi(a)g_a(\chi) = \chi(a)\sum_t \chi(t)\zeta^{at} = \sum_t \chi(at)\zeta^{at} = g_1(\chi)$$

Now if $a \neq 0$ but $\chi = \epsilon$ then, $\chi(a) = \epsilon(a) = 1$, and $a \in \mathbb{F}_p$, so $p \nmid a$ and we have:

$$g_a(\chi) = \sum_t \epsilon(t)\zeta^{at} = \sum_t \zeta^{at} = 0$$

If $a = 0$ and $\chi = \epsilon$ then $g_0 = \sum_t \epsilon(t) = \sum_t 1 = p$. □

Recall that Proposition 3.9 was used to prove the Proposition 3.10, which played a key role in the proof of the law of quadratic reciprocity as well in deciding the sign of the quadratic Gauss sum. Hence, given its importance, we wish to find the absolute value of $g_1(\chi)$. Let us denote $g_1(\chi)$ by $g(\chi)$ and generalise Proposition 3.10.

Proposition 3.16 ([9, p. 92])**.** *If $\chi \neq \epsilon$, then $|g(\chi)| = \sqrt{p}$.*

Proof of Proposition 3.16. We will follow an outline very similar to the proof of Proposition 3.10. Let us evaluate $\sum_a g_a(\chi)\overline{g_a(\chi)}$. We know that $g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})g(\chi)\overline{\chi(a^{-1})g(\chi)}$ by Proposition 3.15.By the properties of multiplicative characters, we have: $\overline{\chi(a^{-1})} = \chi(a^{-1})^{-1} = \chi(a)$.

Substituting this in $g_a(\chi)\overline{g_a(\chi)}$ we get $g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)}$

$\chi(a^{-1})\chi(a) = \chi(a^{-1}a) = \chi(1) = 1$ by the properties of multiplicative characters.

So, $g_a(\chi)\overline{g_a(\chi)} = |g(\chi)|^2$, and since $g_0(\chi) = 0$ if $\chi \neq \epsilon$ by Proposition 3.15, we have:

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2 \tag{9}$$

Also, $\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_x \chi(x)\zeta^{ax} \sum_y \overline{\chi(y)}\zeta^{-ay} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}$

Hence, using the lemma 3.11, we have:

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = (p-1)p \tag{10}$$

Comparing equations 9 and 10, we get that $|g(\chi)|^2 = p \implies |g(\chi)| = \sqrt{p}$ □

Recall that in Proposition 3.10, we proved that $g(\chi)^2 = (-1)^{\frac{p-1}{2}}p$, so let us see how it relates with our result in Proposition 3.16:

We know that $|g(\chi)|^2 = g(\chi)\overline{g(\chi)}$.

$$\overline{g(\chi)} = \sum_t \overline{\chi(t)}\zeta^{-t} = \chi(-1)\sum_t \overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi})$$

So, we have the following relation:

Remark ([9, p. 92]). $g(\chi)g(\overline{\chi}) = \chi(-1)p$.

If χ is the Legendre symbol then this reduces to $g^2 = \chi(-1)p = (-1)^{\frac{p-1}{2}}p$.

3.3.2 Jacobi Sums

We introduced the Jacobi sums in the beginning of section 3.3 as product of the powers of Gauss sums and discussed the role they will play in the proof of the law of cubic reciprocity. Let us now define them formally:

Definition 3.17 ([9, p. 93])**.** Let χ, λ be characters on $\mathbb{F}_p$ and set $J(\chi,\lambda) = \sum_{a+b=1}\chi(a)\lambda(b)$, then $J(\chi,\lambda)$ is called a Jacobi sum.

Having defined the Jacobi sums, a natural question that one might ask is what are the values of the Jacobi sums at trivial and non-trivial characters? And how are they related to the Gauss sums? Let us answer these now with the following theorem:

Theorem 3.18 ([9, p. 93])**.** *Let χ, λ be non-trivial characters, then:*

- $J(\epsilon,\epsilon) = p$.
- $J(\epsilon,\chi) = 0$.
- $J(\chi,\chi^{-1}) = -\chi(-1)$.
- *If $\chi\lambda \neq \epsilon$ then,* $J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Proof of Theorem 3.18. Let χ, λ be characters such that $\chi, \lambda \neq \epsilon$, then,

- $$J(\epsilon,\epsilon) = \sum_{a+b=1}\epsilon(a)\epsilon(b) = \sum_{a+b=1} 1 = p.$$
- $$J(\epsilon,\chi) = \sum_{a+b=1}\epsilon(a)\chi(b) = \sum_{a+b=1}\chi(b) = 0.$$

- $$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a+b=1} \chi(ab^{-1}) = \sum_{a+b=1, b\neq 0} \chi\left(\frac{a}{b}\right)$$

  We have, $a + b = 1, b \neq 0$ so, let $b = 1 - a$ then clearly, $a \neq 1$. This leads us to:

  $$\chi\left(\frac{a}{b}\right) = \chi\left(\frac{a}{1-a}\right)$$

  Moreover, if c is an integer, such that $c \neq -1$, then we have $c = \frac{a}{1-a} \implies a = \frac{c}{1+c}$. Since a, c do not vary over $1, -1$ respectively, we have:

  $$\sum_{c\neq -1} \chi(c) + \chi(-1) = 0 \implies J(\chi, \chi^{-1}) = -\chi(-1)$$

- Expand $g(\chi), g(\lambda)$, then

  $$g(\chi)g(\lambda) = \sum_x \chi(x)\zeta^x \sum_y \lambda(y)\zeta^y$$

  $$= \sum_{x,y} \chi(x)\lambda(y)\zeta^{x+y} = \sum_t \sum_{x+y=t} \chi(x)\lambda(y)\zeta^t$$

  If $t = 0$ then $\zeta^t = 1$ and $\sum_{x+y=0} \chi(x)\lambda(y) = 0$

  If $t \neq 0$, then let $x = x't, y = y't$ and $x + y = t \implies x' + y' = 1$, then by definition of Jacobi sums, we have

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

  This gives us that

  $$\sum_{x+y=t} \chi(x)\lambda(y) = \chi.\lambda(t)J(\chi, \lambda)$$

  $$\implies g(\chi)g(\lambda) = \sum_t \chi.\lambda(t)J(\chi, \lambda)\zeta^t = g(\chi.\lambda)J(\chi, \lambda)$$

  This leads to the result:

  $$\chi\lambda \neq \epsilon, \implies J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi.\lambda)} \tag{11}$$

□

The last property along with the proposition 3.16, gives us the absolute value of the Jacobi sum.

Remark ([9, p. 94]). If $\chi, \lambda, \chi\lambda$ are non-trivial characters, then $J(\chi, \lambda) = \sqrt{p}$.

Thus far, we have equipped ourselves with the knowledge on the value of the Jacobi sum and its relation with the Gauss sum. However, the most interesting relation between the Gauss sums and Jacobi sums that we developed this whole theory for, is as following:

Proposition 3.19 ([9, p. 96])**.** *If $p \equiv 1 \pmod{n}$ and χ is a character of order $n > 2$, then $g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})$.*

Proof of Proposition 3.19. We know from Proposition 3.18 that

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\cdot\lambda)}$$

If $\chi = \lambda$ then

$g(\chi)^2 = J(\chi,\chi)g(\chi^2)$. This means that

$$g(\chi)^3 = J(\chi,\chi)g(\chi^2)g(\chi)$$

and by Theorem 3.18, we have $g(\chi^2)g(\chi) = J(\chi,\chi^2)g(\chi^3)$. This leads us to:

$$g(\chi)^3 = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$$

Repeating this $n-1$ times, we get

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})g(\chi^{n-1})$$

Since the order of χ is n, we have $\chi^n = \epsilon = 1 \implies \chi^{n-1}\chi = 1 \implies \chi^{n-1} = \chi^{-1} = \overline{\chi}$, so

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})g(\overline{\chi})$$

Multiplying both sides by $g(\chi)$, we get:

$$g(\chi)^n = J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})g(\overline{\chi})g(\chi)$$

Since $|g(\chi)|^2 = p$ and $g(\chi)g(\overline{\chi}) = \pm p = \chi(-1)p$, so,

$$g(\chi)^n = J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})g(\overline{\chi})g(\chi)$$

$$\implies g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})$$

□

With this proposition, we have found the value of $g(\chi)^3 = pJ(\chi,\chi)$ as $\chi(-1) = \chi(-1^3) = \chi(-1)^3 = 1$. Thus we equipped ourselves with most of the tools needed to prove the law of cubic reciprocity. What remains now is to acquaint ourselves with the arithmetic in the ring $\mathbb{Z}[\omega]$, where ω is the third root of unity. We shall do this in the next section.

3.4 Cubic Reciprocity using Gauss Sums

In the beginning of this thesis, we highlighted the need for the higher reciprocity laws and have gained sufficient background in subsequent sections to prove them. However, as mentioned earlier, we need to be familiar with the arithmetic of the ring of algebraic integers. Gauss

claimed that the theory of higher residues is difficult to prove without the properties of these rings. Since, he managed to prove the law of biquadratic reciprocity[21] by investigating the arithmetic in the ring $\mathbb{Z}[\sqrt{-1}]$, which is known as the Gaussian ring.

One of the higher reciprocity laws is the law of cubic reciprocity tells us for which primes $x^3 \equiv a \pmod{p}$ has solutions. The first proof of the law of cubic reciprocity was by Eisenstein. Owing to this, the complex numbers of form $a+b\omega$, where a, b are integers are called Eisenstein integers. In this section, we aim to prove this law. We shall now begin our study with the ring $\mathbb{Z}[\omega]$.

3.4.1 Arithmetic of the ring $\mathbb{Z}[\omega]$

Let $\omega = \frac{-1+i\sqrt{3}}{2}$, we know that $1 + \omega + \omega^2 = 0$. The ring $\mathbb{Z}[\omega]$ is a Euclidean domain[22] with elements of the form $a + b\omega$, where a, b are integers. Since every Euclidean domain is a principal ideal domain, every irreducible element in the ring is a prime, and unique factorization holds. It is closed under complex conjugation, which means if $\alpha = a + b\omega$ then $\overline{\alpha} = a + b\omega^2 = (a - b) - b\omega \in \mathbb{Z}[\omega]$. We can therefore, define norm of an element $a + b\omega$ to be given by $a^2 - ab + b^2$.

Proposition 3.20. *There are* 6 *units in the ring* $\mathbb{Z}[\omega]$ *and they are* $\pm 1, \pm\omega, \pm\omega^2$.

Proof of Proposition 3.20. An element $a + b\omega$ is a unit if its norm is 1. This means that $a^2 - ab + b^2 = 1$, or $4 = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$. Then, $(2a - b)^2 + 3b^2 = 4 \iff$ either $2a - b = \pm 2, b = 0$ or $(2a - b) = \pm 1, b = \pm 1$. This means that either $a = \pm 1, b = 0$, $a = 1, b = 1$, $a = 0, b = 1$, $a = 0, b = -1$, $a = -1, b = -1$. So we have, the units as $\pm 1, \pm\omega, \pm\omega^2$. □

We know that $\mathbb{Z}[\omega]$ is a principal ideal domain. So every irreducible element is a prime. Hence, if the norm of an element is p^2 where p is a rational odd prime then it tells us that p is also a prime in $\mathbb{Z}[\omega]$. However, if norm of an element in $\mathbb{Z}[\omega]$ is p then the element is a complex prime, which means that the prime p splits in the ring $\mathbb{Z}[\omega]$. Let us formalise this as the following theorem:

Theorem 3.21 ([9, p. 110])**.** *Let* π *be a prime in* $\mathbb{Z}[\omega]$*, and* p, q *are primes in* $\mathbb{Q}$*. Then,* $p = \pi\overline{\pi}$*, if* $p \equiv 1 \pmod{3}$*, and* q *is a prime in* $\mathbb{Z}[\omega]$*, if* $q \equiv 2 \pmod{3}$*. Moreover,* 3 *splits in* $\mathbb{Z}[\omega]$

Proof of Theorem 3.21. Let p, a rational odd prime such that it is not a prime in $\mathbb{Z}[\omega]$, then $p = \pi\gamma$, for some primes $\pi, \gamma \in \mathbb{Z}[\omega]$. Taking norms, we see that $p^2 = N(\pi)N(\gamma)$. If $N(\pi) = p$, then $p = a^2 - ab + b^2$, for $\pi = a + b\omega$. This means that $4p = (2a - b)^2 + 3b^2 \implies p \equiv (2a - b)^2$

[21] It answers the question that for which primes p is the congruence $x^4 \equiv a \pmod{p}$ solvable, where a is a fixed integer.

[22] To show that $\mathbb{Z}[\omega]$ is a Euclidean domain:

Let $\alpha \in \mathbb{Z}[\omega]$, then $\alpha = a + b\omega$, where a, b are integers. Let $\lambda(\alpha) = a^2 - ab + b^2$, then one can see that $\alpha\overline{\alpha} = \lambda(\alpha)$. Note that $0 < \lambda(\alpha) \in \mathbb{Z}$. Let $\alpha, \beta \in \mathbb{Z}[\omega]$ and $\alpha \neq 0$. We want to express β/α as an element of $\mathbb{Z}[\omega]$. Let $p, q \in \mathbb{Q}$ such that $\frac{\beta}{\alpha} = \frac{\beta\overline{\alpha}}{\alpha\overline{\alpha}} = p + q\omega$. Let $\delta = m + n\omega$, where $|p - m| \leq 1/2$ and $|q - n| \leq 1/2$. The value of $\lambda(\beta/\alpha - \delta) = \lambda(\tau)$, where $\tau = (p - m) + (q - n)\omega$. Solving $\lambda((p - m) + (q - n)\omega)$ further gives $\lambda(\tau) \leq 3/4 < 1$. Let $\tau\alpha = \beta - \delta\alpha$, then $\tau\alpha = 0 \implies \beta = \delta\alpha$ or $\lambda(\tau\alpha) = \lambda(\alpha)\lambda(\beta/\alpha - \delta) < \lambda(\alpha)$.

(mod 3). Since 1 is the only square modulo 3, so $p \equiv 1 \pmod 3$. It follows immediately that p is a prime in $\mathbb{Z}[\omega]$ if $p \equiv 2 \pmod 3$.

Now, let us prove the last part, $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$. This means that $\frac{x^3-1}{x-1} = x^2 + x + 1 = (x-\omega)(x-\omega^2)$. Set $x = 1$, then $3 = (1-\omega)(1-\omega^2) = -\omega^2(1-\omega)^2$. □

In the ring $\mathbb{Z}$, an element splits into equivalence classes $\mathbb{Z}/(p)$ by the relation $a \equiv b \pmod p$. Now we know when an element is a prime and when it splits in $\mathbb{Z}[\omega]$, let us try to formalise a similar relation in the ring $\mathbb{Z}[\omega]/(\pi)$, where π is a prime in $\mathbb{Z}[\omega]$. This ring is called the residue class ring. To split elements into equivalence classes, we first need to know the elements in this ring.

Proposition 3.22 ([9, p. 111])**.** *Let π be a prime in $\mathbb{Z}[\omega]$. Then $\mathbb{Z}[\omega]/(\pi)$ is a finite field with $N(\pi)$ elements.*

Proof. Let $\pi \in \mathbb{Z}[\omega]$ be a prime. Since $\mathbb{Z}[\omega]$ is a unique factorization domain, π is a prime $\iff$ π is irreducible $\iff$ (π) is maximal $\iff$ $\mathbb{Z}[\omega]/(\pi)$ is a field.

Suppose π is a rational prime q, where $q \equiv 2 \pmod 3$.

Claim: $\{a + b\omega | 0 \le a, b < q\}$ is a complete set of coset representatives. Let $x = m + n\omega \in \mathbb{Z}[\omega]$. Then by division algorithm for integers m, n, there exist integers a, b, r, s such that $m = qr + a$ and $n = qs + b$, where $0 \le a, b < q$. Substituting the values of m, n in the equation $x = m + n\omega \in \mathbb{Z}[\omega]$, we get: $x = q(r + s\omega) + (a + b\omega)$. By applying reduction modulo q, we have $x = a + b\omega$. There will be at most q^2 elements of this form. Suppose $a + b\omega = a' + b'\omega \pmod q$. Then $q|a - a'$ and $q|(b - b')$. Since q is a rational prime, hence $q|(b - b')$. However, $a, b, a', b' < q$, so $q|(b - b')$ is possible only when $b = b'$ and $a = a'$. Therefore, there are exactly q^2 elements.

Let $\pi = a + b\omega$ be a complex prime such that $N(\pi) = p$, where p is a rational prime $\equiv 1 \pmod 3$. Note that $p = N(\pi) = a^2 - ab + b^2$ so $p \nmid b^2$.

Claim: $\{0, 1, 2, \ldots, p-1\}$ is the complete set of coset representatives. Let $x = m + n\omega \in \mathbb{Z}[\omega]$. Since, $p \nmid b^2$, $gcd(b, p) = 1$. There exists $c \in \mathbb{Z}$, such that $bc \equiv n \pmod p$. So, $bc = n + kp$, where k is some integer. Multiplying $\pi = a + b\omega$ by c, we have $\pi c = ac + bc\omega$. We know that $bc = n + kp$, so $\pi c = ac + (n + kp)\omega$. Subtracting $\pi c = ac + (n + kp)\omega$ from $x = m + n\omega$, we get: $x - \pi c = (m - ac) - kp\omega$. Reducing modulo p, we get $x - \pi c \equiv (m - ac) \pmod p$. We can rewrite this as $x - \pi c = (m - ac) + tp$ for some t. Since $p = \pi\overline{\pi}$, we have $x = m - ac + \pi(t\overline{\pi} + c)$. This gives us $x = m - ac \pmod \pi$. Every element in $\mathbb{Z}[\omega]$ is congruent to some rational integer modulo π. We know by division algorithm that if $y \in \mathbb{Z}$, and $y = pq + r$, where $0 \le q, r < p$, then $y \equiv r \pmod p$. Similarly, here we have $y \equiv r \pmod \pi$. Therefore, every element in $\mathbb{Z}[\omega]$ is congruent to $\{0, 1, \ldots p-1\} \pmod \pi$. If $r \equiv r' \pmod \pi$, then $r - r' = \pi t$ and we know that $N(\pi) = p$, so $N(r - r') = N(\pi)N(t) \implies p|(r - r')^2$ hence, $p|r - r'$. Recall that $0 \le r, r' < p$, so $r = r'$. Hence, there are only p elements in $\mathbb{Z}/(\pi)$.

Let $\pi = 1 - \omega$. $N(1 - \omega) = 3$.

Claim: {0,1,2} is the complete set of coset representatives. Let the coset that contains $1-\omega$ be represented by [0], then the coset containing ω is represented by [1]. Moreover, any element of the form $a + b\omega$ can be represented by the coset[23] $[a + b]$. Moreover, $\mathbb{Z}[\omega]/(1 - \omega) \cong \mathbb{Z}/3\mathbb{Z}$,

[23] Substituting 1 in place of ω

hence, any element that is 0 in $\mathbb{Z}[\omega]/(1-\omega)$ is divisible by 3 and since 3 is divisible by $1-\omega$ it maps to $0 \in \mathbb{Z}[\omega]/(1-\omega)$. Hence, we have only three equivalence classes $[0], [1], [2]$ in the ring $\mathbb{Z}[\omega]/(1-\omega)$ and every multiple of 3 goes to $[0]$. □

3.4.2 Cubic Residue Character

Now let us work in this residue class ring. If α is an integer such that $\pi \nmid \alpha$ then, we have an analog of the Fermat's little theorem.

Proposition 3.23 ([9, p. 112])**.** *If $\pi \nmid \alpha$ then $\alpha^{N(\pi)-1} \equiv 1 \pmod 3$.*

Proof of Proposition 3.23. We proved in Proposition 3.22 that $\mathbb{Z}[\omega]/(\pi)$ is a field, so every non-zero element has an inverse. This means that the order of $(\mathbb{Z}[\omega]/(\pi))^\times$ is $N(\pi)-1$, which means that if $\alpha \in (\mathbb{Z}[\omega]/(\pi))^\times$, then $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$. □

If the norm of $\pi \neq 3$, then the residue classes of $1, \omega, \omega^2$ are all distinct in $(\mathbb{Z}[\omega]/(\pi))$. Suppose $\omega = 1$ in $(\mathbb{Z}[\omega]/(\pi))$, then $\omega \equiv 1 \pmod \pi$, which implies that $\pi|(1-\omega)$ and hence, $N(\pi)|N(1-\omega)$ but since both are primes in $(\mathbb{Z}[\omega]/(\pi))$, so $\pi, 1-\omega$ are associates. $3 = -\omega^2(1-\omega)^2$, hence, $N(\pi) = 3$ which is a contradiction. Hence, $1, \omega, \omega^2$ are all distinct in $(\mathbb{Z}[\omega]/(\pi))$. Moreover, since $1, \omega, \omega^2$ form a cyclic group generated by ω of order 3, hence, $3|N(\pi)-1$. We know that $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$. So, we have

$$\alpha^{N(\pi)-1} = (\alpha^{\frac{N(\pi)-1}{3}} - 1)(\alpha^{\frac{N(\pi)-1}{3}} - \omega)(\alpha^{\frac{N(\pi)-1}{3}} - \omega^2)$$

Since $\pi|\alpha^{N(\pi)-1} - 1$ by Proposition 3.23, hence, it divides one of the three factors. In fact, it can only divide one, since if it divides two factors then it divides their difference, which means $N(\pi) = 3$, which is not true as per our above discussion. Hence,

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod \pi \tag{12}$$

where $m = 0, 1, 2$. This leads us to the definition of the cubic residue character.

Definition 3.24 ([9, p. 112])**.** If $N(\pi) \neq 3$, the cubic residue character $\left(\frac{\alpha}{\pi}\right)_3$ of $\alpha \pmod \pi$ is given by the equation:

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod \pi$$

where the value of $\left(\frac{\alpha}{\pi}\right)_3$ is $1, \omega, \omega^2$ given as per equation 12.

Remark ([9, pp. 112–113])*.* The cubic residue character is like the Legendre symbol but for cubic residues, hence, we have a very similar properties that hold as follows:

1. $\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff \alpha$ is a cubic residue modulo π.
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 $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

Since, the cubic character is a multiplicative character, therefore, we will denote it by χ_π. Let us study the behaviour of χ under complex conjugation.

Proposition 3.25 ([9, p. 113])**.** *The behaviour of the cubic residue character under complex conjugation is as follows:*

1. $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.
2. $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

Proof of Proposition 3.25.

1. The value of the cubic residue character is either $1, \omega$ or ω^2, hence the conjugate of $1 = 1, \omega = \omega^2$, so, the conjugate of the the cubic residue character is the square of the value of the cubic residue character.
2. From definition 3.24, we have $\alpha^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi}$, then the conjugate of this is: $\overline{\alpha}^{\frac{N(\pi)-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$ which is equivalent to $\overline{\alpha}^{\frac{N(\overline{\pi})-1}{3}} \equiv \chi_{\overline{\pi}}(\alpha) \pmod{\overline{\pi}}$, since $N(\pi) = N(\overline{\pi})$.

□

We now have all the tools needed to prove the law of cubic reciprocity. However, we still need to know the notion of primary primes. Since there are six units in the ring $\mathbb{Z}[\omega]$, each prime has 6 unit multiples or rather, 6 associates and hence, to avoid ambiguity, we introduce the idea of a primary prime. Taking $\pi = a + b\omega$, one can check that exactly one of the 6 associates is primary by checking each case.

Definition 3.26 ([9, p. 113])**.** If π is a prime in $\mathbb{Z}[\omega]$, then π is primary if $\pi \equiv 2 \pmod 3$.

For example, let $N(\pi) = 7$, and $\pi = 3 + \omega$, then $-\omega^2(3 + \omega) = -3\omega^2 - 1 = 2 + 3\omega$ is the primary prime associated to π.

We will now prove the law of cubic reciprocity in the next section.

3.4.3 The Law of Cubic Reciprocity

Let π be a prime in $\mathbb{Z}[\omega]$ such that $N(\pi) = p \equiv 1 \pmod 3$. We know that the ring $\mathbb{Z}[\omega]/(\pi)$ has p elements and so does $\mathbb{Z}/(p)$. The two fields are isomorphic since, the coset of n in $\mathbb{Z}/(p)$ can be identified with some coset in $\mathbb{Z}[\omega]/(\pi)$. This allows us to consider χ_π as a character on $\mathbb{F}_p$. So, we may now use the Gauss and Jacobi sums to prove the law of cubic reciprocity. This proof follows the same argument as our proof of the law of quadratic reciprocity, however, we would need to use few properties of the Jacobi sums. Recall the Proposition 3.19 from 3.3.2. Let us prove it for $n = 3$.

Proposition 3.27 ([9, p. 96])**.** $g(\chi)^3 = pJ(\chi, \chi)$

Proof of Proposition 3.27. Substituting the value of $n = 3$ in Proposition 3.19, we get: $g(\chi)^n = \chi(-1)pJ(\chi, \chi)$. Since $(-1) = (-1)^3$ so $\chi(-1) = \chi(-1^3) = \chi^3(-1) = 1$, as the order of χ is 3 here. □

We cannot directly use $g(\chi)^3 = pJ(\chi,\chi)$ as it does not give us much information. In the proof of the law of quadratic reciprocity, we had that $g(\chi)^2 = p*$ which was a rational prime. Do we have any equivalent here?

Proposition 3.28 ([9, pp. 96–97, 115])**.** *Let χ denote the cubic residue symbol. In $\mathbb{Z}[\omega]$, $J(\chi,\chi)$ is a primary prime. The value of $J(\chi,\chi) = \pi$, where $\pi = a + b\omega$ and $N(\pi) = p$, which is an odd prime.*

Proof of Proposition 3.28. From proposition 3.27, $g(\chi)^3 = pJ(\chi,\chi)$. Moreover by definition of $g(\chi)$, we have $g(\chi)^3 = \sum_t \zeta^{3t} \equiv -1 \pmod 3$. Since $p \equiv 1 \pmod 3$, we have $J(\chi,\chi) \equiv 2 \pmod 3$. Hence, it is a primary prime.

We know $|J(\chi,\chi)|^2 = p$, so $J(\chi,\chi)|p$. Now, let $J(\chi,\chi) = \pi \cdot \pi^*$. So, either π or π^* divides p. We have $J(\chi,\chi) = \sum_t \chi(t)\chi(1-t) = \sum_t t^{(p-1)/3}(1-t)^{(p-1)/3}$. This is a polynomial of degree less than $p-1$. We know that $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod p$ if $(p-1) \nmid k$ so, we get $\sum_t t^{(p-1)/3}(1-t)^{(p-1)/3} \equiv 0 \pmod p$ which means that $J(\chi,\chi) \equiv 0 \pmod \pi$. Hence, $\pi^*|\pi$, so $\pi^* = \pi$ as both are primary, and $J(\chi,\chi) = \pi$. □

Hence, we have obtained a simpler form of $g(\chi)^3$ which we will use in our proof. Let us see how an element splits in $\mathbb{Z}[\omega]$:

Any element that splits in $\mathbb{Z}[\omega]$ will split as $\mathfrak{u}(1-\omega)^m\pi_1^{e_1}\pi_2^{e_2}\ldots\pi_k^{e_k}$, where π_i are primary primes.

Let us find out the cubic character of unit $\mathfrak{u}$. A unit in $\mathbb{Z}[\omega]$ will be of the form $\pm\omega^m$ where $m = 0, 1, 2$. So, the value of $\mathfrak{u}^{\frac{N(\pi)-1}{3}}$ will determine the the cubic character of $\mathfrak{u}$ over π. Hence the values $N(\pi) = 1, 4, 7 \pmod 9$ yield cubic character of $\mathfrak{u} = 1, \omega, \omega^2$, respectively. The cubic character of -1 over π is 1. The cubic character of $(1-\omega) = \omega^{2(p+1)/3} \pmod \pi$ when π is a rational prime p. If $\pi = a + b\omega$ then the cubic character of $(1-\omega) = \omega^{2(a+1)/3}$. These are supplements to the law of cubic reciprocity. We suggest our readers to refer to [45] for a detailed computation of the same.

Let us now state and prove the law of cubic reciprocity for two primes π_1, π_2.

Theorem 3.29 ([9, pp. 115–117])**.** *Let π_1, π_2 be primary, i.e. $\pi_1 \equiv 2 \pmod 3$ and $\pi_2 \equiv 2 \pmod 3$, with distinct norms $\neq 3$, then, $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$.*

Proof of Theorem 3.29. We will consider three cases:

When π_1, π_2 are rationals, π_1 is rational and π_2 is a complex, π_1, π_2 are both complex.

1. π_1, π_2 are both rational primes such that $\pi_1 = p \equiv 2 \pmod 3$ and $\pi_2 = q \equiv 2 \pmod 3$ and $N(p) = p^2, N(q) = q^2$. Also, note that p, q are distinct.

$$\chi_q\overline{p} = \chi_{\overline{q}}(\overline{p}) = \overline{\chi_q(p)} = \chi_q(p^2) = (\chi_q(p))^2 \implies \chi_q(p) = 1$$

. Similarly,

$$\chi_p(q) = (\chi_p(q))^2 = \chi_p(q) - (\chi_p(q))^2$$

Since, $\chi_p(q) \neq 0$ so, it is equal to 1, hence,

$$\chi_p(q) = \chi_q(p)$$

.

2. π_1 is a rational prime $= q \equiv 2 \pmod 3$ and $\pi_2 = \pi$ where $N(\pi) = p$.

   We have, $g(\chi_\pi)^3 = p\pi$. Raising both sides to the power of $\frac{N(\pi_1)-1}{3} = \frac{q^2-1}{3}$.

   We get, $g(\chi_\pi)^{q^2-1} = (p\pi)^{\frac{q^2-1}{3}}$. Reducing mod q on both sides, we get:

   $$g(\chi_\pi)^{q^2-1} = \chi_q(p\pi) \pmod q$$

   Since, p is a rational prime, $\chi_q(p) = 1 \implies$

   $$g(\chi_\pi)^{q^2-1} = \chi_q(\pi) \pmod q$$

   We also have,

   $$g(\chi_\pi)^{q^2} = \sum \chi_\pi(t)^{q^2} \zeta^{q^2 t} \pmod q$$

   Since $q \equiv 2 \pmod 3 \implies q^2 \equiv 1 \pmod 3$, so $\chi_\pi(t)$ is a cube root of 1, so $g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi) \pmod q$.

   We know $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2}) g(\chi_\pi) = \chi_\pi(q) g(\chi_\pi)$ Hence, we have,

   $$\chi_q(\pi) g(\chi_\pi) = \chi_\pi(q) g(\chi_\pi)$$

   Multiplying both sides by $\overline{g(\chi_\pi)}$ then $g(\chi_\pi)\overline{g(\chi_\pi)} = |g(\chi_\pi)|^2 = p$

   $$\chi_q(\pi) p = \chi_\pi(q).$$

3. Let π_1, π_2 be complex primes, where $N(\pi_1) = p_1, N(\pi_2) = p_2$ and $p_1, p_2 \equiv 1 \pmod 3$. Then, $p_1 = \pi_1 \overline{\pi}_1$ and $p_2 = \pi_2 \overline{\pi_2}$. $g(\chi_{\overline{\pi}_1})^3 = p_1 \overline{\pi}_1$. Raising both sides to the power of $\frac{N(\pi_2)-1}{3}$, we get:

   $$g(\chi_{\overline{\pi}_1})^{N(\pi_2)-1} = (p_1 \overline{\pi}_1)^{\frac{N(\pi_2)-1}{3}}$$

   Reducing modulo $\pmod{\pi_2}$,

   $$g(\chi_{\overline{\pi}_1})^{N(\pi_2)} = \chi_{\pi_2}(p_1 \overline{\pi}_1) g(\chi_{\overline{\pi}_1}) \pmod{\pi_2}$$

   Analysing the left hand side,

   $$g(\chi_{\overline{\pi}_1})^{p_2} \equiv \sum_t \chi_{\overline{\pi}_1}(t)^{p_2} \zeta^{p_2 t} \pmod{\pi_2}$$

   Since $p_2 \equiv 1 \pmod 3$ and $\chi_{\overline{\pi}_1}$ is a cube root of 1, we have:

   $$g(\chi_{\overline{\pi}_1})^{p_2} \equiv g_{p_2}(\chi_{\overline{\pi}_1}) \pmod{\pi_2}$$

   Note that,

   $$g_{p_2}(\chi_{\overline{\pi}_1}) = \chi_{\overline{\pi}_1}(p_2^{-1}) g(\chi_{\overline{\pi}_1}) = \chi_{\overline{\pi}_1}(p_2^2) g(\chi_{\overline{\pi}_1})$$

So we get,

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

Similarly, repeating these steps by raising $g(\chi_{\overline{\pi}_2})^3 = p_2\overline{\pi}_2$ to the power of $\frac{p_1-1}{3}$ and then reducing modulo π_1 to get:

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

Now,

$$\chi_{\overline{\pi}_1}(p_2^2) = \overline{\chi_{\overline{\pi}_1}(p_2)} = \chi_{\pi_1}(\overline{p_2}) = \chi_{\pi_1}(p_2)$$

We can now easily prove the law of cubic reciprocity as:

$$\chi_{\pi_2}(p_1\overline{\pi}_1) = \chi_{\overline{\pi}_1}(p_2^2) = \chi_{\pi_1}(p_2)$$

Multiplying both sides by $\chi_{\pi_1}(\pi_2)$

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi}_1) = \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2)$$

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi}_1) = \chi_{\pi_1}(\pi_2 p_2) = \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\overline{\pi_1})$$

$$= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\overline{\pi}_1)$$

Cancelling, $\chi_{\pi_2}(p_1\overline{\pi}_1)$ from both sides, we get,

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$$

□

Similar to the law of cubic reciprocity, is the law of biquadratic reciprocity. However, that is out of the scope of this thesis. We deal with the ring $\mathbb{Z}[i]$ and the units are $\pm 1, \pm i$, however, everything else- the bi-quadratic residue character, the finite field with $N(\lambda)$ elements- $\mathbb{Z}[i]/(\lambda)$, where λ is a prime in $\mathbb{Z}[i]$, are all analogous to the case of the cubic reciprocity. We suggest our readers to refer to [8, 9] for an interesting treatment of the law of biquadratic reciprocity.

4 Galois Theoretic Approach to the Reciprocity Laws

As promised in the beginning of this dissertation, we have proved the law of quadratic and cubic reciprocity using Gauss sums. We will now aim to gain a deeper comprehension of our proofs using Artin reciprocity. The central notion of this section is to study the quadratic and the cubic reciprocity reciprocity laws using Artin reciprocity. Our goal is to make this section more accessible to the reader. We will begin by studying the ramification of finite and infinite primes, the Frobenius element or the Artin symbol and build the necessary theory needed to understand Artin reciprocity theorem and work out our proofs. On our way we will also prove the Kronecker-Weber theorem, and understand its usage in proving these laws. We will, however, not delve too deep into Artin reciprocity or the Kronecker-Weber theorem as

they require rigorous class field theory. We suggest our curious readers to refer to [7, 12, 14] for all their queries on the topic.

4.1 Primes that Ramify in the Ring of Integers

Let K be a number field such that $[K : \mathbb{Q}] = n$. A prime number p is said to be *ramified* (or *respectively unramified*) in a number field K if the ideal factorisation of p:

$$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_d^{e_d} \tag{13}$$

has $e_i > 1$ (respectively $e_i = 1$). The integer e_i is called the ramification index of p. The prime ideals $\mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_d$ are said to be primes lying above p.

Another way to think about ramification of primes is in term of $\mathcal{O}_K/(p)$, where $\mathcal{O}_K$ is the ring of integers of K. We know that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module [[8, p. 98]] so, $\mathcal{O}_K/(p)$ is also a finitely generated $\mathbb{Z}/p\mathbb{Z}$-module. By Chinese remainder theorem on the $\mathbb{F}_p$ vector space $\mathcal{O}_K/(p)$ of dimension n, we get:

$$\mathcal{O}_K/(p) = \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \mathcal{O}_K/\mathfrak{p}_2^{e_2} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_d^{e_d}. \tag{14}$$

The dimension of $\mathcal{O}_K/\mathfrak{p}_i$ an $\mathbb{F}_p$ vector space is called the inertial degree of p. p is said to be ramified, inert or split, based on the following possibilities:

1. $1 \leq i \leq d$, then the inertia degree of $\mathfrak{p}_i \leq n$ and $= n \iff p$ is inert, that is, if $p\mathcal{O}_K$ is the prime ideal.

2. $d \leq n$ and $d = n$ that is $e_i = 1, n_i = 1$, then p is totally split. That is (p) factors as a product of distinct $[K : \mathbb{Q}]$ prime ideals.

3. If one of $e_i > 1$ then p is ramified. The ramification index is the greatest value of e_i such that $\mathfrak{p}_i^{e_i}|p$.

4. p is unramified if (p) factors as product of distinct prime ideals or $\mathcal{O}_K/p$ has no non-trivial nilpotent elements.

Now that we are aware of these terms, let us establish a relationship between the discriminant of the ring of integers $\mathcal{O}_K$ and primes that ramify in K.

Theorem 4.1 ([11, p. 127])**.** *Let p be an odd prime then p is ramified in $K \iff p|\Delta(\mathcal{O}_K)$.*

Proof of Theorem 4.1. This proof is from [46]. Let p be an odd prime number and $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying above p such that $e_\mathfrak{p} > 1$ then $(p) = \mathfrak{p}I$, where I is divisible by $\mathfrak{p}$ and all other primes lying above p. Consider $\sigma_1, \sigma_2, \dots \sigma_n$ embeddings from $K \longrightarrow \mathbb{C}$. Let $K \subset L$ be some extension, then extending σ_i to the automorphism of L over K such that L is normal over $\mathbb{Q}$. Let $a_1, a_2, \dots a_n$ be integral basis for $\mathcal{O}_K$. Replacing one of these α_i by some suitable element will allow us to see $p|\Delta(\mathcal{O}_K)$. Let this suitable element be $\beta \in I \setminus (p)$ then β is contained in every prime of $\mathcal{O}_K$ lying above p but not in (p). If $\beta = m_1a_1 + m_2a_2 + \cdots + m_na_n$,

$m_i \in \mathbb{Z}$ then $\beta \notin (p) \implies$ not all m_i are divisible by p. WLOG, assume $p \nmid m_1$ and set $\Delta(\mathcal{O}_K) = disc(a_1, a_2, \ldots, a_n)$.

Recall that discriminant of an n tuple $(a_i)_{i=1}^n$ is given by $|\sigma_i(a_k)|^2$, which is square of determinant of matrix with given $(i,k)^{th}$ entry where σ_i are embeddings from $K \longrightarrow \mathbb{C}$ and expanding these determinants gives : $(ra_1, a_2, \ldots, a_n) = r^2(a_1, \ldots, a_n)\ \forall\ r \in \mathbb{Q}$.

Now, disc $(\beta, a_2, \ldots, a_n) =$ disc $(m_1 a_1, a_2, \ldots, a_n) = m_1^2$ disc $(a_1, a_2, \ldots, a_n) = m_1^2 \Delta(\mathcal{O}_K)$. Since $p \nmid m_1$ so it will be sufficient to show $p|$ disc $(\beta, a_2, \ldots, a_n)$.

Recall that β is in every prime of $\mathcal{O}_K$ lying above p, so it is in every prime of $\mathcal{O}_L$ lying above p. Every such prime contains p and its intersection with $\mathcal{O}_K$ is a prime lying above p so $\beta \in Q \cap \mathcal{O}_K \subset Q$. Fixing this Q above p, we claim $\sigma(\beta) \in Q$ for each $\sigma \in Aut(L)$. Notice, $\sigma^{-1}Q$ is a prime of $\sigma^{-1}\mathcal{O}_L$ lying over p and contains β. So we have that for all i, $\sigma_i(\beta) \in Q$. It follows that $disc(\beta, a_2, \ldots, a_n) \in Q$ and since this discriminant is in $\mathbb{Z}$, therefore, it is in $Q \cap \mathbb{Z} = p\mathbb{Z}$. □

Since the discriminant of a number field is a non-zero integer, it has only finitely many divisors. Hence, there are only finitely many primes which are ramified in K.

Primes that ramify in $\mathbb{Q}(\sqrt{n})$

Proposition 4.2 ([11, pp. 128–129])**.** *Let $n = d$ which is a fundamental discriminant of the quadratic number field K. Let $\mathcal{O}_K$ be the ring of integers and p be a prime number, then:*

1. *$p|d$, then p is ramified in $\mathcal{O}_K$.*
2. *if $x^2 \equiv d \pmod p$ is solvable, and p is an odd prime then p splits in $\mathcal{O}_K$.*
3. *if $x^2 \equiv d \pmod p$ is not solvable, and p is an odd prime then p is inert in $\mathcal{O}_K$.*

Proof of Proposition 4.2. Let K be a quadratic number field of discriminant d. Let $d \equiv 0 \pmod 4$ then $d = 4d'$. Let $\mathcal{O}_K = \mathbb{Z}[x]/(f(x))$ where $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of $\alpha = \sqrt{d}/2$. Clearly $\alpha = \sqrt{d'}$ and $f(x) = x^2 - d'$. So, $\mathcal{O}_K/(p) = \mathbb{Z}_p[x]/(f(x))$. This ring has no non-zero nilpotent elements $\iff p \nmid d'$ and p is odd, hence p is ramified $\iff p|d$.

Let p be unramified. We know $\mathcal{O}_K/(p)$ is an integral domain $\iff p$ is prime in $\mathcal{O}_K$. So, p splits then $\iff \mathcal{O}_K/(p)$ is not integral domain. This means $x^2 - d'$ is reducible which is possible $\iff d$ is a square modulo p.
Let us now take the case when $d \equiv 1 \pmod 4$. Then p splits $\iff f(x) = x^2 - x + \frac{1-d}{4}$ is reducible $\iff d$ is a square modulo p. □

Now that we know:
if $\left(\frac{d}{p}\right) = 0$ then p is ramified in $\mathcal{O}_K$, if $\left(\frac{d}{p}\right) = 1$ or -1, then p splits completely or is inert in $\mathcal{O}_K$, respectively.

Let us study ramification of primes in cyclotomic extensions.

Primes that ramify in $\mathbb{Q}(\zeta_n)$

Let p be an odd prime. The cyclotomic number field $\mathbb{Q}(\zeta_p)$ has ring of integers $\mathbb{Z}[\zeta_p] = \mathbb{Z}[x]/(\Phi(x))$, where $\Phi(x)$ is the cyclotomic polynomial $\frac{x^p-1}{x-1}$.

Now let us see which primes ramify in K:

Theorem 4.3 ([11])**.** *p is the only prime that ramifies in $\mathbb{Q}(\zeta_p)$.*

Proof of Theorem 4.3. We already know that $\Phi_p(x) = \frac{x^p-1}{x-1} = (x-1)^{p-1}(p)$ and $\mathbb{Z}[\zeta_p]/(p) \cong \mathbb{F}_p/(x-1)^{p-1}$. Clearly this ring is not reduced as it has a non-zero element $(1-\zeta_p)^{p-1} = (p)$, that is, it is 0 in the ring. So, p is ramified.

We now show that if $l \neq p$, then $\Phi_p(x) \in \mathbb{F}_l[x]$ factors into a product of distinct irreducibles. Suppose to the contrary that one of the factors is repeated. Let $\Phi_p(x) = q^2 r$ where both q, r are irreducible polynomials in $\mathbb{F}_l[x]$, then since $\Phi_p(x)$ has a repeated root, it is not separable. However, we see that it is separable by Jacobian criterion, hence, a contradiction. So, $\Phi_p(x) \in \mathbb{F}_l[x]$ is splits into distinct irreducibles and so, l is unramified in K.

Hence, only p ramifies in K. □

We now know the primes that ramify in the quadratic and cyclotomic extensions. Clearly, the prime p that ramifies in the quadratic extension $\mathbb{Q} \subset K = \mathbb{Q}(\sqrt{p})$ also ramifies in $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$. This is because every quadratic extension is contained in a cyclotomic extension (see section 4.4). In this case, if $p \equiv 1 \pmod 4$, then p is the conductor of the extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. Conductor plays an important role in the splitting of a prime, say q in K as it provides a congruence condition for q to be in some particular subgroup of the ray class group. We will study about conductors and ray class group in the coming sections. However, so far, we have only discussed the finite primes of the conductor. To completely understand these conductors, we need to study the infinite primes:

4.2 Infinite Primes

In general, the conductor of a number field $K/\mathbb{Q}$ contains ramified infinite primes. These are embeddings of $K \longrightarrow \mathbb{C}$. In this section, we will closely follow [15, 28], and will study about the infinite primes and their ramification in a quadratic number field.

Definition 4.4. Let K be a number field of degree n. The set of n embeddings from $K \longrightarrow \mathbb{C}$ contain r real embeddings such that if $\sigma : K \longrightarrow \mathbb{C}$ then $Im(\sigma) \subset \mathbb{R}$ and $2s$ complex embeddings such that for each embedding, there is a conjugate. Thus, $n = r + 2s$. The first class of embeddings is called real infinite primes and the second class of embeddings is called complex infinite primes.

Remark. If all embeddings are real or if all infinite primes are real, then K is called totally real, and if all infinite primes are complex then K is called totally complex.

Example 4.5 ([15])**.**

1. $\mathbb{Q}$ has a single real infinite prime ∞.
2. $\mathbb{Q}(\sqrt{-p})$ has single complex infinite prime and no real infinite prime. So, $\mathbb{Q}(\sqrt{-p})$ is totally complex.

3. $\mathbb{Q}(\sqrt{p})$ has two real infinite primes and no complex infinite prime. Hence, $\mathbb{Q}(\sqrt{p})$ is totally real.

Note that ∞ **ramifies** in the extension L/K if for a real prime of K, a complex prime lies above it in L, otherwise it is unramified. So if K is totally complex then all infinite primes are unramified in the extension L/K. Hence, a real infinite prime ∞ is ramified in L/K if $L = \mathbb{Q}(\sqrt{-p})$ and $K = \mathbb{Q}$.

Modulus

Definition 4.6 ([15])**.** A modulus $\mathfrak{m}$ is a formal product of all primes (finite and infinite) in $\mathcal{O}_K$ raised to a power such that the power of infinite primes is 0 and of finite primes is ≤ 1. So, $\mathfrak{m} = \mathfrak{m}_o\mathfrak{m}_\infty$

Let $\mathfrak{m}$ be the modulus of K, then $Cl^{\mathfrak{m}}(\mathcal{O}_K)$ is called the ray class group. This group is always finite. We shall study about this now.

Ray Class Group

We know from section 2 that the ideal class group $Cl(\mathcal{O}_K) = I_K/P_K$, where I_K is the group of all fractional ideals of K and P_K is the group of all principal fractional ideals of K, $P_K \subset I_K$ and I_K is abelian. Let $I_K^{\mathfrak{m}}$ denote the set of all fractional ideals which are coprime to $\mathfrak{m}$ and $P_K^{\mathfrak{m}}$ denote the set of all principal fractional ideals which are coprime to $\mathfrak{m}$. The ray class group of modulus $\mathfrak{m}$ is defined as $Cl^{\mathfrak{m}}(\mathcal{O}_K) = I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. When this modulus is equal to 1, we have our class group defined as $Cl(\mathcal{O}_K) = I_K/P_K$, with I_K as the group of fractional ideals and P_K as the group of principal fractional ideals.

Let us now consider some examples:

Example 4.7. Let $K = \mathbb{Q}$ in these examples unless otherwise specified.

1. Let $\mathfrak{m} = 1$ then, $I_{\mathbb{Q}}$ is the set of all fractional ideals and $P_{\mathbb{Q}}$ is the set of all principal ideals, so $Cl(\mathcal{O}_K) = \mathbb{Z}$.

2. If $\mathfrak{m} = 10$ then, $I_K(10) \cong \left\{\frac{a}{b}\mathbb{Z} | \frac{a}{b} = 1, 3, 7, 9 \pmod{10}\right\}$ and
   $P_K(10) \cong \left\{\frac{a}{b}\mathbb{Z} | \frac{a}{b} = 1, 9 \pmod{10}\right\}$, so $Cl(\mathcal{O}_K) = (\mathbb{Z}/5\mathbb{Z})^*$

3. Let $\mathfrak{m} = \infty$, then $I_K(\infty) = \mathbb{Q} - \{0\}$ and $P_K(\infty) = \left\{\frac{a}{b}\mathbb{Z} | \frac{a}{b} > 0\right\}$ so $Cl(\mathcal{O}_K) = e$.

4. If $\mathfrak{m} = 10\infty$ then, $I_K(10\infty) \cong \left\{\frac{a}{b}\mathbb{Z} | \frac{a}{b} = 1, 3, 7, 9 \pmod{10}\right\}$ and
   $P_K(10\infty) \cong \left\{\frac{a}{b}\mathbb{Z} | 0 < \frac{a}{b} \equiv 1 \pmod{10}\right\}$, so $Cl(\mathcal{O}_K) = (\mathbb{Z}/10\mathbb{Z})^*$.

5. In this case, $K = \mathbb{Q}(\omega)$. Note that $\mathbb{Z}[\sqrt{-3}]$ is a principal ideal domain and and for any element in it, we have the following factorization:
   $\pm\omega^a(1-\omega)^m \prod_{i=1}^n \pi_{m_i}^{t_i}$ where $t_i, m \in \mathbb{Z}$ and $a \in \{0, 1, 2\}$.
   If $\mathfrak{m} = 3\pi_1$ then elements in $I_K^{3\pi_1}$ can be written as a product of principal prime ideals, generated by primary primes which are coprime to $3\pi_1$. So, $I_K^{3\pi_1}$ is the set of all principal

prime ideals that are coprime to $3\pi_1$ i.e. the set of all principal fractional ideals that are primary and coprime to π_1. $P_K^{3\pi_1}$ is the set of all principal fractional ideals that are 1 (mod $3\pi_1$), i.e. the set of all principal fractional ideals that are primary and are congruent to 1 (mod π_1). So, we have $Cl^{3\pi_1}(\mathcal{O}_K)$ is the group of all principal prime ideals that are primary and coprime to π_1, hence, $Cl^{3\pi_1}(\mathcal{O}_K) \cong (O_K/3\pi_1)^\times$

We now have the full knowledge to understand the Artin map, conductors as well as prove our quadratic and cubic reciprocity laws.

4.3 The Artin Symbol

The Artin symbol plays the key role in the splitting of an unramified prime q in a number field K. If the value of the Artin symbol is identity, then q splits in this number field. The Artin symbol refers to a specific Frobenius element in the Galois group of the extension $K/\mathbb{Q}$.

Let $K \subset L$ be an abelian extension. Let q be a prime unramified in K, then Artin symbol tells us whether q is inert or splits in L. Let β be the prime of $\mathcal{O}_L$ lying above q, then the Artin symbol is denoted by

$$\left(\frac{L/K}{\beta}\right)$$

The Artin symbol is the unique element in $Gal(L/K)$. This unique element is the Frobenius automorphism defined as:

Definition 4.8. Let L/K be a Galois extension. If $\mathfrak{p}$ is a prime unramified in K and β is a prime lying above $\mathfrak{p}$ in L then Fr_β is the unique element in the Galois group of L/K such that $\forall \alpha \in \mathcal{O}_L$,

$$Fr_\beta(\alpha) = \alpha^{N(\mathfrak{p})} \pmod{\beta}$$

Recall that for cyclotomic extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $n \in \mathbb{N}$, if $q \in (\mathbb{Z}/n\mathbb{Z})^\times$ is an odd prime and β is a prime above q, then $Fr_\beta(x) = \sigma_q(x)$, where $\sigma_i \in Gal(L/K)$ $\forall 1 \leq i \leq n, (i,n) = 1$. These extensions are ramified at ∞ and prime factors of n. However, the Frobenius element behaves like usual- it is the generator of the Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$ and maps $\zeta \mapsto \zeta^q$. An important property of Frobenius element is its order related to the decomposition of q, which is, as follows:

Theorem 4.9. *Let L/K be a Galois extension then $Fr_\beta \in Gal(L/K)$ has order equal to the inertial degree of β.*

Proof. Consider $Fr_\beta(x) : x \longrightarrow x^{N(p)}$ on the residue field $\mathcal{O}_K/\beta$. We know that $\mathbb{F}_p \subset \mathcal{O}_K/\beta$ and it is the splitting field of $x^{N(p)} - x$. The degree of $\mathbb{F}_p \subset \mathcal{O}_K/\beta$ is the inertial degree f. Since, Artin symbol (Frobenius element) maps to a generator of $Gal(L/K)$, the Artin symbol has order f. □

This theorem tells us that if $Fr_p = id$ then, p splits completely in L/K as $f = 1$, and since the extension is unramified, we have $e = 1$ already.

Having understood the behaviour of the Frobenius element, we are ready to see how the Artin symbol subsumed the quadratic and the cubic residue characters.

Legendre symbol and the Artin symbol:

We know from section 3.2.2 that $g^2 = p^*$. Let us look at it in the light of the Artin symbol. Let q be an unramified primes in $K/\mathbb{Q}$, where $K = \mathbb{Q}(\sqrt{p^*})$ and $p^* = (-1)^{\frac{p-1}{2}}p$, then by coupling with Euler's criterion, we get:

$$\left(\frac{K/\mathbb{Q}}{(q)}\right)(g) \equiv g^q \equiv (g^2)^{\frac{q-1}{2}}.g \equiv \left(\frac{p^*}{q}\right)g \pmod{\mathfrak{q}}$$

Here, $\left(\frac{p^*}{q}\right)$ is the Legendre symbol and $\mathfrak{q}$ is the prime lying above q in $\mathbb{Q}(g)$. If the Artin symbol is identity, then we have $\left(\frac{p^*}{q}\right) = 1$, which means that q splits in K.

Cubic residue symbol and the Artin symbol:

Let q be a primary prime in K, where $K = \mathbb{Q}(\sqrt{-3})$ and let $L = K(p^{1/3})$, then by coupling with definition of the cubic residue character 3.24, we get:

$$\left(\frac{L/K}{(q)}\right)(p) \equiv (p^3)^{\frac{N(q)-1}{3}} \cdot p \equiv \left(\frac{p}{q}\right)_3 \cdot p \pmod{\beta}$$

Here, $\left(\frac{p}{q}\right)_3$ is the cubic residue symbol and β is the prime lying above q in K. If the Artin symbol is identity, then we have $\left(\frac{p}{q}\right)_3 = 1$, which means that q splits in L.

We now know everything to state Artin reciprocity law and prove our reciprocity laws. However, we will first use the Kronecker Weber theorem to prove the law of quadratic reciprocity, as it just uses the fact that an unramified prime q splits in a number field K if and only if Fr_q is identity in K. It also makes it easier to understand the application of Artin reciprocity theorem which we will observe in section 4.5.

4.4 Kronecker Weber Theorem

The Kronecker Weber theorem is a consequence of Artin reciprocity law. It furnishes a simple proof of quadratic reciprocity via restriction on the Frobenius automorphism Fr_q in the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ to the quadratic extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p^*})$, where p, q are distinct odd primes, and $p^* = (-1)^{\frac{p-1}{2}}p$.

The Kronecker-Weber theorem can be stated as:

Theorem 4.10. *If $K/\mathbb{Q}$ is a finite abelian extension, then $K \subset \mathbb{Q}(\zeta_n)$ for some positive integer n.*

The proof uses Artin reciprocity theorem and can be found on [13, 29, p. 6]. We will only prove the following special case:

4.4.1 Kronecker Weber Theorem for Quadratic Extensions

In this section, we will not be constructing the proof of the theorem. Our goal is to find the unique quadratic subextension$K \subset \mathbb{Q}(\zeta_p)$ of conductor p, where p is an odd prime. The definition of conductor of $K/\mathbb{Q}$ that we are using in this section is as follows:

The smallest integer n such that $K \subset \mathbb{Q}(\zeta_n)$ is called the *conductor of the extension* $K/\mathbb{Q}$.

The Kronecker Weber theorem for quadratic extensions says that if $p \equiv 1 \pmod 4$ then $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ and if $p \equiv 3 \pmod 4$ then $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$. But why is that true?

Theorem 4.11. *There is a unique quadratic subfield* $K = \mathbb{Q}(\sqrt{\pm p}) \subset \mathbb{Q}(\zeta_p)$ *such that* $K = \mathbb{Q}(\sqrt{p})$ *if* $p \equiv 1 \pmod 4$ *and* $K = \mathbb{Q}(\sqrt{-p})$ *if* $p \equiv 3 \pmod 4$.

Proof. Let ζ be the p^{th} root of unity, where p is an odd prime.

Consider the extension $\mathbb{Q} \subset L = \mathbb{Q}(\zeta_p)$. Let $G = Gal(L/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^*$ and the order of G is $p-1$. Clearly, $2|(p-1)$ for p an odd prime so, there is subgroup of G with order 2, which means that there exists a subextension of L of degree 2 over $\mathbb{Q}$. Since G is cyclic, let it be generated by a generator g, then $G = 1, g, g^2, \ldots, g^{p-2}$. Since every subgroup of a cyclic group is cyclic, so the subgroup of order 2 is also cyclic. Let H be a subgroup of G such that the index of H in G is 2 then H has order $\frac{p-1}{2}$.

Recall that there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p. So, H has $\frac{p-1}{2}$ elements which are quadratic residues and G/H has 2 elements. All index 2 subgroups are normal, so the subextension $\mathbb{Q} \subset K$ of L is normal. This means K is a primitive extension. Let us find out the primitive element.

We have seen that the only prime that ramifies in L is p, so the prime that ramifies in K must also be p, but K is the extension of degree 2 over $\mathbb{Q}$, hence $K = \mathbb{Q}(\sqrt{\pm p})$.

We want to determine when $K = \mathbb{Q}(\sqrt{p})$ and when $\mathbb{Q}(\sqrt{-p})$. So, the determinant of K is p when it is $1 \pmod 4$ and $4p$ when $p \equiv 2, 3 \pmod 4$. So, in the latter case, 2 is ramified as the discriminant of K is $4p$. Here, we claimed that the only prime that ramifies in K is p, so we take $p^* \equiv 1 \pmod 4$ where $p^* = (-1)^{\frac{p-1}{2}} p$. □

Another approach: We know that $g = \sum_t \left(\frac{t}{p}\right) \zeta^t$ is the Gauss sum with respect to 1, so the square of g^2 is $(-1)^{\frac{p-1}{2}} p$, which is p^*. Clearly g is contained in $\mathbb{Q}(\zeta_p)$, hence, we have $\mathbb{Q}(g) \subset \mathbb{Q}(\zeta_p)$.

4.4.2 Law of Quadratic Reciprocity

We can now prove the law of quadratic reciprocity. Let $L = \mathbb{Q}(\zeta_p)$, where p is an odd prime, and $G = Gal(L/\mathbb{Q})$. Let $q \neq p$ be an odd prime. We will denote $(-1)^{\frac{p-1}{2}} = p^* \equiv 1 \pmod 4$ and $K = \mathbb{Q}(\sqrt{p^*})$. We will show the following:

Proposition 4.12. $\left(\frac{p^*}{q}\right) = 1 \iff$ *q splits completely in* $\mathcal{O}_K$.

Proof of Theorem 4.12. Recall that this is just our proposition 4.2. We know that $p^* \equiv 1 \pmod 4$ and the ring of integers of K is $\mathbb{Z}\left[\frac{1+\sqrt{p^*}}{2}\right]$. Now, we know that the distinct odd prime q, which is unramified in the extension $K/\mathbb{Q}$ splits in $\mathcal{O}_K \iff x^2 - x - \left(\frac{1-p^*}{4}\right)$ is reducible in $\mathbb{F}_q \iff \frac{p^*}{4}$ is a square modulo $q \iff p$ is a square modulo q i.e., $\left(\frac{p^*}{q}\right) = 1$. □

Proposition 4.13. *A distinct odd prime* q *splits in* $\mathcal{O}_K \iff Fr_q \in Gal(L/\mathbb{Q})$ *fixes* $K \iff \left(\frac{q}{p}\right) = 1$.

Proof of Proposition 4.13. Consider an odd prime q such that q splits in $\mathcal{O}_K$. Let $Fr_q \in G$. Let $\mathfrak{q}$ be a prime ideal containing (q) in $\mathcal{O}_L$. Then consider $Fr_q \in Gal((\mathcal{O}_L/\mathfrak{q})/\mathbb{F}_q)$ such that $x \longrightarrow x^q \pmod{\mathfrak{q}}$. So, we have $Fr_q \in G$ and we restrict it to K. Now, q splits in $K \iff Fr_q = id$ on $K \iff x \longrightarrow x^q \pmod{\mathfrak{q}} = x \ \forall\, x \in \mathcal{O}_K$.

Since, $Fr_q \in G$ fixes $K \iff q \in Gal(L/K)$ and we already know that this is the group of all the residues modulo p. So, $\left(\frac{q}{p}\right) = 1$. □

Theorem 4.14. *Let p, q be distinct odd primes and $K = \mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{\frac{p-1}{2}} p$. Then*

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

Proof of Theorem 4.14. Combining propositions 4.12 and 4.13, we proved that $\left(\frac{p^*}{q}\right) = 1 = \left(\frac{q}{p}\right)$, which proves the law of quadratic reciprocity. □

Recall our treatment of quadratic reciprocity using Gauss sums in section 3.2.2. We seem to have figured the correct intuition but it is still a bit dissatisfying. Let us reconsider it. Recall, that $K = \mathbb{Q}(g)$ and we had $g^2 = p^*$ in $\mathcal{O}_K/(q)$, where q is an odd prime distinct from p. We raised g^q and proceeded by comparing what it would give from relation $g^2 = p^*$ vs its definition. The idea behind doing our first step is precisely Frobenius element being identity.

$Fr_q(g) = g^q \equiv (g^2)^{\frac{q-1}{2}} g \pmod{q}$. However, since Fr_q is identity, we have $g^q = g$. So, by Euler's criterion, $g \equiv (g^2)^{\frac{q-1}{2}} g \pmod{q} \implies 1 = \equiv (g^2)^{\frac{q-1}{2}} \pmod{q}$, which clearly means the Legendre symbol is 1, hence q splits in $K = \mathbb{Q}(g)$. And we are done. We have now built the correct intuition for our treatment of quadratic reciprocity in section 3. Thence, we shall now study Artin reciprocity and understand how our reciprocity laws are just a special case of it.

4.5 Reciprocity Laws via Artin Reciprocity

To unlock the power of Artin reciprocity, we will define the Artin map in terms of the Artin symbol. Let L/K be an abelian extension and $\mathfrak{p}$ be a prime unramified in K, we denote the Artin symbol by:

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in Gal(L/K)$$

which extends multiplicatively to give $\phi_{L/K} : I_K^{\mathfrak{f}} \longrightarrow Gal(L/K)$, called the Artin map where $\mathfrak{f}$ is the conductor of the extension L/K. A conductor of an extension L/K is defined as the smallest modulus $\mathfrak{m}$ such that $P_K^{\mathfrak{f}} \subset ker(\phi_{L/K})$[12].

Theorem 4.15 ([7, p. 62])**.** *The Artin map $\phi_{L/K} : I_K^{\mathfrak{f}} \longrightarrow Gal(L/K)$, is surjective and its kernel contains $P_K^{\mathfrak{f}}$. Thus, the Artin map gives an explicit isomorphism between the class group $\frac{(I_K^{\mathfrak{f}}/P_K^{\mathfrak{f}})}{ker\phi_{L/K}}$ and the Galois group $Gal(L/K)$.*

Proof of Theorem 4.15. The proof of Artin reciprocity requires extensive class field theory and is well beyond the scope of the thesis. We direct the curious readers to [12] for the proof of the theorem and their questions. □

$(I_K^{\mathfrak{f}}/P_K^{\mathfrak{f}}) = Cl^{\mathfrak{f}}(\mathcal{O}_K)$ is called the ray class group[24]. L here is referred to as the Hilbert class field of the number field K. It is the maximal unramified extension of K. It is central to Class field theory, which is the study of all such class fields. The extension L/K is finite and is isomorphic to $Cl(\mathcal{O}_K)$ which is the ideal class group.

Corollary 4.16 ([8, p. 109])**.** *Let L be the Hilbert class field of a number field K, and p be a prime ideal of K. Then p splits completely in $L \iff p$ is a principal ideal.*

Proof of Corollary 4.16. p splits completely in $L \iff \left(\frac{L/K}{p}\right) = 1 \iff p$ is trivial in $Cl(\mathcal{O}_K) \iff p$ is the principal ideal. □

We use this concept exclusively in section 5. Proof of this is by Artin reciprocity law (see [12]). Artin reciprocity, roughly speaking, predicts the splitting of an unramified prime p in a number field K via the unique Frobenius element Fr_p determined by some congruence condition. This condition is determined by which coset for a subgroup $H \subset Cl_K^{\mathfrak{f}}$ of index n the ideal p lies in. Loosely speaking, this subgroup H corresponds to the group of n^{th} residues modulo $\mathfrak{f}$.

This gives a general framework to prove these laws. In the next two subsections, we shall apply this argument to quadratic reciprocity law and cubic reciprocity law.

Dissecting the proof of Quadratic Reciprocity Law

Now that we have a clear picture of Artin reciprocity, let us keep our promise of seeing how our proof in section 4.4.1 helps us understand the application of Artin reciprocity to the law of quadratic reciprocity.

Let p be an odd prime. Let $p^* = (-1)^{\frac{p-1}{2}}p$ and $K = \mathbb{Q}(\sqrt{p^*})$ be a quadratic number field. Let q be an odd prime distinct from p. q is unramified in the extension $K/\mathbb{Q}$. Whether or not q splits in the extension, is given by whether $\phi_{K/\mathbb{Q}} = id$ map. By Artin reciprocity, if $\phi_{k/\mathbb{Q}} = id$ means Fr_q is identity on $K/\mathbb{Q}$, that is, $Fr_q(x) \equiv x \pmod{\mathfrak{f}}\ \forall x \in \mathcal{O}_K$, where $\mathfrak{f}$ is the ideal of $\mathcal{O}_K$ called the conductor. In this case, $\mathfrak{f} = p$ as $p^* \equiv 1 \pmod 4$, so p is the only prime ramified in the extension $K/\mathbb{Q}$. So, to confirm if Fr_q is identity, we need to see if $q \in$ some subgroup of index 2 in $Cl(\mathcal{O}_K) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. The only such subgroup is the group of squares, so q is a square modulo p, hence, $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$.

Since we are now familiar with the whole argument of applying Artin reciprocity theorem to the reciprocity laws, we can now venture forth to the law of cubic reciprocity by motivating it through the following section:

4.5.1 Law of Cubic Reciprocity

Recall the arithmetic of the ring $\mathbb{Z}[\omega]$ from section 3.4.1. We shall now follow the same argument as we did in section 4.5 and prove the law of cubic reciprocity. Note that *primary primes* here refers to a prime congruent to 1 (mod 3).

[24] We mentioned this earlier, see section 4.2.

Theorem 4.17 ([7, p. 63]). *Suppose π_1 and π_2 are distinct primes in $\mathcal{O}_K$, both coprime to 3. Then there exists a unique unit multiple π_2^* of π_2 which is congruent to 1 (mod 3) and we have:*

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

Proof of Theorem 4.17. We have shown already that there are 6 units in $\mathcal{O}_K$ so each prime has 6 unit multiples and since they are all distinct modulo 3, so we have shown the first part.

Let $K = \mathbb{Q}(\omega)$ and $L = K(\pi_1^{1/3})$. The conductor of L/K is $3\pi_1$. Since, K is complex, so we know there are no real infinite primes. Let us apply Artin reciprocity and repeat the argument we presented for quadratic reciprocity. The value of ϕ_{π_2} or of the Artin symbol[25] $\phi_{L/K}$ is given by some congruence condition modulo $3\pi_1$. Let us determine the class group given by $I_K^{3\pi_1}/P_K^{3\pi_1}$. Note that $\mathbb{Z}[\omega]$ is a Euclidean domain and hence, a principal ideal domain. The elements in $I_K^{3\pi_1}$ are principal fractional ideals generated by primary primes coprime to π_1. Elements in $P_K^{3\pi_1}$ are principal fractional ideals generated by primary primes that are congruent to 1 (mod π_1). From Example 5, the class group of conductor $3\pi_1$ is $(\mathcal{O}_K/\pi_1)^*$. Using Artin reciprocity, to see if π_2 is a cubic residue modulo π_1, we see if ϕ_{π_2} is 1. This depends on whether π_2^* is in the quotient group of $(\mathcal{O}_K/\pi_1)^*$ of index 3 and only such cyclic subgroup is the subgroup of cubes which is $Gal(L/K)$. Thus far, we have proved that $Fr_{\pi_2} = 1$ in $Gal(L/K) \iff \left(\frac{\pi_2^*}{\pi_1}\right)_3 = 1$. So, π_2^* splits in $L \iff \pi_1^3 \equiv 1 \pmod{\pi_2} \iff \left(\frac{\pi_1}{\pi_2}\right)_3 = 1$. Hence, we get:

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

□

5 Primes of the form $x^2 + ny^2$

This section follows [8, 30, 31]. The goal of this section is to apply the knowledge we gained so far to investigate:

Let $n > 0$ be an integer then, for which primes is $p = x^2 + ny^2$ solvable?

The answer is provided by the following theorem:

Theorem 5.1 ([8, p. 180]). *Let $n > 0$ be an integer, then $\exists$ a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that for prime p, $p \nmid n$, $p \nmid$ discriminant of f_n,*

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \\ f_n(x) \equiv 0 \pmod{p} \text{ has deg } (f_n) \text{ integer solutions.} \end{cases}$$

Moreover $f_n(x)$ is the minimal polynomial of an algebraic integer α such that $L = K(\alpha)$ is the ring class field of order $\mathbb{Z}[\sqrt{-n}]$ in the quadratic number field $\mathbb{Q}(\sqrt{-n})$. If $f_n(x)$ is any degree $h(-4n)$ monic irreducible polynomial over $\mathbb{Z}$ then the above equivalence holds and it is the minimal polynomial of a primitive element of the aforementioned ring class field.

[25] This refers to the cubic residue symbol of π_2^* over π_1

Using Theorem 5.1, we can find the values of p such that $p = x^2 + ny^2$ solvable for infinitely many n but we will not prove it in this thesis. We refer our readers to [8] for a detailed treatment of this topic.

We divide our investigation into several parts. In the first part, we prove the following special case of our Theorem 5.1:

Theorem 5.2 ([8])**.** *Let $n\rangle 0$ be a square-free integer such that $n \not\equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{-n})$. There is a monic irreducible polynomial $f_n(x)$ with integer coefficients of degree equal to the class number of discriminant*[26] *D such that for an odd prime p, $p \nmid n$ and $p \nmid$ discriminant of $f_n(x)$ then*

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \text{ and } f_n(x) \equiv 0 \pmod p \text{ is solvable.}$$

Moreover, $f_n(x)$ is the minimal polynomial of an algebraic integer α such that $L = K(\alpha)$ is the Hilbert class field of K.

To prove this, recall our discussion of Artin reciprocity[27]. We discussed the Hilbert class field L of the number field K, where an unramified odd prime q splits completely. Note that:

If no elements of a number field K ramify in the extension L of K then L/K is called an unramified extension.

Definition 5.3 ([8, p. 180])**.** The Hilbert class field is the maximal unramified abelian extension of K.

Throughout this section, we shall denote the Hilbert class field of a number field K by L. The primes that can be represented by the form $x^2 + ny^2$ are unramified in L/K, where $K = \mathbb{Q}(\sqrt{-n})$ and split completely in L. This is proved by the following theorem:

Theorem 5.4 ([8, p. 110])**.** *Let L be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$. Assume that n is square-free and $\not\equiv 3 \pmod 4$. The ring of integers of $K = \mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. If p is an odd prime, $p \nmid n$, then $p = x^2 + ny^2 \iff p$ splits completely in L.*

Proof of Theorem 5.4. We shall prove this theorem in three parts:

The first step is to prove:

$p = x^2 + ny^2 \iff (p) = \mathfrak{p}\overline{\mathfrak{p}}$, and $\mathfrak{p}$ is a principal ideal in $\mathcal{O}_K$.

For the first equivalence, let p be an unramified prime in K and suppose $p = x^2 + ny^2 = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$. Set $\mathfrak{p} = \langle (x + \sqrt{-n}y)\rangle$, then the prime factorization of p in $\mathcal{O}_K$ is $p = \mathfrak{p}\overline{\mathfrak{p}}$ (if otherwise, then p will be ramified in the K.). Since, p is unramified so $\mathfrak{p} \neq \overline{\mathfrak{p}}$ and $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$.

Conversely, suppose that if $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, where $\mathfrak{p}$ is principal then $(p) = \langle (x^2 + ny^2)\rangle \implies p = x^2 + ny^2$.

The second step is to prove:

$p = x^2 + ny^2 \iff (p) = \mathfrak{p}\overline{\mathfrak{p}}$, and $\mathfrak{p}$ splits completely in L.

[26] In this case, the discriminant D is equal to $-4n$.

[27] see theorem 4.15.

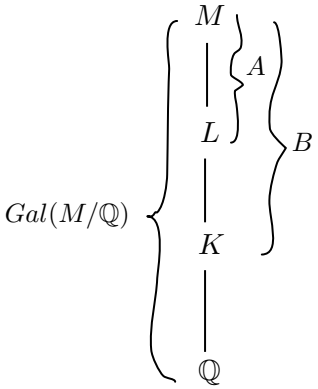
From corollary 4.16 we get that $\mathfrak{p}$ splits completely in L $\iff$ $\mathfrak{p}$ is a principal ideal so the second equivalence follows immediately: $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, and $\mathfrak{p}$ is principal in $\mathcal{O}_K \iff (p) = \mathfrak{p}\overline{\mathfrak{p}}$, and $\mathfrak{p}$ splits completely in L.

At last, we have to prove that:
$(p) = \mathfrak{p}\overline{\mathfrak{p}}$, and $\mathfrak{p}$ splits completely in $L \iff p$ splits completely in L.

To show this, we will need the following lemma:

Lemma 5.5 ([8, pp. 110–111])**.** *Let L be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$ and τ be the complex conjugation. Then $\tau(L) = L$ and consequently L is Galois over $\mathbb{Q}$*

Proof of Lemma 5.5. Notice that $\tau(L)$ is an unramified abelian extension of K. Since L is the maximal abelian extension of K, so $\tau(L) \subset L$. However, $[\tau(L) : K] = [L : K]$, so $\tau(L) = L$. To show that L is Galois over $\mathbb{Q}$, let $L \subset M$ and $G = Gal(M/\mathbb{Q})$. Let A, B be subgroups of G that fix L, K respectively.



We want to show that $\tau A = A\tau \implies A$ is normal subgroup of G. Then by fundamental theorem of Galois theory, G/B corresponds to $Gal(K/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z}) = \langle 1, \tau \rangle$. This means that every element in G is of the form $b, b\tau$ where $b \in B$. Since L/K is Galois, A is the normal subgroup of B. Hence, A is normal subgroup of G so L is Galois over $\mathbb{Q}$. □

We have that $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ and $\mathfrak{p}$ splits completely in L. Since p splits completely in $\mathcal{O}_K$ and $\mathfrak{p}$ containing p splits completely in $\mathcal{O}_L$, therefore, p splits completely in L. □

The primes that split in L satisfy certain conditions. One of them is that all such primes are quadratic residue modulo d, which is the discriminant of K. Another condition is that $f(x)$ modulo p splits, where $f(x)$ is the minimal polynomial of some algebraic integer $\alpha \in L$ such that $L = K(\alpha) = K[x]/(f(x))$. Hence, we have an elementary way of stating the splitting of p in the Hilbert class field L. This is made more clear by Proposition 5.6. Before proving this proposition, we need to know the minimal polynomial of an algebraic integer α.

Proposition 5.6 ([8, p. 111])**.** *Let $K = \mathbb{Q}(\sqrt{-n})$ and L be a finite extension of K, such that $L/\mathbb{Q}$ is Galois. Then there exists an algebraic integer α such that $L = K(\alpha)$. Let $f(x) \in \mathbb{Z}[x]$ be monic minimal polynomial of α and an odd prime $p \nmid$ discriminant of $f(x)$, then:*

p splits completely in L $\iff \left(\frac{d}{p}\right) = 1$ *and* $f(x) \equiv 0 \pmod{p}$ *has deg (f) integer solutions.*

Proof of Proposition 5.6. We know that $L/\mathbb{Q}$ is Galois by lemma 5.5. $L \cap \mathbb{R}$ is the field fixed by complex conjugation. So we have $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$. Let $\alpha \in L \cap \mathbb{R}$, then $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$ such that $f(x)$ is reducible over K. Then $f(x) = f_1(x)f_2(x)\dots f_n(x)$, where each $f_i(x)$ is irreducible over K. Since $L/\mathbb{Q}$ is Galois, therefore $f(x)$ splits completely in L. This means that there exists some i such that $f_i(\alpha) = 0$. WLOG, let $f_1(x)$ be such that it is 0 at α. Let M be the splitting field of $f_1(x)$. Then we have $M = K(\alpha)$. Let τ be a complex conjugation, then M is fixed under the action of τ. So, by lemma 5.5, the extension $M/\mathbb{Q}$ is Galois. Hence, $f(x)$ splits completely in M which means that $[M : \mathbb{Q}] \rangle deg(f(x))$. Note that since M is the splitting field of $f_1(x)$, and $f(x)$ splits completely in M so, $M \subset L$. We know that $[L : L \cap \mathbb{R}] = [K : \mathbb{Q}] = 2$. So, we have $M = L$. We also have that $[L : \mathbb{Q}] = \deg\, f_1(x) \langle \deg\, f(x)$. So, $[L \cap \mathbb{R} : \mathbb{Q}] = [L : \mathbb{K}]$.

Therefore, if $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ satisfied $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$ then $L = K(\alpha)$. We already have that $f(x)$ is the minimal polynomial of α over K. So, let p be a prime that does not divide the discriminant of $f(x)$, then $f(x) \equiv f_1(x)\dots f_n(x) \pmod{p}$, so p is unramified in L. Therefore, $\left(\frac{d}{p}\right) = 1$. Since p splits completely in L, we let $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/\mathfrak{p}$. So, $f(x)$ is separable over $\mathbb{Z}/p\mathbb{Z}$ implies that it is also separable over $\mathcal{O}_K/\mathfrak{p}$. Thus, $\mathfrak{p}$ splits completely in $L \iff f(x) \equiv 0 \pmod{\mathfrak{p}}$ is solvable in $\mathcal{O}_K \iff f(x) \equiv 0 \pmod{p}$ is solvable in $\mathbb{Z}$. □

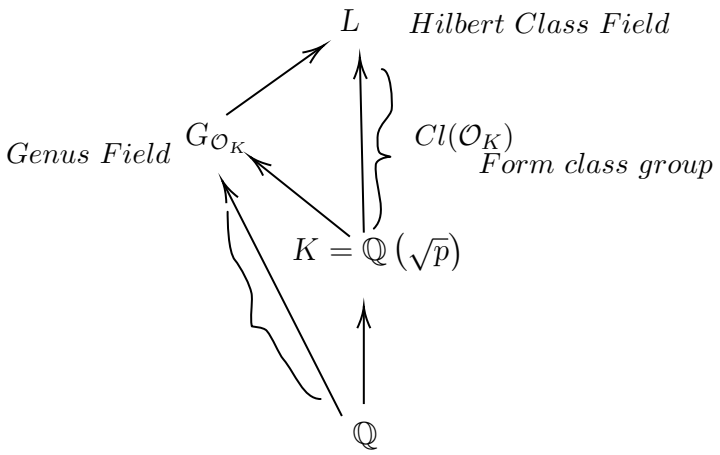
We are now ready to prove our theorem 5.2.

Proof of Theorem 5.2. By combining our Propositions 5.4 and 5.6, we have the required equivalence. The degree of $f_n(x)$ is equal to the class number of $\mathcal{O}_K$ since $f_n(x)$ is the minimal polynomial of $\alpha \in L$, therefore, $[L : K] = \deg\, f_n(x)$. By theorem 4.15, degree of $f_n(x) = [L : K] = |Cl(\mathcal{O}_K)|$. □

We have completed the first part towards our investigation of primes which can be represented by the form $x^2 + ny^2$. Note that our n is constrained to be square-free and $\not\equiv 3 \pmod{4}$.

As evident by Theorem 5.1 and its special case Theorem 5.2, Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$ plays a central role in finding the congruence conditions on p to be represented by the form $x^2 + ny^2$. However, we first need to determine the Hilbert class field. An important step in this direction is the introduction of Genus fields. This is the second part of our investigation of prime p such that $p = x^2 + ny^2$ is solvable.

Consider the following diagram:



Let K be a number field. The genus field $G_{\mathcal{O}_K}$ is the largest abelian subextension of the Hilbert class field such that $Gal(G_{\mathcal{O}_K}/\mathbb{Q})$ is abelian. The genus number is defined as the degree of the extension $[L : G_{\mathcal{O}_K}]$. It is a divisor of the class number[28]. Let us explicitly state the definition of the genus field:

Definition 5.7 ([8, p. 121])**.** Let K be a number field of discriminant d and let μ be number of primes dividing K, such that $p_1, p_2, \cdots p_r$ be odd primes dividing d and $\mu = r$ or $r+1$ according to $d \equiv 0 \pmod 4$ or $d \equiv 1 \pmod 4$. Let $p_i^* = (-1)^{\frac{p-1}{2}} p_i$, then the genus field is the maximal unramified extension of K which is abelian over $\mathbb{Q}$ and is given by $K(\sqrt{p_1^*}, \cdots, \sqrt{p_r^*})$, where r is number of odd primes.

We shall be discussing three cases of primes of the form $x^2 + ny^2$ for $n = 5, 27, 26$. We shall calculate the genus field and the Hilbert class field of the number field $\mathbb{Q}(\sqrt{-n})$ and find the conditions on p such that $p = x^2 + ny^2$ is solvable for $n = 5, 27, 26$.

5.1 Case of $p = x^2 + 5y^2$

The discriminant of the quadratic form $x^2 + 5y^2$ is -20 and all primes which are quadratic residue modulo 20 are such that $\left(\frac{-5}{p}\right) = 1 \iff p \equiv 1, 3, 7, 9 \pmod{20}$.

Given the discriminant -20, we find that there are two reduced form of discriminant -20, given by $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. Hence, the order of class group is 2.

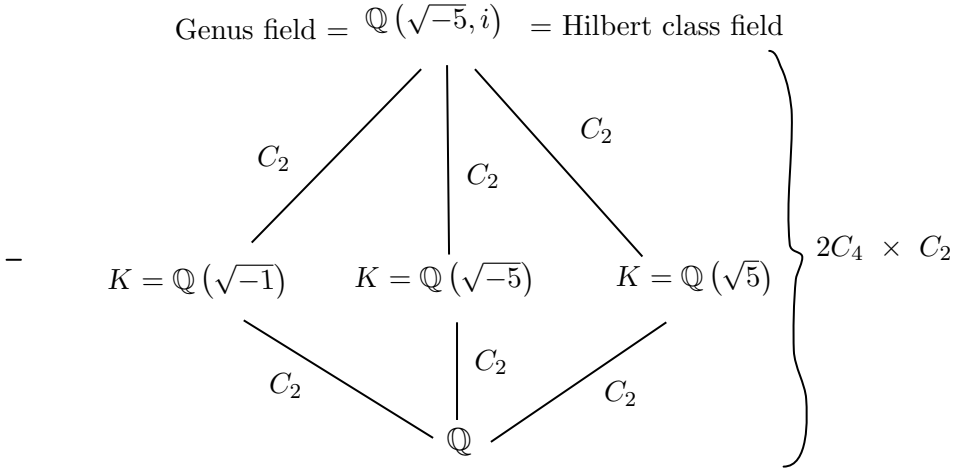
Notice that not all primes which are quadratic residue modulo 20 are represented by $x^2 + 5y^2$. For example: $p = 23 = x^2 + 5y^2$ has no integer solutions. To find out which congruence class modulo 20 is represented by $x^2 + 5y^2$, we first begin the quest for Hilbert class field of $\mathbb{Q}(\sqrt{-5})$. Let $K = \mathbb{Q}(\sqrt{-5})$ and L be the Hilbert class field of K. Let $L = K(\alpha)$, where α is an algebraic integer. Claim: $L = K(\alpha) = K(i)$.

Since the degree of the extension $[L : K] = 2$ so if $K(i)$ is an unramified abelian extension then it will be the maximal unramified abelian extension. We shall prove that $K(i)/K$ is an unramified abelian extension.

Since $[K(i) : K) = 2]$, hence the extension is abelian as it is normal and the Galois group is C_2. We shall now prove that the extension is unramified.

[28]To get an overview of the algorithm to calculate the genus number, we refer our readers to [47].

We have$L = K(i) = \mathbb{Q}(i, \sqrt{-5})$ and $\mathbb{Q}(\sqrt{5}) \subset L$. Let $\mathbb{Q}(\sqrt{5}) = M$. Observe the diagram below:



To prove that the primes of K are unramified in L, we check that all primes in $\mathbb{Q}$ are unramified in $\mathbb{Q}(i)$. We do this since only 2 is ramified in $\mathbb{Q}(i)/\mathbb{Q}$ and the compositum of these fields with $\mathbb{Q}(\sqrt{-5})$ yields L which is ramified only at primes above 2. The discriminant of $\mathbb{Q}(i)$ is -4, and the only prime that divides this discriminant is 2. Hence, all primes except 2 are ramified in $\mathbb{Q}(i)$. If primes lying above 2 in K are unramified in L then the extension is unramified. Hence, we need to check that $\mathfrak{p}$, a prime in $\mathbb{Q}(\sqrt{-5})$ lying above 2 is unramified in L. We know that $(2) = (2, 1 + \sqrt{-5})^2$ in K. Clearly 2 is ramified in K. Now, consider the ramification index of $\mathfrak{p} \in \mathcal{O}_K, \mathfrak{q} \in \mathcal{O}_M$ in L and of $2 \in \mathbb{Q}$ in M, K, L as: $e_L(\mathfrak{p}), e_L(\mathfrak{q}), e_M(2), e_K(2), e_L(2)$. We will apply the tower law on the ramification index to show that for $\mathfrak{p} = (2, 1 + \sqrt{-5})$, we have $e_L(\mathfrak{p}) = 1$. We know that, $e_K(2) = 2$ so if we show that in $e_L(2) = e_L(\mathfrak{p})e_K(2)$, $e_L(2) = 2$, then we are done.

Consider $e_L(2) = e_M(2)e_L(\mathfrak{q})$. The discriminant of $M = \mathbb{Q}(\sqrt{5})$ is 5 which is not divisible by 2 and hence, $e_M(2) = 1$. So, $e_L(2) = e_L(\mathfrak{q}) \leq 2$ as $[L : M] = 2$ and $e_L(2) = 2$, therefore, $e_L(\mathfrak{p}) = 1$. Hence, $\mathfrak{p}$ lying above 2 in K is unramified in L. Thus the extension L/K is unramified.

Since, we have shown that L is an abelian unramified extension of degree 2, hence, L is the Hilbert class field of K.

The Hilbert class field is a biquadratic field with $-5, -1$ as distinct and squarefree integers, we can express α which is the primitive element of $L = K(\alpha)$ as $\frac{1+\sqrt{5}}{2}$ (see [46]. The minimal polynomial of α is $f(x) = (2x-1)^2 - 5 = 4x^2 - 4 - 4xy = x^2 - x - 1$. So, $f(x) \equiv 0 \pmod{p}$ has a solution $\iff \left(\frac{5}{p}\right) = 1 \iff p \equiv 1, 4 \pmod{5}$.

We know that the probable primes which can be expressed in the form $x^2 + 5y^2$ are given by $\left(\frac{-20}{p}\right) = 1$. So, we have: $(-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = 1$. Since for $f_n(x) \pmod{p}$ to be solvable we have $p \equiv 1, 4 \pmod{5}$, therefore, $\left(\frac{-20}{p}\right) = 1$ holds $\iff p \equiv 1, 9 \pmod{20}$. We can rewrite this in terms of our theorem 5.1 as: $p = x^2 + 5y^2 \iff p \equiv 1, 3, 7, 9 \pmod{20}$ and $f(x)$ of degree $h(d)$ has a solution modulo p.

Now that we know the Hilbert class field of K, let us find the genus field $G_{\mathcal{O}_K}$ of K. The discriminant of K is -20 and there is only one odd prime dividing the discriminant of K,

which is 5. So, the genus field is $\mathbb{Q}(\sqrt{-5}, \sqrt{5})$ which is just the Hilbert class field of K.

Genus fields make it easier for us to compute the Hilbert class field. For instance, in this case, the genus field is the Hilbert class field and Proposition 5.6 provides us with a straightforward way to compute it.

In this case, we initially had two equivalence classes. The class containing the principal quadratic form corresponds to the principal fractional ideal which is generated by $\langle 9 \pmod{20} \rangle$. While the class containing the other reduced form corrsponds to the coset of $\langle 9 \pmod{20} \rangle$ in the class group. This case encapsulates the essence of genus theory - the classification of forms into classes based on the primes they represent in $(\mathbb{Z}/d\mathbb{Z})$, where $d = 4n$ is the discriminant of $Q(\sqrt{-n})$. Two forms that represent same values $\pmod{d}$ belong to the same *genus*. Moreover, the genus containing the principal quadratic form is called the *principal genus*. We saw in this case that the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ is also the genus field of $\mathbb{Q}(\sqrt{-5})$. This is because there is only one class containing the principal quadratic form lying in the principal genus[29]. One might ponder what may happen if the principal genus has more than one form?

5.2 Case of $p = x^2 + 27y^2$

The discriminant of $x^2 + 27y^2$ is -108. There are 3 distinct equivalence classes corresponding to this discriminant, given by: $x^2 + 27y^2$ and $4x^2 \pm 2xy + 7y^2$. The forms $x^2 + 27y^2$ and $4x^2 + 2xy + 7y^2$ lie in the same genus since they represent primes p such that $p \equiv 1 \pmod 3$ by quadratic reciprocity. This makes us question as to for what primes is $p = x^2 + 27y^2$ solvable. Notice that $13 \equiv 1 \pmod 3$ but $x^2 + 27y^2 = 13$ is not solvable.

Let $K = \mathbb{Q}(\omega)$ and L be the Hilbert class field of K. The Galois group of L/K is of order 3 as it is isomorphic to the form class group, which has class number 3. $Gal(L/\mathbb{Q})$ has order[30] 6. Let p be a prime unramified in the extension L/K. If p splits in L, then $p = x^2 + 27y^2$. The ring of integers of the number field K is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and the order is $\mathbb{Z}[\sqrt{-27}]$. The conductor of the order $\mathbb{Z}[\sqrt{-27}] \subset \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is 6.

Let M be a cubic extension of K. We want to show that the Hilbert class field $L = K(2^{1/3}) = M$. We know that for M to be L, it has to satisfy the following properties: $[L : K] = 3$ and $[L : \mathbb{Q}] = 6$. Moreover $Gal(L/\mathbb{Q}) \cong S_3$ as the discriminant of the polynomial $x^3 - m$ is $-4 * 27 * m^2$ which is not a square and hence, the Galois group is S_3. Since the conductor of L/K is 6, the primes of K which ramify in L must divide 6.

We let M be a cubic extension of K and $Gal(M/K) \cong S_3$. The elements of S_3 are $\{1, \sigma, \sigma^2\tau, \tau\sigma, \tau\sigma^2\}$. Let $\tau \in Gal(M/K)$ be the complex conjugation. If σ generates the group $Gal(L/K)$ then $\tau\sigma\tau^{-1} = \sigma^{-1}$ since $Gal(L/\mathbb{Q}) \cong S_3$. By proposition 5.6, we can find a real algebraic integer α such that $M = K(\alpha)$ is a cubic extension. Let $x_i \in M$, then $x_i = \alpha + \omega^i\sigma^{-1}(\alpha) + \omega^{2i}\sigma^{-2}(\alpha)$ for $i = 0, 1, 2$. Now $\sigma(x_i) = \sigma(\alpha) + \omega^i(\alpha) + \omega^{2i}\sigma^{-1}(\alpha) = \omega_i x_i$. Now $\tau(x_i) = \tau(\alpha) + \omega^i\tau\sigma^{-1}(\alpha) + \tau\omega^{2i}\sigma^{-2}(\alpha) = x_i$, so, x_i is real. Hence, all x_i are real for $i = 0, 1, 2$. Note that $\sigma(x_0) = \omega^0 x_0 = x_0$ and $\tau(x_0) = x_0$. Similarly, $\sigma(x_1^3) = x_1^3$ and

[29] In this example, we have only scratched the surface of genus theory. For a detailed intuitive account of genus theory, our readers may refer to [8].

[30] By tower law, $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}]$, and we already know that $[K : \mathbb{Q}] = 2$.

$\sigma(x_2^3) = x_2^3$. So, x_0, x_1^3, x_2^3 are all integers. WLOG, let $x_1 \neq 0$ and $M = K(x_1)$. Recall that $[M : K] = 3$ as $[M : \mathbb{Q}] = 6$ (being isomorphic to S_3). If $x_1 \in K$ then $M \neq K(x_1)$. Since x_1 is real, then $x_1 \in K \implies x_1$ is an integer but then σ fixes x_1 and that contradicts the fact that $\sigma(x_1) = \omega x_1$ and x_1 is non-zero. So, we let $m = x_1^3 \in \mathbb{Z}$ such that $M = K(x_1) = K(m^{1/3})$. Note: we assume that $m > 0$ and is not a cube.

Now, if $x_2 \neq 0$, then we apply the same argument and we are done. If $x_1, x_2 = 0$, then we apply Cramer's rule and let $\alpha = \frac{x_1+x_2+x_3}{3}$. This shows that $\alpha \in K$ and since it is a real algebraic integer, α is rational.

We now let $K \subset L = K(m^{1/3})$, where m is a cubefree integer. Any prime of K that ramifies in L must divide m. Since, all ramified primes divide the conductor 6, hence, $2, 3$ which divide 6, give us possible values of positive and cubefree m. So, $m = 2^a 3^b$ where $a, b = 0, 1, 2$. So, all possible values of m such that m is cubefree and positive are: $2, 4, 3, 9, 6, 12, 18, 36$.

We need L to satisfy conditions that we listed in the beginning of the section, which were to be satisfied by $K(2^{1/3})$, such as $[L : K] = 3$, $Gal(L/\mathbb{Q}) \cong S_3$ and that primes that ramify in L/K divide the conductor 6. The values of m, which satisfy these conditions are given by $2, 3, 6, 12$. We want $x^3 - m$ to be such that $x^3 - m \equiv 0 \pmod{p}$ for all primes that are represented by $x^2 + 27y^2$. To make this process a bit easier, I made the following python program which disqualifies those $x^3 - m$ which do not have solutions for *primes* that can be algorithmically checked to be representable by the form $x^2 + ny^2$:

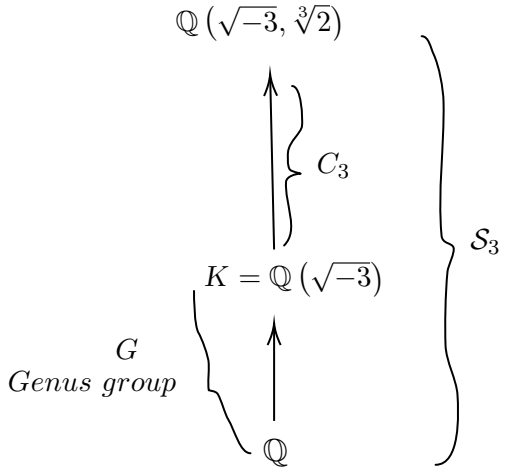
```
import itertools as it
import sympy as sp
import numpy as np
from sympy.ntheory import primefactors as pf
from math import *
n = 27
N = 3 # the base of the modularity condition for (-n/p) = 1
ms = [1] #list of all quadratic residues modulo n
#check_form helps determine if the given p can be written as x ** 2 + n y ** 2
def check_form(p):
  for y in range(int(sqrt(p / n)) + 1):
    x = sqrt(p - n * y ** 2)
    if x.is_integer():
      return (int(x), y)
  return False
PS = []
#This for loop determines which p can be written as x **2 + ny**2 and lists them as variables
↪  in PS
for k in range(100):
  ps = [N * k + m for m in ms]
  ps = [(p, check_form(p)) for p in ps if sp.isprime(p) and check_form(p)]
  PS += ps
# x^3 - ax - b
#This part lists which polynomials are solvable mod p
a = [0, 1]
facs = pf(4 * n) #calculates prime factors of the discriminant
# ternary bit sequences excluding (0,0,...) because that's just 1
ter_seqs = list(it.product(range(3), repeat = len(facs)))[1:]
```

```
def helper(facs, t):
  facs = np.array(facs)
  t = np.array(t)
  return np.prod(facs ** t)
b = [helper(facs, t) for t in ter_seqs]
abs = it.product(a, b)
def find_x(f, p): #finds solutions to f(x)% p==0
  for x in range(p):
    if f(x) % p == 0:
      return x
  return False
#The part from here prints the list of solutions, i.e., for each prime p, it tells whether
↪  f(x)%p==0
#If it is solvable then it gives the solution x else returns False.
def minpol(ab):
  a, b = ab
  f = lambda x : x ** 3 - a * x - b
  ps = [p for (p, xy) in PS]
  xs = [find_x(f, p) for p in ps]
  pxs = zip(ps, xs)
  print('---------')
  print('Solution to x ^ 3 - {}x - {} = 0 (mod p) for each p'.format(a, b))
  for px in pxs:
    print(px)
print(PS)
for ab in abs:
  minpol(ab)
```

All degree 3 monic irreducible polynomials except for x^3-2, failed to be solvable at atleast one p, where p is an odd prime that satisfies $p \equiv 1 \pmod 3$ and $p = x^2 + 27y^2$.

So the only polynomial remaining is the minimal polynomial $x^3 - 2$ corresponding to the real algebraic integer $2^{1/3}$ such that $L = K(2^{1/3})$.

Let us now find the genus field of $K = \mathbb{Q}(\sqrt{-3})$ in this case. The only odd prime that ramifies in L is 3 and by our definition 5.7, we have $G_{\mathcal{O}_K} = \mathbb{Q}(\sqrt{-3}) = K$.



We can infer that p splits in the Hilbert class field $L \iff 2$ is a cubic residue modulo p. So,

we have:

$$p = x^2 + 27y^2 \iff (-3/p) = 1 \text{ and } x^3 - 2 \equiv 0 \pmod{p} \text{ has integral solutions.}$$

We have seen two cases so far. One where the genus field is the Hilbert class field and the other where it is the quadratic number field. In the next example, it is however distinct from the two.

5.3 Case of $p = x^2 + 26y^2$

Let $K = \mathbb{Q}(\sqrt{-26})$. The form $x^2 + 26y^2$ has discriminant -104. Corresponding to this discriminant there are 6 reduced forms, hence 6 equivalence classes. The class group $\cong (\mathbb{Z}/6\mathbb{Z})$. From definition 5.7, one can deduce that the genus field is $G_{\mathcal{O}_K} = \mathbb{Q}(\sqrt{13}, \sqrt{-2})$. Notice that the degree of extension $[G_{\mathcal{O}_K} : K] = 2$. Since $|Cl(\mathcal{O}_K)| = 6$, hence $G_{\mathcal{O}} \neq L$. To find the Hilbert class field of K, we use Theorem 5.2 since $n = -26$ is square-free and $\not\equiv 3 \pmod 4$. The Hilbert class field L will be a degree 3 extension over $G_{\mathcal{O}}$. The primes that ramify in this extension are $2, 13, 3$. Hilbert class field L will be of the form $G_{\mathcal{O}}(t)$, where t is an algebraic integer. To find out t, notice that t will be divisible by $2, 13$, hence, it can be $2^a 13^b$ for some values of a, b. The values of a, b come from the discriminant of $L/G_{\mathcal{O}_K}$. However, not all of these values can be t. They need to satisfy the facts that $|Cl(\mathcal{O}_K)| = [L : K] = 6$, $Gal(L/\mathbb{Q}) \cong C_2 \times C_6$ and must divide the conductor. To find the value of t, we use our Theorem 5.2: Let $L = G_{\mathcal{O}}(t)$, that there exists $f(x)$ of degree 3 such that it is the minimal polynomial of t and $f_n(x) \equiv 0 \pmod p$, where p is an odd prime such that $p = x^2 + 26y^2$. In the ideal case, to find $f_n(x)$, we need to find the possible values of the local discriminant of $L/G_{\mathcal{O}_K}$ which will be of the form $-4 * 27 * (p^3 + q^2)$ given the ramification index $= 2$ of the primes $2, 13$. The solution that we get is $p = -1, q = -2$ and hence, $f_n(x) = x^3 - x - 2$ which is a degree 3 monic, irreducible polynomial. It is the minimal polynomial of our algebraic integer t.

In what follows, we will verify the fact the $p = x^2 + 26y^2 \iff p$ is a quadratic residue modulo 104 and $f_n(x) = x^3 - x - 2 \equiv 0 \pmod p$. We will check the cases when $x^2 - ax - t \equiv 0 \pmod p$, for $a = 0, 1$ and for all primes p which are quadratic residues modulo 104 and are represented by the form $x^2 + 26y^2$. Making slight modifications to the python code which we used in our Example 5.2 will furnish us with $f_n(x)$. In the program for this, the values of b are calculated from the discriminant -104 by taking all possible combinations of $13^a, 2^b$ such that $a = 0, 1$ and it calculates the value of b as factors of 104.

A snippet of the output 1 shows that $x^3 - x - 26$ cannot be $f_(x)$ as the code renders false at $p = 251$. However, none of the entries corresponding to $x^3 - x - 2$ render false, rather we get a list of all x such that $f_n(x) \equiv 0 \pmod p$ which does not happen in other cases[31]. Replacing the following lines in the program 5.2, we get the output as given in Table 1.

```
n = 26
N = 26 # the base of the modularity condition for (-n/p) = 1
```

[31] Full code has not been included here, however one can generate full output on any Python notebook for complete results.

Solution to x^3−1x−2=0 (mod p) for each p	Solution to x^3−1x−26=0 (mod p) for each p
(107, 26)	(107, 57)
(113, 28)	(113, 92)
(107, 26)	(107, 57)
(113, 28)	(113, 92)
(251, 8)	(251, False)

Table 1: Output

```
ms = [1, 81, 17, 9, 49, 25, 79, 55, 95, 87, 23, 103]
```

We get that for all values of t such that $x^3 - t \equiv 0 \pmod{p}$, the output is false at at least one prime p such that $p = x^2 + 26y^2$. However, $x^3 - x - 2 \equiv 0 \pmod{p}$ renders output for all primes p such that $p = x^2 + 26y^2$. Hence, $f_n(x) = x^3 - x - 2$ is the minimal polynomial of t. This gives us our Hilbert class field $L = G_{\mathcal{O}}[x]/(x^3 - x - 2)$.

Hence $p = x^2 + 26y^2 \iff \left(\frac{-26}{p}\right) = 1$ and $x^3 - x - 2 \equiv 0 \pmod{p}$.

We thus conclude our investigation of primes p of the form x^2+5y^2, x^2+27y^2 and x^2+26y^2. While we did not provide a detailed argument of when can a prime p be represented by $x^2 + ny^2$ for infinitely many n, we can, however, conclude from our little investigation that there is always the general criterion that $(-n/p) = 1$ and some polynomial of degree $h(\mathcal{O}_K)$, which is the class number corresponding to the discriminant of K has a root modulo p. For an interesting account of the full treatment of this problem, we suggest our readers to refer to [8, 30] and [31].

6 Concluding Remarks

We have covered a lot of ground in this thesis. We began our study of quadratic reciprocity law with the introduction of the quadratic Gauss sums. Our treatment of these sums in section 3.2.2, hinted that in general, for any cyclotomic extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, where p is a odd prime such that $m|(p-1)$, the m^{th} power of the Gauss sum g is an element of the field[32] $\mathbb{Q}(\tau)$, such that it gives us an intermediate sub-extension $\mathbb{Q}(\tau) \subset \mathbb{Q}(\tau, g^m) \subset \mathbb{Q}(\zeta_p, \tau)$, which is a radical extension. This points towards the fact that the Gauss sums are Lagrange resolvents (see [38, 39]). Generalising the quadratic Gauss sums and introducing Jacobi sums helped us prove the law of cubic reciprocity. The Jacobi sums arise naturally when finding the number of solutions to the equations over some finite field (see [9]). Further generalisation of these sums to some degree n extension of $\mathbb{F}_p$, allows us to establish the rationality of the congruence zeta function introduced by Artin (see [9, pp. 151–171]).

To understand these laws intuitively and see if generalisation of our previous work to higher reciprocity laws is possible, the second part of the thesis, was centered around Artin reciprocity to study the quadratic and cubic reciprocity laws. Using the language of class field theory, Artin reciprocity presented an algebraic viewpoint on these reciprocity laws. Without invoking its full force, it provided a framework from which higher reciprocity laws will follow.

[32]Here, τ is the m^{th} root of unity.

As an application of the theory that we developed, we discussed three cases of primes of the form $x^2 + ny^2$. The first case $p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$ had class number 2 and only one class corresponding to the principal quadratic form was contained in the principal genus. The genus field was isomorphic to the Hilbert class field of the number field $K = \mathbb{Q}(\sqrt{-5})$.

The second case was of primes $p = x^2+27y^2 \iff p \equiv 1 \pmod{3}$ and $x^3-2 \equiv 0 \pmod{p}$. Here 27 is non-squarefree and $\equiv 3 \pmod{4}$ and there are two classes corresponding to the reduced forms $x^2 + 27y^2$ which is the principal quadratic form and $4x^2 + 2xy + 7y^2$. The genus field was isomorphic to the number field and the splitting of p in the Hilbert class field $K(2^{1/3})$ gave us the additional condition that separates the principal quadratic form from $4x^2 + 2xy + 7y^2$, even though they lie in the principal genus.

The third case was of primes $p = x^2 + 26y^2 \iff -26$ is a quadratic residue modulo p and $x^3 - x - 2 \equiv 0 \pmod{p}$. We wrote a python code to eliminate the other possibilities of the minimal polynomial of α, where the Hilbert class field $L = K(\alpha)$ of number field $K = \mathbb{Q}(\sqrt{-26})$. Here, our number field, Hilbert class field and genus field of K are all different and hence, this example very well suited the structure of this dissertation. An alternate example could be $p = x^2 + 14y^2 \iff -14$ is a quadratic residue modulo p and $f_n(x) \equiv 0 \pmod{p}$, where $f_n(x)$ is the degree $h(\mathcal{O}_K)$ minimal polynomial of α such that the Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ is $L = K(\alpha)$.

Further developments in finding for which prime p is $p = x^2 + ny^2$ solvable for any n, are marked by Cebotarev Density theorem and estimation of the aforementioned polynomial $f_n(x)$. This requires the theory of complex multiplication and an elaborate discussion on class equation, which will lead to a constructive solution to primes of the form $x^2 + ny^2$ (see [8, pp. 199–330]).

Notice that in all these cases that we considered, the Galois group of the maximal unramified extension L/K, where K is the number field $\mathbb{Q}(\sqrt{-n})$ is always solvable. For a general reciprocity law, we need to push beyond the solvability criteria. Developments have been made in this direction in [36], and there is an ongoing effort to push the ideas further via the Langlands program [42, 43].

7 Acknowledgements

I would like to thank my supervisor Dr Jack Sempliner for his guidance and valuable comments on earlier drafts.

References

[1] Mark Beintema and Azar Khosravani. "The origins of the genus concept in quadratic forms". In: *The Mathematics Enthusiast* 6.1-2 (2009), pp. 137–150. DOI: 10.54870/1551-3440.1141.

[2] "Introduction". In: *Primes of the Form x2 + ny2*. John Wiley & Sons, Ltd, 2013, pp. 1–5. ISBN: 9781118400722. DOI: https://doi.org/10.1002/9781118400722.ch0. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118400722.ch0. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118400722.ch0.

[3] "From Fermat to Gauss". In: *Primes of the Form x2 + ny2*. John Wiley & Sons, Ltd, 2013. Chap. 1, pp. 7–85. ISBN: 9781118400722. DOI: https://doi.org/10.1002/9781118400722.ch1. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118400722.ch1. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118400722.ch1.

[4] Ram Murty. "Quadratic reciprocity via linear algebra". In: *journalId:00001884* 12 (Jan. 2001).

[5] B. F. Wyman. "What is a Reciprocity Law?" In: *The American Mathematical Monthly* 79.6 (1972), pp. 571–586. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2317083 (visited on 08/21/2022).

[6] tracing (https://math.stackexchange.com/users/200415/tracing). *Are the discriminant of abelian cubic extensions of $\mathbb{Q}$ equal to the square of their conductor?* Mathematics Stack Exchange. eprint: https://math.stackexchange.com/q/1104946. URL: https://math.stackexchange.com/q/1104946.

[7] Noah Snyder. *Artin's L-functions: A Historical Approach*. 2002. URL: https://nsnyder1.pages.iu.edu/thesismain.pdf.

[8] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*. Vol. 34. John Wiley & Sons, 2011.

[9] Kenneth F. Ireland. *A classical introduction to modern number theory*. eng. 2nd ed. Graduate texts in mathematics ; 84. New York ; Springer-Verlag, 1990. ISBN: 038797329X.

[10] Gergely Harcos. *Equidistribution on themodular surface and L-functions*. URL: https://users.renyi.hu/~gharcos/heegner.pdf.

[11] *Lecture Notes - Algebraic Number Theory*. URL: https://learn-eu-central-1-prod-fleet01-xythos.content.blackboardcdn.com/60faa9080242d/4761639?X-Blackboard-Expiration=1662238800000%5C&X-Blackboard-Signature=1H.

[12] Kiran S. Kedlaya. URL: https://kskedlaya.org/cft/book-1.html.

[13] BOWEN WANG. *INTRODUCTION TO CLASS FIELD THEORY*. URL: https://math.uchicago.edu/~may/REU2015/REUPapers/Wang,Bowen.pdf.

[14] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[15] Evan Chen. *Artin reciprocity*. 2016. URL: https://blog.evanchen.cc/2016/05/03/artin-reciprocity/.

[16] Sean Elvidge. *The history of the law of quadratic reciprocity - Sean Elvidge*. URL: http://seanelvidge.com/wp-content/uploads/2011/04/HistoryQR.pdf.

[17] P. Shiu. "Reciprocity laws: from Euler to Eisenstein, by Franz Lemmermeyer. (Springer Monographs in Mathematics) Pp. 487. $44.50. 2000. ISBN 3 540 66957 4 (Springer-Verlag)". eng. In: *Mathematical gazette* 85.502 (2001), pp. 171–172. ISSN: 0025-5572.

[18] Akhil Mathew. *The Artin Reciprocity Law*. June 2012. URL: https://amathew.wordpress.com/2010/06/22/the-artin-reciprocity-law/.

[19] BF Wyman. *What is a reciprocity law? - JSTOR*. URL: https://www.jstor.org/stable/2317083.

[20] *from quadratic reciprocity to langlands' program - abelprize.no*. URL: https://abelprize.no/sites/default/files/2021-08/Sletsj%5C%C3%5C%B8e_Arne_B_Langlands_Quadratic.pdf.

[21] Alex Kontorovich and substantive Quanta Magazine moderates comments to facilitate an informed. *What is the Langlands program?* June 2022. URL: https://www.quantamagazine.org/what-is-the-langlands-program-20220601/.

[22] Franz Lemmermeyer. *Hermite's identity and the quadratic reciprocity law*. 2022. DOI: 10.48550/ARXIV.2206.01170. URL: https://arxiv.org/abs/2206.01170.

[23] Franz Lemmermeyer. *Proofs of the Quadratic Reciprocity Law*. URL: https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html.

[24] Franz Lemmermeyer. *Hermite's identity and the Quadratic Reciprocity Law*. May 2022. URL: https://arxiv.org/abs/2206.01170.

[25] Ezra Brown. *The First Proof of the Quadratic Reciprocity Law, Revisited*. Apr. 1981. URL: https://www.jstor.org/stable/2320549.

[26] David Helm. *Number Theory*. Oct. 2021.

[27] Alan. Baker. *A concise introduction to the theory of numbers*. eng. Cambridge: Cambridge University Press, 1984. ISBN: 0521243831.

[28] Andrew Sutherland. *Class Field theory, Ray class groups and Ray Class elds*. URL: https://math.mit.edu/classes/18.785/2015fa/LectureNotes20.pdf.

[29] Lawrence C. Washington. "The Kronecker—Weber Theorem". In: *Introduction to Cyclotomic Fields*. New York, NY: Springer New York, 1997, pp. 321–331. ISBN: 978-1-4612-1934-7. DOI: 10.1007/978-1-4612-1934-7_14. URL: https://doi.org/10.1007/978-1-4612-1934-7_14.

[30] Che Li. *Introduction to Class Field Theory and Primes of the Form x2 + ny2*. Oct. 2018. URL: http://math.uchicago.edu/~may/REU2018/REUPapers/Li,Che.pdf.

[31] Peter Stevenhagen. *Primes represented by quadratic forms - universiteit leiden*. URL: https://websites.math.leidenuniv.nl/algebra/Stevenhagen-Primes.pdf.

[32] Sukumar Das Adhikari. *The early reciprocity laws: From Gauss to Eisenstein - bprim.org*. URL: https://www.bprim.org/sites/default/files/recipro1.pdf.

[33] Parvati Shastri. *Reciprocity laws: Artin-Hilbert - bprim.org*. URL: https://www.bprim.org/sites/default/files/rlmain.pdf.

[34] MICHAEL ZSHORNACK. *Cyclotomic Extensions*. Nov. 2021. URL: https://web.math.ucsb.edu/~agboola/teaching/2021/fall/225A/notes/lecture_XVII.pdf.

[35] Harvey Cohn. *Advanced number theory*. Aug. 1980. URL: https://books.google.com/books/about/Advanced_Number_Theory.html?id=yMGeElJ8M0wC.

[36] Goro Shimura. In: 1966.221 (1966), pp. 209–220. DOI: doi:10.1515/crll.1966.221.209. URL: https://doi.org/10.1515/crll.1966.221.209.

[37] Kazım Ikeda and Erol Serbest. "Non-abelian local reciprocity law". In: *manuscripta mathematica* 132 (May 2010), pp. 19–49. DOI: 10.1007/s00229-010-0336-6.

[38] Jerry Shurman. *Cyclotomic-intermediate fields via Gauss sums*. URL: https://people.reed.edu/~jerry/332/30kummer.pdf.

[39] Paul Garrett. *Kummer, Eisenstein, computing gauss sums as Lagrange resolvents*. July 2010. URL: https://www-users.cse.umn.edu/~garrett/m/v/kummer_eis.pdf.

[40] Caroline Gates. *SUPERCHARACTERS and superclasses for algebra groups*. URL: https://statweb.stanford.edu/~cgates/PERSI/papers/supercharacters.pdf.

[41] Christopher F. Fowler, Stephan Ramon Garcia, and Gizem Karaali. *Ramanujan sums as supercharacters*. 2013.

[42] Matthew Emerton. *Langlands reciprocity: L-functions, automorphic forms, and Diophantine equations (chapter 15) - the genesis of the Langlands program*. July 2021. URL: https://www.cambridge.org/core/books/genesis-of-the-langlands-program/langlands-reciprocity-lfunctions-automorphic-forms-and-diophantine-equations/BADBF1835A5356FA0F97898BBA1401F0.

[43] Gaëtan Chenevier. *An introduction to langlands' reciprocity conjecture*. Oct. 2019. URL: https://www.phys.ens.fr/~kashani/slides_chenevier.pdf.

[44] Matt Baker. *The sign of the quadratic Gauss sum and quadratic reciprocity*. Feb. 2019. URL: https://mattbaker.blog/2015/04/30/the-sign-of-the-quadratic-gauss-sum-and-quadratic-reciprocity.

[45] Kenneth S. Williams. *ON EISENSTEIN'S SUPPLEMENT TO THE LAW OF CUBIC RECIPROCITY*. 1975.

[46] Daniel A. Marcus. *Number Fields*. 2018. URL: https://www.math.toronto.edu/~ila/2018_Book_NumberFields.pdf.

[47] YOSHIOMI FURUTA. *The genus field and genus number in algebraic number fields*. 1967. URL: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/22B8BD0185574A44D494C911E211C441/S0027763000024387a.pdf/div-class-title-the-genus-field-and-genus-number-in-algebraic-number-fields-div.pdf.