HONOURS PROJECT

PRIMITIVE ROOTS

Prof. Dr. S. Alaca

and

Student Gregory Doyle - Id 239952

School of Mathematics and Statistics Carleton University

????, 2003 or 4

Introduction

At some point during his illustrious career, Paul Erdos conjectured that every odd prime has a prime primitive root [10]. Various work has been done on this problem. However, the most popular methods so far have been analytic. For this paper, we present some algebraic methods of attacking the conjecture. Indeed, it is this conjecture which led to the study of higher reciprocity laws, which are the main focus of this paper. However, the reasoning behind the study of these laws is to better understand the conjecture. Hence, throughout the paper, we prove results which may appear somewhat obtuse, but it is understood that they lead to further understanding of Erdos' conjecture.

The first two chapters will present some necessary background to understand the proof of the reciprocity laws. It is understood that the reader knows a little bit about introductory field theory. The first chapter presents some basic theorems about number theory. For most, this chapter will be review. However, we use these theorems later on to present some simple ideas about primitive roots. The second chapter presents various theorems related to algebraic number theory. This chapter is long, but is necessary background for the presentation of the Eisenstein reciprocity law. The reader who is well versed in algebraic number theory may wish to skip this chapter, referring back to specific theorems when reading chapter 6.

The third chapter presents a brief introduction to Gauss sums and Jacobi sums. The results in these chapters are particularly important, and those new to Gauss or Jacobi sums would be well advised to read this chapter. In proving any reciprocity law, we will often refer back to this chapter.Additionally, the theorems presented here are very elegant. Those who are familiar with Gauss and Jacobi sums may wish to read this chapter, if only to marvel at the beauty of these ideas.

The fourth chapter proves the quadratic reciprocity law. Those who have seen this law before may skip ahead a chapter, losing nothing in the process. However, the proof of the quadratic reciprocity law uses Gauss sums, and those who found chapter 3 scintillating may care to look at this proof.

The fifth chapter proves the cubic reciprocity law. It is here that some of the background of chapters 2 and 3 becomes necessary. Most of this background material will be familiar to anyone who has taken a course in either algebraic number theory, or a meaty course on field theory. The concepts are not difficult, and even the beginning reader should have no problems with this chapter.

The sixth chapter presents the Eisenstein reciprocity theorem. We rely

heavily on the material in chapters 2 and 3 and refer to it frequently. Most of these theorems of chapter 6 will provide references. We emphasize that, although we managed to prove a small bit of Erdos' conjecture, Eisenstein reciprocity is the main focus of this paper. The proof of the theorem is long, and somewhat of an acquired taste. However, it is an excellent generalization of an nth power reciprocity law.

Finally, the seventh chapter gives some conclusions related to the conjecture. We will see that we have found certain classes of primes which have prime primitive roots.

To conclude, this author believes that the reciprocity law approach to Erdos' conjecture may yield further ideas. This approach becomes somewhat limited, as not much (or as much as we would like) is known about prime ideal decompositions in cyclotomic fields. Furthermore, the author believes that as the knowledge of these decomposition increases, the reciprocity approach and indeed, the reciprocity laws in general, will become more and more valuable.

Contents

Chapter 1

Number Theory

1.1 Divisibility

Definition 1.1.1. *Suppose a and b are integers with $a > b$. If there exists a positive integer c such that $a = bc$, then we say b divides a and is denoted as $b \mid a$. As well, we say that b is a divisor of a.*

Theorem 1.1.1. *We have several important properties about divisibility. Let a, b, c and d be nonzero integers.*

1. *If $a \mid b$ and $b \mid c$ then $a \mid c$*
2. *If $a \mid b$ and $b \mid a$ then $a = \pm b$*
3. *If $a \mid b$ and $a \mid c$ then for any integers x and y, $a \mid bx + cy$.*
4. *If $a \mid b$ and $c \mid d$ then $ac \mid bd$.*

Proof.

1. Suppose $b = ax$, $c = by$ and $z = xy$, for some integers x, y, z. Then $c = (ax)y = az$, and so $a \mid c$.
2. If $a = bx$ and $b = ay$ for some integers x and y, then $a = axy$ and $b = bxy$. Thus $1 = xy$ which means $x = y$ and $x = \pm 1$.
3. Suppose $b = ax$ and $c = ay$. Let x' and y' be any integers. Then
$$bx' + cy' = axx' + ayy' = a(xx' + yy')$$
and so $a \mid bx' + cy'$.
4. Suppose $b = ax$ and $d = cy$. Then $bd = acxy$ and so $ac \mid bd$.

□

Theorem 1.1.2. *(The Division Theorem) For integers a, b, with $b \neq 0$, there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < |b|$*

Proof. Consider the set $S = \{\ldots, a + 2b, a + b, a, a - b, a - 2b, \ldots\}$, (eg: all multiples m of $a - mb$). Since S contains positive elements, there exists a smallest nonnegative element; we call this r. Let q be such that $a - bq = r$; and note that we must have $0 \leq r < |b|$. (Otherwise, if $r \geq |b|$, and b is positive, then $a - b(q + 1)$ is less than r, and is in S, a contradiction. The argument is similar if $b < 0$).

Now, suppose $a = bq + r = bq' + r'$, with $0 \leq r < |b|$ and $0 \leq r' < |b|$. Then $b(q - q') = r' - r$. Since $|r' - r| < |b|$, we must have $q - q' = 0$. Hence, $r' - r = 0$, and so $q = q'$ and $r = r'$. □

1.2 Primes

Definition 1.2.1. *We define the greatest common divisor of two integers a and b, denoted by (a, b) to be the largest positive number d such that $d \mid a$ and $d \mid b$. If $(a, b) = 1$, we say that a and b are relatively prime, or that a is prime to b. Similarly, for integers a, b, c, if $(a, b) = 1$, $(a, c) = 1$, and $(b, c) = 1$, we say that a, b and c are pairwise relatively prime. Additionally, this definition can be extended to any finite number of integers.*

Theorem 1.2.1. *For any two integers a and b there exist m and n such that $ma + nb = (a, b)$.*

Proof. Suppose that $d = (a, b)$ for any integers a and b. Furthermore, assume a and b are positive. Notice that every linear combination of a and b is a multiple of d. Thus, if d can be expressed as a linear combination of a and b, then it is the least such integer with this property. Indeed, suppose $a = da'$, $b = db'$, $d = ax + by$ and $e = ax' + by'$ and $e < d$. Then $e = da'x' + db'y'$ and so $e \mid d$, which contradicts our choice of d as the greatest common divisor of a and b.

Consider the set

$$S = \{ma + nb \mid m, n \in \mathbb{Z}\}$$

Let c be the smallest integer in S and $c = m'a + n'b$ for some integers m' and n'. We claim that $c \leq a$ and $c \leq b$. Assume otherwise, and that $c > a$. Then $(m' - 1)a + n'b = m'a - a + n'b = c - a > 0$, contradicting our assumption that c is the least positive element of S. (A similar argument holds to show that $c \leq b$.)

Thus, since $c \leq a$ and $c \leq b$ we can use the division algorithm to get

$$a = qc + r$$

for some integers q and r with $0 \leq r < c$. Thus, we have

$$r = a - qc = a - m'a - n'b = a(1 - m') - n'b$$

Thus, we have expressed r as a linear combination of a and b, and $r < c$. This means we must have $r = 0$, and so $a = qc$. This means that $c \mid a$. Similarly, we conclude that $c \mid b$. Thus, c is the least positive integer, expressible as a linear combination of a and b. Furthermore, since c divides both a and b, we conclude that $c = d$. □

Theorem 1.2.2. *Every integer $n > 1$ is either prime or a product of primes*

Proof. We use induction on n. The base case, $n = 2$ is true since 2 is prime. Hence, assume the theorem holds for all integers less than n. If n is not prime, then it is divisible by some number d, say $n = cd$. Since both c and d are less than n, they are either prime or products or primes. This means that n is a product of primes, which proves the theorem. □

Theorem 1.2.3. *(The Fundamental Theorem of Arithmetic) Every positive integer greater than 1 can be factored uniquely, up to order, into a product of primes.*

Proof. We again use induction on n. When $n = 2$, n is prime and the theorem holds. Assume the theorem is true for all integers less than n.

When n is prime, the theorem holds, so assume n is not prime. Furthermore, from the previous theorem, we know n is a product of primes. It remains to show that these primes are unique. So, suppose n has two factorizations, say

$$n = p_1 p_2 \dots p_m = q_1 q_2 \dots q_m$$

for primes p_i and q_i. We have that $p_1 \mid q_1 q_2 \dots q_m$ and so p_1 must divide one of the individual primes q_i. Relabel the q_i such that $p_1 \mid q_1$. Since both p_1 and q_1 are primes, we have $q_1 = 1 \cdot p_1$ and $q_1 = p_1$. Thus, we have

$$\frac{n}{p_1} = p_2 \dots p_m = q_2 \dots q_m$$

Specifically, we have $1 < \frac{n}{p_1} < n$. Thus, by the induction hypothesis, $\frac{n}{p_1}$ can be represented uniquely as a product of primes, up to order. Thus, rearranging if we have to, we get $m = n$ and $p_i = q_i$ for $2 \leq i \leq n$. □

1.3 Modulo Arithmetic

Definition 1.3.1. *Suppose a, b and m are integers, and $m \mid a - b$, we then say that a is congruent to b, denoted by $a \equiv b \pmod{m}$. If $m \nmid a - b$, then a is incongruent to b, and is denoted by $a \not\equiv b \pmod{m}$*

Theorem 1.3.1. *We have some simple consequences of the definition.*

1. *For every integer a, $a \equiv a \pmod{m}$.*
2. *If a, b and m are integers, then $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$.*
3. *If a, b, c and m are integers and $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*
4. *If a, b, m and d are integers, with $a \equiv b \pmod{m}$. If $d \mid m$, then $a \equiv b \pmod{d}$.*

Proof.

1. We notice that if n is any integer, then $n \mid 0$ since $0 = 0 \cdot n$. Thus, $m \mid a - a = 0$ for any integer a.
2. Suppose $a \equiv b \pmod{m}$. Then $m \mid a - b$, say $a - b = mx$, for some integer x. Then $m(-x) = b - a$ and so $b \equiv a \pmod{m}$. The converse is exactly the same.
3. Suppose $mx = a - b$ and $my = b - c$. Then $b = my + c$ and we get $mx = a - (my + c)$. We work this out to get $m(x - y) = a - c$ and hence $a \equiv c \pmod{m}$.
4. Suppose we have $m = dx$ and $a - b = my$. Then, substituting we get $a - b = d(xy)$ and so $a \equiv b \pmod{d}$.

□

Definition 1.3.2. *Suppose for integers a and m, there exists an integer a' such that $aa' \equiv 1 \pmod{m}$. In this case, we say a' is the inverse of a, and we say that a is invertible modulo m.*

Theorem 1.3.2. *If a and m are integers, then a is invertible modulo m if and only if $(a, m) = 1$.*

Proof. Suppose a is invertible modulo m, and that a' is an integer such that $aa' \equiv 1 \pmod{m}$. This means that $m \mid aa' - 1$, say $aa' - 1 = km$. Thus, m cannot divide aa', and so $(a, m) = 1$.

Conversely, suppose $(a, m) = 1$. Then there exist integers x and y such that $ax + my = 1$, or $ax - 1 = -my$. Thus, $ax \equiv 1 \pmod{m}$, and x is the inverse of a modulo m. □

Definition 1.3.3. *We define a complete residue system modulo m to be a set $\mathcal{S}$ of integers such that every element of $\mathbb{Z}$ is congruent to exactly one element of S.*

Consider any set

$$\mathcal{S} = \{km + 0, km + 1, \ldots, km + (m - 1)\}$$

where m is a fixed integer and k is any integer. Modulo m, we see that this set is

$$\mathcal{S} = \{0, 1, \ldots, m - 1\}$$

We call this the standard residue system modulo m.

Clearly, in a complete residue system, there will exist a number of elements a_i such that $(a_i, m) = 1$. The total number of these elements in a complete residue system is denoted by the function $\phi(m)$, and is called Euler's phi-function.

Theorem 1.3.3. *Let p be a prime. Then $a^p \equiv a \pmod{p}$ for all integers a. In particular, if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Assume a is a positive integer. If we prove the theorem for positive a, then since $(-1)^p \equiv -1 \pmod{p}$ for any odd prime p, we will be done. (We ignore the trivial case $p = 2$ where $-1 \equiv 1 \pmod{p}$. Thus, we proceed by induction on a. Clearly, when $a = 1$ this theorem is true.

Thus, suppose this theorem holds for all integers less than $n + 1$. Then, by the Binomial Theorem

$$(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \ldots + \binom{p}{p-1} n + 1$$

Now, consider the binomial coefficient $\binom{p}{k}$, for $1 \leq k \leq p - 1$. We have that

$$\binom{p}{k} = \frac{p!}{(p-k)!k!}$$

Since $k < p$ and $p - k < p$, we have that $p \mid \binom{p}{k}$. So, modulo p, we have that

$$(n + 1)^p \equiv n^p + 1 (\text{mod } p)$$

By the induction hypothesis, $n^p \equiv n \pmod{p}$, and so $(n+1)^p \equiv n+1 \pmod{p}$. This proves the first part of the theorem.

The second part of the theorem follows from the fact that, since $(a,p) = 1$, a is invertible modulo p. Thus, $a^p \cdot a^{-1} \equiv aa^{-1} \pmod{p}$. Thus, we conclude that $a^{p-1} \equiv 1 \pmod{p}$. □

Theorem 1.3.4. *If a and m are integers such that $(a,m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Proof. Suppose $S = \{r_1, r_2, \ldots, r_m\}$ is a complete residue system modulo m. Let $r_1, \ldots r_{\phi(m)}$ denote the $\phi(m)$ invertible elements of S. Then the elements $ar_1, \ldots, ar_{\phi(m)}$ are all invertible. Note that if $ar_i \equiv ar_j \pmod{m}$, for $i \neq j$, then $r_i \equiv r_j \pmod{m}$, since a is invertible modulo m. But, in a complete residue system, $r_i \not\equiv r_j \pmod{m}$ for any $i \neq j$. Hence, the set $aS = \{ar_1, \ldots, ar_{\phi(m)}\}$ is equivalent to the set S modulo m. Thus, each element in aS is congruent to exactly one element in S. This gives

$$(ar_1)(ar_2)\ldots(ar_{\phi(m)}) \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m}$$

Rewriting this, we have $a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m}$. Since the r_i are all invertible, we conclude that $a^{\phi(m)} \equiv 1 \pmod{m}$. □

1.4 Lagrange's Theorem

Theorem 1.4.1. *Let p be a prime number, and let $f(x)$ be a polynomial of degree $n \geq 1$, not all of whose coefficients are divisible by p. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n solutions in a complete residue system modulo p.*

Proof. We prove this theorem by induction on the degree of $f(x)$. If $deg(f(x)) = 1$, then $f(x) = ax + b$ for some a and b. Suppose $p \nmid a$, then $ax + b \equiv 0 \pmod{p}$ has a solution, regardless of whether $p \mid b$ or not. If $p \mid a$, then $p \nmid b$, and there is no solution. Thus, in either case, there is at most one solution.

Assume that all polynomials, with degree less than n and not all coefficients divisible by p, satisfy this theorem. Let $f(x)$ be a polynomial of degree n. If $f(x)$ has no solutions, then the theorem holds. So assume that a is a root of $f(x)$. By long division of polynomials, there exist $q(x)$ and $r(x)$ such that

$$f(x) = (x-a)q(x) + r(x)$$

with $deg(r(x)) < deg(x-a)$. Since $deg(x-a) = 1$, we must have that $r(x)$ is an integer, which we denote by r.

Now, $f(a) \equiv 0 \pmod{p}$ implies that $r \equiv 0 \pmod{p}$, and so $p \mid r$. Hence, $f(x) \equiv (x-1)q(x) \pmod{p}$. But, modulo p, $q(x)$ has at most, degree $n-1$. Furthermore, by the assumption on $f(x)$, not all the coefficients of $q(x)$ are divisible by p. Thus, by the induction hypothesis, $q(x)$ has at most $n-1$ solutions modulo p.

Suppose a is not a root of $q(x)$, so $q(a) \not\equiv 0 \pmod{p}$. Then if b is a root of $f(x)$, either $b \equiv a \pmod{p}$ or $b \not\equiv a \pmod{p}$. If $b \equiv a \pmod{p}$, then we have $q(b) \equiv q(a) \pmod{p}$. Thus, we either have $b = a$ or b is a root of $q(x)$. Suppose $b \neq a$ and $q(b) \equiv 0 \pmod{p}$. By the induction hypothesis, there can be at most $n-1$ roots distinct from a. Thus, f has at most n roots.

Now suppose a is a root of $q(x)$. If $q(a) \equiv 0 \pmod{p}$ then we can divide $q(x)$ by $(x-a)$ and thus $q(x) \equiv (x-a)q_1(x) \pmod{p}$, for some $q_1(x)$. So, $f(x) \equiv (x-a)^2 q_1(x) \pmod{p}$. Continuing in this fashion, we have $f(x) \equiv (x-a)^k q'(x) \pmod{p}$, where k is the multiplicity of a as a root in $f(x)$. Thus, $q'(a) \not\equiv 0 \pmod{p}$. So, $deg(q'(x)) = n-k$ and so, by the induction hypothesis, there are at most $k-a$ roots of $q'(x)$. If b is a root of $f(x)$, we must have $b \not\equiv a \pmod{p}$. Then $f(b) \equiv (b-a)^k q'(b) \equiv 0 \pmod{p}$ means that $q'(b) \equiv 0 \pmod{p}$. Hence, every root of f different from a is a root of $q'(x)$. So, since there are at most $n-k$ distinct roots of $q'(x)$, and a is root k times means that f has at most n roots. □

Corollary 1.4.2. *Let p be a prime and $d \mid p-1$; then the congruence $x^d - 1 \equiv 0$ (mod p) has exactly d solutions.*

Proof. By Theorem 1.3.6, we have $x^{p-1} \equiv x \pmod{p}$ for all x relatively prime to p. Thus, this congruence has at most $p-1$ solutions and, modulo p, this congruence has exactly $p-1$ solutions, namely, the elements $1, 2, \ldots, p-1$. Let $p-1 = dk$, then

$$x^{p-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1)$$

By the previous theorem, $x^d - 1 \equiv 0 \pmod{p}$ has at most d solutions, and $x^{d(k-1)} - 1 \equiv 0 \pmod{p}$ has at most $d(k-1)$ solutions. Thus, the righthand side of the above equality has at most $d(k-1) + d = dk = p-1$ solutions. But, the lefthand side has exactly $p-1$ solutions. This means that each polynomial on the righthand side has the maximum number of solutions. Since we have $d \mid p-1$, we've shown that $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions. □

1.5 Primitive Roots and Order

Definition 1.5.1. *Let a and n be integers such that $(a, n) = 1$. Then the order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$, and we denote this as $ord_n(a)$ or $|a|$. If $ord_n(a) = \phi(n)$, then a is called a primitive root.*

Theorem 1.5.1. *Suppose $a^m \equiv 1 \pmod{n}$, then $ord_n(a) \mid m$.*

Proof. Suppose $k = ord_n(a)$. By the division algorithm, there exist integers q, r such that $m = kq + r$ and $0 \leq r < k$. If $ord_n(a) \nmid m$ then we have $r \neq 0$. However, we have

$$a^m \equiv a^{kq+r} = a^{kq}a^r \equiv a^r \equiv 1 (\text{mod } n)$$

Thus, $a^r \equiv 1$ and $r < k$ means that, to avoid contradiction, we must have $r = 0$. Thus, we conclude that $ord_n(a) \mid m$. □

Corollary 1.5.2. *If $(a, n) = 1$ and if $a^i \equiv a^j \pmod{m}$, then $i \equiv j \pmod{ord_n(a)}$.*

Proof. Since $(a, n) = 1$, a is invertible modulo n. This means that for any integer $j \geq 0$, a^j is invertible modulo n, with inverse $(a^{-1})^j = a^{-j}$. Thus, $a^i a^{-j} \equiv a^{-i}a^j \equiv a^{i-j} \equiv 1 \pmod{m}$. (Here, we've assumed that $a^i \equiv a^j \pmod{m}$.) Thus, $ord_n(a) \mid i - j$ or $i \equiv j \pmod{ord_n(a)}$ as claimed. □

Definition 1.5.2. *An integer $\lambda > 0$ is called the minimal universal exponent if λ is the smallest integer such that, for any x relatively prime to n, $x^\lambda \equiv 1 \pmod{n}$.*

Lemma 1.5.1. *Suppose M is the maximum possible order of all elements modulo n. Then $M = \lambda$. (In particular, this implies there exists an element of order λ.)*

Proof. If M is the maximum possible order, then for any $(x, n) = 1$, $ord_n(x) \mid M$. (This follows from the previous theorem.) Thus, $x^M \equiv 1 \pmod{n}$ for all $(x, n) = 1$ and so $\lambda \leq M$. Since λ is the smallest integer such that this occurs, we must have $M \leq \lambda$ and so $M = \lambda$. □

Theorem 1.5.3. *For any prime number p, there exists a primitive root.*

Proof. Let $\lambda > 0$ be an integer such that, for any $(a, p) = 1$, $a^\lambda \equiv 1 \pmod{p}$. If $\lambda = p - 1$, then there exists an element with order $p - 1$, which means there exists a primitive root. Hence, suppose $\lambda < p - 1$. But, all elements

relatively prime to p satisfy $x^{\lambda} \equiv 1 \pmod{p}$. Specifically, there exist $p-1$ elements (namely, the integers from 1 to $p-1$) which satisfy this equation. This contradicts the assumption that λ has at most less than $p-1$ solutions. Hence, $\lambda = p-1$ and there exists a primitive root. $\square$

Chapter 2

Algebraic Number Theory

2.1 Ideals

Definition 2.1.1. *Let D be an integral domain. Suppose I is a subset of D which satisfies the following conditions*

1. *If $a \in I$ and $b \in I$ then $a + b \in I$.*
2. *For any $a \in I$ and for any $r \in D$, $ra \in I$.*

Then we say that I is an ideal of D.

If $\{a_1, \ldots, a_n\}$ are elements of D, then the set

$$\{\sum_{i=1}^{n} r_i a_i \mid r_i \in D\}$$

is an ideal of D. We call this the ideal generated by the elements $a_1, \ldots, a_n$ and denote this by $< a_1, \ldots, a_n >$. When an ideal is generated by a single element, say $I =< a >$, then we say that I is a principal ideal and a is the generator of I. Furthermore, if D is any integral domain such that every ideal in D is a principal ideal, then we say that D is a principal ideal domain (PID).

Definition 2.1.2. *Let D be an integral domain. The for ideals I and J, we define the sum and product as follows*

1. $I + J = \{i + j \mid i \in I, j \in J\}$
2. $IJ = \{x \in D \mid x = \sum_{k=1}^{n} i_k j_k, i_k \in I, j_k \in J, n \in \mathbb{N}\}$

Theorem 2.1.1. *For an integral domain D, and ideals A and B, $A+B$ and AB are ideals.*

Proof. We first check $A + B$. Suppose $x, y \in A + B$. Then $x = a_0 + b_0$ and $y = a_1 + b_1$ for some $a_0, a_1 \in A$ and $b_0, b_1 \in B$. Then $x + y = (a_0 + a_1) + (b_0 + b_1) \in A + B$. If $d \in D$ then $dx = d(a_0 + b_0) = da_0 + db_0 \in A + B$. Thus, $A + B$ is an ideal. We can extend this idea to any finite number of ideals.

Now, suppose x and y are elements of AB. Then, since x and y are finite sums of elements $a_i b_i$, it is clear that $x + y$ is also a finite sum of elements. Now, suppose

$$x = \sum_{k=1}^{n} a_k b_k$$

for some $n \geq 0$ and $a_k \in A$, $b_k \in B$. Then for any $d \in D$,

$$dx = d\sum_{k=1}^{n} a_k b_k = \sum_{k=1}^{n} (da_k) b_k \in AB$$

since A is an ideal and $da_k \in A$ for all $d \in D$. Thus, AB is an ideal. □

Corollary 2.1.2. *In an integral domain D, if $I =< i >$ and $J =< j >$ are principal ideals, then*

$$I + J =< i, j > \text{ and } IJ =< ij >$$

Proof. If $i_0 \in I$, then $i_0 = ri$ for some $r \in D$. Similarly, $j_0 \in J$ means $j_0 = rj$, $r \in D$. Hence,

$$I + J = \{i_0 + j_0 \mid i_0 \in I, j_0 \in J\} = \{ri + rj \mid r \in D\} =< i, j >$$

Furthermore,

$$\begin{aligned} IJ &= \{x \in D \mid x = \sum_{k=1}^{n} i_k j_k, i_k \in I, j_k \in J, n \in \mathbb{N}\} \\ &= \{x \in D \mid x = \sum_{k=1}^{n} (r_0 i)(r_1 j), r_0, r_1 \in D, n \in \mathbb{N}\} \\ &= \{x \in D \mid x = \sum_{k=1}^{n} r(ij), r \in D, n \in \mathbb{N}\} \\ &= \{r(ij) \mid r \in D\} \end{aligned}$$

where the last equality follows due to the fact that IJ is closed under addition. □

Corollary 2.1.3. *If D is an integral domain and $I =< i >$ is a principal ideal, then for any positive integer n,*

$$< i^n >=< i >^n$$

Proof. From the previous corollary, we have $I^2 =< i \cdot i >=< i^2 >$ and by definition, $I^2 =< i >^2$. Clearly, we can extend this idea for any finite number n. □

Definition 2.1.3. *Suppose D is an integral domain. An element $\mu \in O_K$ is called a unit if $\mu \mid 1$. This means there exists some element $\mu^{-1} \in D$ such that $\mu\mu^{-1} = 1$. In other words, any element which has an inverse is a unit. We denote the set of all units of D by $U(D)$.*

Theorem 2.1.4. *For an integral domain D, if $\mu \in U(D)$, then $< \mu >= D$.*

Proof. Suppose $\mu^{-1} \in D$ is the inverse of μ. Then, we have $\mu^{-1}\mu \in < \mu >$. So, $1 \in < \mu >$ means that, for any $d \in D$, $d \cdot 1 \in < \mu >$. This means $D \subseteq < \mu >$. Since, $< \mu > \subseteq D$, we have equality. □

Definition 2.1.4. *Let D be an integral domain. Suppose a and b are non-unit, non-zero elements of D such that $a \mid b$ and $b \mid a$. Then we say that a and b are associates, and denote this by $a \sim b$. Notice that if a and b are associates, then there exists some unit μ such that $a = \mu b$.*

Theorem 2.1.5. *For an integral domain D, if $a \sim b$ then $< a >=< b >$.*

Proof. Suppose $\mu \in U(D)$ is such that $a = \mu b$, and $\mu^{-1}\mu = 1$. Then, if $x \in < a >$, $x = ra$ for some $r \in D$. So, $\mu^{-1}x = \mu^{-1}ra = r(\mu^{-1}a) = rb$. Thus, $x \in < b >$ and so $< a > \subseteq < b >$. Similarly, we copy this procedure to conclude $< b > \subseteq < a >$ and hence $< a >=< b >$. □

Definition 2.1.5. *Let D be an integral domain. If P is an ideal such that, whenever $ab \in P$ then either $a \in P$ or $b \in P$, then we say that P is a prime ideal. Suppose M is an ideal such that, if I is any ideal of D with the property $M \subseteq I \subseteq D$, then either $I = M$ or $I = D$. If this is the case, then we call M a maximal ideal.*

Lemma 2.1.1. *Let D be an integral domain and let I be an ideal of D. Then D/I is a field iff I is a maximal ideal.*

Proof. Suppose that D/I is a field, for some ideal I and J is an ideal of D with $I \subset J \subseteq D$. Since I is strictly contained in J there exists an element $b \in J$ with $b \notin I$. Then $b + I$ is a nonzero element of D/I. Since D/I is a field, $b + I$ has an inverse, say $c + I$ for some $c \in D$, such that $(b + I)(c + I) = bc + I = 1 + I$. So, $bc - 1 \in I \subset J$. Since J is an ideal, and $c \in D$, we have $bc \in J$. Thus, $1 = bc - (bc - 1) \in J$ means that $J = D$. This shows that I is maximal.

Conversely, assume that I is a maximal ideal of D. To show that D/I is a field, we must show that for any $b + I \in D/I$ with $b \notin I$, $b + I$ has an inverse. Consider

$$B = \{x \in D \mid x = by + w \text{for some } y \in D \text{ and some } w \in I\}$$

Clearly, B is an ideal. Furthermore, for any $c \in I$, $c = w + 0 \cdot b$ and so $I \subset B$. Since I is maximal, we have $B = D$. Hence, $1 \in B$ and so $1 = by' + w'$ for some $y' in D$ and $w' in I$. Then

$$(b + I)(y' + I) = by' + I = 1 - w' + I = 1 + I$$

So, $b + I$ has an inverse, and hence D/I is a field. □

Lemma 2.1.2. *Let D be an integral domain. Then D/I is an integral domain iff I is a prime ideal.*

Proof. Assume D/I is an integral domain and suppose $a, b \in D$ are such that $ab \in I$. Then $(a + I)(b + I) = ab + I = 0 + I$. Since D/I is an integral domain, this means one of $a + I, b + I$ is equal to $0 + I$. This translates into one of $a, b \in I$. Thus, I is a prime ideal.

Conversely, suppose I is a prime ideal. To check that D/I is an integral domain, we must check that there are no zero divisors. Suppose $a+I, b+I \in D/I$. Then if $(a + I)(b + I) = 0 + I$, then $ab + I = 0 + I$ means that $ab \in I$, and so one of $a, b \in I$. This means that one of $a + I, b + I$ is the zero divisor. This implies that there are no zero divisors in D/I, and so it is an integral domain. □

Theorem 2.1.6. *A maximal ideal of an integral domain is always a prime ideal.*

Proof. Let D be an integral domain. If I is a maximal ideal of D, then D/I is a field. But, a field is an integral domain, so we have that D/I is an integral domain. This means that I is a prime ideal. □

Theorem 2.1.7. *$\mathbb{Z}$ is a PID.*

Proof. Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$, then $I =< 0 >$, so assume I is nonzero. Suppose $a \in I$. Since $-1 \in \mathbb{Z}$, $-a \in I$, so we can assume that $a > 0$. Thus, I must contain at least one positive integer. Denote the least positive integer of I by m. By the division algorithm, we have integers q and r such that $a = qm + r$ and $0 \leq r < m$. Since both a and m are elements of I, we have that $r = a - qm \in I$. So, to avoid contradiction, we must have that $r = 0$. Hence, $a = qm$ and since a was an arbitrary element of I, we conclude that $I =< m >$. □

Definition 2.1.6. *Let D be an integral domain. Then if $p \in D$ is prime, it has the property that for any $\alpha, \beta \in D$ such that $p \mid \alpha\beta$, then either $p \mid \alpha$ or $p \mid \beta$. Suppose $r \in D$ and $r \notin U(D)$ is such that $r = \alpha\beta$ for elements $\alpha, \beta \in D$ means that one of α, β is a unit.*

Theorem 2.1.8. *For any integral domain D, any prime element p is also an irreducible element.*

Proof. Let p be prime in D. Suppose $p = \alpha\beta$ for some element $\alpha, \beta \in D$. Also, assume that both α and β are not units. Since $1 \cdot p = \alpha\beta$, we have $p \mid \alpha\beta$ and so $p \mid \alpha$ or $p \mid \beta$. This means we have $\frac{\alpha}{p}\beta = 1$ or $\alpha\frac{\beta}{p} = 1$. So, one of α, β is a unit, which is a contradiction. Hence, p is irreducible. □

Theorem 2.1.9. *If D is a PID, then every irreducible element is prime.*

Proof. Let p be an irreducible element of a PID D. Suppose $p \mid ab$ for some $a, b \in D$. If $p \nmid a$, then we consider the ideal $< p, a >$. Since D is a PID, there exists an element $c \in D$ such that $< c >=< p, a >$. Since both $p \in < c >$ and $a \in < c >$, we have $c \mid p$ and $c \mid a$. Suppose c is not a unit. Since p is irreducible, $c \mid p$ means that $c \sim p$ and hence $p \mid a$, a contradiction. Thus, we must have that c is a unit, and hence $cd = 1$ for some $d \in U(D)$. As $c \in < c >=< p, a >$, there exist $x, y \in D$ such that $c = px + ay$. Thus, we have $cd = 1 = dpx + day$. Multiplying both sides by b, we have

$$b = (bdx)p + (dy)ab$$

Since $p \mid ab$, we can take p as a common factor on the right hand side. This means that $p \mid b$ or $p \mid a$ and so p is a prime element of D. □

Corollary 2.1.10. *In a PID an element p is prime iff p is an irreducible element.*

Proof. This follows immediately from the previous two theorems. □

Theorem 2.1.11. *If D is a PID, and $< a >$ and $< b >$ are ideals of D such that $< a > \subseteq < b >$, then $b \mid a$.*

Proof. If $< a > \subseteq < b >$, then $a = sb$ for some $s \in D$. Thus, $b \mid a$. □

2.2 Modules

Definition 2.2.1. *Suppose D is an integral domain and M is an additive abelian group. Then a function $\lambda : D \times M \to M$ is called a D-action on M is λ satisfies the following properties: let $a, b \in D$ and $m, n \in M$*

1. $\lambda(a + b, m) = \lambda(a, m) + \lambda(b, m)$
2. $\lambda(a, m + n) = \lambda(a, m) + \lambda(a, n)$
3. $\lambda(a, \lambda(b, m)) = \lambda(ab, m)$
4. $\lambda(1, m) = m$

Here, we denote the identity of D as 1.

Thus, any group M combined with a D-action on M is called a D-module. Additionally, a subgroup N of M is called a submodule of M if $an \in N$ for all $a \in D$ and $n \in N$.

If S is a subset of a D-module M, then we define the submodule generated by S to be the set

$$\{\sum_{i=1}^{n} d_i s_i \mid d_i \in D, s_i \in S\}$$

where n is any positive integer. We say that a D-module M is finitely generated if there exists some finite subset S such that M is generated by the elements of S.

Definition 2.2.2. *Let D be an integral domain. We say that D satisfies the ascending chain condition if, for any infinite chain of ideals in D*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

there exists some integer k such that, for all $n \geq k$, $I_n = I_k$. When this integer k exists, we say that this ascending chain terminates. If no such k exists, then this chain does not terminate, and D does not satisfy the ascending chain condition. Finally, if D satisfies the ascending chain condition, we call D Noetherian, or a Noetherian domain.

Theorem 2.2.1. *$\mathbb{Z}$ is a Noetherian domain*

Proof. Since $\mathbb{Z}$ is a PID, the chain

$$I_1 \subseteq I_2 \subseteq \dots$$

implies there exist integers $i_1, i_2, \dots$ such that

$$< i_1 > \subseteq < i_2 > \subseteq \dots$$

But, this means that we have $\dots \mid i_2 \mid i_1$. So, by the fundamental theorem of arithmetic, there exists some prime integer p such that $p \mid i_n \mid i_{n-1} \dots \mid i_2 \mid i_1$. Thus, we must have $I_{n+1} =< p >= I_{n+2} \dots$ and so $\mathbb{Z}$ satisfies the ascending chain condition. Hence, $\mathbb{Z}$ is Noetherian. □

Definition 2.2.3. *If D is an integral domain and M is a D-module, then we call M a Noetherian module if every ascending chain of submodules of M terminates. Furthermore, if N is a submodule of a D-module M, then we define the factor module*

$$M/N = \{m + N \mid m \in M\}$$

Combined with the D-action

$$r(m + N) = rm + N$$

for each $r \in D$ and each coset $m + N \in M/N$. It is clear that M/N is a D-module under the specified D-action.

Theorem 2.2.2. *Let D be an integral domain, M a D-module and N a submodule of M. Then M is a Noetherian module iff both N and M/N are Noetherian modules.*

Proof. Assume that M is Noetherian. Suppose $N_1 \subseteq N_2 \subseteq \dots$ is an ascending chain of submodules of N. Since N is a submodule of M, this chain is an ascending chain of submodules of M. Since M is Noetherian, this chain terminates, and hence, N is Noetherian. Now, suppose

$$M_1/N \subseteq M_2/N \subseteq \dots$$

is an ascending chain of submodules of the factor module M/N. For $i = 1, 2, \dots$, we let

$$M_i = \{m \in M_i \mid m \in M_i/N\}$$

We claim now that $M_i \subseteq M_{i+1}$ and M_i is a submodule of M. Consider $M_i/N \subseteq M_{i+1}/N$ If $x \in M_i/N$, then $x = m_i + N$ for some $m_i \in M_i$. But $x \in M_{i+1}/N$ and so $m_i + N \in M_{i+1}/N$, which means $m_i \in M_{i+1}$. Thus, $M_i \subseteq M_{i+1}$. Furthermore, by the defined D-action, we have $rm_i \in M_i$ for every $m_i \in M_i$ and every $r \in D$. Thus, $M_1 \subseteq M_2 \subseteq \ldots$ is an ascending chain of submodules of M, which means that it terminates at some point. This means that, for some integer k, $M_k/N = M_{k+1}/N = \ldots$. Hence, M/N is Noetherian.

Conversely, assume N and M/N are Noetherian modules. Let

$$M_1 \subseteq M_2 \subseteq \ldots$$

be an ascending chain of submodules of M. For $i = 1, 2, \ldots$ we set

$$M_i/N = \{m_i + N \mid m_i \in M_i\}$$

Again, we can see that $M_i/N \subseteq M_{i+1}/N$ and that M_i/N is a submodule of M/N. Since M/N is Noetherian, the ascending chain $M_1/N \subseteq M_2/N \subseteq \ldots$ terminates. Let l_1 be the positive integer such that

$$M_i/N = M_{l_1}/N \text{ for } i \geq l_1$$

Consider $M_i \bigcap N$. Clearly, this is a submodule of N, as we have $M_i \bigcap N \subseteq N$ and both M_i and N are modules. Furthermore, we have $M_i \bigcap N \subseteq M_{i+1} \bigcap N$. Thus, we get the ascending chain

$$M_1 \bigcap N \subseteq M_2 \bigcap N \subseteq \ldots$$

which are submodules of N. Since N is Noetherian, this chain terminates. Let l_2 be the positive integer such that $M_i \bigcap N = M_{l_2} \bigcap N$ for $i \geq l_2$.

Set $l = \max(l_1, l_2)$. Then if $i \geq l$, we have

$$M_i/N = M_l/N \text{ and } M_i \bigcap N = M_l \bigcap N$$

Assume that the chain $M_1 \subseteq M_2 \subseteq \ldots$ is not Noetherian. Then for some integer $k > l$, we have the strict inclusion $M_k \subset M_{k+1}$. This means we can choose an $m_{k+1} \in M_{k+1}$ such that $m_{k+1} \notin M_k$. Thus, $m_{k+1} + N \in M_{k+1}/N$. However, we have that $M_{k+1}/N = M_k/N$ since $k > l$. Thus, there exists some $m_k \in M_k$ and $n \in N$ such that $m_{k+1} = m_k + n$. So, $n = m_{k+1} - m_k \in N$. Furthermore, since $M_k \subset M_{k+1}$, $m_{k+1} - m_k \in M_{k+1}$. Thus, $m_{k+1} - m_k \in M_{k+1} \bigcap N$. Since $M_{k+1} \bigcap N = M_k \bigcap N$, we have $m_{k+1} - m_k \in M_k$. This implies that $m_{k+1} \in M_k$, which is a contradiction. Thus, the chain $M_1 \subseteq M_2 \subseteq \ldots$ must terminate and so M is Noetherian. $\square$

Theorem 2.2.3. *Suppose D is a Noetherian domain. Then any finitely generated D module is Noetherian.*

Proof. Let M be any finitely generated D-module. Suppose the elements $m_1, m_2, \ldots, m_n$ are the generators of M. Thus, $M = Dm_1 + Dm_2 + \ldots + Dm_n$, and each Dm_i is a D-module. For $i = 1, 2, \ldots n$ define

$$M_i = Dm_1 + Dm_2 + \ldots + Dm_i$$

It is clear that M_i is a submodule of M, and $M_n = M$.

Suppose D_0 is a submodule of D. We claim that in order to be a submodule, D_0 must be an ideal. Indeed, if $x \in D_0$, then for all $d \in D$, $dx \in D_0$. If α is the D-action defined on D_0, then for any $x, y \in D_0$, $\alpha(1, x + y) = \alpha(1, x) + \alpha(1, y) = x + y \in D_0$. Thus, D_0 must be an ideal. Hence, since D is a Noetherian domain, any ascending chain of ideals in D terminates. This means that any ascending chain of submodules of D terminates, which means D is a D-module.

Define a submodule of D by $N_i = \{d \in D \mid dm_i = 0\}$ for $i = 1, 2, \ldots, n$. Clearly, since N_i is an ideal, N_i is a submodule of D. Thus, from the previous theorem, we conclude that D/N_i is Noetherian, for each i.

We claim that $D/N_i \cong Dm_i$. If $x \in D/N_i$, then $x = d + N_i$ for some $d \in D$. But, this d has the property that $dm_i \neq 0$. So, all $d \notin N_i$ are contained in Dm_i, and thus it is clear that these two modules are isomorphic. In particular, this means that Dm_i is a Noetherian module.

Suppose that $M_1, M_2, \ldots, M_{k-1}$ are Noetherian, for $2 \leq k \leq n$. If we can show that M_k is Noetherian, then we conclude that $M_n = M$, the finitely generated D-module, is Noetherian.

We claim that $Dm_k \bigcap M_{k-1}$ is a submodule of Dm_k. Clearly, we will have $Dm_k \bigcap M_{k-1} \subseteq Dm_k$. As well, if $x \in Dm_l \bigcap M_{k-1}$, then since both of these are modules, for any $d \in D$, $dx \in Dm_1 \bigcap M_{k-1}$, and so we have proven the claim. From the previous theorem, this means the factor module $Dm_k/Dm_k \bigcap M_{k-1}$ is Noetherian, since Dm_k has been shown to be Noetherian.

Hence,

$$M_k/M_{k-1} = (M_{k-1} + Dm_k)/M_{k-1} \cong Dm_k/Dm_k \bigcap M_{k-1}$$

is Noetherian. Then, by the previous theorem, we conclude that M_k is Noetherian. This completes the proof. □

In particular, we see that any finitely generated $\mathbb{Z}$-module is Noetherian.

2.3 Algebraic Elements

Definition 2.3.1. *Suppose $A \subseteq B$ are integral domains. If $\alpha \in B$ is the root of a monic polynomial in $A[x]$, then we say that α is integral over A. Furthermore, if every element in B is integral over A, then we say that B is integral over A. We define an algebraic integer to be a complex number which is integral over $\mathbb{Z}$. We do not prove it here, but is important to note that for integral domains $A \subseteq B \subseteq C$, if C is integral over B and B is integral over A, then C is integral over A. A proof of this can be found in [5].*

If instead of integral domains, we have that A is a field, then if $\alpha \in B$ is integral over A, we instead say that α is algebraic over A. We define an algebraic number to be a complex number which is algebraic over $\mathbb{Q}$. For this section, we will assume that K is a subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$ is algebraic over K. In particular, these theorems will be highly significant when $K = \mathbb{Q}$ and α is an algebraic number.

Theorem 2.3.1. *There exists a unique polynomial $p(x) \in K[x]$, called the minimal polynomial of α over K, which is monic, irreducible and has the least degree such that $p(\alpha) = 0$. Furthermore, if $f(x) \in K[x]$ and $f(\alpha) = 0$, then $p(x) \mid f(x)$.*

Proof. Let $S = \{f(x) \in K[x] \mid f(\alpha) = 0, deg(f) > 0\}$. Suppose $p(x) \in S$ has the least degree. If $p(x)$ is not irreducible, then we can write $p(x) = a(x)b(x)$, for some polynomials $a(x), b(x) \in K[x]$. But $p(\alpha) = a(\alpha)b(\alpha) = 0$. This implies that one of $a(\alpha), b(\alpha)$ is equal to 0, and hence is in S. This contradicts our assumption that $p(x)$ has the least degree, and so we must have that $p(x)$ is irreducible.

Suppose there exist two polynomials in S, $p(x)$ and $q(x)$, which both have the least degree. Then, by the division algorithm, we get $p(x) = a(x)q(x) + r(x)$ for some $a(x), r(x) \in K[x]$ and $0 \leq deg(r) < deg(q)$. But

$$p(\alpha) = a(\alpha)q(\alpha) + r(\alpha) = 0$$

which implies that $r(\alpha) = 0$ and so $r(x) \in S$. Since $p(x)$ and $q(x)$ have least degree, this means to avoid contradiction, we must have $r(x) \notin S$ and so $r = 0$. Thus, $p(x) = a(x)q(x)$ and $deg(p) = deg(q)$ means that $a(x)$ is a constant in K. So, $p(x)$ is unique up to a constant. Since we are in a field, we may assume the leading coefficient of $p(x)$ is 1.

Finally, suppose $f(x) \in S$. If $p(x) \nmid f(x)$, then since $p(x)$ is irreducible, $(p(x), f(x)) = 1$. So, we can find $a(x), b(x) \in K$ such that

$$a(x)p(x) + b(x)q(x) = 1$$

But, $a(\alpha)p(\alpha) + b(\alpha)q(\alpha) = 0 \neq 1$, a contradiction. Thus, $p(x) \mid f(x)$. □

Theorem 2.3.2. *If $m(x)$ is the minimal polynomial of α over K, then $m(x)$ has no repeated roots.*

Proof. Suppose α is twice a root of $m(x)$. Then we have

$$m(x) = (x - \alpha)^2 g(x)$$

for some polynomial $g(x) \in K[x]$. Thus, taking the derivatives, we get

$$m'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$$

Thus, $m'(\alpha) = 0$. But, from the previous theorem, $m(x) \mid m'(x)$. Since $deg(m') < deg(m)$, we have a contradiction, and hence $m(x)$ has no repeated roots. □

Definition 2.3.2. *If $m(x)$ is the minimal polynomial of α over K, then the roots of $m(x)$ are called the conjugates of α (over K). Hence, if $deg(m) = n$, α has n conjugates. As well, we now denote the minimal polynomial of α over K by $min_K(\alpha)$.*

2.4 Algebraic Number Fields

Definition 2.4.1. *Suppose K is a subfield of $\mathbb{C}$. The we define the simple extension $K(\alpha)$ to be the intersection of all subfields of $\mathbb{C}$ containing both K and α. Note that $K(\alpha)$ will be the smallest field containing both K and α. Similarly, we define the multiple extension $K(\alpha_1, \ldots, \alpha_n)$ to be the intersection of all those subfields of $\mathbb{C}$ containing K and every α_i. Note that if $\alpha \in K$, then $K(\alpha) = K$. If $\alpha \in \mathbb{C}$ is algebraic over K, then this is called a (simple) algebraic extension of K.*

Suppose $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ are all algebraic numbers. Then the multiple extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is defined to be an algebraic number field.

Theorem 2.4.1. *Let $K \subseteq \mathbb{C}$ be a field and $\alpha \in \mathbb{C}$ is algebraic over K. Furthermore, suppose $n = deg(min_K(\alpha))$. Then*

$$K(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$$

Proof. Consider the set

$$S = \left\{ \frac{b_0 + b_1\alpha + \ldots + b_k\alpha^k}{c_0 + c_1\alpha + \ldots + c_h\alpha^h} \mid k, h \geq 0, b_i, c_i \in K, c_0 + \ldots + c_h\alpha^k \neq 0 \right\}$$

It is clear that S is a subfield of $\mathbb{C}$. Furthermore, S is a subfield which contains both K and α. Moreover, any subfield of $\mathbb{C}$ which contains both K and α must contain every element of S. Thus, S is the smallest subfield which contains K and α, which means $S = K(\alpha)$.

If $\beta \in S$, then it is of the form

$$\beta = \frac{f(\alpha)}{g(\alpha)}$$

where $f(x), g(x) \in K[x]$ and $g(\alpha) \neq 0$. This last condition implies that $min_K(\alpha) \nmid g(x)$. Furthermore, since $min_K(\alpha)$ is irreducible in $K[x]$, we have

$$< min_K(\alpha), g(x) >= K[x]$$

So, we can find polynomials $m(x), n(x)$ such that $m(x)min_K(\alpha)+g(x)n(x) = 1$. Since $min_K(\alpha)$ has α as a root, we must have $g(\alpha)n(\alpha) = 1$. This gives

$$\frac{1}{g(\alpha)} = n(\alpha)$$

and so $\beta = f(\alpha)n(\alpha)$. Thus, every element $\beta \in S$ can be expressed as some element of $K[x]$.

Suppose $\beta \in S$ and

$$\beta = a_0 + a_1\alpha + \ldots + a_m\alpha^m$$

for $a_i \in K$. Let $h(x) = a_0+a_1x+\ldots a_mx^m$ and so $\beta = h(\alpha)$. By the division algorithm, we can obtain polynomials $q(x), r(x) \in K[x]$ such that

$$h(x) = q(x)min_K(\alpha) + r(x)$$

and $deg(r) < deg(min_K(\alpha))$. Recall that $deg(min_K(\alpha)) = n$. So, since α is a root of $min_K(\alpha)$, we have that

$$h(\alpha) = r(\alpha) = \beta$$

Thus, every element of $K(\alpha)$ is of the form

$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

where $a_i \in K$, $n = deg(min_K(\alpha))$. □

Corollary 2.4.2. *$K(\alpha)$ is algebraic over K.*

We omit the proof, as the corollary seems somewhat intuitive, and the proof is not very illuminating. Those curious can find a proof in [4],[5] or [7].

Definition 2.4.2. *If $E \subseteq E(\alpha) \subseteq F$ is an extension of fields, where $\alpha \in F$ is algebraic over E. Then if $deg(min_E(\alpha)) = n$, the set $\{1, \alpha, \alpha^2, \ldots, \alpha_{n-1}\}$ is called a basis of $E(\alpha)$ over E. In general, let $E \subseteq F$ be a field extension and let $\{\gamma_1, \ldots, \gamma_m\}$ be a collection of elements in F such that every element $\beta \in F$ can be expressed uniquely as*

$$\beta = e_1\gamma_1 + e_2\gamma_2 + \ldots + e_m\gamma_m$$

where $e_i \in E$. Then this set is called a basis of F over E. Since this representation is unique, the basis has the property that if $e_1\gamma_1 + \ldots + e_m\gamma_m = 0$ then $e_i = 0$ for each i. This property is known as linear independence.

Theorem 2.4.3. *If $\mathbb{Q}(\alpha, \beta)$ is an algebraic number field, then there exists some $\gamma \in \mathbb{Q}(\alpha)$ such that*

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$$

Proof. Let $p(x) = min_{\mathbb{Q}}(\alpha)$ and $q(x) = min_{\mathbb{Q}}(\beta)$, with $deg(p) = m$, $deg(q) = n$. Furthermore, let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ and $\beta = \beta_1, \beta_2, \ldots, \beta_n$ denote the m and n conjugates of α and β, respectively. Note that these conjugates are all distinct. Moreover, since $p(x), q(x) \in \mathbb{Q}$ we have that

$$p(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_m) \in \mathbb{Q}[x]$$

and

$$q(x) = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_n) \in \mathbb{Q}[x]$$

Consider the set

$$S = \left\{ \frac{\alpha_r - \alpha_s}{\beta_t - \beta_u} \mid 1 \leq r, s \leq m, 1 \leq t, u \leq n, t \neq u \right\}$$

S is a finite set, whose elements are complex numbers. Let $c \in \mathbb{Q}$ and $c \notin S$. We claim that the set $T = \{\alpha_i + c\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ consists of distinct elements. If $\alpha_i + c\beta_j = \alpha_k + c\beta_l$ for some i, j, k, l, then we get that

$$\frac{\alpha_i - \alpha_k}{\beta_l - \beta_j} = c$$

a contradiction. Thus, the claim holds.

Let $\gamma = \alpha_1 + c\beta_1$ and let $K = \mathbb{Q}(\gamma)$. Furthermore, let $p_1(x) = p(\gamma - cx)$. Notice that $p_1(x) \in K[x]$. Now, since $p_1(\beta) = p(\gamma - c\beta) = 0$ (since $\beta_1 = \beta$), we have that β is a common root of $p_1(x)$ and $q(x)$. We claim that this is the only common root of $p_1(x)$ and $q(x)$. Suppose not, and that $\lambda \in \mathbb{C}$ is a root of both polynomials. Also, assume that $\lambda \neq \beta$. Thus, since $q(\lambda) = 0$, $\lambda = \beta_j$ for some j and $2 \leq j \leq n$. Now, we have

$$p(\gamma - c\beta_j) = p_1(\beta_j) = 0$$

and so $\gamma - c\beta_j = \alpha_k$, with $2 \leq k \leq m$. Hence,

$$\gamma = \alpha_k + c\beta_j = \alpha_1 + c\beta_1$$

which is a contradiction, as seen before. This proves the claim.

Now, let $h(x) = \min_K(\beta)$. Then $h(x) \mid p_1(x)$ and $h(x) \mid q(x)$. Since $p_1(x)$ and $q(x)$ only have one common root, we must have $deg(h) = 1$, say $h(x) = x + \delta$, where $\delta \in K$. Now, $h(\beta) = 0 = \beta + \delta$ and so $\beta = -\delta \in K$. Then $\alpha = \gamma - c\beta \in K$ shows that

$$\mathbb{Q}(\alpha, \beta) \subseteq K = \mathbb{Q}(\gamma)$$

Conversely, since $\gamma = \alpha + \beta$, we have $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta)$ which implies equality. □

Corollary 2.4.4. *If $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is an algebraic number field, then there exists some $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ such that*

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\alpha)$$

Proof. We can view the multiple extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ as a number of successive simple extensions. Specifically,

$$\mathbb{Q}(\alpha_1, \alpha_2) = (\mathbb{Q}(\alpha_1))(\alpha_2)$$

Thus, when $n = 2$, the case has already been proven. Let $\mathbb{Q}(\beta_1) = \mathbb{Q}(\alpha_1, \alpha_2)$. Then

$$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = (\mathbb{Q}(\beta_1))(\alpha_3) = \mathbb{Q}(\beta_1, \alpha_3)$$

and we let $\mathbb{Q}(\beta_2) = \mathbb{Q}(\beta_1, \alpha_3)$. Continuing in this fashion, we see we will eventually end up with $\mathbb{Q}(\beta_{n-1}) = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. □

Definition 2.4.3. *If $\mathbb{Q}(\alpha)$ is an algebraic number field, and $deg(min_{\mathbb{Q}}(\alpha)) = n$, then the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is defined by*

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$$

2.5 The Monomorphisms Of An Algebraic Number Field

Lemma 2.5.1. *Let K is a subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$ is algebraic over K. Then if β is any conjugate of α,*

$$min_K(\alpha) \sim min_K(\beta)$$

Proof. Let $\alpha = \alpha_1, \ldots, \alpha_m$ denote the conjugates of α. Then, $\beta = \alpha_k$ for some k. Since

$$min_K(\alpha) = (x - \alpha_1) \ldots (x - \alpha_k) \ldots (x - \alpha_m)$$

we have that α_k is a root of $min_K(\alpha)$. So, $min_K(\alpha_k) = min_K(\beta) \mid min_K(\alpha)$. But $min_K(\alpha)$ is irreducible, and so we must have $min_K(\alpha) = \mu min_K(\beta)$, where μ is some unit. Thus, $min_K(\alpha) \sum min_K(\beta)$ as claimed. □

Theorem 2.5.1. *Let K be an algebraic number field with $n = [K : \mathbb{Q}]$. Then there are exactly n distinct monomorphisms $\sigma_k : K \to \mathbb{C}$, with $k = 1, 2, \ldots n$.*

Proof. Let $\theta \in K$ be an algebraic number such that $K = \mathbb{Q}(\theta)$. Also, let $p(x) = \min_{\mathbb{Q}}(\theta)$. Then $deg(p) = deg(min_{\mathbb{Q}}(\theta)) = [K : \mathbb{Q}] = n$ and so there are n distinct conjugates of θ over $\mathbb{Q}$. Denote these by $\theta = \theta_1, \theta_2, \ldots, \theta_n$ and so

$$p(x) = (x - \theta_1)(x - \theta_2) \ldots (x - \theta_n)$$

For any $\alpha \in K$, α can be expressed uniquely in the form $\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$, for $a_i \in \mathbb{Q}$. Define $\sigma_k : K \to \mathbb{C}$ by

$$\sigma_k(\alpha) = \sigma_k(a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}) = a_0 + a_1\theta_k + \ldots + a_{n-1}\theta_k^{n-1}$$

We claim that σ_k is a field homomorphism, for $k = 1, \ldots, n$.

Let $\alpha, \beta \in K$ with

$$\alpha = \sum_{i=0}^{n-1} a_i\theta^i \text{ and } \beta = \sum_{i=0}^{n-1} b_i\theta^i$$

for some $a_i, b_i \in \mathbb{Q}$. Then we have

$$\sigma_k(\alpha) + \sigma_k(\beta) = \sum a_i\theta_k^i + \sum b_i\theta_k^i = \sum (a_i + b_i)\theta_k^i = \sigma_k(\alpha + \beta)$$

Keeping the same notation, we let $f(x) = \sum a_i x^i$ and $g(x) = \sum b_i x^i$, so that $f(x), g(x) \in \mathbb{Q}[x]$ and $f(\theta) = \alpha$, $g(\theta) = \beta$. By the division algorithm, there exist $q(x), r(x) \in \mathbb{Q}[x]$ such that

$$f(x)g(x) = q(x)p(x) + r(x)$$

and $deg(r) < deg(p) = n$. Since $p(\theta) = 0$ we get $\alpha\beta = f(\theta)g(\theta) = r(\theta)$. Furthermore, we have $p(\theta_k) = 0$ and so $f(\theta_k)g(\theta_k) = r(\theta_k)$ for each conjugate θ_k. Thus,

$$\sigma_k(\alpha\beta) = \sigma_k(r(\theta)) = r(\theta_k) = f(\theta_k)g(\theta_k) = \sigma_k(\alpha)\sigma_k(\beta)$$

This shows that the mappings σ_k are additive and multiplicative, and hence σ_k is a homomorphism, for $k = 1, \ldots, n$.

We now show that σ_k is a 1:1 mapping. Keeping the above notation, suppose that $\sigma_k(\alpha) = \sigma_k(\beta)$ and thus

$$a_0 + a_1\theta_k + \ldots a_{n-1}\theta_k^{n-1} = b_0 + b_1\theta_k + \ldots + b_{n-1}\theta_k^{n-1}$$

So, θ_k is a root of

$$\sum_{i=0}^{n-1}(a_i - b_i)x^i \in \mathbb{Q}[x]$$

Since $min_{\mathbb{Q}}(\theta_k) = p(x)$, we have that the above polynomial must be the zero polynomial. (If not, then this would contradict the degree of $min_{\mathbb{Q}}(\theta_k)$.) Thus, we must have $a_i = b_i$ for each i and so $\alpha = \beta$. This shows that σ_k is an injective map.

Finally, suppose $\lambda : K \to \mathbb{C}$ is another monomorphism. Then $p(\lambda(\theta)) = \lambda(p(\theta)) = \lambda(0) = 0$ and so $\lambda(\theta) = \theta_k$ for some k. Thus, $\lambda(\theta) = \sigma_k(\theta)$ and we have

$$\lambda(\sum_{i=0}^{n-1} a_i\theta^i) = \sum_{i=0}^{n-1} a_i\theta_k^i = \sigma_k(\sum_{i=0}^{n-1} a_i\theta^i)$$

Hence, the set $\{\sigma_k \mid k = 1, \ldots, n\}$ consists of all monomorphisms from K to $\mathbb{C}$. □

2.6 The Ring Of Integers

Definition 2.6.1. *Let K be an algebraic number field. Then the collection of all algebraic integers of K forms an integral domain, which we denote by O_K. We omit the proof of this fact here, but those interested may find it in [4] or [5].*

Definition 2.6.2. *Suppose $L \supseteq K$ is a finite algebraic extension of fields, with $n = [L : K]$. Furthermore, suppose $\gamma_1, \gamma_2, \ldots, \gamma_n \in K$ is a basis for L and $\alpha \in L$. Then, for each γ_i we have*

$$\alpha\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j$$

where $a_{ij} \in K$. Notice that the coefficients form an $n \times n$ matrix.

We define the trace of an element α, denoted by $t(\alpha)$ to be $a_{11} + a_{22} + \ldots + a_{nn}$.

Definition 2.6.3. *Suppose $\alpha_1, \alpha_2, \ldots, \alpha_n$ are elements of L, the algebraic extension defined above. Then we define the discriminant of these n elements, denoted by $\Delta(\alpha_1, \ldots, \alpha_n)$ to be $det(t(\alpha_i\alpha_j))$ where $i, j = 1, 2, \ldots, n$.*

For the remainder of this section, we work in a generic algebraic number field K, with ring of integers O_K. As well, we will assume all our ideals are non-zero. Recall that if K is an algebraic number field, $K = \mathbb{Q}(\theta)$ for some $\theta \in \mathbb{C}$. If we assume that $n = [K : \mathbb{Q}]$, then $\{1, \theta, \ldots, \theta^{n-1}\}$ will be a basis for K over $\mathbb{Q}$. We mention this in order to point out that a basis for K over $\mathbb{Q}$ does exist. We use this fact in the remainder of the chapter.

Lemma 2.6.1. *Suppose $\beta \in K$. Then there exists an integer $b \neq 0$ such that $b\beta \in O_K$.*

Proof. Since K is an algebraic number field, all elements of K are algebraic. Thus, for some elements $a_0, \ldots a_n \in \mathbb{Z}$ we have

$$a_n\beta^n + \ldots + a_1\beta + a_0 = 0$$

and we assume $a_n \neq 0$. If we multiply this equation by a_n^{n-1} we get

$$(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + a_{n-2}a_{n-1}(a_n\beta)^{n-2} + \ldots + a_1a_n^{n-2}(a_n\beta) + a_0a_n^{n-1}$$

Thus, $a_n\beta$ is an algebraic integer. □

Lemma 2.6.2. *Every ideal A of O_K contains a basis for K over $\mathbb{Q}$.*

Proof. Let $\beta_1, \ldots, \beta_n$ be a basis of K over $\mathbb{Q}$. By the previous lemma, there exists a nonzero integer b such that $b\beta_1, \ldots, b\beta_n \in O_K$. Choose $\alpha \in A$, $\alpha \neq 0$. Then the elements $b\beta_1\alpha, \ldots, b\beta_n\alpha$ are in A and are a basis for K over $\mathbb{Q}$. □

Lemma 2.6.3. *Suppose $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are bases for K. Let $\alpha_i = \sum_{j=1}^{n} a_{ij}\beta_j$. Then $\Delta(\alpha_1, \ldots, \alpha_n) = det(a_{ij})^2 \Delta(\beta_1, \ldots, \beta_n)$.*

Proof. Consider the identity

$$\alpha_i \alpha_k = \left(\sum_{j=1}^{n} a_{ij}\beta_j \right) \left(\sum_{l=1}^{n} a_{kl}\beta_l \right) = \sum_{j=1}^{n} \sum_{l=1}^{n} a_{ij} a_{kl} \beta_j \beta_l$$

We take the trace of both sides. Let $A = (t(\alpha_i \alpha_j))$, $B = (t(\beta_j \beta_l))$, and $C = (a_{ij})$. The we find the matrix identity $A = C'BC$ where C' is the transpose of C. Since $detC' = detC$, taking the determinant of both sides results in the lemma. □

Theorem 2.6.1. *Let A be an ideal in O_K and suppose $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ is a basis for K with $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ minimal. Then $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \ldots + \mathbb{Z}\alpha_n$.*

Proof. Consider the set S of all discriminants $|\Delta|$ of bases in A. Because we are taking the absolute value of the discriminants, there exists a basis with the least discriminant. Assume $\alpha_1, \ldots, \alpha_n$ is such a basis.

Suppose $\alpha \in A$ with $\alpha = \gamma_1\alpha_1 + \ldots + \gamma_n\alpha_n$ with $\gamma_i \in \mathbb{Q}$. Assume that $\gamma_i \notin \mathbb{Z}$. Let $\gamma_i = m + \theta$ where $m \in \mathbb{Z}$ and $0 < \theta < 1$. Let $\beta_1 = \alpha_1$, $\beta_2 = \alpha_2$, …, $\beta_i = \alpha - m\alpha_i$, …, $\beta_n = \alpha_n$.Then $\beta_1, \ldots, \beta_n \in A$ and is a basis for K. Since $\beta_i = \gamma_1\alpha_1 + \ldots + \theta\alpha_i + \ldots + \gamma_n\alpha_n$, the transition matrix between these two bases is an $n \times n$ identity matrix with the i^{th} row replaced by

$$[\gamma_1 \ \gamma_2 \ \ldots \ \gamma_{i-1} \ \theta \ \ldots \ \gamma_n]$$

By the previous lemma, we have that

$$\Delta(\beta_1, \ldots, \beta_n) = \theta^2 \Delta(\alpha_1, \ldots, \alpha_n)$$

which contradicts the minimality of $|\Delta(\alpha_1, \ldots, \alpha_n)|$ since $0 < \theta < 1$. Hence, $\gamma_i \in \mathbb{Z}$ and the theorem follows. □

Corollary 2.6.2. *O_K is a Noetherian domain*

Proof. Since O_K is a finitely generated $\mathbb{Z}$-module, it is Noetherian. This follows from theorem 1.2.3, since $\mathbb{Z}$ is a Noetherian domain. □

Lemma 2.6.4. *Suppose I is an ideal contained in O_K. Then $I \bigcap \mathbb{Z} \neq 0$.*

Proof. Suppose $\alpha \in I$, $\alpha \neq 0$. Thus, α is an algebraic integer and there exist constants $a_0, \ldots, a_{n-1}$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$$

If $a_0 \neq 0$ then we're done. Assume $a_0 = 0$. Since $\alpha \neq 0$, we have $\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1) = 0$ Hence, if $a_1 \neq 0$, we're done. Otherwise, we continue in this fashion until we find an a_i such that $\alpha^{n-i} + \ldots + a_i = 0 \in I$ which implies $a_i \in I$, which implies the lemma. □

Theorem 2.6.3. *For any ideal A, O_K/A is finite.*

Proof. By the previous lemma, there exists an integer $a \neq 0$ such that $a \in A$. Let $< a >$ denote the principal ideal generated by a in O_K. Consider $O_K/ < a >= \{r+ < a > | r \in O_K\}$. Since $a \in A$, for all $r \in O_K$, $ra \in A$. Thus, the map $\phi : O_K/ < a > \rightarrow O_K/A$ given by $\phi(\rho) = \phi(r+ < a >) = r+a$ is an onto map, where $\rho \in O_K/ < a >$ and $\rho = r+ < a >$ for some $r \in O_K$.

Hence, it is sufficient to show that $O_K/ < a >$ has finitely many elements.

Suppose $\omega_1, \ldots, \omega_n$ is a basis for K over $\mathbb{Q}$, and $\omega_i \in O_K$. Then we can write $O_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \ldots + \mathbb{Z}\omega_n$. Let $S = \{\gamma_i\omega_i | 0 \leq \gamma_i < a, \gamma_i \in \mathbb{Z}\}$. We will show that S is a set of coset representatives for $O_K/ < a >$.

If $\omega \in O_K$, then

$$\omega = \sum_{i=1}^{n} m_i\omega_i$$

for some $m_i \in \mathbb{Z}$. Since $a \in \mathbb{Z}$, we use the division algorithm and write $m_i = q_ia + \gamma_i$, where $0 \leq \gamma_i < a$. Thus, $m_i \equiv \gamma_i \pmod{a}$ and hence $\omega \equiv \sum \gamma_i\omega_i \pmod{a}$. Hence, the coset ω can be represented as an element of S, as claimed.

If $\sum \gamma_i\omega_i$ and $\sum \gamma_i'\omega_i$ are in S and in the same coset modulo a, then since the ω_i are linearly independent

$$\sum \gamma_i\omega_i = \sum \gamma_i'\omega_i \Rightarrow \sum \omega_i(\gamma_i - \gamma_i') = 0$$

implies that $\gamma_i = \gamma_i'$. Hence, S is a set of coset representatives. □

Corollary 2.6.4. *$O_K/ < a >$ has a^n elements.*

Proof. We prove this by induction on n. If $O_K/ < a >= \mathbb{Z}\omega_1 = \{\gamma_1\omega_1 \mid 0 \leq \gamma_1 < a, \gamma_i \in \mathbb{Z}\}$, then clearly $|O_K/ < a > | = a$. (In fact, any coset contains a elements.)

Suppose this holds true for basis of up to $n-1$ elements. If $O_K/ < a >= \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$, then since there are a elements in ω_n and a^{n-1} elements in

$\mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_{n-1}$, there are $aa^{n-1} = a^n$ elements in $O_K/ < a >$, and the corollary follows. □

Corollary 2.6.5. *$|O_K/A| \leq a^n$. Equality holds if A is a principal ideal generated by an integer.*

Proof. In the proof of the theorem, we showed that $|O_K/A| \leq |O_K/ < a >|$, where $a \in A \bigcap \mathbb{Z}$. From the previous corollary, the conclusion to this corollary follows immediately. □

2.7 O_K Is Integrally Closed

Definition 2.7.1. *Suppose K is any integral domain. We define the quotient field of K, denoted $Q(K)$ to be the set*

$$\{[a, b] \mid a, b \in K, b \neq 0\}$$

where $[a, b]$ and $[c, d]$ are equal if $ad - bc = 0$. Multiplication is done component-wise, and addition $[a, b] + [c, d] = [ad + bc, bd]$. It is easily checked that $Q(K)$ is a field. As well, we usually write $[a, b] = \frac{a}{b}$.

K is integrally closed if every element of the quotient field $Q(K)$ which is integral over K is contained in K.

Lemma 2.7.1. *If α is an algebraic number, then $\alpha = \frac{a}{b}$ where a is an algebraic integer and b is some nonzero integer.*

Proof. Suppose α is a root of

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

where $a_i \in \mathbb{Q}$. Let b be the least common multiple of the denominators of $a_1, \ldots, a_{n-1}$ Then

$$(b\alpha)^n + (ba_{n-1})(b\alpha)^{n-1} + \ldots + (b^{n-1}a_1)(b\alpha) + (b^n a_0) = 0$$

where $b^i a_j \in \mathbb{Z}$ and $b \in \mathbb{Z}$. Hence, $b\alpha$ is an algebraic integer, say a. Thus $\alpha = \frac{a}{b}$ where a is an algebraic integer, and b is a nonzero integer. □

Lemma 2.7.2. *For any algebraic number field K, the quotient field of O_K is K.*

Proof. Suppose A is the quotient field of O_K. If $\alpha \in A$, then $\alpha = \frac{a}{b}$ for some $a, b \in O_K$ with $b \neq 0$. Since $O_K \subseteq K$, $a, b \in K$ and hence $\alpha = \frac{a}{b} \in K$. Hence, $A \subseteq K$.

Conversely, if $\alpha \in K$, then α is an algebraic number. Thus, we can write $\alpha = \frac{a}{b}$ where a is an algebraic integer and b is a non-zero integer. Thus, since $\mathbb{Z} \subseteq O_K$ and O_K contains all algebraic integers of K, we have $a, b \in O_K$ and hence $\alpha \in A$. Hence, $K \subseteq A$ which implies equality. □

Theorem 2.7.1. *Let K be an algebraic number field. Then O_K is integrally closed.*

Proof. From the previous lemma, the quotient field of O_K is K. Suppose $\alpha \in K$ is integral over O_K. Since O_K is integral over $\mathbb{Z}$, we have that α is integral over $\mathbb{Z}$. This, by definition, means that α is an algebraic integer, and hence $\alpha \in O_K$. Thus, O_K is integrally closed. □

2.8 Dedekind Domains

Definition 2.8.1. *Suppose R is a ring that satisfies the following three properties*

1. *R is a Noetherian domain*
2. *Every prime ideal of R is maximal*
3. *R is integrally closed.*

Then we call R a Dedekind domain, or a Dedekind ring.

For the remainder of this section, we will assume that K is an algebraic number field with ring of integers O_K.

Lemma 2.8.1. *Every prime ideal of O_K is a maximal ideal.*

Proof. Let P be a prime ideal of O_K. Then O_K/P is a finite integral domain. This follows from Lemma 2.1.2 and the fact that O_K/P is finite. We claim that any finite integral domain is a field. If this claim holds, then we have proven the lemma.

Suppose $|O_K/P| = n$, with distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n$. Choose some nonzero element $\beta \in O_K/P$ and consider the set $S = \beta(O_K/P) = \{\beta\alpha_1, \ldots, \beta\alpha_n\}$. The elements of S are all distinct, as $\beta\alpha_i = \beta\alpha_j$ implies $\alpha_i = \alpha_j$, which happens only if $i = j$. Hence, since $S \subseteq O_K/P$ and S has n elements, this implies that $S = O_K/P$. In particular, this implies $1 \in S$, say $1 = \beta\alpha_k$. This means that β is a unit and hence O_K/P is a field. □

Theorem 2.8.1. *O_K is a Dedekind domain*

Proof. We've already seen that O_K is a Notherian domain and O_K is integrally closed. From the lemma, we can conclude that O_K is a Dedekind domain. □

Definition 2.8.2. *Let D be an integral domain. Denote the quotient field of D by D'. If A is a (nonempty) subset of D' such that*

1. *$\alpha \in A$, $\beta \in A$ implies that $\alpha + \beta \in A$*
2. *$\alpha \in A$, $r \in D$ implies that $r\alpha \in A$*
3. *There exists some nonzero $\gamma \in D$ such that $\gamma A \subseteq D$.*

then A is called a fractional ideal of D.

Lemma 2.8.2. *If I is an ideal of O_K such that $I \neq O_K$ then I contains a product of prime ideals.*

Proof. Assume the contrary, there exists at least one proper ideal in O_K that does not contain a product of prime ideals. Let S denote the set of all such ideals. Since O_K is Noetherian, there must be a maximal ideal in S, say A. We have that A must not be a prime ideal, and so there exists $a, b \in O_K$ such that $ab \in A$, $a \notin A$ and $b \notin A$. Let $< A, a >$ denote the ideal generated by A and a. We have $< A, a >= \{r_1 A + r_2 a \mid r_1, r_2 \in O_K\}$ and hence $A \subset < A, a >$. Similarly, A is also properly contained in $< A, b >$. Furthermore, since A is the maximal element of S, both $< A, a >$ and $< A, b >$ are not in S. Hence, we have

$$< A, a > \supseteq P_1 \dots P_m$$

and

$$< A, b > \supseteq Q_1 \dots Q_n$$

for prime ideals P_i, Q_j $1 \leq i \leq m$, $1 \leq j \leq n$.

Now, consider

$$\begin{aligned} < A, a >< A, b > &= \{\sum (r_1 A + r_2 a)(s_1 A + s_2 b) \mid r_1, r_2, s_1, s_2 \in O_K\} \\ &= \{\sum t_1 A + t_2 aA + t_3 bA + t_4 ab \mid t_1, t_2, t_3, t_4 \in O_K\} \\ &= \{\sum uA + vab \mid u, v \in O_K\} \\ &= < A, ab > \end{aligned}$$

But, since $ab \in A$ we have $A =< A, ab >$. Hence,

$$A =< A, ab >=< A, a >< A, b >\supseteq P_1 \dots P_m Q_1 \dots Q_n$$

is a contradiction. Thus, the set S must be empty and hence any ideal of O_K contains a product of prime ideals. □

Lemma 2.8.3. *Let P be a prime ideal of O_K. Then there exists $z \in K$, $z \notin O_K$ such that $zP \subseteq O_K$.*

Proof. Let $x \in P$ and consider $< x >$. By the previous lemma, $< x >$ contains a product of prime ideals. Let r be the least integer such that $< x >$ contains a product of r prime ideals. Thus we have

$$P_1 \dots P_r \subseteq < x > \subseteq P$$

for prime ideals P_i. Hence, $P_i \subseteq P$ for some prime ideal. Without loss of generality, we can assume $P_1 \subseteq P$. But, P_1 is a prime ideal in O_K, and so, it is a maximal ideal. Hence, we must have $P_1 = P$.

Now, since r was assumed to be minimal, we have $P_2 \dots P_r \not\subseteq < x >$. If $y \in P_2 \dots P_r$, then $y \notin (x)$. Thus, for $x^{-1} \in K$,

$$\begin{aligned} yx^{-1}P &= yx^{-1}P_1 \\ &\subseteq (P_2 \dots P_r)(x^{-1}P_1) \\ &= x^{-1}(P_1 P_2 \dots P_r) \\ &\subseteq x^{-1} < x >= x^{-1} \cdot \{rx \mid r \in O_K\} \\ &= O_K \end{aligned}$$

Let $z = yx^{-1}$. Then $zP \subseteq O_K$.

Suppose $z \in O_K$. Then $yx^{-1} \in O_K$ and $y \in xO_K = (x)$, a contradiction. Hence, $z \in K$, $z \notin O_K$ and $zP \subseteq O_K$ as claimed. □

Definition 2.8.3. *Let P be a prime ideal in O_K. Define*

$$P^{-1} = \{x \in K \mid xP \subseteq O_K\}$$

Theorem 2.8.2. *Let P be a prime ideal of O_K. The P^{-1} is a fractional ideal and $PP^{-1} = O_K$.*

Proof. We first show that P^{-1} is a fractional ideal. If $\alpha, \beta \in P^{-1}$ then $\alpha P \subseteq O_K$, $\beta P \subseteq O_K$. Hence, $(\alpha + \beta)P \subseteq \alpha P + \beta P \subseteq O_K$. As well, for $r \in O_K$, $\alpha \in P^{-1}$ we have $\alpha P \subseteq O_K$ and hence $r\alpha P \subseteq O_K$ and so $r\alpha \in P^{-1}$. Thus, P^{-1} is an ideal of O_K. Furthermore, suppose $\beta \in P$, $\beta \neq 0$. Then for any $\alpha \in P^{-1}$ we have $\alpha P \subseteq O_K$ and specifically we have $\alpha\beta \in O_K$. Hence, $\beta P^{-1} \subseteq O_K$ and P^{-1} is a fractional ideal.

We now show that $PP^{-1} = O_K$ or $PP^{-1} = P$. Since P and P^{-1} are both fractional ideals of O_K, so is PP^{-1}. Clearly, $PP^{-1} \subset O_K$ and so PP^{-1} is an ideal in O_K. Since $1 \in P^{-1}$, we have $P \subseteq PP^{-1}$. So, since P is a prime ideal, it is maximal. Thus, since we have $P \subseteq PP^{-1} \subseteq O_K$, either $PP^{-1} = O_K$ or $PP^{-1} = P$.

We claim that $O_K \subset P^{-1}$. For any $\alpha \in O_K$, $\alpha P \subseteq O_K$, and thus $\alpha \in P^{-1}$. So, we have $O_K \subseteq P^{-1}$. It remains to show that there exists some element $\gamma \in P^{-1}$ which is not in O_K. Suppose β is a non-zero element of P. Then by Lemma 2.8.2, there exist prime ideals $P_1, \ldots, P_k$, with $k \geq 1$ such that

$$< \beta > \supseteq P_1 P_2 \ldots P_k$$

Choose k to be the least such integer for which this inclusion holds. So, because

$$P_1 P_2 \ldots P_k \subseteq < \beta > \subseteq P$$

then for some i, with $1 \leq i \leq k$, we have $P_i \subseteq P$. We relabel this, if necessary, so that $P_i = P_1$ and we have $P_1 \subseteq P$. But, P_1 is a prime ideal, and hence is maximal. Thus $P_1 = P$, since $P \neq O_K$.

If $k = 1$, then $P = P_1 =< \beta >$ and since $\beta \neq 0$, we let $\gamma = \frac{1}{\beta} \in K$. If we suppose $\gamma \in O_K$, then β is a unit, which contradicts the fact that P is a prime ideal. Thus, $\gamma \in K$. Notice also that $\gamma P = \frac{1}{\beta} < \beta >= O_K$ and so $\gamma \in P$. So, when $k = 1$, $O_K \subset P^{-1}$.

Suppose $k \geq 2$. Then we have $P_2 \ldots P_k \not\subseteq < \beta >$, by the minimality of k. So, choose some $\delta \in P_2 \ldots P_k$ and $\delta \notin < \beta >$. Then we define $\gamma = \frac{\delta}{\beta} \in K$. Note that $\gamma \notin O_K$, as that would mean $\gamma\beta = \delta \in < \beta >$, which is a contradiction. But, we have that

$$P < \delta >= P_1 < \delta > \subseteq P_1 P_2 \ldots P_k \subseteq < \beta >$$

This means that $P\gamma = P\frac{\delta}{\beta} \subseteq O_K$ and hence $\gamma \in P^{-1}$. Thus, we have proven the claim.

Finally, we show that $PP^{-1} = O_K$. Recall that $PP^{-1} = P$ or $PP^{-1} = O_K$. If we show that $PP^{-1} \neq P$, then we're done. Assume the contrary, that $PP^{-1} = P$. Then $xP \subseteq P$ for all $x \in P^{-1}$. Since P is a finitely generated

$\mathbb{Z}$-module, $xP \subseteq P$ means that $x \in O_K$ for all $x \in P^{-1}$. So, $P^{-1} \subseteq O_K$. But, we've just seen that $O_K \subseteq P^{-1}$ so we conclude that $PP^{-1} \neq P$. Hence, $PP^{-1} = O_K$. □

Theorem 2.8.3. *Any ideal of O_K can be expressed uniquely as a product of prime ideals.*

Proof. We first show the existence of the theorem, then finish with the uniqueness.

Let S be the set of ideals in O_K that cannot be written as a product of prime ideals. Since O_K is Noetherian, S has a maximal element, say A. We have that $A \subseteq P$ for some prime ideal P, since prime ideals are maximal in O_K. Notice that $A \neq P$, since that would contradict our assumption of $A \in S$.

Consider $P^{-1}A$. We have $P^{-1}A \subset P^{-1}P = O_K$. Let $x \in P$ and $x \in A$. Then

$$P^{-1}x \subseteq P^{-1}A$$

which implies

$$x \in PP^{-1}A = O_K A = A$$

which is not true. Thus, $P^{-1}A$ is a proper ideal of O_K and contains A properly since P^{-1} contains O_K properly. Thus, $P^{-1}A \notin S$ since A is a maximal element of S. Thus, $P^{-1}A = P_1 \dots P_r$ for some prime ideals P_i. Then, $PP^{-1}A = PP_1 \dots P_r$, so $A = PP_1 \dots P_r$. But then $a \notin S$, a contradiction. Hence, S is empty and every ideal can be expressed as a product of prime ideals.

Suppose that $A = P_1 \dots P_r = Q_1 \dots Q_s$ are two factorizations of A as a product of prime ideals. Then $Q_1 \supseteq Q_1 \dots Q_s = P_1 \dots P_r$, so $Q_1 \supseteq P_i$ for some i. Without loss of generality, we can assume $Q_1 \supseteq P_1$. But, P_1 is maximal and hence $Q_1 = P_1$. Hence, multiplying both sides by Q_1^{-1} we see that $Q_2 \dots Q_s = P_2 \dots P_r$. We continue in the manner above and conclude that $r = s$ and $Q_i = P_i$ for $1 \leq i \leq s$. Hence, aside from the order, an ideal expressed as a product of prime ideals is unique. □

2.9 The EFG Theorem

For this section, we assume K is an algebraic number field with $[K : \mathbb{Q}] = n$.

Definition 2.9.1. *If A is an ideal in O_K then*

$$A = \prod_{i=1}^{g} P_i^{e_i}$$

for some prime ideals P_i. We define the order of the ideal A with respect to the prime ideal P_i to be the integer e_i. We denote this by $ord_{P_i}(A) = e_i$. If $\alpha \in O_K$, then

$$ord_P(< \alpha >) = ord_P(\alpha)$$

Additionally, we call e_i the ramification degree.

Suppose P is a prime ideal containing $p \in \mathbb{Z}$. Then O_K/P is a finite field containing $\mathbb{Z}/p\mathbb{Z}$. Thus, we can infer that $|O_K/P| = p^f$, for some integer $f \geq 1$. We call f the degree of P.

Theorem 2.9.1. *For ideals $A, B \in O_K$ and a prime ideal P, we have the following properties*

1. $ord_P(P) = 1$
2. *If $Q \neq P$ is a prime ideal, then $ord_P(Q) = 0$*
3. $ord_P(AB) = ord_P(A) + ord_P(B)$

Proof. The first two conditions follow almost immediately from the definition. Hence, we only prove the third condition. We can express A and B as unique products of prime ideals. Specifically, we let

$$A = P_1^{a_1} P_2^{a_2} \dots P_m^{a_m}$$

and

$$B = Q_1^{b_1} Q_2^{b_2} \dots Q_m^{b_m}$$

Suppose P is a prime ideal common to both A and B. Without loss of generality, we can assume $P = P_1 = Q_1$. Thus since $AB = P_1^{a_1} Q_1^{b_1} \dots P_m^{a_m} Q_m^{b_m} = P^{a_1+b_1} \dots Q_m^{b_m}$ we have

$$ord_P(AB) = a_1 + b_1 = ord_P(A) + ord_P(B)$$

□

Definition 2.9.2. *Suppose A and B are ideals of a ring R. Then*

$$A \oplus B = \{(a, b) \mid a \in A, b \in B\}$$

Furthermore, addition and multiplication are done component-wise.

Lemma 2.9.1. *Let R be a commutative ring. Suppose $A_1, A_2, \dots, A_g$ are ideals such that $A_i + A_j = R$ whenever $i \neq j$. Then if we let $A = A_1 A_2 \dots A_g$ we have*

$$R/A \cong R/A_1 \oplus R/A_2 \oplus \dots \oplus R/A_g$$

Proof. Let ψ_i be the map from R to R/A_i given by $\psi(r) = r + A_i$. We define $\psi : R \to R/A_1 \oplus \ldots \oplus R/A_g$ by $\psi(\gamma) = (\psi_1(\gamma), \psi_2(\gamma), \ldots, \psi_g(\gamma))$. We will show that ψ is an onto map and the kernel is A. Then, the isomorphism theorem for rings tells us that, for a ring homomorphism $\phi : R_1 \to R_2$ with $B = ker(\phi)$, $\overline{\phi} : R_1/B \to \phi(R_1)$ is an isomorphism, given by $\overline{\phi}(r+B) = \phi(r)$, for all $r \in R_1$. (A proof of the isomorphism theorem is given in [7].) Thus, this will tell us that $\overline{\psi}(R/A) \to \psi(R) = R/A_1 \oplus \ldots \oplus R/A_g$ is an isomorphism.

To show that ψ is onto, it is sufficient to show that for any $\gamma_1, \ldots, \gamma_g \in R$, the set of simultaneous congruences $x \equiv \gamma_i(A_i)$ is solvable for each i.

Consider $(A_1 + A_2)(A_1 + A_3)\ldots(A_1 + A_g) = R$. Expanding this, we see that each term of the expansion contains the ideal A_1, except the final summand, $A_2 \ldots A_g$. Since $A_1 \supseteq A_1 I$ for any ideal I, we have that A_1 contains each summand except the last. Thus, $A_1 + A_2 A_3 \ldots A_g = R$. So, there exist elements $v_1 \in A_1$, $u_1 \in A_2 \ldots A_g$ such that $u_1 + v_1 = 1$. Thus, we get $u_1 \equiv 1 \pmod{A_1}$ and $u_1 \equiv 0 \pmod{A_i}$ for $2 \leq i \leq g$. Similarly, for each j there is a u_j such that $u_j \equiv 1 \pmod{A_j}$ and $u_j \equiv 0 \pmod{A_i}$ for $i \neq j$. Thus, we let $x = \gamma_1 u_1 + \gamma_2 u_2 + \ldots \gamma_g u_g$, which is a solution for the simultaneous set of congruences.

Clearly, $ker(\psi) = A_1 \bigcap A_2 \bigcap \ldots \bigcap A_g$. We claim that this intersection is equal to $A_1 A_2 \ldots A_g$. We prove this by induction on g. If $g = 2$, then since $A_1 + A_2 = R$ there exist $a_1 \in A_1$ and $a_2 \in A_2$ such that $a_1 + a_2 = 1$. If $a \in A_1 \bigcap A_2$, then $a = a(a_1 + a_2) = aa_1 + aa_2 \in A_1 A_2$. Thus, $A_1 \bigcap A_2 \subseteq A_1 A_2$. Clearly, $A_1 A_2 \subseteq A_1 A_2$, and so we have equality.

Now suppose $g > 2$ and we have proved up to the $g - 1^{st}$ case. Then $A_1 \bigcap A_2 \bigcap \ldots \bigcap A_g = A_1 \bigcap A_2 A_3 \ldots A_g$ by the induction hypothesis. Above, we've seen that $A_1 + A_2 \ldots A_g = R$, and so we repeat the process similar to that of $g = 2$ to conclude that $A_1 \bigcap \ldots \bigcap A_g = A_1 \ldots A_g$. Since $A_1 \ldots A_g = A$, we've shown that $ker(\psi) = A$, and we're done. □

Lemma 2.9.2. *If P is a prime ideal in O_K with $|O_K/P| = p^f$ then $|O_K/P^e| = p^{ef}$, where e is any positive integer.*

Proof. We prove this lemma by induction on e. Clearly, when $e = 1$ the lemma holds. Now suppose $e > 1$ and we've proven up to the $e - 1^{st}$ case. Since O_K/P^e has P^{e-1}/P^e as a subgroup, then by the second law of isomorphism:

$$(O_K/P^e)/(P^{e-1}/P^e) \cong O_K/P^{e-1}$$

if we show that $|P^{e-1}/P^e| = p^f$, then the result will follow by induction. (A proof of the second law of isomorphism is given in [7].)

We have that $P^e \subset P^{e-1}$, so there exists $\alpha \in P^{e-1}$ such that $\alpha \notin P^e$. We claim that $< \alpha > + P^e = P^{e-1}$. Since $< \alpha > + P^e$ is an ideal, with $P^e \subset < \alpha > + P^e$, we must have that $< \alpha >$ is a power of the prime ideal P. Thus, since $< \alpha > + P^e \subseteq P^{e-1}$, this implies equality, which proves the claim.

Consider the map $\phi : O_K \to P^{e-1}/P^e$ given by $\phi(\gamma) = \gamma\alpha + P^e$. Clearly this is a homomorphism. Furthermore, if we have $\beta\alpha + P^e$, then since $\beta \in O_K$, $\phi(\beta) = \beta\alpha + P^e$, and so this map is onto.

An element γ is in the kernel of ϕ iff $\gamma\alpha \in P^e$. This means that $ord_P(\gamma\alpha) \geq e$. Now, $ord_P(\gamma\alpha) = ord_P(\gamma) + ord_P(\alpha) = ord_P(\gamma) + e - 1$. So, γ is in the kernel iff $ord_P(\gamma) \geq 1$, which means $\gamma \in P$. Thus, $O_K/P \cong P^{e-1}/P^e$, and so the latter group has p^f elements. This proves the lemma. □

Theorem 2.9.2. *Let $p \in \mathbb{Z}$ be prime. Suppose $P_1, P_2, \ldots P_g$ are prime ideals in O_K containing p. Then we can write*

$$< p >= P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g}$$

where $e_i = ord_{P_i}(p)$. If f_i denotes the ramification index of P_i then

$$\sum_{i=1}^{g} e_i f_i = n$$

where $[K : \mathbb{Q}] = n$.

Proof. We have that

$$< p >= P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g}$$

We must first show that $P_i^{e_i} + P_j^{e_j} = O_K$ when $i \neq j$. We have that $P_i^{e_i}$ and $P_j^{e_j}$ are two maximal ideals, not equal to each other. Thus, since $P_i^{e_i} + P_j^{e_j}$ is an ideal containing both $P_i^{e_i}$ and $P_j^{e_j}$, by the maximality of these ideals, we have $P_i^{e_i} + P_j^{e_j} = O_K$.

Thus, we can use Lemma 2.9.1 and write

$$O_K/ < p > \cong O_K/P_1^{e_1} \oplus \ldots \oplus O_K/P_g^{e_g}$$

From corollary 2.6.4, we have that $|O_K/ < p > | = p^n$. From the previous Lemma, we have $|O_K/P^e| = p^{ef}$. Thus

$$p^n = p^{e_1 f_1} p^{e_2 f_2} \ldots p^{e_g f_g}$$

and hence $n = e_1 f_1 + \ldots + e_g f_g$. □

2.10 The Norm

Definition 2.10.1. *Let K be an algebraic number field with ring of integers O_K. Suppose $n = [K : \mathbb{Q}]$, and let $\sigma_1, \ldots, \sigma_n$ denote the n monomorphisms from K to $\mathbb{C}$. If A is any ideal in O_K, then we denote the norm of the ideal A, denoted by $N(A)$, to be $|O_K/A|$. If α is any element in O_K, then we denote the norm of α, denoted by $N(\alpha)$ to be*

$$\prod_{i=1}^{n} \sigma_i(\alpha)$$

To avoid confusion, we have that $N(<\alpha>)$ refers to the norm of the principal ideal generated by α. As well, it is clear that for any $\alpha, \beta \in O_K$, $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

Theorem 2.10.1. *For an algebraic number field K, if A, B are ideals in O_K, then $N(AB) = N(A)N(B)$.*

Proof. If A and B are relatively prime, then $O_K/AB \cong O_K/A \oplus O_K/B$ and clearly $N(AB) = N(A)N(B)$.

Suppose $A = P_1^{a_1} \ldots P_n^{a_n}$. Since each prime ideal is relatively prime, it is enough to show that $N(P^a) = N(P)^a$ for any prime ideal P. However, this follows immediately from Lemma 1.4.3. Hence, since we can decompose AB as a product of prime ideals, the lemma follows. □

Theorem 2.10.2. *For any $\alpha \in O_K$, where K is an algebraic number field, $N(\alpha) \in \mathbb{Z}$.*

A proof of this requires certain topics which we have not introduced. Consult [5] for a proof of this theorem.

Theorem 2.10.3. *Let D be an integral domain. Then for any $\mu \in U(D)$, $N(\mu) = \pm 1$*

Proof. Suppose $\mu \in U(D)$ and $\mu^{-1} \in U(D)$ is such that $\mu\mu^{-1} = 1$. Thus, since $\sigma_k(1) = 1$ for each $k = 1, \ldots, n$, then

$$N(\mu)N(\mu^{-1}) = N(1) = 1$$

Hence, we must have $N(\mu) \mid 1$ which implies $N(\mu) = \pm 1$. □

2.11 Galois Groups and Galois Extensions

Definition 2.11.1. *Let E/F be an extension of fields. Consider a map $\sigma : E \to E$ such that if $f \in F$, then $\sigma(f) = f$. We call such a map an $F-$ automorphism of E.*

Theorem 2.11.1. *For a field extension E/F, the collection of all $F-$ automorphisms of E is a group, under composition of functions.*

Proof. Suppose $\sigma_1, \sigma_2, \ldots, \sigma_n$ are all the $F-automorphisms$ of E. Clearly, since the identity map fixes every element of E, the identity map is an $F-automorphism$. Denote this map by ε, and let $\sigma_1 = \varepsilon$. If $\alpha \in E$, then $\sigma_k(\alpha) = \beta$, for some $\beta \in E$. Since σ_k is a bijection, there exists an inverse mapping σ_k^-1 such that $\sigma_k^{-1}(\beta) = \alpha$. Thus, every $F-automorphism$ has an inverse. Since composition of functions is always associative, we have proven the theorem. □

Definition 2.11.2. *For a field extension E/F, we denote the group of $F-$ automorphisms by $gal(E/F)$, and call this the Galois group of the extension E/F. It is important to notice that if K is an algebraic number field, then K is an extension of $\mathbb{Q}$. Moreover, if $n = [K : \mathbb{Q}]$, then there exists n distinct monomorphisms from K to $\mathbb{C}$. Since $K \subseteq \mathbb{C}$, we conclude that when K is an algebraic number field, $|gal(K : \mathbb{Q})| \leq n$. Moreover, the Galois group is a subset of the collection of monomorphisms from K to $\mathbb{C}$.*

Suppose F is a field and $f(x) \in F[x]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the conjugates of $f(x)$. If there exists some α_i such that $\alpha_i \notin F$, then we can create the simple extension $F(\alpha_i)$ which contains it. Furthermore, we can create additional extensions so that a field $F(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_m})$ contains all the conjugates of $f(x)$. We call this the splitting field of $f(x)$ over F. Denote the splitting field of $f(x)$ over F by E. Thus, E is the smallest field for which

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

holds. In other words, the polynomial $f(x)$ splits into linear factors in $E[x]$.

Let $f(x)$ be a polynomial in $F[x]$ and suppose $n = deg(f(x))$. Then we call $f(x)$ a separable polynomial if it has n distinct roots in some splitting field E. A finite extension E/F is called a separable extension if every element of E is the root of some polynomial in $F[x]$. In other words, every irreducible polynomial in $F[x]$ has distinct roots in K.

If K/F is a finite extension of fields, and there exists some polynomial $f(x) \in F[x]$ such that K is the splitting field of $f(x)$ over F. Then we call K a Galois extension.

For the remainder of this section, we assume K is an algebraic number field such that $n = [K : \mathbb{Q}]$. It has ring of integers O_K. We let $G = gal(K/\mathbb{Q})$ with elements $\varepsilon = \sigma_1, \sigma_2, \ldots, \sigma_n$.

Lemma 2.11.1. *Let $p \in \mathbb{Z}$ be a prime number. Suppose P_i and P_j are prime ideals of O_K containing p. Then there exists a $\sigma \in G$ such that $\sigma P_i = P_j$.*

Proof. Consider the set $S = \{\sigma_k P_i \mid \sigma_k \in G, p \in P_i\}$ and all the P_i are prime ideals. Suppose P_0 is a prime ideal containing p and $P_0 \notin S$. Then we can find an $\alpha \in D$ such that $\alpha \equiv 0 \pmod{P_0}$ and $\alpha \equiv 1 \pmod{\sigma_k(P_i)}$, for $k = 1, \ldots, n$. Then

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in P_0 \bigcap \mathbb{Z} = p\mathbb{Z}$$

Since each prime ideal P_i contains $p\mathbb{Z}$, it follows that $N(\alpha) \in P_i$. Thus, since P_i is a prime ideal, $N(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) \cdot \ldots \cdot \sigma_n(\alpha) \in P_i$ means that $\sigma_k(\alpha) \in P_i$ for some k. Thus, $\alpha \in \sigma_k^{-1} P_i$ is a contradiction, and so we must have that $P_0 \in S$. This means there is some $\sigma \in G$ and some prime ideal P containing p such that $\sigma P = P_0$. This proves the lemma. □

Theorem 2.11.2. *Let E/F be a field extension of degree n. If E is a Galois extension, then $|gal(E/F)| = n$.*

The proof of this theorem is somewhat long, and more related to field theory than number theory. Thus, we omit the proof for the sake of brevity. Those interested may consult [7] for a proof.

Corollary 2.11.3. *When K is a Galois extension, the n monomorphisms of K form a group.*

Proof. Let $S = \{\phi_1, \phi_2, \ldots, \phi_n\}$ denote the monomorphisms of K. Since $G \subseteq S$, and $|G| = |S|$, we conclude that $S = G$. Thus, the n monomorphisms of K form the Galois group of K over $\mathbb{Q}$. □

Theorem 2.11.4. *(The Perfect EFG Theorem)*
Suppose K is a Galois extension. Let $p \in \mathbb{Z}$ be a prime with $< p >= P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g}$, where P_i are prime ideals in O_K. Then $e_1 = e_2 = \ldots = e_g$ and $f_1 = f_2 = \ldots = f_g$, where f_i denotes the ramification index of P_i. If we let $e = e_1$ and $f = f_1$ then $n = [K : \mathbb{Q}] = efg$.

Proof. From the lemma, we see that for any index i, there exists some $\sigma \in G$ such that $\sigma(P_1) = P_i$. Since we have $O_K/P_1 \cong O_K/\sigma(P_1) = O_K/P_i$, we have $f_1 = f_i$. Since i is an arbitrary index, all the f_i's are the same.

Apply σ to both sides of $< p >= P_1^{e_1} \dots P_g^{e_g}$. Since $p \in \mathbb{Z}$, $\sigma(p) = p$. Thus, we get that

$$< \sigma(p) >=< p >= \sigma(P_1)_1^e \dots \sigma(P_g)^{e_g}$$

Hence, the exponent of $\sigma(P_1) = e_1$. But $\sigma(P_1) = P_i$, and its exponent is e_i. Thus, $e_1 = e_i$ and so all the e_i's are the same.

Finally, by the EFG theorem, $\sum e_i f_i = n$. Thus, if we let $f = f_i$ and $e = e_i$ then we see that $efg = n$. □

Theorem 2.11.5. *Suppose $K/\mathbb{Q}$ is a Galois extension with group G. Then for any ideal $A \in O_K$,*

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

Proof. Since the norm of ideals are multiplicative, and O_K is a Dedekind domain, we can prove this for a prime ideal P, and the general result will follow. Let P be a prime ideal containing $p \in \mathbb{Z}$, a prime, and suppose that $N(P) = p^f$, for some $f \geq 1$.

Consider the set $\{\sigma(P) \mid \sigma \in G\}$. From lemma 2.11.1, there are g distinct prime ideals P_i in this set. If we let $G(P) = \{\sigma \in G \mid \sigma(P) = P\}$, then we have that

$$|G| = g|G(P)| = n = efg$$

Thus, we have that $G(P) = ef$. So,

$$\prod_{\sigma \in G} \sigma(P) = (P_1 P_2 \dots P_g)^{ef} =< p >^f =< p^f >= \langle N(P) \rangle$$

□

2.12 Cyclotomic Fields

Definition 2.12.1. *Let $\zeta_m \in \mathbb{C}$ be such that $\zeta_m^m = 1$ and if $\zeta_m^n = 1$, then $m \mid n$. We call ζ_m the (primitive) m^{th} root of unity. A cyclotomic field is the algebraic number field $\mathbb{Q}(\zeta_m)$.*

For the remainder of the chapter, we work in the cyclotomic field $K = \mathbb{Q}(\zeta_m)$, with ring of integers O_K. We let $G = gal(K/\mathbb{Q})$. It is clear that if $n = [K : \mathbb{Q}]$, $\{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{n-1}\}$ is a basis for K over $\mathbb{Q}$. Thus, $O_K = \mathbb{Z} + \mathbb{Z}\zeta_m + \ldots + \mathbb{Z}\zeta_m^{n-1}$.

Definition 2.12.2. *Suppose P is a prime ideal in O_K. Then we say that P is unramified if it has (ramification) degree 1. (ie: $|O_K/P| = p$, $p \in \mathbb{Z}$ is prime.) We say P is ramified if it has degree $f > 1$ and we say it ramifies completely if $n = [K : \mathbb{Q}]$ and P has degree $f = n$.*

Lemma 2.12.1. *Let p be an odd prime. Then*

$$\sum_{i=0}^{p-1} \zeta_p^i = 1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1} = 0$$

Proof. Consider the polynomial $x^p - 1 = 0$. Notice that all ζ_p^i satisfy this polynomial. Thus, we rewrite this as

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + 1) = 0$$

or

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1 = 0$$

Thus, substituting in ζ_p, we get the desired conclusion. □

The above sum is called a cyclotomic sum. Notice that we could have substituted in ζ_p^n for any n which was not congruent to 0 modulo p.

Theorem 2.12.1. *Any cyclotomic field is a Galois extension.*

Proof. Let $f(x) = x^m - 1$. Then $f(\zeta_m^a) = 0$ for all a with $1 \leq a \leq m$. Thus, we have

$$x^m - 1 = (x - \zeta_m)(x - \zeta_m^2)\ldots(x - \zeta_m^{m-1})(x - 1)$$

Thus, K is the splitting field of $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$, and so K is a Galois extension. □

Theorem 2.12.2. *There is a homomorphism $\theta : G \to \mathbb{Z}_m^*$ such that, for $\sigma \in G$*

$$\sigma(\zeta_m) = \zeta_m^{\theta(\sigma)}$$

Proof. Since $\zeta_m^m = 1$, we have that $\sigma(\zeta_m^m) = \sigma(\zeta_m)^m = 1$. Thus, $\sigma(\zeta_m)$ is an m^{th} root of unity. So, $\sigma(\zeta_m) = \zeta_m^{\theta(\sigma)}$ where $\theta(\sigma)$ is some integer modulo m. Let $\tau = \sigma^{-1}$. Then

$$\zeta_m = \tau\sigma(\zeta_m) = \zeta_m^{\theta(\tau)\theta(\sigma)}$$

and so $\theta(\tau)\theta(\sigma) \equiv 1 \pmod{m}$. So, since each $\sigma \in G$ has an inverse, every $\theta(\sigma)$ has an inverse, which means $\theta : G \to \mathbb{Z}_m^*$. Since θ maps elements of G to integers modulo m, it is clear that θ is additive and multiplicative. (This follows since these properties holds modulo m.) Thus, θ is a homomorphism. □

Lemma 2.12.2. *Suppose p is a prime such that $p \nmid m$. Then for all $w \in O_K$, $\sigma_p w \equiv w^p \pmod{p}$.*

Proof. Write $O_K = \mathbb{Z}\gamma_1 + \ldots + \mathbb{Z}\gamma_n$ where $\gamma_1, \ldots, \gamma_n$ is a basis for K over $\mathbb{Q}$ in O_K. Since $1, \zeta_m, \ldots, \zeta_m^{\phi(m)}$ is a basis for $K = \mathbb{Q}(\zeta_m)$ we have that

$$w = \sum_{i=1}^{n} w_i \zeta_m^i \equiv \sum_{i=1}^{n} a_i \zeta_m^i (\text{mod } p)$$

Taking σ_p of both sides, we see that

$$\sigma_p w \equiv \sum_{i=1}^{n} a_i \zeta_m^{pi} (\text{mod } p)$$

because we have $a_i \in \mathbb{Z}$. Thus, by Fermat's theorem, we have

$$\sum a_i \zeta_m^{pi} \equiv \sum a_i^p \zeta_m^{pi} \equiv \left(\sum a_i \zeta_m^i\right)^p (\text{mod } p)$$

Hence, $\sigma_p w \equiv w^p \pmod{p}$ as claimed. □

Corollary 2.12.3. *Let P be a prime ideal of O_K containing p. Then $\sigma_p P = P$.*

Proof. If $w \in P$ then $\sigma_p w \equiv w^p \pmod{p}$. Hence, $w^p \equiv 0 \pmod{P}$, since $p \in P$. Thus, $\sigma_p P \subseteq P$. Since $\sigma_p P$ is a prime ideal, it is a maximal ideal and hence $\sigma_p P = P$. □

Lemma 2.12.3. *If p is a prime with $p \nmid m$, then every prime ideal $P \in O_K$ containing p is unramified.*

Proof. Assume the contrary: P is a prime ideal containing p with ramification degree $e \geq 2$. Then $(p) \subseteq P^2$. Let $w \in P$ and $w \notin P^2$. Then, if f is the least integer such that $p^f \equiv 1 \pmod{m}$, and $\gamma_1, \ldots, \gamma_n$ is a basis for K over $\mathbb{Q}$ in O_K, we have

$$\begin{aligned} w &\equiv \sum_{i=1}^{n} a_i \zeta_m^i (\text{mod } p) \\ w^p &\equiv \sum_{i=1}^{n} (a_i \zeta_m^i)^p (\text{mod } p) \\ &\equiv \sum_{i=1}^{n} a_i \zeta_m^{pi} (\text{mod } p) \\ w^{p^f} &\equiv \sum_{i=1}^{n} a_i \zeta_m^i (\text{mod } p) \end{aligned}$$

where $\zeta_m^{p^f} = \zeta_m$. Thus, $w \equiv w^{p^f} \pmod{p}$ and hence $w \equiv w^{p^f} \pmod{P^2}$. Since $p^f > 1$, we have $w \in P^2$ a contradiction. Hence, every prime ideal P containing p is unramified. □

Theorem 2.12.4. *Let P be a prime ideal in $\mathbb{Q}(\zeta_m)$ and set $P \bigcap \mathbb{Z} = p\mathbb{Z}$. If p is odd, the P is ramified iff $p \mid m$. If $p = 2$ then P is ramified iff $4 \mid m$.*

Proof. Assume p is an odd prime. If $p \nmid m$ then by Lemma 2.12.2, P is unramified.

Suppose $p \mid m$. Then $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_m)$. Let D denote the ring of integers of $\mathbb{Q}(\zeta_p)$. From the previous theorem, for a prime p we have that $pD = (1 - \zeta_p)^{p-1}$. Thus, $(1 - \zeta_p)O_K = P_1 P_2 \ldots P_t$ for prime ideals $P_i \in O_K$, not necessarily distinct. Then $pO_K = (P_1 \ldots P_t)^{p-1}$ and hence all the primes in O_K containing p are ramified.

Now assume $p = 2$. If $2 \mid m$ and $4 \nmid m$, then $m = 2x$ for some odd integer x. In this case, $-\zeta_x$ is a primitive m^{th} root of unity and so $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_x)$. Since $2 \nmid x$, P is unramified.

Finally, assume $p = 2$ with $4 \mid m$. Then $\zeta_4 = \sqrt{-1} = \imath \in \mathbb{Q}(\zeta_m)$. Since $(1 - \imath)^2 = -2\imath$, we see $2O_K = ((1 - \imath)O_K)^2$ and thus it follows from the previous theorem that all prime ideals in O_K containing 2 are ramified. □

Definition 2.12.3. *Let $\Phi_m(x) = \prod_{(a,m)=1}(x - \zeta_m^a)$ where $1 \leq a < m$. Then $\Phi_m(x)$ is called the m^{th} cyclotomic polynomial. Furthermore, $deg(\Phi_m(x)) = \phi(m)$. (A proof of this is given in [2].) Notice that since $\mathbb{Q}(\zeta_m)$ is the splitting field of $\Phi_m(x)$, $\phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$.*

Lemma 2.12.4. *Let P be a prime ideal in O_K containing p, a prime such that $p \nmid m$. Then $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}$ are distinct, when considered as cosets of O_K/P. Furthermore, if $|O_K/P| = p^f = q$, then $q \equiv 1 \pmod{m}$.*

Proof. We have that the cyclotomic polynomial

$$\Phi_n(x) = \prod_{(i,n)=1} (x - \zeta_n^i) = 1 + x + \ldots + x^{n-2} + x^{n-1}$$

whenever n is prime. Hence, if we define

$$\Theta_n(x) = \prod_{i=1}^{n-1} (x - \zeta_n^i) = 1 + x + \ldots + x^{n-1}$$

then we have

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

If P is a prime ideal not containing m, then $m \not\equiv 0 \pmod{P}$. Consider $\Theta_n(1) \pmod{P}$. If $\zeta_m^a \equiv \zeta_m^b \pmod{P}$, for some a and b, then $\zeta_m^{a-b} \equiv 1 \pmod{P}$. This implies that $\Theta_n(1) \equiv m \equiv 0 \pmod{P}$, a contradiction. Hence, the roots of unity can be considered as distinct cosets of O_K/P.

Furthermore, since O_K/P is a field, then the multiplicative group $(O_K/P)^*$ has $q - 1$ units. Consider the coset ζ_m^i. Then

$$(\zeta_m^i)^m = (\zeta_m^i + P)^m = 1 + P$$

which is the multiplicative identity in $(R/P)^*$. Hence, ζ_m^i has order m, and by Lagrange's theorem, $m \mid q - 1$. This implies $q \equiv 1 \pmod{m}$. □

Theorem 2.12.5. *Let p be a prime, $p \nmid m$ and f is the least positive integer such that $p^f \equiv 1 \pmod{m}$. Then in the ring of integers O_K, for $K = \mathbb{Q}(\zeta_m)$ we have*

$$< p >= P_1 P_2 \ldots P_g$$

where each prime ideal P_i has degree f and $g = \phi(m)/f$.

Proof. Suppose P_1 has degree f_1. Then for all $w \in O_K$ we have $w^{p^{f_1}} \equiv w \pmod{P_1}$ since O_K/P_1 is a finite field. As well, f_1 is the least such integer with this property.

Notice that by definition, $|\sigma_p| = f$. Hence, for all $w \in O_K$ we have

$$w \equiv \sigma_p^f(w) \equiv w^{p^f} (\text{mod } P_1$$

and so $f_1 \leq f$.

Conversely, $\zeta_m^{p^{f_1}} \equiv \zeta_m \pmod{P_1}$ implies $\zeta_m^{p^{f_1}} = \zeta_m$. Thus, $p^{f_1} \equiv 1 \pmod{m}$ and so $f \leq f_1$. Hence, $f = f_1$.

Thus, the degree of $P_1 = f_1$ and hence all the P_i have degree f. By the previous lemma, all the P_i are unramified. Hence, by the EFG theorem, $e = 1$ and $fg = \phi(m)$. Hence, $g = \phi(m)/f$. □

Theorem 2.12.6. *If $(m, n) = 1$ the $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_m\zeta_n)$.*

Proof. Since $\zeta_m n^m = \zeta_n$ and $\zeta_m n^n = \zeta_m$ we have $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_m n)$.

Conversely, since $(m, n) = 1$, there exist integers x, y such that $mx+ny = 1$. Thus

$$\zeta_{mn} = \zeta_{mn}^{mx+ny} = \zeta_{mn}^{mx}\zeta_m n^{ny} = \zeta_n^x \zeta_m^y \in \mathbb{Q}(\zeta_m, \zeta_n)$$

Thus, $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m, \zeta_m)$, which implies equality. □

Theorem 2.12.7. *Let p be a prime such that $(p, m) = 1$. Then in $K = \mathbb{Q}(\zeta_m, \zeta_p)$,*

$$< p >= pO_K = (P_1 P_2 \dots P_g)^{p-1}$$

for prime ideals P_i. Furthermore, each prime ideal P_i has degree f, f is the least positive integer such that $p^f \equiv 1$ (mod m) and $g = \phi(m)/f$.

Proof. Since $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_p, \zeta_m)$, the previous lemma tells us that all the ramification indices of prime ideals in D containing p are divisible by $p - 1$. Thus,

$$pD = (P_1 P_2 \dots P_{g'})^{e'(p-1)}$$

for prime ideals P_i, each with degree f', say. As well, e' is a positive integer.

From theorem 1.1.4, $pO_K = Q_1 Q_2 \dots Q_g$, where Q_i are prime ideals in O_K of degree f, and $g = \phi(m)/f$. Since $pO_K \subset pD$ we must have that $g \leq g'$ and $f \leq f'$.

Since $\mathbb{Q}(\zeta_p, \zeta_m) = \mathbb{Q}(\zeta_{pm})$, by the EFG theorem, we have

$$(p-1)\phi(m) = \phi(pm) = e'(p-1)f'g' \geq e'(p-1)f\frac{\phi(m)}{f}$$

Hence, $\phi(m) \geq e'\phi(m)$ which implies $e' = 1$. Thus, we have that $f'g' = \phi(m)$ and conclude that $g' = g = \phi(m)/f'$ and $f' = f$. □

Theorem 2.12.8. *Let m be an odd prime number. Then in the ring of integers of $\mathbb{Q}(\zeta_m)$*

$$< m >=< 1 - \zeta_m >^{m-1}$$

and $< 1 - \zeta_m >$ is a prime ideal of degree 1.

Proof. Since m is prime, we have

$$x^{m-1} + x^{m-2} + \ldots + 1 = \prod_{i=1}^{m-1} (x - \zeta_m^i)$$

Hence,

$$\prod_{i=1}^{m-1} (1 - \zeta_m^i) = m$$

Let $u_i = (1 - \zeta_m^i)/(1 - \zeta_m) = 1 + \zeta_m + \ldots + \zeta_m^{i-1}$, where $1 \leq i \leq m - 1$. We claim that u_i is a unit. Since $m \nmid i$ there exists a $j \in \mathbb{Z}$ such that $ij \equiv 1 \pmod{m}$. Hence,

$$u_i^{-1} = (1 - \zeta_m)/(1 - \zeta_m^i) = (1 - \zeta_m^{ij})/(1 - \zeta_m^i) = 1 + \zeta_m^i + \ldots + (\zeta_m^i)^{j-1}$$

So, u_i^{-1} is an algebraic integer, and hence u_i is a unit.

It follows that

$$m = \prod_{i=1}^{m-1} (1 - \zeta_m^i) = (1 - \zeta_m)^{m-1} \prod_{i=1}^{m-1} u_i$$

Hence, $(m) = (1 - \zeta_m)^{m-1}$. The EFG theorem tells us that $efg = m - 1$. Since $g = 1$ and corollary 4.3.5 tells us that $f = 1$, we must have $e = m - 1$ and hence $(1 - \zeta_m)$ is prime. □

Chapter 3

Characters, Gauss Sums and Jacobi Sums

3.1 Characters

Definition 3.1.1. *Let F_q be a field of characteristic p with $q = p^r$ elements, $r \geq 1$. We define a function $\chi : F_q^* \to \mathbb{C}^*$ such that, if $\alpha, \beta \in F_q^*$ then*

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$$

We call this function the multiplicative character χ defined on F_q.

As well, we let $F_p = \mathbb{Z}/p\mathbb{Z}$ denote the residue classes $0, 1, \ldots, p-1$ modulo p.

Theorem 3.1.1. *We present some simple facts about multiplicative characters. Suppose $a \in F_q^*$ and χ is a multiplicative character defined on F_q.*

1. $\chi(1) = 1$.
2. $(\chi(a))^{q-1} = 1$
3. $\chi(a^{-1}) = (\chi(a))^{-1} = \overline{\chi(a)}$

Where $\overline{\chi(a)}$ denotes complex conjugation, and 1 denotes the multiplicative identity of F_q.

Proof. 1. We have $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$ which implies $\chi(1) = 1$.

2. We find directly that $1 = \chi(1) = \chi(a^{q-1}) = \chi(a)^{q-1}$. Here, we have used the fact that F_q^* is a multiplicative group of order $q - 1$.

3. Similarly, $1 = \chi(1) = \chi(a \cdot a^{-1}) = \chi(a)\chi(a^{-1})$ implies that $\chi(a^{-1}) = \chi(a)^{-1}$. From (2), $\chi(a)$ is a complex number with absolute value less than or equal to 1. Thus, $\chi(a)^{-1} = \overline{\chi(a)}$.

□

Definition 3.1.2. *The special character ε defined on F_q is called the (multiplicative) identity character. If $a \in F_q^*$, then $\varepsilon(a) = 1$.*

We now extend the definition of multiplicative characters to include the additive identity, denoted by 0. If $\chi \neq \varepsilon$ is a multiplicative character defined on F_q, then $\chi(0) = 0$. Otherwise, we have $\varepsilon(0) = 1$.

From now on, we assume that $\chi \neq \varepsilon$ is a multiplicative character defined on F_q.

Theorem 3.1.2.

$$\sum_{t \in F_q} \chi(t) = 0 \text{ and } \sum_{t \in F_q} \varepsilon(t) = q$$

Proof. We first consider $\sum \varepsilon(t)$. Since $\varepsilon(t) = 1$ for every element $t \in F_q$ and $|F_q| = q$, then clearly we have

$$\sum_{t \in F_q} \varepsilon(t) = q$$

Now, let $S = \sum \chi(t)$. Suppose $a \in F_q^*$, is such that $\chi(a) \neq 1$. Then since χ is a multiplicative character, we have

$$\chi(a)S = \chi(a) \sum_{t \in F_q} \chi(t) = \sum_{t \in F_q} \chi(a)\chi(t) = \sum_{t \in F_q} \chi(at) = S$$

Here, we have used the fact that since t runs through all elements of F_q, multiplying by a non-zero element of F_q will merely change the order of the sum. Thus, we have that $\chi(a)S = S \Rightarrow S(\chi(a) - 1) = 0$. Thus, since $\chi(a) \neq 1$ we have that $S = 0$. □

3.2 The Trace Function And The Additive Character

Definition 3.2.1. *Suppose $a \in F_q$, then we define*

$$\tau(a) = \sum_{i=0}^{r-1} a^{p^i}$$

and call this the trace of a.

For the upcoming theorem, we will use the fact that since $F_p \subseteq F_q$, $\alpha \in F_q$ is an element of F_p iff $\alpha^p = \alpha$. A proof of this can be found in [2].

Theorem 3.2.1. *We present some elementary properties of the trace function. Suppose $\alpha, \beta \in F_q$ and $a \in F_p$. Then*

1. $\tau(\alpha) \in F_p$
2. $\tau(\alpha + \beta) = \tau(\alpha) + \tau(\beta)$
3. $\tau(a\alpha) = a\tau(\alpha)$
4. *τ maps F_q onto F_p.*

Proof. 1. We have that

$$\tau(\alpha)^p = (\alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{f-1}})^p = \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^f}$$

Here, we have used the fact that F_q has characteristic p, and so any term with a multinomial coefficient will disappear. Now, since $\alpha^{p^f} = \alpha$, we have shown that $\tau(\alpha)^p = \tau(\alpha)$. Thus, we must have that $\tau(\alpha) \in F_p$.

2. Since we are in a field of characteristic p, we have that $(\alpha + \beta)^p = \alpha^p + \beta^p$ for any $\alpha, \beta \in F_q$. Thus, it follows that

$$\tau(\alpha+\beta) = (\alpha+\beta)+(\alpha+\beta)^p+\ldots+(\alpha+\beta)^{p^{f-1}} = \alpha+\ldots+\alpha^{p^{f-1}}+\beta+\ldots+\beta^{p^{f-1}} = \tau(\alpha)+\tau(\beta)$$

3. We compute this directly.

$$\tau(a\alpha) = a\alpha+(a\alpha)^p+\ldots+(a\alpha)^{p^{f-1}} = a\alpha+a^p\alpha^p+\ldots+a^{p^{f-1}}\alpha^{p^{f-1}} = a(\alpha+\alpha^p+\ldots+\alpha^{p^{f-1}}) = a\tau(\alpha)$$

Here, we have used the fact that since $a \in F_p$, $a^p = a$.

4. The polynomial

$$\tau(x) = x + x^p + \ldots + x^{p^{f-1}}$$

has at most p^{f-1} distinct roots in F_q. However, there are p^f elements in F_q, so there exists some element $\alpha \in F_q$ such that $\tau(\alpha) = c \in F_p^*$. If $b \in F_p^*$ then, by property (3) we have $\tau(\frac{b}{c}\alpha) = \frac{b}{c}\tau(\alpha) = \frac{b}{c}c = b$. Hence, τ is an onto map.

□

Definition 3.2.2. *We define $\psi : F_q \to \mathbb{C}$ by $\psi(\alpha) = \zeta_p^{\tau(\alpha)}$. We call this the additive character defined on F_q.*

Theorem 3.2.2. *Now we present some elementary properties of the additive character.*

1. $\psi(\alpha+\beta)=\psi(\alpha)\psi(\beta)$
2. *There exists some* $\alpha \in F_q$ *such that* $\psi(\alpha)\neq 1$.
3. $\sum_{\alpha\in F_q}\psi(\alpha)=0$

Proof. 1. $\psi(\alpha+\beta)=\zeta_p^{\tau(\alpha+\beta)}=\zeta_p^{\tau(\alpha)+\tau(\beta)}=\zeta_p^{\tau(\alpha)}\zeta_p^{\tau(\beta)}=\psi(\alpha)\psi(\beta)$.

2. Since τ is an onto mapping, we have some $\alpha\in F_q$ such that $\tau(\alpha)=1$. Then, $\psi(\alpha)=\zeta_p\neq 1$.

3. Let $S=\sum\psi(\alpha)$ and suppose $\beta\in F_q$ is such that $\psi(\beta)\neq 1$. Then

$$\psi(\beta)S=\psi(\beta)\sum_{\alpha\in F_q}\psi(\alpha)=\sum_{\alpha\in F_q}\psi(\alpha+\beta)=S$$

Thus, this implies that $S=0$

□

3.3 Gauss Sums

Definition 3.3.1. *Suppose* χ *and* φ *are two multiplicative characters defined on* F_q. *Then for* $a\in F_q^*$ *we define*

$$(\chi\varphi)(a)=\chi(a)\varphi(a)$$

and

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

Under this definition, all the characters defined on F_q *form an abelian group, which we call the character group of* F_q. *It is important to notice that if* χ *is a character, then* $(\chi^{-1}\chi)(a)=\varepsilon(a)=1$. *Hence,* $\chi^{-1}(a)\chi(a)=1$ *implies that* $\chi^{-1}=\overline{\chi}$, *the complex conjugate of* χ.

Definition 3.3.2. *Let* χ *be a multiplicative character defined on* F_q, ψ *defined as above,* $\alpha\in F_q$ *and* $\zeta_p=e^{2\pi\imath/p}$ *is a primitive* p^{th} *root of unity. Then we define the Gauss sum on* F_q, *belonging to the character* χ *to be*

$$\sum_{t\in F_q}\chi(t)\psi(\alpha t)$$

and denote this by $G_\alpha(\chi)$.

Theorem 3.3.1. $G_0(\chi) = 0$

Proof. By definition, we have

$$G_0(\chi) = \sum_{t \in F_q} \chi(t)\psi(0) = \sum_{t \in F_q} \chi(t)\zeta_p^{\tau(0)} = \sum_{t \in F_q} \chi(t)$$

By Theorem 1.1.2, this sum is equal to 0. □

Theorem 3.3.2. *Suppose $a \neq 0 \in F_q$, then $G_a(\chi) = \chi(a^{-1})G_1(\chi)$.*

Proof. We have that

$$\chi(a)G_a(\chi) = \chi(a)\sum_{t \in F_q} \chi(t)\psi(at) = \sum_{t \in F_q} \chi(at)\psi(at) = G_1(\chi)$$

Thus, multiplying both sides by $\chi(a)^{-1}$, we get that

$$G_a(\chi) = \chi(a)^{-1}G_1(\chi)$$

which proves the theorem. □

From now on, we let $G_1(\chi) = G(\chi)$.

Lemma 3.3.1. *If $\alpha \in F_q^*$ then $G_\alpha(\chi)G_\alpha(\overline{\chi}) = \chi(-1)q$*

Proof. In light of Theorems 3.3.1 and 3.3.2 we have

$$\begin{aligned}
\sum_{\alpha \in F_q} G_\alpha(\chi)G_\alpha(\overline{\chi}) &= \sum_{\alpha \in F_q^*} \chi(\alpha)^{-1}G(\chi)\overline{\chi}(\alpha)^{-1}G(\overline{\chi}) \\
&= G(\chi)G(\overline{\chi})\sum_{\alpha \in F_q^*} \chi(\alpha)^{-1}\chi^{-1}(\alpha)^{-1} \\
&= G(\chi)G(\overline{\chi})\sum_{\alpha \in F_q^*} 1 \\
&= G(\chi)G(\overline{\chi})(p^f - 1)
\end{aligned}$$

Now, if we write this out directly, we get

$$\begin{aligned}
\sum_{\alpha \in F_q} G_\alpha(\chi)G_\alpha(\overline{\chi}) &= \sum_{\alpha \in F_q}\left(\sum_{\gamma \in F_q} \chi(\gamma)\psi(\alpha\gamma)\right)\left(\sum_{\delta \in F_q} \overline{\chi}(\delta)\psi(\alpha\delta)\right) \\
&= \sum_{\gamma \in F_q}\sum_{\delta \in F_q} \chi(\gamma)\overline{\chi}(\delta)\sum_{\alpha \in F_q} \psi(\alpha(\gamma + \delta))
\end{aligned}$$

From theorem 3.2.2, part (3), we have that $\sum \psi(\alpha(\gamma+\delta)) = 0$ unless $\gamma+\delta = 0$. In this case, then $\sum \psi(0) = q$. Thus,

$$\begin{aligned}\sum_{\gamma\in F_q}\sum_{\delta\in F_q}\chi(\gamma)\overline{\chi}(\delta)\sum_{\alpha\in F_q}\psi(\alpha(\gamma+\delta)) &= q\sum_{\gamma\in F_q}\chi(\gamma)\overline{\chi}(-\gamma)\\ &= q\overline{\chi}(-1)\sum_{\gamma\in F_q}\chi(\gamma)\overline{\chi}(\gamma)\\ &= q\chi(-1)\sum_{\gamma\in F_q^*}1\\ &= q\chi(-1)(p^f-1)\end{aligned}$$

Note that we used the fact that $\overline{\chi}(-1) = \chi(-1)$. Also, we reduced this sum to be over F_q^* since $\chi(\gamma)\overline{\chi}(\gamma) = 0$ when $\gamma = 0$.

Thus, equating the results of $\sum G_\alpha(\chi)G_\alpha(\overline{\chi})$, we get

$$(p^f-1)G(\chi)G(\overline{\chi}) = q\chi(-1)(p^f-1)$$

Cancelling $p^f - 1$ we get $G(\chi)G(\overline{\chi}) = q\chi(-1)$. Thus, considering Theorem 3.3.2, we conclude

$$G_\alpha(\chi)G_\alpha(\overline{\chi}) = \chi(\alpha^{-1})G(\chi)\overline{\chi}(\alpha^{-1})G(\overline{\chi}) = q\chi(-1)$$

□

Lemma 3.3.2. *If $\alpha \in F_q^*$, $\overline{G_\alpha(\chi)} = \chi(-1)G_\alpha(\overline{\chi})$*

Proof. Suppose $\alpha \in F_q^*$, then

$$\begin{aligned}\overline{G_\alpha(\chi)} &= \overline{\sum_{t\in F_q}\chi(t)\psi(\alpha t)}\\ &= \sum_{t\in F_q}\overline{\chi}(t)\zeta_p^{-\tau(\alpha t)}\\ &= \sum_{t\in F_q}\overline{\chi}(t)\psi(-\alpha t)\\ &= \overline{\chi}(-1)\sum_{t\in F_q}\overline{\chi}(-t)\psi(\alpha(-t))\\ &= \chi(-1)G_\alpha(\overline{\chi})\end{aligned}$$

□

Theorem 3.3.3. $G(\chi)\overline{G(\chi)} = |G(\chi)|^2 = q$.

Proof. Considering the last two lemmas, we have

$$G(\chi)\overline{G(\chi)} = G(\chi)G(\overline{\chi})\chi(-1) = q\chi(-1)\chi(-1) = q$$

□

3.4 Jacobi Sums

Definition 3.4.1. *If χ and λ are two multiplicative characters defined on F_q, then we call the following sum*

$$\sum_{a+b=1} \chi(a)\lambda(b)$$

a Jacobi sum, where a and b are elements of F_q. We denote this Jacobi sum by $J(\chi, \lambda)$. Alternatively, it is clear that we can write

$$J(\chi, \lambda) = \sum_{\alpha \in F_q} \chi(\alpha)\lambda(1-\alpha)$$

Lemma 3.4.1. $J(\chi, \chi^{-1}) = -\chi(-1)$.

Proof. $J(\chi, \chi^{-1}) = J(\chi, \overline{\chi}) = \sum_{\alpha \in F_q^*} \overline{\chi}(\alpha)\chi(1-\alpha) = \sum_{\alpha \in F_q^*} \chi(\alpha^{-1}-1) = \sum_{\alpha \in F_q^*} \chi(\alpha - 1)$. Over all of F_q, this sum is equal to 0, by theorem 3.1.2. Thus, we have

$$\sum_{\alpha \in F_q^*} \chi(\alpha - 1) + \chi(-1) = 0$$

which implies $J(\chi, \chi^{-1}) = -\chi(-1)$. □

Theorem 3.4.1. *If $\chi\lambda \neq \varepsilon$ then*

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

Proof. We consider $G(\chi)G(\lambda)$. By definition,

$$\begin{aligned} G(\chi)G(\lambda) &= \left(\sum_{t \in F_q} \chi(t)\psi(t)\right)\left(\sum_{s \in F_q} \lambda(s)\psi(t)\right) \\ &= \sum_{t \in F_q}\sum_{s \in F_q} \chi(t)\lambda(s)\psi(t+s) \\ &= \sum_{\gamma \in F_q} \psi(\gamma) \sum_{s+t=\gamma} \chi(s)\lambda(t) \end{aligned}$$

If $\gamma = 0$, then $\psi(\gamma) = 1$ and we get

$$\sum_{s \in F_q} \chi(s)\lambda(-s) = \lambda(-1) \sum_{s \in F_q} \chi\lambda(s) = 0$$

since $\chi\lambda \neq \varepsilon$.

So, we now consider this sum over F_q^*. Define s' and t' by $s = \gamma s'$ and $t = \gamma t'$. We can see that $s + t = \gamma$ implies $s' + t' = 1$. Hence,

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

Substituting into the above equation, we see that

$$G(\chi)G(\lambda) = \sum_{\gamma \in F_q^*} \psi(\gamma)\chi\lambda(\gamma)J(\chi, \lambda) = G(\chi\lambda)J(\chi, \lambda)$$

This completes the proof. □

Lemma 3.4.2. *If $\chi\lambda \neq \varepsilon$ then*

$$|J(\chi, \lambda)|^2 = q$$

Proof. We have $|J(\chi, \lambda)| = |\frac{G(\chi)G(\lambda)}{G(\chi\lambda)}| = \frac{|G(\chi)||G(\lambda)|}{|G(\chi\lambda)|} = \sqrt{q}$ by applying theorem 3.3.3. Hence, $|J(\chi, \psi)|^2 = q$. □

Theorem 3.4.2. *Suppose χ has order n, then*

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

Proof. From the previous lemma, we have

$$G(\chi)^2 = J(\chi, \chi)G(\chi^2)$$

If we multiply both sides by $G(\chi)$, we get

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

Since

$$J(\chi, \chi^2) = \frac{G(\chi)G(\chi^2)}{G(\chi^3)}$$

we have that

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

We continue in this fashion to get

$$G(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})G(\chi^{n-1}) \tag{3.4.1}$$

Since χ is a character of order n, we have $\chi^{n-1} = \chi^{-1} = \overline{\chi}$. So, since

$$G(\chi)G(\chi^{n-1}) = G(\chi)G(\overline{\chi}) = \chi(-1)q$$

by Lemma 3.3.1. We multiply both sides of (3.4.1) by $G(\chi)$ to finish the proof. □

Corollary 3.4.3. *If χ is a multiplicative character of order 3 defined on F_p, where $p \equiv 1$ (mod 3), then $G(\chi)^3 = pJ(\chi,\chi)$.*

Proof. From the theorem,

$$G(\chi)^3 = \chi(-1)pJ(\chi,\chi)$$

Since χ has order 3, we have

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

which yields the theorem. □

Chapter 4

Quadratic Reciprocity

Definition 4.0.2. *Let p be a prime, and let x be any integer. If there exists an integer a such that $a^2 \equiv x \pmod{p}$, then we call x a quadratic residue modulo p. If no such integer exists, we say that x is a quadratic non-residue.*

4.1 The Legendre Symbol

Definition 4.1.1. *Let p be a prime. We define the Legendre symbol to be $\left(\frac{x}{p}\right)$. It has the following values: if x is a quadratic residue modulo p, then*

$$\left(\frac{x}{p}\right) = 1$$

if x is a quadratic non-residue, then

$$\left(\frac{x}{p}\right) = -1$$

and if $p \mid x$ then

$$\left(\frac{x}{p}\right) = 0$$

For the remainder of the chapter, we assume p is an odd prime number and a is any integer. Since we are working over congruences modulo p, we can assume that $a \in \mathbb{Z}_p^*$. If $a = 0$, then all properties of the Legendre symbol are easily checked, which is why we exclude this case.

Lemma 4.1.1. *$a^{(p-1)/2} \equiv 1 \pmod{p}$ iff $\left(\frac{a}{p}\right) = 1$.*

Proof. Suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$ and let g be a primitive root modulo p. Suppose $g^x \equiv a \pmod{p}$. Then

$$g^{x((p-1)/2)} \equiv a^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p)$$

This implies that $2 \mid x$, say $x = 2n$. Then $(g^n)^2 \equiv a \pmod{p}$, and $\left(\frac{a}{p}\right) = 1$.

Conversely, suppose a is a quadratic residue, say $x^2 \equiv a \pmod{p}$. Then

$$x^{2((p-1)/2)} \equiv a^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p)$$

This completes the lemma. □

Corollary 4.1.1. *(Euler's Criterion)*
$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$ *(mod p).*

Proof. We have that $a^{p-1} \equiv 1 \pmod{p}$, by Theorem 1.3.6. Thus, we have that

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 (\mathrm{mod}\ p)$$

and so we conclude that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. From the lemma, we see that when a is a quadratic residue, $\left(\frac{a}{p}\right) = 1 \equiv a^{(p-1)/2} (\mathrm{mod}\ p)$. If a is not a quadratic residue, then $\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} \pmod{p}$. □

Corollary 4.1.2. *If* $a \equiv b$ *(mod p), then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Proof. If $a \equiv b \pmod{p}$ then $a^{(p-1)/2} \equiv b^{(p-1)/2} \pmod{p}$. Thus, $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \pmod{p}$. Since the Legendre symbols are equal to ± 1, this equivalence implies equality. □

Theorem 4.1.3. *For any integers a and b,*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Proof. Using corollary 4.1.1, we get that

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} (\mathrm{mod}\ p) \\ &\equiv a^{(p-1)/2} b^{(p-1)/2} (\mathrm{mod}\ p) \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\ p) \end{aligned}$$

Since both sides are equal to ± 1, this congruence implies equality. □

4.2 Quadratic Reciprocity

We deal with two special cases first, before proving the general quadratic reciprocity law.

Theorem 4.2.1. *For an odd prime p*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 mod\ 4 \\ -1, & p \equiv 3 mod\ 4 \end{cases}$$

Proof. By Euler's Criterion, we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} (\text{mod } p)$$

Suppose $p \equiv 1 \pmod 4$. Then $p = 4k+1$ for some $k \in \mathbb{Z}$. So, $\frac{p-1}{2} = 2k$ and so $\left(\frac{-1}{p}\right) \equiv 1 \pmod p$.

Similarly, if $p \equiv 3 \pmod 4$, then $p = 4m+3$ for some $m \in \mathbb{Z}$. Since $\frac{p-1}{2} = 2m+1$ we have $\left(\frac{-1}{p}\right) \equiv -1 \pmod p$. □

Theorem 4.2.2. *For an odd prime p,*

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

Thus, we see that $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1$ (mod 8) and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3$ (mod 8)

Proof. Consider the following congruences, all taken modulo p

$$\begin{aligned} p-1 &\equiv 1(-1)^1 (\text{mod } p) \\ 2 &\equiv 2(-1)^2 (\text{mod } p) \\ p-3 &\equiv 3(-1)^3 (\text{mod } p) \\ &\vdots \\ r &\equiv \frac{p-1}{2}(-1)^{(p-1)/2} (\text{mod } p) \end{aligned}$$

where r is $p - \frac{p-1}{2}$ or $\frac{p-1}{2}$. Note that since p is an odd prime, all the integers on the left hand side above are even. Thus, multiplying both sides together, we get

$$2 \cdot 4 \cdot \ldots \cdot (p-1) \equiv \left(\frac{p-1}{2}\right)! (-1)^{1+2+\ldots+(p-1)/2} (\text{mod } p)$$

Factoring out 2 from the left hand side, we get

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\ldots+(p-1)/2} (\text{mod } p)$$

So, cancelling the factorial results in

$$2^{(p-1)/2} \equiv (-1)^{1+2+\ldots+(p-1)/2} (\text{mod } p)$$

Thus, if we show that $1+2+\ldots+(p-1)/2 = (p^2-1)/8$, by Euler's Criterion, we can conclude the theorem.

Let $S = 1+2+\ldots+(p-1)/2$. Then

$$\begin{aligned}
S &= 1+2+\ldots+\frac{p-1}{2} \\
S &= \frac{p-1}{2}+\frac{p-3}{2}+\ldots+1 \\
2S &= (1+\frac{p-1}{2})+(2+\frac{p-3}{2})+\ldots+(1+\frac{p-1}{2}) \\
2S &= \frac{p+1}{2}+\frac{p+1}{2}+\ldots+\frac{p+1}{2} \\
2S &= \frac{p-1}{2}\cdot\frac{p+1}{2} \\
S &= \frac{p^2-1}{8}
\end{aligned}$$

This proves the theorem. □

Definition 4.2.1. *Since* $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$*, we can consider the Legendre symbol as a multiplicative character defined on the field* $\mathbb{Z}_p$*, where* p *is some odd prime. Thus, we have the following Gauss sum*

$$\sum_{a\in\mathbb{Z}_p}\left(\frac{a}{p}\right)\zeta_p^a$$

Denote this sum by S*. Since the values of the Legendre symbol are not all equal to 1, it is not equivalent to the identity character* ε*. Thus, by Theorem 3.1.2, we conclude that*

$$\sum_{a\in\mathbb{Z}_p}\left(\frac{a}{p}\right) = 0$$

by Theorem 3.1.2.

Lemma 4.2.1. *For any odd prime p, $S^2 = \left(\frac{-1}{p}\right) p$*

Proof. By definition, we have

$$S^2 = \left(\sum_{a\in\mathbb{Z}_p} \left(\frac{a}{p}\right)\zeta_p^a\right)\left(\sum_{b\in\mathbb{Z}_p} \left(\frac{b}{p}\right)\zeta_p^b\right)$$

This gives us

$$S^2 = \sum_{a,b\in\mathbb{Z}_p} \left(\frac{ab}{p}\right)\zeta_p^{a+b}$$

When a or b equals 0 in $\mathbb{Z}_p$, then $\left(\frac{a}{p}\right) = 0$. So, assume that $a, b \neq 0$. This means that every b has an inverse in $\mathbb{Z}_p$, so we can write $b = ca$, where c runs through $\mathbb{Z}_p^*$. Hence, we rewrite the above sum as

$$S^2 = \sum_{a\in\mathbb{Z}_p^*}\sum_{c\in\mathbb{Z}_p^*} \left(\frac{a^c}{p}\right)\zeta_p^{a(1+c)}$$

It is easy to see that $\left(\frac{a^2}{p}\right) = 1$ for every a with $(a, p) = 1$. Hence, we get

$$S^2 = \sum_{a\in\mathbb{Z}_p^*}\sum_{c\in\mathbb{Z}_p^*} \left(\frac{c}{p}\right)\zeta_p^{a(1+c)} = \sum_{c\in\mathbb{Z}_p^*}\left(\frac{c}{p}\right)\left(\sum_{a\in\mathbb{Z}_p^*}\zeta_p^{a(1+c)}\right)$$

Within the brackets, if $c \neq p-1$, then this sum is equal to 0 if taken over all $a \in \mathbb{Z}_p$. Thus, we must have

$$\sum_{a\in\mathbb{Z}_p^*}\zeta_p^{a(1+c)} + 1 = 0$$

Hence, this sum (within the brackets) is equal to -1 when $c \neq p-1$. If $c = p-1$, then $\zeta_p^{a(c+1)} = 1$ and so this sum within the brackets is equal to $p-1$. Thus, we have that

$$\begin{aligned} S^2 &= \sum_{1\leq c\leq p-2}\left(\frac{c}{p}\right)(-1) + \left(\frac{p-1}{p}\right)(p-1) \\ &= (-1)\sum_{1\leq c\leq p-2}\left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1) \end{aligned}$$

However, as mentioned in the above definition, we have

$$0 = \sum_{1 \le c \le p-1} \left(\frac{c}{p}\right) = \sum_{1 \le c \le p-2} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)$$

Thus, substituting in, we have

$$\begin{aligned} S^2 &= (-1)\left(-\left(\frac{-1}{p}\right)\right) + \left(\frac{-1}{p}\right)(p-1) \\ &= p\left(\frac{-1}{p}\right) \end{aligned}$$

This completes the proof. □

Lemma 4.2.2. *Let p and q be nonequal odd primes. Then $S^q \equiv \left(\frac{q}{p}\right) S$ (mod q).*

Proof. Let $K = \mathbb{Q}(\zeta_q)$, with ring of integers O_K and let $Q =< q >$ be an ideal in O_K. Then,

$$S^q = \left(\sum_{a \in \mathbb{Z}_p} \left(\frac{a}{p}\right) \zeta_p^a\right)^q \equiv \sum_{a \in \mathbb{Z}_p} \left(\frac{a}{p}\right)^q \zeta_p^{aq} (\text{mod } Q)$$

follows since $(x_1 + \ldots + x_n)^q \equiv x_1^q + \ldots + x_n^q \pmod q$. Furthermore, since q is an odd prime, $\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right)$. Thus, we have

$$S^q \equiv \sum_{a \in \mathbb{Z}_p} \left(\frac{a}{p}\right) \zeta_p^{aq} (\text{mod } Q)$$

Recall that $\left(\frac{a^2}{p}\right) = 1$ for all a relatively prime to p. Thus, since $q \neq p$, we have

$$S^q \equiv \sum_{a \in \mathbb{Z}_p} \left(\frac{q^2 a}{p}\right) \zeta_p^{aq} \equiv \left(\frac{q}{p}\right) \sum_{a \in \mathbb{Z}_p} \left(\frac{aq}{p}\right) \zeta_p^{aq} (\text{mod } Q)$$

However, since $(p, q) = 1$, $\sum \left(\frac{aq}{p}\right) \zeta_p^{aq}$ is equal to S. Thus, we have

$$S^q \equiv \left(\frac{q}{p}\right) S (\text{mod } Q)$$

and $S^q - \left(\frac{q}{p}\right) S = rq$ for some $r \in O_K$. Thus, modulo q, we have

$$S^q \equiv \left(\frac{q}{p}\right) S (\text{mod } q)$$

which finishes the proof. □

Theorem 4.2.3. *(The Quadratic Reciprocity Law)*
For nonequal odd primes p and q,

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

Proof. From the previous lemma, we have $S^q \equiv \left(\frac{q}{p}\right) S \pmod{q}$. Multiplying by the inverse of S gives

$$S^{q-1} \equiv \left(\frac{q}{p}\right) (\text{mod } q)$$

Since q is odd, we rewrite this as

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

which follows from the first lemma. Hence,

$$\left(\frac{q}{p}\right) \equiv \left(p\left(\frac{-1}{p}\right)\right)^{\frac{q-1}{2}} (\text{mod } q)$$

From the beginning of this section, we have that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, and so

$$\left(\frac{q}{p}\right) \equiv p^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} (\text{mod } q)$$

Finally, by Euler's Criterion, $p^{(q-1)/2} \equiv \left(\frac{p}{q}\right) \pmod{q}$, and so

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p}{q}\right) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} (\text{mod } q)$$

But, since the Legendre symbol gives a value of ± 1, and $q \geq 3$ we conclude

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

□

Chapter 5

Cubic Reciprocity

For this chapter, we work in the field $K = \mathbb{Q}(\zeta_3)$, where $\zeta_3 = e^{2\pi\imath/3}$ is a primitive 3rd root of unity. Denote the ring of integers by O_K. Since $\phi(3) = 2 = [K : \mathbb{Q}]$, $\{1, \zeta_3, \zeta_3^2\}$ is a basis for K over $\mathbb{Q}$. This means that $O_K = \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\zeta_3^2$. But, $1 + \zeta_3 + \zeta_3^2 = 0$, and so $\zeta_3^2 = -1 - \zeta_3$ means $O_K = \mathbb{Z} + \mathbb{Z}\zeta_3$. Let $\omega = \zeta_3$. Notice that $\omega^2 = \overline{\omega}$. If $\alpha = a + b\omega \in O_K$, then we have $N(\alpha) = N(a + b\omega) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$. Observe that $N(\alpha) > 0$ whenever $\alpha \neq 0$. Finally, we let F be a finite field such that $|F| = p$, a prime with the property that $p \equiv 1 \pmod 3$. We let χ be a multiplicative character of order 3 defined on F.

In this chapter, we will use the fact that $O_K = \mathbb{Z} + \mathbb{Z}\omega$ is a PID. A proof of this is given in [5]. As such, an element of O_K is prime if and only if it is irreducible. We use this in the proof of a theorem in this chapter. Namely, we prove an element is irreducible and conclude it is prime.

5.1 The Units of O_K

Theorem 5.1.1. *The units of O_K are $\pm 1, \pm\omega$ and $\pm\omega^2$.*

Proof. Suppose $\alpha = a + b\omega$ is a unit in O_K. Then $N(\alpha) = a^2 - ab + b^2 = \pm 1$. We rearrange this to a slightly better format to yield

$$4a^2 - 4ab + b^2 + 3b^2 = (2a - b)^2 + 3b^2 = \pm 4$$

Solving this, we see we have 6 possibilities:

1. $a = \pm 1$, $b = 0$ corresponds to the units ± 1
2. $a = 0$, $b = \pm 1$ corresponds to the units $\pm\omega$

3. $a = b = 1$ corresponds to $-\omega^2$
4. $a = b = -1$ corresponds to ω^2

Since these are the only solutions, there are no more units. □

5.2 Primes in O_K

Definition 5.2.1. *Suppose $\alpha \in O_K$ is such that if $\alpha \mid \beta\gamma$ then either $\alpha \mid \beta$ or $\alpha \mid \gamma$. When this happens, then we say α is prime. (Recall definition 2.1.6 in chapter 2.) If $p \in \mathbb{Z}$ is prime, then we call it a rational prime, as p is not necessarily prime in O_K.*

Theorem 5.2.1. *Suppose π is prime. Then there exists a rational prime p such that $N(\pi) = p$ or $N(\pi) = p^2$.*

Proof. Suppose $N(\pi) = \pi\overline{\pi} = n$. Since π is not a unit, we have $n > 1$. Furthermore, since n is a product of rational primes, we have $\pi \mid p$ for some rational prime p. Suppose $p = \pi\gamma$, for some $\gamma \in O_K$. Then if γ is a unit, $N(\gamma) = 1$ and it follows that $N(\pi) = p^2$. Otherwise, if γ is not a unit, $N(\pi\gamma) = p^2$ implies that $N(\pi) = p$. □

Theorem 5.2.2. *If $\pi \in O_K$ is such that $N(\pi)$ is a rational prime, then π is prime.*

Proof. Assume the contrary, that $\pi = \alpha\beta$ and neither of α, β is a unit. If $N(\pi) = p$, a rational prime, then $N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta) = p$ and it follows that one of $N(\alpha), N(\beta)$ equals 1. Thus, one of α, β is a unit, a contradiction, and so π is irreducible. By the opening remarks of the chapter, we conclude that π is prime. □

Lemma 5.2.1. $J(\chi, \chi) \in O_K$

Proof. We have that

$$J(\chi, \chi) = \sum_{t \in F} \chi(t)\chi(1-t)$$

Each term of this sum is either 0, 1, ω or ω^2. Thus, a finite sum of these terms will yield an element in O_K. □

Theorem 5.2.3. *For a rational prime $p \equiv 1$ (mod 3), there exist integers a and b such that $a^2 - ab + b^2 = p$.*

Proof. By the previous lemma, we know $J(\chi, \chi) \in O_K$. Let $J(\chi, \chi) = a+b\omega$. Then

$$p = |J(\chi, \chi)|^2 = (a + b\omega)\overline{(a + b\omega)} = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$$

□

Corollary 5.2.4. *If $p \equiv 1$ (mod 3) is a rational prime, there exists an element $\pi \in O_K$ such that $N(\pi) = p$.*

Proof. Suppose a and b are integers such that $p = a^2-ab+b^2$. Let $\pi = a+b\omega$ and the conclusion follows. □

Theorem 5.2.5. *If q is a rational prime such that $q \equiv 2$ (mod 3), then q is also prime.*

Proof. Assume that q is not prime and $q = \alpha\beta$ for some elements α, β. This implies that neither α or β is a unit and hence $N(q) = N(\alpha)N(\beta)$ further implies that $N(\alpha) = q$. If $\alpha = a + b\omega$, then $a^2 - ab + b^2 = q \equiv 2 \pmod 3$. Since $4 \equiv 1 \pmod 3$, we get $4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2 \equiv q \pmod 3$. Hence, $(2a - b)^2 \equiv q \equiv 2 \pmod 3$. Since 2 is a quadratic non-residue modulo 3, this equivalence is a contradiction. So, we have that $q \equiv 2 \pmod 3$ is prime. □

Theorem 5.2.6. *$1 - \omega$ is prime in O_K.*

Proof. We have that $N(1 - \omega) = 3$. Thus by theorem 5.2.2, we see that indeed $1 - \omega$ is prime. □

Corollary 5.2.7. $3 = -\omega^2(1 - \omega)^2$

Proof. A simple computation shows this to be true. □

Definition 5.2.2. *If π is prime and $\pi \equiv 2$ (mod 3) then we say that π is primary.*

Theorem 5.2.8. *If $\pi = a + b\omega$ is primary, then $a \equiv 2$ (mod 3) and $b \equiv 0$ (mod 3)*

Proof. When $\pi = q$ is a rational prime, this theorem clearly holds. Hence, assume $\pi = a + b\omega$ and $\pi \equiv 2 \pmod 3$. Thus, if $a + b\omega \equiv 2 \pmod 3$ then $3 \mid a-2+b\omega$. So, let $x+y\omega \in O_K$ be such that $a-2+b\omega = 3x+3y\omega$. This means that $a \equiv 2 \pmod 3$ and $b\omega \equiv 0 \pmod 3$. Hence, either $b \equiv 0 \pmod 3$ or $\omega \equiv 0 \pmod 3$. Suppose $\omega \equiv 0 \pmod 3$. Then $3 \mid \omega$ means there exists

$m + n\omega \in O_K$ such that $3m + 3n\omega = \omega$. Thus, $m = 0$ and $(3n - 1)\omega = 0$ means that $n = 1/3 \notin \mathbb{Z}$. Thus, $\omega \neq 0 \pmod 3$ and we conclude that $b \equiv 0 \pmod 3$. □

Theorem 5.2.9. *If π is prime and is not a rational prime and is not primary. Then π is associate to exactly one primary prime.*

Proof. The units in O_K are $\pm 1, \pm\omega, \pm(-1 - \omega)$. Suppose $\pi = a + b\omega$. We break this up into cases.

1. $b \equiv 0 \pmod 3$. Notice that $a \not\equiv 0 \pmod 3$, since $3 \mid \pi$ would mean that π is not prime. Thus, when $a \equiv 1 \pmod 3$, we multiply by -1 to get $-\pi = -a - b\omega$ and $-a \equiv 2 \pmod 3$.

2. $b \equiv 1 \pmod 3$. If $a \equiv 0 \pmod 3$, we multiply by $(1 + \omega)$ to get $(a - b) + a\omega$. If $a \equiv 1 \pmod 3$, we multiply by ω to get $-b + \omega(a - b)$. If $a \equiv 2 \pmod 3$, then we claim that π is not prime. Indeed $N(\pi) = a^2 - ab + b^2 \equiv 0 \pmod 3$.

3. $b \equiv 2 \pmod 3$. When $a \equiv 0$, we multiply by $(-1-\omega)$ to get $(b-a)-a\omega$. When $a \equiv 1 \pmod 3$, by the same type of reasoning as above, π is not prime. So, when $a \equiv 2 \pmod 3$, we multiply by $-\omega$ to get $b+(b-a)\omega$.

It is easily verifiable that these associates are all primary. □

5.3 The Cubic Reciprocity Character

Theorem 5.3.1. *Suppose π is prime. Then $O_K/ < \pi >$ is a finite field with $N(\pi)$ elements.*

Proof. We've seen that for any algebraic number field K, and any ideal A in O_K, O_K/A is a finite field. So, it remains to show that $O_K/ < \pi >$ contains $N(\pi)$ elements. We have 3 cases to consider: π is a rational prime congruent to 2 modulo 3, $N(\pi) = p$, a rational prime, congruent to 1 modulo 3, or $\pi = 1 - \omega$.

1. Suppose $\pi = q \equiv 2 \pmod 3$ is a rational prime. Then $N(\pi) = N(q) = q^2$. If we let $O_K = \mathbb{Z} + \mathbb{Z}\omega$ then since $< \pi >=< q >$ we have

$$\begin{aligned}(\mathbb{Z} + \mathbb{Z}\omega)/ < q > &= \{a + b\omega + < q > \mid a, b \in \mathbb{Z}\} \\ &= \{a + b\omega + q(c + d\omega) \mid a, b, c, d \in \mathbb{Z}\} \\ &= \{a + qc \mid a, c \in \mathbb{Z}\} \bigcup \{\omega(b + qd) \mid b, d \in \mathbb{Z}\} \\ &= \mathbb{Z}_q + \omega\mathbb{Z}_q\end{aligned}$$

Thus, $O_K/ < \pi >$ contains q^2 elements.

2. Suppose $N(\pi) = p \equiv 1 \pmod 3$ is a rational prime. Let $\pi = a + b\omega$ with $p = a^2 - ab + b^2$. We claim that $\{0, 1, \ldots, p-1\}$ is a complete set of coset representatives. If true, this shows that $O_K/ < \pi >$ has $N(\pi) = p$ elements.

   If π and $\widetilde{\pi}$ are associates, then $< \pi >=< \widetilde{\pi} >$, so we may assume π is a primary element. Thus, since $b \equiv 0 \pmod 3$, we have that $p \nmid b$. So, for any $\gamma = x + y\omega \in O_K$, there exists an integer c such that $bc \equiv y \pmod p$. So, $\gamma - c\pi \equiv x - ca \pmod p$ and $\gamma \equiv x - ca \pmod \pi$. This shows that any element of O_K is congruent to an integer modulo π. Now, if $n \in \mathbb{Z}$, $n = qp + r$ with $0 \leq r < p$. Thus, $n \equiv r \pmod p$ and $\pi \mid p$ implies that $n \equiv r \pmod \pi$. It follows that every element of O_K is congruent to an element of $\{0, 1, \ldots, p-1\}$ modulo π.

   If $r \equiv r' \pmod \pi$, for $r, r \in \mathbb{Z}$, $0 \leq r, r' < p$, then $r - r' = \pi\gamma$ for some $\gamma \in O_K$. Thus, $(r - r')^2 = pN(\gamma)$ and $p \mid r - r'$ means that $r \equiv r' \pmod p$ implying that $r = r'$. So this representation is unique.

3. Let $\pi = 1 - \omega$. Then we claim that $\{0, 1, 2\}$ is a complete set of coset representatives, and prove this similar to the previous method. Clearly, $3 \nmid 2$ and so for any $\gamma = x + y\omega \in O_K$ there exists an integer c such that $2c \equiv y \pmod 3$. So, $\gamma - c(1-\omega) \equiv x - c \pmod 3$ and hence $\gamma \equiv x - c \pmod{(1-\omega)}$. Since $(1-\omega) \mid 3$, if $n \in \mathbb{Z}$ and $n \equiv m \pmod 3$, then $n \equiv m \pmod{(1-\omega)}$. Thus, for reasons similar to the previous case, $\{0, 1, 2\}$ is a complete set of coset representatives.

□

For the remainder of this chapter, we let π be a prime in O_K and we work in the field $O_K/ < \pi >$. We assume this has characteristic p

Lemma 5.3.1. *Suppose π is prime in O_K, then if $\pi \nmid \alpha$, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$, for any element $\alpha \in O_K$.*

Proof. If π is prime, then $O_K/ < \pi >$ is a finite field of order $N(\pi)$. Then the multiplicative group $(O_K/ < \pi >)^*$ has order $N(\pi) - 1$ and thus

$$\alpha^{N(\pi)-1} \equiv 1 (\text{mod } \pi)$$

for any $\alpha \in O_K/ < \pi >$. □

Theorem 5.3.2. *Suppose $\pi \neq (1-\omega)$ is prime and $\alpha \in O_K$ is such that $\pi \nmid \alpha$. Then $\alpha^{(N\pi-1)/3} \equiv \omega^n \pmod \pi$, where n is one of 0, 1 or 2.*

Proof. Observe that

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

Since $\pi \mid \alpha^{N(\pi)-1} - 1$ and π is prime, it must divide at least one of the terms on the right of the above equation. This yields the theorem. □

Definition 5.3.1. *If $\pi \neq 1-\omega$ is prime, then we define the cubic residue character as*

1. $\left(\frac{\alpha}{\pi}\right)_3 = 0$ *if* $\pi \mid \alpha$
2. $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\pi)-1)/3} \pmod{\pi}$ *if* $\pi \nmid \alpha$

for any element $\alpha \in O_K$.

Notice that this is very similar to the Legendre symbol. As such, it has many of the same properties

Lemma 5.3.2. *If π is a prime with $N(\pi) \neq 3$, and α and β are elements of O_K, then we have*

1. $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$
2. *If* $\alpha \equiv \beta \pmod{\pi}$, *then* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$
3. $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *iff* $x^3 \equiv \alpha \pmod{\pi}$

Proof. 1.

$$\begin{aligned}\left(\frac{\alpha\beta}{\pi}\right)_3 &\equiv (\alpha\beta)^{(N(\pi)-1)/3} (\text{mod } \pi) \\ &\equiv \alpha^{(N(\pi)-1)/3}\beta^{(N(\pi)-1)/3} (\text{mod } \pi) \\ &\equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 (\text{mod } \pi)\end{aligned}$$

Thus, this implies equality.

2. If $\alpha \equiv \beta \pmod{\pi}$ then

$$\alpha^{(N(\pi)-1)/3} \equiv \beta^{(N(\pi)-1/3} (\text{mod } \pi)$$

and so

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \left(\frac{\beta}{\pi}\right)_3 (\text{mod } \pi)$$

which again implies equality.

3. Suppose $\left(\frac{\alpha}{\pi}\right)_3 = 1$. Then $\alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi}$. Since $(O_K/ < \pi >)^*$ is a cyclic group, there exists a generator γ such that $\gamma^3 \equiv \alpha \pmod{\pi}$.

   Conversely, suppose $x^3 \equiv \alpha \pmod{\pi}$. Then

$$x^{3\cdot(N(\pi)-1)/3} \equiv \alpha^{(N(\pi)-1)/3} \equiv 1 (\text{mod } \pi)$$

   and so $\left(\frac{\alpha}{\pi}\right)_3 = 1$

□

Definition 5.3.2. *Suppose π is prime. Then it is clear that we can view $\left(\frac{\alpha}{\pi}\right)_3$ as a multiplicative character. Thus, we let $\chi_\pi(\alpha)$ denote $\left(\frac{\alpha}{\pi}\right)_3$.*

Theorem 5.3.3. *Suppose $\alpha \in O_K/ < \pi >$ for some prime π. Then*

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

Proof. We have that $\chi_\pi(\alpha)$ is one of $1, \omega$ and ω^2. Since $\overline{\omega} = \omega^2$, $\overline{\omega^2} = (\omega^2)^2 = \omega$, it follows that

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

Furthermore, since $\chi_\pi(\alpha)$ is a multiplicative character defined on a field, $\chi_\pi(\alpha) = \chi_\pi(\alpha^2)$. □

Theorem 5.3.4. *For $\alpha \in O_K/ < \pi >$, π is prime, we have*

$$\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$$

Proof. By definition, $\alpha^{(N(\pi)-1)/3} \equiv \chi_\pi(\alpha) \pmod{\pi}$. Since $N(\pi) = N(\overline{\pi})$ we get

$$\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\alpha}^{N(\pi)-1/3} \equiv \overline{\chi_\pi(\alpha)} (\text{mod } \overline{\pi})$$

This shows that $\overline{\chi_\pi(\alpha)} \equiv \chi_{\overline{\pi}}(\overline{\alpha}) \pmod{\pi}$ and hence $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$. □

Corollary 5.3.5. *If $q \equiv 2$ (mod 3) is a rational prime, then*

$$\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$$

Furthermore, if $n \in \mathbb{Z}$ and $(q, n) = 1$ then

$$\chi_q(n) = 1$$

Proof. Since $\overline{q} = q$ we have

$$\chi_q(\overline{\alpha}) = \chi_{\overline{q}}(\overline{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$$

Additionally, since $\overline{n} = n$ we have

$$\chi_q(n) = \overline{\chi_q(n)} = \chi_q(n)^2$$

Since $q \nmid n$, we obtain $\chi_q(n) = 1$. □

5.4 Jacobi Sums and the Cubic Reciprocity Character

Let π be primary such that $N(\pi) = p \equiv 1 \pmod 3$, where p is a rational prime. Then the field $O_K/ < \pi >$ has p elements. Let $O_K/ < \pi >= F$. Thus, the two fields F and $\mathbb{Z}_p$ are isomorphic. Thus, we can consider χ_π as a cubic character defined on $\mathbb{Z}_p$. Now we may use Gauss sums and Jacobi sums. We let the field F denote $\mathbb{Z}_p \cong O_K/ < \pi >$.

Lemma 5.4.1. *For any cubic character χ, $J(\chi, \chi) = a + b\omega$ where $a \equiv 2$ (mod 3) and $b \equiv 0$ (mod 3).*

Proof. Consider

$$G(\chi)^3 = \left(\sum_{t \in F} \chi(t)\psi(t)\right)^3 \equiv \sum_{t \in F} \chi(t)^3 \psi(3t) (\text{mod } 3)$$

Since $\chi(0) = 0$ and $\chi(t)^3 = 1$ for $t \neq 0$, we have

$$\sum_{t \in F} \chi(t)^3 \psi(3t) = \sum_{t \in F^*} \psi(3t) = -1$$

From Corollary 3.4.3, we have

$$G(\chi)^3 = pJ(\chi, \chi)$$

Thus, $pJ(\chi, \chi) = pa + pb\omega \equiv a + b\omega \equiv -1 \pmod 3$.

Since $\overline{G(\chi)} = G(\overline{\chi})$ we have

$$G(\overline{\chi})^3 = pJ(\overline{\chi}, \overline{\chi}) \equiv a + b\overline{\omega} \equiv -1 (\text{mod } 3)$$

Thus, $a + b\omega \equiv a + b\overline{\omega} \pmod 3$ shows that $b(\omega - \overline{\omega}) \equiv 0 \pmod 3$. This gives that $2b\omega + b \equiv 0 \pmod 3$ and thus $3 \mid b$. From this, we have that $a + b\omega \equiv -1 \pmod 3$ implies that $a \equiv -1 \equiv 2 \pmod 3$. □

Lemma 5.4.2. *For an odd prime p,*

$$\sum_{x=1}^{p-1} x^k$$

is congruent to 0 modulo p if $p - 1 \nmid k$ and -1 modulo p if $p - 1 \mid k$.

Proof. Suppose $p-1 \mid k$, and that $n(p-1) = k$, for some $n \in \mathbb{Z}$. Then

$$1^k+\ldots+(p-1)^k = (1^{p-1})^n+\ldots+((p-1)^{p-1})^n \equiv 1+1+\ldots+1 \equiv -1(\text{mod } p)$$

Let g be a primitive root modulo p. Notice that g^x is a p^{th} root of unity for any x. Then we can rewrite this sum as

$$\sum_{x=1}^{p-1} x^k = \sum_{x=1}^{p-1} g^{xk}$$

Modulo p, this can be considered as a cyclotomic sum, as g^{xk} runs through all the p^{th} roots of unity. This, this sum will be congruent to 0 modulo p. □

Theorem 5.4.1. *$J(\chi_\pi, \chi_\pi) = \pi$.*

Proof. Suppose $J(\chi_\pi, \chi_\pi) = \pi'$. Since $|J(\chi_\pi, \chi_\pi)|^2 = p$, we have

$$\pi'\overline{\pi'} = p = \pi\overline{\pi}$$

which implies $\pi \mid \pi'$ or $\pi \mid \overline{\pi'}$. Since π' is prime by theorem 5.2.2 and primary by lemma 5.4.1 we have that $\pi = \pi'$ or $\pi = \overline{\pi'}$. We will show that $\pi = \pi'$.

We have

$$J(\chi_\pi, \chi_\pi) = \sum_{t\in F} \chi_\pi(t)\chi_\pi(1-t) \equiv \sum_{t\in F} t^{(N(\pi)-1)/3}(1-t)^{(N(\pi)-1)/3}(\text{mod } \pi)$$

Since $\pi \mid p$, $\pi \nmid (p-1)/3$ and the previous lemma tells us the sum is congruent to 0 modulo p, we have $J(\chi_\pi, \chi_\pi) \equiv 0 \pmod{\pi}$, $\pi \mid \pi'$ and hence $\pi = \pi'$. □

Corollary 5.4.2. *$G(\chi_\pi)^3 = p\pi$.*

Proof. This follows from the fact that $G(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi)$. □

5.5 Cubic Reciprocity

Theorem 5.5.1. *Suppose π_1 and π_2 are primary with $N(\pi_1) \neq N(\pi_2)$. Furthermore, assume that $N(\pi_1) \neq 3$ and $N(\pi_2) \neq 3$. Then we have*

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

Proof. We have three cases to consider; when π_1 and π_2 are either both complex, both rational or one is complex and the other is rational.

Assume both π_1 and π_2 are rational primes. Then π_1 and π_2 are both congruent to 2 modulo 3 and $(\pi_1, \pi_2) = 1$. Then from corollary 5.3.5, $\chi_{\pi_1}(\pi_2) = 1 = \chi_{\pi_2}(\pi_1)$.

Now assume π_1 is a rational prime and π_2 is a complex prime. Let $\pi_1 = q \equiv 2 \pmod 3$ and $\pi_2 = \pi$. Furthermore, suppose $N(\pi) = p$. Consider $G(\chi_\pi)^3 = p\pi$. Raised to the $(q^2 - 1/3)$ power gives

$$G(\chi_\pi)^{q^2-1} = (p\pi)^{(q^2-1)/3}$$

Taking this modulo q, we get

$$G(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi) (\text{mod } q)$$

Since $q \nmid p$, $\chi_q(p) = 1$ and so

$$G(\chi_\pi)^{q^2} \equiv G(\chi_\pi)\chi_q(\pi) (\text{mod } q) \tag{5.5.1}$$

If we examine the left hand side of this congruence, we see

$$G(\chi_\pi)^{q^2} = \left(\sum_{t \in F} \chi_\pi(t)\psi(t) \right)^{q^2} \equiv \sum_{t \in F} \chi_\pi(t)^{q^2} \psi(q^2 t) (\text{mod } q)$$

Since $q^2 \equiv 1 \pmod 3$, the term $\chi_\pi(t)^{q^2}$ reduces to $\chi_\pi(t)$. Thus

$$G(\chi_\pi)^{q^2} \equiv G_{q^2}(\chi_\pi) (\text{mod } q)$$

From Theorem 3.3.1, $G_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})G(\chi_\pi)$. Observe that

$$\chi_\pi(q^{-2}) = \chi_\pi(q^{-1})^2 = \overline{\chi_\pi(q^{-1})} = \chi_\pi^{-1}(q^{-1}) = \chi_\pi(q)$$

Thus, $G_{q^2}(\chi_\pi) = \chi_\pi(q)G(\chi_\pi)$. From (5.5.1) this gives us

$$\chi_\pi(q)G(\chi_\pi) \equiv G(\chi_\pi)\chi_q(\pi) (\text{mod } q)$$

We multiply both sides by $\overline{G(\chi_\pi)}$ to get

$$\begin{aligned} \chi_\pi(q)p &\equiv \chi_q(\pi)p (\text{mod } q) \\ \chi_\pi(q) &\equiv \chi_q(\pi) (\text{mod } q) \end{aligned}$$

This last equivalence implies $\chi_\pi(q) = \chi_q(\pi)$.

Now, we suppose π_1 and π_2 are both complex primes. Assume $N(\pi_1) = p_1 \equiv 1 \pmod 3$ and $N(\pi_2) = p_2 \equiv 1 \pmod 3$. Suppose $\gamma_1 = \overline{\pi}_1$ and $\gamma_2 = \overline{\pi}_2$. A quick calculation reveals that γ_1 and γ_2 are both primary. As well, we have $p_1 = \pi_1\gamma_1$ and $p_2 = \pi_2\gamma_2$.

We proceed similar to the last method of proof. Consider

$$G_1(\chi_{\gamma_1})^3 = p_1\gamma_1$$

Similar to the previous method of proof, we raise this to the $(N(\pi_2)-1)/3$ power, and modulo π_2 we get

$$\begin{aligned} G(\chi_{\gamma_1})^{p_2} &\equiv \chi_{\pi_2}(p_1\gamma_1)G(\chi_{\gamma_1})(\text{mod } \pi_2) \\ G_{p_2}(\chi_{\gamma_1}) &\equiv \chi_{\pi_2}(p_1\gamma_1)G(\chi_{\gamma_1})(\text{mod } \pi_2) \\ \chi_{\gamma_1}(p_2^{-1})G(\chi_{\gamma_1}) &\equiv \chi_{\pi_2}(p_1\gamma_1)G(\chi_{\gamma_1})(\text{mod } \pi_2) \\ \chi_{\gamma_1}(p_2^2) &\equiv \chi_{\pi_2}(p_1\gamma_1)(\text{mod } \pi_2) \end{aligned}$$

Hence,

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1) \tag{5.5.2}$$

Here, we have used the fact that $p_2 \equiv 1(\text{mod } 3)$ to deduce $G(\chi_{\gamma_1})^{p_2} \equiv G_{p_2}(\chi_{\gamma_1})$, using the method above.

Similarly, if we consider $G(\chi_{\pi_2})^3 = p_2\pi_2$, raise this to the $(N(\pi_1)-1)/3$ power, take congruences modulo π_1, we get

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2) \tag{5.5.3}$$

Now, observe that

$$\begin{aligned} \chi_{\gamma_1}(p_2^2) &= \chi_{\gamma_1}(p_2)^2 \\ &= \overline{\chi_{\gamma_1}(p_2)} \\ &= \chi_{\overline{\gamma_1}}(\overline{p_2}) \\ &= \chi_{\pi_1}(p_2) \end{aligned}$$

Keeping this under consideration, we find that

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) = \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) \qquad \text{from (5.5.2)}$$

$$\begin{aligned} &= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) \\ &= \chi_{\pi_1}(p_2\pi_2) \\ &= \chi_{\pi_2}(p_1^2) \qquad \text{from (5.5.3)} \\ &= \chi_{\pi_2}(p_1\gamma_1\pi_1) \\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1) \end{aligned}$$

Cancelling out $\chi_{\pi_2}(p_1\gamma_1)$ we find that

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

□

Chapter 6

Eisenstein Reciprocity

6.1 The Power Residue Symbol

For this chapter, we will be working in the algebraic number field $K = \mathbb{Q}(\zeta_m)$, where m is a positive integer. (At times, m will be assumed to be an odd prime, but these will be clearly specified.) Thus, we denote it's ring of integers by O_K.

We assume that $p \in \mathbb{Z}$ is a prime, $(p, m) = 1$ always, and P is a prime ideal in O_K not containing m. Furthermore, $P \bigcap \mathbb{Z} = p\mathbb{Z}$ and hence

$$\mathbb{Z}/p\mathbb{Z} \subseteq O_K/P$$

Thus, $N(P) = |O_K/P| = p^f$ for some integer $f \geq 1$. We let $q = p^f$ and we denote O_K/P by F. Recall that $q \equiv 1 \pmod{m}$ from Lemma 2.12.4. That same lemma also tells us that $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}$ can be considered as distinct cosets modulo P. Since O_K/P is finite, the multiplicative group F^* is cyclic of order $q - 1$. Finally, we let $G = gal(K/\mathbb{Q})$, where $\sigma \in G$ is an arbitrary element. We fix this notation for the remainder of the chapter.

Lemma 6.1.1. *Suppose $\alpha \in O_K$, and P is a prime ideal such that $\alpha \notin P$. Then there exists a unique integer i modulo m such that*

$$\alpha^{(N(P)-1)/m} \equiv \zeta_m^i (mod\ P)$$

Proof. We have that

$$\prod_{i=0}^{m-1} (x - \zeta_m^i) = (x^m - 1)$$

so

$$\prod_{i=0}^{m-1}(\alpha^{(N(P)-1)/m}-\zeta_m^i)=\alpha^{N(P)-1}-1$$

Since F^* is a multiplicative group of order $N(P)-1$, we have

$$\alpha^{N(P)-1}-1\equiv 0(\text{mod } P)$$

Hence,

$$\prod_{i=0}^{m-1}\alpha^{(N(P)-1)/m}-\zeta_m^i\equiv 0(\text{mod } P)$$

Since P is a prime ideal, it follows that there exists some i such that $\alpha^{(N(P)-1)/m}\equiv\zeta_m^i \pmod P$.

If we suppose $\zeta_m^i\equiv\zeta_m^j \pmod P$. Then $\zeta_m^{i-j}\equiv 1 \pmod P$ implies that $i\equiv j \pmod m$. Thus, i is unique modulo m. □

Definition 6.1.1. *Let $\alpha\in R$ and recall that P is a prime ideal not containing m. Then we define the power residue symbol, $(\frac{\alpha}{P})_m$ by:*

1. $\left(\frac{\alpha}{P}\right)_m=0$ *if* $\alpha\in P$.
2. *If $\alpha\notin P$, then $\left(\frac{\alpha}{P}\right)_m$ is the unique m^{th} root of unity such that*

$$\alpha^{(N(P)-1)/m}\equiv\left(\frac{\alpha}{P}\right)_m (mod\ P)$$

If A is an ideal in O_K not containing m with $A=P_1\dots P_n$ for prime ideals P_i then for any $\alpha\in O_K$ we define

$$\left(\frac{\alpha}{A}\right)_m=\prod_{i=1}^{n}\left(\frac{\alpha}{P_i}\right)_m$$

Furthermore, if $\beta\in O_K$ and β is prime to m, then for any $\alpha\in O_K$, we define

$$\left(\frac{\alpha}{\beta}\right)_m=\left(\frac{\alpha}{<\beta>}\right)_m$$

Theorem 6.1.1. *If $\alpha,\beta\in O_K$ and P is a prime ideal not containing m, then:*

1. $\left(\frac{\alpha\beta}{P}\right)_m=\left(\frac{\alpha}{P}\right)_m\left(\frac{\beta}{P}\right)_m$.

2. *If* $\alpha \equiv \beta \pmod{P}$, *then* $\left(\frac{\alpha}{P}\right)_m = \left(\frac{\beta}{P}\right)_m$.

3. $\left(\frac{\alpha}{P}\right)_m = 1$ *iff* $x^m \equiv \alpha \pmod{P}$ *is solvable in* O_K

Proof. All these results follow in exactly the same manner as the cubic residue character. □

Corollary 6.1.2. *For ideals* A *and* B *prime to* m,

1.
$$\left(\frac{\alpha\beta}{A}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\beta}{A}\right)_m$$

2.
$$\left(\frac{\alpha}{AB}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\alpha}{B}\right)_m$$

3. *If* $\alpha \notin A$ *and* $x^m \equiv \alpha \pmod{A}$ *is solvable in* O_K, *then* $\left(\frac{\alpha}{A}\right)_m = 1$.

Proof. The first two properties follow due to multiplicativity. We prove the third property. Suppose $A = P_1 P_2 \dots P_n$ is the prime decomposition of A and

$$x^m \equiv \alpha (\text{mod } A)$$

for some $x, \alpha \in O_K$ and $\alpha \notin A$. Thus, $\alpha \notin P_i$ for each i and we have

$$x^m \equiv \alpha (\text{mod } P_i)$$

since $P_i \mid A$. Thus, $\left(\frac{\alpha}{P_i}\right)_m = 1$ for each i, and so the product of these is 1. This gives $\left(\frac{\alpha}{A}\right)_m = 1$. □

It is important to notice that the converse statement of (3) is not true. That is: $\left(\frac{\alpha}{A}\right) = 1$ does not imply the existence of an element $x \in O_K$ such that $x^m \equiv \alpha \pmod{A}$.

From now on, for an element $\sigma \in G$, and $\alpha \in O_K$ we write

$$\sigma(\alpha) = \alpha^\sigma$$

Theorem 6.1.3. *For* $\sigma \in G$ *and* $\alpha \in O_K$,

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

Proof. By definition,

$$\left(\frac{\alpha}{P}\right)_m \equiv \alpha^{(N(P)-1)/m} (\text{mod } P)$$

or

$$\left(\frac{\alpha}{P}\right)_m - \alpha^{(N(P)-1)/m} \in P$$

Thus

$$\left(\left(\frac{\alpha}{P}\right)_m - \alpha^{(N(P)-1)/m}\right)^\sigma \in P^\sigma$$

and hence

$$\left(\frac{\alpha}{P}\right)_m^\sigma \equiv (\alpha^\sigma)^{(N(P)-1)/m} (\text{mod } P^\sigma)$$

where $N(P^\sigma) = N(P)$. Furthermore,

$$\left(\frac{\alpha^\sigma}{P^\sigma}\right)_m \equiv (\alpha^\sigma)^{(N(P)-1)/m} (\text{mod } P^\sigma)$$

and hence

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

as claimed. □

Corollary 6.1.4. *If A is an ideal prime to m and $\sigma \in G = gal(K/\mathbb{Q})$ then*

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

Proof. This result follows easily due to the multiplicative nature of the power residue symbol. □

Definition 6.1.2. *Let m be an odd prime number. Then if $\alpha \in O_K$ and α and m are relatively prime, then we call α primary if it is congruent to a rational integer modulo $(1-\zeta_m)^2$.*

Theorem 6.1.5. *Let m be an odd prime number. Suppose $\alpha \in O_K$ and α and m are relatively prime. Then there exists an integer c, unique modulo m such that $\zeta_m^c \alpha$ is primary.*

Proof. Let $\lambda = 1 - \zeta_m$. From theorem 2.12.8, we know that λ generates a prime ideal. Furthermore, since $< \lambda >$ has degree 1, $|O_K / < \lambda > |$ is prime. So, if $\alpha \in O_K$, then there exists an integer a such that $\alpha \equiv a \pmod{\lambda}$ and so $\lambda \mid \alpha - a$. If we let $\beta = \frac{\alpha - a}{\lambda}$, then $\beta \in O_K$ and $\beta \equiv b \pmod{\lambda}$ for some $b \in \mathbb{Z}$. Thus, $\lambda \mid \frac{\alpha-a}{\lambda} - b$ implies $\frac{\alpha-a}{\lambda^2} - \frac{b}{\lambda} \in O_K$. Furthermore, $\alpha - a - b\lambda \equiv 0$

(mod λ^2) and $\alpha \equiv a + b\lambda \pmod{\lambda^2}$. Suppose $ac \equiv b \pmod{m}$, for some $c \in \mathbb{Z}$. Then, since

$$\zeta_m^c \equiv (1-\lambda)^c \equiv 1 - c\lambda (\text{mod } \lambda^2)$$

we have

$$\zeta_m^c \alpha \equiv (1-c\lambda)(a+b\lambda) \equiv a + \lambda(b-ac) (\text{mod } \lambda^2)$$

Since $< m >= \lambda^{m-1}$, $m \in \lambda^2$ and thus

$$\zeta_m^c \alpha \equiv a (\text{mod } \lambda^2)$$

Finally, if $\zeta_m^c \alpha \equiv \zeta_m^d \alpha \pmod{\lambda^2}$, then $\lambda_m^{c-d} \alpha \equiv \alpha \pmod{\lambda^2}$. Hence, $c \equiv d \pmod{m}$ and hence c is unique modulo m. □

6.2 Stickelberger's Relation: Definitions

Definition 6.2.1. *We define a multiplicative character χ_P on F as follows: Let $t \in F^*$ and $\gamma \in O_K$ be such that $\gamma \equiv t$ (mod P). We will denote this residue class by $\overline{\gamma}$. Then, we define*

$$\chi_P(t) = \left(\frac{\gamma}{P}\right)_m^{-1} = \overline{\left(\frac{\gamma}{P}\right)}_m$$

It is easy to see that this is equivalent to

$$\chi_P(t) \equiv t^{-(N(P)-1)/m} (mod\ P)$$

Definition 6.2.2. *We have the Gauss sum*

$$G_\alpha(\chi_P) = \sum_{t \in F} \chi_P(t)\psi(\alpha t)$$

. Since we are concerned primarily when $\alpha = 1$ we have the special notation

$$G(P) = G(\chi_P) = \sum_{t \in F} \chi_P(t)\psi(t)$$

Finally, we let $\Phi(P) = (G(P))^m$

Lemma 6.2.1. *Since $G(P)$ is a Gauss sum, it has the following properties:*

1. $G(P) \in \mathbb{Q}(\zeta_m, \zeta_p)$.

2. $|G(P)|^2 = q$.

3. $\Phi(P) \in \mathbb{Q}(\zeta_m)$.

Proof. 1. Since $(m,p) = 1$, $\mathbb{Q}(\zeta_m, \zeta_p) = \mathbb{Q}(\zeta_m \zeta_p)$. Thus, the Gauss sum $G(P) = \sum \chi_P(t)\psi(t) = \sum \zeta_m^i \zeta_p^j$, for various indices i and j. Thus, $G(P) \in \mathbb{Q}(\zeta_m, \zeta_p)$.

2. Since $G(P)$ is a Gauss sum defined on a field of order q, the result follows from Theorem 3.3.3.

3. We recall that Theorem 3.4.2 states

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

where χ is a multiplicative character of order n, defined on a field with q elements. So, in this case

$$G(\chi_P)^m = \chi_P(-1)qJ(\chi_P,\chi_P)\dots J(\chi_P,\chi_p^{m-2})$$

And since $J(\chi_P, \chi_P)$ is a sum of elements in $\mathbb{Q}(\zeta_m)$ (specifically, the elements ζ_m^i) it follows that $G(\chi_P)^m \in \mathbb{Q}(\zeta_m)$.

□

6.3 Stickelberger's Relation: Lemmas

Lemma 6.3.1. *Let $p > 1$ be a positive integer. Then every positive integer can be written uniquely in the form*

$$\sum_{i=0}^{n} a_i p^i$$

where $0 \le a_i < p$ and n is some positive integer.

Proof. Let a be any positive integer. Then there exists a unique, nonnegative integer n such that $p^n \le a < p^{n+1}$. Using the division algorithm, we see that $a = a_n p^n + r$ where $0 \le r < p$. Also notice that $a_n < p$. Similarly, for the integer r, there exists a unique nonnegative integer m such that $p^m \le r < p^{m+1}$. Again, we see that $r = a_m p^m + r_1$, where $0 \le r_1 < p$ and $a_m < p$. We continue this process for finitely many steps and get the desired form of a.

Suppose $\sum a_i p^i = \sum b_i p^i$ with $0 \le a_i, b_i < p$. Taking both sides modulo p, we see that $a_0 \equiv b_0 \pmod{p}$. But this implies $p \mid a_0 - b_0$ which we

can't have, as both are less than p. Thus, we conclude that $a_0 = b_0$. If we subtract $a_0 = b_0$ from both sides, then divide by p, we can follow this line of reasoning to conclude that $a_1 = b_1$. Continuing in this manner, we conclude that $a_i = b_i$ for each i and hence the expression for a is unique. □

Definition 6.3.1. *Consider $p^f = q$. If $0 \leq a < q-1$ write*

$$a = \sum_{i=0}^{f-1} a_i p^i$$

where $0 \leq a_i < p$. Then we define

$$S(a) = \sum_{i=0}^{f-1} a_i$$

If $a \geq q-1$, then $a \equiv r \pmod{(q-1)}$ for some r, and we let $S(a) = S(r)$, where r is expressed in the desired form.

Definition 6.3.2. *For a real number u, we define $\ll u \gg$ to be $u - [u]$, where $[u]$ denotes the largest integer less than or equal to u. We call this the fractional part of u.*

Notice that if $u = a + b$, where $a \in \mathbb{Z}$, $b \in \mathbb{Q}$, then $[u] = [a+b] = a + [b]$. We will make use of this in the following lemma.

Lemma 6.3.2. *For a nonnegative integer a, and $q = p^f$ we have*

$$S(a) = (p-1) \sum_{i=0}^{f-1} \ll p^i a/(q-1) \gg$$

Proof. If $a = 0$, then clearly the lemma is true. Furthermore, if $a > q-1$ then $a = n(q-1) + r$ for some $n, r \in \mathbb{Z}$. Thus

$$\ll p^i a/(q-1) \gg = \ll p^i(n(q-1)+r)/(q-1) \gg = \ll p^i n + p^i r/(q-1) \gg$$

This gives

$$p^i n + p^i r/(q-1) - [p^i n + p^i r/(q-1)] = \ll p^i r/(q-1) \gg$$

Hence, we can assume $1 \leq a < q-1$.

Let $a = a_0 + a_1 p + \ldots + a_{f-1}p^{f-1}$, where $0 \leq a_i < p$. Notice that $p^f = q \equiv 1 \pmod{(q-1)}$. Hence,

$$\begin{aligned} a &\equiv a_0 + a_1 p + \ldots + a_{f-1}p^{f-1} \pmod{(q-1)} \\ pa &\equiv a_0 p + a_1 p^2 + \ldots + a_{f-1} \pmod{(q-1)} \\ p^2 a &\equiv a_0 p^2 + a_1 p^3 + \ldots + a_{f-1} p \pmod{(q-1)} \\ &\vdots \\ p^{f-1} &\equiv a_0 p^{f-1} + a_1 + \ldots + a_{f-1}p^{f-2} \pmod{(q-1)} \end{aligned}$$

The right-hand sides of these congruences are all less than $q-1$ so that $\ll p^i a/(q-1) \gg$ is equal to the right-hand side of the i^{th} congruence divided by $q-1$. Thus

$$\sum_{i=0}^{f-1} \ll \frac{p^i a}{q-1} \gg = \frac{1}{q-1} S(a)(1 + p + \ldots + p^{f-1})$$

We have that

$$\frac{1 + p + \ldots + p^{f-1}}{q-1} = \frac{p^{f-1} + p^{f-2} + \ldots + 1}{p^f - 1} = \frac{1}{p-1}$$

and so we have

$$(p-1)\sum_{i=0}^{f-1} \ll p^i a/(q-1) \gg = S(a)$$

□

Lemma 6.3.3. $\sum_{a=1}^{q-2} S(a) = (f(p-1)(q-2))/2$, *and we assume* $1 \leq a < q-1$.

Proof. Let $a = a_0 + a_1 p + \ldots a_{f-1}p^{f-1}$, with $0 \leq a_i < p$. Notice that

$$q - 1 = p^f - 1 = (p-1)(1 + p + \ldots + p^{f-1})$$

Then

$$\begin{aligned} q - 1 - a &= (p-1)(1 + p + \ldots + p^{f-1}) - a \\ &= (p-1) + (p-1)p + \ldots + (p-1)p^{f-1} - a_0 - a_1 p - \ldots - a_{f-1}p^{f-1} \\ &= (p - 1 - a_0) + (p - 1 - a_1)p + \ldots + (p - 1 - a_{f-1})p_{f-1} \end{aligned}$$

and

$$\begin{aligned} S(a) + S(q-1-a) &= a_0 + a_1 + \ldots + a_{f-1} + (p-1-a_0) + \ldots + (p-1-a_{f-1}) \\ &= (p-1) + (p-1) + \ldots + (p-1) \\ &= f(p-1) \end{aligned}$$

Thus, when we take the sum of the left hand from $a = 1$ to $a = q-2$ we get

$$2\sum_{a=1}^{q-2} S(a) = f(p-1)(q-2)$$

which yields the lemma. □

In an upcoming proof, we will need to work in the field $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$. Thus, we have the following notation: $K = \mathbb{Q}(\zeta_m)$, $L = \mathbb{Q}(\zeta_{q-1})$, $M = \mathbb{Q}(\zeta_{q-1}, \zeta_p) = \mathbb{Q}(\zeta_{p(q-1)})$. We denote their ring of integers by O_K, O_L and O_M respectively. Finally, let $P \in O_K, Q \in O_L, R \in O_M$ be prime ideals containing $p \in \mathbb{Z}$.

Lemma 6.3.4. *Considering the above definitions, we have:*

1. $ord_R(pO_M) = p-1$
2. $ord_R(1-\zeta_p) = 1$
3. $ord_R(P) = p-1$

Proof. 1. From theorem 2.12.7 we have that

$$pD = (P_1 P_2 \ldots P_g)^{p-1}$$

where D denotes the ring of integers of $\mathbb{Q}(\zeta_m, \zeta_p)$. We substitute $q-1$ for m in this theorem. Thus, since $R \in O_M$ it appears in the decomposition of pO_M. Hence, we conclude that $ord_R(pO_M) = p-1$.

2. From theorem 2.12.8 in the chapter of cyclotomic polynomials, we have that $1-\zeta_p$ generates a prime ideal of degree 1 and $pO_K = (1-\zeta_p)^{p-1}$. Hence,

$$pO_M = (pO_K)O_M = (1-\zeta_p)^{p-1}O_M = (R_1 R_2 \ldots R_g)^{p-1}$$

where $R = R_1$, say. Taking the $p-1^{st}$ root, we have $(1-\zeta_p)O_M = RR_2 \ldots R_g$ and so $ord_R(1-\zeta_p) = 1$.

3. We have that $pO_K = P_1 \dots P_g$ for prime ideals P_i. Notice that $P_i \neq P_j$ whenever $i \neq j$. Hence, $P_1 \dots P_g \cdot O_M = (R_1 \dots R_g)^{p-1}$ for distinct prime ideals R_i. Thus, $PO_M = R^{p-1}$ and the result follows.

□

Lemma 6.3.5. $F \cong O_L/Q$

Proof. Consider the map $\phi : F \to O_L/Q$ by $\phi(\alpha) = \phi(a + P) = a + Q$. We claim this is a monomorphism. Suppose $\alpha, \beta \in F$. Then if $\alpha = a + P$ and $\beta = b + P$, then

$$\begin{aligned}
\phi(\alpha + \beta) &= \phi(a + b + P) \\
&= a + b + Q \\
&= a + Q + b + Q \\
&= \phi(\alpha) + \phi(\beta) \\
\phi(\alpha\beta) &= \phi((a + P)(b + P)) \\
&= \phi(ab + P) \\
&= ab + Q \\
&= (a + Q)(b + Q) \\
&= \phi(\alpha)\phi(\beta)
\end{aligned}$$

Furthermore, if $\phi(\alpha) = \phi(\beta)$, then

$$\begin{aligned}
\phi(a + P) &= \phi(b + P) \\
a + Q &= b + Q \\
(a - b) + Q &= 0
\end{aligned}$$

Hence, $a - b \in Q$ and since $P \subseteq ker(\phi)$, we have $a - b \in P$ and so $a \equiv b \pmod{P}$ hence $a + P = b + P$ and $\alpha = \beta$.

To show this is an isomorphism, it is enough to show that $|F| = |O_L/Q|$. Since, $p \in Q$, we have that $p^{f'} = |O_L/Q|$, where f' is the smallest integer such that $p^{f'} \equiv 1 \pmod{q-1}$. But, we have $p^f = q \equiv 1 \pmod{q-1}$. Thus, $p^f \equiv p^{f'} \pmod{q-1}$. Hence, we have $f = f'$ and so the two fields are isomorphic. □

Notice that if we assume $q - 1 \notin Q$, then the elements $1, \zeta_{q-1}, \dots \zeta_{q-1}^{q-2}$ can be considered distinct cosets in O_L/Q. This follows from Lemma 2.12.1. From now on, we will denote O_L/Q by $\mathcal{F}$.

Definition 6.3.3. *If $q-1 \notin Q$, then if $\alpha \in O_L$ we define*

1. $(\frac{\alpha}{Q}) = 0$ *if* $\alpha \in Q$
2. *If* $\alpha \notin Q$ *then* $\left(\frac{\alpha}{Q}\right)$ *is the unique* $(q-1)^{st}$ *root of unity such that*

$$\alpha \equiv \left(\frac{\alpha}{Q}\right) (mod\ Q)$$

Notice that this is almost exactly the same as the previous definition for a power residue symbol. The two main differences is that it is defined over O_L, and α has no exponent value. Since $F \cong \mathcal{F}$, $\left(\frac{\alpha}{Q}\right)$ has the same first 2 properties defined in Theorem 6.1.1

Lemma 6.3.6. *If $\alpha \in O_K$,*

$$\left(\frac{\alpha}{Q}\right)^{(q-1)/m} = \left(\frac{\alpha}{P}\right)_m$$

Proof. Suppose $\alpha \equiv \zeta_{q-1}^i \pmod{Q}$. Then

$$\alpha^{(q-1)/m} \equiv \zeta_{q-1}^{(q-1)i/m} \equiv \zeta_{q-1}^{i/m} (\text{mod } Q)$$

But since $N(P) = q$, the left hand side is equal to $\left(\frac{\alpha}{P}\right)_m$ and the right hand side is $\left(\frac{\alpha}{Q}\right)^{(q-1)/m}$. Thus, this congruence implies equality. □

Definition 6.3.4. *Consider the field $\mathcal{F}$. We define a multiplicative character ω on this field such that*

$$\omega(t) = \left(\frac{\gamma}{Q}\right)$$

where $\gamma \in O_L$ is such that $\gamma \equiv t$ (mod Q). We denote this residue class by $\overline{\gamma}$.

Lemma 6.3.7. $\omega(\overline{\zeta}_{q-1}^i) = \zeta_{q-1}^i$

Proof. Since $\overline{\zeta}_{q-1}^i = \zeta_{q-1}^i$, we have that if $\gamma \equiv \zeta_{q-1}^i$ for some $\gamma \in O_L$ then

$$\omega(\overline{\zeta}_{q-1}^i) = \omega(\zeta_{q-1}^i) = \left(\frac{\gamma}{Q}\right) \equiv \zeta_{q-1}^i (\text{mod } Q)$$

Since the ζ_{q-1}^j, $j = 1, \ldots, q-2$ are distinct cosets in $\mathcal{F}$, it follows that $\omega(\overline{\zeta}_{q-1}^i) = \zeta_{q-1}^i$. □

Definition 6.3.5. *Let a be a nonnegative integer. Define*

$$G_a = G(\omega^{-a}, \psi) = \sum_{t \in \mathcal{F}} \omega^{-a}(t)\psi(t) = \sum_{t \in \mathcal{F}} \omega(t)^{-a}\psi(t)$$

Theorem 6.3.1. *$G(P) = G_a$ iff $a = (q-1)/m$.*

Proof.

$$\begin{aligned} G(P) &\Leftrightarrow \sum_{t \in F} \chi_P(t)\psi(t) \\ &\Leftrightarrow \sum_{t \in F} \left(\frac{\gamma}{P}\right)_m^{-1} \psi(t) \\ &\Leftrightarrow \sum_{t \in \mathcal{F}} \left(\frac{\gamma}{Q}\right)^{-(q-1)/m} \psi(t) \\ &\Leftrightarrow \sum_{t \in \mathcal{F}} \left(\frac{\gamma}{Q}\right)^{-a} \psi(t) \\ &\Leftrightarrow \sum_{t \in \mathcal{F}} \omega^{-a}(t)\psi(t) \\ &\Leftrightarrow G_a \end{aligned}$$

□

6.4 Stickelberger's Relation: A Preliminary Theorem

Lemma 6.4.1. *$ord_R(G_1) = 1$*

Proof. Let m_i be a positive integer such that $m_i \equiv \tau(\overline{\zeta}_{q-1}^{i}) \pmod{p}$. Let $\lambda_p = 1 - \zeta_p$. Then

$$G_1 = \sum_{t \in \mathcal{F}} \omega(t)^{-1}\psi(t) = \sum_{i=0}^{q-2} \zeta_{q-1}^{-i}(1-\lambda_p)^{m_i}$$

Since $ord_R(\lambda_p) = 1$, $< \lambda_p >= RA$, for some ideal A with $R \nmid A$. Thus, $R \mid< \lambda_p >$, $R^2 \nmid< \lambda_p >$ and so

$$(1-\lambda_p)^{m_i} = \sum_{r=0}^{m_i} (-1)^r \binom{m_i}{r} \lambda_p^{m_i - r} \equiv 1 - m_i\lambda_p (\text{mod } R^2)$$

Thus

$$G_1 \equiv -\left(\sum_{i=0}^{q-2} m_i \zeta_{q-1}^{-i}\right) \lambda_p (\text{mod } R^2)$$

because $\sum \zeta^{-i}$ is a cyclotomic sum, which equals 0.

Now since $m_i \equiv \overline{\zeta}_{q-1}^{i} + \overline{\zeta}_{q-1}^{ip} + \ldots + \overline{\zeta}_{q-1}^{ip^{f-1}} (\text{mod } p)$, $Q \subseteq R$ and $ord_R(p) = p-1$ means $p \in R^2$, we have

$$m_i \lambda_p \equiv (\zeta_{q-1}^{i} + \zeta_{q-1}^{ip} + \ldots + \zeta_{q-1}^{ip^{f-1}}) \lambda_p (\text{mod } R^2)$$

Substituting this into the above equation, we get

$$G_1 \equiv -\sum_{i=0}^{q-2} \zeta_{q-1}^{-i} \left(\zeta_{q-1}^{i} + \zeta_{q-1}^{ip} + \ldots + \zeta_{q-1}^{ip^{f-1}}\right) \lambda_p (\text{mod } R^2)$$

Consider

$$\sum_{i=0}^{q-1} \zeta_{q-1}^{i(p^j-1)} \text{ for } j = 0, 1, 2, \ldots, f-1$$

When $j \neq 0$, this is a cyclotomic sum, and hence equals 0. When $j = 0$, this sum is equal to $q-1$. Hence,

$$G_1 \equiv -\lambda_p (q-1) \equiv \lambda_p - \lambda_p q (\text{mod } R^2)$$

But, $q = p^f$, and $p \in R^2$, thus we get

$$G_1 \equiv \lambda_p (\text{mod } R^2)$$

We've already used the fact that $\lambda_p \notin R^2$ and hence, we conclude that $ord_R(G_1) = 1$. □

For simplicity, we denote $ord_R(G_a)$ by $\nu(a)$. We now establish several properties of $\nu(a)$.

Lemma 6.4.2. *Assume* $1 \leq a, b, a+b < q-1$.

1. $\nu(a+b) \leq \nu(a) + \nu(b)$
2. $\nu(a+b) \equiv \nu(a) + \nu(b)$ *(mod* $p-1$*)*
3. $\nu(pa) = \nu(a)$
4. $\nu(a) = a$

Proof. Observe that G_a is a Gauss sum, with the multiplicative character ω.

1. We have
$$J(\omega^{-a}, \omega^{-b}) = \frac{G_a G_b}{G_{a+b}}$$
Thus, $G_a G_b = J(\omega^{-a}, \omega^{-b}) G_{a+b}$. If we take the order of both sides, we get
$$\nu(a) + \nu(b) = ord_R(J(\omega^{-a}, \omega^{-b})) + \nu(a+b)$$
Since the order of any element is nonnegative, we have $\nu(a) + \nu(b) \geq \nu(a+b)$.

2. If we can show that $p-1 \mid ord_R(J(\omega^{-a}, \omega^{-b})$, then from the relation $\nu(a) + \nu(b) = ord_R(J(\omega^{-a}, \omega^{-b}) + \nu(a+b)$. We will be done,
We have that
$$\begin{aligned} J(\omega^{-a}, \omega^{-b}) &= \sum_{t \in \mathcal{F}} \omega^{-a}(t) \omega^{-b}(1-t) \\ &= \sum_{t \in \mathcal{F}} \omega^{a-b}(1-t) \\ &= \sum_{t \in \mathcal{F}} \left(\frac{\gamma}{Q}\right)^{a-b} \text{ where } \gamma \equiv 1 - t \pmod{Q} \end{aligned}$$
Since this sum is over all $\mathcal{F}$, we have a sum of q elements. Thus, we see that this sum will be congruent to 0 modulo Q. Since $QO_M = R^{p-1}$ and $J(\omega^{-a}, \omega^{-b}) \in Q$ it follows that $p-1 \mid ord_R(J(\omega^{-a}, \omega^{-b}))$.

3. Observe that since $\tau : \mathcal{F} \to F_p$, $\tau(t^p) = \tau(t)$. Thus
$$G_{pa} = \sum_{t \in \mathcal{F}} \omega^{-pa}(t) \psi(t) = \sum_{t \in \mathcal{F}} \omega^{-a}(t^p) \psi(t^p)$$
Since $t \to t^p$ is an automorphism of $\mathcal{F}$, we have $G_{pa} = G_a$ and hence $\nu(pa) = \nu(a)$.

4. We prove by induction on a and b. If $a = b = 1$, then $\nu(2) \leq 2$ and $\nu(2) \equiv 2 \pmod{p-1}$. Thus, $p-1 \mid \nu(2) - 2$ and since $\nu(2) \geq 0$, we have $\nu(2) = 2$.
If we assume this holds for all a and b such that $a + b < n$, then if $a + b = n$, we have $\nu(n) \leq \nu(n-1) + nu(1) = n$. Since $p-1 \mid \nu(n) - n$ this implies $\nu(n) = n$ for all $1 \leq n < q$.

□

Theorem 6.4.1. *$\nu(a) = S(a)$, where $1 \leq a < q$.*

Proof. If we let $a = a_0 + a_1 p + \ldots + a_{f-1}p^{f-1}$, where $0 \leq a_i < p$, then we have that

$$\nu(a) \leq \sum_{j=0}^{f-1} \nu(a_j p^j) = \sum_{j=0}^{f-1} \nu(a_j) = \sum_{j=0}^{f-1} a_j = S(a)$$

So, $\nu(a) \leq S(a)$ for all a such that $1 \leq a < q$. Now, we claim that

$$\sum_{a=1}^{q-2} \nu(a) = \frac{f(p-1)(q-2)}{2}$$

If we can show this, then we conclude that since

$$\sum_{a=1}^{q-2} \nu(a) \leq \sum_{a=1}^{q-2} S(a) = \frac{f(p-1)(q-2)}{2} = \sum_{a=1}^{q-2} \nu(a)$$

then $S(a) = \nu(a)$.

Consider $G_a G_{q-1-a}$. Since these are Gauss sums, we use their properties to obtain

$$G(\omega^{-a})G(\omega^{a-q+1}) = \omega^{-a}(1^{-1})\omega^{a-q+1}(1^{-1})G(\omega^{-a})G(\omega^{a-q+1})$$

This gives us $\omega^{-a}(1)p^f$. Note that $\omega^{-a}(1)$ reduces to 1, which is not in the proper ideal R. Since $ord_R(p) = p - 1$ we conclude that

$$\nu(a) + \nu(q-1-a) = f(p-1)$$

Thus, when we sum both sides of this equation from $a = 1$ to $a = q - 2$ we have $2\sum \nu(a) = f(p-1)(q-2)$, which completes the proof. □

Corollary 6.4.2. *$ord_P(\Phi(P)) = (m/(p-1))S((q-1)/m)$*

Proof. Since $ord_R(P) = (p-1)$ we have $(p-1)ord_P(\Phi(P)) = ord_R(\Phi(P))$. When $a = (q-1)/m$ we have $G(P) = G_a$. Hence, we have

$$ord_R(\Phi(P)) = ord_R(G(P)^m) = m \cdot ord_R(G(P)) = mS((q-1)/m)$$

Hence, $ord_P(\Phi(P)) = (m/(p-1))S((q-1)/m)$ as claimed. □

6.5 Stickelberger's Relation: The Proof

Definition 6.5.1. *Let $G = gal(\mathbb{Q}(\zeta_m) : \mathbb{Q})$. If P' is another prime ideal of O_K containing p then we've seen that there is an automorphism $\sigma_t \in G$ such that $P' = \sigma_t^{-1}P$. We will denote this by $P^{\sigma_t^{-1}}$. For $1 \leq t < m$, and $(t, m) = 1$, define $P_t = P^{\sigma_t^{-1}}$.*

Lemma 6.5.1. *$ord_{P_t}(\Phi(P)) = (m/(p-1))S(t((q-1)/m))$.*

Proof. Suppose $ord_{P_t}(\Phi(P)) = c$. Then since $\Phi(P) \subseteq P_t^c = P^{c\sigma_t^{-1}}$ we have $\Phi(P)^{\sigma_t} \subseteq P^c$ it follows that $ord_{P_t}(\Phi(P)) = ord_P(\Phi(P)^{\sigma_t})$.

Let t' be an integer such that $t' \equiv t \pmod m$ and $t' \equiv 1 \pmod p$. Then

$$G(P)^{\sigma_{t'}} = \left(\sum_{r\in F} \chi_P(r)\psi(r)\right)^{\sigma_{t'}} = \sum_{r\in F} \chi_P(r)^t\psi(r)$$

Since $\Phi(P) \in \mathbb{Q}(\zeta_m)$ we have that

$$\Phi(P)^{\sigma_{t'}} = \Phi(P)^{\sigma_t} = \left(\sum_{r\in F} \chi_P(r)^t\psi(r)\right)^m$$

Thus, when $a = t((q-1)/m)$ we have $\Phi(P)^{\sigma_t} = G_a^m$. Thus, following the same process as in the last corollory we conclude that $ord_{P_t}(\Phi(P)) = (m/(p-1))S(t((q-1)/m))$.

□

Theorem 6.5.1. *$\langle\Phi(P)\rangle = P^{\sum t\sigma_t^{-1}}$, where the sum is over all $t < m$ relatively prime to m.*

Proof. From the chapter on cyclotomic polynomials, we know the group $\{\sigma \in gal(\mathbb{Q}(\zeta_m) : \mathbb{Q}) \mid P^\sigma = P\}$ is a cyclic group of order f with generator σ_p. Since $g = \phi(m)/f$, there are g elements in $\mathbb{Z}_m^*$. Let $t_1, \ldots, t_g$ represent the cosets of $\mathbb{Z}_m^*$. Consider these g elements modulo the cyclic subgroup generated by the image of p. Then, if $1 \leq t < m$, there exists a unique pair (i, j) such that $t \equiv t_i p^j \pmod m$, $1 \leq i \leq g$, $0 \leq j < f$.

By the previous lemma, the prime decomposition of $\Phi(P)$ is given by $P^{\gamma'}$ where

$$\gamma' = \frac{m}{p-1}\sum_{i=1}^{g} S\left(t_i\frac{q-1}{m}\right)\sigma_{t_i}^{-1}$$

By lemma 6.3.2, this can be rewritten as

$$\gamma' = m \sum_{i=1}^{g} \left(\sum_{j=0}^{f-1} \ll \frac{p^j t_i}{m} \gg \right) \sigma_{t_i}^{-1}$$

Since P is unchanged under σ_{p^j}, for any $j = 0, 1, \ldots, f-1$, we have $P^{\gamma'} = P^{\gamma \sigma_{p^j}^{-1}}$. Thus,

$$\begin{aligned} \gamma &= m \sum_{i=1}^{g} \sum_{j=0}^{f-1} \ll \frac{p^j t_i}{m} \gg \sigma_{t_i}^{-1} \sigma_{p^j}^{-1} \\ &= m \sum_{(t,m)=1} \ll \frac{t}{m} \gg \sigma_t^{-1} \\ &= m \sum_{(t,m)=1} \left(\frac{t}{m} \right) \sigma_t^{-1} \text{ since } t < m \\ &= \sum_{(t,m)=1} t \sigma_t^{-1} \end{aligned}$$

This yields the proof. □

6.6 Eisenstein Reciprocity: Lemmas

In this section, we let $G = gal(\mathbb{Q}(\zeta_m) : \mathbb{Q})$, with elements σ_t, $1 \leq t < m$ and $(t, m) = 1$. As well, we fix $\gamma = \sum_t t \sigma_t^{-1}$ where the sum is taken over all $t < m$ such that $(t, m) = 1$.

Lemma 6.6.1. *The only roots of unity in $\mathbb{Q}(\zeta_m)$ are $\pm\zeta_m^i$ where $1 \leq i \leq m$.*

Proof. For our purposes, it is sufficient to prove this when $m = l$ is an odd prime. Suppose $\zeta_n \in \mathbb{Q}(\zeta_l)$. If $4 \mid n$ then $\imath \in \mathbb{Q}(\zeta_l)$. But, from our chapter on algebraic number theory, we have that a prime ideal P containing 2 is ramified iff $4 \mid l$. Since l is prime, this does not happen. Hoever, we have that a prime ideal P containing 2 is ramified in $\mathbb{Q}(\imath)$. We've established $\imath \in \mathbb{Q}(\zeta_l n)$ and so it follows that $qq(\imath) \subset \mathbb{Q}(\zeta_l)$. Thus, we have contradicted the assumption that $4 \mid n$.

So, write $n = 2n_0$ where n_0 is some odd integer. Thus, we have $\zeta_n^j = \pm\zeta_{n_0}^j$ and so we lose nothing by assuming n is odd.

For any odd prime l' dividing n, this means $\zeta_{l'} \in \mathbb{Q}(\zeta_l)$. But, again we see that any prime ideal containing l' is ramified iff $l' \mid l$. But, l is prime which implies that $l' = l$, and so n is a power of l, say $n = l^a$. But, since $\zeta_{l^a} \in \mathbb{Q}(\zeta_l)$ this implies $\mathbb{Q}(\zeta_{l^a}) \subseteq \mathbb{Q}(\zeta_l)$. Hence

$$l^{a-1}(l-1) = [\mathbb{Q}(\zeta_{l^a}) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_l) : \mathbb{Q}] = l - 1$$

implies that $a = 1$. Hence, in $\mathbb{Q}(\zeta_l)$, where l is an odd prime, the only roots of unity are ζ_l^i, $i = 0, 1, 2, \ldots, l-1$. □

In the next proof we will use the fact that for an algebraic number field K, of degree n, with monomorphisms $\sigma_1, \ldots, \sigma_n$ and for an element $\alpha \in K$, the polynomial

$$\prod_{i=1}^{n}(x - \alpha^{\sigma_n})$$

has integer coefficients. We omit the lengthy proof here. One is given in [5].

Lemma 6.6.2. *Let K be an algebraic number field such that $n = [K : \mathbb{Q}]$. Then we have n isomorphisms of K into $\mathbb{C}$, which we denote by $\sigma_1, \ldots, \sigma_n$. Let $mon_K = \{\sigma_1, \ldots, \sigma_n\}$. If $\alpha \in K$ is such that $|\sigma_i(\alpha)| \leq 1$ for all $1 \leq i \leq n$, then α is a root of unity.*

Proof. Let

$$f(x) = \prod_{i=1}^{n}(x - \alpha^{\sigma_i})$$

By the above remarks, we have that $f(x) \in \mathbb{Z}[x]$.

Consider the coefficient of x^m in $f(x)$. Since $|\alpha^{\sigma_i}| \leq 1$ for all σ_i, we have

$$f(x) \leq \prod_{i=1}^{n}(x - 1) = (x-1)^n$$

Hence, the coefficient of x^m is bounded by $\binom{n}{m}$. So, in $\mathbb{Z}[x]$, there are finitely many ways of creating polynomials of degree n with the bounds placed on the coefficients.

If $|\alpha^{\sigma_i}| \leq 1$ for all $\sigma_i \in mon_K$, then for all $a \in \mathbb{Z}$,

$$|(\alpha^a)^{\sigma_i}| = |(\alpha^{\sigma_i})^a| = |\alpha^{\sigma_i}|^a \leq 1$$

Thus, infinitely many elements α^a, $a \in \mathbb{Z}$ are roots of finitely many polynomials. Hence, it follows that there must be two distinct powers of α which are equal. Thus, if $|\alpha^j| = |\alpha^m|$ for some integers j and m, then $|\alpha^{j-m}| = 1$, which implies that α is a root of unity. □

Definition 6.6.1. *Suppose $A \subset O_K$ is an ideal not containing m. Furthermore, assume $A = P_1P_2 \dots P_n$ is the prime decomposition of A. Then we define $\Phi(A) = \Phi(P_1) \dots \Phi(P_n)$. Thus, it is clear that for ideals A, B not containing m that $\Phi(AB) = \Phi(A)\Phi(B)$.*

For elements $\alpha, \beta \in O_K$, we say these are prime to each other if the prime ideal decomposition of each element has no ideals in common.

Lemma 6.6.3. *Let $A, B \subset O_K$ be ideals not containing m and $\alpha \in O_K$ is an element prime to m. Then*

1. $|\Phi(A)|^2 = N(A)^m$
2. $\langle \Phi(A) \rangle = A^\gamma$
3. $\Phi(< \alpha >) = \varepsilon(\alpha)\alpha^\gamma$, *where $\varepsilon(\alpha)$ is a unit in O_K.*

Proof. 1. We show this for a prime ideal P, such that $N(P) = q$. Then the general case will follow by multiplicativity. Thus, by definition

$$|\Phi(P)|^2 = (|G(P)|^2)^m = q^m = N(P)^m$$

2. Suppose $A = P_1 \dots P_n$. Then $\langle \Phi(A) \rangle = \langle \Phi(P_1) \dots \Phi(P_n) \rangle = P_1^\gamma \dots P_n^\gamma = A^\gamma$.

3. Notice that we have $\langle \Phi(< \alpha >) \rangle = \langle \alpha \rangle^\gamma = \langle \alpha^\gamma \rangle$. Thus, $\Phi(< \alpha >)$ and α^γ generate the same principal ideal. This means they must be associates, and differ by a unit, as claimed.

□

From now on, we let $\Phi(\alpha)$ denote $\Phi(< \alpha >)$.

Lemma 6.6.4. *Suppose A is an ideal in O_K not containing m. If $\sigma \in G$, then $\Phi(A)^\sigma = \Phi(A^\sigma)$*

Proof. Since Φ is multiplicative, we prove this theorem for a prime ideal P, and the general theorem will follow.

Similar to the proof of lemma 6.5.1, we let $\tilde{\sigma}$ be an automorphism of $\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q}$ which restricts to σ on $\mathbb{Q}(\zeta_m)$ and the identity on $\mathbb{Q}(\zeta_p)$. Since

$$G(P) = \sum_{r \in F} \chi_P(r)\psi(r) = \sum_{r \in F} \left(\frac{\gamma}{P}\right)_m^{-1} \psi(r)$$

we have

$$G(P)^{\tilde{\sigma}} = \sum_{r \in F} \left(\frac{\gamma^\sigma}{P^\sigma}\right)_m^{-1} \psi(r) = G(P^\sigma)$$

Here, we have used the fact that $\psi(r)^{\tilde{\sigma}} = \psi(r)$ since $\psi(r) \in \mathbb{Q}(\zeta_p)$. Thus, since $G(P)^{\tilde{\sigma}} = G(P^{\sigma})$, when we raise this to the m^{th} power, we get

$$\Phi(P)^{\tilde{\sigma}} = \Phi(P)^{\sigma} = \Phi(P^{\sigma})$$

□

Lemma 6.6.5. *For $\alpha \in O_K$, $|\alpha^{\gamma}|^2 = |N(\alpha)|^m$.*

Proof. Consider the automorphism σ_{-1}. Since the automorphisms of G only rearrange the powers of ζ_m, we have

$$\zeta_m^{\sigma_{-1}} = \zeta_m^{-1}$$

Hence,

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

We also have

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

Since we are considering t relatively prime to m, we can write σ_{-t} as σ_{m-t}. Similarly, we let $\gamma = \sum (m-t)\sigma_{m-t}^{-1}$. Thus,

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

Thus, since $N(\alpha) = \prod \alpha^{\sigma_t^{-1}} = \alpha^{\sum \sigma_t^{-1}}$, we conclude $|\alpha^{\gamma}|^2 = |N(\alpha)|^m$. □

Lemma 6.6.6. *Let $\alpha \in O_K$ be an element prime to m. Then $\Phi(\alpha) = \varepsilon(\alpha)\alpha^{\gamma}$, where $\varepsilon(\alpha) = \pm\zeta_m^i$ for some i.*

Proof. Considering Lemma 6.6.3, part (3), we need only prove that $\varepsilon(\alpha) = \pm\zeta_m^i$. (Recall that $\Phi(< \alpha >) = \Phi(\alpha)$.) From Lemma 6.6.3, part (1), we have $|\Phi(\alpha)|^2 = N(< \alpha >)^m$. The previous theorem tells us that $|\alpha^\gamma|^2 = |N(\alpha)|^m$ and we know that $N(< \alpha >) = |N(\alpha)|$ from the chapter on algebraic number theory.

Thus, combining these facts, we get $|\Phi(\alpha)| = |\varepsilon(\alpha)\alpha^\gamma|$. Thus, we must have $|\varepsilon(\alpha)| = 1$. From Lemma 6.6.4, $\Phi(\alpha)^\sigma = \Phi(\alpha^\sigma)$ for each $\sigma \in G$. Thus, we must have that $|\varepsilon(\alpha)^\sigma| = 1$ for each σ. From Lemma 6.6.2, this implies that $|\varepsilon(\alpha)|$ is a root of unity. Finally, since $\varepsilon(\alpha) \in \mathbb{Q}(\zeta_m)$, Lemma 6.6.1 tells us that $\varepsilon(\alpha) = \pm\zeta_m^i$, for some i. □

Theorem 6.6.1. *Suppose P and P' are ideals in O_K both not containing m. Furthermore, assume $(N(P), N(P')) = 1$. Then*

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

Proof. Let $N(P') = q' = p'^{f'}$, and recall that $q' \equiv 1 \pmod{m}$. Then,

$$\begin{aligned} G(P)^{q'} &\equiv \sum_{t\in F} \chi_P(t)^{q'}\psi(t)^{q'} (\text{mod } P') \\ &\equiv \sum_{t\in F} \chi_P(t)\psi(q't) (\text{mod } P') \\ &\equiv \chi_P(q')^{-1} \sum_{t\in F} \chi_P(q't)\psi(q't) \\ &\equiv \left(\frac{q'}{P}\right)_m G(P) (\text{mod } P') \end{aligned}$$

Thus, we've shown that $G(P)^{q'-1} \equiv \left(\frac{N(P')}{P}\right)_m \pmod{P'}$.

Conversely, we have

$$G(P)^{q'-1} = \Phi(P)^{(q'-1)/m} = \Phi(P)^{(N(P')-1)/m} \equiv \left(\frac{\Phi(P)}{P'}\right) (\text{mod } P')$$

Thus, since roots of unity are distinct cosets, we have that

$$\left(\frac{N(P')}{P}\right) = \left(\frac{\Phi(P)}{P'}\right)$$

□

Since both the power residue symbol, and the Φ symbol are multiplicative, we immediately conclude the following corollary.

Corollary 6.6.2. *Suppose $A, B \subset O_K$ are ideals prime to m and $(N(A), N(B)) = 1$. Then*

$$\left(\frac{N(B)}{A}\right)_m = \left(\frac{\Phi(A)}{B}\right)_m$$

Corollary 6.6.3. *Suppose $A, B \subset O_K$ are ideals not containing m with $(N(A), N(B)) = 1$. Furthermore, assume A is a principal ideal with $A = (\alpha)$. Then*

$$\left(\frac{\varepsilon(\alpha)}{B}\right)_m \left(\frac{\alpha}{N(B)}\right)_m = \left(\frac{N(B)}{\alpha}\right)_m$$

Proof. First, we have

$$\left(\frac{\Phi(\alpha)}{B}\right)_m = \left(\frac{\varepsilon(\alpha)}{B}\right)_m \left(\frac{\alpha^\gamma}{B}\right)_m$$

by Lemma 6.6.3.

Next, we note that, considering theorem 6.1.3

$$\left(\frac{\alpha^{t\sigma_t^{-1}}}{B}\right)_m = \left(\frac{\alpha^{\sigma_t^{-1}}}{B}\right)_m^t = \left(\frac{\alpha^{\sigma_t^{-1}}}{B}\right)_m^{\sigma_{t'}} = \left(\frac{\alpha}{B^{\sigma_{t'}}}\right)_m$$

Here, we have used the fact that there exists a monomorphism $\theta : G \to \mathbb{Z}_m^*$ such that $\zeta_m^\sigma = \zeta_m^{\theta(\sigma)}$. Note that $t' \in \mathbb{Z}_m^*$.

Thus, from these two facts, we get that

$$\left(\frac{\alpha^\gamma}{B}\right)_m = \left(\frac{\alpha^{\sum t\sigma_t^{-1}}}{B}\right)_m = \prod_{(t,m)=1} \left(\frac{\alpha^{t\sigma_t^{-1}}}{B}\right)_m = \prod_{(t,m)=1} \left(\frac{\alpha}{B^{\sigma_t}}\right)_m = \left(\frac{\alpha}{N(B)}\right)_m$$

This last equality follows from theorem 2.11.5 in the chapter on algebraic number theory.

Thus, we conclude that, since $\left(\frac{\Phi(\alpha)}{B}\right)_m = \left(\frac{N(B)}{\alpha}\right)_m$ by the previous corollary,

$$\left(\frac{N(B)}{\alpha}\right)_m = \left(\frac{\varepsilon(\alpha)}{B}\right)_m \left(\frac{\alpha}{N(B)}\right)_m$$

□

6.7 Eisenstein Reciprocity: The Proof

From now on, we will assume m is an odd prime.

Lemma 6.7.1. *If $A \in O_K$ is an ideal not containing m, then $\Phi(A) \equiv \pm 1$ (mod m).*

Proof. Since Φ is multiplicative, it is enough to show that, for a prime ideal $P \in O_K$ not containing m, $\Phi(P) \equiv -1 \pmod{m}$.

If P is such a prime ideal, then

$$\Phi(P) = G(P)^m \equiv \sum_{t \in F^*} \chi_P(t)^m \psi(t)^m \equiv \sum_{t \in F^*} \psi(mt) (\text{mod } m)$$

Thus, from theorem 3.2.2, this last sum is equal to 0. Hence, we must have

$$\sum_{t \in F^*} \psi(mt) + \psi(0) \equiv 0 (\text{mod } m)$$

Since $\psi(0) = 1$, we have shown that $\Phi(P) \equiv -1 \pmod{m}$. □

Lemma 6.7.2. *If $\alpha \in O_K$ is primary, then $\varepsilon(\alpha) = \pm 1$*

Proof. We've seen that $< m >=< 1 - \zeta_m >^{m-1}$ in O_K, and $< 1 - \zeta_m >$ is a prime ideal.Hence, since $< 1 - \zeta_m >$ is a maximal ideal, it is the unique ideal containing m. Thus, if $\sigma \in G$, then σ will fix m. So, $< 1 - \zeta_m >^{\sigma} =< 1 - \zeta_m >$ for all $\sigma \in G$. Hence,

$$< 1 - \zeta_m >^{\gamma} =< 1 - \zeta_m >^{\sum t\sigma_t^{-1}} =< 1 - \zeta_m >^{\sum t} \subset < 1 - \zeta_m >$$

We have that $\Phi(\alpha) = \varepsilon(\alpha)\alpha^{\gamma}$, and we've seen that $\Phi(\alpha) \equiv \pm 1 \pmod{m}$. Thus, $\varepsilon(\alpha)\alpha^{\gamma} \equiv \pm 1 \pmod{m}$.

Since α is primary, it is congruent to some integer x modulo $(1 - \zeta_m)^2$. Thus, from this we get

$$\alpha^{\gamma} \equiv x^{\gamma} \equiv x^{\sum t\sigma_t^{-1}} \equiv x^{1+2+\ldots+m-1} (\text{mod } (1 - \zeta_m)^2)$$

Euler's theorem tells us that $x^{(m-1)/2} \equiv \pm 1 \pmod{m}$. Thus, since $1 + 2 + \ldots + m - 1 = \frac{m(m-1)}{2}$, we have

$$\alpha^{\gamma} \equiv (\pm 1)^m \equiv \pm 1 (\text{mod } (1 - \zeta_m)^2)$$

From this, we must have that $\varepsilon(\alpha) \equiv \pm 1 \pmod{(1-\zeta_m)^2}$. From Lemma 1.6.6., we have $\varepsilon(\alpha) = \pm\zeta_m^i$. If we can show that $m \mid i$, then we can conclude the lemma.

We have shown that $\zeta_m^i \equiv \pm 1 (\text{mod } (1-\zeta_m)^2)$. If we write $1-(1-\zeta_m)$ for ζ_m then

$$\zeta_m^i = (1-(1-\zeta_m))^i \equiv 1 - i(1-\zeta_m) \equiv \pm 1 (\text{mod } (1-\zeta_m)^2)$$

We cannot have $1 - i(1-\zeta_m) \equiv 1 \pmod{(1-\zeta_m)^2}$. If so, this would imply that $(1-\zeta_m) \mid 2$, which means $2 \in < 1-\zeta_m >$. But we have $m \in < 1-\zeta_m >$, and m is an odd prime. So this is a contradiction. Thus, we have that $1 - i(1-\zeta_m) \equiv 1 \pmod{(1-\zeta_m)^2}$ and hence, subtracting 1 from both sides, we conclude

$$(1-\zeta_m)^2 \mid i(1-\zeta_m) \Rightarrow (1-\zeta_m) \mid i$$

Thus, we have $m \mid (1-\zeta_m)$ and $(1-\zeta_m) \mid i$, and since $i \in \mathbb{Z}$ we conclude $m \mid i$. This completes the lemma. □

Lemma 6.7.3. *If $\alpha \in O_K$ is primary, B is an ideal not containing m and α and $N(B)$ are prime to each other, then*

$$\left(\frac{\alpha}{N(B)}\right)_m = \left(\frac{N(B)}{\alpha}\right)_m$$

Proof. From Corollary 6.6.3, we have

$$\left(\frac{N(B)}{\alpha}\right)_m = \left(\frac{\varepsilon(\alpha)}{B}\right)_m \left(\frac{\alpha}{N(B)}\right)_m$$

From the previous lemma, we have $\varepsilon(\alpha) = \pm 1$. If $\varepsilon(\alpha) = 1$, the lemma holds. Hence, assume $\varepsilon(\alpha) = -1$. Thus, from theorem 6.1.1, we have that

$$\left(\frac{-1}{B}\right)_m = 1 iff x^m \equiv -1 (\text{mod } B)$$

is solvable in O_K. Since m is an odd prime, $-1^m = 1$ and we're done. □

Theorem 6.7.1. *(Eisenstein Reciprocity Theorem)*

If $a \in \mathbb{Z}$, $(a,m) = 1$ and $\alpha \in O_K$ is primary and prime to a such that $(\alpha, a) = 1$. Then

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

Proof. Suppose $p \in \mathbb{Z}$ is prime, $p \neq m$ and p is prime to α in O_K. Let P be a prime ideal in O_K containing p. Then $N(P) = p^f$ for some $f \geq 1$. Consider the previous lemma, with P substituted for B. Then

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

Here, we have used the fact that

$$\left(\frac{\alpha}{p^f}\right)_m = \left(\frac{\alpha}{<p>^f}\right)_m = \left(\frac{\alpha}{<p>}\right)^f = \left(\frac{\alpha}{p}\right)_m^f$$

We have that $p^f \equiv 1 \pmod{m}$ and hence $f \mid m-1$. Thus, $(m, f) = 1$, and an inverse to f exists modulo m. Hence, we conclude that

$$\left(\frac{\alpha}{p}\right)_m = \left(\frac{p}{\alpha}\right)_m$$

Finally, due to multiplicativity, we conclude that, for all $a \in \mathbb{Z}$ prime to m and α, with $\alpha \in O_K$ a primary element, we have

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

□

Chapter 7

Applications

7.1 Erdos' Conjecture

Conjecture 7.1.1. *Every odd prime q has a prime primitive root p, with $p < q$.*

7.2 Residues And Divisibility

Lemma 7.2.1. *Suppose x is a QNR modulo q, an odd prime. Then x^n is a QNR iff n is odd.*

Proof. Suppose x^n is a QNR. If $n = 2k$, for some $k \in \mathbb{Z}$, then $(x^k)^2 \equiv x^n \pmod{q}$. This contradicts the fact that x is a QNR. Hence, we must have that n is odd.

Conversely, suppose n is an odd integer, say $n = 2k + 1$ for some $k \in \mathbb{Z}$. We know that $y^2 \neq x \pmod{q}$, for all $y \in \mathbb{Z}$. So, if $z^2 \equiv x^n \equiv x^{2k+1} \pmod{q}$, for some z, we then get $z^2 \equiv x^{2k+1} \equiv x^{2k}x \pmod{q}$. This implies that $(zx^{-k})^2 \equiv x \pmod{q}$, a contradiction. Hence, x^n is a QNR. □

Theorem 7.2.1. *Suppose q is an odd prime, $n \mid \phi(q)$ and x is an n^{th} non residue. Then x can never have order $\frac{q-1}{n}$.*

Proof. Suppose x is an n^{th} non residue modulo q and $|x| = \frac{q-1}{n}$. Furthermore, assume g is a primitive root modulo q and $g^m \equiv x \pmod{q}$ Since x is an n^{th} non residue, by the division algorithm, we write $m = an + b$, for $a \geq 0$ and $0 < b < n$. (Note that $b \neq 0$.)

We then have $g^m \equiv g^{an+b} \pmod{q}$ and $g^{m\frac{q-1}{n}} \equiv x^{\frac{q-1}{n}} \equiv 1 \pmod{q}$. This gives

$$g^{(an+b)(\frac{q-1}{n})} \equiv g^{a(q-1)} g^{b(\frac{q-1}{n})} \equiv 1 (\text{mod } q)$$

However, this implies that $g^{b(\frac{q-1}{n})} \equiv 1 \pmod{q}$, a contradiction as $b < n$. Hence, we conclude that x does not have order $\frac{q-1}{n}$. □

Theorem 7.2.2. *If q is any odd prime and n is an integer such that $n \mid \phi(q)$, then for any $x < q$, $|x| \mid \frac{q-1}{n}$ iff x is an n^{th} residue.*

Proof. Suppose $|x| \mid \frac{q-1}{n}$ and $m \in \mathbb{Z}$ is such that $\frac{q-1}{n} = m|x|$. This implies that $|x| = \frac{q-1}{mn}$. Let g be a primitive root with $g^a \equiv x \pmod{q}$, for some integer a. Then $g^{a(\frac{q-1}{mn})} \equiv x^{\frac{q-1}{mn}} \equiv 1 \pmod{q}$. Hence, $\frac{a}{mn} \in \mathbb{Z}$. Suppose z is an integer such that $a = mnz$. Then we have

$$g^a \equiv (g^{mz})^n \equiv x (\text{mod } q)$$

and x is an n^{th} residue.

Conversely, assume x is an n^{th} residue, and $|x| = \frac{q-1}{m}$. It remains to show that $n \mid m$. Suppose g is a primitive root and $g^m \equiv x \pmod{q}$. Since x is an n^{th} residue, we have $g^m \equiv g^{na} \equiv x \pmod{q}$, for some integer a. Hence, $m = na$ and $n \mid m$. Thus, $|x| \mid \frac{q-1}{n}$. □

Theorem 7.2.3. *If q is any odd prime and $n \neq 1$ is any integer such that $n \mid \phi(q)$, then if x is an n^{th} non residue, $n \mid |x|$.*

Proof. Suppose x is an n^{th} non residue and $|x| = m$. Furthermore, suppose g is a primitive root such that $g^{\frac{q-1}{m}} \equiv x \pmod{q}$. Consider $(\frac{q-1}{m}, n)$. Since x is an n^{th} non residue, $(\frac{q-1}{m}, n) < n$. Furthermore, since $n \mid q-1$, we must have $n \mid m$. Hence, $n \mid |x|$. □

Theorem 7.2.4. *Let q be any odd prime and denote the set of all non-unit divisors of q by D. Then g is a primitive root modulo q iff $\forall n \in D$, g is an n^{th} non residue.*

Proof. Suppose g is a primitive root mod q. Then $|g| = q - 1$. Suppose $d \in D$ and $g \equiv h^d \pmod{q}$, for some $h < q$. Thus, g is a d^{th} residue means $|g| \mid \frac{q-1}{d}$. This implies there exists an integer n such that $\frac{q-1}{d} = n(q-1)$ which further implies that $\frac{1}{d} = n$. Clearly, this is false unless $d = 1$. Since $1 \notin D$, there does not exist any h such that $h^d \equiv g \pmod{q}$. Hence, for every $d \in D$, g is a d^{th} non residue.

Conversely, suppose g is an n^{th} non residue $\forall n \neq 1$ with $n \mid \phi(q)$. Furthermore, assume $g = \frac{q-1}{m}$. If $m \neq 1$, this means there exists an integer y such that $y^m \equiv g \pmod{q}$ with $m \mid \phi(q)$. Clearly, this is false and so $m = 1$ and g is a primitive root. □

7.3 Completely Residue Free

Definition 7.3.1. *Suppose q is any odd prime. Denote by D the set of all proper divisors of $\phi(q)$. (So, $1 \notin D$.) We say that an element g is completely residue free if, for all $d \in D$, g is a d^{th} non residue. (Note that this is equivalent to saying that g is a primitive root.)*

Theorem 7.3.1. *Let q be any odd prime and $n, a \in \mathbb{Z}$ are such that $n^a \mid \phi(q)$, with $a \neq 0$. If x is an n^{th} non residue, the for $1 \leq k \leq a$, x is an $(n^k)^{th}$ non residue.*

Proof. Suppose x is an n^{th} non residue but $(y^n)^a \equiv x \pmod{q}$ for some integer $a \neq 0$. But,

$$(y^n)^a \equiv y^{na} \equiv (y^a)^n (\text{mod } q)$$

is a contradiction. Hence, the theorem holds. □

Hence, we've shown that if $q - 1 = p_1^{a_1} \dots p_n^{a_n}$, then a prime p is a primitive root if it is a p_i^{th} non residue, for $1 \leq i \leq n$.

7.4 Quadratic Reciprocity

In this section, our methods of proof depends heavily on identifying the possible orders of a prime p, then reducing those possibilities. Hence we define $\alpha_q(p)$ to be the set of all possible orders of p modulo q. In this fashion, we will have $|\alpha_q(p)| > 1$, then reduce the number of elements to 1.

Theorem 7.4.1. *If q is an odd prime such that $q = 2p + 1$, for a prime $p \equiv 3$ (mod 4), then p is a primitive root modulo q.*

Proof. We have that $q - 1 = 2p$. Hence, $\alpha_q(p) = \{p, 2p\}$. (Clearly, $|p| \neq 2$, and so we have tacitly eliminated that possibility.) It remains to show that p is a quadratic non residue. Once we have done that, then by theorem 3.2.3, $2 \mid |p|$ and hence we must have $|p| = 2p$.

Since $p \equiv 3 \pmod{4}$, we have $q \equiv 7 \equiv 3 \pmod{4}$ and hence

$$(\frac{p}{q}) = -(\frac{q}{p}) = -(\frac{1}{p}) = -1$$

and so p is a quadratic non residue and p is a primitive root modulo q. $\square$

7.5 Cubic Reciprocity

In this section, we will demonstrate that primes of the form $6p+1$, where p is a certain prime, have p as a primitive root.

Lemma 7.5.1. *Suppose $p \equiv 1$ (mod 3) is a prime. Then there exist integers a, b such that $p = a^2 - ab + b^2$.*

Proof. If $p \equiv 1 (\text{mod } 3)$, there is a character χ of order 3. The values of χ are in the set $\{1, \omega, \omega^2\}$, where $\omega = e^{2\pi\imath/3} = \frac{1}{2}(-1+\sqrt{-3})$. Thus, $J(\chi, \chi) \in \mathbb{Z}[\omega]$. Since $J(\chi, \chi) = a + b\omega$, where $a, b \in \mathbb{Z}$, then $p = |J(\chi, \chi)|^2 = |a + b\omega|^2 = a^2 - ab + b^2$. $\square$

Theorem 7.5.1. *Suppose $q = 6p + 1$, where $p \equiv 3$ (mod 4) and $q = a^2 - ab + b^2$ where $a, b > 0$. Then if $p \neq 7$, p is a primitive root modulo q.*

Proof. We have $\phi(q) = 6p$ and so the possible orders of p are: $2, 3, 6, p, 2p, 3p, 6p$. We will first show p is a quadratic residue, which reduces the possible orders to: $2, 6, 2p, 6p$. We then show p is a cubic residue, giving orders: $6, 6p$. We finish by showing that if $p \neq 7$, $ord_q(p) \neq 6$.

Since $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$, thus, from quadratic reciprocity, we have

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

and so p is a quadratic residue.

We have that $q \equiv 1 \pmod 3$. So, in Ω, there exists a prime π such that $N(\pi) = q$. Hence, the cubic reciprocity law tells us

$$\left(\frac{p}{\pi}\right)_3 \equiv p^{(N(\pi)-1)/3} \equiv p^{2p} (\text{mod } \pi)$$

We have assumed that $\pi = a + b\omega$, for positive integers a, b. Thus, for the above equation to equal 1, there must exist an element $\beta = x + y\omega \in \Omega$ such that

$$p^{2p} - 1 = (x + y\omega)(a + b\omega)$$

or

$$p^{2p} - 1 = (ax - by) + (ay + bx - by)\omega$$

Hence, we have $ax - by = p^{2p} - 1$ and $ay + bx - by = 0$. Then,

$$\begin{aligned} 0 &= ay + b(x - y) && (7.5.1)\\ ay &= b(y - x) && (7.5.2)\\ a &= \frac{b(y - x)}{y} && (7.5.3)\\ p^{2p} - 1 &= \frac{bx(y - x)}{y} - by && (7.5.4)\\ &= bx - \frac{bx^2}{y} - by && (7.5.5)\\ p^{2p} - 1 + \frac{bx^2}{y} &= b(x - y) && (7.5.6) \end{aligned}$$

If we assume $y > 0$, then the left hand side of (7.5.6) is greater than zero. Thus, $b(x - y) > 0 \Rightarrow x > y$. But, from (7.5.3), we see that this is a contradiction. Thus, we must have $y < 0$. So, from (7.5.3) we see that $y > x$.

Suppose $a < b$. Then, considering (7.5.3) we have

$$\frac{a}{b} = \frac{y - x}{y} \Rightarrow y - x < y \Rightarrow 0 < x$$

a contradiction.

Now, suppose $a > b$. Let $y = -n$ and $x = -m$, with $n, m > 0$. Then we rearrange (7.5.3) to get

$$b(n - m) = an \Rightarrow \frac{b}{a} = \frac{n}{n - m} \Rightarrow n - m > n \Rightarrow -m > 0$$

a contradiction. Thus, this shows that p is a cubic non-residue, and hence p has order 6 or $6p$.

Finally, suppose $p \neq 7$. If $ord_q(p) = 6$ then $p^3 \equiv -1 \pmod{q}$ or $p^3 \equiv 6p \pmod{q}$. Thus, $p^2 \equiv 6 \pmod{q}$. So, $p^2 = n(6p + 1) + 6$ for some $n < p$. Taking both sides modulo p, we see $n = p - 6$. Hence,

$$\begin{aligned} p^2 &= (p - 6)(6p + 1) + 6\\ p^2 &= 6p^2 - 35p\\ 0 &= 5p^2 - 35p\\ 0 &= 5p(p - 7) \end{aligned}$$

Hence, we have assumed $p \neq 7$, so this equality never holds. □

7.6 Eisenstein Reciprocity

For this final section, we let $K = \mathbb{Q}(\zeta_r)$ with ring of integers O_K. As well, r is an odd prime greater than 3. We let $GF(p^n)$ denote the Galois field with p^n elements. We have that $\phi(r) = r - 1 = [K : \mathbb{Q}]$. Consider the prime ideal generated by p, $pO_K = (P_1 P_2 \dots P_g)^e$ and $N(P_i) = p^f$ for each i. From Lemma 2.12.3, we know that $e = 1$, so that $gf = r - 1$. We can draw some simple conclusions for specific cases of the prime p.

Lemma 7.6.1. *Every integer is primary.*

Proof. Let x be any integer. Then $x \equiv x \pmod{(1-\zeta_r)^2}$ since $(1-\zeta_r)^2 \mid 0$. So, every integer is congruent to itself, which implies every integer is primary. □

In particular, we will be concerned with $q = 2pr + 1$ and the ideals generated by q and p. If $p^f = N(P_i)$ for some ideal P_i containing p, then recall that Theorem 2.12.5 tells us that f is the smallest integer such that $p^f \equiv 1 \pmod{r}$. This gives us our next theorem.

Theorem 7.6.1. *Let $q = 2pr + 1$ be prime, and let $p \neq r$ be prime as well. Then if $p \equiv 1 \pmod{r}$, p is an r^{th} residue modulo q.*

Proof. We have that $q \equiv 1 \pmod{p}$. Consider

$$pO_K =< p >= \prod_{i=1}^{g} P_i$$

Since $p \equiv 1 \pmod{r}$, $p^f \equiv 1 \pmod{r}$, and so $f = 1$. Thus, $N(P_i) = p$ and so the field O_K/P_i is isomorphic to $\mathbb{Z}_p$. Thus, an element α modulo P_i is equivalent to α modulo p. Thus, we have

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \equiv q^{(N(P)-1)/r} \equiv 1^{(N(P)-1)/r} \equiv 1 (\text{mod } p)$$

Thus, $\left(\frac{p}{q}\right) = 1$ means that p is an r^{th} residue modulo q. □

7.7 Conclusion

In general, the field O_K/P will be isomorphic to $GF(p^f)$. Suppose $\sigma : O_K/P \to GF(p^f)$. Then since

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \equiv q^{(N(P)-1)/r} (\text{mod } P)$$

If $\sigma(q)^{(p^f-1)/r} = 1$, then we can conclude that p is an r^{th} residue modulo q. Notice that p is an r^{th} residue if and only if σ takes $q^{(N(P)-1)/r}$ to 1. Thus, the difficulty lies not in the construction of $GF(p^f)$. Since we are concerned only with the orders of the elements, this field construction will be polynomial independent. The difficulty lies in finding a mapping, without knowing the generators of either field. The purpose of Eisenstein reciprocity was to simplify Erdos' conjecture, and possibly come up with conditions and classes of primes which have a prime primitive root. Unfortunately, there is no general mapping between these fields.

It is the author's belief that, should a mapping exist, and its properties become well-known and well-developed, then we should see some significant results using the Eisenstein reciprocity law.

Chapter 8

Bibliography

1. F. Lemmermeyer, Reciprocity Laws, Springer-Verlag, 1991
2. K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, 1980
3. H. Cohen, A Course In Computational Algebraic Number Theory, Springer-Verlag,1993
4. J. Esmonde, M.R. Murty, Problems in Algebraic Number Theory, Springer-Verlag, 1999
5. S. Alaca, K.S. Williams, Introductory Algebraic Number Theory, Cambridge University Press,2004
6. R. Kumanduri, C. Romero, Number Theory With Computer Applications, Prentice-Hall,1998
7. W. K. Nichloson, Introduction to Abstract Algebra, John Wiley & Sons, 1999
8. T. M. Apostol Introduction to Analytic Number Theory, Springer-Verlag, 1976
9. B. Berndt, R. Evans, K.S.Williams, Gauss and Jacobi Sums, John Wiley & Sons, 1998
10. R. K. Guy, Unsolved Problems in Number Theory; Unsolved Problems in Intuitive Mathematics - Vol. 1, Springer-Verlag, 1981
11. P. Elliott, L. Murata, On The Average Of The Least Primitive Root Modulo p, J. London Math Soc. (2) 56, 1997, pp. 435-454

12. P. Elliott, The Least Prime Primitive Root and Linnik's Theorem, Number Theory for the Millennium I, A K Peters, 2002

13. A. Paszkiewicz, A. Schinzel, On the Least Prime Primitive Root Modulo A Prime, Mathematics Of Computation, (71) 239, 2002, pp. 1307-1321