NOTES ON INTRODUCTORY ALGEBRAIC NUMBER THEORY

NATE SAUDER

Abstract. This paper introduces the basic results of Algebraic Number Theory. Accordingly, having established the existence of integral bases and the result that ideals in Dedekind domains can be uniquely decomposed into prime ideals, we then give the relation between ramification index, residue class degree and the degree of the extension. Moreover, we also demonstrate the connection between the decomposition group and the Galois groups of certain tower extensions. We then employ Minkowski's bound to prove several properties of algebraic number fields. Furthermore, we develop this theory in the context of quadratic and cyclotomic extensions of $\mathbb{Q}$ in order to prove quadratic reciprocity and to demonstrate the strong relationship between the Čebotarev and Dirichlet prime density theorems. This paper assumes a background knowledge of Commutative Algebra and Galois theory.

Contents

Date: August 20th 2013.

1. Ring of Integers

1.1. **Factorization in the ring $\mathbb{Z}$.** The prime factorization theorem says that every integer can be factored uniquely (up to sign) into a product of prime numbers; i.e. for all z in $\mathbb{Z}$, there exists $p_1, \ldots, p_n$ such that $z = \pm p_1 \cdot \ldots \cdot p_n$.

1.2. **Ring of Integers definition.**

Definition 1.1. An *algebraic number field* is a finite algebraic extension of $\mathbb{Q}$.

Definition 1.2. Let A be an integral domain, K be a field that contains A and L be an extension of K. $x \in L$ is an *integral element* if and only if there exist

$$a_{n-1}, \ldots, a_0 \in A \text{ such that } x^n + a_{n-1}x^{n-1} \ldots + a_0 = 0$$

In an algebraic number field, integral elements are called *algebraic integers*.

We will see that the integral elements form the *Ring of Integers* and that every element in the ring of integers can be decomposed into irreducible elements (using the Noetherian Ring property). However, uniqueness cannot always be insured. Instead, we will restrict our attention to the ideals of the Ring of Integers and demonstrate that they can be decomposed *uniquely* into prime ideals.

1.3. **Integral Elements form a Ring.** In order to show that the set of integral elements do indeed form a ring, we first need the following lemma.

Proposition 1.3. *$x \in K$ is integral over A if and only if there is a finitely generated A-submodule of K such that $xM \subset M$*

Proof. $\Rightarrow$ If $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ for $a_{n-1}, ..., a_0 \in A$, then consider the A-module

$$N = \text{span}(1, x, ..., x^{n-1})$$

$a_n = 1$ implies that $x^n \in N$. Therefore, N is finitely generated and $xN \subset N$. The others powers of x follow from induction.

$\Leftarrow$ Conversely, let $M = \text{span}_A(u_1, \ldots, u_n)$ be a finitely generated module over K. Furthermore, assume that $xM \subset M$ for some $x \in K$. Then

$$xu_i = a_{i1}u_1 + \ldots + a_{in}u_n, \forall i \in (1, \ldots, n)$$

This leads to the following linear equations:

$$\begin{aligned} (x - a_{11})u_1 - a_{12}u_2 - \ldots - a_{1n}u_n &= 0 \\ &\vdots \\ -a_{n1}u_1 - \ldots - a_{n(n-1)}u_{n-1} + (x - a_{nn})u_n &= 0 \end{aligned}$$

Let B be the matrix formed by the coefficients of these linear equations. Since B has a non-zero kernel, we conclude that $\det(B) = 0$. This implies that x satisfies an equation of the form

$$\beta_n x^n + \beta_{n-1} x^{n-1} + \ldots + \beta_0 = 0$$

where the $\beta_i \in \mathrm{A}$. This polynomial is monic since the permutation definition of the determinant shows that degree n terms only occur when multiplying $\prod b_{ii}$. Thus, $\beta_n = 1$ and x is an integral element. □

Proposition 1.4. *If A is an integral domain, K a field that contains A and L an extension of K, then the set*

$$\{x \in L : \exists a_{n-1}, \ldots, a_0 \in A : x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0\}$$

forms a ring.

Proof. Let x and y be integral elements and M and N be finitely generated submodules of K such that $xM \subset M$ and $yN \subset N$. We verify that $x \cdot y$ and $x + y$ are also integral. We do so by considering the (finitely generated) submodule MN formed by the span of all products of elements in M and N. MN is closed under multiplication by $x \cdot y$ and $x + y$ since $xm \in M$ and $yn \in N$ for $m \in M$ and for $n \in N$. □

1.4. **Ring of Integers are Finitely Generated.**

Lemma 1.5. *Let K be a number field and $\alpha \in K$, then there exists an integer multiple of α that is an algebraic integer.*

Proof. By assumption, α satisfies an equation of the form

$$\sum b_i \alpha^i = 0 \text{ where } b_i \in \mathbb{Q} \text{ and } b_n = 1 \tag{1.6}$$

Let l be the l.c.m of the b_i. Then, multiplying (1.6) by l^m, we have that

$$l^m \alpha^m + b_{n-1} l(l^{n-1})\alpha^{n-1} + \ldots + b_0 l^m = 0 \tag{1.7}$$

Thus, $l \cdot \alpha$ is an integral element. □

2. Trace and Norm

Definition 2.1. Trace and Norm: Let $A \subset B$ be rings such that B is a free A-module of rank m and $\beta \in B$. $x \mapsto \beta x$ defines a linear mapping on B as a A-module. Then, $\mathrm{Tr}_{B/A}(\beta)$ is defined to be the trace of this mapping and the $\mathrm{Nm}_{B/A}\beta$ its determinant.

Lemma 2.2. *Let L be a finite extension of K, let $\mathcal{O}_L = B$ and let $\mathcal{O}_K = A$. Then, $\alpha \in L$ is integral over A if and only if the coefficients of its minimal polynomial over K belong to A.*

Proof. $\implies$ Clear.

$\impliedby$ Let α be an integral element, $f_\alpha(x)$ be the minimal polynomial for α, and β be another root of f. Then, there is an isomorphism, σ, from $K[\alpha]$ to $K[\beta]$ since each is isomorphic to $K[x]/(f_\alpha(x))$. Furthermore, there exists a_i in A such that

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

Applying σ to this polynomial, we have that

$$\beta^n + a_{n-1}\beta^{n-1} + \ldots + \beta_0 = 0$$

Thus, β is integral and, by similar logic, all conjugates of α are integral. But, the coefficients of the minimal polynomial are symmetric polynomials of the roots and thus are also integral.

□

Corollary 2.3. *Let K be an algebraic number field and α be an algebraic integer. Then $Tr_K(\alpha) = \sum_{k=1}^{n} \sigma_k(\alpha)$ and $Nm_K(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha)$ and so $Tr_K(\alpha)$ and $Nm_K(\alpha)$ are in $\mathbb{Z}$.*

Proof. Let $v_1, ..., v_n$ be a basis for K over $\mathbb{Q}$. If $\alpha \cdot v_i = \sum a_{ij} v_j$, then $Tr_K(\alpha)$ is the trace of the matrix (a_{ij}) and $Nm_K(\alpha)$ the determinant. The equation still holds under action by $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Thus, we arrive at the set of equations:

$$\sigma_k(\alpha) \cdot \sigma_k(v_i) = \sum_{j=1}^{n} a_{ij}\sigma_k(v_j)$$

These equations can be concatenated using the Kronecker delta function as follows:

$$\sum_{j=1}^{n} \delta_{ik}\sigma_j(\alpha) \cdot \sigma_j(v_i) = \sum_{j=1}^{n} a_{ij}\sigma_k(v_j)$$

If $A_0 = (\sigma_j(\alpha) \cdot \delta_{ij})$, $S = (\sigma_j(v_i))$, and $A = (a_{ij})$, then $S \cdot A_0 = A \cdot S$. Therefore,

$$\mathrm{Tr}(A) = \mathrm{Tr}(A_0) = \sum_{k=1}^{n} \sigma_k(\alpha)$$

$$\det(A) = \det(A_0) = \prod_{k=1}^{n} \sigma_k(\alpha)$$

But, the $\sigma_k(\alpha)$ are the conjugate roots of α and thus all algebraic integers by Lemma 2.2.

□

Example 2.4. Computation of the Trace and Norm of elements in Cyclotomic Fields:

Let $K = \mathbb{Q}[\zeta_p]$ be the p^{th} cyclotomic field (p is prime), and let ζ_p^k be a primitive element. Then,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p^k) = \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{p-1} = \Phi(\zeta_p) - 1 = -1$$

This is the coefficient of the x^{p-1} term as expected. Furthermore, by linearity of the trace,

$$\mathrm{Tr}_{K/\mathbb{Q}}(1-\zeta^k) = (p-1) - (-1) = p$$

From the relation $p = \prod_j (1-\zeta^j)$, $\mathrm{Nm}_{K/\mathbb{Q}}(1-\zeta^k) = p$.

Proposition 2.5. *If L is a finite separable extension of K, the trace pairing is non-degenerate. In other words, if $v_1, \ldots, v_n$ is a basis for L over K, then the determinant of the bilinear pairing $(v_i, v_j) \mapsto Tr_{L/K}(v_i v_j)$ is non-zero.*

Proof. Since the arguments in Corollary 2.3 generalize to any finite separable extension L/K, we see that

$$\mathrm{Tr}(v_i v_j) = \sum_k \sigma_k(v_i)\sigma_k(v_j) = SS^T$$

where $S = (\sigma_j v_i)$ as above. Since $(v_1, \ldots, v_n)$ is a basis and L is a separable extension of K, S is non-singular and therefore $\mathrm{Tr}(v_i v_j)$ is also non-singular. Thus, the trace pairing is non-degenerate.

□

3. Integral Bases

Theorem 3.1. *Let K be a number field of degree n, then its ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-Module of rank n.*

Proof. Let $(a_1, \ldots, a_n)$ be a basis for K over $\mathbb{Q}$. By Lemma 1.5, we can multiply $(a_1, \ldots, a_n)$ by an integer and arrive at a basis, $(b_1, ..., b_n)$, for K such that the b_i are in $\mathcal{O}_K$. We now construct a group homomorphism, ϕ, from K to $\mathbb{Q}^n$ and verify that restricted to $\mathcal{O}_K$ it forms an injection from $\mathcal{O}_K$ to $\mathbb{Z}^n$.

$$\phi(\gamma) := (Tr_{K/\mathbb{Q}}(b_1 \cdot \gamma), \ldots, Tr_{K/\mathbb{Q}}(b_n \cdot \gamma)).$$

ϕ is injective since the trace pairing is non-degenerate by Proposition 2.5. Furthermore, if α is integral, $Tr_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ by Corollary 2.3. $\phi : \mathcal{O}_K \hookrightarrow \mathbb{Z}^n$ implies that $\mathcal{O}_K$ must have rank less than or equal to n since, by the Fundamental Theorem of Abelian groups, an isomorphism between the $\mathbb{Z}$-modules $Im(\phi) \subset \mathbb{Z}^n$ and $\mathcal{O}_K$ is only possible if

$$\mathrm{rank}(\mathcal{O}_K) = \mathrm{rank}(\mathrm{Im}(\phi)) \leq n$$

But, $(b_1, \ldots, b_n)$ are linearly independent. We conclude that $\mathcal{O}_K$ is of rank n as $\mathbb{Z}$-module. □

3.1. Integral Bases of $\mathbb{Q}[\sqrt{D}]$ and $\mathbb{Q}[\zeta]$.

Example 3.2. Integral Basis of $\mathbb{Q}[\sqrt{D}]$:

Let $K = \mathbb{Q}[\sqrt{D}]$ and take $\alpha = a + b\sqrt{D} \in K$ Since K is a quadratic field extension, there is only one other conjugate: $a - b\sqrt{D}$. Thus, $Tr_k(\alpha) = 2a$ and $Nm_K(\alpha) = a^2 - b^2 D$. Furthermore, $Tr_k(\alpha)$ and $Nm_K(\alpha)$ are in $\mathbb{Z}$ by Corollary 2.3.

If α is an algebraic integer, the trace being an integer dictates that $2a \in \mathbb{Z}$ and similarly $a^2 - b^2 D \in \mathbb{Z}$ dictates that $2b \in \mathbb{Z}$ since the denominator of a is at most 2. Setting $a = \frac{z_1}{2}$ and $b = \frac{z_2}{2}$ where z_1 and $z_2 \in \mathbb{Z}$, the following restriction holds:

$$\frac{z_1^2 - z_2^2 \cdot D}{4} \in \mathbb{Z}$$

We now investigate the three different possibilities of D mod (4).

Possibility 1: $D \equiv 2, 3 \bmod 4$.

$z_1^2 \equiv z_2^2 D \bmod 4$ implies that either z_1 and z_2 must be even. Thus, $(1, \sqrt{D})$ is an integral basis for $\mathcal{O}_K$.

Possibility 2: $D \equiv 1 \bmod 4$.

$z_1^2 \equiv z_2^2 D \bmod 4$ implies that z_1 and z_2 are either both odd or both even. So, a and b are either both integers or both fractions with denominator equal to 2. Both choices are spanned by $(1, \frac{1+\sqrt{D}}{2})$. Therefore, $(1, \frac{1+\sqrt{D}}{2})$ is an integral basis since $\frac{1+\sqrt{D}}{2}$ is an algebraic integer.

Example 3.3. We find that $\mathbb{Z}[\zeta_p]$ is an integral basis for $K = \mathbb{Q}[\zeta_p]$ but to show this we use the following two lemmas:

Lemma 3.4. $(1 - \zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$

Proof. Let $\zeta = \zeta_p$ for simplicity of notation. $p = \prod_j (1 - \zeta^j)$ implies that $p\mathbb{Z} \subseteq (1 - \zeta)\mathcal{O}_K \cap \mathbb{Z}$. Suppose this is a strict inclusion. Since $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$, we would have that $(1 - \zeta)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$. Therefore, there would exist α in $\mathcal{O}_K$ such that $\alpha \cdot (1 - \zeta) = 1$. This is a contradiction since $\mathrm{Nm}_{K/\mathbb{Q}}(1 - \zeta) = p$. □

Lemma 3.5. *For every $\alpha \in \mathcal{O}_K$, $Tr_K/\mathbb{Q}(\alpha(1 - \zeta)) \in p\mathbb{Z}$.*

Proof.

$$\begin{aligned} Tr_K/\mathbb{Q}(\alpha(1-\zeta)) &= \sigma_1((\alpha(1-\zeta)) + \sigma_2(\alpha(1-\zeta)) + \ldots + \sigma_{p-1}(\alpha(1-\zeta)) \\ &= \sigma_1(\alpha)(1-\zeta)) + \sigma_2(\alpha)(1-\zeta^2) + \ldots + \sigma_{p-1}(\alpha)(1-\zeta^{p-1}) \end{aligned}$$

For each j, we have that

$$(1 - \zeta^j) = (1 + \zeta + \ldots + \zeta^{j-1})(1 - \zeta)$$

and thus,

$$Tr_{K/\mathbb{Q}}(\alpha(1 - \zeta)) \in (1 - \zeta)\mathcal{O}_K$$

However, $Tr_{K/\mathbb{Q}}(\alpha(1 - \zeta)) \in Z$ by Corollary 2.3 and so

$$Tr_{K/\mathbb{Q}}(\alpha(1 - \zeta)) \in (1 - \zeta)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$$

□

Proposition 3.6. *$\mathbb{Z}[\zeta_p]$ is the ring of integers in $\mathbb{Q}[\zeta_p]$.*

Proof. Given α in $\mathcal{O}_K$,

$$\alpha = b_0 + b_1\zeta + \ldots + b_{p-2}\zeta^{p-2} \text{ for some } b_i \in \mathbb{Q}$$

Then,

$$\alpha(1-\zeta) = b_0(1-\zeta) + b_1(1-\zeta^2) + \ldots + b_{p-2}(\zeta^{p-2} - \zeta^{p-1})$$

Example 2.4 implies that $Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) = pb_0$ but

$$Tr_{K/\mathbb{Q}}(\alpha(1-\zeta)) \in p\mathbb{Z}$$

by Lemma 3.5 and thus $b_0 \in \mathbb{Z}$. Multiplying by the integral element ζ^{p-1}, we arrive at

$$(\alpha - b_0)\zeta^{p-1} = b_1 + \ldots + b_{p-2}\zeta^{p-3}$$

Repeating the argument, we find that $b_1 \in \mathbb{Z}$ and so $b_0, \ldots, b_{p-2} \in \mathbb{Z}$ by induction. □

4. Factorization into Prime Ideals in Dedekind Domains

Definition 4.1. An integral domain is a *discrete valuation ring* if it is Noetherian, integrally closed, and has exactly one non-zero prime ideal.

Definition 4.2. An integral domain is called a *Dedekind domain* if it is Noetherian, integrally closed and every non-zero prime ideal is maximal.

The first definition appears to be a "localization" of the second – indeed, it is clear that a local ring is a Dedekind domain if and only if it is a discrete valuation ring. The localization connection extends further but first we need the following result.

Proposition 4.3. *If B is a Dedekind domain, then $S^{-1}B$ is also a Dedekind domain.*

Proof. All Prime ideals are Maximal: Under the correspondence between prime ideals in B such that $\mathfrak{p} \cap S = \emptyset$ and prime ideals in $S^{-1}B$, $\mathfrak{p}_1 \subset \mathfrak{p}_2$ in $S^{-1}B$ implies that $\mathfrak{p}_1 \subset \mathfrak{p}_2$ in B. Therefore, if there are non-maximal prime ideals in $S^{-1}B$, then there are non-maximal prime ideals in B. Thus,

$$\text{Krull Dimension of B is 1} \implies \text{Krull Dimension of } S^{-1}B \text{ is 1}$$

The proofs of the facts that

$$\text{B is Noetherian} \implies S^{-1}B \text{ is Noetherian}$$

and

$$\text{B is integrally closed} \implies S^{-1}B \text{ is integrally closed}$$

are omitted. □

Proposition 4.4. *Localization Connection: A Noetherian integral domain, B, is a Dedekind domain if and only if $B_{\mathfrak{p}}$ is a discrete valuation ring for every non-zero prime ideal in B.*

Proof. $\implies$ $B_{\mathfrak{p}}$ is a local ring and Proposition 4.3 implies that it is a discrete valuation ring.

$\impliedby$ Given x, an element in the field of fractions of B that is integral over B, consider the ideal

$$\mathfrak{a} := \{y \in B \ : \ y \cdot x \in B\}$$

We will show that this ideal is the whole ring and thus contains the identity. For every non-zero prime ideal of B, $x \in B_{\mathfrak{p}}$ since $B_{\mathfrak{p}}$ is integrally closed. Thus, there exists s in $B - \mathfrak{p}$ such that $x \cdot s \in B$. Each s belongs to $\mathfrak{a}$ and thus $\mathfrak{a}$ is not contained in any prime ideal. This implies that $\mathfrak{a} = B$. Therefore, $1 \in \mathfrak{a}$ and so x is integral. It remains to show that every-nonzero prime ideal of B is maximal. Suppose not. Consider $\mathfrak{p} \subsetneq \mathfrak{m}$ in B. Under the correspondence between prime ideals in B and the prime ideals in $B_{\mathfrak{m}}$, $\mathfrak{p}_{\mathfrak{m}} \subsetneq \mathfrak{m}_{\mathfrak{m}}$. But, $B_{\mathfrak{m}}$ is a discrete valuation ring and so we have arrived at a contradiction. □

Proposition 4.5. *Every ideal in a Dedekind domain can be factored uniquely (up to units) into a product of prime ideals.*

The proof of this proposition will rely primarily on the Chinese Remainder Theorem and the fact that $B_{\mathfrak{p}}$ is a discrete valuation ring. However, we need a couple of lemmas first.

Lemma 4.6. *Let R be a Noetherian ring. Then, each ideal $\mathfrak{b}$ in R contains a product of prime ideals.*

Proof. Consider the set of all ideals not containing a product of prime ideals. Since R is Noetherian, this set has a maximal element, say $\mathfrak{b}$. Clearly, $\mathfrak{b}$ is not prime. Therefore, there exist $x, y \in R$ such that $x \cdot y \in \mathfrak{b}$ but $x, y \notin \mathfrak{b}$. Then, $\mathfrak{b} + (x)$ and $\mathfrak{b} + (y)$ both strictly contain $\mathfrak{b}$ but their product is contained in $\mathfrak{b}$. Since $\mathfrak{b} + (x)$ and $\mathfrak{b} + (y)$ contain a product of prime ideals, it follows that $\mathfrak{b}$ does as well. □

Lemma 4.7. *Let R be a commutative ring. Then, if $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime ideals of R, then $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are also relatively prime for all $n,m \in \mathbb{N}$.*

Proof. If $\mathfrak{a}^r$ and $\mathfrak{b}^s$ are not relatively prime, $\mathfrak{a}^r + \mathfrak{b}^s \neq 1$. Therefore, $\mathfrak{a}^r + \mathfrak{b}^s$ is contained in a prime ideal $\mathfrak{m}$. But, $\mathfrak{a}^r \subset \mathfrak{m}$ and $\mathfrak{b}^s \subset \mathfrak{m}$ imply that $\mathfrak{a} \subset \mathfrak{m}$ and $\mathfrak{b} \subset \mathfrak{m}$ since $\mathfrak{m}$ is prime – a contradiction of $\mathfrak{a}$ and $\mathfrak{b}$ being relatively prime. □

Lemma 4.8. *Let $\mathfrak{p}$ be a maximal ideal in a ring A and let $\mathfrak{q}$ be the corresponding ideal in $A_{\mathfrak{p}}$. Then, the map $\phi : A/\mathfrak{p}^n \to A_{\mathfrak{p}}/\mathfrak{q}^n : a + \mathfrak{p}^n \mapsto a + \mathfrak{q}^n$ is an isomorphism.*

Proof. Injectivity: Let $S = A - \mathfrak{p}$. $S^{-1}\mathfrak{p}^m = \mathfrak{q}^m$ and so

$$\phi \text{ injective} \iff \mathfrak{p}^n = (S^{-1}\mathfrak{p}^n) \cap A$$

If $a = \frac{b}{s}$ belongs to $(S^{-1}\mathfrak{p}^n) \cap A$, then $a \cdot s = 0$ in $A/\mathfrak{p}^n$. Since $\mathfrak{p}$ is the only maximal ideal containing $\mathfrak{p}^n$, A/$\mathfrak{p}^n$ is a local ring. Thus,

$$s + \mathfrak{p}^n \notin \mathfrak{p}/\mathfrak{p}^n \implies s + \mathfrak{p}^n \text{ is a unit}$$

So, $a \cdot s = 0$ in $A/\mathfrak{p}^n$. This implies that a belongs to $\mathfrak{p}^n$. Therefore, ϕ is injective.

Surjectivity: Let $\frac{a}{s} \in A_\mathfrak{p}$. Since $\mathfrak{p}$ is maximal

$$s \notin \mathfrak{p} \implies (s) + \mathfrak{p} = 1$$

This means that (s) and $\mathfrak{p}^n$ are relatively prime and so

$$\exists b \in A, r \in \mathfrak{p}^n : bs + r = 1$$

Therefore $\phi(b) = s^{-1}$ in $A_\mathfrak{p}/\mathfrak{q}^m$ and so $\phi(ab) = \frac{a}{s}$.

□

We are now prepared to prove that Dedekind domains have unique prime factorizations.

Proof. Existence: Let A be a Dedekind domain. By Lemma 4.6, a non-zero ideal $\mathfrak{a}$ contains a product of prime ideals, say $\mathfrak{c} = \prod \mathfrak{p}_i^{r_i}$. We now consider A/$\mathfrak{c}$. By Chinese Remainder Therorem,

$$A/\mathfrak{c} \cong A/\mathfrak{p}_1^{r_1} \times \ldots \times A/\mathfrak{p}_n^{r_n}$$

Furthermore, by Lemma 4.8,

$$A/\mathfrak{p}_1^{r_1} \times \ldots \times A/\mathfrak{p}_n^{r_n} \cong A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \ldots \times A_{\mathfrak{p}_n}/\mathfrak{q}_n^{r_n}, \text{ where } \mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$$

Since each of the $A_{\mathfrak{p}_i}$ is a discrete valuation ring,

$$\mathfrak{a}/\mathfrak{c} \cong \mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \ldots \times \mathfrak{q}_n^{s_n}/\mathfrak{q}_n^{r_n}, s_i \leq r_i$$

This is also the image of $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$. Thus, $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$ in $A/\mathfrak{c}$. But, $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$ and $\mathfrak{a}$ both contain $\mathfrak{c}$. These results and the correspondence between ideals of A that contain $\mathfrak{c}$ and ideals of $A/\mathfrak{c}$ imply that $\mathfrak{a}$ and $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$ are equal.

Uniqueness: Let ${\mathfrak{p}_1}^{r_1} \ldots {\mathfrak{p}_n}^{r_n} = \mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$ – common primes may be assumed by adding in zero-powers. Since, as a discrete valuation ring, $A_{\mathfrak{p}_i}$ is principal ideal domain and has only one non-zero prime ideal, we have that

$$\mathfrak{q}_i^{r_i} = \mathfrak{a} A_{\mathfrak{p}_i} = \mathfrak{q}_i^{s_i}$$

which implies that $r_i = s_i, \ \forall i \in (1, .., n)$. □

4.1. **Corollaries of Dedekind Prime Factorization Theorem.**

Corollary 4.9. *Let $\mathfrak{a} \subset \mathfrak{b}$ be ideals in a Dedekind domain A. Then, there exists f in A such that $\mathfrak{b} = \mathfrak{a} + (f)$.*

Proof. Let $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdot \ldots \cdot \mathfrak{p}_n^{r_n}$ and $\mathfrak{b} = \mathfrak{p}_1^{s_1} \cdot \ldots \cdot \mathfrak{p}_n^{s_n}$ be the prime decompositions for $\mathfrak{a}$ and $\mathfrak{b}$ respectively. Since $\mathfrak{a}$ is contained in $\mathfrak{b}$, the s_i must be less than or equal to the r_i. Now, $\forall i \in (1, ..., n)$, choose x_i such that $x_i \in \mathfrak{p_i}^{s_i}$ but $x_i \notin p_i^{s_i+1}$. Then, Chinese Remainder Theorem implies that there exists f in A such that

$$f \equiv x_i \bmod p_i^{r_i}$$

It follows from localizing at each $\mathfrak{p}$ and checking the ideals generated that $(f) + \mathfrak{a} = \mathfrak{b}$. □

Corollary 4.10. *Let $\mathfrak{a}$ be an ideal in a Dedekind domain A, then if $a \in \mathfrak{a}$ then $\exists f \in A$ such that $\mathfrak{a} = (a, f)$.*

Proof. Immediate conclusion of Corollary 4.9 by taking (a) $\subset \mathfrak{a}$. □

Proposition 4.11. *Let $\mathfrak{a} \subset A$ where $\mathfrak{a}$ is an ideal inside a Dedekind domain A. Then, for every prime ideal $\mathfrak{p} \in spec(A)$, there exists g in A such that $g \bmod \mathfrak{p} \neq 0$ and $\mathfrak{a}A_g$, the image of $\mathfrak{a}$ in the localization of A at $1, g, g^2, ...,$ is principal.*

Proof. Since $A_\mathfrak{p}$ is a discrete valuation ring, $\mathfrak{a} \cdot A_\mathfrak{p}$ is principal and thus,

$$\mathfrak{a} \cdot A_\mathfrak{p} = (\frac{\pi}{f}) \tag{4.12}$$

for some $\pi \in \mathfrak{a}$ and $f \in A - \mathfrak{p}$. Furthermore, Corollary 4.10 implies that $\mathfrak{a} = (\pi, \phi)$ for some $\phi \in \mathfrak{a}$. From 4.12, we have that

$$\frac{\pi}{f}\frac{s}{t} = \frac{\phi}{1}, \text{ for some } s \in A \text{ and } t \in A - \mathfrak{p} \tag{4.13}$$

Since $\mathfrak{p}$ is prime, $ft \bmod \mathfrak{p} \neq 0$. We claim that

$$\mathfrak{a} \cdot A_{(ft)} = (\frac{\pi}{ft}), \text{ where } A_{(ft)} \text{ is the localization of } A \text{ at } \{1, ft, (ft)^2, \ldots\}$$

Since $\mathfrak{a} = (\pi, \phi)$, it is sufficient to show that

$$\frac{\pi}{1}, \frac{\phi}{1} \in (\frac{\pi}{ft})$$

The first inclusion is clear and the second is true since

$$(\frac{\pi}{ft})(\frac{s}{1}) = \frac{\phi}{1}, \text{ by 4.1}$$

□

5. Discriminant

Definition 5.1. Discriminant: Let K and L be fields such that L is a finite extension of K. The map from $L \times L \to K$ given by $(a, b) \mapsto \mathrm{Tr}_{L/K}(ab)$ is a symmetric bilinear form on L considered as a K-vector space. The *discriminant* of L over K, $\mathrm{Disc}(L/K)$, is the determinant of this form for a given integral basis.

The definition can be further generalized. Let $A \subset B$ be rings and let B be a free A-module of rank n, then $\text{Disc}(\beta_1, ..., \beta_n) = \det(\text{Tr}_{B/A}(\beta_i\beta_j))$ where $(\beta_1, \ldots, \beta_n)$ are elements of B.

Example 5.2. Discriminant of Quadratic Fields.

Case $m \equiv 2, 3 \mod 4$:

$$\text{Disc}(\mathbb{Q}[\sqrt{m}]/\mathbb{Q}) = \text{Disc}(1, \sqrt{m}) = \det \begin{bmatrix} \sqrt{m} & -\sqrt{m} \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} \sqrt{m} & 1 \\ -\sqrt{m} & 1 \end{bmatrix} = 4m$$

Case $m \equiv 1 \mod 4$:

$$Disc(\mathbb{Q}[\sqrt{m}]/\mathbb{Q}) = \text{Disc}(1, \frac{1+\sqrt{m}}{2}) = \det \begin{bmatrix} \frac{1+\sqrt{m}}{2} & \frac{1+\sqrt{m}}{2} \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} \frac{1+\sqrt{m}}{2} & 1 \\ \frac{1+\sqrt{m}}{2} & 1 \end{bmatrix} = m$$

Thus, if $D = Disc(\mathbb{Q}[\sqrt{m}]/\mathbb{Q})$, the integral basis for $\mathbb{Q}[\sqrt{m}]$ is $(1, \frac{D+\sqrt{D}}{2})$.

Example 5.3. Discriminant of Prime Cyclotomic Fields: From Proposition 3.6, $(1, \zeta_p, \ldots, \zeta_p^{p-2})$ is an integral basis for $\mathbb{Q}[\zeta_p]$. Then,

$$Disc(\mathbb{Q}[\zeta_p]/\mathbb{Q}) = Disc((1, \zeta_p, \ldots, \zeta_p^{p-2})) = \det(CC^T) = \det(C)^2,\ C = \begin{bmatrix} 1 & \zeta_p & \ldots & \zeta_p^{p-2} \\ 1 & \zeta_p^2 & \ldots & \zeta_p^{2(p-2)} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta_p^{p-1} & \ldots & \zeta_p^{(p-1)(p-2)} \end{bmatrix}$$

Let $\zeta = \zeta_p$. The Vandermonde determinant formula implies that

$$\begin{aligned} \text{Disc}((1, \zeta, \ldots, \zeta^{p-2})) &= \prod_{1 \le i < j \le (p-1)} (\zeta_i - \zeta_j)^2, \text{ where } \zeta_i = \sigma_i(\zeta) \\ &= (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{i=1}^{p-1} [\prod_{i \neq j} (\zeta_i - \zeta_j)] \\ &= (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{i=1}^{p-1} (-\frac{p\zeta^{p-j}}{1-\zeta_j}) \\ &= (-1)^{\frac{(p-1)(p-2)}{2}} (-p)^{p-1} \frac{\prod_{i=1}^{p-1} \zeta^{p-j}}{\prod_{i=1}^{p-1} (1-\zeta^j)} \\ &= (-1)^{\frac{(p-1)(p-2)}{2}} (-1)^{p-1} \frac{-p^{p-1}}{p} \\ &= (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2} \\ &= (-1)^{\frac{p-1}{2}} p^{p-2}, \text{ since p is odd} \end{aligned}$$

5.1. **Ramification definition.**

Definition 5.4. Let L be an extension of K, $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ and $\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_n^{e_n}$ be its prime decomposition, then we say that:

$\mathfrak{p}$ is split if $e_i = 1, \forall i \in (1, \ldots, n)$;

$\mathfrak{p}$ is inert if $\mathfrak{p}$ remains prime in L

$\mathfrak{p}$ is ramified if $e_j \geq 2$ for some j $\in (1, \ldots, n)$

Theorem 5.5. *Let L be a finite extension of a number field K and let A be a Dedekind Domain with K as its field of fractions. Furthermore, let B be the integral closure of A and assume further that B is a free A-module. Then, a prime ideal $\mathfrak{p} \subset A$ ramifies in B if and only if $\mathfrak{p}$ divides Disc(B/A).*

5.2. **Ramification lemmas.** The theorem will be a natural conclusion of the following lemmas.

Lemma 5.6. *Let A be a ring, α an ideal of A, and M an A-module. Then $M/\alpha M \cong (A/\alpha) \otimes_A M$.*

Proof. We have the exact sequence:

$$0 \to \alpha \to A \to A/\alpha \to 0$$

Tensoring with M gives another exact sequence:

$$\alpha \otimes_A M \to M \to A/\alpha \otimes_A M \to 0$$

The image of $\alpha \otimes_A M$ in M are sums of elements of the form $a_i \cdot m_i$ where $a_i \in \alpha$ and $m_i \in M$. This implies that $M/\alpha M \cong A/\alpha \otimes_A M$. □

Lemma 5.7. *Let A be a ring and let $B \supset A$ be an A-algebra of finite rank with basis $(e_1, ..., e_n)$ as an A-module. Then, for any ideal $\mathfrak{a} \subset A$, $(\bar{e_1}, ..., \bar{e_n})$ is a basis for the $A/\mathfrak{a}$-module $B/\mathfrak{a}B$.*

Proof. The map $(a_1, ..., a_n) \mapsto \sum_{i=1}^n a_i e_i$ defines an isomorphism from A^n to B. By tensoring with $A/\mathfrak{a}$,

$$(\bar{a_1}, ..., \bar{a_n}) \mapsto \sum_{i=1}^{n} a_i \bar{e_i}$$

defines an isomorphism from $(A/\mathfrak{a})^n$ to $B/\alpha B$. Therefore, $(\bar{e_1}, ..., \bar{e_n})$ is a basis for the $A/\mathfrak{a}$-module $B/\mathfrak{a}B$. □

From the definitions, it is also clear that $Disc(e_1, ..., e_n) \bmod \mathfrak{a} = Disc(\bar{e_1}, ...\bar{e_n})$.

Lemma 5.8. *Let A be a ring and let $B_1, ..., B_m$ be rings that contain A and are free of finite rank over A. Then, $Disc((\prod_{i=1}^m B_i)/A) = \prod_{i=1}^m Disc(B_i/A)$.*

Proof. Let $(e_{i1}, ..., e_{in})$ be a basis for the B_i, then taking $\cup_i (e_{i1}, ..., e_{in})$ gives a basis for $\prod_{i=1}^n B_i$. The result then follows by block determinant rule. □

Lemma 5.9. *Let k be a perfect field and B be free k-algebra of finite rank. Then the radical of B is $0 \Leftrightarrow Disc(B/k) \neq 0$.*

Proof. $\Leftarrow$ Let $b \neq 0 \in B$ be nilpotent. Then, choose a basis $(e_1, ..., e_n)$ for B/k such that $e_1 = b$. The maps

$$x \mapsto be_i x$$

are linear and therefore can be described by matrices A_i. Furthermore,

$$b \text{ is nilpotent } \implies \text{ each map is nilpotent } \implies A_i \text{ are nilpotent}$$

Therefore,

$$\mathrm{Tr}(A_i) = 0 \implies Tr(e_1 e_j) = 0, j \in (1, \ldots, n) \implies \det(\mathrm{Tr}(e_i, e_j)) = 0$$

since the rows must be linearly dependent.

$\Rightarrow$ Let $\mathfrak{p}$ be a prime ideal of B. $B/\mathfrak{p}$ is an integral domain and algebraic over k. $B/\mathfrak{p}$ is also field. We show this by proving that map

$$k[\bar{\beta}] \to k[\bar{\beta}] : x \mapsto \bar{\beta} x$$

is an isomorphism. Since $\bar{\beta}$ is non-zero in $B/\mathfrak{p}$, the map is linear and injective (injectivity follows from $B/\mathfrak{p}$ being an integral domain). Since $B/\mathfrak{p}$ is a finite-dimensional k-vector space, the map is also surjective. Therefore, β has an inverse.

If $\mathfrak{p}_1, ..., \mathfrak{p}_n$ are prime ideals of B, then they are also maximal. This implies that each pair is relatively prime. Furthermore,

$$[B : k] \geq [B/ \cap_i \mathfrak{p}_i : k] = [\prod_{i=1}^{n} B/\mathfrak{p}_i : k] = \sum_{i=1}^{n} [B/\mathfrak{p}_i : k] \geq n$$

Since $[B : k]$ is finite, it follows that there are finitely many prime ideals, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$. Taking $g = n$ results in $B = \prod_{i=1}^{n} B/\mathfrak{p}_i$. Each $B/\mathfrak{p}_i$ is a finite extension. Each is also separable since k is perfect. L is a finite and separable extension of K while implies that $L = K[\alpha]$ for some primitive element α. Then, $(1, \alpha, \ldots, \alpha^{n-1})$ forms a basis for L over K. Furthermore,

$$\mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i \neq j} (\alpha_{(i)} - \alpha_{(j)})^2 \neq 0$$

where $\alpha_{(j)}$ are the conjugates of α. The conjugates are all distinct since L is a separable extension. Therefore,

$$\mathrm{Disc}(B/k) = \mathrm{Disc}((\prod_{i=1}^{n} B/\mathfrak{p}_i)/k) = \prod_{i=1}^{n} (\mathrm{Disc}((B/\mathfrak{p}_i)/k) \neq 0$$

□

Theorem 5.5 follows directly from these lemmas:

Proof. Disc(B/A) mod $\mathfrak{p}$ = Disc$((B/\mathfrak{p}B)/(A/\mathfrak{p}))$. But,

$$B/\mathfrak{p}B = B/\prod \mathfrak{q}_i^{s_i} \cong \prod B/\mathfrak{q}_i^{s_i}$$

for some prime ideals $\mathfrak{q}_i \in B$. Thus,

$$rad(B/\mathfrak{p}B) = 0 \iff rad(B/\mathfrak{q}_i^{s_i}) = 0,\ i \in (1, .., n) \iff s_1 = \ldots = s_n = 1$$

Since

$$\text{Disc}((B/\mathfrak{p}B)/(a/\mathfrak{p})) = 0 \iff \mathfrak{p} \text{ divides the Disc(B/A)}$$

it follows that

$$\mathfrak{p} \text{ ramifies} \iff \mathfrak{p} \text{ divides Disc(B/A)}$$

□

Example 5.10. We do the simple verification of the ramification result for the Gaussian Integers. First, $\mathbb{Z}[i]$ is a PID and $\text{Disc}(\mathbb{Q}[i]/\mathbb{Q}) = 4$ by 3.2. We therefore expect that only 2 ramifies.

Case $p \equiv 3 \pmod 4$:

p remains inert. Since if $\alpha\beta = p$, then $\text{Nm}(\alpha) = p$ but there are no solutions to $a^2 + b^2 = p$ if $p \equiv 3 \pmod 4$.

Case $p \equiv 1 \pmod 4$:

p splits in $\mathbb{Z}[i] \iff X^2 + 1$ reduces in $\mathbb{F}_p \iff \mathbb{F}^\times$ contains an element of order $4 \iff 4 \mid p - 1$. Thus, p splits if and only if $p \equiv 1 \pmod 4$.

Case $p = 2$.

$2 = i(1 - i)^2$. Therefore, it is the only prime to ramify as the theorem predicts.

5.3. **Irreducible polynomials factoring method.**

Proposition 5.11. *Let L be a finite separable extension of K, $A = \mathcal{O}_K$ be a Dedekind domain and B be the ring of integers for L. Suppose that $B = A[\alpha]$ and let $f(x)$ be the minimal polynomial for α. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ and $\prod g_i(x)^{e_i} \equiv f(x) \pmod{\mathfrak{p}}$ is the decomposition into irreducible polynomials modulo $\mathfrak{p}$, then*

$$\mathfrak{p}B = \prod(\mathfrak{p}, g_i(\alpha))^{e_i}$$

is the decomposition of $\mathfrak{p}B$ into prime ideals. Furthermore,

$$B/(\mathfrak{p}, g_i(\alpha))^{e_i} \cong (A/\mathfrak{p})[x]/\bar{g}_i(x)$$

and thus the residue class degree f_i is equal to the degree of the polynomial g_i.

Proof. By assumption, the mapping $x \mapsto \alpha$ defines an isomorphism between

$$A/f(x) \cong B$$

and dividing out by $\mathfrak{p}$ we arrive at:

$$(A/\mathfrak{p})[x]/\prod \bar{g}_i(x)^{e_i} \cong B/\mathfrak{p}B \tag{5.12}$$

By Chinese Remainder theorem, 5.12 becomes:

$$(A/\mathfrak{p})[x]/\prod \bar{g}_1(x)^{e_1} \times \ldots \times (A/\mathfrak{p})[x]/\prod \bar{g}_n(x)^{e_n} \cong B/\mathfrak{p}B$$

Therefore, the ring $(A/\mathfrak{p})[x]/\prod \bar{g}_i(x)^{e_i}$ has maximal ideals $\bar{g}_i$. In addition, $\prod \bar{g_i}^{e_i} = 0$ but $\prod \bar{g_i}^{e_i'} \neq 0$ for any $e_i' < e_i$. Finally, $(\mathfrak{p}, g_i(\alpha))$ are the only prime ideals that contain $\mathfrak{p}B$. Thus,

$$\prod(\mathfrak{p}, g_i(\alpha))^{d_i} = \mathfrak{p}B$$

is the prime decomposition of $\mathfrak{p}B$ for some d_i.

$$\mathfrak{p}B \supset \prod (\mathfrak{p}, g_i(\alpha))^{e_i}$$

but

$$\mathfrak{p}B \not\supset \prod (\mathfrak{p}, g_i(\alpha))^{e_i'} \; \forall \; e_i' < e_i$$

Thus, $d_i = e_i \; \forall \; i \in (1, \ldots, n)$.

□

Example 5.13. Totally Ramified primes in cyclotomic fields:

Let $K = \mathbb{Q}[\zeta_p]$ and let p be a prime in $\mathbb{Z}$. We find the prime decomposition of $p\mathbb{Z}[\zeta_p]$. Employing the previous proposition, we divide both sides of the isomorphism

$$\mathbb{Z}[x]/\Phi[x] \cong \mathcal{O}_K \tag{5.14}$$

by p. 5.14 becomes:

$$\mathbb{F}_p[x]/\overline{\Phi(x)} \cong \mathcal{O}_K/p\mathcal{O}_K$$

But,

$$\overline{\Phi(x)} = \bar{x}^{p-1} + \ldots + 1 = \frac{\bar{x}^p - 1}{\bar{x} - 1} = \frac{(\bar{x} - 1)^p}{\bar{x} - 1} = (x - 1)^p$$

Thus, the decomposition is

$$p\mathcal{O}_K = (p, (1 - \zeta_p))^{p-1}$$

5.4. **Ramification Index Theorem.**

Lemma 5.15. *Let L be a finite extension of K, B be the ring of integers for L, and A be the ring of integers for K. Furthermore, let A be a Dedekind domain and $\mathfrak{p}$ be a prime ideal in A. Then, $B/\mathfrak{p}B \cong B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$.*

Proof. The map $B/\mathfrak{p}B \hookrightarrow B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ is injective since $\mathfrak{p}B_\mathfrak{p} \cap B = \mathfrak{p}B$.

Surjectivity: Let $\frac{a}{c}$ $(a \in B, c \in A - \mathfrak{p})$ be a representative for an arbitrary residue class in $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$. From the injection

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{p}B$$

we have that c^{-1} exists in $B/\mathfrak{p}B$. Thus, the element ac^{-1} is well-defined in $B/\mathfrak{p}B$ and the map is surjective. □

Proposition 5.16. *Let m be the degree of L over K and $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ be the primes ideals dividing $\mathfrak{p}$. Then, $\sum_{i=1}^{g} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}] = m$. If L is also Galois over K, then all the ramification numbers are equal and all the residue class degrees are equal and thus $m = efg$.*

Proof. First,

$$B/\mathfrak{p}B = B/\prod_{i=1}^{g} \mathfrak{q}_i^{e_i} \cong \prod_{i=1}^{g} B/\mathfrak{q}_i^{e_i}$$

by Chinese Remainder Theorem. Therefore, to prove that $\sum_{i=1}^{g} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}]$, it is sufficient to show that $[B/\mathfrak{q}_i^{e_i} : A/\mathfrak{p}] = e_i f_i$. To show this, we consider the chain of $B/\mathfrak{q}_i$-modules

$$B \supset \mathfrak{q}_i \supset \mathfrak{q}_i^2 \supset \ldots \supset \mathfrak{q}_i^{e_i}$$

Since no ideals reside between $\mathfrak{q}_i^m$ and $\mathfrak{q}_i^{m+1}$, $\mathfrak{q}^{m+1}/\mathfrak{q}^m$ has degree one as a $B/\mathfrak{q}_i$-module. We can also see this fact by noting the isomorphisms

$$B/\mathfrak{q} \cong B_{\mathfrak{q}}/\mathfrak{q}_{\mathfrak{q}}, \text{ where } \mathfrak{q}_{\mathfrak{q}} = \mathfrak{q} \cdot B_{\mathfrak{q}}$$
$$\mathfrak{q}^m/\mathfrak{q}^{m+1} \cong (\mathfrak{q}_{\mathfrak{q}})^m/(\mathfrak{q}_{\mathfrak{q}})^{m+1} \cong B_{\mathfrak{q}}/\mathfrak{q}_{\mathfrak{q}}$$

Furthermore, $\mathfrak{q}_i^{m_i}/\mathfrak{q}_i^{m_i+1}$ has degree f_i as a $A/\mathfrak{p}$ module. Taking the chain all together, i.e. e_i-times, we find that $[B/\mathfrak{q}_i^{e_i} : A/\mathfrak{p}] = e_i f_i$.

To prove that $[B/\mathfrak{p}B : A/\mathfrak{p}] = m$, we first show the result in the case where B is free A-module and then reduce the general case to the free case by localization at $\mathfrak{p}$.

If B is a free A-module, there is an isomorphism

$$A^m \to B \tag{5.17}$$

When tensored with $A/\mathfrak{p}$, 5.17 gives a new isomorphism

$$(A/\mathfrak{p})^m \to B/\mathfrak{p}B$$

and so $[B/\mathfrak{p}B : A/\mathfrak{p}] = m$.

If B is not a free A-module, then we can localize at $\mathfrak{p}$ and thereby get the rings $B_{\mathfrak{p}}$ and $A_{\mathfrak{p}}$. $A_{\mathfrak{p}}$ is a Dedekind domain and, since $\mathfrak{p} \cdot A_{\mathfrak{p}}$ is principal, it is a discrete valuation ring. Therefore, we have that $A_{\mathfrak{p}}$ is a PID. Since $B_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$, by the PID case already considered, we have that $[B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}B : A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}] = m$.

If L/K is a Galois extension, then $\mathrm{Gal}(L/K)$ acts on B. In particular, $\sigma(\mathfrak{q})$ is also a prime ideal in B. If $\mathfrak{q}$ divides $\mathfrak{p}$, then $\sigma(\mathfrak{q})$ also divides $\mathfrak{p}$ since $\mathfrak{p}$ is in the fixed field of σ. This implies that

$$e(\mathfrak{q}/\mathfrak{p}) = e(\sigma(\mathfrak{q})/\mathfrak{p})$$
$$f(\mathfrak{q}/\mathfrak{p}) = f(\sigma(\mathfrak{q})/\mathfrak{p})$$

Thus, it only remains to show that Gal(L/K) acts transitively on the primes sitting above any given $\mathfrak{p}$ in A, i.e. $\forall \mathfrak{q}_i, \mathfrak{q}_j \ \exists \sigma : \sigma(\mathfrak{q}_i) = \mathfrak{q}_j$.

Suppose there exist prime ideals $\mathfrak{q}$ and $\mathfrak{q}'$ in L such that for all σ in $\mathrm{Gal}(L/K)$, $\sigma(\mathfrak{q})$ is not equal to $\mathfrak{q}'$. Then, by Chinese Remainder theorem, there exists $\beta \in B$ such that β belongs to $\mathfrak{q}'$ but β does not belong to $\sigma(\mathfrak{q})$ for all σ in $\mathrm{Gal}(L/K)$. Then, taking the norm of β we arrive at

$$Nm_{L/K}(\beta) = \prod \sigma(\beta)$$

Thus, the $Nm(\beta)$ belongs to $\mathfrak{q}' \cap A$ which implies that $Nm(\beta) \in \mathfrak{p}$. However,

$$Nm(\beta) \in \mathfrak{p} \implies Nm(\beta) \in \mathfrak{q}$$

which is a contradiction of the primality of $\mathfrak{q}$ since $\sigma(\beta) \notin \mathfrak{q}\ \forall \sigma \in \mathrm{Gal(L/K)}$. □

6. Fractional Ideals, Ideal Class Group, Decomposition group, Galois groups of tower extensions, Frobenius element

Definition 6.1. Let A be a Dedekind domain and K be its field of fractions. Then a *fractional ideal* $\mathfrak{a}$ is a A-submodule of K for which there exists d in K such that $d\mathfrak{a} \subseteq A$, i.e. elements with a common denominator. If $\mathfrak{a} \subset A$, then $\mathfrak{a}$ is an *integral ideal*. Furthermore, it is clear that a single element, b, in K defines a fractional ideal (b). These are called *principal fractional ideals*.

Proposition 6.2. *Let A be a Dedekind domain. Then, Id(A), the set of fractional ideals forms a group. Indeed, it is a free abelian group on the set of prime ideals of A.*

Proof. The group operation is defined to be composition. It is clear from the algebraic structure on A and K that composition on $\mathrm{Id}(A)$ is commutative and associative. Furthermore, the identity of $\mathrm{Id}(A)$ is A itself.

We must also ensure that there is a compositional inverse for $\mathfrak{a}$. Taking $d \in A$ such that $d\mathfrak{a}$ is integral, we have that $d\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_n^{e_n}$ since A is a Dedekind domain. Choose $a \in d\mathfrak{a}$, then

$$(a) = \mathfrak{p}_1^{s_1} \cdot \ldots \cdot \mathfrak{p}_n^{s_n},\ s_i \geq e_i$$

Thus, if $\mathfrak{a}^* := \mathfrak{p}_1^{s_1 - e_1} \cdot \ldots \cdot \mathfrak{p}_n^{s_n - e_n}$, then $d\mathfrak{a}\mathfrak{a}^* = (a)$ and so $d^{-1}a^{-1}\mathfrak{a}^*$ is an inverse for $\mathfrak{a}$.

Moreover, $\mathrm{Id}(A)$ is free on the prime ideals of A. As above,

$$d\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_n^{e_n}$$

for some prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. But, (d) has a prime decomposition as well

$$(d) = \mathfrak{p}_1^{f_1} \cdot \ldots \cdot \mathfrak{p}_n^{f_n}$$

and thus $\mathfrak{a}$ is uniquely defined by its decomposition

$$\mathfrak{a} = \mathfrak{p}_1^{e_1 - f_1} \cdot \ldots \cdot \mathfrak{p}_n^{e_n - f_n}$$

□

Definition 6.3. We define the *ideal class group* of A to be the group $Id(A)/P(A)$ where $\mathrm{Id}(A)$ is the group of fractional ideals and $\mathrm{P}(A)$ the subgroup of principal fractional ideals. The *class number* of A is defined to be the order of the ideal class group should the group be finite.

Definition 6.4. Decomposition Group: Let L/K be a Galois extension, let B be the ring of integers for L, let A be the ring of integers for K and let $\mathfrak{q}$ be a prime in B sitting above $\mathfrak{p}$ in A. Then, the *decomposition group* of $\mathfrak{q}$, $D_\mathfrak{q}$, is define to be:

$$D_\mathfrak{q} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

The size of the orbit for each $\mathfrak{q}$ is g, where g is the number of primes $\mathfrak{q}_i$ lying above $\mathfrak{p}$, and thus, by the orbit stabilizer theorem, we have that

$$g = [Gal(L/K) : D] = |Gal(L/K)|/|D|$$

which implies that

$$|D| = n/g = ef$$

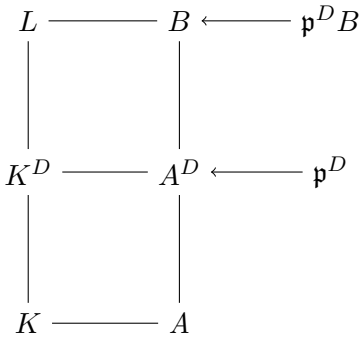
by the Fundamental theorem of Galois theory.

σ maps B isomorphically to itself, i.e. $\sigma(B) = B$. Therefore, if $\sigma \in D_{\mathfrak{q}}$, we have an induced mapping

$$\sigma \mapsto \bar{\sigma} : D \to Gal((B/\mathfrak{q})(A/\mathfrak{p}))$$

The *inertial group* is the subgroup of D such that its image under σ is the identity on $B/\mathfrak{q}$, i.e. $I_D = (\sigma \in D | \bar{\sigma} = Id)$. We will see that this map is surjective but to do so we need a lemma.

Lemma 6.5. *Let K^D be the fixed field of D, let A^D be its ring of integers, and let $\mathfrak{p}^D = \mathfrak{q} \cap A^D$, i.e we have the following diagram:*



If $\mathfrak{p}_D B = \mathfrak{q}^{e'}$ (only one prime factor since $\sigma(\mathfrak{q}) = \mathfrak{q}$) and if $f' = [B/\mathfrak{q} : A_D/\mathfrak{p}_D]$, then $e' = e$ and $f' = f$. Furthermore,

$$A/\mathfrak{p} \cong A_D/\mathfrak{p}_D$$

Proof. First, by the fundamental theorem of Galois theory and the ramification index theorem

$$e'f' = [L; K_D] = |D|$$

The orbit stabilizer theorem implies that $|D| = ef$ and thus

$$ef = e'f'$$

Since $A/\mathfrak{p} \subset A_D/\mathfrak{p}_D \subset B/\mathfrak{q}$, we have that $f' \leq f$. Furthermore, $e' \leq e$ since

$$\mathfrak{p}A_D \subset \mathfrak{p}_D \implies \mathfrak{p}_D \text{ divides } \mathfrak{p}A_D \implies \mathfrak{p}_D B \text{ divides } \mathfrak{p}B$$

Finally,

$$f' \leq f,\ e' \leq e, \text{ and } e'f' = ef \implies e = e' \text{ and } f = f'$$

Thus, $[B/\mathfrak{q} : A/\mathfrak{p}] = [B/\mathfrak{q} : A_D/\mathfrak{p}_D]$. Since $A/\mathfrak{p}$ is a subfield of $A_D/\mathfrak{p}_D$, we have that

$$A/\mathfrak{p} \cong A_D/\mathfrak{p}_D$$

□

Proposition 6.6. *Let L/K be a Galois extension, A be the ring of integers for K and let B be the ring of integers for L. If $((B/\mathfrak{q})/(A/\mathfrak{p}))$ is separable, then the map $\sigma \mapsto \bar{\sigma}$ from $D_\mathfrak{q}$ to $Gal((B/\mathfrak{q})/(A/\mathfrak{p}))$ is surjective with kernel $I_\mathfrak{q}$. Thus, $Gal((B/\mathfrak{q})/(A/\mathfrak{p})) \cong D_\mathfrak{q}/I_\mathfrak{q}$.*

Proof. Let $\bar{x}$ be a primitive element of $((B/\mathfrak{q})/(A/\mathfrak{p}))$, and let x be a representative with minimal polynomial $F(x) = x^n + \ldots + a_1x_1 + a_0$ over K_D with coefficients a_i in A_D. The roots of $f(x)$ are $\sigma(x)$ ($\sigma \in D$). Since $D = \mathrm{Gal}(L/K_D)$, the roots of $f(x)$ are $\sigma(x)$ where σ belongs to D. If we reduce $f(x)$ modulo $\mathfrak{q}$, we obtain a polynomial

$$\bar{x}^n + \ldots + \bar{a_0}$$

with coefficients in $A/\mathfrak{p}$. Since $\bar{x}$ is a *primitive element* of $((B/\mathfrak{q})/(A/\mathfrak{p}))$, we can take the minimal monic polynomial $\overline{\phi}(x)$. This divides $\phi(x)$ reduced modulo $\mathfrak{q}$ and thus all its roots are images of the roots of $\phi(x)$, i.e roots of $\overline{F}(\bar{x})$ are $\bar{\sigma}(\bar{x})$. Furthermore, since

$$\sigma \in D_\mathfrak{q} \implies \sigma(\mathfrak{q}) = \mathfrak{q}$$

all the conjugates of $\bar{x}$ belong to $((B/\mathfrak{q})/(A/\mathfrak{p}))$ which means that $((B/\mathfrak{q})/(A/\mathfrak{p}))$ is Galois.

Since every conjugate of $\bar{x}$ can be written as $\bar{\sigma}(\bar{x})$, every automorphism in $\mathrm{Gal}((B/\mathfrak{q})/(A/\mathfrak{p}))$ is of the form σ and thus

$$D/I_\mathfrak{q} \cong Gal((B/\mathfrak{q})/(A/\mathfrak{p}))$$

□

Corollary 6.7. *$\mathfrak{p}$ does not ramify if and only if the $I_\mathfrak{q}$ is trivial for all $\mathfrak{q}$ lying above $\mathfrak{p}$.*

Proof. By fundamental theorem of Galois theory, $Gal((B/\mathfrak{q})/(A/\mathfrak{p})) = f$. Furthermore,

$$|D| = ef \implies |I_\mathfrak{q}| = e$$

Thus, if $\mathfrak{p}$ is unramified, $|I_\mathfrak{q}| = 1$. □

Definition 6.8. Frobenius Conjugacy Class: Let K be a number field, let L/K a finite Galois extension and let $\mathfrak{p}$ be a prime ideal in A that does not ramify in B. Then, for each $\mathfrak{q}$ lying above $\mathfrak{p}$, $\mathrm{Gal}((B/\mathfrak{q})/(A/\mathfrak{p}))$ is cyclic since $A/\mathfrak{p}$ is a finite field. Furthermore, r^{th}-power map is the canonical generator where $r = |A/\mathfrak{p}|$, i.e. $r = p$ if $A = \mathbb{Z}$. Then, since

$$D_\mathfrak{q} \cong \mathrm{Gal}((B/\mathfrak{q})/(A/\mathfrak{p}))$$

, there is a pre-image of this generator in $D_\mathfrak{q}$ called $Frob_\mathfrak{q}$. Thus,

$$Frob_\mathfrak{q}(x) \equiv x^r \mod \mathfrak{q}\ \forall x \in B$$

Employing the following proposition, we arrive at the *Frobenius Conjugacy Class.*

Proposition 6.9. *Let* $\mathfrak{q}$ *and* $\mathfrak{q}' = \sigma(\mathfrak{q})$ *be primes lying above* $\mathfrak{p}$*. Then,*

$$Frob_{\mathfrak{q}'} = \sigma Frob_{\mathfrak{q}} \sigma^{-1}$$

Proof.

$$Frob_{\mathfrak{q}}(\sigma^{-1}(x)) \equiv (\sigma^{-1}(x))^p \equiv (\sigma^{-1})(x)^p \mod \mathfrak{q}$$

The result follows from taking the action of σ on both sides. □

Remark 6.10. It is clear that the $D(\sigma(\mathfrak{q}))$ are all equal and the $I(\sigma(\mathfrak{q}))$ are all equal when Gal(L/K) is abelian since the σ act transitively on the primes above $\mathfrak{p}$. Thus, if Gal(L/K) is abelian, $D(\sigma(\mathfrak{q}))$ depends only on $\mathfrak{p}$ and the Frobenius conjugacy class consists of a single element called the *Frobenius element*.

6.1. **Definition of Norm of Ideal.**

Definition 6.11. Let A be a Dedekind domain with field of fractions K and let B be the integral closure of A in L where L is an algebraic extension of K. For a principal ideal (π) in B, we define the norm of this ideal, $\mathcal{N}(\mathfrak{B}_i)$, to be $\mathfrak{p}^{f_i}$ where $f_i = [B/\mathfrak{B}_i : A/\mathfrak{p}]$. The definition for the norm of a general ideal follows from prime factorization of ideals in Dedekind domains.

6.2. **Equivalence with Index Norm.**

Let $\mathfrak{b}$ be an ideal in the ring of integers of a number field K. Then, we define the index norm of $\mathfrak{b}$ to be $\mathbb{N}(\mathfrak{b}) = |(\mathcal{O}_k/\mathfrak{b})| = (\mathcal{O}_K : \mathfrak{b})$.

There is an immediate relation between the norm of ideals and the index norm.

Proposition 6.12. *For any ideal* $\mathfrak{b} \subset \mathcal{O}_K$*,* $\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{b}) = (\mathbb{N}(\mathfrak{b}))$*.*

Proof. Since B is a Dedekind domain, $\mathfrak{b} = \prod q_i^{r_i}$. Then, $\mathcal{N}(\mathfrak{b}) = \prod (p_i)^{r_i f_i}$ where $p_i = \mathfrak{q}_\mathfrak{i} \cap \mathbb{Z}$ and $f_i = [B/\mathfrak{q}_\mathfrak{i} : \mathbb{F}_{p_i}]$. On the other hand,

$$\mathcal{O}_K/\mathfrak{b} \cong \prod \mathcal{O}_K/\mathfrak{q}_i^{r_i}$$

by Chinese Remainder Theorem. So, $[\mathcal{O}_k : \mathfrak{b}] = \prod [\mathcal{O}_K : \mathfrak{q}_\mathfrak{i}^{r_i}]$. But,

$$[\mathcal{O}_K : \mathfrak{q}_\mathfrak{i}^{r_i}] = p_i^{r_i \cdot f_i}$$

where $(p_i) = q_i \cap \mathbb{Z}$ since each quotient in the chain

$$B \supset B/\mathfrak{q}_i \ldots \subset B/q_i^{r_i}$$

is a $\mathbb{F}_{p_i}$ vector space of dimension f_i. Taking the product, $(\mathcal{O}_K : \mathfrak{b}) = \prod (p_i)^{r_i f_i}$. □

We check to see that the norm on elements agrees with the norm on ideals. Let $\mathfrak{p} = (\pi)B$ be a prime ideal in B, then

$$\mathcal{N}((\pi) \cdot B) = (\prod_i \mathcal{N}(\mathfrak{B}_i^{e_i}) = (\pi)^{\sum e_i f_i} = (\pi)^{[L:K]} = (Nm(\pi))$$

If K is also a number field, there is an alternative proof using the index norm. Consider $\pi \cdot B$ and let $\{v_i\}$ be a $\mathbb{Z}$-basis for B. Then, $\{\pi v_i\}$ is also a $\mathbb{Z}$-basis and $\pi v_j = \sum_i a_{ij} v_i$ for some a_{ij}. So,

$$|\mathcal{O}_K/\pi\mathcal{O}_K| = \det(a_{ij}) = \mathrm{Nm}(\pi)$$

7. Minkowski's Bound

We will state without proof the theorem and then examine a few of its consequences.

Theorem 7.1. *Let K be a degree n extension of $\mathbb{Q}$. Then, in every equivalence class of the ideal class group of K, there is an integral ideal representative, $\mathfrak{a}$, such that*

$$\mathbb{N}(\mathfrak{a}) \leq \frac{n!}{n^n}(\frac{4}{\pi})^s |Disc(K/\mathbb{Q})|^{\frac{1}{2}}$$

where s is the number of complex embeddings of K.

7.1. Finiteness of Ideal Class Number.

Proposition 7.2. *Let K be a finite algebraic extension of $\mathbb{Q}$, then $Cl(K)$ is finite.*

Proof. Given the Minkowski bound, it suffices to show that, for every positive integer, M there are only finitely many integral ideals with norm less than M. Let $\mathfrak{b}$ be an ideal in $\mathcal{O}_K$, then $\mathfrak{b} = \prod_i \mathfrak{q}_i^{r_i}$ and $\mathcal{N}(\mathfrak{b}) = \prod_i p_i^{r_i f_i}$. Therefore, if $\mathcal{N}(\mathfrak{b}) \leq M$, there are a finite number of r_i and p_i possible. This implies that there are a finite number of $\mathfrak{q}_i$ possible since only a finite number of $\mathfrak{q}_i$ lie above a given prime. Thus, there are a finite number of integral ideals with norm is less than M. □

7.2. Existence of Unramified extensions of $\mathbb{Q}$.

Proposition 7.3. *Let K be an extension of $\mathbb{Q}$. Then, at least one prime ideal in $\mathbb{Q}$ ramifies in $\mathcal{O}_K$.*

Proof. Every coset in the ideal class group must have at least one integral ideal representative and that element will have index norm ≥ 1. The Minkowski bound implies that

$$|Disc(K/\mathbb{Q})|^{\frac{1}{2}} \geq \frac{n^n}{n!}(\frac{\pi}{4})^s \geq \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}$$

Let $a_n = r.h.s.$ Then, $a_2 > 1$ and $\frac{a_{n+1}}{a_n} > 1$. Therefore, $|Disc(K/\mathbb{Q})| > 1$ which implies that there exists a prime that divides $Disc(K/\mathbb{Q})$. Thus, at least one prime ramifies in $\mathcal{O}_K$. □

8. Cyclotomic extensions and Quadratic Reciprocity

Theorem 8.1. *If $\mathbb{Q}[\zeta_n]$ is the nth cyclotomic field, then $Gal(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. Every automorphism in $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ is determined by its action on ζ_n. Therefore, each automorphism is of the form $\sigma_a : \zeta_n \to \zeta_n^a$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^x$ such that $(a, n) = 1$. The map $\phi : a \mapsto \sigma_a$ is a homomorphism since

$$(\sigma_a\sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n^b)^a = \zeta_n^{ab} = \sigma_{ab}(\zeta_n)$$

This map is injective since each automorphism is uniquely determined by its action on ζ_n and it is surjective since $|\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})|=\phi(n)$. □

Remark 8.2. The isomorphism $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$ is canonical. Let ζ_n and ζ_n^m be two different n^{th} roots of unity. Furthermore, consider $\sigma_a : \zeta_n \mapsto \zeta_n^a$ and $\tau_a : \zeta_n^m \mapsto \zeta_n^{am}$ – the two possible images of a – in $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$. Then,

$$\sigma_a(\zeta_n^m) = \zeta_n^{ma} = \tau_a(\zeta_n^m)$$

Since automorphisms in $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ are uniquely determined by their action on a primitive root, $\sigma_a = \tau_a$. Therefore, the automorphism between $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ and $\mathbb{Z}/n\mathbb{Z}$ is independent of the choice of primitive root of unity and so it is a canonical isomorphism.

Remark 8.3. Compatibility of the Isomorphism:

If n divides N, define π_1 from $\mathrm{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q})$ to $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ to be

$$\pi_1 : \sigma^a \mapsto \sigma^{\bar{a}}, \text{ where } \bar{a} \equiv a \mod n$$

and define π_2 from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the natural reduction modulo n map:

$$\pi_2 : a \mapsto \bar{a}$$

Furthermore, let ϕ_n and ϕ_N be defined as in previous theorem. Then, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}[\zeta_N]/\mathbb{Q}) & \xrightarrow{\phi_N} & (\mathbb{Z}/N\mathbb{Z})^\times \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) & \xrightarrow{\phi_n} & (\mathbb{Z}/n\mathbb{Z})^\times \end{array}$$

Therefore, the isomorphism is compatible.

We will show later that for any odd prime, p, $\mathbb{Q}[\sqrt{\pm p}] \subset \mathbb{Q}[\zeta_p]$ (positive sign if $p = 1 \mod(4)$ and negative if $p = 3 \mod(4)$). However, we now

develop a strong relation between the Galois groups of subfields of cyclotomic extensions and finite abelian groups:

Proposition 8.4. *Every finite abelian group appears as the Galois group of a subfield of a cyclotomic extension.*

Proof. Let G be a finite abelian group. By the fundamental stucture theorem of abelian groups, $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$. By Dirichlet's theorem, for every m $\in \mathbb{Z}$ there exists an infinite number of primes such that $p \equiv 1 \mod m$ (also can be shown using cyclotomic extensions). Thus, we can choose $p_1, ...p_r$ all distinct such that $p_i \equiv 1 \mod n_r$. If $n = p_1 \cdot \ldots \cdot p_n$, then

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^\times \cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \ldots \times \mathbb{Z}/(p_n-1)\mathbb{Z}$$

Let H_i be a subgroup of Z_{p_i-1} of order $\frac{p_i-1}{n_i}$. Then, Z_{p_i-1}/H_i is cyclic of order n_i. Thus,

$$(\mathbb{Z}/n\mathbb{Z})^\times/(H_1 \times ... \times H_n) \cong G$$

By the fundamental theorem of Galois theory, the fixed field of G will be a subfield of $\mathbb{Q}[\zeta_n]$. □

Proposition 8.5. *If K be a cyclotomic extension of* $\mathbb{Q}$*. Then, the Frobenius conjucacy class for a prime, p, is a single element. In fact,* $Frob_p = \sigma_p : \zeta_n \mapsto \zeta_n^p$.

Proof. Since $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ is abelian, the Frobenius conjugacy class is a single element. Furthermore, if p is a prime that does not divide n, then the image of p under the isomorphism of Theorem 8.1 is σ_p which maps ζ_n to ζ_n^p. Since p is unramified, Theorem 6.6 implies that the decomposition group is isomorphic to $\mathrm{Gal}((\mathbb{Z}[\zeta_n]/\mathfrak{q})/(\mathbb{F}_p))$ where $\mathfrak{q}$ is a prime lying above p. Thus, we have the isomorphism

$$D_p \cong \mathrm{Gal}((\mathbb{Z}[\zeta_n]/\mathfrak{q})/(\mathbb{F}_p)) \tag{8.6}$$

$\Phi(x)$ is separable over $\mathbb{F}_p$ since $\Phi'(x) = nx^{n-1}$ and p does not divide n. Thus, the roots of unity remain distinct modulo $\mathfrak{q}$, i.e. $\overline{\zeta_i} \neq \overline{\zeta_j}$. Thus, there is exists an injection $\mathrm{Gal}((\mathbb{Z}[\zeta_n]/\mathfrak{q})/(\mathbb{F}_p)) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ Combining with 8.6, we have that

$$D_p \cong \mathrm{Gal}((\mathbb{Z}[\zeta_n]/\mathfrak{q})/(\mathbb{F}_p)) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

Since the pre-image of $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ in $\mathrm{Gal}((\mathbb{Z}[\zeta_n]/\mathfrak{q})/(\mathbb{F}_p))$ is the Frobenius automorphism and the preimage in D_p is σ_p, we have that $\sigma_p = \mathrm{Frob}_p$. □

8.1. **Quadratic fields contained in Cyclotomic fields.**

Proposition 8.7. *Every quadratic field is contained in a cyclotomic field. In fact,* $\mathbb{Q}[\sqrt{m}]$ *is contained in the* D^{th} *cyclotomic field, where* $D = Disc(\mathbb{Q}[\sqrt{m}])$.

Proof. Case: m is an odd prime

From Example 5.3, $\mathrm{Disc}(\mathbb{Q}[\zeta_p]) = (-1)^{(p-1)/2}p^{p-2}$. But, Disc($\mathbb{Q}[\zeta_p]$)=$(\det(\sigma_i(\zeta_p^j))^2$ and so

$$|\sigma_i(\zeta_p^j)| = p^{(p-3)/2} \cdot \sqrt{\pm p}$$

Since all the $\sigma_i(\zeta_p^j)$ are just permutations of the cyclotomic roots, $\sqrt{\pm p} \in \mathbb{Q}[\zeta_p]$. This implies that $\mathbb{Q}[\sqrt{\pm p}] \subset \mathbb{Q}[\zeta_p]$. Also, if $\mathbb{Q}[\zeta_r] \supset \mathbb{Q}[\sqrt{p}]$, then $\mathbb{Q}[\zeta_{4r}] \supset \mathbb{Q}[\sqrt{-p}]$ since $\mathbb{Q}[\zeta_{4r}]$ contains the fourth roots of unity.

Case: $m = 2$

It is easily checked that $\sqrt{2} = e^{(i\pi)/4} + e^{(7i\pi)/4} = \zeta_8 + \zeta_8^{-1}$ and therefore $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\zeta_8]$.

Case: $m = p_1 \cdot \ldots \cdot p_n$ For each p_i, we take the cyclotomic field which contains $\mathbb{Q}[\sqrt{p}]$ and then take the smallest cyclotomic field, say $\mathbb{Q}[\zeta_m]$, that contains all these cyclotomic fields.

Furthermore, we can show that $\mathbb{Q}[\zeta_D]$, where $D = \text{Disc}(\mathbb{Q}[\sqrt{m}]/\mathbb{Q})$, is the smallest cyclotomic field.

If $m \equiv 1 \mod 4$, then $\sqrt{m} \in \mathbb{Q}[\zeta_m]$ since $\mathbb{Q}[\zeta_m] = \prod \mathbb{Q}[\zeta_{p_i}]$ and since the $\sqrt{-p_j}$ (when $p_j \equiv 3 \mod 4$) become positive in pairs.

If $m \equiv 2, 3 \mod 4$, then $\sqrt{m} \in \mathbb{Q}[\zeta_m]$ but $\sqrt{-m} \notin \mathbb{Q}[\zeta_m]$ since it is necessary to to generate the fourth root of unity in order to balance the signs. Thus, the smallest cyclotomic field is $\mathbb{Q}[\zeta_D]$. □

Remark 8.8. The converse also holds: Given an odd prime q and its associated cyclotomic field $K = \mathbb{Q}[\zeta_q]$, $\mathbb{Q}[\sqrt{q^*}]$ is the unique quadratic field contained in K where $q^* = (-1)^{(q-1)/2}q$.

Proof. Since Gal(K/$\mathbb{Q}$) is cyclic of order $q-1$, it has a *unique* subgroup of index 2. Thus, the quadratic field contained in K must be unique.

Furthermore, $\sqrt{D}$ does not belong to $\mathbb{Q}$ since $D =$Disc(K/$\mathbb{Q}$) $= (-1)^{(q-1)/2}q^{q-2}$. $\sqrt{D}$ belongs to K since $\sqrt{D} = \prod(\zeta_i - \zeta_j)$ by Lemma 5.3. Furthermore,

$$\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{q^*}]$$

□

Definition 8.9. *Legendre Symbol*: Let p be an odd prime and a an integer, then

$$(\frac{a}{p}) := \begin{cases} 1 & \text{if } a \equiv m^2 \bmod p,\ m \in \mathbb{Z} \text{ and } m \neq 0 \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p \\ 0 & \text{if } a \equiv 0 \bmod p \end{cases}$$

8.2. **Proof of Quadratic Reciprocity.**

Proposition 8.10. *Quadratic reciprocity: p is a quadratic residue modulo q if and only if q is a quadratic residue modulo p. More succinctly,* $(\frac{p}{q}) = (\frac{q^*}{p})$

Proof. Let $K = \mathbb{Q}[\sqrt{q^*}]$ and $L = \mathbb{Q}[\zeta_q]$. From above,

$$\mathbb{Q} \subset K \subset L$$

By 8.8, K is the unique quadratic subfield of L. Furthermore, let $Frob_{q,K}$ be the Frobenius automorphism on $Gal(K/\mathbb{Q})$ and let $Frob_{q,L}$ be the Frobenius automorphism on $Gal(L/\mathbb{Q})$. By reduction on residue fields,

$$Frob_{q,L}|_K = Frob_{q,K}$$

Given an integer prime, p splits if and only if p is a quadratic residue of q^*. Furthermore, if p splits, then the decomposition group is trivial and $Frob_{q,K}$ is the identity. If, however, p is inert, then $e = 1$ and $f = 2$. Therefore, the decomposition group is non-trivial. Since $Gal(K/\mathbb{Q})$ can be identified as the multiplicative group $\{-1, 1\}$, we have that

$$p \text{ is not a quadratic residue modulo } q \iff p \text{ is inert} \implies Frob_{q,K} = -1$$

Thus,

$$Frob_{q,K} = (\frac{q^*}{p})$$

On the other hand, $Frob_{q,L}|_K = Frob_{q,K}$ implies that $Frob_{q,K} = Id$ if and only if $Frob_{q,L}$ belongs to the unique index 2 subgroup of $Gal(L/\mathbb{Q})$. However, this is equivalent to $Frob_{q,L}$ being a square. From $Frob_{q,L}(x) = x^p \bmod q$, we have that

$$Frob_{q,L} \text{ is a square} \iff (\frac{p}{q}) = 1$$

Therefore,

$$Frob_{q,K} = (\frac{p}{q})$$

Thus, we have that

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

□

9. Čebotarev Prime Density Theorem

9.1. **Definition of Natural Density.**

Definition 9.1. Let K be an algebraic number field and S be a set of prime ideals in K. The *natural density* of S, $\delta(S)$, is defined to be:

$$\delta(S) = \lim_{n\to\infty} \frac{|\{\mathfrak{p} \in S : \mathcal{N}(\mathfrak{p}) \leq n\}|}{|\{\mathfrak{p} : \mathcal{N}(\mathfrak{p}) \leq n\}|}$$

provided the limit exists.

9.2. **Statement of Čebotarev Prime Density Theorem.**

Theorem 9.2. *Let L be a finite Galois extension of K, an algebraic number field, G be its Galois group, and C be a conjugacy class of G. Then, the density of the primes such that $\sigma_\mathfrak{p} \in C$ exists and is equal to $|C|/|G|$.*

Remark 9.3. Proofs of Čebotarev Prime Density Theorem: While most modern expositions rely upon class field theory to prove this result ([3]), Čebotarev himself arrived at the result by reducing to cyclotomic extensions. See ([5]) for a complete and rigorous exposition.

9.3. **Dirichlet implies Čebotarev in $\mathbb{Q}[\sqrt{m}]$.** If $K = \mathbb{Q}[\sqrt{m}]$, then $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Since the group is abelian, then each element has only a single conjugate. Thus, Čebotarev's theorem implies that the primes that split and those that remain inert each have density equal to $1/2$. However, this result can also achieved directly from Dirichlet's density theorem.

Proof. A prime $p \in \mathbb{Z}$ remains prime in $\mathcal{O}_K$ if and only if m is not a square modulo p. Thus, it is equivalent to show that the primes such that m is a square modulo p has density $1/2$ since only finitely many primes ramify.

Case 1: m is a prime and $m \equiv 1 \bmod 4$.

Let $m = q$. Then, from quadratic reciprocity 8.10,

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

for each p. Furthermore, $\phi(q)/2$ residues are squares modulo q and the density of primes for each residue is $1/\phi(q)$. Therefore, the density of primes p such that $(\frac{p}{q}) = 1$ is

$$\frac{1}{\phi(q)} \cdot \frac{\phi(q)}{2} = 1/2$$

Case 2: m is a prime and $m \equiv 3 \bmod 4$.

Let $m = q$. This case cannot be handled as simply as the first since quadratic reciprocity implies that

$$(\frac{p}{q}) = -(\frac{q}{p}) \text{ if } p \equiv 3 \bmod 4$$
$$(\frac{p}{q}) = (\frac{q}{p}) \text{ if } p \equiv 1 \bmod 4$$

Thus,

$$(\frac{p}{q}) = 1 \iff p \bmod 4q \in 1\times\{\text{squares in } (\mathbb{Z}/q\mathbb{Z})^\times\} \cup 3\times\{\text{non-squares in } (\mathbb{Z}/q\mathbb{Z})^\times\}$$

But, the right hand side is contained in

$$(\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(4q\mathbb{Z})$$

The first case implies that the primes such that

$$p \bmod 4q \in 1 \times \{\text{squares in } \mathbb{Z}/q\mathbb{Z}\}$$

have density equal to $1/2$. The case where $p = 3 \bmod 4$ follows similarly. Thus, $(\frac{p}{q}) = 1$ for half the residue classes in $\mathbb{Z}/(4q\mathbb{Z})$.

Case 4: m is an arbitrary natural number. Let $m = q_1 \cdot \ldots \cdot q_n$ be the prime decomposition of m. We consider each of the equivalence classes modulo $q_1 \cdot \ldots \cdot q_{n-1}$ independently. Since

$$(\frac{m}{p}) = (\frac{q_1 \cdot \ldots \cdot q_{n-1}}{p})(\frac{q_n}{p})$$

the $(\frac{q_1 \cdot \ldots \cdot q_{n-1}}{p})$ are constant on each equivalence class. Furthermore, let R be the primes congruent to $r \bmod q_1 \cdot \ldots \cdot q_{n-1}$. Then, the subset of R congruent to some $s \bmod q_n$ must have density $1/\phi(q_n)$ in R. Thus, the primes p in

R such that $(\frac{m}{p}) = 1$ have density $1/2$ in R. However, this holds for every equivalence class since the choice of a was arbitrary. Thus, the primes p in $\mathbb{Z}$ such that $(\frac{m}{p}) = 1$ have density $1/2$. □

9.4. Čebotarev's Prime Density Theorem is equivalent to Dirichlet's on $\mathbb{Q}[\zeta_n]$.

Theorem 9.4. *Dirichlet's Theorem: Let m be a positive integer. Then, for each a in $\mathbb{Z}$ such that $(a, m) = 1$, the set of prime numbers such that $p \equiv a \bmod m$ has density equal to $1/\phi(m)$.*

Theorem 9.5. *Čebotarev's Prime Density Theorem is equivalent to Dirichlet's for cyclotomic extensions of $\mathbb{Q}$.*

Proof. Let K be equal to $\mathbb{Q}$ and L be a cyclotomic extension of K. Then, if $\mathfrak{q}$ lies above $p \neq 0 \bmod m$, Proposition 8.5 implies that

$$Frob_{\mathfrak{q}} = p \bmod m$$

So, for an arbitrary automorphism $\sigma_a : \zeta_m \mapsto \zeta_m^a$,

$$\sigma_a = Frob_{\mathfrak{q}} \iff p \equiv a \bmod m$$

Assuming Čebotarev's Prime density theorem, the set $S_a := \{p \in \mathbb{Z} : p \equiv a \bmod m\}$ corresponds to the set $\mathrm{S}|_{\sigma=\sigma_a}$ from Čebotarev's theorem. So,

$$\delta(S_a) = |C|/|G| = 1/\phi(m)$$

and Čebotarev $\implies$ Dirichlet.

We can easily reverse the order of the argument to obtain the opposite direction. Since $\delta(S|_{\sigma=\sigma_a}) = \delta(S_a)$, Dirichlet's theorem implies that $\delta(S|_{\sigma=\sigma_a}) = 1/\phi(m) = |C|/|G|$ and so Dirichlet $\implies$ Čebotarev.

Thus, Dirichlet's Prime Density Theorem is equivalent to Čebotarev's for cyclotomic extensions of $\mathbb{Q}$. □

10. Acknowledgements

I first want to thank the University of Chicago Math department for providing the financial assistance for all REU participants. Secondly, I am deeply grateful to Peter May for organizing the REU, kindly accepting me to the program and thereby ensuring the most enjoyable summer of my life. Finally, I would like to extend profuse thanks to my mentor Sean Howe for his encouragement, lucid explanations, persistent enthusiasm and his tireless editing. It has been the definite highlight of my freshman year to have the chance to work with him over the past months through the DRP and REU programs.

References

[1] Ash, Robert *A Course in Algebraic Number Theory* 2003
[2] Milne, James S. *Algebraic Number Theory (v3.03)*, 2011
[3] Milne, James S. *Class Field Theory* 2013
[4] Jody Esmonde, M. Ram Murty *Problems in Algebraic Number Theory* Springer. 1999
[5] P. Stevenhagen, H. W. Lenstra, Jr *Čebotarev and his density theorem* Math. Intelligencer (1996), no.2, 26-37