QUADRATIC RECIPROCITY VIA NUMBER FIELDS

ZACHARY FENG

Abstract. The goal of these notes are to present a motivated discussion of the quadratic reciprocity theorem using number field techniques. In fact, most of our discussion will be about prime ramification in number fields, and the actual quadratic reciprocity theorem will follow at the end as an easy consequence. These notes are mainly based on the material presented in *Chapters 2-4* of *Number Fields* by Daniel A. Marcus. [Mar18] The particular section on the Kummer-Dedekind Theorem is adapted from Keith Conrad's notes on *Factoring in Quadratic Fields*. [Con] Any ambiguous discussions are reinterpreted in my own words and any proofs left as exercises to the reader are completed accordingly.

1. Cyclotomic fields

Let $\omega = e^{2\pi i/m}$. The conjugates of ω are complex numbers which share the same irreducible polynomial as ω over $\mathbb{Q}$. Clearly, every conjugate of ω must be an m^{th} root of unity. Moreover, the conjugates of ω cannot be n^{th} roots of unity for any $n < m$. To see this, notice that the irreducible polynomial for ω over $\mathbb{Q}$ divides $X^m - 1$ but cannot divide $X^n - 1$ for any $n < m$ since $\omega^n \neq 1$. Hence, it follows that the only candidates for the conjugates of ω are ω^k for $1 \leq k \leq m$ with k and m coprime. In this section, we will show that all of the candidates are in fact conjugates of ω, and then use this result to determine the Galois group of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, which we find to be isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 1.1. *Let f be a monic polynomial in $\mathbb{Z}[X]$ and suppose $f = gh$ where g and h are monic polynomials in $\mathbb{Q}[X]$ then both g and h are in $\mathbb{Z}[X]$.*

Lemma 1.2. *If f and g are polynomials over a field K and $f^2 \mid g$ in $K[X]$ then $f \mid g'$.*

Theorem 1.3. *ω^k is a conjugate of ω for all k such that $1 \leq k \leq m$ and $(k, m) = 1$.*

Proof. The relation $\sim$ of being conjugates is transitive. Therefore, it suffices to show that for each k such that $(k, m) = 1$ and for each prime p such that $p \nmid m$ that $\omega^k =: \theta \sim \theta^p$.

Let $\theta = \omega^k$ and p be a prime such that $p \nmid m$. Let f be the minimal polynomial for θ in $\mathbb{Q}[X]$ then $X^m - 1 = f(X)g(X)$ for some monic $g \in \mathbb{Q}[X]$, and in fact, both $f, g \in \mathbb{Z}[X]$ using Lemma 1.1. Since θ^p is a root of $X^m - 1$ one has θ^p is a root of f or g; it remains to show that θ^p is a root of f. Suppose that $g(\theta^p) = 0$ for contradiction, then θ is a root of $g(X^p)$ and so $f(X) \mid g(X^p)$ in $\mathbb{Q}[X]$. Therefore, $f(X) \mid g(X^p)$ in $\mathbb{Z}[X]$, again, calling to Lemma 1.1. Let the bar denote the image of a polynomial under the ring homomorphism $\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$ then $\overline{f}(X) \mid \overline{g}(X^p)$ in $\mathbb{Z}/p\mathbb{Z}[X]$. The "freshman's dream" tells us that $\overline{g}(X^p) = (\overline{g}(X))^p$ and $\mathbb{Z}/p\mathbb{Z}[X]$ is a unique factorization domain. Therefore, $\overline{f}$ and $\overline{g}$ share a common factor $h \in \mathbb{Z}/p\mathbb{Z}[X]$, and moreover, $h^2 \mid \overline{fg} = X^m - 1$. Therefore, $h \mid \overline{m}X^{m-1}$ using

Lemma 1.2. However, $p \nmid m$ so $\overline{m} \neq 0$. Therefore, h is just a monomial. However, this is impossible since $h \mid X^m - 1$. □

Corollary 1.4. *$\mathbb{Q}(\omega)$ has degree $\varphi(m)$ over $\mathbb{Q}$.*

Proof. ω has $\varphi(m)$ conjugates. Therefore, the irreducible polynomial for ω over $\mathbb{Q}$ has degree $\varphi(m)$. □

Corollary 1.5. *There is the following group isomorphism.*

$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}\left(\mathbb{Q}(\omega)/\mathbb{Q}\right)$$
$$k \mapsto (\omega \mapsto \omega^k)$$

Proof. An automorphisms of $\mathbb{Q}(\omega)$ is uniquely determined by the image of ω and Theorem 1.3 has that ω can be sent to any of the ω^k for $(k, m) = 1$ and nothing else. Therefore, there is a bijection between the group of units and the Galois group. Moreover, that the map is a homomorphism is clear. □

Therefore, the subfields of $\mathbb{Q}(\omega)$ correspond to the subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$. Moreover, if p is prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, and hence the p^{th} cyclotomic field contains a unique subfield of each degree that divides $p-1$. In particular, for every odd prime p, the p^{th} cyclotomic field contains a unique quadratic subfield. The quadratic subfield is $\mathbb{Q}(\sqrt{\pm p})$ with the sign depending on $p \pmod 4$. This phenomenon can be most succinctly explained with the quadratic Gauss sum:

$$\sum_{n=0}^{p-1} e^{\frac{2\pi i n^2}{p}} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Our discussion is summarized in the following proposition.

Proposition 1.6. *For each odd prime p, the p^{th} cyclotomic field contains the unique quadratic field:*

$$\begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Q}(-\sqrt{p}) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

2. Norms and traces

Let K be a finite extension over $\mathbb{Q}$ with degree $n = [K : \mathbb{Q}]$ then $K/\mathbb{Q}$ is separable since every finite extension over $\mathbb{Q}$ is separable. Therefore, using the primitive element theorem, there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial for θ over $\mathbb{Q}$ then $f(X)$ is separable and has n distinct roots $z_1, \ldots, z_n$ in $\mathbb{C}$. It is not difficult to show that the map $\sigma_i : \theta \mapsto z_i$ extends into an embedding of $\mathbb{Q}(\theta)$ into $\mathbb{C}$ for each $1 \leq i \leq n$. To see that each one is a field embedding, consider the ring homomorphism $\mathbb{Q}[X] \to \mathbb{C}$ that sends $\mathbb{Q}$ onto itself and $X \mapsto z_i$. The kernel of this map is the ideal generated by the minimal polynomial $f(X)$. Taking the quotient gives an embedding of fields.

$$\mathbb{Q}(\theta) \cong \mathbb{Q}[X]/(f(X)) \hookrightarrow \mathbb{C}$$

Moreover, these are the only embeddings because an embedding must send $0 \mapsto 0$ and $1 \mapsto 1$ and hence map $\mathbb{Q}$ onto itself in $\mathbb{C}$. Therefore, an embedding is determined by the image of θ which can only be mapped onto other roots of $f(X)$. For $\alpha \in K$, we define the norm of α over $\mathbb{Q}$ to be:

$$\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\theta)$$

A particularly useful property of the norm is that $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Q}$ for all $\alpha \in K$, and moreover, if $\alpha \in \mathcal{O}_K$ then in fact $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Z}$. Now, let us suppose, in addition, that K is a Galois extension over $\mathbb{Q}$, then $\mathrm{Gal}(K/\mathbb{Q}) = \{\tau_1, \ldots, \tau_n\}$ are n distinct automorphisms of K that fix $\mathbb{Q}$ pointwise. If we fix an embedding $\sigma = \sigma_1$ into $\mathbb{C}$ then I claim that the composition maps $\sigma\tau_i$ for each $1 \leq i \leq n$ gives back each of the original n embeddings of K into $\mathbb{C}$. This is not hard to show. Let τ_i be a Galois automorphism, then $\tau_i(\theta)$ must be another root of $f(X)$, and hence $\sigma\tau_i(\theta)$ as well. Therefore, since embeddings are determined by the image of θ we have that $\theta \mapsto \sigma\tau_i(\theta)$ is an embedding for each $1 \leq i \leq n$. Moreover, the embeddings $\sigma\tau_i(\theta)$ are all distinct because suppose $\sigma\tau_i(\theta) = \sigma\tau_j(\theta)$ for $i \neq j$ then $\tau_i(\theta) = \tau_j(\theta)$ since every map of fields is injective, and hence $\tau_i = \tau_j$ is a contradiction. Therefore, $\{\sigma_i\}_{1 \leq i \leq n} = \{\sigma\tau_i\}_{1 \leq i \leq n}$. Now, in the special case where K is a Galois extension over $\mathbb{Q}$, there is an equivalent way to define the norm $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)$ as the product of Galois conjugates:

$$\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = \prod_{i=1}^{n} \tau_i(\alpha)$$

To see that these are equivalent definitions, notice that $\sigma \prod_{i=1}^{n} \tau_i(\alpha) = \prod_{i=1}^{n} \sigma\tau_i(\alpha)$ is our original number which is an element of $\mathbb{Q}$. Then, using the fact that σ is injective and maps $\mathbb{Q}$ onto itself, we conclude that our new definition $\prod_{i=1}^{n} \tau_i(\alpha)$ is indeed the same number.

There is a similar definition of the norm for finite extensions over fields other than $\mathbb{Q}$. Let L be a finite extension over K with degree $n = [L : K]$. Suppose that $L = K(\theta)$ for a primitive element $\theta \in L$ then there are n distinct embeddings $\{\sigma_1, \ldots, \sigma_n\}$ of L into $\mathbb{C}$ that fix K pointwise. In almost the same way, for $\alpha \in L$, we define the norm of α over K to be:

$$\mathrm{N}_{K}^{L}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

Once again, we know that $\mathrm{N}_{K}^{L}(\alpha) \in K$ for all $\alpha \in K$, and moreover, if $\alpha \in \mathcal{O}_L$ then $\mathrm{N}_{K}^{L}(\alpha) \in \mathcal{O}_K$. Similarly, if L happens to be a Galois extension over K then let $\mathrm{Gal}(L/K) = \{\tau_1, \ldots, \tau_n\}$ and there is an equivalent definition for the norm of L into K defined as the product of α-conjugates in L:

$$\mathrm{N}_{K}^{L}(\alpha) = \prod_{i=1}^{n} \tau_i(\alpha)$$

A related notion to the norm is that of the trace. Let L be a finite extension over K with degree $n = [L : K]$ and $\{\sigma_1, \ldots, \sigma_n\}$ be the n distinct embeddings of L into $\mathbb{C}$ that fix K pointwise as before.

For $\alpha \in L$, the trace of α over K is defined to be the following sum:

$$\mathrm{Tr}_K^L(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

Whereas the the norm is a homomorphism of the multiplicative group structure of L into K, the trace should be thought of as a homomorphism of the additive group structure of L into K. Unsurprisingly, it is again true that $\mathrm{Tr}_K^L(\alpha) \in K$ for all $\alpha \in L$ with $\mathrm{Tr}_K^L(\alpha) \in \mathcal{O}_K$ whenever $\alpha \in \mathcal{O}_L$. If L is a Galois extension over K, then let $\mathrm{Gal}(L/K) = \{\tau_1, \ldots, \tau_n\}$, and using the same argument as we did for the norm, we can show that the sum of α-Galois conjugates in L is an equivalent definition of the trace:

$$\mathrm{Tr}_K^L(\alpha) = \sum_{i=1}^{n} \tau_i(\alpha)$$

3. Prime decomposition in number rings

The study of prime decomposition in number rings begins with the careful study of the properties of a particular integral domain known as the *Dedekind domain*. The most important property of Dedekind domains is that any ideal can be uniquely represented as a product of prime ideals. This property generalizes the notion of unique factorization of integers in $\mathbb{Z}$ into prime numbers. Conveniently, it turns out that every number ring is a Dedekind domain, and hence it makes sense to consider the notion of *prime decomposition* in a number ring. In this section, we first state a number of properties of Dedekind domains, without proof, for reference. Then, the rest of this section will be dedicated to building up the theory for prime decomposition in number rings, culminating in the proof of the Kummer-Dedekind Theorem for quadratic extensions, a crucial ingredient for quadratic reciprocity.

Definition 3.1. A *Dedekind domain* is an integral domain R such that

(1) Every ideal is finitely generated;
(2) Every non-zero prime ideal is a maximal ideal;
(3) R is integrally closed in its field of fractions.

Proposition 3.1. *The following are equivalent for a commutative ring R.*

(1) Every ideal is finitely generated;
(2) Every increasing sequence of ideals is eventually constant: $I_1 \subset I_2 \subset I_3 \subset \ldots$ implies that all I_n are equal for sufficiently large n;
(3) Every non-empty set S of ideals has a maximal member, not necessarily unique: there exists $M \in S$ such that $M \subset I \in S$ implies $M = I$.

A ring satisfying any of the equivalent conditions of Proposition 3.1 is called a *Noetherian ring*.

Theorem 3.2. *Every number ring is a Dedekind domain.*

Corollary 3.3. *If I is any non-zero ideal in a number ring R then R/I is finite.*

Theorem 3.4. *Let I be an ideal in a Dedekind domain R. Then, there is an ideal J such that IJ is principal.*

Lemma 3.5. *In a Dedekind domain, every ideal contains a product of prime ideals.*

Lemma 3.6. *Let A be a proper ideal in a Dedekind domain R with field of fractions K, then there is an element $\gamma \in K \setminus R$ such that $\gamma A \subset R$.*

Corollary 3.7. *The ideal classes in a Dedekind domain form a group.*

The group in Corollary 3.7 is referred to as the *ideal class group.*

Corollary 3.8. *If A, B, C are ideals in a Dedekind domain, and $AB = AC$, then $B = C$.*

Corollary 3.9. *If A and B are ideals in a Dedekind domain R, then $A \mid B$ if and only if $A \supset B$.*

Theorem 3.10. *Every ideal in a Dedekind domain is uniquely representable as a product of prime ideals.*

Theorem 3.11. *Let I be an ideal in a Dedekind domain R, and let α be any non-zero element of I. Then, there exists $\beta \in I$ such that $I = (\alpha, \beta)$.*

Until further notice, let us consider K and L to be number fields with $K \subset L$.

Theorem 3.12. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ then the following conditions are equivalent:*
(1) $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$
(2) $\mathfrak{P} \supset \mathfrak{p}\mathcal{O}_L$
(3) $\mathfrak{P} \supset \mathfrak{p}$
(4) $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$
(5) $\mathfrak{P} \cap K = \mathfrak{p}$

For a pair of primes $\mathfrak{p}$ and $\mathfrak{P}$ that satisfy any of the equivalent conditions stated in Theorem 3.12 we use the terminology that either $\mathfrak{P}$ *lies over* $\mathfrak{p}$ or $\mathfrak{p}$ *lies under* $\mathfrak{P}$.

Theorem 3.13. *Every prime $\mathfrak{P}$ of $\mathcal{O}_L$ lies over a unique prime $\mathfrak{p}$ of $\mathcal{O}_K$; every prime $\mathfrak{p}$ of $\mathcal{O}_K$ lies under at least one prime $\mathfrak{P}$ of $\mathcal{O}_L$.*

The primes lying over a prime $\mathfrak{p}$ are exactly the ones which occur in the prime decomposition of $\mathfrak{p}\mathcal{O}_L$. The exponents with which they occur are called the *ramification indices.* Thus, if $\mathfrak{P}^e$ is the exactly power of $\mathfrak{P}$ dividing $\mathfrak{p}$ then e is called the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, denoted $e(\mathfrak{P}|\mathfrak{p})$. There is another important number associated with a pair of primes $\mathfrak{p}$ and $\mathfrak{P}$ with $\mathfrak{P}$ lying over $\mathfrak{p}$. We know that the quotient rings $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$ are fields since $\mathfrak{p}$ and $\mathfrak{P}$ are maximal ideals. The containment of $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induces composition ring homomorphism $\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{P}$ with kernel $\mathcal{O}_K \cap \mathfrak{P}$.

However, we know that $\mathcal{O}_K \cap \mathfrak{P} = \mathfrak{p}$, and hence there is a natural embedding of fields $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{P}$. The fields $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$ are called the *residue fields* of $\mathfrak{p}$ and $\mathfrak{P}$, respectively. We know that both $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$ are finite. Thus, this is an extension of finite fields. Let f be the degree of this finite field extension, then f is called the *inertial degree* of $\mathfrak{P}$ over $\mathfrak{p}$, denoted $f(\mathfrak{P}|\mathfrak{p})$.

Proposition 3.14. *Let $P \subset Q \subset U$ be primes in three number rings $R \subset S \subset T$, then:*

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

Proof. Consider the prime decomposition of P in S and then in T:

$$\begin{aligned} PS &= Q^{e(Q|P)}Q_1^{e_1} \dots Q_r^{e_r} \\ PT &= (Q^{e(Q|P)}Q_1^{e_1} \dots Q_r^{e_r})T \\ &= (QT)^{e(Q|P)}(Q_1T)^{e_1} \dots (Q_rT)^{e_r} \end{aligned}$$

Here, the prime decomposition of QT contains $U^{e(U|Q)}$ and hence $e(Q|P) \geq e(U|Q)e(Q|P)$. To see that the prime decompositions of Q_iT for $Q_i \neq Q$ did not produce any additional factors of U we recall the fact that every prime of T lies over a unique prime in S. Therefore, U could have only appeared in the prime decomposition of QT, and hence $e(Q|P) \leq e(U|Q)e(Q|P)$. Next, consider the chain of inclusions of finite fields $R/P \to S/Q \to T/U$. Then, the result that $f(U|P) = f(U|Q)f(U|P)$ follows from the fact that the degree of field extensions is multiplicative in towers. □

Theorem 3.15. *Let $n = [L : K]$ and let $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ be the primes of $\mathcal{O}_L$ lying over a prime $\mathfrak{p}$ of $\mathcal{O}_K$. Let $e_1, \dots, e_r$ and $f_1, \dots, f_r$ denote the corresponding ramification indices and inertial degrees, then $\sum_{i=1}^r e_i f_i = n$.*

The proof of Theorem 3.15 will be concurrent with another theorem. For an ideal I in a number ring R, we denote $\|I\|$ to be the index $|R/I|$ which we know to be finite.

Theorem 3.16. *Let $n = [L : K]$.*

(a) For ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$,

$$\|\mathfrak{ab}\| = \|\mathfrak{a}\|\|\mathfrak{b}\|$$

.

(b) Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$. For the $\mathcal{O}_L$-ideal $\mathfrak{a}\mathcal{O}_L$:

$$\|\mathfrak{a}\mathcal{O}_L\| = \|\mathfrak{a}\|^n.$$

(c) Let α be non-zero in $\mathcal{O}_K$. For the principal ideal (α):

$$\|(\alpha)\| = \left|\mathrm{N}_{\mathbb{Q}}^K(\alpha)\right|$$

Proof of Theorem 3.16(a). We will prove this statement for $\mathfrak{a}$ and $\mathfrak{b}$ relatively prime, and then show that $\|\mathfrak{p}^m\| = \|\mathfrak{p}\|^m$ for all prime ideals $\mathfrak{p}$. Thus, we will have shown that $\|\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r}\| = \|\mathfrak{p}_1\|^{m_1} \dots \|\mathfrak{p}_r\|^{m_r}$. Then, factoring $\mathfrak{a}$ and $\mathfrak{b}$ into prime ideals, and applying this formula, we will obtain the first result.

Hence, suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, then $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$ and $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. Using the Chinese Remainder Theorem, we know that $\mathcal{O}_K/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$ and hence $\|\mathfrak{a}\mathfrak{b}\| = \|\mathfrak{a}\|\|\mathfrak{b}\|$.

Next, consider $\|\mathfrak{p}^m\|$ with $\mathfrak{p}$ being a prime ideal. Consider the natural chain of ideal inclusions $\mathcal{O}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots \supset \mathfrak{p}^m$. The third isomorphism theorem tells us the following:

$$\mathcal{O}_K/\mathfrak{p}^{m-1} \cong \frac{\mathcal{O}_K/\mathfrak{p}^m}{\mathfrak{p}^{m-1}/\mathfrak{p}^m}$$

Continue in this fashion with $\mathcal{O}_K/\mathfrak{p}^{m-2}$ and so forth to conclude that:

$$|\mathcal{O}_K/\mathfrak{p}^m| = |\mathcal{O}_K/\mathfrak{p}|\left|\mathfrak{p}/\mathfrak{p}^2\right| \dots \left|\mathfrak{p}^{m-1}/\mathfrak{p}^m\right|$$

Therefore, it suffices to show that for each k:

$$\|\mathfrak{p}\| = \left|\mathfrak{p}^k/\mathfrak{p}^{k+1}\right|$$

Here, the $\mathfrak{p}^k$ are just considered as additive groups. In fact, we claim that there is an isomorphism:

$$\mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^k/\mathfrak{p}^{k+1}$$

First, fix any $\alpha \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$ then there is the obvious isomorphism:

$$\mathcal{O}_K/\mathfrak{p} \to \alpha\mathcal{O}_K/\alpha\mathfrak{p}$$

Next, the inclusion $\alpha\mathcal{O}_K \hookrightarrow P^k$ induces the homomorphism $\alpha\mathcal{O}_K \to \mathfrak{p}^k/\mathfrak{p}^{k+1}$ with kernel $(\alpha\mathcal{O}_K) \cap \mathfrak{p}^{k+1}$ and image $(\alpha\mathcal{O}_K + \mathfrak{p}^{k+1})/\mathfrak{p}^{k+1}$. Thus, we are done if we can show the following equalities:

$$(\alpha\mathcal{O}_K) \cap \mathfrak{p}^{k+1} = \alpha\mathfrak{p}$$
$$\alpha\mathcal{O}_K + \mathfrak{p}^{k+1} = \mathfrak{p}^k$$

Since $\alpha \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$ we know that $\mathfrak{p}^k$ is the highest power of $\mathfrak{p}$ that divides $\alpha\mathcal{O}_K$. Hence, considering the unique prime decomposition of $\alpha\mathcal{O}_K$ into primes $\mathfrak{p}^k\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r}$ we obtain our result:

$$(\alpha\mathcal{O}_K) \cap \mathfrak{p}^{k+1} = (\mathfrak{p}^k\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r} \cap \mathfrak{p}^{k+1}) = \mathfrak{p}^k(\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r} \cap \mathfrak{p}) = \mathfrak{p}^k(\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r}\mathfrak{p}) = \alpha\mathfrak{p}$$
$$\alpha\mathcal{O}_K + \mathfrak{p}^{k+1} = \mathfrak{p}^k\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r} + \mathfrak{p}^{k+1} = \mathfrak{p}^k(\mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r} + \mathfrak{p}) = \mathfrak{p}^k\mathcal{O}_K = \mathfrak{p}^k$$

□

Proof of Theorem 3.15, special case. We prove the theorem for $K = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$ for a prime $p \in \mathbb{Z}$.

$$p\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

$$\|p\mathcal{O}_L\| = \prod_{i=1}^{r} \|\mathfrak{P}_i\|^{e_i} = \prod_{i=1}^{r} (p^{f_i})^{e_i}$$

Here, $\|\mathfrak{P}_i\| = p^{f_i}$ because $\mathcal{O}_L/\mathfrak{P}_i$ is a degree f_i extension of the finite field $\mathbb{Z}/p\mathbb{Z}$. Moreover, we know that $\mathcal{O}_L \cong \mathbb{Z}^n$ as additive groups. Therefore, since the quotient of $\mathbb{Z}^n$ by $p\mathbb{Z}^n$ has p^n equivalence classes, we obtain that $\|p\mathcal{O}_L\| = p^n$. Therefore, $n = \sum_{i=1}^{r} f_i e_i$. □

Proof of Theorem 3.16(b). Using the result of Theorem 3.16*(a)*, it suffices to prove this statement for the case where $\mathfrak{a}$ is a prime $\mathfrak{p}$. The general result is then obtained by factoring $\mathfrak{a}$ into prime ideals.

First, notice that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a vector space over the field $\mathcal{O}_K/\mathfrak{p}$. To see this, notice that the natural inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induces the ring homomorphism $\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ with kernel $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{p}$. Hence, there is an inclusion $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. We claim that the dimension of this vector space is n.

First, we will show that its dimension is at most n. It will be equivalent to showing that any $n+1$ elements are linearly dependent. Thus, fixing $\alpha_1, \ldots, \alpha_{n+1} \in \mathcal{O}_L$ we will show that the corresponding elements in $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ are linearly dependent over $\mathcal{O}_K/\mathfrak{p}$. Of course, we know that $\alpha_1, \ldots, \alpha_{n+1}$ are linearly dependent over K since L is an n-dimensional vector space over K. Therefore, they are linearly dependent over $\mathcal{O}_K$ as well, since if $c_1\alpha_1 + \cdots + c_{n+1}\alpha_{n+1} = 0$ with $c_i \in K$ and not all $c_i = 0$, then there exists a non-zero integral element $r \in \mathcal{O}_K$ such that $rc_i \in \mathcal{O}_K$ for all $1 \le i \le n+1$. Intuitively, this can be thought of as "clearing the denominator". Therefore, $\alpha_1, \ldots, \alpha_{n+1}$ are linearly dependent over $\mathcal{O}_K$. We can assume that all of the c_i are in $\mathcal{O}_K$ without loss of generality. It remains to show that the c_i are not all in $\mathfrak{p}$ so that when we reduce modulo $\mathfrak{p}$ they do not all become zero. Showing this requires the following lemma.

Lemma 3.17. *Let A and B be non-zero ideals in a Dedekind domain R with $B \subset A$ and $A \neq R$. Then, there exists $\gamma \in K$ such that $\gamma B \subset R$ with $\gamma B \not\subset A$.*

Proof. Using Theorem 3.4, there exists a non-zero ideal C such that $BC = (\alpha)$ for some $\alpha \in R$. Therefore, $BC \not\subset \alpha A$. Fix any $\beta \in C$ such that $\beta B \not\subset \alpha A$ and set $\gamma = \beta/\alpha$. □

To conclude, choose $A = \mathfrak{p}$ and $B = (c_1, \ldots, c_{n+1})$ and use the above lemma, then there exists $\gamma \in K$ such that $\gamma(c_1, \ldots, c_{n+1}) \subset \mathcal{O}_K$ with $\gamma B \not\subset \mathfrak{p}$. In particular, this implies that $\gamma c_i \in \mathcal{O}_K$ for all $1 \le i \le n+1$ and there exists j such that $\gamma c_j \notin \mathfrak{p}$. Hence, the vector space is at most n-dimensional.

To establish equality, suppose $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ and consider all the primes $\mathfrak{p}_i$ of $\mathcal{O}_K$ lying over p. We have just shown that $\mathcal{O}_L/\mathfrak{p}_i\mathcal{O}_L$ is a vector space over $\mathcal{O}_K/\mathfrak{p}_i$ of dimension $n_i \le n$. Now, we will show that equality holds for all i and hence in particular for $\mathfrak{p}_i = \mathfrak{p}$. Let $e_i = e(\mathfrak{p}_i|p)$ and $f_i = f(\mathfrak{p}_i|p)$ then using the special case of Theorem 3.15 we obtain that $\sum e_i f_i = m$ where $m = [K : \mathbb{Q}]$. Moreover, $p\mathcal{O}_K = \prod \mathfrak{p}_i^{e_i}$ and hence $p\mathcal{O}_L = \prod (\mathfrak{p}_i\mathcal{O}_L)^{e_i}$. Using Theorem 3.16*(a)*, we obtain that:

$$\|p\mathcal{O}_L\| = \prod \|\mathfrak{p}_i\mathcal{O}_L\|^{e_i} = \prod \|\mathfrak{p}_i\|^{n_i e_i} = \prod (p^{f_i})^{n_i e_i}$$

On the left, $\|p\mathcal{O}_L\| = p^{mn}$ by the same argument as in the proof of the special case of Theorem 3.15. Therefore, $mn = \sum f_i n_i e_i$. Since $n_i \le n$ and $\sum e_i f_i = m$ it follows that $n_i = n$ for all i. □

Proof of Theorem 3.15, general case. Let $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}$ then:

$$\|\mathfrak{p}\mathcal{O}_L\| = \prod \|\mathfrak{P}_i\|^{e_i} = \prod \|\mathfrak{p}\|^{f_i e_i}$$

Here, the first equality is due to Theorem 3.16*(a)* and the second equality used the definition of f_i. Moreover, Theorem 3.16*(b)* gives that $\|\mathfrak{p}\mathcal{O}_L\| = \|\mathfrak{p}\|^n$. Therefore, $n = \sum e_i f_i$. □

Proof of Theorem 3.16(c). Let $n = [K : \mathbb{Q}]$. Consider an extension M of K that is normal over $\mathbb{Q}$. For each embedding σ of K into $\mathbb{C}$, we can extend it into a Galois automorphism of M, then:

$$\|\sigma(\alpha)\mathcal{O}_M\| = \|\alpha\mathcal{O}_M\|$$

Let $N = \mathrm{N}_{\mathbb{Q}}^K(\alpha)$. Then, using Theorem 3.16*(a)*, we obtain that:

$$\|N\mathcal{O}_M\| = \prod_\sigma \|\sigma(\alpha)\mathcal{O}_M\| = \|\alpha\mathcal{O}_M\|^n$$

Now, using Theorem 3.16*(b)* twice, we obtain both that $\|N\mathcal{O}_M\| = |N|^{nm}$ and $\|\alpha\mathcal{O}_M\| = \|\alpha\mathcal{O}_K\|^m$ where $m = [M : K]$. Putting it all together: $|N| = \|\alpha\mathcal{O}_K\|$. □

Let L be a Galois extension of K and $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, then the Galois group $G = \mathrm{Gal}(L/K)$ permutes the primes lying over $\mathfrak{p}$. If $\mathfrak{P}$ is a prime lying over $\mathfrak{p}$ and $\sigma \in G$, then $\sigma(\mathfrak{P})$ is a prime ideal in $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ lying over $\sigma(\mathfrak{p}) = \mathfrak{p}$. Moreover, the following theorem shows that this action is transitive.

Theorem 3.18. *Let L be a Galois extension over K, and $\mathfrak{P}$ and $\mathfrak{P}'$ be two primes of $\mathcal{O}_L$ lying over the same prime $\mathfrak{p}$ of $\mathcal{O}_K$, then there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Proof. Suppose $\mathfrak{P}$ and $\mathfrak{P}'$ are two primes that contain $\mathfrak{p}$. Suppose $\mathfrak{P}' \neq \sigma(\mathfrak{P})$ for all $\sigma \in G$. Using the Chinese Remainder Theorem, there exists a solution to the following system of congruences:

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{P}'} \\ x &\equiv 1 \pmod{\sigma(\mathfrak{P})} \qquad \text{(for all } \sigma \in G\text{)} \end{aligned}$$

Let $\alpha \in \mathcal{O}_L$ be solution, then $\mathrm{N}_K^L(\alpha) \in \mathcal{O}_K \cap \mathfrak{P}' = \mathfrak{p}$ since one of the factors of the norm is $\alpha \in \mathfrak{P}'$. However, we chose α such that $\alpha \notin \sigma(\mathfrak{P})$ for all $\sigma \in G$ and hence $\sigma^{-1}(\alpha) \notin \mathfrak{P}$ for all $\sigma \in G$. Now, we can express the norm of α as the product of $\sigma^{-1}(\alpha)$ for all $\sigma \in G$. However, since none of the $\sigma^{-1}(\alpha)$ are in $\mathfrak{P}$ it follows that $\mathrm{N}_K^L(\alpha) \notin \mathfrak{P}$ either. Yet, we have already seen that $\mathrm{N}_K^L(\alpha) \in \mathfrak{p} \subset \mathfrak{P}$. □

Corollary 3.19. *Let L be a Galois extension over K, and $\mathfrak{P}$ and $\mathfrak{P}'$ be two primes of $\mathcal{O}_L$ lying over the same prime $\mathfrak{p}$ of $\mathcal{O}_K$, then $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}'|\mathfrak{p})$ and $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{p})$.*

Proof. Consider $G = \mathrm{Gal}(L/K)$ then $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p})\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^r \sigma(\mathfrak{P}_i)^{e(\mathfrak{P}_i|\mathfrak{p})}$ for all $\sigma \in G$. However, the unique factorization of $\mathfrak{p}$ into prime ideals in $\mathcal{O}_L$ together with the transitive action of the Galois group on the primes lying over $\mathfrak{p}$ implies that there exists $e = e(\mathfrak{P}_i|\mathfrak{p})$ for all $1 \leq i \leq r$. Next, we show that there exists a single $f = f(\mathfrak{P}_i|\mathfrak{p})$ for all $1 \leq i \leq r$. Consider two primes $\mathfrak{P}$ and $\mathfrak{P}'$ lying over $\mathfrak{p}$ with $\mathfrak{P}' = \sigma(\mathfrak{P})$ and we will show that there is an isomorphism $\mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}'$. First,

notice that $\sigma : \mathcal{O}_L \to \mathcal{O}_L$ is an automorphism, and hence the composition $\tau : \mathcal{O}_L \xrightarrow{\sigma} \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}'$ is a surjective homomorphism. We show that $\ker(\tau) = \mathfrak{P}$. Clearly, $\mathfrak{P} \subset \ker(\tau)$. Suppose $x \in \ker(\tau)$ then $\sigma(x) \in \mathfrak{P}'$ and hence $x \in \sigma^{-1}(\mathfrak{P}') = \mathfrak{P}$. Therefore, $\mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}'$ is an isomorphism. □

Corollary 3.19 shows that if L is a Galois extension over K, then a prime $\mathfrak{p}$ of $\mathcal{O}_K$ factors into $(\mathfrak{P}_1 \dots \mathfrak{P}_r)^e$ in $\mathcal{O}_L$ where the $\mathfrak{P}_i$ are distinct primes, all sharing the same inertial degree f over $\mathfrak{p}$. Therefore, in the Galois case, Corollary 3.19 implies the following simplification for Theorem 3.15:

$$n = efr$$

Theorem 3.20. *Let K be a Galois extension over $\mathbb{Q}$ with $G = \mathrm{Gal}(K/\mathbb{Q})$, then for an ideal $\mathfrak{a} \subset \mathcal{O}_K$:*

$$\prod_{\sigma \in G} \sigma(\mathfrak{a}) = (\|\mathfrak{a}\|)$$

Proof. It suffices to show the equation for $\mathfrak{a}$ being a prime ideal $\mathfrak{p}$ because both sides of the equation are multiplicative on ideal products. Let $\mathfrak{p}_1$ be a prime lying over the rational prime p, then:

$$p\mathcal{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^e$$

Let f be the shared inertial degree of the $\mathfrak{p}_i$ over p, then by definition:

$$(\|\mathfrak{p}_1\|) = (|\mathcal{O}_K/\mathfrak{p}_1|) = (p^f)$$

Finally, the following chain of equalities gives the result:

$$\prod_{\sigma \in G} \sigma(\mathfrak{p}_1) = \left(\prod_{i=1}^{r} \mathfrak{p}_i \right)^{ef} = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^{ef} = (p\mathcal{O}_K)^f = (p)^f = (p^f) = (\|\mathfrak{p}_1\|)$$

The first equality might seem a little suspicious. Let us define the *decomposition group* of $\mathfrak{p}_1$ as:

$$D_{\mathfrak{p}_1} = \{\sigma \in G : \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\}$$

For each $\sigma \in G$, the coset $\sigma D_{\mathfrak{p}_1}$ sends $\mathfrak{p}_1$ to $\sigma(\mathfrak{p}_1)$. The cosets $\{\sigma D_{\mathfrak{p}_1}\}$ form a partition of G, and moreover, there are exactly r cosets corresponding to each prime $\mathfrak{p}_i$ lying over p. Therefore, we conclude using group theory that the size of each coset is $n/r = ef$. This shows the first equality. □

Theorem 3.21. *An ideal whose norm is prime in $\mathbb{Z}$ is a prime ideal.*

Proof. Let $\|\mathfrak{a}\| = p$ be prime. If $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, then taking the norms on both sides we get $p = \|\mathfrak{a}\| = \|\mathfrak{b}\|\|\mathfrak{c}\|$. Since p is prime, either $\mathfrak{b}$ or $\mathfrak{c}$ is the ideal (1). This is it. □

Theorem 3.22. *Let $\mathfrak{a} = (\alpha, \beta)$ be an ideal in $\mathcal{O}_K$ with two generators. Then*

$$\mathfrak{a}\overline{\mathfrak{a}} = (\mathrm{N}_{\mathbb{Q}}^K(\alpha), \mathrm{Tr}_{\mathbb{Q}}^K(\alpha\overline{\beta}), \mathrm{N}_{\mathbb{Q}}^K(\beta))$$

Finally, we are ready to state and prove the Kummer-Dedekind Theorem.

Theorem 3.23 (Kummer-Dedekind)**.** *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with square-free d and $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $f(X)$ being the quadratic polynomial having ω and $\overline{\omega}$ as roots:*

$$f(X) = \begin{cases} X^2 - d & \text{if } d \not\equiv 1 \pmod 4 \\ X^2 - X + \frac{1-d}{4} & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

For each prime number p, how (p) factors in $\mathcal{O}_K$ matches how $f(X)$ factors modulo p:

(1) If $f(X) \pmod p$ is irreducible then (p) is prime in $\mathcal{O}_K$ with norm p^2.
(2) If $f(X) \equiv (X-c)(X-c') \pmod p$ with $c \not\equiv c' \pmod p$ then $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ where $\mathfrak{p} \neq \overline{\mathfrak{p}}$ and the conjugate ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ both have norm p.
(3) If $f(X) = (X-c)^2 \pmod p$ then $(p) = \mathfrak{p}^2$ and $\|\mathfrak{p}\| = p$.

In particular, prime ideals in $\mathcal{O}_K$ have prime norm except for principal ideals (p) where p is a prime number such that $f(X) \pmod p$ is irreducible.

Proof. See that $\mathcal{O}_K = \mathbb{Z}[\omega] \cong \mathbb{Z}[X]/(f(X))$ then consider the following sequence of isomorphisms:

$$\mathcal{O}_K/(p) \cong \mathbb{Z}[X]/(p, f(X)) \cong (\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$$

This is the key observation. We will be comparing the ring structures of $\mathcal{O}_K/(p)$ and $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$ to see that the way (p) factors in $\mathcal{O}_K$ resembles the way that $f(X)$ factors in $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$.

First, suppose that $f(X) \pmod p$ is irreducible, then $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$ is a field. Next, suppose that $f(X) \equiv (X-c)(X-c') \pmod p$ with $c \not\equiv c' \pmod p$ then $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$ factors as:

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})[X]/(f(X)) &\cong (\mathbb{Z}/p\mathbb{Z})[X]/(X-c) \times (\mathbb{Z}/p\mathbb{Z})[X]/(X-c') \\ &\cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})\end{aligned}$$

Here, $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$ is the direct product of two fields, which is not a field, and has no non-zero nilpotent elements. Finally, suppose that $f(X) \equiv (X-c)^2 \pmod p$ then $(\mathbb{Z}/p\mathbb{Z})[X]/(X-c)^2$ has a non-zero nilpotent element: $(X-c) \pmod{(X-c)^2}$. Therefore, the way that $f(X)$ factors in $(\mathbb{Z}/p\mathbb{Z})[X]$ is reflected in the ring structure of $(\mathbb{Z}/p\mathbb{Z})[X]/(f(X))$.

The ring $\mathcal{O}_K/(p)$ is a field if and only if (p) is a maximal ideal, and this is equivalent to (p) being a prime ideal since $(p) \neq (0)$. Therefore, based on our discussion, we can immediately conclude that $f(X) \pmod p$ is irreducible if and only if (p) is a prime ideal in $\mathcal{O}_K$.

Now, suppose that (p) is not prime, then $(p) = \mathfrak{a}\mathfrak{b}$ where neither $\mathfrak{a}$ nor $\mathfrak{b}$ is equal to (1). We saw in the proof of Theorem 3.15 that $\|(p)\| = p^2$. Taking norms on both sides, we get that $p^2 = \|(p)\| = \|\mathfrak{a}\|\|\mathfrak{b}\|$. Therefore, both $\mathfrak{a}$ and $\mathfrak{b}$ have norm p and are prime ideals. Using Theorem 3.20, since $\|\mathfrak{a}\| = p$, we obtain that $(p) = (\|\mathfrak{a}\|) = \mathfrak{a}\overline{\mathfrak{a}}$, and hence, by unique factorization, we have that $\mathfrak{b} = \overline{\mathfrak{a}}$. Let us write $\mathfrak{a}$ as $\mathfrak{p}$ since it is a prime ideal. Now, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, but we do not know whether or not $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are equal.

Suppose that $\mathfrak{p} = \overline{\mathfrak{p}}$ then $\mathcal{O}_K/\mathfrak{p}^2$ has a non-zero nilpotent element: the class of any element in $\mathfrak{p} \setminus \mathfrak{p}^2$. Therefore, $f(X) \equiv (X-c)^2 \pmod p$ for some c. Suppose that $\mathfrak{p} \neq \overline{\mathfrak{p}}$ then $\mathcal{O}_K/\mathfrak{p}\overline{\mathfrak{p}}$ is not a field and has no non-zero nilpotent elements. Suppose that $x^m \equiv 0 \pmod{\mathfrak{p}\overline{\mathfrak{p}}}$, then $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ both divide

$(x^m) = (x)^m$. Hence, $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ both divide (x) by their primality, and moreover, $\mathfrak{p}\overline{\mathfrak{p}} \mid (x)$ since $\mathfrak{p} \neq \overline{\mathfrak{p}}$. Therefore, $x \equiv 0 \pmod{\mathfrak{p}\overline{\mathfrak{p}}}$. Therefore, $f(X) = (X-c)(X-c') \pmod p$ with $c \not\equiv c' \pmod p$. □

Corollary 3.24. *If (p) is not a prime ideal in $\mathcal{O}_K$ then $f(X) \pmod p$ has a root. Suppose that $c \pmod p$ is a root of $f(X) \pmod p$ then $(p, \omega - c)$ is one of the prime ideals that divide (p).*

Proof. Let $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ by Theorem 3.23. Consider $\mathfrak{a} = (p, \omega - c)$. Since $p \in \mathfrak{a}$ we have that $\mathfrak{a} \mid (p)$. Moreover, we know that $\omega - c \notin (p)$. Suppose instead that $\omega - c \in (p)$ for a contradiction then $X - c \in (f(X), p)$ along the natural surjection $\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\omega]$. It follows that $(X-c, p) \subset (f(X), p)$ and hence there is another surjection $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[X]/(X-c, p) \twoheadrightarrow \mathbb{Z}[X]/(f(X), p) \cong \mathbb{Z}[\omega]/(p)$. Suppose $\mathbb{Z}[\omega]/(p) \cong \mathbb{Z}/p\mathbb{Z}$ then this contradicts that (p) is not prime in $\mathbb{Z}[\omega]$. Moreover, $\mathbb{Z}[\omega]/(p) \neq \{0\}$ because $\mathbb{Z}[\omega]/(p) \cong \mathbb{Z}[X]/(f(X), p) \cong \mathbb{Z}/p\mathbb{Z}[X]/(f(X))$ is the trivial ring if and only if $f(X)$ is a non-zero constant modulo p. However, $f(X)$ is monic and hence this is impossible. Therefore, $\omega - c \notin (p)$, and hence $\mathfrak{a} \neq (p)$. So either $\mathfrak{a}$ is one of the primes dividing (p) or $\mathfrak{a} = (1)$. We show that $\mathfrak{a} \neq (1)$. We look at the norm $\|\mathfrak{a}\|$. Theorem 3.20 and Theorem 3.22 together tell us that $(\|\mathfrak{a}\|) = (\mathrm{N}_{\mathbb{Q}}^K(p), \mathrm{Tr}_{\mathbb{Q}}^K(p(\overline{\omega} - c)), \mathrm{N}_{\mathbb{Q}}^K(\omega - c))$. Therefore, $\|\mathfrak{a}\|$ is divided by the greatest common divisor of the three generators. Let us calculate: $\mathrm{N}_{\mathbb{Q}}^K(p) = p^2$; $\mathrm{Tr}_{\mathbb{Q}}^K(p(\overline{\omega} - c)) = p\,\mathrm{Tr}_{\mathbb{Q}}^K(\overline{\omega} - c)$; $\mathrm{N}_{\mathbb{Q}}^K(\omega - c)) = f(c) \equiv 0 \pmod p$. Since p divides each of them, $p \mid \|\mathfrak{a}\|$ and this implies $\mathfrak{a} \neq (1)$. Therefore, either $\mathfrak{a} = \mathfrak{p}$ or $\mathfrak{a} = \overline{\mathfrak{p}}$. Since $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are symmetric, we can just set $\mathfrak{p} = (p, \omega - c)$. We are done. □

Consider a quadratic polynomial $aX^2 + bX + c$ with a, b, c integers. The solutions to this polynomial in a finite field $\mathbb{F}_p$ for $p \neq 2$ (so that $2 \not\equiv 0$) are described by the usual quadratic formula:

$$X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The reason for this is that the proof of the quadratic formula in $\mathbb{F}_p$ is essentially the same as its proofs over more familiar fields such as $\mathbb{R}$ or $\mathbb{C}$. Let us call $\Delta = b^2 - 4ac$ the *discriminant* of $aX^2 + bX + c$. This polynomial has two distinct solutions if Δ is a non-zero square modulo p; a single repeated solution if $\Delta \equiv 0 \pmod p$; and no solutions if Δ is not a square modulo p. To see that the two solutions are in fact distinct in the first case, suppose instead that $x + y \equiv x - y \pmod p$ then $2y \equiv 0 \pmod p$ and this implies that $y \equiv 0 \pmod p$ since $p \neq 2$. This contradicts that Δ is non-zero.

The discriminant of the minimal polynomial $f(X)$ of ω is either d or $4d$. Therefore, whether or not the discriminant of $f(X)$ is a square modulo p is equivalent to whether or not d is a square modulo p. Consider the *Legendre symbol* of an integer a and a prime p to be defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a non-zero square modulo } p \\ 0 & \text{if } a \equiv 0 \pmod p \\ -1 & \text{if } a \text{ is not a square modulo } p \end{cases}$$

Thus, our entire discussion can be succinctly summarized in the following table for $p \neq 2$.

$(\frac{d}{p})$	(p)	$\mathfrak{p}$
1	$\mathfrak{p}\overline{\mathfrak{p}}$	$(p, \omega - c)$
-1	$\mathfrak{p}$	(p)
0	$\mathfrak{p}^2$	$(p, \omega - c)$

On the other hand, suppose $p = 2$ then $f(X) \pmod 2$ can only be one of the following: X^2, $X^2 + 1$, $X^2 + X$ and $X^2 + X + 1$. Moreover, $X^2 + X + 1$ is irreducible, $X^2 + X = X(X + 1)$ has distinct roots, and $X^2 = X \cdot X$ and $X^2 + 1 = (X + 1)(X + 1)$ both contain repeated roots. Now, a meticulous analysis of these four cases will show that how $f(X)$ factors modulo 2 depends exactly on $d \pmod 8$. The details are omitted, but the results for $p = 2$ are summarized in the following table.

$d \pmod 8$	(2)	$\mathfrak{p}$
1	$\mathfrak{p}\overline{\mathfrak{p}}$	$(2, \frac{1+\sqrt{d}}{2})$
5	$\mathfrak{p}$	(2)
$3, 7$	$\mathfrak{p}^2$	$(2, \sqrt{d} - 1)$
even	$\mathfrak{p}^2$	$(2, \sqrt{d})$

4. Quadratic reciprocity

Let K and L be number fields and assume that L is a Galois extension of K with degree $n = [L : K]$. Let $G = \mathrm{Gal}(L/K)$ be the Galois group of L/K. Consider a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ and another prime ideal $\mathfrak{P}$ in $\mathcal{O}_L$ that lies over $\mathfrak{p}$. Let us define the following two subgroups of G:

$$D = D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\} \qquad \text{(Decomposition group at } \mathfrak{P})$$

$$E = E(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathcal{O}_L\} \qquad \text{(Inertia group at } \mathfrak{P})$$

Indeed, both D and E are actually subgroups of G. Moreover, $E \subset D$. To see this, let $\sigma \in E$ then the condition $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$ is equivalent to saying that σ sends the cosets of $\mathfrak{P}$ in $\mathcal{O}_L$ into themselves. Therefore, $\sigma(\mathfrak{P}) \subset \mathfrak{P}$ implies $\mathfrak{P} \subset \sigma^{-1}(\mathfrak{P})$. However, $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$ if and only if $\alpha \equiv \sigma^{-1}(\alpha) \pmod{\mathfrak{P}}$. Therefore, $\mathfrak{P} \subset \sigma^{-1}(\mathfrak{P}) \subset \mathfrak{P}$ and hence $\sigma(\mathfrak{P}) = \mathfrak{P}$. This implies that $\sigma \in D$.

Next, we show that the elements of D induce automorphisms of the field $\mathcal{O}_L/\mathfrak{P}$ in a natural way. Every $\sigma \in G$ restricts to an automorphism of $\mathcal{O}_L$ since $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Moreover, for every $\sigma \in D$, the composition map $\mathcal{O}_L \xrightarrow{\sigma} \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$ has kernel $\mathfrak{P}$. Hence, every $\sigma \in D$ induces the unique automorphism $\overline{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$ via the first isomorphism theorem:

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\quad\sigma\quad} & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \mathcal{O}_L/\mathfrak{P} & \xrightarrow{\quad\overline{\sigma}\quad} & \mathcal{O}_L/\mathfrak{P} \end{array}$$

Moreover, $\overline{\sigma}$ fixes the subfield $\mathcal{O}_K/\mathfrak{p}$ pointwise since σ fixes K pointwise. Therefore, $\overline{\sigma}$ is an element of the Galois group $\overline{G}$ of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$. In other words, we constructed a well-defined map $D \to \overline{G}$.

In fact, the map $D \to \overline{G}$ is a group homomorphism. To see this, observe that in the following diagram the uniqueness of the induced maps of the first isomorphism theorem implies that $\overline{\tau\sigma} = \overline{\tau} \circ \overline{\sigma}$.

$$\begin{array}{ccccc}
\mathcal{O}_L/\mathfrak{P} & & \xrightarrow{\quad\overline{\tau\sigma}\quad} & & \mathcal{O}_L/\mathfrak{P} \\
\uparrow & & & & \uparrow \\
\mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L & \xrightarrow{\tau} & \mathcal{O}_L \\
\downarrow & & \downarrow & & \downarrow \\
\mathcal{O}_L/\mathfrak{P} & \xrightarrow{\overline{\sigma}} & \mathcal{O}_L/\mathfrak{P} & \xrightarrow{\overline{\tau}} & \mathcal{O}_L/\mathfrak{P}
\end{array}$$

Clearly, the kernel of the homomorphism $D \to \overline{G}$ is E. Therefore, E is a normal subgroup of D and there is a natural embedding of the quotient group $D/E \to \overline{G}$. Later, we will see that $D \to \overline{G}$ is onto as well, and hence $D/E \to \overline{G}$ defines a group isomorphism. From finite field theory, we know that every finite extension of finite fields is Galois, and moreover, the Galois group is cyclic. Therefore, we conclude that $\overline{G}$ is cyclic of order f and the same must be true for D/E.

Now, let us denote L_D and L_E to be the fixed fields of D and E, respectively. We call L_D the *decomposition field* and L_E the *inertia field*. In general, for any subgroup H of G, we denote L_H to be the fixed field of H. Moreover, for any subset $X \subset L$, we denote $X_H := X \cap L_H$. The behaviour of our notation is as expected. First, we show $(\mathcal{O}_L)_H = \mathcal{O}_{(L_H)}$. Let $\mathbb{A}$ be the set of all algebraic integers.

$$\mathcal{O}_{(L_H)} = \mathbb{A} \cap L_H = \mathbb{A} \cap L \cap L_H = \mathcal{O}_L \cap L_H = \mathcal{O}_L \cap (\mathcal{O}_L)_H = (\mathcal{O}_L)_H$$

Next, $\mathfrak{P}_H = \mathfrak{P} \cap L_H$ is precisely the unique prime of $(\mathcal{O}_L)_H$ that lies under $\mathfrak{P}$. Moreover, it is also immediate that $\mathfrak{P}_H$ is a prime lying over $\mathfrak{p}$ since $\mathfrak{P}_H \cap K = \mathfrak{P} \cap L_H \cap K = \mathfrak{P} \cap K = \mathfrak{p}$. Finally, it is clear from our discussion that $(\mathcal{O}_L)_H/\mathfrak{P}_H$ is an intermediate field between $\mathcal{O}_L/\mathfrak{P}$ and $\mathcal{O}_K/\mathfrak{p}$.

Theorem 4.1. *Let r be the number of primes in $\mathcal{O}_L$ lying above $\mathfrak{p}$. Let e and f be their shared ramification and inertial indices, respectively. Then, the following is true.*

DEGREES			RAMIFICATION INDICES	INERTIAL DEGREES
	L	$\mathfrak{P}$		
e			e	1
	L_E	$\mathfrak{P}_E$		
f			1	f
	L_D	$\mathfrak{P}_D$		
r			1	1
	K	$\mathfrak{p}$		

Proof. First, let us show that $[L_D : K] = r$. Galois theory gives us that $[L_D : K]$ is equal to the index of D in G. Therefore, it suffices to find the index of D in G. For each $\sigma \in G$, every element in the left coset σD sends $\mathfrak{P}$ to $\sigma\mathfrak{P}$. Moreover, there is a bijection of the left cosets σD and the primes $\sigma\mathfrak{P}$.

$$(\sigma D = \tau D) \Leftrightarrow (\tau^{-1}\sigma D = D) \Leftrightarrow (\tau^{-1}\sigma Q = Q) \Leftrightarrow (\sigma Q = \tau Q)$$

Using Theorem 3.18, these primes include all of the primes in $\mathcal{O}_L$ that lie over $\mathfrak{p}$. There are r of them.

Next, we show that $e(\mathfrak{P}_D|\mathfrak{p})$ and $f(\mathfrak{P}_D|\mathfrak{p})$ are both 1. First, we claim that $\mathfrak{P}$ is the only prime of $\mathcal{O}_L$ that lies over $\mathfrak{P}_D$. To see this, recall that the primes of $\mathcal{O}_L$ that lie over $\mathfrak{P}_D$ are permuted transitively by the Galois group of L over L_D. This Galois group is D. However, every element in D fixes $\mathfrak{P}$.

$$[L : L_D] = e(\mathfrak{P}|\mathfrak{P}_D)f(\mathfrak{P}|\mathfrak{P}_D)$$

The left hand side is equal to ef since we just showed that $[L_D : K] = r$ and we know that $n = efr$. Moreover, both $e(\mathfrak{P}|\mathfrak{P}_D) \leq e$ and $f(\mathfrak{P}|\mathfrak{P}_D) \leq f$ and hence necessarily $e(\mathfrak{P}|\mathfrak{P}_D) = e$ and $f(\mathfrak{P}|\mathfrak{P}_D) = f$.

$$e(\mathfrak{P}_D|\mathfrak{p}) = f(\mathfrak{P}_D|\mathfrak{p}) = 1$$

Next, we show that $f(\mathfrak{P}|\mathfrak{P}_E) = 1$. Equivalently, this means that $\mathcal{O}_L/\mathfrak{P}$ is a trivial extension of $(\mathcal{O}_L)_E/\mathfrak{P}_E$. Indeed, since every finite extension of finite fields is Galois, it suffices to show that the Galois group of $\mathcal{O}_L/\mathfrak{P}$ over $(\mathcal{O}_L)_E/\mathfrak{P}_E$ is trivial. We will show that for each $\theta \in \mathcal{O}_L/\mathfrak{P}$ there exists an integer $m \geq 1$ such that the polynomial $(X - \theta)^m$ has coefficients in $(\mathcal{O}_L)_E/\mathfrak{P}_E$. Thus, it will follow that since the Galois group fixes the polynomial, every member of the Galois group must send θ to another root of $(X - \theta)^m$ which can only be θ. Let us show that this is true.

Consider $\theta \in \mathcal{O}_L/\mathfrak{P}$ and choose any lift $\alpha \in \mathcal{O}_L$ of θ into $\mathcal{O}_L$. Consider the following polynomial.

$$g(X) = \prod_{\sigma \in E} (X - \sigma(\alpha))$$

Here, E is the Galois group of L over L_E. Therefore, $g(X)$ is the minimal polynomial of α with coefficients in L_E. In fact, since $\alpha \in \mathcal{O}_L$ the coefficients of $g(X)$ are in particular elements of $(\mathcal{O}_L)_E$. Now, let us reduce the coefficients of $g(X)$ modulo $\mathfrak{P}$. Indeed, after reduction, we find that our polynomial $\overline{g}(X) \in (\mathcal{O}_L/\mathfrak{P})[X]$ has coefficients in $(\mathcal{O}_L)_E/\mathfrak{P}_E$. Moreover, every one of the $\sigma(\alpha)$ reduce to $\theta \pmod{\mathfrak{P}}$ because $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$ for all $\sigma \in E$ and α was chosen such that $\alpha \equiv \theta \pmod{\mathfrak{P}}$. Therefore, $\overline{g}(X) = (X - \theta)^m$ with $m = |E|$. This completes the proof that $f(\mathfrak{P}|\mathfrak{P}_E) = 1$.

Finally, we tie up the loose ends. We just showed $f(\mathfrak{P}|\mathfrak{P}_E) = 1$ which together with $f(\mathfrak{P}_D|\mathfrak{p}) = 1$ implies that $f(\mathfrak{P}_E|\mathfrak{P}_D) = f(\mathfrak{P}|\mathfrak{p}) = f$. Therefore, also $[L_E : L_D] \geq f$. We have seen that D/E admits an embedding into $\overline{G}$ which is a group of order f, and hence $[L_E : L_D] = |D/E| \leq f$. Therefore, also $e(\mathfrak{P}_E|\mathfrak{P}_D) = 1$. Finally, we can obtain that $[L : L_E] = e$ and $e(\mathfrak{P}|\mathfrak{P}_E) = e$ by considering the facts that we have already established. This concludes the proof. □

Corollary 4.2. *The group D maps onto $\overline{G}$ via the natural mapping $\sigma \mapsto \overline{\sigma}$ with kernel E. Therefore, D/E is a cyclic group of f.*

Proof. We have already seen that D/E admits an embedding into $\overline{G}$. Now, we know that both groups have order f since $|D/E| = [L_E : L_D] = f$. This is it. □

Corollary 4.3. *Suppose that D is a normal subgroup of G, then $\mathfrak{p}$ splits into r distinct primes in L_D. If E is also a normal subgroup in G, then each of them remains prime (is "inert") in L_E. Finally, each one becomes an e^{th} power in L.*

Proof. If D is normal in G then L_D is a Galois extension of K. We know that the ramification index and inertial degree for $\mathfrak{P}_D$ over $\mathfrak{p}$ are both 1 and hence the same must be true for every other prime $\mathfrak{P}'$ in L_D that lies over $\mathfrak{p}$. Therefore, there must be exactly r such primes. Next, it follows that there are exactly r primes in L_E that lie over $\mathfrak{p}$ since the same is true in both L_D and L. Therefore, each prime $\mathfrak{P}'$ in L_D lies under a unique prime $\mathfrak{P}''$ in L_E. However, it can still happen that the $\mathfrak{P}''$ are ramified over $\mathfrak{P}'$. If E is normal in G then L_E is a Galois extension of K. Therefore, $e(\mathfrak{P}''|\mathfrak{p}) = e(\mathfrak{P}_E|\mathfrak{p}) = 1$ and this implies that $e(\mathfrak{P}''|\mathfrak{P}') = 1$. This shows that the $\mathfrak{P}'$ are inert in L_E. Finally, each $\mathfrak{P}''$ becomes an e^{th} power in L. We know that each $\mathfrak{P}''$ lies under a unique $\mathfrak{P}'''$ in L. Therefore, we simply calculate that $e(\mathfrak{P}'''|\mathfrak{P}'') = e(\mathfrak{P}'''|\mathfrak{p})/e(\mathfrak{P}''|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p})/e(\mathfrak{P}''|\mathfrak{p}) = e/1 = e$. This is it. □

Consider an intermediate field K' with $K \subset K' \subset L$. We know $K' = L_H$ for a subgroup $H \subset G$. The ring of integers $\mathcal{O}_{K'}$ is $(\mathcal{O}_L)_H$ and $\mathfrak{P}' = \mathfrak{P} \cap K'$ is the unique prime of $\mathcal{O}_{K'}$ that lies under $\mathfrak{P}$. Moreover, $\mathfrak{P}'$ lies (not necessarily uniquely) over $\mathfrak{p}$. We know that L is a Galois extension over K' and hence the decomposition and inertia groups $D(\mathfrak{P}|\mathfrak{P}')$ and $E(\mathfrak{P}|\mathfrak{P}')$ can be considered.

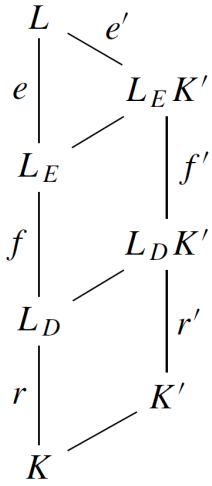
$$D(\mathfrak{P}|\mathfrak{P}') = \{\sigma \in H : \sigma(\mathfrak{P}) = \mathfrak{P}\} = D \cap H$$
$$E(\mathfrak{P}|\mathfrak{P}') = \{\sigma \in H : \sigma(\alpha) = \alpha \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathcal{O}_L\} = E \cap H$$

Here, $D = D(\mathfrak{P}|\mathfrak{p})$ and $E = E(\mathfrak{P}|\mathfrak{p})$ as before. Moreover, using the Galois correspondence, we observe that the decomposition and inertia fields are $L_{D\cap H} = L_D L_H = L_D K'$ and $L_{E\cap H} = L_E L_H = L_E K'$.

Theorem 4.4. *(1) L_D is the largest intermediate field K' such that $e(\mathfrak{P}'|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{p}) = 1$;*
(2) L_D is the smallest K' such that $\mathfrak{P}$ is the only prime of $\mathcal{O}_L$ lying over $\mathfrak{P}'$;
(3) L_E is the largest K' such that $e(\mathfrak{P}'|\mathfrak{p}) = 1$;
(4) L_E is the smallest K' such that $\mathfrak{P}$ is totally ramified over $\mathfrak{P}'$. In other words, $e(\mathfrak{P}|\mathfrak{P}') = [L : K']$.

Proof. First, observe that both L_D and L_E satisfy these properties.

Suppose that $K' = L_H$ is any intermediate field in which $\mathfrak{P}$ is the only prime lying over $\mathfrak{P}'$ then we know that $\sigma(\mathfrak{P}) = \mathfrak{P}$ for all $\sigma \in H$. Therefore, $H \subset D$ and hence $L_D \subset K'$ and this establishes *(2)*.



The result of *(2)* can also be obtained using the above diagram. The diagram is constructed by applying Theorem 4.1 to both situations in which $\mathfrak{P}$ lies over $\mathfrak{p}$ and in which $\mathfrak{P}$ lies over $\mathfrak{P}'$. Thus, r' is the number of primes in $\mathcal{O}_L$ lying over $\mathfrak{P}'$. Therefore, $r' = 1$ implies $K' = L_D K'$ and hence $L_D \subset K'$.

Next, suppose that $e(\mathfrak{P}'|\mathfrak{p}) = 1$ and $f(\mathfrak{P}'|\mathfrak{p}) = 1$ then $e' = e(\mathfrak{P}|\mathfrak{P}') = e$ and $f' = f(\mathfrak{P}|\mathfrak{P}') = f$. Considering the diagram, one finds that $[L_D : L] = ef = e'f' = [L_D K' : L]$. Therefore, $L_D \subset L_D K'$ implies that in fact $L_D = L_D K'$ and hence $K' \subset L_D$. This establishes *(1)*.

Similarly, suppose that $e(\mathfrak{P}'|\mathfrak{p}) = 1$ then $e' = e(\mathfrak{P}|\mathfrak{P}') = e$. Considering the diagram, one finds that $[L_E : L] = e = e' = [L_E K' : L]$. Therefore, $L_E \subset L_E K'$ implies $L_E = L_E K'$ and hence $K' \subset L_E$.

Finally, suppose that $\mathfrak{P}$ is totally ramified over $\mathfrak{P}'$ then $[L : K'] = e'$. Considering the diagram, one finds that $K' = L_E K'$ and hence $L_E \subset K'$. This establishes *(4)*. □

We are almost ready to prove the theorem of quadratic reciprocity. A prime $\mathfrak{p}$ in a number field K *splits completely* in an extension field F if and only if $\mathfrak{p}$ splits into $[F : K]$ distinct primes.

Corollary 4.5. *If D is a normal subgroup of G then $\mathfrak{p}$ splits completely in K' if and only if $K' \subset L_D$.*

Proof. Suppose that $\mathfrak{p}$ splits completely in K' then in particular $e(\mathfrak{P}'|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{p}) = 1$. Therefore, using Theorem 4.4, one obtains that $K' \subset L_D$. Conversely, using Corollary 4.3, one obtains that $\mathfrak{p}$ splits completely in L_D. Therefore, $\mathfrak{p}$ splits completely in any subfield K' with $K \subset K' \subset L_D$. □

The last concept that we need to introduce is that of a discriminant. Let $f(X)$ be a monic polynomial of degree n defined over a field K. The fundamental theorem of algebra tells us that $f(X)$ has n roots $r_1, \ldots, r_n$ in an algebraically closed extension of K. The *discriminant of* $f(X)$ is defined to be:

$$\operatorname{disc}(f) = \prod_{i<j} (r_i - r_j)^2$$

We remark that $\operatorname{disc}(f) = 0$ if and only if f has repeated roots. The following proposition gives an alternative method of computing $\operatorname{disc}(f)$ that may be simpler in some circumstances.

Proposition 4.6. $\operatorname{disc}(f) = \pm f'(r_1) \ldots f'(r_n)$

Proof. This proposition is a consequence of the differentiation product rule.

$$f(X) = \prod_{i=1}^{n}(X - r_i) \quad \Longrightarrow \quad f'(X) = \sum_{i=1}^{n}\prod_{j\neq i}(X - r_j)$$
$$\Longrightarrow \quad f'(r_i) = \prod_{j\neq i}(r_i - r_j)$$

For a pair i, j with $i < j$ the factor $\pm(r_i - r_j)$ appears exactly once in each of $f'(r_i)$ and $f'(r_j)$. □

Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K into $\mathbb{C}$. Consider the n-tuple of elements $\alpha_1, \ldots, \alpha_n$ the *discriminant of* $\alpha_1, \ldots, \alpha_n$ is defined to be:

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2$$

In other words, the discriminant of $\alpha_1, \ldots, \alpha_n$ is the square of the determinant of the matrix with $\sigma_i(\alpha_j)$ in the i^{th} row and j^{th} column. In general, we write $[a_{ij}]$ to denote the matrix with a_{ij} in the i^{th} row and j^{th} column, and $|a_{ij}|$ to denote its determinant. The following theorem tells us that the discriminant can be expressed in terms of the trace function $\operatorname{Tr}_{\mathbb{Q}}^{K}$ discussed at the beginning.

Theorem 4.7. $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \left|\operatorname{Tr}_{\mathbb{Q}}^{K}(\alpha_i\alpha_j)\right|$

An important consequence of Theorem 4.7 is that $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. Moreover, if all of the $\alpha_1, \ldots, \alpha_n$ are algebraic integers then in fact $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. Similar to the norm and trace functions $\mathrm{N}_{\mathbb{Q}}^{K}$ and $\operatorname{Tr}_{\mathbb{Q}}^{K}$, there is a natural generalization of the discriminant if we replace $\mathbb{Q}$ with an arbitrary number field. However, for our purposes, we will not need this generalization. Next, consider the ring of integers $\mathcal{O}_K$. We know that $\mathcal{O}_K$ is a free abelian group of rank $n = [K : \mathbb{Q}]$. The following theorem tells us that the discriminant of an integral basis does not depend on the choice of basis.

Theorem 4.8. *Let* $\{\beta_1, \ldots, \beta_n\}$ *and* $\{\gamma_1, \ldots, \gamma_n\}$ *be two integral bases for the number ring* $\mathcal{O}_K$ *then* $\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n)$.

Therefore, the discriminant of an integral basis can be seen as an invariant of the number ring $\mathcal{O}_K$. Let us denote this as $\operatorname{disc}(K)$. The following theorem relates the discriminant of a number field $\operatorname{disc}(K)$ to the ramification behaviour of a rational prime $p \in \mathbb{Z}$ in the number ring $\mathcal{O}_K$.

Theorem 4.9. *Let* p *be a prime in* $\mathbb{Z}$ *then* p *is ramified in* $\mathcal{O}_K$ *if and only if* p *divides* $\operatorname{disc}(K)$.

An important consequence of Theorem 4.9 is that only finitely many rational primes can ramify in a number ring. Just for the record, there is a generalization of Theorem 4.9 to arbitrary number field extensions L/K in which one defines the relative discriminant $\Delta_{L/K}$ in a similar way. The generalized theorem states that a prime ideal $\mathfrak{p}$ of K ramifies in L if and only if $\mathfrak{p}$ divides $\Delta_{L/K}$ (or $\mathfrak{p} \subset \Delta_{L/K}$).

Finally, suppose that $\mathcal{O}_K$ is monogenic. In other words, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for a generating element $\alpha \in K$. In this special (and common) case, one has that in fact $\operatorname{disc}(K) = \operatorname{disc}(f)$ with f being the minimal polynomial of α over $\mathbb{Q}$. Now, one can easily see that actually Theorem 4.9 is equivalent to the

statement about ramification in Theorem 3.23 (Kummer-Dedekind). In Theorem 3.23, we saw that a rational prime p ramifies in a quadratic extension if and only if $f(X) \pmod p$ has repeated roots. However, indeed the latter condition is equivalent to $\operatorname{disc}(K) = \operatorname{disc}(f) \equiv 0 \pmod p$.

Proposition 4.10. *Let p be an odd prime, and let $\Phi_p(X)$ be the p^{th} cyclotomic polynomial, then there exists $k \in \mathbb{N}$ such that $\operatorname{disc}(\Phi_p(X))$ divides p^k.*

Proof. Since $\Phi_p(X)$ divides $X^p - 1$ it follows from the definitions that $\operatorname{disc}(\Phi_p(X))$ divides $\operatorname{disc}(X^p - 1)$ as well because the discriminant of a polynomial is defined in terms of its roots. Therefore, it suffices to show that $\operatorname{disc}(X^p - 1)$ is a power of p. This is most easily done using the formula in Proposition 4.6. Let $\omega = e^{2\pi i/p}$. We find that pX^{p-1} is the derivative of $X^p - 1$.

$$\begin{aligned}
\operatorname{disc}(X^p - 1) &= \pm \prod_{j=0}^{p-1} p(\omega^j)^{p-1} \\
&= \pm p^p \prod_{j=0}^{p-1} \omega^{j(p-1)} \\
&= \pm p^p \omega^{p(p-1)^2/2} \\
&= \pm p^p
\end{aligned}$$

□

Let p be an odd prime. Let $\omega = e^{2\pi i/p}$ and consider the cyclotomic field $\mathbb{Q}(\omega)$. We know that the Galois group G of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$. Since p is prime, G is cyclic of order $p-1$ and hence there exists a unique subfield $F_d \subset \mathbb{Q}(\omega)$ with degree d over $\mathbb{Q}$ for every divisor d of $p-1$. In other words, F_d is the fixed field of the unique subgroup of G with order $(p-1)/d$. Moreover, the containment of subfields satisfies that $F_{d_1} \subset F_{d_2}$ if and only if $d_1 \mid d_2$.

Theorem 4.11. *Let p be an odd prime, and let q be any prime not equal to p. Fix a divisor d of $p-1$. Then q is a d^{th} power modulo p if and only if q splits completely in F_d.*

Proof. Let q be a prime not equal to p. We know that q splits into r distinct primes in $\mathbb{Z}[\omega]$. Here, we remark that $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{Q}(\omega)$. Let $\mathfrak{Q}$ be a prime of $\mathbb{Z}[\omega]$ lying over q. Moreover, we know that q does not ramify in $\mathbb{Z}[\omega]$ because q does not divide $\operatorname{disc}(\Phi_p(X))$. In other words, the ramification index $e = 1$ and the inertial subgroup $E \subset G$ is the trivial subgroup.

I claim that the order of $q \in (\mathbb{Z}/p\mathbb{Z})^\times$ is the inertial degree f. To see this, recall that q identifies in the Galois group G as the automorphism $[q]$ that sends $\omega \mapsto \omega^q$. Moreover, recall that there is a group isomorphism $D \simeq D/E \simeq \overline{G}$ where $\overline{G}$ is the Galois group of $\mathbb{Z}[\omega]/\mathfrak{Q}$ over $\mathbb{Z}/q\mathbb{Z}$. The order of $\overline{G}$ is f and we know from finite field theory that $\overline{G}$ is a cyclic group generated by the q^{th} power Frobenius element $(x \mapsto x^q)$. Let $\operatorname{Fr}_q \in D$ be the Frobenius lift of $(x \mapsto x^q)$ into D. It suffices to show $\operatorname{Fr}_q = [q]$.

Let $\mu_p = \{\omega^k : 0 \le k \le p-1\}$ be the subgroup of the p^{th} roots of unity in $\mathbb{Z}[\omega]$. I claim that the order of μ_p is stable under the quotient map $\mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\mathfrak{Q}$. In other words, the quotient map injects

the subgroup μ_p. This follows directly from the fact that $\operatorname{disc}(X^p - 1) = \pm p^p \not\equiv 0 \pmod{\mathfrak{Q}}$. In other words, the entire set of p roots of $X^p - 1$ remain distinct under passing to the quotient. Good.

We know that $\mathrm{Fr}_q = [a]$ for some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. We will show that $a = q$. Suppose that $\mathrm{Fr}_q = [a]$ then $\omega^q \equiv \omega^a \pmod{\mathfrak{Q}}$ for all $\omega \in \mu_p$. Therefore, $\omega^{q-a} \equiv 1 \pmod{\mathfrak{Q}}$ for all $\omega \in \mu_p$. Since the group μ_p is cyclic of order p and remains so inside $\mathbb{Z}[\omega]/\mathfrak{Q}$ we obtain that $p \mid q - a$ and hence $q \equiv a \pmod{p}$. It follows that the automorphisms $\omega \mapsto \omega^a$ and $\omega \mapsto \omega^q$ of $\mathbb{Q}(\omega)$ are the same, and hence $[a] = [q]$. Therefore, the order of $q \in (\mathbb{Z}/p\mathbb{Z})^\times$ is the inertial degree f.

Now, we remark that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p - 1$ and hence the d^{th} powers form the unique subgroup of order $(p-1)/d$ consisting of all the elements whose orders divide $(p-1)/d$. Therefore, the following are all equivalent:

(1) q is a d^{th} power modulo p
(2) $f \mid (p-1)/d$
(3) $d \mid r$
(4) $F_d \subset F_r$

(3) $\Leftrightarrow$ (4) since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic; (2) $\Leftrightarrow$ (3) since $p - 1 = fr$; (1) $\Leftrightarrow$ (2) since the order of q is f and the d^{th} powers form the unique subgroup of order $(p-1)/d$ consisting of all elements whose orders divide $(p-1)/d$. Finally, we observe that F_r is the decomposition field for $\mathfrak{Q}$ over q for any prime $\mathfrak{Q}$ of $\mathbb{Z}[\omega]$ lying over q. This is because the decomposition field must have degree r over $\mathbb{Q}$ and F_r is the only one. Therefore, q is a d^{th} power modulo p is equivalent to $F_d \subset F_r$ which in turn is equivalent to the condition that q splits completely in F_d using Corollary 4.5. □

Proposition 4.12. *Let p be an odd prime, then $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.*

Proof. Suppose that -1 is a square modulo p then $-1 \equiv x^2 \pmod{p}$ for some $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ and hence the order of x is 4. The order of the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p - 1$. Therefore, $4 \mid p - 1$ and this implies that $p \equiv 1 \pmod 4$. In the other direction, we know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$ and hence there is an isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. The Chinese Remainder Theorem tells us that:

$$\mathbb{Z}/(p-1)\mathbb{Z} \simeq \bigoplus_{\substack{q \mid p-1 \\ q \text{ prime}}} \mathbb{Z}/q^{n_q}\mathbb{Z}$$

We assume that $p \equiv 1 \pmod 4$ which is equivalent to $4 \mid p - 1$. Therefore, $n_2 \geq 2$. The element in the direct sum with $2^{n_2 - 1}$ in the $q = 2$ factor and 0 in the other factors is the unique element of order 2 in the cyclic group. Therefore, this element is identified with $-1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ under the isomorphism. Moreover, this element is twice the element with $2^{n_2 - 2}$ in the $q = 2$ factor and 0 in the other factors. Therefore, if we identify this element with $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ then $-1 = x^2 \pmod{p}$. It works. □

Theorem 4.13 (Quadratic Reciprocity)**.** *Let p be an odd prime, then:*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

For odd primes $q \neq p$:

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Proof. Let q be any prime not equal to p then $\left(\frac{q}{p}\right) = 1$ if and only if q splits completely in F_2. We have seen that $\mathbb{Q}(\omega)$ contains $\mathbb{Q}(\sqrt{\pm p})$ with the $+$ sign if and only if $p \equiv 1 \pmod 4$. This must be F_2. Let q be an odd prime. Suppose that $p \equiv q \equiv 3 \pmod 4$, then:

$$\begin{aligned} \left(\frac{q}{p}\right) = 1 &\Leftrightarrow q \text{ splits completely in } \mathbb{Q}(\sqrt{-p}) && \text{(Theorem 4.11)} \\ &\Leftrightarrow \left(\frac{-p}{q}\right) = 1 && \text{(Theorem 3.23)} \\ &\Leftrightarrow \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = 1 \end{aligned}$$

However, $\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right)$. Moreover, $\left(\frac{-1}{q}\right) = -1$ since $q \equiv 3 \pmod 4$. Therefore, $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$. Now, suppose that $p \equiv 1 \pmod 4$, then:

$$\begin{aligned} \left(\frac{q}{p}\right) = 1 &\Leftrightarrow q \text{ splits completely in } \mathbb{Q}(\sqrt{p}) && \text{(Theorem 4.11)} \\ &\Leftrightarrow \left(\frac{p}{q}\right) = 1 && \text{(Theorem 3.23)} \end{aligned}$$

Indeed, if instead $q \equiv 1 \pmod 4$ then the same argument works if we flip the roles of p and q:

$$\begin{aligned} \left(\frac{p}{q}\right) = 1 &\Leftrightarrow p \text{ splits completely in } \mathbb{Q}(\sqrt{q}) && \text{(Theorem 4.11)} \\ &\Leftrightarrow \left(\frac{q}{p}\right) = 1 && \text{(Theorem 3.23)} \end{aligned}$$

Finally, let us consider $q = 2$. The arguments are similar. Suppose that $p \equiv 3 \pmod 4$, then:

$$\begin{aligned} \left(\frac{2}{p}\right) = 1 &\Leftrightarrow 2 \text{ splits completely in } \mathbb{Q}(\sqrt{-p}) && \text{(Theorem 4.11)} \\ &\Leftrightarrow -p \equiv 1 \pmod 8 && \text{(Theorem 3.23)} \end{aligned}$$

On the other hand, suppose that $p \equiv 1 \pmod 4$, then:

$$\begin{aligned} \left(\frac{2}{p}\right) = 1 &\Leftrightarrow 2 \text{ splits completely in } \mathbb{Q}(\sqrt{p}) && \text{(Theorem 4.11)} \\ &\Leftrightarrow p \equiv 1 \pmod 8 && \text{(Theorem 3.23)} \end{aligned}$$

This is the end of the proof of quadratic reciprocity. □

5. Acknowledgements

These notes were completed under the guidance of Peter Xu for the Directed Reading Program at McGill University. I would like to thank Peter for his consistent support which propelled me to finish this set of notes. I would also like to thank Khoi Nguyen for his helpful insights on ring theory.

References

[Con] Keith Conrad. Factoring in quadratic fields.

[Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer International Publishing, 2018.