Chapter 3

Ramification Theory

This chapter introduces ramification theory, which roughly speaking asks the following question: if one takes a prime (ideal) \( p \) in the ring of integers \( \mathcal{O}_K \) of a number field \( K \), what happens when \( p \) is lifted to \( \mathcal{O}_L \), where \( L \) is an extension of \( K \). We know by the work done in the previous chapter that \( p\mathcal{O}_L \) has a factorization as a product of primes, so the question is: will \( p\mathcal{O}_L \) still be a prime? or will it factor somehow?

In order to study the behavior of primes in \( L/K \), we first consider absolute extensions, that is when \( K = \mathbb{Q} \), and define the notions of discriminant, inertial degree and ramification index. We show how the discriminant tells us about ramification. When we are lucky enough to get a “nice” ring of integers \( \mathcal{O}_L \), that is \( \mathcal{O}_L = \mathbb{Z}[\theta] \) for \( \theta \in L \), we give a method to compute the factorization of primes in \( \mathcal{O}_L \). We then generalize the concepts introduced to relative extensions, and study the particular case of Galois extensions.

3.1 Discriminant

Let \( K \) be a number field of degree \( n \). Recall from Corollary 1.8 that there are \( n \) embeddings of \( K \) into \( \mathbb{C} \).

**Definition 3.1.** Let \( K \) be a number field of degree \( n \), and set

\[
\begin{align*}
  r_1 &= \text{number of real embeddings} \\
  r_2 &= \text{number of pairs of complex embeddings}
\end{align*}
\]

The couple \((r_1, r_2)\) is called the **signature** of \( K \). We have that

\[ n = r_1 + 2r_2. \]

**Examples 3.1.**

1. The signature of \( \mathbb{Q} \) is \((1, 0)\).

2. The signature of \( \mathbb{Q}(\sqrt{d}), d > 0 \), is \((2, 0)\).
3. The signature of $Q(\sqrt{d})$, $d < 0$, is $(0, 1)$.

4. The signature of $Q(\sqrt{2})$ is $(1, 1)$.

Let $K$ be a number field of degree $n$, and let $O_K$ be its ring of integers. Let $\sigma_1, \ldots, \sigma_n$ be its $n$ embeddings into $C$. We define the map

$$\sigma : K \rightarrow C^n$$

$$x \mapsto (\sigma_1(x), \ldots, \sigma_n(x)).$$

Since $O_K$ is a free abelian group of rank $n$, we have a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of $O_K$. Let us consider the $n \times n$ matrix $M$ given by

$$M = (\sigma_i(\alpha_j))_{1 \leq i,j \leq n}.$$

The determinant of $M$ is a measure of the density of $O_K$ in $K$ (actually of $K/O_K$). It tells us how sparse the integers of $K$ are. However, $\det(M)$ is only defined up to sign, and is not necessarily in either $R$ or $K$. So instead we consider

$$\det(M^2) = \det(M^tM)$$

$$= \det\left(\sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right)_{i,j}$$

$$= \det(\text{Tr}_{K/Q}(\alpha_i\alpha_j))_{i,j} \in \mathbb{Z},$$

and this does not depend on the choice of a basis.

**Definition 3.2.** Let $\alpha_1, \ldots, \alpha_n \in K$. We define

$$\text{disc}(\alpha_1, \ldots, \alpha_n) = \det(\text{Tr}_{K/Q}(\alpha_i\alpha_j))_{i,j}.$$

In particular, if $\alpha_1, \ldots, \alpha_n$ is any $\mathbb{Z}$-basis of $O_K$, we write $\Delta_K$, and we call discriminant the integer

$$\Delta_K = \det(\text{Tr}_{K/Q}(\alpha_i\alpha_j))_{1 \leq i,j \leq n}.$$

We have that $\Delta_K \neq 0$. This is a consequence of the following lemma.

**Lemma 3.1.** The symmetric bilinear form

$$K \times K \rightarrow \mathbb{Q}$$

$$(x, y) \mapsto \text{Tr}_{K/Q}(xy)$$

is non-degenerate.

**Proof.** Let us assume by contradiction that there exists $0 \neq \alpha \in K$ such that $\text{Tr}_{K/Q}(\alpha\beta) = 0$ for all $\beta \in K$. By taking $\beta = \alpha^{-1}$, we get

$$\text{Tr}_{K/Q}(\alpha\beta) = \text{Tr}_{K/Q}(1) = n \neq 0.$$
3.2. PRIME DECOMPOSITION

Now if we had that $\Delta_K = 0$, there would be a non-zero column vector $(x_1, \ldots, x_n)^t$, $x_i \in \mathbb{Q}$, killed by the matrix $(\text{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{1 \leq i, j \leq n}$. Set $\gamma = \sum_{i=1}^n \alpha_i x_i$, then $\text{Tr}_{K/\mathbb{Q}}(\alpha_j \gamma) = 0$ for each $j$, which is a contradiction by the above lemma.

Example 3.2. Consider the quadratic field $K = \mathbb{Q}(\sqrt{5})$. Its two embeddings into $\mathbb{C}$ are given by

- $\sigma_1: a + b\sqrt{5} \mapsto a + b\sqrt{5}$,
- $\sigma_2: a + b\sqrt{5} \mapsto a - b\sqrt{5}$.

Its ring of integers is $\mathbb{Z}[(1 + \sqrt{5})/2]$, so that the matrix $M$ of embeddings is

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}$$

and its discriminant $\Delta_K$ can be computed by

$$\Delta_K = \det(M^2) = 5.$$

3.2 Prime decomposition

Let $p$ be a prime ideal of $\mathcal{O}$. Then $p \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Indeed, one easily verifies that this is an ideal of $\mathbb{Z}$. Now if $a, b$ are integers with $ab \in p \cap \mathbb{Z}$, then we can use the fact that $p$ is prime to deduce that either $a$ or $b$ belongs to $p$ and thus to $p \cap \mathbb{Z}$ (note that $p \cap \mathbb{Z}$ is a proper ideal since $p \cap \mathbb{Z}$ does not contain 1, and $p \cap \mathbb{Z} \neq \emptyset$, as $N(p) = |\mathcal{O}/p| < \infty$).

Since $p \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, there must exist a prime number $p$ such that $p \cap \mathbb{Z} = p\mathbb{Z}$. We say that $p$ is above $p$.

$$p \subset \mathcal{O}_K \subset K$$

$$p\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q}$$

We call residue field the quotient of a commutative ring by a maximal ideal. Thus the residue field of $p\mathbb{Z}$ is $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. We are now interested in the residue field $\mathcal{O}_K/p$. We show that $\mathcal{O}_K/p$ is a $\mathbb{F}_p$-vector space of finite dimension. Set

$$\phi: \mathbb{Z} \to \mathcal{O}_K \to \mathcal{O}_K/p,$$

where the first arrow is the canonical inclusion $\iota$ of $\mathbb{Z}$ into $\mathcal{O}_K$, and the second arrow is the projection $\pi$, so that $\phi = \pi \circ \iota$. Now the kernel of $\phi$ is given by

$$\ker(\phi) = \{a \in \mathbb{Z} \mid a \in p\} = p \cap \mathbb{Z} = p\mathbb{Z},$$

so that $\phi$ induces an injection of $\mathbb{Z}/p\mathbb{Z}$ into $\mathcal{O}_K/p$, since $\mathbb{Z}/p\mathbb{Z} \simeq \text{Im}(\phi) \subset \mathcal{O}_K/p$.

By Lemma 2.1, $\mathcal{O}_K/p$ is a finite set, thus a finite field which contains $\mathbb{Z}/p\mathbb{Z}$ and we have indeed a finite extension of $\mathbb{F}_p$. 
Definition 3.3. We call inertial degree, and we denote by $f_p$, the dimension of the $\mathbb{F}_p$-vector space $O/\mathfrak{p}$, that is

$$f_p = \dim_{\mathbb{F}_p}(O/\mathfrak{p}).$$

Note that we have

$$N(\mathfrak{p}) = |O/\mathfrak{p}| = |\mathbb{F}_p^{f_p}| = |\mathbb{F}_p|^{f_p} = p^{f_p}.$$

Example 3.3. Consider the quadratic field $K = \mathbb{Q}(i)$, with ring of integers $\mathbb{Z}[i]$, and let us look at the ideal $2\mathbb{Z}[i]$:

$$2\mathbb{Z}[i] = (1 + i)(1 - i)\mathbb{Z}[i] = \mathfrak{p}^2, \quad \mathfrak{p} = (1 + i)\mathbb{Z}[i]$$

since $(-i)(1 + i) = 1 - i$. Furthermore, $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$, so that $\mathfrak{p} = (1 + i)$ is said to be above 2. We have that

$$N(\mathfrak{p}) = N_{K/\mathbb{Q}}(1 + i) = (1 + i)(1 - i) = 2$$

and thus $f_p = 1$. Indeed, the corresponding residue field is

$$O_K/\mathfrak{p} \simeq \mathbb{F}_2.$$

Let us consider again a prime ideal $\mathfrak{p}$ of $O$. We have seen that $\mathfrak{p}$ is above the ideal $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. We can now look the other way round: we start with the prime $p \in \mathbb{Z}$, and look at the ideal $pO$ of $O$. We know that $pO$ has a unique factorization into a product of prime ideals (by all the work done in Chapter 2). Furthermore, we have that $p \subset \mathfrak{p}$, thus $\mathfrak{p}$ has to be one of the factors of $pO$.

Definition 3.4. Let $p \in \mathbb{Z}$ be a prime. Let $\mathfrak{p}$ be a prime ideal of $O$ above $p$. We call ramification index of $p$, and we write $e_p$, the exact power of $\mathfrak{p}$ which divides $pO$.

We say that $p$ is ramified if $e_p_i > 1$ for some $i$. On the contrary, $p$ is non-ramified if

$$pO = p_1^{e_1} \cdots p_g^{e_g},$$

where $e_p_i > 1$ for some $i$. Both the inertial degree and the ramification index are connected via the degree of the number field as follows.

Proposition 3.2. Let $K$ be a number field and $O_K$ its ring of integers. Let $p \in \mathbb{Z}$ and let

$$pO = p_1^{e_p_1} \cdots p_g^{e_p_g}$$

be its factorization in $O$. We have that

$$n = [K : \mathbb{Q}] = \sum_{i=1}^{g} e_p_i f_p_i.$$
3.2. PRIME DECOMPOSITION

Proof. By Lemma 2.1, we have

\[ N(p\mathcal{O}) = |N_{K/Q}(p)| = p^n, \]

where \( n = [K : \mathbb{Q}] \). Since the norm \( N \) is multiplicative (see Corollary 2.12), we deduce that

\[ N(p_1^{e_1} \cdots p_g^{e_g}) = \prod_{i=1}^g N(p_i)^{e_i} = \prod_{i=1}^g p^{f_i e_i}. \]

There is, in general, no straightforward method to compute the factorization of \( p\mathcal{O} \). However, in the case where the ring of integers \( \mathcal{O} \) is of the form \( \mathcal{O} = \mathbb{Z}[\theta] \), we can use the following result.

**Proposition 3.3.** Let \( K \) be a number field, with ring of integers \( \mathcal{O}_K \), and let \( p \) be a prime. Let us assume that there exists \( \theta \) such that \( \mathcal{O} = \mathbb{Z}[\theta] \), and let \( f \) be the minimal polynomial of \( \theta \), whose reduction modulo \( p \) is denoted by \( \bar{f} \). Let

\[ \bar{f}(X) = \prod_{i=1}^g \phi_i(X)^{e_i} \]

be the factorization of \( f(X) \) in \( \mathbb{F}_p[X] \), with \( \phi_i(X) \) coprime and irreducible. We set

\[ p_i = (p, f_i(\theta)) = p\mathcal{O} + f_i(\theta)\mathcal{O} \]

where \( f_i \) is any lift of \( \phi_i \) to \( \mathbb{Z}[X] \), that is \( f_i \equiv \phi_i \mod p \). Then

\[ p\mathcal{O} = p_1^{e_1} \cdots p_g^{e_g} \]

is the factorization of \( p\mathcal{O} \) in \( \mathcal{O} \).

Proof. Let us first notice that we have the following isomorphism

\[ \mathcal{O}/p\mathcal{O} = \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \frac{\mathbb{Z}[X]/f(X)}{p(\mathbb{Z}[X]/f(X))} \cong \mathbb{Z}[X]/(p, f(X)) \cong \mathbb{F}_p[X]/\bar{f}(X), \]

where \( \bar{f} \) denotes \( f \mod p \). Let us call \( A \) the ring

\[ A = \mathbb{F}_p[X]/\bar{f}(X). \]

The inverse of the above isomorphism is given by the evaluation in \( \theta \), namely, if \( \psi(X) \in \mathbb{F}_p[X] \), with \( \psi(X) \mod \bar{f}(X) \in A \), and \( g \in \mathbb{Z}[X] \) such that \( \bar{g} = \psi \), then its preimage is given by \( g(\theta) \). By the Chinese Theorem, recall that we have

\[ A = \mathbb{F}_p[X]/\bar{f}(X) \cong \prod_{i=1}^g \mathbb{F}_p[X]/\phi_i(X)^{e_i}, \]

since by assumption, the ideal \((\bar{f}(X))\) has a prime factorization given by \((\bar{f}(X)) = \prod_{i=1}^g (\phi_i(X))^{e_i} \).
CHAPTER 3. RAMIFICATION THEORY

We are now ready to understand the structure of prime ideals of both \( \mathcal{O}/p\mathcal{O} \) and \( A \), thanks to which we will prove that \( p_i \) as defined in the assumption is prime, that any prime divisor of \( p\mathcal{O} \) is actually one of the \( p_i \), and that the power \( e_i \) appearing in the factorization of \( f \) are bigger or equal to the ramification index \( e_{p_i} \) of \( p_i \). We will then invoke the proposition that we have just proved to show that \( e_i = e_{p_i} \), which will conclude the proof.

By the factorization of \( A \) given above by the Chinese theorem, the maximal ideals of \( A \) are given by \( (\phi_i(X))A \), and the degree of the extension \( A/(\phi_i(X))A \) over \( \mathbb{F}_p \) is the degree of \( \phi_i \). By the isomorphism \( A \simeq \mathcal{O}/p\mathcal{O} \), we get similarly that the maximal ideals of \( \mathcal{O}/p\mathcal{O} \) are the ideals generated by \( f_i(\theta) \mod p\mathcal{O} \).

We consider the projection \( \pi: \mathcal{O} \to \mathcal{O}/p\mathcal{O}. \) We have that

\[
\pi(p_i) = \pi(p\mathcal{O} + f_i(\theta)\mathcal{O}) = f_i(\theta)\mathcal{O} \mod p\mathcal{O}.
\]

Consequently, \( p_i \) is a prime ideal of \( \mathcal{O} \), since \( f_i(\theta)\mathcal{O} \) is. Furthermore, since \( p_i \supset p\mathcal{O} \), we have \( p_i \mid p\mathcal{O} \), and the inertial degree \( f_{p_i} = [\mathcal{O}/p_i : \mathbb{F}_p] \) is the degree of \( \phi_i \), while \( e_{p_i} \) denotes the ramification index of \( p_i \).

Now, every prime ideal \( p \) in the factorization of \( p\mathcal{O} \) is one of the \( p_i \), since the image of \( p \) by \( \pi \) is a maximal ideal of \( \mathcal{O}/p\mathcal{O} \), that is

\[
p\mathcal{O} = p_1^{e_1} \cdots p_g^{e_g}
\]

and we are thus left to look at the ramification index.

The ideal \( \phi_i^e A \) of \( A \) belongs to \( \mathcal{O}/p\mathcal{O} \) via the isomorphism between \( \mathcal{O}/p\mathcal{O} \simeq A \), and its preimage in \( \mathcal{O} \) by \( \pi^{-1} \) contains \( p_i^{e_i} \) (since if \( \alpha \in p_i^{e_i} \), then \( \alpha \) is a sum of products \( \alpha_1 \cdots \alpha_{e_i} \), whose image by \( \pi \) will be a sum of product \( \pi(\alpha_1) \cdots \pi(\alpha_{e_i}) \) with \( \pi(\alpha_i) \in \phi_i A \). In \( \mathcal{O}/p\mathcal{O} \), we have \( 0 = \cap_i^{g} (\phi_i(\theta))^{e_i} \), that is

\[
p\mathcal{O} = \pi^{-1}(0) = \cap_i^{g} \pi^{-1}(\phi_i^e A) \supset \cap_i^{g} p_i^{e_i} = \prod_i^{g} p_i^{e_i}.
\]

We then have that this last product is divided by \( p\mathcal{O} = \prod_i^{g} p_i^{e_i} \), that is \( e_i \geq e_{p_i} \).

Let \( n = [K : \mathbb{Q}] \). To show that we have equality, that is \( e_i = e_{p_i} \), we use the previous proposition:

\[
n = [K : \mathbb{Q}] = \sum_{i=1}^{g} e_{p_i} f_{p_i} \leq \sum_{i=1}^{g} e_i \deg(\phi_i) = \dim_{\mathbb{F}_p}(A) = \dim_{\mathbb{F}_p}(\mathbb{Z}/p\mathbb{Z}^n) = n.
\]

\[\square\]

The above proposition gives a concrete method to compute the factorization of a prime \( p\mathcal{O}_K \):

1. Choose a prime \( p \in \mathbb{Z} \) whose factorization in \( p\mathcal{O}_K \) is to be computed.
2. Let \( f \) be the minimal polynomial of \( \theta \) such that \( \mathcal{O}_K = \mathbb{Z}[\theta] \).
3.2. PRIME DECOMPOSITION

3. Compute the factorization of $\bar{f} = f \mod p$:

$$\bar{f} = \prod_{i=1}^{g} \phi_i(X)^{e_i}.$$  

4. Lift each $\phi_i$ in a polynomial $f_i \in \mathbb{Z}[X]$.

5. Compute $p_i = (p, f_i(\theta))$ by evaluating $f_i$ in $\theta$.

6. The factorization of $p \mathcal{O}$ is given by

$$p \mathcal{O} = p_1^{e_1} \cdots p_g^{e_g}.$$  

**Examples 3.4.**  

1. Let us consider $K = \mathbb{Q}(\sqrt{2})$, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. We want to factorize $5\mathcal{O}_K$. By the above proposition, we compute

$$X^3 - 2 \equiv (X - 3)(X^2 + 3X + 4) \equiv (X + 2)(X^2 - 2X - 1) \mod 5.$$  

We thus get that

$$5\mathcal{O}_K = p_1 p_2, \quad p_1 = (5, 2 + \sqrt{2}), \quad p_2 = (5, \sqrt{4} - 2\sqrt{2} - 1).$$

2. Let us consider $\mathbb{Q}(i)$, with $\mathcal{O}_K = \mathbb{Z}[i]$, and choose $p = 2$. We have $\theta = i$ and $f(X) = X^2 + 1$. We compute the factorization of $f(X) = f(X) \mod 2$:

$$X^2 + 1 \equiv X^2 - 1 \equiv (X - 1)(X + 1) \equiv (X - 1)^2 \mod 2.$$  

We can take any lift of the factors to $\mathbb{Z}[X]$, so we can write

$$2\mathcal{O}_K = (2, i - 1)(2, i + 1) \text{ or } 2 = (2, i - 1)^2$$

which is the same, since $(2, i - 1) = (2, 1 + i)$. Furthermore, since $2 = (1 - i)(1 + i)$, we see that $(2, i - 1) = (1 + i)$, and we recover the result of Example 3.3.

**Definition 3.5.** We say that $p$ is inert if $p \mathcal{O}$ is prime, in which case we have $g = 1$, $e = 1$ and $f = n$. We say that $p$ is totally ramified if $e = n$, $g = 1$, and $f = 1$.

The discriminant of $K$ gives us information on the ramification in $K$.

**Theorem 3.4.** Let $K$ be a number field. If $p$ is ramified, then $p$ divides the discriminant $\Delta_K$.
We are thus left to prove that \( \alpha \notin p\mathcal{O} \). We write
\[
\alpha = b_1\alpha_1 + \ldots + b_n\alpha_n, \quad b_i \in \mathbb{Z}.
\]
Since \( \alpha \notin p\mathcal{O} \), there exists a \( b_i \) which is not divisible by \( p \), say \( b_1 \). Recall that
\[
\Delta_K = \det \begin{pmatrix}
\sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\
\vdots & \ddots & \vdots \\
\sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n)
\end{pmatrix}^2
\]
where \( \sigma_i, \ i = 1, \ldots, n \) are the \( n \) embeddings of \( K \) into \( \mathbb{C} \). Let us replace \( \alpha_1 \) by \( \alpha \), and set
\[
D = \det \begin{pmatrix}
\sigma_1(\alpha) & \ldots & \sigma_1(\alpha_n) \\
\vdots & \ddots & \vdots \\
\sigma_n(\alpha) & \ldots & \sigma_n(\alpha_n)
\end{pmatrix}.
\]
Now \( D \) and \( \Delta_K \) are related by
\[
D = \Delta_K b_1^2,
\]
since \( D \) can be rewritten as
\[
D = \det \begin{pmatrix}
\sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\
\vdots & \ddots & \vdots \\
\sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n)
\end{pmatrix} \begin{pmatrix} b_1 & 0 & \ldots & 0 \\ b_2 & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ b_n & \ldots & 1 \end{pmatrix}^2
\]
We are thus left to prove that \( p \mid D \), since by construction, we have that \( p \) does not divide \( b_1^2 \).

Intuitively, the trick of this proof is to replace proving that \( p \mid \Delta_K \) where we have no clue how the factor \( p \) appears, with proving that \( p \mid D \), where \( D \) has been built on purpose as a function of a suitable \( \alpha \) which we will prove below is such that all its conjugates are above \( p \).

Let \( L \) be the Galois closure of \( K \), that is, \( L \) is a field which contains \( K \), and which is a normal extension of \( \mathbb{Q} \). The conjugates of \( \alpha \) all belong to \( L \). We know that \( \alpha \) belongs to all the primes of \( \mathcal{O}_K \) above \( p \). Similarly, \( \alpha \in K \subseteq L \) belongs to all primes \( \mathfrak{P} \) of \( \mathcal{O}_L \) above \( p \). Indeed, \( \mathfrak{P} \cap \mathcal{O}_K \) is a prime ideal of \( \mathcal{O}_K \) above \( p \), which contains \( \alpha \).

We now fix a prime \( \mathfrak{P} \) above \( p \) in \( \mathcal{O}_L \). Then \( \sigma_i(\mathfrak{P}) \) is also a prime ideal of \( \mathcal{O}_L \) above \( p \) (\( \sigma_i(\mathfrak{P}) \) is in \( L \) since \( L/\mathbb{Q} \) is Galois, \( \sigma_i(\mathfrak{P}) \) is prime since \( \mathfrak{P} \) is, and \( p = \sigma_i(p) \in \sigma_i(\mathfrak{P}) \)). We have that \( \sigma_i(\alpha) \in \mathfrak{P} \) for all \( \sigma_i \), thus the first column of the matrix involves in the computation of \( D \) is in \( \mathfrak{P} \), so that \( D \in \mathfrak{P} \) and \( D \in \mathbb{Z} \), to get
\[
D \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}.
\]
3.3. RELATIVE EXTENSIONS

We have just proved that if \( p \) is ramified, then \( p \mid \Delta_K \). The converse is also true.

**Examples 3.5.**

1. We have seen in Example 3.2 that the discriminant of \( K = \mathbb{Q}(\sqrt{5}) \) is \( \Delta_K = 5 \). This tells us that only 5 is ramified in \( \mathbb{Q}(\sqrt{5}) \).

2. In Example 3.3, we have seen that 2 ramifies in \( K = \mathbb{Q}(i) \). So 2 should appear in \( \Delta_K \). One can actually check that \( \Delta_K = -4 \).

**Corollary 3.5.** There is only a finite number of ramified primes.

*Proof.* The discriminant only has a finite number of divisors. \( \square \)

### 3.3 Relative Extensions

Most of the theory seen so far assumed that the base field is \( \mathbb{Q} \). In most cases, this can be generalized to an arbitrary number field \( K \), in which case we consider a number field extension \( L/K \). This is called a relative extension. By contrast, we may call absolute an extension whose base field is \( \mathbb{Q} \). Below, we will generalize several definitions previously given for absolute extensions to relative extensions.

Let \( K \) be a number field, and let \( L/K \) be a finite extension. We have correspondingly a ring extension \( \mathcal{O}_K \to \mathcal{O}_L \). If \( \mathfrak{P} \) is a prime ideal of \( \mathcal{O}_L \), then \( p = \mathfrak{P} \cap \mathcal{O}_K \) is a prime ideal of \( \mathcal{O}_K \). We say that \( \mathfrak{P} \) is above \( p \). We have a factorization

\[
p\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_{\mathfrak{P}_i/p}},
\]

where \( e_{\mathfrak{P}_i/p} \) is the relative ramification index. The relative inertial degree is given by

\[
f_{\mathfrak{P}_i/p} = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/p].
\]

We still have that

\[
[L : K] = \sum e_{\mathfrak{P}/p} f_{\mathfrak{P}/p}
\]

where the summation is over all \( \mathfrak{P} \) above \( p \).

Let \( M/L/K \) be a tower of finite extensions, and let \( \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'' \) be prime ideals of respectively \( M, L, \) and \( K \). Then we have that

\[
f_{\mathfrak{P}/p} = f_{\mathfrak{P}/\mathfrak{P}', \mathfrak{P}/\mathfrak{P}'}
\]

\[
e_{\mathfrak{P}/p} = e_{\mathfrak{P}/\mathfrak{P}', e_{\mathfrak{P}/\mathfrak{P}'''}}.
\]

Let \( I_K, I_L \) be the groups of fractional ideals of \( K \) and \( L \) respectively. We can also generalize the application norm as follows:

\[
N: \quad I_L \to I_K
\]

\[
\mathfrak{P} \mapsto p^{f_{\mathfrak{P}/p}}.
\]
which is a group homomorphism. This defines a relative norm for ideals, which
is itself an ideal!

In order to generalize the discriminant, we would like to have an \( \mathcal{O}_K \)-basis
of \( \mathcal{O}_L \) (similarly to having a \( \mathbb{Z} \)-basis of \( \mathcal{O}_K \)), however such a basis does not exist
in general. Let \( \alpha_1, \ldots, \alpha_n \) be a \( K \)-basis of \( L \) where \( \alpha_i \in \mathcal{O}_L, \ i = 1, \ldots, n \). We set
\[
disc_{L/K}(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix}
\sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\
\vdots & & \vdots \\
\sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n)
\end{pmatrix}^2
\]
where \( \sigma_i : L \to \mathbb{C} \) are the embeddings of \( L \) into \( \mathbb{C} \) which fix \( K \). We define \( \Delta_{L/K} \) as the ideal generated by all \( \disc_{L/K}(\alpha_1, \ldots, \alpha_n) \). It is called relative
discriminant.

### 3.4 Normal Extensions

Let \( L/K \) be a Galois extension of number fields, with Galois group \( G = \text{Gal}(L/K) \).
Let \( \mathfrak{p} \) be a prime of \( \mathcal{O}_K \). If \( \mathfrak{P} \) is a prime above \( \mathfrak{p} \) in \( \mathcal{O}_L \), and \( \sigma \in G \), then \( \sigma(\mathfrak{P}) \)
is a prime ideal above \( \mathfrak{p} \). Indeed, \( \sigma(\mathfrak{P}) \cap \mathcal{O}_K \subset K \), thus \( \sigma(\mathfrak{P}) \cap \mathcal{O}_K = \mathfrak{P} \cap \mathcal{O}_K \) since \( K \) is fixed by \( \sigma \).

**Theorem 3.6.** Let
\[
p\mathcal{O}_L = \prod_{i=1}^g \mathfrak{P}_i^{e_i}
\]
be the factorization of \( p\mathcal{O}_L \) in \( \mathcal{O}_L \). Then \( G \) acts transitively on the set \( \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\} \).
Furthermore, we have that
\[
e_1 = \ldots = e_g = e \quad \text{where } e_i = e_{\mathfrak{P}_i}\mathfrak{p}
\]
\[
f_1 = \ldots = f_g = f \quad \text{where } f_i = f_{\mathfrak{P}_i}\mathfrak{p}
\]
and
\[
[L : K] = efg.
\]
**Proof.** \( G \) acts transitively. Let \( \mathfrak{P} \) be one of the \( \mathfrak{P}_i \). We need to prove that
there exists \( \sigma \in G \) such that \( \sigma(\mathfrak{P}_j) = \mathfrak{P} \) for \( \mathfrak{P}_j \) any other of the \( \mathfrak{P}_i \). In the proof
of Corollary 2.10, we have seen that there exists \( \beta \in \mathfrak{P} \) such that \( \beta\mathcal{O}_L \mathfrak{P}^{-1} \) is
an integral ideal coprime to \( p\mathcal{O}_L \). The ideal
\[
I = \prod_{\sigma \in G} \sigma(\beta\mathcal{O}_L \mathfrak{P}^{-1})
\]
is an integral ideal of \( \mathcal{O}_L \) (since \( \beta\mathcal{O}_L \mathfrak{P}^{-1} \) is), which is furthermore coprime to
\( p\mathcal{O}_L \) (since \( \sigma(\beta\mathcal{O}_L \mathfrak{P}^{-1}) \) and \( \sigma(p\mathcal{O}_L) \) are coprime and \( \sigma(p\mathcal{O}_L) = \sigma(p)\sigma(\mathcal{O}_L) = p\mathcal{O}_L \).
3.4. NORMAL EXTENSIONS

Thus $I$ can be rewritten as

$$I = \frac{\prod_{\sigma \in G} \sigma(\beta)\mathcal{O}_L}{\prod_{\sigma \in G} \sigma(\mathfrak{P})} = \frac{N_{L/K}(\beta)\mathcal{O}_L}{\prod_{\sigma \in G} \sigma(\mathfrak{P})}$$

and we have that

$$I \prod_{\sigma \in G} \sigma(\mathfrak{P}) = N_{L/K}(\beta)\mathcal{O}_L.$$ 

Since $N_{L/K}(\beta) = \prod_{\sigma \in G} \sigma(\beta)$, $\beta \in \mathfrak{P}$ and one of the $\sigma$ is the identity, we have that $N_{L/K}(\beta) \in \mathfrak{P}$. Furthermore, $N_{L/K}(\beta) \in \mathcal{O}_K$ since $\beta \in \mathcal{O}_L$, and we get that $N_{L/K}(\beta) \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, from which we deduce that $\mathfrak{p}$ divides the right hand side of the above equation, and thus the left hand side. Since $I$ is coprime to $\mathfrak{p}$, we get that $\mathfrak{p}$ divides $\prod_{\sigma \in G} \sigma(\mathfrak{P})$. In other words, using the factorization of $\mathfrak{p}$, we have that

$$\prod_{\sigma \in G} \sigma(\mathfrak{P}) \text{ is divisible by } \mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

and each of the $\mathfrak{P}_i$ has to be among $\{\sigma(\mathfrak{P})\}_{\sigma \in G}$.

**All the ramification indices are equal.** By the first part, we know that there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_k$, $i \neq k$. Now, we have that

$$\sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{g} \sigma(\mathfrak{P}_i)^{e_i} = p\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

where the second equality holds since $\mathfrak{p} \in \mathcal{O}_K$ and $L/K$ is Galois. By comparing the two factorizations of $\mathfrak{p}$ and its conjugates, we get that $e_i = e_L$.

**All the inertial degrees are equal.** This follows from the fact that $\sigma$ induces the following field isomorphism

$$\mathcal{O}_L/\mathfrak{P}_i \simeq \mathcal{O}_L/\sigma(\mathfrak{P}_i).$$

Finally we have that


For now on, let us fix $\mathfrak{P}$ above $\mathfrak{p}$.

**Definition 3.6.** The stabilizer of $\mathfrak{P}$ in $G$ is called the **decomposition group**, given by

$$D = D_{\mathfrak{P}/\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} < G.$$
The index \([G : D]\) must be equal to the number of elements in the orbit \(G\mathfrak{P}\) of \(\mathfrak{P}\) under the action of \(G\), that is \([G : D] = |G\mathfrak{P}|\) (this is the orbit-stabilizer theorem).

By the above theorem, we thus have that \([G : D] = g\), where \(g\) is the number of distinct primes which divide \(p\mathcal{O}_L\). Thus

\[
\begin{align*}
    n &= efg \\
    &= ef\frac{|G|}{|D|}
\end{align*}
\]

and

\[
|D| = ef.
\]

If \(\mathfrak{P}'\) is another prime ideal above \(p\), then the decomposition groups \(D_{\mathfrak{P}/p}\) and \(D_{\mathfrak{P}'/p}\) are conjugate in \(G\) via any Galois automorphism mapping \(\mathfrak{P}\) to \(\mathfrak{P}'\) (in formula, we have that if \(\mathfrak{P}' = \tau(\mathfrak{P})\), then \(\tau D_{\mathfrak{P}/p} \tau^{-1} = D_{\tau(\mathfrak{P})/p}\)).

**Proposition 3.7.** Let \(D = D_{\mathfrak{P}/p}\) be the decomposition group of \(\mathfrak{P}\). The subfield

\[
L^D = \{\alpha \in L \mid \sigma(\alpha) = \alpha, \ \sigma \in D\}
\]

is the smallest subfield \(M\) of \(L\) such that \((\mathfrak{P} \cap \mathcal{O}_M)\mathcal{O}_L\) does not split. It is called the decomposition field of \(\mathfrak{P}\).

**Proof.** We first prove that \(L/L^D\) has the property that \((\mathfrak{P} \cap \mathcal{O}_M)\mathcal{O}_L\) does not split. We then prove its minimality.

We know by Galois theory that \(\text{Gal}(L/L^D)\) is given by \(D\). Furthermore, the extension \(L/L^D\) is Galois since \(L/K\) is. Let \(\Omega = \mathfrak{P} \cap \mathcal{O}_L\) be a prime below \(\mathfrak{P}\).

By Theorem 3.6, we know that \(D\) acts transitively on the set of primes above \(\Omega\), among which is \(\mathfrak{P}\). Now by definition of \(D = D_{\mathfrak{P}/p}\), we know that \(\mathfrak{P}\) is fixed by \(D\). Thus there is only \(\mathfrak{P}\) above \(\Omega\).

Let us now prove the minimality of \(L^D\). Assume that there exists a field \(M\) with \(L/M/K\), such that \(\Omega = \mathfrak{P} \cap \mathcal{O}_M\) has only one prime ideal of \(\mathcal{O}_L\) above it. Then this unique ideal must be \(\mathfrak{P}\), since by definition \(\mathfrak{P}\) is above \(\Omega\). Then \(\text{Gal}(L/M)\) is a subgroup of \(D\), since its elements are fixing \(\mathfrak{P}\). Thus \(M \supset L^D\). \(\square\)
Proposition 3.8. Let \( \Omega \) be the prime of \( L^D \) below \( \mathfrak{P} \). We have that
\[
f_{\Omega/p} = e_{\Omega/p} = 1.
\]
If \( D \) is a normal subgroup of \( G \), then \( p \) is completely split in \( L^D \).

Proof. We know that \([G : D] = g(\mathfrak{P}/p)\) which is equal to \([L^D : K]\) by Galois theory. The previous proposition shows that \( g(\mathfrak{P}/\Omega) = 1 \) (recall that \( g \) counts how many primes are above). Now we compute that
\[
e(\mathfrak{P}/\Omega)f(\mathfrak{P}/\Omega) = \frac{[L : L^D]}{g(\mathfrak{P}/\Omega)} = \frac{[L : L^D]}{[L : K]} = \frac{[L^D : K]}{[L : K]}.
\]
Since we have that
\[
[L : K] = e(\mathfrak{P}/p)f(\mathfrak{P}/p)g(\mathfrak{P}/p)
\]
and \([L^D : K] = g(\mathfrak{P}/p)\), we further get
\[
e(\mathfrak{P}/\Omega)f(\mathfrak{P}/\Omega) = \frac{e(\mathfrak{P}/p)f(\mathfrak{P}/p)g(\mathfrak{P}/p)}{g(\mathfrak{P}/p)} = e(\mathfrak{P}/p)f(\mathfrak{P}/p) = e(\mathfrak{P}/\Omega)f(\mathfrak{P}/\Omega)e(\Omega/p)f(\Omega/p)
\]
where the last equality comes from transitivity. Thus
\[
e(\Omega/p)f(\Omega/p) = 1
\]
and \( e(\Omega/p) = f(\Omega/p) = 1 \) since they are positive integers.

If \( D \) is normal, we have that \( L^D/K \) is Galois. Thus
\[
[L^D : K] = e(\Omega/p)f(\Omega/p)g(\Omega/p) = g(\Omega/p)
\]
and \( p \) completely splits.

\[\square\]
Let $\sigma$ be in $D$. Then $\sigma$ induces an automorphism of $O_L/\mathfrak{P}$ which fixes $O_K/p = \mathbb{F}_p$. That is we get an element $\phi(\sigma) \in \text{Gal}(\mathbb{F}_p/\mathbb{F}_p)$. We have thus constructed a map

$$\phi : D \rightarrow \text{Gal}(\mathbb{F}_p/\mathbb{F}_p).$$

This is a group homomorphism. We know that $\text{Gal}(\mathbb{F}_p/\mathbb{F}_p)$ is cyclic, generated by the Frobenius automorphism defined by

$$\text{Frob}_p(x) = x^q, \quad q = |\mathbb{F}_p|.$$

**Definition 3.7.** The inertia group $I = I_{\mathfrak{p}/p}$ is defined as being the kernel of $\phi$.

**Example 3.6.** Let $K = \mathbb{Q}(i)$ and $O_K = \mathbb{Z}[i]$. We have that $K/\mathbb{Q}$ is a Galois extension, with Galois group $G = \{1, \sigma\}$ where $\sigma : a + ib \mapsto a - ib$.

- We have that
  
  $$(2) = (1 + i)^2 \mathbb{Z}[i],$$

  thus the ramification index is $e = 2$. Since $efg = n = 2$, we have that $f = g = 1$. The residue field is $\mathbb{Z}[i]/(1 + i)\mathbb{Z}[i] = \mathbb{F}_2$. The decomposition group $D$ is $G$ since $\sigma((1 + i)\mathbb{Z}[i]) = (1 + i)\mathbb{Z}[i]$. Since $f = 1$, $\text{Gal}(\mathbb{F}_2/\mathbb{F}_2) = \{1\}$ and $\phi(\sigma) = 1$. Thus the kernel of $\phi$ is $D = G$ and the inertia group is $I = G$.

- We have that
  
  $$(13) = (2 + 3i)(2 - 3i),$$

  thus the ramification index is $e = 1$. Here $D = 1$ for $(2 + 3i)$ since $\sigma((2 + 3i)\mathbb{Z}[i]) \neq (2 - 3i)\mathbb{Z}[i]$. We further have that $g = 2$, thus $efg = 2$ implies that $f = 1$, which as for 2 implies that the inertia group is $I = G$. We have that the residue field for $(2 + 3i)$ is $\mathbb{Z}[i]/(2 + 3i)\mathbb{Z}[i] = \mathbb{F}_{13}$.

- We have that $(7)\mathbb{Z}[i]$ is inert. Thus $D = G$ (the ideal belongs to the base field, which is fixed by the whole Galois group). Since $e = g = 1$, the inertial degree is $f = 2$, and the residue field is $\mathbb{Z}[i]/(7)\mathbb{Z}[i] = \mathbb{F}_{49}$. The Galois group $\text{Gal}(\mathbb{F}_{49}/\mathbb{F}_7) = \{1, \tau\}$ with $\tau : x \mapsto x^7$, $x \in \mathbb{F}_{49}$. Thus the inertia group is $I = \{1\}$.

We can prove that $\phi$ is surjective and thus get the following exact sequence:

$$1 \rightarrow I \rightarrow D \rightarrow \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \rightarrow 1.$$

The decomposition group is so named because it can be used to decompose the field extension $L/K$ into a series of intermediate extensions each of which has a simple factorization behavior at $p$. If we denote by $L^I$ the fixed field of $I$, then the above exact sequence corresponds under Galois theory to the following
3.4. NORMAL EXTENSIONS

Intuitively, this decomposition of the extension says that $L^D / K$ contains all of the factorization of $\mathfrak{p}$ into distinct primes, while the extension $L^I / L^D$ is the source of all the inertial degree in $\mathfrak{P}$ over $\mathfrak{p}$. Finally, the extension $L / L^I$ is responsible for all of the ramification that occurs over $\mathfrak{p}$.

Note that the map $\phi$ plays a special role for further theories, including reciprocity laws and class field theory.

The main definitions and results of this chapter are

- Definition of discriminant, and that a prime ramifies if and only if it divides the discriminant.
- Definition of signature.
- The terminology relative to ramification: prime above/below, inertial degree, ramification index, residue field, ramified, inert, totally ramified, split.
- The method to compute the factorization if $\mathcal{O}_K = \mathbb{Z}[\theta]$.
- The formula $[L : K] = \sum_{i=1}^{g} e_i f_i$.
- The notion of absolute and relative extensions.
- If $L/K$ is Galois, that the Galois group acts transitively on the primes above a given $\mathfrak{p}$, that $[L : K] = efg$, and the concepts of decomposition group and inertia group.