# Contents

# Part I

# Linear Algebra

# Part II

# Field Theory

# Part III

# Ring Theory

# Part IV

# Number Theory

# Chapter 1

# The Trace, the Norm, and the Discriminant

**Definition 1.** A prime number $p \in \mathbb{N}$ is said to be ramified in an algebraic number field $K$ if the prime ideal factorization

$$(p) = p\mathcal{O}_K = \mathfrak{p}_r^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

has some $e_i$ greater than 1. If every $e_i$ equals 1 for $1 \leq i \leq r$, we say $p$ is unramified in $K$.

**Example 1.1.** In $\mathbb{Z}[i]$, 2 ramifies because $(1+i)^2 = (2)$, and it is the only prime to do so.

**Theorem 2.** For an algebraic number field $K$, the primes which ramify are those dividing the integer $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)$. In particular, only finitely many primes ramify.

# Chapter 2

# Dedekind Domain

# Chapter 3

# The Ideal Class Group

**Definition 3** (Fractional Ideals)**.** Let $R$ be a integral domain with fraction field $F$. A fractional ideal is a nonzero $R$-submodule $\mathcal{A} \subseteq F$ such that $d\mathcal{A} \subseteq R$ for some nonzero $d \in A$.

**Remark.** We say integral ideals of $R$ and simply mean ideals of $R$ to distinguish them from fractional ideals which are, despite its name and similarities, not true ideals.

**Definition 4** (Equivalence of Fractional Ideals)**.** Let $R$ be a integral domain. Two fractional ideals $\mathcal{A}$ and $\mathcal{B}$ of $R$ are said to be equivalent if there exist $\alpha$ and $\beta$ in $R$ such that

$$(\alpha)\mathcal{A} = (\beta)\mathcal{B}.$$

In this case, we write $\mathcal{A} \sim \mathcal{B}$ or simply $\mathcal{A} = \mathcal{B}$.

**Proposition 5.** The relation defined above $\mathcal{A} \sim \mathcal{B}$ is indeed a equivalence relation.

*Proof.* Let $\mathcal{A}$ and $\mathcal{B}$ be two fractional ideals of an integral domain $R$. We show that the relation $\mathcal{A} \sim \mathcal{B}$ as defined above is a equivalence relation.

1. **Reflexivity.** Trivially, $(\alpha)\mathcal{A} = (\alpha)\mathcal{A}$ for any $\alpha \in R$, and we have $\mathcal{A} \sim \mathcal{A}$.
2. **Symmetry.** If $\mathcal{A} \sim \mathcal{B}$, then $(\alpha)\mathcal{A} = (\beta)\mathcal{B}$, and again it is trivial that $(\beta)\mathcal{B} = (\alpha)\mathcal{A}$, hence $\mathcal{B} \sim \mathcal{A}$.
3. **Transitivity.** Let $\mathcal{A} \sim \mathcal{B}$ and $\mathcal{B} \sim \mathcal{C}$ hold. There are $\alpha, \beta, \gamma, \theta \in R$ such that

   $$(\alpha)\mathcal{A} = (\beta)\mathcal{B} \quad \text{and} \quad (\gamma)\mathcal{B} = (\theta)\mathcal{C}.$$

   Multiplying both sides of both equalities by $(\gamma)$ and $(\beta)$ respectively yields

   $$(\gamma)(\alpha)\mathcal{A} = (\gamma)(\beta)\mathcal{B} \quad \text{and} \quad (\beta)(\gamma)\mathcal{B} = (\beta)(\theta)\mathcal{C}.$$

   Therefore, we have that $(\alpha\gamma)\mathcal{A} = (\beta\theta)\mathcal{C}$ or in other words $\mathcal{A} \sim \mathcal{C}$.

□

**Definition 6.** Let $K$ be an algebraic number field. The equivalence classes of ideals of $R$ form a group called the ideal class group of $K$ or just class group of $K$, and write it as $\mathrm{Cl}(K)$.

**Theorem 7.** Let $K$ be an algebraic number field.

1. The ideal class group is indeed an abelian group with ideal multiplication as its operation. $[(1)] = [R]$ is the identity element and
2. Each ideal class has an integral ideal representant.
3. The ideal class group is trivial, i.e. $\mathrm{Cl}(K) = [(1)]$, if and only if all fractional ideals in $K$ are principal, which is equivalent to $\mathcal{O}_K$ being a principal ideal domain.
4. The ideal class group of $K$ is finite.

**Remark.**
1. For some integral domains not all fractional ideals are invertible, so not all ideal classes are invertible. In other words, the ideal classes need not be a group for arbitary integral domains.
2. For Dedekind domains fractional ideals are invertible, so the ideal classes form a group, but they need not be finite.
3. For a Dedekind domain $R$, the group $\mathrm{Cl}(R)$ is trivial if and only if $R$ is a principal domain which is equivalent to $R$ being a unique factorization domain, so $\mathrm{Cl}(R)$ is a measure of how far $R$ is from having unique factorization of elements.
4. Every abelian group is isomorphic to the ideal class group of some Dedekind domain.
5. It is believed that every finite abelian group is isomorphic to the ideal class group of some algebraic number field, but this is unsolved.
6. If $R$ is Dedekind, $\mathrm{Cl}(R)$ can be regarded as a quotient Group
$$\mathrm{Cl}(R) = \{\,\text{fractional } R\text{-ideals}\,\} \,/\, \{\,\text{principal fractional } R\text{-ideals}\,\}$$
7. If all fractional ideal of an integral domain is invertible, then it is a Dedekind domain.

**Definition 8.** The Kronecker Bound (or Hurwitz bound?)
$$C = \prod_{\sigma : K \to \mathbb{C}} \sum_{i=1}^{n} |\sigma(e_i)|$$

**Theorem 9.** The ideal classes of $\mathcal{O}_K$ are
1. represented by ideals in $\mathcal{O}_K$ with norm at most $C$
2. generated as a group by prime ideals $\mathfrak{p}$ with norm at most $C$.

**Theorem 10.** Let $K$ be an algebraic number field of degree $n$, $\Delta_K$ be the discriminant of $K/\mathbb{Q}$, and $2r_2 = n - r_1$ be the number of complex embeddings where $r_1$ is the number of real embeddings. Then every class in the ideal class group of $K$ contains an integral ideal of norm not exceeding Minowski's bound
$$M_K = \sqrt{|\Delta_K|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$
Moreover, the ideal class group is generated by the prime ideals with the norm not exceeding this bound.

| | | |
|---|---|---|
| $K = \mathbb{Q}(\sqrt{2})$ | $M_K \approx 1.41$ | $\mathrm{Cl}(K) \cong Z_1$ |
| $K = \mathbb{Q}(\sqrt{3})$ | $M_K \approx 1.73$ | $\mathrm{Cl}(K) \cong Z_1$ |
| $K = \mathbb{Q}(\sqrt{5})$ | $M_K \approx 1.12$ | $\mathrm{Cl}(K) \cong Z_1$ |
| $K = \mathbb{Q}(\sqrt{6})$ | $M_K \approx$ | $\mathrm{Cl}(K) \cong$ |
| $K = \mathbb{Q}(\sqrt{7})$ | $M_K \approx 2.65$ | $\mathrm{Cl}(K) \cong Z_1$ |
| cell4 | cell5 | cell6 |
| cell7 | cell8 | cell9 |

**Example 10.1.** If the Minkowski bound is less than 2, the ideal class group is generated by just one element, the identity, and every (fractional and integral) ideals are equivalent to (1). In such a case, we call the ideal class group trivial.

**Example 10.2.** Let $K = \mathbb{Q}(\sqrt{7})$. Then, $M_K \approx 2.65$ and $\mathrm{Cl}(K) \cong Z_1$.

*Proof.* We have $7 \equiv 3 \mod 4$, thus the discriminant is $\Delta_K = 4 \cdot 7$. There are $r_2 = 0$ complex embeddings and the degree of the algebraic number field $K$ is $n = 2$. This gives us the Minkowski bound

$$M_K = \sqrt{4 \cdot 7} \left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{7} \approx 2.65.$$

We find the prime factorization of the ideal (2). It is

$$X^2 - 7 \equiv X^2 - 1 \equiv X^2 + 1 \equiv (X+1)^2 \mod 2.$$

Thus, $(2) = \mathfrak{p}_2^2$ for some prime ideal $\mathfrak{p}_2$ in $\mathcal{O}_K$. Because (2) is equivalent to the identity (1) in the ideal class group, we know $\mathfrak{p}_2$ has an order not more than 2.

Here, we will use the fact that 2 has a factorization in $\mathcal{O}_K$ namely $2 = (3+\sqrt{7})(3-\sqrt{7})$. It is

$$\frac{3+\sqrt{7}}{3-\sqrt{7}} = \frac{(3+\sqrt{7})^2}{2} = 8 + 3\sqrt{7}.$$

Now, $8 + 3\sqrt{7}$ is a unit because of $(8+3\sqrt{7})(8-3\sqrt{7}) = 1$, thus $3+\sqrt{7}$ and $3-\sqrt{7}$ generate the same ideal. We had $(2) = \mathfrak{p}_2^2$, therefore $\mathfrak{p}_2 = (8+3\sqrt{7})$ which is principal. Hence, $\mathfrak{p}_2 \sim (1)$ and the ideal class group $\mathrm{Cl}(K)$ is isomorphic to the cyclic group of order 1. □

**Example 10.3.** Let $K = \mathbb{Q}(\sqrt{82})$.

*Proof.* Since $82 \equiv 2 \mod 4$, the ring of integer of $K$ is $\mathbb{Z}[\sqrt{82}]$ and $\left\{1, \sqrt{82}\right\}$ being an integral basis. Thus, the discriminant of $K$ is

$$\Delta_K = \left(\det \begin{pmatrix} 1 & \sqrt{82} \\ 1 & -\sqrt{82} \end{pmatrix}\right)^2 = \left(-2\sqrt{82}\right)^2 = 328.$$

There are $r_2 = 0$ complex embeddings and the degree of $K$ is $n = 2$. The Minkowski bound is therefore

$$M_K = \sqrt{328} \left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{82} \approx 9.06.$$

Since the ideal class group of $K$ is generated by prime ideals with norm not exceeding $M_K$, we will look at (2), (3), (5), and (7).

1. To find the factorization of (2), we have

$$X^2 - 82 \equiv X^2 \mod 2,$$

so $(2) = (2, \sqrt{82})^2$.

2. For (3), we have

$$X^2 - 82 \equiv X^2 - 1 \equiv (X+1)(X-1) \mod 3$$

hence $(3) = (3, \sqrt{82}+1)(3, \sqrt{82}-1)$.

3. For (5), it is

$$X^2 - 82 \equiv X^2 + 3 \mod 5$$

therefore, $(5) = (5, 85) = (5)$ which is prime.

4. For (7), we have

$$X^2 - 82 \equiv X^2 + 2 \mod 7$$

therefore $(7) = (7, 85) = (7)$ which is also prime.

Since $(5) \sim (7) \sim (1)$, we are only interested in $(2) = (2, \sqrt{82})^2$ and $(3) = (3, \sqrt{82}+1)(3, \sqrt{82}-1)$.
Since $(1) \sim (3) = (3, \sqrt{82}+1)(3, \sqrt{82}-1)$, we have $(3, \sqrt{82}+1)^{-1} = (3, \sqrt{82}-1)$.
I don't understand this part, but $(2, \sqrt{82}) \sim (3, \sqrt{82} \pm 1)^2$ (either plus or minus).
Now we want to show that $(2, \sqrt{82})$ is not principal. If $(2, \sqrt{82}) = (a + b\sqrt{82})$, then $(2) = ((2, \sqrt{82})^2)$ □

**Example 10.4.** Let $K = \mathbb{Q}(\sqrt{-14})$.

*Proof.* Firstly, $-14 \equiv 2 \mod 4$, so the ring of integers of $K$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$. We can compute the discriminant using the integral basis $\left\{ 1, \sqrt{-14} \right\}$

$$\Delta_K = \left( \det \begin{pmatrix} 1 & \sqrt{-14} \\ 1 & -\sqrt{-14} \end{pmatrix} \right)^2 = \left( -2\sqrt{-14} \right)^2 = -4 \cdot 14.$$

The number of complex embeddings are $r_2 = 1$ and the degree of the algebraic number field $K$ is $n = 2$, thus the Minkowski bound is

$$M_K = \sqrt{|-4 \cdot 14|} \left( \frac{4}{\pi} \right)^1 \frac{2}{4} = \frac{4\sqrt{14}}{\pi} \approx 4.76.$$

The ideal class group is generated by the prime ideals dividing the ideals (2) and (3).

$$X^2 + 14 \equiv X \cdot X \mod 2$$
$$X^2 + 14 \equiv X^2 + 2 \equiv X^2 - 1 \equiv (X+1)(X-1) \mod 3$$

Therefore, we have the factorizations $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ for some prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_3'$ in $\mathcal{O}_K$. Because (2) and (3) are equivalent to the identity (1) in the ideal class group, we have $\mathfrak{p}_2^{-1} = \mathfrak{p}_2$ and $\mathfrak{p}_3^{-1} = \mathfrak{p}_3'$. Therefore, the ideal class group of $K$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$.

Both $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are nonprincipal because

$$4 = \mathrm{N}((2)) = \mathrm{N}(\mathfrak{p}_2)\mathrm{N}(\mathfrak{p}_2) \Rightarrow \mathrm{N}(\mathfrak{p}_2) = 2$$
$$9 = \mathrm{N}((3)) = \mathrm{N}(\mathfrak{p}_3)\mathrm{N}(\mathfrak{p}_3') \Rightarrow \mathrm{N}(\mathfrak{p}_3) = \mathrm{N}(\mathfrak{p}_3') = 3,$$

but the equations $a^2 + 14b^2 = 2$ and $a^3 + 14b^2 = 3$ have no integer solutions.

To find the relations between $\mathfrak{p}_2$ and $\mathfrak{p}_3$, we use $N(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$. □