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 α and β 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 (γ) and (β) 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 $\mathcal{A} \sim \mathcal{C}$.

$\square$

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. $\text{Cl}(K) = [(1)]$, 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 $\text{Cl}(R)$ is trivial if and only if R is a principal domain which is equivalent to R being a unique factorization domain, so $\text{Cl}(R)$ 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, $\text{Cl}(R)$ can be regarded as a quotient Group

$$\text{Cl}(R) = \{ \text{ fractional } R\text{-ideals} \} / \{ \text{ principal fractional } R\text{-ideals} \}$$

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, Δ_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.

3.1   Appendix: Computation of Some Ideal Class Groups

$$
\begin{array}{lll}
K = \mathbb{Q}(\sqrt{2}) & M_K \approx 1.41 & \mathrm{Cl}(K) \cong Z_1 \\
K = \mathbb{Q}(\sqrt{3}) & M_K \approx 1.73 & \mathrm{Cl}(K) \cong Z_1 \\
K = \mathbb{Q}(\sqrt{5}) & M_K \approx 1.12 & \mathrm{Cl}(K) \cong Z_1 \\
K = \mathbb{Q}(\sqrt{6}) & M_K \approx 2.45 & \mathrm{Cl}(K) \cong Z_1 \\
K = \mathbb{Q}(\sqrt{7}) & M_K \approx 2.65 & \mathrm{Cl}(K) \cong Z_1 \\
K = \mathbb{Q}(\sqrt{10}) & M_K \approx 3.16 & \mathrm{Cl}(K) \cong Z_2 \\
K = \mathbb{Q}(\sqrt{11}) & M_K \approx 3.32 & \mathrm{Cl}(K) \cong Z_1 \\
K = \mathbb{Q}(\sqrt{13}) & M_K \approx 1.80 & \mathrm{Cl}(K) \cong Z_1 \\
K = \mathbb{Q}(\sqrt{14}) & M_K \approx & \mathrm{Cl}(K) \cong \\
\end{array}
$$

cell4	cell5	cell6
cell7	cell8	cell9

Remark. If $d \in \mathbb{Z}$ is not a square-free integer, i.e. there is an integer $a \in \mathbb{Z}$ with $a^2 \cdot b = d$ for some intger $b \in \mathbb{Z}$, then

$$
\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(a\sqrt{b}\right) = \mathbb{Q}\left(\sqrt{b}\right).
$$

Thus, if the algebraic number field is of the form $\mathbb{Q}(\sqrt{d})$, then we will only consider the cases where d is square-free.

Remark. 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, the ideal class group is trivial, i.e. it is isomorphic to the cyclic group of order 1.
There are algebraic number fields with a Minkowski bound not less than 2 that have trivial ideal class groups, e.g. $\mathbb{Q}(\sqrt{6})$. In other words, a Minkowski bound of 2 or more does not guarantee that the algebraic number field has a trivial ideal class group.

Example 10.1. Let $K = \mathbb{Q}(\sqrt{6})$. Then, $M_K \approx 2.45$ and $\mathrm{Cl}(K) \cong Z_1$.

Proof. 6 is congruent to 2 modular 4, thus the discriminant is $\Delta_K = 4 \cdot 6$. There are $r_2 = 0$ complex embeddings and the degree of the algebraic number field K is 2. Then, the Minkowski bound is

$$
M_K = \sqrt{4 \cdot 6}\left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{6} \approx 2.45.
$$

Hence, the ideal (2) is of interest. It is

$$
X^2 - 6 \equiv X^2 \pmod 2.
$$

Thus, $(2) = (2, \sqrt{6})^2$ where $(2, \sqrt{6})$ is a prime ideal in $\mathcal{O}_K$.

We want to show that $(2, \sqrt{6})$ is principal. If there is a common divisor x of 2 and $\sqrt{6}$, then its norm must divide $N(2) = 4$ and $N(\sqrt{6}) = -6$. Hence $N(x) = \pm 2$. This is the same as solving the equation $a^2 - 6b^2 = \pm 2$ for integers. A solution is $a = 2$ and $b = 1$, and indeed $2 + \sqrt{6}$ is a common divisor because $(2 + \sqrt{6})(-2 + \sqrt{6}) = 2$ and $(2 + \sqrt{6})(3 - \sqrt{6}) = 6 - 2\sqrt{6} + 3\sqrt{6} - 6 = \sqrt{6}$. Therefore, $(2, \sqrt{6}) = (2 + \sqrt{6})$ and the ideal class group is trivial. $\qquad \square$

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. $\qquad \square$

Example 10.3. Let $K = \mathbb{Q}(\sqrt{10})$. Then, the Minkowski bound is $M_K \approx 3.16$ and the ideal class group is $\mathrm{Cl}(K) \cong Z_2$.

Proof. It is $10 \equiv 2 \mod 4$, so the discriminant of K is $\Delta_K = 4 \cdot 10$. There are $r_2 = 0$ complex embeddings, and the degree of the algebraic number field is $n = 2$. This gives us the Minkowski bound of

$$M_K = \sqrt{4 \cdot 10} \left(\frac{4}{\pi} \right)^0 \frac{2}{4} = \sqrt{10} \approx 3.16.$$

Hence there are two ideals to analyse (2) and (3). It is

$$X^2 - 10 \equiv X^2 \mod 2$$
$$X^2 - 10 \equiv X^2 - 1 = (X + 1)(X - 1) \mod 3.$$

This gives us 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 $\mathfrak{p}_3'$. If $\mathfrak{p}_2$ was principal, then $\mathfrak{p}_2 = (a + b\sqrt{10})$ for some integers $a, b \in \mathbb{Z}$. The norm of $\mathfrak{p}_2$ is 2 because $4 = \mathrm{N}((2)) = (\mathrm{N}(\mathfrak{p}_2))^2$, therefore we would have

$$a^2 - 10b^2 = \pm 2$$
$$\Longleftrightarrow a^2 = \pm 2 \mod 5.$$

It is easy to verify that no such integer a exists, and hence $\mathfrak{p}_2$ is principal.

Now, consider $\mathfrak{p}_2 \mathfrak{p}_3$. Taking the norm gives $\mathrm{N}(\mathfrak{p}_2 \mathfrak{p}_3) = 6$ and since $\mathrm{N}(2 + \sqrt{10}) = -6m$ we have $p_2 p_3$ is principal. This also means $p_2 \sim p_3$, so $\mathrm{Cl}(\mathbb{Q}(\sqrt{10})) \cong Z_2$. $\qquad \square$

Example 10.4. Let $K = \mathbb{Q}(\sqrt{11})$.

Proof. We have $11 \equiv 3 \mod 4$. This gives us the discriminant of K which is $\Delta_K = 4 \cdot 11$. There are $r_2 = 0$ complex embeddings, and the degree of the algebraic number field is $n = 2$. Thus, the Minkowski bound is

$$M_K = \sqrt{4 \cdot 11} \left(\frac{4}{\pi} \right)^0 \frac{2}{4} = \sqrt{11} \approx 3.32.$$

The two ideals to investigate are therefore (2) and (3). It is

$$X^2 - 11 \equiv X^2 - 1 \equiv (X + 1)(X - 1) \mod 2$$
$$X^2 - 11 \equiv X^2 - 2 \mod 3.$$

$X^2 - 2 \mod 3$ is irreducible, therefore (3) is prime. On the other hand, we have a factorization $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ for some prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ of $\mathcal{O}_K$. But they are principal as $\mathfrak{p}_2 = (3 + \sqrt{11})$ (because of the norm). Hence, $\mathrm{Cl}(K) \cong Z_1$. $\qquad\square$

Example 10.5. Let $K = \mathbb{Q}(\sqrt{13})$

It is $13 \equiv 1 \mod 4$. Then, the discriminant of K is $\Delta_K = 13$. There are $r_2 = 0$ complex embeddings, and the degree of the algebraic number field is $n = 2$. This gives us the Minkowski bound of

$$M_K = \sqrt{13} \left(\frac{2}{\pi}\right)^0 \frac{2}{4} = \frac{\sqrt{13}}{2}$$

Example 10.6. Let $K = \mathbb{Q}(\sqrt{82})$.

Proof. Since $82 \equiv 2 \mod 4$, the discriminant of K is $\Delta_K = 4 \cdot 82$. There are $r_2 = 0$ complex embeddings and the degree of K is $n = 2$. The Minkowski bound is therefore

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

Hence the ideals of interest are (2), (3), (5), and (7). It is

$$X^2 - 82 \equiv X^2 \mod 2$$
$$X^2 - 82 \equiv X^2 - 1 \equiv (X + 1)(X - 1) \mod 3$$
$$X^2 - 82 \equiv X^2 + 3 \mod 5$$
$$X^2 - 82 \equiv X^2 + 2 \mod 7.$$

I'm not exactly sure why, but $X^2 + 3 \mod 5$ and $X^2 + 2 \mod 7$ are irreducible, so (5) and (7) are already prime and principal.

On the other hand, we have the factorization $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ for some prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$. We immediately have the relation $\mathfrak{p}_2^{-1} \sim \mathfrak{p}_2$ and $\mathfrak{p}_3^{-1} \sim \mathfrak{p}_3'$.

Now, we show that $\mathfrak{p}_2$ is nonprincipal. Suppose it isn't, then $\mathfrak{p}_2 = (a + b\sqrt{82})$ for some $a, b \in \mathbb{Z}$. Since $\mathfrak{p}_2^2$ is principal, we have

$$u\left(a + b\sqrt{82}\right)^2 = 2$$

for some unit $u \in \mathcal{O}_K$. If we take the norms, then $\qquad\square$

Example 10.7. 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 $\{1, \sqrt{-14}\}$

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

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 $N(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$. $\square$