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. $\mathrm{Cl}(K) = [(1)]$, 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, 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.

Example 10.1. Let $K = \mathbb{Q}(i)$.