9. The Ideal Class Group and Minkowski's Theorem

We introduce the notions of the ideal class group and the class number, and prove Minkowski's Theorem, which will be used later to compute class numbers explicitly.

9.1. **The ideal class group.** We show some important applications of the theorem of unique factorisation of ideals. The following definition plays a major role in algebraic number theory.

Definition 9.1. Let K be a number field and $\mathcal{O}_K$ its ring of integers. Two non-zero ideals I, J in $\mathcal{O}_K$ are said to be equivalent, $I \sim J$, if there exist non-zero $\alpha, \beta \in \mathcal{O}_K$, such that $(\alpha)I = (\beta)J$. This is an equivalence relation. Each equivalence class is called an *ideal class*.

We leave it in Exercise 9.3 to verify that $I \sim J$ is an equivalence relation.

Theorem 9.2. *For any number field K, the set of ideal classes in $\mathcal{O}_K$ form an abelian group.*

Proof. For any non-zero ideal I of $\mathcal{O}_K$, let $\overline{I}$ denote the ideal class containing I. For two ideals I and J of $\mathcal{O}_K$, we define the product of the ideal classes $\overline{I}$ and $\overline{J}$ to be the ideal class $\overline{IJ}$. The product is closed since IJ is an ideal. We need to check the product is well-defined; that is, the product of two ideal classes does not depend on the choice of the ideals in the two classes. This is Exercise 9.3. The commutativity and associativity follow from those of multiplications of ideals. The ideal class containing $\mathcal{O}_K$ serves as the identity for the multiplication. For any non-zero ideal I of $\mathcal{O}_K$, by Proposition 8.13 there exists some ideal J in $\mathcal{O}_K$ such that IJ is a non-zero principle ideal, hence the inverse of $\overline{I}$ is given by $\overline{J}$. Therefore the ideal classes form an abelian group. □

Based on the above theorem, we make the following definitions.

Definition 9.3. Let K be a number field and $\mathcal{O}_K$ its ring of integers. The group of ideal classes in $\mathcal{O}_K$ under multiplication is called the *ideal class group* of K. The order of the ideal class group is called the *class number* of K, denoted by h_K.

Remark 9.4. It can be proved that there are only finitely many ideal classes for every number field, hence the class number is always finite. However, we will only prove the finiteness for quadratic fields. And we will also show how to compute the class number in some explicit examples.

In some sense, the class number measures how far $\mathcal{O}_K$ is from being a PID.

Proposition 9.5. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then $h_K = 1$ iff $\mathcal{O}_K$ is a PID.*

Proof. It is clear that that $h_K = 1$ iff every non-zero ideal I is equivalent to $\mathcal{O}_K$, and $\mathcal{O}_K$ is a PID iff every non-zero ideal is principal. Therefore it suffices to show that, for any non-zero ideal I, we have $I \sim \mathcal{O}_K$ iff I is principal.

For one direction, assume that I is a principal ideal (α). Then we have $(1)I = (\alpha)\mathcal{O}_K$, hence $I \sim \mathcal{O}_K$.

For the other direction, assume that $I \sim \mathcal{O}_K$. Then there are non-zero $\alpha, \beta \in \mathcal{O}_K$, such that $(\alpha)I = (\beta)\mathcal{O}_K = (\beta)$. From $\beta \in (\alpha)I$ we know $\beta = \alpha\gamma$ for some $\gamma \in I$. We claim $I = (\gamma)$. It is clear that $I \supseteq (\gamma)$ since $\gamma \in I$. For any $a \in I$, $\alpha a \in (\beta)$ hence $\alpha a = \beta b$ for some $b \in \mathcal{O}_K$. Therefore $a = \gamma b \in (\gamma)$, from which we conclude $I \subseteq (\gamma)$. □

In this proof we have actually showed

Corollary 9.6. *Let I be a non-zero ideal in $\mathcal{O}_K$, then $I \sim \mathcal{O}_K$ iff I is a principal ideal.*

Proof. The proof is already contained in that of Proposition 9.5. □

Corollary 9.7. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. If $h_K = 1$, then $\mathcal{O}_K$ is a UFD.*

Proof. This is an immediate consequence of Proposition 9.5 and Theorem 1.11. □

Example 9.8. If $K = \mathbb{Q}[i]$, then $\mathcal{O}_K = \mathbb{Z}[i]$ by Proposition 7.2. From Exercise 1.4 we know $\mathbb{Z}[i]$ is a Euclidean domain, hence a PID and UFD. Then we know the class number of $K = \mathbb{Q}[i]$ is 1. In many other examples, the opposite direction could be more useful: if we can show the class number $h_K = 1$, then $\mathcal{O}_K$ is a UFD. Hence it is important to find a systematic way to compute class numbers. We will see it later.

Our next goal is to prove Minkowski's Theorem, which is the main tool for computing class numbers. We need to introduce some terminologies before stating the theorem.For the moment we forget number theory and think about some geometry.

Definition 9.9. Let e_1, e_2 be two linearly independent vectors in $\mathbb{R}^2$. The abelian group $L = \{m_1e_1 + m_2e_2 \mid m_1, m_2 \in \mathbb{Z}\}$ is called a *lattice* of rank 2 in $\mathbb{R}^2$. The set $\{e_1, e_2\}$ is called a *generator* of L. The *fundamental domain* of L with respect to the generator $\{e_1, e_2\}$ is the set $T = \{a_1e_1 + a_2e_2 \mid a_1, a_2 \in \mathbb{R}, 0 \leqslant a_1 < 1, 0 \leqslant a_2 < 1\}$.

Using the standard metric on $\mathbb{R}^2$, we can define the *volume* (or *area*) of a measurable subset $X \subseteq \mathbb{R}^2$ in the usual way, more precisely by $\int_X \mathrm{d}x\mathrm{d}y$, denoted by $\mathrm{vol}(X)$. However

the only examples that we are interested in are the volumes of rectangles, disks, and parallelograms, which are familiar. For instance, let $e_i = (x_i, y_i)$ for $i = 1, 2$, then the volumn of the fundamental domain of the lattice L is given by

$$\mathrm{vol}(T) = \left| \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \right|.$$

Definition 9.10. A subset $X \subseteq \mathbb{R}^2$ is *convex* if, whenever $p, q \in X$, the point $\lambda p + (1 - \lambda)q \in X$ for all real λ, $0 \leqslant \lambda \leqslant 1$. A subset $X \subset \mathbb{R}^2$ is *centrally symmetric* if $p \in X$ implies $-p \in X$.

In other words, if X is convex, then the straight line segment joining two points in X completely lies in X. For example a disk, a square, a triangle is convex, but an annulus is not. A disk is centrally symmetric only when its centre is at $(0, 0)$.