10. Computation of Class Numbers

We will establish the Minkowski bound for class numbers, and show how to use it to make explicit computations in examples.

10.1. **Minkowski bound.** We will show an upper bound for class numbers due to Minkowski. The formula is still a little different for real quadratic fields and imaginary quadratic fields.

Proposition 10.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d < 0$. For any non-zero ideal I of $\mathcal{O}_K$, there exists a non-zero element $\alpha \in I$ such that $|N(\alpha)| \leqslant \frac{2}{\pi} N(I) \, |\Delta_K|^{\frac{1}{2}}$.*

Proof. By Proposition 9.13, we know that L_I is a rank 2 lattice in $\mathbb{R}^2$ with the volume of the fundamental domain $\operatorname{vol}(T_I) = \frac{1}{2} N(I) \, |\Delta_K|^{\frac{1}{2}}$.

Now we consider the closed disk D with centre $(0, 0)$ and radius $r = \left(\frac{2}{\pi} N(I) \, |\Delta_K|^{\frac{1}{2}} \right)^{\frac{1}{2}}$. D is centrally symmetric, convex, compact, with volume $\operatorname{vol}(D) = \pi r^2 = 2N(I) \, |\Delta_K|^{\frac{1}{2}} = 4 \operatorname{vol}(T_I)$. By Corollary 9.12, D contains non-zero lattice point in L_I. In other words, there exists some $\alpha \in I$, such that the point $(\operatorname{Re} \alpha, \operatorname{Im} \alpha) \in D$. Hence $(\operatorname{Re} \alpha)^2 + (\operatorname{Im} \alpha)^2 \leqslant r^2$. If we write $\alpha = a + b\sqrt{d}$, then $\operatorname{Re} \alpha = a$ and $\operatorname{Im} \alpha = b\sqrt{-d}$, hence $(\operatorname{Re} \alpha)^2 + (\operatorname{Im} \alpha)^2 = a^2 - b^2 d = N(\alpha)$ by Example 6.18. In particular, $N(\alpha) \geqslant 0$. It follows that $|N(\alpha)| = N(\alpha) \leqslant r^2 = \frac{2}{\pi} N(I) \, |\Delta_K|^{\frac{1}{2}}$. □

To prove next result we need the following lemma

Lemma 10.2. *For any numeber field K, let I and J be non-zero ideals in $\mathcal{O}_K$. Then $N(IJ) = N(I)N(J)$.*

Proof. The proof is omitted and non-examinable. It is a consequence of Theorem 8.16. □

Proposition 10.3. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d < 0$. Then every ideal class $\mathcal{C}$ of $\mathcal{O}_K$ contains an ideal I with $N(I) \leqslant \frac{2}{\pi} \, |\Delta_K|^{\frac{1}{2}}$.*

Proof. By Theorem 9.2, the ideal class $\mathcal{C}$ has an inverse in the ideal class group. We denote this inverse ideal class by $\overline{J}$ where J is any representative. Then by Proposition 10.1, there exists a non-zero element $\beta \in J$ such that $|N(\beta)| \leqslant \frac{2}{\pi} N(J) \, |\Delta_K|^{\frac{1}{2}}$. Since we have $(\beta) \subseteq J$, there exists some ideal I such that $IJ = (\beta)$ by Corollary 8.15. Since the ideal class containing (β) is the identity element in the ideal class group, $\overline{I}$ and $\overline{J}$ are inverse of each other, hence I is an ideal in $\mathcal{C}$. It remains to show $N(I)$ satisfies the given bound.

By Lemma 10.2 and Proposition 8.9, we have the following calculation

$$N(I)N(J) = N(IJ) = N((\beta)) = |N(\beta)| \leqslant \frac{2}{\pi} N(J) \, |\Delta_K|^{\frac{1}{2}} .$$

Since $N(J)$ is a positive integer by Proposition 8.3, we cancel it to get $N(I) \leqslant \frac{2}{\pi} \, |\Delta_K|^{\frac{1}{2}}$ as required. □

We can get the following parallel results for real quadratic fields. We leave the proofs as exercises.

Proposition 10.4. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d > 0$. For any ideal I of $\mathcal{O}_K$, there exists a non-zero element $\alpha \in I$ such that $|N(\alpha)| \leqslant \frac{1}{2} N(I) \, |\Delta_K|^{\frac{1}{2}}$.*

Proof. The proof is similar to that of Proposition 10.1. See Exercise 10.3. □

Proposition 10.5. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d > 0$. Then every ideal class $\mathcal{C}$ of $\mathcal{O}_K$ contains an ideal I with $N(I) \leqslant \frac{1}{2} \, |\Delta_K|^{\frac{1}{2}}$.*

Proof. The proof is similar to that of Proposition 10.3. See Exercise 10.3. □

Summarising the above results, we get the following definition:

Definition 10.6. Let d be a square-free integer, $d \neq 1$, and $K = \mathbb{Q}(\sqrt{d})$ a quadratic field. The *Minkowski bound* M_K is defined by

$$M_K = \begin{cases} \frac{2}{\pi} \, |\Delta_K|^{\frac{1}{2}} & \text{if } d < 0, \\ \frac{1}{2} \, |\Delta_K|^{\frac{1}{2}} & \text{if } d > 0, \end{cases}$$

with the property that every ideal class in $\mathcal{O}_K$ contains an ideal whose norm is at most M_K.

This allows us to prove the following important result:

Theorem 10.7. *Let d be a square-free integer, $d \neq 1$, and $K = \mathbb{Q}(\sqrt{d})$ a quadratic field. The class number h_K is finite.*

Proof. By Definition 10.6, every ideal class contains an ideal with norm not larger than M_K. Hence it remains to show there are only finitely many ideals with norm not larger than M_K. By Proposition 8.3, every such norm is a positive integer not larger than M_K, hence there are only finitely many choices for such norms. It suffices to show that for every fixed positive integer $q \leqslant M_K$, there are only finitely many ideals I with $N(I) = q$.

By Corollary 8.5, we know $q \in I$, hence $(q) \subseteq I$. By Corollary 8.15, we can find some ideal J such that $(q) = IJ$. By Theorem 8.16, the ideal (q) has a unique factorisation

into finitely many prime ideals, say $(q) = P_1 P_2 \cdots P_r$. Since I is a factor of (q), it must be the product of some prime ideals in the factorisation of (q), hence there are at most finitely many choices for such I. This completes the proof. □

Remark 10.8. This proof not only shows the finiteness of class numbers, but also provide a recipe for computation. Namely, we can factor all ideals (q) for positive integers $q \leqslant M_K$ to find all ideals with norm q. Then every ideal class is representated by some of these ideals. By eliminating repeated ideal classes and analysing the multiplicative structure, we should in principle understand the ideal class group.

We give one simple example as follows:

Example 10.9. Consider the quadratic field $\mathbb{Q}(i)$. By Proposition 7.2, we know its ring of integers is $\mathcal{O}_K = \mathbb{Z}[i]$. Since $d = -1$, we have $\Delta_K = -4$ by Proposition 7.14. The Minkowski bound for this field is $M_K = \frac{4}{\pi} < 2$. Therefore every ideal class contains an ideal I of norm $N(I) = 1$. By Corollary 8.6, the only possibility is $I = \mathcal{O}_K$. So there is only one ideal class, and $h_K = 1$. By Proposition 9.5 and Corollary 9.7, the ring $\mathcal{O}_K = \mathbb{Z}[i]$ is a PID and UFD. This is consistent with the result in Exercise 1.4. The same argument works for every quadratic field K with $M_K < 2$.