10.2. **Computing class numbers.** We compute class numbers for quadratic fields in some concrete examples.

In Example 10.9, we have seen that, if the Minkowski bound is smaller than 2, then the class number $h_K = 1$ and the class group is a trivial group. In general, we need to use the strategy mentioned in Remark 10.8. More precisely, we need to first factor ideals of the form $(q)$ for all positive integers $q \leqslant M_K$ to find all ideals of norm $q$, then analyse the relation among these ideals.

There is, in fact, a systematic way to factor any ideal of the form $(p)$ for any prime $p$ in $\mathcal{O}_K$ when $K$ is a quadratic field.

**Proposition 10.10.** *Let $d \neq 1$ be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$. Then we can factor $(2)$ into prime ideals as follows*

(1) *If $d \not\equiv 1 \pmod 4$, then $(2) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$, which is the only ideal of norm $2$;*
(2) *If $d \equiv 1 \pmod 8$, then $(2) = \mathfrak{p}_1\mathfrak{p}_2$ for distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$, which are the only ideals of norm $2$;*
(3) *If $d \equiv 5 \pmod 8$, then $(2)$ is a prime ideal itself, and there is no ideal of norm $2$.*

**Proposition 10.11.** *Let $d \neq 1$ be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$. For any odd prime $p$, we can factor $(p)$ into prime ideals as follows*

(1) *If $p \mid d$, then $(p) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$, which is the only ideal of norm $p$;*
(2) *If $(\frac{d}{p}) = 1$, then $(p) = \mathfrak{p}_1\mathfrak{p}_2$ for distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$, which are the only ideals of norm $p$;*
(3) *If $(\frac{d}{p}) = -1$, then $(p)$ is a prime ideal itself, and there is no ideal of norm $p$.*

*Proof of Propositions 10.10 and 10.11.* In both propositions, we can in fact write down the prime ideals in the factorisations explicitly. Parts (1) and (2) can be proved by verifying the mutual inclusions of the two sides of the equations. Part (3) can be proved by showing the quotient ring is a field (hence an integral domain). The details of the proofs are omitted due to limitation of time. This proof is non-examinable. □

If we want to factor $(q)$ for some composite $q$, we can factor $q$ into primes in $\mathbb{Z}$, say $q = p_1 p_2 \cdots p_r$, then write $(q) = (p_1)(p_2)\cdots(p_r)$ and factor each $(p_i)$ using Propositions 10.10 and 10.11.

The following examples show how to compute class numbers using the general strategy mentioned above.

**Example 10.12.** Let $K = \mathbb{Q}(\sqrt{-19})$. We want to compute $h_K$. Since $d = -19$, we have $\Delta_K = -19$ by Proposition 7.14. The Minkowski bound for this field is $M_K = \frac{2\sqrt{19}}{\pi} < 3$. By Definition 10.6, every ideal class contains an ideal of norm at most 2. By Corollary 8.6, an ideal of norm 1 must be $\mathcal{O}_K$. Since $d = -19 \equiv 5 \pmod 8$, by Proposition 10.10, there is no ideal of norm 2. We conclude that $h_K = 1$. By Proposition 9.5 and Corollary 9.7, the ring $\mathcal{O}_K$ is a PID and UFD when $K = \mathbb{Q}(\sqrt{-19})$.

**Example 10.13.** Let $K = \mathbb{Q}(\sqrt{-5})$. We want to compute $h_K$. Since $d = -5$, we have $\Delta_K = -20$ by Proposition 7.14. The Minkowski bound for this field is $M_K = \frac{2\sqrt{20}}{\pi} < 3$. By Definition 10.6, every ideal class contains an ideal of norm at most 2. By Corollary 8.6, an ideal of norm 1 must be $\mathcal{O}_K$. Since $d = -5 \not\equiv 1 \pmod 4$, by Proposition 10.10, $(2) = \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ which is the only ideal of norm 2. Therefore there are at most 2 ideal classes, represented by $\mathcal{O}_K$ and $\mathfrak{p}$. We still need to know whether they are the same ideal class or distinct ideal classes.

Assume $\mathcal{O}_K$ and $\mathfrak{p}$ are in the same ideal class, then $\mathfrak{p}$ is a principal ideal. Say, $\mathfrak{p} = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. By Proposition 7.2, we can write $\alpha = a + b\sqrt{-5}$ for some $a, b \in \mathbb{Z}$. By Proposition 8.9, we know that $|N(\alpha)| = N((\alpha)) = 2$, hence $N(\alpha) = \pm 2$. By Example 6.18, we know that $N(\alpha) = a^2 + 5b^2$. Therefore we have $a^2 + 5b^2 = \pm 2$ for some $a, b \in \mathbb{Z}$. This equation has no integer solutions. Contradiction. It follows that $\mathfrak{p}$ cannot be a principal ideal. By Corollary 9.6, $\mathfrak{p}$ and $\mathcal{O}_K$ are in different ideal classes, hence $\mathcal{O}_K$ does have two distinct ideal classes. We conclude that $h_K = 2$ for $K = \mathbb{Q}(\sqrt{-5})$.

**Example 10.14.** Let $K = \mathbb{Q}(\sqrt{10})$. We want to compute $h_K$. Since $d = 10$, we have $\Delta_K = 40$ by Proposition 7.14. The Minkowski bound for this field is $M_K = \frac{\sqrt{40}}{2} < 4$. By Definition 10.6, every ideal class contains an ideal of norm at most 3. By Corollary 8.6, an ideal of norm 1 must be $\mathcal{O}_K$. Since $d = 10 \not\equiv 1 \pmod 4$, by Proposition 10.10, $(2) = \mathfrak{p}_0^2$ for some prime ideal $\mathfrak{p}$ which is the only ideal of norm 2. Since $(\frac{10}{3}) = (\frac{1}{3}) = 1$, by Proposition 10.11, $(3) = \mathfrak{p}_1\mathfrak{p}_2$ for prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ which are the only ideals of norm 3. Therefore we have at most 4 ideal classes, represented by $\mathcal{O}_K$, $\mathfrak{p}_0$, $\mathfrak{p}_1$ and $\mathfrak{p}_2$. However, some of them might be in the same ideal class. So we still need to understand their relations.

We first show that $\mathfrak{p}_0$ is not a principal ideal, thus $\mathcal{O}_K$ and $\mathfrak{p}_0$ are in two different ideal classes. If $\mathfrak{p}_0 = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. By Proposition 7.2, we can write $\alpha = a + b\sqrt{10}$ for some $a, b \in \mathbb{Z}$. By Proposition 8.9, we know that $|N(\alpha)| = N((\alpha)) = 2$, hence $N(\alpha) = \pm 2$. By Example 6.18, we know that $N(\alpha) = a^2 - 10b^2$. Therefore we have $a^2 - 10b^2 = \pm 2$ for some $a, b \in \mathbb{Z}$. This would imply $a^2 \equiv \pm 2 \pmod 5$, hence either 2 or $-2$ must be a quadratic residue modulo 5. However, $(\frac{2}{5}) = (\frac{-2}{5}) = -1$. Contradiction. It follows that $\mathfrak{p}_0$ cannot be a principal ideal. Therefore we have at least two distinct ideal classes, given by $\overline{\mathcal{O}_K}$ and $\overline{\mathfrak{p}_0}$.

Finally we analyse $\mathfrak{p}_1$ and $\mathfrak{p}_2$. We will show that they are in the same ideal class as $\mathfrak{p}_0$. For this purpose we look at $\alpha = 2 + \sqrt{10} \in \mathcal{O}_K$. By Example 6.18, $N(\alpha) = -6$. By Proposition 7.2, $N((\alpha)) = |N(\alpha)| = 6$. By Corollary 8.5, we know $6 \in (\alpha)$, hence $(6) \subseteq (\alpha)$. By Corollary 8.15, we can find some ideal $I$ such that $(6) = I(\alpha)$. By Theorem 8.16, the ideal $(6)$ has a unique factorisation into finitely many prime ideals. Indeed, we can find it as $(6) = (2)(3) = \mathfrak{p}_0^2\mathfrak{p}_1\mathfrak{p}_2$. Since $(\alpha)$ is a factor of $(6)$, it must be the product of some prime ideals in the factorisation of $(6)$. On the other hand, $N((\alpha)) = 6$, so it has to be the product of an ideal of norm 2 and an ideal of norm 3, i.e., $(\alpha) = \mathfrak{p}_0\mathfrak{p}_1$ or $(\alpha) = \mathfrak{p}_0\mathfrak{p}_2$. If the first case happens, then the ideal classes $\overline{\mathfrak{p}_1} = \overline{\mathfrak{p}_0}^{-1}$ in the ideal class group because $(\alpha)$ is a principal ideal. Similarly from $(2) = \mathfrak{p}_0^2$ and $(3) = \mathfrak{p}_1\mathfrak{p}_2$, we also know $\overline{\mathfrak{p}_0}^{-1} = \overline{\mathfrak{p}_0}$ and $\overline{\mathfrak{p}_2} = \overline{\mathfrak{p}_1}^{-1} = \overline{\mathfrak{p}_0}$. It follows $\overline{\mathfrak{p}_0} = \overline{\mathfrak{p}_1} = \overline{\mathfrak{p}_2}$. If the second case happens, then we can prove the same result by switching the subscripts in $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Hence the only distinct ideal classes are the ones represented by $\mathcal{O}_K$ and $\mathfrak{p}_0$. We conclude $h_K = 2$ for $K = \mathbb{Q}(\sqrt{10})$.