1. (1) Explain why the equations

$$2 \cdot 11 = (5 + \sqrt{3})(5 - \sqrt{3})$$

and

$$(2 + \sqrt{7})(3 - 2\sqrt{7}) = (5 - 2\sqrt{7})(18 + 7\sqrt{7})$$

are not inconsistent with the fact that $\mathbf{Z}[\sqrt{3}]$ and $\mathbf{Z}[\sqrt{7}]$ have unique factorisation.

(2) Find equations to show that $\mathbf{Z}[\sqrt{d}]$ is not a UFD for $d = -10, -13, -14$.

2. Let K be a number field, and let $I, J \subset \mathcal{O}_K$ be non-zero ideals.

(1) Determine the factorisations into prime ideals of $I + J$ and $I \cap J$ in terms of those for I and J. Show that if $I + J = \mathcal{O}_K$ then $I \cap J = IJ$ and there is an isomorphism of rings $\mathcal{O}_K/IJ \cong \mathcal{O}_K/I \times \mathcal{O}_K/J$.

(2) Show that I can be generated by at most 2 elements.

(3) Let $\phi(I) = |(\mathcal{O}_K/I)^\times|$. Show that

$$\phi(I) = \mathrm{N}(I) \prod_{P|I} \left(1 - \frac{1}{\mathrm{N}(P)}\right),$$

where the product is over the set of prime ideals P dividing I.

3. Let K be a number field, and let $I = \langle x_1, x_2, \ldots, x_k \rangle$ be the ideal of $\mathcal{O}_K$ generated by $x_1, \ldots, x_k$. Show that $\mathrm{N}(I)$ divides $\gcd(\mathrm{N}(x_1), \ldots, \mathrm{N}(x_k))$. Do we always have $\mathrm{N}(I) = \gcd(\mathrm{N}(x_1), \ldots, \mathrm{N}(x_k))$?

4. Let $K = \mathbf{Q}(\sqrt{-5})$. Show by computing norms, or otherwise, that $P = \langle 2, 1 + \sqrt{-5} \rangle$, $Q_1 = \langle 7, 3 + \sqrt{-5} \rangle$ and $Q_2 = \langle 7, 3 - \sqrt{-5} \rangle$ are prime ideals in $\mathcal{O}_K$. Which (if any) of the ideals $P, Q_1, Q_2, P^2, PQ_1, PQ_2$ and Q_1Q_2 are principal? Factor the principal ideal $\langle 9 + 11\sqrt{-5} \rangle$ as a product of prime ideals.

5. Let K be a number field, and let $I \subset \mathcal{O}_K$ be a non-zero ideal. Let m be the least positive integer in I. Prove that m and $\mathrm{N}(I)$ have the same prime factors.

6. Let $K = \mathbf{Q}(\sqrt{35})$ and $\omega = 5 + \sqrt{35}$. Verify the ideal equations $\langle 2 \rangle = \langle 2, \omega \rangle^2$, $\langle 5 \rangle = \langle 5, \omega \rangle^2$ and $\langle \omega \rangle = \langle 2, \omega \rangle \langle 5, \omega \rangle$. Show that the ideal class group of K contains an element of order 2. Find all ideals of norm dividing 100 and determine which are principal.

7. Let $K = \mathbf{Q}(\sqrt{-m})$ where $m > 1$ is a square-free integer. Establish the following facts about the factorisation of principal ideals in $\mathcal{O}_K$:

(1) If m is composite and p is an odd prime divisor of m then $\langle p \rangle = P^2$ where P is not principal.

(2) If $m \equiv 1$ or $2 \pmod 4$ then $\langle 2 \rangle = P^2$ where P is not principal unless $m = 1$ or 2.

(3) If $m \equiv 7 \pmod 8$ then $\langle 2 \rangle = PP'$ where $P \neq P'$ and P, P' are not principal unless $m = 7$.

Deduce that if the ideal class group of K is trivial then either $m = 1$, 2 or 7, or m is prime and $m \equiv 3 \pmod 8$.

8. Let $K = \mathbf{Q}(\sqrt{-m})$ where $m > 1$ is the product of distinct primes $p_1, \ldots, p_k$. Show that $\langle p_i \rangle = P_i^2$ where $P_i = \langle p_i, \sqrt{-m} \rangle$. Show that just two of the ideals $\prod P_i^{r_i}$ with $r_i \in \{0, 1\}$ are principal. Deduce that the class group $\mathrm{Cl}(\mathcal{O}_K)$ contains a subgroup isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{k-1}$.

9. Let $K = \mathbf{Q}(\theta)$ where θ is a root of $X^3 - 4X + 7$. Determine the ring of integers and discriminant of K. Determine the factorisation into prime ideals of $p\mathcal{O}_K$ for $p = 2, 3, 5, 7, 11$. Find all non-zero ideals I of $\mathcal{O}_K$ with $\mathrm{N}(I) \leq 11$.

10. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(X) = X^3 + X^2 - 2X + 8$. [*This polynomial is irreducible over* $\mathbf{Q}$ *and has discriminant* -4×503.]

(1) Show that $\beta = 4/\alpha \in \mathcal{O}_K$ and $\beta \notin \mathbf{Z}[\alpha]$. Deduce that $\mathcal{O}_K = \mathbf{Z}[\alpha, \beta]$.
(2) Show that there is an isomorphism of rings $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbf{F}_2 \times \mathbf{F}_2 \times \mathbf{F}_2$. Deduce that 2 splits completely in K.
(3) Use Dedekind's criterion to show that $\mathcal{O}_K \neq \mathbf{Z}[\theta]$ for any θ.

11. Let $f(X) \in \mathbf{Z}[X]$ be a monic, irreducible polynomial, and let $K = \mathbf{Q}(\theta)$, where θ is a root of $f(X)$.

(1) Show that if p is a prime and $r \in \mathbf{Z}$ is such that $p \nmid \operatorname{disc} f$ and $f(r) \equiv 0 \pmod{p}$, then there is a ring homomorphism $\mathcal{O}_K \to \mathbf{F}_p$ which sends θ to $r \pmod{p}$.
(2) Suppose that $f(X) = X^3 - X - 1$. Show that θ is not a square in K.
(3) Suppose instead that $f(X) = X^5 + 2X - 2$. Show that the equation $x^4 + y^4 + z^4 = \theta$ has no solutions with $x, y, z \in \mathcal{O}_K$.

12. Let K be a number field, and let $p \in \mathbf{Z}$ be a prime. Let $\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r}$, where each P_i is a non-zero prime ideal with $\mathrm{N}(P_i) = p^{f_i}$.

(1) Let $\alpha \in I = P_1 \cdots P_r$. Show that $\mathrm{Tr}_{K|\mathbf{Q}}(\alpha) \equiv 0 \pmod{p}$.
(2) Let (θ_i) be an integral basis for K, and (α_i) a basis for I. By considering the matrix $\mathrm{Tr}_{K|\mathbf{Q}}(\alpha_i \theta_j)$, show that d_K is divisible by $\prod p^{(e_i - 1)f_i}$.