1. (i) 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 $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{7}]$ have unique factorisation.

(ii) Find equations to show that $\mathbb{Z}[\sqrt{d}]$ 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.

(i) 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 $\mathcal{O}_K/IJ \cong \mathcal{O}_K/I \times \mathcal{O}_K/J$.

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

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

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

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

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

4. Let $K = \mathbb{Q}(\sqrt{-5})$. Show by computing norms, or otherwise, that $P = (2, 1 + \sqrt{-5})$, $Q_1 = (7, 3 + \sqrt{-5})$ and $Q_2 = (7, 3 - \sqrt{-5})$ 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 $(9 + 11\sqrt{-5})$ 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 $N(I)$ have the same prime factors.

6. Let $K = \mathbb{Q}(\sqrt{35})$ and $\omega = 5 + \sqrt{35}$. Verify the ideal equations $(2) = (2, \omega)^2$, $(5) = (5, \omega)^2$ and $(\omega) = (2, \omega)(5, \omega)$. 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 $K = \mathbb{Q}(\sqrt{-d})$ where $d > 1$ is a square-free integer. Establish the following facts about the factorisation of principal ideals in $\mathcal{O}_K$:

 a.j.scholl@dpmms.cam.ac.uk

(i) If d is composite and p is an odd prime divisor of d then $(p) = P^2$ where P is not principal.

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

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

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

8. Let $K = \mathbb{Q}(\sqrt{-m})$ where $m > 0$ is the product of distinct primes $p_1, \dots, p_k$. Show that $(p_i) = P_i^2$ where $P_i = (p_i, \sqrt{-m})$. 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 $(\mathbb{Z}/2\mathbb{Z})^{k-1}$.

9. Let $K = \mathbb{Q}(\theta)$ 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 $N(I) \leq 11$.

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

    (i) Show that $\beta = 4/\alpha \in \mathcal{O}_K$ and $\beta \notin \mathbb{Z}[\alpha]$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.

    (ii) Show that there is an isomorphism of rings $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Deduce that 2 splits completely in K.

    (iii) Use Dedekind's criterion to show that $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ for any θ.

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

    (i) Show that if p is a prime and $r \in \mathbb{Z}$ is such that $p \nmid \mathrm{disc} f$ and $f(r) \equiv 0 \pmod p$, then there is a ring homomorphism $\mathcal{O}_K \to \mathbb{F}_p$ which sends θ to $r \pmod p$.

    (ii) Suppose that $f(X) = X^3 - X - 1$. Show that θ is not a square in K.

    (iii) 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 $(p) = P_1^{e_1} \cdots P_r^{e_r}$ with $N(P_i) = p^{f_i}$.

    (i) Let $\alpha \in I = P_1 \cdots P_r$. Show that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \equiv 0 \pmod p$.

    (ii) Let (θ_i) be an integral basis for K, and (α_i) a basis for I. By considering the matrix $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \omega_j)$, show that d_K is divisible by $\prod p^{(e_i - 1)f_i}$.

 a.j.scholl@dpmms.cam.ac.uk