Suggested solutions to
Number Theory (SF2728, MM8012), Re-exam , 22 August 2022

1. (a) Define what it means for a complex number α to be algebraic over $\mathbb{Q}$.
   (b) Define what it means for a complex number α to be an algebraic integer.
   (c) Show that for every algebraic number $\alpha \in \mathbb{C}$ there exists a non-zero rational integer $C \in \mathbb{Z}$ such that $C\alpha$ is an algebraic integer.

   Solution. (c) Suppose that α is a zero of $P(X) = C_nX^n + \cdots + C_0 \in \mathbb{Z}[X]$, $C_n \neq 0$. Consider the polynomial

   $$Q(X) = C_n^{n-1}P(X/C_n) = X^n + C_{n-1}X^{n-1} + C_{n-2}C_nX^{n-2}\cdots + C_n^{n-1}C_0.$$

   This is a monic polynomial with coefficients in $\mathbb{Z}$ and $Q(C_n\alpha) = C_n^{n-1}P(\alpha) = 0$. Hence $C_n\alpha$ is an algebraic integer, where C_n is a non-zero rational integer.

2. Let $\theta = (1+\sqrt{-11})/2$.
   (a) Show that θ is an algebraic integer and that $\theta \in K$ for $K = \mathbb{Q}(\sqrt{-11})$.
   (b) Show that $\{1, \theta\}$ is an integral basis for $K = \mathbb{Q}(\sqrt{-11})$.

   Solution. $\theta = (1+\sqrt{-11})/2$ is a zero of the polynomial

   $$\left(X - \frac{1+\sqrt{-11}}{2}\right)\left(X - \frac{1-\sqrt{-11}}{2}\right) = X^2 - X + \frac{1}{4} + \frac{11}{4} = X^2 + X + 3,$$

   which is monic and belongs to $\mathbb{Z}[X]$. Hence, θ is an algebraic integer. Since $\{1, \sqrt{-11}\}$ is a $\mathbb{Q}$-basis for K, we have $(1+\sqrt{-11})/2 \in K$. More precisely, $\theta \in \mathscr{O}_K$.
   (b) The discriminant

   $$\operatorname{disc}(1, (1+\sqrt{-11})/2) = \begin{vmatrix} 1 & \frac{1+\sqrt{-11}}{2} \\ 1 & \frac{1-\sqrt{-11}}{2} \end{vmatrix}^2 = -11$$

   is non-zero and square-free. Since $\theta \in \mathscr{O}_K$ by part (a), it follows that $\{1, \theta\}$ is an integral basis for $K = \mathbb{Q}(\sqrt{-11})$

3. Let K be a number field of degree n over $\mathbb{Q}$. Show that every natural number $N \in \mathbb{N}$, $N > 0$, belongs to only finitely many integral $\mathscr{O}_K$-ideals.
   [Hint: Suppose that $N \in I$, $I = (\alpha_1, \ldots, \alpha_n)$. Note that $I = (\alpha_1, \ldots, \alpha_n, N)$. Represent all α_j in a fixed integral basis for K and deduce that I has a system of generators $\{\beta_1, \ldots, \beta_n, N\}$ where the β_j belong to a finite set. To find the finite set, consider elements β_j of the form $\alpha_j - \lambda_j N$ with $\lambda_j \in \mathscr{O}_K$.]

   Solution. Let $\omega_1, \ldots, \omega_n$ denote a $\mathbb{Z}$-basis for $\mathscr{O}_K$. Then $\alpha_j = x_{1,j}\omega_1 + \cdots + x_{n,j}\omega_n$, where $x_{i,j} \in \mathbb{Z}$ for $1 \leqslant i \leqslant n$. Let $\lambda_j = u_{1,j}\omega_1 + \cdots + u_{n,j}\omega_n$ with $u_{i,j} \in \mathbb{Z}$ for $1 \leqslant i \leqslant n$ be such that $x_{i,j} - Nu_{i,j} \in \{0, \ldots, N-1\}$. Then

   $$\beta_j = \alpha_j - \lambda_j N = r_{1,j}\omega_1 + \cdots + r_{n,j}\omega_n$$

   with $r_{i,j} \in \{0, \ldots, N-1\}$, leading to a finite set of representatives as claimed.

4. Let $q, r \in \mathbb{Z}$, suppose that q is square-free and $q \notin \{0, 1\}$, and that
$$r^2 - q = 25.$$
(a) Show that $\gcd(q, r) = 1$.
(b) Let $K = \mathbb{Q}(\sqrt{q})$. Show that the $\mathscr{O}_K$-ideals $(r + \sqrt{q})$ and $(r - \sqrt{q})$ are co-prime.
Solution. (a) Since $r^2 - q = 25$, we have $\gcd(q, r) \mid 25$. If $5 \mid \gcd(q, r)$, then $25 \mid (r^2 - 25) = q$, contradicting the assumption that q was square-free. Hence $\gcd(q, r) = 1$.
(b) Let $J \subset \mathscr{O}_K$ be a prime ideal that divides both $(r + \sqrt{q})$ and $(r - \sqrt{q})$. Then $N(J) = p^f$ for some rational prime p and $f \in \{1, 2\}$. Then $N(J) | N((r + \sqrt{q})) = |r^2 - q| = 25$, which shows that $p = 5$. Furthermore, $2r \in J$ and $2\sqrt{q} \in J$. Hence, $N(J) | \gcd(4r^2, 4q) = 4 \nmid 5^2$, which is a contradiction.

5. Show that $h_{\mathbb{Q}(\sqrt{-11})} = 1$.
[Hint: The Minkowski constant is given by
$$\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |d_K|^{1/2},$$
where $n = r + 2s$.]
Solution. $K = \mathbb{Q}(\sqrt{-11})$ is an extension of degree $n = 2$, with $r = 0$ and $s = 1$. Since $-11 \equiv 12 - 11 \equiv 1 \pmod 4$, we have $d_K = -11$ and any ideal class in $Cl(K)$ contains an integral ideal of norm bounded by
$$\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |d_K|^{1/2} = \frac{4}{\pi} \cdot \frac{2}{4}\sqrt{11} < \frac{2}{\pi}\sqrt{16} = \frac{8}{\pi} < \frac{8}{3} < 3.$$
Hence, $Cl(K)$ is generated by the prime ideals of norm 2. By Problem 2, we have $\mathscr{O}_K = \mathbb{Z}[\theta]$ and $m_\theta(X) = X^2 - X + 3$. Modulo 2, we obtain the polynomial $X^2 + X + 1$, which is irreducible over $\mathbb{F}_2$. If it was reducible, it would be of the form
$$X^2 + X + 1 \equiv (X + a)(X + b) \equiv X^2 + (a + b)X + ab \mod 2$$
for $a, b \in \{0, 1\}$, and thus either of the form $X^2 + X$ or of the form $X^2 + 1$. By Dedekinds result this shows that the principal ideal (2) is a prime ideal of $\mathscr{O}_K$. This shows that the class group is trivial and $h_K = 1$