Suggested solutions to
Number Theory (SF2728, MM8012), Final Exam, 1 June 2020

1. Consider the element $\alpha = 2 + \sqrt{-3} \in K := \mathbb{Q}(\sqrt{-3})$.
   (a) Show that α belongs to $\mathscr{O}_K$.
   (b) Is α an irreducible element of $\mathscr{O}_K$? Justify your answer.
   Solution. (b) $N_{K/\mathbb{Q}}(\alpha) = (2+\sqrt{-3})(2-\sqrt{-3}) = 4+3 = 7$ is prime. Since $N_{K/\mathbb{Q}} : \mathscr{O}_{\mathscr{K}} \to \mathbb{Z}$ is multiplicative, and $N_{K/\mathbb{Q}}(\varepsilon) = \pm 1$ for $\varepsilon \in \mathscr{O}_K$ iff ε is a unit, α is irreducible.

2. Let h_K denote the class number of a number field K. By considering the class group, show that if $p \nmid h_K$ is a prime number and if $J \subset K$ is an $\mathscr{O}_K$-ideal (fractional or integral) such that J^p is principal, then J is principal.
   Solution. Since $(p, h_K) = 1$, there are $p', q \in \mathbb{Z}$ such that $pp' + qh_K = 1$. Hence,
   $$[J^{pp'}] = [J^{1-qh_k}] = [J][J^{-q}]^{h_k} = [J]$$
   in the class group, and $[J^p] = 1$ implies $[J^{pp'}] = 1$. Hence, $[J] = 1$, as required.

3. Let $K = \mathbb{Q}(\sqrt{-15})$. Let $P_2 \subset \mathscr{O}_K$ be a prime ideal such that $P_2 | (2)$. Is P_2 principal?
   Solution. Since $-15 \equiv 1 \pmod 4$, we have $\mathscr{O}_K = \mathbb{Z}[\theta]$ for $\theta = \frac{1+\sqrt{-15}}{2}$ and
   $$m_\theta(X) = \Big(X - \frac{1+\sqrt{-15}}{2}\Big)\Big(x - \frac{1-\sqrt{-15}}{2}\Big) = X^2 - X + 4.$$
   By Dedekind's result, $m_\theta(X) \equiv X(X+1) \pmod 2$ implies that $(2) = P_2 P_2'$ splits. This shows that $N(P_2) = 2$. If P_2 is principal, then $P_2 = (a + b\theta)$ for some $a, b \in \mathbb{Z}$ and
   $$2 = N(P_2) = |N_{K/\mathbb{Q}}(a + b\sqrt{-15})| = \Big(a + \frac{b}{2}\Big)^2 + \frac{15b^2}{4}.$$
   Since $15/4 > 2$, we deduce that $b = 0$. Since 2 is not a square, P_2 is non-principal.

4. (a) Let $P \in \mathbb{Z}[X]$ be a polynomial. Show that $P(X)$ is irreducible if and only if $P(X+1)$ is irreducible.
   (b) Let $p \geqslant 3$ be a prime number. Show that $\zeta = e^{2\pi i/p}$ is an algebraic integer of degree $p-1$ over $\mathbb{Q}$.
   Solution. (a) If $P(X)$ is reducible over $\mathbb{Z}$, then there are $Q(X), R(X) \in \mathbb{Z}[X] \setminus \{\pm 1\}$ such that $P(X) = Q(X)R(X)$. Hence $P(X+1) = Q(X+1)P(X+1)$ and $Q(X+1), R(X+1) \in \mathbb{Z}[X] \setminus \{\pm 1\}$. Hence $P(X+1)$ is reducible. In the other direction, $P(X+1) = Q(X)P(X)$ with $Q(X), R(X) \in \mathbb{Z}[X] \setminus \{\pm 1\}$ implies $P(X) = Q(X-1)P(X-1)$, where $Q(X-1), P(X-1) \in \mathbb{Z}[X] \setminus \{\pm 1\}$.
   (b) ζ satisfies the polynomial $X^p - 1$. Let $P(X) = \frac{X^p-1}{X-1}$. Then P is irreducible iff $P(X+1)$ is irreducible.
   $$P(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + a_{p-2}X^{p-2} + \cdots + a_0,$$

where $a_j = \binom{p}{j+1}$. Since p is prime, $\gcd(p, n!) = 1$ for all $n < p$. Hence $p|a_j$ for all $0 \leqslant j \leqslant p-2$ and $p^2 \nmid p = a_0$. Hence, by Eisenstein's criterion, $m_\zeta(X+1)$ is irreducible.

5. Let $J \subset \mathscr{O}_K$ be a non-zero integral $\mathscr{O}_K$-ideal. Consider the set

$$S = \{x \in K : xJ \subset \mathscr{O}_K\}$$

(a) Show that S is a non-zero fractional $\mathscr{O}_K$-ideal. [2p]
(b) Show that $J^{-1} \subseteq S$. [1p]
(c) Show that $J^{-1} = S$. [2p]
[Hint: Show that $JS \subseteq \mathscr{O}_K$ and relate this product to JJ^{-1}.]

Solution. (a) $\mathscr{O}_K \subseteq S$. Hence, S is non-zero. S satisfies:
(i) $\alpha, \beta \in S, \lambda, \mu \in \mathscr{O}_K \implies (\lambda\alpha + \mu\beta)J \subset \mathscr{O}_K \implies \lambda\alpha + \mu\beta \in S$.
(ii) there exists $0 \neq \omega \in K$ such that $\omega S \subseteq \mathscr{O}_K$. Indeed, any $\omega \in J \setminus \{0\}$ has this property.
Hence, S is a fractional ideal.
(b) For every $\alpha \in J^{-1}$, we have $\alpha J \subseteq \mathscr{O}_K$. Hence, $J^{-1} \subseteq S$.
(c). $\mathscr{O}_K = JJ^{-1} \subseteq JS \subseteq \mathscr{O}_K$. Hence equality holds. Since $J \neq (0)$, cancellation or multiplication with J^{-1} implies $J^{-1} = S$.

6. Let K be a number field of degree n over $\mathbb{Q}$ and suppose that $K \subseteq \mathbb{R}$ [and that all embeddings into $\mathbb{C}$ are real]. Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{R}$ denote the n distinct embeddings of K. Show that for every $1 \leqslant j \leqslant n$ and every non-zero integral $\mathscr{O}_K$-ideal J, there is an element $0 \neq \alpha \in J$ such that all the conjugates of α, except for $\sigma_j(\alpha)$, are bounded in absolute value by one, i.e. $|\sigma_i(\alpha)| \leqslant 1$ for all $i \neq j$ with $1 \leqslant i \leqslant n$.

Solution. Since all σ_i are real, the Minkowski embedding takes the form $\iota : K \hookrightarrow \mathbb{R}^n$, $\iota(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$. We may employ Minkowski's theorem from the geometry of numbers with a set $S_j \subseteq \mathbb{R}^n$ of the form

$$S_j = \{\mathbf{x} \in \mathbb{R}^n : |x_i| \leqslant 1 \text{ for all } i \neq j, |x_j| \leqslant t\}.$$

Then $\operatorname{vol} S_j = 2^n t$ and S_j is convex, measurable, and centrally symmetric. Choosing $t > \operatorname{vol}(\mathbb{R}^n/\Lambda)$ ensures that S_j contains a non-zero lattice point λ. $\alpha = \iota^{-1}(\lambda)$ has the required properties.