Suggested solutions to
Number Theory (SF2728, MM8012), Re-Exam, 14 August 2024

1. Let $K = \mathbb{Q}(\sqrt{-15})$. Show that there are no principal integral $\mathscr{O}_K$-ideals of norm 2. [Hint: Express the norm as a sum of squares.]
Solution. We have $-15 \equiv 1 \pmod 4$. Hence, $d_K = -15$ and $\mathscr{O}_K = \mathbb{Z}[\theta]$ for $\theta = \frac{1+\sqrt{-15}}{2}$. Hence, any $\alpha \in \mathscr{O}_K$ can be uniquely expressed as $\alpha = a + \theta b$ with $a, b \in \mathbb{Z}$. We have

$$\begin{aligned} N((a+\theta b)) &= |N_{K/\mathbb{Q}}(a+\theta b)| = |(a + b(1+\sqrt{-15})/2)(a + b(1-\sqrt{-15})/2)| \\ &= (a+b/2)^2 + 15(b/2)^2. \end{aligned}$$

Since $15/4 > 2$, we must have $b = 0$ in order for $N((\alpha)) = 2$. However $a^2 = 2$ has no solution in $\mathbb{Z}$. Hence, there are no principal integral $\mathscr{O}_K$-ideals of norm 2.

2. Let K, $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, be a number field, let $f, g \in K[x]$ be polynomials and suppose that f is irreducible in $K[x]$.
   (a) Show that if f and g have a common root $\alpha \in \mathbb{C}$, then $f \mid g$ in $K[x]$.
   (b) Show that f does not have a repeated root in $\mathbb{C}$.
Solution. (a) Consider the $h = \gcd(f, g)$. We know that $h \in K[x]$ and that $(x-\alpha) \mid h(x)$ in $\mathbb{C}[x]$. Hence, $\deg h > 0$. Since f is irreducible, $h \mid f$ and $\deg h > 0$, we must have $\gcd(f, g) = cf$ for some non-zero $c \in K$.
(b) f has a repeated root iff f and f' have a common root, where f' denotes the formal derivative of f. By part (a), we have $f \mid \gcd(f, f')$ if f and f' have a common root. Since $\deg f < \deg f'$, this is impossible.

3. Let K denote a number field of degree $n = [K : \mathbb{Q}]$ over $\mathbb{Q}$.
   (a) Given $\alpha_1, \dots \alpha_n \in K$, define $\operatorname{disc}(\alpha_1, \dots \alpha_n)$.
   (b) Let $\alpha \in K$ be of degree n over $\mathbb{Q}$. Show that $\operatorname{disc}(1, \alpha, \dots \alpha^{n-1})$ can be expressed as a polynomial over $\mathbb{Q}$ in the coefficients of m_α.
   (c) Give a definition of the discriminant d_K of K.
   (d) If $n = r + 2s$, where r denotes the number of real embeddings of K and s the number of pairs of complex conjugate non-real embeddings, show that the sign of the discriminant is given by
$$\operatorname{sgn} d_K = (-1)^s.$$
[Hint: Compare Δ^2 with $\Delta\overline{\Delta}$, where Δ is the relevant determinant.]
Solution. (a) If $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ denote the n field embeddings of K into $\mathbb{C}$, we have
$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det((\sigma_i(\alpha_j))_{1 \leqslant i,j, \leqslant n})^2$$
(b) We have
$$\operatorname{disc}(1, \alpha, \dots \alpha^{n-1}) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{\binom{n}{2}} \prod_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} (\sigma_i(\alpha) - \sigma_j(\alpha)).$$

This expression is a symmetric polynomial over $\mathbb{Z}$ in the conjugates of α. By the symmetric functions theorem, it can therefore be rewritten as a polynomial over $\mathbb{Z}$ in the elementary symmetric functions of the conjugates of α. The latter expressions are, up to sign, equal to the coefficients of m_α.

(c) $d_K = \mathrm{disc}(\omega_1, \ldots, \omega_n)$ for any integral basis $\{\omega_1, \ldots, \omega_n\}$ of K.

(d) If $\{\omega_1 \ldots, \omega_n\}$ denotes a $\mathbb{Z}$-basis for K, we have $d_K = \Delta^2$ for $\Delta = \Delta(\omega_1 \ldots, \omega_n) = \det((\sigma_i(\omega_j))_{1 \leqslant i,j \leqslant n})$. Since $\Delta\overline{\Delta} > 0$, the sign of is equal to $\Delta/\overline{\Delta}$. Passing from Δ to $\overline{\Delta}$ interchanges the embeddings in each pair of complex conjugate non-real embeddings. The determinant therefore changes by $(-1)^s$, as required.

4. Let $K = \mathbb{Q}(\sqrt{-15})$. Show that $h_K = 2$.
Solution. As we already know from Problem 1, we have $d_K = -15$ and $\mathscr{O}_K = \mathbb{Z}[\theta]$ where $\theta = \frac{1+\sqrt{-15}}{2}$. Further, we have $[K : \mathbb{Q}] = 2$, $r = 0$, $s = 1$ and therefore
$$\Big(\frac{4}{\pi}\Big)^s \frac{n!}{n^n} |d_K|^{1/2} = \frac{4}{\pi}\frac{1}{2} = \frac{2}{\pi} < \frac{2}{3}.$$
It follows that every ideal class in the class group thus contains an integral ideal J of norm
$$N(J) < \frac{2}{3}\sqrt{|d_K|} = \frac{2}{3}\sqrt{15} < \frac{2 \cdot 4}{3} < 3.$$
Since $m_\theta(X) = (X - \frac{1+\sqrt{-15}}{2})(X - \frac{1-\sqrt{-15}}{2}) = X^2 - X + 4$ and
$$m_\theta(X) \equiv X(X-1) \pmod 2,$$
we have $2\mathscr{O}_K = (2, \frac{1+\sqrt{-15}}{2})(2, \frac{-1+\sqrt{-15}}{2})$ by Dedekind's result. Hence there are two distinct prime ideals P_2, P_2' of norm 2, and $[P_2] = [P_2']^{-1}$ in the class group. By Problem 1, neither of these ideals is principal, i.e. $h_K > 1$. We determine the order of P_2 in the class group. We have:
$$P_2^2 = \Big(2, \frac{1+\sqrt{-15}}{2}\Big)^2 = \Big(4, 1+\sqrt{-15}, \frac{1+2\sqrt{-15}-15}{4}\Big) = \Big(4, \frac{1+\sqrt{-15}}{2}\Big).$$
Note that $N_{K/\mathbb{Q}}((1+\sqrt{-15})/2) = \frac{1+\sqrt{-15}}{2}\frac{1-\sqrt{-15}}{2} = 16/4 = 4$. Thus, $P_2^2 = (\frac{1+\sqrt{-15}}{2})$ is principal. This shows that $[P_2] = [P_2'] \neq [(1)]$ and $h_K = 2$.

5. State and prove Minkowski's theorem on lattice points in convex subsets of $\mathbb{R}^n$.
Solution. See notes/book.