Suggested solutions to
Number Theory (SF2728, MM8012), Final Exam, 29 May 2024

1. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{-5})$.
   (a) Find the conjugates of $\sqrt{3} + \sqrt{-5}$ over $\mathbb{Q}$.
   (b) Determine whether $K = \mathbb{Q}(\sqrt{3} + \sqrt{-5})$.
   (c) Find the minimum polynomial for $\sqrt{3} + \sqrt{-5}$ over $\mathbb{Q}$.
   (d) Compute $N_{K/\mathbb{Q}}(a\sqrt{3} + b\sqrt{-5})$ for $a, b \in \mathbb{Q}$.

   Solution. (a) $\pm\sqrt{3}$, $\pm\sqrt{-5}$, $\pm\sqrt{3} \pm \sqrt{-5}$. (b) We have $[K : \mathbb{Q}] = 4$ by the tower law, $\sqrt{3} + \sqrt{-5} \in K$ and $\sqrt{3} + \sqrt{-5}$ has 4 conjugates over $\mathbb{Q}$. Hence the equality holds. (c)

$$\begin{aligned}
&(X - \sqrt{3} - \sqrt{-5})(X - \sqrt{3} + \sqrt{-5})(X + \sqrt{3} - \sqrt{-5})(X + \sqrt{3} + \sqrt{-5}) \\
&= ((X - \sqrt{3})^2 + 5)((X + \sqrt{3})^2 + 5) = (X^2 + 8)^2 - 4 \cdot 3X^2 \\
&= X^4 + 4X^2 + 64
\end{aligned}$$

   (d)

$$\begin{aligned}
&(a\sqrt{3} + b\sqrt{-5})(a\sqrt{3} - b\sqrt{-5})(-a\sqrt{3} + b\sqrt{-5})(-a\sqrt{3} - b\sqrt{-5}) \\
&= (3a^2 + 5b^2)^2
\end{aligned}$$

2. Let $K = \mathbb{Q}(\sqrt{-29})$ and consider the $\mathscr{O}_K$-ideal $I = (6, 1 + \sqrt{-29})$.
   (a) Show that $2 \in P$ or $3 \in P$ for any prime ideal P dividing I.
   (b) Determine the prime factorisations of $2\mathscr{O}_K$ and $3\mathscr{O}_K$.
   (c) Determine the prime factorisation of I.

   Solution. (a) We have $6 \in I$, hence $P \mid I$ implies $P \mid (2)(3)$, i.e. $P \mid (2)$ or $P \mid (3)$. (b) $-29 \equiv -1 \equiv 3 \pmod 4$. Hence, $d_K = -4 \cdot 29$ and $\mathscr{O}_K = \mathbb{Z}[\sqrt{-29}]$. The minimum polynomial for the generator is

$$(x - \sqrt{-29})(x + \sqrt{-29}) = x^2 + 29.$$

   Over $\mathbb{Z}/2\mathbb{Z}$ we obtain $x^2 + 29 \equiv x^2 + 1 \equiv (x + 1)^2 \pmod 2$. Hence,

$$2\mathscr{O}_K = (2, 1 + \sqrt{-29})^2.$$

   Over $\mathbb{Z}/3\mathbb{Z}$ we obtain $x^2 + 29 \equiv x^2 - 1 \equiv (x + 1)(x - 1) \pmod 3$. Hence,

$$3\mathscr{O}_K = (3, 1 + \sqrt{-29})(3, 1 - \sqrt{-29}).$$

   (c) Note that $(2, 1 + \sqrt{-29}) \supseteq (6, 1 + \sqrt{-29})$ and $(3, 1 + \sqrt{-29}) \supseteq (6, 1 + \sqrt{-29})$, which gives us two prime factors of I. These are all prime factors since

$$\begin{aligned}
(2, 1 + \sqrt{-29})(3, 1 + \sqrt{-29}) &= (6, 2(1 + \sqrt{-29}), 3(1 + \sqrt{-29}), (1 + \sqrt{-29})^2) \\
&= (6, 1 + \sqrt{-29}) = I.
\end{aligned}$$

3. Let K be a number field and let $\mathscr{O}_K$ denote its ring of integers. Prove the following statement without appealing to unique factorisation into prime ideals: For any non-zero integral $\mathscr{O}_K$-ideals $I_1, I_2 \subseteq \mathscr{O}_K$ there exists a unique integral $\mathscr{O}_K$-ideal J such that $J|I_1$, $J|I_2$ and $J'|J$ for any other common divisor $J' \subseteq \mathscr{O}_K$ of I_1 and I_2.
Solution. We define $J = I_1 + I_2 = \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}$. This is an $\mathscr{O}_K$-ideal, and $I_1, I_2 \subseteq J$ since $0 \in I_1, I_2$. Thus, J is a common divisor. If J' is another common divisor, then $I_1, I_2 \subseteq J'$ and, since J' is an ideal, $i_1 + i_2 \in J'$ for all $i_1 \in I_1$, $i_2 \in I_2$. Hence, $J = I_1 + I_2 \subseteq J'$, i.e. $J' \mid J$. Uniqueness follows since if J_1 and J_2 both have the described properties, then $J_1|J_2$ and $J_2|J_1$.

4. Let $p \in \mathbb{Z}$ be an odd prime and define $\tau = \sum_{b \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{b}{p}\right) e^{2\pi i b/p}$.
   (a) Show that
   $$\tau\overline{\tau} = \sum_{b,c \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{c}{p}\right) e^{2\pi i b/p} e^{-2\pi i bc/p}.$$
   (b) Show that
   $$\tau\overline{\tau} = p.$$
   [Hint: What happens for fixed c in the expression from (a)?]
   Solution. (a) We have
   $$\tau\overline{\tau} = \sum_{b,b' \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{b}{p}\right)\left(\frac{b'}{p}\right) e^{2\pi i b/p} e^{-2\pi i b'/p}.$$
   Only invertible residues $b \in \mathbb{Z}/p\mathbb{Z}$ have a non-zero contribution to the sum. Given any such residue b, consider the invertible change of variables $b' = cb$ from $b' \in (\mathbb{Z}/p\mathbb{Z})^\times$ to $c \in (\mathbb{Z}/p\mathbb{Z})^\times$. This leads to the given expression since $\left(\frac{b}{p}\right)^2 = 1$ for all $b \in (\mathbb{Z}/p\mathbb{Z})^\times$.
   (b) We have
   $$\begin{aligned}
   \tau\overline{\tau} &= \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{c}{p}\right) \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^\times} e^{2\pi i b/p} e^{-2\pi i bc/p} \\
   &= \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{c}{p}\right) \Big(-1 + \sum_{b \in (\mathbb{Z}/p\mathbb{Z})} e^{2\pi i b(1-c)/p} \Big) \\
   &= -\sum_{\substack{c \in (\mathbb{Z}/p\mathbb{Z})^\times \\ c \neq 1}} \left(\frac{c}{p}\right) + (-1+p) = 1 - \sum_{c \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{c}{p}\right) + (-1+p) = p,
   \end{aligned}$$
   using orthogonality relations.

5. State and prove the symmetric functions theorem.
   [Hint. Start by defining a suitable ordering on the set of monomials in n variables $x_1, \ldots x_n$. If $s_1, \ldots, s_n$ denote the elementary symmetric functions in these variables, what are their leading monomials and what is the leading monomial of $s_1^{a_1} \ldots s_n^{a_n}$?]
   Solution. See notes/book.