S.-T. Yau College Student Mathematics Contests 2022

Algebra and Number Theory

Solve every problem.

Problem 1.

(a) Let $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ be a polynomial over an integral domain R. Let K denote the fraction field of R. Suppose $a/b \in K$ is a root of $p(x)$, where $a, b \in R$ and are relatively prime. Then, show that $a|a_0$ and $b|a_n$.

(b) Prove that $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Solution:

(a) Easy.

(b) It suffices to show $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbf{Q}(\sqrt{2} + \sqrt{3})$.
Let $\alpha = \sqrt{2} + \sqrt{3}$. It is a root of

$$p(x) = x^4 - 10x^2 + 1.$$

By (a), $p(x)$ has no rational roots. We claim that $p(x)$ is irreducible over $\mathbf{Z}$. Otherwise, $p(x) = (a + bx + cx^2)(d + ex + fx^2)$. A direct computation will yield such a decomposition is impossible. Hence, $p(x)$ is a minimal polynomial α over $\mathbf{Q}$. As $\mathbf{Q}(\alpha)$ is a vector subspace of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, we obtain

$$4 = \dim \mathbf{Q}(\alpha) \leq \dim \mathbf{Q}(\sqrt{2}, \sqrt{3}) \leq 4.$$

This implies the statement.

Problem 2. Let R be an integral domain with the fraction field K. An R-module P is projective if there is an R-module Q such that $P \oplus Q \cong F$ for some free R-module F. A fractional ideal A is an R-submodule of K such that $A = d^{-1}I$ for some ideal I of R and a nonzero element $d \in R$. A fractional ideal A is called invertible if $AB = R$ for some fractional ideal B.

Show that an invertible fractional ideal A is a projective R-module.

Solution: Assume that A is an invertible fractional ideal. Let A^{-1} its inverse. Then

$$a_1 a_1' + \cdots + a_n a_n' = 1$$

for some $a_1, \ldots, a_n \in A$ and $a_1', \ldots, a_n' \in A'$ since $AA^{-1} = R$. Let S be a free R-module of rank n, say, generated by $y_1, \ldots, y_n$. Define $\varphi : S \to A$ by $\varphi(y_i) = a_i$ and $\psi : A \to S$ by $\varphi(c) = c(a_1' y_1 + \cdots a_n' y_n)$. This makes sense because $ca_i' \in R$. Obviously, $\varphi\psi = id_A$, hence A is a direct summand of S. In other words, A is a projective module.

Problem 3. Give a *direct* proof that the Lie algebra $\mathfrak{sl}(4, \mathbf{C})$ is isomorphic to the Lie algebra $\mathfrak{so}(6, \mathbf{C})$. (You should construct a Lie algebra homomorphism and prove that it is an ismorphism; you should not use Dynkin diagrams or the classification theory of simple Lie algebras.)

Solution: We have the representation $\mathfrak{sl}(4, \mathbf{C}) \to \mathfrak{gl}(W)$ where $W = \wedge^2 \mathbf{C}^4$. Let e_1, e_2, e_3, e_4 be the standard basis of $\mathbf{C}^4$. Then $e_1 \wedge e_2 \wedge e_3 \wedge e_4$ gives an identification $\wedge^4 \mathbf{C}^4 \cong \mathbf{C}$. We define a complex symmetric bilinear form $S : W \times W \to \mathbf{C}$ by

$$S(\theta, \tau) = \theta \wedge \tau \in \wedge^4 \mathbf{C}^4 \cong \mathbf{C}$$

for $\theta, \tau \in W$. By writing out an explicit orthogonal basis, you can show that S is non-degenerate. Then, one checks that for any $A \in \mathfrak{sl}(4, \mathbf{C})$, we have

$$S(A\theta, \tau) + S(\theta, A\tau) = A\theta \wedge \tau + \theta \wedge A\tau = A(\theta \wedge \tau) = 0.$$

Note here that $\mathfrak{sl}(4,\mathbf{C})$ acts trivially on $\wedge^4\mathbf{C}^4$.

Hence, we obtain a Lie algebra homomorphism $\mathfrak{sl}(4,\mathbf{C}) \to \mathfrak{so}(6,\mathbf{C})$.This must be an isomorphism since both Lie algebras have the same dimension and $\mathfrak{sl}(4,\mathbf{C})$ is simple.

Problem 4. Let $A = \mathcal{O}_K$ be the ring of integers of a number field K. Given a nonzero ideal $\mathfrak{a} \subset A$ and an arbitrary nonzero element $a \in \mathfrak{a}$, show that there exists $b \in \mathfrak{a}$ such that a and b generate $\mathfrak{a}$ (in particular, every ideal is 2-generated).

Solution: Since $\mathcal{O}_K$ is a Dedekind domain, every nonzero ideal of it has a unique factorization as a product of nonzero prime ideals. Write $aA = \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_r^{n_r}$ ($\mathfrak{p}_i$'s are distinct nonzero prime ideals of A, $n_i \in \mathbf{N}$). Since $a \in \mathfrak{a}$, we have $\mathfrak{a}$ divides aA, so that $\mathfrak{a} = \mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r}$ with $0 \le m_i \le n_i$. For each i, pick $x_i \in \mathfrak{p}_i^{m_i} \setminus \mathfrak{p}_i^{m_i+1}$. Since $\mathfrak{p}_i^{m_i+1}$ and $\mathfrak{p}_j^{m_j+1}$ are coprime when $i \neq j$, by the Chinese Remainder Theorem, the system of congruences $b \equiv x_i (\mathrm{mod}\ \mathfrak{p}_i^{m_i+1}), 1 \le i \le r$ has a solution $b \in A$.

By the congruence relation above, we see that $b \in \mathfrak{p}_i^{m_i} \setminus \mathfrak{p}_i^{m_i+1}$ as well. So for each $1 \le i \le r$, the order of $\mathfrak{p}_i$ in the prime ideal factorization of bA is exactly m_i. In other words

$$bA = \mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r}\mathfrak{q}_l^{k_1}\cdots\mathfrak{q}_l^{k_l}, \quad m_i, k_j > 0,$$

where $\mathfrak{q}_j$'s are nonzero prime ideals different from those $\mathfrak{p}_i$'s (if they exist). Therefore

$$aA + bA = \mathfrak{p}_1^{\min\{m_1,n_1\}}\cdots\mathfrak{p}_r^{\min\{m_r,n_r\}}\mathfrak{q}_l^{\min\{0,k_1\}}\cdots\mathfrak{q}_l^{\min\{0,k_l\}} = \mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r} = \mathfrak{a},$$

as desired.

Problem 5. Let p be a prime number and ζ_p be a primitive p-th root of unity. Let $K = \mathbf{Q}(\zeta_p)$.

(a) Show that $\Phi_p = \sum_{i=0}^{p-1} X^i$ is the minimal polynomial of ζ_p over $\mathbf{Q}$.

(b) Compute the trace $\mathrm{Tr}_{K/\mathbf{Q}}(1-\zeta_p)$ and the norm $\mathcal{N}_{K/\mathbf{Q}}(1-\zeta_p)$.

(c) Show that $(1-\zeta_p)\mathcal{O}_K \cap \mathbf{Z} = p\mathbf{Z}$ and deduce that for all $y \in \mathcal{O}_K$, we have

$$\mathrm{Tr}_{K/\mathbf{Q}}(y(1-\zeta_p)) \in p\mathbf{Z}.$$

(d) Determine explicitly the ring of integers of K.

Solution:

(a) Consider $g(X) = \Phi_p(X+1) = (X+1)^{p-1} + \cdots + X + 1$. Then $g(X) = \frac{1}{X}[(X+1)^p - 1] = \sum_{i=0}^{p-1}\binom{p}{i+1}X^i$. Notice that for all $0 \le i \le p-2$, we have $p \mid \binom{p}{i+1}$, but $p^2 \nmid \binom{p}{1} = p$. By the Eisenstein's criterion, $g(X)$ is irreducible over $\mathbf{Q}$, so is $\Phi_p(X) = g(X-1)$. Since ζ_p is a root of $X^p - 1 = (X-1)\Phi_p(X)$ but not of $(X-1)$, we have $\Phi_p(\zeta_p) = 0$. Therefore, $\Phi_p(X)$, being monic, is the minimal polynomial of ζ_p over $\mathbf{Q}$.

(b) For each $1 \le i \le p-1$, we have $\zeta_p^i \in K$ is also a root of $X^p - 1 = (X-1)\Phi_p(X)$ but not of $(X-1)$, we have $\Phi_p(\zeta_p^i) = 0$. Thus $K/\mathbf{Q}$ is a Galois extension whose Galois group is $\mathrm{Gal}(K/\mathbf{Q}) = \{\sigma_i;\ \sigma_i(\zeta_p) = \zeta_p^i,\ 1 \le i \le p-1\}$. So

$$\mathrm{Tr}_{K/\mathbf{Q}} = \sum_{i=1}^{p-1}(1-\zeta_p^i) = (p-1) - \sum_{i=1}^{p-1}\zeta_p^i = (p-1) - (\Phi_p(\zeta_p) - 1) = (p-1) - (-1) = p,$$

and

$$\mathcal{N}_{K/\mathbf{Q}} = \prod_{i=1}^{p-1}(1-\zeta_p^i) = \Phi_p(1) = \sum_{i=0}^{p-1} 1^i = p.$$

(c) Notice that ζ_p is a root of a monic $\Phi_p \in \mathbf{Z}[X]$, so ζ_p is integral over $\mathbf{Z}$. For each $m \in \mathbf{Z}$, let $z = m\prod_{i=2}^{p-1}(1-\zeta_p^i) \in \mathcal{O}_K$. Then $z(1-\zeta_p) = m\prod_{i=1}^{p-1}(1-\zeta_p^i) = mp$. Thus $p\mathbf{Z} \subset (1-\zeta_p)\mathcal{O}_K \cap \mathbf{Z}$. On the other hand, suppose $z \in \mathcal{O}_K$ satisfies

$m = z(1-\zeta_p) \in \mathbf{Z}$. Taking norms on both sides, we get $m^p = \mathcal{N}_{K/\mathbf{Q}}(z)p$. Since z is integral, $\mathcal{N}_{K/\mathbf{Q}}(z) \in \mathbf{Z}$, we have $p \mid m^p$, so $p \mid m$. Thus $(1-\zeta_p)\mathcal{O}_K \cap \mathbf{Z} \subset p\mathbf{Z}$. As a consequence, $(1-\zeta_p)\mathcal{O}_K \cap \mathbf{Z} = p\mathbf{Z}$.

Now take any $y \in \mathcal{O}_K$. Observe that for each $1 \le i \le p-1$, we have

$$\sigma_i(y(1-\zeta_p)) = \sigma_i(y)(1-\zeta_p^i) = (1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1})\sigma_i(y) \in (1-\zeta_p)\mathcal{O}_K,$$

so $\mathrm{Tr}_{K/\mathbf{Q}}(y(1-\zeta_p)) = \sum_{i=1}^{p-1}\sigma_i(y(1-\zeta_p)) \in (1-\zeta_p)\mathcal{O}_K$ as well. On the other hand, $y(1-\zeta_p) \in \mathcal{O}_K$, so its trace is in $\mathbf{Z}$. Therefore $\mathrm{Tr}_{K/\mathbf{Q}}(y(1-\zeta_p)) \in (1-\zeta_p)\mathcal{O}_K \cap \mathbf{Z} = p\mathbf{Z}$.

(d) Let $y = b_0 + b_1\zeta_p + \cdots + b_{p-1}\zeta_p^{p-1} \in \mathcal{O}_K$ where $b_i \in \mathbf{Q}$. Notice that for any $1 \le i \le p-1$, ζ_p^i is a conjugate of ζ_p over $\mathbf{Q}$, so

$$\mathrm{Tr}_{K/\mathbf{Q}}(\zeta_p^i) = \mathrm{Tr}_{K/\mathbf{Q}}(\zeta_p) = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1.$$

Set $b_p = b_0$, then for any $1 \le l \le p-1$, we have

$$\begin{aligned} p\mathbf{Z} \ni \mathrm{Tr}_{K/\mathbf{Q}}((\zeta^l y)(1-\zeta_p)) &= \sum_{i=0}^{p-1} b_i \,\mathrm{Tr}_{K/\mathbf{Q}}(\zeta_p^{i+l} - \zeta_p^{i+l+1}) \\ &= b_{p-l}\,\mathrm{Tr}_{K/\mathbf{Q}}(1-\zeta_p) + b_{p-l-1}\,\mathrm{Tr}_{K/\mathbf{Q}}(\zeta_p^{p-1} - 1) \\ &= p(b_{p-l} - b_{p-l-1}), \end{aligned}$$

which implies that $b_{p-l} - b_{p-l-1} \in \mathbf{Z}$. Thus $b_i - b_0 \in \mathbf{Z}$ for all $1 \le i \le p-1$. Notice that

$$y - \sum_{i=1}^{p-1}(b_i - b_0)\zeta_p^i = b_0(1+\zeta_p+\cdots+\zeta_p^{p-1}) = 0,$$

so $y = \sum_{i=1}^{p-1}(b_i - b_0)\zeta_p^i \in \mathbf{Z}[\zeta_p]$. Therefore $\mathcal{O}_K = \mathbf{Z}[\zeta_p]$.

Problem 6. Let $\theta \in \overline{\mathbf{Q}}$ be a root of the polynomial $f(X) = X^3 + 12X^2 + 8X + 1$. Let $K = \mathbf{Q}(\theta)$.

(a) Let $g(X) = X^3 + pX + q \in \mathbf{Z}[X]$. Compute the discriminant $\mathrm{disc}(g)$ of $g(X)$ in terms of p, q.

(b) Show that $f(X)$ is irreducible over $\mathbf{Q}$.

(c) Compute the discriminant $d_K(1, \theta, \theta^2)$. Please provide necessary details.

(d) For any arbitrary number field F of degree n, let $a_1, a_2, \ldots, a_n \in \mathcal{O}_F$. Find and verify a sufficient condition in terms of the discriminant $d_F(a_1, \ldots, a_n)$ that the $a_1, \ldots, a_n$ form an integral basis of F.

(e) Write down an explicit integral basis of K in terms of θ by using the above sufficient condition you have found. Please justify your arguments.

Solution:

(a) Let $\alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbf{Q}}$ be three roots of g, then by Viète's theorem

$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p, \quad \alpha_1\alpha_2\alpha_3 = -q.$$

According to the theory of symmetric polynomials, $\mathrm{disc}(g) = [(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)]^2$ can be expressed as a polynomial H of p, q. For any $\lambda \in \overline{\mathbf{Q}}$, consider

$$g_\lambda(X) = (X-\lambda\alpha_1)(X-\lambda\alpha_2)(X-\lambda\alpha_3) = X^3 + \lambda^2 pX + \lambda^3 qX,$$

we obtain that $H(\lambda^2 p, \lambda^3 q) = \lambda^6 H(p, q)$. Thus $H(p, q)$ has an expression such that each of its monomials has shape $r_{i,j}p^i q^j$ with $r_{i,j} \in \overline{\mathbf{Q}}$ and $2i + 3j = 6$. Thus $(i, j) = (3, 0)$ or $(0, 2)$, which means $\mathrm{disc}(g) = ap^3 + bq^2$ for some fixed $a, b \in \overline{\mathbf{Q}}$.

Let $g(X) = X^3 - X = X(X-1)(X+1)$, we have

$$a \cdot (-1)^3 + b \cdot 0^2 = [(0-1)(0-(-1))(1-(-1))]^2 = 4 \Rightarrow a = -4.$$

Let $g(X) = X^3 - 1 = X(X-\omega)(X-\omega^{-1})$, where $\omega = e^{2\pi i/3}$, then we have

$$a \cdot 0^3 + b \cdot (-1)^2 = \left[(1-\omega)(1-\omega^{-1})(\omega-\omega^{-1})\right]^2 = (1-\omega)^6 = \left(\sqrt{-3}e^{2\pi i/6}\right)^6 = -27 \Rightarrow b = -27.$$

Therefore $\mathrm{disc}(g) = -(4p^3 + 27q^2)$.

(b) Suppose f is reducible over $\mathbf{Q}$, then it has a factor $X - \tau$ where $\tau \in \mathbf{Q}$. Since τ is a root of $f(X)$, a monic integer polynomial, we have $\tau \in \mathcal{O}_K$. Thus $\tau \in \mathbf{Q} \cap \mathcal{O}_K = \mathbf{Z}$. Notice that $\tau(\tau^2 + 12\tau + 8) = -1$, we obtain that $\tau \mid 1$. Thus $\tau = \pm 1$. But a direct computation shows that neither of ± 1 is a root of $f(X)$, a contradiction.

(c) By (b) we see that $f(X)$ is the minimal polynomial of θ over $\mathbf{Q}$. Let $\theta_1 = \theta, \theta_2, \theta_3$ be the three roots of $f(X)$. Then

$$\begin{aligned}
d_K(1,\theta,\theta^2) &= \det\begin{pmatrix} 1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \end{pmatrix}^2 \\
&= \left[(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_3-\theta_1)\right]^2 \\
&= \left[((\theta_1+4)-(\theta_2+4))((\theta_2+4)-(\theta_3+4))((\theta_3+4)-(\theta_1+4))\right]^2 \\
&= \mathrm{disc}(f(X-4)) \\
&= \mathrm{disc}(X^3 - 40X + 97) \\
&= -\left[4 \cdot (-40)^3 + 3 \cdot 97^2\right] \\
&= 1957.
\end{aligned}$$

(d) We claim that if $d_F(a_1, \dots, a_n)$ is a square free integer, then $a_1, \dots, a_n$ is an integral basis of F. To see this, fix an integral basis $\omega_1, \dots, \omega_n$ of F. Then for any $1 \le i \le n$, there exist $t_{ij} \in \mathbf{Z}$ such that $a_i = \sum_{i=1}^n t_{ij}\omega_j$. Let $T = (t_{ij})_{1 \le i,j \le n} \in M_n(\mathbf{Z})$. Then linear algebra gives the following relation of integers

$$d_F(a_1, \dots, a_n) = (\det T)^2 d_F(\omega_1, \dots, \omega_n).$$

Since the left hand side is square free, we have $\det T = \pm 1$. This implies that T^{-1} has integer entries as well, thus $\omega_1, \dots, \omega_n$ can be written as $\mathbf{Z}$-linear combinations of $a_1, \dots, a_n$. Therefore, $a_1, \dots, a_n$ is an integral basis of F.

(e) Since $d_K(1,\theta,\theta^2) = 1957 = 19 \cdot 103$ is square free, $1, \theta, \theta^2$ is an integral basis of K by (d).