

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

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.

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 isomorphism; you should not use Dynkin diagrams or the classification theory of simple Lie algebras.)

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).

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 $\text{Tr}_{K/\mathbf{Q}}(1 - \zeta_p)$ 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

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

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

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 $\text{disc}(g)$ 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 $a_1, a_2, \dots, a_n \in \mathcal{O}_F$. Find and verify a sufficient condition in terms of the discriminant $d_F(a_1, \dots, a_n)$ that the a_1, \dots, 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.