S.-T. Yau College Student Mathematics Contests 2024

Algebra and Number Theory

Question 1. *Let G be a finite group.*

(1) *Let K be a field. Show that G has a finite-dimensional faithful K-linear representation.*

(2) *Show that G has a faithful one-dimensional complex representation if and only if G is cyclic.*

(3) *Assume moreover that G is commutative. Let $n \geq 1$ be an integer. Show that G has a faithful n-dimensional complex representation if and only if G can be generated by n elements.*

(4) *Classify all finite groups having a faithful 2-dimensional real representation.*

Question 2. *Let $n \geq 1$ be an integer. Let A be a discrete valuation ring with K its field of fractions and $\pi \in A$ a uniformizer. For $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ write*

$$D_\lambda = \mathrm{diag}(\pi^{\lambda_1}, \ldots, \pi^{\lambda_n}) = \begin{pmatrix} \pi^{\lambda_1} & 0 & \ldots & 0 \\ 0 & \pi^{\lambda_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \pi^{\lambda_n} \end{pmatrix} \in \mathbf{GL}_n(K).$$

Show that, for $\lambda, \mu \in \mathbb{Z}^n$, the following intersection inside $\mathbf{GL}_n(K)$

$$\mathbf{GL}_n(A) \cdot D_\mu \cdot \mathbf{GL}_n(A) \bigcap \mathbf{U}(K) \cdot D_\lambda$$

is non-empty if and only if $\lambda_{\mathrm{dom}} \leq \mu_{\mathrm{dom}}$. Here

- *$\mathbf{GL}_n(K)$ (resp. $\mathbf{GL}_n(A)$) is the group of invertible $n \times n$ square matrices with coefficients in K (resp. in A), and $\mathbf{U}(K) \subset \mathbf{GL}_n(K)$ is the standard unipotent subgroup, that is, the subgroup of upper triangular matrices with coefficients 1 on the diagonal.*
- *for $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ two elements in $\mathbb{Z}^n$, we write $\alpha \leq \beta$ if*

$$\sum_{i=1}^{k} a_i \leq \sum_{i=1}^{k} b_i, \quad \text{for any } 1 \leq k \leq n,$$

and if $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$. Write also $\alpha_{\mathrm{dom}} := (a'_1, \ldots, a'_n)$ with $a'_1, \ldots a'_n$ an arrangement of $a_1, \ldots, a_n$ such that

$$a'_1 \geq a'_2 \geq \ldots \geq a'_n.$$

Question 3. *Let k be an imperfect field of characteristic $p > 0$. Let $a \in k \setminus k^p$.*

(1) *Show that the polynomial $X^p - a \in k[X]$ is irreducible.*

(2) *Let $A = k[X]/(X^{p^2} - aX^p)$. Compute A_{red}, the quotient of A by its nilpotent radical.*

Question 4. *Let k be a field of character $p > 0$ and consider $k(t) \subset k((t))$.*

(1) *Show that the field extension $k((t))/k(t)$ is transcendental, i.e., $k((t))$ contains at least one transcendental element over $k(t)$. (**Hint: don't spend too much time on this question.**)*

(2) *Let $\alpha \in k[[t]]$ which is transcendental over $k(t)$, and write $\beta = \alpha^p \in k[[t]]$. Let $K = k(t, \beta)$ and $L = k(t, \alpha)$: both are subfields of $k((t))$. Let $A = k[[t]] \cap k(t, \beta)$. Determine the integral closure B of A in L, and show that A and B are two discrete valuation rings.*

(3) *Is B finitely generated over A as a module? Justify your assertion.*

Question 5. *Let p be a prime number. Consider $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) the ring of p-adic integers (resp. field of p-adic numbers). Clearly $\mathbb{Z} \subset \mathbb{Z}_p$.*

(1) *Show that the set $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, and deduce that a map $f : \mathbb{Z} \to \mathbb{Q}_p$ can be extended to a continuous function on $\mathbb{Z}_p$ if and only if f is uniformly continuous, i.e., for any $\epsilon > 0$, there exists some integer $N > 0$ so that $|f(n) - f(m)| < \epsilon$ for any integers $n, m \in \mathbb{Z}$ with $m \equiv n \ (mod\ p^N)$.*

(2) *Let $a \in \mathbb{Q}_p \setminus \{0\}$. Under what condition on a, the map*

$$f : \mathbb{Z} \longrightarrow \mathbb{Q}_p, \quad n \mapsto a^n$$

can be extended to a continuous function over $\mathbb{Z}_p$? Justify your assertion.

(3) *Assume that the condition in (2) is fulfilled. Can we even extend the function f in (2) to a continuous map*

$$a^x : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p,$$

so that $a^{x+y} = a^x a^y$ for any $x, y \in \mathbb{Q}_p$? Justify your assertion.

Question 6. *Let $n \geq 1$ be an integer and write $\Phi_n(X)$ the n-th cyclotomic polynomial, that is, the minimal polynomial of a primitive n-th root of unity in $\mathbb{C}$ over $\mathbb{Q}$. Write also $\varphi(n) = \deg(\Phi_n(X))$.*

(1) *Let q be a power of a prime number such that $(q, n) = 1$. Show that Φ_n, viewed as an element in $\mathbb{F}_q[X]$, can be decomposed as a product of $\varphi(n)/d$ irreducible polynomials of degree d, with d the order of q in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.*

(2) *From now on, assume $n = 2^{r+1}$ for some integer $r \geq 1$. Let $\zeta = \zeta_n$ be a primitive n-th root of unity and $K = \mathbb{Q}[\zeta]$. Let p be a prime with $p \equiv -3 \ (mod\ 8)$.*

   (a) *For $x, y \in K = \mathbb{Q}[\zeta]$, define*

$$(x, y) := \sum_\tau \tau(x) \cdot \overline{\tau(y)}$$

   where τ runs through all the embeddings $K \hookrightarrow \mathbb{C}$ of K into the field $\mathbb{C}$ of complex numbers. Write $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$, and we use the same notation to denote the (à priori $\mathbb{C}$-valued) bilinear form on $K_\mathbb{R}$ obtained by extension of scalars. Show that $(\cdot, \cdot)$ gives an inner product on $K_\mathbb{R}$ and for $0 \leq i, j < 2^r$,

$$(\zeta^i, \zeta^j) = \begin{cases} 2^r, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

   In particular, we obtain an Euclidean space $K_\mathbb{R}$ and $(\zeta^i/\sqrt{2^r})_{0 \leq i < 2^r}$ is an orthonormal basis.

   (b) *Decompose $p\mathcal{O}_K$ into a product of prime ideals.*

   (c) *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal of $\mathcal{O}_K$ containing p. Show that for every $\alpha \in \mathfrak{p}$, $|\alpha|^2 \in 2^r p\mathbb{Z}$, and compute the length of the shortest non-zero vector in the prime ideal $\mathfrak{p} \subset K_\mathbb{R}$.*