S.-T. Yau College Student Mathematics Contests 2025

Algebra and Number Theory
(5 problems)

Problem 1. *Let F be a field of characteristic $\neq 2$. Let F^* be the multiplicative group of non-zero elements of F, and $F^{*2} := \{a^2 | a \in F^*\} \subset F^*$. Show that F has a Galois extension of group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if $[F^* : F^{*2}] > 2$. Furthermore, show that such Galois extensions are precisely the splitting fields of irreducible polynomials of the form*

$$X^4 + aX^2 + b \in F[X]$$

with $b \in F^{*2}$.

Problem 2. *Let p be prime number, $e, f \in \mathbb{Z}_{\geq 1}$. Let G be a finite group of order $n := ef$ generated by two elements σ and τ, satisfying the relations*

$$\sigma^f = 1, \quad \tau^e = 1, \quad \text{and} \quad \sigma\tau\sigma^{-1} = \tau^p.$$

(1) *Show that such a group G exists if and only if $p^f \equiv 1 \pmod{e}$. If the latter condition is satisfied, there exists, up to isomorphisms, a unique finite group G as described above.*

(2) *Let $\mathbb{F}_{p^f}$ denote the finite field with p^f elements, and $\eta \in \mathbb{F}_{p^f}$ a primitive e-th root of unity. Let G act on $A := \mathbb{F}_{p^f}$ via*

$$\sigma(a) = a^p, \quad \tau(a) = \eta \cdot a.$$

Show that the following three assertions are equivalent:

(a) *The $\mathbb{F}_p$-representation A of G is absolutely irreducible in the sense that the C-representation $C \otimes_{\mathbb{F}_p} A$ of G is irreducible, where C is any algebraically closed field containing $\mathbb{F}_p$;*

(b) *the $\mathbb{F}_p$-representation A of G is irreducible;*

(c) *p is of order f in $(\mathbb{Z}/e\mathbb{Z})^\times$.*

Problem 3. *Let k be field.*

(1) *Let R be the localization of the polynomial ring $k[T]$ at the prime ideal (T). Let $n \geq 1$ be an integer. Let $\alpha_1, \ldots, \alpha_n \in k \setminus \{0\}$ be non-zero elements that are mutually different. Show that the following elements*

$$\frac{1}{T - \alpha_i}, \quad 1 \leq i \leq n$$

form a basis of the k-vector space $R/(T^n)$.

(2) *Let $A \subset k$ be an infinite subset (thus k is an infinite field). Let K/k be a finite field extension. Let $V \subset K(T)$ be the k-subspace of the rational function field $K(T)$ generated by*

$$\frac{1}{T - \alpha}, \quad \alpha \in A.$$

Let $\beta \in K \setminus A$ and consider the following additive valuation

$$\mathrm{ord}_\beta : K(T) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

normalized by $\mathrm{ord}_\beta(T - \beta) = 1$. Let $\Omega := \{\mathrm{ord}_\beta(f) : f \in V\} \subset \mathbb{Z}$, and for $n \geq 1$

$$u_n := \#\left(\Omega \cap \{0, 1 \ldots, n-1\}\right).$$

Show that $\frac{u_n}{n} \geq \frac{1}{[K:k]}$.

Problem 4. *Let E/F be a finite Galois extension of p-adic local fields, with Galois group Γ. Write $\mathcal{O}_F$ and $\mathcal{O}_E$ their rings of integers.*

(1) *Assume that E/F is unramified. Show that the following map*

$$\alpha : \mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_E \longrightarrow \prod_{\gamma\in\Gamma} \mathcal{O}_E, \quad c \otimes x \mapsto (c\gamma(x))_{\gamma\in\Gamma}$$

is an isomorphism. Here $\prod_{\gamma\in\Gamma} \mathcal{O}_E$ denotes the product of copies of $\mathcal{O}_E$ indexed by Γ.

(2) *Assume that E/F is unramified. Let $\mathcal{M}$ be an $\mathcal{O}_E$-module equipped with a semi-linear action of Γ: so for $\gamma \in \Gamma$ we have*

$$\gamma(a \cdot m) = \gamma(a) \cdot \gamma(m), \quad \forall a \in \mathcal{O}_E,\ m \in \mathcal{M}.$$

Show that the following natural map

$$\iota_M : \mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{M}^\Gamma \longrightarrow \mathcal{M}, \quad a \otimes m \mapsto am.$$

is an isomorphism. Here $\mathcal{M}^\Gamma = \{m \in M | \gamma(m) = m,\ \forall \gamma \in \Gamma\}$.

(3) *Assume that E/F is unramified. Write $\mathbf{Mod}_{\mathcal{O}_F}$ be the category of $\mathcal{O}_F$-modules, and $\mathbf{Mod}^\Gamma_{\mathcal{O}_E}$ be the category of $\mathcal{O}_E$-modules equipped with a semi-linear action of Γ. Show that the natural functor*

$$\Phi_{E/F} : \mathbf{Mod}_{\mathcal{O}_F} \longrightarrow \mathbf{Mod}^\Gamma_{\mathcal{O}_E}, \quad M \mapsto \mathcal{O}_E \otimes_{\mathcal{O}_F} M$$

is an equivalence of categories.

(4) *Assume that E/F is ramified. Is the corresponding functor $\Phi_{E/F}$ still an equivalence of categories? Justify your assertion.*

Problem 5. *Consider the polynomial $f(X) = X^5 - X + 1 \in \mathbb{Q}[X]$. Write $E/\mathbb{Q}$ its splitting field over $\mathbb{Q}$. Recall that for a polynomial $X^5 + aX + b \in \mathbb{Q}[X]$, its discriminant is $4^4a^5 + 5^5b^4$.*

(1) *Show that $f(X) \in \mathbb{Q}[X]$ is irreducible.*

(2) *Determine all the finite primes p that are ramified in E, and compute the order of the inertia subgroups.*

(3) *Show that $E/\mathbb{Q}[\sqrt{D}]$ is unramified at all finite primes of $\mathbb{Q}[\sqrt{D}]$, and that it is ramified at the Archimedean primes of $\mathbb{Q}[\sqrt{D}]$.*

(4) *Show that $\mathrm{Gal}(E/\mathbb{Q})$ can be generated by its inertia subgroups.*

(5) *Show that $\mathrm{Gal}(E/\mathbb{Q}) \simeq S_5$, and $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{D})) \simeq A_5$.*