S.-T. Yau College Student Mathematics Contests 2021

Algebra and Number Theory

Solve every problem.

Problem 1. For any prime p and a nonzero element $a \in \mathbf{F}_p$, prove that the polynomial $A(x) = x^p - x - a$ is irreducible and separable over $\mathbf{F}_p$.

Problem 2. Determine the automorphism group of the splitting field of $f(x) = x^3 - 3x + 1$ over $\mathbf{Q}$.

Problem 3. Let $R = F[x, y]/(x^2 - y^3)$ for some field F.

(a) Prove that R is an integral domain.

(b) If t denotes the element x/y in the fraction field K of R, prove that K is equal to $F(t)$.

(c) Prove that $F[t]$ is the integral closure of R in $K = F[t]$.

Problem 4. Let $p_1, \ldots, p_n$ be n distinct prime numbers. Show: $\sqrt{p_1} + \cdots + \sqrt{p_n}$ is not rational.

Problem 5. Find all integral solutions (x, y) for the equation $x^2 + 13 = y^3$. (**Hint:** You can use the fact that $\mathbf{Q}(\sqrt{-13})$ has class number 2).

Problem 6. Let p be a prime number and $\mathbf{Q}_p$ be the field of p-adic numbers. Fix an algebraic closure $\overline{\mathbf{Q}_p}$ of $\mathbf{Q}_p$. Let $g\colon \mathbf{Z}_{\geq 0} \to \mathbf{N}$ be a strictly increasing function. For each $i \in \mathbf{Z}_{\geq 0}$, pick a primitive $(p^{g(i)} - 1)$-th root of unity ζ_i in $\overline{\mathbf{Q}_p}$.

(a) Show that for each $i \geq 0$, $K_i := \mathbf{Q}_p(\zeta_i)$ is an unramified Galois extension of $\mathbf{Q}_p$ of degree $g(i)$.

(b) Give an explicit function g as above such that $K_{i-1} \subset K_i$ for all $i > 0$. Let $0 = N_0 < N_1 < N_2 \cdots$ be an increasing sequence of nonnegative integers. Let $\alpha_i := \sum_{j=0}^{i} \zeta_j p^{N_j}$. Show that for each $i \geq 0$, $K_i = \mathbf{Q}_p(\alpha_i)$ and that (α_i) is a Cauchy sequence in $\overline{\mathbf{Q}_p}$.

(c) Let $\eta \in \overline{\mathbf{Q}_p}$ be of degree g over $\mathbf{Q}_p$, prove that there exists $M \in \mathbf{N}$ such that ζ_i does not satisfy any congruence

$$s_{g-1}\eta^{g-1} + s_{g-2}\eta^{g-2} + \cdots + s_1\eta + s_0 \equiv 0 \pmod{p^M}$$

in which the s_i's are p-adic integers not all of which are divisible by p.

(d) Take a suitable sequence (N_i) as above such that (a_i) does not converge in $\overline{\mathbf{Q}_p}$. Conclude that $\mathbf{Q}_p$ is not complete with respect to the p-adic topology.