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 $\mathbf{F}_p$.

Solution: First of all, $A(x)$ is separable because $A'(x) = -1$ is non-zero. Second, $A(x)$ has no root in $\mathbf{F}_p$, since $A(b) = b^p - b - a = -a$ for any $b \in \mathbf{F}_p$. Notice that $A(x+a) = (x+a)^p - (x+a) - a = x^p + a^p - x - a - a = x^p - x - a = A(x)$. Therefore, by iteration, we see that $A(x + ba) = A(x)$ for all $b = 1, 2, \ldots$. As b runs over all positive integers, ba runs over $\mathbf{F}_p$. This means that in the splitting field K of $A(x)$ over $\mathbf{F}_p$, if a is a root, then, so is $a + k$, $k \in \mathbf{F}_p$. It follows that

$$A(x) = \prod_{k=0}^{p-1}(x - a - k).$$

If $A(x)$ is not irreducible over $\mathbf{F}_p$, then there exist $r(x), s(x) \in \mathbf{F}_p[x]$ such that $A(x) = r(x)s(x)$ and $0 < d = \deg r(x) < p$. Being a divisor of $A(x)$, $r(x)$ has the form

$$r(x) = \prod_{k \in J}(x - a - k),$$

for some subset $J \subset \mathbf{F}_p$. The coefficient of x^{d-1} of $r(x)$ is the negative of the sum of all roots of $r(x)$, hence it is equal to

$$\sum_{i \in J}(a + i) = da + \sum_{i \in J} i \in \mathbf{F}_p.$$

Then, $a \in \mathbf{F}_p$, a contradiction.

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

Solution: $f(x)$ is irreducible over $\mathbf{Z}$ (hence over $\mathbf{Q}$ as well). To see this we reduce mod 2 and evaluate: $f(0) = 1, f(1) = 1$.

Next, $f'(x) = 3x^2 - 3$ is positive outside the interval $(-1, 1)$ and negative in the interval $(-1, 1)$. Since $f(-1) = 3$ and $f(1) = 1$, we see that there are three real roots, denoted a_1, a_2 and a_3. Since $f(x)$ is irreducible of degree 3, $\dim_{\mathbf{Q}} \mathbf{Q}(a_i) = 3$. Let K denote the splitting field of $f(x)$. Thus, K is either degree 6 over $\mathbf{Q}$, or it is degree 3 over $\mathbf{Q}$. In the latter case the automorphism group is cyclic group of order 3. Let us prove that the former case is not possible. In fact, in the former case the automorphism group $G = \mathrm{Aut}_{\mathbf{Q}}K = S_3$, the symmetric group on 3 letters. We let σ be the automorphism that maps a_1 to a_3, a_3 to a_1 and a_2 to a_2. Write $f(x) = (x - a_1)(x - a_2)(x - a_3)$. By taking the derivative of $f(x)$ and substituting a_i into this equation gives

$$(a_1 - a_2)(a_1 - a_3) = 3a_1^2 - 3,$$

$$(a_2 - a_1)(a_2 - a_3) = 3a_2^2 - 3,$$

$$(a_3 - a_1)(a_3 - a_2) = 3a_3^2 - 3.$$

Take the product of the above three equations and then take the square roots, we have

$$\prod_{1 \le i < j \le 3} (a_i - a_j) = 9.$$

Then apply the permutation σ to the above, the left is sent to its negative, but 9 is obviously fixed by σ. Therefore, σ cannot be in G. It follows that the automorphism group G must be the cyclic group of order 3. Moreover, $\mathbf{Q}(a_1) = \mathbf{Q}(a_1, a_2, a_3)$.

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 $K = F[t]$.

Solution:

(a) To prove $x^2 - y^3$ is irreducible, it suffices to show that it is irreducible in $F(y)[x]$. Since it is a quadratic polynomial in x over $F(y)$, it is reducible if and only if it has a root in $F(y)$. Suppose $f(y)/g(y)$ is a root, where $f(y)$ and $g(y)$ are co-prime. But, $(f(y)/g(y))^2 - y^3 = 0$ implies $f(y)^2 = y^3 g(y)^2$. Thus, an irreducible factor of $g(y)$ divides $f(y)^2$, hence divides $f(y)$, a contradiction. This implies the ideal generated by $x^2 - y^3$ is prime since $F[x, y]$ is a UFD. Hence, R is an integral domain.

(b) Since $x^2 = y^3$ in R, we have $y = (x/y)^2 = t^2$ in K. Also, $x = yx/y = yt = t^3$. Thus, any element $f(x, y) \in R$ is a polynomial in t in K. Therefore, any element $f(x, y)/g(x, y) \in K$ belongs to $F(t)$. On the other hand, $F(t) \subset K$, hence $K = F(t)$.

(c) Let $h(t) \in F[t] \subset F(t)$. Replacing t^2 by y and t^3 by x (from **(b)**), we have $h(t) = at + g(x, y)$ for some $g(x, y) \in R$. Then, we have $(h(t) - g(x, y))^2 = (at)^2 = a^2 y$. Thus, $h(t)$ is a root of $X^2 - 2g(x, y)X + g(x, y)^2 - a^2 y^2 \in R[X]$. This implies that $F[t]$ is integral over R. Suppose now that $h(t) \in F(t)$ is integral over R. Then $h(t)$ is also integral over $F[t]$. But, $F(t)$ is the fraction field of $F[t]$ and $F[t]$ is a UFD, hence $F[t]$ is integrally closed. Therefore, $h(t) \in F[t]$.

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

Solution: It suffices to show $[\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbf{Q}] = 2^n$ (this implies that the 2^n numbers $1, \sqrt{p_{\alpha_1} \cdots p_{\alpha_k}}$ $(1 \le \alpha_1 < \cdots < \alpha_k \le n)$ are linear independent over $\mathbf{Q}$). We show the following stronger result:

Lemma: *Suppose K is a field with characteristic 0, and $\{x_1, \ldots, x_n\} \subset K$ is a subset such that the product of elements of any non-empty subset of $\{x_1, \ldots, x_n\}$ is not a square in K. Then $[K(\sqrt{x_1}, \ldots, \sqrt{x_n}) : K] = 2^n$.*

We prove the lemma by induction on n. The case $n = 1$ is trivial. Suppose $n = 2$ and we aim to show $[K(\sqrt{x_1}, \sqrt{x_2}) : K] = 4$. Since we have $[K(\sqrt{x_1}) : K] = 2$, it suffices to prove $[K(\sqrt{x_1}, \sqrt{x_2}) : K(\sqrt{x_1})] = 2$. We only need to prove $\sqrt{x_2} \notin K(\sqrt{x_1})$. If not, then $\sqrt{x_2} = a + b\sqrt{x_1}$ with $a, b \in K$. Since $\sqrt{x_1} \notin K$, we have $b \neq 0$. Then $a^2 = (\sqrt{x_2} - b\sqrt{x_1})^2$ implies that $\sqrt{x_1 x_2} \in K$, which is a contradiction. We conclude the lemma for $n = 2$.

Now suppose $n \ge 3$ and suppose for smaller n the lemma holds. By the induction assumption, we have $[K(\sqrt{x_3}, \ldots, \sqrt{x_n}) : K] = 2^{n-2}$. Denote $L = K(\sqrt{x_3}, \ldots, \sqrt{x_n})$. Then we only need to show $[L(\sqrt{x_1}, \sqrt{x_2}) : L] = 4$. It suffices to prove $\sqrt{x_1}, \sqrt{x_2}, \sqrt{x_1 x_2} \notin L$. Suppose one of $\sqrt{x_1}, \sqrt{x_2}, \sqrt{x_1 x_2}$, say y, belong to L. Then $L(y) = L$, which implies that $[K(y, \sqrt{x_3}, \ldots, \sqrt{x_n}) : K] = 2^{n-2}$. But on the other hand, by the induction-assumption, we must have $[K(y, \sqrt{x_3}, \ldots, \sqrt{x_n}) : K] = 2^{n-1}$, a contradiction!

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).

Solution: The only solutions are $(x, y) = (\pm 70, 17)$.

Suppose $x^2 + 13 = y^3$ has integral solution (x, y). We may first assume x, y are positive. It is easy to see that $\gcd(x, y) = 1$. If y is even, then x is odd and $x^2 + 13 \equiv 6 \pmod 8$. But $y^3 \equiv 0 \pmod 8$. This is impossible. Therefore, x is even and y is odd.

In $\mathbf{Z}[\sqrt{-13}]$ we have $(x + \sqrt{-13})(x - \sqrt{-13}) = y^3$. Consider the principal ideals $(x + \sqrt{-13}), (x - \sqrt{-13}), (y) \subset \mathbf{Z}[\sqrt{-13}]$. Suppose $(x + \sqrt{-13})$ and $(x - \sqrt{-13})$ are not coprime to each other, then there exists a prime ideal $P \subset \mathbf{Z}[\sqrt{-13}]$ such that $P \big| (x + \sqrt{-13})$ and $P \big| (x - \sqrt{-13})$. Then $x \pm \sqrt{-13} \in P$, which implies that $2\sqrt{-13} \in P$ and $2x \in P$. We have also $P \big| (y)^3$ which implies that $P \big| (y)$. Thus $y \in P$. But $\gcd(2x, y) = 1$, a contradiction.

We conclude that $(x+\sqrt{-13})$ and $(x-\sqrt{-13})$ are two ideals coprime to each other. Since $\mathbf{Z}[\sqrt{-13}]$ is a Dedekind ring, there exists ideals P_1, P_2 such that $(x+\sqrt{-13}) = P_1^3$, $(x-\sqrt{-13}) = P_2^3$ and $(y) = P_1P_2$.

Since the class number of $\mathbf{Z}[\sqrt{-13}]$ is 2, the square of any fractional ideal is principal. Since P_i^3 is principal, we know that P_i is principal. Note that the units of $\mathbf{Z}[\sqrt{-13}]$ are ± 1. Thus there exists $a, b \in \mathbf{Z}$, such that $x+\sqrt{-13} = (a+b\sqrt{-13})^3$. Comparing the coefficient of $\sqrt{-13}$, we conclude that $1 = 3a^2b - 13b^3$. This implies $b = -1$ and $a = \pm 2$. Thus $x = \pm 70$, $y = 17$.

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.

Solution:

(a) Let v_p be the usual p-adic valuation of $\mathbf{Q}_p$, then v_p has a unique extension to K_i, which is $v_{K_i}(x) := [K_i\colon \mathbf{Q}_p]^{-1} v_p(\mathcal{N}_{K_i/\mathbf{Q}_p}(x))$. The relation $\zeta_i^{p^{g(i)}-1} = 1$ implies that $v_{K_i}(\zeta_i) = 0$, so $\zeta_i \in O_{K_i}$. Let $P(X) \in \mathbf{Z}_p[X]$ be the minimal polynomial of ζ_i over $\mathbf{Q}_p$, then $P(X)$ is a factor of $X^{p^{g(i)}-1} - 1$. Since ζ_i is primitive, we see that $\zeta_i^l \in K_i, 0 \leq l \leq p^{g(i)} - 1$ are all roots of $X^{p^{g(i)}-1} - 1$. Thus each root of $P(X)$ has shape $\zeta_i^l \in K_i$, which implies that $K_i/\mathbf{Q}_p$ is normal. Since $\mathrm{char}(\mathbf{Q}_p) = 0$, all its extensions are separable. So $K/\mathbf{Q}_p$ is a Galois extension.

The reduction $\overline{P}(X) \in \mathbf{F}_p[X]$ of $P(X)$ is also a factor of $X^{p^{g(i)}-1} - 1 \in \mathbf{F}_p[X]$. Since p and $p^{g(i)} - 1$ are coprime, $X^{p^{g(i)}-1} - 1 \in \mathbf{F}_p[X]$ has no multiple roots. Using Hensel's lemma and the fact that $P(X) \in \mathbf{Z}_p[X]$ is irreducible, we see that $\overline{P}(X)$ is also irreducible.

Let $\overline{K_i}$ be the residue field of K_i, then $\overline{\zeta_i} \in \overline{K_i}$ is a root of $\overline{P}(X)$. We see that $[\overline{K_i}\colon \mathbf{F}_p] \geq [\mathbf{F}_p(\overline{\zeta_i})\colon \mathbf{F}_p] = \deg(\overline{P}) = \deg(P) = [K_i\colon \mathbf{Q}_p]$. It follows that the ramification index e satisfies

$$1 \leq e = [K_i\colon \mathbf{Q}_p]/[\overline{K_i}\colon \mathbf{F}_p] \leq 1.$$

Thus $e = 1$, i.e. $K/\mathbf{Q}_p$ is an unramified extension.

The argument above also implies the equality $[\overline{K_i}\colon \mathbf{F}_p] = [K_i\colon \mathbf{Q}_p]$, the relation $\overline{K_i} = \mathbf{F}_p[\overline{\zeta_i}]$ and the property that $\overline{K_i}$ contains all $(p^{g(i)}-1)$-th roots of unity. Thus $\overline{K_i}/\mathbf{F}_p$ is cyclotomic and $\overline{\zeta_i}$ is primitive. Now, since $\overline{K_i}^\times$ is a cyclic group of order $p^{[K_i\colon \mathbf{Q}_p]} - 1$, we get that $[K_i\colon \mathbf{Q}_p] = g(i)$. Thus the degree of ζ_i over $\mathbf{Q}_p$ is $g(i)$.

(b) Take any sequence $g(i)$ such that $g(i)/g(i-1)$ is an integer at least 2, *e.g.*, $g(i) = 2^i$. Then $(p^{g(i-1)}-1) \mid (p^{g(i)}-1)$, so ζ_{i-1} is a power of ζ_i. Thus $K_{i-1} \subset K_i$ holds for each $i > 0$. For any $1 < i < i'$, we have

$$v_{K_{i'}}(\alpha_{i'} - \alpha_i) = v_{K_{i'}}(p^{i+1}) + v_{K_{i'}}(\text{an element in } O_{K_{i'}}) \geq i + 1,$$

which means that (α_i) is a Cauchy sequence.

Take any $\sigma \in \mathrm{Gal}(K_i/\mathbf{Q}_p)\backslash\{\mathrm{id}\}$. Notice that $\sigma(\alpha_i) = \sum_{j=0}^{i} \sigma(\zeta_i) p^{N_i}$. Since $\zeta_i \neq \sigma(\zeta_i)$, we get $v_{K_i}(\alpha - \sigma(\alpha_i)) = v_{K_i}((\zeta_i - \sigma(\zeta_i))p^{N_i} + \cdots) = N_i < \infty$. So $\sigma(\alpha_i) \neq \alpha_i$, *i.e.*, σ does not fix α_i. Thus $\mathbf{Q}_p(\alpha_i) = K_i$.

(c) Suppose the contrary, then for any $M \in \mathbf{N}$, there exist $s_{g-1}^M, \cdots, s_0^M \in \mathbf{Z}_p$, not all divisible by p, such that

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

By the pigenhole principle, there are an $0 \leq j \leq g-1$ and an infinite subset $R \subset \mathbf{Z}_{\geq 0}$ such that $p \nmid s_i^M$ for all $M \in R$. Since $\mathbf{Z}_p$ is sequentially compact, so is $\mathbf{Z}_p^g$. Thus the sequence $(s_{g-1}^M, \cdots, s_0^M)_{M \in R} \in \mathbf{Z}_p^g$ has a convergent subsequence. Let $(s_{g-1}, \cdots, s_0) \in \mathbf{Z}_p^g$ be the limit of this subsequence. Then $p \nmid s_j$ and

$$s_{g-1}\eta^{g-1} + s_{g-2}\eta^{g-2} + \cdots + s_\eta + s_0 \equiv 0 \pmod{p^r}, \text{ for any } r \in \mathbf{N}.$$

In other words, $v_{\mathbf{Q}_p(\eta)}(s_{g-1}\eta^{g-1} + s_{g-2}\eta^{g-2} + \cdots + s_\eta + s_0) \geq r$ for all $r \in \mathbf{N}$, thus equals to ∞. So $s_{g-1}\eta^{g-1} + s_{g-2}\eta^{g-2} + \cdots + s_\eta + s_0 = 0$, contradicting the assumption that η has degree g over $\mathbf{Q}_p$.

(d) We will take an increasing sequence (N_i) by induction. We have $N_0 = 0$ already given. Suppose we have defined N_j for all $j \leq i$, so that we have $\alpha_i = \sum_{j=0}^{i} \zeta_j p^{N_j}$ determined. Since α_i has degree $g(i)$ over $\mathbf{Q}_p$, by **(c)**, there exists $N_{i+1} > N_i$ such that ζ_i does not satisfy any congruence

$$t_n \alpha_i^n + t_{n-1}\alpha_i^{n-1} + \cdots + t_1\alpha_i + t_0 \equiv 0 \pmod{p^{N_{i+1}}},$$

for any $n < g(i)$ and $t_j \in \mathbf{Z}_p$ not all divisible by p. Then the sequence (N_i) is completely defined.

Suppose $\overline{\mathbf{Q}_p}$ is complete, then (α_i) converges to certain $\alpha \in \overline{\mathbf{Q}_p}$. Then there exist $t_n, t_{n-1}, \ldots, t_0 \in \mathbf{Z}_p$, not all divisible by p, such that

$$t_n \alpha^n + t_{n-1}\alpha^{n-1} + \cdots + t_1\alpha + t_0 = 0.$$

Choose i with $g(i) > n$. Since $\alpha \equiv \alpha_i \pmod{p^{N_i}}$, we have

$$t_n \alpha_i^n + t_{n-1}\alpha_i^{n-1} + \cdots + t_1\alpha_i + t_0 \equiv 0 \pmod{p^{N_{i+1}}},$$

a contradiction. This proves the assertion.