S.-T. Yau College Student Mathematics Contests 2020

Algebra and Number Theory

Solve every problem.

Problem 1. Let F be a field of characteristic zero. Consider the polynomial ring $F[x_1, \dots, x_n]$.

(a) Prove Newton's identity over the field F

$$p_k - p_{k-1}e_1 + \cdots + (-1)^{k-1}p_1 e_{k-1} + (-1)^k k e_k = 0,$$

where

$$e_k(x_1, \dots, x_n) = \sum_{1 \le i_1 < \cdots < ß_k \le n} x_{i_1} \cdots x_{i_k}$$

for $1 \le k \le n$, $e_0 = 1$, $e_k = 0$ when $k > n$, and

$$p_k(x_1, \dots, x_n) = x_1^k + \cdots + x_n^k.$$

(b) Prove that over the field of F of characteristic zero, an $n \times n$ matrix A is nilpotent if and only if the trace of A^k is equal to zero for all $k = 1, 2 \dots$

Hint: use Part (a).

(c) Prove that over the field of F of characteristic zero, two $n \times n$ matrix A and B have the same characteristic polynomial if and only if the trace of A^k and trace of B^k are equal for all $k = 1, 2 \dots$

Hint: use Part (a).

Solution: Part (a): Consider

$$E(y) = \prod_{i=1}^{n}(1 - x_i y) = 1 - e_1 y + e_2 y^2 + \cdots (-1)^n e_n y^n.$$

Using $-\ln(1-t) = \sum_{j=1}^{\infty} t^j/j$, we obtain

$$\ln(E(y)) = \sum_{i=1}^{n} \ln(1 - x_i y) = -\sum_{i=1}^{n}\sum_{j=1}^{\infty}(x_i y)^j/j = -\sum_{j=1}^{\infty} p_j y^j/j.$$

Apply d/dy to the above, we have

$$E'(y)/E(y) = -\sum_{j=1}^{\infty} p_j y^{j-1}, \quad \text{or} \quad -E'(y) = E(y)\sum_{j=1}^{\infty} p_j y^{j-1}.$$

By comparing the coefficients of y^{k-1} of both sides, we obtain

$$-(-1)^k k e_k = \sum_{j=0}^{k-1}(-1)^j e_j p_{k-j}.$$

Part (b): Suppose A is nilpotent. Then, the minimal polynomial of A is x^r for some integer r. It follows that the characteristic of A is $f(x) = x^n$. The trace of A is equal to a_{n-1} where $-a_{n-1}$ is the coefficient of x^{n-1} of $f(x)$, hence is equal to 0. Similarly, A^k is nilpotent, hence its trace is zero.

Conversely, assume trace of A^k equals 0 for all $k \geq 1$. If λ is an eigenvalue of A, then λ^k is an eigenvalue of A^k. Since the trace is the sum of eigenvalues, we see that (the sums of powers) $p_k(\ldots,\lambda,\ldots) = 0$. By Part (a), we see that $e_k(\ldots,\lambda,\ldots) = 0$. Since the coefficients of the characteristic polynomial $f(t)$ of A are precisely $e_k(\ldots,\lambda,\cdots)$ for $0 \leq k \leq n$ (possibly up to $\pm$ signs), we obtain $f(t) = t^n$, hence $A^n = 0$.

Part (c): Suppose that A and B have the same characteristic polynomials. Let λ_A (resp. λ_B) be an eigenvalue of A (resp. B). Then, $e_k(\ldots,\lambda_A,\ldots) = e_k(\ldots,\lambda_B,\ldots)$ for all $k \geq 0$. By (a), $p_k(\ldots,\lambda_A,\ldots) = p_k(\ldots,\lambda_B,\ldots)$. Since the trace is the sum of eigenvalues, we obtain the trace of A^k and trace of B^k are equal. Conversely, if the trace of A^k and trace of B^k are equal for all k, then $p_k(\ldots,\lambda_A,\ldots) = p_k(\ldots,\lambda_B,\ldots)$. Hence, $e_k(\ldots,\lambda_A,\ldots) = e_k(\ldots,\lambda_B,\ldots)$ for all $k \geq 0$. Thus, A and B have the same characteristic polynomials.

Problem 2.

(a) Let M be a finitely generated R-module and $\mathfrak{a} \subset R$ an ideal. Suppose $\phi : M \longrightarrow M$ is an R-module map such that $\phi(M) \subseteq \mathfrak{a}M$. Prove that there is a monic polynomial $p(t) \subset R[t]$ with coefficients from $\mathfrak{a}$ such that $p(\phi) = 0$.

Hint: $p(t)$ is basically just the characteristic polynomial.

(b) If M is a finitely generated R-module such that $\mathfrak{a}M = M$ for some ideal $\mathfrak{a} \subset R$, then there exits $x \in R$ such that $1 - x \in \mathfrak{a}$ and $xM = 0$.

Solution: Part (a): Let $x_1, \ldots, x_m$ be a generating set for M as an R-module. We have

$$\phi(x_i) = \sum a_{ij} x_j$$

for some $a_{ij} \in \mathfrak{a}$. Let A_{ij} be the operator $\delta_{ij}\phi - a_{ij}\mathrm{Id_M}$ where $\mathrm{Id_M} : M \longrightarrow M$ is the identity hom and δ_{ij} is the Kronecker's symbol. Then we have $\sum_j A_{ij}x_j = 0$ for all j. The matrix $A = (A_{ij})$ annihilates the column vector $v = (x_j)_{j=1}^m$, Consider M as an $R[\phi]$-module, then $A_{ij} \in R[\phi]$. Thus, A is a matrix with entries in $R[\phi]$. Its adjugate is well-defined. Multiplying $Av = 0$ on the left by the adjugate gives rise to $\det A \ x_j = 0$ for all j. Let $p(\phi) = \det A(\phi)$ (recall $A = (\delta_{ij}\phi - a_{ij}\mathrm{Id_M})$). Then, $p(t)$ is a monic polynomial and $p(\phi) = 0$ on M.

Part (b): By Part (a), $\mathrm{Id_M} : M \longrightarrow M$ satisfies

$$\mathrm{Id_M}^r + a_1 \mathrm{Id_M}^{r-1} + \cdots + a_r \mathrm{Id_M} = 0$$

for some $a_j \in \mathfrak{a}$. Let $x = 1 + a_1 + \cdots + a_r$, then $x - 1 \in \mathfrak{a}$ and $xM = 0$.

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

(a) Prove that R is an integral domain.

(b) Compute the normalization of R (*i.e.*, the integral closure of R in its field of fraction).

Solution: Part (a): It suffices to prove that $y^2 - x^2 - x^3$ is irreducible in $F(x)[y]$. It is reducible if it has a root $f(x)/g(x) \in F(x)$, where $f(x)$ and $g(x)$ are co-prime. But $(f(x)/g(x))^2 - x^2 - x^3 = 0$ implies $f(x)^2 = g(x)^2(x^2 + x^3) = (g(x)x)^2(x+1)$. Thus, $(x+1)$ divides $f(x)$. Hence, $(x+1)^2$ divides $f(x)^2$. It follows that $(x+1)$ divides $g(x)$, a contradiction. This implies that R is an integral domain.

Part (b): We have $0 = y^2 - x^3 - x^2 = x^2(y^2/x^2 - x - 1) = x^2(t^2 - x - 1)$. As K is an integral domain, $t^2 - x - 1 = 0$, that is, $x = t^2 - 1$. Then $y = xy/x = (t^2 - 1)t$. It follows that any element of R is a polynomial in t, hence $R \subset F[t]$. Therefore $K \subset F(t)$. Thus, $K = F(t)$.

Now let S be the integral closure of R in K. We claim $S = F[t]$. Let $f(t) \in F[t]$. Let $s = 2k$ be an even integer. Then

$$t^s = (t^2)^k = ((t^2 - 1) + 1)^k = \sum_{i=0}^{k} \binom{k}{i} (t^2 - 1)^i = \sum_{i=0}^{k} \binom{k}{i} x^i.$$

Let $s = 2k + 1$ be an odd integer with $s > 3$, using the above, we obtain

$$t^s = t^s - t^{s-2} + t^{s-2} = t^{s-3}(t^2 - 1)t + t^{s-2} = \left(\sum_{i=0}^{k-1} \binom{k-1}{i} x^i\right) y + t^{s-2}.$$

Repeat the above for the odd integer $s - 2$, by induction, we see that t^s is of the form $g(x, y) + at$. Combing all the above, we see that $f(t)$ is of the form $h(x, y) + bt$ for some $b \in \mathbb{Z}$ and $h(x, y) \in R$. Then, $f(t)$ is a root of

$$(X - h(x, y))^2 - b^2 - b^2 x \in R[X].$$

it follows that $f(t) \in S$. Hence, $F[t] \subset S$. But, $R \subset F[t]$ and $F[t]$ is integrally closed in $F(t)$, hence $S \subset F[t]$. Therefore $S = F[t]$.

Problem 4. Let p and ℓ be two prime numbers and $[\ell_x]$ denote the ℓ-th cyclotomic polynomial $1 + x + \cdots + x^{\ell-1}$.

(a) Prove that $[\ell_x]$ is an irreducible element of $\mathbb{Q}[x]$.

(b) Show that $[\ell_x]$ is divisible by $x - 1$ in $\mathbb{F}_p[x]$ if $p = \ell$. Here $\mathbb{F}_p$ is the finite field $\mathbb{Z}/p\mathbb{Z}$.

(c) Suppose $p \neq \ell$. let a be the order of p in $\mathbb{F}_\ell$. Show that a is the first value of m for which the group $\mathrm{GL}_m(\mathbb{F}_p)$ of invertible $m \times m$ matrices with entries from $\mathbb{F}_p$ contains an element of order ℓ.

Hint: Derive and use the formula for the number of elements in $\mathrm{GL}_m(\mathbb{F}_p)$.

Solution: Part (a): $[\ell_x]$ is irreducible over $\mathbb{Q}$ if and only if $[\ell_{x+1}]$ is irreducible$\mathbb{Q}$.

$$[\ell_{x+1}] = ((x+1)^\ell - 1)/((x+1) - 1) = x^{\ell-1} + \ell x^{\ell-2} + \cdots + \ell(\ell-1)/2x + \ell.$$

This is irreducible by Eisenstein's criterion.

Part (b): $p = \ell$. If $p = 2$, then $[2]_x = 1 + x = x - 1$ If $p > 2$, then

$$[p]_x = (x^p - 1)/(x - 1) = (x - 1)^{p-1}.$$

Part (c): Let $e_1, \ldots, e_m$ be the standard basis of $\mathbb{F}_q^n$, where q is a prime power. If $A \in \mathrm{GL}_m(\mathbb{F}_q)$, then the columns of A, $\{Ae_1, \ldots, Ae_n\}$, form a basis for $\mathbb{F}_q^n$. Conversely, any basis form columns of an element $A \in \mathrm{GL}_m(\mathbb{F}_q)$. Thus, it is equivalent to count the number of bases $\mathcal{B} = (f_1, \ldots, f_n)$ for $\mathbb{F}_q^n$. The first vector has $q^m - 1$ choices. The second, not a multiple of the first, has $q^m - q$ choices. The third vector $f_3 \in \mathbb{F}_q^n \setminus \{af_1 + bf_2 \mid a, b \in \mathbb{F}_q\}$ has $q^m - q^2$ choices. Inductively, f_i has $q^m - q^i$ choices. Therefore

$$\left|\mathrm{GL}_m(\mathbb{F}_q)\right| = (q^m - 1)(q^m - q)\cdots(q^m - q^{m-1}).$$

If $\mathrm{GL}_m(\mathbb{F}_p)$ contains an element of order ℓ, then ℓ divides

$$|\mathrm{GL}_m(\mathbb{F}_p)| = p^{\binom{m}{2}} \prod_{i=1}^{m} (p^i - 1).$$

Sicne $\ell \neq p$, the first value of m such that ℓ divides the above is when ℓ divides the highest term $p^m - 1$ for the first time. This happens when $p^a - 1 = 0 \bmod \ell$.

Problem 5. Let $p \geq 3$ be a prime number and let $\mathbb{Z}_p$ be the ring of p-adic integers.

(a) Show that an element in $1 + p\mathbb{Z}_p$ is a p-th power in $\mathbb{Z}_p$ if and only if it lives in $1 + p^2\mathbb{Z}_p$.

(b) Let $\mathbb{Z}_p^\times$ denote the group of units in $\mathbb{Z}_p$. Show that there exist $a, b, c \in \mathbb{Z}_p^\times$ such that $a^p + b^p = c^p$ if and only if

$$\sum_{i=1}^{p-1} i^{p-2} t^i \equiv 0 \pmod{p}$$

for some integer $t \in \{2, 3, \ldots, p-1\}$. (In particular, this condition holds for $p = 7$ by taking $t = 3$. Therefore, Fermat's Last Theorem does not hold for $\mathbb{Z}_7$.)

Solution: Part (a): If an element in $1 + p\mathbb{Z}_p$ is a p-th power, it must have form $(1 + p\alpha)^p$ for some $\alpha \in \mathbb{Z}_p$. A simple calculation yields

$$(1 + p\alpha)^p = 1 + \binom{p}{1} p\alpha + \binom{p}{2} (p\alpha)^2 + \cdots \in 1 + p^2\mathbb{Z}_p.$$

To prove sufficiency, recall the two functions

$$\exp : p\mathbb{Z}_p \longrightarrow 1 + p\mathbb{Z}_p, \qquad \log : 1 + p\mathbb{Z}_p \longrightarrow p\mathbb{Z}_p$$

which are inverses to each other. For any $a = 1 + p^2 x \in 1 + p^2\mathbb{Z}_p$, consider

$$a^{\frac{1}{p}} := \exp\left(\frac{1}{p}\log(a)\right).$$

Notice that

$$\frac{1}{p}\log(a) = \frac{1}{p}\log\left(1 + p^2 x\right) = \frac{1}{p}\sum_{i=1}^{\infty} \frac{(-1)^{i-1}}{i}\left(p^2 x\right)^i \in p\mathbb{Z}_p$$

and hence $a^{\frac{1}{p}}$ is well-defined. It is clear that $\left(a^{\frac{1}{p}}\right)^p = a$.

Part (b): As an immediate corollary from Part (a), if we write an element $a \in \mathbb{Z}_p^\times$ in terms of Witt coordinates $a = (a_0, a_1, \ldots)$, then a is a p-th power in $\mathbb{Z}_p$ if and only if $a_1 = 0$. In particular, whether an element in $\mathbb{Z}_p^\times$ is a p-th power can be detected by its image under the projection $\mathbb{Z}_p = W(\mathbb{F}_p) \longrightarrow W_2(\mathbb{F}_p)$.

Hence, there exist $a, b, c \in \mathbb{Z}_p^\times$ such that $a^p + b^p = c^p$ if and only if there exist $a_0, b_0, c_0 \in \mathbb{F}_p^\times$ such that $(a_0, 0) + (b_0, 0) = (c_0, 0)$ in $W_2(\mathbb{F}_p)$. Using the addition formula of Witt coordinates, the later equation translates to $a_0 + b_0 = c_0$ and

$$\frac{1}{p}\left(a_0^p + b_0^p - (a_0 + b_0)^p\right) = 0.$$

Direct calculation gives

$$\begin{aligned}
\frac{1}{p}(a_0^p + b_0^p - (a_0 + b_0)^p) &= -\sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} a_0^i b_0^{p-i} \\
&= -\sum_{i=1}^{p-1} \frac{1}{i} \frac{(p-1)(p-2)\cdots(p-i+1)}{(i-1)\cdots 1} a_0^i b_0^{p-i} \\
&\equiv \sum_{i=1}^{p-1} \frac{1}{i}(-1)^i a_0^i b_0^{p-i} \equiv \sum_{i=1}^{p-1} i^{p-2}\left(-\frac{a_0}{b_0}\right)^i \pmod{p}
\end{aligned}$$

Since $a_0 + b_0 = c_0 \neq 0$, we have $-\frac{a_0}{b_0} \neq 1$. Namely, there exists $t \in \{2, 3, \ldots, p-1\}$ such that

$$\sum_{i=1}^{p-1} i^{p-2} t^i \equiv 0 \pmod{p}.$$

All steps above are clearly reversible and hence cover both the "if" and "only if" parts. This completes the proof.

Problem 6. Recall that a metric space is called *spherically complete* if any decreasing sequence of closed balls has nonempty intersection.

Let p be a prime number and let $\mathbb{Q}_p$ be the field of p-adic numbers. For every integer $n \geq 1$, consider the finite extension $\mathbb{Q}_p(\mu_{p^n})$ of $\mathbb{Q}_p$ generated by all p^n-th roots of unity. Let $\mathbb{Q}_p(\mu_{p^\infty}) =$

$\cup_{n\geq 1}\mathbb{Q}_p(\mu_{p^n})$. All of these algebraic extensions of $\mathbb{Q}_p$ are equipped with the unique norm $|\cdot|$ extending the usual p-adic norm on $\mathbb{Q}_p$.

Question: Which of the following are spherically complete? Explain why.

(a) $\mathbb{Q}_p$;

(b) $\mathbb{Q}_p(\mu_{p^n})$;

(c) $\mathbb{Q}_p(\mu_{p^\infty})$;

(d) $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$, the completion of $\mathbb{Q}_p(\mu_{p^\infty})$.

Hint: Show that there exists a sequence $a_1, a_2, \ldots \in \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ such that $|a_1| > |a_2| > \cdots$ and $\lim |a_i| > 0$, and such that the closed balls

$$B_i := \left\{x \in \widehat{\mathbb{Q}_p(\mu_{p^\infty})} \ : \ |x - a_1 - a_2 - \cdots - a_i| \leq |a_i|\right\}$$

have empty intersection.

Solution: (a) and (b) are spherically complete. In fact, every finite extension of $\mathbb{Q}_p$ is spherically complete. Such a field is discretely valued and complete. In this case, a decreasing sequence of closed balls either eventually stabilizes, or has radius converging to 0. In both cases, the intersection is nonempty.

(c) is not spherically complete. Notice that spherical completeness implies completeness. (Why? From any Cauchy sequence, one can construct a decreasing sequence of closed balls whose intersection gives the limit of the Cauchy sequence.) However, it is well-known that $\mathbb{Q}_p(\mu_{p^\infty})$ is not complete, hence not spherically complete.

(d) is not spherically complete. Assume that $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ is spherically complete. Notice that

$$\left|\widehat{\mathbb{Q}_p(\mu_{p^\infty})}\right| = 0 \cup \left\{p^{\frac{m}{p^n(p-1)}} \ : \ m \in \mathbb{Z},\, n \geq 0\right\}.$$

In particular, $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ is not discretely valued. Choose and fix a sequence of negative rational numbers $r_1 > r_2 > \cdots$ such that

$$r_i \in \left\{-\frac{m}{p^n(p-1)} \ : \ m \in \mathbb{Z}_{>0},\, n \geq 0\right\}$$

and $r := \lim_i r_i$ exists. We can find a sequence of elements $a_1, a_2, \ldots \in \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ such that $|a_i| = p^{r_i}$ for all i. In particular, we have $|a_1| > |a_2| > \cdots$ and $\lim |a_i| = p^r > 0$. Consider closed balls

$$B_i := \left\{x \in \widehat{\mathbb{Q}_p(\mu_{p^\infty})} \ : \ |x - a_1 - a_2 - \cdots - a_i| \leq |a_i|\right\}.$$

If $|x - a_1 - a_2 - \cdots - a_{i+1}| \leq |a_{i+1}|$, then

$$|x - a_1 - a_2 - \cdots - a_i| \leq |a_{i+1}| < |a_i|.$$

This means $B_1 \supsetneq B_2 \supsetneq \cdots$ is a strictly decreasing sequence of closed balls. By assumption, $B := \cap_{i=1}^{\infty} B_i$ is nonempty. It is necessarily an open subset of $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$, and hence contains at least an element $q \in \mathbb{Q}_p(\mu_{p^\infty})$.

Now, we vary $a = (a_1, a_2, \ldots)$ and write "B_a," "q_a" instead of "B," "q." Running through all possible a's, we obtain uncountably many disjoint B_a's. (Why? If two a's have the same $a_1, \ldots, a_{i-1}$ but $|a_i - a_i'| > |a_{i+1}|$, then the two B_{i+1}'s are disjoint.) On the other hand, from each of these B_a, we have an element

$$q_a \in B_a \cap \mathbb{Q}_p(\mu_{p^\infty}).$$

These q_a's map to distinct elements in $\mathbb{Q}_p(\mu_{p^\infty})/(s)$ where $s \in \mathbb{Q}_p(\mu_{p^\infty})$ has $0 < |s| \leq p^r$. However, $\mathbb{Q}_p(\mu_{p^\infty})/(s)$ is a countable set, a contradiction.