S.-T. Yau College Student Mathematics Contests 2015

Algebra and Number Theory

Individual (5 problems)

This exam of 160 points is designed to test how much you know rather than how much you don't know. You are not expected to finish all problems but do as much as you can.

Problem 1. (20 pt) Let G be an finite $\mathbb{Z}$-module (i.e., a finite abelian group with additive group law) with a bilinear, (strongly) alternative, and non-degenerate pairing

$$\ell : G \times G \to \mathbb{Q}/\mathbb{Z}.$$

Here "(strongly) alternating" means for every $a \in G$, $\ell(a, a) = 0$; "non-degenerate" means for every nonzero $a \in G$ there is a $b \in G$ such that $\ell(a, b) \neq 0$. Show in steps the following statement:

(S) : *G is isomorphic to $H_1 \oplus H_2$ for some finite abelian groups $H_1 \simeq H_2$ such that $\ell|_{H_i \times H_i} = 0$.*

(1.1) (5pt) For every $a \in G$, write $o(a)$ for the order of a and $\ell_a : G \longrightarrow \mathbb{Q}/\mathbb{Z}$ for the homomorphism $\ell_a(b) = \ell(a, b)$. Show that the image of ℓ_a is $o(a)^{-1}\mathbb{Z}/\mathbb{Z}$.

(1.2) (5pt) Show that G has a pair of elements a, b with the following properties:

(a) $o(a)$ is maximal in the sense that for any $x \in G$, $o(x) \mid o(a)$;

(b) $\ell(a, b) = o(a)^{-1} \mod \mathbb{Z}$.

(c) $o(a) = o(b)$

We call the subgroup $< a, b >:= \mathbb{Z}a + \mathbb{Z}b$ a *maximal hyperbolic subgroup* of G.

(1.3) (5pt) Let $< a, b >$ be a maximal hyperbolic subgroup of G. Let G' be the orthogonal complement of $< a, b >$ consisting of elements $x \in G$ such that $\ell(x, c) = 0$ for all $c \in< a, b >$. Show that G is a direct sum as follows:

$$G = \mathbb{Z}a \oplus \mathbb{Z}b \oplus G'.$$

(1.4) (5pt) Finish the proof of (S) by induction.

Problem 2 (40pt)**.** Let $\mathrm{O}_n(\mathbb{C})$ denote the group of $n \times n$ orthogonal complex matrices, and $M_{n\times k}(\mathbb{C})$ the space of $n \times k$ complex matrices, where n and k are two positive integers. For $i = 0, 1$, let F_i be the space of rational function f on $\mathrm{M}_{n\times k}(\mathbb{C})$ such that

$$(*) \qquad f(gx) = \det(g)^i f(x) \quad \text{for all } g \in \mathrm{O}_n(\mathbb{C}) \text{ and } x \in M_{n\times k}(\mathbb{C}).$$

We want to study in steps the structures of F_0 and F_1.

(2.1) (10pt) For each $x \in M_{n\times k}$, let V_x denote the subspace of $\mathbb{C}^n$ generated by columns of x, and let $Q(x) = x^t \cdot x \in M_{k\times k}(\mathbb{C})$. Show the following are equivalent:

   (a) the space V_x has dimension k, and the Euclidean inner product $(\cdot,\cdot)$ is non-degenerate on V_x in the sense that $V_x^\perp \cap V_x = 0$.

   (b) $\det Q(x) \neq 0$.

(2.2) (10pt) Show that F_0 is a field generated by entries of $Q(x)$.

(2.3) (10pt) Assuem $k < n$ and let $f \in F_1$. Show that $f = 0$ by the following two steps:

   (a) for any $x \in M_{n\times k}(\mathbb{C})$ with $\det Q(x) \neq 0$, construct a $g \in O_n(\mathbb{C})$ such that $g|_{V_x} = 1$ and $\det g = -1$.

   (b) Show that f vanishes on a general point $x \in M_{n\times k}(\mathbb{C})$ with $\det Q(x) \neq 0$, thus $f \equiv 0$.

(2.4) (10pt) Assume $k \geq n$. Show that F_1 is a free vector space of rank 1 over F_0.

Problem 3. (40pt) Consider the equation $f(x) := x^3 + x + 1 = 0$. We want to show in steps that

for any prime p, if $\left(\frac{31}{p}\right) = -1$, then $x^3 + x + 1$ is solvable mod p.

Let x_1, x_2, x_3 be three roots of $f(x) := x^3 + x + 1 = 0$. Let $F = \mathbb{Q}(x_1)$, and $L = \mathbb{Q}(x_1, x_2, x_3)$, and $K = \mathbb{Q}(\sqrt{\Delta})$ where Δ is the discriminant of $f(x)$:

$$\Delta = [(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)]^2.$$

(3.1) (10pt) Show that f is irreducible, that $\Delta = -31$, and that F is not Galois over $\mathbb{Q}$;

(3.2) (10pt) Show that $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$, the permutation group of three letters, that $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}$, and that $\mathrm{Gal}(L/F) \simeq \mathbb{Z}/2\mathbb{Z}$;

(3.3) (20pt) Let O_F, O_K, O_L = be rings of integers of F, K, L respectively. Let p be a prime such that $x^3 + x + 1 = 0$ is not soluble in $\mathbb{Z}/p\mathbb{Z}$. Show the following:

   (a) (5pt) pO_F is still a prime ideal in O_F,

   (b) (5pt) pO_L is product of two prime ideals in O_L, and

   (c) (5pt) pO_K is product of two primes ideals in O_K, and

   (d) (5pt) $x^2 + 31 = 0$ is soluble in $\mathbb{F}_p$.

Problem 4. (40pt) Let p be a prime and $\mathbb{Z}_p$ the ring of p-adic integers with a p-adic norm normalized by $|p| = p^{-1}$. Let $\phi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ be a map defined by a power series of the form

$$\phi(x) = x^p + p \sum a_n x^n, \qquad a_n \in \mathbb{Z}_p, \quad |a_n| \longrightarrow 0.$$

Let E be a field, and F the E-vector space of locally constant E-valued functions on $\mathbb{Z}_p$ with an operator ϕ^* defined by $\phi^* f = f \circ \phi$. We want to show in steps the following statement:

The set of eigenvalues of ϕ^* on F is $\{0, 1\}$.

(4.1) (10pt) Show that ϕ is a contraction map on each residue class $R \in \mathbb{Z}_p/p\mathbb{Z}_p$:

$$|\phi(x) - \phi(y)| \leq p^{-1}|x - y|, \qquad \forall x, y \in R.$$

(4.2) (10pt) Show that there is a $\epsilon_R \in R$ for each residue class R such that

$$\lim_n \phi^n(x) = \epsilon_R, \qquad \forall x \in R.$$

Here ϕ^n is defined inductively by $\phi^1 = \phi$, $\phi^n = \phi^{n-1} \circ \phi$.

(4.3) (10pt) Let F_0 (resp. F_1) be the subspace of functions f vanishing on each ϵ_R (resp. constant on R) for all residue class R. Show that $\phi^* = 1$ on F_1, and that for each $f \in F_0$ $\phi^{*n} f = 0$ for some $n \in \mathbb{N}$.

(4.4) (10pt) Show that for any $a \in E$, $a \neq 0, 1$, the operator $\phi^* - a$ is invertible on F.

Problem 5 (20pt). Check if the following rings are UFD (unique factorization domain).

(5.1) (5pt) $R_1 = \mathbb{Z}[\sqrt{6}]$;

(5.2) (5pt) $R_2 = \mathbb{Z}[(1 + \sqrt{-11})/2]$;

(5.3) (5pt) $R_3 = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$;

(5.4) (5pt) $R_4 = \mathbb{C}[x, y]/(x^3 + y^3 - 1)$.