Week 8

Linear Algebra

1. (2019B3) Let Q be an n-by-n real orthogonal matrix, and let $u \in \mathbb{R}^n$ be a unit column vector (that is, $u^T u = 1$). Let $P = I - 2uu^T$, where I is the n-by-n identity matrix. Show that if 1 is not an eigenvalue of Q, then 1 is an eigenvalue of PQ.

2. (2015A6) Let $A, B, M \in M_n(\mathbb{C})$ be $n \times n$ matrices with real coefficients. Suppose $AM = MB$ and that A and B have the same characteristic polynomial. Prove that for any $X \in M_n(\mathbb{R})$, we have $\det(A - MX) = \det(B - XM)$.

Mock Putnam problems

A1 Let R be a (not necessarily commutative) ring containing $\mathbb{Q}$ as a subring. Let $a, b, c \in R$ be idempotents ($a^2 = a$, $b^2 = b$, $c^2 = c$) such that $a + b + c = 0$. Prove that $a = b = c = 0$.

A2 Let $A, B \in M_n(\mathbb{C})$ be $n \times n$ matrices with complex coordinates. Does there exist a polynomial $p(x) \in \mathbb{C}[x]$ such that $p(AB)$ is nilpotent but $p(BA)$ is not nilpotent? (Nilpotent means some power of it is 0.)

A4 Let $n \in \mathbb{N}$. Prove that for any $f(x) \in \mathbb{Z}[x]$ of degree n, there exists $a \in \mathbb{R}$ with $0 \leq a \leq 1$ such that $|f(a)| \geq e^{-n}$.

A6 Let $p \equiv 2 \pmod 3$ be a prime. Let π be a permutation of $\mathbb{F}_p^\times$ given by $r \mapsto r^3$. When is π an even permutation?

Linear Algebra

1. (2019B3) Let Q be an n-by-n real orthogonal matrix, and let $u \in \mathbb{R}^n$ be a unit column vector (that is, $u^T u = 1$). Let $P = I - 2uu^T$, where I is the n-by-n identity matrix. Show that if 1 is not an eigenvalue of Q, then 1 is an eigenvalue of PQ.

   Since PQ and QP have the same eigenvalues, it suffices to find some nonzero vector w in the kernel of $I - QP$. We have

   $$\begin{aligned}(I-QP)v &= (I-Q)v, \text{ if } v \in u^\perp \\ (I-QP)u &= (I+Q)u.\end{aligned}$$

   Since 1 is not an eigenvalue of Q, we see that $I-Q$ is invertible. Hence the only possible w (up to scaling) is $u+v$ where $(I-Q)v = -(I+Q)u$. We need to check that $v = (I-Q)^{-1}(I+Q)u$ belongs to $u^\perp$. Let $A = (I-Q)^{-1}(I+Q)$. Then

   $$A^T = (I+Q^{-1})(I-Q^{-1})^{-1} = -A.$$

   Hence
   $$\langle u, Au\rangle = \langle A^T u, u\rangle = -\langle Au, u\rangle.$$

   Therefore, $\langle v, u\rangle = 0$.

   Alternatively, one can prove by induction on n that an n-by-n orthogonal matrix is a product of r reflections where $r \le n$. Its determinant is then $(-1)^r$. Since $\det(PQ) = -\det(Q)$, we see that either PQ or Q is a product of less than n reflections. Any product of less than n reflections fixes some vector.

2. (2015A6) Let $A, B, M \in M_n(\mathbb{C})$ be $n \times n$ matrices with real coefficients. Suppose $AM = MB$ and that A and B have the same characteristic polynomial. Prove that for any $X \in M_n(\mathbb{R})$, we have $\det(A - MX) = \det(B - XM)$.

   Solution 1: Let $A_t = A - tI$ and $B_t = B - tI$ be matrices in $M_n(\mathbb{C}[t])$. To prove

   $$\det(A_t - MX) = \det(B_t - XM),$$

   we may assume A_t, B_t, X are invertible, since both sides are polynomial in t and the coefficients of X. From $AM = MB$, we have $A_t M = MB_t$ so $M = A_t M B_t^{-1}$. Then

   $$\begin{aligned}\det(A_t - MX) &= \det(A_t - A_t M B_t^{-1} X) \\ &= \det(A_t)\det(I_n - MB_t^{-1}X) \\ &= \det(A_t)\det(I_n - XMB_t^{-1}) \qquad \text{by conjugating by } X \\ &= \det(A_t)\det(B_t^{-1})\det(B_t - XM) \\ &= \det(B_t - XM).\end{aligned}$$

   Solution 2: Note that the characteristic polynomial of a matrix A is determined by $\mathrm{tr}(A^k)$ for $k = 1, \ldots, n$. We prove that

   $$\mathrm{tr}((A - MX)^k) = \mathrm{tr}((B - XM)^k)$$

for every $k \in \mathbb{N}$. Expanding both sides, we see that it suffices to show that the corresponding terms have the same traces. That is, we show that for $k_1, \dots, k_m \in \mathbb{Z}_{\geq 0}$,

$$\mathrm{tr}(A^{k_1}MXA^{k_2}MX \cdots A^{k_{m-1}}MXA^{k_m}) = \mathrm{tr}(B^{k_1}XMB^{k_2}XM \cdots B^{k_{m-1}}XMB^{k_m}).$$

We have

$$\begin{aligned}
\mathrm{tr}(A^{k_1}MXA^{k_2}MX \cdots A^{k_{m-1}}MXA^{k_m}) &= \mathrm{tr}(A^{k_m+k_1}MXA^{k_2}MX \cdots A^{k_{m-1}}MX) \\
&= \mathrm{tr}(MB^{k_m+k_1}XMB^{k_2}X \cdots MB^{k_{m-1}}X) \\
&= \mathrm{tr}(B^{k_1}XMB^{k_2}XM \cdots B^{k_{m-1}}XMB^{k_m}).
\end{aligned}$$

Mock Putnam problems

A1 Let R be a (not necessarily commutative) ring containing $\mathbb{Q}$ as a subring. Let $a, b, c \in R$ be idempotents ($a^2 = a$, $b^2 = b$, $c^2 = c$) such that $a + b + c = 0$. Prove that $a = b = c = 0$.

Squaring $a + b = -c$ gives $ab + ba = 2c = -2a - 2b$. Then

$$\begin{aligned}
ab + aba = a(ab + ba) = -2a - 2ab, \\
aba + ba = (ab + ba)a = -2a - 2ba.
\end{aligned}$$

Subtracting gives $3(ab - ba) = 0$ and so $ab = ba = c$. From $a + b + ab = 0$, we obtain

$$a + 2ab = 0 \qquad \text{and} \qquad b + 2ab = 0 \qquad \text{so} \qquad ab = c = 4ab.$$

Hence $ab = 0 = a = b = c$.

A2 Let $A, B \in M_n(\mathbb{C})$ be $n \times n$ matrices with complex coordinates. Does there exist a polynomial $p(x) \in \mathbb{C}[x]$ such that $p(AB)$ is nilpotent but $p(BA)$ is not nilpotent? (Nilpotent means some power of it is 0.)

The two matrices $p(AB)$ and $p(BA)$ are similar if A is invertible. Hence they have the same characteristic polynomial. From an algebraic geometry point of view, the characteristic polynomials of $p(AB)$ and $p(BA)$ are polynomials in the coordinates of A and agree on a Zariski open subset (where $\det(A) \neq 0$) and so are equal as polynomials. Being nilpotent is equivalent to the characteristic polynomial being x^n.

A4 Let $n \in \mathbb{N}$. Prove that for any $f(x) \in \mathbb{Z}[x]$ of degree n, there exists $a \in \mathbb{R}$ with $0 \leq a \leq 1$ such that $|f(a)| \geq e^{-n}$.

Let $M = \max_{a \in [0,1]} |f(a)|$. For any $k \in \mathbb{N}$, we have

$$M^{2k} \geq \int_0^1 f(x)^{2k} dx = \int_0^1 \sum_{j=0}^{2kn} a_j x^j dx = \sum_{j=0}^{2kn} \frac{a_j}{j+1} \geq \frac{1}{\mathrm{lcm}(1, 2, \dots, 2kn+1)}.$$

For any $\epsilon > 0$, we know that for k large enough, we have

$$\mathrm{lcm}(1, 2, \dots, 2kn+1) < e^{(1+\epsilon)(2kn)}.$$

Hence $M > e^{-(1+\epsilon)n}$. Letting $\epsilon \to 0$ does the job.

A6 Let $p \equiv 2 \pmod 3$ be a prime. Let π be a permutation of $\mathbb{F}_p^\times$ given by $r \mapsto r^3$. When is π an even permutation?

(2012 B6) Recall that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$. Since $p-1$ is coprime to 3, there is a group homomorphism $\mathbb{F}_p^\times \to \overline{\mathbb{F}}_3^\times$ sending a primitive element to a primitive $p-1$-th root of unity. The image of $\mathbb{F}_p^\times$ is the set of roots of $x^{p-1}-1$ in $\overline{\mathbb{F}}_3^\times$, and π acts as the Frobenius map σ_3 on $\overline{\mathbb{F}}_3^\times$.

For a monic polynomial $g(x) \in \mathbb{F}_3[x]$, its discriminant is defined by

$$\Delta(g) = \prod (\text{root}_i \text{ of } g - \text{root}_j \text{ of } g)^2.$$

Viewing σ_3 as a permutation on the roots of g, we have

$$\sigma_3\left(\prod (\text{root}_i \text{ of } g - \text{root}_j \text{ of } g)\right) = \operatorname{sgn}(\sigma_3) \prod (\text{root}_i \text{ of } g - \text{root}_j \text{ of } g).$$

In other words, σ_3 is an even permutation on the roots of g if and only if $\Delta(g)$ is a square in $\mathbb{F}_3$. So it remains to compute $\Delta(x^{p-1}-1)$. Let $r_1, \ldots, r_{p-1}$ be the roots of $f(x) = x^{p-1}-1$. Then

$$\Delta(f) = (-1)^{\binom{p-1}{2}} \prod_{i \neq j} (r_i - r_j) = (-1)^{\frac{p-1}{2}} \prod_{i=1}^{p-1} f'(r_i) = (-1)^{\frac{p-1}{2}} p^{p-1} \left(\prod_{i=1}^{p-1} r_i\right)^{p-2} = (-1)^{\frac{p+1}{2}} p^{p-1}.$$

Hence we see that $\Delta(f)$ is a square if and only if $(-1)^{(p+1)/2}$ is a square in $\mathbb{F}_3$. Since -1 is not square, we see that $(-1)^{(p+1)/2}$ is a square in $\mathbb{F}_3$ if and only if $(p+1)/2$ is even if and only if $p \equiv 3 \pmod 4$.