Solutions for the AAC Competition Problems 2008

1. Let P be a square matrix with complex entries. Prove that P has the property $P^2 = P$ if and only if $\operatorname{rk} P = \operatorname{tr} P$ and $\operatorname{rk}(I - P) = \operatorname{tr}(I - P)$.

In fact we do not need the entries of P to be complex numbers: they can be elements of an arbitrary field $\mathbb{K}$ of characteristic zero. Consider the linear transformation $\mathbb{K}^n \to \mathbb{K}^n$ defined by $x \mapsto Px$, where n is the order of A. We will denote this transformation by $\mathcal{P}$. Let $V = \operatorname{im} \mathcal{P}$ and $W = \operatorname{im}(\mathcal{I} - \mathcal{P})$. They are subspaces of $\mathbb{K}^n$, with $\dim V = \operatorname{rk} P$ and $\dim W = \operatorname{rk}(I - P)$. For any $x \in \mathbb{K}^n$, we have $x = Px + (I - P)x$, hence $V + W = \mathbb{K}^n$. Set $Z = V \cap W$.

($\Rightarrow$) Suppose $P^2 = P$. Then $(I - P)^2 = I - 2P + P^2 = I - P$. Let $v \in Z$. Then we have $v = Px$ for some x, hence $Pv = P^2x = Px = v$. Similarly, $v = (I - P)y$ for some y and $(I - P)v = (I - P)^2y = (I - P)y = v$. Thus $v = Pv + (I - P)v = 2v$, which yields $v = 0$. We have shown that $Z = \{0\}$. Therefore, $\mathbb{K}^n = V \oplus W$. The above calculations also show that the restriction of $\mathcal{P}$ to V is the identity map (hence the restriction of $\mathcal{I} - \mathcal{P}$ is zero) and the restriction of $\mathcal{I} - \mathcal{P}$ to W is the identity map (and hence the restriction of $\mathcal{P}$ is zero). Now select a basis $\{v_1, \dots, v_k\}$ in V and a basis $\{w_1, \dots, w_{n-k}\}$ in W, where $k = \operatorname{rk} P$. Then $\{v_1, \dots, v_k, w_1, \dots, w_{n-k}\}$ is a basis for $\mathbb{K}^n$. Relative to this basis, $\mathcal{P}$ has matrix $Q = \begin{bmatrix} I_k & 0 \\ 0 & 0_{n-k} \end{bmatrix}$ and $\mathcal{I} - \mathcal{P}$ has matrix $I - Q = \begin{bmatrix} 0_k & 0 \\ 0 & I_{n-k} \end{bmatrix}$. Hence $\operatorname{tr} Q = k = \operatorname{rk} Q$ and $\operatorname{tr}(I - Q) = n - k = \operatorname{rk}(I - Q)$. Since Q is similar to P and $I - Q$ is similar to $I - P$, the result follows.

($\Leftarrow$) Suppose $\operatorname{rk} P = \operatorname{tr} P$ and $\operatorname{rk}(I - P) = \operatorname{tr}(I - P)$. Then we have $\operatorname{rk} P + \operatorname{rk}(I - P) = \operatorname{tr} P + \operatorname{tr}(I - P) = \operatorname{tr} I = n$. We also have $\dim V + \dim W - \dim Z = n$. It follows that $\dim Z = 0$, so $Z = \{0\}$. We have shown that $\mathbb{K}^n = V \oplus W$. Then for any $x \in \mathbb{K}^n$, the vectors $v \in V$ and $w \in W$ in the decomposition $x = v + w$ are determined uniquely. In particular, if $x \in V$, then $v = x$, $w = 0$ is the only possibility. Therefore, if $x \in V$, then in the decomposition $x = Px + (I - P)x$ we necessarily have $(I - P)x = 0$. Now for any $y \in \mathbb{K}^n$, we have $Py \in V$ and hence $(I - P)Py = 0$. This shows that $(I - P)P = 0$, so $P^2 = P$.

2. Student X. decided to compute the 100-th powers of all 17×17 matrices over the field of 17 elements and see what their sum would be, but at that

moment his computer broke. Help the student.

We will prove, more generally, that if $n \geq 1$ is an integer and R is a finite ring such that there exists an element ζ in the centre of R with both ζ and $1-\zeta^n$ invertible, then the sum of the n-th powers of the elements of R is equal to zero. Taking $n = 100$, $R = \mathrm{Mat}_{17}(\mathbb{Z}_{17})$ and $\zeta = 2I$, we then obtain that the sum in question is zero. (To see that $I - \zeta^{100}$ is invertible, we observe that by the Little Fermat Theorem $2^{100} \equiv 2^4 \equiv -1 \bmod 17$, so $I - \zeta^{100} = \zeta$.)

Let $S = \sum_{r \in R} r^n$. Since ζ is invertible, we see that when r ranges over R, so does ζr. Hence $\sum_{r \in R} (\zeta r)^n = S$. On the other hand, since ζ is central, we have $(\zeta r)^n = \zeta^n r^n$ and hence $\sum_{r \in R} (\zeta r)^n = \zeta^n \sum_{r \in R} r^n = \zeta^n S$. We have shown that $\zeta^n S = S$. Hence $(1 - \zeta^n)S = 0$ and we conclude that $S = 0$, since $1 - \zeta^n$ is invertible.

3. Let $\mathbb{K}$ be a field.

(a) Prove that any subalgebra of $\mathbb{K}[x]$ is finitely generated.

(b) Is the same statement true for $\mathbb{K}[x, y]$?

(a) Suppose A is a subalgebra of $\mathbb{K}[x]$ (with or without 1). Let $S(A)$ be the subset of $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$ that consists of the degrees of all nonzero polynomials in A. Since $\deg(fg) = \deg f + \deg g$ and A is closed under multiplication, we see that $S(A)$ is a subsemigroup of the additive semigroup $\mathbb{Z}_{\geq 0}$. If $S(A)$ is generated by some $n_1, \ldots, n_t$ and f_i are nonzero polynomials in A with $\deg f_i = n_i$, $i = 1, \ldots, t$, then the algebra A is generated by $f_1, \ldots, f_t$. Indeed, assume to the contrary that $f_1, \ldots, f_t$ generate a proper subalgebra $B \subset A$ and pick an element $f \in A \setminus B$ of minimal possible degree, say, $\deg f = m$. Then $m \in S(A)$ and hence $m = \xi_1 n_1 + \cdots + \xi_t n_t$ for some integers $\xi_i \geq 0$. Let $a \in \mathbb{K}$ be the highest coefficient of the polynomial f. Set $g = f - a f_1^{\xi_1} \cdots f_t^{\xi_t}$. Then $\deg g < \deg f$ and $g \in A \setminus B$ — a contradiction. The result now follows from the next lemma.

Lemma. Any subsemigroup S of the additive semigroup $\mathbb{Z}_{\geq 0}$ is finitely generated.

Proof. If $S = \{0\}$, there is nothing to prove. Otherwise let $d = \gcd S$. Then $d > 0$ and S is contained in the semigroup $d\mathbb{Z}_{\geq 0}$, which is isomorphic to $\mathbb{Z}_{\geq 0}$. Since S is sent to $S' = \frac{1}{d} S$ by the isomorphism and $\gcd S' = 1$, we may assume without loss of generality that $\gcd S = 1$. Then there exist

$n_1, \dots, n_t \in S$ such that $\gcd\{n_1, \dots, n_t\} = 1$. Let T be the subsemigroup of S generated by $n_1, \dots, n_t$. We claim that T (and hence S) contains all sufficiently large integers. Indeed, there exist integers $a_1, \dots, a_t$ such that $a_1 n_1 + \dots + a_t n_t = 1$. Let $M = \sum^- |a_i| n_i$ where the summation $\sum^-$ is over all i such that $a_i < 0$. Then for any integer $n \geq M^2$ we can write $n = qM + r$ where the integers q and r satisfy $q \geq M$ and $0 \leq r < M$. Then

$$n = q \sum^- |a_i| n_i + r \sum a_i n_i = \sum^- |a_i|(q - r) n_i + \sum^+ a_i r n_i$$

where the summation $\sum$ is over all $i = 1, \dots, t$ and the summations $\sum^{\pm}$ are over all i with $a_i > 0$, resp. $a_i < 0$. So n is a linear combination of $n_1, \dots, n_t$ with nonnegative integer coefficients and hence $n \in T$, as desired. Finally, let $m_1, \dots, m_s$ be all elements of S between 0 and M^2. Then the set $\{n_1, \dots, n_t, m_1, \dots, m_s\}$ generates S.

(b) Unlike $\mathbb{Z}_{\geq 0}$, the semigroup $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ has subsemigroups that are not finitely generated. For example, consider

$$S = \{(m, n) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \mid 0 < m \leq n\}.$$

Assume S is generated by (m_i, n_i), $i = 1, \dots, t$. Let $\alpha = \max\{\frac{n_i}{m_i}\}$. Then for any linear combination $(m, n) = \sum_i \xi_i (m_i, n_i)$ with nonnegative integer coefficients ξ_i, we will have $n \leq \alpha m$. But S contains elements (m, n) with arbitrarily large ratio $\frac{n}{m}$ — a contradiction.

Let S be any subsemigroup of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ that is not finitely generated. Then the subalgebra

$$A = \operatorname{span}\{x^m y^n \mid (m, n) \in S\} \subset \mathbb{K}[x, y]$$

is not finitely generated. Indeed, suppose A is generated by the polynomials $f_1, \dots, f_s$ and let $x^{m_i} y^{n_i}$, $i = 1, \dots, t$, be all monomials occuring in $f_1, \dots, f_s$. Then the elements (m_i, n_i), $i = 1, \dots, t$, generate S — a contradiction.

4. Let R be a commuatative ring with 1. As usual, for $a, b \in R$, $a|b$ means $b = ax$ for some $x \in R$. We will write $a \sim b$ if $b = au$ for some invertible element $u \in R$. Let $\mathcal{S}$ be the statement: "If $a|b$ and $b|a$, then $a \sim b$". It is easy to see that $\mathcal{S}$ holds if R is an integral domain.

(a) Prove that $\mathcal{S}$ holds in the ring $\mathbb{Z}_m$ of integers modulo m, for any $m \geq 2$.

(b) Does $\mathcal{S}$ hold in $\mathbb{Z}_m[x]$?

(a) First assume that $m = p^k$ where p is prime. Let $a, b \in \mathbb{Z}_m$ be such that $a = rb$ and $b = sa$ for some $r, s \in \mathbb{Z}_m$. Then $a = rsa$ and hence $a(1-rs) = 0$. If $a = 0$, then $b = 0$ and hence $a \sim b$. So assume $a \neq 0$. Let $\tilde{a}, \tilde{r}, \tilde{s}$ be integers representing the residues a, r, s, resp. Then we have $\tilde{a}(1 - \tilde{r}\tilde{s}) \equiv 0 \bmod p^k$. Let j be the highest power of p dividing $\tilde{a}$. Since $\tilde{a} \not\equiv 0 \bmod p^k$, we have $0 \leq j < k$. Let $a' = \frac{\tilde{a}}{p^j}$. Then we have $a'(1 - \tilde{r}\tilde{s}) \equiv 0 \bmod p^{k-j}$. It follows that p divides $1 - \tilde{r}\tilde{s}$ and hence p does not divide $\tilde{r}\tilde{s}$. Therefore, r and s are invertible in $\mathbb{Z}_m$. This proves $a \sim b$.

For general m, we can write $m = p_1^{k_1} \cdots p_t^{k_t}$ and apply Chinese Remainder Theorem. Namely, if $a = rb$ and $b = sa$ in $\mathbb{Z}_m$, then, using the symbol " ˜ " again for integers representing residues, we get $\tilde{a} \equiv \tilde{r}\tilde{b} \bmod p_i^{k_i}$ and $\tilde{b} \equiv \tilde{s}\tilde{a} \bmod p_i^{k_i}$, for any $i = 1, \ldots, t$. Then by the above we obtain $\tilde{b} \equiv \tilde{a}u_i \bmod p_i^{k_i}$ for some integer u_i that is not divisible by p_i. Let u be an integer such that $u \equiv u_i \bmod p_i^{k_i}$ for all i. Then $\tilde{b} \equiv \tilde{a}u \bmod p_i^{k_i}$ for all i and hence $\tilde{b} \equiv \tilde{a}u \bmod m$. Since the residue of u is invertible in $\mathbb{Z}_m$, we conclude that $a \sim b$.

(b) We will give a similar argument for $R = \mathbb{Z}_m[x]$. Let $\tilde{R} = \mathbb{Z}[x]$. First assume that $m = p^k$ where p is prime. We have to prove that, for any $a, b \in \tilde{R}$, if $a \equiv rb \bmod m$ and $b \equiv sa \bmod m$ for some $r, s \in \tilde{R}$, then there exists $u \in \tilde{R}$ such that $b \equiv au \bmod m$ and the residue of u is invertible in R. If $a \equiv 0 \bmod m$, then we are done. So assume $a \not\equiv 0 \bmod m$ and let j be the highest power of p dividing a, $0 \leq j < k$. Then we can write $a = a'p^j$ for some $a' \in \tilde{R}$ that is not divisible by p. Since $\tilde{R}$ is an integral domain, the congruence $a(1 - rs) \equiv 0 \bmod p^k$ implies the congruence $a'(1 - rs) \equiv 0 \bmod p^{k-j}$ and hence mod p. Since $a' \not\equiv 0 \bmod p$ and $\tilde{R}/(p) \cong \mathbb{Z}_p[x]$ is an integral domain, we conclude that $1 - rs \equiv 0 \bmod p$, i.e., $rs = 1 - \xi$ where ξ is divisible by p. But then $\xi^k \equiv 0 \bmod m$ and hence rs is invertible mod m (the inverse being $1 + \xi + \xi^2 + \cdots + \xi^{k-1}$). It follows that r and s are invertible mod m and thus we can take $u = s$.

For general $m = p_1^{k_1} \cdots p_t^{k_t}$, Chinese Remainder Theorem applied to the ring $\tilde{R}$ yields $R \cong R_1 \times \cdots \times R_t$ where $R_i = \mathbb{Z}_{p_i^{k_i}}[x]$. We already proved property $\mathcal{S}$ for R_i, $i = 1, \ldots, t$. It follows that R also has property $\mathcal{S}$.

5. Let G be a group. Suppose m and n are relatively prime integers such that $x^n y^n = y^n x^n$ and $x^m y^m = y^m x^m$ for all $x, y \in G$. Prove that G is abelian.

Let M be the subgroup of G generated by all elements x^m, $x \in G$, and let N be the subgroup of G generated by all elements x^m, $x \in G$. From the given

conditions it follows that M and N are abelian. Since $\gcd(m,n)=1$, there exist integers α,β such that $\alpha m+\beta n=1$. Then for any $g\in G$, we have $g=g^{\alpha m+\beta n}=(g^\alpha)^m(g^\beta)^n$, which shows that $MN=G$. Hence it suffices to prove that for any $a\in M$ and $b\in N$ we have $ab=ba$. Let $c=aba^{-1}b^{-1}$. Since for any $g\in G$, $gx^mg^{-1}=(gxg^{-1})^m$, the subgroup M is normal in G. It follows that $c=a(ba^{-1}b^{-1})\in M$. Similarly, N is normal in G and hence $c=(aba^{-1})b^{-1}\in N$. Thus $c\in M\cap N$. It follows that c commutes with any element of M and with any element of N. Hence c is central in G. Now $ab=cba$ implies

$$ab^m=(ab)b^{m-1}=(cba)b^{m-1}=(cb)ab^{m-1}=(cb)^2ab^{m-2}=\ldots=(cb)^ma.$$

Since c is central, we have $(cb)^m=c^mb^m$. Since both a and b^m are in M, they commute, so we obtain $b^ma=ab^m=c^mb^ma$ and hence $c^m=1$. Similarly, $c^n=1$. Since $\gcd(m,n)=1$, we conclude that $c=1$, as desired.

6. A group G acts on a set such that any non-identity element has a unique fixed point.

(a) Suppose G is finite. Show that the fixed point is the same for all non-identity elements of the group.

(b) Is the same statment true for infinite groups?

(a) Let $\tilde{X}$ be the set of all fixed points for $g\in G$, $g\neq 1$. Note that G acts on $\tilde{X}$, since if $gx=x$ and $hx=y$, then y is a fixed point of the element $g^h=hgh^{-1}$. Hence without loss of generality we may assume that $\tilde{X}=X$.

Denote $G'=G\setminus\{1\}$. We have a surjection $\varphi: G'\to X$ which takes an element $g\neq 1$ to its unique fixed point. Hence $|G|-1=|G'|\geq|X|$.

For any $x\in X$, denote its orbit $\mathcal{O}_x=\{gx\mid g\in G\}$. Then $|G|=|O_x||G_x|$ where G_x is the stabilizer of x. Let N be the number of orbits of the action $G:X$. For an orbit $\mathcal{O}=\mathcal{O}_x$, let $N_{\mathcal{O}}=|G_x|$ (clearly, this number does not depend on the choice of $x\in\mathcal{O}$). Then $N|G|=\sum_{\mathcal{O}}|\mathcal{O}|N_{\mathcal{O}}$ where the summation is over all orbits. On the other hand,

$$\sum_{\mathcal{O}}|\mathcal{O}|N_{\mathcal{O}}=\#\{(g,x)\in G\times X\mid gx=x\}=|X|+|G|-1,$$

because there are $|X|$ pairs of the form $(1,x)$ and $|G|-1$ pairs of the form $(g,\varphi(g))$, $g\in G'$. Thus $N|G|=|X|+|G|-1$, i.e., $|G|(N-1)=|X|-1$.

But the right-hand side is at most $|G| - 2$. Therefore $N = 1$ and $|X| = 1$. The latter means that the fixed point is common to all $g \in G'$.

(b) If G is infinite, the statement may fail to be true. For example, the group of rotations $G = SO(3)$ naturally acts on the 2-dimensional sphere $S^2 \subset \mathbb{R}^3$. Let X be the set of the diameters of the sphere (so X can be identified with the projective plane $\mathbb{R}P^2$). Then each rotation has a unique fixed point (its axis), which is not common to all rotations.