JAN 2019 ALGEBRA PRELIM SOLUTIONS

MICHAEL MORROW

FOREWORD. The following solutions are not necessarily guaranteed to be correct. Please let me know via email if you find any errors, or have any suggestions. Last revised: March 30, 2020.

(1) Let $M_{n\times n}(K)$ be the vector space of $n\times n$ matrices over a field K, and let $I_n \in M_{n\times n}(K)$ denote the $n\times n$ identity matrix.

a) Show that the trace map $\mathrm{tr} : M_{n\times n} \longrightarrow K$, $A \longmapsto \mathrm{tr}(A)$ is K-linear and $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.
b) Show there exist no matrices $A, B \in M_{n\times n}(\mathbb{Q})$ such that $AB - BA = I_n$.
c) Find $A, B \in M_{2\times 2}(\mathbb{F}_2)$ such that $AB - BA = I_2$.

Solution for a. Let $A, B \in M_{n\times n}(K)$, and let $\lambda \in K$. We have

$$\mathrm{tr}(\lambda A + B) = \sum_{j=1}^{n} (\lambda A + B)_{jj} = \sum_{j=1}^{n} \lambda a_{jj} + b_{jj} = \lambda \sum_{j=1}^{n} a_{jj} + \sum_{j=1}^{n} b_{jj} = \lambda \mathrm{tr}(A) + \mathrm{tr}(B).$$

Thus tr is a K-linear map. Furthermore,

$$\mathrm{tr}(AB) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ji} = \sum_{j=1}^{n}\sum_{i=1}^{n} a_{ji}b_{ij} = \sum_{j=1}^{n}\sum_{i=1}^{n} b_{ij}a_{ji} = \mathrm{tr}(BA).$$

■

Solution for b. Suppose there are matrices $A, B \in M_{n\times n}(\mathbb{Q})$ satisfying $AB - BA = I_n$. Then

$$\begin{aligned} 0 &= \mathrm{tr}(AB) - \mathrm{tr}(AB) \\ &= \mathrm{tr}(AB) - \mathrm{tr}(BA) \\ &= \mathrm{tr}(AB - BA) \\ &= \mathrm{tr}(I_n) \\ &= n, \end{aligned}$$

a contradiction. Thus no such matrices exist. ■

Solution for c. Let

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } BA = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Subtracting and reducing mod 2,

$$AB - BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \in M_{2\times 2}(\mathbb{F}_2).$$

■

(2) Let $A \in M_{3\times 3}(\mathbb{Q})$ have characteristic polynomial $\chi_A(t) = t^3 + 3t^2 + 2t$. Find the rank of A.

Solution. We have the factorization

$$\chi_A(t) = t(t+1)(t+2),$$

so the eigenvalues of A are $0, -1, -2$. Each eigenvalue has algebraic multiplicity 1, thus the corresponding geometric multiplicities are also 1 (geo. mult. is bounded above by alg. mult). So A is diagonalizable, therefore

$$\operatorname{rank}(A) = \deg(\chi_A) - \operatorname{alg}(\chi_A, 0) = 3 - 1 = 2.$$

■

(3) Let G be a p-group. Suppose that G acts on a finite set X such that p does not divide $|X|$. Show that this action has a fixed point.

Solution. Let n be the number of fixed points. Since G is a p-group, the Fixed Point Lemma says that $n \equiv |X| \bmod p$. Since p does not divide $|X|$, it cannot be the case that $n = 0$. Therefore, the action has at least one fixed point. ■

(4) Consider the symmetric group S_5.

a) Show that there are exactly 20 distinct 3-cycles in S_5.
b) Show that the 3-Sylow subgroups and the 5-Sylow subgroups of S_5 are contained in the alternating group A_5.
c) Determine the number of 3-Sylow subgroups and the number of 5-Sylow subgroups in S_5.

Solution for a. We have a formula for the number of k-cycles in S_n:

$$m = \frac{n!}{k(n-k)!}$$

Plugging in $n = 5$ and $k = 3$ yields $m = 20$. ■

Solution for b. We have $|S_5| = 5 \cdot 4 \cdot 3 \cdot 2$. Thus the 5-Sylow subgroups have order 5, and the 3-Sylow subgroups have order 3. Any 5-Sylow subgroup has the identity, and 4 elements of order 5. Since these elements are of odd order, they are even permutations. Hence they belong to A_5. Similarly, all elements of any 3-Sylow subgroup belong to A_5 as well. ■

Solution for c. By Sylow Theory, $n_5 \equiv 1 \bmod 5$, and n_5 divides $4 \cdot 3 \cdot 2 = 24$. So $n_5 = 1$ or $n_5 = 6$. Suppose $n_5 = 1$. Then there is a unique normal 5-Sylow subgroup N contained in S_5. By part b, N is also contained in A_5, so N is normal in A_5. This is a contradiction, since A_5 is simple. Thus $n_5 = 6$, so there are 6 5-Sylow subgroups in S_5. For the 3-Sylow subgroups, $n_3 \equiv 1 \bmod 3$, and n_3 divides $5 \cdot 4 \cdot 2 = 40$. Thus $n_3 = 1, 4, 10$, or 40. Note that any 3-cycle is contained in some 3-Sylow subgroup, and any element of order 3 must be a 3-cycle. Furthermore, any 3-Sylow subgroup contains 2 elements of order 3, so $n_3 = 10$ by part a. ■

(5) Let A be a commutative ring, and let $P \subset A$ be a prime ideal. For ideals $I, J \subset A$ show that if $I \cap J \subset P$ then $I \subset P$ or $J \subset P$.

Solution. Let $I, J \subset A$ be ideals such that $I \cap J \subset P$, and assume $J \not\subset P$. Let $x \in I$, and let $y \in J$ such that $y \notin P$. Then $xy \in I$ and $xy \in J$, so $xy \in P$. Since P is a prime ideal, either $x \in P$ or $y \in P$. We already know $y \notin P$, so $x \in P$. Hence $I \subset P$ and we're done. ∎

(6) Let R and S be integral domains and let $\varphi : R \to S$ be a surjective ring homomorphism (in particular, $\varphi(1_R) = 1_S$). Prove or find a counterexample to each of the following:

a) If R is a PID then S is a PID.
b) If R is a UFD then S is a UFD.

Solution for a. Let R be a PID. If φ is injective there is nothing to show, so assume $\ker \varphi \neq (0)$. Since φ is surjective, the First Isomorphism Theorem tells us that $R/\ker \varphi \cong S$. Since S is an integral domain, $\ker \varphi$ is a prime ideal in R. Since R is a PID, every non-zero prime ideal is a maximal ideal. Thus $\ker \varphi$ is maximal, so S is a field, hence a PID. ∎

Counterexample for b. Let $R = \mathbb{Z}[x]$. Since $\mathbb{Z}$ is a UFD, so is R. Let $S = \mathbb{Z}[x]/(x^2+5)$, and take φ to be the (surjective) canonical map $p(x) \longmapsto p(x) + (x^2+5)$. It remains to show that S is not a UFD. We first observe the following isomorphism:

$$\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]\big/(x^2+5)$$

which may be verified using the map $p(x) \longmapsto p(\sqrt{-5})$ and the First Isomorphism Theorem. In $\mathbb{Z}[\sqrt{-5}]$ we have $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, which are honest factorizations since the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. Hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, so S is not a UFD. ∎

(7) Let $K = \mathbb{F}_3(t)$, the field of rational functions over $\mathbb{F}_3$. Find a polynomial $p(x) \in K[x]$ which is irreducible but not separable.

Solution. Let $p(x) = x^3 - t \in K[x]$. We first show $p(x)$ is irreducible over $\mathbb{F}_3[t]$, then Gauss' Lemma will tell us that it's irreducible over K (recall that K is the field of fractions of $\mathbb{F}_3[t]$). Note that (t) is a prime ideal in $\mathbb{F}_3[t]$. This is because if the product of any two polynomials is divisible by t, one of the factors must also be divisible by t. Therefore $x^3 - t$ is irreducible over $\mathbb{F}_3[t]$ using Eisenstein and the prime ideal (t). Finally, $p(x)$ is not separable since $p'(x) = 3x^2 = 0$ in $K[x]$ since K is of characteristic 3. ∎

(8) a) Find a Galois extension $\mathbb{Q} \subset K$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.
b) Find a Galois extension $\mathbb{Q} \subset K$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Solution for a. We look at subfields of cyclotomic extensions. Consider the extension $\mathbb{Q}(\zeta_7)$ where ζ_7 is some primitive 7^{th} root of unity. The Galois group of this extension is C_6, the cyclic group on 6 elements. Elements of this Galois group can be represented as automorphisms determined by $\zeta_7 \mapsto \zeta_7^k$ for any $1 \leq k \leq 6$. Observe that the (complex conjugation) map $\sigma : \zeta_7 \mapsto \zeta_7^6$ is of order 2, since $\sigma^2 : \zeta_7 \mapsto \zeta_7^{36} = \zeta_7$. Thus σ generates a subgroup N of C_6 of order 2, which is of index 3. Since C_6 is cyclic, it is abelian, so N is normal. By the Fundamental Theorem of Galois Theory, N corresponds to a Galois extension $\mathbb{Q} \subset K$ of degree 3. Such an extension has a Galois group of order 3, so $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. To write down explicitly what K is, we note that K is the fixed field of N, and since σ fixes $\zeta_7 + \zeta_7^6$, we claim $K \cong \mathbb{Q}(\zeta_7 + \zeta_7^6)$. To verify this is correct, we need

to check that $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ is indeed a degree 3 extension. Observe that $\zeta_7 + \zeta_7^6$ is a root of the cubic polynomial

$$f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x],$$

which is irreducible over $\mathbb{Q}$ via the Rational Roots Theorem. Since $f(x)$ is monic, it is the minimal polynomial for $\zeta_7 + \zeta_7^6$, thus $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ really is degree 3 and we're done. ∎

Solution for b. A similar argument as in part a) shows that $\mathbb{Q}(\zeta_9 + \zeta_9^8)$ is another Galois extension with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$. It then follows that the compositum of $\mathbb{Q}(\zeta_9 + \zeta_9^8)$ and $\mathbb{Q}(\zeta_7 + \zeta_7^6)$ is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. ∎

(9) Let $F \subset K$ be a Galois extension with finite Galois group G. Suppose that K is the splitting field of $f(x) \in F[x]$, and that $f(x)$ is the minimal polynomial of $a \in K$. Show

$$f(x) = \prod_{\delta \in G} (x - \delta(a)),$$

where $\delta(a) \neq \gamma(a)$ for all $\delta \neq \gamma \in G$.

Solution. We first show that Galois actions permute the roots of $f(x)$. Since a is a root of $f(x)$, we may write

$$f(a) = a^n + \lambda_{n-1}a^{n-1} + \ldots + \lambda_0 = 0$$

where each $\lambda_i \in F$ and n is the degree of $f(x)$. Let $\delta \in G$. We have

$$\begin{aligned} f(\delta(a)) &= \delta(a)^n + \lambda_{n-1}\delta(a)^{n-1} + \ldots + \lambda_0 \\ &= \delta(a^n) + \lambda_{n-1}\delta(a^{n-1}) + \ldots + \lambda_0 \\ &= \delta(a^n) + \delta(\lambda_{n-1})\delta(a^{n-1}) + \ldots + \delta(\lambda_0) \\ &= \delta(a^n + \lambda_{n-1}a^{n-1} + \ldots + \lambda_0) \\ &= \delta(0) \\ &= 0, \end{aligned}$$

so $\delta(a)$ is again a root of $f(x)$. Since $\delta(a) \neq \gamma(a)$ for all $\delta \neq \gamma \in G$, every root of $f(x)$ shows up exactly once in the product, hence equality holds. ∎