JAN 2018 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 suggestions. Last revised: April 15, 2020.

(1) a) Let A be an $n \times n$ matrix with entries in a field. Suppose that $A^5 - A$ is invertible. Argue that 1 is not an eigenvalue of A.

b) Let $V \subset \mathbb{F}_2^n$ be the subset of vectors with an even number of nonzero entries. Show that V is a vector space over $\mathbb{F}_2$ and determine its dimension.

Solution for a. Suppose 1 is an eigenvalue of A. Then there is some non-zero eigenvector v such that $Av = v$. We have $(A^5 - A)v = A^5v - Av = v - v = 0$, but since $A^5 - A$ is invertible, cancellation says $v = 0$. This is a contradiction, so 1 is not an eigenvalue of A. ∎

Solution for b. First, $V \neq \varnothing$ since $0 \in V$. Now let $v, w \in V$, and let $\lambda \in \mathbb{F}_2$. Then v and w have an even number of nonzero entries. Note that if $\lambda = 0$, then $\lambda v + w = w \in V$. So assume $\lambda = 1$. Suppose v has $2j$ nonzero entries, and suppose w has $2k$ nonzero entries. Assume their nonzero entries overlap in i slots. Then v has $2j - i$ nonzero entries not in common with w, and w has $2k - i$ nonzero entries not in common with v. Therefore $v + w$ will have $2j - i + 2k - i = 2(j + k - i)$ nonzero entries. Thus $v + w \in V$, so V is a vector space. The dimension of V is $n - 1$, since a basis is given by

$$\begin{gathered}(1, 1, 0, 0, 0, \ldots, 0),\\ (0, 1, 1, 0, 0, \ldots, 0),\\ (0, 0, 1, 1, 0, \ldots, 0),\\ \vdots\\ (0, \ldots, 0, 0, 0, 1, 1).\end{gathered}$$

Verification that this is indeed a basis is left as an exercise to the reader. ∎

(2) Let $\varphi : V \to W$ and $\psi : W \to V$ be linear maps of vector spaces. Suppose that $\psi \circ \varphi$ is the identity on V. Show that there is an isomorphism of vector spaces $W \cong V \oplus \ker \psi$.

Proof. Define the map

$$\begin{aligned}\gamma : V \oplus \ker \psi &\longrightarrow W\\ (v, w) &\longmapsto \varphi(v) + w.\end{aligned}$$

Let $(v_1, w_1), (v_2, w_2) \in V \oplus \ker \psi$, and let $\lambda \in F$. Then we have

$$\begin{aligned}\gamma(\lambda(v_1, w_1) + (v_2, w_2)) &= \gamma(\lambda v_1 + v_2, \lambda w_1 + w_2) \\ &= \varphi(\lambda v_1 + v_2) + \lambda w_1 + w_2 \\ &= \lambda(\varphi(v_1) + w_1) + \varphi(v_2) + w_2 \\ &= \lambda\gamma(v_1, w_1) + \gamma(v_2, w_2).\end{aligned}$$

Thus γ is F-linear. Now let $w \in W$. Then $\psi(w) = v$ for some $v \in V$. By the Fiber Lemma, $\psi^{-1}(v) = w + \ker \psi$. Furthermore, $\psi(\varphi(v)) = v = \psi(w)$, so $\varphi(v) \in \psi^{-1}(v)$. Thus $\varphi(v) = w + k$ for some $k \in \ker \psi$. Hence $\gamma(v, -k) = \varphi(v) - k = w + k - k = w$, so γ is surjective. For injective, let $(a, b) \in \ker \gamma$. Then $\varphi(a) + b = 0$, and since $b \in \ker \psi$, we have

$$a = a + \psi(b) = \psi(\varphi(a)) + \psi(b) = \psi(\varphi(a) + b) = \psi(0) = 0.$$

Thus $\varphi(a) = \varphi(0) = 0$, so $b = 0$. Hence $\ker \gamma$ is trivial, so $W \cong V \oplus \ker \psi$. ∎

(3) Let N be a normal subgroup of a finite group G, and let P be a Sylow p-subgroup of G. Show that $P \cap N$ is a Sylow p-subgroup of N.

Proof. Let $|G| = p^k a$ where $p \nmid m$, so $|P| = p^k$. By Lagrange's Theorem, $P \cap N$ is a p-subgroup of N. Since N is normal in G, PN is a subgroup of G. We have

$$|PN| = \frac{|P||N|}{|P \cap N|},$$

so $|PN|/|P| = |N|/|P \cap N|$. Since $p \nmid m$, and

$$m = |G : P| = |G : PN||PN : P|,$$

we know $p \nmid |PN : P| = |N : P \cap N|$. Thus $P \cap N$ is a Sylow p-subgroup of N. ∎

(4) Let G be a group of order $3825 = 17 \cdot 25 \cdot 9$. If N is a normal subgroup of order 17 in G, then prove that N is contained in the center of G.

Proof. Define the map

$$\begin{aligned}\varphi : G &\longrightarrow \mathrm{Aut}(N) \\ g &\longmapsto (n \mapsto gng^{-1}).\end{aligned}$$

We must first show that for any $g \in G$, the map $\sigma : n \mapsto gng^{-1}$ is indeed an automorphism of N. Since N is normal, $\sigma(n) \in N$ for all $n \in N$, so σ is well-defined. Let $n_1, n_2 \in N$. Then $\sigma(n_1 n_2) = gn_1 n_2 g^{-1} = gn_1 g^{-1} gn_2 g^{-1} = \sigma(g_1)\sigma(g_2)$, so σ is a homomorphism. Now let $n \in \ker \sigma$, so $gng^{-1} = 1$. It follows that $n = 1$, so $\ker \sigma$ is trivial. Thus σ is injective, and since N is finite, it's also surjective. Hence σ really is an automorphism of N. Now let $g_1, g_2 \in G$. Then we have

$$\begin{aligned}\varphi(g_1 g_2) &= (n \mapsto g_1 g_2 n (g_1 g_2)^{-1}) \\ &= (n \mapsto g_1 g_2 n g_2^{-1} g_1^{-1}) \\ &= (n \mapsto g_1 n g_1^{-1}) \circ (n \mapsto g_2 n g_2^{-1}) \\ &= \varphi(g_1)\varphi(g_2).\end{aligned}$$

Thus φ is a homomorphism. Let $k \in \ker \varphi$. Then $n \mapsto knk^{-1}$ is the identity map on N, so $knk^{-1} = n$ for all $n \in N$. This happens precisely when $k \in C_G(N)$, the centralizer of N in G. Hence $\ker \varphi = C_G(N)$. By the First Isomorphism Theorem, $G/C_G(N)$ is isomorphic to a subgroup of $\mathrm{Aut}(N)$. Since N is of prime order, it is cyclic, so $\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}/17\mathbb{Z}) \cong \mathbb{Z}/17\mathbb{Z}^\times \cong \mathbb{Z}/16\mathbb{Z}$. Thus $|G|/|C_G(N)|$ divides 16 by Lagrange's Theorem. So $|G|/|C_G(N)| = 1, 2, 4, 8$, or 16. Since $|G|$ is not divisible by $2, 4, 8$, or 16, we must have $|G|/|C_G(N)| = 1$. Hence $C_G(N) = G$, so N is contained in the center of G. ∎

(5) Let R be a UFD such that any ideal of R generated by two elements is principal. Prove that R is a PID. (Hint: Recall that a UFD satisfies the ascending chain condition for principal ideals.)

Proof. We first show that every finitely generated ideal is principal via induction. For $n = 2$, the claim already holds by the assumption. Let $n \geq 2$, and assume the claim holds for $n-1$. Suppose $I = (a_1, \ldots, a_n)$ for $a_1, \ldots, a_n \in R$. Then $(a_1, \ldots, a_{n-1}) = (b)$ for some $b \in R$. Furthermore, $(b, a_n) = (c)$ for some $c \in R$. We now obtain

$$(a_1, \ldots, a_n) = a_1R + \ldots + a_nR = (a_1, \ldots, a_{n-1}) + a_nR = (b) + a_nR = (b, a_n) = (c).$$

Thus every finitely generated ideal is principal. Now let J be some ideal that is not finitely generated. Then there are elements $x_1, x_2, \ldots \in J$ such that

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq J$$

where each $(x_1, \ldots, x_i)$ is principal (via our previous work). Since R is a UFD, it satisfies the ascending chain condition for principal ideals. Thus there must exist some $k \in \mathbb{N}$ such that $(x_1, \ldots, x_k) = (x_1, \ldots, x_m)$ for all $m \geq k$. Since J is not finitely generated, we may find some $x_p \in J$ such that $x_p \notin (x_1, \ldots, x_k)$ where $p > k$. But then $(x_1, \ldots, x_k) \neq (x_1, \ldots, x_k, x_p)$, a contradiction. Hence J must be finitely generated so it is principal. Therefore R is a PID. ∎

(6) Determine all ring homomorphisms $\mathbb{Q}[x]/(x^{100} + 2) \to \mathbb{Q}[x]/(x^{501} - 2)$.

Proof. Since $x^{100}+2$ and $x^{501}-2$ are both irreducible over $\mathbb{Z}$ by Eisenstein, they are irreducible over $\mathbb{Q}$ via Gauss' Lemma. Thus $\mathbb{Q}[x]/(x^{100} + 2)$ and $\mathbb{Q}[x]/(x^{501} - 2)$ are actually fields. Furthermore, we have

$$\mathbb{Q}[x]\big/(x^{100} + 2) \cong \mathbb{Q}(\alpha) \quad \text{and} \quad \mathbb{Q}[x]\big/(x^{501} - 2) \cong \mathbb{Q}(\beta)$$

where α and β are roots of the polynomials $x^{100} + 2$ and $x^{501} - 2$ respectively. So we are really looking for ring maps from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\beta)$. The kernel of any such map is an ideal, and ring maps must take 1 to 1, so the only possible maps will be injective. Suppose we have an injective map φ. Then φ is an embedding of $\mathbb{Q}(\alpha)$ into $\mathbb{Q}(\beta)$. We may thus regard $\mathbb{Q}(\alpha)$ as a subextension of $\mathbb{Q}(\beta)$. Since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is degree 100, and $\mathbb{Q}(\beta)/\mathbb{Q}$ is degree 501, the Degree Formula says

$$501 = [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] \cdot 100.$$

This implies that 100 divides 501, a contradiction. Hence there are no ring maps between these two rings. ∎

(7) Show that the ideal I of $\mathbb{Z}[x]$ generated by 29 and x^2+1 is not a maximal ideal.

Proof. Since $x^2+1 = (x+17)(x-17)+290$, we have $(29, x^2+1) \subset (29, x-17)$. To show proper inclusion, suppose for sake of contradiction that $x - 17 = 29f(x) + (x^2+1)g(x)$ for some $f(x), g(x) \in \mathbb{Z}[x]$. Plugging in $x = -17$ we obtain $-34 = 29f(-17)+290g(-17)$, so 29 divides 34. This is a contradiction, so $(29, x^2+1) \subsetneq (29, x-17)$. To see why $(29, x-17) \subsetneq \mathbb{Z}[x]$, suppose again for sake of contradiction that $1 = 29p(x) + (x-17)q(x)$ for some $p(x), q(x) \in \mathbb{Z}[x]$. Plugging in $x = 46$ we obtain $1 = 29p(x) + 29q(x)$, so 29 divides 1. This is a contradiction, so

$$(29, x^2+1) \subsetneq (29, x-17) \subsetneq \mathbb{Z}[x].$$

Hence $(29, x^2+1)$ is not a maximal ideal. ∎

(8) Find the isomorphism type of the Galois group of the polynomial $f = (x^{12}-1)(x^2+5)$ over $\mathbb{Q}$, and describe the action of its elements on the splitting field.

Proof. The splitting field for f is $K = \mathbb{Q}(\zeta_{12}, \sqrt{-5})$ where ζ_{12} is a primitive 12^{th} root of unity. By the Degree Formula, we have

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta_{12}, \sqrt{-5}) : \mathbb{Q}(\zeta_{12})][\mathbb{Q}(\zeta_{12}) : \mathbb{Q}] = 2\varphi(12) = 2(4) = 8.$$

Thus K is Galois over $\mathbb{Q}$ of degree 8, so $|\mathrm{Gal}(K/\mathbb{Q})| = 8$. Any element of the Galois group is completely determined by its action on the generators ζ_{12} and $\sqrt{-5}$. So define the automorphisms

$$\sigma_{ij} : \begin{cases} \zeta_{12} & \longmapsto \ \zeta_{12}^i \\ \sqrt{-5} & \longmapsto \ (-1)^{j+1}\sqrt{-5} \end{cases}$$

where $\gcd(12, i) = 1$ and $j = 1, 2$. Counting the σ_{ij} we see there are 8 distinct automorphisms, so we have accounted for all elements in $\mathrm{Gal}(K/\mathbb{Q})$. The action of the Galois group on the splitting field is completely described by the σ_{ij}. It remains to determine the isomorphism type of $\mathrm{Gal}(K/\mathbb{Q})$. Let's compute the orders of the elements in the Galois group:

$$\begin{aligned} \mathrm{ord}(\sigma_{11}) &= 1 \qquad & \mathrm{ord}(\sigma_{51}) &= 2 \\ \mathrm{ord}(\sigma_{71}) &= 2 \qquad & \mathrm{ord}(\sigma_{11,1}) &= 2 \\ \mathrm{ord}(\sigma_{12}) &= 2 \qquad & \mathrm{ord}(\sigma_{52}) &= 2 \\ \mathrm{ord}(\sigma_{72}) &= 2 \qquad & \mathrm{ord}(\sigma_{11,2}) &= 2. \end{aligned}$$

The only group of order 8 where every non-identity element has order 2 is $C_2 \times C_2 \times C_2$. So we conclude that $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2^3$. ∎

(9) Consider the polynomial $f = x^5 - 5p^4x + p$, where p is a prime number.

a) Show that f has exactly three real roots.
b) Determine the Galois group of f over $\mathbb{Q}$.

Solution for a. We use Descartes' Rule of Signs. The terms of f have exactly two sign changes, so f has either two or zero positive real roots. Now look at $f(-x) = -x^5 + 5p^4x + p$, whose terms have exactly one sign change. Thus f has exactly one negative real root. To find how many positive real roots f has, note that $f(0) = p > 0$ and $f(1) = 1 - 5p^4 + p < 0$. By the Intermediate Value Theorem, f has a positive real root between 0 and 1, so f must have exactly two positive real roots. Hence f has exactly three real roots. ∎

Solution for b. First note that f is irreducible over $\mathbb{Z}$ via Eisenstein. Using Gauss' Lemma, f is irreducible over $\mathbb{Q}$. This means the Galois group acts transitively on the roots of f. Since $\deg(f) = 5$, the Galois group is a transitive subgroup of S_5. By part a, f has two complex roots. Therefore the complex conjugation action is an element of the Galois group. Since complex conjugation is of order 2, the Galois group contains a transposition. We now prove a mini-claim: if G is a transitive subgroup of S_p where p is prime, and G contains a transposition, then $G = S_p$. To see why, suppose G acts on $\{1, 2, \ldots, p\}$. Since G is transitive, $|\text{Orb}(1)| = p$, so by the Orbit Stabilizer Theorem, $|G : \text{Stab}(1)| = |\text{Orb}(1)| = p$. This means p divides $|G|$, so by Cauchy's Theorem, G contains a p-cycle. Since p is prime, the transposition and the p-cycle generate all of S_p. Applying this to our case of $p = 5$, we discover that the Galois group of f over $\mathbb{Q}$ is S_5. ∎