JAN 2017 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: May 18, 2020.

(1) Let A be an $n \times n$ matrix over an algebraically closed field K. Prove that $A^n = 0$ if and only if $\lambda I_n - A$ is invertible for all nonzero $\lambda \in K$.

Solution. For the forward direction, assume $A^n = 0$. Since K is algebraically closed, A has an eigenvalue. Let λ be some eigenvalue of A, and let v be the associated eigenvector. Observe

$$0 = 0v = A^n v = \lambda^n v,$$

so $\lambda^n = 0$, hence $\lambda = 0$. This shows that 0 is the only eigenvalue of A, so $\det(\lambda I_n - A) = 0$ for all nonzero λ, hence $\lambda I_n - A$ is invertible for all nonzero λ. For the reverse direction, assume $\lambda I_n - A$ is invertible for all nonzero λ. Therefore $\det(\lambda I_n - A) \neq 0$ for $\lambda \neq 0$, and since K is algebraically closed, $\lambda = 0$ is the only eigenvalue of A. This means the characteristic polynomial of A is $\chi_A(x) = \alpha x^n$ for some $0 \neq \alpha \in K$. By Cayley-Hamilton, we have $\chi_A(A) = \alpha A^n = 0$, so $A^n = 0$ and we're done. ∎

(2) Let V be a 4-dimensional vector space over a field K, and let $T : V \to V$ be a linear map with characteristic polynomial $\chi_T = x^4 - x^3$. Prove:
a) T is not surjective.
b) V has T-invariant subspaces of dimensions 1, 2, and 3.

Solution for a. We have $\chi_T = x^3(x-1)$, so 0 is an eigenvalue of T. Then $T(v) = 0v = 0$ for some corresponding eigenvector v. Since v cannot be zero, $\dim(\ker T) \geq 1$. By Rank-Nullity, $\dim(\text{im } T) < 4$, so T is not surjective. ∎

Solution for b. From the factorization in part (a), we see 0 is an eigenvalue of algebraic multiplicity 3, and 1 is an eigenvalue of algebraic multiplicity 1. So $\text{eig}(T,1)$ is a T-invariant subspace of dimension 1. Furthermore, $\text{eig}(T,1) \oplus \text{span}(v)$ where $0 \neq v \in \text{eig}(T,0)$ is a T-invariant subspace of dimension 2. Finally, for the dimension 3 subspace, there are two cases. If $\dim \text{eig}(T,0) \geq 2$, let $v_1, v_2 \in \text{eig}(T,0)$ be linearly independent, and then $\text{span}(v_1,v_2) \oplus \text{eig}(T,1)$ is what we're looking for. On the other hand, if $\dim \text{eig}(T,0) = 1$, then $\dim \ker T = 1$, so $\dim \text{im } T = 3$ by Rank-Nullity, hence $\text{im } T$ is the subspace we're looking for. ∎

(3) Let p be a prime number, and consider the group $G = C_{p^5} \times C_{p^6} \times C_{p^7} \times C_{p^8} \times C_{p^9}$, where C_n denotes a cyclic group of order n.
a) How many elements in C_{p^k} have order at most p^i if $i \leq k$?
b) How many elements in G have order p^7?

Solution for a. In general, a cyclic group of order n has an element of order d if and only if $d \mid n$. In this case, the number of elements of order d is given by $\varphi(d)$, where φ is the Euler totient function. Therefore, if $\eta(p^i)$ denotes the number of elements in C_{p^k} having order at most p^i, then

$$\eta(p^i) = \sum_{\substack{d \mid p^k \\ d \leq p^i}} \varphi(d) = \sum_{d \mid p^i} \varphi(d) = p^i.$$

■

Solution for b. For any $x = (r, s, t, u, v) \in G$, we must have $\operatorname{ord}(x) = \operatorname{lcm}(\operatorname{ord}(r), \ldots, \operatorname{ord}(v))$. Using this fact along with part (a), we have $p^5p^6p^7p^7p^7$ elements of order at most p^7, and $p^5p^6p^6p^6p^6$ elements of order at most p^6. This gives

$$p^5p^6p^7p^7p^7 - p^5p^6p^6p^6p^6 = p^{32} - p^{29}$$

elements of order exactly p^7. ■

(4) a) Give the definition of a solvable group.
b) Let $p < q$ be primes, and let G be of order pq^n for $n \in \mathbb{N}$. Show G is solvable.

Solution for a. A group G is *solvable* if there is a subnormal series

$$G_0 = \{e\} \lhd G_1 \lhd \cdots \lhd G_k = G$$

such that each quotient G_j/G_{j-1} is abelian for $j = 1, 2, \ldots, k$. ■

Solution for b. Sylow's Theorem says that the number n_q of Sylow q-subgroups of G must satisfy $n_q \equiv 1 \pmod{q}$ and $n_q \mid p$. This forces $n_q = 1$, so G has a normal Sylow q-subgroup, call it Q. Since $|Q| = q^n$, Q has subgroups Q_i of order q^i for each $0 \leq i < n$. Set $Q_n = Q$. Since each Q_i is of index q in Q_{i+1} for $i < n$, and q is the smallest prime dividing the order of Q_{i+1}, each Q_i is normal in Q_{i+1}. This gives rise to the subnormal series

$$Q_0 = \{e\} \lhd Q_1 \lhd \cdots \lhd Q_n = Q \lhd G.$$

The quotient G/Q has order $pq^n/q^n = p$, so G/Q is abelian. Each quotient Q_{i+1}/Q_i is of order q for $0 \leq i < n$, so Q_{i+1}/Q_i is abelian. Hence G is solvable. ■

(5) Consider the ring of Gaussian integers $R = \mathbb{Z}[i]$. Determine all ring maps $R \times R \to R$ that map the identity of $R \times R$ onto the identity of R.

Solution. Note that $R \times R$ is generated by $a = (1, 0)$, $b = (0, 1)$, $c = (i, 0)$ and $d = (0, i)$. Any ring map φ is completely determined by its action on these generators. Suppose $(1, 1) \mapsto 1$. Then $\varphi(a) + \varphi(b) = \varphi(a + b) = \varphi(1, 1) = 1$. Furthermore, $\varphi(a)^2 = \varphi(a^2) = \varphi(a)$, and $\varphi(b)^2 = \varphi(b^2) = \varphi(b)$. This means either $\varphi(a) = 1$ and $\varphi(b) = 0$, or $\varphi(a) = 0$ and $\varphi(b) = 1$. We proceed by cases.

<u>Case 1:</u> Suppose $\varphi(a) = 1$ and $\varphi(b) = 0$. We have $\varphi(c)^2 = \varphi(c^2) = \varphi(-a) = -\varphi(a) = -1$. Thus $\varphi(c) = \pm i$. Also, $\varphi(d)^2 = \varphi(d^2) = \varphi(-b) = -\varphi(b) = 0$. So $\varphi(d) = 0$.

<u>Case 2:</u> Suppose $\varphi(a) = 0$ and $\varphi(b) = 1$. A similar argument as in Case 1 shows that $\varphi(c) = 0$ and $\varphi(d) = \pm i$.

The above two cases show that the only ring maps sending $(1, 1)$ to 1 are $(x + yi, v + wi) \mapsto x \pm yi$ and $(x + yi, v + wi) \mapsto v \pm wi$. ■

(6) Let R be an integral domain such that the set of nonzero ideals of R contains a minimal element I (with respect to inclusion). Prove that R is a field. (Hint: For a nonzero $a \in I$ consider its square a^2.)

Solution. Let $a \in I$ be nonzero. Then $a^2 \in I$, so $(a^2) \subset I$. Since $a \neq 0$, we have $a^2 \neq 0$ (since R has no zero divisors), and thus $(a^2) \neq (0)$. Since I is minimal, we must have $(a^2) = I$. This means $a = ra^2$ for some $r \in R$. Since R is an integral domain, we have cancellation, thus $1 = ra$. Therefore a is a unit, so $I = R$. Hence R is the smallest nonzero ideal of R, so R is a field. ∎

(7) Let $f \in K[x]$ be an irreducible polynomial of degree n over a field K. Let L/K be a field extension of degree m. If $(m, n) = 1$, then show that f is irreducible in $L[x]$.

Solution. Let α be a root of f. Since f is irreducible over K, $[K(\alpha) : K] = n$. Since the minimal polynomial m_α of α over L divides f, we have $[L(\alpha) : L] \leq n$. Observe

$$[L(\alpha) : K] = [L(\alpha) : L][L : K] = m[L(\alpha) : L] \leq mn,$$

and

$$[L(\alpha) : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K] = n[L(\alpha) : K(\alpha)].$$

So $[L(\alpha) : K] \leq mn$, is a multiple of n, and is a multiple of m. Since $(m, n) = 1$, we have $[L(\alpha) : K] = mn$. Thus $[L(\alpha) : L] = n$, so m_α is of degree n. Therefore $\beta m_\alpha = f$ for some $\beta \in L$. Since m_α is irreducible in $L[x]$, it follows that f is irreducible in $L[x]$, as desired. ∎

(8) Let $\mathbb{F}_q$ denote a finite field with $q = p^n$ elements, where p is a prime number.

a) Prove that the map $\varphi : \mathbb{F}_q \to \mathbb{F}_q$, $a \mapsto a^p - a$, is $\mathbb{F}_p$-linear.

b) Consider the polynomial $f = x^{p^{n-1}} + x^{p^{n-2}} + \ldots + x^p + x$ and the sets

$$S = \{a^p - a \mid a \in \mathbb{F}_q\},$$
$$T = \{b \in \mathbb{F}_q \mid f(b) = 0\}.$$

Show that $S = T$.

Solution for a. Let $a, b \in \mathbb{F}_q$ and let $\lambda \in \mathbb{F}_p$. Then

$$\varphi(\lambda a + b) = (\lambda a + b)^p - (\lambda a + b) = \lambda(a^p - a) + (b^p - b) = \lambda\varphi(a) + \varphi(b).$$

This follows from the fact that $\mathbb{F}_p$ is fixed by the Frobenius automorphism. ∎

Solution for b. Let $x \in S$. Then $x = a^p - a$ for some $a \in \mathbb{F}_q$. We have

$$\begin{aligned} f(x) &= (a^p - a)^{p^{n-1}} + (a^p - a)^{p^{n-2}} + \ldots + (a^p - a)^p + (a^p - a) \\ &= a^{p^n} + a^{p^{n-1}} + \ldots + a^{p^2} + a^p - a^{p^{n-1}} - a^{p^{n-2}} - \ldots - a^p - a \\ &= a^{p^n} - a \\ &= a - a \\ &= 0. \end{aligned}$$

Therefore $x \in T$, so $S \subset T$. For equality, first note that since f is of degree p^{n-1}, f has at most p^{n-1} roots in $\mathbb{F}_q$. Thus $|T| \leq p^{n-1}$. Since $a^p - a$ has at most p roots in $\mathbb{F}_q$, we have $|\ker\,\varphi| \leq p$, so $\dim \ker\,\varphi \leq 1$. By Rank-Nullity,

$$\dim \mathbb{F}_q = \dim \mathrm{im}\,\varphi + \dim \ker\,\varphi \leq \dim \mathrm{im}\,\varphi + 1,$$

so $n - 1 \leq \dim \operatorname{im} \varphi$. Since $S = \operatorname{im} \varphi$, this shows that $p^{n-1} \leq |S|$. Finally, since $S \subset T$, we have $|S| \leq |T|$, so

$$p^{n-1} \leq |S| \leq |T| \leq p^{n-1}.$$

Therefore $|S| = |T|$, hence $S = T$. ∎

(9) Let p be a prime number and suppose the polynomial $f = x^p - a \in \mathbb{Q}[x]$ is irreducible. Let $\zeta \in \mathbb{C}$ be a primitive p^{th} root of unity, and consider the field $K = \mathbb{Q}(b, \zeta)$ where $b \in \mathbb{C}$ is any root of f.

a) Prove that the field extension $K/\mathbb{Q}$ is a Galois extension.
b) Determine the order of the Galois group G of K over $\mathbb{Q}$.
c) If P is a subgroup of G with order p, then show that P is a normal subgroup and that G/P is a cyclic group. Furthermore, describe the fixed field of K with respect to P explicitly.

Solution for a. The roots of f are $\sqrt[p]{a}, \zeta\sqrt[p]{a}, \ldots, \zeta^{p-1}\sqrt[p]{a}$. Let b be any root of f. Then $b = \zeta^i\sqrt[p]{a}$ for some $0 \leq i < p$. Hence the splitting field for f is $K = \mathbb{Q}(b, \zeta)$, so K is Galois over $\mathbb{Q}$. ∎

Solution for b. The degree formula says

$$[K : \mathbb{Q}] = [\mathbb{Q}(b, \zeta) : \mathbb{Q}] = [\mathbb{Q}(b, \zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = p(p-1).$$

Thus $|\operatorname{Gal}(K/\mathbb{Q})| = p(p-1)$. ∎

Solution for c. Let P be a subgroup of G of order p, then P is a Sylow p-subgroup of G (since p is the highest power of p occurring in the order of G). Sylow's Theorem says $n_p \equiv 1 \pmod{p}$, and $n_p \mid (p-1)$. This forces $n_p = 1$, so P is the unique normal Sylow p-subgroup of G. Let $E = \operatorname{Fix}(P)$. Then $E/\mathbb{Q}$ is Galois with $\operatorname{Gal}(E/\mathbb{Q}) \cong G/P$. This shows that $[E : \mathbb{Q}] = p - 1$. Moreover, we claim that E is the unique subextension of $K/\mathbb{Q}$ with degree $p-1$. Suppose $E' \subset K$ satisfies $[E' : \mathbb{Q}] = p - 1$. Then $E' = \operatorname{Fix}(H)$ for some subgroup $H \subset G$ of order $p - 1$. Therefore $[G : H] = [E' : \mathbb{Q}] = p - 1$, so $|H| = p$. But P is the unique subgroup of G of order p, so $H = P$. Hence $E' = E$, as desired. Finally, $\mathbb{Q}(\zeta)/\mathbb{Q}$ is one such extension of degree $p - 1$, so $E \cong \mathbb{Q}(\zeta)$. The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is cyclic (namely $\mathbb{Z}/p\mathbb{Z}^\times$), so G/P is cyclic and we're done. ∎