JUNE 2016 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 20, 2020.

(1) In the real vector space of continuous real-valued functions defined on $\mathbb{R}$ consider the functions p_i, $i = 0, 1, 2$, and exp, defined as

$$p_i(x) = x^i, \ \exp(x) = e^x \text{ for all } x \in \mathbb{R}.$$

Set $V = \text{span}_{\mathbb{R}}(p_0, p_1, p_2, \exp)$ and consider the endomorphism $\sigma : V \to V$ defined as

$$(\sigma f)(x) = f(x-1) \text{ for all } x \in \mathbb{R}.$$

a) Give the matrix representation of σ with respect to the basis $\{p_0, p_1, p_2, \exp\}$.
b) Determine all eigenvalues and find bases of all eigenspaces of σ.
c) Is σ diagonalizable?
d) Determine the minimal polynomial of σ.

Solution for a. We have

$$\begin{aligned} \sigma(p_0) &= (x-1)^0 = 1 = p_0, \\ \sigma(p_1) &= (x-1)^1 = x - 1 = p_1 - p_0, \\ \sigma(p_2) &= (x-1)^2 = x^2 - 2x + 1 = p_2 - 2p_1 + p_0, \\ \sigma(\exp) &= e^{x-1} = e^x e^{-1} = e^{-1}\exp. \end{aligned}$$

So our matrix representation is

$$A = \begin{pmatrix} 1 & -1 & 1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{-1} \end{pmatrix}.$$

■

Solution for b. By part (a), the eigenvalues are 1 (with algebraic multiplicity 3) and e^{-1} (with algebraic multiplicity 1). To find bases for the eigenspaces, we look at RREF for $I_4 - A$ and $e^{-1}I_4 - A$. It is left as an exercise to the reader to verify that

$$\text{RREF}(I_4 - A) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \text{RREF}(e^{-1}I_4 - A) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Using 11.5 Proposition (algorithm for describing all solutions of $Ax = c$) from Linear Algebra by Professor Heide Gluesing-Luerssen, we find bases $\{(1, 0, 0, 0)\}$ and $\{(0, 0, 0, 1)\}$ for $\text{eig}(\sigma, 1)$ and $\text{eig}(\sigma, e^{-1})$ respectively. ■

Solution for c. From parts (a) and (b), the algebraic multiplicities and geometric multiplicities of the eigenvalues don't match. Hence σ is not diagonalizable. ■

Solution for d. Since the minimal polynomial equals the characteristic polynomial if and only if the dimension of every eigenspace is 1, we conclude that $\chi_\sigma = (x-1)^3(x-e^{-1})$. ■

(2) Let V be an n-dimensional vector space over a field K, and let U be a k-dimensional subspace of V. Consider the set

$$M = \{\varphi : V \to V \mid \varphi \text{ is linear and } \varphi(U) \subset U\}.$$

a) Argue that M is a K-vector space.
b) Determine the dimension of M.

Solution for a. Since $\mathrm{id}_V(U) = U$, we have $\mathrm{id}_V \in M$. Let $\varphi, \psi \in M$ and let $\lambda, \mu \in K$. Since linear combinations of linear maps are still linear (this is a straightforward exercise) we know $\lambda\varphi + \mu\psi$ is linear. Furthermore, observe

$$(\lambda\varphi + \mu\psi)(U) = \lambda\varphi(U) + \mu\psi(U) \subset U.$$

Hence M is a K-vector space (it is a subspace of the space of linear maps). ■

Solution for b. Let $\{u_1, \ldots, u_k\}$ be a basis for U. Extend this to a basis for V, call it $B = \{u_1, \ldots, u_k, v_{k+1}, \ldots, v_n\}$. Then the matrix representation of any map $\varphi \in M$ with respect to the basis B is given by

$$A^B_\varphi = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix}$$

where the representation of $\varphi_{|U}$ is A_{11}. Since $|A_{11}| = k^2$, $|A_{12}| = k(n-k)$, and $|A_{22}| = (n-k)^2$,

$$\dim M = k^2 + k(n-k) + (n-k)^2 = k^2 + n^2 - kn.$$

This follows from the fact that any linear map is completely determined by its action on B. ■

(3) Let G be a group with center Z. Assume that G/Z is cyclic. Show that G is abelian.

Solution. Write $G/Z = \langle gZ \rangle$ for some generator gZ. Let $a, b \in G$. Then $aZ = g^jZ$ and $bZ = g^kZ$ for some $j, k \in \mathbb{Z}$. So $a = g^jx$ and $b = g^ky$ for some $x, y \in Z$. We have

$$ab = g^jxg^ky = g^jg^kyx = g^kg^jyx = g^kyg^jx = ba.$$

Therefore G is abelian. ■

(4) Let G be a finite group, and let p be the smallest prime divisor of the order of G. Suppose H is a subgroup of G with index p. Show that H is a normal subgroup of G.

Solution. Let G act on the set of left cosets of H by left-multiplication. Let π_H be the associated permutation representation. Let $K = \ker \pi_H$ and denote $k = |H : K|$. We have

$$|G : K| = |G : H||H : K| = pk.$$

Since H has p left cosets, the First Isomorphism Theorem tells us G/K is isomorphic to a subgroup of S_p. Therefore $pk = |G/K|$ divides $|S_p| = p!$ by Lagrange's Theorem, so $k \mid (p-1)!$. The prime divisors of $(p-1)!$ are all less than p, and since k is a divisor of $|G|$, the minimality of p ensures every prime divisor of k is greater than or equal to p. Thus $k = 1$, so $H = K$, hence $H \lhd G$. ■

(5) Let R, S be commutative rings with 1.

a) Prove that every ideal of the product ring $R \times S$ is of the form $I \times J$, where I is an ideal of R and J is an ideal of S.

b) Describe all prime ideals of $R \times S$ in terms of the ideals of R and S.

Solution for a. Let X be an ideal of $R \times S$. Since $X \subset R \times S$, $X = I \times J$ for some $I \subset R$ and $J \subset S$. Since $(0,0) \in X$, we have $0 \in I$ and $0 \in J$. Let $a, b \in I$. Then $(a,0), (b,0) \in X$, so $(a-b, 0) \in X$. Thus $a - b \in I$, so I is an additive subgroup of R. Let $r \in R$ and $a \in I$. Then $(r,0)(a,0) = (ra, 0) \in X$. So $ra \in I$, hence I (and similarly J) is an ideal of R. ■

Solution for b. Let $I \times J$ be a prime ideal of $R \times S$. Let $ab \in I$. Then $(ab, 0) \in I \times J$, so either $(a, 0) \in I$ or $(b, 0) \in I$, so either $a \in I$ or $b \in I$. Thus I is a prime ideal of R. Similarly J is a prime ideal of S. Thus the prime ideals of $R \times S$ are the cartesian products of the prime ideals of R and S. ■

(6) Consider the ring $R = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ differentiable}\}$ and the ideal

$$I = \{f \in R \mid f(2) = f'(2) = 0\}.$$

a) Find a map $R \to \mathbb{R}[x]/(x^2)$ to show that the rings R/I and $\mathbb{R}[x]/(x^2)$ are isomorphic.

b) Show that every ideal of R/I is a principal ideal.

Solution for a. Define the map $\varphi : R \to \mathbb{R}[x]/(x^2),\ f \mapsto f(2) + f'(2)x$. Let $f, g \in R$. Then

$$\begin{aligned}\varphi(f+g) &= (f+g)(2) + (f+g)'x \\ &= f(2) + f'(2)x + g(2) + g'(2)x \\ &= \varphi(f) + \varphi(g).\end{aligned}$$

Furthermore,

$$\begin{aligned}\varphi(f)\varphi(g) &= (f(2) + f'(2)x)(g(2) + g'(2)x) \\ &= f(2)g(2) + f(2)g'(2)x + f'(2)g(2)x + f'(2)g'(2)x^2 \\ &= f(2)g(2) + f(2)g'(2)x + f'(2)g(2)x \ \ \text{(since } (x^2) = 0 \text{ in } \mathbb{R}[x]/(x^2)) \\ &= f(2)g(2) + [f(2)g'(2) + f'(2)g(2)]x \\ &= (fg)(2) + (fg)'(2)x \\ &= \varphi(fg).\end{aligned}$$

Thus φ is a ring homomorphism. The elements of $\mathbb{R}[x]/(x^2)$ are of the form $a + bx$ where $a, b \in \mathbb{R}$ since modding out by (x^2) essentially "kills off" any polynomial terms of degree ≥ 2. So let $a + bx \in \mathbb{R}[x]/(x^2)$. Then $h(x) = bx + (a - 2b)$ is differentiable and satisfies $h(2) = a$ and $h'(2) = b$, so $\varphi(h) = a + bx$. Hence φ is surjective, and clearly $\ker\varphi = I$. So by the First Isomorphism Theorem, $R/I \cong \mathbb{R}[x]/(x^2)$. ■

Solution for b. By the Correspondence Theorem for Rings, the ideals of $\mathbb{R}[x]/(x^2)$ correspond to the ideals of $\mathbb{R}[x]$ containing (x^2) via the map $J \mapsto J + (x^2)$. Since $\mathbb{R}[x]$ is a PID, every ideal $J \subset \mathbb{R}[x]$ is principal. Suppose $J = (f)$ for some $f \in \mathbb{R}[x]$. Then $J + (x^2) = (f) + (x^2) = (f + (x^2))$, so $J + (x^2)$ is principal. Hence $\mathbb{R}[x]/(x^2)$ is a principal ideal ring. Using the isomorphism from part (a), R/I is a principal ideal ring. ■

(7) Let $n \in \mathbb{N}$, and let K be a field with $\mathrm{char}(K) \nmid n$. Consider $f = x^n - c \in K[x]$ for some $c \neq 0$, and let E be a splitting field of f over K. Thus, E contains a primitive n^{th} root of unity ζ.

a) Argue, for any root $\alpha \in E$ of f, that $E = K(\zeta, \alpha)$.

b) Suppose $\zeta \in K$. Show that all irreducible factors of f have degree $[E : K]$, and conclude that $[E : K]$ divides n.

c) Assume $\zeta \notin K$. Suppose $n = 2^k$ is a power of 2. Use induction to prove that $[K(\zeta) : K]$ is a power of 2.

d) Suppose n is a power of 2. Use (b) and (c) to show that $[E : K]$ is a power of 2.

Solution for a. The roots of f are $\sqrt[n]{c}, \zeta\sqrt[n]{c}, \ldots, \zeta^{n-1}\sqrt[n]{c}$. So if α is a root of f, then $\alpha = \zeta^i \sqrt[n]{c}$ for some $0 \leq i < n$. Therefore $E = K(\zeta, \alpha)$. ∎

Solution for b. Let g be an irreducible factor of f, and let β be a root of g. Since $\zeta \in K$, we have $E = K(\beta)$. Since g is irreducible, $[E : K] = [K(\beta) : K] = \deg(g)$. Finally, since the degree of f is the sum of the degrees of its irreducible factors, we conclude that $[E : K]$ divides n. ∎

Solution for c. We give an induction-free proof that $[K(\zeta) : K]$ divides $\varphi(n)$, where φ is Euler's totient function. First, since $\mathrm{char}(K) \nmid n$, the polynomial $x^n - 1$ is separable. Since $\zeta \notin K$, the splitting field of $x^n - 1$ is $K(\zeta)$ over K. Therefore $K(\zeta)/K$ is Galois. Next, note that the elements of $G = \mathrm{Gal}(K(\zeta)/K)$ are maps of the form $\sigma_i : \zeta \mapsto \zeta^i$ for some $0 \leq i < n$. We claim that the map $\gamma : G \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\sigma_i \mapsto i$ is injective. Indeed, $\sigma_i \in \ker \gamma$ iff $i = 1$ iff $\sigma_i = \mathrm{id}$, so $\ker \gamma$ is trivial. Thus $G \cong \mathrm{im}\,\gamma \subset (\mathbb{Z}/n\mathbb{Z})^\times$, so $|G|$ divides $\varphi(n)$. But $|G| = |\mathrm{Gal}(K(\zeta)/K)| = [K(\zeta) : K]$, so $[K(\zeta) : K]$ divides $\varphi(n) = \varphi(2^k) = 2^{k-1}$. Hence $[K(\zeta) : K]$ is a power of 2. ∎

Solution for d. Suppose $n = 2^k$. Assume $\zeta \in K$. Then part (b) says $[E : K]$ divides $n = 2^k$, so $[E : K]$ is a power of 2. Now assume $\zeta \notin K$. Part (c) shows that $[K(\zeta) : K] = 2^\ell$ for some $\ell \leq k - 1$. Furthermore, $K(\zeta, \beta)$ is the splitting field of f over $K(\zeta)$, and a similar argument as in part (c) says that $[K(\zeta, \beta) : K(\zeta)]$ is a power of two. Since degrees multiply, it follows that $[E : K]$ is a power of 2. ∎

(8) Let E be the splitting field of $f = x^6 + 1$ over $\mathbb{Q}$.

a) Describe all automorphisms of E explicitly, and determine the isomorphism type of this automorphism group.

b) Describe all subfields of E by specifying suitable elements that one needs to adjoin to $\mathbb{Q}$.

Solution for a. Note that $x^{12} - 1 = (x^6 - 1)(x^6 + 1)$, so $E \subset \mathbb{Q}(\zeta_{12})$ where ζ_{12} is a primitive 12^{th} root of unity. Furthermore, ζ_{12} cannot be a root of $x^6 - 1$ (since then it wouldn't be primitive), so ζ_{12} is a root of $f = x^6 + 1$. Hence $E = \mathbb{Q}(\zeta_{12})$ since all other roots of f are powers of ζ_{12}. Since $[\mathbb{Q}(\zeta_{12}) : \mathbb{Q}] = \varphi(12) = 4$, the Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$ is of order 4. Elements of G are of the form $\sigma_i : \zeta_{12} \mapsto \zeta_{12}^i$ for $(i, 12) = 1$. Since there is no element σ_i of order 4, we conclude that $G \cong C_2 \times C_2$. ∎

Solution for b. We first find the subgroup structure of $C_2 \times C_2$. Denote $C_2 = \{1, g\}$ where $g^2 = 1$. Then the subgroups are

$$\begin{gathered} \{(1,1)\}, \\ \{(1,1),(1,g)\},\ \{(1,1),(g,1)\},\ \{(1,1),(g,g)\}, \\ \{(1,1),(1,g),(g,1),(g,g)\}. \end{gathered}$$

This means we are looking for three intermediate quadratic extensions (since the index of each intermediate subgroup above is 2). The automorphism $\sigma_{11} : \zeta_{12} \mapsto \zeta_{12}^{11}$ is complex conjugation, and thus fixes $\zeta_{12} + \zeta_{12}^{-1}$. Similarly, $\sigma_5 : \zeta_{12} \mapsto \zeta_{12}^5$ fixes $\zeta_{12} + \zeta_{12}^5$. Finally, $\sigma_7 : \zeta_{12} \mapsto \zeta_{12}^7$ fixes $\zeta_{12}^2 + \zeta_{12}^{14} = 2\zeta_{12}^2$. Hence our non-trivial subfields are $\mathbb{Q}(\zeta_{12} + \zeta_{12}^{-1})$, $\mathbb{Q}(\zeta_{12} + \zeta_{12}^5)$ and $\mathbb{Q}(\zeta_{12}^2)$. ■

(9) Let $\alpha = \sqrt{5 + 2\sqrt{6}} \in \mathbb{R}$.

a) Compute the minimal polynomial f of α over $\mathbb{Q}$.
b) Show that f splits into linear factors over $\mathbb{Q}(\alpha)$.
c) Find the isomorphism type of the Galois group of f over $\mathbb{Q}$.
d) How many subfields does $\mathbb{Q}(\alpha)$ have?

Solution for a. Observe that $\alpha^2 = 5 + 2\sqrt{6}$, so $\alpha^2 - 5 = 2\sqrt{6}$. Then $\alpha^4 - 10\alpha^2 + 25 = 24$, so $\alpha^4 - 10\alpha^2 + 1 = 0$. Therefore α is a root of $f = x^4 - 10x^2 + 1$. By the Rational Roots Theorem, f has no linear factors over $\mathbb{Q}$. Since f is an even function, any factorization over $\mathbb{Q}$ into quadratics must satisfy

$$x^2 - 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + b).$$

Expanding the product we see that $b^2 = 1$ and $a^2 - 2b = 10$, a contradiction. ■

Solution for b. Note that $-\alpha$ is also a root of f, and observe

$$\frac{1}{\alpha} = \frac{1}{\sqrt{5 + 2\sqrt{6}}} \iff \alpha = \sqrt{5 + 2\sqrt{6}},$$

so $1/\alpha$ is also a root of f. This shows that $\alpha, -\alpha, 1/\alpha$ are roots of f, so f must split into linear factors over $\mathbb{Q}(\alpha)$. This is because we can write f as $f = (x - \alpha)(x + \alpha)(x - 1/\alpha)(x + 1/\alpha)$. ■

Solution for c. By part (b), the splitting field $E/\mathbb{Q}$ of f is $\mathbb{Q}(\alpha)$. Since the minimal polynomial of α is of degree 4, we have $[E : \mathbb{Q}] = 4$. Since the elements of $G = \mathrm{Gal}(E/\mathbb{Q})$ are completely determined by their action on the generator α, and must permute the roots of f, we have the following automorphisms:

$$\sigma_1 : \alpha \mapsto \alpha,\ \sigma_2 : \alpha \mapsto \alpha^{-1},\ \sigma_3 : \alpha \mapsto \alpha,\ \sigma_4 : \alpha \mapsto -\alpha^{-1}.$$

Since there is no element of order 4, we conclude that $G \cong C_2 \times C_2$. ■

Solution for d. As in problem (8), there are five subgroups of $C_2 \times C_2$, so there are five subfields of $\mathbb{Q}(\alpha)$ by the Galois correspondence. ■