JAN 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 27, 2020.

(1) In the real vector space $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continuously differentiable}\}$ consider the subspace $V = \langle e_1, e_2, e_3, e_4 \rangle$, where

$$e_1(x) = e^x, \quad e_2(x) = e^{2x}, \quad e_3(x) = \sin(x), \quad e_4(x) = \cos(x).$$

Then $\mathcal{A} = \{e_1, e_2, e_3, e_4\}$ forms a basis of V. Consider the linear map

$$T : V \longrightarrow V, \quad f \longmapsto f' \text{ (the derivative of } f).$$

a) Give the matrix representation of T with respect to the basis $\mathcal{A}$.
b) Determine all eigenvalues of T in $\mathbb{R}$.
c) For each eigenvalue determine the corresponding eigenspace of T.
d) Is T diagonalizable over $\mathbb{R}$?
e) Is T triangulable over $\mathbb{R}$?

Solution for a. Observe

$$\begin{aligned} T(e_1) &= 1 \cdot e_1 + 0 \cdot e_2 + 0 \cdot e_3 + 0 \cdot e_4, \\ T(e_2) &= 0 \cdot e_1 + 2 \cdot e_2 + 0 \cdot e_3 + 0 \cdot e_4, \\ T(e_3) &= 0 \cdot e_1 + 0 \cdot e_2 + 0 \cdot e_3 + 1 \cdot e_4, \\ T(e_4) &= 0 \cdot e_1 + 0 \cdot e_2 - 1 \cdot e_3 + 0 \cdot e_4. \end{aligned}$$

So our matrix representation of T w.r.t $\mathcal{A}$ is

$$A_T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

■

Solution for b. Note that $\det(\lambda I_4 - A_T) = (\lambda - 1)(\lambda - 2)(\lambda^2 + 1)$. Eigenvalues in $\mathbb{R}$: $1, 2$. ■

Solution for c. We leave it as an exercise to the reader to check that

$$\text{RREF}(I_4 - A_T) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \text{RREF}(2I_4 - A_T) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

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 $\{(0, -1, 0, 0)\}$ for $\text{eig}(T, 1)$ and $\text{eig}(T, 2)$ respectively. ■

Solution for d. Since V is 4-dimensional over $\mathbb{R}$, and T has only two eigenvectors over $\mathbb{R}$, then T is not diagonalizable. This is because a linear map T is diagonalizable if and only if V has a basis consisting of eigenvectors of T. ∎

Solution for e. Since $\chi_T = (\lambda-1)(\lambda-2)(\lambda^2+1)$ does not factor linearly over $\mathbb{R}$, T is not triangulable over $\mathbb{R}$. ∎

(2) Let V be a finite-dimensional inner product space with inner product denoted by $\langle \cdot, \cdot \rangle$. Let T be a self-adjoint linear map on V, that is,

$$\langle v, T(w) \rangle = \langle T(v), w \rangle \text{ for all } v, w \in V.$$

Show T nilpotent $\implies T = 0$.

Solution. Since T is nilpotent, 0 is the only eigenvalue of T. Furthermore, by the Spectral Theorem for Self Adjoint Maps, there exists a basis for V consisting of eigenvectors of T. Call this basis $\{v_1, \dots, v_n\}$. Now let $v \in V$. We can write $v = \lambda_1 v_1 + \dots + \lambda_n v_n$ for some $\lambda_1, \dots, \lambda_n \in F$. Then

$$T(v) = T(\lambda_1 v_1 + \dots + \lambda_n v_n) = \lambda_1 T(v_1) + \dots + \lambda_n T(v_n) = \lambda_1 \cdot 0 v_1 + \dots + \lambda_n \cdot 0 v_n = 0.$$

Hence $T = 0$ as desired. ∎

(3) Let G be a finite group and let $N \lhd G$ be a normal subgroup of G. Let p be a prime divisor of $|N|$ and suppose N has a unique Sylow p-subgroup.

a) Suppose p does not divide $[G : N]$. Show that G has a unique Sylow p-subgroup.

b) Suppose p divides $[G : N]$. Give an example where the conclusion from (a) does not hold.

Solution for a. Write $|G| = p^k m$ and $|N| = p^\ell n$ where $(p, m) = (p, n) = 1$. Let $P \subset N$ be the unique Sylow p-subgroup of N. Observe

$$[G : P] = [G : N][N : P] = [G : N]n.$$

Since $p \nmid n$ and $p \nmid [G : N]$, then $p \nmid [G : P]$. Since $[G : P] = (p^k m)/p^\ell$ and $\ell \leq k$, it follows that $k = \ell$. This means P is a Sylow p-subgroup of G. Now let P' be any Sylow p-subgroup of G. Then we have $gP'g^{-1} = P$ for some $g \in G$. Therefore $gP'g^{-1} \subset N$. Since N is normal, it is invariant under conjugation by elements in G, so $g^{-1}(gP'g^{-1})g = P' \subset N$. Since P is the *unique* Sylow p-subgroup of N, we have $P = P'$. Thus P is the unique Sylow p-subgroup of G. ∎

Solution for b. Consider D_{12}, the dihedral group on the regular hexagon. Denote

$$D_{12} = \{1, r, \dots, r^5, sr, \dots, sr^5\},$$

where $r^6 = s^2 = 1$ and $sr = rs^{-1}$. Note that $C_6 \cong \langle r \rangle$ is normal in D_{12}, since $[D_{12} : C_6] = 2$. Furthermore, $\{1, r^3\}$ is the unique Sylow 2-subgroup of C_6. Finally, observe that D_{12} does not have a unique Sylow 2-subgroup. This is because the Sylow 2-subgroups of D_{12} are of order 4, and two of them are $\langle s, r^3 \rangle$, and $\langle sr^2, r^3 \rangle$. ∎

(4) Let $n \geq 5$ and let A_n denote the alternating group on n symbols.

a) Let $G \subset A_n$ be a subgroup such that $[A_n : G] < n$. Show that $G = A_n$.

b) Is there a subgroup $H \subset A_n$ such that $[A_n : H] = n$?

Solution for a. Assume there is some subgroup $G \subset A_n$ with $[A_n : G] = m < n$. Let $\mathcal{A}$ be the set of all left cosets of G in A_n, and let A_n act on $\mathcal{A}$ by left-multiplication. Let $\pi : A_n \to S_m$ be the associated permutation representation. Since $n!/2 > m!$ (for $n \geq 5$), the map π cannot be injective. Thus $\ker \pi$ is nontrivial. Since $\ker \pi$ is normal in A_n, and A_n is a simple group, we must have $\ker \pi = A_n$. In particular, we have $aG = G$ for all $a \in A_n$. So there is only one coset of G in A_n, hence $G = A_n$. ∎

Solution for b. Yes. Clearly $A_{n-1} \subset A_n$ for all $n \in \mathbb{N}$, and A_{n-1} is of index n in A_n. ∎

(5) Let

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(m) \in \mathbb{Z} \text{ for all } m \in \mathbb{N}\}.$$

a) Determine the group of units of $\mathrm{Int}(\mathbb{Z})$.
b) Show that 2 is irreducible but not prime in the ring $\mathrm{Int}(\mathbb{Z})$.

Solution for a. Since $\mathrm{Int}(\mathbb{Z})$ is a subring of $\mathbb{Q}[x]$, the units of $\mathrm{Int}(\mathbb{Z})$ must also be units in $\mathbb{Q}[x]$. Note that the units of $\mathbb{Q}[x]$ are the nonzero constant polynomials. Since any unit in $\mathrm{Int}(\mathbb{Z})$ must be an integer after plugging in any element of $\mathbb{N}$, the units of $\mathrm{Int}(\mathbb{Z})$ must be integers. Hence the units of $\mathrm{Int}(\mathbb{Z})$ are $\{-1, 1\}$. ∎

Solution for b. Suppose 2 is reducible in $\mathrm{Int}(\mathbb{Z})$. Then $2 = fg$ where $f, g \in \mathrm{Int}(\mathbb{Z})$ are constant non-unit polynomials. Plugging in 1 on both sides yields $2 = f(1)g(1) = fg$, where $f, g \in \mathbb{Z}$. Since 2 is irreducible in $\mathbb{Z}$, either f or g is a unit in $\mathbb{Z}$. But the units of $\mathbb{Z}$ are precisely the units of $\mathrm{Int}(\mathbb{Z})$, which contradicts our assumption that f, g are non-units. Hence 2 is irreducible in $\mathrm{Int}(\mathbb{Z})$. Finally, we have

$$x(x-1) = 2\binom{x}{2} \in \mathrm{Int}(\mathbb{Z}),$$

so the product of two elements in $\mathrm{Int}(\mathbb{Z})$ is divisible by 2, but neither factor is divisible by 2. ∎

(6) For which $n \in \mathbb{N}$ is the polynomial $f = \sum_{i=0}^{n} x^i \in \mathbb{Q}[x]$ irreducible?

Proof. We have

$$f = \sum_{i=0}^{n} x^i = \frac{x^{n+1} - 1}{x - 1} = \frac{1}{x-1} \prod_{d \,|\, n+1} \Phi_d(x).$$

Since $\Phi_1(x) = x - 1$, the RHS will have exactly one factor iff $n + 1$ is prime. Hence f is irreducible iff $n + 1$ is prime. ∎

(7) Let $K \subset \mathbb{C}$ be a subfield such that $K/\mathbb{Q}$ is Galois with cyclic Galois group of order 4.

a) Show that K has a unique subfield L such that $[L : \mathbb{Q}] = 2$.
b) Show that $\sigma(K) \subset K$, where σ denotes complex conjugation.
c) Show that the subfield L in part (a) is contained in $\mathbb{R}$.

Solution for a. Let $G = \mathrm{Gal}(K/\mathbb{Q}) \cong C_4$. Then G has a unique subgroup of index 2, namely C_2. By the Fundamental Theorem of Galois Theory, C_2 corresponds to a subextension $L/\mathbb{Q}$ such that $[L : \mathbb{Q}] = [C_4 : C_2] = 2$. The uniqueness of L follows from the uniqueness of C_2. ∎

Solution for b. Let $z \in K$. Since $K/\mathbb{Q}$ is a finite extension, it is algebraic. Thus z has a minimal polynomial $m_z(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Q}[x]$. Since σ is an automorphism of $\mathbb{C}$ that fixes $\mathbb{Q}$ pointwise, we have

$$\begin{aligned} m_z(\sigma(z)) &= \sigma(z)^n + a_{n-1}\sigma(z)^{n-1} + \ldots + a_0 \\ &= \sigma(z^n) + \sigma(a_{n-1})\sigma(z^{n-1}) + \ldots + \sigma(a_0) \\ &= \sigma(z^n + a_{n-1}z^{n-1} + \ldots + a_0) \\ &= \sigma(0) \\ &= 0. \end{aligned}$$

Thus $\sigma(z)$ is also a root of $m_z(x)$. Since $K/\mathbb{Q}$ is Galois, it is normal. Thus $\sigma(z) \in K$. ■

Solution for c. By part (b), $\sigma(z) \in K$, so $z = \sigma(\sigma(z)) \in \sigma(K)$. Thus $\sigma(K) = K$, so σ is an automorphism of K, hence $\sigma \in G$. Note that $\text{ord}(\sigma)$ is at most 2. We proceed by cases. Suppose $\text{ord}(\sigma) = 1$. Then $\sigma(x) = x$ for all $x \in K$, so $L \subset K \subset \mathbb{R}$. Now suppose $\text{ord}(\sigma) = 2$. Then σ generates the unique two element subgroup of G, and hence fixes all of L by part (a). Therefore $L \subset \mathbb{R}$. In both cases, the claim has been proven. ■

(8) Let q be a prime power and $m \in \mathbb{N}$. Consider the finite fields $\mathbb{F}_q \subset \mathbb{F}_{q^m}$ and the map

$$\tau : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}, \quad a \longmapsto \sum_{i=0}^{m-1} a^{q^i}.$$

a) τ is $\mathbb{F}_q$-linear.
b) $\text{im } \tau \subset \mathbb{F}_q$.
c) τ is not the zero map.
d) $\text{im } \tau = \mathbb{F}_q$.

Solution for a. Let $a, b \in \mathbb{F}_{q^m}$, and let $\lambda \in \mathbb{F}_q$. We have

$$\tau(\lambda a + b) = \sum_{i=0}^{m-1} (\lambda a + b)^{q^i} = \lambda \sum_{i=0}^{m-1} a^{q^i} + \sum_{i=0}^{m-1} b^{q^i} = \lambda\tau(a) + \tau(b).$$

We can do this via the Frobenius automorphism, and since $\lambda^{q^i} = \lambda$ for all $q \geq 1$. ■

Solution for b. Let $a \in \mathbb{F}_{q^m}$. Observe

$$\tau(a)^q = \left(\sum_{i=0}^{m-1} a^{q^i}\right)^q = \sum_{i=0}^{m-1} a^{q^{i+1}} = \underbrace{a^q + a^{q^2} + \ldots + a^{q^m} = a + a^q + \ldots + a^{q^{m-1}}}_{\text{since } a^{q^m} = a \text{ in } \mathbb{F}_{q^m}} = \tau(a).$$

Hence $\tau(a) \in \mathbb{F}_q^\times$, so $\text{im } \tau \subset \mathbb{F}_q$. ■

Solution for c. Note that $\tau(a) = 0$ implies a is a root of the polynomial $f = x + \ldots + x^{q^{m-1}}$. Since $\deg(f) = q^{m-1}$, we know f has at most q^{m-1} roots in $\mathbb{F}_{q^m}$. Since $q^{m-1} < q^m$, there must exist an element $b \in \mathbb{F}_{q^m}$ such that $f(b) \neq 0$. Therefore $\tau(b) \neq 0$, hence τ is not the zero map. ■

Solution for d. Write $q = p^k$ for some $k \geq 1$. By similar reasoning as in part (c), the biggest $\ker \tau$ can be is $\mathbb{F}_{q^{m-1}}$. Therefore $\dim \ker \tau \leq k(m-1) = km - k$. By part (b), $\dim \text{im } \tau \leq k$. By rank-nullity, $km = \dim \ker \tau + \dim \text{im } \tau \leq km - k + \dim \text{im } \tau$. Therefore $km - (km - k) \leq \dim \text{im } \tau$, so $k \leq \dim \text{im } \tau$. Hence $\dim \text{im } \tau = k$, so $\text{im } \tau = \mathbb{F}_q$. ■

(9) Let $K \subset \mathbb{C}$ be the splitting field of $f = x^5 - 2$ over $\mathbb{Q}$.

a) Show that $[K : \mathbb{Q}] = 20$.

b) Show that there exists a unique subfield L of K such that $[K : L] = 5$.

c) Give the subfield L explicitly.

Solution for a. The roots of f are $\sqrt[5]{2}, \zeta_5\sqrt[5]{2}, \ldots, \zeta_5^4\sqrt[5]{2}$, where ζ_5 is a primitive 5^{th} root of unity. Therefore $K \cong \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$. By the degree formula,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}, \zeta_5) : \mathbb{Q}(\zeta_5)][\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 5\varphi(5) = 5 \cdot 4 = 20.$$

■

Solution for b. Since K is the splitting field of the separable polynomial f, we know $K/\mathbb{Q}$ is Galois with $|G = \mathrm{Gal}(K/\mathbb{Q})| = 20$. Let n_5 denote the number of Sylow 5-subgroups of G. By Sylow's Theorem, $n_5 \equiv 1 \pmod 5$, and $n_5 \mid 4$. This forces $n_5 = 1$, so G has a unique subgroup P with $|P| = 5$. Let $L = \mathrm{Fix}(P)$. By the Fundamental Theorem of Galois Theory, $[K : L] = |P| = 5$. The uniqueness of L follows from the uniqueness of P. ■

Solution for c. $L \cong \mathbb{Q}(\zeta_5)$. ■