JUNE 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 13, 2020.

(1) Let $n \in \mathbb{N}$, and let K be a field whose characteristic does not divide n. Consider the $n \times n$ matrix with entries in K

$$A = \frac{1}{n} \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}.$$

a) Show that A is idempotent, that is, $A^2 = A$.
b) Find an invertible matrix S such that $S^{-1}AS$ is a diagonal matrix. Specify S and the diagonal matrix explicitly.

Solution for a. Each entry $c_{ij} \in A^2$ is given by

$$c_{ij} = \sum_{k=1}^{n} \frac{1}{n} \cdot \frac{1}{n} = \frac{1}{n^2} \sum_{k=1}^{n} 1 = \frac{1}{n^2} \cdot n = \frac{1}{n},$$

so $A^2 = A$ as desired. ∎

Solution for b. By part (a), we have $A^2 - A = 0$. So A is a root of the polynomial $x^2 - x$, thus the minimal polynomial $\mu_A(x)$ for A is either $x, x-1, x^2-x$. By inspection, $\mu_A(x) = x^2 - x$. Since the characteristic polynomial $\chi_A(x)$ of A is of degree n and is divisible by $\mu_A(x)$, we must have $\chi_A(x) = x^n - x^{n-1} = x^{n-1}(x-1)$. Thus 0 is of algebraic multiplicity $n-1$, and 1 is of algebraic multiplicity 1. So a basis for the eigenspace of 0 is $\{v_1, \ldots, v_{n-1}\}$, where each v_i is the column vector with a 1 and a -1 in the i^{th} and $(i+1)^{\text{th}}$ positions respectively. Furthermore, a basis for the eigenspace of 1 is just $\{v\}$, where v is the column vector containing all 1s. It is left as a straightforward exercise to the reader to verify that these are indeed bases. Finally, the desired matrices are given as

$$S^{-1}AS = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ -1 & 1 & \cdots & \vdots & \vdots \\ 0 & -1 & \cdots & \vdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & 1 \end{pmatrix}.$$

∎

(2) Let $\varphi, \psi : V \to V$ be endomorphisms on a finite-dimensional vector space over a field K such that $\varphi \circ \psi = \psi \circ \varphi$. Denote the identity map on V by id_V.
a) For every $\mu \in K$, show that $\mu \mathrm{id}_V - \varphi$ maps eigenvectors of ψ onto eigenvectors of ψ.

b) Assume V has a basis consisting of eigenvectors of ψ and a basis consisting of eigenvectors of φ. Prove that V has a basis consisting of vectors that are eigenvectors of both φ and ψ.

Solution for a. Let $\mu \in K$, let v be an eigenvector of ψ, and let $\lambda \in K$ be the corresponding eigenvalue to v. We have

$$\psi((\mu \mathrm{id}_V - \varphi)(v)) = \mu\psi(v) - \psi(\varphi(v)) = \mu\lambda v - \varphi(\psi(v)) = \mu\lambda v - \lambda\varphi(v) = \lambda(\mu \mathrm{id}_V - \varphi)(v).$$

Therefore $\mu \mathrm{id}_V - \varphi$ maps eigenvectors of ψ onto eigenvectors of ψ. ∎

Solution for b. Let $\lambda_1, \ldots, \lambda_n$ be the distinct eigenvalues of φ. For each λ_i, let $c_{i,1}, \ldots, c_{i,m_i}$ be the corresponding eigenvectors of φ. By assumption, φ is diagonalizable, so we can write

$$V \cong V_1 \oplus \cdots \oplus V_n$$

where each $V_i = \mathrm{eig}(\varphi, \lambda_i)$. For each $v_i \in V_i$, we have $v_i = \alpha_1 c_{i,1} + \ldots + \alpha_{m_i} c_{i,m_i}$ for $\alpha_j \in K$. Observe

$$\begin{aligned}
\varphi(\psi(v_i)) &= \psi(\varphi(v_i)) \\
&= \psi(\alpha_1\varphi(c_{i,1}) + \ldots + \alpha_{m_i}\varphi(c_{i,m_i})) \\
&= \psi(\alpha_1\lambda_i c_{i,1} + \ldots + \alpha_{m_i}\lambda_i c_{i,m_i}) \\
&= \lambda_i\psi(v_i).
\end{aligned}$$

Thus $\psi(v_i)$ is an eigenvector of φ corresponding to λ_i, so $\psi(v_i) \in V_i$. Therefore $\psi(V_i) \subset V_i$, and since ψ is diagonalizable by assumption, we can find find a basis $\{d_{i,1}, \ldots, d_{i,m_i}\}$ for each V_i consisting of eigenvectors of ψ. Finally, we know that

$$\bigcup_{i=1}^{n} \{d_{i,1}, \ldots, d_{i,m_i}\}$$

forms a basis for V, and each $\varphi(d_{i,j}) = \lambda_i d_{i,j}$. Thus V has a basis consisting of vectors who are eigenvectors of both φ and ψ. ∎

(3) Consider the symmetric group S_8 on 8 elements.

a) How many elements of S_8 can be written as a disjoint product of a 4-cycle and a 2-cycle?

b) Determine the number of elements in S_8 that have order four.

Solution for a. The number of 4+2 cycles is given by

$$\frac{8!}{4 \cdot 2 \cdot 1^2(2!)} = 2520.$$

∎

Solution for b. The elements of order 4 in S_8 are the 4 cycles, the 4+2 cycles, the 4+2+2 cycles, and the 4+4 cycles. By part (a), the number of 4+2 cycles is 2520. We can count the others as follows:

$$\begin{aligned}
\#(4 \text{ cycles}) &= \frac{8!}{4 \cdot 1^4(4!)} = 420 \\
\#(4{+}2{+}2 \text{ cycles}) &= \frac{8!}{4 \cdot 2^2(2!)} = 1260 \\
\#(4{+}4 \text{ cycles}) &= \frac{8!}{4^2(2!)} = 1260
\end{aligned}$$

for a total of $420 + 2520 + 1260 + 1260 = 5460$ elements of order 4. ∎

(4) Let H be a subgroup of G with $[G : H] = n$. Prove that there is a normal subgroup N of G with $N \subset H$ such that $[G : N] \leq n!$.

Solution. Let A be the set of left cosets of H in G, and let G act on A by left-multiplication. Let $\pi_H : G \longrightarrow S_A$ be the associated permutation representation. Then $\ker \pi_H$ is a normal subgroup of G. Furthermore, $\ker \pi_H \subset H$ since if $x \in \ker \pi_H$, then x acts as the identity on any left coset of H, so $x \in H$. By the First Isomorphism Theorem,

$$G/\ker \pi_H \cong \text{im } \pi_H \subset S_A.$$

Since $[G : H] = n$, we have $|A| = n$, so $|S_A| = n!$. Thus $|G/\ker \pi_H| = |\text{im } \pi_H| \leq |S_A| = n!$, so $[G : \ker \pi_H] \leq n!$. Hence $N = \ker \pi_H$ satisfies the requirements. ∎

(5) Let K be a field, and consider the set $R = \{f \in K[x] \mid f'(1) = f''(1) = 0\}$. Show:

a) R is a subring of $K[x]$.
b) $(x-1)^3$ and $(x-1)^4$ are irreducible elements of R.
c) R is not a UFD.

Solution for a. First of all, $\mathbb{1}(x) = 1 \in R$ since $\mathbb{1}'(x) \equiv \mathbb{1}''(x) \equiv 0$. Now let $f, g \in R$. We have

$$(fg)'(1) = f(1)g'(1) + f'(1)g(1) = 0 + 0 = 0,$$

and

$$(fg)''(1) = (fg')'(1) + (f'g)'(1) = f(1)g''(1) + 2f'(1)g'(1) + f''(1)g(1) = 0 + 0 + 0 = 0,$$

so $fg \in R$. Furthermore, observe

$$(f - g)'(1) = f'(1) - g'(1) = 0 - 0 = 0,$$

and

$$(f - g)''(1) = f''(1) - g''(1) = 0 - 0 = 0,$$

so $f - g \in R$. Hence R is a subring of $K[x]$. ∎

Solution for b. It is straightforward to verify $(x-1)^3$ and $(x-1)^4$ are elements of R. If $(x-1)^3$ were reducible, it would have a non-zero linear factor. However, the first derivative of a non-zero linear polynomial is a non-zero constant, so $(x-1)^3$ is irreducible in R. If $(x-1)^4$ were reducible, it would either have a non-zero linear factor, or a non-zero quadratic factor. We already covered the case of a linear factor, and if it had a quadratic factor, the second derivative of the factor would be a non-zero constant. Thus $(x-1)^4$ is irreducible in R. ∎

Solution for c. We have the non-unique factorization

$$(x-1)^3(x-1)^3(x-1)^3(x-1)^3 = (x-1)^{12} = (x-1)^4(x-1)^4(x-1)^4$$

into irreducibles. Thus R is not a UFD. ∎

(6) Fix a prime number p, and consider the subset

$$R = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z} \text{ coprime, } p \text{ does not divide } b \right\} \subset \mathbb{Q}.$$

a) Show that R is a subring of $\mathbb{Q}$.
b) Determine the units of R.
c) Prove that each non-zero ideal of R is principal and equal to (p^e) for some $e \in \mathbb{N}_0$.
d) Describe explicitly the quotient field of R as a subfield of $\mathbb{Q}$.

Solution for a. Clearly $1 \in R$. Let $a/b, c/d \in R$. Then $(a/b)(c/d) = ac/bd$, and $(a/b) - (c/d) = (ad - bc)/(bd)$. Since $p \nmid b$ and $p \nmid d$, we have $p \nmid bd$. Thus (when writing in reduced form) we have $(a/b)(c/d) \in R$ and $(a/b) - (c/d) \in R$. Hence R is a subring of $\mathbb{Q}$. ∎

Solution for b. The units of R are the elements a/b such that $(a, b) = 1$ and p does not divide a and b. ∎

Solution for c. Let $I \subset R$ be a non-zero ideal. Any element of R can be written as $(x/y)p^w$ where $p \nmid y$, $p \nmid x$ and $(x, y) = 1$ for some $w \geq 0$ (since we can pull every factor of p out of a). So we can find $(a/b)p^n \in I$ such that n is minimal. Since $p \nmid a$, part (b) says that a/b is a unit in R. Thus $b/a \in R$, so $(b/a)(a/b)p^n \in I$, hence $p^n \in I$. We claim $I = (p^n)$. To see why, let $(c/d)p^m \in I$ where $n \leq m$ (n is minimal). Then $(c/d)p^{m-n} \in R$, so $(c/d)p^m = (c/d)p^{m-n} \cdot p^n \in (p^n)$. Hence $I \subset (p^n)$, and since $(p^n) \subset I$ is clear, we are done. ∎

Solution for d. $\mathbb{Q}$ does not contain any proper subfields, so the quotient field of R is given as

$$RR^{-1} = \left\{ \frac{ad}{bc} \,\middle|\, (a, b) = (c, d) = 1,\ c \neq 0,\ p \text{ does not divide } b, d \right\} \cong \mathbb{Q}.$$

∎

(7) Let t be a variable. Show that the field extension $\mathbb{C}(t)/\mathbb{C}(t^{20})$ is Galois and determine the isomorphism type of its Galois group.

Solution. The roots of the polynomial $f(x) = x^{20} - t^{20} \in \mathbb{C}(t^{20})[x]$ are $t, \zeta_{20}t, \ldots, \zeta_{20}^{19}t$, where ζ_{20} is a primitive 20^{th} root of unity. Since $\zeta_{20} \in \mathbb{C}$, the splitting field of $f(x)$ over $\mathbb{C}(t^{20})$ is $\mathbb{C}(t)$. Clearly $f(x)$ is separable, so $\mathbb{C}(t)$ is Galois over $\mathbb{C}(t^{20})$. Furthermore, since $f(x)$ is irreducible via Eisenstein, this is a degree 20 extension, so the Galois group is of order 20. Elements of the Galois group are completely determined by how they act on the generator t, and must also permute the roots of $f(x)$. So we can define the automorphisms $\sigma_k : t \mapsto \zeta_{20}^k t$ for $0 \leq k \leq 19$. There are 20 such σ_k, so we have found all elements of the Galois group. Any σ_r where $\gcd(r, 20) = 1$ is a generator for this Galois group, so we conclude that $\mathrm{Gal}(\mathbb{C}(t)/\mathbb{C}(t^{20})) \cong C_{20}$, the cyclic group on 20 elements. ∎

(8) Let K be the splitting field of the polynomial $f = x^4 + x^3 + 1$ over $\mathbb{F}_2$.
- a) Determine K up to isomorphism.
- b) Find the least $m \in \mathbb{N}$ such that f divides $x^m - 1$ in $\mathbb{F}_2[x]$.
- c) Let α be a root of f. Describe explicitly all roots of f.

Solution for a. Plugging in the elements of $\mathbb{F}_2$ into f shows that f has no linear factors. Assume $f = gh$ where g, h are quadratics in $\mathbb{F}_2[x]$. Since the only unit in $\mathbb{F}_2$ is 1, we can assume g, h are monic. Furthermore, since f has constant term 1, we can assume g, h have constant terms 1. Write $g = x^2 + ax + 1$ and $h = x^2 + bx + 1$. Expanding the product, we obtain

$$f = gh = x^4 + (a + b)x^3 + (ab + 2)x^2 + (a + b)x + 1.$$

Equating coefficients, we must have $a + b = 1$ on the cubic term, and $a + b = 0$ on the linear term, a contradiction. Thus f is irreducible over $\mathbb{F}_2$, so adjoining one root of f to $\mathbb{F}_2$ generates a degree 4 extension. By uniqueness of finite fields, this extension is $\mathbb{F}_{2^4} = \mathbb{F}_{16}$. Since any finite extension of a finite field is normal, every other root of f must belong to $\mathbb{F}_{16}$. Hence $K \cong \mathbb{F}_{16}$. ∎

Solution for b. By part (a), $\mathbb{F}_{16}^{\times}$ is the smallest cyclic group containing the roots of f. Since $|\mathbb{F}_{16}^{\times}| = 15$, each root of f is a 15^{th} root of unity, so f divides $x^{15} - 1$ over $\mathbb{F}_2$. Note that $m = 15$ must be minimal, since if any $k < m$ had the property that each root of f is a k^{th} root of unity, then the splitting field of f over $\mathbb{F}_2$ would contain $\mathbb{F}_{k+1}$, but be properly contained in $\mathbb{F}_{16}$, a contradiction. ∎

Solution for c. The other roots of f are $\alpha^2, \alpha^4, \alpha^8$. To see why these are all distinct, we prove the following claim: $\alpha^{2^i} = \alpha^{2^j}$ if and only if $i \equiv j \bmod 4$. Without loss of generality, suppose $i \leq j$, so $j = i + k$ for some $k \geq 0$. Then

$$\begin{aligned}
\alpha^{2^i} = \alpha^{2^j} &\iff \alpha^{2^i} = (\alpha^{2^k})^{2^i} \\
&\iff (\alpha^{2^k})^{2^i} - \alpha^{2^i} = 0 \\
&\iff (\alpha^{2^k} - \alpha)^{2^i} = 0 \\
&\iff \alpha^{2^k} - \alpha = 0 \\
&\iff f \mid (x^{2^k} - x) \text{ in } \mathbb{F}_2[x] \\
&\iff 4 \mid k \\
&\iff i \equiv j \bmod 4.
\end{aligned}$$

This proves the claim, hence each α^{2^r} where $0 \leq r \leq 3$ is distinct, so we have completely described the roots of f. ∎

(9) a) Determine the Galois group of the polynomial $x^3 - 5$ over $\mathbb{Q}$ explicitly.
b) Show that the real number $\sqrt[3]{5}$ is not contained in any cyclotomic field extension of $\mathbb{Q}$.

Solution for a. The roots of $f = x^3 - 5$ are $\sqrt[3]{5}, \zeta_3\sqrt[3]{5}, \zeta_3^2\sqrt[3]{5}$, where ζ_3 is some primitive 3^{rd} root of unity. So the splitting field for f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{5}, \zeta_3)$. By the Degree formula, we have

$$[\mathbb{Q}(\sqrt[3]{5}, \zeta_3) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}, \zeta_3) : \mathbb{Q}(\zeta_3)][\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 3\varphi(3) = 6.$$

Since f is clearly separable, $\mathbb{Q}(\sqrt[3]{5}, \zeta_3)$ is Galois over $\mathbb{Q}$ whose Galois group G has order 6. As before, any element of G is completely determined by its action on the generators $\sqrt[3]{5}$ and ζ_3, and must also permute the roots of their minimal polynomials. Define the automorphisms

$$\sigma_{ij} : \begin{cases} \sqrt[3]{5} & \mapsto \quad \zeta_3^i\sqrt[3]{5} \\ \zeta_3 & \mapsto \quad \zeta_3^j \end{cases}$$

where $0 \leq i \leq 2$, and $1 \leq j \leq 2$. Counting the σ_{ij}, we see that we have found all 6 elements of G. Since there is no element of order 6, we must have $G \cong S_3$. ∎

Solution for b. Suppose $\sqrt[3]{5} \in \mathbb{Q}(\zeta_n)$ for some primitive n^{th} root of unity ζ_n. Then we have $\mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{Q}(\zeta_n)$. The Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is abelian, so all of its subgroups are normal. The Fundamental Theorem of Galois Theory then says that every subextension of $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$, and therefore normal over $\mathbb{Q}$. In particular, $\mathbb{Q}(\sqrt[3]{5})$ is normal over $\mathbb{Q}$, which means any irreducible polynomial in $\mathbb{Q}[x]$ having a root in $\mathbb{Q}(\sqrt[3]{5})$ must have all its roots in $\mathbb{Q}(\sqrt[3]{5})$. However, $x^3 - 5$ is irreducible over $\mathbb{Q}$ via Eisenstein and has a root $\sqrt[3]{5} \in \mathbb{Q}(\sqrt[3]{5})$, but $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{5})$, so not all roots are in $\mathbb{Q}(\sqrt[3]{5})$. This is a contradiction, so $\sqrt[3]{5}$ cannot be contained in any cyclotomic extension of $\mathbb{Q}$. ∎