JUNE 2015 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: June 1, 2020.

(1) Let K be a field of characteristic not equal to 2. Let

$$M = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \in K^{2\times 2}$$

and consider the linear map

$$\varphi : K^{2\times 2} \longrightarrow K^{2\times 2}, \quad X \longmapsto MX - XM.$$

a) Find the matrix represenation of φ with respect to the standard basis of $K^{2\times 2}$.
b) Find $\ker \varphi$.
c) Find all eigenvalues of φ.
d) Show that φ is diagonalizable.

Solution for a. We leave it to the reader to check that

$$\varphi \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix}, \quad \varphi \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix},$$
$$\varphi \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 2 & -2 \end{pmatrix}, \quad \varphi \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}.$$

So the matrix representation of φ is

$$A_\varphi = \begin{pmatrix} 0 & 0 & 2 & 0 \\ -2 & -2 & 0 & 2 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & -2 & 0 \end{pmatrix}.$$

■

Solution for b. We have

$$\mathrm{RREF}(A_\varphi) = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

We then form

$$\tilde{A}_\varphi = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Hence ker $A_\varphi = \langle (1,-1,0,0), (-1,0,0,-1) \rangle$. Therefore,

$$\text{ker } \varphi = \langle \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle.$$

■

Solution for c. The eigenvalues of φ are the eigenvalues of A_φ. Therefore, we compute

$$\det(\lambda I_4 - A_\varphi) = \det \begin{pmatrix} \lambda & 0 \\ 2 & \lambda+2 \end{pmatrix} \det \begin{pmatrix} \lambda-2 & 0 \\ 2 & \lambda \end{pmatrix} = \lambda^2(\lambda^2-4).$$

So the eigenvalues of φ are 0 with alg. mult. 2, and ± 2 with alg. mults. 1. ■

Solution for d. Since the algebraic multiplicities of the eigenvalues ± 2 are both 1, this forces the geometric multiplicities to be 1. So we need only check that the geometric multiplicity of the eigenvalue 0 is 2. Since ker φ is the eigenspace of the eigenvalue 0, part (b) says that the dimension is 2, so φ is diagonalizable. ■

(2) Let K be a field, a an element in a field extension such that a is algebraic over K. Denote by $f \in K[x]$ the minimal polynomial of a over K. Consider the K-vector space $V = K[x]/(f)$ and the K-linear map

$$\varphi : V \longrightarrow V, \quad g + (f) \longmapsto xg + (f).$$

Thus, $\varphi \in \text{End}(V)$. Show that the minimal polynomial of φ is given by f.

Solution. It is easier to think about this problem in terms of the isomorphism $V \cong K(a)$. Here, $x + (f)$ corresponds to a, so we are really working with the map

$$\varphi : K(a) \to K(a), \quad v \mapsto av.$$

Let $f = x^n + b_{n-1}x^{n-1} + \ldots + b_0$ for some $b_i \in K$, let $v \in K(a)$, and observe

$$\begin{aligned} f(\varphi)(v) &= (\varphi^n + b_{n-1}\varphi^{n-1} + \ldots + b_0\text{id})(v) \\ &= \varphi^n(v) + b_{n-1}\varphi^{n-1}(v) + \ldots + b_0\text{id}(v) \\ &= a^n v + b_{n-1}a^{n-1}v + \ldots + b_0 v \\ &= (a^n + b_{n-1}a^{n-1} + \ldots + b_0)v \\ &= f(a)v \\ &= 0 \text{ (since } a \text{ is a root of } f). \end{aligned}$$

Therefore $f(\varphi) = 0$, and since f is monic-irreducible, f is the minimal polynomial of φ. ■

(3) Let G be a finite group and $\mathcal{X} = \{H \leq G\}$, that is, $\mathcal{X}$ is the set of all subgroups of G. Consider the action

$$G \times \mathcal{X} \longrightarrow \mathcal{X}, \quad (g, H) \longmapsto gHg^{-1}$$

and denote by $\mathcal{O}_H$ the orbit of $H \in \mathcal{X}$. Show the following:

a) For any $H \in \mathcal{X}$ we have $|\mathcal{O}_H| = 1 \iff H \lhd G$.

b) Let p be a prime and G be a nontrivial p-group. Let $n = |\mathcal{X}|$ and m be the number of normal subgroups of G. Show that $p \mid (n - m)$.

Solution for a. Observe

$$\begin{aligned}|\mathcal{O}_H| = 1 &\iff |\{gHg^{-1} \,|\, g \in G\}| = 1 \\ &\iff gHg^{-1} = H \text{ for all } g \in G \text{ (since } eHe^{-1} = H \in \mathcal{O}_H) \\ &\iff H \lhd G.\end{aligned}$$

■

Solution for b. By part (a), this action has precisely m fixed points. By the Fixed Point Lemma for p-groups, $m \equiv n \pmod{p}$, hence $p \mid (n - m)$. ■

(4) Consider the group $G = \mathbb{Q}/\mathbb{Z}$ under addition.

a) Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and suppose $\gcd(a, b) = 1$. Show that $\langle \frac{a}{b} + \mathbb{Z} \rangle = \langle \frac{1}{b} + \mathbb{Z} \rangle$ for the cyclic subgroups of G generated by the given elements.

b) Show that for each $n \in \mathbb{N}$ there exists a unique subgroup of order n.

Solution for a. Observe

$$\begin{aligned}x \in \langle \frac{a}{b} + \mathbb{Z} \rangle &\iff x = \frac{a}{b} \cdot k + \mathbb{Z} \text{ for some } k \in \mathbb{Z} \\ &\iff x = \frac{1}{b} \cdot ak + \mathbb{Z} \\ &\iff x \in \langle \frac{1}{b} + \mathbb{Z} \rangle.\end{aligned}$$

■

Solution for b. Let $n \in \mathbb{N}$. Then $N = \langle \frac{1}{n} + \mathbb{Z} \rangle$ is a subgroup of order n. Since any other subgroup of order n must be of the form $\langle \frac{a}{n} + \mathbb{Z} \rangle$ for some $a \in \mathbb{Z}$, it follows that N is unique by part (a). ■

(5) Let K be a field and $f, g \in K[x]$. Show TFAE:

i) There exists a ring map of the form

$$\varphi : K[x]/(f) \longrightarrow K[x]/(g),\; p + (f) \longmapsto p + (g).$$

ii) g divides f in $K[x]$.

Solution. ($i \implies ii$) We have $f + (g) = \varphi(f + (f)) = \varphi((f)) = (g)$, so $f \in (g)$, hence g divides f in $K[x]$. Note that $\varphi((f)) = (g)$ since ring maps must take zero to zero.

($i \impliedby ii$) Since g divides f, we have $f \in (g)$, so $(f) \subset (g)$. We need to show φ is a ring map. First, let's show φ is well-defined. Let $p_1 + (f) = p_2 + (f) \in K[x]/(f)$. Then $p_1 - p_2 \in (f) \subset (g)$, so $p_1 + (g) = p_2 + (g)$. Therefore $\varphi(p_1 + (f)) = \varphi(p_2 + (f))$, so φ is well-defined. Now observe

$$\begin{aligned}\varphi(p_1 + (f) + p_2 + (f)) &= \varphi((p_1 + p_2) + (f)) \\ &= (p_1 + p_2) + (g) \\ &= p_1 + (g) + p_2 + (g) \\ &= \varphi(p_1 + (f)) + \varphi(p_2 + (f)).\end{aligned}$$

Furthermore,

$$\begin{aligned}\varphi((p_1 + (f))(p_2 + (f))) &= \varphi(p_1p_2 + (f)) \\ &= p_1p_2 + (g) \\ &= (p_1 + (g))(p_2 + (g)) \\ &= \varphi(p_1 + (f))\varphi(p_2 + (f)).\end{aligned}$$

Therefore φ is a ring map. ■

(6) Consider the ring $\mathbb{Z}[i]$ of Gaussian integers, and let f be the ring map

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}[i]/(3 + 2i),\ c \longmapsto c + (3 + 2i).$$

Show the following.
a) f is surjective.
b) $\ker f = 13\mathbb{Z}$.
c) $|\mathbb{Z}[i]/(3 + 2i)| = 13$.

Solution for a. Let $a+bi+(3+2i) \in \mathbb{Z}[i]/(3+2i)$. Let $x = a+bi$, and we want to find a $c \in \mathbb{Z}$ such that $x+(3+2i) = c+(3+2i)$. This happens when $x-c \in (3+2i)$. Write $x-c = (a-c)+bi = d+bi$. We have thus reduced the problem to finding a suitable $d \in \mathbb{Z}$ for which $d + bi \in (3 + 2i)$. Note that $d + bi \in (3 + 2i)$ if and only if $\frac{d+bi}{3+2i} \in \mathbb{Z}[i]$. Computation gives

$$\frac{d + bi}{3 + 2i} = \frac{d + bi}{3 + 2i} \cdot \frac{3 - 2i}{3 - 2i} = \frac{3d + 2b + (3b - 2d)i}{13} \in \mathbb{Q}[i].$$

In order for the above quantity to live in $\mathbb{Z}[i]$ rather than $\mathbb{Q}[i]$, we must have $13 \mid 3d + 2b$ and $13 \mid 3b - 2d$. If 13 divides both of these numbers, it will divide their sum, namely $5b + d$. Let's pick $d = 13 - 5b$. Then

$$3d + 2b = 3(13 - 5b) + 2b = 3 \cdot 13 - 15b + 3b = 3 \cdot 13 - 13b,$$

which is clearly divisible by 13. Furthermore, we have

$$3b - 2d = 3b - 2(13 - 5b) = 3b - 2 \cdot 13 + 10b = 13b - 2 \cdot 13,$$

which is also divisible by 13. We have therefore found $d \in \mathbb{Z}$ such that $x - c = (a - c) + bi = d + bi \in (3 + 2i)$. Hence f is surjective. ■

Solution for b. Let $a \in \ker f$. Then $a + (3 + 2i) = (3 + 2i)$, so $a \in (3 + 2i)$. Therefore $a = (r + si)[3 + 2i]$ for some $r, s \in \mathbb{Z}$. We have

$$a = (r + si)[3 + 2i] = 3r + 2ir + 3si - 2s = 3r - 2s + (2r + 3s)i,$$

so $2r+3s = 0$ and $3r-2s = a$. Then $s = -(2/3)r$, so $3r+(4/3)r = a$. Therefore $13r = 3a$, so $13 \mid a$, hence $a \in 13\mathbb{Z}$. This shows $\ker f \subset 13\mathbb{Z}$. For the reverse inclusion, let $b \in 13\mathbb{Z}$, so $b = 13w$ for some $w \in \mathbb{Z}$. We have $f(b) = f(13w) = 13w+(3+2i)$, and we want $f(b) = (3+2i)$. This happens precisely when $13w \in (3 + 2i)$, so we need to find a $c + di \in \mathbb{Z}[i]$ such that $13w = (c + di)[3 + 2i]$. Expanding, we obtain

$$13w = (c + di)[3 + 2i] = 3c + 2ci + 3di - 2d = 3c - 2d + (2c + 3d)i,$$

so $2c+3d = 0$ and $3c-2d = 13w$. Then $d = -(2/3)c$, so $3c+(4/3)c = 13w$. Therefore $13c = 3\cdot 13w$, so $c = 3w$ ($\mathbb{Z}$ is an integral domain). It then follows that $d = -(2/3)c = -(2/3)3w = -2w$. This shows that $c, d \in \mathbb{Z}$, so $b = 13w = (c + di)[3 + 2i] \in (3 + 2i)$. Hence $\ker f = 13\mathbb{Z}$. ■

Solution for c. By the FIT, $\mathbb{Z}/13\mathbb{Z} \cong \mathbb{Z}[i]/(3 + 2i)$, so $|\mathbb{Z}[i]/(3 + 2i)| = 13$. ■

(7) Let $[K : F] = n$ and let $a \in K$ such that there exist automorphisms $\sigma_1, \dots, \sigma_n \in \operatorname{Aut}(K/F)$ with $\sigma_i(a) \neq \sigma_j(a)$ whenever $i \neq j$. Show $K = F(a)$.

Solution. Since K/F is finite, it is algebraic. So the minimal polynomial $m_a(x) \in F[x]$ for a exists. Write $m_a(x) = x^k + \lambda_{k-1}x^{k-1} + \ldots + \lambda_0$ where $\lambda_i \in F$. Then we have

$$\begin{aligned} m_a(\sigma_i(a)) &= \sigma_i(a)^k + \lambda_{k-1}\sigma_i(a)^{k-1} + \ldots + \lambda_0 \\ &= \sigma_i(a^k + \lambda_{k-1}a^{k-1} + \ldots + \lambda_0) \\ &= \sigma_i(0) \\ &= 0. \end{aligned}$$

Thus each $\sigma_i(a)$ is also a root of $m_a(x)$, so $k = \deg(m_a(x)) \geq n$. This means $[F(a) : F] \geq n$, so

$$n = [K : F] = [K : F(a)][F(a) : F] \geq [K : F(a)]n,$$

hence $[K : F(a)] = 1$. This happens precisely when $K = F(a)$, as desired. ■

(8) Consider the field extension $\mathbb{F}_{5^4}/\mathbb{F}_5$.
a) Determine the number of elements $a \in \mathbb{F}_{5^4}$ such that $\mathbb{F}_{5^4} = \mathbb{F}_5(a)$.
b) Determine the number of irreducible polynomials of degree 4 in $\mathbb{F}_5[x]$.

Solution for a. Any $a \in \mathbb{F}_{5^4}$ will satisfy $\mathbb{F}_{5^4} = \mathbb{F}_5(a)$ if and only if a does not lie in a proper subfield. This is because if a did lie in some proper subfield, the most it could generate is that proper subfield. Since $\mathbb{F}_{5^2}$ is the largest proper subfield, there are $5^4 - 5^2 = 625 - 25 = 600$ such values of a. ■

Solution for b. Each irreducible polynomial over $\mathbb{F}_5$ of degree 4 will have 4 distinct roots out of the 600 we found in part (a). This is because adjoining a root of an irreducible polynomial of degree 4 generates a degree 4 extension, namely $\mathbb{F}_{5^4}$. So we can group the 600 elements from part (a) into 150 groups of 4, where the elements of each group have the same minimal polynomial. Thus there are 150 minimal polynomials of degree 4 in $\mathbb{F}_5[x]$, and since there are 4 choices for the leading coefficient, there are 600 total irreducible polynomials of degree 4 in $\mathbb{F}_5[x]$. ■

(9) Denote by Z_n the cyclic group of order n.
a) Find a field extension $K/\mathbb{Q}$ such that $\operatorname{Gal}(K/\mathbb{Q}) \cong Z_5$.
b) Let $L = K(\sqrt{2})$. Argue that $L/\mathbb{Q}$ is Galois and determine the cardinality of $\operatorname{Gal}(L/\mathbb{Q})$.
c) Give the isomorphism type of the Galois group $\operatorname{Gal}(L/\mathbb{Q})$ and describe the automorphisms explicitly.

Solution for a. Let ζ_{11} be a primitive 11^{th} root of unity. Then $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ is a Galois extension of degree $\varphi(11) = 10$, and has Galois group $\operatorname{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}) \cong Z_{10}$. Since Z_{10} is abelian, every subgroup is normal. Thus Z_2 is a normal subgroup of Z_{10} corresponding to a Galois extension $K/\mathbb{Q}$ with $\operatorname{Gal}(K/\mathbb{Q}) \cong Z_{10}/Z_2 \cong Z_5$. ■

Solution for b. Since K is Galois over $\mathbb{Q}$, we know K is the splitting field of a separable polynomial $f(x) \in \mathbb{Q}[x]$. Since $[K : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we must have $[K \cap \mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 1$. Therefore $\sqrt{2} \notin K$. Thus $K(\sqrt{2})$ is the splitting field of the separable polynomial $f(x)(x^2 - 2) \in \mathbb{Q}[x]$, hence is Galois over $\mathbb{Q}$. Finally, $[L : \mathbb{Q}] = 5 \cdot 2 = 10$, so $|\operatorname{Gal}(L/\mathbb{Q})| = 10$. ■

Solution for c. Let $G = \mathrm{Gal}(L/\mathbb{Q})$. Since $K(\sqrt{2})$ is the compositum of the abelian extensions K and $\mathbb{Q}(\sqrt{2})$, $K(\sqrt{2})$ is also an abelian extension. This forces $G \cong Z_{10}$, since Z_{10} is the only abelian group of order 10. ■