JUNE 2018 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 16, 2020.

(1) Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be a linear transformation. Assume that $T^2 = T$. Prove the following statements.

a) $\operatorname{im}(T) \cap \ker(T) = (0)$.
b) $V = \operatorname{im}(T) \bigoplus \ker(T)$.
c) There exists a basis β of V such that the matrix of T with respect to β is a diagonal matrix where each diagonal entry lies in $\{0, 1\}$.

Solution for a. Let $x \in \operatorname{im}(T) \cap \ker(T)$. So $T(x) = 0$ and $x = T(y)$ for some $y \in V$. We have $x = T(y) = T^2(y) = T(x) = 0$, so $\operatorname{im}(T) \cap \ker(T) = (0)$. ■

Solution for b. By part (a), it suffices to show $V = \operatorname{im}(T) + \ker(T)$. Inclusion in one direction is obvious. For the other direction, let $v \in V$. So $T(v) = w$ for some $w \in V$. By the Fiber Lemma, $T^{-1}(w) = v + \ker(T)$. Since $T^2 = T$, we have $w = T(v) = T^2(v) = T(w)$, so $w \in T^{-1}(w)$. Therefore $w = v + x$ for some $x \in \ker(T)$. So $v = w - x = T(w) + (-x) \in \operatorname{im}(T) + \ker(T)$. Hence $V = \operatorname{im}(T) \bigoplus \ker(T)$. ■

Solution for c. Let $A = \{a_1, \dots, a_n\}$ be a basis for $\operatorname{im}(T)$, and let $B = \{b_1, \dots, b_m\}$ be a basis for $\ker(T)$. Then by parts (a) and (b), $\beta = A \cup B = \{a_1, \dots, a_n, b_1, \dots, b_m\}$ forms a basis for V. Then each $T(a_i) = a_i$ (since $a_i \in \operatorname{im}(T)$), and each $T(b_i) = 0$ (since $b_i \in \ker(T)$). So the matrix of T w.r.t. β will be a diagonal matrix with each diagonal entry lying in $\{0, 1\}$. ■

(2) Let $V \subset \mathbb{R}[x]$ be a vector space of dimension k. We say that a polynomial f vanishes to order n at $a \in \mathbb{R}$ if $f(a) = 0$ and n is the smallest positive integer such that $f^{(n)}(a) \neq 0$.

a) Show that $V_n = \{f \in V \mid f \text{ vanishes to order} \geq n \text{ at } a\}$ is a subspace of V.
b) Let $a \in \mathbb{R}$. Show that $\dim(V_n) - \dim(V_{n+1})$ is either 0 or 1.
c) Conclude that there are precisely k integers n such that there exists a nonzero $f \in V$ that vanishes to order n at a.

Solution for a. Let $a \in \mathbb{R}$. Clearly $(x - a)^n$ vanishes to order n at a, so $V_n \neq \varnothing$. Now let $f, g \in V_n$, and let $\lambda, \mu \in \mathbb{R}$. So $f(a) = 0$ and $i \geq n$ is minimal such that $f^{(i)}(a) \neq 0$. Similarly, $g(a) = 0$ and $j \geq n$ is minimal such that $g^{(j)}(a) \neq 0$. Without loss of generality, assume $i \leq j$. Now $\lambda f(a) + \mu g(a) = 0$, and we have

$$\frac{d^i}{dx^i}(\lambda f + \mu g)(a) = \lambda f^{(i)}(a) + \mu g^{(i)}(a) = \lambda f^{(i)}(a) \neq 0.$$

Clearly i is minimal, so $\lambda f + \mu g \in V_n$. Hence V_n is a subspace of V. ■

Solution for b. Let $\varphi : V_n \to \mathbb{R}$ be the linear functional defined by $\varphi(f) = f^{(n)}(a)$. Note that

$$V_n = \{f \in V \mid f(a) = f'(a) = \cdots = f^{(n-1)}(a) = 0\}.$$

Also, we have

$$\ker\varphi = \{f \in V_n \mid f^{(n)}(a) = 0\} = \{f \in V \mid f(a) = f'(a) = \cdots = f^{(n)}(a) = 0\} = V_{n+1}.$$

By Rank-Nullity,

$$\dim \operatorname{im}\varphi + \dim V_{n+1} = \dim V_n.$$

Since $\operatorname{im}\varphi \subset \mathbb{R}$, either $\dim\operatorname{im}\varphi = 1$ or $\dim\operatorname{im}\varphi = 0$. If $\dim\operatorname{im}\varphi = 0$, then $\dim V_n - \dim V_{n+1} = 0$. On the other hand, if $\dim\operatorname{im}\varphi = 1$, then $\dim V_n - \dim V_{n+1} = 1$. ■

Solution for c. Let $M \geq k - 1$ be the highest degree of any polynomial in V. We can do this because V is finite dimensional. Note $V = V_0$, and consider the sequence of subspaces

$$V = V_0 \supset V_1 \supset V_2 \supset \cdots \supset V_{M+1}.$$

Since M was chosen to be maximal, the highest possible vanishing order of any nonzero element in V is M. Thus $V_{M+1} = \{0\}$. Taking dimensions, we have

$$k = \dim V \geq \dim V_1 \geq \dim V_2 \geq \cdots \geq 0.$$

By part (b), any strict inequality above drops the dimension by 1. So we must have exactly k nonnegative distinct integers $0 \leq n_1, \ldots, n_k \leq M$ such that $\dim V_{n_i+1} + 1 = \dim V_{n_i}$. Finally, suppose $0 \neq f \in V$ vanishes to order n. Then $f \in V_n \backslash V_{n+1}$, and since $V_{n+1} \subset V_n$, this implies $\dim V_n > \dim V_{n+1}$. By our work above, this happens for precisely k such n. ■

(3) See my *Jan 2017 Algebra Prelim Solutions* for how to do this. It's a repeat problem. ■

(4) Let G be a finite group that acts transitively on a set X with $|X| > 1$. Show that G contains at least one element with no fixed points.

Solution. Define $X/G = \{\mathrm{Orb}(x) \mid x \in X\}$. Since G acts transitively on $|X|$, we have $|X/G| = 1$. By Burnside's Lemma,

$$|G| = |X/G||G| = \sum_{g \in G} |X^g| \tag{1}$$

where X^g is the set of points in X fixed by g. Since e fixes all of X, $|X^e| = |X| \geq 2$. Now assume for sake of contradiction that $|X^g| \geq 1$ for each $e \neq g \in G$. Then equation (1) says $|G| > |G|$ which is absurd. Hence there must be at least one element of G with no fixed points. ■

(5) Let G be a finite group with identity element e, and let H, K be cyclic, normal subgroups of G such that $H \cap K = \{e\}$ and $|G| = |H||K|$. Prove the following statements.

a) $hk = kh$ for all $h \in H$ and $k \in K$.
b) If $|H|$ and $|K|$ are relatively prime, then G is cyclic.

Solution for a. Let $h \in H$ and $k \in K$. Since $h^{-1} \in H$, we have $h(kh^{-1}k^{-1}) \in H$ by normality. Similarly, $(hkh^{-1})k^{-1} \in K$. Thus $hkh^{-1}k^{-1} \in H \cap K$, so $hkh^{-1}k^{-1} = e$. Hence $hk = kh$. ■

Solution for b. Let h and k be generators for H and K respectively. Let $|H| = m$ and $|K| = n$. We will show $\mathrm{ord}(hk) = mn$. By part (a), we have

$$(hk)^{mn} = h^{mn}k^{mn} = e.$$

Now suppose $(hk)^r = e$ for some arbitrary $r \in \mathbb{N}$. Then

$$e = (hk)^{rm} = h^{rm}k^{rm} = k^{rm}.$$

So $n \mid rm$ and hence $n \mid r$ (since $(m,n) = 1$). Similarly $m \mid r$, and since $(m,n) = 1$, we have $mn \mid r$. Therefore

$$\operatorname{ord}(hk) = mn = |H||K| = |G|,$$

so G is cyclic. ∎

(6) Let R be a commutative ring with 1. Let I and J be two ideals in R. Use the First Isomorphism Theorem (FIT) to prove the following statements.

a) $(I + J)/J \cong I/(I \cap J)$.
b) If $I \subset J$ then $(R/I)/(J/I) \cong R/J$.

Solution for a. Define the map

$$\begin{aligned} \gamma : I &\longrightarrow (I + J)/J \\ x &\longmapsto x + J. \end{aligned}$$

Let $a, b \in I$. Then

$$\gamma(a + b) = (a + b) + J = (a + J) + (b + J) = \gamma(a) + \gamma(b).$$

Furthermore,

$$\gamma(ab) = ab + J = (a + J)(b + J) = \gamma(a)\gamma(b).$$

Now let $(i + j) + J \in (I + J)/J$. Then

$$(i + j) + J = (i + J) + (j + J) = i + J + 0 + J = i + j,$$

so γ is surjective. Let $z \in \ker\gamma$. Then $z \in I$ and $z + J = J$, so $z \in J$. Hence $z \in I \cap J$. I $z \in I \cap J$, then $z + J = J$, so $z \in \ker\gamma$. Hence $\ker\gamma = I \cap J$, so we're done by the FIT. ∎

Solution for b. Define the map

$$\begin{aligned} \eta : R/I &\longrightarrow R/J \\ r + I &\longmapsto r + J. \end{aligned}$$

Let $a + I, b + I \in R/I$. Then

$$\begin{aligned} \eta(a + I + b + I) &= \eta((a + b) + I) \\ &= (a + b) + J \\ &= a + J + b + J \\ &= \eta(a + I) + \eta(b + I). \end{aligned}$$

Furthermore,

$$\begin{aligned} \eta((a + I)(b + I)) &= \eta(ab + I) \\ &= ab + J \\ &= (a + J)(b + J) \\ &= \eta(a + I)\eta(b + I). \end{aligned}$$

Clearly η is surjective. Now let $z + I \in \ker\eta$. Then $\eta(z) = z + J = J$, so $z \in J$, hence $z + I \in J/I$. On the other hand, if $z + I \in J/I$, then $\eta(z) = z + J = J$, so $z + I \in \ker\eta$. Hence $\ker\eta = J/I$, so we're done by the FIT. ∎

(7) Let R be a commutative ring with 1. Prove that $R[x]$ is a PID if and only if R is a field.

Solution. For the forward direction, assume $R[x]$ is a PID. Note that the ideal $(x) \subset R[x]$ is prime, since if the product of two polynomials in $R[x]$ is divisible by x, at least one of the factors must also be divisible by x. Since $R[x]$ is a PID, (x) is a maximal ideal. Then the quotient $R[x]/(x) \cong R$ is a field. For the reverse direction, assume R is a field, and let $I \subset R[x]$ be a nonzero ideal. Pick a nonzero polynomial $g \in I$ with minimal degree. Let $f \in I$ be any polynomial, and use the Division Algorithm (we can do this since we are over a field) to write

$$f = gq + r$$

for some $q, r \in R[x]$ with either $r = 0$ or $\deg r < \deg g$. Note that $r = f - gq$, so $r \in I$. Since $\deg r < \deg g$ contradicts the minimality of g, we must have $r = 0$. Thus $f = gq$, so $I = (g)$. ■

(8) Let $p \neq 2, 3$ be a prime. Prove that the splitting field of $x^{12} - 1$ over $\mathbb{F}_p$ is of degree 1 or 2. Give a rule to determine when the degree is 1 or 2.

Solution. Let L be the splitting field of $f(x) = x^{12} - 1$ over $\mathbb{F}_p$, and let $k = [L : \mathbb{F}_p]$. So $|L| = p^k$, thus $|L^\times| = p^k - 1$. The roots of $f(x)$ form a cyclic group of order 12, and since L is a finite field, $L^\times$ is a cyclic group. So $L^\times$ contains the group of roots of $f(x)$ if and only if $12 \mid p^k - 1$. Since L is the splitting field of $f(x)$, k is the smallest integer such that $12 \mid p^k - 1$. To find k, note that if $12 \mid p - 1$, then $k = 1$. Otherwise, observe $p^2 - 1 = (p-1)(p+1)$. Since p is odd, each factor is even, so the product is divisible by 4. One of $p-1, p, p+1$ must be divisible by 3, but since $p \neq 3$ is prime, it must be one of $p-1$ or $p+1$. Thus $12 \mid p^2 - 1$, so $k = 2$ as desired. The "rule" here is that $k = 1$ if p is one more than a multiple of 12, and $k = 2$ otherwise. ■

(9) Let $K \in \mathbb{C}$ be the splitting field of $x^{28} - 1$ over $\mathbb{Q}$.

a) Find the Galois group of K over $\mathbb{Q}$.
b) Find the lattice of all subfields of K.

Solution for a. The Galois group of $x^{28} - 1$ over $\mathbb{Q}$ is $\mathbb{Z}/28\mathbb{Z}^\times$. By the Chinese Remainder Theorem,

$$\mathbb{Z}/28\mathbb{Z}^\times \cong (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})^\times \cong C_2 \times C_6.$$

So the Galois group of $x^{28} - 1$ is actually $C_2 \times C_6$. ■

Solution for b. By part (a), the hint, and the Fundamental Theorem of Galois Theory, it suffices to find the lattice of subgroups for $C_2 \times C_6$ (then you can just re-label it to get the subfields). First of all, let's figure out the subgroups of $C_2 \times C_6$. Denote $C_2 = \{e, g\}$ and $C_6 = \{e, h, \ldots, h^5\}$. Then the 10 subgroups are

$$\begin{aligned}
\{(e,e)\}&,\\
\{(e,e),(g,e)\}, \quad \{(e,e),(e,h^3)\}, \quad \{(e,e),(g,h^3)\}&,\\
\{(e,e),(e,h^2),(e,h^4)\}, \quad \{(e,e),(e,h^3),(g,e),(g,h^3)\}&,\\
\{(e,e),(e,h),(e,h^2),(e,h^3),(e,h^4),(e,h^5)\}&,\\
\{(e,e),(e,h^2),(e,h^4),(g,e),(g,h^2),(g,h^4)\}&,\\
\{(e,e),(g,h^5),(e,h^4),(g,h^3),(e,h^2),(g,h)\}&,\\
C_2 \times C_6&.
\end{aligned}$$

Drawing the diagram, we have

$$\begin{tikzcd}[column sep=small]
 & & & 1 \arrow[dlll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drrr, dash] & & & \\
C_2 \arrow[d, dash] \arrow[drr, dash] & & C_2 \arrow[d, dash] \arrow[drr, dash] & & C_3 \arrow[dllll, dash] \arrow[d, dash] \arrow[drr, dash] & & C_2 \arrow[dllll, dash] \arrow[d, dash] \\
C_6 \arrow[drrr, dash] & & C_2^2 \arrow[dr, dash] & & C_6 \arrow[dl, dash] & & C_6 \arrow[dlll, dash] \\
 & & & C_2 \times C_6 & & &
\end{tikzcd}$$

I'll leave it as a simple exercise to the reader to fill in the corresponding group indexes, and therefore the subfield degrees (I'm not that good at TikZ yet). ■