JUNE 2019 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: March 28, 2020.

(1) Let $\mathbb{F}_3$ be the field of order 3. Consider the matrix

$$M = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{F}_3^{3\times 3}.$$

Show that

$$\mathbb{F}_3[M] := \Big\{ \sum_{i=0}^{n} a_i M^i \;\Big|\; n \in \mathbb{N}_0, a_i \in \mathbb{F}_3 \Big\}$$

is a field of order 27.

Solution. One calculates that the characteristic polynomial of M is $p(x) = x^3 - x - 2$. Since $p(x)$ is degree 3, $p(x)$ is irreducible over $\mathbb{F}_3$ if and only if $p(x)$ has no roots in $\mathbb{F}_3$. Plugging in every element of $\mathbb{F}_3$ into $p(x)$ shows that $p(x)$ is irreducible over $\mathbb{F}_3$. Hence $(p(x))$ is a prime ideal in $\mathbb{F}_3[x]$, but since $\mathbb{F}_3[x]$ is a PID, $(p(x))$ must be a maximal ideal. Thus the quotient $\mathbb{F}_3[x]/(p(x))$ is a field. We have the isomorphism

$$\mathbb{F}_3[M] \cong \mathbb{F}_3[x] \big/ (p(x))$$

so that $\mathbb{F}_3[M]$ is a field as well. Cayley-Hamilton says that $p(M) = M^3 - 2M - 2I = 0$, thus $M^3 = 2M + 2I$. This means the elements of $\mathbb{F}_3[M]$ are of the form

$$xI + yM + zM^2$$

for $x, y, z \in \mathbb{F}_3$. So I, M, M^2 generate $\mathbb{F}_3[M]$, and since there are 3 choices for any of x, y or z, there are $3^3 = 27$ total elements. So $\mathbb{F}_3[M]$ is a field of order 27. ∎

(2) Let A be an integral domain which contains a field $K \subset A$ and suppose that A is finite dimensional as a vector space over K. Show that A is a field extension of K.

Solution. Let $0 \neq a \in A$. It suffices to show a has an inverse in A. Note that the map

$$\begin{aligned} f : A &\longrightarrow A \\ x &\longmapsto ax \end{aligned}$$

is clearly K-linear, and is injective since if $ax_1 = ax_2$, then $x_1 = x_2$ by cancellation (A is an integral domain). Because f is an injective linear map over a finite dimensional vector space, f is also surjective. This means $f(b) = 1$ for some $b \in A$. So $ab = 1$, thus a has an inverse in A. This shows that A is a field, so it's a field extension of K. ∎

(3) Let G be a group and let $[G, G]$ be the subgroup of G generated by the set $\{hgh^{-1}g^{-1} | h, g \in G\}$.

a) Let A be an abelian group. Show that if $\varphi : G \to A$ is a group homomorphism, then $[G, G] \subset \ker \varphi$.
b) Show that if H is a subgroup of G containing $[G, G]$, then H is normal in G and G/H is an abelian group.

Solution for a. Let $x \in [G, G]$. Then

$$x = \prod_{i=1}^{n} x_i$$

where each $x_i \in \{hgh^{-1}g^{-1} | h, g \in G\}$. We have

$$\varphi(x) = \prod_{i=1}^{n} \varphi(x_i) = \prod_{i=1}^{n} \varphi(h_i g_i h_i^{-1} g_i^{-1}) = \prod_{i=1}^{n} \varphi(h_i)\varphi(h_i)^{-1}\varphi(g_i)\varphi(g_i)^{-1} = 1.$$

Thus $[G, G] \subset \ker \varphi$. ■

Solution for b. Let $g \in G$ and $x \in H$. Then

$$gxg^{-1} = gxg^{-1}x^{-1}x \in H$$

since $x \in H$ and $gxg^{-1}x^{-1} \in [G, G] \subset H$. So H is normal in G, therefore G/H is a group. Now let $aH, bH \in G/H$. We have

$$aH \cdot bH = abH = baa^{-1}b^{-1}abH = baH = bH \cdot aH.$$

The second to last equality holds since $a^{-1}b^{-1}ab \in [G, G] \subset H$. Thus G/H is abelian. ■

(4) Let p be a prime and let G be a finite group with $\mathrm{Aut}(G) \cong \mathbb{Z}/p\mathbb{Z}$.

a) Show that $\mathrm{Aut}(G)$ contains a subgroup isomorphic to $G/Z(G)$.
b) Use (a) to show that G is abelian.
c) Use (b) to show that $p = 2$.

Solution for a. Define

$$\mathrm{Inn}(G) = \{\sigma \in \mathrm{Aut}(G) \mid \sigma(x) = gxg^{-1} \text{ for all } x \in G \text{ and some fixed } g \in G\}.$$

Clearly $\mathrm{Inn}(G) \neq \varnothing$ since $\mathrm{id} \in \mathrm{Inn}(G)$. Now let $\sigma, \tau \in \mathrm{Inn}(G)$. So there exists $g_1, g_2 \in G$ such that $\sigma(x) = g_1 x g_1^{-1}$ and $\tau(x) = g_2 x g_2^{-1}$. Then τ^{-1} is given by $\tau^{-1}(x) = g_2^{-1} x g_2$. For $x \in G$, we have

$$(\sigma\tau^{-1})(x) = \sigma(\tau^{-1}(x)) = g_1 g_2^{-1} x g_2 g_1^{-1}.$$

Since $(g_1 g_2^{-1})^{-1} = g_2 g_1^{-1}$, we see that $\sigma\tau^{-1} \in \mathrm{Inn}(G)$. Hence $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Define the map

$$\begin{aligned} \Psi : G &\longrightarrow \mathrm{Inn}(G) \\ g &\longmapsto (x \mapsto gxg^{-1}). \end{aligned}$$

Let $a, b \in G$. Then

$$\Psi(ab) = x \mapsto abx(ab)^{-1} = x \mapsto abxb^{-1}a^{-1} = (x \mapsto axa^{-1}) \circ (x \mapsto bxb^{-1}) = \Psi(a)\Psi(b),$$

showing that Ψ is a group homomorphism. Also, Ψ is surjective since given any $\sigma = (x \mapsto gxg^{-1}) \in \mathrm{Inn}(G)$, we have $\Psi(g) = \sigma$. Finally, $z \in \ker \Psi$ if and only if $\Psi(z) = (x \mapsto zxz^{-1}) = \mathrm{id}$, if and only if $zx = xz$ for all $x \in G$, if and only if $z \in Z(G)$. Thus $\ker \Psi = Z(G)$, so $G/Z(G) \cong \mathrm{Inn}(G)$ by the First Isomorphism Theorem. ■

Solution for b. By part (a), $\mathrm{Aut}(G) \cong \mathbb{Z}/p\mathbb{Z}$ always contains a subgroup isomorphic to $G/Z(G)$. But there are no non-trivial subgroups of $\mathbb{Z}/p\mathbb{Z}$, so either $G/Z(G)$ is trivial or $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$. If $G/Z(G)$ is trivial, then $Z(G) = G$, so G is abelian. If $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z}$, then $G/Z(G)$ is cyclic, so G is abelian. In both cases, the claim has been proven. ∎

Solution for c. Define the map

$$\begin{aligned} f : G &\longrightarrow G \\ x &\longmapsto x^{-1}. \end{aligned}$$

Let $a, b \in G$. Because G is abelian by part (b), we have

$$f(ab) = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1} = f(a)f(b).$$

Therefore f is a group homomorphism. Furthermore, $x \in \ker f$ if and only if $x^{-1} = 1$ if and only if $x = 1$. Thus $\ker f$ is trivial, so f is injective. Because G is finite, f is also surjective, so f is an automorphism. Clearly $f^2 = \mathrm{id}$, so f generates a subgroup of order 2 in $\mathrm{Aut}(G)$. However, this is only possible if $p = 2$. ∎

(5) Show that the following polynomials are irreducible in the given ring.

a) $f = x^3 + (y^2 - 1)x^2 + 3(y^2 - y)x - 4y + 4 \in \mathbb{Q}[x, y]$.
b) $g = y^3 + xy + x^2(x - 1)^2 \in \mathbb{R}[x, y]$.
c) $h = 5x^4 + 4x^3 - 2x^2 - 3x + 21 \in \mathbb{Q}[x]$.

Solution for a. Note that we can view f as a polynomial in $\mathbb{Q}[y][x]$. Because $\mathbb{Q}$ is an integral domain, so is $\mathbb{Q}[y]$. Thus we can consider quotients of $\mathbb{Q}[y]$ by proper ideals. Here, we choose the ideal (y), so our new polynomial becomes

$$\overline{f} = x^3 - x^2 + 4 \in \mathbb{Q}[x].$$

Since $\overline{f}$ is a monic polynomial with integer coefficients over the rationals, any root must divide 4. Plugging in $\pm 1, \pm 2, \pm 4$ we see that $\overline{f}$ is irreducible over $\mathbb{Q}[x]$, so f is irreducible over $\mathbb{Q}[x, y]$. (For the relevant literature, we are using Prop. 11 and 12 in Dummit and Foote, pages 308-309). ∎

Solution for b. Suppose g could be properly factored as

$$g(x, y) = a(x, y)b(x, y).$$

Since g is of degree 3 in y, we must have

$$a(x, y) = p(x)y + q(x) \quad \text{and} \quad b(x, y) = r(x)y^2 + s(x)y + t(x)$$

where $p(x), q(x), r(x), s(x), t(x) \in \mathbb{R}[x]$ are of degree at most 4. Looking at the first term of the product $a(x, y)b(x, y)$ we see that

$$g(x, y) = p(x)r(x)y^3 + (\text{other terms}).$$

Equating coefficients with the original definition of g, we have $p(x)r(x) = 1$, so $p(x)$ and $r(x)$ are constant polynomials who are inverses of each other. This means we can divide $a(x, y)$ by $p(x)$ and multiply $b(x, y)$ by $p(x)$ to obtain another factorization of g where each factor is monic with respect to y. Thus we may assume without loss of generality that $p(x) = r(x) = 1$. Using this, we expand to obtain

$$\begin{aligned} g(x, y) &= p(x)r(x)y^3 + (p(x)s(x) + q(x)r(x))y^2 + (p(x)t(x) + q(x)s(x))y + q(x)t(x) \\ &= y^3 + (s(x) + q(x))y^2 + (t(x) + q(x)s(x))y + q(x)t(x). \end{aligned}$$

Equating coefficients again, we get $s(x) = -q(x)$, $t(x) = -q(x)s(x)+x$, and $q(x)t(x) = x^2(x-1)^2$. Therefore $t(x) = q(x)^2 + x$, so $q(x)(q(x)^2 + x) = x^2(x-1)^2$. This is a contradiction since the LHS has degree divisible by 3, and the RHS has degree 4. Hence g is irreducible. ■

Solution for c. We first show h is irreducible over $\mathbb{Z}$, then Gauss' Lemma will tell us it is irreducible over $\mathbb{Q}$. Since $\mathbb{Z}$ is an integral domain, we again use Proposition 12 from Dummit and Foote page 309, and look at the reduction of h modulo the proper ideal (2):

$$\overline{h} = x^4 - x + 1 \in \mathbb{Z}/2\mathbb{Z}[x].$$

Plugging in the elements of $\mathbb{Z}/2\mathbb{Z}$ into $\overline{h}$, we see that $\overline{h}$ does not have a linear factor. So assume $\overline{h} = (ax^2+bx+c)(dx^2+ex+f) \in \mathbb{Z}/2\mathbb{Z}[x]$. Equating coefficients, we see right away that $a = c = d = f = 1$. Hence we are really looking at $\overline{h} = (x^2+px+1)(x^2+qx+1) = x^4+(p+q)x^3+pqx^2+(p+q)x+1$. Equating coefficients again, we must have $p + q = 0$ and $p + q = -1$ which is impossible. Thus $\overline{h}$ is irreducible, so h is irreducible over $\mathbb{Z}$ (Prop. 12). By Gauss' Lemma, h is irreducible over $\mathbb{Q}$. ■

(6) Consider the ring

$$R := \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}.$$

a) Determine the field of fractions, Q, of R inside $\mathbb{C}$.
b) Show that $f = x^2 + 1$ is reducible in $Q[x]$, but irreducible in $R[x]$.
c) Argue that R is not a UFD.

Solution for a. Define

$$\mathbb{Q}[2i] := \Big\{\frac{m}{n} + 2\frac{p}{q}i \;\Big|\; \frac{m}{n}, \frac{p}{q} \in \mathbb{Q}\Big\}.$$

We show the field of fractions $Q = \mathbb{Q}[2i]$. Let $\frac{a+2bi}{c+2di} \in Q$. Then we may write

$$\frac{a+2bi}{c+2di} = \frac{ac - 2adi + 2bci + 4bd}{c^2 + 4d^2} = \frac{ac + 4bd}{c^2 + 4d^2} + \frac{2bc - 2ad}{c^2 + 4d^2}i \in \mathbb{Q}[2i].$$

Conversely, let $\frac{m}{n} + 2\frac{p}{q}i \in \mathbb{Q}[2i]$. Then we have

$$\frac{m}{n} + 2\frac{p}{q}i = \frac{mq + 2pni}{nq} \in Q,$$

since both $mq + 2pni$ and nq are elements of $\mathbb{Z}[2i]$. Thus $Q = \mathbb{Q}[2i]$. ■

Solution for b. Since f is degree 2, we need only check that f has a root in Q but not in R. Observe (using the fact that the roots of $x^2 + 1$ are $\pm i$),

$$i = \frac{0 + 2(1)i}{2 + 2(0)i} \in Q,$$

so f is reducible in $Q[x]$. Now suppose $i = a + 2bi$ for some $a, b \in \mathbb{Z}$. We have

$$-1 = i^2 = a^2 + 4bi - 4b^2$$

which is a contradiction since the LHS is real but the RHS is complex. Thus $i \notin \mathbb{Z}[2i]$. A similar argument shows $-i \notin \mathbb{Z}[2i]$. Hence f is irreducible in $R[x]$. ■

Solution for c. We have the non-unique factorization of 8:

$$(2 + 2i)(2 - 2i) = 8 = 4 \cdot 2.$$

Hence R is not a UFD. ■

(7) Let K/F be a finite, normal field extension and L/K be any field extension. Furthermore, let $\varphi : K \longrightarrow L$ be an F-homomorphism. Show that $\varphi(K) \subset K$.

Solution. Since K/F is normal, it is the splitting field of some polynomial $f(x) \in F[x]$. Denote by $\alpha_1, \ldots, \alpha_n$ the roots of $f(x)$. Since K/F is finite we may write $K = F(\alpha_1, \ldots, \alpha_n)$. Now let

$$v = \sum_{i_1,\ldots,i_n} \lambda_{i_1\ldots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \in K$$

where each $\lambda_{i_1\ldots i_n} \in F$. We have

$$\begin{aligned} \varphi(v) &= \sum_{i_1,\ldots,i_n} \varphi(\lambda_{i_1\ldots i_n})\varphi(\alpha_1^{i_1} \cdots \alpha_n^{i_n}) \\ &= \sum_{i_1,\ldots,i_n} \lambda_{i_1\ldots i_n}\varphi(\alpha_1)^{i_1} \cdots \varphi(\alpha_n)^{i_n} \in K. \end{aligned}$$

This is because φ is an F-homomorphism, so it fixes F pointwise and permutes the roots of $f(x)$. Hence $\varphi(K) \subseteq K$. ∎

(8) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

a) Show that $K/\mathbb{Q}$ is Galois and that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
b) Show that $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
c) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$.

Solution for a. Observe that the polynomial $p(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ is separable and has roots $\pm\sqrt{2}, \pm\sqrt{3}$. So $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $p(x)$, hence it is Galois (splitting fields of separable polynomials are Galois). Note that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

so $|\mathrm{Gal}(K/\mathbb{Q})| = 4$. Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is completely determined by its action on the generators $\sqrt{2}$ and $\sqrt{3}$, and we know σ must permute the roots of polynomials. Define the following automorphisms:

$$\sigma_1 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Then we may compute the product:

$$\sigma_1\sigma_2 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Since $\{\mathrm{id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$ are 4 distinct automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$, we know we have accounted for *all* elements in $\mathrm{Gal}(K/\mathbb{Q})$. Finally, any group of order 4 must either be isomorphic to the cyclic group C_4 or the Klein 4-group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since every non-identity element of $\mathrm{Gal}(K/\mathbb{Q})$ is of order 2, it must be the case that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ∎

Solution for b. Since $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, we have $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. For the other inclusion, we have

$$\sqrt{2} = \frac{1}{2}\Big[(\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3})\Big] \in \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$

and similarly

$$\sqrt{3} = \frac{-1}{2}\Big[(\sqrt{2}+\sqrt{3})^3 - 11(\sqrt{2}+\sqrt{3})\Big] \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Hence $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. ■

Solution for c. Let $\alpha = \sqrt{2}+\sqrt{3}$. Then $\alpha^2 = 5+2\sqrt{6}$, so $\alpha^2 - 5 = 2\sqrt{6}$. Squaring both sides again, we get $\alpha^4 - 10\alpha^2 + 25 = 24$, so $\alpha^4 - 10\alpha^2 + 1 = 0$. Thus α is a root of the monic polynomial $m(x) = x^4 - 10x^2 + 1$. Via the Rational Roots Theorem, $m(x)$ has no roots in $\mathbb{Q}$, so $m(x)$ has no linear factors over $\mathbb{Q}$. Since $m(x) = m(-x)$, we may assume $m(x) = (x^2+ax+b)(x^2-ax+b)$. Expanding, we have

$$m(x) = x^4 + (2b-a^2)x^2 + b^2.$$

Equating coefficients, $b^2 = 1$ and $a^2 - 2b = 10$, so $a^2 = 10 + 2(\pm 1)$. This is a contradiction since neither 12 nor 8 are rational squares. Hence $m(x)$ is irreducible, so it is the minimal polynomial for $\sqrt{2}+\sqrt{3}$. ■

(9) Let K be a field of characteristic $p > 0$, let $a \in K$ and let β be a root of the polynomial $f(x) = x^p - x - a$.

a) Show that $\beta + 1$ is also a root of $f(x)$. Conclude that $K(\beta)$ is a Galois extension of K.
b) Determine the Galois group of this extension. Give explicitly all its elements and give its isomorphism type.

Solution for a. Suppose $f(\beta) = \beta^p - \beta - a = 0$. Then we have

$$f(\beta+1) = (\beta+1)^p - (\beta+1) - a = \beta^p + 1^p - \beta - 1 - a = \beta^p - \beta - a = 0,$$

so $\beta+1$ is also a root of $f(x)$. Hence the p roots of $f(x)$ are of the form $\beta + r$ where $0 \le r < p$. Clearly each root is distinct. We have thus shown that $K(\beta)$ is the splitting field for the separable polynomial $f(x)$, hence it is a Galois extension of K (splitting fields of separable polynomials are Galois). ■

Solution for b. We know from (a) that $K(\beta)$ is a degree p extension of K, so $|\mathrm{Gal}(K(\beta)/K)| = p$. Any automorphism $\sigma \in \mathrm{Gal}(K(\beta)/K)$ is completely determined by its action on the generator β, and σ must permute the roots of $f(x)$. Define the automorphism

$$\sigma : \beta \longmapsto \beta + 1.$$

Computing powers of σ we see that σ generates p elements in $\mathrm{Gal}(K(\beta)/K)$. Since the size of the Galois group is p, we have accounted for *all* elements of $\mathrm{Gal}(K(\beta)/K)$. Finally, there is only one group of prime order up to isomorphism, so we conclude that $\mathrm{Gal}(K(\beta)/K) \cong C_p$, the cyclic group on p elements. ■