MOCK QUALIFYING EXAMINATION, ALGEBRA, PART A, 2019

September n^3, 2019

Solve any four questions; indicate which ones are supposed to be graded. You must show all work and justify all statements either by referring to an appropriate theorem or by providing a full solution.

1. Let $G = \mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}$ and $\mathbb{Z}$ are considered as additive groups. Prove that for any positive integer n, G has a unique subgroup $G(n)$ of order n, and that $G(n)$ is cyclic.

A subgroup $G(n) < \mathbf{Q}/\mathbf{Z}$ of order n is finite, and so it must be finitely generated by $\{\overline{r_i}\}_{i\in\{1\ldots k\}}$ for some rational numbers r_i. Let $\pi\colon \mathbf{Q} \to \mathbf{Q}/\mathbf{Z}$ be quotient map. Lift each of these generators $\overline{r_i}$ to the unique element $a_i/n_i \in [0,1) \subset \mathbf{Q}$ such that $\pi(a_i/n_i) = r_i$. Now let $n = \operatorname{lcm}(n_1, \ldots, n_k)$ and

$$a = \gcd\left(a_1\frac{n}{n_1}, \ldots, a_k\frac{n}{n_k}\right).$$

By construction each of these elements a_i/b_i will be a multiple of $\frac{a}{n}$, This means that the subgroup $G(n)$ will be generated by $\pi(a/n)$. Furthermore a and n are relatively prime by construction, so there exists integers x and y such that $xa + ny = 1$. This means that $x\frac{a}{n} + y\frac{n}{n} = \frac{1}{n}$, so $\pi(1/n)$ is in $G(n)$ too. Since $\pi(1/n)$ has order n, it too must generate $G(n)$, and so $G(n)$ is uniquely characterized as being the cyclic subgroup of $\mathbf{Q}/\mathbf{Z}$ that contains $\pi(1/n)$.

2. For groups $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$, provide a counterexample to each of the following statements.

(a) $G_1 \cong G_2$ and $N_1 \cong N_2$ implies that $G_1/N_1 \cong G_2/N_2$.
(b) $G_1 \cong G_2$ and $G_1/N_1 \cong G_2/N_2$ implies that $N_1 \cong N_2$.
(c) $N_1 \cong N_2$ and $G_1/N_1 \cong G_2/N_2$ implies that $G_1 \cong G_2$.

(a) Let $G_1 \cong G_2$ be the dihedral group D_6, symmetries of the regular hexagon, with presentation $\langle r, s \mid s^2, r^n, (rs)^2\rangle$. Now D_6 has two normal subgroups isomorphic to $\mathbf{Z}_2$: one generated by the reflection $\langle s\rangle$, and the other generated by a rotation of 180°, $\langle r^3\rangle$. But the quotients by these normal subgroups are different: $D_6/\langle s\rangle = \mathbf{Z}_6$ while $D_6/\langle r^3\rangle = D_3$.

(b) Again let $G_1 \cong G_2$ be the dihedral group D_6, and consider the subgroups $\langle r\rangle \cong \mathbf{Z}_6$ and $\langle s, r^2\rangle \cong D_3$. Since each of these subgroups have index two, so they're normal, and the quotient of D_6 by each of them will be isomorphic to $\mathbf{Z}_2$.

(c) Let $G_1 = D_6$ and $G_2 = \mathbf{Z}_{12}$. Each of these has a normal subgroup of index two, and so a quotient isomorphic to $\mathbf{Z}_2$, that is isomorphic to $\mathbf{Z}_6$.

3. Let R be a unital integral domain. For a nonzero element of $s \in R$, let $S = \{1, s, s^2, \dots\}$. Prove that $S^{-1}R \cong R[x]/(xs-1)$.

Solution by Jacob Garcia.

Discussion: Before we present the solution, a quick discussion on why we might believe why this is true. When looking at the construction for $S^{-1}R$, we see that, essentially, we are choosing our favorite nonzero element s and adding in an inverse, $\frac{1}{s}$. So we are motivated to find a similar inverse for s in $R[x]/(xs-1)$. Note that since we are taking the quotient with respect to the ideal $(xs-1)$, we have that $xs-1 \equiv 0$, and so $xs \equiv 1$. So in the quotient, the indeterminate x is acting as an inverse for s. Thus, mapping $\frac{1}{s}$ to x should produce the desired isomorphism.

Solution: We consider $\varphi : S^{-1}R \to R[x]/(xs-1)$ via $\varphi(\frac{r}{s^n}) = rx^n$. This map is well defined: Suppose $\frac{r}{s^n} = \frac{r'}{s^m}$. Without loss of generality, assume $m \geq n$. Then $t(rs^m - r's^n) = 0$ for some $t \neq 0$, and since R is an integral domain, we have $0 = rs^n - r's^m = s^n(rs^{m-n} - r')$, so as $s^n \neq 0$, we have $rs^{m-n} - r' = 0$. Then

$$\varphi(\frac{r'}{s^m}) = r'x^m = (rs^{m-n})x^m = r(sx)^{m-n}x^n = rx^n = \varphi(\frac{r}{s^n}).$$

Now we show φ is a ring homomorphism: Let $\frac{r}{s^n}$ and $\frac{r'}{s^m}$ be arbitrary. Then $\varphi(\frac{r}{s^n}) + \varphi(\frac{r'}{s^m}) = rx^n + r'x^m$, and $\varphi(\frac{r}{s^n} + \frac{r'}{s^m}) = \varphi(\frac{rs^m + r's^n}{s^{m+n}}) = (rs^m + r's^n)x^{m+n} = r(sx)^m x^n + r'(sx)^n x^m = rx^n + r'x^m$. This shows φ respects addition. Now we check $\varphi(\frac{r}{s^n})\varphi(\frac{r'}{s^m}) = rx^n r'x^m = rr'(x^{m+n})$, and also see $\varphi(\frac{r}{s^n}\frac{r'}{s^m}) = \varphi(\frac{rr'}{s^{m+n}}) = rr'(x^{m+n})$.

φ is injective: Let $\frac{r}{s^n}$ and $\frac{r'}{s^m}$ be arbitrary, and assume $m \geq n$. If $\varphi(\frac{r}{s^n}) = \varphi(\frac{r'}{s^m})$, then $rx^n = r'x^m$, so multiplying both sides by 1 gives $rx^n(sx)^m = r'x^m(sx)^n$, i.e., $(rs^m - r's^n)x^{m+n} = 0$. In particular for $x = 1$, we get $rs^m - r's^n = 0$, so $\frac{r}{s^n} = \frac{r'}{s^m}$.

Finally, to show φ is surjective, we make the observation that since the degree of $xs-1$ is 1, every equivalence class of $R[x]/(xs-1)$ is represented by a constant polynomial, and every constant polynomial is in some equivalence class. So it suffices to show that φ surjects to the constant polynomial r for each $r \in R$. This is easily seen by $\varphi(r) = r$.

Solution by Mike Pierce,

Notice that the RHS says that we're appending an element x to R and forcing it to be the inverse to s, which should inspire our choice of maps here. First let φ denote the composite of the natural maps $R \hookrightarrow R[x] \twoheadrightarrow R[x]/(xs-1)$ and let $\overline{r}$ be shorthand for $\varphi(r)$, noting that since φ is a ring homomorphism we have $\overline{\rho r} = \overline{\rho}\,\overline{r}$. Since $\overline{x}\,\overline{s} = 1$, s is a unit in the quotient $R[x]/(xs-1)$ with inverse x. Then we can extend φ to a homomorphism $\widetilde{\varphi}\colon S^{-1}R \to R[x]/(xs-1)$ where $\widetilde{\varphi}\colon r/(s^n) \mapsto \overline{r}\,\overline{x}^n$.

In the other direction we can start by defining a map $\theta\colon R[x] \to S^{-1}R$ where $\theta(r) = r/1$ and $\theta(x) = 1/s$. Then since $\theta(xs-1) = (1/s)(s) - 1 = 0$, this maps factors through $R[x]/(xs-1)$, giving us a map $\widetilde{\theta}\colon R[x]/(xs-1) \to S^{-1}R$. Then we simply note that $\widetilde{\theta}$ and $\widetilde{\varphi}$ are inverses, and we're done.

4. Given a finite p-group G, prove that G has a normal subgroup of every order dividing $|G|$.

It's worth noting that this is close to, but not exactly, the first Sylow theorem.

Suppose that G has order p^n. We'll proceed inductively. So first note that $\langle e \rangle$ is normal, covering our base case. Let N be a normal subgroup of order p^k for some $k < n$, and consider the quotient G/N, letting $\pi\colon G \to G/N$ denote the quotient map. Note that since G/N is a p-group (of order p^{n-k}) it has nontrivial center, and so it'll have some element of order p. Take aN in the center of G/N or order p, and note that $\langle aN \rangle$ is a normal subgroup of G/N of order p. We want to look at $\pi^{-1}(\langle aN \rangle)$. Since the homomorphic preimage of a normal subgroup is normal, this will be a normal subgroup of G of order $p \cdot p^k = p^{k+1}$.

5.

(a) Define the characteristic of a ring.

(b) Assume that R is a commutative unitary ring having only one maximal ideal $\mathfrak{m}$. Show that the characteristic of R is either zero or a power of a prime.

(c) For R as described in (b) show that if $R/\mathfrak{m}$ has characteristic zero, then R contains a field.

(d) Give an example of a ring R as in (b) of characteristic zero having a non-maximal prime ideal P such that the characteristic of R/P is *not* zero.

(a) For a ring R suppose that there exists a positive integer n such that

$$\underbrace{r + r + \cdots + r}_{n \text{ times}} = 0 \ \ \forall r \in R\,.$$

If such an n exists, then the characteristic of R, denoted $\operatorname{char} R$ is the smallest such n with this property. If no such n exists, we say that $\operatorname{char} R = 0$. If R is a unital ring, then we can more simply define $\operatorname{char} R$ to be the generator of the kernel of the unique ring homomorphism $\mathbf{Z} \to R$.

(b) Let $\mathfrak{m}$ be the unique max ideal in your ring. Suppose $\operatorname{char} R > 0$, but for the sake of contradiction that $\operatorname{char} R = nm$ for coprime n and m. You can think of m and n as living in your ring. Let $\operatorname{Ann}(n) = \{r \in R \mid nr = 0\}$ and $\operatorname{Ann}(m) = \{r \in R \mid mr = 0\}$ be the annihilators of these elements, noting that $m \in \operatorname{Ann}(n)$ and $n \in \operatorname{Ann}(m)$ Recall that since n and m are coprime, using the Euclidean algorithm you can find a and b such that $an + bm = 1$ in your ring, so $\operatorname{Ann}(n) + \operatorname{Ann}(m) = R$. This means that only one of $\operatorname{Ann}(n)$ or $\operatorname{Ann}(m)$ can be in $\mathfrak{m}$, contradicting the fact that $\mathfrak{m}$ is maximal. So $\operatorname{char} R$ must be a power of a prime.

You could make basically the same argument using the principal ideals (m) and (n) instead of the annihilators.

Here's a very different-looking approach to saying the same thing. Since $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ will be a field and must have characteristic either 0 or p^n. So the kernel of the unique homomorphism $\iota\colon \mathbf{Z} \to R/\mathfrak{m}$ will be either (0) or (p^n) respectively. Now ι will pull back to a ring homomorphism $\tilde{\iota}\colon \mathbf{Z} \to R$ such that this diagram commutes:

$$\begin{tikzcd}
& \mathbf{Z} \arrow[dl, dashed, bend right, "\tilde{\iota}"'] \arrow[d, "\iota"] \\
R \arrow[r, two heads] & R/\mathfrak{m}
\end{tikzcd}$$

But then $\operatorname{Ker} \tilde{\iota} \subset \operatorname{Ker} \iota$ as a subgroup, and so it must be of the form either (0) or (p^{nk}) depending on the characteristic of $R/\mathfrak{m}$.

(c) If $R/\mathfrak{m}$ has characteristic zero, then we have an injection $\mathbf{Z} \hookrightarrow R/\mathfrak{m}$, and like in the last part this injection factors through the quotient $\mathbf{Z} \hookrightarrow R \twoheadrightarrow R/\mathfrak{m}$.

So $\mathbf{Z} \cap \mathfrak{m} = \{0\}$ in R, and since in a local ring $\mathfrak{m}$ consists of all the non-units, each element of $\mathbf{Z}$ is a unit, so $\mathbf{Q} \subset R$.

(d) An example will be the ring $\mathbf{Z}[x]$ localized at $(x, 2)$, so $\mathbf{Z}[x]_{(x,2)}$. An important fact here that makes this a reasonable example to come up is that the localization of a ring R at a prime ideal P will be a local ring R_P, the max ideal being P_P, and furthermore the prime ideals of R_P will be all be of the form Q_P for some prime ideal Q of R that is contained in P. So for our particular example, we're looking at the chain of prime ideals $(0) \hookrightarrow (2) \hookrightarrow (2, x) \hookrightarrow \mathbf{Z}[x]$. The ideal $(2)_{(2,x)}$ will be prime in $\mathbf{Z}[x]_{(x,2)}$, and since $\mathbf{Z}[x]_{(x,2)}$ is still unital, the quotient of $\mathbf{Z}[x]_{(x,2)}$ by $(2)_{(2,x)}$ will have characteristic 2.

Mock Algebra Qualifying Examination, Fall 2019, Part b

Attempt any four, all questions are worth 10 points.

1. (a) Let R be a ring with identity and M a left module for R. Recall that M is indecomposable if M cannot be written as a direct sum of two non-zero submodules. Prove that if $f\colon M \to M$ is a homomorphism of modules then $f^2 = f$ implies that either $f = 0$ or $f = id$.

(b) Suppose now that M is decomposable. Prove that there exists $f\colon M \to M$ a homomorphism of modules such that $f^2 = f$ and f different from zero and the identity.

(a) It's not explicitly said, but we're assuming M is indecomposable. Suppose that $f^2 = f$ and that $f \neq \mathbf{1}_M$. The key thing to note here is that if $f^2 = f$, then f restricted to the image of f must be the identity on that image. Notationally, $f|_{\operatorname{Im} f} = \mathbf{1}_{\operatorname{Im} f}$. This means that if f is surjective, we're done because then it would be the identity on M. But if f is *not* surjective, it will have a nontrivial kernel. This means that the short exact sequence $\operatorname{Ker} f \hookrightarrow M \twoheadrightarrow \operatorname{Im} f$ splits, with splitting map $f\colon \operatorname{Im} f \to M$, so $M = \operatorname{Ker} f \oplus \operatorname{Im} f$ with $\operatorname{Ker} f$ and $\operatorname{Im} f$ nontrivial, contradicting our assumption that M is indecomposable.

(b) Suppose $M = A \oplus B$ for nonzero A and B, and let $f\colon M \to M$ be the projection map $\pi_A\colon M \to A$. Note that $f^2 = f$, that f is neither zero nor the identity on M since both A and B are nonzero.

Note also, we could have chosen the map π_B, and that $\pi_B = \mathbf{1}_M - \pi_A$, so these two maps are orthogonal idempotents in $\operatorname{End}_R(M)$.

2. Suppose R is a ring with identity and $e \in R$ such that $e^2 = e$.

(a) Prove that $(1-e)$ has the same property.

(b) Prove that $Re \cap R(1-e) = \{0\}$, and hence $R = Re \oplus R(1-e)$.

(c) Regarding the principal ideal Ra as a left R-module, prove that Ra is projective if and only if the annihilator $\operatorname{Ann}(a) = \{r \in R \mid ra = 0\}$ is of the form Re for e such that $e^2 = e$.

(a) Such an element e is called idempotent. Note that $(1-e)^2 = 1 - 2e + e = 1 - e$, so $1-e$ is idempotent.

(b) If we take some element $re \in Re \cap R(1-e)$ we'll have $re = (re)e \in R(1-e)e = \{0\}$. Then since $eR + (1-e)R$ spans R, we have that $R = Re \oplus R(1-e)$.

(c) Consider the map $\varphi\colon R \twoheadrightarrow Ra$ where $\varphi\colon r \mapsto ra$. Then $\operatorname{Ann}(a) = \operatorname{Ker}\varphi$ and we have a short exact sequence $\operatorname{Ann}(a) \hookrightarrow R \twoheadrightarrow Ra$. If $\operatorname{Ann}(a)$ is of the form Re for some idempotent e, then since $R = Re \oplus R(1-e)$, the short exact sequence will split, which means Ra is projective (and isomorphic to $R(1-e)$).

Conversely if Ra is projective, then the short exact sequence splits and we have $R \cong \operatorname{Ann}(a) \oplus Ra$. Now $\operatorname{Ann}(a)$ and Ra are both ideals (submodules) of R, so this $\oplus$ will actually be an internal direct sum since $\operatorname{Ann}(a) \cap Ra = \{0\}$ in R. There's a subtly here though: $\operatorname{Ann}(a)$ is a submodule of R via the inclusion map i in the short exact sequence, but to realize Ra as a submodule of R we should really be considering the splitting map $\psi\colon Ra \to R$ such that $\varphi\psi = \mathbf{1}_{Ra}$. Then while $R \cong \operatorname{Ann}(a) \oplus Ra$, we only have the equality with an internal direct sum $R = i(\operatorname{Ann}(a)) + R\psi(a)$. The difference here is really only up to an automorphism of each of $\operatorname{Ann}(a)$ and Ra as submodules of R. An important point though, is that the idempotent element e that we're looking for won't necessarily be a, but will be $\varphi(a)$ (which will be y in the proof, but I don't bother to flush that out). Considering the element 1 under this isomorphism:

$$\begin{aligned} R &\cong \operatorname{Ann}(a) \oplus Ra \\ 1 &\leftrightarrow (x, y) \\ 1 &= x + y \end{aligned}$$

And then multiplying though by y, we have $y = xy + y^2$, but $xy = 0$ since $\operatorname{Ann}(a) \cap Ra = \{0\}$. So $y = y^2$ is an idempotent of R, and since for $z \in Ra$ $1 = x + y \implies z = 0 + zy$, y is the identity of Ra considered as a subring of R, and generates Ra, so $Ra = Ry$.

3. Let R be a ring with identity. Regard R as a right R-module in the usual way and let M be a right R module. Prove that $\operatorname{Hom}_R(R, M) \cong M$ as abelian groups.

Solution by Jacob Garcia.

Define $f : \operatorname{Hom}_R(R, M) \to M$ via $f(\varphi) = \varphi(1)$. Clearly f is well defined. If $\varphi,\ \psi \in \operatorname{Hom}_R(R, M)$, then $f(\varphi + \psi) = (\varphi + \psi)(1) = \varphi(1) + \psi(1) = f(\varphi) + f(\psi)$. We can also see that if $f(\varphi) = 0$, then $\varphi(1) = 0$, but then for all $r \in R$, $\varphi(r) = r\varphi(1) = r0 = 0$, so $\varphi \equiv 0$. This f is injective. Finally, for each $m \in M$, define φ via $\varphi(r) = rm$. Then $\varphi \in \operatorname{Hom}_R(R, M)$ (as you can check) and $f(\varphi) = m$. Therefore, f is an isomorphism of abelian groups.

4. Consider the ring $R = \mathbf{C}[x]$ of polynomials in an indeterminate x with coefficients in $\mathbf{C}$.
(a) Let M be a torsion free module for R with two generators. Prove that M is free of rank at most two.
(b) Prove that if M is a cyclic R-module and $M \neq R$ then M is torsion. Under what condition on the torsion ideal will M be simple?

(a) Since R is a PID and M is finitely generated, M being torsion free implies that M is free. We can see this with the classification theorem for finitely generated modules over PIDs: if M is torsion free, it'll have not torsion summands, but only summands isomorphic to R. Since M is generated by two elements, say a and b, every element of M can be written as a sum of $ra + sb$ for some choice of $r, s \in R$. If M had rank greater than two, then it would have three elements such that none of them can be written as an R-linear combination of the others. But writing each of these elements in terms of a and b will show that this cannot happen.

(b) Since M is a cyclic R-module, there is some $m \in M$ such that $M = Rm = \{rm \mid r \in R\}$. That is, we get a surjection $\pi\colon R \to M$ via the map $r \mapsto rm$, and we have $M \cong R/\operatorname{Ker}\pi$. Since $R \neq M$, $\operatorname{Ker}\pi$ is nonzero, and anything in $\operatorname{Ker}\pi$ annihilates all of M, so M is a torsion R-module.

Let $\operatorname{Ker}\pi = I$ to clean up the notation to come. If M admits a quotient by a submodule N, we have $M/N \cong (R/I)/N$. But this means that N corresponds to some ideal of R/I, which corresponds to some ideal of R that contains I. So this tells us that if we want M to be simple (N trivial) we need to require that there be no ideals of R that strictly contain I, so I needs to be maximal.

So M ends up being a field isomorphism to a quotient of R.

5. (a) Prove that if A and B are invertible $n \times n$ matrices with entries in an integral domain R, then $A + rB$ is invertible in the quotient field K of R for all but finitely many r.

(b) Prove that the minimal polynomial of a linear transformation of an n-dimensional vector space has degree at most n.

(a) For $n \times n$ matrices A and B which are invertible over an integral domain, the matrix $A+rB$, for $r \in K$, is *not* invertible in K if and only if $\det(A+rB) = 0$. But $\det(A+rB)$ is just a polynomial in r. Furthermore it'll be a non-constant polynomial of degree n since the coefficient on r^n will be $\det(B)$, and so it'll have at most n roots in K. That is, there will be at most n distinct values of r such that $\det(A + rB) = 0$.

(b) For your vector space over field $\boldsymbol{k}$, fix a basis, so your linear transformation can be thought of as a matrix M. The characteristic polynomial of M is defined as $\det(M - xI_n) \in \boldsymbol{k}[x]$, and this will have degree at most n. Note that M is a root of it's characteristic polynomial since, letting $x = M$, we have $\det(M - MI_n) = \det(0) = 0$. The minimal polynomial of M, being the smallest monic polynomial of which M is a root, must divide the characteristic polynomial, and so will have degree at most n.

6. Suppose that φ and ψ are commuting linear transformations of an n-dimensional vector space E. Prove that if E_1 is a ~~φ-invariant subspace of E~~ eigenspace of φ then E_1 is ~~also~~ ψ-invariant. Use this to prove that if φ and ψ both have linear elementary divisors then there exists a basis of E with respect to which the matrix φ and the matrix ψ are both diagonal.

Take $\boldsymbol{v} \in E_1$. If φ and ψ commute, since

$$\varphi\boldsymbol{v} = \lambda\boldsymbol{v} \quad \Longrightarrow \quad \psi\varphi\boldsymbol{v} = \psi\left(\lambda\boldsymbol{v}\right) \quad \Longrightarrow \quad \varphi\left(\psi\boldsymbol{v}\right) = \lambda\left(\psi\boldsymbol{v}\right) ,$$

$\psi\boldsymbol{v}$ is an eigenvector for φ too. This means that the eigenspace E_1 is ψ-invariant.

Now φ and ψ both having linear elementary divisors is the same as saying there exists bases of E relative to which φ and ψ are each (individually) diagonalizable, and this is the same as saying that there exists bases of E consisting of eigenvectors for each of φ and ψ.

There is a much easier version of this statement to prove, where we require that one of φ or ψ have *distinct* elementary divisors. In this case, supposing φ has distinct elementary divisors, E will decompose into $\dim E$ one-dimensional eigenspaces $E_\lambda = \langle\boldsymbol{v}_\lambda\rangle$, one for each elementary divisor $(x - \lambda)$. Then since each of these E_λ are ψ-invariant. each $\boldsymbol{v}_\lambda$ will be an eigenvector for ψ too. So the basis you're looking for consists of these $\boldsymbol{v}_\lambda$.

To prove the question posed though, we've got to get our hands a bit dirtier.

Lemma 1 — Any φ-invariant subspace of E has a basis consisting of eigenvectors of φ.

Proof Let $\{\lambda_1, \dots, \lambda_k\}$ be the distinct eigenvalues of φ. Each of these eigenvalues λ_i corresponds to an eigenspace E_{φ,λ_i}, and since E has a basis of eigenvectors of φ, we can decompose E as $\bigoplus_j E_{\varphi,\lambda_j}$ (i.e. these eigenspaces cover all of E). Take $\boldsymbol{w} \in W$ and under this decomposition we can write $\boldsymbol{w} = \boldsymbol{v}_1 + \ldots + \boldsymbol{v}_n$ where each $\boldsymbol{v}_i$ is in E_{φ,λ_i}. Since W is φ-invariant, we have that $\{\boldsymbol{w}, \varphi\boldsymbol{w}, \varphi^2\boldsymbol{w}, \dots\}$ are all in W. Then since φ is linear, for any positive integer m we have

$$\varphi^m(\boldsymbol{w}) = \lambda_1^m \boldsymbol{v}_1 + \cdots + \lambda_n^m \boldsymbol{v}_n\,.$$

Over each $m \in \{0, \dots, k-1\}$ this gives us a system of k linear equations

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \dots & \lambda_k^{k-1} \end{pmatrix} \begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_k \end{pmatrix} = \begin{pmatrix} \boldsymbol{w} \\ \varphi\boldsymbol{w} \\ \vdots \\ \varphi^{k-1}\boldsymbol{w} \end{pmatrix}.$$

The matrix on the left is the Vandermonde matrix of the $\{\lambda_1, \dots, \lambda_k\}$, and will be invertible since the $\{\lambda_1, \dots, \lambda_k\}$ are distinct. This means that we can write each $\boldsymbol{v}_i$ as a linear combination of the $\{\boldsymbol{w}, \varphi\boldsymbol{w}, \dots, \varphi^{k-1}\boldsymbol{w}\}$ as

$$\begin{pmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \\ \vdots \\ \boldsymbol{v}_k \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{k-1} & \lambda_2^{k-1} & \dots & \lambda_k^{k-1} \end{pmatrix}^{-1} \begin{pmatrix} \boldsymbol{w} \\ \varphi\boldsymbol{w} \\ \vdots \\ \varphi^{k-1}\boldsymbol{w} \end{pmatrix}.$$

The point being that each $\boldsymbol{v}_i$ must then be in W, and so the eigenspace decomposition $E = \bigoplus_j E_{\varphi,\lambda_j}$ restricts to a decomposition $W = \bigoplus_j \left(E_{\varphi,\lambda_j} \cap W\right)$, and W will inherit a basis of eigenvectors of φ from each E_{φ,λ_j}. □

Now to finish things off, let $\{\lambda_1, \dots, \lambda_k\}$ be the distinct eigenvalues of φ, and let $\{\kappa_1, \dots, \kappa_r\}$ be the distinct eigenvalues of ψ. Since φ and ψ are each diagonalizable, we have two decompositions of E into eigenspaces for φ and ψ as

$$E = \bigoplus_j E_{\varphi,\lambda_j} \qquad\qquad E = \bigoplus_j E_{\psi,\kappa_j}$$

Each one of these E_{φ,λ_j} is a ψ-invariant subspace since φ and ψ commute. And since E_{φ,λ_j} is ψ-invariant, by Lemma 1 we we can restrict the decomposition of eigenspaces of ψ to each E_{φ,λ_j}, giving us a basis of E_{φ,λ_j} of eigenvectors for both φ and ψ. Glueing all the E_{φ,λ_j} back together into E Then this gives us a basis of E of eigenvectors for both φ and ψ.

Mock Algebra Qualifier 2019 - Part C

Do 4 out of the 5 problems.

(1) Let F be a splitting field over $\mathbf{Q}$ of the polynomial $x^4 - 5$. Find all the intermediate fields of F over $\mathbf{Q}$, and indicate which ones are Galois over $\mathbf{Q}$.

Solution by James Alcala.

First, factor the polynomial in the most obvious way:

$$\begin{aligned} x^4 - 5 &= (x^2 + 5^{1/2})(x^2 - 5^{1/2}) \\ &= (x + i5^{1/4})(x - i5^{1/4})(x + 5^{1/4})(x - 5^{1/4}) \end{aligned}$$

which indicates that we have four roots to work with. Because we have complex roots, one of our group actions will correspond to complex conjugation, and the other corresponds to multiplying $5^{1/4}$ by i, which will 'rotate' our roots and generate a subgroup of our group of automorphisms of order 4. One can either write out a presentation of this group or draw out pictures of permutations of the roots to find that this group is isomorphic to D_4, which has ten total subgroups, with eight nontrivial. We can write out its presentation as $\langle r, s \mid r^2, s^4, sr^2 = r^2 s, rs = sr^3, sr = r^3 s\rangle$.

Think of r as multiplying $5^{1/4}$ by i, and s as complex conjugation. Because the splitting field of this polynomial, $K = \mathbb{Q}(i, 5^{1/4})$, has degree 8 over $\mathbb{Q}$ and is Galois, the distinct subfields of $K/\mathbb{Q}$ will correspond to distinct subgroups of the Galois group, exactly to the subgroup that fixes that subfield. Here are the subgroups, complete with their correspondence to subfields:

$$\begin{aligned}
\langle e\rangle &\iff \mathbb{Q}(i, 5^{1/4})(a) \\
\langle r^2\rangle &\iff \mathbb{Q}(i, 5^{1/2})(b) \\
\langle sr^2\rangle &\iff \mathbb{Q}(i5^{1/4})(c) \\
\langle rs\rangle &\iff \mathbb{Q}((1+i)5^{1/4})(d) \\
\langle sr\rangle &\iff \mathbb{Q}((1-i)5^{1/4})(e) \\
\langle s\rangle &\iff \mathbb{Q}(5^{1/4})(f) \\
\langle r\rangle &\iff \mathbb{Q}(i)(g) \\
\langle s, r^2\rangle &\iff \mathbb{Q}(5^{1/2})(h) \\
\langle rs, sr\rangle &\iff \mathbb{Q}(i5^{1/2})(i) \\
\langle s, r\rangle &\iff \mathbb{Q}(j)
\end{aligned}$$

and their containments:

- The group at (a) is contained in the groups (b), (c), (d), (e), and (f), and the they are index 2 subgroups of order 2; the subfield at (a) is the splitting field of our original polynomial and contains the fields (b), (c), (d), and (e) as subfields of index 2.

- The group at (b) is contained in the groups (g), (h), and (i) with an index of 2; the field at (b) contains the the fields at (g), (h), and (i) as subfields of index 2.

- The group at (c) is contained in the group (h) with index 2; the field at (c) contains only the field at (h) as a subfield of index 2.

- The group at (d) is contained in the group (i) with index two; similarly the field at (d) contains the field at (i) as a subfield of index 2.

- The group at (e) is contained in the group at (i) with index two, and the field at (e) contains the field (i) as a subfield of index two.

- The group (f) is contained in the group (h) with index two, and the field (f) contains the field (h) with index two.

- The groups (g), (h) and (i) are all subgroups of the group (j) of index two, and similarly the fields (g), (h) and (i) contain (J) as a subfield of index two.

The extensions that are NOT Galois are (c), (f).

(2) Prove that $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$

Page 141 of Kayla's Notes ◀

(3) Let F be the splitting field of $f \in K[x]$ over K. Prove that if an irreducible polynomial $g \in K[x]$ has a root in F, then g splits into linear factors over F. (This result is part of a theorem characterizing normal extensions and you may not, of course, quote this theorem or its corollaries).

Let u be a root of g in F let v be a root of g that is not necessarily in F. Let G denote the splitting field of g over K. Both u and v are roots of the irreducible polynomial g so there is some automorphism $\varphi \in \mathrm{Aut}_K(G)$ that swaps v and u, because the Galois group acts transitively on the roots of the polynomial. So $K(v) \simeq K(u)$ via this isomorphism. Now the heavy lifting thanks to Theorem 3.8 in Chapter V of Hungerford: since F is a splitting field of f over $K(u)$ and $F(v)$ is a splitting field of $\varphi f = f$ over $K(v)$, then φ extends to an isomorphism $F \simeq F(v)$.

(But the proof of this theorem is long, and we aren't even wielding it's full power, so maybe it's not too hard to just prove the bit that we need?)

$$\begin{tikzcd}
F(v) & & \\
& F \arrow[ul] & \\
K(v) \arrow[uu] & & K(u) \arrow[ul] \\
& K \arrow[ul] \arrow[ur] \arrow[uu] &
\end{tikzcd}$$

But if $F \cong F(v)$, well then F and $F(v)$ have the same degree over K, so they must be equal. I.e, $v \in F$ all along.

(4) Let p be a prime and n be any natural number.

(a) Prove that there exists an irreducible polynomial f of degree n in $\mathbf{Z}_p[x]$.

(b) Let $f \in \mathbf{Z}_p[x]$ be an irreducible polynomial of degree n. Determine with proof the degree of the splitting field of f over $\mathbf{Z}_p$.

(c) Exhibit with proof irreducible polynomials of degree 2, 3, and 4 over $\mathbf{Z}_2$.

(a) If a monic polynomial f of degree n is reducible then it must have a monic irreducible factor of degree i for some $i \in \{1, \dots, m\}$, where $m = \lfloor n/2 \rfloor$. We can simply count the possible number of polynomials f and the possible number of irreducible factors, and note that the former number is greater than the latter to conclude that some f must be irreducible. There are p^n ways to choose the coefficients of f and, again choosing coefficients, there are $p + p^2 + \cdots + p^m$ possibilities of irreducible factor. Then we're good since

$$p + p^2 + \cdots + p^m = \frac{p^{m+1} - p}{p - 1} < p^{m+1} \leq p^n \,.$$

(b) Let F be a splitting field of f over $\mathbf{Z}_p$. Recall that the multiplicative group of units of F must be cyclic*. Letting u be a generator of that cyclic group, note that $u \notin \mathbf{Z}_p$, else it couldn't generate all of F. So $F = \mathbf{Z}_p(u)$, and since u is a root of f and f is irreducible, u has degree n over $\mathbf{Z}_p$, so $[F : \mathbf{Z}_p] = n$.

($*$) If you really want to prove that $F^\times$, the group of units of F, must be a cyclic group, notice first that it must be a finite abelian group, so $F^\times$ decomposes as $\mathbf{Z}_{m_1} \oplus \cdots \oplus \mathbf{Z}_{m_k}$ where the m_i are the *invariant factors* of the multiplicative group. So $m_1 | m_2 | \cdots | m_k$, and all the elements of $F^\times$ have order dividing m_k. In particular every element of $F^\times$ is a root of $x^{m_k} - 1$ which has exactly m_k distinct roots, so $|G| = m_k$ and $G \simeq \mathbf{Z}_{m_k}$

(c) There are many answers to this part. Since $\mathbf{Z}_2$ has characteristic 2 though, it's probably smart to guess polynomials with an odd number of terms that have non-zero constant term to ensure that neither 0 or 1 is a root.

$$x^2 + x + 1 \qquad x^3 + x + 1 \qquad x^4 + x + 1$$

None of these have 0 or 1 as a root. Then since a reducible polynomial of degree ≤ 3 must have a linear factor, the first three polynomials must be irreducible. Now we've just got to check that $x^4 + x + 1$ doesn't factor into quadratics. If it did, its factorization would look something like $x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$. Cranking out the right-hand-side we see that the coefficients of the x^3 term and the x term both have to be $(a + b)$, so such a factorization can't exist.

(5) Let $\boldsymbol{F}_7$ be a cyclotomic extension of $\mathbf{Q}$ of order seven. If ζ is a primitive seventh root of unity, what is the irreducible polynomial over $\mathbf{Q}$ of $\zeta + \zeta^{-1}$? You must justify your answer.

Solution by Nobel Williamson

Let ζ be a primitive 7-th root of unity. The minimal polynomial of ζ over $\mathbf{Q}$ is the 7-th cyclotomic polynomial $\Phi_7(x)$. Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$ we have

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} \Phi_d(x)}$$

and since $n = 7$ is prime, $d = 1$ so

$$\Phi_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Note that since $[F : \mathbf{Q}] = 6$ and since $Q(\zeta + \zeta^{-1})$ is a proper subextension of F, it must be an extension of $\mathbf{Q}$ of degree either 2 or 3 which means the degree of the minimal polynomial of $\zeta + \zeta^{-1}$ over $\mathbf{Q}$ must be either 2 or 3. Observe that

$$\begin{aligned}
& (\zeta+\zeta^{-1})^3+(\zeta+\zeta^{-1})^2-2(\zeta+\zeta^{-1})-1 \\
= \quad & \zeta^3+3\zeta+3\zeta^{-1}+\zeta^{-3}+\zeta^2+2+\zeta^{-2}-2\zeta-2\zeta^{-1}-1 \\
= \quad & \zeta^3+3\zeta+3\zeta^6+\zeta^4+\zeta^2+2+\zeta^5-2\zeta-2\zeta^6-1 \\
= \quad & \zeta^6+\zeta^5+\zeta^4+\zeta^3+\zeta^2+\zeta+1 \\
= \quad & 0
\end{aligned}$$

So $\zeta+\zeta^{-1}$ satisfies the polynomial $f(x)=x^3+x^2-2x-1$. Now we must check if f is irreducible over $\mathbf{Q}$. Since it's a degree 3 polynomial, if it were reducible over $\mathbf{Q}$, it would have a linear factor, hence a rational root. However, the rational root test states that if a polynomial with integer coefficients has a rational root p/q then p is a factor of the constant term and q is a factor of the leading coefficient. Since both the constant term and leading coefficient of f are 1, the only possible rational roots for f are -1 and 1 which clearly are not roots. Hence, f has no rational roots so it is irreducible over $\mathbf{Q}$. Since $\zeta+\zeta^{-1}$ is a root of f, its minimal polynomial must divide f but f is irreducible so $f(x)=x^3+x^2-2x-1$ is the minimal polynomial of $\zeta+\zeta^{-1}$ over $\mathbf{Q}$.