MOCK QUALIFYING EXAMINATION, ALGEBRA, PART A, 2019

September n^2, 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 be a group, and let A be an abelian group. Let $\varphi\colon G \to \mathrm{Aut}(A)$ be a group homomorphism. Let $A \times_\varphi G$ denote the set $A \times G$ with the binary operation

$$(a, g)(a', g') = (a + \varphi(g)(a'), gg').$$

(a) Prove that $A \times_\varphi G$ is a group.
(b) Find a map $\varphi\colon \boldsymbol{Z}_2 \to \mathrm{Aut}(\boldsymbol{Z}_m)$ such that the dihedral group D_m is isomorphic to $\boldsymbol{Z}_m \times_\varphi \boldsymbol{Z}_2$. *Do not forget to prove the isomorphism!*

Solution by Joe Wagner. Transcribed by Jacob Garcia. Corrected by James Alcala.

(a) Associativity is work. Do it for practice.

The element $(0, 1)$ is the identity:

$$(0, 1) \cdot (a, g) = (0 + \varphi(1)(a), 1g) = (0 + a, g) = (a, g)$$

$$(a, g) \cdot (0, 1) = (a + \varphi(g)(0), g1) = (a + 0, g) = (a, g)$$

Given $(a, g) \in A \times_\varphi G$, we claim $(a, g)^{-1} = (\varphi(g^{-1})(-a), g^{-1})$, since

$$(a, g)^{-1}(a, g) = (\varphi(g^{-1})(-a)+\varphi(g^{-1})(a), g^{-1}g) = (\varphi(g^{-1})(a-a), 1) = (\varphi(g^{-1})(0), 1) = (0, 1)$$

$$(a, g)(a, g)^{-1} = (a+\varphi(g)(\varphi(g^{-1})(-a)), gg^{-1}) = (a+\varphi(1)(-a), 1) = (a-a, 1)-(0, 1)$$

Note in the above that $\varphi(g)^{-1} = \varphi(g^{-1})$ and $\varphi(g)(a)+\varphi(g)(b) = \varphi(g)(a+b)$.

(b) Define $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_m)$ via $\varphi(0)(\bar{k}) = \bar{k}$ and $\varphi(1)(\bar{k}) = -\bar{k}$. Now define $\psi : \mathbb{Z}_m \times_\varphi \mathbb{Z}_2 \to D_m$ via $\psi(1, 0) = r$ and $\psi(0, 1) = s$, where r and s are the rotation and reflection of D_m respectively.

This map is a homomorphism. We do this in cases:

(a) $(n, 0), (k, 0)$: Then $\psi((n, 0)(k, 0)) = \psi(n+\varphi(0)(k), 0+0) = \psi(n+k, 0) = r^{n+k}$, and $\psi(n, 0)\psi(k, 0) = r^n r^k = r^{n+k}$.

(b) $(n,1),(k,0)$: Then $\psi((n,1)(k,0)) = \psi(n+\varphi(1)(k), 1+0) = \psi(n-k,1) = r^{n-k}$, and $\psi(n,1)\psi(k,0) = r^n s r^k = r^{n-k}$.

(c) $(n,0),(k,1)$: Then $\psi((n,0)(k,1)) = \psi(n+\varphi(0)(k), 0+1) = \psi(n+k,1) = r^{n+k}s$, and $\psi(n,0)\psi(k,1) = r^n r^k s = r^{n+k}s$.

(d) $(n,1),(k,1)$: Then $\psi((n,1)(k,1)) = \psi(n+\varphi(1)(k), 1+1) = \psi(n-k,0) = r^{n-k}$, and $\psi(n,1)\psi(k,1) = r^n s r^k s = r^{n-k}ss = r^{n-k}$.

Then this map is easily seen to be surjective, and since $|D_m| = |\mathbb{Z}_m \times \mathbb{Z}_2| = |\mathbb{Z}_m \times_\varphi \mathbb{Z}_2| < \infty$, this is also an injection.

2. Let G be a finite group, and let $\mathrm{Z}(G)$ denote the *center* of G.

(a) Prove that if $G/\mathrm{Z}(G)$ is cyclic, then G is abelian.
(b) Prove that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian.
(c) Prove that if $\mathrm{Aut}(G)$ is nontrivial and cyclic, then $|\mathrm{Aut}(G)|$ must be even.
(d) Prove that there is no group with infinite cyclic automorphism group.

(a) First let $Z = \mathrm{Z}(G)$. Since G/Z is cyclic, there exists some $g \in G$ such that $(gZ)^n = aZ$ for any $aZ \in G/Z$. On the level of elements, given any $a \in G$ and any $\zeta \in Z$ we can find $z \in Z$ such that $(gz)^n = g^n z^n = a\zeta$. In particular, $a = g^n z^n \zeta^{-1}$, so every element $a \in G$ can be written as the product of a power of g and an element in Z. Using this fact, we can take $a, b \in G$ and see that

$$ab = (g^n z_a)(g^m z_b) = g^n g^m z_a z_b = g^m g^n z_b z_a = g^m z_b g^n z_a = ba\,,$$

which is what we wanted to show. Note that this mean that really $\mathrm{Z}(G) = G$, and so for no (nontrivial) group can we have $G/\mathrm{Z}(G)$ cyclic.

(b) Let $\mathrm{Inn}(G)$ denote the set of inner automorphisms of G, automorphisms given by conjugation by some element of G. Recall that $\mathrm{Inn}(G)$ is a (normal) subgroup of $\mathrm{Aut}(G)$. If $\mathrm{Aut}(G)$ is cyclic then $\mathrm{Inn}(G)$, being a subgroup, will be cyclic too. But note that $\mathrm{Inn}(G) \cong G/\mathrm{Z}(G)$, so G is abelian by the first part.

(c) If $\mathrm{Aut}(G)$ is cyclic, the G is abelian. Consider the map $\varphi\colon G \to G$ that sends an element to its inverse. Since

$$\varphi(ab) = ab^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)\,,$$

φ is a homomorphism, and will be a bijection, so $\varphi \in \mathrm{Aut}(G)$. Note that either φ has order two in $\mathrm{Aut}(G)$ or is trivial, In the former case, since $\mathrm{Aut}(G)$ is finite (because G is finite) two must divide the order of $\mathrm{Aut}(G)$. In the latter case, every element will be its own inverse. Since G is a finite abelian group consisting entirely of elements of order two, $G \cong \bigoplus_n \mathbf{Z}_2$. If $n = 1$, $\operatorname{Aut}(G) = \operatorname{Aut}(\mathbf{Z}_2)$ is trivial. If $n > 1$, then the map that swaps the first two components of the direct sum, $(g_1, g_2, \cdots) \mapsto (g_2, g_1, \cdots)$, will be an automorphism of order two, which again divides the order of $\operatorname{Aut}(G)$.

(d) If there were such a group, it would be abelian. But we can extend the argument in part (c) above to *any* abelian group G. Unless every element of G has order two, the automorphism $\varphi\colon g \mapsto g^{-1}$ will be nontrivial and have order two in $\operatorname{Aut}(G)$, meaning $\operatorname{Aut}(G) \ncong \mathbf{Z}$. If every element of G does have order two, then swapping two generators will similarly give you an automorphism of G of order two.

3.

(a) Prove that any subgroup of index 2 must be normal.

(b) How many index 2 subgroups are there of a free group on two generators? Write down these subgroups in terms of their generators.

(a) Take $N < G$ of index two and $g \in G$. If $g \in N$, then $gN = Ng$ since N is a subgroup, so N is normal in G. Otherwise if $g \notin N$, because N has index two $gN = G \setminus N$, but also $Ng = G \setminus N$, so $gN = Ng$ which means N is normal.

(b) If $N < \langle a, b \rangle$ has index 2, it will be normal we can form the quotient $\langle a, b \rangle / N$ and it will be isomorphic to $\mathbf{Z}_2$. I.e. we have a sort exact sequence $N \hookrightarrow \langle a, b \rangle \twoheadrightarrow \mathbf{Z}_2$, and we can count the possible normal subgroups N by counting the possible maps $\pi\colon \langle a, b \rangle \twoheadrightarrow \mathbf{Z}_2$. A brief analysis shows that π must send both a^2 and b^2 to zero, so we must only consider where π could send the elements $\{a, b\}$. A briefer analysis shows that we have three possibilities, each characterized by the following mappings:

$$\begin{array}{ccc} a \mapsto 1 & b \mapsto 1 & a, b \mapsto 1 \\ b, a^2 \mapsto 0 & a, b^2 \mapsto 0 & ab, ba, a^2, b^2 \mapsto 0 \end{array}$$

Then in each of these cases respectively we can write N in terms of it's generators (remember any subgroup of a free group is free) as follows

$$\langle b, a^2 \rangle \qquad \langle a, b^2 \rangle \qquad \langle ab, a^2, b^2 \rangle .$$

4. An element e in a ring R is said to be idempotent if $e^2 = e$. The center $\mathrm{Z}(R)$ of a ring R is the set of all elements $x \in R$ such that $xr = rx$ for all $r \in R$. An element of $\mathrm{Z}(R)$ is called central. Two central idempotents f and g are called orthogonal if $fg = 0$. Suppose that R is a unital ring.

(a) If e is a central idempotent, then so is $1_R - e$, and e and $1_R - e$ are orthogonal.

(b) eR and $(1_R - e)R$ are ideals and $R = eR \times (1_R - e)R$.

(c) If $R_1, \ldots, R_n$ are rings with identity then the following statements are equivalent.

(i) $R \cong R_1 \times \cdots \times R_n$

(ii) R contains a set of orthogonal central idempotents $e_1, \ldots, e_n$ such that $e_1 + \cdots + e_n = 1_R$ and $e_i R \cong R_i$, $1 \le i \le n$.

(iii) $R = I_1 \times \cdots \times I_n$ where I_k is an ideal of R and $R_k \cong I_k$.

(a) Note that $(1_R - e)^2 = 1_R - 2e + e = 1_R - e$, so $1_R - e$ is idempotent. Also, $(1_R - e)$ will be central since both 1_R and e are central. Furthermore, $e(1_R - e) = e - e^2 = e - e = 0$, so e and $1_R - e$ are orthogonal.

(b) Notationally, eR and $(1_R - e)R$ are just the *right* ideals generated by e and $1_R - e$ respectively. But since e and $1_R - e$ are central, $eR = Re$ and $(1_R - e)R = R(1_R - e)$. Then we can prove that R is an internal direct product of its ideals $eR \times (1_R - e)R$ by showing that $eR + (1_R - e)R$ spans R and that $eR \cap (1_R - e)R = \{0\}$: For any $r \in R$ we have $er + (1_R - e)r = r$ so $eR + (1_R - e)R$ spans R, and if we take some element $er \in eR \cap (1_R - e)R$ we'll have $er = e(er) \in e(1_R - e)R = \{0\}$.

(c) First, (iii) implies (i) obviously. Now assume (i). Take $e_i = (0, \ldots, 1_{R_i}, \ldots, 0)$ in $R_1 \times \cdots \times R_n$. Verifying these e_i are central idempotents and are pairwise orthogonal is straightforward. In the isomorphism $R \cong R_1 \times \cdots \times R_n$ the identity 1_R identifies with $(1_{R_1}, \ldots, 1_{R_n})$, so $e_1 + \cdots + e_n = 1_R$. Then we have $e_i R \cong e_i (R_1 \times \cdots \times R_n) = \{0\} \times \cdots \times 1_{R_i} R_i \times \cdots \times \{0\} \cong R_i$. So (i) implies (ii). Now assume (ii). Note that by parts (a) and (b),

$$\begin{aligned} R &= e_1 R \times (e_2 + \cdots + e_n)R \\ &= e_1 R \times e_2 R \times (e_3 + \cdots + e_n)R \\ &= \cdots \\ &= e_1 R \times e_2 R \times \cdots \times e_n R \end{aligned}$$

and each of these $e_i R$ will be an ideal of R.

5.

(a) Give an example of a category in which a morphism between two objects is epic if and only if it is surjective.

(b) Give an example of a category $\mathcal{C}$ and of an epic morphism between two objects in $\mathcal{C}$ which is not surjective.

(a) Recall that for objects A and B in a category $\mathcal{C}$ the morphism $A \xrightarrow{\varphi} B$ is epic (is an epimorphism) if for any diagram

$$\begin{tikzcd} A \arrow[r, two heads, "\varphi"] & B \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] & C \end{tikzcd} \qquad (\star)$$

we have that $f\varphi = g\varphi$ implies $f = g$. This question only makes sense for concrete categories, categories where the objects have an underlying set structure (to define this precisely, we need to require that there exists a faithful functor $\mathcal{C} \to \text{Set}$) [1]. The walking example of a category in which a morphism is epic iff it's surjective is the category Set itself (proving this is a reasonable exercise). Furthermore, since surjectivity is a very set-theoretic notion, I imagine that we *define* a morphism in an arbitrary concrete category $\mathcal{C}$ to be surjective if it gets sent to an epimorphism by the faithful functor $\mathcal{C} \to \text{Set}$.

For a silly example though, you could consider the category $\mathcal{C}$ that has no objects. This category is vacuously concrete (there is an empty functor $\mathcal{C} \to \text{Set}$) and vacuously a morphism is epic iff it's surjective.

(b) The classic example of this is the morphism $\mathbf{Z} \to \mathbf{Q}$ in the category Ring of unital rings. The map $\mathbf{Z} \to \mathbf{Q}$ is very not surjective, but for any other unital ring R there is a unique morphism $\mathbf{Q} \to R$ (Hungerford III.1, Exercise 18) so we get that $\mathbf{Z} \to \mathbf{Q}$ is epic trivially.

Again though, to find the silliest example, Let $\mathcal{C}$ be the full subcategory of Set consisting of the objects $\varnothing$ and 1. There is a single morphism $\varnothing \to 1$ that is epic but not surjective.

See Wikipedia for more meaty examples though.

[1] The notable example of a *non*-concrete cagetory to keep in mind is hTop, the category of topological spaces with maps being homotopy classes of continuous functions. If you consider a contractable topological space, the identity function and the function that sends the whole space to some point in the space are homotopic, so they'll be the same morphism in hTop. Where could a faithful functor $\text{hTop} \to \text{Set}$ send such a morphism? Nowhere.

Mock Algebra Qualifying Examination, Fall 2019, Part b

Attempt as many questions as you like. A perfect score is 50.

Assume that all rings have identity.

1. (5 points) Let V be a vector space over a field K of dimension r. Let $f \in \mathrm{Hom}_K(V, K)$. Prove that if f is non-zero, then it is surjective and determine the dimension of the kernel of f.

Solution by Joe Wagner. Transcribed by Jacob Garcia.

Let V be a vector space over K, and let $f : V \to K$ be a nonzero K homomorphism. Thus, there exists a nonzero $k \in K$ such that $f(v) = k$ for some $v \in V$. But then $\mathrm{Im} f$ is a nonzero ideal in the field K, so $\mathrm{Im} f = K$.

By the rank-nullity theorem, $\dim(\ker(f)) + \dim(\mathrm{im}(f)) = \dim(V)$, so $\dim(\ker(f)) = r - 1$.

2. (7 points) (a) Suppose that R and S are commutative rings and that M is a (R, S)-bimodule. This means that M is a left R-module and a right S-module and the actions are compatible, i.e. $r(ms) = (rm)s$, for all $r \in R$, $s \in S$, and $m \in M$. Let N be a left S-module. How does one define a left R-module structure on $M \otimes_S N$? What must you check to see that the action is well-defined? If we assume now in addition that N is a (S, R)-bimodule that can you say about $M \otimes_S N$?

(b) (3 points) Suppose now that K is a field and let V, W be vector space over K. Use (a) to show that $V \otimes_K W$ is also a vector space over K. What is the most natural way to find a basis for $V \otimes_K W$?

Solution by Jacob Garcia.

(a) The natural thing to do is to define $r \cdot (m \times n) = (r \cdot m) \otimes n$. We then check to make sure this is well defined. Note that it is enough to check this on the simple tensors because it is a generating set for $M \otimes_S N$. Let $r, r' \in R$, and let $m, m' \in M$, $n, n' \in N$. Then we need to check that

$$(rs)(m \otimes n) = (r(s(m \otimes n)))$$

$$(r + s)(m \otimes n) = r(m \otimes n) + s(m \otimes n)$$

$$r(m \otimes n + m' \otimes n') = r(m \otimes n) + r(m' \otimes n')$$

If N is, in addition, a (S, R)-bimodule, then we claim that $M \otimes_S N$ is a (R, R)-bimodule. In particular, we define the right action similarly to the left action, and so

$$(r(m \otimes n))s = (rm \otimes n)s = rm \otimes ns = r(m \otimes ns) = r((m \otimes n)s)$$

(b) By part (a), since $V \otimes_K W$ is a bimodule over the field K, then by definition, $V \otimes_K W$ is a vector space of K. The natural way to construct a basis is as follows. Let X be a basis for V and Y a basis for X. Then the set $\{a \otimes b \ : \ a \in X, b \in Y\}$ is the natural basis.

3. (5 points) (a) Let V, W be vector spaces over a field K. How does one define a vector space structure on $\mathrm{Hom}_K(V, W)$? Suppose now that $W = K$. Given a basis for V, how would you produce a natural basis for $V^* = \mathrm{Hom}_K(V, K)$? More generally, if $\dim V = r$ and $\dim W = s$ and you are given bases for V and W, find a natural basis for $\mathrm{Hom}_K(V, W)$.

(b) (10 points) Let W be another vector space over K. Define the natural map of vector spaces $V^* \otimes W \to \mathrm{Hom}_K(V, W)$ and prove that it is an isomorphism of vector spaces.

Solution from Derek Lowenberg

(a) We define a vector space structure on $\mathrm{Hom}_K(V, W)$ as follows: for $a \in K$, $v \in V$ and $f, g \in \mathrm{Hom}_K(V, W)$ we define af by $(af)(v) = af(v)$ and $f+g$ by $(f+g)(v) = f(v)+g(v)$.

Let $\{e_1, \ldots, e_r\}$ be a basis for V. Then one can produce a natural basis for V^* by defining for $i \in \{1, \ldots, r\}$ the function $e_i^* \colon V \to K$ on the given basis by $e_i^*(e_k) = 0$ if $k \neq i$ and $e_i^*(e_k) = 1$ if $k = i$ and extending by linearity to give a map $V \to K$.

More generally, if W has a basis $\{w_1, \ldots, w_s\}$ then one can define a natural basis for $\mathrm{Hom}_K(V, W)$ by defining for $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, s\}$ the map $h_{ij} \colon V \to W$ by $h_{ij}(e_k) = 0$ if $k \neq i$ and $h_{ij}(e_k) = w_j$ if $k = i$ and extending by linearity to give a map $V \to W$.

(b) Define $h \colon V^* \otimes W \to \mathrm{Hom}_K(V, W)$ on basis elements by $h(e_i^* \otimes w_j)(e_k) = e_i^*(e_k)w_j$ and extend by linearity to give the desired homomorphism. That is, $h(e_i^* \otimes w_j) = h_{ij}$ hence we see that this map is surjective. Since both source and target have dimension rs over K it follows that h is also injective, hence an isomorphism.

4. (10 points) Let R be the polynomial ring $\mathbf{C}[t]$ in one variable with coefficients in the complex numbers and let I be the ideal generated by t^2 and let $M = R/I$. Prove that M has a proper non-zero submodule and that M cannot be written as a direct sum of proper non-zero submodules. Suppose now that we take J to be the ideal generated by $t(t-1)$. Prove that the module $N = R/J$ is isomorphic to a direct sum of two proper non-zero submodules.

Solution from Derek Lowenberg

Consider $M = \mathbb{C}[t]/I$ where $I = \langle t^2 \rangle$ and let N be the submodule generated (as a $\mathbb{C}[t]$-module) by $t + I$. This is a proper submodule since one cannot write $1 + I$ as a sum of elements of the form $f(t + I)$ for $f \in \mathbb{C}[t]$. Hence M has a nonzero proper submodule.

Suppose $M = N \oplus L$ where N and L are nonzero proper submodules. Then N or L must contain an element of the form $at + b$ where $b \neq 0$. This follows because we can write $1 + I = v + w + I$ where $v + I \in N$ and $w + I \in L$, and we cannot have $k + I \in N$

for any constant k, for then $N = M$. In particular we can assume that $v = at + b$ and $w = ct + d$ are linear, for if they had higher order terms these would differ from the linear term by a multiple of t^2. Further, at least one of b or d must be nonzero, say b. Then $(at - b)(at + b) + I = -b^2 + I \in N$ where $-b^2 \neq 0$, hence $1 + I \in N$ so that $N = M$ and $L = 0$. This contradicts our initial assumption, hence M cannot be written as a direct sum of proper nonzero submodules.

Now suppose J is the ideal generated by $t(t-1)$ and consider $N = \mathbb{C}[t]/J$. Then $N = \langle t + J \rangle \oplus \langle t - 1 + J \rangle$. To verify this, we note that if $v \in N$ is such that $v \in \langle t + J \rangle$ and $v \in \langle t - 1 + J \rangle$, then $v \in \langle t(t-1) + J \rangle$, or $v \in J$, hence the intersection of these two ideals is trivial. Finally, for any $v \in N$, say $a_n t^n + \cdots + a_2 t^2 + a_1 t + a_0 + J$, we have

$$a_n t^n + \cdots + a_2 t^2 + a_1 t + a_0 + J = (a_n t^{n-1} + a_2 t + a_1 + a_0)(t + J) + -a_0(t - 1 + J)$$

showing that these two proper nonzero submodules together span N as a $\mathbb{C}[t]$-module.

5. (5 points) Prove that an $n \times n$-matrix with entries in a field K is invertible iff 0 is not an eigenvalue of the matrix.

Let A be your matrix, and recall that A can be regarded as a linear endomorphism of a n-dimensional K-vector space V.

LEMMA 1 — If A is injective, the it's surjective too, and hence an isomorphism, and hence it's invertible.

Proof If $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a basis for V, note that the vectors $\{A\boldsymbol{v}_1, \ldots, A\boldsymbol{v}_n\}$ will be linearly independent. If they weren't you'd have some nontrivial linear combination

$$c_1 A\boldsymbol{v}_1 + \cdots + c_n A\boldsymbol{v}_n = A\left(c_1 \boldsymbol{v}_1 + \cdots + c_n \boldsymbol{v}_n\right) = 0$$

but this cannot be since A is injective and the $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ are linearly independent. Since the vectors $\{A\boldsymbol{v}_1, \ldots, A\boldsymbol{v}_n\}$ are linearly independent, they form a basis for V, and hence A is surjective, and invertible. □

If A is invertible, then it has to be injective. This means that the equation $A\boldsymbol{v} = 0\boldsymbol{v} = 0$ can't have any nonzero solutions $\boldsymbol{v}$, so zero is not an eigenvalue. Conversely, suppose that A is not invertible. By the lemma this means that A is not injective, and so $A\boldsymbol{v} = 0\boldsymbol{v} = 0$ has a nontrivial solution.

6. (10 points) What is the companion matrix A of the polynomial $q = x^2 - x + 2$? Prove that q is the minimal polynomial of A.

Answering this first bit just comes down to recalling that the companion matrix of a *monic* polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a + 0$ is

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}.$$

Note that this is how Hungerford defines it, but most other authors consider the transpose matrix instead (and I suppose they define their action of $\boldsymbol{k}[x]$ on a vector space over $\boldsymbol{k}$ to be a right action instead too). So the companion matrix of our polynomial q is

$$\begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}.$$

To show that q is the minimal polynomial of A, you just need to show that A satisfies $q(A) = 0$, and that $g(A) \neq 0$ for any linear polynomial g. The second bit should obviously be true. The first bit we just need to verify manually:

$$\begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}^2 - \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix} + 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0.$$

7. (10 points) Suppose that P_1 and P_2 are R-modules. Prove that $P_1 \oplus P_2$ is projective iff P_1 and P_2 are projective.

Recall we have an isomorphism

$$\operatorname{Hom}_R(P_1, X) \oplus \operatorname{Hom}_R(P_2, X) \cong \operatorname{Hom}_R(P_1 \oplus P_2, X).$$

This isomorphism basically tells us that if we have a maps f and g from P_1 and P_2 respectively with a common codomain, we can glue them together to get a map $f + g$ from $P_1 \oplus P_2$. Another key fact is that $\oplus$ is both the product and coproduct in the category R-Mod, so for $i \in \{1, 2\}$ we have the projection maps $\pi_i \colon P_i \oplus P_2 \twoheadrightarrow P_i$ and inclusion maps $\iota_i \colon P_i \hookrightarrow P_1 \oplus P_2$.

Start with a surjective map of R-modules $\varphi \colon C \twoheadrightarrow A$.

Suppose that $P_1 \oplus P_2$ is projective, and suppose we have a map $p \colon P_i \to A$. Then we have a map $p\pi_i \colon P_1 \oplus P_2 \to A$ which will lift to maps $\widetilde{p\pi}_i \colon P_1 \oplus P_2 \to C$. Then by construction the map $\widetilde{p\pi}_i \iota_i$ will be the lifting of p such that $\varphi \widetilde{p\pi}_i \iota_i = p$, which shows P_i

is projective.

$$\begin{tikzcd}
 & P_1 \oplus P_2 \arrow[d, bend right, "\pi_i"'] \arrow[ddl, bend right=60, "\widetilde{p\pi}_i"'] \\
 & P_i \arrow[u, bend right, "\iota_i"'] \arrow[d, "p"] \arrow[dl, dashed, "\widetilde{p\pi}_i\iota_i"'] \\
C \arrow[r, two heads, "\varphi"'] & A
\end{tikzcd}$$

Conversely suppose that both P_1 and P_2 are projective and we have a map $p\colon P_1 \oplus P_2 \to A$. Since P_1 and P_2 are each projective, the maps $p\iota_i$ will each lift to a map $\widetilde{p\iota}_i\colon P_i \to C$. Then by construction the map $\widetilde{p\iota}_1 + \widetilde{p\iota}_2$ (which uses each π_i) will be the lifting of p such that $\varphi(\widetilde{p\iota}_1 + \widetilde{p\iota}_2) = p$, which shows $P_1 \oplus P_2$ is projective.

$$\begin{tikzcd}
 & P_i \arrow[d, bend right, "\iota_i"'] \arrow[ddl, bend right=60, "\widetilde{p\iota}_i"'] \\
 & P_1 \oplus P_2 \arrow[u, bend right, "\pi_i"'] \arrow[d, "p"] \arrow[dl, dashed, "\widetilde{p\iota}_1+\widetilde{p\iota}_2"'] \\
C \arrow[r, two heads, "\varphi"'] & A
\end{tikzcd}$$

8. (10 points) Let $0 \to L \to M \to N \to 0$ be a short exact sequence of R-modules such that we have a short exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(N, L) \longrightarrow \mathrm{Hom}_R(N, M) \longrightarrow \mathrm{Hom}_R(N, N) \longrightarrow 0$$

Prove that the original short exact sequence is split.

It's not very clear from the question statement, but the short exact sequence

$$\mathrm{Hom}_R(N, L) \hookrightarrow \mathrm{Hom}_R(N, M) \twoheadrightarrow \mathrm{Hom}_R(N, N)$$

isn't just any short exact sequence, but must be *the* short exact sequence induced by the functor $\mathrm{Hom}_R(N, -)$ from the short exact sequence $L \hookrightarrow M \twoheadrightarrow N$. This is necessary.

Since $\mathrm{Hom}_R(N, M) \twoheadrightarrow \mathrm{Hom}_R(N, N)$ is surjective, there is some $\varphi \in \mathrm{Hom}_R(N, M)$ that maps to the identity on N. This φ is the splitting map $N \to M$. Showing this in more detail would require naming more maps, and I don't want to.

Mock Algebra Qualifier 2019 - Part C

Do 4 out of the 5 problems.

(1) Prove or disprove the following: If $K \to F$ is an extension (not necessarily Galois) with $[F : K] = 6$ and $\mathrm{Aut}_K(F)$ isomorphic to the Symmetric group S_3, then F is the splitting field of an irreducible cubic in $K[x]$.

Let E be the fixed field of $\mathrm{Aut}_K(F)$. So $E \to F$ is Galois and has degree $|\mathrm{Aut}_K(F)| = |S_3| = 6$. But since $[F : K] = 6$ and E is an intermediate field, we must have that $E = K$, so $K \to F$ is Galois. Now look at the subgroup $\langle(1\,2)\rangle$ in S_3, and let L be the intermediate field of $K \to F$ Since $\langle(1\,2)\rangle$ is an index 3 subgroup, $[L : K] = 3$, and so $L = K(a)$ for any $a \in L \setminus K$ (because there's no room for $K(a)$ be an intermediate extension). So a is the root of some irreducible cubic f over K, but since $\langle(1\,2)\rangle$ is not a normal subgroup of S_3, there is some automorphism of $\mathrm{Aut}_K(F)$ that sends a to some other root of f outside of L. In particular, L doesn't contain all the roots of f, so you've got to go up to F to get all the roots, and so F is the splitting field of f.

(2) Let $f = x^3 - x + 1 \in \boldsymbol{F}_3[x]$. Show that f is irreducible over $\boldsymbol{F}_3$. Let K be the splitting field of f over $\boldsymbol{F}_3$. Compute the degree $[K : \boldsymbol{F}_3]$ and the number of elements of K.

Since f is a cubic polynomial, if it's reducible it'll have a linear factor, which means it'll have a root. But checking each element of $\boldsymbol{F}_3$ yields no root, so it's irreducible over $\boldsymbol{F}_3$. Let $a \in K$ be a root of f. Doing some good ol' fashion long division we see that

$$x^3 - x + 1 \big/ (x-a) = \big(x - (a+1)\big)\big(x - (a-1)\big) .$$

So *all* the roots of f are in $K = \boldsymbol{F}_3(a)$, and it'll be a simple extension of degree 3, and so K has $3^3 = 27$ elements.

(3) Let $K \subseteq F$ be a finite dimensional extension.

(a) Define what it means for F to be separable over K.

(b) Prove from scratch that if K is a finite field then F is separable over K.

(c) Prove that if K is of characteristic zero then F is separable over K.

(d) Given an example of a non-separable finite dimensional extension.

Solution from Derek Lowenberg

(a) Let F/K be a field extension, and $\alpha \in F$. Then α is separable over K if it is algebraic over K and its minimal polynomial is separable, that is, it may be factored into distinct linear factors over an algebraic closure of F. The extension is separable if F is generated over K by separable elements.

(b) We want to show that if F/K is a finite extension of a finite field, then it is separable. Suppose that K is a finite field (of characteristic p), so that $K \cong F_{p^n}$ for some n, and F is a finite extension of K, so that $F \cong F_{p^{nm}}$ for some m, say $F \cong F_{p^k}$. Then F is the splitting field over K of the polynomial $f(x) = x^{p^k} - x$.

Since the multiplicative group of F_{p^k} has $p^k - 1$ elements, for any $b \in F_{p^k} \setminus \{0\}$ we have $b^{p^k-1} = 1$, or $b^{p^k} - b = 0$, so every element of F_{p^k} is a root of $f(x) = x^{p^k} - x$, and all p^k of its roots are in F. Given this bijection between roots of f and elements of F, one sees that f has no repeated roots. For any $a \in F$, the minimal polynomial of a over K must divide f, since $f \in K[x]$, and therefore it has no repeated roots. Hence F/K is separable.

(c) Let F/K be an algebraic extension of a field of characteristic 0. We want to show that this extension is separable.

First we'll show that if a polynomial $p \in K[x]$ is relatively prime to its formal derivative p' in $K[x]$ then p is separable (the converse is also true). Arguing by contrapositive, suppose p has a repeated root a in some splitting field L over K. Then $p(x) = (x-a)^2 q(x)$ for some $q(x) \in L[x]$ and by the product rule $p'(x) = (x-a)^2 q'(x) + 2(x-a)q(x)$ so that a is also a root of $p'(x)$. Therefore the minimal polynomial of a over K divides both p and p', showing that they are not relatively prime.

Now let $b \in F$ and let $f \in K[x]$ be its minimal polynomial. If f is not separable then it has a common factor with f', but since f is irreducible we must have that f divides f'. However, f' has strictly lower degree than f, implying that $f' = 0$. Thus if $f' \neq 0$ then f is separable (the converse is also true, for an irreducible polynomial). This is always true when $f \in K[x]$ where K has characteristic 0 and f is nonconstant, which is the case. Hence F/K is separable.

(d) We want to exhibit an inseparable, finite dimensional field extension. Let p be a prime and let $K = F_p(y)$, the field of rational functions in the variable y over F_p. Consider $f(x) = x^p - y$ in $K[x]$. This polynomial is irreducible by the Eisenstein criterion: all non-leading coefficients are in the prime ideal (y), the constant term is not in (y^2), and the coefficient of the leading term is not in (y). If a is a root of f in some extension of F, then $a^p = y$, so $x^p - y = x^p - a^p = (x-a)^p$ hence f is inseparable. Therefore the finite-dimensional extension $K(a)/K$ is inseparable.

(4) Let F_{12} be a cyclotomic extension of $\mathbb{Q}$ of order 12. Determine $\mathrm{Aut}_{\mathbb{Q}}(F_{12})$ and all intermediate fields.

Solution from Derek Lowenberg

Lemma 2 — $\mathrm{Aut}(\mathbb{Q}(z)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$, the group of units of $\mathbb{Z}/n$, where z is a primitive n^{th} root of unity.

Proof First, for any n^{th} root of unity y and any $\sigma \in \mathrm{Aut}(\mathbb{Q}(z)/\mathbb{Q})$ there is an integer a which is relatively prime to n such that $\sigma(y) = y^a$. This follows because for any primitive root of unity, z, we have $\sigma(z)^n = 1$ and $\sigma(z)^j \neq 1$ for any $1 \leq j < n$, so $\sigma(z)$ is indeed a primitive n^{th} root of unity and hence can be written z^a where $\gcd(a,n) = 1$. Then since $y = z^k$ for some integer k, we have $\sigma(y) = \sigma(z^k) = \sigma(z)^k = z^{ak} = (z^k)^a = y^a$. This integer a is determined modulo n by σ, and indeed the map $\sigma \mapsto a \bmod (n)$ gives an injective group homomorphism $\mathrm{Aut}(\mathbb{Q}(z)/\mathbb{Q}) \to (\mathbb{Z}/n)^\times$. To verify this, let $\sigma, \tau \in \mathrm{Aut}(\mathbb{Q}(z)/\mathbb{Q})$, with $\sigma \mapsto a$, $\tau \mapsto b$ and $\sigma\tau \mapsto c$, then for a primitive root of unity $z^c = \sigma\tau(z) = \sigma(z^b) = z^{ab}$ so $ab = c \bmod (n)$. If σ is in the kernel of this homomorphism, then $\sigma \mapsto 1 \bmod (n)$, so $\sigma(z) = z$. Since σ also fixes $\mathbb{Q}$, it is the identity in $\mathrm{Aut}(\mathbb{Q}(z)/\mathbb{Q})$.

To show this map $\mathrm{Aut}(\mathbb{Q}(z)/\mathbb{Q}) \to (\mathbb{Z}/n)^\times$ is a surjection, we'll show that for any integer a with $\gcd(a, n) = 1$ that z and z^a are $\mathbb{Q}$-conjugate, that is, they have the same minimal polynomial over $\mathbb{Q}$. Since the size of $\mathrm{Aut}(\mathbb{Q}(z)/\mathbb{Q})$ is the number of $\mathbb{Q}$-conjugates of z, this will show surjectivity. To show this it suffices to show that for any prime p not dividing n that z and z^p have the same minimal polynomial, denoted $f(T)$ and $g(T)$ respectively. Suppose towards a contradiction that $g(T) \neq f(T)$.

By Gauss' lemma, any monic factor of $T^n - 1$ in $\mathbb{Q}[T]$ is in $\mathbb{Z}[T]$. To see this, suppose $T^n - 1 = f(T)p(T)$. Since f is monic, so is p. By letting a be the lcm of all the denominators of the (non-leading) coefficients of $f(T)$ and setting $F(T) = af(T)$, and similarly setting $P(T) = bp(T)$ for the corresponding lcm b of denominators of p, we have $ab(X^n - 1) = F(T)P(T)$ where now $F(T), P(T) \in \mathbb{Z}[T]$. Gauss' lemma states that the content of the left-hand side is the product of the contents of $F(T)$ and $P(T)$, up to multiplication by a unit. But the gcd of $m = \mathrm{lcm}(a_1, \ldots, a_r)$, $m/a_1, \ldots, m/a_r$ must be 1, by the definition of a least common multiple. So $F(T)$ and $P(T)$ have content 1, while the content of the left-hand side is ab, which is a contradiction unless both a and b are 1, implying $f(T) \in \mathbb{Z}[T]$.

Then we have $T^n - 1 = f(T)g(T)h(T)$ for a monic $h(T) \in \mathbb{Z}[T]$ (again by Gauss' lemma). Now reduce this equation modulo p to obtain $T^n - \overline{1} = \overline{f}(T)\overline{g}(T)\overline{h}(T)$. Since p does not divide n, $T^n - \overline{1}$ is separable in $F_p[T]$ hence $\overline{f}(T)$ and $\overline{g}(T)$ are relatively prime in $F_p[T]$. Since f and g are monic, their reductions have the same degree and in particular are non constant. Now $g(z^p) = 0$, so $g(T^p)$ also has z as a root, hence $f(T)$ divides $g(T^p)$ in $\mathbb{Q}[T]$. Write $g(T^p) = f(T)k(T)$ for $k(T)$ a monic polynomial in $\mathbb{Q}[T]$. Again by Gauss' lemma, in fact $k(T) \in \mathbb{Z}[T]$. Now reduce this equation modulo p to get $\overline{g}(T^p) = \overline{g}(T)^p = \overline{f}(T)\overline{k}[T]$ in $F_p[T]$. Finally we see that any irreducible factor of $\overline{f}(T)$ is also a factor of $\overline{g}(T)$, contradicting that they are relatively prime in $F_p[T]$. Hence $g(T) = f(T)$. $\square$

(The above proof would most likely not be required for this question on a qual. But it might come in handy, who knows?)

In particular, $\mathrm{Aut}(F/\mathbb{Q}) \cong (\mathbb{Z}/12)^{\times} \cong \langle 5, 11 \rangle$, where 5 and 11 each have order 2, and $5 \times 11 = 7 \mod (12)$ has order 2, hence $\mathrm{Aut}(F/\mathbb{Q}) \cong (\mathbb{Z}/2)^2$, which has 3 subgroups of order 2. Under the Galois correspondence, this gives us 3 intermediate field extensions of dimension 2 over $\mathbb{Q}$ (quadratic extensions). Since F contains all third and fourth primitive roots of unity, it contains $\frac{1+i\sqrt{3}}{2}$ and i. Thus two of the intermediate quadratic extensions are $\mathbb{Q}(i)$ and $\mathbb{Q}(i\sqrt{3})$, and we see $\sqrt{3} \in F$, so that the third quadratic extension is $\mathbb{Q}(\sqrt{3})$.

Mike:

Another way to think about that last paragraph: Letting ζ be a primitive 12th root of unity, the Galois group of $\mathbf{Q}(\zeta)$ will be the multiplicative group of $\mathbf{Z}_{12}$, which contains $\{1, 5, 7, 11\}$. So $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}(\zeta))$ has order four, and each of $1, 5, 7, 11$ has order two, so it's $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. Now since $\zeta = \frac{\sqrt{3}+\mathfrak{i}}{2} \in \mathbf{C}$, and $\zeta^3 = \mathfrak{i}$, we have that both $\mathfrak{i}$ and $\sqrt{3}$ are in $\mathbf{Q}(\zeta)$, and so the intermediate fields of $\mathbf{Q} \to \mathbf{Q}(\zeta)$ are $\mathbf{Q}(\mathfrak{i})$, $\mathbf{Q}(\sqrt{3})$, and $\mathbf{Q}(\mathfrak{i}\sqrt{3})$.

(5) Let $F = \mathbb{C}(t^4) \subset K = \mathbb{C}(t)$, where t is a formal variable. Compute the Galois group $\mathrm{Aut}_F(K)$, and determine its subgroups and corresponding intermediate fields.

First notice that $L = F(t)$. Consider the polynomial $x^4 - t^4 \in F[x]$. Note that t is a root of this degree-4 polynomial, which makes L and algebraic extension so $[L : F] \le 4$ and so $|\operatorname{Gal}(L/F)| \le 4$. Take σ such that $\sigma \colon t \mapsto \mathfrak{i}t$. This σ is an automorphism of L, and since $\sigma(t^4) = \sigma(t)^4 = (\mathfrak{i}t)^4 = t^4$, σ fixes F and is in $\operatorname{Gal}(L/F)$. Now since $\sigma^4(t) = \sigma^3(\mathfrak{i}t) = \sigma^2(-t) = \sigma(-\mathfrak{i}t) = t$, σ has order four in $\operatorname{Gal}(L/F)$ and we can see that $\operatorname{Gal}(L/F) \cong \mathbf{Z}/4\mathbf{Z} = \langle \sigma \rangle$.

Now $\mathbf{Z}/4\mathbf{Z}$ has only a single proper, nontrivial subgroup. That subgroup is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and is generated by σ^2. Since $\mathbf{C}(t^2)$ is properly an intermediate field of $F \subset L$, it must correspond to this subgroup.