Fall 2012
Algebra Qualfying Exam Solutions

Hannah Hoganson, Allechar Serrano

July 21, 2016

1. Suppose G is a group acting on a finite set S. Prove that there exists an element $\sigma \in G$ such that $\sigma(s) \neq s$ for all $s \in S$.

   Solution 1: Recall that we say a group G acts *transitively* on a set S if for every pair of elements $s, t \in S$ there is an element $g \in G$ such that $g \cdot s = t$. If $h \in \mathrm{Stab}(s)$ then $ghg^{-1}(t) = gh(s) = g(s) = t$, so all the stabilizer groups are conjugate.

   Now, assume G is finite and the claim is false; i.e. every element $g \in G$ has a fixed point. That is, for all $g \in G$, $g \in \cup_{s \in S} \mathrm{Stab}(s)$. Then using that the stabilizer groups are conjugate we get

   $$G = \bigcup_{s \in S} \mathrm{Stab}(s) = \bigcup_{g \in G} g\,\mathrm{Stab}(s)g^{-1}$$

   But, a finite group can not be the union of conjugates of a proper subgroup, contradiction.

   Proof of last claim: Say $H < G$, $H \neq G$ and $|G| = m|H|$. Then there are at most m distinct conjugate subgroups of H all containing the identity, so

   $$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq m(|H| - 1) + 1 = m|H| - (m - 1) < m|H| = |G|$$

   G infinite: Because S is a finite set there are only finitely many permutations of S, so there are only finitely many different ways elements from G can act on S. So, we can find $H \leq S_{|S|}$, a subgroup of the symmetric group on $|S|$ elements, and a surjective homomorphism $\varphi : G \twoheadrightarrow H$ such that

   $$g \cdot x = \varphi(g) \cdot x$$

for all $g \in G$ and all $x \in S$. Now we have a transitive action of a finite group on S and so there is an element with no fixed point, and thus an element in G with no fixed point.

Solution 2: We know that σ has a fixed point if and only if $\sigma \in \cup_{s\in S}\text{Stab}_G(s)$. We also know that the stabilizers of two elements in the same orbit are conjugate. Since the action is transitive, then the set of elements in G fixing some point in S is $\cup_{s\in S}\text{Stab}_G(s) = \cup_{\sigma\in G}\sigma\text{Stab}_G(s_0)\sigma^{-1}$, where s_0 is fixed. This set cannot be equal to G since $\text{Stab}_G(s_0) \leqslant G$ has finite index $|S|$ by Orbit-Stabilizer theorem. Since, $\cup_{s\in S}\text{Stab}_G(s)$ has at most $(|\text{Stab}_G(s)| - 1)|S| + 1$, there exists σ such that $\sigma(s) \neq s$ for all $s \in S$.

2. Let S^1 be the circle group, i.e., the group of all complex numbers of norm 1 with multiplication. If A is a finite abelian group, define the dual group $\hat{A}$ to be the multiplicative group of all group homomorphisms $A \to S^1$. Prove that $A \cong \hat{A}$.

   Solution: Since A is a finite abelian group, we can write $A = \langle x_1\rangle \times \cdots \times \langle x_k\rangle$ for a set $x_1, \ldots, x_k$ of generators of A. Let $n_j = |\langle x_j\rangle|$. Consider the character $\chi_j(x_l)$ which is either equal to $e^{\frac{2\pi i}{n_j}}$, if $j = l$, or 1, otherwise. Consider $\varphi \in \text{Hom}(A, S^1)$. We can write $\varphi(x_1^{r_1}\cdots x_k^{r_k}) = \varphi(x_1)^{r_1}\cdots\varphi(x_k)^{r_k} = \chi_1(x_1)^{r_1 m_1}\cdots\chi_k(x_k)^{r_k m_k}$, for some integers m_j. Since $\varphi(x_j)^{n_j} = 1$, then $\varphi(x_j) = (e^{\frac{2\pi i}{n_j}})^{m_j} = \chi_j(x_j)^{n_j}$. So $\hat{A} \cong \langle x_1\rangle \times \cdots \times \langle x_k\rangle \cong A$.

3. Let R be a commutative ring with 1 and $M_n(R)$ the ring of $n \times n$ matrices with coefficients in R. Prove that every ideal of $M_n(R)$ is of the form $M_n(I)$, for some ideal I of R.

   Solution: Let J be an ideal of $M_n(R)$, and I be the set of all $(1,1)$ entries of matrices in J. Then I is an ideal of R. Consider E_{ij} the elementary $(i,j)-$matrix. For a matrix $A = (a_{ij}) \in M_n(R)$, we have $E_{ij}AE_{kl} = a_{jk}E_{il}$. Hence, if $A \in J$, we have that $a_{ij}E_{11} = E_{1i}AE_{j1} \in J$ and $a_{ij} \in I$ for all i, j. Thus, $J \subseteq M_n(R)$. Now, if $r \in I$, then there exists a matrix $C = (c_{ij}) \in J$ such that $r = c_{11}$ and $rE_{ij} = E_{i1}CE_{j1} \in J$ for all i, j. Hence $A = (a_{ij}) \in M_n(I)$ implies $A = \sum_{i,j} a_{ij}E_{ij} \in I$.

4. Met M be a 5×5 matrix with real entries. Suppose M has finite order and $\det(M - I_5) \neq 0$. Find $\det(M)$.

Solution: Suppose M has order k, then $\det(M^k) = \det(M)^k = \det(I_5) = 1$ and $\det(M)$ is a root of unity. M has real entries and its complex eigenvalues must come in pairs. Note that 1 is not an eigenvalue since $\det(M - I_5) \neq 0$. So the eigenvalues of M are some copies of -1 and some complex roots of unity that come in conjugate pairs. Since the conjugate of a root of unity is its inverse, the complex eigenvalues cancel out in $\det(M)$. Since 5 is odd, there must be an odd number of -1's, so $\det(M) = -1$.

5. Let φ denote the Frobenius map $x \longmapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Determine the Jordan canonical form (over $\overline{\mathbb{F}}_p$) for φ regarded as an $\mathbb{F}_p-$linear transformation of $\mathbb{F}_p^n$.

   Solution: Since $\mathbb{F}_{p^n}^\times$ is a cyclic group of order $p^n - 1$, we have that $x^{p^n-1} = 1$ for every $x \in \mathbb{F}_{p^n}$. Hence $\varphi^n(x) = x$ for all $x \in \mathbb{F}_{p^n}$, so φ^n is the identity map. Suppose there exists $1 \leqslant k \leqslant n$ such that $\varphi^k = \mathrm{id}$, then $\varphi^k(x) - x = 0$ for all $x \in \mathbb{F}_{p^n}$, but this equation has at most p^k solutions over $\mathbb{F}_{p^n}$ and $|\mathbb{F}_{p^n}| = p^n$. Therefore, $k = n$. Note that $x^n - 1$ is the minimal polynomial of φ since it is zero for every element in $\mathbb{F}_{p^n}$ and must have degree p^n, it is also the characteristic polynomial. The eigenvalues of $x^n - 1$ are the $n-$th roots of unity in $\overline{\mathbb{F}}_p$. Let $n = p^k m$ where $(p, m) = 1$, then the number of $n-$th roots of unity is m and each of these has multiplicity p^k. Since the minimal polynomial and characteristic polynomial are equal, each eigenvalue occurs in exactly one Jordan block. The Jordan form of φ contains m Jordan blocks of size p^k. Each Jordan block J_i is of the form

$$\begin{pmatrix} \zeta^i & 1 & 0 & \dots & 0 & 0 \\ 0 & \zeta^i & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \zeta^i & 1 \\ 0 & 0 & 0 & \dots & 0 & \zeta^i \end{pmatrix}$$

   where ζ is a $m-$th root of unity.

6. Determine the splitting field and the Galois group for the polynomial $x^3 - 2$ over $\mathbb{Q}$.

   Solution 1: Let ω be a third root of unity and $\alpha = \sqrt[3]{2}$. The splitting field of the polynomial is $\mathbb{Q}(\omega, \alpha)$. The roots of the polynomial are $\alpha, \omega\alpha, \omega^2\alpha$ and $|\mathbb{Q}(\alpha, \omega)| = 6$. Consider the automorphisms

$\tau : \alpha \longmapsto \omega\alpha, \omega \longmapsto \omega$ and $sigma : \alpha \longmapsto \alpha, \omega \longmapsto \omega^2$. Since $\tau\sigma \neq \sigma\tau$, the Galois group of the polynomial is S_3.

Solution 2: First note that $f(x) = x^3 - 2$ is irreducible by Eisenstein's criterion. $f(x)$ has roots $\{\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\sqrt[3]{2}, e^{\frac{4\pi i}{3}}\sqrt[3]{2}\}$, so the splitting field of $f(x)$ is $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$. Because f is the minimal polynomial of $\sqrt[3]{2}$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. The minimal polynomial of $e^{\frac{2\pi i}{3}}$ over $\mathbb{Q}(\sqrt[3]{2})$ is $g(x) = x^2 + x + 1$ so $[\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Together we get

$$[\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \cdot 2 = 6$$

So, $\left|\mathrm{Gal}(x^3 - 2)\right| = 6$. We can also see that $\mathbb{Q}(\sqrt[3]{2})$ is an intermediate field which is not Galois; this is because f is the minimal polynomial of $\sqrt[3]{2}$ and f does not split over $\mathbb{Q}(\sqrt[3]{2})$. Hence, the Galois group of f has a non-normal subgroup, so can not be abelian. Thus, $\mathrm{Gal}(x^3 - 2) \cong S_3$.

7. Show that the polynomial $x^4 + 1$ is reducible modulo every prime p.

   Solution If $p = 2$, then $x^4 + 1 = (x + 1)^4$ is reducible. Otherwise, we have $p \equiv 1 \bmod 8$. Then $x^4 + 1 | x^8 - 1 | x^{p^2-1} - 1 | x^{p^2} - x$. If α is a root of $x^4 + 1$, then it is a root of $x^{p^2} - x$. Recall that the solutions of $x^{p^2} - x$ form the field $\mathbb{F}_{p^2}$. Therefore $\mathbb{F}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^2}$. Thus $|\mathbb{F}_p(\alpha) : \mathbb{F}_p| \leqslant 2 \neq 4$, so $x^4 + 1$ is reducible.

8. Let $K \subseteq L$ be fields, and let $f(x)$ be an irreducible polynomial in $K[x]$. If there exists a in L with $f(a) = 0 = f(a^2)$, prove that $f(x)$ splits in $L[x]$.

   Solution: Recall that the Galois group of an irreducible polynomial acts transitively on the roots. So, there is a $\sigma \in \mathrm{Gal}(f)$ with $\sigma(a) = a^2$. Because σ permutes roots of f and $\sigma(a^m) = a^{m^2}$ it must be that $a, a^2, a^4, ..., a^{2^n}$ are all roots of f, where n is such that $a^{2^{n+1}} = a$. Then $a^{2^{n+1}-1} = 1$, so a is a root of unity. Because f is the minimal polynomial of a, f divides $x^k - 1$ for some k and the only possible roots for f are $\{a, a^2, a^3, ..., a^{k-1}\}$, all of which live in L (because $a \in L$), so f splits over $L[x]$.

9. Prove that the $\mathbb{Z}$-module $\mathbb{Q}$ is not projective.

   Solution: Homological algebra was not covered in the 2015-2016 algebra sequence, so we assume this topic will not appear on the August 2016 qualifying exam.

10. Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ as left $\mathbb{Q}$-modules.

    Solution: Tensor products were not covered in the 2015-2016 algebra sequence, so we assume this topic will not appear on the August 2016 qualifying exam.