January 2010
Algebra Qualfying Exam Solutions

Allechar Serrano and Anna Romanova

June 24, 2016

1. Show that for any positive integer n, every element of order 2 in the alternating group A_n is the square of an element of order 4 in the symmetric group S_n.

   Solution: Every element of order 2 in S_n (and in A_n) is a product of commuting transpositions. Let $\sigma \in A_n$ have order 2, then $\sigma = (a_1b_1)(c_1d_1)\dots(a_kb_k)(c_kd_k)$ and note that σ has an even number of transpositions. Note that $(a_ic_ib_id_i)^2 = (a_ib_i)(c_id_i)$, so we can rewrite σ as $\sigma = (a_1c_1b_1d_1)^2 \dots (a_kc_kb_kd_k)^2$ and $|\sigma| = 4$ in S_n.

2. Let G be a finite $p-$group, with $|G| > p$. Prove that the order of $\mathrm{Aut}(G)$ is divisible by p.

   Solution: We know that $|G| = p^n$ for $n \geqslant 2$.
   If G is not abelian. Consider G acting on itself by conjugation φ, then $G/\ker\varphi \cong \mathrm{Inn}(G)$. So $\frac{|G|}{|Z(G)|} = |\mathrm{Inn}(G)|$. Since $|G|$ is a $p-$group, $Z(G)$ is nontrivial. Therefore, p divides $|\mathrm{Inn}(G)|$. Since $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$, then p divides $|\mathrm{Aut}(G)|$.
   If G is abelian, then $G \cong \mathbb{Z}_{p^k} \oplus H$, where $\mathbb{Z}_{p^k}$ is of maximal order. Then $\mathrm{Aut}(G)$ has a subgroup isomorphic to $\mathrm{Aut}(\mathbb{Z}_{p^k})$ and $|\mathrm{Aut}(\mathbb{Z}_{p^k})| = (p-1)p^{k-1}$, so p divides $|\mathrm{Aut}(G)|$ if $k > 1$. If $k = 1$, then $G = \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ and consider $\sigma : \mathbb{Z}_p \oplus \mathbb{Z}_p \to \mathbb{Z}_p \oplus \mathbb{Z}_p$ an morphism in the first two summands of G given by $(0,1) \longmapsto (1,1)$ and $(1,0) \longmapsto (1,0)$ then $|\sigma| = p$ and $\sigma \in \mathrm{Aut}(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ since we can extend σ to an automorphism of G trivially, then p divides $|\mathrm{Aut}(G)|$.

3. Let R be a ring with 1. A left $R-$module is called simple if $M \neq 0$ and if the only submodules of M are M and 0. Show that every simple module is isomorphic to R/I for some maximal left ideal I and that I is unique if R is commutative.

Solution: Let M be simple, since $0 \neq M$ there exists $x \in M$ and $x \neq 0$ such that Rx is a submodule of M. Since M is simple, then $Rx = M$. Let $f : R \to M$ given by $r \longmapsto rx$. We have that $R/\ker f \cong M$ is simple and $\ker f = \mathrm{ann}_R(x)$. Suppose that $\mathrm{ann}_R(x)$ is contained in an ideal J. Then Jx is a submodule of M, so either $Jx = M$ and $J = R$ or $Jx = 0$ and $\mathrm{ann}_R(x) = 0$. Since $\mathrm{ann}_R(x) \cap J = \mathrm{ann}_R(x)$, so $J/\mathrm{ann}_R(x) \cong Jx$ and $\mathrm{ann}_R(x)$ is a maximal ideal.

Assume R is commutative. Let J be a maximal left ideal in R such that $R/J \simeq M$. For any $j \in J$ and $r + J \in R/J$,

$$j \cdot (r + J) = jr + J = rj + J = J$$

since R is commutative. This implies that $J \subseteq \mathrm{ann}_R(M)$. But J is maximal, so $J = \mathrm{ann}_R(M)$. Since $M = Rx$, $\mathrm{ann}_R(M) = \mathrm{ann}_R(x)$. Indeed, any $r \in \mathrm{ann}_R(M)$ has the property that $r \cdot m = 0$ for all $m \in M$. But all $m \in M$ are of the form $m = r'x$ since $M = Rx$, so if $r \in \mathrm{ann}_R(M)$, then $r \cdot r'x = 0$ for all $r' \in R$. In particular, $r \cdot 1x = rx = 0$ so $r \in \mathrm{ann}_R(x)$. Conversely, if $r \in \mathrm{ann}_R(x)$, then $rx = 0$, so for any $r' \in R$, $rr'x = r'rx = 0$ since R is commutative. Therefore, $J = \mathrm{ann}_R(x)$, so I must be unique.

4. In the category of $\mathbb{Z}-$modules, is the module $\mathbb{Q}/\mathbb{Z}$

   (a) projective? It is not projective since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$.

   (b) injective? Since $\mathbb{Q}$ is a divisible $\mathbb{Z}-$ module and $\mathbb{Z}$ is a PID, then $\mathbb{Q}$ is injective.

   (c) flat?

   Solution: This material was not covered in the algebra qualifying exam courses in Fall 2015 - Spring 2016, so we skipped this problem.

5. Let G be a group of order p^2q, where p and q are distinct primes. Show that G has a normal Sylow subgroup.

   Solution: If $p > q$. Since $n_p | q$ and $n_p = 1 + kp$, then $n_p = 1$. So the Sylow $p-$subgroup is normal in G.
   If $p < q$. If $n_q = 1$, then the Sylow $q-$subgroup is normal in G. Suppose $n_q \neq 1$, so $n_q = 1 + kq$ for an integer $k \geqslant 1$. Since $n_q | p^2$, we must have either $n_q = p$ or $n_q = p^2$. Since $p < q$, then $n_q = p^2$. Therefore, there are $p^2(q-1)$ distinct elements in the p^2 Sylow $q-$subgroups. Therefore, there are only p^2 elements of order $\neq q$, then $n_p = 1$ and the Sylow $p-$subgroup is normal in G.

6. Let M be a 5 by 5 matrix with real coefficients such that $M^2 = 2M - I$. Show that the subspace of $\mathbb{R}^5$ consisting of vectors fixed by M has dimension at least 3.

   Solution: Since M satisfies the polynomial equation $x^2 - 2x + 1 = (x-1)^2 = 0$, then its minimal polynomial is either $x - 1$ or $(x-1)^2$. We know that the invariant space associated to the eigenvalue 1 is the subspace consisting of vectors fixed by M. So the dimension of this invariant subspace is equal to the number of blocks in the Jordan canonical form of M. If the minimal polynomial is $x - 1$, then the Jordan form of M has five blocks of size 1, so the dimension of the space fixed by M is 5. If the minimal polynomial is $(x-1)^2$, then the Jordan form of M can have two blocks of size 2 and one block of size 1 or one block of size 2 and three blocks of size 1. Then the dimension of the space fixed by M is 3 or 4, respectively.

7. Let R be a commutative ring with 1. Show that every $R-$module is free if and only if R is a field.

   Solution: Let I be an ideal of R and $I \neq R$. Then R/I is an $R-$module and it is free, so the annihilator of R/I is zero. Since I annihilates R/I, then $I = 0$. So the ideals of R are R and (0), then R is a field.
   If R is a field, and $R-$modules S has a basis $B \subset S$, which defines an isomorphism from the free vector space on B to S.

8. Compute the number of monic irreducible polynomials of degree 3 over the field $\mathbb{Z}_7$.

   Solution: *Claim:* The number of irreducible polynomials of degree p over $\mathbb{F}_q$ is $\frac{q^p - q}{p}$.

   Proof: We have that $[\mathbb{F}_{q^p} : \mathbb{F}_q] = p$, so there are not intermediate subfields. Consider $f(x) = x^{q^p} - x$. Every irreducible polynomial that divides f must have degree p or 1. Since each linear polynomial over $\mathbb{F}_q$ divides f and since f has distinct roots, then we have exactly q different linear polynomials that divide f. Multiplying all the irreducible monic polynomials that divide f will give us f, so summing up their degrees will give us q^p. Let n be the number of irreducible monic polynomials of degree p, then $np + q = q^p$, so $n = \frac{q^p - q}{p}$.

   Now, take $p = 3$ and $\mathbb{F}_q = \mathbb{Z}_7$, then the number of irreducible polynomials of degree 3 over $\mathbb{Z}_7$ is $\frac{7^3 - 7}{3} = \frac{7(49-1)}{3} = 7 \times 16 = 112$.

9. Let F be a field that contains a primitive $n-$th root of unity. Show that if a is an element of F and the field E is obtained from F by adjoining an $n-$th root of a, then E is a Galois extension of F with cyclic Galois group.

   Solution: We have that E is the splitting field of $p(x) = x^n - a$, which is a separable polynomial. Hence $F \subset E$ is Galois. Consider α the $n-$th root of a and ω a primitive $n-$th root of unity, then the roots of p are $\alpha, \omega\alpha, \ldots, \omega^{n-1}\alpha$. Consider the morphism $\sigma_i : \omega^j \alpha \longmapsto \omega^{i+j}\alpha$ of $\operatorname{Gal}(E/F)$, then $|\sigma| = |\operatorname{Gal}(E/F)|$, so σ generates the Galois group.

10. State and prove Hilbert's basis theorem.

    Solution: See Dummit and Foote, Section 9.6, Theorem 21. (p.316)