ALGEBRA PH.D. QUALIFYING EXAM SOLUTIONS

May 20, 2008

A passing paper consists of four problems solved completely plus significant progress on two other problems; moreover, the set of problems solved completely must include one from each of Sections A, B and C.

Section A.

In this section you may quote without proof basic theorems and classifications from group theory and group actions as long as you state clearly what facts you are using.

1. Let G be a *solvable* group of order $168 = 2^3 \cdot 3 \cdot 7$. The aim of this exercise is to show that G has a normal Sylow p-subgroup for some prime p. Let M be a minimal normal subgroup of G.

(a) Show that if M is not a Sylow p-subgroup for any prime p, then $|M| = 2$ or 4.
[You may quote without proof any results you need about minimal normal subgroups of solvable groups.]

(b) Assume $|M| = 2$ or 4, and let $\overline{G} = G/M$. Prove that $\overline{G}$ has a normal Sylow 7-subgroup.

(c) Under the same assumptions and notation as (b), let H be the complete preimage in G of the normal Sylow 7-subgroup of $\overline{G}$. Prove that H has a normal Sylow 7-subgroup, P, and deduce that P is normal in G.

SOLUTION

a. M is an elementary abelian p-group for some prime p, by considering first M' and then M^p for p dividing M. Both are normal subgroups of G smaller than M, so must be trivial. Hence in this case M has order 2,4,8,3, or 7. If M is not a Sylow subgroup, it must have order 2 or 4.

b. When $|M| = 2$ or 4, G/M has order 84 or 42. The number of Sylow 7-subgroups divides 12 and is congruent to 1 mod 7. The only possiblity is a single $\overline{P}_7$, which must therefore be normal in G/M.

c. If H is the preimage in G of $\overline{P}_7$, then $|H| = 14$ or 28 and a Sylow 7-subgroup P_7 of H is normal in H for similar reasons as above. Now P_7 is a Sylow 7-subgroup of G. If P_7' is any other such subgroup of G, we know that its image in G/M is the same as that of P_7, by the uniqueness of the Sylow 7-subgroup there. Hence $P_7' \subset P_7 M = H$. By uniqueness of the Sylow 7-subgroup in H, we have $P_7' = P_7$. We conclude that P_7 is the unique Sylow 7-subgroup in G, and is therefore normal.

2. Let G be a finite group acting transitively (on the left) on a nonempty set Ω. Let $N \trianglelefteq G$, and let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ be the orbits of N acting on Ω. For any $g \in G$ let $g\mathcal{O}_i = \{g\alpha \mid \alpha \in \mathcal{O}_i\}$.

(a) Prove that $g\mathcal{O}_i$ is an orbit of N, for any $i \in \{1, 2, \ldots, r\}$, i.e., $g\mathcal{O}_i = \mathcal{O}_j$ for some j.

(b) Explain why G permutes $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ *transitively* (acting as in part (a)).

(c) Deduce from (b) that $r = |G : NG_\alpha|$, where G_α is the subgroup of G stabilizing the point $\alpha \in \mathcal{O}_1$.

SOLUTION

a. If $\mathcal{O}$ is the N-orbit of ω and $g \in G$, we show that $g\mathcal{O}$ is the N-orbit of $g \cdot \omega$. This is because $\eta \in g\mathcal{O} \iff \eta = g \cdot n\omega$ for some $n \in N \iff \eta = gng^{-1}g \cdot \omega$ for some $n \in N \iff \eta = n'g \cdot \omega$ for some $n' \in N$.

b. If $\mathcal{O}_i$ is the N-orbit of ω_i and $\mathcal{O}_j$ is the N-orbit of ω_j, then there is a $g \in G$ such that $\omega_j = g \cdot \omega_i$, since G acts transitively on Ω. Then from part (a), we see that $g\mathcal{O}_i = \mathcal{O}_j$, so G acts transitively on the N-orbits.

c. By the above, an element $g \in G$, stabilizes $\mathcal{O}_i \iff g \cdot \omega_i = n \cdot \omega_i$ for some $n \in N \iff n^{-1}g \cdot \omega_i = \omega_i$ for some $n \in N \iff n^{-1}g \in G_{\omega_i}$ for some $n \in N \iff g \in nG_{\omega_i}$ for some $n \in N \iff g \in NG_{\omega_i}$. Then since the size of an orbit is the index of the stabilizer, we get $r = |G : NG_{\omega_i}|$

3. Let G be a finite group, let p be a prime and let $P \in Syl_p(G)$. Assume P is abelian.

(a) Prove that two elements of P are conjugate in G if and only if they are conjugate in $N_G(P)$.

(b) Prove that $P \cap gPg^{-1} = 1$ for every $g \in G - N_G(P)$ if and only if $P \trianglelefteq C_G(x)$ for every nonidentity element $x \in P$.

Solution

a. We show that if x lies in P and another Sylow p-subgroup P', then there is an element h in G such that $hxh^{-1} = x$ and $hPh^{-1} = P'$. This is because P and P' are both abelian hence their elements commute with the element x in their intersection, and hence both are contained in the subgroup $C_G(x)$. Applying the Sylow theorem to this subgroup, we get that P and P' are conjugate in $C_G(x)$, and this is exactly our claim. Given two conjugate elements x and $g^{-1}xg$ lying in P, we apply the claim to x in the interesection of P and $P' = gPg^{-1}$. This yields the desired result.

b. Note that P is a subgroup of $C_G(x)$ for $x \in P$, since P is abelian. If $P \cap gPg^{-1} = 1$ for every $g \in G - N_G(P)$, take any nontrivial $x \in P$ and $y \in C_G(x)$. Then $x \in P$ and $x = y^{-1}xy \in P$. So $1 \neq x \in P \cap yPy^{-1}$. By our assumption, this implies $y \in N_G(P)$. We conclude that $C_G(x) \subset N_G(P)$, and consequently P is normal in $C_G(x)$. Conversely suppose that P is normal in $C_G(x)$ for every $x \in P$. Take any $g \in G - N_G(P)$. If $1 \neq x \in P \cap gPg^{-1}$, then $x = gx'g^{-1}$ for $x' \in P$. Using part (a), x and x' are conjugate in $N_G(P)$, so $x = nx'n^{-1}$ for some $n \in N_G(P)$. Then x commutes with ng^{-1}, so $ng^{-1} \in C_G(X)$. Our assumption gives that $ng^{-1} \in N_G(P)$. But $n \in N_G(P)$, and we may conclude that g^{-1}, and hence $g \in N_G(P)$. This contradicts the assumption on g. Hence no such x exists: we must have $P \cap gPg^{-1} = 1$, as desired.

Section B.

4. Let $F_1, F_2, \ldots, F_n$ be fields.

(a) Explicitly describe all the ideals in the direct product ring $F_1 \times F_2 \times \cdots \times F_n$. (Explain briefly why your list is complete.)

(b) Which of the ideals in (a) are prime? (Justify.)

(c) Which of the ideals in (a) are maximal? (Justify.)

Solution

a. Let e_i be the idempotent whose ith component is 1 and whose other components are 0. The sum of these is the identity in the direct product ring. So if I is an ideal of the direct product, we see that I is the direct product of the $I_i = e_iI$, each of which is an ideal in

F_i, hence is either F_i or 0. It is also clear that such a direct product is an ideal. So there are 2^n ideals: each may be described uniquely as direct sum of $\epsilon_i F_i$, where each ϵ_i may be 0 or 1.

b. An ideal is prime if and only if the associated quotient ring is an integral domain. Since $(F_1 \times F_2 \times \cdots \times F_n)/(e_1F_1 \times e_2F_2 \times \cdots \times e_nF_n) \cong (1-e_1)F_1 \times (1-e_2)F_2 \times \cdots \times (1-e_n)F_n$, we see that this quotient will have zero divisors and hence is not an integral domain if there are two nonzero summands. If there is only one nonzero summand, it is a field, and hence an integral domain. Thus there are n prime ideals, each of which is a direct product of $n-1$ of the fields F_i.

c. The solution to (b) shows that the prime ideals are the same as the maximal ideals, for which the corresponding quotient is a field.

5. Let R be an integral domain and assume R contains a subring F that is a field (R and F have the same 1). Prove that if R is finite dimensional as a vector space over F then R is a field.

SOLUTION

We show that an arbitrary non-zero element $r \in R$ has an inverse. Let n be the dimension of R as an F-vector space. Then $1, r, r^2, \ldots r^n$ must be F-linearly dependent. We can use the fact that R is an integral domain and repeatedly factor r out of the dependence relation to arrive at a dependence relation involving 1. Solving for 1 in this dependence relation then shows that 1 is a multiple of r. In other words, r is a unit, as desired.

6. Let R be a commutative ring with 1 and let A, B and C be left R-modules. Prove that $\mathrm{Hom}_R(A, B \oplus C) \cong \mathrm{Hom}_R(A, B) \oplus \mathrm{Hom}_R(A, C)$, where this is an isomorphism of R-modules.

SOLUTION

The isomorphism is given by sending φ to $(\pi_B \circ \varphi, \pi_C \circ \varphi)$. One can check that the inverse is obtained by sending (ψ_1, ψ_2) to $(\psi_1 \oplus \psi_2) \circ \triangle$, where $\triangle\ (a) = (a, a) \in A \oplus A$.

7. (a) How many similarity classes of 8×8 matrices A with rational number entries are there that satisfy $A^8 = I$ but $A^n \neq I$ for every $n \in \{1, \ldots, 7\}$? (Justify.)

(b) Answer the same question as in part (a) but with the field of rational numbers replaced by the field $\mathbb{F}_2$ with 2 elements. (Justify.)

SOLUTION

a. Given that $A^8 = I$, we have that $A^n = I$ if and only if $A^{gcd(8,n)} = I$. So the information is equivalent to the statement that the minimimal polynomial of A divides $x^8 - 1$ but does not divide $x^4 - 1$. According to the theory of cyclotomic polynomials, $x^8 - 1$ factors into irreducibles x^4+1, x^2+1, $x+1$, and $x-1$. The minimal polynomial $m_A(x)$ of A is then a multiple of x^4+1. There are 8 such possibilities which divide x^8-1, one for each subset of the remaining 3 irreducible factors. Using rational canonical form, A is similar to a unique matrix of blocks of companion matrices for polynomials, each dividing the next in such a way that the product is degree 8 and the last is $m_A(x)$. In each case one finds that the divisibility and degree criteria allow only one possibility for each of the 8 choices of $m_A(x)$, except when $m_A(x) = (x^4+1)(x+1)(x-1)$, in which case there may be two preceding invariant factors both equal to $(x+1)$ or both equal to $(x-1)$; or there may be a single preceding invariant factor equal to $(x+1)(x-1)$. This gives a total of 10 possibilities.

b. Here the minimal polynomial of A divides $(x-1)^8$, but not $(x-1)^4$. Thus it may be

$(x-1)^k$ for $k = 5, 6, 7, 8$. The first leads to 3 options, the second to 2, and each of the others to 1. The total is 7.

Section C.

8. Let E be the splitting field in $\mathbb{C}$ of the polynomial $p(x) = x^6 + 3x^3 + 3$ over $\mathbb{Q}$, and let α be any root of $p(x)$ in E.

(a) Find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

(b) Show that $\alpha^3 + 1 = \omega$ is a primitive cube root of unity. Describe the roots of $p(x)$ in terms of radicals involving rational numbers and ω.

(c) Assume $E \neq \mathbb{Q}(\alpha)$, and prove $[E : \mathbb{Q}] = 18$.
[Hint: Show first that $\mathbb{Q}(\beta)$ is a Galois extension of $\mathbb{Q}(\omega)$ of degree 3, for every root β of $p(x)$.]

(d) Again assume $E \neq \mathbb{Q}(\alpha)$, and prove that E contains a *unique* subfield F with $[F : \mathbb{Q}] = 2$.

Solution

a. The polynomial is irreducible by the Eisenstein criterion. Thus $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(p(x))$ and is of degree 6 over $\mathbb{Q}$.

b. Using $p(\alpha) = 0$, one obtains that $\omega^2 = (\alpha^3+1)^2 = \alpha^6 + 2\alpha^3 + 1 = -3\alpha^3 - 3 + 2\alpha^3 + 1 = -\alpha^3 - 2 = -\omega - 1$. So $\omega^2 + \omega + 1 = 0$, and ω satisfies the 3rd cyclotomic polynomial $x^2 + x + 1$. Thus ω is a primitive cube root of unity.

c. The field $\mathbb{Q}(\omega)$ is of degree 2 over $\mathbb{Q}$ as the 3rd cyclotomic polynomial is irreducible of degree 2. It contains all primitive cube roots of unity. By multiplicativity of degrees in towers, we must have $[\mathbb{Q}(\alpha) : \mathbb{Q}(\omega)] = 3$. Note that α is a cube root of $\omega - 1 \in \mathbb{Q}(\omega)$, so that $\mathbb{Q}(\alpha)/\mathbb{Q}(\omega)$ is a Kummer extension. Hence it is Galois (necessarily with cyclic Galois group of order 3). Since α is any root of $p(x)$, the same goes for any other root β.

Assuming $E \neq \mathbb{Q}(\alpha)$, there must be some other root $\beta \notin \mathbb{Q}(\alpha)$. We then have $\mathbb{Q}(\beta) \neq \mathbb{Q}(\alpha)$ both of degree 3 over $\mathbb{Q}(\omega)$. The intersection is of degree dividing 3 and strictly less than 3 over $\mathbb{Q}(\omega)$. Since 3 is prime, the degree must be 1 and the intersection equals $\mathbb{Q}(\omega)$. Since both extensions are Galois, we may apply the theorem of Natural Irrationalities to conclude that $\mathbb{Q}(\alpha, \beta)$ is of degree 9 over $\mathbb{Q}(\omega)$ (indeed with Galois group equal to an elementary 3-group of order 9). Again by multiplicativity of degrees in towers, this makes $\mathbb{Q}(\alpha, \beta)$ of degree 18 over $\mathbb{Q}$. Clearly E contains $\mathbb{Q}(\alpha, \beta)$. If this is not the splitting field of $p(x)$, there is yet another root γ, not lying in $\mathbb{Q}(\alpha, \beta)$. But we know $\mathbb{Q}(\gamma)$ is also degree 3 over $\mathbb{Q}(\omega)$, and the same theorem would yield that $\mathbb{Q}(\alpha, \beta, \gamma)$ is of degree 54 over $\mathbb{Q}$. Then $[E : \mathbb{Q}]$ would be a multiple of 54. However, the splitting field of a polynomial of degree 6 must be of degree dividing 6!, so this degree cannot be a multiple of 54. Hence $E = \mathbb{Q}(\alpha, \beta)$ of degree 18 over $\mathbb{Q}$.

d. First $E/\mathbb{Q}$ is Galois as it is a splitting field. By the Fundamental Theorem of Galois theory, intermediate fields of degree 2 over $\mathbb{Q}$ correspond to subgroups of index two in the Galois group G of order 18. Such a subgroup must be of order 9, and hence a Sylow 3-subgroup of G. The number n_3 of such subgroups must divide 2 and be congruent to 1 modulo 3. Hence $n_3 = 1$, and there is only 1 such subgroup. This makes the quadratic extension of $\mathbb{Q}$ in E unique.

9. Let K/F be an extension of odd degree, where F is any field of characteristic 0.

(a) Let $a \in F$ and assume the polynomial $x^2 - a$ is irreducible over F. Prove that $x^2 - a$ is also irreducible over K.

(b) Assume further that K is Galois over F. Let $\alpha \in K$ and let E be the Galois closure of $K(\sqrt{\alpha})$ over F. Prove that $[E : F] = 2^r[K : F]$ for some $r \geq 0$.

SOLUTION

a. Since $x^2 - a$ is irreducible, any field containing a root must contain the splitting field of degree 2, and hence must have even degree of F. Thus there is no root in K. This implies that $x^2 - a$ is irreducible over K, as a nontrivial factor would be of degree 1, implying the existence of a root.

b. You may take E to be the field generated by K together with all elements that are Galois conjugates over F of β, where $\pm\beta$ are the roots of $x^2 - \alpha$. Note that a Galois conjugate $\sigma(\beta)$ is a root of $x^2 - \sigma(\alpha)$, with $\sigma(\alpha) \in K$, since K/F is Galois. Thus each conjugate $\sigma(\beta)$ lies in a quadratic extension of K. Thus E is a composite of quadratic extensions of K, and is therefore of degree a power of 2. The argument is as in the last problem, with 3 replaced by 2.

10. Let p be a prime, let $F = \mathbb{F}_p$ be the field of order p, and let $\overline{F}$ be an algebraic closure of F. Let n be a positive integer relatively prime to p and let F_n be the splitting field of the polynomial $f_n(X)$ in $\overline{F}$, where

$$f_n(X) = X^n - 1.$$

(a) Explain briefly why $[F_n : F]$ is equal to the order of p in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. [Quote without proof basic facts you need about finite fields.]

(b) If n and m are relatively prime and neither is divisible by p, is $F_{nm} = F_nF_m$? (Justify briefly.)

SOLUTION

a. By the derivative test and the fact that p does not divide n, we see that $f_n(x)$ has no repeated roots. Thus it has n distinct roots in $\overline{F}$. The roots form an abelian group of nth roots of 1. This group must be cyclic, as it is a subgroup of the multiplicative group of a field. Thus there is a primitive nth root ω which generates all others. Thus the splitting field F_n of $f_n(x)$ is the smallest field extension in which $f_n(x)$ contains a primitive nth root of unity, that is, an element of order n. The unique field extension of degree m is $\mathbb{F}_{p^m}$, so F_n is obtained when m is the smallest positive integer for which $\mathbb{F}_{p^m}^\times$ contains an element of order n. Since $\mathbb{F}_{p^m}^\times$ is cyclic of order $p^m - 1$, m is the smallest integer for which n divides $p^m - 1$. Equivalently, m is the smallest positive integer for which $p^m \equiv 1 \pmod{n}$. In other words, m is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.

b. Yes, part (a) shows that F_n is the smallest finite field of characteristic p containing a primitive nth root of unity. When n, m, and p are pairwise relatively prime, $\mathbb{F}_{p^t}$ contains a primitive nmth root of unity if and only if it contains an nth root and an mth root of unity. The field F_{nm} is the smallest finite field of characteristic p containing the former, and F_nF_m is the smallest containing the latter, so they are identical.