ALGEBRA PH.D. QUALIFYING EXAM

September 27, 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 p and q be distinct primes and let G be a group of order p^3q.

(a) Show that if $p > q$ then a Sylow p-subgroup of G is normal in G.

(b) Assume G has more than one Sylow p-subgroup. Show that if the intersection of any pair of distinct Sylow p-subgroups is the identity, then G has a normal Sylow q-subgroup.

(c) Assume the Sylow p-subgroups of G are abelian. Show that G is not a simple group. (Do not quote Burnside's p^aq^b-Theorem.)

Solution: (a): By Sylow's Theorem the number of Sylow p-subgroups, n_p, is congruent to 1 (mod p) and divides q, hence is equal to 1 or q. If $p > q$ the congruence condition forces $n_p = 1$.

(b): As in (a), if $n_p > 1$ then $n_p = q$. In this case each Sylow p-subgroup contains $p^3 - 1$ nonidentity elements. By hypothesis distinct Sylow p-subgroups have no nonidentity elements in common, so the number of nonidentity elements in all Sylow p-subgroups is $(p^3 - 1)q$. Only q elements remain, and since a Sylow q-subgroup has q elements, there must be a unique, hence normal, Sylow q-subgroup.

(c): Assume G is simple. Thus $n_p > 1$, $n_q > 1$ and, by (b), there are distinct Sylow p-subgroups P_1, P_2 such that $H = P_1 \cap P_2 \neq 1$. Let $N = N_G(H)$. Since P_i is abelian $H \trianglelefteq P_i$, i.e., $P_i \leq N$ for $i = 1, 2$. Since N contains more than one Sylow p-subgroup, it is not a p-group. Order considerations force $N = G$, i.e., $H \trianglelefteq G$, contrary to the assumed simplicity of G.

Note that all arguments hold when p^3 is replaced by an arbitrary power of p.

2. Let G be a finite group acting transitively (on the left) on a nonempty set Ω. For $\omega \in \Omega$ let G_ω be the usual stabilizer of the point ω:

$$G_\omega = \{g \in G \mid g\omega = \omega\}$$

where $g\omega$ denotes the action of the group element g on the point ω.

(a) Prove that $hG_\omega h^{-1} = G_{h\omega}$, for every $h \in G$.

(b) Assume G is *abelian*. Let N be the kernel of the transitive action. Prove that $N = G_\omega$ for every $\omega \in \Omega$, and deduce that $|G : N| = |\Omega|$.

Solution: (a): To show $hG_\omega h^{-1} \leq G_{h\omega}$ consider an arbitrary element $hgh^{-1} \in hG_\omega h^{-1}$, where $g \in G_\omega$. This group element fixes the set element $h\omega$ because, by the axioms of a group action,

$$(hgh^{-1})(h\omega) = hg(h^{-1}h)\omega = hg\omega = h\omega,$$

where the last equality holds because $g \in G_\omega$. This proves the containment $hG_\omega h^{-1} \leq G_{h\omega}$. The reverse containment holds by applying this containment with h^{-1} in place of h and $h\omega$ in place of ω (or because these two finite subgroups have the same order, hence coincide).

(b): By definition of the kernel of an action, N is the subgroup of G that fixes every point, i.e.,

$$N = \bigcap_{\omega \in \Omega} G_\omega. \tag{2.1}$$

Fix some $\alpha \in \Omega$. For any $\omega \in \Omega$, the transitive action gives that $\omega = h\alpha$ for some $h \in G$. By (a) therefore $G_\omega = hG_\alpha h^{-1}$. Since G is assumed to be abelian, $hG_\alpha h^{-1} = G_\alpha$. Putting these together: every term in the intersection (2.1) is equal to G_α, whence $N = G_\alpha$. Finally, by the transitive action and usual results on group actions, $|\Omega| = |G : G_\alpha| = |G : N|$, as desired.

3. Let N be a normal subgroup of the group G and for each $g \in G$ let ϕ_g denote conjugation by g acting on N, i.e.,

$$\phi_g(x) = gxg^{-1} \qquad \text{for all } x \in N.$$

(a) Prove that ϕ_g is an automorphism of N for each $g \in G$.

(b) Prove that the map $\Phi : g \mapsto \phi_g$ is a homomorphism from G into $\mathrm{Aut}(N)$, where $\mathrm{Aut}(N)$ is the automorphism group of N.

(c) Prove that $\ker \Phi = C_G(N)$ and deduce that $G/C_G(N)$ is isomorphic to a subgroup of $\mathrm{Aut}(N)$.

Solution: (a): Since N is normal, ϕ_g maps N to itself. It is a homomorphism because $\phi_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y)$. Finally, one checks by direct computation that ϕ_g has the 2-sided inverse $\phi_{g^{-1}}$, hence is an automorphism. (Or, by (b) we have $\phi_g \circ \phi_{g^{-1}} = \phi_1 = id$.)

(b): By applying both sides to an arbitrary element $x \in N$ one checks directly that $\phi_g \circ \phi_h = \phi_{gh}$. This shows $\Phi(g)\Phi(h) = \Phi(gh)$, as needed for (b).

(c): Now $\ker \Phi = \{g \in G \mid \phi_g = id = \phi_1\} = \{g \in G \mid gxg^{-1} = x \text{ for all } x \in N\} = C_G(N)$. By the First Isomorphism Theorem, $G/C_G(N)$ is isomorphic to $\Phi(G)$, which is a subgroup of $\mathrm{Aut}(N)$.

Section B.

4. Let X be any nonempty set and let R be the (commutative) ring of all integer-valued functions on X under the usual pointwise operations of addition and multiplication of functions: $R = \{f \mid f : X \longrightarrow \mathbb{Z}\}$. For each $a \in X$ define $M_a = \{f \in R \mid f(a) = 0\}$.

(a) Prove that M_a is a prime ideal in R.

(b) Prove that M_a is not a maximal ideal in R.

(c) Find all units in R.

(d) Find all zero divisors in R.

Solution: (a): Since M_a is the kernel of the surjective ring homomorphism from R to $\mathbb{Z}$ given by evaluation at a, $R/M_a \cong \mathbb{Z}$. The latter is an integral domain, hence M_a is a prime ideal.

(b): By (a), $R/M_a \cong \mathbb{Z}$, which is not a field, so M_a is not a maximal ideal.

(c): Let u be a unit in R, so there is some $v \in R$ such that $uv = 1$. Thus $u(a)v(a) = 1$ in $\mathbb{Z}$ for every $a \in X$. This means $u(a)$ and $v(a)$ are both 1 or both -1 for every a (these are the only units in $\mathbb{Z}$). Conversely, if u is any function on X that takes only the values ± 1, then u is its own inverse in R, hence is a unit.

(d): A nonzero element f is a zero divisor in R if and only if this function f is not identically zero but takes the value zero at least once: There is some $g \in R$ such that $fg = 0$ if and only if $f(a)g(a) = 0$ in $\mathbb{Z}$ for every $a \in X$. Thus $g(a)$ must be zero whenever $f(a) \neq 0$; and $g(a)$ can be any value when $f(a) = 0$. Given f we may construct one g such that $fg = 0$ by defining

$$g(a) = \begin{cases} 0 & \text{if } f(a) \neq 0 \\ 1 & \text{if } f(a) = 0, \end{cases}$$

and this g is not the zero function precisely when f has at least one zero on X.

5. Let F and K be finite fields with $F \subseteq K$. Let $F[x]$ and $K[x]$ denote the respective polynomial rings in the variable x, so $F[x]$ is a subring of $K[x]$.

(a) Prove that if M is any maximal ideal in $K[x]$, then $M \cap F[x]$ is a maximal ideal in $F[x]$.

(b) Give an explicit example of commutative rings $A \subseteq B$ and a maximal ideal I of B such that $I \cap A$ is not a maximal ideal of A.

Solution: (a): Since M is a maximal ideal in $K[x]$, the quotient ring $K[x]/M$ is a field, and is isomorphic to a finite extension of K. Thus $K[x]/M$ is a finite field. The image of $F[x]$ in this quotient ring is $F[x]/(M \cap F[x])$, and this is a subring of a finite field. Since any finite integral domain is a field (a familiar result), $F[x]/(M \cap F[x])$ is a field. This proves $M \cap F[x]$ is a maximal ideal in $F[x]$.

(b): Take $A = \mathbb{Z}$, $B = \mathbb{Q}$ and $I = (0)$. Or, take $A = \mathbb{Z}[x]$, $B = \mathbb{Q}[x]$ and $I = (x)$.

6. Let R be a Principal Ideal Domain, let p and q be distinct primes in R, and let $a = p^\alpha q^\beta$ for some $\alpha, \beta \in \mathbb{Z}^+$. Let M be any R-module annihilated by (a). Prove that

$$M \cong M_p \oplus M_q$$

where M_p is the submodule of M annihilated by (p^α) and M_q is the submodule of M annihilated by (q^β).

Solution: Because R is a P.I.D., we have $(p^\alpha, q^\beta) = (1)$, so $p^\alpha s + q^\beta t = 1$ for some s and t in R. One checks that the isomorphism is given by sending m to $(q^\beta m, p^\alpha m)$, with inverse sending (x, y) to $tx + sy$.

7. (a) How many similarity classes of 8×8 matrices A with rational number entries are there that satisfy $A^8 = A$? (Explain briefly; you need not explicitly list all classes.)

(b) How many similarity classes of 3×3 matrices A with entries from the field $\mathbb{Z}/7\mathbb{Z}$ are there that satisfy $A^8 = A$? (Explain briefly; you need not explicitly list all classes.)

Solution: (a): This is equivalent to counting rational 8×8 matrices in rational canonical form with minimal polynomial dividing $x^8 - x = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. These factors are irreducible, the last one being the 7^{th} cyclotomic polynomial $\Phi_7(x)$. There are then potentially 7 possibilities for the minimal polynomial $m_A(x)$, one for each nonempty subset of these three irreducible factors. For each of these, one counts the number of ways of choosing a sequence of invariant factors, each dividing the next, so that the last one is the minimal polynomial and the

degree of the product is 8. Here one finds that m_A cannot be $\Phi_7(x)$. For each of the remaining 6 choices of $m_A(x)$, one finds a single such sequence, except when $m_A(x) = x(x-1)$ and there are 7 choices. This makes 12 in all.

(b): By the same theory of rational canonical forms, we reduce to counting 3×3 matrices with entries in $\mathbb{Z}/7\mathbb{Z}$ whose minimal polynomial divides $x(x-1)^7$. Now $m_A(x)$ may be x, $x(x-1)$, $x(x-1)^2$, $x-1$, $(x-1)^2$, or $(x-1)^3$. For each of these, we count one possible sequence of invariant factors, except that for $x(x-1)$ we count two. This makes 7 in all.

Section C.

8. Let E be the splitting field in $\mathbb{C}$ of the polynomial $p(x) = x^6 + 3x^3 - 10$ over $\mathbb{Q}$, and let α be any root of $p(x)$ in E.

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

(b) Describe the roots of $p(x)$ in terms of radicals involving rational numbers and roots of unity.

(c) Find $[E : \mathbb{Q}]$. (Justify)

(d) Prove that E contains a *unique* subfield F with $[F : \mathbb{Q}] = 2$.

Solution: (a): Note that $p(x) = (x^3 - 2)(x^3 + 5)$, and both of these factors are irreducible over $\mathbb{Q}$ by Eisenstein. A root of $p(x)$ is then a root of one of these irreducible cubics, and thus generates an extension of degree 3.

(b): Let ω be a primitive 3^{rd} root of unity in $\mathbb{C}$. Let α and β be the real cube roots of 2 and -5 respectively. Then the roots of $p(x)$ are α, $\omega\alpha$, $\omega^2\alpha$, β, $\omega\beta$, and $\omega^2\beta$, which are radical expressions.

(c): Clearly $E = \mathbb{Q}(\alpha, \beta, \omega)$. Let $E_0 = \mathbb{Q}(\alpha, \omega)$ so that E_0 is the splitting field of $x^3 - 2$ and $\mathrm{Gal}(E_0/\mathbb{Q}) \cong S_3$. We claim $x^3 + 5$ is irreducible over E_0, in which case

$$[E : \mathbb{Q}] = [E : E_0][E_0 : \mathbb{Q}] = 3 \cdot 6 = 18. \tag{8.1}$$

If not, then the cubic polynomial $x^3 + 5$ must have a root in E_0, hence must have all its roots in E_0 (as $\omega \in E_0$). Thus if $x^3 + 5$ is reducible over E_0 we get $E_0 = E$ is of degree 6 over $\mathbb{Q}$. In this situation there is a unique real subfield of degree 3 over $\mathbb{Q}$, and so $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. There are a number of ways to see that this leads to a contradiction; one way without computation is as follows: View E as the splitting field of $x^3 - 2$ over $\mathbb{Q}$ and let $\mathrm{Gal}(E/Q) = \langle\, \sigma, \tau \,\rangle$ where τ is complex conjugation and $\sigma(\alpha) = \omega\alpha$. Now β, being real, is fixed by τ; and $\sigma(\beta)$ is another (different) root of $x^3 + 5$; thus $\sigma(\beta) = \omega\beta$ or $\omega^2\beta$. One immediately checks that σ fixes α/β (in the first case) or fixes $\alpha\beta$ (in the second case). Thus either α/β or $\alpha\beta$ is fixed by both σ and τ, hence is fixed by all of G, so is a rational number. This is a contradiction because α/β is a root of $5x^3 + 2$ and $\alpha\beta$ is a root of $x^3 + 10$, both of which are irreducible over $\mathbb{Q}$ by Eisenstein. This contradiction proves (8.1).

(d): A subfield F of degree 2 over $\mathbb{Q}$, corresponds via Galois theory to a subgroup of order 9 in the Galois group of order 18. Such a subgroup is a Sylow 3-subgroup. The conditions of Sylow's Theorem imply that there can be only one such subgroup, hence F is likewise unique. (Or, if there were two quadratic extensions of $\mathbb{Q}$ in E, their composite would have degree 4, whereas $4 \not| 18$.)

9. Let p be a prime, let F be a field of characteristic 0, let E be the splitting field over F of an irreducible polynomial of degree p, and let $G = Gal(E/F)$.

(a) Explain why $[E : F] = pm$ for some integer m with $(p, m) = 1$.

(b) Prove that if G has a normal subgroup of order m, then $[E : F] = p$ (i.e., $m = 1$).

(c) Assume $p = 5$ and E is *not* solvable by radicals over F. Show that there are exactly 6 fields K with $F \subseteq K \subseteq E$ and $[E : K] = 5$.
(You may quote without proof basic facts about groups of small order.)

Solution: (a): If α is any root of the irreducible polynomial, then $[F(\alpha) : F] = p$. Hence $[E : F] = [E : F(\alpha)][F(\alpha) : F] = mp$. Also, the degree over F of the splitting field of any degree p polynomial divides $p!$ (G is isomorphic to a subgroup of S_p, the group of all permutations of the p roots). So p does not divide m as p^2 does not divide $p!$.

(b): Suppose N is a normal subgroup of G of index p, let α be any root of the irreducible polynomial and let H be the subgroup of G fixing $F(\alpha)$. By Galois theory $|G : H| = p$ as well. If $H \neq N$, then the Diamond Isomorphism Theorem gives $HN = G$ and $p = |G : N| = |H : H \cap N|$. In this case $p^2 = |G : H \cap N|$, contrary to p^2 not dividing $pm = |G|$. Since α was arbitrary, this contradiction proves that $N = H$ is the subgroup of G that fixes every root, hence $N = 1$. Thus $|G| = p = [E : F]$, as needed.

(c): By the solvability by radicals theorem, this means that G is not a solvable group. We count subgroups of order 5, which must be Sylow 5-subgroups in G, where $|G| = 5m$, and m divides $4! = 24$. If there is only one Sylow 5-subgroup P, it must be normal and cyclic, hence abelian. The quotient G/P has order less than 25, and hence is solvable, so G is solvable and this is a contradiction. Hence by Sylow's Theorem the number n_5 of Sylow 5-subgroups must satisfy $n_5 \equiv 1 \pmod 5$, $n_5 \neq 1$, and $n_5 \mid 24$. The only solution is $n_5 = 6$. The Galois correspondence then gives that there are six fields K, as asserted. (Alternatively, you may just quote that the only nonsolvable subgroups of S_5 are S_5 and A_5, and these each have 6 Sylow 5-subgroups by inspection or by Sylow.)

10. Let p be a prime, let $\mathbb{F}_p$ be the field of order p, and let $f(x)$ be a nonconstant polynomial in $\mathbb{F}_p[x]$. Assume f factors as

$$f(x) = q_1(x)^{\alpha_1} q_2(x)^{\alpha_2} \cdots q_r(x)^{\alpha_r} \tag{10.1}$$

for some distinct irreducible polynomials $q_1, \ldots, q_r$ in $\mathbb{F}_p[x]$ and $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}^+$. Let E be a splitting field of f over $\mathbb{F}_p$.

(a) Give an expression for $[E : \mathbb{F}_p]$ in terms of the q_i in (10.1).
[Hint: Your answer should only involve the degrees of the q_i's, and not depend on the α_i's.]

(b) Fix a natural number N and assume $q_1, \ldots, q_r$ are *all* the distinct irreducible polynomials of degree $\leq N$ in $\mathbb{F}_p[x]$. Find an expression for $[E : \mathbb{F}_p]$ in terms of N, where f is as in (10.1).

Solution: (a): Note that the splitting field for f is the same as the splitting field for $q_1 q_2 \ldots q_r$; so in both parts we may assume all $\alpha_i = 1$. Since finite fields of the same order are isomorphic, E must simply be the smallest finite field of characteristic p and degree divisible by each of the degrees of the q_i. Thus $[E : \mathbb{F}_p]$ is the least common multiple of the degrees of the q_i's.

(b): In this case, $[E : \mathbb{F}_p] = d$ is the least common multiple of the positive integers up to N. For each prime r define r^{e_r} to be the largest power of r that is $\leq N$. Note that $r^{e_r} = 1$ whenever $r > N$. Then one easily see that $d = \prod r^{e_r}$, where the product is over all primes r in $\mathbb{Z}^+$.