ALGEBRA PH.D. QUALIFYING EXAM — SOLUTIONS

January 13, 2009

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, group actions, solvable groups, commutators, etc. as long as you state what facts you are using.

1. Let G be a group of order 10,989 (note that $10989 = 3^3 \cdot 11 \cdot 37$).

(a) Compute the number, n_p, of Sylow p-subgroups permitted by Sylow's Theorem for each of $p = 3$, 11, and 37; for each of these n_p give the order of the normalizer of a Sylow p-subgroup.

(b) Show that G contains either a normal Sylow 37-subgroup or a normal Sylow 3-subgroup.

(c) Explain briefly why (in all cases) G has a normal Sylow 11-subgroup.

(d) Deduce that the center of G is nontrivial.

Solution: For each prime p let P_p be a Sylow p-subgroup of G.

(a): Quick calculation shows that if $n_p \neq 1$, then $n_3 = 37$ or $n_{11} = 3 \cdot 37$ or $n_{37} = 3^3 11$. In the latter cases $|N_G(P_p)| = 3^3 11$, $3^2 11$ and 37 respectively.

(b): Assume $n_{37} \neq 1$ so that G contains $3^3 11(37-1)$ elements of order 37, leaving only $3^3 11$ elements remaining. If P_3 were not normal, then $N_G(P_3)$ would have order $3^3 11$, hence would be the unique subgroup of this order. Then P_3, being characteristic in $N_G(P_3)$, would be normal in G, contrary to assumption. Thus when $n_{37} \neq 1$ we must have $P_3 \trianglelefteq G$.

(c): By Sylow applied in either G/P_{37} or G/P_3, depending on which is normal by (b), we see that the quotient group contains a normal Sylow 11-subgroup. Taking the preimage of this normal subgroup gives a normal subgroup H of G of order $11 \cdot 37$ or $3^3 11$ respectively. Again by Sylow, P_{11} is characteristic in H, hence normal in G. (Note that all the Sylow numerology was done in (a), so the possible Sylow-11 numbers need not be recomputed in the quotient group or in H.)

(d): Since by (c), $N_G(P_{11})/C_G(P_{11}) = G/C_G(P_{11})$ and the former is isomorphic to a subgroup of $\mathrm{Aut}(P_{11}) = \mathrm{Aut}(Z_{11}) \cong Z_{10}$, by Lagrange $C_G(P_{11}) = G$. Thus $P_{11} \leq Z(G)$, as needed.

2. Let G be a finite group.

(a) Suppose A and B are normal subgroups of G and both G/A and G/B are solvable. Prove that $G/(A \cap B)$ is solvable.

(b) Deduce from (a) that G has a subgroup that is the unique smallest subgroup with the properties of being normal with solvable quotient — this subgroup is denoted by $G^{(\infty)}$ (i.e., show there is a subgroup $G^{(\infty)} \trianglelefteq G$ with $G/G^{(\infty)}$ is solvable, and if G/N is any solvable quotient, then $G^{(\infty)} \leq N$).

(Remark: For example, when G is solvable, $G^{(\infty)} = 1$; or if G is a perfect group, $G^{(\infty)} = G$.)

(c) If G has a subgroup S isomorphic to A_5 (not necessarily normal), show that $S \leq G^{(\infty)}$.

Solution: (a): Observe that in the solvable quotient group G/A, for some r the r^{th} term of the derived series is trivial. Since the derived series for G/A is the image mod A of the derived series for G, this says $G^{(r)} \leq A$. Likewise, for some s we have $G^{(s)} \leq B$. Thus $G^{(r+s)} \leq A \cap B$ and so $G/(A \cap B)$ is solvable. Alternatively, you can do this by the Diamond Isomorphism Theorem, arguing that both G/A and $A/(A \cap B)$ are solvable, hence so is $G/(A \cap B)$.

(b): Let $G^{(\infty)}$ be the intersection of all normal subgroups A such that G/A is solvable. Then $G^{(\infty)}$ has the desired properties (provided G is a finite group!). Note that $G^{(\infty)}$ is simply the terminal member of the derived series for G (the subgroup in this series where all succeeding terms are the same).

(c): If $S \cong A_5$ then S is non-abelian simple; and since $S \cap G^{(\infty)} \trianglelefteq S$, either $S \leq G^{(\infty)}$ or $S \cap G^{(\infty)} = 1$. In the latter case, however, $S \cong SG^{(\infty)}/G^{(\infty)}$, which is a non-abelian simple subgroup of the solvable group $G/G^{(\infty)}$, a contradiction. We must therefore have $S \leq G^{(\infty)}$.

3. Let G be a group of odd order and let σ be an automorphism of G of order 2.

(a) Prove that for every prime p dividing the order of G there is some Sylow p-subgroup P of G such that $\sigma(P) = P$ (i.e., σ stabilizes the subgroup P — note that σ need not fix P elementwise).

(b) Suppose G is a cyclic group. Prove that $G = A \times B$ where

$$A = C_G(\sigma) = \{g \in G \mid \sigma(g) = g\} \qquad \text{and} \qquad B = \{x \in G \mid \sigma(x) = x^{-1}\}.$$

(Remark: This decomposition is true more generally when G is abelian.)

Solution: (a): By Sylow applied in G, the number of Sylow p-subgroups is odd. Since σ, which has order 2, permutes these, it must fix one of them.

(b): One way to do this is to observe that for each prime p, σ acts on the (unique) cyclic Sylow p-subgroup P of G. Since the automorphism group of a cyclic p-group is cyclic (p is odd), P has a unique automorphism of order 2, namely inversion. Thus for each P either σ inverts P or acts trivially on P. Let A be the product of all Sylow subgroups fixed elementwise by σ and let B be the product of all Sylow subgroups inverted by σ. These are seen to be the desired subgroups, and by construction they decompose G as a direct product.

Alternatively, for any abelian G let $A = C_G(\sigma)$ and define $B = \{x\sigma(x)^{-1} \mid x \in G\}$. Show that B is a subgroup, σ inverts B (so $A \cap B = 1$), and $G = AB$ (to do the latter write each x^2 as $(x\sigma(x))(x\sigma(x)^{-1}) \in AB$, and note that because $|G|$ is odd, every element of G is a square).

Section B.

4. Let R be a commutative ring with 1.

(a) Prove that each nilpotent element of R lies in every prime ideal of R.

(b) Assume every nonzero element of R is either a unit or a nilpotent element. Prove that R has a unique prime ideal.

Solution: (a): Let P be a prime ideal and let x be a nilpotent element. Since x maps to a nilpotent element in the integral domain R/P, it must map to zero, i.e., $x \in P$, as desired.

(b): A prime ideal P contains all nilpotent elements but no units. Thus any prime ideal must consist of exactly the set of all nilpotent elements, as needed to establish uniqueness. (Note that R has at least one maximal ideal, since it has a 1, so it does have a prime ideal.)

5. Let $R = \mathbb{C}[x, y]$ be the ring of polynomials in the variables x and y, so R may be viewed as $\mathbb{C}$-valued functions on (affine) complex 2-space, $\mathbb{C}^2$, in the usual way (R is called the *coordinate ring* of this affine space). Let I be the ideal of all functions in R that vanish on both coordinate axes, i.e., that are zero on the set $\{(a, 0) \mid a \in \mathbb{C}\} \cup \{(0, b) \mid b \in \mathbb{C}\}$. (You may assume I is an ideal.)

(a) Exhibit a set of generators for I. (Be sure to explain briefly why they generate I.)

(b) Show that I is not a prime ideal.

(c) Show that R/I has no nilpotent elements.

Solution: (a): By direct calculation if $p(x, y)$ is zero on both coordinate axes then it has no constant term and is divisible by both x and y. Since conversely any such polynomial is zero on both axes, $I = (xy)$. Alternatively, in the language of algebraic sets, (x) is the ideal of functions that vanish on the y-axis and (y) is the ideal that vanishes on the x-axis. Thus the ideal of functions that vanish on the union of the two axes is the product ideal $(x)(y) = (xy)$.

(b): (xy) is clearly not a prime ideal (and the corresponding zero set is clearly a union of two varieties, the axes).

(c): This follows by easy direct manipulation. Alternatively, since the ring R/I acts faithfully as $\mathbb{C}$-valued functions on the coordinate axes and $\mathbb{C}$ has no nonzero nilpotent elements, neither does this ring of functions. In other words, the ideal of functions that vanish on any subset of affine space is always a radical ideal.

6. Classify all finitely generated R-modules, where R is the ring $\mathbb{Q}[x]/(x^2 + 1)^2$.

Solution: A module over $\mathbb{Q}[x]/(x^2 + 1)^2$ is a module over $\mathbb{Q}[x]$ that is annihilated by $(x^2 + 1)^2$. Since $\mathbb{Q}[x]$ is a PID, we know that a finitely generated module is a direct sum of cyclic modules. This means we have a direct sum of modules of the form $\mathbb{Q}[x]/(x^2 + 1)^i$ for $i = 1$ or 2.

(If one wanted more information: A finitely generated R-module M is necessarily finite dimensional over $\mathbb{Q}$ — let its dimension be d. If M is a direct sum of d_1 copies of $\mathbb{Q}[x]/(x^2 + 1)$ and d_2 copies of $\mathbb{Q}[x]/(x^2 + 1)^2$, then one see that $d = 2d_1 + 4d_2$. Moreover, if N is the submodule of M annihilated by $(x^2 + 1)$, then N has dimension $d_1 + d_2$ over the field $\mathbb{Q}[x]/(x^2 + 1)$, hence has dimension $2(d_1 + d_2)$ over $\mathbb{Q}$. Thus M/N has dimension $2d_2$ over $\mathbb{Q}$. In other words, knowledge of the $\mathbb{Q}$-dimensions of M and N is sufficient to determine the precise isomorphism type of M.)

7. (a) Find all possible canonical forms for a matrix over $\mathbb{F}_3$ with characteristic polynomial $x^4 - 1$.

(b) Find all possible canonical forms for a matrix over $\mathbb{F}_2$ with characteristic polynomial $x^4 - 1$.

Solution: (a): The polynomial $x^4 - 1$ has no repeated roots mod 3, so the minimal and characteristic polynomials are equal: the only (rational) canonical form is the companion matrix for $x^4 - 1$.

(b): In $\mathbb{F}_2[x]$ we have $x^4 - 1 = (x + 1)^4$. The elementary divisors that comprise each possible Jordan canonical form are $(x + 1)^i$, and the sum of their exponents is 4; i.e., the JCFs are in bijection with the five partitions of 4.

Section C.

8. Let $K = \mathbb{Q}(\sqrt{3+\sqrt{5}}\,)$.

(a) Show that $K/\mathbb{Q}$ is a Galois extension.

(b) Determine the Galois group of $K/\mathbb{Q}$.

(c) Find all subfields of K.

Solution: (a): The field K clearly contains $F = \mathbb{Q}(\sqrt{5})$. The conjugates of $\sqrt{3+\sqrt{5}}$ are among $\pm\sqrt{3\pm\sqrt{5}}$. The product of any two of these lies in F, hence in K. Since K contains the first of these, it contains all conjugates. This makes it a Galois extension.

(b): Clearly $\sqrt{3+\sqrt{5}}$ is a root of a degree 4 polynomial over $\mathbb{Q}$ so $[K:\mathbb{Q}] \le 4$. Also, $[F:\mathbb{Q}] = 2$ by Eisenstein. Note that $(\sqrt{3+\sqrt{5}} + \sqrt{3-\sqrt{5}})^2 = 10$, so $\sqrt{10} \in K$, and hence $\sqrt{2} = \sqrt{10}/\sqrt{5} \in K$. Thus by degree consideration K equals the biquadratic extension $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ of degree 4 over $\mathbb{Q}$ with Galois group the Klein fourgroup. As usual, the three subfields of K of degree 2 are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{10})$.

9. Let K_1 and K_2 be finite abelian Galois extensions of F contained in a fixed algebraic closure of F. Show that their composite, K_1K_2, is a finite abelian Galois extension of F as well.

Solution: We know that K_i is the splitting field of the separable polynomial $p_i(x)$. The composite is the splitting field of the l.c.m. of $p_1(x)$ and $p_2(x)$, which makes it normal, separable and thence Galois. Consider a commutator in the Galois group of K_1K_2/F. Its restriction to K_1 and K_2 is trivial since these are abelian over F. Therefore it is trivial on the composite and so must be the identity in $\mathrm{Gal}(K_1K_2/F)$. This shows that every commutator is trivial, so the Galois group is abelian.

10. Let q be a power of a prime, let $Gal(\mathbb{F}_{q^2}/\mathbb{F}_q) = \langle\, \sigma \,\rangle$ (note that σ has order 2). Let N be the usual *norm map* for this extension:

$$N : \mathbb{F}_{q^2}^{\times} \longrightarrow \mathbb{F}_q^{\times} \qquad \text{by} \qquad N(x) = x\,\sigma(x).$$

(a) Prove that N is surjective.

(b) Show that $\mathbb{F}_{q^2}^{\times}$ has an element of order $q+1$ whose norm is 1.

(c) Find the following index: $|\,\mathbb{F}_q^{\times} : N(\mathbb{F}_q^{\times})\,|$.

Solution: (a): Note that $N(x) = xx^q = x^{1+q}$ for all $x \in \mathbb{F}_{q^2}^{\times}$. Since $\mathbb{F}_{q^2}^{\times}$ is a cyclic group of order $q^2 - 1 = (q-1)(q+1)$, the image of N is the unique subgroup of index $q+1$ (order $q-1$) which is $\mathbb{F}_q^{\times}$.

(b): By (a) the kernel of N is cyclic of order $q+1$.

(c): Since σ fixes $\mathbb{F}_q$, $N(x) = x^2$ for all $x \in \mathbb{F}_q^{\times}$. Since the latter group is cyclic of order $q-1$, the squaring map has index 1 when q is even (i.e., in characteristic 2) and index 2 when q is odd. Alternatively, this follows from the Diamond Isomorphism Theorem by looking at $\ker N \cap \mathbb{F}_q^{\times} = \{x \in \mathbb{F}_q^{\times} \mid x^2 = 1\}$.