ALGEBRA PH.D. QUALIFYING EXAM — SOLUTIONS

October 20, 2011

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 as long as you state clearly what facts you are using.

1. Let G be a group of order 9045 (note that $9045 = 3^3 \cdot 5 \cdot 67$).

(a) Compute the number, n_p, of Sylow p-subgroups permitted by Sylow's Theorem for each of $p = 3$, 5, and 67; for each of these n_p give the order of the normalizer of a Sylow p-subgroup.

(b) Show that G has a normal Sylow p-subgroup for some prime p dividing $|G|$.

(c) Show that G must have a normal Sylow 5-subgroup.

Solution:

(a) Direct computation shows that $n_3 = 1$ or 67; $n_5 = 1$ or $3 \cdot 67 = 201$; and $n_{67} = 1$ or $3^3 5 = 135$. If P_p is a Sylow p-subgroup, then in the cases were P_p is not normal in G we have $|N_G(P_3)| = 3^3 5$; $|N_G(P_5)| = 3^2 5$; and $|N_G(P_{67})| = 67$.

(b) If G does not have a normal Sylow 67-subgroup, then since distinct Sylow 67-subgroups intersect in the identity, by (a) there are $135(67 - 1) = 8910$ elements of order 67. Only 135 elements remain. If G does not have a normal Sylow 5-subgroup, then analogously there are $201(5 - 1) = 804$ elements of order 5. Thus G must have either a normal Sylow 67-subgroup or a normal Sylow 5-subgroup.

[Alternatively, if G does not have a normal Sylow 67-subgroup or a normal Sylow 3-subgroup, then the normalizer of a Sylow 3-subgroup, which has order 135, must account for all the elements of G that are not of order 67. Thus $N_G(P_3)$ is normal in G. This is impossible as P_3 is characteristic in $N_G(P_3)$, and so P_3 would be normal in G, contrary to assumption.]

(c) If P_5 is not normal in G, then by (b), P_{67} is normal. Let overbars denote passage to G/P_{67}. By Sylow's Theorem $\overline{P_5}$ is normal in $\overline{G}$. If H is the complete preimage in G of $\overline{P_5}$, then H is a normal subgroup of G of order $5 \cdot 67$. By Sylow's Theorem in H we see that P_5 is normal, hence characteristic, in H. Since H is normal in G, this gives P_5 is normal in G too.

[Alternatively, the corresponding argument will work if P_3 is normal in G. Or, simply consider $H = P_{67}P_5$ or P_3P_5 and derive a contradiction from (a) by showing 67 or $3^3 \bigm| |N_H(P_5)|$ respectively.]

2. Let p be a prime and let G be a finite group whose order is divisible by p. Let P be a normal p-subgroup of G (i.e., $|P| = p^b$ for some b).

(a) Prove that P is contained in *every* Sylow p-subgroup of G.

(b) Prove that if M is any *maximal* subgroup of G, then either $P \le M$ or $|\,G : M\,| = p^c$ for some $c \le b$.

Solution: (a) By Sylow's Theorem P is contained in one Sylow p-subgroup, Q, of G. Thus for all $g \in G$ we have $P = gPg^{-1} \le gQg^{-1}$. By Sylow's Theorem every Sylow p-subgroup equals gQg^{-1} for some $g \in G$, so P is contained in every Sylow p-subgroup.

(b) If P is not contained in M, then since P is normal, PM is a subgroup of G that properly contains M. By maximality, $PM = G$. By the Second (Diamond) Isomorphism Theorem, $G/P = PM/P \cong M/(P \cap M)$. Looking at the other "parallel" sides of this diamond lattice gives that $|\, G : M \,| = |\, P : P \cap M \,|$. The latter index is a power of p by Lagrange's Theorem so the second conclusion of (b) holds.

3. Let G be a group acting faithfully and transitively (on the left) on a finite set Ω, and let $\omega \in \Omega$. Let G_ω be the stabilizer of the point ω:

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

(a) For any $g \in G$, prove that $gG_\omega g^{-1} = G_{g\omega}$.

(b) Show that if G_ω is a normal subgroup of G, then $G_\omega = 1$.

(c) Suppose in addition that G is the quaternion group of order 8. Deduce that we must have $|\Omega| = 8$.

Solution: (a) It is straightforward from the definition to show $gG_\omega g^{-1} \subseteq G_{g\omega}$. Because these subgroups have the same order (G is finite here), we obtain equality. Alternatively (for infinite G too), conjugating the first containment by g^{-1} and applying the containment for g^{-1} gives

$$G_\omega \subseteq g^{-1}G_{g\omega}g \subseteq G_{g^{-1}\cdot g\omega}.$$

Since $g^{-1} \cdot g\omega = \omega$ all three subgroups above are equal, as desired.

(b) If G_ω is normal in G then by (a) we have $G_\omega = G_{g\omega}$ for every $g \in G$. Since G is transitive on Ω, this shows G_ω fixes every point of Ω. Since G acts faithfully on Ω, $G_\omega = 1$.

(c) Since every subgroup of the quaternion group of order 8 is normal, by (b) we must have $G_\omega = 1$ for any $\omega \in \Omega$. Since G is transitive on Ω, by results from group actions we have $|\Omega| = |\, G : G_\omega \,| = 8$.

Section B.

4. Let $R = \mathbb{Z}[\sqrt{-13}]$ and let $N(a + b\sqrt{-13}) = a^2 + 13b^2$ be the usual field norm. (You may assume $N : R \to \mathbb{Z}$ is multiplicative.)

(a) Let $\alpha = 1 + \sqrt{-13}$. Show that $\alpha^2 \in (2)$ but $\alpha \notin (2)$.

(b) Show that 2 is irreducible in R, and determine if (2) is a prime ideal.

(c) Is R is a Unique Factorization Domain? (Justify.)

Solution: (a) Clearly $\alpha^2 = -12 + 2\sqrt{-13} \in (2)$. Since $1, \sqrt{-13}$ are linearly independent over $\mathbb{Q}$, $\alpha \neq 2(a + b\sqrt{-13})$ for any integers a, b, i.e., $\alpha \notin (2)$.

(b) Suppose $2 = \beta\gamma$ for some $\beta, \gamma \in R$. Then $4 = N(\beta\gamma) = N(\beta)N(\gamma)$. In the quadratic integer ring R the elements of norm 1 are units (no norms are negative); so if neither β nor γ is a unit, both must have norm 2. For $\beta = a + b\sqrt{-13}$ we would have $N(\beta) = a^2 + 13b^2 = 2$, which is clearly impossible for integers a, b. This proves 2 is irreducible.

(c) Since 2 is irreducible but not prime, R is not a U.F.D.

5. Let x be an indeterminate over the field $\mathbb{Q}$. Describe explicitly all isomorphism types of $\mathbb{Q}[x]$-modules that are 2-dimensional vector spaces over $\mathbb{Q}$. (Be sure to quote explicitly any theorems that you use.)

Solution: By the Fundamental Theorem for Finitely Generated Modules over a P.I.D. (such as $\mathbb{Q}[x]$), any 2-dimensional module, M—which is necessarily finitely generated, even over $\mathbb{Q}$, by a basis—is a direct sum of cyclic modules:

$$M \cong \frac{\mathbb{Q}[x]}{(a_1(x))} \oplus \frac{\mathbb{Q}[x]}{(a_2(x))} \oplus \cdots \oplus \frac{\mathbb{Q}[x]}{(a_n(x))}$$

for monic polynomials $a_1, a_2, \ldots, a_n$, each dividing the next (the Invariant Factor Decomposition). Since the $\mathbb{Q}$-dimension of each $\mathbb{Q}[x]/(a_i(x))$ is the degree of a_i, we must have $n = 1$ or 2. Furthermore, if $n = 1$ then $M \cong \mathbb{Q}[x]/(a_1(x))$ for a monic quadratic polynomial in $\mathbb{Q}[x]$. If $n = 2$ then the divisibility condition forces $a_1 = a_2$ and both are degree 1, i.e, $M \cong \mathbb{Q}[x]/(x-a) \oplus \mathbb{Q}[x]/(x-a)$. By the Fundamental Theorem these are all possibilities, and all are distinct (nonisomorphic).

6. (a) Find, with justification, the smallest positive integer n such that there is an $n \times n$ matrix A with rational number entries satisfying $A^9 = I$ but $A^i \neq I$ for $1 \leq i \leq 8$.

(b) Exhibit an explicit matrix A satisfying the conditions of (a) for the smallest n you found.

(c) Find, with justification, the smallest positive integer k such that there are two, *nonsimilar* $k \times k$ matrices with rational number entries, both satisfying $X^9 = I$ but $X^i \neq I$ for $1 \leq i \leq 8$.

Solution: (a) and (b) First factor the cyclotomic polynomial $x^9 - 1 = (x^3)^3 - 1$ into irreducibles in $\mathbb{Q}[x]$ as

$$x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1)$$

where the last irreducible factor is $\Phi_9(x)$ of degree $\phi(9) = 6$. The given conditions are equivalent to the minimal polynomial of A dividing $x^9 - 1$ but not $x^3 - 1$. Thus the minimal polynomial of A must have a factor of $\Phi_9(x)$. The degree of such a matrix A is at least 6. Since the companion matrix of $\Phi_9(x)$ is a 6×6 matrix whose characteristic and minimal polynomials are both $\Phi_9(x)$, this matrix satisfies the given conditions.

(c) As noted above, the specified conditions are equivalent to the minimal polynomial dividing $x^9 - 1$ and containing a factor of $\Phi_9(x)$. If A and B are nonsimilar matrices of smallest degree satisfying the conditions, then the two lists of invariant factors resulting in the smallest degree matrices (= the degree of the product of all invariant factors) are seen to be:

(i) $a_1(x) = x - 1, \quad a_2(x) = (x-1)\Phi_9(x),$ and

(ii) $a_1(x) = (x^2+x+1)\Phi_9(x)$.

The lists are distinct, so the matrices are nonsimilar; and there is no possible pair of invariant factor lists—each invariant factor dividing the next with $\Phi_9(x)$ dividing the last invariant factor—for degrees 6 or 7. The minimal degree of A and B is therefore 8.

Section C.

7. Let K be the splitting field of $x^6 - 2$ over $\mathbb{Q}$.

(a) Find the isomorphism type of the Galois group of K over $\mathbb{Q}$.

(b) Find all subfields of K that are quadratic over $\mathbb{Q}$. (Justify why you found all of them.)

(c) Find a subfield of K that is normal over $\mathbb{Q}$ of degree 6.

Solution: (a) The roots of $x^6 - 2$ are $\zeta^i \sqrt[6]{2}$, $i = 0, 1, \ldots, 5$, where ζ is a primitive sixth root of unity in $\mathbb{C}$, and $\sqrt[6]{2}$ is the real, positive sixth root of 2. Argue as usual that $K = \mathbb{Q}(\sqrt[6]{2}, \zeta)$ by easily showing containment in both directions. The irreducible polynomial of ζ in $\mathbb{Q}[x]$ is $\Phi_6(x) = x^2 - x + 1$. By Eisenstein for $p = 2$, $x^6 - 2$ is irreducible over $\mathbb{Q}$, hence $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$. Since ζ is not real, $\zeta \notin \mathbb{Q}(\sqrt[6]{2})$; and since ζ is a root of a quadratic with rational coefficients we obtain

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}, \zeta) : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 2 \cdot 6 = 12. \qquad (7.1)$$

Each Galois automorphism, σ, of K is uniquely determined by its action on $\sqrt[6]{2}$ and ζ. Since σ fixes $\mathbb{Q}$, $\sigma(\sqrt[6]{2})$ must be a root of $x^6 - 2$ and $\sigma(\zeta)$ must be a root of $x^2 - x + 1$. There are at most 12 possible choices, hence by (7.1) all such indeed do determine automorphisms of $K/\mathbb{Q}$. Let ρ and σ be the Galois automorphisms defined by

(i) $\rho(\sqrt[6]{2}) = \zeta \sqrt[6]{2}$ and $\rho(\zeta) = \zeta$, and

(ii) $\sigma(\sqrt[6]{2}) = \sqrt[6]{2}$ and $\sigma(\zeta) = \zeta^5 = \overline{\zeta}$ (complex conjugation restricted to K).

Easy direct computation shows that $|\rho| = 6$, $|\sigma| = 2$ and $\rho\sigma = \sigma\rho^{-1}$. Thus ρ and σ satisfy the familiar presentation relations for generators (r and s respectively) in the dihedral group of order 12. This proves $\mathrm{Gal}(K/\mathbb{Q}) \cong D_{12}$.

(b) The field generated by all quadratic extensions of $\mathbb{Q}$ that are contained in K is of 2-power degree over $\mathbb{Q}$. Clearly $\sqrt{2} = (\sqrt[6]{2})^3$ and ζ generate distinct quadratic extensions of $\mathbb{Q}$, so $L = \mathbb{Q}(\sqrt{2}, \zeta) = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ is a normal biquadratic extension of degree 4 over $\mathbb{Q}$. Since $8 \nmid [K : \mathbb{Q}]$, all quadratic extensions lie in L. The three quadratic subfields of L (and hence of K) are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-6})$.

(c) Since $(\sqrt[6]{2})^2 = \sqrt[3]{2}$ is a root of $x^3 - 2$ and ζ^2 is a primitive cube root of unity (which generates the same field as ζ), the subfield $\mathbb{Q}((\sqrt[3]{2}, \zeta)$ is the splitting field of $x^3 - 2$, hence is normal over $\mathbb{Q}$. Alternatively, $\langle \rho^3 \rangle$ is a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of index 6 (it has order 2 and is the center of the Galois group); its fixed field is thus the required subfield (and this fixed field is seen to be L).

8. Let F be the finite field with 3^{20} elements.

(a) Draw the lattice of all subfields of F.

(b) Give an expression for the number of field generators for the extension $F/\mathbb{F}_3$, i.e., the number of primitive elements for this extension (you need not compute the actual numerical value).

(c) Give an expression for the number of generators for the multiplicative group, $F^\times$, of nonzero elements of F (you need not compute the actual numerical value).

(d) Does F contain a primitive eighth root of 1? (Briefly justify.)

Solution: (a) Since $\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_{p^m}$ if and only if $n \mid m$, the lattice of subgroups of $\mathbb{F}_{3^{20}}$ is the same as the lattice of subgroups of the cyclic group of order 20 (which is the same lattice as that of $\mathbb{Z}/12\mathbb{Z}$ in Section 2.5 of Dummit–Foote).

(b) An element $\alpha \in F$ is a primitive element if and only if α does not lie in either of the two maximal subfields of F, namely $\alpha \notin \mathbb{F}_{3^{10}} \cup \mathbb{F}_{3^4}$. The number of such α is therefore $3^{20} - 3^{10} - 3^4 + 3^2$, where we've added on the last term because the order of $\mathbb{F}_{3^{10}} \cap \mathbb{F}_{3^4} = \mathbb{F}_{3^2}$ has been subtracted twice.

(c) The number of multiplicative generators for the cyclic group $F^\times$ is $\phi(3^{20} - 1)$, where ϕ is Euler's function.

(d) Yes, F contains a primitive eighth root of unity because 8 divides the order of the cyclic group $F^\times$, so this group contains a (cyclic) subgroup of order 8. (Easily, $3^{20} = (3^2)^{10} \equiv 1 \pmod 8$; or use the equivalent fact that $\mathbb{F}_9^\times \leq F^\times$.)

9. Let a and b be relatively prime odd integers, both > 1. Let ζ be a primitive $(ab)^{\text{th}}$ root of 1 in $\mathbb{C}$. Prove that the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is *not* a cyclic group. (Be sure to quote explicitly any theorems that you use.)

Solution: By the basic theory of cyclotomic extensions, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/ab\mathbb{Z})^\times$. By the Chinese Remainder Theorem (applied to the units in the ring $\mathbb{Z}/ab\mathbb{Z}$), since $(a, b) = 1$,

$$(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times. \tag{9.1}$$

Note that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ is seen from its formula to be even for all odd integers $n > 1$. Thus the direct product in (9.1) is not cyclic since both factors have even order (it contains a noncyclic subgroup, the Klein 4-group).