Algebra Comprehensive Exam

— Fall 2007 —

Instructions: Complete five of the seven problems below. If you attempt more than five questions, then clearly indicate which five should be graded.

(1) Let G be a finite group such that $Aut(G)$ acts transitively on the set $G \setminus \{e\}$. Show that G is a p-group for some prime p, and that G is abelian.

Solution. Let p be a prime dividing the order of G. Then there is an element $x \in G$ with $|x| = p$. Let $y \in G \setminus \{e\}$ be an arbitrary element. Then there exists $\phi \in Aut(G)$ with $\phi(y) = x$, and $e = \phi(x^p) = y^p$, which implies that $|y| = p$. Consequently if $q \neq p$ is a prime, then G has no element of order q, and so $|G|$ is a power of p.

Since G is a p-group, there exists a $z \neq e$ in the center of G. If $a, b \in G \setminus \{e\}$ are arbitrary elements, then there exists $\psi \in Aut(G)$ with $\psi(b) = z$. But then

$$\psi(ab) = \psi(a)z = z\psi(a) = \psi(ba).$$

Since ψ is an automorphism, and hence injective, $ab = ba$. □

(2) An element $e \in A$ is an *idempotent* if $e^2 = e$. A commutative ring with $1 \neq 0$ that has a unique maximal ideal is called a *local ring*. Prove that the only idempotent elements in a local ring are 0 and 1.

Solution. Let $\mathfrak{m}$ be the unique maximal ideal of A. Then $e(1-e) = 0 \in \mathfrak{m}$ and since $\mathfrak{m}$ is prime, $e \in \mathfrak{m}$ or $1 - e \in \mathfrak{m}$. Note that e and $1 - e$ cannot both be elements of $\mathfrak{m}$ since this would imply $1 = e + (1 - e) \in \mathfrak{m}$.

If $e \in \mathfrak{m}$, then $1 - e \notin \mathfrak{m}$, and so $1 - e$ is a unit. (Indeed, if a is a nonunit then (a) is a proper ideal of A. Thus (a) is contained in some maximal ideal but since there is only one we have $(a) \subset \mathfrak{m}$. So all nonunits are contained in $\mathfrak{m}$.) But then $e = 0$. Similarly, if $1 - e \in \mathfrak{m}$, then e is a unit and so $1 - e = 0$. □

(3) If $p < q < r$ are primes and G is a finite group of order pqr, prove that the Sylow r-subgroup of G is normal. It is true and you may assume (without proving it) that one of the Sylow subgroups is normal.

Solution. If the Sylow p-subgroup P is normal then consider $G' = G/P$. (The argument when the q-subgroup is normal is analogous.) This is a group of order qr. Let n'_r be the number of Sylow r subgroups in G'. We know by the Sylow theorems that n'_r must divide q and be equal to $1 + nr$ for some non-negative integer n. Thus $n = 0$, since $r > p$, and $n'_r = 1$. So there is a unique Sylow r-subgroup R' in G' which must be normal. From the fourth isomorphism theorem there is a normal subgroup R'' in G such that R''/P is isomorphic to R'. Thus the order of R'' is rp. Considering R'' as a group in its own right we can argue as above (since r is larger than p) that there is a unique Sylow r subgroup of R'' which we denote by R. So the order of R is r and R is a subgroup of G. So it is a Sylow r-subgroup. If S is another Sylow r-subgroup of G then, again by the Sylow theorems, there is some element $g \in G$ such that $gRg^{-1} = S$ so $S = gRg^{-1} \subset gR''g^{-1} = R''$. Thus S is a subgroup of R'' that has order r. Since the order r-subgroup of R'' is unique we know $S = R$. We have shown that R is the only Sylow r-subgroup of G and thus it is normal. □

(4) The operators $A_1, \ldots, A_k$ in a vector space of dimension n are such that $A_1 + \cdots + A_k = I$. Prove that the following conditions are equivalent.

(a) Each A_i is a projection.
(b) $A_iA_j = 0, i \neq j$.
(c) $\text{rank}(A_1) + \cdots + \text{rank}(A_k) = n$.

Solution. (a)$\Rightarrow$(c). Notice that if the range of l of the A_i's nontrivially overlapped and v was in this common range then $(A_1 + \cdots + A_k)v = lv$ This is not possible unless $l = 1$. Thus the ranges do not overlap and if r_i denotes the rank of A_i we see that $r_1 + \cdots + r_k \leq n$. However $A_1 + \cdots + A_k = I$ implies that $r_1 + \cdots + r_k \geq n$. (Since the range of a sum of operators must be contained in the span of the ranges of each operator.)

(c)$\Rightarrow$(b) Since the whole vector space is contained in the span of the images of the A_i and $r_1 + \cdots + r_k = n$ we see that the images of the A_i can only have trivial intersection. Thus if v_i is a vector in the image of A_i and $v_1 + \cdots + v_k = 0$ then all the $v_i = 0$. Now if v is in the image of A_1 then $A_1v + A_2v + \cdots + A_kv = v$ so $(A_1v - v) + A_2v + \cdots + A_kv = 0$ and we see that $A_iv = 0$ for $i \neq 1$ and $A_1v = v$. In particular $A_iA_1 = 0$ for all $i \neq 1$. Similarly $A_jA_i = 0$ for all $i \neq j$.

(b)$\Rightarrow$(a). Not $A_1 = A_1(A_1+\cdots+A_k) = A_1^2+A_1A_2+\cdots+A_1A_k = A_1^2$ so A_1 is a projection. Similarly the other A_i are projections. $\square$

(5) Let F be a field and K an extension of K of degree n. Let $f(x) \in F[x]$ be an irreducible polynomial of degree m. Suppose n and m are relatively prime. Show that $f(x)$ is irreducible as a polynomial in $K[x]$.

Solution. Suppose $f(x)$ factors in $K[x]$ as $f_1(x)f_2(x)$, with $f_1(x)$ irreducible. Let m_1 and m_2 be the degrees of f_1 and f_2, respectively. If m_1 or m_2 is 1 then there is a root a of $f(x)$ in K and if we let $E = K(a)$ then we know $[E : F] = m$ and $[K : F] = [K : E][E : F] = [K : E]m$ and hence m divides n, a contradiction. Thus $1 < m_i < m$ for $i = 1, 2$. Let $K' = K[x]/(f_1(x))$. We know $[K' : K] = m_1$ and K' has a root of $f_1(x)$, hence a root of $f(x)$. Since K' is a field extension of F that contains a root of $f(x)$, as argued above, we know m divides $[K' : F] = m_1n$. Therefore m_2 divides n, but this contradicts m and n being relatively prime unless $m_2 = 1$ which we already argued is not the case. Hence $f(x)$ is irreducible in $K[x]$. $\square$

(6) Let R be a commutative ring with 1 and let M be an ideal of R. Show that if M is maximal and principal then there is no ideal I such that $M^2 \subsetneq I \subsetneq M$. Moreover, give examples to show that this is not true if M is not assumed to be maximal and give an example to show that this is not true if M is not assumed to be principal.

Solution. Suppose $M = (a)$ and I is an ideal contained in M and containing M^2. One may easily check that $M^2 = (a^2)$. Thus $a^2r \in I$ for all $r \in R$. If we assume $I \neq M^2$ then there is some element in M that is not in M^2 in I. That is there is some element of the form ar in I for some $r \in R$ with a not dividing r. Thus $r \notin M$ and (a, r) is an ideal properly containing M. So $(a, r) = R$ and we know there are r_1 and r_2 such that $ar_1 + rr_2 = 1$. Which implies that $a = a^2r_1 + arr_2$ is in I. So $I = M$.

To see the necessity of M being maximal consider $R = \mathbb{Z}$ and $M = (6)$. Then $M^2 = (36)$ and $I = (12)$ is properly between M and M^2.

To see the necessity of M begin principal consider $R = \mathbb{Z}[x]$ and $M = (2, x)$. Consider $I = (2, x^2)$. Clearly $x \notin I$ so I is a proper sub-ideal of M. Moreover, $2 \notin M^2$. (Indeed if it were then $2 = (a2 + bx)(c2 + dx) = ac4 + (ad + bc)2x + dbx^2$, thus $db = 0$ which implies, say $d = 0$. Thus $2 = ac4 + bc2x$. This implies $bc2 = 0$. If $b = 0$ then $2 = ac4$ a clear contradiction, so we must have $c = 0$. But this implies $2 = a2 + bx$ also a clear contradiction.) Thus $I \neq M^2$. $\square$

(7) Let G be a non-abelian group of order p^3 where p is a prime. Prove that the center $Z(G)$ of G is of order p and that $Z(G) = [G, G]$ where $[G, G]$ is the commutator subgroup of G, that is the subgroup generated by $xyx^{-1}y^{-1}$ for all $x, y \in G$.

Solution. Since G is a p-group it has nontrivial center. Thus $|Z(G)| = p, p^2$ or p^3, but since G is non-abelian the order cannot be p^3. Thus we are left to show that $|Z(G)| \neq p^2$. If this were the case then $G/Z(G)$ would have order p and hence be cyclic. So $G/Z(G)$ is generated by a single element say, $gZ(G)$. Thus any element in G is of the from $g^n h$ for some n and $h \in Z(G)$. Given two elements a and b in G write them as $a = g^n z$ and $b = g^m z'$. We now see

$$ab = g^n z g^m z' = g^n g^m z z' = g^m g^n z' z = g^m z' g^n z = ab.$$

Thus G would have to be abelian, a contradiction. Therefore $|Z(G)| = p$.

Since $G/Z(G)$ has order p^2 we know it is an abelian group (indeed, we know it has nontrivial center and when we quotient by it we get a cyclic group, so arguing as above it must be abelian). Thus if we denote $Z(G)$ by Z then for any $a, b \in G$ we have $abZ = aZbZ = bZaZ = baZ$ so $b^{-1}a^{-1}ba \in Z(G)$ and $[G, G] \subset Z(G)$. Since G is non-abelian we know $[G, G] \neq \{e\}$ and since it is a subgroup of G it has order divisible by p. Thus $[G, G] = Z(G)$. □

(8) Let $M_n(\mathbb{C})$ be the group of $n \times n$ matrices with entries in the complex numbers $\mathbb{C}$.
   (a) Given two diagonalizable elements A and B in $M_n(\mathbb{C})$ there is an invertible matrix T in $M_n(\mathbb{C})$ such that TAT^{-1} and TBT^{-1} are both diagonal matrices if and only if $AB = BA$.
   (b) Let A be a nonsingular diagonalizable matrix in $M_n(\mathbb{C})$. Prove there is a polynomial $f(x) \in \mathbb{C}[x]$ such that $A^{-1} = f(A)$.

Solution. (a) Suppose v is an eigenvector for A so that $Av = \lambda v$. Then notice that

$$ABv = BAv = B\lambda v = \lambda v.$$

Thus is we let E_λ be the eigenspace of A corresponding to the eigenvalue λ then $B(E_\lambda) \subset E_\lambda$. That is B preserves the eigenspaces of A. Thus we can choose eigenvectors $v_1, \ldots, v_n$ for B that span $\mathbb{C}^n$ and so that each v_i is also an eigenvector of A. (This is easy to do, just restrict B to E_λ and pick eigenvectors for B as a linear transformation on E_λ. Do this for each eigenspace.) Let T be the $n \times n$ matrix with columns given by the v_i's. Clearly TAT^{-1} and TBT^{-1} are both diagonal matrices.

Conversely assume that you can find the desired T then

$$AB = (T^{-1}DT)(T^{-1}D'T) = T^{-1}DD'T = T^{-1}D'DT = T^{-1}D'TT^{-1}DT = BA,$$

where $D = TAT^{-1}$ and $D' = TBT^{-1}$.

(b) Consider $A = A$ and $B = A^{-1}$. Clearly A and B satisfy the hypotheses of part (a) so there is aK that simultaneously diagonalizes A and B. Let $c_1, \ldots, c_n$ be the values along the diagonal of D (from part (a)) and $d_1, \ldots, d_n$ the values along the diagonal of D'. Of course $d_i = c_i^{-1}$. There is a polynomial $f(x)$ that will take the value d_i at the point c_i. (If we look at the distinct values of the c_i's and the d_i's we get a one-to-one correspondence between them. Given such a correspondence it is easy to construct a polynomial that will induce this correspondence.) Thus

$$f(A) = f(TDT^{-1}) = Tf(D)T^{-1} = TD'T^{-1} = B = A^{-1},$$

where the second inequality follows since $(TDT^{-1})^k = TD^kT^{-1}$ and the third inequality follows since evaluating a polynomial on a diagonal matrix is the same as evaluating the polynomial on the diagonal elements of the matrix. □