Algebra Comprehensive Exam
— Spring 2010 —

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

(1) If a group G contains a subgroup H of finite index and $H \neq G$ then it contains a normal subgroup of finite index (that is not equal to all of G). Hint: consider actions of G.

Solution: Let C be the set of cosets of H in G. The group G acts on C, that is given $g \in G$ there is a bijection $\sigma_g : C \to C$ which sends a coset $g'H$ to $(gg')H$. If S_C denotes the group of permutations of C then we have a homomorphism $r : G \to S_C$. We know S_C is finite since C is, thus $G/\ker r$, being isomorphic to a subgroup of S_C, is finite. Since $[G : \ker r]$ equals the order of $G/\ker r$ we know that $\ker r$ is a finite index subgroup of G and kernels are always normal so it is also normal. Since $H \neq G$, we have $\ker r \neq G$.

(2) If G is a non-abelian group of order p^3 for p a prime, then the center of G is the subgroup generated by all elements of the from $aba^{-1}b^{-1}$ for $a, b \in G$.

Solution: The center $Z(G)$ of G is a normal subgroup of G and has index either 1, p, p^2 or p^3. If the index is not 1 since that would imply G is abelian. If the index is p then $G/Z(G)$ would be a group of order p and hence a cyclic group. This implies that G is abelian (see * below), thus the index cannot be p. From the class equation we know the center of a group whose order is a prime power cannot be trivial. Thus the index is not p^3. Thus the index of $Z(G)$ in G is p^2 and $Z(G)$ has order p. So $G/Z(G)$ is a group of order p^2. This implies $G/Z(G)$ is abelian (if H is a group of order p^2 then suppose $Z(H) \neq H$, from above we know $Z(H) \neq 0$ so $H/Z(H)$ is a cyclic group and hence H is abelian). So if a, b are any elements in G we have $abZ(G) = (aZ(G))(bZ(G)) = (bZ(G))(aZ(G)) = baZ(G)$ and hence $aba^{-1}b^{-1} \in Z(G)$. Thus the commutator subgroup $[G, G]$ is a subgroup of $Z(G)$. The subgroup $[G, G]$ must thus have order 0 or p. If its oder was 0 then G would be abelian so we know $Z(G) = [G, G]$.

Proof of *: Since $G/Z(G)$ is cyclic there is some $g \in G$ such that 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 $b = g^m z'$, with $z, z' \in Z(G)$. We now see $ab = g^n z g^m z' = g^n g^m z z' = g^m g^n z' z = g^m z' g^n z = ab$.

(3) Prove that two $n \times n$ complex matrices A, B have the same characteristic polynomial if and only if $\mathrm{tr}(A^k) = \mathrm{tr}(B^k)$ for all integers $k \geq 1$.

Solution:

($\Rightarrow$) Suppose A and B have the same characteristic polynomial. Then A and B have the same eigenvalues, say $\lambda_1, \ldots, \lambda_n$. So $\lambda_1^k, \ldots, \lambda_n^k$ are the eigenvalues of A^k and B^k. Hence $\mathrm{tr}(A^k) = \mathrm{tr}(B^k)$, for all $k \geq 1$.

($\Leftarrow$) Let e_k be the kth elementary symmetric polynomial in n variables $x_1, \ldots x_n$, That is

$$e_k(x_1, \ldots, x_n) = \sum_{1 \leq j_1 < \cdots < j_k \leq n} x_{j_1} \cdots x_{j_n}.$$

We know that any symmetric polynomial in $x_1, \ldots, x_n$ can be written as some polynomial combination of $e_1, \ldots, e_n$. Let

$$p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k.$$

From the above fact we know that each p_k is some polynomial combination of the e_i. Notice that $e_1 = p_1$. One can also easily see that $2e_2 = p_1^2 - p_2 = p_1 e_1 - p_2$. In general from Newton's identity we know that p_k can be written as a combination of the $e_j, j < k$ and $p_i, i \leq k$.

Since $\mathrm{tr}(A) = \mathrm{tr}(B)$ we know the contact term of their characteristic polynomials is the same since the contact term for, say A, is $e_1(\lambda_1, \ldots, \lambda_n) = p_1(\lambda_1, \ldots, \lambda_n) = \mathrm{tr}(A)$ and similarly for B. Since the linear term in the characteristic polynomial is e_2 evaluated on the eigenvalues and this can be written in terms of e_1 and the traces of the powers of the matrices, we see that the linear term is the same as well. We can inductively see that each successive term in the characteristic polynomials of A and B are the same.

(4) Let K be field extension of the field F and $\alpha \in K$. Show that the degree of $F(\alpha)$ over F is finite if and only if α is algebraic over F. When proving finite dimensionality of $F(\alpha)$ over F construct a basis for $F(\alpha)$.

Solution: ($\Rightarrow$) Since $F(\alpha)$ is finite dimensional over F the infinite the sequence $1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots$ is linearly dependent. Let n be the smallest positive integer such that $1, \alpha, \ldots, \alpha^n$ is dependent over F. There exists $c_0, \ldots, c_n$ such that $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$; so α satisfies the polynomial $c_0 + c_1 x + \cdots + c_n x^n \in F[x]$.

($\Leftarrow$) Since α is algebraic over F it is a root of some polynomial in $F[x]$. Let $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in F[x]$ be a polynomial of minimal degree with α as a root. Any element in $F(\alpha)$ is some linear combination of powers of α so it is of the form $f(\alpha)$ for some element $f(x) \in F[x]$. By the Euclidean Algorithm in $F[x]$ we know there are polynomials $q(x)$ and $r(x)$ with the degree of $r(x)$ less than n such that $f(x) = p(x)q(x) + r(x)$. Thus our given element is of the form

$$f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Since the degree of r is less than n that means there are constants $d_0, \ldots, d_{n-1}$ such that $f(\alpha) = d_0 + d_1\alpha + \cdots + d_{n-1}\alpha^{n-1}$. So clearly $1, \alpha, \ldots, \alpha^{n-1}$ spans $F(\alpha)$. This set is also linearly independent since if not then there would be some degree $n-1$ polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$ contradicting the minimality of $p(x)$.

(5) Let A be a commutative ring with identity and let N be the ideal of nilpotent elements. It is known, and you may use without proof, that N is the intersection of all prime ideals in A. Show the following are equivalent:
(a) A has one prime ideal,
(b) every element of A is either a unit or nilpotent,
(c) A/N is a field.

Solution: ((a) $\Rightarrow$ (b)): If $a \in A$ then consider the ideal (a) generated by a. If $(a) = A$ then a is a unit as $1 \in (a)$. If $(a) \neq A$ then (a) is contained in a proper maximal ideal M. Since maximal ideals in a commutative ring with identity are prime, M must be the unique maximal ideal. Thus from the fact stated in the problem $N = M$ so $a \in N$ showing that it is nilpotent.

((b) $\Rightarrow$ (c)): Let $a + N$ be an element of A/N. If $a + N \neq N$ then $a \notin N$ so a is a unit in A. Thus there is an element b such that $ab = 1$ and so $(a + N)(b + N) = 1 + N$. So $a + N$

has a multiplicative inverse unless it is the zero element in A/N. In other words A/N is a field.

((c) $\Rightarrow$ (a)): Since A is commutative we know that A/N is a field if and only if N is a maximal ideal. Thus N is a maximal ideal. Since N is the intersection of prime ideals in A we see that for any prime ideal P we have $N \subset P$. Since N is maximal $N = P$. Hence there is only one prime ideal.

(6) If S and T are finite dimensional vector spaces of some field and $V = S \oplus T$ then the linear map $p : V \to V$ defined by $p(s + t) = s$ where $s \in S$ and $t \in T$ is called a projection along T.
 (a) Show that a linear map $\rho : V \to V$ is a projection if and only if $\rho^2 = \rho$.
 (b) Show that if ρ is a projection then there is another projection ρ' such that $v = \rho(v)+\rho'(v)$ for all $v \in V$.
 (c) If ρ and ρ' are two projections and $\rho\rho' = \rho'\rho$ then show that $\rho\rho'$ is a projection. Show that $\rho\rho'$ does not have to be a projection if ρ and ρ' do not commute.
 (d) What are the eigenvalues of a projection?

Solution: Part (a): If ρ is a projection then $V = S \oplus T$ and $\rho(s+t) = s$, so $\rho^2(s+t) = \rho(s) = s = \rho(s+t)$. That is $\rho^2 = \rho$. Conversely, if $\rho^2 = \rho$ then set $S = \mathrm{Im}\rho$ and $T = \ker \rho$. Notice that if $v \in S \cap T$ then there is some $w \in V$ such that $\rho(w) = v$; so $0 = \rho(v) = \rho(\rho(w)) = \rho(w) = v$. Thus $T \cap S = 0$. Since the rank nullity theorem says $\dim(T) + \dim(S) = \dim(V)$ we know that $V = S \oplus T$ and $\rho(s + t) = \rho(\rho(s')) + \rho(t) = \rho(s') = s$ where $s' \in V$ such that $\rho(s') = s$.

Part (b): Given a projection $\rho : V \to V$ let $\rho' = id_V - \rho$. Notice that $(\rho')^2 = 1 - 2\rho + \rho^2 = 1 - 2\rho + \rho = 1 - \rho = \rho'$, so ρ' is a projection by part (a). Clearly $v = \rho(v) + \rho'(v)$.

Part (c): Clearly $(\rho\rho')^2 = \rho\rho'\rho\rho' = \rho\rho\rho'\rho' = \rho\rho'$; so $\rho\rho'$ is a projection. Now let v_1 and v_2 be the two standard basis vectors for $\mathbb{R}^2$ and set $V_1 = \text{span } v_1, V_2 = \text{span } v_2, V_3 = \text{span } v_1 + v_2$. Let ρ be the projection to V_1 along V_2 and ρ' the projection to V_2 along V_3. then $\rho'\rho(v_1) = \rho'(v_1) = \rho'((v_1 + v_2) - v_2) = -v_2$, but $\rho'\rho\rho'\rho(v_1) = \rho'\rho(-v_2) = \rho'(0) = 0$. So $\rho'\rho$ is not a projection.

Part (d): One can easily see that if ρ is a projection to S along T then any vector $s \in S$ is an eigenvector with eigenvalue 1 and any vector $t \in T$ is an eigenvector with eigenvalue 0. As $V = S \oplus T$ we clearly have that 0 and 1 are the only possible eigenvalues (and they both occur except in the trivial cases).

(7) Let G be a group of order 5075 ($= 5^2 \cdot 7 \cdot 29$). Let P be a Sylow 5-subgroup of G, let Q be a Sylow 29-subgroup of G.
 (a) Show P is a normal subgroup of G.
 (b) Show that G has a normal subgroup H of oder $5^2 \cdot 29$. [Hint: Look at G/P.]
 (c) Show that Q is a normal subgroup of G. [Hint: Relate Q to H.]

Solution: (a) $n_5 = 1(\mod 5)$, and $n_5 | 7 \cdot 29$ so $n_5 = 1, 7, 29$, or 203. Hence $n_5 = 1$, and a Sylow theorem says P is normal.

(b) Consider the group G/P. This is a group since P is normal and the group has order $7 \cdot 29$. In this group consider the Sylow 29 subgroup $\overline{H}$. We know there are $1, 30, \ldots$ Sylow 29 subgroups but the number of them must divide 7 so there is just one and again it must be normal by a Sylow theorem. Now we know the subgroups of G/P are in one to one correspondence with subgroups of G containing P and this correspondence respects normality. So let H be the subgroup of G containing P such that $H/P \cong \overline{H}$. $|H| = |P|[H : P] = 5^2 \cdot 29$ and H is normal in G.

(c) Note that H has an element of order 29 by Cauchy's theorem. So H has a subgroup Q' of order 29. Since this is a Sylow 29 subgroup of G we know that Q' is conjugate to Q. Thus there is some g such that $Q = gQ'g^{-1} \leq gHg^{-1} = H$. So $Q \leq H$. Since the number of Sylow 29 subgroups of H is a divisor of 25 and equal to $1, 30, \ldots$ we know there is just one. Thus Q is a normal and characteristic subgroup of H. But since H is normal in G we know Q is normal in G.

(8) Let R be a ring (not-necessarily commutative). We say an ideal P of R is prime if $P \neq R$ and whenever there are two ideals I and$J$ such that $IJ \subset P$ then either $I \subset P$ or $J \subset P$. (When R is commutative this is equivalent to the definition of prime in terms of elements of R.) Show the following are equivalent:
(a) All ideals not equal to R are prime.
(b) The ideals of R are linearly ordered (under set containment) and all ideals I satisfy $I^2 = I$.
If either of these conditions holds and R is a commutative ring with identity show that R is either the trivial ring or a field.

Solution: ((a) $\Rightarrow$ (b)) Given two ideals I and J of R we have that $I \cap J$ is a prime ideal and hence $IJ \subset I \cap J$ implies $I \subset I \cap J$ or $J \subset I \cap J$. Thus $I \subset J$ or $J \subset I$. Now for I a proper ideal in R notice that $II \subset I^2$ so the primeness of I^2 implies $I \subset I^2$. Thus $I = I^2$.

((b) $\Rightarrow$ (a)) Let P be any ideal of R. Suppose that $IJ \subset P$ for I, J ideals of R. We know that $I \subset J$ or $J \subset I$, without loss of generality we assume $I \subset J$. Thus $II \subset IJ \subset P$. But since $I = I^2$ we see that $I \subset P$. So P is prime.

Now assume R is commutative and all ideals are prime. Then the zero ideal (0) is prime so R contains no zero divisors and $1 \neq 0$. If a is a non-zero element then consider the ideal (a^2). Since $aa \in (a^2)$ and (a^2) is prime we have $a \in (a^2)$. Thus there is some $b \in R$ such that $a = a^2b$. thus $1 = ab$. That is a is a unit with inverse b.