Algebra Comprehensive Exam
— Spring 2007 —

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

(1) Let A be a commutative ring. The ring A is called *Artinian* if it satisfies the decreasing chain condition: if $I_1 \supseteq I_1 \supseteq, \ldots.$ is a sequence of ideals in A then there is some N such that $I_N = I_{N+1} = \ldots.$ If A is an Artinian integral domain show that A is a field. (Hint: given a non-zero element consider the ideal generated by it.)

Solution. Consider a non-zero element $a \in A$. Assume a is not a unit then $I = (a)$ is a proper ideal of A. The idea $I^n = (a^n)$. Notice that I^{k+1} is a proper subset of I^k. To see this suppose that $a^k \in I^{k+1}$, then $a^k = a^{k+1}g$ for some $g \in A$. So $a^k(1 - ag) = 0$. Since A is an integral domain either $a^k = 0$ or $1 - ag = 0$. But we cannot have $s^k = 0$ since if k is the smallest positive integer such that $a^k = 0$ then a and a^{k-1} are zero divisors which don't exist in an integral domain. So we know $1 - ag = 0$ and hence g is the inverse of a and a is a unit. This contradicts a not being a unit so I^{k+1} is a proper subset of I^k for all k. But this contradicts A being Artinian, thus a must be a unit. □

(2) Let G be a group of order p^n, where p is a prime number and n is a positive integer. If N is a normal subgroup of G of order p then show N is in the center of G.

Solution. Note that the conjugate of any element in N by any element of G remains in N since N is normal. Thus the orbit of any element of N under the action of conjugation by elements of G is contained in N. The size of the orbit of $x \in N$ is given by $[G : G_x]$ where G_x is the stabilizer of x under the action of conjugation. Since $|G| = [G : G_x]|G_x|$ we know that $[G : G_x]$ is a power of p. But since this is the size of the orbit of x it must be less than or equal to p since the orbit is contained in N. If the size of the orbit were p then conjugation by G is transitive on N, but this is not possible since $1 \in N$ is fixed by conjugation. Thus the orbit of x cannot have size p and hence must have size 1. Of course any element whose conjugacy orbit has size 1 is in the center of the group. Thus N is in the center of G. □

(3) In which of the following rings is every ideal principal? Justify your answer.

$$(i)\ \mathbb{Z} \oplus \mathbb{Z}, \qquad (ii)\ \frac{\mathbb{Z}}{(4)}, \qquad (iii)\ \frac{\mathbb{Z}}{(6)}[x], \qquad (iv)\ \frac{\mathbb{Z}}{(4)}[x].$$

Solution. Note that every ideal of the ring $A \oplus B$ is of the form $\mathfrak{a} \oplus \mathfrak{b}$ for ideals $\mathfrak{a} \subset A$ and $\mathfrak{b} \subset B$. If $\mathfrak{a} = (a)$ and $\mathfrak{b} = (b)$, then it is easily seen that $\mathfrak{a} \oplus \mathfrak{b}$ is generated by the element $(a, b) \in A \oplus B$, hence is a principal ideal.

(i) Since $\mathbb{Z}$ is a principal ideal domain, the above shows that every ideal of $\mathbb{Z} \oplus \mathbb{Z}$ is principal.

(ii) Every ideal of $\mathbb{Z}/(4)$ is the image of an ideal of $\mathbb{Z}$, hence is principal.

(iii) The Chinese remainder theorem implies that $\frac{\mathbb{Z}}{(6)}[x] \approx \frac{\mathbb{Z}}{(2)}[x] \oplus \frac{\mathbb{Z}}{(3)}[x]$. Since each of $\frac{\mathbb{Z}}{(2)}[x]$ and $\frac{\mathbb{Z}}{(3)}[x]$ is a principal ideal domain, it follows that every ideal of $\frac{\mathbb{Z}}{(6)}[x]$ is principal.

(iv) Suppose the ideal $(2, x)$ of $\mathbb{Z}/(4)[x]$ is principal, then so is its image in the ring $\mathbb{Z}[x]/(4, x^2)$. Consequently there exist $a, b \in \mathbb{Z}/(4)$ with $(2, x) = (a + bx)$ in $\mathbb{Z}[x]/(4, x^2)$. Examining this modulo x and modulo 2, we see that $a = 2$ and $b = \pm 1$, i.e., without loss of generality, we have $(2, x) = (2 + x)$ in $\mathbb{Z}[x]/(4, x^2)$. In particular, $2 = (2 + x)(c + dx)$ and so $2c = 2$ and $c + 2d = 0$ in $\mathbb{Z}/(4)$. But this gives a contradiction, so $(2, x)$ in not a principal ideal of $\mathbb{Z}/(4)[x]$. □

(4) Let F be a field extension of K of degree n.
   (a) Show for each $\alpha \in F$, multiplication by α induces a linear map of F to itself (recall F is a vector space over K).
   (b) Show every field extension of K of degree n is (ring) isomorphic to a subring of $GL(n, K)$. ($GL(n, K)$ is the ring of $n \times n$ matrices with entries in K.)

Solution. (a) Let α be an element of F. Clearly $f_\alpha : K \to K$ is a well-defined map. Note $f_\alpha(a + b) = \alpha(a + b) = \alpha a + \alpha b = f_\alpha(a) + f_\alpha(b)$ for all a and b in F. Moreover $f_\alpha(ab) = \alpha ab = a(\alpha b) = af_\alpha(b)$ for $a \in K$ and $b \in F$. Thus f_α is a linear map.

(b) Let $b_1, \ldots, b_n$ be a basis for K thought of as a vector space over F. So $f_\alpha(b_i) = \sum c_{ij} b_j$. Thus if we set M_α to be the matrix (c_{ij}) then we get a matrix representing the map f_α. Moreover, this matrix is in $GL(n, K)$. Thus we have defined a map $\phi : F \to GL(n, K)$ that sends α to M_α (we will use the same basis b_i for all $\alpha \in F$). We must now show ϕ is a homomorphism. To this end let α and β be elements of F. Then $f_{\alpha\beta}(a) = \alpha\beta(a) = \beta\alpha(a) = f_\beta(\alpha(a)) = f_\alpha \circ f_\beta(a)$ and recall that matrix multiplication correspond to composition of the associated map. Thus $M_{\alpha\beta} = M_\alpha M_\beta$ and $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$. Similarly $f_{\alpha+\beta}(a) = (\alpha+\beta)a = \alpha a + \beta a = f_\alpha(a) + f_\beta(a)$ and so $M_{\alpha+\beta} = M_\alpha + M_\beta$. Thus ϕ is a ring homomorphism. Finally it is clear that ϕ is not the trivial homomorphism since $\phi(\alpha)(a) = \alpha a \neq 0$ if α and a not equal to zero. Thus, since the only ideals in F are the trivial ideal and F, the kernel of ϕ is the trivial idea. And ϕ is a monomorphism from K to $GL(n, K)$. □

(5) Let k be a field of characteristic $\neq 2, 3$. Prove that the following statements are equivalent:
   (a) Any sum of squares in k is itself a square.
   (b) Whenever a cubic polynomial f factors completely in k, so does its derivative f'.

Solution. (a) $\Rightarrow$ (b): Let $f(X) = (X - a)(X - b)(X - c)$, with $a, b, c \in k$. Then, $f'(X) = 3X^2 - 2(a + b + c)X + (ab + bc + ca)$. Consider, the discriminant of f' namely,

$$4(a + b + c)^2 - 12(ab + bc + ca) = 2((a - b)^2 + (b - c)^2 + (c - a)^2).$$

The righthand side is a sum of square and hence itself a square say d^2. Then, $f'(X) = 3(X - \frac{2(a+b+c)+d}{6})(X - \frac{2(a+b+c)-d}{6})$.

(b) $\Rightarrow$ (a): Let $\alpha, \beta \in k$. Consider the cubic polynomial, $f(X) = (X - \alpha)(X - \beta)(X + \alpha)$. Since, the discriminant of f' has to be a square we have that, $2((\alpha-\beta)^2 + (\beta+\alpha)^2 + (2\alpha)^2) = 4(3\alpha^2 + \beta^2)$ is a square. Hence, $3\alpha^2 + \beta^2$ is square for all $\alpha, \beta \in k$.

Now, let $x, y \in$. Then, $x^2 + y^2 = 3(x^2/3) + y^2$. We claim that, $x^2/3$ is a square. This is true because, $x^2/3 = 3(x/3)^2 + 0^2$ which is a square as proved earlier. Thus, $x^2 + y^2 = 3(x^2/3) + y^2$ is a square too. The rest follows by induction on the number of terms in the sum of squares. □

I

(6) Assume B is an $n \times n$ real symmetric matrix that and satisfies $v^T B v > 0$ for all non-zero vectors v. (Here v^T means the transpose of v.) Show that there is a real matrix C such that $C^2 = B$. (Hint: diagonalize.)

Solution. Since B is diagonalizable there is a matrix E and a diagonal matrix D such that $B = EDE^{-1}$. Note that since B is diagonalizable there is a basis of eigenvectors. Since B is symmetric, eigenvectors for distinct eigenvalues are orthogonal and we can assume this eigen-bases is othonormal (just apply Gram-Schmidt to each eigenspace). Recall we can take E^{-1} to be the matrix whose columns consist of the eigenvectors. Thus it is easy to check that $E^{-1} = E^T$ and we have $B = EDE^T$. We claim that all the diagonal entries in D are positive. Indeed, let e_i be a standard basis vector in $\mathbb{R}^n$ and let $v_i = Ee_i$. Then $e_i^T De_i = (E^T v_i)^T D(E^T v_i) = v_i^T EDE^T v_i = v_i^T Bv_i > 0$. But $e_i^T Dd_i$ is the i^{th} diagonal element in D. Let D' the diagonal matrix with diagonal entries equal to the square root of the diagonal entries on D. Set $C = ED'E^T$. So $C^2 = ED'E^T ED'E^T = E(D'D')E^T = EDE^T = B$. $\square$

(7) Let G be a *non-abelian* group of order p^2q where $p > q$ are prime.
  (a) Show G contains a normal subgroup.
  (b) Can the Sylow p and Sylow q-subgroups of G both be normal? Justify your answer.

Solution. (a) Let G be a group of order p^2q.. Let n_p be the number of Syow p-subgroups of G. We know $n_p = 1 + mp$ for some non-negative integer m. Moreover $n_p|q$ and since $q < p$ we see that $m = 0$ and the Sylow p-subgroup is normal.

(b) No the Sylow q-subgroup cannot be normal. From above we know there is a unique Sylow p-subgroup P and it is normal. If there is a Sylow q-subgroup Q that is normal then notice that $Q \cap P = \{1\}$ since elements of Q are powers of q and elements of P are powers of p. In addition PQ will be a subgroup of G whose order is larger than p^2 so by Lagrange's theorem we know $PQ = G$. Thus $G = P \times Q$. We also know that P is abelian since all groups of order a prime squared are abelian. Finally Q is abelian since groups of order a prime are cyclic. Thus G is the product of two abelian groups and therefore must be abelian. This contradicts the fact that G is non-abelian. So the Sylow q-subgroup cannot be normal. $\square$

(8) Let G be a finite group with an automorphism φ such that $\varphi(x) = x$ if and only if $x = e$.
  (a) Show that every element of G can be written as $x^{-1}\varphi(x)$.
  (b) If p is a prime dividing $|G|$, prove that G has a unique p-Sylow subgroup P satisfying $\varphi(P) = P$.

Solution. (a) If $x^{-1}\varphi(x) = y^{-1}\varphi(y)$, then $yx^{-1} = \varphi(yx^{-1})$, and so we must have $yx^{-1} = e$, i.e., $y = x$. Consequently the map $f : G \longrightarrow G$ with $f(x) = x^{-1}\varphi(x)$ is injective. Since G is finite, it must be surjective as well.

(b) Let $P_0 < G$ be a p-Sylow subgroup. The order of every element of $\varphi(P_0)$ is a power of p, and so $\varphi(P_0)$ is also a p-Sylow subgroup of G. Consequently there exists $g \in G$ such that $\varphi(P_0) = gP_0g^{-1}$. There exists $x \in G$ such that $g^{-1} = x^{-1}\varphi(x)$. Then

$$\varphi(xP_0x^{-1}) = \varphi(x)gP_0g^{-1}\varphi(x^{-1}) = xP_0x^{-1}.$$

Consequently $P = xP_0x^{-1}$ is a p-Sylow subgroup with $\varphi(P) = P$.

Next, suppose that $y \in N_P$. Then $\varphi(yPy^{-1}) = \varphi(P)$, i.e., $\varphi(y)P\varphi(y^{-1}) = P$, and so $\varphi(y) \in N_P$. This implies that $\varphi(N_P) \subseteq N_P$, and since φ is injective, we have $\varphi(N_P) = N_P$. Since N_P is a group with an automorphism φ with no fixed points except e, by part (a), every element of N_P can be written uniquely as $n^{-1}\varphi(n)$ with $n \in N_P$.

Now suppose zPz^{-1} is another p-Sylow subgroup of G satisfying $\varphi(zPz^{-1}) = zPz^{-1}$, then $\varphi(z)P\varphi(z^{-1}) = zPz^{-1}$, and so $z^{-1}\varphi(z) \in N_P$. By the observation above, we must have $z \in N_P$, and so $zPz^{-1} = P$. $\square$