MATHEMATICS QUALIFYING EXAMINATION
in
ALGEBRA

January, 2005

Instructions: Complete six of the following problems, including three problems from each section. *Only your best three problems from each section will count.* Complete solutions are worth more than partial solutions.

Time permitted: 4 hours.

SECTION A

1. Let A be an $n \times n$ complex matrix. Suppose that A is unitary and all eigenvalues of A are nonnegative real numbers. Prove that $A = I$, the $n \times n$ identity matrix.

2. Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be a linear operator. Let $F[T]$ denote the ring of all linear operators on V that can be expressed as polynomials in T. Assume that no nonzero proper subspace of V is mapped into itself by T.
   (a) If $0 \neq S \in F[T]$, show that $\{v : S(v) = 0\}$ is the zero subspace.
   (b) Prove that every nonzero $S \in F[T]$ is invertible.

3. For every $n \times n$ complex matrix A, denote by $C(A)$ the complex vector space of all $n \times n$ complex matrices X such that $AX = XA$. If A is a 2×2 matrix, what are the possibilities for the dimension of $C(A)$? Justify your answer.

4. Let V be the vector space of all real 3×3 matrices. Show that every 4-dimensional subspace $U \leq V$ contains a nonzero diagonalizable matrix.
   Hint: Consider the subspace S consisting of all symmetric 3×3 matrices.

5. Let V be a 4-dimensional vector space over a field F, and let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two bases for V. Show that there exists a basis for V consisting of two members of $\mathcal{B}_1$ and two members of $\mathcal{B}_2$.

6. Let V be the vector space of all continuous functions $\mathbb{R} \to \mathbb{R}$. For *at least two* of the following indicated subspaces in (a,b,c), find the dimension of the indicated subspace, and give an explicit basis.

   (a) The subspace consisting of all functions f such that f is piecewise linear, with the restriction of f to each of the intervals $(-\infty, -1]$, $[-1, 1]$, $[1, \infty)$ being linear.

   (b) The subspace consisting of all functions f satisfying $f(a+b) = f(a) + f(b)$ for all $a, b \in \mathbb{R}$.

   (c) The subspace spanned by all functions of the form $f(x) = \sin(x+a)\sin(x+b)$ where $a, b \in \mathbb{R}$.

7. Let $v_1, v_2, \ldots, v_n$ be vectors in a real inner product space. Define A to be the $n \times n$ matrix whose (i,j)-entry is (v_i, v_j). Prove that A is positive definite if and only if the vectors are linearly independent.

8. Let V be an n-dimensional vector space over a field F. Let $(\ ,\ ) : V \times V \to F$ be a map which is linear on the 1st position and also linear in the 2nd position. (Such a map is called a *bilinear form.*) Let $w_1, w_2, \ldots, w_k \in V$. Prove that $\{v \in V \ : \ (w_i, v) = 0$ for $i = 1, 2, \ldots, k\}$ is a subspace of V of dimension at least $n - k$.

   Hint: Consider $L : V \to F^k$ mapping a vector $v \in V$ to the transpose of $[(w_1, v), (w_2, v), \ldots, (w_k, v)]$.

SECTION B

9. Let G be a group, and let S be a subset of G. If S is a right coset of a subgroup $H_1 \leq G$ and also a right coset of a subgroup $H_2 \leq G$, prove that $H_1 = H_2$.

10. Let G be a finite group.

    (a) If G is cyclic and H is a subgroup of G, prove that $\phi(H) = H$ for all $\phi \in Aut(G)$.

    (b) If $C \leq H \trianglelefteq G$ where H is cyclic, show that C is a normal subgroup of G.

11. Let G be a finite group with exactly n Sylow p-subgroups for some prime p. Show that there exists a subgroup H of the symmetric group S_n such that H also has exactly n Sylow p-subgroups.

12. Let G be a subgroup of the multiplicative group of real invertible 2×2 matrices. If $A^2 = I$ for every $A \in G$, prove that the order of G divides 4.

13. Let $f(X, Y)$ be a polynomial with real coefficients, and suppose $f(a, a^2) = 0$ for every $a \in \mathbb{R}$. Prove that $f(X, Y) = (Y - X^2)g(X, Y)$ for some polynomial $g(X, Y)$ with real coefficients.

14. Let R be the ring of all continuous real-valued functions $\mathbb{R} \to \mathbb{R}$, and for every $a \in \mathbb{R}$, let M_a be the set of all $f \in R$ such that $f(a) = 0$. Prove that M_a is a maximal ideal of R.

15. Let $F = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$ where α is the real cube root of 2. Prove that F is a field, and that $\sqrt{2} \notin F$.

16. Let F be an arbitrary field, and let $F[\![X]\!]$ be the set of formal Laurent series $a_k X^k + a_{k+1}X^{k+1} + a_{k+2}X^{k+2} + \cdots$ where $a_i \in F$ and $k \in \mathbb{Z}$. Prove that $F[\![X]\!]$ has a multiplicative identity, and that every nonzero element of $F[\![X]\!]$ has a multiplicative inverse. (It follows that $F[\![X]\!]$ is a field; you are *not* required to show this.)

SOLUTIONS

DISCLAIMER: You should not read solutions for any problem until *after* trying the problem yourself, and that should happen only after you have studied the relevant material (any graduate-level textbooks on linear and abstract algebra will suffice). Moreover, these printed solutions are *not a substitute* for personal attention of our faculty who are anxious to discuss your work on any problems you have attempted. In any case, *do not* expect that memorized solutions such as these will be helpful to reproduce in written work on future exams. It is the most basic themes (how to use diagonal and other canonical forms for matrices; applications of the isomorphism theorems; etc.. . .) and not individual problems that you may expect to recur. *Again:* it is only by attempting problems, then seeking help if you find you are stuck, that you can hope to learn; *not* by memorizing printed solutions.

1. Since A is unitary, we have $A = U^{-1}DU$ where U is invertible (in fact unitary, although we don't need this) and D is diagonal with diagonal entries $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$ such that $|\lambda_i| = 1$ for all i. Now the hypothesis that $\lambda_i \in [0, \infty)$ forces every eigenvalue $\lambda_i = 1$, so $D = I$ and $A = U^{-1}U = I$.

2. Since $S \in F[T]$, we have that S commutes with T and so $\ker(S)$ is invariant under T. (This is a standard fact with a short proof: if $Sv = 0$ then $TSv = STv = 0$ so $Tv \in \ker(S)$.) By hypothesis we must have $\ker(S) = \{0\}$ or V. The first alternative is ruled out by the hypothesis that $S \neq 0$, so in fact $\ker(S) = 0$ and (a) holds. Also since V is finite dimensional, $\ker(S) = 0$ implies that S is surjective, so (b) holds.

3. Consider first the case that A is in Jordan normal form. If $A = \left[\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right]$ then comparing entries on both sides of $AX = XA$ we see that X must be diagonal, unless $\lambda = \mu$ in which case X is arbitrary; thus $C(A)$ has dimension 2 or 4 respectively. Otherwise $A = \left[\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right]$ and comparing entries on both sides of $AX = XA$ shows that $X = \left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right]$ for some $a, b \in \mathbb{C}$, i.e. $C(A)$ is 2-dimensional.

   Now $C(A)$ must have dimension 2 or 4 in the general case as well. This is because for every invertible matrix U, we have that X commutes with A, iff $U^{-1}XU$ commutes with $U^{-1}AU$, and in particular $C(U^{-1}AU) = U^{-1}C(A)U$ has the same dimension as $C(A)$.

4. Let $U \leq V$ be any 4-dimensional subspace, and let $S \leq V$ be the subspace consisting of all symmetric matrices. Note that S is 6-dimensional; in fact S has basis $\{E_{11}, E_{22}, E_{33}, E_{12}+E_{21}, E_{13}+E_{31}, E_{23}+E_{32}\}$ where E_{ij} is the elementary matrix with entry 1 in the (i, j)-position and zeroes elsewhere. Now

$$\dim(U \cap S) = \dim U + \dim S - \dim(U+S) \geq 4 + 6 - 9 = 1$$

   so $U \cap S$ contains a nonzero matrix; and this matrix is real symmetric, hence diagonalizable.

5. Let $\mathcal{B}_1 = \{u_1, u_2, u_3, u_4\}$ and $\mathcal{B}_2 = \{v_1, v_2, v_3, v_4\}$ be two bases for V. Since $\mathcal{B}_1$ spans V, there exist $a_1, \ldots, a_4 \in F$ such that $v_1 = a_1u_1+a_2u_2+a_3u_3+a_4u_4$. Since $v_1 \neq 0$, not all a_i are zero; so we may assume (after permuting the members of $\mathcal{B}_1$ if necessary) that $a_1 \neq 0$. Thus $u_1 = a_1^{-1}(v_1-a_2u_2-a_3u_3-a_4u_4)$. It follows that $V = \langle v_1, u_1, u_2, u_3, u_4\rangle = \langle v_1, u_2, u_3, u_4\rangle$ where $\langle S\rangle \leq V$ denotes the subspace spanned by a subset $S \subseteq V$. Thus $\{v_1, u_2, u_3, u_4\}$ is a basis of V. Similarly, $v_2 = b_1v_2+b_2u_2+b_3u_3+b_4u_4$ for some $b_i \in F$. Since $\{v_1, v_2\}$ is linearly independent, the coefficients b_2, b_3, b_4 are not all zero; so we may assume (after permuting u_2, u_3, u_4 if necessary) that $b_2 \neq 0$; thus $u_2 = b_2^{-1}(v_2-b_1v_2-b_3u_3-b_4u_4)$. It follows that $V = \langle v_1, v_2, u_2, u_3, u_4\rangle = \langle v_1, v_2, u_3, u_4\rangle$ and so $\{v_1, v_2, u_3, u_4\}$ is a basis for V.

6. (a) Every function $f \in V$ is uniquely determined by four real constants $a = f'(-2)$, $b = f(-1)$, $c = f(1)$, $d = f'(2)$ and has the form $f = af_1 + bf_2 + cf_3 + df_4$ where

$$f_1(x) = \begin{cases} x+1, & \text{if } x<-1; \\ 0, & \text{if } x\geq -1; \end{cases} \quad f_2(x) = \begin{cases} 1, & \text{if } x<-1; \\ (1-x)/2, & \text{if } -1\leq x<1; \\ 0, & \text{if } x\geq 1; \end{cases}$$

$$f_3(x) = \begin{cases} 0, & \text{if } x<-1; \\ (1+x)/2, & \text{if } -1\leq x<1; \\ 0, & \text{if } x\geq 1; \end{cases} \quad f_4(x) = \begin{cases} 0, & \text{if } x<1; \\ x-1, & \text{if } x\geq -1. \end{cases}$$

So $\{f_1, \ldots, f_4\}$ spans V and the uniqueness of the coefficients $a, \ldots, d$ in this linear combination means that we have a basis; thus $\dim(V) = 4$.

(b) By induction we have $f(mx) = mf(x)$ for all $m \in \mathbb{Z}$ and $x \in \mathbb{R}$; also if $m, n \in \mathbb{Z}$ with $n \neq 0$ then $nf\left(\frac{m}{n}\right) = mnf\left(\frac{1}{n}\right) = mf(1)$ so $f\left(\frac{m}{n}\right) = \frac{m}{n}f(1)$. Since f is continuous and $\mathbb{Q}$ is dense in $\mathbb{R}$, this means that $f(x) = f(1)x$ for all $x \in \mathbb{R}$. Thus the function $f_1(x) = x$ forms a basis for V, which has dimension 1.

(c) Note that

$$\begin{aligned} \sin(x+a)\sin(x+b) &= [\sin a\cos x + \cos a\sin x][\sin b\cos x + \cos b\sin x] \\ &= \sin a\sin b\cos^2 x + [\sin a\cos b + \cos a\sin b]\sin x\cos x \\ &\qquad + \cos a\cos b\sin^2 x \end{aligned}$$

is a linear combination of the functions $f_1(x) = \sin^2 x$, $f_2(x) = \sin x\cos x$, $f_3(x) = \cos^2 x$. If $af_1+bf_2+cf_2 = 0$ then evaluating at $0, \frac{\pi}{4}, \frac{\pi}{2}$ respectively gives $c = 0$, $(a+b+c)/2 = 0$, $a = 0$ which yields $a = b = c = 0$. Thus $\{f_1, f_2, f_3\}$ is a basis for V, which accordingly has dimension 3.

7. Let $v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ where $a_1, a_2, \ldots, a_n \in \mathbb{R}$; then

$$0 \leq (v, v) = \sum_{i=1}^{n}\sum_{j=1}^{n}(v_i, v_j)a_ia_j = a^TAa$$

where $a = (a_1, a_2, \ldots, a_n)^T \in \mathbb{R}^n$. In any case, A is positive semidefinite. Note that equality holds above iff $v = 0$. The matrix A is indefinite (i.e. *not* positive definite) iff there exists a nonzero n-tuple a such that $0 = a^T A a = (v, v)$, iff there exists a nonzero $a \in \mathbb{R}^n$ such that the linear combination $v = 0$, iff the vectors $v_1, v_2, \ldots, v_n$ are linearly dependent.

8. Consider $L : V \to F^k$ mapping a vector $v \in V$ to the transpose of $[(w_1, v), (w_2, v), \ldots, (w_k, v)]$. Clearly L is linear, with image $L(V) \leq F^k$ of dimension at most k. The required dimension is simply

$$\dim(\ker L) = \dim V - \dim L(V) \geq n - k.$$

9. Suppose $S = H_1 g_1 = H_2 g_2$ for some $g_1, g_2 \in G$. Denoting $S^{-1} = \{s^{-1} : s \in S\}$, we have

$$\begin{aligned} SS^{-1} &= \{s_1 s_2^{-1} : s_1, s_2 \in S\} = \{(xg_1)(yg_1)^{-1} : x, y \in H_1\} \\ &= \{xg_1 g_1^{-1} y^{-1} : x, y \in H_1\} = \{xy^{-1} : x, y \in H_1\} = H_1. \end{aligned}$$

   The same reasoning gives $SS^{-1} = H_2$.

10. (a) Let $H \leq G$ where G is a finite cyclic group. Then for every $\phi \in Aut(G)$, the subgroup $\phi(H) \leq G$ has the same order as H. Since H is the unique subgroup of order $|H|$, this forces $\phi(H) = H$.
    (b) Let $C \leq H \trianglelefteq G$ where C is cyclic. Let $g \in G$ and consider the inner automorphism of G given by $\psi_g(x) = gxg^{-1}$ for $x \in G$. Then $\psi_g(H) = H$ since $H \trianglelefteq G$, and the restriction of ψ_g to H gives an automorphism of H (not necessarily inner). Since H is cyclic, by (a) we must have $\psi_g(C) = C$, i.e. $C \trianglelefteq G$.

11. Let $P_1, P_2, \ldots, P_n$ be the distinct Sylow p-subgroups of G. For every $g \in G$, conjugation by g gives rise to a permutation $\psi_g \in S_n$ of the Sylow p-subgroups: $gP_i g^{-1} = P_{\psi_g(i)}$. Here we have identified each permutation of the Sylow p-subgroups, with the corresponding permutation of subscripts $1, 2, \ldots, n$. This is a permutation action of G of degree n, i.e. the map $\psi : G \to S_n$ given by $g \mapsto \psi_g$ is a homomorphism; the fact that $\psi_{gh} = \psi_g \psi_h$ for all $g, h \in G$ follows from

$$P_{\psi_{gh}(i)} = (gh)P_i(gh)^{-1} = ghP_i h^{-1} g^{-1} = gP_{\psi_h(i)} g^{-1} = P_{\psi_g(\psi_h(i))}.$$

   Let $H = \psi(G) \leq S_n$ and let $K = \ker(\psi) \trianglelefteq G$. We claim that the Sylow p-subgroups of H are given by $\psi(P_1), \ldots, \psi(P_n)$. In fact $|\psi(P_i)| = |P_i|/|P_i \cap K|$ by the First Isomorphism Theorem, so $\psi(P_i) \leq H$ is a p-subgroup; also the index

$$[H : \psi(P_i)] = [G : K]/[P_i : P_i \cap K] = [G : P_i]/[K : P_i \cap K]$$

   divides $[G : P_i]$ which is not divisible by p. Thus $\psi(P_i) \leq H$ is a Sylow p-subgroup.

12. Since every element of G has order 1 or 2, G is elementary abelian of order 2^k for some $k \geq 0$. By hypothesis, every $A \in G$ has minimal polynomial dividing $X^2 - 1 = (X+1)(X-1)$ so A is diagonalizable with eigenvalues ± 1, and since elements of G commute, they are *simultaneously* diagonalizable. Up to similarity (i.e. conjugation by a real 2×2 invertible matrix) H is contained in the Klein 4-subgroup $\left\{ \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \right\}$ so $|H|$ divides 4.

13. Every monomial X^iY^j satisfies $X^iY^j \equiv X^{i+2j} \bmod (Y - X^2)$. [Here $(Y - X^2) \subset \mathbb{R}[X,Y]$ denotes the ideal generated by $Y - X^2$.] This means that every $f(X,Y) \in \mathbb{R}[X,Y]$ can be written in the form $f(X,Y) = (Y - X^2)q(X,Y) + r(X)$ for some $q(X,Y) \in \mathbb{R}[X,Y]$ and some $r(X) \in \mathbb{R}[X]$. Evaluating at (a, a^2) gives $0 = 0 + r(a)$ for all $a \in \mathbb{R}$ so $r(X) = 0$ (the zero polynomial).

14. Define $\phi : R \to \mathbb{R}$ by $f \mapsto f(a)$. Such evaluation of functions is always a ring homomorphism: we have $\phi(f+g) = (f+g)(a) = f(a) + g(a) = \phi(f) + \phi(g)$ and $\phi(fg) = (fg)(a) = f(a)g(a) = \phi(f)\phi(g)$ for all $f, g \in R$. By definition M_a is the kernel of this homomorphism, so $M_a \subset R$ is an ideal. Also ϕ is surjective since every $a \in \mathbb{R}$ is the image of (for example) the function with constant value a. The First Isomorphism Theorem gives $R/M_a \cong \mathbb{R}$, which is a field; therefore the ideal $M_a \subset R$ is maximal.

15. The polynomial $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (the prime 2 divides all but the leading coefficient, and 4 does not divide the constant term). Therefore $\mathbb{Q}[X]/(f(X)) \cong \mathbb{Q}(\alpha) = F$ is a field which is an extension of $\mathbb{Q}$ of degree $\deg f(X) = 3$. [This is the standard construction of field extensions. Note that the evaluation map $\mathbb{Q}[X] \to \mathbb{Q}[\alpha]$ given by $g(X) \mapsto g(\alpha)$ is a surjective ring homomorphism with kernel $(f(X))$, so the isomorphism $\mathbb{Q}[X]/(f(X)) \cong \mathbb{Q}[\alpha]$ follows from the First Isomorphism Theorem as in Question 14. Moreover the Division Algorithm applied to an arbitrary polynomial $g(X) \in \mathbb{Q}[X]$ gives $g(X) = (X^3 - 2)q(X) + a + bX + cX^2$ for some $q(X) \in \mathbb{Q}[X]$ and $a, b, c \in \mathbb{Q}$ so that $g(\alpha) = a + b\alpha + c\alpha^2$ and $\mathbb{Q}[\alpha] = F$.]

    We have $[F : \mathbb{Q}] = 3$ and a similar argument gives $[K : \mathbb{Q}] = 2$ where $K = \mathbb{Q}[\sqrt{2}]$. If $\sqrt{2} \in F$ then $[F : \mathbb{Q}] = [F : K][K : \mathbb{Q}]$, which is impossible since 2 does not divide 3.

16. Clearly $1 \in F[\![X]\!]$ (regarded as a Laurent series) is a multiplicative identity. Let $f(X) = \sum_{i \geq k} a_i X^i \in F[\![X]\!]$ be nonzero; we may assume that a_k is nonzero. We show that $f(X)$ has a multiplicative inverse $g(X) = \sum_{i \geq -k} b_i X^i \in F[\![X]\!]$; thus we require
$$(a_k X^k + a_{k+1}X^{k+1} + a_{k+2}X^{k+2} + \cdots)(b_{-k}X^{-k} + b_{-k+1}X^{-k+1} + b_{-k+2}X^{-k+2} + \cdots) = 1.$$
In particular $b_{-k} = a_k^{-1} \in F$ exists since $a_k \neq 0$. We proceed to determine the remaining coefficients of $g(X)$ inductively: having found $b_{-k}, b_{-k+1}, \ldots, b_{-k+j-1} \in F$, then equating coefficients of X^j on both sides of the above relation yields
$$a_k b_{-k+j} + a_{k+1} b_{-k+j-1} + \cdots + a_{k+j} b_{-k} = 0$$
and so $b_{-k+j} = -a_k^{-1} \sum_{i=1}^{j} a_{k+i} b_{-k+j-i} \in F$. Conversely, the element $g(X) = \sum_i b_i X^i$ having these coefficients satisfies $f(X)g(X) = 1$.