MAT247 Algebra II
Assignment 6 Solutions

1. Let F be a field and $f(t), g(t), h(t) \in F[t]$. Suppose $f(t)$ and $g(t)$ are relatively prime.

(a) Show that if $f(t) \mid g(t)h(t)$, then $f(t) \mid h(t)$.
(b) Show that if $f(t)$ and $g(t)$ both divide $h(t)$, then $f(t)g(t) \mid h(t)$.
(c) Show that for every positive integers m and n, $f(t)^m$ and $g(t)^n$ are relatively prime. (Note: If two polynomials have a common divisor $q(x)$ of positive degree, then they have an irreducible common divisor, because $q(x)$ has an irreducible divisor.)

Solution: (a) Since $f(t)$ and $g(t)$ are relatively prime, there exist $a(t), b(t) \in F[t]$ such that

$$a(t)f(t) + b(t)g(t) = 1.$$

Thus

$$a(t)f(t)h(t) + b(t)g(t)h(t) = h(t).$$

Since $f(t)$ divides both summands on the left, it also divides $h(t)$.

(b) Write $h(t) = f(t)q(t)$. Then $g(t) \mid f(t)q(t)$. Since $f(t)$ and $g(t)$ are relatively prime, by (a), $g(t) \mid q(t)$. Writing $q(t) = g(t)q_1(t)$, we then have $h(t) = f(t)g(t)q_1(t)$, so that $f(t)g(t)$ divides $h(t)$.

(c) Let m, n be positive integers. Suppose $f(t)^m$ and $g(t)^n$ are not relatively prime. Then there exists a polynomial $h(t) \in F[t]$ of positive degree such that $h(t)$ divides both $f(t)^m$ and $g(t)^n$. Being a polynomial of positive degree, $h(t)$ has an irreducible factor $\phi(t)$. Then $\phi(t)$ divides both $f(t)^m$ and $g(t)^n$. Since $\phi(t)$ is irreducible, it follows that $\phi(t)$ divides both $f(t)$ and $g(t)$, contradicting the assumption that $f(t)$ and $g(t)$ are relatively prime.

2. Let V be a nonzero finite-dimensional vector space over $\mathbb{C}$. Denote the identity map on V by I. Let T a linear operator on V such that $T^k = I$ for some positive integer k. Show that T is diagonalizable. (Suggestion: Use Theorem 7.16 (we'll prove it in class on Tuesday).)

Solution: Consider the polynomial $f(t) = t^k - 1$. Since $f(T) = 0$, the minimal polynomial of T divides $f(t)$. Since $f(t)$ splits over $\mathbb{C}$ and has no repeated root (the roots of $f(t)$ being $e^{2a\pi i/k}$, $a = 0, 1, \ldots, k-1$), the same holds for the minimal polynomial of T. By Theorem 7.16, T is diagonalizable.

3. Let V be a nonzero finite-dimensional vector space and T a diagonalizable linear operator on T. Let W be a T-invariant subspace of V. Show that T_W (the restriction of T to W) is diagonalizable. (Suggestion: Use Theorem 7.16. Does the minimal polynomial of T_W divide the minimal polynomial of T?)

Solution: Let $f(t)$ (resp. $f_W(t)$) be the minimal polynomial of T (resp. T_W). Then $f(T_W) = 0$ (as $f(T) = 0$). Hence $f_W(t) \mid f(t)$. Since T is diagonalizable, $f(t)$ splits and has no repeated root. Since $f_W(t) \mid f(t)$, same is true for $f_W(t)$, so that T_W is also diagonalizable.

4. Let V be a nonzero finite-dimensional vector space. Let $\mathcal{S}$ be a collection of diagonalizable linear operators on V such that any two maps in $\mathcal{S}$ commute with each other. Show that the maps in $\mathcal{S}$ can be simultaneously diagonalized. That is, show that there exists a basis β of V such that for every $T \in \mathcal{S}$, the matrix $[T]_\beta$ is diagonal. (Suggestion: Argue by induction on the dimension of V. In the induction step, consider two cases: (i) if every $T \in \mathcal{S}$ has only one eigenvalue, and (ii) if there exists $T \in \mathcal{S}$ which has at least two eigenvalues.)

Solution: We argue by induction on the dimension of V. If $\dim(V) = 1$, then the statement is certainly true (why?). Suppose $n \geq 2$ and that the result is true for vector spaces of dimension $< n$. Let $\dim(V) = n$, and $\mathcal{S}$ be a family of commuting diagonalizable operators on V. If all the maps in $\mathcal{S}$ have only one eigenvalue, then any basis of V does the job. (Note that any diagonalizable map with only one eigenvalue is of the form λI.) Suppose $\mathcal{S}$ contains an operator T with at least two eigenvalues. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of T. Then we have

$$V = \bigoplus_{i=1}^{k} E_{\lambda_i}(T),$$

and since $k \geq 2$, each eigenspace $E_{\lambda_i}(T)$ has dimension $< n$. It is enough to show that each $E_{\lambda_i}(T)$ has a basis β_i the elements of which are eigenvectors for all the maps in $\mathcal{S}$; then $\beta = \cup\beta_i$ will be a basis of V the elements of which are eigenvectors for all the elements of $\mathcal{S}$, so that $[S]_\beta$ is diagonal for every $S \in \mathcal{S}$.

Fix $1 \leq i \leq k$ and let $W = E_{\lambda_i}(T)$. Let

$$\mathcal{S}' = \{S_W : S \in \mathcal{S}\}.$$

This is a family of linear operators on W. The maps in $\mathcal{S}'$ commute with one another (as those in $\mathcal{S}$ do). Since every $S \in \mathcal{S}$ is diagonalizable, by the previous problem, so is every element of $\mathcal{S}'$. Thus $\mathcal{S}'$ is a family of commuting diagonalizable operators on W. Since $\dim(W) < n$, by the induction hypothesis, there exists a basis of W the elements of which are eigenvectors for every $S_W \in \mathcal{S}'$, and hence every $S \in \mathcal{S}$. (Note that any eigenvector of S_W is also an eigenvector of S.)

5. Let F be a field and $A \in M_{n\times n}(F)$. By the minimal polynomial of A over F we mean the minimal polynomial of $L_A : F^n \to F^n$. Equivalently, the minimal polynomial of A over F is the unique monic polynomial $f(t) \in F[t]$ satisfying the following properties: (i) $f(A) = 0$, and (ii) if $g(t) \in F[t]$ is any nonzero polynomial such that $g(A) = 0$, then $\deg(f(t)) \leq \deg(g(t))$.

(a) Show that the degree of the minimal polynomial of A over F is equal to the smallest integer k such that there exists a nonzero vector $(c_0, \ldots, c_k) \in F^{k+1}$ such that

$$c_0 I + c_1 A + c_2 A^2 + \cdots + c_k A^k = 0.$$

(b) Let K be a field that contains F (as a subfield). Show that the minimal polynomial of A over F is the same as its minimal polynomial over K. (Hint: Let $B \in M_{\ell\times m}(F)$. If the equation $Bx = 0$ has a solution in K^m, then does it also have a solution in F^m?)

Solution: (a) Let k be the smallest positive integer such that there exist $c_0, \ldots, c_k \in F$, not all zero, such that $c_0 I + c_1 A + c_2 A^2 + \cdots + c_k A^k = 0$. By the minimality of k, c_k is nonzero. Let $f(t) = \frac{1}{c_k} \sum_{i=1}^{k} c_i t^i$. Note that $\deg(f(t)) = k$. We claim that $f(t)$ is the minimal polynomial of A over F. That $f(t)$ is monic and $f(A) = 0$ are clear. Let $g(t)$ be a nonzero polynomial, say of degree m, such that $g(A) = 0$. Writing $g(t) = \sum_{i=0}^{m} a_i t^i$, we have $\sum_{i=0}^{m} a_i A^i = 0$, so that by definition of k, we have $k \leq m$.

(b) Let $f_F(t)$ and $f_K(t)$ denote the minimal poynomials of A over F and K, respectively. The minimal polynomial of A over K divides any polynomial $g(t) \in K[t]$ such that $g(A) = 0$. In particular, it divides $f_F(t)$.

Since $f_K(t)$ and $f_F(t)$ are both monic and $f_K(t) \mid f_F(t)$, to show that $f_K(t) = f_F(t)$ it is enough to argue that $\deg(f_K(t)) = \deg(f_F(t))$. Let

$$I(F) = \{k \geq 0 : c_0 I + c_1 A + c_2 A^2 + \cdots + c_k A^k = 0 \text{ has a nontrivial solution in } F\}$$

and

$$I(K) = \{k \geq 0 : c_0 I + c_1 A + c_2 A^2 + \cdots + c_k A^k = 0 \text{ has a nontrivial solution in } K\}.$$

In view of (a), it is enough to have $I(F) = I(K)$. Let k be a nonnegative integer. *The equation*

$$c_0 I + c_1 A + c_2 A^2 + \cdots + c_k A^k = 0$$

can be written as a homogeneous system of linear equations with coefficients in F, and as such, it has a nontrivial solution over F if and only if it has a nontrivial solution over K. Thus $I(F) = I(K)$, as desired.

(Expanded version of the part in italic: Let $\beta = \{E_{11}, \ldots, E_{nn}\}$ be the standard ordered basis of $M_{n\times n}(F)$ (and $M_{n\times n}(K)$). Then the equation

$$c_0 I + c_1 A + c_2 A^2 + \cdots + c_k A^k = 0$$

is equivalent to

$$c_0[I]_\beta + c_1[A]_\beta + c_2[A^2]_\beta + \cdots + c_k[A^k]_\beta = 0,$$

which can be rewritten in matrix form as

$$([I]_\beta\ [A]_\beta\ [A^2]_\beta\ \cdots\ [A^k]_\beta)x = 0,$$

where $x = (c_0\ \cdots c_k)^t$. Let

$$B = ([I]_\beta\ [A]_\beta\ [A^2]_\beta\ \cdots\ [A^k]_\beta) \in M_{n^2\times(k+1)}(F).$$

By uniqueness of reduced row echelon form (RREF),

$$\dim_F\left(\{x \in F^{k+1} : Bx = 0\}\right) \ = \ \dim_K\left(\{x \in K^{k+1} : Bx = 0\}\right).$$

(Indeed, if R is the RREF of B over F, then it is also the RREF of B over K, and hence the two dimensions above are both equal to $k+1$ minus the number of nonzero rows of R.) Thus in particular, $Bx = 0$ has a nontrivial solution in F^{k+1} if and only if it has a nontrivial solution in K^{k+1}.)

6. Suppose $A \in M_{5\times 5}(\mathbb{Q})$ has characteristic polynomial $f(t) = (t+1)^4(t-2)$. Let $g(t)$ be the minimal polynomial of A.

(a) List all possibilities for $g(t)$. What is the Jordan canonical form of A in each case? (List all possible Jordan canonical forms if there is more than one.)

(b) Suppose $g(t) = (t+1)^2(t-2)$ and that moreover $\dim(N(A+I)) = 2$. What is the Jordan canonical form of A?

(Suggestion: See exercise 13 of 7.3.)

Solution: (a) The minimal polynomial $g(t)$ is of the form $(t+1)^i(t-2)$, with $1 \leq i \leq 4$ the size of the largest Jordan block corresponding to eigenvalue -1 in the Jordan canonical form

(JFC) of A. If $i = 1$, then the JCF is diagonal with four -1's and one 2. If $i = 2$, the JCF is either

$$\begin{pmatrix} J_{-1,2} & & \\ & J_{-1,2} & \\ & & 2 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} J_{-1,2} & & & \\ & -1 & & \\ & & -1 & \\ & & & 2 \end{pmatrix}.$$

(Here and in what follows $J_{\lambda,k}$ denotes the $k \times k$ Jordan block with λ on the diagonal.) If $i = 3$, then the JCF is

$$\begin{pmatrix} J_{-1,3} & & \\ & -1 & \\ & & 2 \end{pmatrix}.$$

Finally, if $i = 4$, the JCF is

$$\begin{pmatrix} J_{-1,4} & \\ & 2 \end{pmatrix}.$$

(b) In (a) we saw that there are two cases in which the minimal polynomial is $g(t) = (t+1)^2(t-2)$. Since $\dim(E_{-1}) = \dim(N(A+I)) = 2$, there are two Jordan blocks corresponding to eigenvalue -1, so that the JCF must be

$$\begin{pmatrix} J_{-1,2} & & \\ & J_{-1,2} & \\ & & 2 \end{pmatrix}.$$