MAT247 Algebra II

Assignment 7

Solutions

Notation. In what follows we shall use the following notation: for a polynomial f, we denote the companion matrix of f by $C(f)$. Given a scalar λ, we denote the $n \times n$ Jordan block corresponding to λ by $J_{\lambda,n}$.

1. Let F be a field.

(a) Let $\phi_1, \phi_2, \ldots, \phi_k$ be distinct monic irreducible polynomials in $F[t]$. For each i, let $p_{i,j}$ $(1 \leq j \leq e_i)$ be integers with

$$p_{i,e_i} \geq p_{i,e_i-1} \geq \cdots \geq p_{i,1} \geq 1.$$

Let R be the following block diagonal matrix:

$$\begin{pmatrix} C(\phi_1^{p_{1,e_1}}) & & & & & & & & \\ & \ddots & & & & & & & \\ & & C(\phi_1^{p_{1,1}}) & & & & & & \\ & & & C(\phi_2^{p_{2,e_2}}) & & & & & \\ & & & & \ddots & & & & \\ & & & & & C(\phi_2^{p_{2,1}}) & & & \\ & & & & & & \ddots & & \\ & & & & & & & C(\phi_k^{p_{k,e_k}}) & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & C(\phi_k^{p_{k,1}}) \end{pmatrix}.$$

Show that the minimal polynomial of R is $\prod_{i=1}^{k} \phi_i^{p_{i,e_i}}$. (Remember that the minimal polynomial of the companion matrix of a monic polynomial f is f itself. Also note that if A is a block diagonal matrix with diagonal blocks $A_1, A_2, \ldots$ and $g \in F[t]$, then $g(A)$ is the block diagonal matrix with diagonal blocks $g(A_1), g(A_2), \ldots$.)

(b) Let ϕ_1 and ϕ_2 be two distinct monic irreducible elements of $F[t]$. Consider the set $\mathcal{M}$ of all matrices A with entries in F whose characteristic polynomial is $\phi_1^4\phi_2^2$. Then similarity is an equivalence relation on $\mathcal{M}$. Find the number of equivalence classes of this relation, give a representative for each class, and give the minimal polynomial of the matrices in each class.

Solution: (a) Let $f = \prod_{i=1}^{k} \phi_i^{p_{i,e_i}}$. It is enough to show that given any $g \in F[t]$, we have $g(R) = 0$ if and only if $f \mid g$. By the remark made in the statement of the question, $g(R) = 0$ if and only if $g(C(\phi_i^{p_{i,j}})) = 0$ for all $1 \le i \le k$ and $1 \le j \le e_i$. Since the minimal polynomial of $C(\phi_i^{p_{i,j}})$ is $\phi_i^{p_{i,j}}$, it follows that $g(R) = 0$ if and only if $\phi_i^{p_{i,j}} \mid g$ for all $1 \le i \le k$ and $1 \le j \le e_i$. Since the $(p_{i,j})_j$ are increasing, the latter is equivalent to that $\phi_i^{p_{i,e_i}} \mid g$ for all i. Since the ϕ_i are pairwise relatively prime, this is equivalent to $f = \prod_{i=1}^{k} \phi_i^{p_{i,e_i}} \mid g$.

(b) The elements of $\mathcal{M}$ are classified up to similarity by their rational canonical forms over F. The possibilities for the blocks corresponding to ϕ_1 in the rational canonical form are

$$(1)\ C(\phi_1^4)\ ,\ (2)\ \begin{pmatrix} C(\phi_1^4) & \\ & C(\phi_1) \end{pmatrix}\ ,\ (3)\ \begin{pmatrix} C(\phi_1^2) & \\ & C(\phi_1^2) \end{pmatrix}$$

$$(4)\ \begin{pmatrix} C(\phi_1^2) & & \\ & C(\phi_1) & \\ & & C(\phi_1) \end{pmatrix}\ ,\ (5)\ \begin{pmatrix} C(\phi_1) & & & \\ & C(\phi_1) & & \\ & & C(\phi_1) & \\ & & & C(\phi_1) \end{pmatrix}.$$

The possibilities for the blocks corresponding to ϕ_2 are

$$(1)\ C(\phi_2^2)\ ,\ (2)\ \begin{pmatrix} C(\phi_2) & \\ & C(\phi_2) \end{pmatrix}.$$

In total, there are 10 possibilities for the rational canonical form of a matrix with characteristic polynomial $\phi_1^4\phi_2^2$. We leave it to the reader to find the minimal polynomial for each possibility using part (a).

2. Consider the polynomials $\phi = t^2 - 2$, $\phi^+ = t - \sqrt{2}$, and $\phi^- = t + \sqrt{2}$ in $\mathbb{R}[t]$. Let A be a matrix with entries in $\mathbb{Q}$.

(a) Suppose the characteristic polynomial of A is ϕ^2. Find all possibilities for the rational canonical form of A over $\mathbb{Q}$.

(b) With A as in part (a), find all possibilities for the rational canonical form of A over $\mathbb{R}$. (Keep in mind that the entries of A are in $\mathbb{Q}$.)

(c) Now suppose the characteristic polynomial of A is ϕ^4. Again, find all possibilities for the rational canonical form of A over $\mathbb{Q}$ and over $\mathbb{R}$.

(d) Let F be a subfield of K. For $1 \le i \le k$, let ϕ_i be distinct monic irreducible polynomials in $F[t]$. Suppose each ϕ_i factors as $\prod_j \psi_{i,j}$ in $K[t]$, where the $\psi_{i,j}$ are distinct, monic, and irreducible in $K[t]$. Let A be a matrix with entries in F whose characteristic polynomial is $p_A = \pm \prod_i \phi_i^{n_i}$. Formulate a conjecture that describes how the rational canonical forms of A over F and K are related. You don't need to prove your conjecture.

Solution: (a) There are two possibilities

$$R_1 = C(\phi^2) \qquad \text{and} \qquad R_2 = \begin{pmatrix} C(\phi) & \\ & C(\phi) \end{pmatrix}.$$

(b) The possibilities for the rational canonical form (RCF) over $\mathbb{R}$ of a matrix with entries in $\mathbb{R}$ with characteristic polynomial $\phi^2 = \phi_-^2\phi_+^2$ are

$$R_1' = \begin{pmatrix} C(\phi_+^2) & \\ & C(\phi_-^2) \end{pmatrix},\ R_2' = \begin{pmatrix} C(\phi_+) & & \\ & C(\phi_+) & \\ & & C(\phi_-^2) \end{pmatrix},\ R_3' = \begin{pmatrix} C(\phi_+^2) & & \\ & C(\phi_-) & \\ & & C(\phi_-) \end{pmatrix}$$

$$R'_4 = \begin{pmatrix} C(\phi_+) & & & \\ & C(\phi_+) & & \\ & & C(\phi_-) & \\ & & & C(\phi_-) \end{pmatrix}.$$

Since A has entries in $\mathbb{Q}$, it is similar to one of the matrices R_1 or R_2 of part (a). Each of R_1 and R_2 is similar to one of the matrices $R'_1, \ldots, R'_4$. The minimal polynomials of R_1, R_2 are respectively ϕ^2, ϕ. The minimal polynomials of R'_1, R'_2, R'_3, R'_4 are respectively $\phi_+^2\phi_-^2 = \phi^2, \phi_+\phi_-^2, \phi_+^2\phi_-, \phi_+\phi_- = \phi$. Thus R_1 (resp. R_2) must be similar to R'_1 (resp. R'_4), and the possible RCFs over $\mathbb{R}$ of A are R'_1 and R'_4.

(c) There are five possible RCFs over $\mathbb{Q}$, corresponding to partitions of 4: (4), (3,1), (2,2), (2,1,1), (1,1,1,1). (The RCF in the first case has one block, which is $C(\phi^4)$, in the second case has two blocks $C(\phi^3)$ and $C(\phi)$, etc.) The characteristic polynomial over $\mathbb{R}$ factors as $\phi_+^4\phi_-^4$. By considering the minimal polynomials it follows that if the RCF over $\mathbb{Q}$ corresponds to the partitions (4), (3,1), or (1,1,1,1), the blocks for each of ϕ_+ and ϕ_- in the RCF over $\mathbb{R}$ will correspond to the same partition. For instance, if the RCF over $\mathbb{Q}$ has one block $C(\phi^4)$, then the RCF over $\mathbb{R}$ will have one block $C(\phi_+^4)$ and one block $C(\phi_-^4)$.

If the RCF over $\mathbb{Q}$ corresponds to the partition (2,2) or (2,1,1), the minimal polynomial is ϕ^2. This tells us that the partition corresponding to each of $\phi_\pm$ in the RCF over $\mathbb{R}$ is either (2,2) or (2,1,1). Suppose the RCF over $\mathbb{Q}$ is

$$R = \begin{pmatrix} C(\phi^2) & \\ & C(\phi^2) \end{pmatrix}.$$

By part (b), $C(\phi^2)$ is similar to

$$R' = \begin{pmatrix} C(\phi_+^2) & \\ & C(\phi_-^2) \end{pmatrix}.$$

Thus R is similar to $\begin{pmatrix} R' & \\ & R' \end{pmatrix}$, and the RCF over $\mathbb{R}$ has blocks for each of ϕ_+ and ϕ_- corresponding to the partition (2,2). Similarly, if the RCF over $\mathbb{Q}$ corresponds to the partition (2,1,1), then the RCF over $\mathbb{R}$ has blocks for each of ϕ_+ and ϕ_- corresponding to the partition (2,1,1) .

REMARK. For the case of partition (2,2) or (2,1,1), alternatively, we could have taken one of the following two approaches: (1) First find the JCF, and then recover the RCF over $\mathbb{R}$ from the JCF (see the first practice problem appended to the assignment). (2) Use problems 3b and 4c of the assignment.

(d) Conjecture: The partition of n_i (or the dot diagram) for each of $\psi_{i,j}$ in the RCF over K is the same as the partition of n_i for ϕ_i in the RCF over F.

3. (a) Let T be a linear operator on a finite-dimensional vector space V over F. Let $f, g \in F[t]$ be relatively prime. Show that the restriction of $f(T)$ to $\ker(g(T))$ is injective. (Note: The statement is equivalent to saying that $\ker(f(T)) \cap \ker(g(T)) = 0$, which we proved in class a few lectures ago. You should rewrite the proof.)

(b) Deduce that if ϕ and ψ are distinct monic irreducible polynomials in $F[t]$, and A is the companion matrix of ψ^m, then $\phi(A)$ is invertible.

Solution: (a) Note that

$$\ker(f(T)_{\ker(g(T))}) = \ker(f(T)) \cap \ker(g(T)).$$

Suppose $v \in \ker(f(T)) \cap \ker(g(T))$. Since $f(t)$ and $g(t)$ are relatively prime, there exist $a(t), b(t)$ such that $a(t)f(t) + b(t)g(t) = 1$. Then $a(T)f(T) + b(T)g(T) = I$. Applying both sided to v, we see that v has to be zero.

(b) Let $A = C(\psi^m)$. Let $L_A :: F^n \to F^n$ be left multiplication by A. Apply part (a) to L_A with $f = \phi$ and $g = \psi^m$. By Cayley-Hamilton, $\psi^m(L_A) = 0$, so that $\ker(\psi^m(L_A)) = F^n$. Thus Part (a) tells us that $\phi(L_A) = L_{\phi(A)}$ is injective, which is equivalent to $\phi(A)$ being invertible (why?).

4. Suppose T is a linear operator on a finite-dimensional vector space V over a field F. Suppose moreover that V is a T-cyclic subspace of itself, and that the characteristic polynomial of T is $\pm\phi^m$, where ϕ is a monic irreducible polynomial in $F[t]$. Let $d = \deg(\phi)$. Let $v \in V$ be a vector such that V is the T-cyclic subspace generated by v.

(a) Show that the set

$$I = \{\phi(T)^{m-1}(v),\ \phi(T)^{m-1}(T(v)),\ \phi(T)^{m-1}(T^2(v)), \dots,\ \phi(T)^{m-1}(T^{d-1}(v))\}$$

is linearly independent. (Hint: What is the minimal polynomial of T?)

(b) By Cayley-Hamilton, $\phi(T)^m = 0$, so that $\phi(T)$ is a nilpotent map. Show that the Jordan canonical form of $\phi(T)$ has the form

$$\begin{pmatrix} J_{0,m} & & & \\ & J_{0,m} & & \\ & & \ddots & \\ & & & J_{0,m} \end{pmatrix},$$

where there are d Jordan blocks in the matrix. In other words, show that the dot diagram for the eigenvalue zero of $\phi(T)$ consists of d columns of length m. (Hint: For each $w_i := \phi(T)^{m-1}(T^i(v))$ $(0 \le i < d)$, form a cycle of length m of generalized eigenvectors of $\phi(T)$ with initial vector w_i. Then use Theorem 7.6.)

(c) Let A be the companion matrix of ϕ^m (with ϕ as above: a monic irreducible element of $F[t]$ of degree d). Deduce from part (b) that for each $1 \le r \le m$, the matrix $\phi^r(A)$ has nullity rd.

Remark: From Problems 3(b) and 4 one can deduce uniqueness of rational canonical form. In fact, one can use them to show the following stronger statement: if R and R' are block diagonal matrices in $M_{n\times n}(F)$ with diagonal blocks that are companion matrices of powers of irreducible polynomials (that is, if they are matrices in rational canonical form), then, unless R and R' are obtained from each other by a permutation of the diagonal blocks, they are not similar over any field extension of F. (In short, this is because the nullities of $\phi^i(R)$ and $\phi^i(R')$ won't be the same for some r and some irreducible polynomial $\phi \in F[t]$.) This statement together with existence of rational canonical form can be used to show that if two matrices $A, B \in M_{n\times n}(F)$ are similar over a field extension of F, then A and B are already similar over F.

Solution: (a) Since V has dimension md and is T-cyclically generated by v, the set $\beta = \{v, T(v), \dots, T^{md-1}(v)\}$ is a basis of V. Suppose I is linearly dependent. Then there exist $c_0, \dots, c_{d-1} \in F$, not all zero, such that

$$\sum_{i=0}^{d-1} c_i \phi(T)^{m-1}(T^i(v)) = 0.$$

Expand

$$\sum_{i=0}^{d-1} c_i \phi(T)^{m-1}(T^i(v)) = \sum_{j=0}^{dm-1} a_j T^j(v)$$

(note $d(m-1)+(d-1) = dm-1$). Let k be the largest index such that $c_k \neq 0$. Then the coefficient of $T^{d(m-1)+k}(v)$ in the above is not zero. Thus we get a nontrivial linear combination of β which is zero, contradicting linear independence of β.

(b) Each of the vectors in I is the initial vector of a cycle of length m of generalized eigenvectors (for eigenvalue 0) of $\phi(T)$. Indeed, for each $0 \leq i \leq d-1$,

$$\gamma_i := \{\phi(T)^{m-1}(T^i(v)), \phi(T)^{m-2}(T^i(v)), \ldots, \phi(T)(T^i(v)), T^i(v)\}$$

is such cycle. The initial vectors of the γ_i are distinct and linearly independent, so that the γ_i are disjoint and $\cup\gamma_i$ is linearly independent set with $\sum |\gamma_i| = dm$ elements. Thus $\alpha = \cup\gamma_i$ is a Jordan basis of $\phi(T)$. The Jordan canonical form $[\phi(T)]_\alpha$ is the matrix given in the statement.

5. So far in MAT240 and MAT247, you have seen the notion of direct sum of a collection of subspaces of a given vector space. There is another notion of direct sum, which we introduce in this problem. Let F be a field and V_i ($1 \leq i \leq k$) vector spaces over F. Consider the cartesian product

$$V_1 \times \cdots \times V_k := \{(v_1, \ldots, v_k) \ : \ v_i \in V_i \text{ for each } 1 \leq i \leq k\}.$$

Equip this set with component-wise addition and scalar multiplication. That is, define

$$(v_1, \ldots, v_k) + (w_1, \ldots, w_k) := (v_1 + w_1, \ldots, v_k + w_k)$$

and

$$c(v_1, \ldots, v_k) := (cv_1, \ldots, cv_k) \qquad (c \in F).$$

(In more compact notation, $(v_i)_{1\leq i\leq k} + (w_i)_{1\leq i\leq k} = (v_i + w_i)_{1\leq i\leq k}$ and $c(v_i)_{1\leq i\leq k} = (cv_i)_{1\leq i\leq k}$.) Then you can easily check that $V_1 \times \cdots \times V_k$ together with the operations defined above is a vector space. This vector space is called the direct sum of the V_i, and is denoted by $V_1 \oplus \cdots \oplus V_k$, or $\bigoplus_{i=1}^{k} V_i$.

For each $1 \leq i \leq k$, one has a natural injection

$$\iota_i : V_i \to V_1 \oplus \cdots \oplus V_k$$

sending $v \in V_i$ to the tuple with v in its i-th entry and zeros elsewhere. One also has a natural surjection (called the projection to the i-th component)

$$\pi_i : V_1 \oplus \cdots \oplus V_k \to V_i \quad (v_1, \ldots, v_k) \mapsto v_i.$$

(a) Show that if β_i is a basis of V_i, then $\bigcup_{i=1}^{k} \iota_i(\beta_i)$ is a basis of $\bigoplus_{i=1}^{k} V_i$. Conclude that if the V_i are finite-dimensional, then $\dim(\bigoplus_{i=1}^{k} V_i) = \sum_{i=1}^{k} \dim(V_i)$.

(b) Let W be any vector space (over the same field F). Show that a map $T : W \to \bigoplus_{i=1}^{k} V_i$ is linear if and only if the component maps $\pi_i \circ T : W \to V_i$ are linear.

(c) The goal of this part is to relate the notion of direct sum introduced here to the one we had seen earlier. Suppose $V_1, \ldots, V_k$ are all subspaces of a vector space V. Let $\bigoplus_{i=1}^{k} V_i$ be the direct sum of the V_i, as introduced here. Then we have a natural map

$$\alpha : \bigoplus_{i=1}^{k} V_i \to V \qquad (v_1, \ldots, v_k) \mapsto \sum_{i=1}^{k} v_i.$$

Note that the image of α is the subspace $\sum_{i=1}^{k} V_i$. Show that the sum of the subspaces V_i is direct (in the sense we had earlier) if and only if the map α is injective. (Thus when the sum of the subspaces V_i is direct, we have the above distinguished isomorphism between the two notions of direct sums for the subspaces V_i. Sometimes people use the term *internal* direct sum for the earlier notion of direct sum, in contrast to the notion defined here being *external*.

Solution: (a) Suppose $v = (v_i)_i \in \bigoplus_i V_i$. Then

$$v = \sum_i \iota_i(v_i).$$

Since $\iota_i(v_i)$ is in the span of $\iota_i(\beta_i)$, we get that $\bigcup_{i=1}^{k} \iota_i(\beta_i)$ spans $\bigoplus_i V_i$. As for linear independence of $\bigcup_{i=1}^{k} \iota_i(\beta_i)$, for each i, suppose $v_{i,1}, \ldots, v_{i,r_i}$ are distinct vectors in β_i, and that

$$\sum_i \sum_j a_{i,j} \iota_i(v_{i,j}) \; = \; 0.$$

Applying π_i, we get

$$\sum_j a_{i,j} \iota_i(v_{i,j}) \; = \; 0.$$

Since ι_i is injective and β_i is linearly independent, from this it follows that $a_{i,j}$ is zero for all j. This is true for all i, so that the $a_{i,j}$ are zero for all i, j.

We showed that $\cup_i \iota_i(\beta_i)$ is a basis of $\bigoplus_i V_i$. If the β_i are all finite, $\cup_i \iota_i(\beta_i)$ has $\sum_i |\beta_i| = \sum \dim(V_i)$ elements. (Note that the sets $\iota_i(\beta_i)$ are disjoint; this is obvious from that $\mathrm{Im}(\iota_i) \cap \mathrm{Im}(\iota_j) = 0$. It also follows from the argument given above.)

(b) Suppose $T : W \to \bigoplus_{i=1}^{k} V_i$ is linear. Since the composition of two linear maps is linear, $\pi_i \circ T$ is linear for all i.

Conversely, suppose $T : W \to \bigoplus_{i=1}^{k} V_i$ is a function such that $\pi_i \circ T$ is linear for all i. Note that for any $v \in \bigoplus_i V_i$, we have $v = (\pi_i(v))_i$. Given $w, w' \in W$ and $a \in F$, we have

$$T(w + aw') = (\pi_i(T(w + aw')))_i \overset{\text{linearity of } \pi_i \circ T}{=} (\pi_i \circ T(w) + a\pi_i \circ T(w'))_i = (\pi_i \circ T(w))_i + a(\pi_i \circ T(w'))_i = T(w) + aT(w').$$

(c) We leave it to the reader to check that α is linear. Thus α is injective if and only if $\ker(\alpha) = 0$, i.e. if and only if

$$\sum_{i=1}^{k} v_i = 0, \; v_i \in V_i \; (1 \le i \le k) \qquad \Rightarrow \qquad v_i = 0 \; (1 \le i \le k).$$

The latter was one of the equivalent conditions for the sum $\sum_i V_i$ to be direct.