Jordan and Rational Canonical Forms

Problem 1: Let K be a field and $A, B \in M_{n\times n}(K)$. Suppose A and B are similar over K. Let F be a subfield of K which contains the entries of A and B. Assuming that the characteristic polynomial of A (which is the same as that of B) splits over F, show that A and B are also similar over F.

Proof. First, we will prove that the Jordan canonical form of a matrix is unique up to an ordering of Jordan blocks. From the previous assignment, we showed that if J_1 and J_2 are similar, then $(J - \lambda I)^k$ is similar to $(L - \lambda I)^k$ for any λ and $k \in \mathbb{N}$. Furthermore, similar matrices will have the same nullity. So, if a matrix A has Jordan forms J_1 and J_2 (in which, all three matrices are mutually similar), then $J_1 = J_2$ since all their generalised eigenspaces will have the same nullity per index.

Now, lets prove that similar matrices have the same Jordan canonical form. Suppose $A = P^{-1}BP$. If J is the Jordan canonical form of A, then there exists matrix M such that $M^{-1}AM = J$. But that implies $J = M^{-1}P^{-1}BPM = (PM)^{-1}B(PM)$, completing the proof.

Now we prove the converse. Suppose A and B have the same Jordan canonical form J, but, for contradiction, are not similar. Well, there exists C and D such that $CAC^{-1} = J = D^{-1}BD$. But that's a contradiction since it implies that $A = (CD)B(CD)^{-1}$ (that is, A and B are similar).

Now, since the characteristic polynomial of A and B splits over F, then all their eigenvectors are in F and so both their Jordan canonical forms J_A and J_B exists over F. But the Jordan canonical form is unique. And so J_A and J_B is the same over F or K. But in K, $J_A = J_B$ since A and B are similar. This implies that $J_A = J_B$ even in F and so, A and B are also similar in the subfield F. $\square$

Problem 2: Suppose T is a linear operator on a finite-dimensional vector space V over a field F. Suppose 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.

Show that the set I=$\{\phi(T)^{m1}(v), \phi(T)^{m1}(T(v)), \phi(T)^{m1}(T2(v)), ..., \phi(T)^{m1}(T^{d1}(v))\}$ is linearly independent.

Then, deduce that for each $1 \leq r \leq m$, the matrix ϕ^r has nullity rd.

Proof. Since V is a T-cyclic subspace generated by v, the minimal polynomial of T is also $\pm\phi^m$ by Theorem 7.15 (since otherwise, the dot-diagram of T would have no cycle of length m which contracts the existence of a dm-dimensional T-cyclic subspace).

Now, by defintion of v, $\{v, T(v), ..., T^{dm-1}(v)\}$ is linearly independent since v generates V. In particular, the set $S = \{T^{d(m-1)}(v), T^{d(m-1)+1}(v), ..., T^{d(m-1)+(d-1)}(v)\}$ is linearly independent.

So, let $\sum_{i=0}^{d-1} c_i\phi(T)^{m-1}(T^i(v)) = 0$. This implies that $c_{d-1} = 0$ since $T^{d(m-1)+(d-i)}(v)$ is linearly independent of all $T^j(v)$ where $j < md-1$, and all other polynomials $\phi(t)^{m-1}(t)^i$ only have terms of degree $< md - 1$.

But that then further implies $c_{d-2} = 0$ by the same reasoning, and so on.

Therefore, $c_0 = c_1 = ... = c_{d-1} = 0$ and thus I is linearly independent.

Since $\phi^m(T) = 0$, $\phi(T)$ is nilpotent and thus only has 0 as an eigenvalue and its characteristic polynomial splits (since every vector must be in K_0). Thus, a Jordan form exists with 0's all in the diagonal.

All that is left to prove is that $\phi(T)$ has d cycles of length m.

Well, I is made up of d linearly independent initial-vectors of $\phi(T)$. Since clearly, applying $\phi(T)$ to any vector in I will kill all those vectors (since $\phi(T)\phi^{m-1}(T) = 0$).

Now, we're done if we show that each of the cycles of the d end-vectors in I has length m (since $\dim V = dm$). Indeed, if you divide the vectors of I by $\phi(T)$ you can keep generating vectors until after $m - 1$ applications, you get the set $\{v, T(v), ..., T^{d-1}(v)\}$ which must be all non-zero as shown in part (a). Additionally, by Theorem 7.6, all these cycles are linearly independent. And thus, each of the d vectors in I was a inital-vector for a cycle of length m.

We can then conclude that the Jordan form is made up of d $J_{0,m}$ blocks.

Since A has characteristic polynomial ϕ^m, by Cayley-Hamilton, $\phi^m(A) = 0$. Thus, V is a A-cyclic vector space of itself. By Theorem 7.15, the minimal polynomial of A must also be ϕ^m. There is only one possible dot diagram for A, which is the exact same as the one for $\phi(T)$ and therefore, $\phi(A)$ is similar to $\phi(T)$. They must then have the same Jordan form.

Thus, by noticing that the Jordan matrix maps d new vectors to its kernel after every application of the transformation, we can deduce that $N(\phi(A)^r) = rd$. $\square$