The Jordan Canonical Form, the Rational Canonical Form, and the Smith Normal Form

Dylan C. Beck

Our goal throughout this expository note is to understand the connections among the Jordan Canonical Form, the Rational Canonical Form, and the Smith Normal Form of a linear operator over a finite-dimensional vector space (or equivalently, square matrix with entries in a field). Previously, we discussed the Fundamental Theorem of Finitely Generated Modules over a Principal Ideal Domain (PID). Put in practice, this theorem allows us to decompose any finite-dimensional vector space over a field k into a direct sum of cyclic subspaces with respect to a linear operator. Before we implement this powerful tool, we should understand some fundamentals of modules.

The Basics of Module Theory

We will assume that R is a commutative unital ring with multiplicative identity 1_R. We say an abelian group $(M, +)$ is an **R-module** if there exists a group action $\cdot : R \times M \to M$ such that

(i.) $r \cdot (m + n) = r \cdot m + r \cdot n$ for all elements $r \in R$ and $m, n \in M$ and

(ii.) $(r + s) \cdot m = r \cdot m + s \cdot m$ for all elements $r, s \in R$ and $m \in M$.

Recall that $\cdot : R \times M \to M$ is a group action of R on M if and only if

(iii.) $r \cdot (s \cdot m) = (rs) \cdot m$ for all elements $r, s \in R$ and $m \in M$ and

(iv.) $1_R \cdot m = m$ for all elements $m \in M$.

Example 1. Every abelian group G is a $\mathbb{Z}$-module with respect to the group action

$$n \cdot g = \underbrace{g + g + \cdots + g}_{n \text{ summands}}.$$

Example 2. Every commutative unital ring R is an R-module: the action is multiplication in R. Further, any subring of R is an R-module, hence every ideal I of R is an R-module.

We say that an R-module M is **finitely generated** if there exist elements $x_1, \dots, x_n \in M$ such that for any element $m \in M$, there exist elements $a_1, \dots, a_n \in R$ with $m = a_1 \cdot x_1 + \cdots + a_n \cdot x_n$.

Example 2, Cont'd. The $\mathbb{Z}$-module $\mathbb{Z}$ is finitely generated by 1 because every non-negative integer n can be written as $n \cdot 1 = 1 + 1 + \cdots + 1$ with n summands. Of course, if n is negative, then we have that $n \cdot 1 = (-1) + (-1) + \cdots + (-1)$ with n summands. On the other hand, by Bézout's Theorem, for any collection of integers $x_1, \dots, x_n$ such that $\gcd(x_1, \dots, x_n) = 1$, there exist integers $a_1, \dots, a_n$ such that $a_1x_1 + \cdots + a_nx_n = 1$. Thus, $\mathbb{Z}$ is generated by $x_1, \dots, x_n$ as a $\mathbb{Z}$-module.

Our previous example illustrates that even though a finitely generated R-module always admits a finite set of generators, the number of generators is not necessarily unique. Going forward, we will not concern ourselves with this predicament when dealing with finitely generated modules.

The $k[x]$-Module Structure of a k-Vector Space

Crucially, our next objective is to establish that every (finite-dimensional) vector space is a (finitely generated) module over a principal ideal domain. Toward this end, let us assume that k is a field and that V is a (finite-dimensional) k-vector space with a linear operator $T : V \to V$. Recall that the univariate polynomial ring $k[x]$ is a Euclidean domain (the norm of a polynomial is its degree) and hence a principal ideal domain. Consider the group action $\cdot : k[x] \times V \to V$ defined by

$$f(x) \cdot v = f(T)(v).$$

Composition and addition of linear operators behaves as desired, so this action turns V into a $k[x]$-module. In the case that V is finite-dimensional over k, there exist vectors $v_1, \dots, v_n$ such that for every vector $v \in V$, there exist unique scalars $a_1, \dots, a_n \in k$ such that

$$v = a_1 v_1 + \cdots + a_n v_n = a_1 \cdot v_1 + \cdots + a_n \cdot v_n,$$

where $a_i \cdot v_i$ denotes the action of the constant polynomial a_i on v_i. Consequently, V is finitely generated as a module over the principal ideal domain $k[x]$. By the Fundamental Theorem of Finitely Generated Modules over a Principal Ideal Domain, we conclude that V can be written as

$$V \cong k[x]^{\oplus m} \oplus \frac{k[x]}{(p_1(x))} \oplus \cdots \oplus \frac{k[x]}{(p_n(x))}$$

for some integers $m \geq 0$ and $n \geq 1$ and some monic polynomials $p_1(x), \dots, p_n(x) \in k[x]$.

By the Cayley-Hamilton Theorem, on the other hand, there exist scalars $c_1, \dots, c_r \in k$ such that $T^r + c_1 T^{r-1} + \cdots + c_r I$ is the zero operator. Consequently, there exists a nonzero polynomial $f(x) = x^r + c_1 x^{r-1} + \cdots + c_r$ such that for every vector $v \in V$, we have that $f(x) \cdot v = f(T)(v) = 0$. We conclude that every element of V is **torsion** so that V is a **torsion $k[x]$-module**. Particularly,

$$V \cong \bigoplus_{i=1}^{n} \frac{k[x]}{(p_i(x))}.$$

Further, the Fundamental Theorem of Finitely Generated Modules over a Principal Ideal Domain guarantees that the monic polynomials satisfy $p_1(x) \mid p_2(x) \mid \cdots \mid p_n(x)$. We refer to these polynomials as the **invariant factors** of V with respect to T (or simply the invariant factors of T). Before we proceed, we advise the reader to review these notes on the Smith Normal Form.

The Rational Canonical Form

Using the invariant factor decomposition of a finite-dimensional k-vector space V as a $k[x]$-module with respect to a linear operator $T : V \to V$, we may deduce that every linear operator $T : V \to V$ is similar to a finite direct sum of companion matrices corresponding to its invariant factors.

Definition 1. Consider a monic polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ with coefficients in a field k. We define the **companion matrix** of $f(x)$ to be the $d \times d$ matrix

$$C_{f(x)} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}.$$

Observe that the quotient ring $k[x]/(f(x))$ can be viewed as a d-dimensional k-vector space with standard ordered basis $\{1+(f(x)), x+(f(x)), \dots, x^{d-1}+(f(x))\}$. On the other hand, multiplication by x is a linear operator on $k[x]/(f(x))$ that acts on the basis vectors of $k[x]/f(x)$ by

$$x \cdot [x^i + (f(x))] = x^{i+1} + (f(x))$$

and $x^d + (f(x)) = -a_0 - a_1 x - \cdots - a_{d-1}x^{d-1} + (f(x))$, hence the companion matrix $C_{f(x)}$ is nothing more than the matrix that represents multiplication by x with respect to the standard ordered basis of $k[x]/(f(x))$. Considering that V is a direct sum of such objects by the previous section, we may take a basis B_i corresponding to each cyclic factor $k[x]/(p_i(x))$ of V as a $k[x]$-module. By definition, we have that $T(v) = x \cdot v$ for each vector v, hence the matrix of T with respect to the basis B_i is none other than the companion matrix $C_{p_i(x)}$. Ultimately, we have the following.

Theorem 1. Let V be an n-dimensional k-vector space. Let T be a linear operator on V. Consider V as a finitely generated $k[x]$-module via the action $f(x) \cdot v = f(T)(v)$. If the invariant factors of V with respect to T are $p_1(x) \mid p_2(x) \mid \cdots \mid p_r(x)$, then the matrix of T with respect to the standard basis of V is similar to the direct sum of the companion matrices $C_1, \dots, C_r$ corresponding to the polynomials $p_1(x), \dots, p_r(x)$. Put another way, there exists an invertible matrix $n \times n$ matrix P with coefficients in k such that the matrix A of T with respect to the standard basis of V satisfies

$$A = P(C_1 \oplus C_2 \oplus \cdots \oplus C_r)P^{-1}.$$

We refer to $\text{RCF}(A) = \oplus_{i=1}^r C_i$ as the **Rational Canonical Form** of T (w.r.t. its invariant factors).

Consequently, in order to compute the Rational Canonical Form of T (with respect to its invariant factors), it suffices to compute the invariant factors of T. Let A be the matrix of T with respect to the basis $B = B_1 \cup B_2 \cup \cdots \cup B_r$ of V corresponding to the invariant factor decomposition

$$V \cong \bigoplus_{i=1}^r \frac{k[x]}{(p_i(x))}$$

of V. Let I be the identity matrix. Observe that $xI - A$ is an $n \times n$ matrix with coefficients in the principal ideal domain $k[x]$. By Theorem 2, the Smith Normal Form of $xI - A$ is given by

$$\text{SNF}(xI - A) = \underbrace{(1) \oplus \cdots \oplus (1)}_{n-r \text{ summands}} \oplus \bigoplus_{i=1}^r (p_i(x)),$$

where $p_1(x) \mid p_2(x) \mid \cdots \mid p_r(x)$ are the invariant factors of V with respect to T.

Proposition 1. Let V be an n-dimensional k-vector space. Let T be a linear operator on V represented by the matrix A. Let I be the $n \times n$ identity matrix. The following statements hold.

(1.) The invariant factors of V with respect to T (or simply the invariant factors of T) are the non-constant polynomials appearing along the diagonal of the Smith Normal Form of $xI - A$.

(2.) The largest invariant factor of T is the minimal polynomial of T.

(3.) The product of all invariant factors of T is the characteristic polynomial of T.

Proof. By the previous paragraph, statement (1.) holds. Considering that $p_1(x) \mid p_2(x) \mid \cdots \mid p_r(x)$, it follows that $p_r(x)$ annihilates each cyclic factor $k[x]/(p_i(x))$ of V, hence $p_r(x)$ annihilates V. By definition, the minimal polynomial of V divides $p_r(x)$. Conversely, $p_r(x)$ is a monic polynomial and $k[x]$ is a principal ideal domain, so the minimal polynomial of V must be $p_r(x)$, and statement (2.) holds. Last, the Smith Normal Form of $xI - A$ is similar to $xI - A$, so we have that

$$\det(xI - A) = \det(\text{SNF}(xI - A)) = p_1(x)p_2(x) \cdots p_r(x).$$

Considering that the characteristic polynomial of T is given by $\det(xI - A)$, statement (3.) holds. □

Combined, Theorem 1 and Proposition 1 above allow us to deduce the invariant factors, minimal polynomial, characteristic polynomial, and Rational Canonical Form of a linear operator.

Example 3. Let V be the $\mathbb{C}$-vector space of univariate polynomials of degree ≤ 3. Let $T : V \to V$ denote the linear operator $T(f(x)) = f(x) + f''(x)$. Compute the Rational Canonical Form of T.

Proof. We refer the reader to the proof as outlined in these notes. □

Example 4. (Exercise 12.2.9, Dummit and Foote) Let k be a field, and let c be an element of k. Compute the invariant factors, minimal polynomial, characteristic polynomial, and Rational Canonical Form of the linear operator $T : k^{\oplus 3} \to k^{\oplus 3}$ represented by the following matrix.

$$A = \begin{pmatrix} c & 0 & -1 \\ 0 & c & 1 \\ -1 & 1 & c \end{pmatrix}$$

Proof. By Theorem 1 and Proposition 1, it suffices to find the Smith Normal Form of $xI - A$. □

Occasionally, it behooves us to keep track of additional information relating to the Rational Canonical Form, e.g., the change-of-basis matrix P such that $P^{-1}AP = \text{RCF}(A)$. We accomplish this by carrying out the recipe outlined in Section 12.2 of Dummit and Foote as follows.

Proposition 2. (Finding the Change-of-Basis Matrix for the Rational Canonical Form) Let k be a field. Let A be an $n \times n$ matrix representing a linear operator $T : k^{\oplus n} \to k^{\oplus n}$. The change-of-basis matrix P such that $P^{-1}AP = \text{RCF}(A)$ can be found as follows.

(i.) Compute the Smith Normal Form of $xI - A$ by using elementary row and column operations to obtain a diagonal matrix with monic polynomials $p_1(x) \mid p_2(x) \mid \cdots \mid p_n(x)$. **Be sure to keep track of all row operations $R_i \leftrightarrow R_j$ and $\alpha R_i + R_j \mapsto R_j$.**

(ii.) Begin with the standard basis $\mathbf{e}_1, \dots, \mathbf{e}_n$ of $k^{\oplus n}$. Using the same order as the elementary row operations were performed, employ the inverse operation to the columns of the matrix $\begin{pmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{pmatrix}$, where the vectors $\mathbf{e}_i$ are taken to be the columns. Explicitly, if the row operation $R_i \leftrightarrow R_j$ was performed, then perform the column operation $C_i \leftrightarrow C_j$; if the row operation $\alpha R_i + R_j \mapsto R_j$ was performed, then perform the column operations $\alpha C_j - C_i \mapsto C_i$.

(iii.) If step (ii.) is completed correctly, the transformed matrix $\begin{pmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{pmatrix}$ should consist of standard basis vectors and polynomials acting on them. Use the action $f(x) \cdot \mathbf{e}_i = f(T)(\mathbf{e}_i)$ to write each column as a linear combination of the standard basis vectors $\mathbf{e}_1, \dots, \mathbf{e}_n$.

(iv.) The ith column of the transformed matrix $\begin{pmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{pmatrix}$ corresponds to the ith entry of the Smith Normal Form of $xI - A$ and so to the ith cyclic factor $k[x]/(p_i(x))$ of V. Consequently, the ith column vector of the transformed matrix corresponds to a $k[x]$-module generator of V. If the ith column of the transformed matrix is 0, then $p_i(x) = 1$ (and vice-versa), so the cyclic factor $k[x]/(p_i(x))$ vanishes. If the degree of $p_i(x)$ is one, then the cyclic factor of V corresponding to $k[x]/(p_i(x))$ has only one generator, and it is the ith column vector. If the degree of $p_i(x)$ is $d_i \geq 2$, then the cyclic factor of V corresponding to $k[x]/(p_i(x))$ has d_i generators, and they are the column vectors v_i, $T(v_i), \dots, T^{d_i - 1}(v_i)$.

(v.) The columns of the change-of-basis matrix P correspond to the generators of the cyclic factors found in step (iv.). Explicitly, if the degree of $p_i(x)$ is 1, then the ith column of the matrix P is the generator of the ith cyclic factor of V. If there is more than one generator, then write the columns in left-to-right order according to the vectors $v_i, T(v_i), \dots, T^{d_i - 1}(v_i)$.

Example 3, Cont'd. Recall that the matrix of T with respect to $B = (1, x, x^2, x^3)$ is given by

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Further, we found that $(x-1)^2$ and $(x-1)^2$ are the elementary divisors of A so that

$$\mathrm{RCF}(A) = C_{(x-1)^2} \oplus C_{(x-1)^2} = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \oplus \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

We employed the following row operations in succession to obtain $\mathrm{SNF}(xI - A)$.

(1.) $\frac{1}{2}(x-1)R_1 + R_3 \mapsto R_3$

(2.) $\frac{1}{6}(x-1)R_2 + R_4 \mapsto R_4$

Consequently, we must transform the 4×4 identity matrix accordingly.

$$\begin{aligned} \begin{pmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 \end{pmatrix} &\xrightarrow{\frac{1}{2}(x-1)C_3 - C_1 \mapsto C_1} \begin{pmatrix} \frac{1}{2}(x-1) \cdot \mathbf{e}_3 - \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 \end{pmatrix} \\ &\xrightarrow{\frac{1}{6}(x-1)C_4 - C_2 \mapsto C_2} \begin{pmatrix} \frac{1}{2}(x-1) \cdot \mathbf{e}_3 - \mathbf{e}_1 & \frac{1}{6}(x-1) \cdot \mathbf{e}_4 - \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 \end{pmatrix} \end{aligned}$$

By definition, we have that $f(x) \cdot v = f(A)v$. Consequently, we find that

$$\frac{1}{2}(x-1) \cdot \mathbf{e}_3 - \mathbf{e}_1 = \frac{1}{2}(A - I)\mathbf{e}_3 - \mathbf{e}_1 = \frac{1}{2}A\mathbf{e}_3 - \frac{1}{2}\mathbf{e}_3 - \mathbf{e}_1 = 0 \text{ and}$$

$$\frac{1}{6}(x-1) \cdot \mathbf{e}_4 - \mathbf{e}_2 = \frac{1}{6}(A - I)\mathbf{e}_4 - \mathbf{e}_2 = \frac{1}{6}A\mathbf{e}_4 - \frac{1}{6}\mathbf{e}_4 - \mathbf{e}_2 = 0.$$

We conclude that the transformed matrix from above is $\begin{pmatrix} 0 & 0 & \mathbf{e}_3 & \mathbf{e}_4 \end{pmatrix}$, hence our $k[x]$-module generators for V are $(x-1)^2$ and $(x-1)^2$. Consequently, the columns of the matrix P from left to right are $\mathbf{e}_3$, $A\mathbf{e}_3$, $\mathbf{e}_4$, and $A\mathbf{e}_4$. Explicitly, we find the following.

$$P = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 6 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Using WolframAlpha (for example), one can verify that $P^{-1}AP = \text{RCF}(A)$.

Example 4, Cont'd. Find the change-of-basis matrix P such that $P^{-1}AP = \text{RCF}(A)$.

The Jordan Canonical Form

We have just established that for any finite-dimensional k-vector space V with a linear operator $T : V \to V$, there exists a unique block-diagonal matrix — called the Rational Canonical Form (with respect to the invariant factors) of T — that is similar to the matrix of T with respect to the standard ordered basis of V. Explicitly, the Rational Canonical Form (w.r.t. invariant factors) is the direct sum of the companion matrices of the invariant factors of T. Consequently, there will generally be nonzero entries both above and below the main diagonal of this matrix.

One natural question to ask is if there is a refinement of the Rational Canonical Form for which the only nonzero entries are on or above the main diagonal. Our immediate task is to investigate this question and answer it in the affirmative when k is an algebraically closed field.

Let $p_1(x) \mid p_2(x) \mid \cdots \mid p_r(x)$ denote the invariant factors of T. Each of these is by definition a polynomial of degree ≥ 1, hence we may write $p_i(x)$ as a product of powers of irreducible polynomials $p_i(x) = q_{i_1}(x)^{e_{i_1}} \cdots q_{i_k}(x)^{e_{i_k}}$. We refer to $q_{i_j}(x)^{e_{i_j}}$ as an **elementary divisor** of T.

Example 3, Cont'd. Observe that the invariant factors of T are $(x-1)^2$ and $(x-1)^2$. Consequently, these are precisely the elementary divisors of T.

Example 5. Let k be a field — not necessarily algebraically closed. Suppose that T is a k-linear operator with invariant factors $x^2 - 4$ and $(x^2-4)(x^2+1)$. Considering that $x^2 - 4 = (x-2)(x+2)$, it follows that the elementary divisors of T are $x-2$, $x+2$, $x-2$, $x+2$, and x^2+1: the repetition of $x-2$ and $x+2$ comes from the fact that x^2-4 divides both of the invariant factors of T.

Proposition 3. Let V be an n-dimensional k-vector space. Let T be a linear operator on V represented by the matrix A. Let I be the $n \times n$ identity matrix. The following statements hold.

(1.) The elementary divisors of V with respect to T (or simply the elementary divisors of T) are the largest powers of the irreducible factors of the non-constant polynomials appearing along the diagonal of the Smith Normal Form of $xI - A$.

(2.) The elementary divisors all divide the minimal polynomial of T. In particular, the minimal polynomial gives rise to all of the elementary divisors — possibly without repetition.

(3.) The product of all elementary divisors of T is the characteristic polynomial of T.

(4.) If k is algebraically closed, then each elementary divisor is a power of a linear polynomial.

Example 4, Cont'd. Compute the elementary divisors of A; then, find the Rational Canonical Form of A with respect to the elementary divisors of A, i.e., $\text{RCF}(A) = \oplus_{i=1}^s C_i$, where C_i is the companion matrix of the ith elementary divisor of A. Explain how (and why) this differs from the Rational Canonical Form of A with respect to the invariant factors of A.

Crucially, if k is an algebraically closed field, then each elementary divisor of T is of the form $(x - \alpha)^d$ for some element $\alpha \in k$ and some integer $d \geq 1$.

Definition 2. Consider the monic polynomial $f_\alpha(x) = (x - \alpha)^d$ for some element $\alpha \in k$ and some integer $d \geq 1$. We define the **Jordan block** corresponding to $(x - \alpha)^d$ to be the $d \times d$ matrix

$$J_{f_\alpha(x)} = \begin{pmatrix} \alpha & 1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha & 1 & 0 & \cdots & 0 \\ 0 & 0 & \alpha & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & 0 & \cdots & \alpha \end{pmatrix}.$$

Put another way, we have that $J_{f_\alpha(x)} = \alpha I + S$, where I is the $d \times d$ identity matrix and S is the $d \times d$ matrix with 1s on the superdiagonal and 0s elsewhere.

Theorem 2. Let k be an algebraically closed field. Let V be an n-dimensional k-vector space. Let T be a linear operator on V. Consider V as a finitely generated $k[x]$-module via the action $f(x) \cdot v = f(T)(v)$. If the elementary divisors of V with respect to T are $q_1(x), \ldots, q_s(x)$, then the Jordan blocks $J_1, \ldots, J_s$ corresponding to the polynomials $q_1(x), \ldots, q_s(x)$ exist. Further, the matrix of T with respect to the standard basis of V is similar to the direct sum of the Jordan blocks $J_1, \ldots, J_s$. Put another way, there exists an invertible matrix $n \times n$ matrix P with coefficients in k such that the matrix A of T with respect to the standard basis of V satisfies $A = P(J_1 \oplus \cdots \oplus J_s)P^{-1}$. We refer to the block-diagonal matrix $\text{JCF}(A) = \oplus_{i=1}^s J_i$ as the **Jordan Canonical Form** of T.

Example 3, Cont'd. (Q5, January 2018) Compute the Jordan Canonical Form of T.

Example 4, Cont'd. Compute the Jordan Canonical Form of A. Explain how (and why) it differs from both Rational Canonical Forms of A.

Proposition 4. (Finding the Change-of-Basis Matrix for the Jordan Canonical Form) Let k be an algebraically closed field. Let A be an $n \times n$ matrix representing a linear operator $T : k^{\oplus n} \to k^{\oplus n}$. The change-of-basis matrix P such that $P^{-1}AP = \text{JCF}(A)$ can be found as follows.

(i.) Compute the Smith Normal Form of $xI - A$ by using elementary row and column operations to obtain a diagonal matrix with monic polynomials $p_1(x) \mid p_2(x) \mid \cdots \mid p_n(x)$. **Be sure to keep track of all row operations $R_i \leftrightarrow R_j$ and $\alpha R_i + R_j \mapsto R_j$.**

(ii.) Begin with the standard basis $\mathbf{e}_1, \dots, \mathbf{e}_n$ of $k^{\oplus n}$. Using the same order as the elementary row operations were performed, employ the inverse operation to the columns of the matrix $\begin{pmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{pmatrix}$, where the vectors $\mathbf{e}_i$ are taken to be the columns. Explicitly, if the row operation $R_i \leftrightarrow R_j$ was performed, then perform the column operation $C_i \leftrightarrow C_j$; if the row operation $\alpha R_i + R_j \mapsto R_j$ was performed, then perform the column operations $\alpha C_j - C_i \mapsto C_i$.

(iii.) If step (ii.) is completed correctly, the transformed matrix $\begin{pmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{pmatrix}$ should consist of standard basis vectors and polynomials acting on them. Use the action $f(x) \cdot \mathbf{e}_i = f(T)(\mathbf{e}_i)$ to write each column as a linear combination of the standard basis vectors $\mathbf{e}_1, \dots, \mathbf{e}_n$.

(iv.) The ith column of the transformed matrix $\begin{pmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_n \end{pmatrix}$ corresponds to the ith entry of the Smith Normal Form of $xI - A$ and so to the ith cyclic factor $k[x]/(p_i(x))$ of V. By hypothesis that k is algebraically closed, we have that $p_i(x) = (x - \alpha_{i_1})^{e_{i_1}} \cdots (x - \alpha_{i_k})^{e_{i_k}}$, hence we have that $k[x]/(p_i(x)) \cong \oplus_{j=1}^k k[x]/((x - \alpha_{i_j})^{e_{i_j}})$. Consequently, the ith column vector of the transformed matrix corresponds to some $k[x]$-module generators of V. If the ith column of the transformed matrix is 0, then $p_i(x) = 1$ (and vice-versa), so the cyclic factor $k[x]/(p_i(x))$ vanishes. If the degree of $p_i(x)$ is one, then the cyclic factor of V corresponding to $k[x]/(p_i(x))$ has only one generator, and it is the ith column vector. If the degree of $p_i(x)$ is $d_i \geq 2$, then the cyclic factor of V corresponding to $k[x]/(p_i(x)) \cong \oplus_{j=1}^k k[x]/((x - \alpha_{i_j})^{e_{i_j}})$ has many generators. Explicitly, they are the column vectors $(T - \alpha_{i_j})^{e_{i_j}-1}(v_i), \dots, (T - \alpha_{i_j})(v_i), v_i$ for each j.

(v.) The columns of the change-of-basis matrix P correspond to the generators of the cyclic factors found in step (iv.). Explicitly, if the degree of $p_i(x)$ is 1, then the ith column of the matrix P is the generator of the ith cyclic factor of V. If there is more than one generator, then write the columns in left-to-right order according to the vectors $(T - \alpha_{i_j})^{e_{i_j}-1}(v_i), \dots, (T - \alpha_{i_j})(v_i), v_i$.

Example 3, Cont'd. Recall that the matrix of T with respect to $B = (1, x, x^2, x^3)$ is given by

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Further, we found that $(x-1)^2$ and $(x-1)^2$ are the elementary divisors of A so that

$$\text{JCF}(A) = J_{(x-1)^2} \oplus J_{(x-1)^2} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We employed the following row operations in succession to obtain $\mathrm{SNF}(xI - A)$.

(1.) $\frac{1}{2}(x-1)R_1 + R_3 \mapsto R_3$

(2.) $\frac{1}{6}(x-1)R_2 + R_4 \mapsto R_4$

Consequently, we must transform the 4 × 4 identity matrix accordingly.

$$\begin{aligned}\begin{pmatrix}\mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4\end{pmatrix} &\xrightarrow{\frac{1}{2}(x-1)C_3 - C_1 \mapsto C_1} \begin{pmatrix}\frac{1}{2}(x-1)\cdot\mathbf{e}_3 - \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4\end{pmatrix} \\ &\xrightarrow{\frac{1}{6}(x-1)C_4 - C_2 \mapsto C_2} \begin{pmatrix}\frac{1}{2}(x-1)\cdot\mathbf{e}_3 - \mathbf{e}_1 & \frac{1}{6}(x-1)\cdot\mathbf{e}_4 - \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4\end{pmatrix}\end{aligned}$$

By definition, we have that $f(x) \cdot v = f(A)v$. Consequently, we find that

$$\frac{1}{2}(x-1)\cdot\mathbf{e}_3 - \mathbf{e}_1 = \frac{1}{2}(A-I)\mathbf{e}_3 - \mathbf{e}_1 = \frac{1}{2}A\mathbf{e}_3 - \frac{1}{2}\mathbf{e}_3 - \mathbf{e}_1 = 0 \text{ and}$$

$$\frac{1}{6}(x-1)\cdot\mathbf{e}_4 - \mathbf{e}_2 = \frac{1}{6}(A-I)\mathbf{e}_4 - \mathbf{e}_2 = \frac{1}{6}A\mathbf{e}_4 - \frac{1}{6}\mathbf{e}_4 - \mathbf{e}_2 = 0.$$

We conclude that the transformed matrix from above is $\begin{pmatrix}0 & 0 & \mathbf{e}_3 & \mathbf{e}_4\end{pmatrix}$, hence our $k[x]$-module generators for V are $(x-1)^2$ and $(x-1)^2$. Consequently, the columns of the matrix P from left to right are $(A-I)\mathbf{e}_3$, $\mathbf{e}_3$, $(A-I)\mathbf{e}_4$, and $\mathbf{e}_4$. Explicitly, we find the following.

$$P = \begin{pmatrix}2 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1\end{pmatrix}$$

Using WolframAlpha (for example), one can verify that $P^{-1}AP = \mathrm{JCF}(A)$.

References

- D.S. Dummit and R.M. Foote, *Abstract Algebra*, John Wiley & Sons, Inc., 2004.