NOTES on Connections between Polynomials, Matrices, and Vectors

Throughout this document, $\mathcal{V}$ will be a finite dimensional vector space over the field F, u, v, w, etc., will be vectors in $\mathcal{V}$, p, q, etc., will be polynomials in $F[x]$, S, T, etc., will be linear transformations/operators acting on $\mathcal{V}$ and mapping into $\mathcal{V}$, and A, B, C, etc., will be matrices with entries in F, but might also be considered the transformation on F^n that has the given matrix as its associated matrix with respect to the usual basis for F^n. The symbol I will represent the identity transformation or the identity matrix appropriate to the context.

- **Characteristic Polynomial:** For A an $n \times n$ matrix, the *characteristic polynomial of* A is the polynomial, p, of degree n given by $p(x) = \det(xI - A)$. The monomial $x - c$ is a factor of p if and only if c is an eigenvalue of A. More generally, if p is factored $p = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where p_1, p_2, $\cdots$, p_k are distinct irreducible monic polynomials over F and r_1, r_2, $\cdots$, r_k are positive integers, then each r_j is the dimension of the null space of $p_j(T)^{r_j}$. The Cayley-Hamilton Theorem says that if p is the characteristic polynomial of T, then $p(T) = 0$.

- **Minimal Polynomial:** The set $\{q \in F[x] : q(A) = 0\}$ includes the characteristic polynomial of A, so it is a non-empty set, and it is easy to see that it is an ideal in $F[x]$. The *minimal polynomial of* A is the monic generator, q, of this ideal. In particular, the minimal polynomial of A divides the characteristic polynomial, and if the characteristic polynomial p is factored $p = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where p_1, p_2, $\cdots$, p_k are distinct irreducible monic polynomials over F, then the minimal polynomial q is factored $q = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ where the s_j are positive integers satisfying $s_j \leq r_j$ for each $j = 1, \cdots, k$. Since the minimal polynomial of A satisfies $q(A) = 0$, then $Av = 0$ for every v in F^n.

- **T-Annihilator:** If T is a linear transformation on $\mathcal{V}$ and v is a vector in $\mathcal{V}$, then the minimal polynomial of T, q, satisfies $q(T)v = 0$. This means the set $\{f \in F[x] : f(T)v = 0\}$ is non-empty, and is clearly an ideal in $F[x]$. The monic generator of this ideal is called the *T-annihilator of* v. Since the minimal polynomial is in this ideal, the T-annihilator of v must divide the minimal polynomial of T, and this is true for every vector in $\mathcal{V}$. In addition, Lemma 1 below says that there is a vector in $\mathcal{V}$ for which the minimal polynomial of T is the T-annihilator of this vector.

- **Cyclic Subspace:** If T is a linear transformation on $\mathcal{V}$ and v is a vector in $\mathcal{V}$, the *cyclic subpace for T generated by* v is the set $Z(v, T) = \{g(T)v : g \in F[x]\}$. Since $F[x]$ is closed under addition and multiplication by scalars, the set $Z(v, T)$ is actually a subspace of $\mathcal{V}$ and it is an invariant subspace for T. If v is a vector for which $Z(v, T) = \mathcal{V}$, we say v *is a cyclic vector for* T. If $v \neq 0$, since $\mathcal{V}$ is a finite dimensional vector space, there is a positive integer k for which v, Tv, $\cdots$, $T^{k-1}v$, are linearly independent and $T^k v$ is a linear combination of these vectors. It is easy to see, by induction, that if g is a polynomial and $\deg(g) \geq k$, then $g(T)v$ is also a linear combination of these vectors. This means $Z(v, T) = \mathrm{span}\{v, Tv, \cdots, T^{k-1}v\}$ and the dimension of $Z(v, T)$ is k. Theorem 3 below says that if p_v is the T-annihilator of v, then the dimension of $Z(v, T)$ is the degree of p_v and that if U is the restriction of T to $Z(v, T)$, then p_v is both the minimal and characteristic polynomial for U.

- **Conductor:** Suppose T is a linear transformation on $\mathcal{V}$, the subspace W is invariant for T, and v is a vector in $\mathcal{V}$. The set $\mathcal{S} = \{f \in F[x] : f(T)v \in W\}$ is not the empty set because the minimal polynomial, q, for T satisfies $q(T)v = 0$ and q is in this set.

The invariance of W means that $f(T)v$ in W implies $(gf)(T)v = g(T)f(T)v$ is also in W and the set $\mathcal{S}$ is an ideal in $F[x]$. The *T-conductor of v into W* or, if context allows, *conductor of v into W*, denoted $S_T(v, W)$, is the monic generator of this ideal. Lemma 2 relates conductors of v into various subspaces and shows that the conductor of v is always a divisor of the minimal polynomial for T.

- **Companion Matrix:** Suppose W is a k-dimensional invariant subspace for T, a linear transformation on $\mathcal{V}$. If U is the restriction of T to W and v is vector in W that is cyclic for U, then the *companion matrix for U on W* is the matrix for U with respect to the basis v, Uv, $\cdots$, $U^{k-1}v$ for W. If p_v is the U-annihilator of v, then $p_v(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0$, and p_v is the minimal polynomial and characteristic polynomial for U on W. In particular, this means $U^kv = -c_0v - c_1Uv - c_2U^2v - \cdots - c_{k-1}U^{k-1}v$ and the companion matrix is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & & 0 & -c_2 \\ & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{k-1} \end{pmatrix}$$

- **Rational Canonical Form:** An $n \times n$ matrix A is said to be in *rational canonical form* if there is a direct sum $F^n = W_1 \oplus W_2 \oplus \cdots \oplus W_r$ for which

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & A_r \end{pmatrix}$$

  where each A_j is a companion matrix for the polynomial p_j and for each j with $2 \le j \le r$, the polynomial p_j divides the polynomial p_{j-1}. In particular, this means p_1 is the minimal polynomial for A and the characteristic polynomial is $p = p_1p_2 \cdots p_r$. It also implies that the W_j are cyclic subspaces for A. The Rational Canonical Form Theorem asserts that every linear transformation on a finite dimensional vector space is similar to a unique matrix in rational canonical form.

- **Jordan Block with Eigenvalue c:** Let c be in the field F and let k be a positive integer. The *Jordan block with eigenvalue c and size k* is the matrix

$$J = \begin{pmatrix} c & 0 & 0 & \cdots & 0 & 0 \\ 1 & c & 0 & \cdots & 0 & 0 \\ 0 & 1 & c & \cdots & 0 & 0 \\ & \vdots & & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & c & 0 \\ 0 & 0 & 0 & \cdots & 1 & c \end{pmatrix}$$

  (Some authors call the transpose of this matrix the Jordan block, but the two matrices are similar).

- **Jordan Canonical Form:** Let A be an $n \times n$ matrix over F whose minimal polynomial factors as a product of linear factors, $q(x) = (x - c_1)^{s_1}(x - c_2)^{s_2} \cdots (x - c_k)^{s_k}$ where the s_j are positive integers and the c_j are the distinct eigenvalues of A. The matrix A is said to be in *Jordan canonical form* if there is a direct sum $F^n = W_1 \oplus W_2 \oplus \cdots \oplus W_r$ for which

$$A = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & J_r \end{pmatrix}$$

where each J_ℓ is a Jordan block of size k_ℓ with eigenvalue one of the c_j's. The Jordan Canonical Form Theorem asserts that any $n \times n$ matrix A on F^n whose minimal polynomial factors into linear factors, is similar to a matrix in Jordan canonical form and it is unique up to the order of the blocks along the diagonal.

- **Admissible Subspace:** Let T be a linear transformation on the vector space $\mathcal{V}$ and let W be a subspace of $\mathcal{V}$. We say W *is an admissible subspace for* T if W is invariant for T and whenever $f(T)v$ is in W for some vector v in $\mathcal{V}$ and polynomial f, then there is a vector w in W such that $f(T)v = f(T)w$. We note that the subspace $W = (0)$ is admissible for every linear transformation: If $f(T)v \in (0)$, then $f(T)v = 0 = f(T)0$.

1. Some Justifications

Lemma 1. *Let A be an $n \times n$ matrix with entries in the field F and let q be the minimal polynomial for A. There is a vector v in F^n for which the A-annihilator of v is the polynomial q.*

Proof. Let $p = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ and $q = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ be, respectively, the characteristic and minimal polynomials of A where p_1, p_2, $\cdots$, p_k are distinct irreducible monic polynomials over F and r_j and s_j are integers with $1 \le s_j \le r_j$. We have seen that $\mathcal{V}$ is a direct sum of the null spaces of the operators $p_j(A)_j^r$ for $j = 1, \cdots, k$ so that every vector v can be written as $v = v_1 + v_2 + \cdots + v_k$ where v_j is in the null space of $p_j(A)^{r_j}$. If u is in the nullspace of $p_j(A)^{r_j}$, then because q is the minimal polynomial for A, we know that $p_j(A)^{s_j} u = 0$. Moreover, because q is the minimal polynomial, there is no number smaller than s_j that works for every vector in nullspace of $p_j(A)^{r_j}$, that is, there is a vector u_j in nullspace of $p_j(A)^{s_j}$ but not in the nullspace of $p_j(A)^{(s_j-1)}$. After finding such vectors for all j, we let $v = u_1 + u_2 + \cdots + u_k$ and see that q is the A-annihilator of v. ◻

Lemma 2. *For $\mathcal{V}$ a finite dimensional vector space, let T be a linear operator on $\mathcal{V}$. If W_1 and W_2 are invariant subspaces for T with $W_1 \subset W_2$ and v is a vector in $\mathcal{V}$, then the T-conductor of v into W_2 divides the T-conductor of v into W_1. In particular, the T-conductor of any vector into any invariant subspace for T divides the minimal polynomial for T.*

Proof. Let J_1 be the ideal $\{f \in F[x] : f(T)v \in W_1\}$ and J_2 be the ideal $\{f \in F[x] : f(T)v \in W_2\}$. Clearly, every polynomial in J_1 is also a polynomial in J_2 because $W_1 \subset W_2$. In particular, the T-conductor of v into W_1, the monic generator of the ideal J_1, is in the ideal J_2. This means the monic generator of J_2, the conductor of v into W_2 divides the conductor of v into W_1. Since (0) is an invariant subspace for T that is a subspace of any invariant subspace for T and since the minimal polynomial, q, for T satisfies $q(T)v = 0$ for all v in $\mathcal{V}$, the T-conductor of any vector into any subspace divides the minimal polynomial of T. ◻

Theorem 3. *Let $\mathcal{V}$ be a finite dimensional vector space and let T be a linear operator on $\mathcal{V}$. If v is a vector in $\mathcal{V}$ and p_v is the T-annihilator of v, then the degree of p_v is the dimension of $Z(v,T)$ and if U is the restriction of T to $Z(v,T)$, then p_v is both the minimal polynomial and the characteristic polynomial of U on $Z(v,T)$.*

Proof. If $p_v(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0$ is the T-annihilator of v, then $p_v(T)v = T^kv + c_{k-1}T^{k-1}v + \cdots + c_2T^2v + c_1Tv + c_0v = 0$, but there is no polynomial, q, of degree $k-1$ or less that has $q(T)v = 0$. In particular, this means the vectors $T^{k-1}v$, $\cdots$, T^2v, Tv, and v are linearly independent. On the other hand,
$T^kv = -c_{k-1}T^{k-1}v - \cdots - c_2T^2v - c_1Tv - c_0v$, which means $Z(v,T)$ has the set $\{T^{k-1}v, \cdots, T^2v, Tv, v\}$ as a basis. We conclude the dimension of $Z(v,T)$ is the degree of p_v and that p_v is the minimal and characteristic polynomial of T restricted to the cyclic subspace $Z(v,T)$. $\square$

Theorem 4. (Cyclic Decomposition Theorem) *Let T be a linear transformation on the finite dimensional vector space $\mathcal{V}$ and let W_0 be a proper subspace of $\mathcal{V}$ that is admissible for T. There are non-zero vectors v_1, v_2, $\cdots$, v_r in $\mathcal{V}$ with, respectively, T-annihilators p_1, p_2, $\cdots$, p_r so that*

(1) $\qquad \mathcal{V} = W_0 \oplus Z(v_1,T) \oplus Z(v_2,T) \oplus \cdots \oplus Z(v_r,T)$

and

(2) $\qquad$ *for* $2 \leq j \leq r$, *the polynomial* p_j *divides the polynomial* p_{j-1}.

Moreover, the integer r and p_1, p_2, $\cdots$, p_r are uniquely determined by (1) *and* (2) *as long as $v_j \neq 0$ for all j.*