6: Applications to Linear Algebra

Throughout, V is a finite-dimensional vector space over a field F, and $M = V_T$; the vector space with endomorphism $T : V \longrightarrow V$.

Remark: The set $End(V)$ of linear transformations $V \longrightarrow V$ is a finite-dimensional vector space over F, the set $\{I, T, T^2, \ldots\}$ is linearly dependent, thus for some non-zero $f(x) \in F[x]$,

$$f(T) = a_0 I + a_1 T + \cdots + a_k T^k = 0.$$

WLOG, assume $f(x)$ is monic, and of minimal (positive) degree. Uniqueness is immediate; if $f(T) = g(T) = 0$, then $\deg(f(x) - g(x)) < \deg f(x)$, and thus $f(x) - g(x) = 0$.

Def. The minimal polynomial $m_T(x)$ of $T \in End(V)$ is the unique monic polynomial of minimal positive degree such that $m_T(T) = 0$.

Remark: By the division algorithm, if $f(T) = 0$, then $m_T(x) \mid f(x)$.

Recall from linear algebra that the characteristic polynomial of $T \in End(V)$ is $f_T(x) = \det(A - \lambda I)$. (We'll prove soon that $m_T(x) \mid f_T(x)$).

Example 1: Let $F = \mathbb{Q}$, $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. $m_T(x) = f_T(x) = x^2 - 2x + 1$

Example 2: Let $F = \mathbb{Q}$, $T = \begin{bmatrix} 4 & -6 & 3 \\ 4 & -7 & 4 \\ 6 & -12 & 7 \end{bmatrix}$

$m_T(x) = x^2 - 3x + 2$, $\quad f_T(x) = -x^3 + 4x^2 - 5x + 2$

* By definition, $m_T(x)$ is the exponent of the torsion module V_T.
If $\mathcal{B} \subseteq V$ is a basis (for V as an F-vector space), the $\mathcal{B}$ clearly generates V_T as a submodule $\Rightarrow$ V_T is finitely generated.

Def: A subspace $W \subseteq V$ is a <u>T-invariant subspace</u> of V if $f(T)\,W \subseteq W$ for all $f(x) \in F[x]$.

Thus, the submodules of V_T are (by definition) just the T-invariant subspaces of V.

Prop 6.1: Suppose $W = R\langle v\rangle$ is a cyclic submodule of V_T, and that W has order $f(x) \in F[x]$, where $\deg f(x) = k > 0$. Then $\mathcal{B} = \{v, Tv, T^2v, \ldots T^{k-1}v\}$ is a (vector space) basis for W.
The vector v is called a <u>cyclic vector</u> for $W \subseteq V_T$.

Pf: If $w \in W$, then $w = g(T)\,v$ for some $g(x)$ with $\deg g(x) < k$, thus $\mathcal{B}$ spans W.
If $\mathcal{B}$ were not linearly independent, then there would be some $a_0, \ldots, a_{k-1} \in F$ s.t. $a_0 v + a_1 Tv + \cdots + a_k T^{k-1} v = 0$, not all $a_i = 0$.
Then the polynomial $g(x) = a_0 + a_1 x + \cdots + a_k x^{k-1}$ would be in the annihilator ideal of v, i.e., $f(x) \mid g(x)$ ↯ $(\deg f(x) > \deg g(x))$. $\square$

Def: Suppose F is a field, and $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ a monic polynomial in $F[x]$. Define the <u>companion matrix</u> of $f(x)$ to be the $n \times n$ matrix

$$C(f) = \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & & 0 & -a_1 \\ & 1 & 0 & -a_2 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & & 1 \quad 0 & \\ 0 & 0 \cdots 0 & 1 & -a_{n-1} \end{pmatrix}$$

Example 3: The companion matrix of $f(x) = 2 - 3x + x^3$ is

$$C(f) = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}.$$

Prop 6.2: If F is a field, $f(x) \in F[x]$ monic of degree n, and $T \in \mathrm{End}(V)$ the linear transformation corresponding to the companion matrix $C(f)$, then the minimal polynomial $m_T(x)$ is $f(x)$.

Pf: Let $e_1, \dots, e_n$ be the standard basis vectors for F^n.

Clearly, $Te_i = e_{i+1}$ for $1 \le i \le n-1$,

and $Te_n = -a_0 e_1 - a_1 e_2 - \cdots - a_{n-1} e_n$.

Together, this implies that $e_2 = Te_1$, $e_3 = T^2 e_1, \dots, e_n = T^{n-1} e_1$.

$\Rightarrow Te_n = T^n e_1 = -a_0 I e_1 - a_1 T e_1 - \cdots - a_{n-1} T^{n-1} e_1$

$\Rightarrow f(T) e_1 = 0$.

Therefore, $f(T) e_i = f(T) T^{i-1} e_1 = T^{i-1} f(T) e_1 = 0$

$\Rightarrow f(T) v = 0$ for all $v \in V$.

$\Rightarrow f(x) \in (m_T(x))$, i.e., $m_T(x) \mid f(x)$. ✓

Now, suppose $g(x) = b_0 + b_1 x + \cdots + b_k x^k \in F[x]$, with $g(T) = 0$ and

$\deg g(x) = k < n = \deg f(x)$. We must show that $g(x) = 0$.

$$g(T)e_1 = \sum_{j=0}^{k} b_j T^j e_1 = \sum_{j=0}^{k} b_j e_{j+1} = 0 \Rightarrow b_j = 0 \Rightarrow g(x) = 0 \checkmark$$

Therefore, $m_T(x) = f(x)$. $\square$

Remark: The characteristic polynomial of a companion matrix $C(f)$ is $\pm f(x)$.

Prop 6.3: Suppose $W = R\langle v\rangle$ is a cyclic submodule of V_T, and that the order of W is the monic polynomial $f(x) \in F[x]$ of degree k. Then the restriction $T|_W$ in matrix form is $C(f)$, w.r.t. the basis $\mathcal{B} = \{v, Tv, \ldots, T^{k-1}v\}$ for W.

Pf: By Prop 6.1, $\mathcal{B}$ is indeed a basis for W.

For $0 \le i \le k-2$, $T(T^i v) = T^{i+1} v$

Let $f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + x^k$ (the order of W, i.e., $\mathrm{Ann}(v) = (f(x))$.)

Thus, $T(T^{k-1}v) = T^k v = -a_0 I v - a_1 T v - \cdots - a_{k-1} T^{k-1} v$. $\square$

Thm 6.4: Let V be a finite-dimensional vector space over F, and $T \in \mathrm{End}(V)$. Then there is a basis for V for which the matrix form of T has the block diagonal form

$$A = \begin{pmatrix} C(f_1) & & & 0 \\ & C(f_2) & & \\ & & \ddots & \\ 0 & & & C(f_k) \end{pmatrix},$$ where each $f_i(x)$ is a (monic) invariant factor of V_T, so that $f_i(x) \mid f_{i-1}(x)$, $2 \le i \le k$. Furthermore,

$m_T(x) = f_1(x)$ and the characteristic polynomial of T is

$f_T(x) = \pm \prod_{i=1}^{k} f_i(x)$.

Pf: By Thm 5.7, V_T is a direct sum of cyclic submodules,

specifically, $V_T = W_1 \oplus \cdots \oplus W_k$, where $W_i = F[x]\langle v_i \rangle$ is cyclic of order $f_i(x)$ (wlog, assume it's monic).

The block diagonal form of A is immediate from Prop 6.3.

By definition, $m_T(x)$ is an exponent of T, and by Thm 5.7, $f_1(x)$ is an exponent of T. Since both are monic, $m_T(x) = f_1(x)$.

By the previous Exercise, the characteristic polynomial is

$\pm f(x) = \prod_{i=1}^{k} f_i(x)$, the product of the companion matrices. □

Cor (Cayley-Hamilton Theorem): The minimal polynomial $m_T(x)$ divides the characteristic polynomial $f_T(x)$, and thus $f_T(T) = 0$.

Def: The matrix A in Theorem 6.4 (in Block diagonal form, $[C(f_i)]$) is said to be a rational canonical matrix

Note: All entries of A lie in F, hence the name "rational" matrix, (unlike a Jordan matrix, to be introduced later!)

Recall: Two matrices A and B represent the same linear transformation (w.r.t. different bases) iff there is an invertible matrix C with entries in F such that $B = C^{-1}AC$.

In the above setting, C is the change of basis matrix, and A and B are said to be <u>similar</u> over F.

Suppose A represents T w.r.t. the basis $\{v_i\}$ and B represents T w.r.t. the basis $\{w_i\}$, and let C be the matrix representing the linear transformation

$$V \longrightarrow V, \qquad w_i \longmapsto v_i. \qquad \left(\text{i.e., } w_i = \sum_{j=1}^{n} c_{ji} v_i\right)$$

Then we have $B = C^{-1}AC$, and so A and B are similar over F:

$$\begin{tikzcd}
V \arrow[r, "B"] \arrow[d, "C"'] & V \arrow[d, "C"] \\
V \arrow[r, "A"'] & V
\end{tikzcd}$$

<u>Thm 6.5</u>: If A is an $n \times n$ matrix with entries in F, then A is similar to a unique rational canonical matrix, called its <u>rational canonical form</u>. Two matrices A and B are similar over F iff they have the same rational canonical form.

<u>Pf</u>: <u>Immediate</u> from Thm 5.8 (uniqueness of cyclic decomposition), and Thm 6.4. $\square$

<u>Cor</u>: Let K/F be an extension field, A and B $n \times n$ matrices with entries in F but similar over K. Then A and B are similar over F.

<u>Pf</u>: By Thm 6.5, A and B are similar to the same rational canonical matrix P; say $C^{-1}AC = P = D^{-1}BD$, with all matrices having entries in F. Therefore,
$A = (DC^{-1})^{-1} B (DC^{-1})$. $\square$

$$\begin{tikzcd} V \arrow[r, "B"] & V \\ V \arrow[u, "D"] \arrow[r, "P"] \arrow[d, "C"'] & V \arrow[u, "D"'] \arrow[d, "C"] \\ V \arrow[r, "A"] & V \end{tikzcd}$$

<u>Next</u>: Interpret primary decomposition and elementary divisors of $M = V_T$ in <u>matrix form</u>. (See Prop 5.10, Thm 5.11).

Prop 5.10 $\Rightarrow V_T = V_T[p_1(x)^{d_1}] \oplus \cdots \oplus V_T[p_k(x)^{d_k}]$, where each $p_i(x)$ is a distinct prime (irreducible factor of $m_T(x)$, and WLOG, irreducible).

Thm 5.11 $\Rightarrow V_T[p_i(x)^{d_i}] = M_{i_1} \oplus \cdots \oplus M_{i_k}$, where M_{i_j} is cyclic of order $p_i(x)^{d_{ij}}$.

<u>Note</u>: The set $\{p_1(x)^{d_1}, \ldots, p_k(x)^{d_k}\}$ are the <u>invariant factors</u>.

The set $\{p_{ij}(x)^{d_{ij}}\}$ are the <u>elementary divisors</u> of T.

We may assume WLOG that all of these polynomials are monic.

8

By Thm 5.11, two $n \times n$ matrices with entries in F are similar over F iff the have the same set of elementary divisors.

Suppose one of the irreducible factors $p_i(x)$ of $m_T(x)$ is linear, say $p_i(x) = x - a_i$. (For example, this is true if F is alg. closed)

Suppose $p_i(x)^{d_{ij}} = (x-a_i)^{d_{ij}}$ is one of the elementary divisors of T, and let $V_{ij} \subseteq V_T$ be a cyclic submodule of order $(x-a_i)^{d_{ij}}$; so say $V_{ij} = R\langle v \rangle$.

$T|_{V_{ij}}$ is a linear transformation $V_{ij} \longrightarrow V_{ij}$, with minimal polynomial $p_i(x)^{d_{ij}} = (x-a_i)^{d_{ij}}$.

Thus every element of V_{ij} is of the form $f(x) \cdot v$, for some $f(x) \mid (x-a_i)^{d_{ij}}$, i.e., $(x-a_i)^{c_i} \cdot v = (T - a_i I)^{c_i} v$, and so we can view V_{ij} as a cyclic submodule of $V_{T-a_i I}$, generated by v.

By Prop 6.3, the set $\{v, (T-a_i I)v, (T-a_i I)^2 v, \ldots, (T-a_i I)^{d_{ij}-1} v\}$ is a basis for V_{ij}.

<u>Note:</u>

$$Tv = a_i v + (T-a_i I)v$$

$$T(T-a_i I)v = a_i (T-a_i I)v + (T-a_i I)^2 v$$

$$T(T-a_i I)^{d_{ij}-2} v = a_i (T-a_i I)^{d_{ij}-2} v + (T-a_i I)^{d_{ij}-1} v$$

$$T(T-a_i I)^{d_{ij}-1} v = a_i (T-a_i I)^{d_{ij}-1} v$$

Thus, the matrix of $T|_{V_{ij}}$ is

$$A_{ij} = \begin{bmatrix} a_i & & & & & \\ 1 & a_i & & & 0 & \\ & 1 & a_i & & & \\ & & 1 & \ddots & & \\ & 0 & & & a_i & \\ & & & & 1 & a_i \end{bmatrix}_{d_{ij} \times d_{ij}}$$

which is called a <u>Jordan block</u>.

A block diagonal matrix whose diagonal blocks are Jordan blocks is a Jordan matrix, e.g., $J = \begin{bmatrix} A_{1j_1} & & & 0 \\ & A_{2j_2} & & \\ & & \ddots & \\ 0 & & & A_{kj_k} \end{bmatrix}$

If $T \in End(V)$ can be represented by a Jordan matrix J, then J is called the <u>Jordan canonical form</u> for T (or for any matrix that represents T.

Since a Jordan matrix is determined by elementary divisors of T, it is unique, up to relabeling of the linear factors $p_i(x)$ (i.e, rearrangement of diagonal blocks).

We say that if Jordan matrices J and J' differ by such a rearrangement, then they are the "same"

The following theorem is a direct application of Thm 5.11 (Elementary Divisor Theorem).

<u>Thm 6.6</u>: If $T \in End(V)$ and all irreducible factors of $m_T(x)$ are linear, then V has a basis relative to which T is represented by a Jordan matrix. If $F = \bar{F}$, and A, B are $n \times n$ matrices with entries in F, then A and B are similar over F iff they have the same Jordan canonical form.

<u>Thm 6.7</u>: If $\dim_F V < \infty$, and $T \in End(V)$, then T can be represented by a diagonal matrix iff $m_T(x)$ splits into distinct linear factors in $F[x]$.

<u>Pf</u>: T can be represented by a diagonal matrix
iff T can be represented by a Jordan matrix with 1×1 blocks
iff every elementary divisor of T has degree 1.
In this case, the exponent of each primary submodule is linear, and the product of these exponents is the exponent of V_T, which is $m_T(x)$. $\square$