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

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

\[
f(T) = a_0 I + a_1 T + \ldots + a_k T^k = 0.
\]

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 \( T \in \text{End}(V) \) 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 \( T \in \text{End}(V) \) is \( f_T(x) = \det (A - xI) \). (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 \( F = \mathbb{Q} \), \( T = \begin{bmatrix} 4 & -6 & 3 \\ 4 & -7 & 2 \\ 6 & -12 & 7 \end{bmatrix} \)

\[ m_T(x) = x^2 - 3x + 2, \quad f_T(x) = -x^3 + 4x^2 - 5x + 2. \]
By definition, $M_T(N)$ is the exponent of the torsion module $V_T$.

If $B \subseteq V$ is a basis (for $V$ as an $F$-vector space), the $B$

clearly generates $V_T$ as a submodule $\Rightarrow$ $V_T$ is finitely generated.

**Def:** A subspace $W \subseteq V$ is a $T$-invariant subspace 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 $W = \mathbb{R}\langle v \rangle$ is a cyclic submodule of $V_T$, and

that $W$ has order $f(x) \in F[x]$, where $\deg f(x) = k > 0$. Then

$B = \{v, Tv, T^2v, \ldots, T^{k-1}v\}$ is a (vector space) basis for $W$.

The vector $v$ is called a cyclic vector for $W \subseteq V_T$.

**Pf:** If $w \in W$, then $w = g(T)v$ for some $g(x)$ with $\deg g(x) < k$,

then $B$ spans $W$.

If $B$ were not linearly independent, then there would be

some $a_0, \ldots, a_{k-1} \in F$ s.t.

$a_0v + a_1Tv + \ldots + a_{k-1}T^{k-1}v = 0$, not all $a_i = 0$.

Then the polynomial $g(x) = a_0 + a_1x + \ldots + a_{k-1}x^{k-1}$ would be in the

annihilator ideal of $v$, i.e., $f(v) | g(x)$ if $\deg f(x) > \deg g(x)$.

**Def:** Suppose $F$ is a field, and $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$

a monic polynomial in $F[x]$. Define the companion matrix of $f(x)$ to be the $n \times n$ matrix
Example 3: The companion matrix of \( f(x) = 2 - 3x + x^3 \) is
\[
C(f) = \begin{pmatrix}
0 & 0 & -a_0 \\
1 & 0 & -a_1 \\
0 & 1 & -a_2 \\
0 & 0 & 1 & -a_3
\end{pmatrix}
\]

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

Proof: Let \( e_1, \ldots, e_n \) be the standard basis vectors for \( F^n \).

Clearly, \( Te_i = e_{i+1} \) for \( 1 \leq i \leq n-1 \), and \( Te_n = -a_0 e_1 - a_1 e_2 - \cdots - a_{n-1} e_n \).

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

\[ T e_n = T^n e_1 = -a_0 T^{n-1} e_1 - a_1 T^{n-2} e_1 - \cdots - a_{n-1} T e_1 - a_n e_1 \]

\[ \Rightarrow f(T) e_1 = 0. \]

Therefore, \( f(T) e_1 = f(T) T^{n-1} e_1 = T^{n-1} f(T) e_1 = 0 \).

\[ \Rightarrow f(T) v = 0 \text{ for all } v \in V. \]

\[ \Rightarrow f(x) \in (m_T(x)), \text{ i.e. } m_T(x) | f(x). \]
Now, suppose \( g(x) = b_0 + b_1 x + \ldots + b_k x^k \in F[x] \), with \( g(T) = 0 \) and \( \deg g(x) = k < n = \deg f(x) \). We must show that \( g(x) = 0 \).

\[
\begin{align*}
    g(T)e_j &= \sum_{j=0}^{k} b_j T^j e_i = \sum_{j=0}^{k} b_j e_{j+1} = 0 \\
    &\implies b_j = 0 \\
    &\implies g(x) = 0 \\
\end{align*}
\]

Therefore, \( m_T(x) = f(x) \). \( \Box \)

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

Prop 6.3: Suppose \( W = \mathbb{R}(v) \) 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 \( B = \{ v, T v, \ldots, T^{k-1} v \} \) for \( W \).

Proof: By Prop 6.1, \( B \) is indeed a basis for \( W \).

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

let \( f(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} + x^k \) (the order of \( W \), i.e., \( \text{Ann}(v) = (f(x)) \)).

Then, \( T(T^{k-1} v) = T^k v = -a_0 I v - a_1 T v - \ldots - a_{k-1} T^{k-1} v \). \( \Box \)

Thu 6.4: Let \( V \) be a finite-dimensional vector space over \( F \), and \( T \in \text{End}(V) \). Then there is a basis for \( V \) for which the matrix form of \( T \) has the block diagonal form.
\[
A = \begin{pmatrix}
C(f_1) & 0 \\
C(f_2) & \ddots \\
0 & \cdots & C(f_k)
\end{pmatrix},
\]
where each \( f_i(x) \) is a \( (n,m_i) \)-invariant factor of \( V_i \), so that \( f_i(y) \mid f_{i-1}(y) \), \( z \leq i \leq k \). Furthermore, \( M_T(x) = f_1(x) \) and the characteristic polynomial of \( T \) is
\[
f_T(x) = \pm \prod_{i=1}^{k} f_i(x).
\]

**Proof:** 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 \( f_i(y) \) (wlog, assume it's monic).

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

By definition, \( m_T(y) \) is an exponent of \( T \), and by Thm 5.7, \( f_i(x) \) is an exponent of \( T \), since both are monic, \( M_T(x) = f_1(x) \).

By the previous Exercise, the characteristic polynomial is
\[
\pm f(x) = \prod_{i=1}^{k} f_i(x), \text{ the product of the companion matrices.}
\]

**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) \textit{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 similar 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 $V \to V$, $w_i \mapsto v_i$. (i.e., $w_i = \sum_j c_{ij} v_i$)

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

\[ \begin{array}{ccc} V & \overset{B}{\longrightarrow} & V \\ C \downarrow & & \downarrow C \\ V & \overset{A}{\longrightarrow} & V \end{array} \]

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

\textbf{PF:} Immediate from Thm 5.8 (uniqueness of cyclic decomposition), and Thm 6.4.
Cor: Let $K/F$ be an extension field, $A$ and $B$ non-matrices with entries in $F$ but similar over $K$. Then $A$ and $B$ are similar over $F$.

**Proof:** By Thm 6.5, $A$ and $B$ are similar to the same rational canonical matrix $P$; say $C^tAC = P = D^tBD$, with all matrices having entries in $F$. Therefore, $A = (DC^{-1})^tB(DC^{-1})$.

Next: Interpret primary decomposition and elementary divisors of $M = V_T$ in matrix form. (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 $P_i(x)^{d_{i_j}}$.

**Note:** The set $\{P_1(x)^{d_1}, \ldots, P_k(x)^{d_k}\}$ are the **invariant factors**.

The set $\{P_i(x)^{d_{i_j}}\}$ are the **elementary divisors** of $T$.

We may assume WLOG that all of these polynomials are **monic**.
By Thm 5.11, two non-singular 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 $V_{ij} \in V_T$ 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 $V_{ij} \to V_{ij}$, 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., $(x-a_i)^{c_i} \cdot v = (T-a_iI)^{c_i}v$, and so

we can view $V_{ij}$ as a cyclic submodule of $V_{T-a_iI}$, generated

by $v$.

By Prop 6.3, the set $\{v, (T-a_iI)v, (T-a_iI)^2v, \ldots, (T-a_iI)^{d_{ij}-1}v\}$

is a basis for $V_{ij}$.

Note:

\[ T \cdot v = a_i \cdot v + (T-a_iI) \cdot v \]

\[ T(T-a_iI) \cdot v = a_i(T-a_iI) \cdot v + (T-a_iI)^2 \cdot v \]

\[ T(T-a_iI)^{d_{ij}-2} \cdot v = a_i(T-a_iI)^{d_{ij}-2} \cdot v + (T-a_iI)^{d_{ij}-1} \cdot v \]

\[ T(T-a_iI)^{d_{ij}-1} \cdot v = a_i(T-a_iI)^{d_{ij}-1} \cdot v \]
Thus, the matrix of $T|_{U_j}$ is

$$A_{ij} = \begin{bmatrix} a_{ij} & 1 & & \cdots & 1 \\ 1 & a_{ij} & & & 1 \\ & 1 & \ddots & & \vdots \\ & & & 1 & a_{ij} \\ & & & 1 & 1 \end{bmatrix}_{d_i \times d_j}$$

which is called a Jordan block.

A block diagonal matrix whose diagonal blocks are Jordan blocks is a Jordan matrix, e.g., $J = \begin{bmatrix} A_{11} & 0 & & \cdots & 0 \\ 0 & A_{22} & & & \vdots \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & A_{kk} & \end{bmatrix}$

If $T \in \text{End}(V)$ can be represented by a Jordan matrix $J$, then $J$ is called the Jordan canonical form 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).
Thm 6.6: If $T \in \text{End}(V)$ 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 $F = \mathbb{F}$, 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.

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

Pf: $T$ can be represented by a diagonal matrix iff $T$ can be represented by a Jordan matrix with $1 \times 1$ 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 $M_T(x)$. \qed