Riesz Representation Theorem

Suppose V is finite dimensional and $\varphi \in \mathcal{L}(V)$. Then $\exists$ a unique vector $u \in V$ such that

$$\varphi(v) = \langle v, u \rangle \qquad \forall v \in V$$

Proof

Let $e_1, \dots, e_n$ be an orthonormal basis for V. Then

$\exists$
$$\begin{aligned}
\varphi(v) &= \varphi(\langle v, e_1\rangle e_1 + \dots + \langle v, e_n \rangle e_n) \\
&= \varphi(e_1)\langle v, e_1\rangle + \dots + \varphi(e_n)\langle v, e_n\rangle \\
&= \langle v, \overline{\varphi(e_1)} e_1\rangle + \dots + \langle v, \overline{\varphi(e_n)} e_n\rangle \\
&= \langle v, \underbrace{\overline{\varphi(e_1)} e_1 + \dots + \overline{\varphi(e_n)} e_n}_{u}\rangle
\end{aligned}$$

$!$

Suppose $u_1, u_2 \in V$ such that

$$\varphi(v) = \langle v, u_1\rangle = \langle v, u_2 \rangle \qquad \forall v \in V.$$

Then

$$0 = \langle v, u_1 - u_2\rangle \rightarrow u_1 - u_2 = 0 \rightarrow u_1 = u_2$$

Orthogonal Complement, $U^\perp$

If $U \subseteq V$, then the **orthogonal** complement of U, denoted $U^\perp$, is the set of all vectors in V that are orthogonal to every vector in U

$$U^\perp = \{ v \in V \mid \langle v, u \rangle = 0 \ \forall u \in U\}$$

Properties of Orthogonal Complement

(a) If $U \subseteq V$, then $U^\perp \subseteq V$

(b) $\{0\}^\perp = V$

(c) $V^\perp = \{0\}$

(d) If $U \subseteq V$, then $U \cap U^\perp \subset \{0\}$

(e) If U, W subsets of V and $U \subset W$, then $W^\perp \subset U^\perp$

Direct Sum of Subspace and Orthogonal Complement

Suppose U is a finite-dimensional subspace of V. Then

$$V = U \oplus U^\perp \qquad \Rightarrow \dim U^\perp = \dim V - \dim U$$

Proof

$$v = u + v - u$$

$$u = \langle v, e_1 \rangle e_1 + \cdots + \langle v, e_m \rangle e_m$$

Orthogonal Complement of Orthogonal Complement

$U \subseteq V$, $\dim U = m < \infty$

$$U = (U^\perp)^\perp$$

Orthogonal Projection, P_U

Suppose U is a finite-dimensional subspace of V. The **orthogonal projection** of V onto U is the operator $P_U \in \mathcal{L}(V)$ defined as follows: For $v \in V$, write $v = u + w$, where $u \in U$ and $w \in U^\perp$. Then $P_U v = u$

Properties of the Orthogonal Projection, P_U

Suppose U is a finite-dimensional subspace of V and $v \in V$. Then

(a) $P_U \in \mathcal{L}(V)$

(b) $P_U u = u \quad \forall\ u \in U$

(c) $P_U w = 0 \quad \forall\ w \in U^\perp$

(d) range $P_U = U$

(e) null $P_U = U^\perp$

(f) $v - P_U v \in U^\perp$

(g) $P_U^2 = P_U$

(h) $\|P_U v\| \leq \|v\|$

(i) For every orthonormal basis $e_1, \ldots, e_m$ of U,

$$P_U v = \langle v, e_1 \rangle e_1 + \cdots + \langle v, e_m \rangle e_m$$

Proof

(a) Need to show $P_U : V \to V$ a linear map.

Suppose $v_1, v_2 \in V$.

Write $\quad v_1 = u_1 + w_1, \quad v_2 = u_2 + w_2$

with $\quad u_1, u_2 \in U, \quad w_1, w_2 \in U^\perp$

thus $\quad v_1 + v_2 = (u_1 + u_2) + (w_1 + w_2)$

where $\quad u_1 + u_2 \in U, \quad w_1 + w_2 \in U^\perp$

concluding $\quad P_U(v_1 + v_2) = u_1 + u_2 = P_U v_1 + P_U v_2$

Now let $\lambda \in \mathbb{F}$ so that $\lambda v = \lambda u_1 + \lambda w_1$.

Then $\quad P_U \lambda v = \lambda u = \lambda P_U v \quad$ as desired

(b) Suppose $u \in U$. $u = u + 0$, where $u \in U$, $0 \in W^\perp$

then $P_U u = u$

(c) Suppose $w \in U^\perp$. $w = 0 + w$, where $0 \in U$, $w \in U^\perp$.

then $P_U w = 0$

(d) range $P_U = \{P_U v \mid v \in V\}$

every $v \in V$ can be written $v = u + w$, $u \in U$, $w \in W^\perp$

$\Rightarrow P_U v = u \in U$ so that range $P_U \subset U$

(b) $\Rightarrow U \subseteq$ range P_U $\rightarrow$ range $P_U = U$

(e) null $P_U = \{v \in V \mid P_U v = 0\} \subseteq U^\perp$

(c) $\Rightarrow$ $U^\perp \subseteq$ null P_U $\rightarrow$ null $P_U = U^\perp$

(f) $v = u + w$, $u \in U$, $w \in U^\perp$

$$v - P_U v = v - u = w \in W^\perp$$

(g) $P_U^2 = P_U$

$v = u + w$, $u \in U$, $w \in U^\perp$

$$P_U^2 v = P_U P_U v = P_U u = u$$

(h) $\|P_U v\|^2 = \langle P_U v, P_U v \rangle = \langle u, u \rangle = \|u\|^2$

$\|u\|^2 \leq \|u\|^2 + \|w\|^2 = \|v\|^2$

(i) Every $u \in U$ can be written as a linear combination of orthonormal basis

Minimizing the Distance to a Subspace

Suppose U is a finite-dimensional subspace of V, $v \in V$, $u \in U$.
Then
$$\|v - P_U v\| \leq \|v - u\|$$

Furthermore, the inequality above is an equality iff $u = P_U v$.

Proof

$$\begin{aligned}\|v - P_U v\|^2 &\leq \|v - P_U v\|^2 + \|P_U v - u\|^2 \\ &= \|v - P_U v + P_U v - u\|^2 \\ &= \|v - u\|^2\end{aligned}$$

Adjoint

Suppose $T \in \mathcal{L}(V,W)$. The adjoint of T is the function $T^*: W \to V$ such that
$$\langle Tv, w \rangle = \langle v, T^* w \rangle$$
$\forall v \in V, w \in W$.

Example

Define $T: \mathbb{R}^3 \to \mathbb{R}^2$ by $(x_1, x_2, x_3) \mapsto (x_2 + 3x_3, 2x_1)$.

Find a formula for $T^*: \mathbb{R}^2 \to \mathbb{R}^3$.

Fix $(y_1, y_2) \in \mathbb{R}^2$. Then for every $(x_1, x_2, x_3) \in \mathbb{R}^3$ we have

$$\begin{aligned}\langle (x_1, x_2, x_3), T^*(y_1, y_2) \rangle &= \langle T(x_1, x_2, x_3), (y_1, y_2) \rangle \\ &= \langle (x_1, x_2, x_3), (2y_2, y_1, 3y_1) \rangle\end{aligned}$$

Thus $T^*(y_1, y_2) = (2y_2, y_1, 3y_1)$

The Adjoint is a Linear Map

If $T \in \mathcal{L}(V,W)$, then $T^* \in \mathcal{L}(W,V)$.

Proof

Suppose $T \in \mathcal{L}(V,W)$, $w_1, w_2 \in W$, $\lambda_1, \lambda_2 \in \mathbb{R}$.

Then $\forall v \in V$,

$$\begin{aligned}
\langle v, T^*(\lambda_1 w_1 + \lambda_2 w_2) \rangle &= \langle Tv, \lambda_1 w_1 + \lambda_2 w_2 \rangle \\
&= \langle Tv, \lambda_1 w_1 \rangle + \langle Tv, \lambda_2, w_2 \rangle \\
&= \bar{\lambda}_1 \langle Tv, w_1 \rangle + \bar{\lambda}_2 \langle Tv, w_2 \rangle \\
&= \bar{\lambda}_1 \langle v, T^* w_1 \rangle + \bar{\lambda}_2 \langle v, T^* w_2 \rangle \\
&= \langle v, \lambda_1 T^* w_1 + \lambda_2 T^* w_2 \rangle
\end{aligned}$$

Properties of the Adjoint

(a) $(S+T)^* = S^* + T^* \quad \forall S, T \in \mathcal{L}(V,W)$

(b) $(\lambda T)^* = \bar{\lambda} T^* \quad \forall \lambda \in \mathbb{F},\ T \in \mathcal{L}(V,W)$

(c) $(T^*)^* = T \quad \forall T \in \mathcal{L}(V,W)$

(d) $I^* = I$, I is the identity operator on V

(e) $(ST)^* = T^* S^* \quad \forall T \in \mathcal{L}(V,W)$ and $S \in \mathcal{L}(W,U)$

(here, U an inner product space over $\mathbb{F}$)

Proof (all similar)

(e) For $T \in \mathcal{L}(V,W)$, $S \in \mathcal{L}(W,U)$; if $v \in V$, $u \in U$

$$\langle v, (ST)^* u \rangle = \langle (ST)v, u \rangle = \langle S[Tv], u \rangle = \langle \overset{\in U}{Tv}, S^* u \rangle = \langle v, T^* S^* u \rangle$$

Null Space and Range of T^*

Suppose $T \in \mathcal{L}(V, W)$. Then

(a) $\ker T^* = (\text{range } T)^\perp$

(b) $\text{range } T^* = (\ker T)^\perp$

(c) $\ker T = (\text{range } T^*)^\perp$

(d) $\text{range } T = (\ker T^*)^\perp$

Matrix of T^*

Suppose $\mathcal{A}$ is an orthonormal basis for V and β is an orthonormal basis for W. Then if

$$A = [T]_{\beta \leftarrow \mathcal{A}}$$

$$[T^*]_{\mathcal{A} \leftarrow \beta} = A^T \qquad \text{(conj. transpose if over } \mathbb{C}\text{)}$$

Proof

Suppose $\dim V = n < \infty$, $\dim W = m < \infty$,

so that $\mathcal{A} = (v_1, \dots, v_n)$, $\beta = (w_1, \dots, w_m)$; $\quad 1 \le j \le m$, $1 \le k \le n$

and $A = [T]_{\beta \leftarrow \mathcal{A}}$, $B = [T^*]_{\beta \leftarrow \mathcal{A}}$

Then

$$T^* w_j = \sum_{r=1}^{n} B_{r,j} v_r \qquad \forall j$$

$$T v_k = \sum_{r=1}^{m} A_{r,k} w_r \qquad \forall k$$

$$\langle v_k, T^* w_j \rangle = \langle T v_k, w_j \rangle = B_{k,j} = A_{j,k} \quad \forall j,k \rightarrow B = A^T$$

Self-Adjoint Operators

An operator $T \in \mathcal{L}(V)$ is called self-adjoint if $T = T^*$. In other words, $T \in \mathcal{L}(V)$ is self-adjoint if and only if

$$\langle Tv, w \rangle = \langle v, Tw \rangle \qquad \forall\, v, w \in \mathbb{F}$$

Eigenvalues of Self-Adjoint Operators are Real

Every eigenvalue of a self-adjoint operator is real.

Proof

$$\lambda \|v\|^2 = \langle \lambda v, v \rangle = \langle Tv, v \rangle = \langle v, Tv \rangle = \langle v, \lambda v \rangle = \bar{\lambda} \|v\|^2$$

$$\Rightarrow \lambda = \bar{\lambda} \Rightarrow \lambda \in \mathbb{R}$$

Self-adjoint Operators Have Eigenvalues

Suppose $V \neq \{0\}$ and $T \in \mathcal{L}(V)$ is a self-adjoint operator. Then T has an eigenvalue.

Self-adjoint Operators and Invariant Subspaces

Suppose $T \in \mathcal{L}(V)$ is self-adjoint and U is a subspace of V that is invariant under T. Then

(a) $U^\perp$ is invariant under T

(b) $T|_U$ is self-adjoint

(c) $T|_{U^\perp}$ is self-adjoint

Real Spectral Theorem

Suppose $\mathbb{F} = \mathbb{R}$ and $T \in \mathcal{L}(V)$. Then the following are equivalent:

(a) T is self-adjoint

(b) V has an orthonormal basis consisting of eigenvectors of T

(c) T has a diagonal matrix with respect to some orthonormal basis of V

($\exists$ orthogonal matrix Q, diagonal matrix Σ s.t. $[T] = Q \Sigma Q^T$)

Isometry

An operator $S \in \mathcal{L}(V)$ is called an isometry if

$$\|Sv\| = \|v\| \qquad \forall\ v \in V$$

Characterization of Isometries

Suppose $S \in \mathcal{L}(V)$. Then the following are equivalent:

(a) S is an isometry

(b) $\langle Su, Sv \rangle = \langle u, v \rangle \quad \forall\ u, v \in V$

(c) $Se_1, \dots, Se_n$ is orthonormal for every orthonormal list $(e_1, \dots, e_n)$

(d) $\exists (e_1, \dots, e_n)$ of V s.t. $Se_1, \dots, Se_n$ orthonormal

(e) $S^* S = I$

(f) $SS^* = I$

(g) S^* is an isometry

(h) S is invertible and $S^{-1} = S^*$

Sequence of Increasing Null Spaces

Suppose $T \in \mathcal{L}(V)$. Then

$$\{0\} = \ker T^0 \subset \ker T^1 \subset \cdots \subset \ker T^k \subset \ker T^{k+1} \subset \cdots$$

Proof

Suppose $k \in \mathbb{Z}_{\geq 1}$ and $v \in \ker T^k$. Then $T(T^k v) = T^{k+1} v = 0$

$\rightarrow v \in \ker T^{k+1} \rightarrow \ker T^k \subset \ker T^{k+1}$

Equality in the Sequence of Null Spaces

Suppose $T \in \mathcal{L}(V)$. Suppose m is a nonnegative integer such that $\ker T^m = \ker T^{m+1}$. Then

$$\ker T^m = \ker T^{m+1} = \ker T^{m+2} = \cdots$$

Proof

Let $k \in \mathbb{Z}_{\geq 1}$. Want

$$\ker T^{m+k} = \ker T^{m+k+1}$$

Know $\ker T^{m+k} \subset \ker T^{m+k+1}$

Need $\ker T^{m+k+1} \subset \ker T^{m}$

Suppose $v \in \ker T^{m+k+1}$.

$$T^{m+1}(T^k v) = T^{m+1+k} v = 0$$

$$\rightarrow T^k v \in \ker T^{m+1} = \ker T^m$$

$$\Rightarrow v \in \ker T^{m+k}$$

So $\ker T^{m+k+1} \subset \ker T^m$ as desired.

Null Spaces Stop Growing

Suppose $T \in \mathcal{L}(V)$. Let $n = \dim V$. Then

$$\ker T^n = \ker T^{n+1} = \ker T^{n+2} = \ker T^{n+3} = \cdots$$

Proof

Only need $\ker T^n = \ker T^{n+1}$.

Suppose $\ker T^n \neq \ker T^{n+1}$.

Then $\{0\} = \ker T^0 \subsetneq \ker T \subsetneq \subsetneq \cdots \subsetneq \ker T^n \subsetneq \ker T^{n+1}$.

At each strict inclusion, dim ker increases by at least one. This give $\dim \ker T^{n+1} \geq n+1$. !

V is the Direct Sum of $\ker T^{\dim V}$ and $\operatorname{im} T^{\dim V}$

Suppose $T \in \mathcal{L}(V)$. Let $n = \dim V$. Then

$$V = \ker T^n \oplus \operatorname{im} T^n .$$

Proof

First show $\ker T^n \cap \operatorname{im} T^n = \{0\}$

Suppose $v \in \ker T^n \cap \operatorname{im} T^n$

then $T^n v = 0$ and $\exists u \in V$ s.t. $T^n v = u$

Applying T^n, $T^{2n} v = T^n u$

$T^{2n} = T^n \rightarrow T^{2n} v = 0 \rightarrow T^n u = 0 \rightarrow v = 0$

$\Rightarrow$ direct sum

Generalized Eigenvector

Suppose $T \in \mathcal{L}(V)$ and λ an eigenvalue of T. A vector $v \in V$ is called a **generalized** eigenvector of T corresponding to λ if $v \neq 0$ and

$$(T - \lambda I)^j v = 0$$

for some positive integer j.

Generalized Eigenspace

Suppose $T \in \mathcal{L}(V)$ and $\lambda \in \mathbb{F}$. The **generalized** eigenspace of T corresponding to λ, denoted $G(\lambda, T)$, is defined to be the set of all generalized eigenvectors of T corresponding to λ, along with the zero vector.

Note: $E(\lambda, T) \subset G(\lambda, T)$

Description of Generalized Eigenspaces

Suppose $T \in \mathcal{L}(V)$ and $\lambda \in \mathbb{F}$. Then $G(\lambda, T) = \ker(T - \lambda I)^{\dim V}$

Proof

Suppose $v \in \ker(T - \lambda I)^{\dim V}$. Then $v \in G(\lambda, T) \Rightarrow \ker(T - \lambda I)^{\dim V} \subset G(\lambda, T)$

Conversely, suppose $v \in G(\lambda, T)$. Then $\exists\ j \in \mathbb{Z}_+$ s.t.

$$v \in \ker(T - \lambda I)^j \subset \ker(T - \lambda I)^{\dim V}$$

$$\Rightarrow G(\lambda, T) \subset \ker(T - \lambda I)^{\dim V}$$

Nilpotent

An operator is called **nilpotent** if some power of it equals 0.

Nilpotent Operator Raised to Dimension of Domain is 0

Suppose $N \in \mathcal{L}(V)$ is nilpotent. Then $N^{\dim V} = 0$.

Proof

Because N is nilpotent, $G(0, N) = V$.

Then $\ker N^{\dim V} = V$

Matrix of a Nilpotent Operator

Suppose N is a nilpotent operator on V. Then there is a basis of V with respect to which the matrix N has the form

$$\begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$$

The Null Space and Range of p(T) are Invariant Under T

Suppose $T \in \mathcal{L}(V)$ and $p \in \mathcal{P}(\mathbb{F})$. Then $\ker p(T)$ and range $p(T)$ are invariant under T.

Description of Operators on Complex Vector Spaces

Suppose V is a complex vector space and $T \in \mathcal{L}(V)$. Let $\lambda_1, \ldots, \lambda_m$ be the distinct eigenvalues of T. Then

(a) $V = G(\lambda_1, T) \oplus \cdots \oplus G(\lambda_m, T)$

(b) each $G(\lambda_j, T)$ in invariant under T

(c) each $(T - \lambda_j I)|_{G(\lambda_j, T)}$ is nilpotent

A Basis of Generalized Eigenvectors

Suppose V is a complex vector space and $T \in \mathcal{L}(V)$. Then there is a basis of V consisting of generalized eigenvectors of T.

Multiplicity

Suppose $T \in \mathcal{L}(V)$. The multiplicity of an eigenvalue λ of T is defined to be the dimension of the corresponding generalized eigenspace $G(\lambda, T)$.

Sum of Multiplicities Equals dim V

Suppose V is a complex vector space and $T \in \mathcal{L}(V)$. Then the sum of all the eigenvalues of T equals $\dim V$.

Note: Geometric Multiplicity $= \dim E(\lambda, T)$

Algebraic Multiplicity $= \dim G(\lambda, T)$

Block Diagonal Matrix

A block diagonal matrix is a square matrix of the form

$$\begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix}$$

where $A_1, \dots, A_m$ are square matrices lying along the diagonal and all other entries of the matrix equal 0.

Block Diagonal Matrix With Upper Triangular Blocks

Suppose V is a complex vector space and $T \in \mathcal{L}(V)$. Let $\lambda_1, \dots, \lambda_m$ be the distinct eigenvalues of T, with multiplictities $d_1, \dots, d_m$. Then there is a basis of V with respect to which T has a block diagonal matrix of the form

$$\begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_m \end{pmatrix}$$

where each A_i is the $d_i \times d_i$ upper triangular matrix of the form

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_m \end{pmatrix}$$

Characteristic Polynomial

Suppose V is a complex vector space and $T \in \mathcal{L}(V)$. Let $\lambda_1, \ldots, \lambda_m$ denote the distinct eigenvalues of T, with multiplicities $d_1, \ldots, d_m$. The polynomial

$$(z-\lambda_1)^{d_1} \cdots (z-\lambda_m)^{d_m}$$

is called the **characteristic polynomial** of T.

Degrees and Zeros of Characteristic Polynomial

Suppose V is a complex vector space and $T \in \mathcal{L}(V)$. Then

(a) the characteristic polynomial of T has degree $\dim V$

(b) the zeros of the characteristic polynomial of T are the eigenvalues of T

Proof

Follows from $\sum d_i = \dim V$

Cayley Hamilton Theorem

Suppose V is a complex vector space and $T \in \mathcal{L}(V)$. Let q denote the characteristic polynomial of T. Then

$$q(T) = 0$$

Proof

Let $\lambda_1, \ldots, \lambda_m$ be the distinct eigenvalues of T with $d_1, \ldots, d_m$ algebraic multiplicity each

For each $j \in \{1, \ldots, m\}$ we have $(T - \lambda_j I)|_{G(\lambda_j, T)}$ is nilpotent.

Thus

$$(T - \lambda_j I)^{d_j}|_{G(\lambda_j, T)} = 0$$

Every $v \in V$ can be written as

$$v = g_1 + \cdots + g_m \quad ; \quad g_j \in G(\lambda_j, T)$$

Suffices to show

$$q(T)|_{G(\lambda_j, T)} = 0 \quad \forall j$$

Fix $j \in \{1, \ldots, m\}$. Then

$$q(T) = (T - \lambda_1 I)^{d_1} \cdots (T - \lambda_m I)^{d_m}$$

All operators on left-hand side commute.

Thus can rearrange to

$$q(T) = (T - \lambda_1 I) \cdots (T - \lambda_m I)^{d_m} (T - \lambda_j I)^{d_j}$$

Since

$$(T - \lambda_j I)|_{G(\lambda_j, T)} = 0 \quad \forall j$$

then

$$q(T)|_{G(\lambda_j, T)} = 0 \quad \forall j$$

as desired.

Monic Polynomial

A monic polynomial is a polynomial whose highest-degree coefficient equals 1.

Minimal Polynomial

Suppose $T \in \mathcal{L}(V)$. Then $\exists$ a unique monic polynomial p of smallest degree such that $p(T) = 0$.

Proof

Let $n = \dim V$ (existence)

Then the list

$$I, T, T^2, \ldots, T^{n^2} \qquad \{n+1 \text{ elements}\}$$

is **NOT** linearly independent in $\mathcal{L}(V)$ since $\dim \mathcal{L}(V) = n^2$.

Let m be the smallest integer such that

$$I, T, T^2, \ldots, T^m$$

is linearly **dependent**.

Then T^m is a linear combination of $I, \ldots, T^{m-1}$ by how we chose m.

Thus $\exists\, a_0, a_1, \ldots, a_{m-1} \in \mathbb{F}$ such that

$$a_0 I + a_1 T + \cdots + a_{m-1} T^{m-1} + T^m = 0$$

Define $p \in \mathcal{P}(\mathbb{F})$ as

$$a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} + z^m.$$

Then $p(T) = 0$ is implied by construction.

(uniqueness)

Choice of m gives that no monic polynomial $q \in \mathcal{P}(\mathbb{F})$ with degree $< m$ satisfies $q(T) = 0$.

Suppose now $q \in \mathcal{P}(\mathbb{F})$ has degree m and $q(T) = 0$.

Then

$$(p-q)T = 0$$

and

$$\deg (p-q) < m.$$

Choice of $m \Rightarrow q = p$.

Q.E.D

Minimal Polynomial

Suppose $T \in \mathcal{L}(V)$. Then the minimal polynomial of T is the unique monic polynomial p of smallest degree such that $p(T) = 0$.

Note: has at MOST degree $\dim V$

$q(T) = 0 \Rightarrow q$ is a Multiple of Minimal Polynomial

Suppose $T \in \mathcal{L}(V)$ and $q \in \mathcal{P}(\mathbb{F})$. Then $q(T) = 0$ if and only if q is a polynomial multiple of the minimal polynomial of T.

Proof

Let p denote the minimal polynomial of T.

($\Leftarrow$) Suppose q is a polynomial multiple of p.

Then $\exists\, s \in \mathcal{P}(\mathbb{F})$ such that

$$q = ps$$

We have

$$q(T) = p(T)s(T) = 0\,s(T) = 0$$

($\Rightarrow$) Suppose $q(T) = 0$.

By the division algorithm, $\exists\, s, r \in \mathcal{P}(\mathbb{F})$ such that

$$q = ps + r$$

and $\deg r < \deg p$.

We have

$$q(T) = p(T)s(T) + r(T) = 0$$

Suppose $r(T) \neq 0$. Then dividing $r(T)$ by its highest degree coefficient would produce a monic polynomial that when applied to T equals zero.

This polynomial would have a smaller degree then the minimal polynomial !C

Thus,

$$r(T) = 0$$

and $q(T)$ is a polynomial multiple of $p(T)$.

Characteristic Polynomial is a Multiple of Minimal Polynomial

Eigenvalues are the Zeros of the Minimal Polynomial

Let $T \in \mathcal{L}(V)$. Then the zeros of the minimal polynomial of T are precisely the eigenvalues of T.

Proof

Let

$$p(z) = a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} + z^m$$

be the minimal polynomial of T.

Suppose λ is a zero of p. Then

$$p(z) = (z - \lambda) q(z)$$

where q is a monic polynomial with coefficients in $\mathbb{F}$ and $\deg q = \deg p - 1$. Since $p(T) = 0$, we have

$$0 = (T - \lambda I)(q(T)v)$$

Then $\exists\ v \in V$ such that $q(T)v \neq 0$, and

$$T(q(T)v) = \lambda(q(T)v)$$

This gives λ is an eigenvalue of T.

Suppose now $\lambda \in \mathbb{F}$ is an eigenvalue of T. Then $\exists\ v \neq 0 \in V$ such that

$$Tv = \lambda v.$$

Applying T to both sides repeatedly gives

$$T^j v = \lambda^j v \qquad j = 1, 2, \ldots$$

Thus

$$
\begin{aligned}
0 = p(T)v &= (a_0 I + a_1 T + \cdots + a_{m-1} T^{m-1} + T^m)v \\
&= (a_0 + a_1 \lambda + \cdots + a_{m-1} \lambda^{m-1} + \lambda^m)v \\
&= p(\lambda)v \Rightarrow p(\lambda) = 0
\end{aligned}
$$

Q.E.D