


Lecture 15

Diagonalization criterion and minimal polynomial

Notation $p(t)$ polynomial over F
$$p(t) = a_n t^n + \dots + a_1 t + a_0, \quad a_i \in F$$

• $A \in M_n(F)$, we define:

$$p(A) = a_n A^n + \dots + a_1 A + a_0 \text{Id} \in M_n(F)$$

• $\alpha \in L(V)$, we define:

$$p(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0 \text{Id}$$
$$\alpha^{\vec{i}} = \underbrace{\alpha \dots \alpha}_i \in L(V),$$

Thm (Sharp criterion of diagonalizability)

• V vector space over F , $\dim V < +\infty$

• $\alpha \in L(V)$

Then α is diagonalizable

$\Leftrightarrow \exists$ a polynomial p which is the product of distinct linear factors such that $p(\alpha) = 0$.

$$\alpha \text{ diag} \Leftrightarrow \exists (\lambda_1, \dots, \lambda_e) \text{ distinct} /$$
$$\left| \begin{array}{l} p(t) = \prod_{i=1}^e (t - \lambda_i) \\ p(\alpha) = 0. \end{array} \right.$$

proof $\Rightarrow$) Suppose that α is diagonalizable, with distinct eigenvalues $\lambda_1, \dots, \lambda_e$. Let

$$p(t) = \prod_{i=1}^e (t - \lambda_i)$$

Let $v \in B$

$B =$ basis of V formed of eigenvectors.

Then $v \in \mathcal{B}$, $\alpha(v) = \lambda_i v$ for some i

$$\Rightarrow (\alpha - \lambda_i \text{Id}) v = 0$$

$$\Rightarrow p(\alpha) = \left[\prod_{i=1}^k (\alpha - \lambda_i \text{Id}) \right] v = 0.$$

These terms commute

$$\begin{aligned} & (\alpha - \lambda_i \text{Id}) (\alpha - \lambda_j \text{Id}) \\ &= (\alpha - \lambda_j \text{Id}) (\alpha - \lambda_i \text{Id}) \end{aligned}$$

$$\Rightarrow \forall v \in \mathcal{B} \quad p(\alpha)(v) = 0$$

$$\Rightarrow p(\alpha) = 0.$$

$\Leftarrow$ Suppose $p(\alpha) = 0$ for some:

$$p(t) = \prod_{i=1}^k (t - \lambda_i)$$

$$\lambda_i \neq \lambda_j, \quad i \neq j.$$

$$\text{let } V_{\lambda_i} = \text{Ker} (\alpha - \lambda_i \text{Id}),$$

We claim:

$$V = \bigoplus_{i=1}^k V_{\lambda_i} \quad (*)$$



Indeed let : $q_j(t) = \prod_{\substack{i=1 \\ i \neq j}}^k \frac{(t - \lambda_i)}{(\lambda_j - \lambda_i)} \quad , \quad 1 \leq j \leq k$

Then : $q_j(\lambda_i) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$

$$q(t) = q_1(t) + \dots + q_k(t)$$

Then $q(t)$ has degree at most $(k-1)$ and :

$$q(\lambda_i) = 1 \quad \text{for } 1 \leq i \leq k$$

$$\Rightarrow \forall t, \quad q(t) = 1.$$

$$\Rightarrow q_1(t) + \dots + q_k(t) = 1 \quad \forall t.$$

let : $\pi_j = q_j(\alpha) \quad (*)$ $\in L(V)$.

By construction, $\sum_{j=1}^k \pi_j(\alpha) = q(\alpha) = \text{Id}.$

This means: $\forall v \in V, \quad e$

$$v = q(\alpha)(v) = \sum_{j=1}^e \pi_j(v) = \sum_{j=1}^e q_j(\alpha)(v)$$

Observe

$$(\alpha - \lambda_j \text{Id}) q_j(\alpha)(v)$$

$\uparrow$
(*)

$$= \frac{1}{\prod_{i \neq j} (\lambda_j - \lambda_i)} p(\alpha)(v) = 0$$

$$\Rightarrow \forall j \in \{1, \dots, e\}, \quad \pi_j(v) \in V_{\lambda_j}$$

$$\Rightarrow V = \sum_{j=1}^e V_{\lambda_j} \quad (*)$$

. It remains to prove that the sum is direct.

Indeed, let: $v \in V_{\lambda_j} \cap \left(\sum_{i \neq j} V_{\lambda_i} \right)$

Let's apply π_j to $\sigma \in V_{\lambda_j} \cap \left(\sum_{i \neq j} V_{\lambda_i} \right)$

$$\cdot \sigma \in V_{\lambda_j} \Rightarrow \pi_j(\sigma) = \left(\prod_{i \neq j} \left(\frac{\lambda_j - \lambda_i}{\lambda_j - \lambda_i} \right) \right) \sigma = \sigma$$

$$\cdot \sigma \in \sum_{i \neq j} V_{\lambda_i} \quad \left| \quad \begin{array}{l} \omega \in V_{\lambda_i}, \quad i \neq j \\ \Rightarrow \pi_j(\omega) = 0. \end{array} \right.$$

$$\Rightarrow \pi_j(\sigma) = 0.$$

This implies: $\sigma = \pi_j(\sigma) = 0$

$\Rightarrow$ the num is direct.

$\Rightarrow \sigma$ is diagonalizable.

0.

Remark We have shown the following: if $\lambda_1, \dots, \lambda_k$ are k distinct eigenvalues of α ,

then the num:

$$\sum_{i=1}^k V_{\lambda_i} = \bigoplus_{i=1}^k V_{\lambda_i}$$

always true. The only way diagonalization fails
is if $\sum_{j=1}^n V_{\lambda_j} \leq V$.

Ex If $A \in M_n(F)$ has finite order
($\equiv (A^m = \text{Id for some } m \in \mathbb{N})$)

Then A is diagonalizable.

proof
$$t^m - 1 = \prod_{j=0}^{m-1} (t - \zeta_m^j)$$

$$\zeta_m = e^{\frac{2\pi i}{m}}$$

Thm (Simultaneous diagonalization)

Let $\alpha, \beta \in L(V)$ diagonalizable. Then
 α, β are simultaneously diagonalizable
(i.e. there exist a basis in which both

matrices are diagonal) iff α and β commute.

proof $\Rightarrow$ $\exists B, \begin{cases} [\alpha]_B = D_1 \\ [\beta]_B = D_2 \end{cases}$

D_1, D_2 diagonal, then $D_1 D_2 = D_2 D_1$
 $\Rightarrow \alpha\beta = \beta\alpha$

$\Leftarrow$ Suppose α, β diagonalizable and commute.
 $V = V_{\lambda_1} \oplus \dots \oplus V_{\lambda_k}$
 $\lambda_1, \dots, \lambda_k$ = k distinct eigenvalues of α

claim $\beta(V_{\lambda_j}) \subseteq V_{\lambda_j}$.

Indeed, let $v \in V_{\lambda_j}$. Then:

$$\alpha\beta(v) = \beta\alpha(v) = \beta(\lambda_j v) = \lambda_j \beta(v)$$

$$\Rightarrow \beta(v) \in V_{\lambda_j}.$$

Since β is diagonalizable, $\exists$ p w distinct linear factors such that $p(\beta) = 0$.

$$\underline{\text{Now}} \quad p(\beta|_{V_{\lambda_i}}) = p(\beta|_{V_{\lambda_i}}) = 0$$

$$\Rightarrow \boxed{\beta|_{V_{\lambda_i}}} \in L(V_{\lambda_i}) \text{ diagonalizable.}$$

I take B_i basis of V_{λ_i} in which $\beta|_{V_{\lambda_i}}$ is diagonalizable. Since the sum is direct, $(\underbrace{B_1}_{V_{\lambda_1}}, \dots, \underbrace{B_r}_{V_{\lambda_r}}) \equiv \text{basis of } V$

in which β is diagonal, and so is α . □

Minimal polynomial

Remainder (Group - Ring - Modulus)

• Euclidean algorithm for polynomials: given a, b polynomials over F with $b \neq 0$, there exist polynomials q, r over F with:

$$\deg r < \deg b \quad \text{and:}$$

$$a = qb + r$$

 remainder.

Def (Minimal polynomial)

V F vector space, $\alpha \in L(V)$, $\dim V < +\infty$.

The minimal polynomial m_α of α is the non zero polynomial with smallest degree

such that: $m_\alpha(\alpha) = 0$.

Pr $\dim_F V = n < +\infty$, $\alpha \in L(V)$,

$\dim_F L(V) = n^2$, Hence:

$\{1, \alpha, \alpha^2, \dots, \alpha^{n^2}\}$ are linearly dependent,

$\Rightarrow$:

$n^2 + 1$ terms

$$\begin{cases} a_{n^2} \alpha^{n^2} + \dots + a_1 \alpha + a_0 = 0 \\ (a_{n^2}, \dots, a_0) \neq (0, \dots, 0) \end{cases}$$

Lemma $\alpha \in L(V)$, $p \in F[t]$.

Then: $p(\alpha) = 0$ iff m_α is a factor of p .

(in particular, m_α is well defined)

proof

$$p \in F[t] \quad / \quad p(\alpha) = 0$$

$$m_\alpha, \quad m_\alpha(\alpha) = 0, \quad \deg m_\alpha \leq \deg p$$

By Euclidean division:

$$p = m_\alpha q + r$$
$$\boxed{\deg r < \deg m_\alpha}$$

$$\text{Then: } p(\alpha) = 0 = \underbrace{m_\alpha(\alpha)}_0 q(\alpha) + r(\alpha)$$

$$\Rightarrow r(\alpha) = 0$$

$$\Rightarrow r = 0$$



minimality of m_α
in terms of degree

. If m_1, m_2 both minimal, then
 m_1 divides m_2 and m_2 divides m_1

$$\Rightarrow m_1 = c m_2, \quad c \in F.$$

Ex $V = \mathbb{F}^2$, $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$\cdot p(t) = (t-1)^2$, $p(A) = p(B) = 0$

$\cdot$ min polynomial is either $(t-1)^2$ or $(t-1)$.

char $\begin{cases} m_A = t-1 \\ m_B = (t-1)^2 \end{cases}$ ↗

$\Rightarrow$ A diagonalizable

$\mid$ B is not diagonalizable.