Review

在學期開始我們先複習上學期的重要內容, 以便我們繼續下學期的課程. 在這個複習單元中我們只是列出以後需要的定義與定理內容, 並不會有任何的證明. 至於證明細節請參考上學其講義的 Chapter 3, Chapter 4A.

1. Linear Operator

當 V 是一個 vector space 時, 從 V 到 V 的 linear transformation, 就稱為是一個 *linear operator* on V. 當 $T:V\to V$ 是一個 linear operator 時, 我們很自然的可以考慮其合成 $T^{\circ 2}=T\circ T$, 以及 $T^{\circ 3}=T\circ T^{\circ 2},\ldots$ 這樣一直下去對任意 $i\in\mathbb{N}$ 都可以定出 $T^{\circ i}=T\circ T^{\circ i-1}$ $(T^{\circ 0}=\mathrm{id})$. 如此一來賦予 V 一個很豐富的代數結構 (稱為 $F[T]$-module), 所以我們可以進一步去了解 T 和 V 的關係.

一個 linear operator 由於定義域和對映域是同一個 vector space, 我們可以選相同的 ordered basis, 這會讓矩陣表示法變得較簡單. 也就是說若 $T:V\to V$ 是一個 linear operator, 要得到 T 的 representative matrix, 我們可以選定 V 的一個 ordered basis $\beta=(\mathbf{v}_1,\ldots,\mathbf{v}_n)$, 兩邊都用 β, 得 ${}_\beta[T]_\beta$ 這一個 $n\times n$ matrix. 為了方便起見當兩邊選的 ordered basis 相同時, T 的 representative matrix, 我們就會用 $[T]_\beta$ 來表示, 也就是說

$$[T]_\beta=\big(\tau_\beta(T(\mathbf{v}_1)),\ldots,\tau_\beta(T(\mathbf{v}_n))\big).$$

例如若 T_1,T_2 皆為 V 的 linear operator 我們知

$$[T_2\circ T_1]_\beta=[T_2]_\beta\cdot[T_1]_\beta.$$

另外依此表法, 我們有 $[\mathrm{id}]_\beta=I_n$.

對同一個 linear operator 若換另外的一個 ordered basis 來處理, 它的 representative matrix 就可能不一樣了, 我們需了解這樣的 matrices 之間有何關係, 就得靠 ${}_{\beta'}[\mathrm{id}]_\beta$ 這樣的 change of basis matrix 來幫忙了. 我們有以下之結果.

Lemma . 設 β,β' 為 V 的 *ordered bases,* $T:V\to V$ 為 *linear operator,* 則

$$[T]_{\beta'}={}_\beta[\mathrm{id}]_{\beta'}^{-1}\cdot[T]_\beta\cdot{}_\beta[\mathrm{id}]_{\beta'}.$$

當 $A,B\in M_n(F)$, 而 P 為 $M_n(F)$ 中的 invertible matrix, 若 $B=P^{-1}\cdot A\cdot P$, 則稱 A,B 為 *similar matrix*, 用 $A\sim B$ 來表示. 此時因 $\det(P^{-1})=\det(P)^{-1}$ 知

$$\det(B)=\det(P^{-1}\cdot A\cdot P)=\det(P^{-1})\det(A)\det(P)=\det(A).$$

由上一個 Lemma 我們知道 $[T]_\beta\sim[T]_{\beta'}$, 故得 $\det([T]_\beta)=\det([T]_{\beta'})$. 也就是說不管用哪一個 ordered basis, T 的 representative matrix 的 determinant 皆相同, 我們也因此定義這就是 T 的 determinant, 也就是說 $\det(T)=\det([T]_\beta)$.

上一個 Lemma 反過來是對嗎? 有就是說若 $A\sim[T]_\beta$, 是否可找到 V 的一個 ordered basis β' 使得 $A=[T]_{\beta'}$ 呢? 事實上, 若 P 是一個 invertible matrix 使得 $A=P^{-1}\cdot[T]_\beta\cdot P$, 則我們能找到 V 的一個 ordered basis β' 滿足 $P={}_\beta[\mathrm{id}]_{\beta'}$, 故知

$$A=P^{-1}\cdot[T]_\beta\cdot P={}_\beta[\mathrm{id}]_{\beta'}^{-1}\cdot[T]_\beta\cdot{}_\beta[\mathrm{id}]_{\beta'}=[T]_{\beta'}.$$

因此我們有以下之結論.

Proposition . 假設 V 為 *finite dimensional vector space,* $\dim(V)=n$ 且 β 為 V 的一個 *ordered basis.* 設 $T:V\to V$ 為 *linear operator* 且 $A\in M_n(F)$, 則 $A\sim[T]_\beta$ 若且唯若存在 V 的一個 *ordered basis* β' 使得 $A=[T]_{\beta'}$.

2. Characteristic Polynomial

前面提過一個 linear operator 的問題, 我們可以轉化成有關於 square matrix 的問題, 所以我們會先探討一般 $n\times n$ matrix, 然後再將之轉化成 linear operator 的情形.

給定一個係數在 F 的 polynomial $f(x)=c_dx^d+\cdots+c_1x+c_0$ 以及一個 $n\times n$ matrix A, 我們定義

$$f(A)=c_dA^d+\cdots+c_1A+c_0I_n.$$

很明顯的, $f(A)$ 仍然是一個 $n\times n$ matrix. 一般來說矩陣相乘是不可交換的, 不過 A^i 和 $f(A)$ 相乘是可以交換的. 事實上

$$\begin{aligned}A^i\cdot f(A)&=A^i\cdot(c_dA^d+\cdots+c_1A+c_0I_n)\\&=c_dA^{d+i}+\cdots+c_1A^{1+i}+c_0A^i=(c_dA^d+\cdots+c_1A+c_0I_n)\cdot A^i=f(A)\cdot A^i.\end{aligned}$$

因此加上利用矩陣加法乘法的分配律, 我們可以得到以下的結果.

Lemma . 假設 $f(x),g(x),h(x)\in F[x]$ 且 $f(x)=g(x)h(x)$. 若 $A\in M_n(F)$, 則

$$g(A)\cdot h(A)=h(A)\cdot g(A)=f(A).$$

再次強調這裡都是和 A 相關的矩陣相乘才會成立, 一般來說若 $g(x),h(x)\in F[x]$ 以及 $A,B\in M_n(F)$, 不一定會有 $g(A)\cdot h(B)=h(B)\cdot g(A)$.

接下來我們有興趣的是若 $A\sim B$, 是否 $f(A)\sim f(B)$ 呢? 首先觀察若 P 為 invertible, 則

$$(P^{-1}\cdot A\cdot P)^2=(P^{-1}\cdot A\cdot P)\cdot(P^{-1}\cdot A\cdot P)=P^{-1}\cdot A^2\cdot P.$$

利用數學歸納法可得

$$(P^{-1}\cdot A\cdot P)^i=P^{-1}\cdot A^i\cdot P.$$

我們有以下結果.

Lemma . 假設 $f(x)\in F[x]$ 且 $A,B\in M_n(F)$. 若 $A\sim B$, 則 $f(A)\sim f(B)$.

我們也可把這概念推廣到 linear operator, 假設 $f(x)=c_dx^d+\cdots+c_1x+c_0\in F[x]$ 以及 $T:V\to V$ 是一個 linear operator, 由於 linear operators 之間的合成和矩陣之間的相乘相對應, 我們定義

$$f(T)=c_dT^{\circ d}+\cdots+c_1T+c_0\,\mathrm{id},$$

很明顯的 $f(T)$ 仍然是 V 到 V 的 linear operator. 我們可以檢查 $T^{\circ i}\circ f(T)=f(T)\circ T^{\circ i}$, 所以一樣有以下結果.

Lemma . 假設 $f(x), g(x), h(x) \in F[x]$ 且 $f(x) = g(x) \cdot h(x)$. 若 $T \in \mathscr{L}(V)$, 則

$$g(T) \circ h(T) = h(T) \circ g(T) = f(T).$$

這裡要強調一下當 $f(x) = g(x) \cdot h(x)$ 時 $f(T) = g(T) \circ h(T)$ 而不是等於 $g(h(T))$. 也就是說將 $g(T)$ 和 $h(T)$ 這兩個 linear operator 合成會得到 $f(T)$ 這個 operator, 但並不是將 $h(T)$ 這個 linear operator 代入 $g(x)$ 這個多項式.

給定 V 的一個 ordered basis β 我們自然要問 $F(T)$ 的 representative matrix 是否和 T 的 representative matrix 有關. 事實上我們有 $[T^{\circ 2}]_\beta = [T]_\beta^2$, 利用數學歸納法可得

$$[T^{\circ i}]_\beta = [T \circ T^{\circ i-1}]_\beta = [T]_\beta \cdot [T]_\beta^{i-1} = [T]_\beta^i,$$

由此我們有以下之結果.

Lemma . 假設 V 是一個 *finite dimensional F-space,* β 為 V 的一個 *ordered basis* 且 $T : V \to V$ 是一個 *linear operator.* 若 $f(x) = c_d x^d + \cdots + c_1 x + c_0 \in F[x]$, 則

$$[f(T)]_\beta = f([T]_\beta) = c_d\,[T]_\beta^d + \cdots + c_1\,[T]_\beta + c_0 I_n.$$

現在回到 $n \times n$ matrix 的情形. 我們知 $\dim(M_n(F)) = n^2$, 現若 $A \in M_n(F)$, 考慮 $S = \{I_n, A, A^2, \ldots, A^{n^2}\}$. 由於 $\#(S) = n^2 + 1 > \dim(M_n(F))$, 我們知 S 為 linearly dependent. 亦即存在 $c_0, c_1, \ldots, c_{n^2} \in F$ 不全為 0 使得

$$c_{n^2} A^{n^2} + \cdots + c_1 A + c_0 I_n = \mathbf{O}.$$

若令 $f(x) = c_{n^2} x^{n^2} + \cdots + c_1 x + c_0$, 則得 $f(A) = \mathbf{O}$. 因此我們可以說: 對任意的 $n \times n$ matrix A, 皆存在一個次數不大於 n^2 的非零多項式 $f(x) \in F[x]$ 使得 $f(A)$ 為 $n \times n$ 的 zero matrix $\mathbf{O}$. 注意這裡 c_{n^2} 有可能是 0 所以我們不能說 $\deg(f(x)) = n^2$, 另外 $c_{n^2}, \ldots, c_1, c_0$ 不全為 0, 所以 $f(x)$ 不是零多項式.

事實上我們可以找到次數為 n 的多項式 $f(x)$ 使得 $f(A) = \mathbf{O}$, 就是所謂的 characteristic polynomial.

Definition . 假設 $A \in M_n(F)$, 考慮 $\chi_A(x) = \det(xI_n - A) \in F[x]$, 稱為 A 的 *characteristic polynomial.*

注意有的書定義 $\det(A - xI_n)$ 為 A 的 characteristic polynomial, 我們用 $\det(xI_n - A)$ 主要是讓 $\chi_A(x)$ 是一個 monic polynomial (最高次項係數為 1). 利用降階求 determinant 的方法以及數學歸納法, 我們可以知當 A 為 $n \times n$ matrix 時, $\chi_A(x)$ 的次數為 n 且最高次項係數為 1. 也可更進一步得到 $\chi_A(x)$ 的次高項 (即 x^{n-1} 項) 係數為 $-\mathrm{tr}(A)$ (註: $\mathrm{tr}(A)$ 為 A 的 trace, 即對角線之和). 另外將 $x = 0$ 代入 $\chi_A(x)$ 可得 $\chi_A(x)$ 的常數項為 $\chi_A(0) = \det(-A) = (-1)^n \det(A)$.

接下來我們來看看 similar matrices 它們的 characteristic polynomial 有什麼關係.

Proposition . 若 $A, B \in M_n(F)$ 且 $A \sim B$, 則 $\chi_A(x) = \chi_B(x)$.

特別的, 當 $T : V \to V$ 是一個 linear operator, β, β' 為 V 的 ordered bases, 由於 $[T]_\beta \sim [T]_{\beta'}$, 上一個 Proposition 告訴我們 $\chi_{[T]_\beta}(x) = \chi_{[T]_{\beta'}}(x)$. 因此我們可以定義 linear operator 的 characteristic polynomial.

Definition . 假設 V 為 *finite dimensional F-space.* 對於 V 的 *linear operator* $T: V \to V$, 任取 V 的一個 *ordered basis* β, 定義 T 的 *characteristic polynomial* 為 $\chi_{[T]_\beta}(x)$, 且以 $\chi_T(x)$ 來表示.

有關於一個方陣的 characteristic polynomial 最重要性質就是以下的定理.

Theorem (Cayley-Hamilton Theorem)**.** 若 $A \in M_n(F)$, $\chi_A(x)$ 為 A 的 *characteristic polynomial,* 則 $\chi_A(A) = \mathbf{O}$.

當 β 為 V 的一個 ordered basis, $T: V \to V$ 為 linear operator, 我們定義 $\chi_T(x) = \chi_{[T]_\beta}(x)$. 此時 $\chi_T(T)$ 為 linear operator, 其對 β 的 representative matrix 為

$$[\chi_{[T]_\beta}(T)]_\beta = \chi_{[T]_\beta}([T]_\beta).$$

故知 $[\chi_T(T)]_\beta = \mathbf{O}$, 因此得 $\chi_T(T) = \mathbf{O}$. 這就是 linear operator 版本的 Cayley-Hamilton Theorem.

Corollary (Cayley-Hamilton Theorem)**.** 若 V 為 *finite dimensional F-space,* $T: V \to V$ 為 *linear operator,* 則 $\chi_T(T) = \mathbf{O}$.

3. Minimal Polynomial

若 A 是 $n \times n$ matrix, 利用 A 的 characteristic polynomial, 我們知道存在次數為 n 的多項式 $f(X) \in F[x]$ 使得 $f(A) = \mathbf{O}$. 會不會有次數更小的多項式可以達到這個目的呢? 這是有可能的, 例如 $A = I_n$ 時, $\chi_{I_n}(x) = (x-1)^n$, 但考慮 $f(x) = x - 1$, 我們有 $f(I_n) = I_n - I_n = \mathbf{O}$. 所以我們想要找到次數最小的非零多項式 $f(X) \in F[x]$ 使得 $f(A) = \mathbf{O}$.

Definition . 設 $A \in M_n(F)$, 在所有非零多項式 $f(x) \in F[x]$ 中滿足 $f(A) = \mathbf{O}$, 且次數最小的 *monic polynomial (*即最高次項係數為 1*)* 稱為 A 的 minimal polynomial, 用 $\mu_A(x)$ 來表示.

我們知道一定存在次數最小的非零多項式 $f(x) \in F[x]$ 使得 $f(A) = \mathbf{O}$, 而這裡要求 monic 就是要求唯一性. 事實上若 $f(x), g(x) \in F[x]$ 為次數最小的非零 monic polynomial 使得 $f(A) = g(A) = \mathbf{O}$, 因皆為次數最小故必有 $\deg(f) = \deg(g)$, 又要求 $f(x), g(x)$ 為 monic, 故知 $\deg(f(x) - g(x)) < \deg(f(x))$. 但此時 $f(A) - g(A) = \mathbf{O} - \mathbf{O} = \mathbf{O}$, 故由次數最小的要求知 $f(x) - g(x)$ 必為零多項式, 即 $f(x) = g(x)$, 所以 minimal polynomial $\mu_A(x)$ 是唯一的.

接下來我們要問若 $A \sim B$, 那麼它們的 minimal polynomial $\mu_A(x), \mu_B(x)$ 是否相等. 首先來看一個 minimal polynomial 最基本的性質.

Lemma . 假設 $A \in M_n(F)$ 且 $f(x) \in F[x]$. 則 $f(A) = \mathbf{O}$ 若且唯若 $\mu_A(x) \mid f(x)$.

現若 $A \sim B$, 知 $\mu_A(B) \sim \mu_A(A) = \mathbf{O}$, 然而和零矩陣 similar 的矩陣必為零矩陣 (因對任意 invertible matrix P, $P^{-1} \cdot \mathbf{O} \cdot P = \mathbf{O}$), 故得 $\mu_A(B) = \mathbf{O}$. 由前一個 Lemma 知 $\mu_B(x) \mid \mu_A(x)$. 同理利用 $\mu_B(A) \sim \mu_B(B) = \mathbf{O}$, 得 $\mu_A(x) \mid \mu_B(x)$. 然而 $\mu_A(x), \mu_B(x)$ 皆為 monic, 故得 $\mu_A(x) = \mu_B(x)$. 證得以下之結果.

Proposition . 若 $A, B \in M_n(F)$ 且 $A \sim B$, 則 $\mu_A(x) = \mu_B(x)$.

我們也可以定一個 linear operator 的 minimal polynomial.

Definition . 設 V 為一個 *finite dimensional F-space,* $T : V \to V$ 為一個 *linear operator.* 在所有非零多項式 $f(x) \in F[x]$ 中滿足 $f(T) = \mathbf{O}$, 且次數最小的 *monic polynomial* 稱為 T 的 minimal polynomial, 用 $\mu_T(x)$ 來表示.

同 matrix 的情形, T 的 minimal polynomial 必存在且唯一. 利用矩陣情形相同的證明方法 (需用到零函數和任何函數合成仍為零函數) 我們會有以下結果.

Lemma . 假設 V 為一個 *finite dimensional F-space,* $T : V \to V$ 為一個 *linear operator.* 則 $f(T) = \mathbf{O}$ 若且唯若 $\mu_T(x) \mid f(x)$.

當 β 為 V 的 ordered basis, T 的 characteristic polynomial $\chi_T(x)$ 是由 T 的 representative matrix $[T]_\beta$ 的 characteristic polynomial $\chi_{[T]_\beta}(x)$ 定義而得. 不過 T 的 minimal polynomial $\mu_T(x)$ 並不是由 $\mu_{[T]_\beta}$ 定義得到, 所以我們要探討它們是否相同.

Proposition . 設 V 為一個 *finite dimensional F-space,* β 為 V 的一個 *ordered basis* 且 $T : V \to V$ 為 *linear operator.* 則

$$\mu_T(x) = \mu_{[T]_\beta}(x).$$

最後我們來探討 minimal polynomial 和 characteristic polynomial 之間的關係.

Theorem .

(1) 假設 $A \in M_n(F)$, 則 $\mu_A(x) \mid \chi_A(x)$. 而且若 $p(x) \in F[x]$ 是一個 *irreducible polynomial,* 則 $p(x) \mid \chi_A(x)$ 若且唯若 $p(x) \mid \mu_A(x)$.

(2) 假設 V 為 *finite dimensional F-space,* $T : V \to V$ 為 *linear operator over F,* 則 $\mu_T(x) \mid \chi_T(x)$. 而且若 $p(x) \in F[x]$ 是一個 *irreducible polynomial,* 則 $p(x) \mid \chi_T(x)$ 若且唯若 $p(x) \mid \mu_T(x)$.

利用以上的 Theorem, 我們馬上有以下的結果.

Corollary . 若 $A \in M_n(F)$ 且 $\chi_A(x) = p_1^{c_1}(x) \cdots p_k^{c_k}(x)$ 其中 $c_i \in \mathbb{N}$, $p_i(x) \in F[x]$ 為 *monic irreducible polynomial* 且 $p_i(x) \neq p_j(x)$ *for* $i \neq j$, 則 $\mu_A(x) = p_1^{m_1}(x) \cdots p_k^{m_k}(x)$ 其中 $1 \leq m_i \leq c_i$.

當然了對於 linear operator 也會有同樣的結果, 我們就不再贅述了. 這裡最重要的便是要知道, 以後我們找一個方陣或一個 linear operator 的 minimal polynomial 的方法便是先找到它的 characteristic polynomial, 然後再利用上一個 Theorem 從最小次數的情形一個一個代入, 直到得到零矩陣或零函數時, 便是其 minimal polynomial 了.

Example . 考慮 *linear operator* $T : P_2(\mathbb{R}) \to P_2(\mathbb{R})$ 滿足

$$T(1) = 2x^2 - 1, T(x+1) = 3x^2 + 2x + 2, T(-x^2 + x + 1) = 4x^2 + 2x + 2.$$

我們想找出 T 的 *minimal polynomial* $\mu_T(x)$.

首先考慮 $P_2(\mathbb{R})$ 的 *ordered basis* $\beta = (-x^2+x+1, x+1, 1)$. 因

$$\begin{array}{rcl} T(-x^2+x+1) & = & (-4)(-x^2+x+1)+6(x+1) \\ T(x+1) & = & (-3)(-x^2+x+1)+5(x+1) \\ T(1) & = & (-2)(-x^2+x+1)+2(x+1)+(-1)1 \end{array}$$

得 $[T]_\beta = \begin{pmatrix} -4 & -3 & -2 \\ 6 & 5 & 2 \\ 0 & 0 & -1 \end{pmatrix}$. 計算得 $\chi_T(x) = \chi_{[T]_\beta}(x) = (x+1)^2(x-2)$. 又

$$([T]_\beta + I_3)\cdot([T]_\beta - 2I_3) = \begin{pmatrix} -3 & -3 & -2 \\ 6 & 6 & 2 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} -6 & -3 & -2 \\ 6 & 3 & 2 \\ 0 & 0 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 6 \\ 0 & 0 & -6 \\ 0 & 0 & 0 \end{pmatrix},$$

知 $\mu_T(x) = \mu_{[T]_\beta}(x) \neq (x+1)(x-2)$, 而得 $\mu_T(x) = \mu_{[T]_\beta}(x) = (x+1)^2(x-2)$. 事實上

$$([T]_\beta + I_3)^2\cdot([T]_\beta - 2I_3) = \begin{pmatrix} -3 & -3 & -2 \\ 6 & 6 & 2 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 6 \\ 0 & 0 & -6 \\ 0 & 0 & 0 \end{pmatrix} = \mathbf{O}.$$

4. Primary Decomposition

當 U, W 皆為 V 的 subspace 且 $U \cap W = \{\mathbf{O}_V\}$ 時, 我們會將 $U+W$ 用 $U \oplus W$ 來表示. 要注意此時 $U \oplus W$ 指的是 V 的 subspace $U+W$. 我們用 $U \oplus W$ 這個符號來強調 $U \cap W = \{\mathbf{O}_V\}$ 並稱之為 U, W 的 *internal direct sum.*

當 V 為 finite dimensional vector space, 且 U 是 V 的 subspace. 我們可以找到另一個 V 的 subspace W 使得 $V = U \oplus W$. 事實上任取 U 的一組 basis $S = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$, 我們知可以將 S 擴大成 V 的一組 basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n\}$. 此時若令 $W = \mathrm{Span}(\{\mathbf{w}_1, \ldots, \mathbf{w}_n\})$, 由於 $\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n\}$ 為 linearly independent, 我們知 $U \cap W = \{\mathbf{O}_V\}$. 所以可得 $U \oplus W$ 這一個 U, W 的 internal direct sum. 又因為 $V = \mathrm{Span}(\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n\})$, 我們得 $U \oplus W = V$. 由於將一組 linearly independent 元素擴展成 basis 的方法並不唯一, 從這裡我們也了解到給定 V 的一個 subspace U, 可將 V 寫成 $U \oplus W$ 的 W 並不唯一.

將 V 寫成 internal direct sum $V = U \oplus W$ 的一個好處就是若 $\mathbf{v} \in V$, 則存在唯一的 $\mathbf{u} \in U$ 以及 $\mathbf{w} \in W$ 使得 $\mathbf{v} = \mathbf{u} + \mathbf{w}$. 我們將 V 寫成兩個 subspaces 的 internal direct sum 的性質列舉如下.

Proposition . 假設 U, W 為 V 的 *subspaces.* 下列是等價的

(1) $V = U \oplus W$.
(2) 若 $\mathbf{v} \in V$, 則存在唯一的 $\mathbf{u} \in U, \mathbf{w} \in W$ 使得 $\mathbf{v} = \mathbf{u} + \mathbf{w}$.
(3) 對任意 U, W 的 *basis* S_1, S_2, 我們有 $S_1 \cap S_2 = \emptyset$ 且 $S_1 \cup S_2$ 為 V 的一組 *basis.*

我們可以把兩個 subspaces 的 internal direct sum 推廣到更多 subspaces 的 internal direct sum. 我們有以下之定義.

Definition . 假設 $V_1,\ldots,V_k$ 為 V 的 *subspaces,* 且

$$V_i\cap(\sum_{j\neq i}V_j)=\{\mathbf{O}_V\},\forall i=1,\ldots,k$$

則 V 的 *subspace* $V_1+\cdots+V_k$ 稱為 $V_1,\ldots,V_k$ 的 internal direct sum, 用 $V_1\oplus\cdots\oplus V_k$ 表示.

再次強調, 對於 V 的 subspaces $V_1,\ldots,V_k$, 我們都有 $V_1+\cdots+V_k$ 這一個 subspace. 若我們寫成 $V_1\oplus\cdots\oplus V_k\subseteq V$ 或強調為 internal direct sum, 便是說 $V_1,\ldots,V_k$ 滿足 $V_i\cap(\sum_{j\neq i}V_j)=\{\mathbf{O}_V\},\forall i=1,\ldots,k$ 這些條件. 另外, 以後我們要談的 decomposition theorem, 都是將一個 vector space 拆解成一些 subspaces 的 internal direct sum, 因為我們不會去談所謂 external direct sum, 所以我們就不再強調為 internal direct sum, 直接稱為 direct sum..

將 vector space 寫成多個 subspaces 的 direct sum, 和寫成兩個 subspaces 的 direct sum 有同樣的性質. 由於證明和前一個 Proposition 相同, 我們就不再證明了.

Proposition . 假設 $V_1,\ldots,V_k$ 為 V 的 *subspace.* 下列是等價的

(1) $V=V_1\oplus\cdots\oplus V_k$.
(2) 若 $\mathbf{v}\in V$, 則對於所有 $i=1,\ldots,k$ 皆存在唯一的 $\mathbf{v}_i\in V_i$ 使得 $\mathbf{v}=\mathbf{v}_1+\cdots+\mathbf{v}_k$.
(3) 對任意 V_i 的 *basis* S_i, 我們有 $S_1\cap\cdots\cap S_k=\emptyset$ 且 $S_1\cup\cdots\cup S_k$ 為 V 的一組 *basis.*

讓我們回到 linear operator. 若 $T:V\to V$ 為 linear operator, 我們希望將 V 寫成一些 subspaces 的 direct sum, 使這些 subspaces 的 ordered basis 所組成 V 的 ordered basis 讓 T 的 representative matrix 有比較好的形式. 要達到這個目的, 我們希望 T 限制在這些 subspaces 上是不會跑掉的 (即希望它們仍為 linear operator), 所以我們有以下的定義.

Definition . 假設 $T:V\to V$ 是一個 *linear operator.* 若 W 為 V 的 *subspace* 且滿足 $T(W)\subseteq W$ *(*即對所有 $\mathbf{w}\in W$ 皆有 $T(\mathbf{w})\in W$*),* 則稱 W 為 T*-invariant.*

很容易判斷 $\mathrm{Im}(T)$ 和 $\mathrm{Ker}(T)$ 皆為 T-invariant. 我們可以利用 $f(x)\in F[x]$ 得到更多 T-invariant subspaces.

Lemma . 假設 V 為 F*-space,* $T:V\to V$ 為 *linear operator* 且 $f(x)\in F[x]$. 則 $\mathrm{Im}(f(T))$ 和 $\mathrm{Ker}(f(T))$ 皆為 T*-invariant subspaces.*

Proof. 假設 $\mathbf{w}\in\mathrm{Im}(f(T))$, 即存在 $\mathbf{v}\in V$ 使得 $\mathbf{w}=f(T)(\mathbf{v})$. 由 $T\circ f(T)=f(T)\circ T$, 因此

$$T(\mathbf{w})=T(f(T)(\mathbf{v}))=(T\circ f(T))(\mathbf{v})=(f(T)\circ T)(\mathbf{v})=f(T)(T(\mathbf{v}))\in\mathrm{Im}(f(T)),$$

得證 $\mathrm{Im}(f(T))$ 為 T-invariant.

假設 $\mathbf{v}\in\mathrm{Ker}(f(T))$, 亦即 $f(T)(\mathbf{v})=\mathbf{O}_V$. 此時 $f(T)(T(\mathbf{v}))=T(f(T)(\mathbf{v}))=T(\mathbf{O}_V)=\mathbf{O}_V$, 亦即 $T(\mathbf{v})\in\mathrm{Ker}(f(T))$, 得證 $\mathrm{Ker}(f(T))$ 為 T-invariant. □

給定一個 linear operator $T:V\to V$, 考慮 V 的一個 subspace W, 我們可以將 T 的定義域限制在 W 上, 即考慮 $T|_W:W\to V$, 定義為 $T|_W(\mathbf{w})=T(\mathbf{w}),\forall\mathbf{w}\in W$. 這是一個從 W 到 V 的 linear transformation, 我們稱為 the *restriction* on W. 當 W 為 T-invariant 時, 因 $T(\mathbf{w})\in W$, $\forall\mathbf{w}\in W$, 我們有 $T|_W:W\to W$, 為一個 W 上的 linear operator. 我們自然可

以探討 $T|_W$ 和 T 的 minimal polynomial 之間的關係. 首先對於 $f(x)\in F[x]$, 因 W 亦為 $f(T)$-invariant, 我們有興趣知道 $f(T)|_W$ 和 $f(T|_W)$ 這兩個 W 的 linear operator 之間的關係. 現對所有 $\mathbf{w}\in W$, 因

$$T^{\circ 2}|_W(\mathbf{w})=T^{\circ 2}(\mathbf{w})=T(T(\mathbf{w}))=T|_W(T|_W(\mathbf{w}))=T|_W{}^{\circ 2}(\mathbf{w}),$$

我們知 $T^{\circ 2}|_W$ 和 $T|_W{}^{\circ 2}$ 為 W 上相同的 linear operator. 利用數學歸納法可得 $T^{\circ i}|_W=T|_W{}^{\circ i}, \forall i\in\mathbb{N}$. 現若 $f(x)=a_dx^d+\cdots+a_1x+a_0\in F[x]$, 則對於任意 $\mathbf{w}\in W$, 皆有

$$\begin{aligned}f(T)|_W(\mathbf{w})=f(T)(\mathbf{w})&=a_d T^{\circ d}|_W(\mathbf{w})+\cdots+a_1 T|_W(\mathbf{w})+a_0\,\mathrm{id}|_W(\mathbf{w})\\&=a_d T|_W{}^{\circ d}(\mathbf{w})+\cdots+a_1 T|_W(\mathbf{w})+a_0\,\mathrm{id}|_W(\mathbf{w})=f(T|_W)(\mathbf{w}).\end{aligned}$$

也就是說 $f(T)|_W$ 和 $f(T|_W)$ 是 W 上相同的 linear operator, 因此知

$$f(T)|_W=f(T|_W).$$

利用此結果, 我們有以下之 Lemma.

Lemma . 假設 $T:V\to V$ 為 *linear operator,* W 為 T*-invariant subspace,* 則 T 的 *restriction on* W*,* $T|_W:W\to W$ 為 W 上的 *linear operator,* 且其 *minimal polynomial* $\mu_{T|_W}(x)$ 滿足

$$\mu_{T|_W}(x)\mid\mu_T(x).$$

假設 V 可以寫成兩個 T-invariant subspace U,W 的 (internal) direct sum $V=U\oplus W$, 分別選取 U,W 的一個 ordered basis $\beta_1=(\mathbf{u}_1,\ldots,\mathbf{u}_l),\beta_2=(\mathbf{w}_1,\ldots,\mathbf{w}_m)$, 則知 $\beta=(\mathbf{u}_1,\ldots,\mathbf{u}_l,\mathbf{w}_1,\ldots,\mathbf{w}_m)$ 亦為 V 的 ordered basis. 此時由於 $T(\mathbf{u}_i)=T|_U(\mathbf{u}_i)\in U$, 我們知 $[T]_\beta$ 的前面 l 個 columns, 每個 column 的前 l 個 entry 都和 $[T|_U]_{\beta_1}$ 相同, 而且後面 m 個 entry 皆為 0. 同樣的, 由於 $T(\mathbf{w}_j)=T|_W(\mathbf{w}_j)\in W$, 我們知 $[T]_\beta$ 的後面 m 個 columns, 每個 column 的前 l 個 entry 都是 0 而後面 m 個 entry 皆和 $[T|_W]_{\beta_2}$ 相同. 也就是說 T 對於 β 的 representative matrix 為

$$[T]_\beta=\begin{pmatrix}[T|_U]_{\beta_1} & \mathbf{O}\\ \mathbf{O} & [T|_W]_{\beta_2}\end{pmatrix}$$

利用這個結果我們就可以得到 characteristic polynomial 的關係了.

Lemma . 假設 V 為 *finite dimensional* F*-space,* $T:V\to V$ 為 *linear operator.* 若 $V=U\oplus W$*,* 其中 U,W 為 T*-invariant subspace,* 則

$$\chi_T(x)=\chi_{T|_U}(x)\chi_{T|_W}(x).$$

至於 minimal polynomial, 我們可以得到以下的關係.

Lemma . 假設 V 為 *finite dimensional* F*-space,* $T:V\to V$ 為 *linear operator.* 若 $V=U\oplus W$*,* 其中 U,W 為 T*-invariant subspace,* 則

$$\mu_T(x)=\mathrm{lcm}(\mu_{T|_U}(x),\mu_{T|_W}(x)).$$

現在我們來說明如何將 V 寫成 T-invariant subspaces 的 direct sum.

Theorem . 假設 V 為 *finite dimensional* F*-space,* $T: V \to V$ 為 *linear operator* 且 $\mu_T(x) = f(x)g(x)$, 其中 $f(x), g(x) \in F[x]$ 為 *monic polynomials* 且 *relatively prime.* 若令 $U = \mathrm{Ker}(f(T))$, $W = \mathrm{Ker}(g(T))$, 則 V 可以寫成 T*-invariant subspaces* U, W 的 *internal direct sum,* 即 $V = U \oplus W$, 而且 $\mu_{T|_U}(x) = f(x)$ 以及 $\mu_{T|_W}(x) = g(x)$.

上個定理告訴我們可以利用找 kernel 得到 T-invariant subspace. 回顧一下, 對於 linear operator $T: V \to V$, 要找到 $\mathrm{Ker}(T)$, 我們可以利用 V 的 ordered basis β, 先得到 representative matrix $[T]_\beta$. 再求 $[T]_\beta$ 的 null space $N([T]_\beta)$ (我們用 $N(A)$ 表示矩陣 A 的 null space). 接著將 null space 的元素用 $\tau_\beta^{\circ -1}$ 還原成 V 的元素, 就得到 $\mathrm{Ker}(T)$ 的元素了.

$F[x]$ 是一個 unique factorization domain (U.F.D.), 表示 $F[x]$ 中的非常數多項式都可以唯一寫成一些 irreducible polynomials 的乘積. 因此對於 linear operator T 的 minimal polynomial, 我們可以找到相異的 monic irreducible polynomials $p_1(x), \ldots, p_k(x)$ 使得 $\mu_T(x) = p_1(x)^{m_1} \cdots p_k(x)^{m_k}$, 其中 $m_1, \ldots, m_k \in \mathbb{N}$. 由於 characteristic polynomial $\chi_T(x)$ 和 $\mu_T(x)$ 有相同的質因式且 $\mu_T(x) \mid \chi_T(x)$, 我們知道 $\chi_T(x) = p_1(x)^{c_1} \cdots p_k(x)^{c_k}$, 其中 $c_i \in \mathbb{N}$ 且 $c_i \geq m_i$.

Theorem (Primary Decomposition Theorem)**.** 假設 V 是 *dimension* 為 n 的 F*-space,* $T: V \to V$ 為 *linear operator* 且

$$\mu_T(x) = p_1(x)^{m_1} \cdots p_k(x)^{m_k} \quad \text{and} \quad \chi_T(x) = p_1(x)^{c_1} \cdots p_k(x)^{c_k}$$

其中 $c_i, m_i \in \mathbb{N}$ 且 $p_1(x), \ldots, p_k(x)$ 為相異的 *monic irreducible polynomials.* 若令 $V_i = \mathrm{Ker}(p_i(T)^{\circ m_i})$, *for* $i = 1, \ldots, k$, 則

$$V = V_1 \oplus \cdots \oplus V_k$$

且

$$\mu_{T|_{V_i}}(x) = p_i(x)^{m_i} \quad \text{and} \quad \chi_{T|_{V_i}}(x) = p_i(x)^{c_i}, \forall i = 1, \ldots, k.$$

Primary Decomposition Theorem 告訴我們, 若 linear operator $T: V \to V$ 的 characteristic polynomial (或 minimal polynomial) 是 $p_1(x)^{c_1} \cdots p_k(x)^{c_k}$, 則我們可以找到 V 的 ordered basis β, 使得 $[T]_\beta$ 為以下的 block diagonal matrix

$$\begin{pmatrix} A_1 & & \mathbf{O} \\ & \ddots & \\ \mathbf{O} & & A_k \end{pmatrix},$$

其中每個 A_i 的 characteristic polynomial 為 $\chi_{A_i}(x) = p_i(x)^{c_i}$. 因此以後我們只要個別探討 linear operator 其 characteristic polynomial 為 $p(x)^c$ (其中 $p(x)$ 為 monic irreducible, $c \in \mathbb{N}$) 這種情形就可以了.

對於 $n \times n$ 方陣 $A \in M_n(F)$, 我們也可以利用 linear operator 的 primary decomposition 的概念找到 invertible matrix $P \in M_n(F)$ 使得 $P^{-1} \cdot A \cdot P$ 為 block diagonal matrix. 我們可以將 A 看成是 linear transformation $T: F^n \to F^n$ 其定義為 $T(\mathbf{x}) = A\mathbf{x}$. 此時 A 便是 T 對於標