

目录

第一章	Linear Equations	3
1.1	Fields	3
1.2	Systems of Linear Equations	3
1.3	Matrices and Elementary Row Operation	3
1.4	Row reduced Echelon Matrices	5
1.5	Matrix Multiplication	7
1.6	Invertible Matrices	9
第二章	Vector Spaces	13
2.1	Vector Spaces	13
2.2	Subspaces	13
2.3	Bases and Dimension	13
2.4	Coordinates	14
2.5	Summery of Row-Equivalence	15
2.6	Computation Concerning Subspaces	17
第三章	Linear Transformations	19
3.1	Linear Transformations	19
3.2	The Algebra of Linear Transformations	20
3.3	Isomorphism	21
3.4	Representation of Transformations by Matrices	22
3.5	Linear Function	24
3.6	The Double Dual	25
3.7	The Transpose of a Linear Transformation	28
第四章	Polynomials	30
4.1	Algebra	30
4.2	The Algebra of Polynomials	30
4.3	Polynomials Ideals	31
4.4	Lagrange Interpolation	34
第五章	Determinant	35
第六章	Elementary Canonical Forms	36
6.1	Introduction	36
6.2	Characteristic Values	36

6.3	Annihilating Polynomial	39
6.4	Invariant Subspaces	42
6.5	Simultaneous Triangulation; Simultaneous Diagonalization	43
6.6	Direct-Sum Decompositions	44
6.7	Invariant Direct Sum	45
6.8	The Primary Decomposition Theorem	46
第七章	The rational and Jordan Forms	47
7.1	Cyclic Subspaces and Annihilators	47
7.2	Cyclic Decompositions and the Rational Form	48
7.3	The Jordan Form	51
7.4	Computation of Invariant Factors	53
7.5	Summary; Semi-Simple Operator	53
第八章	Inner Product Spaces	55
8.1	Inner Products	55
8.2	Adjoint	59

第一章 Linear Equations

1.1 Fields

1.2 Systems of Linear Equations

定义1.2.1 给定域 F ,我们称

$$\begin{cases} A_{11}x_1 + \cdots + A_{1n}x_n = y_1 \\ \cdots \\ A_{m1}x_1 + \cdots + A_{mn}x_n = y_m \end{cases}$$

为线性方程组, 其中 A_{ij} 称为系数, y_i 称为常数项.

我们去研究是否存在解以及解是否唯一. 可以将线性方程组看成工具 (讨论线性空间的性质的工具)

例如在 F^m 中取了若干个向量 $\alpha_1 = (A_{11}, \cdots, A_{1n}), \cdots, \alpha_n = (A_{n1}, \cdots, A_{nn})$ 给定 $\beta = (y_1, \cdots, y_m)$ 是否 $\in \text{span}\{\alpha_1, \cdots, \alpha_n\} = \{(\sum_{i=1}^n x_i A_{1i}, \cdots, \sum_{i=1}^n x_i A_{mi})\}$ 即转化为上述方程组.

下面系统地讨论这个方程的解的问题.

定义1.2.2 我们将满足方程组的解 (x_1, \cdots, x_n) 称为解.

定义1.2.3 如果 $y_1 = \cdots = y_m = 0$, 则称为齐次方程组. 否则称为非齐次方程组. 我们将解 $(0, \cdots, 0)$ 称为平凡解

考虑映射 $T: F \rightarrow F, T(x_1, \cdots, x_m) = (\sum_{i=1}^n x_i A_{1i}, \cdots, \sum_{i=1}^n x_i A_{mi})$

此时 T 是线性映射, 即 $T(\alpha + \beta) = T(\alpha) + T(\beta), T(c\alpha) = cT(\alpha)$ 此时, 对于 $\gamma = (y_1, \cdots, y_m)$ 原方程组可化为求映射的原像集 $T^{-1}(\gamma)$

方程组无解充分必要条件即 γ 是否在 T 的像集里面. 齐次方程组的解即为原点的原像. 且 $0 \in T^{-1}(0)$. 齐次线性方程组的解空间一定为线性子空间, 非齐次方程组解集不构成线性子空间, 称为仿射子空间. 我们即研究齐次方程组解空间的结构, 因为非齐次方程组的解空间可以看成齐次线性方程组解空间的一个平移 (容易看出). 这就是从线性空间的角度来看线性方程组

下面直接从方程组入手来解方程, 称为Guass消元法.

定义1.2.4 我们称两个方程组等价, 如果2中每个方程都是1中的每个方程的线性组合, 同时2中的每个方程也是1中的每个方程的线性组合.

1.3 Matrices and Elementary Row Operation

显然, 等价的方程组同解, 即有相同的解空间. Guass消元法即用等价的方程组去代替原方程组, 从而尽量将方程组化为充分地简单. 即每个方程只有一个 x_i 的系数非0, 且非零的系数为1. 这样, 我们就认为方程被解出来了.

但用方程组的语言不够方便, 于是引入矩阵.

定义1.3.1 给定域 F ,由 F 中的元素构成了 m 行 n 列的数表,则称为 F 上 $m \times n$ 的矩阵.

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{m1} & \cdots & A_{mn} \end{pmatrix}$$

A_{ij} 也叫 ij 元.(事实上,若严密,可以将矩阵看成一个映射)

那么矩阵

$$A = \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{m1} & \cdots & A_{mn} \end{pmatrix}$$

也叫方程组1的系数矩阵.

一个行向量可以看成一个 $1 \times n$ 的矩阵,一个列向量可以看成一个 $m \times 1$ 的矩阵.记

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ A_m \end{pmatrix}$$

我们将这个方程记作 $AX = Y$,记

$$A' = (A, Y) = \begin{pmatrix} A_{11} & \cdots & A_{1n} & y_1 \\ \vdots & & \vdots & \vdots \\ A_{m1} & \cdots & A_{mn} & y_m \end{pmatrix}$$

为这个方程组的增广矩阵.也可将增广矩阵按行向量排为

$$X = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

我们考虑这些行向量线性组合 $\sum_{i=1}^m c_i \alpha_i$,即为刚才定义的方程的线性组合的系数.

即将方程的线性组合化为这些向量的线性组合(它们含有相同的信息),方程的所谓的线性组合即为这些行向量真正的线性组合.

而等价方程组用矩阵的语言来说,即可看成将上述 α_i 的 k 个线性组合

$$\begin{pmatrix} \sum_{i=1}^m c_{i1} \alpha_i \\ \vdots \\ \sum_{i=1}^m c_{ik} \alpha_i \end{pmatrix}_{k \times (n+1)}$$

为了能方便判断可逆与简洁,我们考虑一些特殊的线性组合,称为初等行变换.

定义1.3.2 一个矩阵 $A_{m \times n}$ 的初等行变换指以下三种变换

- (1)用某个 $c \in F - \{0\}$ 乘 A 的某行,其它行不变.记为 $[i] \mapsto [ci]$
- (2)把某行 $c(c \in F)$ 倍加到另一行上,记为 $[i] \mapsto [i] + c[j]$
- (3)互换矩阵的两行,记为 $[i] \leftrightarrow [j]$

我们可以把矩阵的初等行变换看成一个映射.

记 $F_{m \times n}$ 看成所有 $m \times n$ 的矩阵构成的集合,这时,初等行变换可以看成映射 $e: F^{m \times n} \rightarrow F^{m \times n}$ (显然).我们有如下命题,从而可以得出初等行变换得到的方程组是原方程组的等价方程组

命题1.3.1 映射 e 可逆, 且 e 的逆也是初等行变换

证明:直接验证即可

对于(1), 有 $e^{-1} = [i] \mapsto e^{-1}[i]$, 对于(2), $e^{-1} = [i] \mapsto [i] - c[j]$, 对于(3), $e^{-1} = [i] \leftrightarrow [j]$

也可说成将一个方程组的增广矩阵做初等行变换也是另一个方程组的增广矩阵, 且两个方程组同解, 于是Gauss消元法就是将方程组利用初等行变换变成简单的矩阵, 这样的矩阵称为行简化矩阵, 即一种简单的方程组的增广矩阵.

对于两个矩阵 A 和 B , 如果 B 的每一行都是 A 的每一行的线性组合, 可以证明 B 可由 A 的初等行变换得到.

定义1.3.3 如果 $A, B \in F^{m \times n}$ 称 A 和 B 行等价, 如果存在有限个初等行变换 e_1, e_2, \dots, e_k , 使得 $e_1 \cdots e_k(A) = B$

容易验证, 矩阵之间的行等价是一种等价关系.

由此说明, 用矩阵的语言来解线性方程组确实行得通, 行得通是什么意思呢? 可用下述命题表示

命题1.3.2 设 $A, B \in F^{m \times n}, Y, Z \in F^{m \times 1}$ 如果 (A, Y) 与 (B, Z) 行等价, 则这两个方程组 $AX = Y, BX = Z$ 同解, 特别地, 如果 A 和 B , 则这两个矩阵所对应的齐次线性方程组同解

证明是显然的.

1.4 Row reduced Echelon Matrices

那么, 到底什么是充分简单的矩阵, 即行简化矩阵呢?

定义1.4.1 我们称一个矩阵是行简化矩阵, 如果

- (1) 每个非零行的第一个非零元(称为主元)是1.
- (2) 每个主元所在列的其余的矩阵所在列的其他的矩阵元均为0.

例如,

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

就是行简化矩阵, 叫做 n 阶单位矩阵, 适当的时候下标 n 可以不写. 满足 $I_{ij} = \delta_{ij}$ δ_{ij} 为Kronecker符号

行简化矩阵有什么用呢? 事实上, 若 B 是行简化矩阵. 则方程组 $BX = Z$ 的解可以容易写出.

若最后得到的增广矩阵 (B, Z) , 若某一行最后一个非零而其他全为零, 则这个方程组显然无解, 而某一行全为零而其他也全为零, 则这一行没有提供有意义的信息. 由于每个主元所在列的其余的矩阵所在列的其他的矩阵元均为0, 则相当于解出了主元所对应的那个方程组(每个主元只出现了一次).

而我们有如下命题.

命题1.4.1 每个矩阵都等价于某个行简化矩阵.

证明: 如果第一行是零行, 则不用考虑, 否则第一行是非零行, 且不妨设这个非零元前面的每一列均为0, 否则交换两行即可. 找第一个非零元, 每一行均乘它的逆元, 变为1, 然后将这一列非零的数通过第二种初等行变换变为0, 然后类似进行次操作即可.

下面再将方程组化得更简单一点(对解方程组其实没有简化)

定义1.4.2 A 称为行简化阶梯矩阵, 如果下面几条成立

- (1) A 是行简化矩阵.
- (2) 零行都在最下方.
- (3) 非零行的非零行主元的列指标随着行指标的增大而增大.

容易看出每个行简化矩阵可以进一步化成行简化阶梯矩阵(不断交换行的位置即可,先将零行调到最下方,再将非零行按照主元顺序依次排列即可).于是有如下命题.

命题1.4.2 每个矩阵都等价于某个行简化阶梯矩阵.

对于方程组 $AX = Y$ (A 为 $m \times n$ 的矩阵), 利用初等行变换, 将 $(A, Y) \rightarrow (R, Z)$, 其中 R 是行简化阶梯矩阵. 从而 $AX = Y$ 与 $RX = Z$ 同解. 设 R 有 r 个非零行, 显然 $r \leq m$, 而由于主元所在的列互不相同, 故 $r \leq n$, 设前 r 中的第 i 行 ($1 \leq i \leq r$) 的主元在第 k_i 列. 从而有 $k_1 < k_2 < \dots < k_r$. 设 $J = \{1, \dots, n\} - k_1, \dots, k_r$

从而 $RX = Z$ 为

$$\begin{cases} x_{k_1} + \sum_{j \in J} c_{1j} x_j = z_1 \\ \vdots \\ x_{k_r} + \sum_{j \in J} c_{rj} x_j = z_r \\ 0 = z_{r+1} \\ \vdots \\ 0 = z_m \end{cases}$$

根据这个方程组我们可以容易写出原方程的解:

若 $m > r$, 且 z_{r+1}, \dots, z_m 不全为零, 则原方程组无解.

否则, 零行可以忽略, 则只有前面 r 个方程组.

若 $n = r$ 则 $J = \emptyset, k_i = i$ 则说明整个矩阵的非零部分是方的, 即 $R = I_n$ 再下边添上一些零行, 方程组有唯一解 $(x_1, x_2, \dots, x_n) = (x_{k_1}, \dots, x_{k_n}) = (z_1, \dots, z_r)$

若 $n > r, |J| > 0$, 解为

$$\begin{cases} x_{k_1} = z_1 - \sum_{j \in J} c_{1j} x_j \\ \vdots \\ x_{k_r} = z_r - \sum_{j \in J} c_{rj} x_j \end{cases}$$

其中, 对 $j \in J, x_j \in F$ 可任意取值. 此时, 解一定不唯一.

由此, 我们可以得出方程组的一些性质.

命题1.4.3 若 $m < n$, 其中 m 代表方程的个数, n 代表未知量的个数, 则齐次方程组 $AX = Y$ (A 为 $m \times n$ 的矩阵) 一定有非平凡解.

证明: 显然, 前面两种情况都不会出现. 所以只能是 $n > r$ 的情况.

事实上, 上述命题等价于定理2.3.1. 还有

命题1.4.4 设 $F \subset F'$, 若 $AX = Y$ 在 F' 有解, 则在 F 中有解, 其中 $A \in F^{m \times n}, Y \in F^{n \times 1}$

比如, 一个实系数的线性方程组有复数解, 则一定也有实数解.

证明: 我们对 (A, Y) 进行初等行变换, 其中乘的系数都在 F 中, 所以最后得到的简化阶梯形矩阵的数都在 F 中.

另一方面, 上述初等行变换也可以看成在 F' 中的初等行变换, 最后得到了相同的简化阶梯型矩阵. 而有解等价于 z_{r+1}, \dots, z_n 均为0, 这在 F 中也是一样的, 从而原方程在 F 中有解.

这个命题非平凡的原因是只对线性方程组成立, 例如 $x^2 + y^2 + 1 = 0$ 将不对.

命题1.4.5 设 $A \in F^{n \times n}$ 为一个方阵, 则TFAE:(the followings are equivalent)

- (1) $AX = 0$ 只有平凡解
- (2) 对任意 $Y \in F^{n \times 1}$, $AX = Y$ 有唯一解
- (3) A 和 I_n 行等价.

证明: 我们证明(1) \rightarrow (2) \rightarrow (3) \rightarrow (1):

(2) \rightarrow (1) 显然.

(3) \rightarrow (2) 满足上述中 $n = r$ 的情形, 故得证.

(1) \rightarrow (3) 我们将 $(A, 0)$ 通过初等行变换化为 $(R, 0)$, 为 R 简化阶梯型矩阵. 从而上述中也只能 $n = r$ 的情形. 从而 $m = n = r$, 故只能 $R = I_n$ 从而 A 与 I_n 行等价.

下面讨论齐次线性方程组解空间的基和维数.

若 $n = r$, 则齐次方程组只有零解. 基为空集, 维数为0.

若 $n > r$ 则方程组的解即为

$$\begin{cases} x_{k_1} = - \sum_{j \in J} c_{1j} x_j \\ \vdots \\ x_{k_r} = - \sum_{j \in J} c_{rj} x_j \end{cases}$$

从而 x_j 任意取, 就解出了 $(x_{k_1}, \dots, x_{k_n})$. 而一个解指的是 (x_1, \dots, x_n)

对 $j_n \in J$, 在通解中令 $x_{j_0} = 1$, 其余 $x_j = 0$ 得到一个解 $\alpha_0 \in F^n$, 满足 $x_{k_i} = -c_{ij_0}$

将 J 中的每个指标均当作一次 j_0 , 我们证明

命题1.4.6 $\{\alpha_{j_0} | j \in J\}$ 是 $T^{-1}(0)$ 的基. 从而 $\dim T^{-1}(0) = |J| = n - r$

证明: 我们称 $x_j (j \in J)$ 为自由变量, 共有 $|J|$ 个自由变量.

我们先证明它们线性无关, 如果 $\sum_{j \in J} c_j \alpha_j = 0$. 有 α_{j_0} 的选取即得 $c_j = 0$.

在证明 $\text{span} = T^{-1}(0)$ 显然 $\text{span} \subset T^{-1}(0)$

而任取 $\alpha \in T^{-1}(0) = (a_1, \dots, a_n)$. 在通解中, 取 $x_j = a_j (j \in J)$ 得到了一组解. 代入即容易证明

1.5 Matrix Multiplication

给定域 F , 对于 $A, b \in F^{m \times n}$ 我们定义 $A + B$ 满足 $(A + B)_{ij} = A_{ij} + B_{ij}$, 对 $c \in F$, 定义 $(cA)_{ij} = cA_{ij}$ 分别叫做矩阵的加法和纯量乘法

在这样的定义下, $F^{m \times n}$ 是 F 线性空间. 并且 $F^{1 \times n} = F^n$ (行向量), $F^{m \times 1}$ 同构于 F^m 并且有 $\dim F^n = n$, 标准基为 $\delta_1 \dots \delta_n$, $\delta_i = (0, \dots, 0, 1, 0, \dots, 0)$ 其中, 1在第 i 个位置.

类似的, 显然有 $\dim F^{m \times n} = mn$, 基为 $\{E_{rs} | 1 \leq r \leq m, 1 \leq s \leq n\}$ 满足

$$(E_{rs})_{ij} = \begin{cases} 1, (i, j) = (r, s) \\ 0, \text{其他} \end{cases}$$

对于 $A \in F^{n \times n}$ 满足 $A_{ij} = A_{ji}$, 容易验证 $\{A \in F^{n \times n} | A \text{对称}\} \subset F^{m \times n}$ 是子空间. 容易验证其维数为 $\frac{(n+1)n}{2}$

类似可定义反对称矩阵, 即 $A_{ij} = -A_{ji}$, 故若 $\text{char } F$ 不为2, 则维数为 $\frac{(n-1)n}{2}$, 否则维数为 $\frac{(n+1)n}{2}$, 由此也可以看出域的特征为2在有些时候会导致不同的结论

若 $F = \mathbb{C}$, 称一个矩阵 F 为Hermite矩阵或自伴矩阵, (Hermitian matrix)满足 $A_{ij} = \bar{A}_{ji}$ 所有Hermite矩阵不构成 \mathbb{C} 上的子空间, 由于 A 是Hermite, 则 iA 一般不是Hermite, 但若 $c \in \mathbb{R}$, cA 为Hermite. 所以, 我们称构成一个实子空间.

下面回到矩阵的乘法, 矩阵的乘法实质上是映射的复合

定义1.5.1 设 $A \in F^{m \times n}$, $B \in F^{n \times p}$, 定义 AB 满足 $AB \in F^{m \times p}$, 并且

$$(AB)_{ij} = \sum_{r=1}^n A_{ir}B_{rj}, 1 \leq i \leq m, 1 \leq j \leq p$$

一般来说, AB 和 BA 不相等, 若 $AB = BA$, 我们称 AB 可交换.

有了矩阵的乘法的定义之后, 方程组的记号 $AX = Y$ 就有实际的意义了.

对于 n 阶矩阵 A , 若存在 A^{-1} , 满足 $AA^{-1} = I_n$, 我们称 A 为可逆矩阵, 且 A^{-1} 称为 A 的逆矩阵. 从而解方程组 $AX = Y$, 在两边同时左乘 A^{-1} 之后, 变成 $X = A^{-1}Y$ 则解出了线性方程组, 从而, 我们可以发现, 解方程组的问题也可以化为矩阵乘法的问题. 而就算矩阵不可逆, 其实初等行变换也可以看成在对于矩阵的左边乘一个可逆矩阵. 最后使得存在 P , 使得 PA 为简化阶梯矩阵. 从而 $AX = Y$, 化为 $(PA)X = PY$.

命题1.5.1 当有定义时, 有

$$(1) A(BC) = (AB)C$$

$$(2) (A+B)C = AC + BC$$

$$A(B+C) = AB + AC$$

$$(3) \text{对于 } \forall d \in F, d(AB) = (dA)B = A(dB)$$

$$(4) A \in F^{m \times n}, \text{则 } I_m A = A, A I_n = A$$

$$(5) A \in F^{m \times n}, \text{则 } 0_{k,m} A = 0_{k,m}, A 0_{n,p} = 0_{m,p}$$

证明:

(1)

$$\begin{aligned} (A(BC))_{ij} &= \sum_r A_{ir}(BC)_{rj} = \sum_r A_{ir} \left(\sum_s B_{rs}C_{sj} \right) \\ ((AB)C)_{ij} &= \sum_s (AB)_{is}C_{sj} = \sum_s \left(\sum_r A_{ir}B_{rs} \right) C_{sj} \end{aligned}$$

上面两个式子显然相等

(2)(3)(4)(5) 利用定义也可直接验证

由上面的(1) 容易得到符号 ABC 是有意义的(由于和顺序无关), 一般地, 在有意义的情况下, 符号 $A_1 A_2 \cdots A_n$ 也是有意义的.(只是不能交换顺序)

对于 $A \in F^{n \times n}$, A^n 也是有意义的. 它即表示 $A \cdot A \cdots A$

对于 $A \in F^{m \times n}$, $B \in F^{n \times p}$, 记 $B = (B_1, B_2, \cdots, B_p)$ 为 B 按照列向量展开, 从而有 $AB = (AB_1, \cdots, AB_p)$ 类似地, 设

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \text{则 } AB = \begin{pmatrix} \alpha_1 B \\ \vdots \\ \alpha_n B \end{pmatrix}$$

另一方面

$$B = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}, \text{则 } AB = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix}$$

满足 $\gamma_i = \sum_{r=1}^n A_{ir}\beta_r$ 是 β_1, \cdots, β_n 的线性组合.

因此, 这样能表示出任意的 β_i 任意的线性组合, 于是 B 的任意行变换(无论初等还是不初等), 都可以看成在左边乘了一个矩阵. 特别地, 对于 B 的每一个初等行变换, 都可以看成在 B 的左边乘了一个矩阵来实现, 这样的矩阵我们叫做初等矩阵. 于是, 我们有如下定义

定义1.5.2 $E \in F^{m \times m}$ 称为初等矩阵, 如果存在一个初等行变换 $e: F^{m \times m} \rightarrow F^{m \times m}$,使得 $E = e(I_m)$. (1)
 $e = ([i] \rightarrow c[i])$ (c 不为0.则

$$E = \begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \ddots & c & \ddots & \cdots & \cdots \\ \vdots & \vdots & \cdots & \ddots & 1 & 0 & 0 \\ \vdots & \vdots & \cdots & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 0 & 1 \end{pmatrix}_{n \times n}$$

(2) $e = ([i] \rightarrow [i] + c[j])$

$$E = \begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \ddots & c & \cdots & \cdots \\ \vdots & \vdots & \ddots & 1 & \ddots & \cdots & \cdots \\ \vdots & \vdots & \cdots & \ddots & 1 & 0 & 0 \\ \vdots & \vdots & \cdots & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 0 & 1 \end{pmatrix}_{n \times n}$$

(3) $e = ([i] \leftrightarrow [j])$

$$E = \begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 1 & \cdots & \cdots \\ \vdots & \vdots & \ddots & 1 & \ddots & \cdots & \cdots \\ \vdots & \vdots & 1 & \ddots & 0 & 0 & 0 \\ \vdots & \vdots & \cdots & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 0 & 1 \end{pmatrix}_{n \times n}$$

我们说明, 每个初等行变换确实均可看成乘一个初等矩阵.

记 $F^{m \times \mathbb{N}} = \cup_{n=1}^{\infty} F^{m \times n}$,则 e 是 $F^{m \times \mathbb{N}}$ 到自身的映射

命题1.5.2 设 $e: F^{m \times \mathbb{N}} \rightarrow F^{m \times \mathbb{N}}$ 为初等行变换, 若 $E = e(I_m)$,则 $e(A) = EA, \forall A \in F^{m \times \mathbb{N}}$

证明:存在 $P \in F^{m \times m}$ 使得 $e(A) = PA, \forall A \in F^{m \times \mathbb{N}}$,且 P 与 A 无关, 取 $A = I_m$,从而 $P = E$,这样, 我们也得到

$$e(A) = e(I_m)A$$

推论1.5.1 设 $A, B \in F^{m \times n}$,则 A 与 B 行等价等价于存在有限个初等矩阵的乘积 $P = E_1 \cdots E_k$ 使得 $B = PA$

证明: 若 A 和 B 行等价, 存在有限个初等行变换 e_1, \dots, e_k ,使得 $e_1 \circ \dots \circ e_k(A) = B$

记 $E_i = e_i(I_m)$,则 $E_1 \cdots E_k A = B$,记 $P = E_1 \cdots E_k$ 即满足条件.

1.6 Invertible Matrices

定义1.6.1 设 $A \in F^{m \times n}$,若存在 $B \in F^{n \times m}$, 使得 $AB = BA = I_n$, 则称 A 可逆, B 称为 A 的逆矩阵, 或简称逆.

引理1.6.1 若 $AB = CA = I$ 可以推出 $B = C$

证明:

$$I_n B = (CA)B = CAB = C(AB) = CI_n = c$$

由此可以得到

推论1.6.1 可逆矩阵的逆一定是唯一的

从而我们将唯一的逆矩阵记为 A^{-1} .另外,我们有

命题1.6.1 若 A 可逆,则 A^{-1} 也可逆,且 $(A^{-1})^{-1} = A$

并且有

命题1.6.2 若 A, B 可逆,则 AB 也可逆,且 $AB^{-1} = B^{-1}A^{-1}$

代入直接验证即可

由此也可以得到有限个可逆矩阵的乘积也可逆,并且容易验证 $(A_1 \cdots A_k)^{-1} = A_k^{-1} \cdots A_1^{-1}$

我们还有

命题1.6.3 初等矩阵一定可逆

证明: 对于 $e: F^{m \times n} \rightarrow F^{m \times n}$,我们证明 $(e(I_n))^{-1} = e^{-1}(I_n)$

事实上,由 $e(A) = e(I)A, e(e^{-1}(I)) = I$,从而 $e(I)e^{-1}(I) = I$,同理 $e^{-1}(I)e(I) = I$ 即得.

命题1.6.4 设 $A \in F^{n \times n}$,TFAE:

- (1) A 可逆
- (2) A 与 I_n 行等价
- (3) A 为初等矩阵的乘积.

略证: (2)→(3),(3)→(1)均为显然,下面(1)→(2),只需下述命题:可逆的 $n \times n$ 行简化阶梯矩阵为 I_n ,事实上,我们有若 R 不为 I_n ,则最后一行一定为0行.由矩阵乘法知此矩阵不可逆.

推论1.6.2 设 $A, B \in F^{n \times n}$,则 A 和 B 等价的充分必要条件是存在可逆矩阵 P ,使得 $B = PA$

推论1.6.3 设 $A \in F^{n \times n}$ 可逆,初等变换 e_1, \cdots, e_k ,满足 $e_1 \circ \cdots \circ e_k(A) = I_n$,则 $e_1 \circ \cdots \circ e_k(I_n) = A^{-1}$

证明: 记 $E_i = e_i(I_n)$,则对任意 $B, e_i(B) = E_i B$,记 $P = E_1 \cdots E_k$,则 $e_1 \cdots e_k(B) = E_1 \cdots E_k B = PB$ 从而 $PA = I_n$,同时右乘 A^{-1} ,故 $P = A^{-1}$.而 $e_1 \cdots e_k(I_n) = P$,从而得证

从而,为了方便,我们可以同时操作 A 和 I ,最后一定得到 A 的逆矩阵.即

推论1.6.4 设 $A \in F^{n \times n}$,考虑 $n \times 2n$ 的矩阵 (A, I_n) ,满足 (P, B) 满足于 (A, I_n) 行等价,并且 R 为行简化阶梯矩阵,则

- (1)若 $R = I_n$,则 A 可逆,并且 $A^{-1} = B$
- (2)若 $R \neq I_n$,则 A 不可逆

这个推论给出了一个判断即求逆矩阵的操作方法,证明是显然的,由前面的结论可以推出.

还有:设 A 和 R 行等价,若存在 $J_1, J_2 \subset \{1, 2, \cdots, n\}, |J_1| + |J_2| = n + 1$ 使得 $R_{ij} = 0, \forall i \in J_1, j \in J_2$,则 A 与 I_n 不行等价.

注: 只在有限维的时候可以由 $AB = I_n$ 推出 $AB = BA = I_n$.下面证明这个结论:

命题1.6.5 设 $A \in F^{n \times n}$,则TFAE:

- (1) A 可逆
- (2)齐次方程组 $AX = O$ 只有平凡解
- (3)对于任意 $Y \in F^{n \times 1}$,方程组 $AX = Y$ 有解.

容易证明(1)(2),(1)(3)等价.

推论1.6.5 设 $A, B \in F^{n \times n}$,若 $AB = I_n$,则 A, B 可逆且互为逆矩阵.

证明: 我们去证 $BX = 0$ 只有平凡解, 事实上 $X = ABX = A(BX) = 0$ 从而 B 可逆, 从而 $A = A(BB^{-1}) = (AB)B^{-1} = B^{-1}$

推论1.6.6 设 $A = A_1 \cdots A_k, A_i \in F^{n \times n}$, 则 A 可逆等价于每个 A_i 可逆

证明: 有一边显然, 另一边用反证法即可

命题1.6.6 设 $A \in F^{n \times n}$ (1) 设 $A = (A_1, \cdots, A_n), A_i \in F$, 则 A 可逆等价于 A_1, \cdots, A_n 是 $F^{n \times 1}$ 的一组基. (2) 设

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

则 A 可逆等价于 $\alpha_1, \cdots, \alpha_n$ 是 F^n 的一组基

这个命题可以由以下命题推出:

命题1.6.7 设 V 是 F 上的有限维线性空间, 维数为 $n. S = \{\alpha_1, \cdots, \alpha_n\} \subset V$ 则 S 线性无关等价于 $\text{span} S = V$ (即推出 S 是线性空间 V 的一组基)

证明:

" \Rightarrow ": 记 $W = \text{span} S$, 则 S 是 W 的基 $\Rightarrow \dim W = n \Rightarrow W = V$

" \Leftarrow ": 利用反证法, 即存在不全为 0 的 $c_i \in F$ 使得 $\sum c_i \alpha_i = 0$, 设 $c_{i_0} \neq 0$ 则 $\alpha_{i_0} = -c_{i_0}^{-1} \sum_{i \neq i_0} c_i \alpha_i \in \text{span}\{S - \{\alpha_{i_0}\}\} \Rightarrow S \subset \text{span}\{S - \{\alpha_{i_0}\}\} \Rightarrow \text{span} S \subset \text{span}\{S - \{\alpha_{i_0}\}\} \Rightarrow \text{span}\{S - \{\alpha_{i_0}\}\} = V$.

矛盾!

下回到原命题的证明

证明: (1) A 可逆 $\Leftrightarrow AX = 0$ 只有平凡解. 设

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

则 $AX = \sum_{i=1}^n x_i A_i$

这里用到了所谓的分块矩阵乘法:

分块矩阵乘法: 当做矩阵乘法 AB 时, 将 A 分成了若干块, B 分成了若干块. 则在有意义的情况下进行相乘得到相同的结果.

从而 $AX = 0$ 只有平凡解, 即 $\sum_{i=1}^n x_i A_i$ 能够推出 $x_i = 0. \Leftrightarrow A_1, \cdots, A_n$ 线性无关. 从而得证.

(2) 可对 A^T 使用 (1) 即得. 下由不同的方法证 (2)

由于 A 可逆 $\Leftrightarrow \exists B \in F^{n \times n}$ 满足 $BA = I_n$ 将 A 分块成 $n \times 1$ 的矩阵

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

故

$$BA = \begin{pmatrix} \sum_{r=1}^n B_{1r} \alpha_r \\ \vdots \\ \sum_{r=1}^n B_{nr} \alpha_r \end{pmatrix}$$

从而原命题等价于存在 $B_{ij} \in F$ 使得 $\sum_{j=1}^n B_{ij} \alpha_j = \varepsilon_i \Leftrightarrow \{\varepsilon_i\} \subset \text{span}\{\alpha_1, \dots, \alpha_n\} \Leftrightarrow F^n \subset \text{span}\{\alpha_1, \dots, \alpha_n\} \Leftrightarrow \text{span}\{\alpha_1, \dots, \alpha_n\} = F^n$. 从而 $\{\alpha_1, \dots, \alpha_n\}$ 即证.

第二章 Vector Spaces

2.1 Vector Spaces

2.2 Subspaces

2.3 Bases and Dimension

定理2.3.1 设 $S, T \subset V, \text{span}S = V, T$ 线性无关, 若 $|S| < \infty$, 则 $|T| < \infty$, 且 $|T| \leq |S|$

由此可以推出

推论2.3.1 有限维 V 任意两组基有相同的元素个数($\dim V$)

推论2.3.2 $\dim V = \max_{S \subset V \text{ 无关}} |S| = \min_{\text{span}T=V} |T|$

定理2.3.2 设 $\dim V < \infty, W \subset V$ 是子空间, $S_0 \subset W$ 线性无关, 则 $|S_0| \leq \dim V (< \infty)$ 且存在 W 的基 S , 使得 $S_0 \subset S$

证明: 对此我们先证明一下引理:

引理2.3.1 设 $S \subset V$ 线性无关, $\beta \in V, \beta \notin \text{span}S$, 则 $S \cup \{\beta\}$ 也线性无关.

引理的证明: 只需证对任意有限子集 $T \subset S \cup \{\beta\}, \sum_{i=1}^n c_i \gamma_i = 0$ 推出 $c_i = 0$ 分类讨论即可. 显然成立

下面回到原定理, 前半显然, 下面证明存在 W 的基 S , 使得 $S_0 \subset S$. 即 S_0 能够扩充成子空间的一组基. 由于 $\text{span}S_0 \subset W$, 若 $\text{span}S_0 = W$, 则结论已经成立. 否则, 存在 $\beta_1 \in W - \text{span}S_0$, 由引理, $S_0 \cup \{\beta_1\}$ 线性无关. 若 $\text{span}S_0 \cup \{\beta_1\} = W$, 则存在 β_2 , 等等, 重复以上过程.

由于, 以上过程迟早会结束(最多操作 $\dim V$ 次), 故最后得到一组基, 原命题得证.

一些推论:

推论2.3.3 有限维线性空间的子空间一定存在基, 且子空间的维数不超过全空间的维数.(取 $S_0 = \emptyset$)

推论2.3.4 有限维空间的真子空间, 则真子空间的维数一定严格小于全空间的维数.

证明: 设 S 是 W 的基, $|S| = \dim W$ 由引理, 存在 $\beta \in V - W$, 使得 $S \cup \{\beta\}$ 线性无关则 $1 + \dim W = \dim V$

由此, 也可以得到 $\dim W = \dim V$ 推出 $W = V$

推论2.3.5 $S_0 \subset V$ 线性无关, 则 S_0 可以扩充成 V 的基.

定理2.3.3 设 $W_1, W_2 \subset V$ 是有限维子空间, 则 $W_1 + W_2$ 也是有限维, 且

$$\dim W_1 + \dim W_2 = \dim(W_1 + W_2) + \dim(W_1 \cap W_2)$$

这个定理与和容斥原理具有相同的结构.

证明: 显然 $\dim(W_1 \cap W_2) < \infty$ 取 $W_1 \cap W_2$ 的基 $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$, 并扩充为 W_1 的基 $\{\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \dots, \beta_m\}$, 和 W_2 的基 $\{\alpha_1, \alpha_2, \dots, \alpha_k, \gamma_1, \dots, \gamma_n\}$

断言: $A = \{\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \dots, \beta_m, \gamma_1, \dots, \gamma_n\}$ 是子空间的和的一组基. 这可直接推出要证明的结论.

先验证 $\text{span} A = W_1 + W_2$. 这是两个集合, 为了两个集合相等只需验证等式两端互为包含关系. 这是容易验证的

再验证 A 线性无关, 设 $\sum x_i \alpha_i + \sum y_j \beta_j + \sum z_r \gamma_r = 0$

由于前两个和在 W_1 中, 而后一个和在 W_2 中, 而最后一项也可以看成前两项和的相反数, 所以也在 W_1 中, 从而最后一项在 $W_1 \cap W_2$ 中, 故为 α_i 的线性组合, 从而 $z_r = 0$. 再由剩下项线性无关即可得出 $x_i = 0, y_j = 0$

2.4 Coordinates

定义 2.4.1 设 $\dim V < \infty$, 序列 $(\alpha_1, \alpha_2, \dots, \alpha_n)$ 称为 V 的**有序基**, 如果 $\alpha_1, \dots, \alpha_n$ 互不相同, 且 $\{\alpha_1, \dots, \alpha_n\}$ 是一组基.

无歧义时, 称 $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 为有序基. 有序基的意思就是取了一个基之后排了一个顺序, 避免在选取坐标时取相同的基但是坐标不相同.

命题 2.4.1 设 $\dim V < \infty, \mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 是有序基, 则对任意 $\alpha \in V$ 表为 $\{\alpha_1, \dots, \alpha_n\}$ 的线性组合的方式是唯一的, $\alpha = \sum_{i=1}^n x_i \alpha_i$.

证明是显然的. 根据此命题有

定义 2.4.2 称 x_i 称为 α_i 在有序基下的第 i 个**坐标**, $(x_1, \dots, x_n) \in F^n$ 叫做在 $\{\alpha_1, \dots, \alpha_n\}$ 的坐标, x_i 叫做第 i 个**分量**.

于是, 这实现了 V 到 F^n 的一一对应. 记为

$$\Gamma_{\mathcal{B}}(\alpha) = (x_1, \dots, x_n), \alpha = \sum_{i=1}^n x_i \alpha_i$$

这个映射叫做**坐标映射**. 由基的定义, 容易验证这个映射既是单射又是满射.

容易验证 $\Gamma_{\mathcal{B}}(\alpha + \beta) = \Gamma_{\mathcal{B}}(\alpha) + \Gamma_{\mathcal{B}}(\beta), \Gamma_{\mathcal{B}}(c\alpha) = c\Gamma_{\mathcal{B}}(\alpha)$ (注意两个加法的意义不同)

我们将满足上面两个式子的映射叫做**线性同构映射**, 如果两个线性空间之间有线性同构映射, 我们就称这两个线性空间**同构**

于是, 从线性空间意义下, 从坐标可以得到 V 和 F^n 同构. 于是, 我们得到任意有限线性空间均和某个 F^n 同构. 但我们为什么不直接研究 F^n 呢? 因为, 如果取定了 F^n 则有了某种特殊性, 破坏了对称性. 并且 V 的不依赖于基的选取的性质, 才是更本质的性质. 叫做**内蕴性质**. 这样的性质才更加重要, 而如果取定了 F^n 则破坏了这些性质.

(从此跳入 1.2, 以下内容为讲完 1.2-1.6 之后回到 2.4 的部分)

一般来说, 设 $\dim V = n, \mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 是一组基我们用列向量来表达坐标. 记作

$$[\alpha]_{\mathcal{B}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

(由于一般来说矩阵是一个映射, 而映射写为 $f(x)$ 而不是 $(x)f$, 而对于线性映射 T_1, T_2 来说, 若写为行向量, 则有 $T_1(\alpha) = \alpha A_1, T_2(\alpha) = \alpha A_2, T_1 \circ T_2(\alpha) = \alpha A_1 A_2$. 不符合类似于映射的表达.)

从而, 我们引入一种形式矩阵乘法, 即

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n = (\alpha_1, \cdots, \alpha_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\alpha_1, \cdots, \alpha_n)[\alpha]_{\mathcal{B}}$$

容易验证, 这种乘法也满足乘法结合律. 而引入这种形式矩阵乘法只是为了方便. 我们将 $[\alpha]_{\mathcal{B}}$ 称作坐标矩阵或坐标向量.

上述的 $\Gamma_{\mathcal{B}}$ 的像集也看成列向量.

若取了另一组有序基 $\mathcal{B}' = \{\alpha'_1, \cdots, \alpha'_n\}$, 而 $[\alpha]_{\mathcal{B}'}$ 和 $[\alpha]_{\mathcal{B}}$ 有什么关系呢?

设 $P_j = [\alpha'_j]_{\mathcal{B}} \in F^{n \times 1}$, $P = (P_1, \cdots, P_n) \in F^{n \times n}$

故 $\alpha'_j = (\alpha_1, \cdots, \alpha_n)[\alpha'_j]_{\mathcal{B}} = (\alpha_1, \cdots, \alpha_n)P_j$

从而 $(\alpha'_1, \cdots, \alpha'_n) = ((\alpha_1, \cdots, \alpha_n)P_1, \cdots, (\alpha_1, \cdots, \alpha_n)P_n) = (\alpha_1, \cdots, \alpha_n)P$ 其中最后一个等式由分块矩阵的性质得到的.

从而有关系式 $(\alpha'_1, \cdots, \alpha'_n) = (\alpha_1, \cdots, \alpha_n)P$

命题2.4.2 若 $(\alpha'_1, \cdots, \alpha'_n) = (\alpha_1, \cdots, \alpha_n)P$, 则 P 一定可逆, 并且

$$[\alpha]_{\mathcal{B}} = P[\alpha]_{\mathcal{B}'}$$

或

$$[\alpha]_{\mathcal{B}'} = P^{-1}[\alpha]_{\mathcal{B}}$$

证明:

$(\alpha_1, \cdots, \alpha_n)[\alpha]_{\mathcal{B}} = \alpha = (\alpha'_1, \cdots, \alpha'_n)[\alpha]_{\mathcal{B}'} = (\alpha_1, \cdots, \alpha_n) \cdot P[\alpha]_{\mathcal{B}'}$ 而由于 α_i 线性无关, 从而 $[\alpha]_{\mathcal{B}} = P[\alpha]_{\mathcal{B}'}$

又 α'_j 线性无关, 从而 P_j 是 n 个线性无关的向量, 从而 P 可逆. 将上式同时左乘 P^{-1} 得到 $[\alpha]_{\mathcal{B}'} = P^{-1}[\alpha]_{\mathcal{B}}$

命题2.4.3 设 $\mathcal{B} = \{\alpha_1, \cdots, \alpha_n\}$ 是有序基, $P \in F^{n \times n}$ 设 $(\alpha_1, \cdots, \alpha_n)P = (\alpha'_1, \cdots, \alpha'_n)$, 则 $\{\alpha'_1, \cdots, \alpha'_n\}$ 是基 $\Leftrightarrow P$ 可逆.

证明: 只需证明线性无关即可. 即 $(\alpha'_1, \cdots, \alpha'_n)X = 0 \Rightarrow X = 0 \Leftrightarrow (\alpha_1, \cdots, \alpha_n)PX = 0 \Leftrightarrow "PX = 0 \Rightarrow X = 0"$ 从而 P 可逆.

命题2.4.4 $\mathcal{B} = \{\alpha_1, \cdots, \alpha_n\}$ 是有序基, $P \in F^{n \times n}$ 可逆. 则存在唯一的一组有序基 $\mathcal{B}' = \{\alpha'_1, \cdots, \alpha'_n\}$ 使得 $[\alpha]_{\mathcal{B}} = P[\alpha]_{\mathcal{B}'}$ 和 $[\alpha]_{\mathcal{B}'} = P^{-1}[\alpha]_{\mathcal{B}}$ 对 $\forall \alpha$ 成立.

证明:

存在性由前述易证, 只需证唯一性. 取 $\alpha = \alpha'_j$ 即可.

2.5 Summary of Row-Equivalence

定义2.5.1 设 $A \in F^{m \times n}$, 若

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

$\alpha_i \in F^n$ 称为 A 的行向量. $\text{row}(A) := \text{span}\{\alpha_1, \cdots, \alpha_m\} \subset F^n$, 称为 A 的行空间.

列空间同理定义, 记为 $\text{column}A$

定义 A 的核为 $\ker(A) := \{X \in F^{n \times 1} | AX = 0\}$ 是 $F^{n \times 1}$ 的子空间

命题2.5.1 $\dim \text{row}(A) + \dim \ker(A) = n$

其中, $\dim \text{row}(A)$ 叫做 A 的行秩. 记为 $\text{row-rank}(A)$

事实上, 可以将 $\dim \text{row}(A)$ 看成方程组 $AX = 0$ 约束条件的个数, 而 $\dim \ker(A) = n$ 即是解空间的维数, 大概应该为 $n -$ 约束条件的个数, 所以粗略地看这个命题应该成立.

下面来证明上述命题, 对此我们先引入下述命题

命题 2.5.2 A, B 行等价 $\Leftrightarrow \text{row}(A) = \text{row}(B)$

证明:

" \Rightarrow " $A \sim B \Rightarrow$ 存在 P 可逆, $B = PA. \Rightarrow \beta_i = \sum_j p_{ij} \alpha_j \Rightarrow \text{row}(B) \subset \text{row}(A)$ 同理可得 $\text{row}(B) \subset \text{row}(A)$

另外一边稍后再证.

由于每个矩阵均等价于一个行简化阶梯矩阵, 所以我们只需研究行简化阶梯矩阵的一个性质:

命题 2.5.3 设 $R \in F^{m \times n}$ 是一个行简化阶梯矩阵, 则 R 的非零的行向量构成 $\text{row} R$ 的一组基.

证明: 设

$$R = \begin{pmatrix} \rho_1 \\ \vdots \\ \rho_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

只需证 ρ_i 线性无关, 事实上若 $\sum c_i \rho_i = 0$, 考虑第 k_i 个分量, 是 c_i , 故 $c_i = 0$

原命题成立

回到原命题, 设 $A \sim R, R$ 为行简化阶梯矩阵, 则已证 $\text{row}(A) = \text{row}(R)$ 而又显然 $\ker(A) = \ker(R)$, 再结合 $\dim \text{row}(R) = r$ 为非零行个数, 而 $\dim \ker(R)$ 前面已证为自由变量, 即没有主元的列的个数 $= n - r$

从而

$$\dim \text{row}(A) + \dim \ker(A) = \dim \text{row}(R) + \dim \ker(R) = r + (n - r) = n$$

下面回到上面命题的 " \Leftarrow ". 事实上, 我们有

命题 2.5.4 取定 $m \leq n$, 设 $W \subset F^n$ 是子空间, $\dim W \leq m$, 则存在唯一的行简化阶梯矩阵 $R \in F^{m \times n}$ 使得 $\text{row}(R) = W$

证明:

先证存在性, 取 $\alpha_1, \dots, \alpha_m \in W$ 使得 $\text{span}\{\alpha_1, \dots, \alpha_m\} = W$, 这总是可以取到的, 可以先取基再填零向量.

设

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

设行简化阶梯矩阵 $R \sim A$, 则 $\text{row}(R) = \text{row}(A) = W$, 从而 R 存在

再证唯一性: 设 $R \in F^{m \times n}$ 满足 $\text{row}(R) = W$, 设 R 中主元所在列为 $k_1, \dots, k_r (r \leq m)$, 我们断言: $\{k_1, \dots, k_r\}$ 能够从这个子空间中识别出来, 满足 $\{k_1, \dots, k_r\} = \{1 \leq k \leq n | \exists (a_1, \dots, a_n) \in W, \text{使得 } a_k = 1, a_j = 0 (j < k)\}$. 这个断言利用定义是显然的, 容易证明两边的包含关系.

而如果有两个 R, R' 均满足 $\text{row}(R) = \text{row}(R')$,则由上述命题主元所在列相同.设

$$R = \begin{pmatrix} \rho_1 \\ \vdots \\ \rho_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}, R' = \begin{pmatrix} \rho'_1 \\ \vdots \\ \rho'_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

故 $\rho'_i = \sum_{i=1}^r c_i \rho_i$,考虑 ρ'_i 的第 k_i 个分量满足仅当 $i = i'$ 的时候为1, 否则为0. 而 $\sum_{i=1}^r c_i \rho_i$ 的第 k_i 个分量为 c_i . 从而当 $i = i'$ 时 $c_i = 1$ 否则为0, 从而 $\rho'_i = \rho_i$,故唯一性成立.

从而有如下推论

推论2.5.1 任何一个 $A \in F^{m \times n}$, 存在唯一的行简化阶梯矩阵 $R \sim A$

证明: 存在性在有关方程组的结论中已经证明, 而若 $R, R' \sim A$,则 $\text{row}(R) = \text{row}(A) = \text{row}(R')$,由上述定理知 $R = R'$

再回到 \Leftarrow

证明:

设 $A \sim R, B \sim R', R, R'$ 为行简化阶梯矩阵.故 $\text{row}(R) = \text{row}(A) = \text{row}(B) = \text{row}(R')$ 故 $R = R'$,从而 $A \sim R \sim B$,从而 $A \sim B$

2.6 Computation Concerning Subspaces

设 $\alpha_1, \dots, \alpha_n \in F^n$,有一些问题: 是否线性无关? 生成子空间维数? 一个向量 β 是否在生成的子空间中?

设

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \in F^{m \times n}$$

则 $\alpha_i = (A_{i1}, \dots, A_{in})$

故 $\{\alpha_1, \dots, \alpha_n\}$ 线性无关 $\Leftrightarrow \sum x_i \alpha_i = 0 \Rightarrow x_i = 0 \Leftrightarrow$

$$A^t \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = 0$$

只有平凡解.

从而化为方程组问题.

记 $W = \text{span}\{\alpha_1, \dots, \alpha_n\}$,从而 $\beta \in W \Leftrightarrow$

$$A^t \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \beta^t$$

有解.

设 $A \sim R$ 为行简化阶梯矩阵.则 $\{\alpha_1, \dots, \alpha_m\}$ 线性无关 $\Leftrightarrow R$ 无零行.

事实上, $\{\alpha_1, \dots, \alpha_m\}$ 线性无关 $\Leftrightarrow \dim W = m$, 由上节知, 基为 R 的所有非零行, 故等价于 R 无零行.
 设

$$R = \begin{pmatrix} \rho_1 \\ \vdots \\ \rho_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \rho_i \neq 0$$

则 ρ_1, \dots, ρ_r 为 R 的基, 设 ρ_i 中主元在第 k_i 列, $k_1 < \dots < k_r$, 则 $\beta = (b_1, \dots, b_n) \in W \Leftrightarrow \exists c_1, c_2, \dots, c_r \in F$ 使得 $\beta = \sum_{i=1}^r c_i \rho_i \Leftrightarrow \exists c_1, c_2, \dots, c_r \in F$ 使得 $b_j = \sum_{i=1}^r c_i R_{ij}, \forall j = 1, 2, \dots, n$ 取 $j = k_i$ 知 $b_{k_i} = c_i \Rightarrow b_j = \sum_{i=1}^r b_{k_i} r_{ij}$ 取 $\forall j \in \{1, \dots, n\} - \{k_1, \dots, k_n\}$

而且若 $b_{k_i} = c_i \Rightarrow b_j = \sum_{i=1}^r b_{k_i} r_{ij}$ 取 $\forall j \in \{1, \dots, n\} - \{k_1, \dots, k_n\}$, 则 $\beta = (b_1, \dots, b_n) \in W$ 而由行简化阶梯矩阵的性质知 $\sum_{i=1}^r b_{k_i} r_{ij} = \sum_{1 \leq i \leq r} b_{k_i} r_{ij}$

当 $\beta \in W$ 时, 如何求 x_i 使得 $\beta = \sum_{i=1}^n x_i \alpha_i$? 由上面知道 $\beta = \sum_{i=1}^r b_{k_i} \rho_i = (b_{k_1}, \dots, b_{k_r}, 0, \dots, 0)R = (b_{k_1}, \dots, b_{k_r}, 0, \dots, 0)PA$ 故取 x_i 使得 $(x_1, \dots, x_n) = (b_{k_1}, \dots, b_{k_r}, 0, \dots, 0)P$, 则 $\beta = \sum x_i \alpha_i$ 其中 $x_j = \sum b_{k_i} P_{ij}$ 这样就不用转置就可以找到.

最后我们来讨论如何留下 P 的信息. 即如何找 P , 使得 $R = PA$, 事实上, 我们也可用求逆矩阵相同的方法, 即若 $(A, I) = (R, P)$ 则 $R = PA$ 事实上 $(A, I) = (R, P)$ 则存在 Q 可逆, 使得 $Q(A, I) = (R, P)$, 即 $(QA, Q) = (R, P)$.

第三章 Linear Transformations

3.1 Linear Transformations

定义3.1.1 设 V, W 是 F 线性空间, $T: V \rightarrow W$ 是一个映射, 称为线性映射(也叫线性变换), 如果 $T(c\alpha + \beta) = cT(\alpha) + T(\beta), \forall \alpha, \beta \in V, c \in F$ 即 $T(\alpha)$ 线性依赖于 α .

由定义我们能得到 $T(0_V) = 0_W$ (取 $c = 1, \alpha = \beta = 0$ 即得)

且 T 线性 $\Leftrightarrow T(\alpha + \beta) = T(\alpha) + T(\beta), T(c\alpha) = cT(\alpha)$ 从而得到 $T(\sum c_i \alpha_i) = \sum c_i T(\alpha_i)$

例子: 设 $V = W = F, T: F \rightarrow F$ 满足 $T(x) = ax, a \in F$ 为线性. 而若 $T(x) = x + 1$ 则不是线性.

例子: 设 $V = W, T = \text{id}_V$ 为线性映射, 或 $T(\alpha) = 0$ 均为线性映射

例子: $V = F^{m \times n}, W = F^{p \times q}$ 选定 $A \in F^{p \times m}, B \in F^{n \times q}$ 定义 $T(C) = ACB$ 也为线性映射

上面的例子由两个特殊的情况.

例子: $A \in F^{m \times n}, T: F^{n \times 1} \rightarrow F^{m \times 1} T(X) = AX$ 以及 $A \in F^{m \times n}, U: F^m \rightarrow F^n U(\alpha) = \alpha A$

而反过来我们也有

命题3.1.1 (1) 设 $T: F^{n \times 1} \rightarrow F^{m \times 1}$, 则存在唯一 $A \in F^{m \times n}$ 使得 $T(X) = AX$ (2) 对于行向量由相同的结论

证明: (1) 存在性. 记 $A_i = T(\varepsilon_i)$, 记 $A = (A_1, A_2, \dots, A_n)$ 下面说明 A 满足要求.

则对

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

有 $T(X) = T(\sum_{i=1}^n x_i \varepsilon_i) = \sum_{i=1}^n x_i A_i = AX$

从上面的证明当中也可以看出唯一性, 由于 A 只能为 (A_1, \dots, A_n)

命题3.1.2 设 V, W 是 F 线性空间, 且 $\dim V < \infty, \{\alpha_1, \dots, \alpha_n\}$ 是 V 的有序基, 任取 $\beta_1, \dots, \beta_n \in W$, 则存在唯一的线性映射 $T: V \rightarrow W$ 使得 $T(\alpha_i) = \beta_i$

即线性映射可以在基上任意取值, 但是当基上取定值之后, 其他的值也被相应地确定.

证明: 存在性: 对 $\forall \alpha \in V$ 表示为 $\alpha = \sum_{i=1}^n x_i \alpha_i$ 的方式唯一, 定义 $T(\alpha) = \sum_{i=1}^n x_i \beta_i$ 则 $T: V \rightarrow W$ 是良定的.

为了验证 T 是线性映射, 只需验证 $T(c\alpha + \alpha') = cT(\alpha) + T(\alpha')$, 代入定义的式子是显然的.

唯一性: 若存在 $U: V \rightarrow W$ 也满足 $U(\alpha_i) = \beta_i$, 则

$$U\left(\sum_i (x_i \alpha_i)\right) = \sum_i x_i U(\alpha_i) = \sum_i x_i \beta_i$$

从而 $U = T$ 唯一.

定义3.1.2 定义 $\ker(T) := T^{-1}(0) = \{\alpha \in V | T(\alpha) = 0\}$ 为 T 的核(kernel), 也叫零空间(null-space)

定义 $\text{Im}(T) := \{T\alpha | \alpha \in V\} \subset W$ 叫做 T 的像(image, range)

命题3.1.3 $\ker(T) \subset V$ 是 V 的子空间, $\text{Im}(T) \subset W$ 是 W 的子空间.

证明: 由于 $0 \in \ker T$,故 T 非空, 对 $\forall \alpha_1, \alpha_2 \in \ker(T) \rightarrow T(\alpha_i) = 0$ 而像集显然非空, 并且 $\forall \beta_1, \beta_2 \in \text{Im}(T)$, 则存在 $\alpha_1, \alpha_2 \in V$,使得 $T(\alpha_i) = \beta_i$ 则 $c\beta_1 + \beta_2 = T(c\alpha_1 + \alpha_2)$.

记 $\text{nullity}(T) := \dim \ker(T)$, $\text{rank}(T) = \dim \text{Im}(T)$ 分别叫做**零度**和**秩**

定理3.1.1 若 $\dim V < \infty$,则 $\text{nullity}(T) + \text{rank}(T) = \dim V$

在证明之前先看一个结论

命题3.1.4 T 是单射 $\Leftrightarrow \ker(T) = \{0\}$

T 是满射 $\Leftrightarrow \text{Im}(T) = W$

$T = 0 \Leftrightarrow \text{Im} = \{0\} \Leftrightarrow V$

证明是显然的.

下面回到定理的证明

证明: 取 $\ker(T)$ 的一组基 $\alpha_1, \dots, \alpha_k$,将其扩充为 V 的基 $\alpha_1, \dots, \alpha_n$

从而只需证明 $\text{rank}(T) = n - k$, 对此我们断言 $\{T(\alpha_{k+1}), \dots, T(\alpha_n)\}$ 是像集的基事实上, 由于 $\text{Im}(T) = \{T(\sum_{i=1}^n c_i \alpha_i) | c_i \in F\} = \{ \sum_{i=k+1}^n c_i T(\alpha_i) | c_i \in F\} = \text{span}\{T(\alpha_{k+1}), \dots, T(\alpha_n)\}$ 而显然 $\{T(\alpha_{k+1}), \dots, T(\alpha_n)\}$ 线性无关(否则将推出 $\alpha_1, \dots, \alpha_n$ 线性相关).从而得证.

这个定理用处很大

定理3.1.2 设 $A \in F^{m \times n}$, 则 $\text{row rank}(A) = \text{column rank}(A)$,称为 A 的**秩(rank)**,统一记为 $\text{rank}(A)$

证明:

由于 $\dim \ker(A) + \dim \text{row}(A) = n$, 下面我们说明 $\dim \ker(A) + \dim \text{column}(A) = n$ 取 $T : F^{n \times 1} \rightarrow F^{m \times 1}, T(x) = AX$,则 $\ker(T) = \ker(A)$ 而

$$\text{Im}(T) = \left\{ A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_i \in F \right\} = \left\{ \sum_{i=1}^n x_i A_i \mid x_i \in F \right\} = \text{span}\{A_1, \dots, A_n\} = \text{column}(A)$$

3.2 The Algebra of Linear Transformations

记 $L(V, W) = \{T | T : V \rightarrow W \text{ 是线性映射}\}$, 事实上它也是一个线性空间.

对 $\forall T, U \in L(V, W)$,定义 $(T + U)(\alpha) = T(\alpha) + U(\alpha), \forall \alpha \in V, (cT)(\alpha) := cT(\alpha)$

容易验证所有的性质.

设 $\dim V = m, \dim W = n$ 我们有 $\dim L(V, W) = mn$.

设 $T : V \rightarrow W, U : W \rightarrow Z$ 定义 $U \cdot T(\alpha) = (U(T(\alpha)))$.即 $U \circ T \in L(V, Z)$

可以看成 $L(V, W) \times L(W, Z)$ 到 $L(V, Z)$ 的映射. $(T, U) \rightarrow T \times U$ 这个映射是一个双线性的映射, 即对 T, U 都是线性映射.

若 $V = W = Z$,定义 $L(V) := L(V, V)$,此时, 也叫做**线性算子**.对于 $T \in L(V)$,定义 $T^n = T \times T \dots \times T$ 并定义 $T^0 = I_V$ 为恒同映射.

容易验证满足:

(1) $IT = TI = T$

(2) $U(T_1 + T_2) = UT_1 + UT_2, (T_1 + T_2)U = T_1U + T_2U, c(UT) = (cU)T = U(CT)$

这样, 我们将 $L(V)$ 叫做**F-代数**, 即在一个向量空间中, 每两个向量都可以定义乘法, 并且满足某些性质的向量空间.

比如 $F^{n \times n}$ 也可以看成一个 F -代数

3.3 Isomorphism

下面讨论可逆的线性变换

若 $T \in L(V, W)$ 可逆, 则 T^{-1} 也是线性映射, 此时, 称 T 是**同构(Isomorphism)**, 若存在 $T \in L(V, W)$ 是同构, 则称 V, W 是**同构的(Isomorphic)**.

证明: 对任意 $\beta_1, \beta_2 \in W, c \in F$, 则 $T^{-1}(c\beta_1 + \beta_2) = T^{-1}(cT(T^{-1}(c\beta_1))) + T(T^{-1}(\beta_2)) = T^{-1}(T(cT^{-1}(\beta_1) + T^{-1}(\beta_2)))$

显然同构是一个等价关系, 即 $V \cong V, V \cong W \Rightarrow W \cong V, V \cong W, W \cong Z \Rightarrow V \cong Z$

比如 $\dim V = n, B = \{\alpha_1, \dots, \alpha_n\}$ 是有序基.

$$\Gamma_B : \alpha = \sum_{i=1}^n x_i \alpha_i \rightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

就是一个同构映射

定理3.3.1 设 V, W 是一个有限维的 F -线性空间, 则 $V \cong W \Leftrightarrow \dim V = \dim W$

证明: 设 $\dim V = n, \dim W = m$, 则 $V \cong F^{n \times 1}, W \cong F^{m \times 1}$

故 \Leftarrow 则显然, 对于 \Rightarrow 稍后证明.

例: 对 $A \in F^{m \times n}$, 定义 $L_A \in L(F^{m \times 1}, F^{n \times 1})$ 为 $L_A(X) = AX$

从而有 $F^{m \times n} \cong L(F^{m \times 1}, F^{n \times 1})$

命题3.3.1 设 $\dim V, \dim W < \infty, T \in L(V, W)$, 则 TFAE:

- (1) T 可逆.
- (2) 对任意 V 的基 $S, T(S)$ 是 W 的基, 且 $|T(S)| = |S|$
- (3) 存在 V 的基 $S, T(S)$ 是 W 的基, 且 $|T(S)| = |S|$ 是单射

由此命题可以推出上面定理的 \Rightarrow , 对此, 我们先证明以下两个引理

引理3.3.1 TFAE:

- (1) T 是单射
- (2) 对任意线性无关 $S \subset V, T(S) \subset W$ 也线性无关, 且 $|T(S)| = |S|$
- (3) 存在基 $S \subset V, T(S) \subset W$ 也线性无关, 且 $|T(S)| = |S|$

引理3.3.2 TFAE:

- (1) T 是满射
- (2) 对任意 $S \subset V, \text{span}(S) = V, T(S) \subset W$ 生成全空间
- (3) 存在 $S \subset V, \text{span}(S) = V, T(S) \subset W$ 生成全空间

在假设引理的情况下, 先证原命题

(1) \Rightarrow (2): 由于 T 既是单射又是满射, 由引理, 则 $T(S)$ 线性无关且生成全空间

(2) \Rightarrow (3): 显然

(3) \Rightarrow (1): 由两个引理的(3), 则 T 既单又满, 故得证

先证第一个引理

证明:

(1) \Rightarrow (2), 设 $S = \{\alpha_1, \dots, \alpha_k\}$, 若 $\sum c_i T(\alpha_i) = 0 \Rightarrow c_i = 0$

(2) \Rightarrow (3), 任取一组基即可

(3) \Rightarrow (1), 设 $S = \{\alpha_1, \dots, \alpha_n\}$ 是基, 满足 $T(\alpha_1), \dots, T(\alpha_n)$ 线性无关, 故只需证 $\ker(T) = 0$ 任取 $\alpha \in \ker(T)$, 设 $\alpha = \sum c_i \alpha_i$, 故 $0 = T(\alpha) = T(\sum c_i \alpha_i) = \sum c_i T(\alpha_i)$ 由于 $|T(S)| = |S|$ 故它们互不相同, 从而 $c_i = 0, \alpha = 0$

再证第二个引理

证明:

(1) \Rightarrow (2), $\forall \beta \in W$, 下面证明 β 能写成 $T(S)$ 中有限个线性组合. 由于 $\exists \alpha \in V$ 使得 $T(\alpha) = \beta$ 设 $\alpha = \sum c_i \alpha_i, \alpha_i \in S$, 从而 $\beta = T(\alpha) = \sum c_i T(\alpha_i) \in \text{span}(T(S))$

(2) \Rightarrow (3), 显然

(3) \Rightarrow (1), $S \subset V$, 从而 $T(S) \subset T(V) = \text{Im}(T)$, 于是 $\text{span}T(S) \subset \text{Im}(T)$ 又由于 $\text{span}(S) = V$, 从而 $\text{Im} = W$, 从而 T 是满射

命题3.3.2 设 $\dim V = \dim W < \infty$, 则TFAE:(1) T 单, (2) T 满, (3) T 可逆

证明: 取 V 的基 $\{\alpha_1, \dots, \alpha_n\}$ 从而 T 单 $\Leftrightarrow \{T(\alpha_1), \dots, T(\alpha_n)\} = W \Leftrightarrow T$ 满

另证: 由于 $\dim \ker(T) + \dim \text{Im}(T) = n$ 从而, T 是单射 $\Leftrightarrow \dim \ker(T) = 0 \Leftrightarrow \text{Im}(T) = n \Leftrightarrow T$ 是满射

定义 $GL(V) := \{T \in L(V) | T\}$ 可逆, 由于可逆映射的加法不一定可逆, 所以不是线性空间, 只能说 $GL(V)$ 在映射的复合运算下构成一个群, 叫做 V 上面的一般线性群(**general linear group**).

定义3.3.1 设集合 G 上给定了运算 $G \times G \rightarrow G, (x, y) \rightarrow xy$ (乘法)满足:

(1) $(xy)z = x(yz)$

(2) 存在唯一 $e \in G$, 使得 $ex = xe = x \forall x \in G$

(3) $\forall x \in G$ 存在唯一 $x^{-1} \in G$ 使得 $xx^{-1} = x^{-1}x = e$

我们称 G 构成一个群

例如, 所有可逆矩阵构成一个群, 叫做矩阵的一般线性群, 而以后可以用一个量来刻画 T 是否可逆, 就是 T 的行列式 $\det(T)$

设 F 是一个域, 我们只考虑 F 中的加法, 我们把域中的加法称为群里面的乘法, 所以一个域在域的加法上面构成一个群(加法群)

乘法满足交换律的群称作**交换群**, 也叫**Abel 群**, 在提到的加法群, 也就是交换群, 因为现在数学当中所有称为加法的运算都是满足交换律的.

另一方面, 考虑 $F - \{0\}$ 对于乘法也构成一个交换群. 对于域上的线性空间中向量的加法也构成一个群.

3.4 Representation of Transformations by Matrices

设 $\dim V = n, B = \{\alpha_1, \dots, \alpha_n\}$ 是有序基. 则有一个线性同构映射:

$$\Gamma_B : \alpha = \sum_{i=1}^n x_i \alpha_i \rightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

设 $\dim W = m, B' = \{\beta_1, \dots, \beta_m\}$ 也有线性同构的坐标映射

于是有 $\Gamma_{B'} \circ T \circ \Gamma_B^{-1}$, 称为 A 关于 B, B' 的矩阵

有由于存在唯一的 $A \in F^{m \times n}$ 使得 $L(A) = AX$, 即 $L_A = \Gamma_{B'} \circ T \circ \Gamma_B^{-1}$ 将 A 叫做 T 关于 B 和 B' 的矩阵, 记作 $[T]_{B, B'}$.

而 $L_A = \Gamma_{B'} \circ T \circ \Gamma_B^{-1} \Leftrightarrow L_A \circ \Gamma_B = \Gamma_{B'} \circ T \Leftrightarrow L_A(\Gamma_B(\alpha)) = \Gamma_{B'}(T(\alpha)) \Leftrightarrow A[\alpha]_B = [T(\alpha)]_{B'}$ 考虑映射 $L(V, W) \rightarrow F^{m \times n} : T \mapsto [T]_{B, B'}$ 设 $A = [T]_{B, B'}, B = [U]_{B, B'}$ 故 $\Gamma_{B'}(CT + U) = c\Gamma \circ T + \Gamma_{B'} \circ U = cL_A \circ \Gamma_B + L_B \circ \Gamma_B = (cL_A + L_B) \circ \Gamma_B = L_{CA+B} \circ \Gamma_B$

再证是单射: $\ker = 0$, 若 $T \mapsto 0$ 则 $[T\alpha]_{B'} = 0 \Rightarrow T\alpha = 0, \forall \alpha \Rightarrow T = 0$ 同理可以证明是满射, 从而 $\dim L(V, W) = mn$, 且

$$[T\alpha]_{B'} = A[\alpha]_B$$

从而可以从矩阵的基得到 T 的一组基

利用图表分析比较形象, 得到映射的图表是可交换的

从而有

考虑映射 $L(V, W) \rightarrow F^{n \times n}, T \mapsto [T]_{B, B'}$

若取 $U = W, B = B'$, 于是有 $[T\alpha]_B = [T]_B[\alpha]_B$

例子: $V = F^{n \times 1} = W, B, B'$ 为标准基, 看映射图表, 从而两个坐标映射就是恒同映射, 从而 $T = L_A$, 意味着 $[L_A]_{B, B'} = A$.

例子: $V = W = F^2, T(x_1, x_2) = (ax_1 + bx_2, cx_1 + dx_2)$, 其中 $a, b, c, d \in F$ 取 $B = \{\varepsilon_1, \varepsilon_2\}$ 则

$$[T]_B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

从而若 $\alpha = (x_1, x_2), [\alpha]_B = (x_1, x_2)^t$, 从而有

$$\begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

下面考虑映射复合的矩阵, 有三个空间 U, W, Z 两个线性映射 $T: V \rightarrow W, U: W \rightarrow Z$ 取有序基 B, B', B'' , 对此我们有

$$[U \circ T]_{B, B''} = [U]_{B', B''} [T]_{B, B'}$$

事实上, 记 $A = [T]_{B, B'}, B = [U]_{B', B''}$, 仍然从映射图表来看, 只需取 $[U \circ T]_{B, B''} = L_B \circ L_A$ 即可而由矩阵乘法结合律, $L_B \circ L_A = L_{BA}$, 从而得证.

而也可以由上述式子来定义矩阵的乘法, 从而, 由于 $L_{(AB)C} = L_{A(BC)}$ (映射的结合律), 从而也可以直接得到矩阵乘法的结合律 $(AB)C = A(BC)$, 也说明了矩阵的乘法实际上对应着映射的复合.

回到考虑只有一个空间的情况.

若 $T, U \in L(V) \Rightarrow [U \circ T]_B = [U]_B [T]_B$, 由于线性映射空间和方阵空间均为 F -代数, 故可以理解为取 F -代数和矩阵乘法的交换性, 也就是说这两个空间是 F -代数的同构: $[T] \mapsto [T]_B$ (即加上映射之间的乘法也是一回事, 有关线性映射的所有东西都可以看成矩阵上面的运算, 也就是说矩阵描述出了线性映射的所有东西, 只要取了基, 就可以将线性映射看成同构)

而关于 F -代数的同构, 也可以得到 $id \mapsto I_n$, 也可以得到 T 可逆 $\Leftrightarrow [T]_B$ 可逆, 且 $[T^{-1}]_B = [T]_B^{-1}$

但是由于矩阵依赖于基的选取, 对 $T \in L(V)$, 取两个有序基 B, B' , 则 $[T]_B, [T]_{B'}$ 也不是不同的矩阵, 但是我们由 $[T]_B$ 和 $[T]_{B'}$ 相似

仍然从映射图表可以看出存在一个唯一的矩阵 $P \in GL_n(F)$ 使得映射图表可以交换, 做大的矩阵图表, 得到下面的圈也可交换, 从而意味着

$$L_{[T]_{B'}} \circ L_P = L_P \circ L_{[T]_B} \Rightarrow L_{[T]_B P} = L_{P [T]_{B'}} \Rightarrow [T]_B P = P [T]_{B'}$$

从而 $[T]_{B'} = P^{-1} [T]_B P$

下面说明事实上 P 就是坐标变换的过渡矩阵, 事实上, 由于三角形的映射图表可交换. 设 $B = \{\alpha_1, \dots, \alpha_n\}, B' = \{\alpha'_1, \dots, \alpha'_n\}$ 从而有 $(\alpha'_1, \dots, \alpha'_n) = (\alpha_1, \dots, \alpha_n)P$

定义 3.4.1 称 $A, B \in F^{n \times n}$ 相似, 如果存在 $P \in GL_n(F)$ 使得 $B = P^{-1}AP$, 记作 $A \sim B$

容易验证相似是一种等价关系, 考虑 A 的相似等价类: $= \{B \in F^{n \times n} | B \sim A\}$

故在上面提到的映射中取遍所有有序基时, 下面说明所有的矩阵构成一个相似等价类.

事实上, 由定义, 显然每个矩阵都相似, 而反过来, 对于每个 $C \sim [T]_B$, 下面证明存在 B' 使得 $[T]_{B'} = C$ 事实上, 将 B' 取为 C 所对应的矩阵 P 即可. 于是我们得到

$$\{[T]_B | B \text{ 是 } V \text{ 的有序基}\}$$

是一个相似等价类.

而线性代数的意义就在于如果看线性映射不容易看出性质, 但我们可以取一组基使得矩阵充分的简单, 也就是说先任取一个有序基 B , 得到一个矩阵 $[T]_B$, 所以这个问题转化成了找一个与 $[T]_B$ 相似的矩阵有多简单.

再回到两个空间的情况, $TU \rightarrow W, V$ 的基 $B = \{\alpha_1, \dots, \alpha_n\}, B' = \{\beta_1, \dots, \beta_m\}$ 从而有 $[T\alpha]'_B = A[\alpha]_B$

而 $\alpha = (\alpha_1, \dots, \alpha_n)[\alpha]_B, [T\alpha] = (\beta_1, \dots, \beta_m) = [T\alpha]'_B = (\beta_1, \dots, \beta_m)A[\alpha]_B$

又 $T\alpha = (T\alpha_1, \dots, T\alpha_n)[\alpha]_B$ 因此对任意 $\alpha, (T\alpha_1, \dots, T\alpha_n)[\alpha]_B = (\beta_1, \dots, \beta_m)A[\alpha]_B$ 故 $(T\alpha_1, \dots, T\alpha_n) = (\beta_1, \dots, \beta_m)A$, 即 $T\alpha_j = \sum A_{ij}\beta_i, 1 \leq j \leq n$

3.5 Linear Function

一般线性映射指的是 $L(V, W)$, 而若 $W = F$, 则称作线性函数. 记 $V^* = L(V, F)$ 为所有线性函数的集合.

若 $\dim V < \infty$, 由 $\dim F = 1$ 知 $\dim V^* = \dim V$, 若 $\dim V = \infty$, 则 $\dim V^* > \dim V$

例子: 考虑集合 $\{x_1, x_2, \dots\} | x_i$ 只有有限项 $\neq 0$ 则 $\dim V = |\mathbb{N}|$, 记 $W = \{(y_1, y_2, \dots)\}$, 则 $\dim W = |\mathbb{R}|$

定义对 $\alpha \in W$ 定义 $f_\alpha(x_1, \dots, x_n) := \sum_{i=1}^{\infty} x_i y_i$

而考虑 $W \rightarrow V^*$ 是一个单射, 故 $|V^*| \geq |W| > |V|$

取 $B = \{\alpha_1, \dots, \alpha_n\}$ 是 V 的有序基, 则存在唯一 $f_i \in V^*$ 使得 $f_i(\alpha_j) = \delta_{ij}$, 容易验证 f_1, \dots, f_n 是 V^* 的基, 称作 B 的对偶基.

推论3.5.1 对 $\forall f \in V^*$, 存在 $c_1, \dots, c_n \in F$ 使得 $f = \sum_{i=1}^n c_i f_i$

下面求出推论中的 c_i , 即说明 $f = \sum_{i=1}^n f(\alpha_i) f_i$, 事实上考虑 $f(\alpha_i)$ 即可. 于是, 对任意 $\alpha = \sum f_i(\alpha) \alpha_i$, 并且有

$$[\alpha]_B = \begin{pmatrix} f_1(\alpha) \\ \vdots \\ f_n(\alpha) \end{pmatrix}$$

例子: $V = F^n, B = \{\varepsilon_1, \dots, \varepsilon_n\}, f_i$ 满足 $f_i(x_1, \dots, x_n) = x_i$ 对任意 $f \in V^*$ 设 $a_i = \sum f(\varepsilon_i)$, 则 $f = \sum a_i f_i$ 即 $f(x_1, \dots, x_n) = \sum a_i x_i$

一般情况: $\alpha = \sum x_i \alpha_i \Rightarrow f_i(\alpha) = x_i$, 对 $\forall f \in V^*$, 设 $a_i = f(\alpha_i)$ 则 $f = \sum a_i f_i \Rightarrow f(\alpha) = \sum a_i x_i$

例子: $V = F^{n \times n}$ 定义 $\text{tr} \in (F^{n \times n})^*$ 为 $\text{tr}(A) = \sum_{i=1}^n A_{ii}$ 称为迹(trace)

例子: 任取集合 S , 定义 $V = F^S = \{f : S \rightarrow F\}$, 对 $s \in S$, 定义 $L_s(f) := f(s), \forall f \in V$ 为 s 点处的取值函数. 由维数公式可以直接得到, 若 $f \in V^* - \{0\}$, 则 $\dim(f) = n - 1$.

若 $W \subset V, \dim W = \dim V - 1$, 则称 W 为 V 中的超平面(hyperplane), 我们称 $\dim V - \dim W$ 为余维数, 也就是说如果余维数为1, 则为超平面.

定义3.5.1 设 $S \subset V, S^0 := \{f \in V^* | f(\alpha) = 0, \alpha \in S\} \subset V^*$ 称为 S 在 V^* 中的零化子空间(annihilator), 有时记作 S^\perp

由定义 $S^0 = \{f \in V^* | S \subset \ker(f)\} = \{f \in V^* | f(S) = \{0\}\}$

下面证明, 对于任意集合 S , 都有 S^0 是子空间, 事实上, 由于 $S \neq \emptyset$ 且 $f, g \in S^0 \Rightarrow cf + g \in S^0$

若 $S = \{0\} \Rightarrow S^0 = V^*$, 此处不约定 $S^0(\emptyset)$, 若 $S = V$, 则 $S^0 = \{0\}$, 且若 $S_1 \subset S_2 \subset V \Rightarrow S_2^0 \subset S_1^0$

由线性映射的定义容易得到 $S^0 = (\text{span} S)^0$

定理3.5.1 $\dim V < \infty$ 是线性空间, $W \subset V$ 是子空间, 则 $\dim W + \dim W^0 = \dim V$

证明:

取 W 的基 $\{\alpha_1, \dots, \alpha_k\}$,并扩充为 V 的基, $B = \{\alpha_1, \dots, \alpha_n\}$, 设 $B^* = \{f_1, \dots, f_n\} \subset V^*$ 断言: $\{f_{k+1}, \dots, f_n\}$ 是 W_0 的基.

先证明 $i \geq k + 1$ 时, $f_i \in W^0$, 事实上, 此时有 $f_i(\alpha_1) = \dots = f_i(\alpha_k) = 0$ 从而 $f_i \in \{\alpha_1, \dots, \alpha_k\}^0 = W^0$ 而它们显然线性无关, 下面证明 $\text{span} = W^0$, 事实上 $f = \sum_{i=1}^n f(\alpha_i)f_i = \sum_{i=k+1}^n f(\alpha_i)f_i \in \text{span}$ 由此即证

设 $A \in F^{n \times n}$, 以前有过证明 $\dim \text{row}(A) + \dim \ker(A) = n$, 以前利用矩阵的初等行变换证明过这个结论, 而事实上, 取 $V = F^n$, 则 $F^{n \times 1} \cong V^*$: $\forall x \in F^{n \times 1}$, 定义 $f_x \in V^*$ 为 $f_x(\alpha) = \alpha X$ 下面证明 $F^{n \times 1} \rightarrow (F^n)^*$, $x \mapsto f_x$ 是同构映射.

对 $X \in F^{n \times 1}$, $X \in \ker(A) \Leftrightarrow \alpha_1 X = \dots = \alpha_n X = 0 \Leftrightarrow f_x(\alpha_i) = 0 (1 \leq i \leq n) \Leftrightarrow f_x = \{\alpha_1, \dots, \alpha_n\}^0 = \text{row}(A)^0$

特别地, $\dim \ker A = \dim \text{row}(A)^0 = n - \dim \text{row}(A)$, 于是我们不用初等行变换就证明了矩阵的行秩等于列秩, 这种证明是一种conceptual proof.

推论3.5.2 设 $W \in V$ 是子空间, $\dim V = n, \dim W = k$ 则存在 $f_1, \dots, f_{n-k} \in V^*$ 使得

$$W = \bigcap_{i=1}^{n-k} \ker(f_i)$$

特别地, 若 W 是超平面, 则存在 $f \in V - \{0\}$ 使得 $W \in \ker(f)$

证明: 下面证明

$$W = \bigcap_{i=k+1}^n \ker(f_i)$$

其中 f_i 与上述定理证明当中的定义相同. 而这是显然的.

推论3.5.3 设 $W_1, W_2 \subset V$ 是两个子空间, 如果 $W_1^0 = W_2^0$, 则 $W_1 = W_2$

也就是说, 通过取零化子空间没有失去原来子空间的信息, 能够从零化子空间中识别出原来的子空间

证明: 反证法, 如果存在 α , 使得 $\alpha \in W_2, \alpha \notin W_1$ 由前面的推论, 存在 f_1, \dots, f_{n-k} 使得 $W = \bigcap_{i=1}^{n-k} \ker(f_i) \Rightarrow f_i \in W_1^0$ 从而 $f_i(W) = 0$ 故 $\alpha \notin W_1 \Rightarrow \exists i_0$ 使得 $f_{i_0}(\alpha) \neq 0 \Rightarrow f_{i_0} \notin W_2^0$, 从而 $W_1^0 \neq W_2^0$ 从而导致矛盾!

3.6 The Double Dual

这节我们来研究 $(V^*)^*$, 即 $(V^*)^* \cong V$

下面找一个 $V \rightarrow (V^*)^*$ 的同构映射: 对 $\alpha \in V$, 定义 $L_\alpha \in (V^*)^*$ 为 $L_\alpha(f) = f(\alpha)$ 为在 α 处的取值函数.

命题3.6.1 若 $\dim V < \infty$, 则这是一个线性同构映射

证明:

线性 $L_{c\alpha + \beta} = cL_\alpha + L_\beta$, 事实上, 对任意 $f, L_{c\alpha + \beta} := f(c\alpha + \beta) = cf(\alpha) + f(\beta) = (cL_\alpha + L_\beta)(f)$

单射: 设 $L_\alpha = 0$, 即 $L_\alpha(f) = 0, \forall f \in V^* \Rightarrow \alpha = 0$ (若 $\alpha \neq 0$, 则存在基 $\{\alpha_1, \dots, \alpha_n\}$ 使得 $\alpha_1 = \alpha$, 取对偶基, 故 $f_1(\alpha) \neq 0$, 矛盾)

事实上, 上面的证明不依赖有限维.

还可以利用存在 f_i 使得 $\{0\} = \bigcup_{i=1}^n \ker(f_i)$

满射: 由于空间是有限维, 则 $\dim V^{**} = \dim V^* = \dim V$, 故又由于为单射, 从而为满射.

推论3.6.1 对任意的 V^* 的基 f_1, \dots, f_n 存在唯一的 V 的基, 使得 $f_i(\alpha_j) = \delta_{ij}$, 也就是说 V^* 的任意基都是对偶基

证明:

取 $\{f_1, \dots, f_n\}$ 在 V^{**} 中的对偶基 $\{L_1, \dots, L_n\}$ 满足 $L_i(f_j) = \delta_{ij}$ 存在 $\alpha_i \in V$ 使得 $L_i = L_{\alpha_i}$,从而 $L_i(f_j) = L_{\alpha_i}(f_j) = f_j(\alpha_i)$ 而唯一性在于 L_i 与 α_i 均唯一

对此, $\alpha_1, \dots, \alpha_n$ 也是 f_1, \dots, f_n 在 V 中的对偶基.

对 $S \in V, S^0 \in V^*$, 记 $E_1 \subset V^*$, 则 $E_1^0 = \{L \in V^{**} | L(f) = 0, \forall f \in E\}$ 而上式为 $\{L_\alpha \in V^{**} | L_\alpha(f) = f(\alpha) = 0, \forall f \in E\} \cong \bigcap_{f \in E} \ker f$,

由此, 则有 $(S^0)^0 = \text{span}S$ (严格来说应该为 \cong), 特别地, 若 S 是子空间, 则有 $(S^0)^0 = S$

定理3.6.1 $\dim V < \infty, S \subset V$, 则 $(S^0)^0 = \text{span}S$

证明:

特别地, 若 $W \subset V$ 是子空间, 则 $(W^0)^0 = (\cong)W$

对于一个矩阵 $A, \ker A$ 为 $AX = 0$ 为解空间, 而若 $\text{row}(A_1) = \text{row}(A_2)$, 则 $\ker(A_1) = \ker(A_2)$, 而下面证明若 $\ker(A_1) = \ker(A_2)$, 则 $\text{row}(A_1) = \text{row}(A_2)$.

事实上, 取 $V = F^n, V^* \cong F^{n \times 1}$, 这样的意义下, 则 $\ker(A) = \text{row}(A)^0$, 从而, 由于 $\ker(A_1) = \text{row}(A_1)^0, \ker(A_2) = \text{row}(A_2)^0$, 从而 $\text{row}(A_1) = \text{row}(A_2)$

设 V_1, V_2 是两个有限维的向量空间, 一个二元函数 $\phi : V_1 \times V_2 \rightarrow F$, 称为**双线性函数(bilinear function)**, 如果取定一个变量后另一个变量是线性的.

例如, 考虑 $\varphi : V \times V^* \rightarrow F : \varphi(\alpha, f) \mapsto f(\alpha)$, 或者 $\varphi : F^n \times F^{n \times 1} \rightarrow F : \varphi(\alpha, X) \mapsto \alpha X$

我们说, 这两个例子满足某种**非退化**的性质, 即对 $\forall \alpha \neq 0 \in V_1, \exists \beta \in V_2$ 使得 $\varphi(\alpha, \beta) \neq 0$, 对于 $\beta \neq 0 \in V_2$ 也有类似的性质.

我们称非退化的双线性函数为 V_1, V_2 之间的一个**配对(pairing)**, 若 $\dim V_1, \dim V_2 < \infty$, 断言: 如果存在非退化的 V_1 和 V_2 的配对, 则 $\dim V_1 = \dim V_2$

证明:

考虑 $\sigma : V_1 \rightarrow V_2^* : \sigma(\alpha)(\beta) = \varphi(\alpha, \beta)$. 由于 $\forall \alpha \neq 0 \in V_1, \exists \beta \in V_2$, 故 σ 为单射, 从而 $\dim V_1 \leq \dim V_2$.

类似地, 有映射 τ , 从而 $\dim V_2 \leq \dim V_1$, 于是 $\dim V_1 = \dim V_2$

而反过来得到 σ, τ 都是线性同构, 于是通过这个线性同构 $V_1 \cong V_2^*$ 可看成一回事, 另外一个同理, 于是, 从这个方面也可看出 V, V^{**} 也是一回事. 对于配对, 我们也可以记 $\langle \alpha, \beta \rangle = \varphi(\alpha, \beta)$, 于是 $f(\alpha)$ 也可以写成 $\langle f, \alpha \rangle, \langle \alpha, f \rangle$

下面讨论一些无限维的情形, 首先, 我们引入商空间.

定义3.6.1 对于一个线性空间 $V, W \subset V$ 是子空间, 定义 $V/W := \{\alpha + W | \alpha \in V\}$, 其中 $\alpha + W := \{\alpha + \beta | \beta \in W\}$. 每个 $\alpha + W$ 叫做 V 的一个**仿射子空间**, 也叫做一个 **W 的陪集**.

由于 $\alpha_1 + W = \alpha_2 + W \Leftrightarrow \alpha_1 - \alpha_2 \in W$, 且不同的陪集不相交, 于是, 定义 $\alpha_1 \equiv \alpha_2 \pmod{W} \Leftrightarrow \alpha_1 - \alpha_2 \in W$ 是一个等价关系, 并且每个等价类恰好是一个陪集, 于是 V/W , 也可以看成一个等价类的集合.

我们在这些陪集上定义向量加法和纯量乘法: 定义 $(\alpha + W) + (\beta + W) = (\alpha + \beta) + W, c(\alpha + W) = c\alpha + W$. 首先, 需要验证, 这种定义是良定的. 这个由向量空间的定义是显然的. 事实上, 如果 $\alpha_1 + W = \alpha + W, \beta_1 + W = \beta + W$, 那么, 容易得到 $(\alpha_1 + \beta_1) + W = (\alpha + \beta) + W$

于是, 这样这些等价类也构成一个线性空间, 称作**商空间**. 这个空间内的零向量为 W 自己. 从而, 我们有映射 $Q : V \rightarrow V/W$, 是一个线性映射. 称作**商映射**. 是一个线性映射, 并且是满射. $\ker(Q) = W$

于是, 得到

$$\dim(V/W) = \dim V - \dim W$$

命题3.6.2 设 $f \in L(V, Z), W \subset V$ 是子空间, 假设 $W \subset \ker(f)$, 则存在唯一的线性映射 $T' \in L(V/W, Z)$, 使得图表可交换. 即 $T' \circ Q = f$

反之, 如果存在 T' 使它可交换, 则必须有 $W \subset \ker(f)$, 这个命题即说明反过来也成立.

证明: 先证唯一性,如果存在 T' 使得 $T' \circ Q = T \Rightarrow T'(\alpha + W) = T(\alpha)\alpha \in V$,从而, 如果存在, 显然唯一.

再证明存在性: 下面证明: 由 $T'(\alpha + W) = T(\alpha)$ 确实满足条件.只需证明良定.不同的 α 可以定义相同的 $\alpha + W$,故只有在此时 $T(\alpha)$ 也相同才可以定义, 而由于 $W \subset \ker(T)$, 从而成立.

对于上述命题, 此时 $\ker(T') = \ker(T)/W, \text{Im}(T') = \text{Im}(T)$,特别地, 若 $W = \ker(T)$ 且 T 是满射, 从而 T' 是同构映射, 也就说明了若是满射, 则有

$$V / \ker(T) \cong Z$$

一般来说, 有

$$V / \ker(T) \cong \text{Im}(T)$$

证明:

$\alpha + W \in \ker(T) \Leftrightarrow T'(\alpha + W) = 0 \Leftrightarrow \alpha \in \ker(T) \Leftrightarrow \alpha + W \in \ker(T)/W$ 另外一个同理.

下面回到关于无限维线性空间的讨论, 对 $N \subset V$,下面两个叙述等价:

(1) N 是 V 的极大真子空间(N 是真子空间, 并且对子空间 $W \subset V$,若 $N \subset W$,则 $W = N$ 或 V)

(2) $\dim V/W = 1$

如果这两条成立, 我们称 N 是 V 的超平面. 如果 V 有限维, (2) 就是超平面的定义

证明: 考虑映射 $\{V$ 的所有的包含 V 的子空间 $\} \rightarrow \{V/N$ 子空间 $: W \mapsto W/N$ 我们说这是一个一一对应.

首先说明是单射: 若 $N \subset W_1, W_2, W_1/N = W_2/N$ 下面证明 $W_1 = W_2$

对 $\forall \alpha \in W_1, \alpha + N \in W_1/N = W_2/N \Rightarrow \exists \beta \in W_2$ 使得 $\alpha + N = \beta + N \Rightarrow \alpha - \beta \in N \subset W_2 \Rightarrow \alpha = (\alpha - \beta) + \beta \in W_2$,从而 $W_1 \subset W_2$,同理 $W_2 \subset W_1$,从而 $W_1 = W_2$ 是单射.

而下面说明是满射, 对 $\forall U \subset V/N$,考虑商映射 $V \rightarrow V/N$, 下面说明 $Q^{-1}(U) := \{\alpha \in V | Q(\alpha) \in U\}$ 是 V 的包含 W 的子空间, 并且 $Q^{-1}(U) \mapsto U$,这是显然的.

回到原命题, 由于这两个之间有一一对应, 故 V/N 恰有两个元素.故 $\dim(V/N) = 1$.从而原命题得证.

命题3.6.3 (1) 设 $0 \neq f \in V^*$ 则 $\ker(f)$ 是超平面

(2) 若 N 是超平面, 则存在 $f \in V^*$ 使得 $N = \ker(f)$

证明: (1) $f \neq 0 \Rightarrow \text{Im}(f) = F \Rightarrow V / \ker(f) \cong F \Rightarrow V / \ker(f) = \dim F = 1$

(2) $\dim V/N = 1 \cong V/N \cong F$, 即存在同构 $i : V/N \rightarrow F$,又 V 到 V/N 有商映射 Q ,取 $f = i \circ Q$,故 $\ker(f) = \ker(Q) = N$

设 $N, W \subset V^*$,且 $\dim W, N < \infty$,是否有 $W^0 \subset N^0 \Rightarrow N \subset W$,其中, 这里 W^0 指 $\bigcap_{f \in W} \ker(f)$?

命题3.6.4 设 $V, W \subset V^*$ 是有限维子空间, 则 $N \subset W \Leftrightarrow \bigcap_{f \in W} \ker(f) \subset \bigcap_{f \in N} \ker(f)$

证明: 只需证" \Leftarrow "取 W 的基 $\{f_1, \dots, f_r\}$, 可以推出这个命题和下面的命题是一样的

命题3.6.5 设 $g, f_1, \dots, f_r \in V^*$ 则 $g \in \text{span}\{f_1, \dots, f_r\} \Leftarrow \bigcap \ker(f_i) \subset \ker(g)$

只需证" \Leftarrow ".再看下面命题

命题3.6.6 设 $\dim V < \infty, E \subset V^*$ 是子集, 若 $\bigcap_{f \in E} \ker(f) = \{0\}$,则 $\text{span} E = V^*$

证明:

由于 $\text{span}(E) = (E^0)^0 \subset V^{**} = \{0\}^0 = V$

回到上述命题, 记 $W = \bigcap \ker(f_i)$,考虑商空间 V/W ,断言: $\dim V/W < \infty$

考虑映射 $T : V \rightarrow F^r$,定义 $T(\alpha) = (f_1(\alpha), \dots, f_r(\alpha))$, 显然是线性映射.而 $\ker(T) = W \Rightarrow$ 存在 T' 是单射, 满足 $\text{Im}(T') = \text{Im}(T)$ 满足 T' 是单射. $V/W \cong \text{Im}(T')$ 为有限维. (照片)

存在 $G, F_1, \dots, F_r \in (V/W)^*$ 使得 $g = G \circ Q, f_i = F_i \circ Q$, 其中 $Q: V \rightarrow V/W$ 为商映射(这些 G, F_i 就是 T'). 断言:

$$\bigcap_{i=1}^r \ker(F_i) = \{0\} (\{0\} = \{W\})$$

设 $\alpha + W \in \bigcap_{i=1}^r \ker(F_i)$, 故 $F_i(\alpha + W) = 0 = F_i(Q(\alpha)) = f_i(\alpha)$, 故 $\alpha \in \bigcap \ker(f_i) = W$, 故 $\alpha \in W$, 从而 $\alpha + W = W$. 从而成立

在第三个命题当中, 取 $E = \{F_1, \dots, F_r\}$, 从而推出 $\text{span}\{F_1, \dots, F_r\} = (V/W)^*$, 特别地, $G = \sum c_i F_i$ 故 $G \circ Q = (\sum c_i F_i) \circ Q$ 从而得到结论

3.7 The Transpose of a Linear Transformation

设 $T \in L(V, W)$, 则存在 $T^t \in L(W^*, V^*)$, 满足 $T^t(g) = g \circ T, T^t(g)(\alpha) = g(T\alpha)$

首先, T^t 是线性映射. 即 $T^t(cg_1 + g_2) = cT^t(g_1) + T^t(g_2)$, 而 $T^t(cg_1 + g_2) = (cg_1 + g_2)(T\alpha) = cg_1(T\alpha) + g_2(\alpha) = cT^t(g_1)(\alpha) + T^t(g_2)(\alpha) = (cT^t(g_1) + T^t(g_2))(\alpha)$

这种映射称为 T 的转置映射或伴随变换.

设 $T: V \rightarrow W, U: W \rightarrow Z$, 则有 $U^t: Z^* \rightarrow W^*, T^t: W^* \rightarrow V^*$, 则 $(U \circ T)^t = g \circ (U \circ T) = (g \circ U) \circ T = U^t(g) \circ T = T^t(U^t(g)) = (T^t \circ U^t)(g)$, 从而 $(U \circ T)^t = T^t \circ U^t$

命题 3.7.1 设空间有限维, $T \in L(V, W), B, B'$ 分别为 V, W 的两组基, B^*, B'^* 为对偶基, 则

$$[T^t]_{B^*, B'^*} = [T]_{B, B'}^t$$

证明: 记 $[T^t]_{B^*, B'^*} = B, [T]_{B, B'}^t = A$ 设 $B = \{\alpha_1, \dots, \alpha_n\}, B' = \{\beta_1, \dots, \beta_m\}, B^* = \{f_1, \dots, f_n\}, B'^* = \{g_1, \dots, g_m\}$ 于是有 $(T\alpha_1, \dots, T\alpha_n) = (\beta_1, \dots, \beta_m)A$ 同样, 有 $(T^t g_1, \dots, T^t g_m) = (f_1, \dots, f_n)B$ 取转置, 有

$$\begin{pmatrix} T^t g_1 \\ \vdots \\ T^t g_m \end{pmatrix} = B^t \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

另一种意义的形式矩阵乘法:

$$\begin{pmatrix} f_1 \\ \vdots \\ f_p \end{pmatrix} (\alpha_1, \dots, \alpha_q) = \begin{pmatrix} f_1(\alpha_1) & \cdots & f_1(\alpha_q) \\ \vdots & \vdots & \vdots \\ f_p(\alpha_1) & \cdots & f_p(\alpha_q) \end{pmatrix}$$

于是

$$\begin{pmatrix} T^t g_1 \\ \vdots \\ T^t g_m \end{pmatrix} (\alpha_1, \dots, \alpha_n) = B^t \left[\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} (\alpha_1, \dots, \alpha_n) \right] = B^t I_n = B^t$$

另一方面

$$\begin{aligned}
 & \begin{pmatrix} T^t g_1 \\ \vdots \\ T^t g_m \end{pmatrix} (\alpha_1, \dots, \alpha_n) = \begin{pmatrix} T^t g_1(\alpha_1) & \cdots & T^t g_1(\alpha_n) \\ \vdots & & \vdots \\ T^t g_m(\alpha_1) & \cdots & T^t g_m(\alpha_n) \end{pmatrix} \\
 & = \begin{pmatrix} g_1(T\alpha_1) & \cdots & g_1(T\alpha_n) \\ \vdots & & \vdots \\ g_m(T\alpha_1) & \cdots & g_m(T\alpha_n) \end{pmatrix} = \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} \begin{pmatrix} T\alpha_1 & \cdots & T\alpha_n \end{pmatrix} \\
 & = \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} \begin{pmatrix} \beta_1 & \cdots & \beta_m \end{pmatrix} A = I_m A = A
 \end{aligned}$$

从而 $B^t = A$. 对于方阵来说, A, A^t 有很多相同的性质.

命题3.7.2 (1) $\ker(T^t) = \text{Im}(T)^0$ (2) 若 $\dim W < \infty$, 则 $\text{Im}(T^t) = \ker(T)^0$

证明: (1) $\ker(T^t) = \{g \in W^* | g \circ T = 0\} = \{g \in W^* | \text{Im}(T) \subset \ker(g)\} = \text{Im}(g)^0$

于是得到 T^t 是单射 $\Leftrightarrow T$ 是满射 (有限维成立, 无限维需要用到选择公理)

(2) $\text{Im}(T^t) = \{g \circ T | g \in W^*\} \ker(T)^0 = \{f \in V^* | \ker(T) \subset \ker(f)\}$

" \subset " 显然成立, 考虑另一方面, 需要证明对 $f \in V^*$ 如果 $\ker(T) \subset \ker(f)$, 则存在一个 $g \in W^*$, 使得 $f = g \circ T$ 先定义 $g_0 \in \text{Im}(T)^*$ 为 $g_0(T\alpha) = f(\alpha)$ (well-defined) 因此, 对 g_0 满足条件, 其余扩充即可 (因为只依赖于 T 的像集上的性质)

只需要证明 g_0 能够线性扩充到 W 上. $\dim W < \infty \Rightarrow$ 可取 $\text{Im}(T)$ 的基 $\{\beta_1, \dots, \beta_k\}$ 并扩充为 W 的基 $\{\beta_1, \dots, \beta_m\}$ 定义 $g(\sum c_i \beta_i) = g_0(\sum c_i \beta_i)$

由此可以得出 T^t 是满射 $\Leftrightarrow T$ 是单射.

命题3.7.3 若 U, V 是有限维, 则 $\text{rank}(T^t) = \text{rank}(T)$

证明: $\text{rank}(T) + \dim \ker(T^t) = \dim W^*$ 又由于 $\text{rank}(T) + \dim \text{Im}(T)^0 = \dim V$ 从而成立.

另证: $\text{rank}(T) + \dim \ker(T) = \dim V$ 结合 $\dim \ker(T)^0 + \dim \ker(T) = \dim V$

第四章 Polynomials

4.1 Algebra

定义4.1.1 设 F 是一个域, A 是一个 F -线性空间, 称 A 是一个代数(algebra). 如果 A 上的乘法运算 $A \times A \rightarrow A: (\alpha, \beta) \mapsto \alpha\beta$. 使得

- (1) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$
- (2) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma, (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$
- (3) $c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta) \forall c \in F, \alpha, \beta \in A$

矩阵的乘法和 $L(V)$ 就是代数, 另外设两个域 $F \subset F'$ 可以 F 看成 F' 代数.

取 $A = \otimes(V^*) = \bigoplus_{r=0}^{\infty} (V^*)^{\otimes r}$ 也是 F 代数, 即张量代数, 对应地, 利用外积扩充成的代数, 即外代数. 若 $\dim V = n$, 则 $\dim \dots = 2^n$

定义4.1.2 设 A, A' 是 F -代数, 将映射 $\Phi: A \rightarrow A'$, 称为是 F -代数的同态(homomorphism), 如果 Φ 线性, 且 $\Phi(\alpha\beta) = \Phi(\alpha)\Phi(\beta)$. 可逆的同态称为同构(isomorphism).

若 Φ 可逆, 则 Φ^{-1} 也是同态, 此时为同态. 如果两个代数之间存在同构映射, 则称这两个 F -代数同构. 例如 $L(V) \cong F^{n \times n}$. 取一组基 B 定义 $\Phi: L(V) \rightarrow F^{n \times n}: T \rightarrow [T]_B$

一个代数 A 称为有单位元的, 如果存在一个 $1 \in A$, 使得 $1\alpha = \alpha 1 = \alpha$. 若有单位元, 容易验证唯一性.

称 A 是可交换的, 如果 $\alpha\beta = \beta\alpha \forall \alpha, \beta \in V$

注意从 F -代数的同态的定义, 得不到 $\Phi(1_A) = 1_{A'}$

定义 $A = F[[x]] := \{(a_0, a_1, \dots), a_n \in F \text{ 若 } f = (a_0, a_1, \dots), g = (b_0, b_1, \dots) \text{ 定义 } fg = (c_0, c_1, \dots), \text{ 满足 } c_n = \sum_{i=0}^n a_i b_{n-i}\}$. 容易验证乘法满足交换律和结合律, 且有单位元 $(1, 0, 0, \dots)$, 称为 F 上的形式幂级数代数.

记 $x = (1, 0, 0, \dots)$, 则 $x^n = (0, \dots, 0, 1, 0, \dots)$ 的第 n 项为0. 约定 $x^0 = 1$ 记 $(a_0, a_1, \dots) := \sum_{i=0}^{\infty} a_i x^i$, 这只是一个记号而不是等式. 因为代数学里面没有可数个数的加法.

由这个记号, 我们有

$$\left(\sum_{n=0}^{\infty} (a_n x^n)\right) \left(\sum_{n=0}^{\infty} (b_n x^n)\right) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i b_{n-i}\right) x^n$$

可以将最后一项想成(而不是) $\sum_{i,j} a_i b_j x^{i+j}$

4.2 The Algebra of Polynomials

注意 $\{x^0, x^1, \dots\}$ 不是基. 可以验证它们线性无关, 但不生成全空间, 比如 $(1, 1, \dots) \notin \text{span}\{x^0, x^1, \dots\}$ 容易看出 $(a_0, a_1, \dots) \in \text{span}\{x_0, x_1, \dots\}$ 的充分必要条件是 a_i 只有有限项非零.

记 $F[x] := \text{span}\{x^0, x^1, \dots\}$ 即只有有限项非零的和

容易验证 $f, g \in F[x] \Rightarrow fg \in F[x]$, 从而 $F[x]$ 也是一个代数, 叫做 F 的多项式代数

从而 $\{x^0, x^1, \dots\}$ 是多项式代数的一组基. 且交换, 有单位元.

在多项式代数当中, 上面的求和就有意义了. 符号 $\sum_{k=0}^n a_k x^k$ 就是一个记号, 只跟 a_k 有关, x^k 只是一个“石头”.

以后将 $F[x]$ 中的元素叫做一个以 F 为系数的多项式. 将 F 中的元素 c 看成多项式 $(c, 0, \dots)$, 叫做纯量多项式. 这样的多项式乘法和纯量乘法的结果是一样的. 如果 $f \in F[x] \neq 0$, 将使得 $a_k \neq 0$ 的最大的 k 记作 f 的次数 (degree), 记作 $\deg f$. 此时, f 也可以表示成

$$f = \sum_{k=0}^n a_k x^k \quad (a_n \neq 0)$$

约定 $\deg 0 = -\infty$, 这个 $-\infty$ 也是一个约定的记号, 满足一些我们容易接受的性质, 即 $a > -\infty (\forall a \in \mathbb{R}), a + (-\infty) = -\infty, (-\infty) + (-\infty) = -\infty$.

对 $\deg f = n \geq 0$, 称 a_n 为 f 的首项系数. 如果 $a_n = 1$, 称为 f 为首一的 (monic)

命题 4.2.1 设 $f, g \in F[x]$

(1) 若 $f, g \neq 0$, 则 $fg \neq 0$ (多项式代数无零因子), 且 $\deg(fg) = \deg f + \deg g$

(2) 若 f, g 是首一的, 则 fg 也是首一的

(3) fg 是非零的纯量多项式 $\Leftrightarrow f, g$ 也是非零的纯量多项式

(4) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$

证明: 显然.

推论 4.2.1 多项式乘法中有消去律: 若 $f \neq 0, f, g, h \in F[x]$ 满足 $fg = fh$, 则 $g = h$

定义 4.2.1 设 A 是有单位元的 F -代数, $f \in F[x]$, 若 $f = \sum_{k=0}^n a_k x^k$, 对 $\alpha \in A$, 定义 $f(\alpha) = \sum_{k=0}^n a_k \alpha^k \in A$, 称为 f 在 α 处的取值.

若 $A = F$, 就变成了以前关于多项式的理解, 即多项式函数. 此时 f 可以理解成一个 A 到自己的一个映射.

取 $A = L(V), F^{n \times n}, F[x]$ 等均变成了类似的运算. 对 $g \in F[x]$, 由 $f(g) = \sum_{k=0}^n a_k g^k$, 若取 $g = x = (1, 0, \dots)$, 则 $f(x) = \sum_{k=0}^n a_k x^k$, 它就是一个 f . 但意义发生了轻微的改变, 后者代表了一个诱导出的映射.

命题 4.2.2 取定 $\alpha \in A$, 则映射 $\Phi: F[x] \rightarrow A: f \mapsto f(\alpha)$. 是一个 F -代数的同态, 看成一个在 α 处的取值映射.

4.3 Polynomials Ideals

定义 4.3.1 $F[x]$ 的一个子空间 M 称为 $F[x]$ 的理想 (ideal), 如果 $\forall f \in F[x], \forall g \in M, fg \in M$. 即 M 不仅对乘法封闭, 并且只要一个属于 M , 它们的乘积就在 M 中, 可以简单地记为 $F[x]M = M$

比如, 取定 $d \in F[x]$, 考虑 $\{df | f \in F[x]\}$ 是一个理想. 记作 (d)

设 $d_1, \dots, d_n \in F[x]$, 也可以考虑由它们生成的理想 $(d_1, \dots, d_n) := \{\sum_i d_i f_i | f_i \in F[x]\}$

但比如考虑 $\sum_k a_k x^{2k}$ 对乘法也封闭, 但就不是理想.

由一个多项式生成的理想叫做主理想 (main ideal). 我们有下面的定理

定理 4.3.1 $F[x]$ 的理想都是主理想, 事实上, 对任意的非零理想 $M \subset F[x]$, 存在唯一一个首一的 $d \in F[x]$, 使得 $M = (d)$

对此, 我们先证明: 多项式能够做带余除法, 即

定理 4.3.2 设 $f, d \in F[x], d \neq 0$, 则存在唯一的 $q, r \in F[x]$, 其中 $\deg r < \deg d$ 使得 $f = dq + r$

证明:

存在性:用归纳法, 对 $\deg f \in \{-\infty, 0, 1, \dots\}$ 作归纳.

若 $\deg(f) \in \deg(d)$, 则取 $q = 0, r = f$

下面设 $\deg f = m \geq \deg d$, 由归纳法, 可设对次数 $< m$ 的 f 成立, 下面考虑 m 的情形, 设

$$f = \sum_{k=0}^m a_k x^k, d = \sum_{k=0}^n b_k x^k, a_m, b_n \neq 0, m \geq n$$

令 $f' = f - d(\frac{a_m}{b_n} x^{n-m})$, 则 $\deg(f') < m$, 由归纳假设, 存在 $q', r', \deg(r') < \deg d$ 使得 $f' = dq' + r'$ 带入 f 的式子即得存在性

唯一性: 设 $f = dq + r = dq' + r'$, 故 $d(q - q') = r' - r$ 两边取次数, 得

$$\deg(d) + \deg(q - q') = \deg(r' - r) \leq \max\{\deg(r), \deg(r')\} < \deg(d)$$

故只能 $\deg(q - q') = -\infty$, 故 $q = q'$, 从而 $r = r'$

下面回到与原定理的证明:

证明:

存在性: 取 M 中次数最小的多项式首一多项式 d , 下面证明 $M = (d)$ 显然, 对 $\forall df \in (d)$, 又 $d \in M$, 故 $(d) \subset M$

另一方面, 取任意 $f \in M$, 由带余除法定理, 存在 q, r 使得 $f = dq + r, \deg(r) < \deg(d)$, 又 $dq \in M \Rightarrow r \in M$, 又 $\deg(d)$ 故只能 $r = 0$. 从而 $f = dq \in (d)$, 从而 $M = (d)$

唯一性: 设 $(d) = (d')$, 则 $d \in (d')$, 则 $d = d'f$, 同理 $d' = dg$, 从而 $d = dfg$, 又 $d \neq 0$, 从而 $fg = 1$, 故 f, g 是纯量多项式, 又 d 首一, 故只能 $d = 1$

定义 4.3.2 设 p_1, \dots, p_n 是 n 个多项式, 不全为 0, 考虑理想 (p_1, \dots, p_n) 的首一生成元 d 称为 p_1, \dots, p_n 的**最大公因式(greatest common divisor)**, 记为 $d = \gcd(p_1, \dots, p_n)$, 如果 $\gcd(p_1, \dots, p_n) = 1$, 则称 p_1, \dots, p_n **互素(coprime)**, 此时 $(p_1, \dots, p_n) = F[x]$, 即存在 $f_1, \dots, f_n \in F[x]$, 使得 $\sum p_i f_i = 1$

定义 4.3.3 设 $f = dq + r$, 若 $r = 0$, 则记作 $d|f$, 叫做 d **整除** f , f 被 d 整除, d 叫做 f 的**因子(factor)**.

命题 4.3.1 设 $p_1, \dots, p_n, d \in F[x]$, d 首一, 则下面两条等价

(1) $(p_1, \dots, p_n) = (d)$

(2) $d|p_i$, 且对任意的 f , 若 $f|p_i$ 也成立, 则能够推出 $f|d$

(1) \Rightarrow (2), 显然 $d \in (p_i)$, 设 $p_i = fg_i$ 又 $d \in (p_1, \dots, p_n) \Rightarrow d = \sum p_i f_i = fg_i f_i \Rightarrow f|d$

(2) \Rightarrow (1), 设 $(p_1, \dots, p_n) = (d_0)$, 则 $d_0 = \sum p_i g_i$, 又 $d|p_i \Rightarrow p_i = df_i \Rightarrow d_i = \sum df_i g_i \Rightarrow d|d_0$

又 $p_i \in (d_0) \Rightarrow d_0|p_i \Rightarrow d|d_0$, 从而 $d = d_0$

求最大公因式的过程叫做**辗转相除法**: 如 $(d) = (p_1, \dots, p_n) = (p_1) + \dots + (p_n) = (p_1) + (p_2) + (p_3) + \dots + (p_n) = \dots$

下面给出求最大公因式的另一个方法

定义 4.3.4 (1) $f \in F[x]$ 在 F 上**可约**, 如果存在两个多项式 $g, h, \deg(g), \deg(h) \geq 1$, 使得 $f = gh$, 否则称 f **不可约**. 由此定义, 如果 $\deg f \leq 1$, 则 f 一定不可约, 特别低纯量多项式不可约.

(2) 非纯量的不可约多项式叫做 F 上的**素多项式**. (现在这样叫的已经比较少了), 可以得到 $\deg = 1$ 则一定是素多项式, 而如果一个域满足素多项式只能是一次的, 则 F 称为**代数闭域**. 复数域即是代数闭域.

根据定义 $f \neq 0$ 不可约, 如果 $d|f$, 则要么 d 是常数, 要么 $d = cf, c \in F$

命题 4.3.2 设 f, g, p 满足 p 是素多项式, 假设 $p|fg$, 则 $p|f$ 或 $p|g$ (这个才是真正的“素”的定义)

证明: 不妨设 p 首一. 不影响条件和结论, 假设 $p \nmid f$, 下面证明 $p|g$.

设 $d = (f, p)$, 则 $d|p$ 故 $d = 1$ 或 $d = p$. 又 $d|f, p \nmid f$, 则只能有 $d = 1$

从而存在 f_0, p_0 , 使得 $f_0 f + p_0 p = 1$, 因此 $f_0 f g + p_0 p g = g$, 从而 $p|g$

推论4.3.1 p 是素多项式, 且 $p|f_1 \cdots f_n$, 则 $p|f_i$ 对某个 i 成立.

定理4.3.3 (多项式的唯一因子分解定理) $\forall f \in F[x] - F$ 是首一多项式, 则 f 可分解为 $f = p_1 \cdots p_n$, 其中 p_i 是素多项式, 并且在不计 p_i 次序的意义下是唯一的.

证明:

存在性: 对 $n = \deg(f)$ 进行归纳, 当 $n = 1$ 时结论显然.

对于一般情况, 如 f 是素多项式, 则成立, 否则 f 不是素多项式, 则 f 能够写成 g, h , 其中 $\deg(g), \deg(h) < \deg(f)$, 对 g, h 利用归纳假设即可.

唯一性:

设 $f = p_1 \cdots p_n = q_1 \cdots q_m$, 并且 p_i, q_j 素, 首一, 将重复的写在一起, 记为

$f = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s}$, 设 p_i, q_j 互不相同.

任取一个 p_i , 故 $p_i|q_1^{m_1} \cdots q_s^{m_s}$, 故 $p_i|q_j$ 对某个 j 成立. 从而 $p_i = q_j$

从而每个 p_i 都是某个 q_j , 从而 $\{p_1, \cdots, p_r\} \subset \{q_1, \cdots, q_s\}$, 同理有反向的包含关系, 从而 $\{p_1, \cdots, p_r\} = \{q_1, \cdots, q_s\}$. 重排后, 不妨设 $p_i = q_i$, 再显然(确实显然...)每个多项式的幂次相等.

利用这个唯一因子分解定理可以用来求最大公因式.

命题4.3.3 设 $f_1, \cdots, f_n \in F[x] - F$, 由上述定理, 可以将它们写为

$$f_1 = p_1^{k_{11}} \cdots p_m^{k_{1m}}, \cdots, f_n = p_1^{k_{n1}} \cdots p_m^{k_{nm}}$$

其中 p_1, \cdots, p_m 为所有多项式的所有素因子, 指数允许有0, 记 $a_i = \min\{k_{1i}, \cdots, k_{ni}\}$, 则 $\gcd(f_1, \cdots, f_n) = p_1^{a_1} \cdots p_m^{a_m}$

证明:

记 $d = p_1^{a_1} \cdots p_m^{a_m}$ 只需证 $d|f_i$, 并且如果 $g|f_i \Rightarrow g|d$. 而显然 $d|f_i$

另设 $g|f_i$, 设 $g = cp_1^{r_1} \cdots p_m^{r_m} q_1^{s_1} \cdots q_t^{s_t}$. 其中允许某个指数为0, 使得每个 p_i 均出现. 并要求每个 p_i, q_j 均首一

若某个 $s_j > 0$, 则 $q_j|g$, 而 $g|f_i \Rightarrow q_j|f_i (\forall i) \Rightarrow q_j|f_1 \Rightarrow q_j|p_i \Rightarrow q_j = p_i$

类似地, 如果某个 $r_i > a_i$ 也可以证明矛盾.

定义4.3.5 如果 $f(c) = 0$, 则称 c 是 f 的根(root), 也叫零点

命题4.3.4 设 $f \in F[x], c \in F$, 则 c 是 f 的根 $\Leftrightarrow (x - c)|f$

证明: 存在 $q, r \in F[x]$, 使得 $f = (x - c)q + r, \deg(r) \leq 0$ 即 $r \in F$

下面说明上面的式子中我们可以将 c “带进去”, 这样就直接得出了结论. 事实上, 利用 F -代数的同态 $F[x] \rightarrow A: f \mapsto f(A)$ 中将 A 取为 F 即可.

命题4.3.5 对于域 F 下面两个命题等价:

(1) 任何 $f \in F[x] - F$ 总有根

(2) 素多项式的次数一定是1

如果 F 满足上面两种性质的一件, 则称作 F 为代数闭域. 比如 \mathbb{C} 就是代数闭域, 另外考虑所有代数数的集合, 它也是一个代数闭域, 它是有理数域的代数闭包.

证明:

(1) \Rightarrow (2): 设 p 是素多项式, 由(1), p 有根, 故 $p(c) = 0$, 从而 $x - c|p$, 又 p 是素多项式, 从而 $p = a(x - c)(a \in F)$, 从而 $\deg(p) = 1$

(2) \Rightarrow (1) 设 $F = F[x] - F$, 由唯一分解定理, 设 $f = p_1 \cdots p_k$, 又每个 p_i 的次数全都是1, 从而 $p_1 = x - c$, 从而 c 是 p_1 的根, 从而也是 f 的根.

定理4.3.4 设 $f \in F[x] - \{0\}, \deg f = n$, 则 f 至多有 n 个根

证明:

对 n 用数学归纳法, 当 $n = 0$ 显然. 假设 $< n$ 成立, 当 n 时

若 f 无根则成立, 否则, 如果 g 有根, 则把 $x - c$ 除去后用归纳法即可

定义4.3.6 映射 $\phi: F \rightarrow F$ 称为多项式函数, 如果存在 $f \in F[x]$, 使得 $\phi(t) = f(t), \forall t \in F$, 此时记 $\phi = f$

如果 F 有无穷多个元素, 则可以推出 f 唯一, 否则, 若 $F = \mathbb{F}_p$, 则 $x^p = x$, 不唯一

我们考虑所有 F 映到自己的多项式函数的集合 A , 容易看出它也是一个 F 代数. 考虑 $F[x] \rightarrow A: f \mapsto f$, 是一个 f 代数的同态, 由多项式函数的定义知是满映射, 而它是单射的充分必要条件是 F 里面有无穷多个元素, 所以如果 F 是无限域, 这就是一个 F 代数的同构.

定义4.3.7 设 $c \in F$ 是 f 的根, 则 c 作为 f 的根的重数:= $\max_r \{r \geq 1 | (x - c)^r | f\}$

研究多项式重数的一个有效工具是 f 的形式导数, 记作 Df 或 f' , 对于 $f = \sum_{k=0}^n a_k x^k$, 则 $Df := \sum_{k=1}^n k a_k x^{k-1}$

能够证明, 如果 $\text{char} F = 0$, 则 c 的重数= $\min\{k \geq 0 | (D^k f)(c) \neq 0\}$

如果重数 ≥ 2 , 则称 c 是 f 的重根, 如果重数为1, 则叫做 f 的单根.

容易得到 c 是重根 $\Leftrightarrow c$ 是 Df 的根

推论4.3.2 (1)若 $\text{gcd}(f, f') = 1$, 则 f 无重根

(2)若 F 是代数闭域, 则上述命题的逆命题也成立

证明是显然的

4.4 Lagrange Interpolation

定理4.4.1 设 $t_1, \dots, t_n \in F$ 互不相同, 则对任意 $c_1, \dots, c_n \in F$, 则存在唯一一个次数 $\leq n$ 的多项式 $f \in F[x]$, 使得 $f(t_i) = c_i$

$$f = \sum_{i=0}^n c_i \prod_{j \neq i} \frac{x - t_j}{t_i - t_j}$$

存在性代入证明即可, 而唯一性利用 n 次方程至多有 n 个根即可.

记 $V = \{f \in F[x] | \deg(f) \leq n\}$, 则 $\dim V = n + 1$, 基为 $\{1, x, \dots, x^{n+1}\}$

定义 $L_i \in V^*$ 为 $L_i(f) = f(t_i), i = 0, \dots, n$

则 $\{L_1, \dots, L_n\}$ 是 V^* 的基能够推出 t_i 构成的Vandermonde矩阵可逆.

事实上, 设 $\{p_1, \dots, p_n\}$ 是 L_0, \dots, L_n 的对偶基, 则对 $\forall f \in V, f = \sum L_i(f)p_i = \sum f(t_i)p_i$

取 $f = x^j \Rightarrow x_j = \sum t^j p_i$. 从而

$$(1, x, \dots, x^n) = (p_0, \dots, p_n)A$$

A 是Vandermonde矩阵. 倒过来也可以证明成立

第五章 Determinant

见《安金鹏行列式讲义》

第六章 Elementary Canonical Forms

6.1 Introduction

对域 F 上的有限维向量空间 V ,对 $T \in L(V)$,我们要来刻画 T
取 V 的一组基 \mathcal{B} ,则 T 有一个矩阵表示 $A = [T]_{\mathcal{B}}$,即

$$(T\alpha_1, \dots, T\alpha_n) = (\alpha_1, \dots, \alpha_n)A$$

利用矩阵来考虑问题则将变得具体的很多.

例如,判断 T 是否可逆,则可求 A 的行列式即可,再如求 $\dim \text{Ker } T$,也可以将矩阵进行适当的初等行变换即可求.

因此,我们希望找一组基,使得 T 的矩阵 $[T]_{\mathcal{B}}$ 尽量简单.特别地,我们有

定义6.1.1 一个线性变换 T 称为可对角化的,如果存在一组基 \mathcal{B} ,使得 $[T]_{\mathcal{B}}$ 为对角矩阵.

如果可对角化,那么去认识这个矩阵 T 就很简单了.下面我们就来研究可对角化的一些性质以及判断等.我们已经知道,对于 $T \in L(V)$,有

$$\{[T]_{\mathcal{B}} \mid \mathcal{B} \text{ 是有序基}\}$$

是一个相似等价类.

于是问题归结为,需要在一个相似等价类里面找一个尽量简单的矩阵.

定义6.1.2 称矩阵 A 可对角化,如果存在与 A 相似的对角矩阵

对此,我们引入下面的概念

6.2 Characteristic Values

定义6.2.1 设 $T \in L(V)$,对 $c \in F$,记

$$V_c = \text{Ker}(\text{id}_V - T) = \{\alpha \in V \mid T\alpha = c\alpha\}$$

对于绝大多数 c , $\text{id}_V - T$ 可逆,此时 $V_c = \{0\}$,如果 $V_c \neq \{0\}$,则称 c 是 T 的特征值,称 V_c 是关于特征值 c 的特征子空间. V_c 中的非零向量称作关于特征值 c 的特征向量. T 的特征值集合称作 T 的谱集,记作 $\sigma(T) = \{c \in F \mid V_c \neq 0\}$

命题6.2.1 设 $T \in L(V)$, \mathcal{B} 是有序基,则 $[T]_{\mathcal{B}}$ 是对角矩阵 $\Leftrightarrow \mathcal{B}$ 中的向量都是 T 的特征向量

于是, T 可对角化 \Leftrightarrow 存在由特征向量构成的基 $\Leftrightarrow T$ 的特征向量生成全空间

证明 设 $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$, $A = [T]_{\mathcal{B}}$, 则 $T\alpha_j = \sum_{i=1}^n A_{ij}\alpha_i$

于是 A 对角 \Leftrightarrow 对每个 j ,存在 $c_j \in F$ 使得 $T\alpha_j = c_j\alpha_j \Leftrightarrow$ 每个 α_j 是特征向量 □

下面考虑矩阵的情形

定义6.2.2 设 $A \in F^{n \times n}$, 对 $c \in F$, 记

$$\text{Ker}(cI_n - A) = \text{Ker}(\text{cid}_{F^{n \times 1}} - L_A) = \{X \in F^{n \times 1} | AX = cX\}$$

对于绝大多数 $c, cI_n - A$ 可逆, 此时 $\text{Ker}(cI_n - A) = \{0\}$, 如果 $V_c \neq \{0\}$, 则称 c 是 A 的特征值, 称 $\text{Ker}(cI_n - A)$ 是关于特征值 c 的特征子空间. V_c 中的非零向量称作关于特征值 c 的特征向量. A 的特征值集合称作 A 的谱集, 记作 $\sigma(A) = \{c \in F | V_c \neq 0\}$

从而, A 可对角化 \Leftrightarrow 存在由 A 的特征向量构成的 $F^{n \times 1}$ 的基.

下面来求特征值

引理6.2.1 (1) $\sigma(T) = \{c \in F | \det(\text{cid}_V - T) = 0\}$

(2) $\sigma(A) = \{c \in F | \det(cI_n - A) = 0\}$

由于 $\det(cI_n - A)$ 是一个关于 c 的 n 次多项式函数. 但如果域是有限域, 多项式函数的表达式不唯一, 因此我们不仅要将它看成多项式函数, 而应该看成一个多项式.

下面我们将这个说法严格化:

定义6.2.3 考虑集合 $X := F[x] \times (F[x] - \{0\}) = \{(f, g) | f, g \in F[x], g \neq 0\}$ 上的关系: $(f_1, g_1) \sim (f_2, g_2) \Leftrightarrow f_1g_2 = f_2g_1$ 是等价关系

记 $F(x) = X / \sim$ 为 X 中的等价类的集合, 记 (f, g) 所在的等价类为 $\frac{f}{g}$

于是, 我们得到 $\frac{f_1}{g_1} = \frac{f_2}{g_2} \Leftrightarrow f_1g_2 = f_2g_1$

再定义 $\frac{f_1}{g_1} + \frac{f_2}{g_2} := \frac{f_1g_2 + f_2g_1}{g_1g_2}$, $\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1f_2}{g_1g_2}$ 容易验证是良定的, 并且在这样定义的加法和乘法下, $F[x]$ 构成一个域, 称作 F 上的有理函数域. 但这只是一种叫法, 其中的元素其实不是一个函数. 零元素是 $\frac{0}{1}$, 1 元素是 $\frac{1}{1}$, 而 $-\frac{f}{g} = \frac{-f}{g}$, 且当 f 非零时 $\left(\frac{f}{g}\right)^{-1} = \frac{g}{f}$

在这样的严格定义下, 整数不是有理数, 因为有理数是整数对的等价类. 于是, 我们应该把整数和整数所在的等价类等同起来. 类似地, 我们将多项式 $f(x)$, 和有理函数 $\frac{f(x)}{1}$ 等同起来, 在这样意义下, $F \subset F[x] \subset F(x)$, 并且在这样的等同下, 加法和乘法是保持的.

定义6.2.4 设 $A \in F^{n \times n}$, 考虑 $xI_n - A \in F(x)^{n \times n}$ 称 $f_A(x) = \det(xI_n - A) \in F[x]$ 为 A 的特征多项式. 设 $T \in L(V)$, \mathcal{B} 是有序基, $f_T := f_{[T]_{\mathcal{B}}}$ 称为 T 的特征多项式.

有了这个定义之后, 我们知道特征值就是特征多项式的根.

能够直接从线性映射的本身来定义特征多项式呢? 其实是可以的, 考虑 $V \otimes (x)$ 积即可, 它可以看成 $F(x)$ 的线性空间. 此时, 考虑 $\det(\text{id}_V \otimes x - T \otimes \text{id}_{F(x)})$, 具体内容略去.

从而 $\sigma(A) = \{c \in F | \det(cI_n - A) = 0\}$, 关于特征多项式, 有

- f_A 首一, $\deg f_A = n$, 常数项 = $(-1)^n \det(A)$, x^{n-1} 的系数 = $-\text{tr } A$ 由于 n 次多项式至多有 n 个根, 特别地, 我们得到谱集总是一个有限集.
- $A \sim B \Rightarrow f_A = f_B$
- f_T 首一, 且 $\deg f_T = \dim V$
- $\sigma(T) = \{f_T \text{ 的根}\} \Rightarrow |\sigma(T)| \leq \dim V$
- 若 T 对角化, $[T]_{\mathcal{B}} = \text{diag}(c_1, \dots, c_n)$, 则 $f_T = (x - c_1) \cdots (x - c_n)$. 于是, 不可能发生 T 在不同的有序基表示下得到的对角矩阵所对应的对角元不相同. $\Rightarrow [T]_{\mathcal{B}}$ 的对角元在差一个排列的意义下被 T 决定.

(下面转到6.6节)

对于 $T \in L(V)$, $W \subset V$ 是 T -不变子空间(invariant subspace), 指 $T(W) \subset W$

显然 $\text{Ker } T, \text{Im } T$ 均为 T -不变子空间.

命题6.2.2 T 可对角化 $\iff V$ 可分解为一维不变子空间的直和

证明 由于 T 可对角化 \Rightarrow 存在特征向量构成的基.而注意到说明 α 是特征向量 $F\alpha := \text{span}\{\alpha\}$ 是 T -不变子空间.设特征向量 \square

此处补笔记

对 $f(x) \in F[x]$,记 $m(c, f)$ 为 c 作为 f 的根的重数.即 f 能写成 $(f - g)^m g, g(c) \neq 0, \text{若 } c > 1$,称 c 是**重根**.

命题6.2.3 $1 \leq \dim(V_c) \leq m(c, f_T)$,特别地,若 c 不是重根,则特征子空间是1维的.

证明 取 V_c 的有序基 $\{\alpha_1, \dots, \alpha_d\}$,扩充为全空间的一组基 $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 当 $1 \leq g \leq d$ 时, $T\alpha_j = c\alpha_j$ 从而 T 在 \mathcal{B} 下的矩阵形如

$$\begin{pmatrix} cI_d & B_{d \times (n-d)} \\ 0 & D_{(n-d) \times (n-d)} \end{pmatrix}$$

于是

$$f_T = f_{[T]_{\mathcal{B}}} = \det \left(xI_n - \begin{pmatrix} cI_d & B \\ 0 & D \end{pmatrix} \right) = \det \begin{pmatrix} (x-c)I_d & -B \\ 0 & xI_{n-d} - D \end{pmatrix} = (x-c)^d f_D$$

从而 $m(c, f) \geq d$ \square

我们称 $m(c, f)$ 的**代数重数**, $\dim V_c$ 称为特征值的**几何重数**.从而上述结论为几何重数不超过代数重数.

定理6.2.1 设 $T \in L(V)$,则以下几条等价:

(1) T 可对角化

(2) $V = \bigoplus_{c \in \sigma(T)} V_c$

(3) $\dim V = \sum_{c \in \sigma(T)} \dim V_c$

(4) $f_T = \prod_{c \in \sigma(T)} (x-c)^{\dim V_c}$

(5) f_T 可分解为 $F[x]$ 中一次因式的乘积,且 $\forall c \in \sigma(T)$ 的代数重数=几何重数

证明 (1) \iff (2): 事实上,(1) $\iff \exists$ 特征向量构成一组基 \iff (2)

(2) \iff (3): (2) \Rightarrow (3)显然. (3) \Rightarrow (2) $\dim \bigoplus_c V_c = \sum_c \dim V_c = \dim V \Rightarrow$ (2)

(2) \implies (4): 设 $\sigma(T) = \{c_1, \dots, c_k\}, d_i = \dim V_{c_i}$,设 $\mathcal{B}_i = \{\alpha_{i1}, \dots, \alpha_{id_i}\}$ 是 V_{c_i} 的有序基,则

$\mathcal{B} = \{\alpha_{11}, \dots, \alpha_{1d_1}, \dots, \alpha_{k1}, \dots, \alpha_{kd_k}\}$ 是 V 的有序基.

又由于 $T\alpha_{ij} = c_i\alpha_{ij}$,考虑 T 在 \mathcal{B} 下的矩阵表示 $[T]_{\mathcal{B}} = \begin{pmatrix} c_1 I_{d_1} & & \\ & \dots & \\ & & c_k I_{d_k} \end{pmatrix} \Rightarrow f_T = \prod_{i=1}^k (x-c_i)^{d_i}$

(4) \Rightarrow (3) $\dim V = \deg f_T = \sum_{c \in \sigma(T)} \dim V_c$

而(4)和(5)只是同一个事实的不同描述.从而上述5个命题等价. \square

上面的定理就给出了判断一个线性变换是否可对角化的理论.如果特征多项式在 $F[x]$ 中不能分解为一次因式的乘积,则 T 一定不可对角化.另一方面,在判断的时候,只需判断代数重数大于1的特征值是否满足代数重数等于几何重数,而只需判断大于1的那些.一个特征多项式无重根的概率为1,从而一般来说都可以对角化.

- $|\sigma(T)| = \dim V \Rightarrow T$ 可对角化.

利用矩阵的语言,我们可以得到

推论6.2.1 (1) 设 $A \in F^{n \times n}$, 则 A 可对角化 $\iff f_A$ 为 $F[x]$ 中一次式的乘积, 且任意的代数重数大于1的特征值 c 的代数等于 c 的几何重数 $\dim \text{Ker}(cI_n - A) \in F^{n \times 1}$.

(2) 若 A 可对角化, 存在 $P \in GL_n(F)$, 使得 $P^{-1}AP$ 为对角矩阵. 此时, 若 $\{\alpha_{i1}, \dots, \alpha_{id_i}\}$ 是 $\text{Ker}(c_i I_n - A)$ 的有序基, 则 $P = [\alpha_1, \dots, \alpha_{1d_1}, \dots, \alpha_{k1}, \dots, \alpha_{kd_k}]_{n \times n}$ 可逆, 且它就是上面所述的 P , 并且

$$P^{-1}AP = \begin{pmatrix} c_1 I_{d_1} & & \\ & \dots & \\ & & c_k I_{d_k} \end{pmatrix}, f_A = (x - c_1)^{d_1} \dots (x - c_k)^{d_k}$$

证明 下面给出(2)的证明 $A\alpha_{ij} = c_i\alpha_{ij} \Rightarrow AP = [A\alpha_{11}, \dots, \dots, A\alpha_{kd_k}] = [c_1\alpha_{11}, \dots, \dots, c_k\alpha_{kd_k}] = P \cdot$ 上述对角矩阵. \square

一个矩阵不可对角化有两个原因, 一个是 F 不是代数闭域, 另一个是几何重数小于代数重数. 而后一种原因是本质的, 前一种原因可以通过域扩张来解决.

6.3 Annihilating Polynomial

下面介绍如下定理

定理6.3.1 (Cayley-Hamilton) (1) 设 $T \in L(V)$, 则 $f_T(T) = 0$

(2) 设 $A \in F^{n \times n}$ 则 $f_A(A) = 0$

通过取基, 我们知道上面两条是等价的. 当然, 直接代入的证明是错误的. 为了给出一个更加干净的证明, 我们引入环上的模的概念.

定义6.3.1 设集合 R 上有两个运算, 分别叫加法和乘法, 分别对 $x, y \in R$, 给出了新的元素, 我们记作 $x + y$ 和 $x \cdot y$

- (1) R 对加法构成交换群
- (2) R 对乘法构成一个半群 ($\forall x, y, z \in R, (xy)z = x(yz)$)
- (3) 加法和乘法有相容性, $x(y + z) = xy + xz, (x + y)z = xz + yz$

则称 R (连同这两个运算) 是环

进一步地, 如果乘法可交换, 我们称 R 是一个交换环. 进一步, 如果 R 还有1元素, 我们称 R 是一个交换幺环.

例6.3.1 一个 F -代数如 $(F^{n \times n}, L(V), F[x])$ 连同向量乘法和向量加法构成一个环. 而括号中的三个例子都是幺环, 并且 $F[x]$ 还是一个交换幺环. 对正整数 $n, \mathbb{Z}/n\mathbb{Z}$ 也是幺环

在交换幺环的定义当中, 我们没有要求 $1 \neq 0$, 这是由于我们经常讨论 R 商一个理想. 而为了把一个环商一个理想还叫环, 就做了这样的约定. 除了这个区别以外, 交换幺环和域的区别就在于非零元素是否可逆.

设 R 是一个交换幺环, 我们也可以定义矩阵 $R^{m \times n}$, 一切定义和域中的定义相同. 下面给出模的定义

定义6.3.2 设 R 是一个交换幺环, 对集合 V , 有运算

- 加法: $V \times V \rightarrow V, (\alpha_1, \alpha_2) \mapsto \alpha_1 + \alpha_2$, 使 V 成交换群

- 纯量乘法: $R \times V \rightarrow V, (c, \alpha) \mapsto c\alpha$, 满足

$$(c_1 + c_2)\alpha = c_1\alpha + c_2\alpha, c(\alpha_1 + \alpha_2) = c\alpha_1 + c\alpha_2, (c_1c_2)\alpha = c_1(c_2\alpha)$$

并且,我们还要求 $1\alpha = \alpha$

则称 V 连同这两个运算称作 R -模.

例6.3.2 任何一个Abel群可以看成 \mathbb{Z} -模, 事实上 \mathbb{Z} -模 \iff 交换群

而为了证明Cayley-Hamilton定理,我们考虑 $F[x]$ -模,我们说对于 $T \in L(V)$ 诱导了 V -上的一个 $F[x]$ -模结构.

事实上,对 $f \in F[x]$ 我们定义 $f\alpha = f(T)\alpha, \forall f \in F[x], \alpha \in V$. 这样定义以后,容易验证所有性质,这样就使得 V 成为了一个 $F[x]$ -模.

反过来,如果我们有了一个 $f[x]$ -模,我们考虑线性映射 $V \mapsto V : \alpha \mapsto x\alpha$, 记为 T , 从而和上面相同. 于是,我们可以说成一个线性空间加一个线性映射就成了一个 $F[x]$ 模.

设 V 是 R -模,我们可以考虑形式矩阵乘法 $V^n \times R^{m \times p} \rightarrow V^p$:

$$(\alpha_1, \dots, \alpha_n)A = (\beta_1, \dots, \beta_m), \text{ 满足 } \beta_j = \sum_{i=1}^n a_{ij}\alpha_i$$

A 容易验证 $(\alpha_1, \dots, \alpha_n)(AB) = ((\alpha_1, \dots, \alpha_n)A)B$

下面给出Cayley-Hamilton定理的证明

证明 仅考虑(1): 取 V 的有序基为 $B = \{\alpha_1, \dots, \alpha_n\}$ 记 $A = [T]_B$, 视 V 为 $F[x]$ 模. 我们有 $(\alpha_1, \dots, \alpha_n)A = (T\alpha_1, \dots, T\alpha_n) = (x\alpha_1, \dots, x\alpha_n) = (\alpha_1, \dots, \alpha_n)(xI_n)$

$$\Rightarrow (\alpha_1, \dots, \alpha_n)(xI_n - A) = (0, \dots, 0)$$

我们知道 $\forall A \in F^{n \times n}, \exists B \in F^{n \times n}$, 使得 $AB = \det(A)I_n$ (取 $B = \text{adj}(A)$) 而对于 $F[x]$, 我们在 $F(x)$ 考虑, 也有相同的结果. 并且 B 的元均在 $F[x]$ 中.

$$\text{取 } B \in F[x]^{n \times n} \text{ 使得 } (xI_n - A)B = \det(xI_n - A)I_n = f_T I_n$$

于是,由 $(\alpha_1, \dots, \alpha_n)(xI_n - A) = (0, \dots, 0) \Rightarrow (\alpha_1, \dots, \alpha_n)(xI_n - A)B = (0, \dots, 0)B \Rightarrow (\alpha_1, \dots, \alpha_n)f_T(T)I_n = 0 \Rightarrow f_T(T)\alpha_i = 0 \Rightarrow f_T(T)\alpha = 0 (\forall \alpha \in V) \Rightarrow f_T(T) = 0 \quad \square$

对于线性变换 T , 定义

$$M_T := \{f \in F[x] \mid f(T) = 0\}$$

对于 $f \in M_T$ 称作 T 的零化多项式.

下面说明 M_T 是 $F[x]$ 的理想, 显然 M_T 是子空间并且非空, 并且 $f \in M_T, g \in F[x] \Rightarrow fg \in M_T$ 并且 M_T 不是零理想, 并且由Cayley-Hamilton定理知 M_T 非空 (由线性空间的性质也可以得到这个命题). 但Cayley-Hamilton定理得到次数 $\leq n$.

而我们知道非零理想是主理想, 从而存在一个唯一的 M_T 的首项系数为1 的生成元 p_T , 将它称作 T 的最小多项式, 也称极小多项式 (minimal polynomial)

从而 $p \in F[x]$ 是最小多项式的充分必要条件是 $p(T) = 0, p$ 首一, 并且其它的非零的 T 的非零零化多项式的次数 $\geq \deg p_T$, 从而

$$f_T(T) = 0 \iff p_T \mid f_T$$

若 $V = \{0\}$, 约定 $f_T = p_T = 1$, 若 $\dim V \geq 1$, 则 $\deg p_T \geq 1$

命题6.3.1 p_T 和 f_T 具有相同的根.

证明 由于 p_T 的根是 f_T 的根, 下面说明 f_T 的根一定是 p_T 的根, 也就是说 p_T 保留了 f_T 所有的特征值.

$$\text{设 } f_T(c) = 0 \Rightarrow \exists \alpha \in V - \{0\}, T\alpha = c\alpha$$

设 $p_T = x^k + a_{k-1}x^{k-1} + \cdots + a_0$, 由于 $p_T(T) = 0$ 从而 $p_T(T)\alpha = 0$ 从而

$$\left(\sum_{i=0}^k a_i T^i \right) \alpha (a_k = 1) = \sum_{i=0}^k a_i (T^i \alpha) = \sum_{i=0}^k a_i c^i \alpha = p_T(c) \alpha = 0 \Rightarrow p_T(c) \alpha = 0$$

□

设 $\sigma(T) = \{c_1, \cdots, c_k\}$, $f_T = (x - c_1)^{e_1} \cdots (x - c_k)^{e_k}$, 从而由上面的命题得到 $p_T = (x - c_1)^{e_1} \cdots (x - c_k)^{e_k}$, 其中 $1 \leq e_k \leq d_k$, 一般来说, 我们无法进一步确定 e_i , 一般来说, 任给满足不等式控制要求的两个多项式 f_T, p_T , 存在一个线性空间 V 和线性映射 T , 使得 f_T, p_T 恰好就是以前所给的 f_T, p_T . 特别地, $d_i = 1 \Rightarrow p_T = f_T$, 其他情况要决定最小多项式, 要进行尝试.

对于矩阵, 我们有类似的定义. 对于矩阵 A , 考虑 A 的所有的零化多项式 $M_A := \{f \in F[x] | f(A) = 0\}$, 是一个非零理想. M_A 的唯一的首一生成元, 叫做 A 的最小多项式. 显然我们有 $p_{[T]_B} = p_T, p_{L_A} = p_A$, 这是因为它们均有相同的零化多项式. 且 $p_A | f_A \Rightarrow \deg p_A \leq n$, 且 p_A, f_A 有相同的根. 对于矩阵, 我们还有 $A \sim B \Rightarrow p_A = p_B$ (事实上, $B = P^{-1}AP$ $raf(B) = P^{-1}f(A)P$)

对于一个实矩阵, 将它看成实矩阵和看成复矩阵的最小多项式是否相同? 即将域扩大以后, 最小多项式有无可能变小? 事实上, 我们有下面的命题

命题6.3.2 设 $F_1 \subset F_2, A \in F_1^{n \times n}$, 则 A 作为 F_1 矩阵和 F_2 矩阵有相同的最小多项式.

证明 设两种看法, A 的最小多项式分别是 $p_1 \in F_1[x], p_2 \in F_2[x]$, 从而 $p_2 | p_1$, 设 $\deg p_2 = k, p_2 = x^k + \cdots + a_1 x + a_0$ 则

$$A^k + a_{k-1}A^{k-1} + \cdots + a_0A + a_0I = 0$$

视为关于 a_0, \cdots, a_{k-1} 的方程组, 则系数和常数项全都是 F_1 中的元素, 从而在 F_1 中有解 b_1, \cdots, b_{k-1} (命题1.4.4) 若 $q = x^k + b_{k-1}x^{k-1} + \cdots + b_1x + b_0 \in F_1[x] \Rightarrow \deg p_1 \leq \deg q = \deg p_2$

从而 $\deg p_1 = \deg p_2 \Rightarrow p_1 = p_2$ (否则 $p_1 - p_2$ 非零.) □

下面的定理给出了可对角化的另外一些判断方式

定理6.3.2 设 $T \in L(V)$, 则下面几条等价

(1) T 可对角化

(2) 若 $\sigma(T) = \{c_1, \cdots, c_k\}$, 则 $p_T = \prod_{i=1}^k (x - c_i)$

(3) p_T 是互不相伴的一次式的乘积.

证明 (2), (3) 等价是显然的.

(1) \Rightarrow (2): 取 \mathcal{B} , 使得 $[T]_{\mathcal{B}} = \begin{pmatrix} c_1 I_{d_1} & & \\ & \cdots & \\ & & c_k I_{d_k} \end{pmatrix}$ 从而 $\forall f \in F[x], f([T]_{\mathcal{B}}) = \begin{pmatrix} f(c_1) I_{d_1} & & \\ & \cdots & \\ & & f(c_k) I_{d_k} \end{pmatrix}$

从而 $f([T]_{\mathcal{B}}) = 0 \Rightarrow (x - c_1)(x - c_2) \cdots (x - c_k) | f \Rightarrow p_T = (x - c_1) \cdots (x - c_k)$

(2) \Rightarrow (1):

引理6.3.1 设 $\dim V < \infty, T_1, \cdots, T_k \in L(V)$ 则

$$\dim \text{Ker}(T_1 \cdots T_k) \leq \sum_{i=1}^k \dim \text{Ker}(T_i)$$

引理的证明: 只需考虑 $k = 2$ 的情况. 这是容易证明的

下面回到原命题, 由 (2), $\prod_{i=1}^k (T - c_i \text{id}) = 0$, 从而 $\sum_{i=1}^k \dim \text{Ker}(V_{c_i}) = \dim \bigoplus_{i=1}^k V_{c_i} \Rightarrow T$ 可对角化. □

对于矩阵,我们显然有如下平行的结论

推论6.3.1 设 $A \in F^{n \times n}$, 则下面几条等价

(1) A 可对角化

(2) 若 $\sigma(A) = \{c_1, \dots, c_k\}$, 则 $p_T = \prod_{i=1}^k (x - c_i)$

(3) p_A 是互不相伴的一次式的乘积.

设 $f_A = \prod_{i=1}^k (x - c_i)^{d_i}$ 则 A 可对角化 $\prod_{i=1}^k (A - c_i I_n) = 0$

6.4 Invariant Subspaces

不变子空间的定义前面已经提到过,一维不变子空间和特征向量是同一回事.我们知道 $\{0\}, V, \text{Ker } T, \text{Im } T$ 都是不变子空间.

例6.4.1 $A = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \theta \notin \pi\mathbb{Z}$. 考虑 $L_A \in L(\mathbb{R}^{2 \times 1})$ 的特征子空间,2维不变子空间即 \mathbb{R} , 而没有一维特征子空间.因此 L_A 没有非平凡的不变子空间.

我们有如下性质

- W 是 T 不变的, $f \in F[x]$, 则 W 也是 $f(T)$ 不变的. 即 $\alpha \in W, f(T)\alpha$ 也要 $\in W$.

事实上, 设 $f = \sum a_i x^i, f(T)\alpha = \sum a_i T^i \alpha \in W$.

- 若 $T, U \in L(V), TU = UT$, 则 $\text{Ker}(U), \text{Im}(U)$ 都是 T -不变子空间

事实上, 设 $\alpha \in \text{Ker}(U)$ 则 $T\alpha \in \text{Ker}(U) \Leftrightarrow UT\alpha = 0 \Leftrightarrow TU\alpha = 0$ 成立. 而 $\alpha \in \text{Im}(U)$ 则 $\exists \beta \in V, \alpha = U\beta \Rightarrow T\alpha = TU\beta = UT\beta \in \text{Im}(U)$

- 若 U, T 可交换, 则 $U, f(T)$ 可交换 $\Rightarrow \text{Ker}(f(T))$ 是 U 不变. 特别地 $\text{Ker}(c \cdot \text{id}_V - T)$ 是 U 不变. \Rightarrow 所有的 T 的特征子空间都是 U 不变的, 特别地 T 的特征子空间也是 T 不变的. 当然, 这个结论直接验证也很容易.

由于 T 可对角化 $\Leftrightarrow V = \bigoplus_{c \in \sigma(T)} V_c$. 另一方面, 如果 $V = \bigoplus_{i=1}^k W_i$ 其中 W_i 都是 T 不变子空间. 这样, 我们考虑映射 $T|_{W_i} : W_i \rightarrow V$ 就成为了 $W_i \rightarrow W_i$, 将此映射记为 T_{W_i} . 因此, 如果 V 有一个直和分解, 其中每个部分都是 T 不变的. 则研究 T 的性质就只需在每个部分上研究, T 在 W_i 上的行为唯一决定了 T 在 V 上的行为.

若取 W_i 的一组基拼成 V 的一组基 \mathcal{B} , 则 $T_{\mathcal{B}}$ 就是分块矩阵. 我们知道 $T_{V_c} = c \cdot \text{id}_V$. 以后我们要做的就是想办法将 V 分成若干尽量小的不变子空间的直和. 如果 V 不能写成两个非平凡的 T 不变子空间的直和, 则称 V 是 T -不可约的. 以后我们将要证明 T 不可约等价于准素或者循环.

设 $W \subset V$ 是 T 不变的, $T_W \in L(W), T_W \alpha = T\alpha$, 同时 T 还诱导了一个商空间上的一个线性变换, $T \in L(V/W), T_{V/W}(\alpha + W) = T\alpha + W$. 由于 T 不变, 则这个映射是良定的.

下面考虑表示矩阵的性质, 设 $\mathcal{B}_1 = \{\alpha_1, \dots, \alpha_r\}$ 是 W 的基, 扩充为 V 的有序基 $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$. 则 $\alpha_{r+1} + W, \dots, \alpha_n + W$ 是 V/W 的一组基. 设 $A = [T]_{\mathcal{B}}$ 形如 $\begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$, 其中 $B \in F^{r \times r}, C \in F^{r \times n-r}, D \in F^{n-r} \times n-r$

容易发现 $[T_W]_{\mathcal{B}_1} = B, [T_{V/W}]_{\mathcal{B}_2} = D$, 但“丢失”了 C 的信息. 但仍然这个映射仍然是一个很重要的映射.

于是 $\det(T) = \det(T_W) \det(T_{V/W})$, 从而 $f_T = f_{T_W} f_{T_{V/W}}$ 一般来说, 最小多项式没有这样的性质, 但仍然有一些联系.

定义6.4.1 设 $f_1, \dots, f_k \in F[x]$ 是若干多项式. 考虑理想 $\bigcap_{i=1}^k (f_i)$ 的唯一的非零生成元叫做它们的最小公倍式(least common multiple). 记作 $\text{lcm}(f_1, \dots, f_n)$

我们有 $\text{lcm}(p_{T_W}, p_{T_{V/W}}) | p_T | p_{T_W} p_{T_{V/W}}$, 如果 $(p_{T_W}, p_{T_{V/W}})$, 则 $p_T = p_{T_W} p_{T_{V/W}}$

事实上, 由于 $p_T(T) = 0 \Rightarrow p_T(T_W) = 0, p_T(T_{V/W}) = 0 \Rightarrow p_{T_W} | p_T, p_{T_{V/W}} | p_T$, 从而 $\text{lcm}(p_{T_W}, p_{T_{V/W}}) | p_T$. 而对 $\forall \alpha, p_{T_{V/W}} \alpha = p_{T_{V/W}}(T)\alpha$. 而我们有 $\forall f, f(T)\alpha + W = f(T_{V/W})(\alpha + W)$, 从而 $p_{T_{V/W}} \alpha + W = 0$, 于是, 对任意 $\alpha, p_{T_{V/W}} \alpha \in W$. 于是 $p_{T_W}(p_{T_{V/W}} \alpha) = 0 (\forall \alpha)$. 从而 $p_T | p_{T_W} p_{T_{V/W}}$

推论6.4.1 若 T 可对角化, 则 $T_W, T_{V/W}$ 也可对角化.

证明 可对角化 $\iff p$ 是互不相同的一次式的乘积, 从而 $p_{T_W}, p_{T_{V/W}}$ 的互不相同的乘积, 从而两个小映射也可对角化. \square

下面用上面得到的一些结论讨论一些性质.

6.5 Simultaneous Triangulation; Simultaneous Diagonalization

定义6.5.1 (1) $\mathcal{F} \subset L(V)$, 若存在有序基 \mathcal{B} 使得 $\forall T \in \mathcal{F}, [T]_{\mathcal{B}}$ 对角. 则称 \mathcal{F} 可同时对角化.

(2) $\mathcal{M} \subset F^{n \times n}$, 若存在 $G \in GL_n(F)$, 使得 $\forall A \in \mathcal{M}, P^{-1}AP$ 是对角矩阵, 则称 \mathcal{M} 可同时对角化.

对此我们有

定理6.5.1 \mathcal{F} 可同时对角化 $\iff \mathcal{F}$ 中的映射都可对角化并且两两可交换.

证明 “ \implies ”: 显然成立(由于对角矩阵可交换)

“ \impliedby ”: 对 $\dim V$ 归纳. $\dim V = 1$ 时两边条件自然成立. 假设维数小的时候成立. 不妨设 $T \in \mathcal{F}$, 不是恒同映射 id_V 的常数倍. 则 $\forall c \in \sigma(T)$, 有 $\dim V_c = \dim \text{Ker}(cI - T) < \dim V$, 由于所有的映射均和 T 可交换, 从而 V_c 是 F 中所有的映射的不变子空间.

考虑 $\mathcal{F}_c := \{U_{V_c} | U \in \mathcal{F}\}$, 从而 \mathcal{F}_c 中的线性变换也两两可交换且均可对角化. \implies 存在 V_c 的有序基 \mathcal{B}_c , 其中向量都是 U 的特征向量 ($\forall U \in \mathcal{F}$).

由于 T 可对角化, 从而 $V = \bigoplus_{c \in \sigma(T)} V_c \implies \mathcal{B} := \bigcup_{c \in \sigma(T)} \mathcal{B}_c$ 是 V 的基. 于是 $[U]_{\mathcal{B}}$ 对角, $\forall U \in \mathcal{F}$ \square

推论6.5.1 $\mathcal{M} \subset F^{n \times n}$ 可同时对角化的充分必要条件是 \mathcal{M} 中矩阵全都可对角化并且两两可交换.

下面考虑可三角化的问题. 先讨论一个矩阵的情况

定义6.5.2 (1) $\mathcal{F} \subset L(V)$, 若存在有序基 \mathcal{B} 使得 $\forall T \in \mathcal{F}, [T]_{\mathcal{B}}$ 上三角. 则称 \mathcal{F} 可三角化.

(2) $\mathcal{M} \subset F^{n \times n}$, 若存在 $G \in GL_n(F)$, 使得 $\forall A \in \mathcal{M}, P^{-1}AP$ 是上三角矩阵, 则称 \mathcal{M} 可三角化.

注 考虑

$$J_n = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

则 $(J_n)^{-1}$ (上三角) J_n = (下三角) 从而上三角化和下三角化是同一回事. 统称为三角化

我们有如下的结论

定理6.5.2 设 $\dim V = n, T \in L(V)$, 则下面几条性质等价

(1) T 可三角化

(2) f_T 在 $F[x]$ 中可分解为一次式的积

(3) p_T 在 $F[x]$ 中可分解为一次式的积

(4) 存在一串 T 的不变子空间 $\{0\} = W_0 \subset \cdots \subset W_n = V$,使得 $\dim W_i = i$.这样子空间串称作空间的一个旗(flag),为了强调每个空间都出现,也可叫做全旗(full flag)或完备旗(complete flag)

证明 (1) \implies (2): 设 $A = [T]_{\mathcal{B}}$ 上三角 $\implies f_T = \det(xI - A) = \prod_{i=1}^n (x - A_{ii})$

(2) \implies (3): 更显然

(3) \implies (4): 归纳构造这串子空间 W_k ,取 $W_0 = \{0\}$,假设已经有 W_{k-1} 已构造, $1 \leq k \leq n$,考虑 $T_{V/W_{k-1}}(\alpha + W_{k-1}) = T\alpha + W_{k-1}$.而想要构造 W_k 只需要证明在 V/W_{k-1} 中存在一维 $T_{V/W_{k-1}}$ -不变子空间.即 $T_{V/W_{k-1}}$ 有特征向量.即有特征值即可,由于 p_T 是一次式的乘积,从而 $p_{T_{V/W_{k-1}}}$ 也是一次式的乘积.故有特征向量

(4) \implies (1): 取 $\mathcal{B} = \{\alpha_1, \cdots, \alpha_n\}$ 使得 $\{\alpha_1, \cdots, \alpha_n\}$ 是 W_i 的基 $1 \leq i \leq n$.考虑 $A = [T]_{\mathcal{B}}$. 即 $W_j \ni T\alpha_j = \sum_{i=1}^n A_{ij}\alpha_i \implies$ 当 $i > j$ 时, $A_{ij} = 0$,从而 A 是上三角矩阵. \square

推论6.5.2 若 F 是代数闭域,每个 $n \times n$ 的矩阵都可上三角化.

以后还有

定理6.5.3 (Schur三角化定理) 任意矩阵酉相似于上三角矩阵

下面考虑可同时三角化的问题

定理6.5.4 设 F 是代数闭域, $\mathcal{F} \subset L(V)$ 中的映射两两可交换,则存在一个 V 的有序基 \mathcal{B} ,使得 $[T]_{\mathcal{B}}$ 上三角, $\forall T \in \mathcal{F}$

证明 先证明如下引理

引理6.5.1 设 F 是代数闭域, $\mathcal{F} \subset L(V)$ 中的映射两两可交换,则 \mathcal{F} 中的映射存在公共的特征向量.

从引理推定理则比较容易,这是由于可以推出存在空间中的完备旗.使得在每个 F 中的向量均在 \mathcal{F} 中的映射是不变的,再类似于商掉 W_{k-1} 即可. \square

6.6 Direct-Sum Decompositions

为了进一步讨论空间的可对角化的性质,我们考虑另一个概念即空间的直和.

定义6.6.1 设 V_1, \cdots, V_k 是 k 个 F 线性空间.考虑 $V_1 \times \cdots \times V_k := \{(\alpha_1, \cdots, \alpha_k) | \alpha_i \in V_i\}$,记 $\bigoplus_{i=1}^k V_i = \{(\alpha_1, \cdots, \alpha_k) | \alpha_i \in V_i\}$ 定义 $(\alpha_i) + (\beta_i) = (\alpha_i + \beta_i), c(\alpha_i) = (c\alpha_i)$ 这个新的线性空间叫做 V_1, \cdots, V_k 的外直和.

我们可以将每个 V_i 看做外直和的子空间,事实上,考虑映射

$$\tau_i : V_i \rightarrow \bigoplus_{i=1}^k V_i : \tau_i(\alpha) = (0, 0, \cdots, \alpha_i, 0, \cdots, 0)$$

引理6.6.1 设 \mathcal{B}_i 为 V_i 的基,则 $\bigcup_{i=1}^k \tau_i(\mathcal{B}_i)$ 是 $\bigoplus_{i=1}^k V_i$ 的一组基

证明 $\forall (\alpha_1, \cdots, \alpha_k) \in \bigoplus \implies \tau_i(\alpha_i) \in \text{span} \tau_i(\mathcal{B}_i)$ 从而生成全空间,而容易验证线性无关. \square

从而,如果每个 V_i 是有限维的,就有

$$\dim \bigoplus_{i=1}^k V_i = \sum_{i=1}^k \dim V_i$$

接下来考虑内直和,对给定的空间 $V, V_1, \dots, V_k \subset V$,我们有外直和 $\bigoplus_{i=1}^k V_i$,考虑映射 $\Phi: \bigoplus_{i=1}^k V_i \rightarrow V$:

$$\Phi(\alpha_1, \dots, \alpha_n) \mapsto \sum_{i=1}^k \alpha_i. \text{ 则 } \text{Im}(\Phi) = \sum_{i=1}^k V_i$$

若 Φ 是单映射,即 $\text{Ker } \Phi = 0$,我们称 V_1, \dots, V_k 叫做无关的子空间.此时,称和 $\sum_{i=1}^k V_i$ 为 V_1, \dots, V_k 叫做内直和.

此时,外直和与内直和同构.

引理6.6.2 设 $V_1, \dots, V_k \subset V$,则下面几条命题等价:

(1) 无关

$$(2) \alpha_i \in V_i, \sum_{i=1}^k \alpha_i = 0 \Rightarrow \alpha_i = 0$$

$$(3) \forall i \in \{2, \dots, k\}, V_i \cap (V_1 + \dots + V_{i-1}) = \{0\}$$

$$(4) \text{ 任给 } V_i \text{ 的基两两不相交,并且 } \bigcup_{i=1}^k \text{ 是 } \sum_{i=1}^k V_i \text{ 的一组基}$$

(5) 若空间有限维,还等价于

$$\dim \sum_{i=1}^k V_i = \sum_{i=1}^k \dim V_i$$

证明 (1) \Rightarrow (2)是显然的,只是将定义换了一种语言叙述

(2) \Rightarrow (3),设 $\alpha \in V_i \cap (V_1 + \dots + V_{i-1}) \Rightarrow \exists \alpha_1 \in V_1, \dots, \alpha_{i-1} \in V_{i-1}$ 使得 $\alpha = \alpha_1 + \dots + \alpha_{i-1}$.考虑 $\Phi(\alpha_1, \dots, \alpha_{i-1}, -\alpha, 0, \dots, 0) = 0$ 由(2) $\Rightarrow \alpha = 0$

(3) \Rightarrow (2)设 $\alpha \in V_i, \sum \alpha_i = 0$, 若(2)不成立,取使 $\alpha_i \neq 0$ 的成立的最大指标 i_0 ,则 $i_0 \geq 2$,将(3)中的 i 取成 i_0 即得矛盾.

(1) \Leftrightarrow (4) 显然

(1) \Leftrightarrow (5) 显然 □

(3)还有一个加强的版本,即 $\forall i \in \{2, \dots, k\}, V_i \cap (V_1 + \dots + V_{i-1} + V_{i+1} + \dots + V_n) = \{0\}$, 其证明也是比较简单的.

另外,在取 τ_i 之后内直和和外直和是同一回事,因此外直和和内直和是同一回事.内直和和外直和有非常紧密的联系,因此在不引起歧义的情况下,我们将内直和和外直和都简称为直和.

下面回到(6.2)节

6.7 Invariant Direct Sum

对 $T \in L(V)$,若 $V = \sum_{i=1}^k W_i, T_i = T|_{W_i}$,都是不变子空间.此时我们也称 $T = \bigoplus_{i=1}^k T_i$.

T 的性质也就是由 T_i 决定,比如 $\det T = \prod \det T_i, f_T = \prod f_{T_i}$,也可以验证 $p_T = \text{lcm}(p_{T_1}, \dots, p_{T_k}), \text{Ker}(T) =$

$$\bigoplus_{i=1}^k \text{Ker}(T_i), \text{Im}(T) = \bigoplus \text{Im}(T_i).$$

我们要做的是两种分解,一种叫做准素分解,一种叫做循环分解.两种分解合在一起的每个小块叫做“准素循环分解”,而这是最基本的分解.准素分解是唯一的,循环分解不唯一,因此准素循环分解也不唯一.但在同构的意义下是唯一的.循环分解得到有理标准型,准素循环分解得到Jordan标准型.两种标准型用的都比较多,有理标准型不依赖于域,而Jordan标准型需要特征多项式能够分解成一次因式的乘积.但普遍来讲,Jordan标准型用的多一点.

6.8 The Primary Decomposition Theorem

先考虑准素分解.

定义6.8.1 称 $T \in L(V)$ 是准素的(primary),如果 p_T 是素多项式的幂.

这个条件依赖于域.比如 $(x^2 + 1)^3$ 在 \mathbb{R} 上准素. \mathbb{C} 上不准素.我们也称作 T 在 V 上的作用是准素的.或 V 作为 $F[x]$ 模是准素的.

定理6.8.1 (准素分解定理) 设 $T \in L(V)$,设 $p_T = \prod_{i=1}^k p_i^{r_i}$, p_1, \dots, p_k 是互不相同的首项系数为1的素多项式.这种分解是唯一的.记 $W_i = \text{Ker}((p_i)^{r_i}(T))$.则每个 W_i 都是 T -不变子空间. $(p_i^{r_i}(T)$ 与 T 可交换).则 $V = \bigoplus_{i=1}^k W_i$ 记 $T_i = T|_{W_i}$,则 $p_{T_i} = p_i^{r_i}$

证明 先证明 $W_i \neq \{0\}$,记 $q_i = \prod_{j \neq i} p_j^{r_j}$,则 $p_i^{r_i}(T)q_i(T) = p(T)T = 0$,且 $q_i(T) \neq 0$,因此 $p_i^{r_i}(T)$ 不可逆,从而 $W_i \neq 0$

接下来证明 W_i 无关,设 $\alpha_i \in W_i$, $\sum_{j=1}^k \alpha_j = 0$,用模的语言叙述(为了少一个 T),两边乘 q_i ,得 $q_i \alpha_i = 0$,又由于 $p_i^{r_i} \alpha_i = 0$,又存在 $a, b \in F[x]$,使得 $a q_i + b p_i^{r_i} = 1 \Rightarrow a(q_i \alpha_i) + b(p_i^{r_i} \alpha_i) = 1 \alpha_i = \alpha_i \Rightarrow \alpha_i = 0$,从而确实是无关的子空间

再证明 $\sum_{i=1}^k W_i = V$,又 q_1, \dots, q_k 互素 $\Rightarrow \exists a_1, \dots, a_k \in F[x]$ 使得 $\sum_{i=1}^k a_i q_i = 1$. 对 $\forall \alpha \in V$,则 $q_i \alpha_i \in W_i \Rightarrow \alpha = 1 \alpha = \left(\sum_{i=1}^k a_i q_i \right) \alpha$,且 $q_i \alpha_i \in W_i$,因此 $\sum_{i=1}^k W_i = V$.

最后证明 $p_{T_i} = p_i^{r_i}$.首先由于 $\forall \alpha \in V$, $p_i^{r_i} \alpha_i = 0 \Rightarrow p_i^{r_i}(T_i) = 0 \Rightarrow p_{T_i} | p_{r_i}$ 由对于 $\alpha \in V$, $\left(\prod_{i=1}^k p_{T_i} \right) \alpha = \left(\prod_{i=1}^k p_{T_i} \right) \left(\sum_{i=1}^k \alpha_i \right) = \sum_{i=1}^k \left(\prod_{i=1}^k p_{T_i} \alpha_i \right) = 0$ 因此 $p_T | \prod_{i=1}^k p_{T_i}$ \square

我们也把每个 W_i 称作 V 的一个准素分类.

第七章 The rational and Jordan Forms

7.1 Cyclic Subspaces and Annihilators

记 $R := F[x]$, 以后 $F[x]$ 模称作 R -模. 我们曾经记 $F\alpha = \text{span}\{\alpha\}$, 同理定义 $R\alpha := \{f\alpha | f \in R\}$, 则 $R\alpha = \text{span}\{\alpha, T\alpha, T^2\alpha, \dots\}$. 记 $R\alpha$ 为叫做由 α 生成的循环子空间, 或称为循环子模. α 称作 $R\alpha$ 的循环向量. $R\alpha$ 有一些性质, 注意这些性质都和 T 有关.

- $R\alpha$ 是包含 α 的最小的不变子空间.
- $\dim R\alpha = 1 \iff \alpha$ 是特征向量.
- 若 $V = R\alpha$, 称 α 为 V 中的循环向量. 即 V 是循环模.
- 若 V 中存在循环向量, 则称 T 是循环的, 同时也称 V 作为 R -模是一个循环模.

例 7.1.1 记 $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $V = F^{2 \times 1}$, $T = L_A$, $\varepsilon_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\varepsilon_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. 则 $T\varepsilon_1 = \varepsilon_2$, $T\varepsilon_2 = 0$.

此时 $R\varepsilon_1 = V$ 是循环模, 但不是每个向量都是循环向量, 且 $R\varepsilon_2 = F\varepsilon_2$

考虑映射 $\Delta : V \rightarrow \mathbb{Z}$, $\Delta(\alpha) := \dim R\alpha$. 注意它也 and T 有关. 在这样的定义下, T 循环 $\iff \Delta$ 的最大值为 $\dim V$. 此时 α 是循环向量 $\iff \Delta$ 在 α 处取得最大值.

定义 7.1.1 对 $\alpha \in V$, 记 $M(\alpha) := \{f \in R | f\alpha = 0\}$. 称作 α 的零化理想 (见下面的叙述), 称其首项系数为 1 的生成元记作 p_α , 称为 α 的零化子 (annihilator)

$M(\alpha)$ 是理想, 事实上 $p_T \in M(\alpha)$, $f, g \in M(\alpha) \Rightarrow f + cg \in M(\alpha)$, $f \in M(\alpha), g \in R \Rightarrow fg \in M(\alpha)$. 且 $p_\alpha | p_T, \alpha = 0 \iff M(\alpha) = R \iff p_\alpha = 1$

引理 7.1.1 记 $d = \deg p_\alpha$, 则 $\{\alpha, T\alpha, \dots, T^{d-1}\alpha\}$ 是 $R\alpha$ 的基, 因此 $\Delta\alpha = \deg p_\alpha$.

证明 线性无关: $\sum_{i=0}^{d-1} c_i T^i \alpha = 0$, 记 $g = \sum_{i=0}^{d-1} c_i x^i$, 则 $g\alpha = 0 \Rightarrow p_\alpha | g$, 又由于 $\deg g < \deg p_\alpha \Rightarrow g = 0$

生成全空间: $\forall \beta \in R\alpha, \exists f \in R, \beta = f\alpha$. 设 $f = qp_\alpha + r, q, r \in R, \deg r < d$. 从而 $f\alpha = r\alpha \in \{\alpha, T\alpha, \dots, T^{d-1}\alpha\}$ □

从而若 $p_T < \dim V \Rightarrow T$ 不循环. 下面我们证明 $p_T < \dim V \iff T$

引理 7.1.2 存在 α , 使得 $p_\alpha = p_T$

证明 先设 T 准素, 即 $p_T = p^r$, 其中 p 素, $r \geq 1$. 则 $\forall \alpha \in V, p_\alpha = p^{r_\alpha} (0 \leq r_\alpha \leq r)$, 即要证明存在 α , 使得 $r_\alpha = r$. 若 $\forall \alpha, r_\alpha < r \Rightarrow p^{r-1}\alpha = 0 (\forall \alpha) \Rightarrow p_{r-1}(T) = 0$. 矛盾!

一般地, 设 $p_T = p_1^{r_1} \cdots p_k^{r_k}$. 记 $W_i = \text{Ker}(p_i^{r_i}(T)), V = \bigoplus_{i=1}^k W_i, T_{W_i}$ 准素, $p_{T_{W_i}} = p_i^{r_i}$. 则存在 α_i 的零化子 $p_{\alpha_i} = p_{W_i} = p_i^{r_i}$, 下面考虑 $\alpha = \alpha_1 + \cdots + \alpha_k$.

则 $0 = p_\alpha \alpha = p_\alpha \alpha_1 + \cdots + p_\alpha \alpha_k$, 因此由于 W_i 无关, $p_\alpha \alpha_i = 0 \Rightarrow p_i^{r_i} | p_\alpha \Rightarrow p_\alpha = p_T$ □

从上面的引理,我们知道 $\max \dim R\alpha = \max \deg p_\alpha = \deg p_T$. 从而有如下的命题

命题7.1.1 T 是循环的 $\iff \deg p_T = \dim V \iff p_T = f_T$, 此时 α 是循环向量 $\text{ldap}_\alpha = p_T$

下面讨论 T 循环的时候, 矩阵表示能够多简单.

对 $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, 考虑

$$c_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}_{n \times n}$$

称为 f 的相伴矩阵 (companion matrix)

命题7.1.2 设 $\dim V = n, T \in L(V)$

(1) 若 T 循环, α 是循环向量, 则 T 在 $\{\alpha, \cdots, T^{n-1}\alpha$ 下的矩阵为 $c_{p_\alpha} = c_{p_T}$.

(2) 若存在一组基 \mathcal{B} , 使得 $[T]_{\mathcal{B}} = c_f$, 则 T 循环, 且 $p_T = f$

证明 若 $\mathcal{B} = \{\alpha_1, \cdots, \alpha_n\}$, 则 $[T]_{\mathcal{B}} = c_f \iff T\alpha_1 = \alpha_2, \cdots, T\alpha_{n-1} = \alpha_n, T\alpha_n = -a_0\alpha_1 - \cdots - a_{n-1}\alpha_n$

(1) 记 $\alpha_i = T_{i-1}\alpha, 1 \leq i \leq n$, 则对 $f = p_\alpha$ 时, $T\alpha_1 = \alpha_2, \cdots, T\alpha_{n-1} = \alpha_n, T\alpha_n = -a_0\alpha_1 - \cdots - a_{n-1}\alpha_n$ 成立.

(2) 由上式可以推出 α_1 是循环向量. 从而 $f_{\alpha_1} = 0 \Rightarrow p_{\alpha_1} | f \Rightarrow p_{\alpha_1} = f$, 从而成立 □

由此也得到 f_T 的特征多项式为 f , 即 $f_{c_f} = \det(xI_n - c_f) = f$

由此也可以得到 Cayley-Hamilton 定理的另一个证明.

想证 $f_T(T) = 0 \Rightarrow f_T\alpha = 0, \forall \alpha \in V$. 考虑 $R\alpha, f_{T_{R\alpha}} = \det f_{c_{p_\alpha}} = p_\alpha \Rightarrow f_{T_{R\alpha}}\alpha = 0$, 又由于 $f_{T_{R\alpha}} | f_T \Rightarrow f_T(\alpha) = 0$

7.2 Cyclic Decompositions and the Rational Form

定理7.2.1 设 $T \in L(V)$, 则存在 $\alpha_1, \cdots, \alpha_r \in V - \{0\}$, 使得

(1) $V = \bigoplus_{i=1}^r R\alpha_i$

(2) 记 $p_i = p_{\alpha_i}$, 则 $p_r | p_{r-1} | \cdots | p_1 = p_T$

整数 r 和序列 p_1, \cdots, p_r 被 T 唯一决定.

记 $T_i = T_{R\alpha_i}$, 则 $T = T_1 \oplus \cdots \oplus T_r, f_T = f_{T_1} \cdots f_{T_r}, p_T = \text{lcm}\{p_1, \cdots, p_r\}$

因此 $f_T = p_1 \cdots p_r, p_T = p_1$, 这样也推出了 f_T 和 p_T 有相同的素因式.

引理7.2.1 设 $\alpha \in V$,

(1) 对 $L \in R/L_\alpha$ 和 $\beta \in L, R\alpha \cap R\beta = 0 \iff p_\beta = p_L$

(2) 若 $p_\alpha = p_T$, 总存在 $\beta \in L$, 使得 $p_\beta = p_L$

证明 (1) “ \implies ” 总有 $p_L = p_\beta$, 事实上 $p_\beta L = p_\beta(T_{V/R\alpha})(\beta + R\alpha) = p_\beta(T)\beta + R\alpha = 0. p_L L = 0 \implies$

$p_L\beta \in R\alpha$, 事实上 $p_L L = p_L(T_{V/R\alpha})(\beta + R\alpha) = p_L(T)\beta + R\alpha = 0$

从而若 $R\alpha \cap R\beta = 0 \Rightarrow p_\beta | p_L \Rightarrow p_\beta = p_L$

” \impliedby ”, $\forall \delta \in R\alpha \cap R\beta$, 则 $\delta = q\beta \in R\alpha \Rightarrow qL = 0 \Rightarrow p_L | q \Rightarrow p_\beta | q \Rightarrow \delta = 0$

(2) 取 $\beta_0 \in L$, 则 $p_L \beta_0 \in R\alpha$ 即存在 f , 使得 $p_L \beta = f\alpha$. (此处补笔记) □

下面回到循环分解定理的证明

证明 存在性: 对 $\dim V$ 用归纳法. 若 $\dim V = 1$, 显然成立. 假设 $\dim V$ 小的时候成立.

取 α_1 使得 $p_{\alpha_1} = p_T$, 考虑商空间 $V/R\alpha_1$, $\dim V/R\alpha_1 < \dim V$. 对商空间和映射 $T_{V/R\alpha_1}$ 用归纳假设, 从而存在 $L_2, \dots, L_r \in V/R\alpha_1$, 使得 $V/R\alpha_1 = \bigoplus_{i=2}^r RL_i, p_{L_r} | \dots | p_{L_2}$.

由引理, 存在 $\alpha_i \in L_i$, 使得 $p_{\alpha_i} = p_{L_i}, R\alpha_1 \cap R\alpha_i = \{0\}$, 因此整除的链式关系已经成立. 下面去验证 $V = \bigoplus_{i=1}^r R\alpha_i$.

无关: 设 $\sum_{i=1}^r g_i \alpha_i = 0$ 投射到商空间, $\Rightarrow \sum_{i=2}^r (g_i \alpha_i + R\alpha_1) = 0 \Rightarrow \sum g_i L_i = 0 \Rightarrow g_2 L_2 = \dots = g_r L_r = 0$. 从而 $g_2 \alpha_2, \dots, g_r \alpha_r \in R\alpha_1$. 而 $g_i \alpha_i \in R\alpha_i \Rightarrow g_i \alpha_i \in R\alpha_1 \cap R\alpha_i = \{0\}$, 从而 $g_2 \alpha_2 = \dots = g_r \alpha_r = 0 \Rightarrow g_1 \alpha_1 = 0$. 从而无关.

再证明和为全空间. 由于 $\forall \gamma \in V, \gamma + R\alpha_1 \in V/R\alpha_1$, 设其为 $\sum_{i=2}^r g_i L_i$, 因此 $\gamma - g_i \alpha_i \in R\alpha_1$, 从而 $\gamma \in R\alpha_1 + \dots + R\alpha_r$.

唯一性: 我们称 p_1, \dots, p_r 为 T 的不变因子, 整体构成不变因子序列. 粗略地说不变因子序列完全决定了 T 的行为.

我们去说明如果有两组向量, 则 r 和 p_{α_i} 是一样的. 但 $R\alpha_i$ 不一定一样. 设 $\alpha_1, \dots, \alpha_r \in V - \{0\}$, 满足 $V = \bigoplus_{i=1}^r R\alpha_i, p_{\alpha_r} | \dots | p_{\alpha_1}$. 设 β_1, \dots, β_s 也满足 $V = \bigoplus_{i=1}^s R\beta_i, p_{\beta_s} | \dots | p_{\beta_1}$. 假设该结论不成立. 设 t 是使得 $p_{\alpha_t} \neq p_{\beta_t}$ 不相等的最小指标. 由反证假设 $t \leq \min\{r, s\}$ 且一定存在 (由于次数的和为定值). 不妨设 $p_{\beta_t} \nmid p_{\alpha_t}$. 将直和的式子的两端同时乘 p_{α_t} . (即取 $p_{\alpha_t}(T)$). 从而

$$p_{\alpha_t} \left(\bigoplus_{i=1}^r R\alpha_i \right) = p_{\alpha_t} \left(\bigoplus_{i=1}^s R\beta_i \right)$$

因此

$$\bigoplus_{i=1}^r Rp_{\alpha_t} \alpha_i = \bigoplus_{i=1}^s Rp_{\alpha_t} \beta_i$$

而由于整除关系, 上式左端即 $\bigoplus_{i=1}^{t-1} Rp_{\alpha_t} \alpha_i$, 而右端等于 $\left(\bigoplus_{i=1}^{t-1} Rp_{\alpha_t} \beta_i \right) \oplus \left(\bigoplus_{i=t}^s Rp_{\alpha_t} \beta_i \right)$

下面断言: 当 $1 \leq i \leq t-1 \Rightarrow \dim Rp_{\alpha_t} \alpha_i = \dim Rp_{\alpha_t} \beta_i$.

在断言成立的情况下, $p_{\alpha_t} \beta_t = 0 \Rightarrow p_{\beta_t} | p_{\alpha_t}$. 矛盾! 从而只需验证断言: 记 $p_\alpha = fg, f, g$ 首一. $f\alpha$ 的零化子就是 g (容易验证). 而 $\dim Rp_{\alpha_t} \alpha_i = \deg p_{p_{\alpha_t} \alpha_i} = \deg p_{\alpha_i} - \deg p_{\alpha_t}$. 而另一边同理. 从而成立. □

考虑全空间的一组基 $\mathcal{B}_i = \{\alpha_i, T\alpha_i, \dots, T^{d-1}\alpha_i\}$ 是 $R\alpha_i$ 的有序基. 从而 $[T_{R\alpha_i}]_{\mathcal{B}_i} = c_{p_i}$ 为相伴矩阵. 从而, 记 $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_r), [T]_{\mathcal{B}} = \begin{pmatrix} c_{p_1} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & c_{p_r} \end{pmatrix}$. 称作其为有理型矩阵 (p_r, \dots, p_1) . 从而, 由循环分解定理, 我们得到

推论 7.2.1 存在基 \mathcal{B} 使得 $[T]_{\mathcal{B}}$ 是有理型矩阵, 且矩阵被 T 唯一确定. 称作 T 的有理标准型. (有可能 \mathcal{B} 没有唯一决定.)

证明 存在性显然. 下证唯一性. 设 $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_r)$, 其中 $|\mathcal{B}_i| = \deg p_i$. 记 $W_i = \text{span} \mathcal{B}_i$ 是 T 不变的. 且 $[T_{W_i}]_{\mathcal{B}_i} = c_{p_i}$, 从而 T_{W_i} 循环. 设 β_i 是 \mathcal{B}_i 中的第一个向量, 则 $p_{\beta_i} = p_i = p_{W_i}$. $W_i = R\beta_i$. 由此从矩阵推出了一个循环分解, 从而 p_1, \dots, p_r 唯一决定, 从而矩阵也被 T 唯一决定. □

有理标准型是唯一决定的,这是有理标准型的很好的性质.对于矩阵的情况,有

推论7.2.2 对任意 $A \in F^{n \times n}$ 相似于唯一的有理型矩阵.称为 A 的有理标准型.

推论7.2.3 $A \sim B \iff A, B$ 的有理标准型相等. $\iff A, B$ 有相同的不变因子序列.换句话说,不变因子序列是矩阵相似的完全不变量.

推论7.2.4 设 A 的有理标准型为 A' , 不变因子序列为 $p_1, \dots, p_r, K \subset F$, 则若 $A \in K^{n \times n}$, 存在 $A' \in K^{n \times n}$, 并且 $A \sim A'$. 且 p_1, \dots, p_r , 即有理标准型和不变因子序列都不依赖于域的选取.

证明 设 A 作为 K -矩阵的有理标准型是 A'' , 从而 $A', A'' \in F^{n \times n}$ 均为有理型矩阵, 从而 $A' = A''$. 因此 $A' \in K^{n \times n}$ □

注 由此得到在大域中相似的两个矩阵在小域中也相似.

命题7.2.1 $\forall A \in F^{n \times n}, A \sim A^t$

证明 先设 $A = C_g, g = x^n + a_{n-1}x^{n-1} + \dots + a_0$. 则 $f_A = p_A = g \Rightarrow A$ 只有一个不变因子, 且 $p_1 = g$

而 $f_{A^t} = \det(xI - A^t) = \det(xI - A) = f_A$, 且容易证明 $p_{A^t} = p_A$ (即去证明一个多项式零化 A^t 当且仅当零化 A). 因此 $p_{A^t} = f_{A^t} = g$, 从而 A^t 循环, 对 A^t 只有一个不变因子, 且 $p_1 = g$. 从而 A, A^t 具有相同的不变因子序列. 于是 $A \sim A^t$

一般情况, 考虑 A 的有理标准型, 设 $A \sim \text{diag}(C_{p_1}, \dots, C_{p_r}) \sim \text{diag}(C_{p_1}^t, \dots, C_{p_r}^t) \sim A^t$ □

下面考虑一些具体的问题. 对于一个矩阵, 如何找可逆矩阵 P , 使得 $P^{-1}AP$ 是有理型矩阵?

• 设 $A \in F^{n \times n}, \mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 是有序基. $P = [\alpha_1, \dots, \alpha_n]$, 则 $P^{-1}AP = [L_A]_{\mathcal{B}}$. 从而

• 若 $\alpha_1, \dots, \alpha_r \in F^{n \times 1} - \{0\}$ 使得 $F^{n \times 1} = \bigoplus_{i=1}^r R\alpha_i, p_i := p\alpha_i$

在每个 $R\alpha_i$ 中可取一组基, $\{\alpha_i, \dots, A^{d_i-1}\alpha_i\}$, 从而 $[(L_A)_{R\alpha_i}]_{\mathcal{B}_i} = C_{p_i}$ 则取

$$P = \{\alpha_1, \dots, A^{d_1-1}\alpha_1, \dots, \alpha_r, \dots, A^{d_r-1}\alpha_r\}$$

例7.2.1

$$A = \begin{pmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{pmatrix} \in \mathbb{R}^{3 \times 3}$$

可求出 $f_A = (x-1)(x-2)^2, p_A = (x-1)(x-2)$, 从而 $p_1 = p_A = (x-1)(x-2)$, 从而 $p_2 = x-2$ 从而 A 的有

理标准型为 $\begin{pmatrix} C_{p_1} & 0 \\ 0 & C_{p_2} \end{pmatrix} = \begin{pmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

要找 $\alpha_2, \alpha_2 \in \mathbb{R}^{3 \times 1} - \{0\}$ 使得 $\mathbb{R}^{3 \times 1} = R\alpha_1 + R\alpha_2$. 从而要找 α_1 , 使得 $p_{\alpha_1} = p_1$, 从而 $\forall \alpha, p_1\alpha = 0$. 而 $(x-1)\alpha = A\alpha - \alpha$, 从而 $(x-1)\alpha = 0 \iff \alpha \in V_1$ 是 1 的特征向量. 同理 $(x-2)$ 零化 $\alpha \iff \alpha \in V_2$, 从而 $p_{\alpha_1} = p_1 \iff \alpha_1$ 不是特征向量. $p_{\alpha_2} \in p_2 \iff \alpha_2 \in V_2$.

还需要满足 $\mathbb{R}^{3 \times 1} = R\alpha_1 \oplus R\alpha_2$

可以取 $\alpha_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, A\alpha_1 = \begin{pmatrix} 5 \\ -1 \\ 3 \end{pmatrix}$, 而

$$V_2 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mid x_1 = 2x_2 + 2x_3 \right\}$$

有维数可以看出, $R\alpha_1$ 与 $R\alpha_2$ 不是直和 $\iff \alpha_2 \notin R\alpha_1$. 而 $R\alpha_1 = \text{span}\{\alpha_1, A\alpha_1\}$

从而取 $\alpha_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \notin R\alpha_1$. 从而 α_1, α_2 满足要求.

设 $V_1 = \text{span}\{\beta\}, V_2 = \text{span}\{\gamma_1, \gamma_2\}, \alpha_1 = \beta + \gamma_1, \alpha_2 = \gamma_2$ 满足条件. 一般化之后就可以得到下面的命题

命题7.2.2 设 T 可对角化, $\sigma(T) = \{c_1, \dots, c_k\}, V = \bigoplus_{i=1}^k V_{c_i}$

(1) 设 $\alpha = \sum_{i=1}^k \beta_i, \beta_i \in V_{c_i}$ (没有要求 β_i 非零.) 则 $R\alpha = \text{span}\{\beta_1, \dots, \beta_k\}$, 且 $p_\alpha = \prod_{\beta_i \neq 0} (x - c_i)$

(2) 设 $d_i = \dim V_{c_i}$, 则 T 的不变因子 $p_j = \prod_{d_i \geq j} (x - c_i), r = \max d_i$

证明 (1) 由于 $V = \bigoplus_{i=1}^k V_{c_i}$, 从而 $f\alpha = \sum_{i=1}^k f\beta_i = \sum_{i=1}^k f(c_i)\beta_i$ 由于任给 t_i , 由 Lagrange 差值公式, 知存在 $f, f_{c_i} = t_i$, 从而 $R\alpha = \text{span}\{\beta_1, \dots, \beta_k\}$.

而 $f\alpha = 0 \iff \sum_{i=1}^k f(c_i)\beta_i = 0 \iff f(c_i)\beta_i = 0$, 从而 $p_\alpha = \prod_{\beta_i \neq 0} (x - c_i)$

(2) 取 V_{c_i} 的有序基 $\mathcal{B}_{c_i} = \{\beta_{i1}, \dots, \beta_{id_i}\}$. 取 $\alpha_j = \sum_{d_i \geq j} \beta_{ij}$ 且 $p_{\alpha_j} = p_j$ 从而 $V = \bigoplus_{r=1}^r R\alpha_r$, 并且 $p_r | \dots | p_1$

□

7.3 The Jordan Form

定义7.3.1 称 T 是不可分解的, 如果 V 不是两个非零不变子空间的直和.

命题7.3.1 V 总能分解成若干个小空间的直和, 使得 T 限制在每个小空间上都是不可分解的

命题7.3.2 T 不可分解 $\iff T$ 准素循环

证明 " \implies ", 显然成立 (否则就可以做准素分解或循环分解).

" \impliedby ", 设 $f_T = p_T = p^r, p$ 素, 设 $V = V_1 \oplus V_2$ 均 T 不变. 设 $T_i = T_{V_i}$. 设 $f_{T_i} = p^{r_i}, p_{T_i} = p^{s_i}$, 这与 $p = \text{lcm}\{p_1, p_2\}$ 矛盾. □

推论7.3.1 对于任意 T, V 总是若干个准素循环不变子空间的直和.

定理7.3.1 对任意 T, V 总是准素循环不变子空间的直和 $V = \bigoplus_{i=1}^s V_i$ 记 $q_i = p_{T_{V_i}} = f_{T_{V_i}}$, 序列 q_1, \dots, q_s 在不计次序意义下被 T 唯一决定. 这些 q_i 叫做 T 的初等因子, 也叫基本因子 (elementary divisor)

证明 只需证明唯一性. 设 q_1, \dots, q_s 的所有素因子为 p_1, \dots, p_k , 将所有的 (V_i, q_i) 排一个顺序, 重新排成一个表.

$$\begin{aligned} & (V_1 1, p_1^{r_{11}}), \dots, (V_{1, d_1}, p_1^{r_{1, d_1}}) \\ & \dots \\ & (V_k 1, p_k^{r_{k1}}), \dots, (V_{k, d_k}, p_k^{r_{k, d_k}}) \end{aligned}$$

将按照列的顺序构成新的子空间.

$$W_1 = \bigoplus_{i=1}^k V_{i1}, W_2 = \bigoplus_{d_i \geq 2} V_{i2}, \dots, W_j = \bigoplus_{\{i: d_i \geq j\}} V_{ij} (1 \leq j \leq d)$$

我们说明 $V = \bigoplus_{j=1}^d W_j$ 是循环分解. 这是由于 $f_{W_j} = p_{W_j} = \prod_{d_i \geq j} f_{TV_{ij}}$, 设 α_{ij} 是循环向量, $\sum_{\{i: d_i \geq j\}} d_{ij}$ 是 W_j 是循环向量. 从而 f_{TW_j} 是不变因子, 被 T 唯一决定. 从而每一列的乘积被唯一决定. 从而每一列被唯一决定.

由此也得到初等因子就是把不变因子作分解. □

有四种方法来理解准素循环分解

- 将 V 分成不可分解的子空间的直和
- 先做准素分解, 再对每块做循环分解. 从而每一小块仍然是准素的 (看最小多项式即得). 得到的就是准素循环分解
- 先做循环分解, 再对每块做准素分解. (若大的子空间循环则小的子空间也循环 (看最小多项式和特征多项式的关系即得))
- 同时做准素分解和循环分解. 设准素分解为 $V = \bigoplus_i V_i$ 和循环分解 $V = \bigoplus_{W_j}$ 是循环分解. 得到 $V = \bigoplus_{ij} V_i \cap W_j$ (对于准素分解 WT -不变, 有 $W = \bigoplus_i W \cap W_i$)

一般来说, 得到的所谓的“准素有理标准型”不如有理标准型好, 由于它依赖于域的选取. 而相应的, 准素循环分解可以得到的是一种 Jordan 标准型

下面为了简单起见, 假设 F 是代数闭域. 从而基本因子只能为 $(x - c_i)^{n_i}$. 从而也是在每个 V_i 取一组基, 拼成全空间的一组基. 下面假设 T 准素循环. 设 $p_T = f_T = (x - c)^n$, 记 $N = T - \text{cid}_V$, 从而利用定义容易验证 $p_N = f_N = x^n$, 从而 $N^n = 0$, 我们将这种矩阵称为 **幂零 (nilpotent)** 的.

定义 7.3.2 称 $N \in L(V)$ 幂零, 如果存在 $r \geq 1$, 使得 $N^r = 0$

命题 7.3.3 设 $\dim V = n, T \in L(V)$, 则以下几条等价

- (1) T 幂零
- (2) p_T 是 x 的幂
- (3) $f_T = x^n$
- (4) $x^n = 0$

证明都是显然的

回到原来的讨论, 由于 N 也准素循环, 从而存在 \mathcal{B} , 使得 $[N]_{\mathcal{B}} = C_{p_N}$, 而 $C_{p_N} = \begin{pmatrix} 0 & 0 \\ I_{n-1} & 0 \end{pmatrix}$

因此形如 $\begin{pmatrix} c & & & & \\ 1 & c & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & c \end{pmatrix}$ 的矩阵叫做 Jordan 块, 记作 $J_n(c)$

命题 7.3.4 设 $\dim V = n, T \in L(V)$

(1) 若 T 准素循环, $f_T = p_T = (x - c)^n$, 则存在 \mathcal{B} , 使得 $[T]_{\mathcal{B}} = J_n(c)$

(2) 若存在 \mathcal{B} 使得 $[T]_{\mathcal{B}} = J_n(c)$, 则 T 准素循环, 且 $f_T = p_T = (x - c)^n$

证明 (1)已经证明, 下面考虑(2). 取 $N = T - c\text{id}_V$, 则 $[N]_{\mathcal{B}} = [T]_{\mathcal{B}} - cI_n = J_n(0) = C_{x^n}$ 因此 $f_N = p_T = x^n$, 于是 $f_T = p_T = (x - c)^n$ (当然这个结论也可以直接算出), 因此 $f_T = p_T = (x - c)^n$ \square

定理7.3.2 设 F 是代数闭域, $T \in L(V)$, 则存在一组基 \mathcal{B} , 使得 $[T]_{\mathcal{B}} = \text{diag}(J_{n_1}(c_1) \cdots J_{n_s}(c_s))$ 并且这些Jordan块在不计次序的意义下被 T 唯一决定. 这样的矩阵称作 T 的**Jordan标准型**

证明 设 \mathcal{B} 使得 $[T]_{\mathcal{B}}$ 为Jordan型矩阵(即将存在性的证明反过来), 设 $\mathcal{B} = (\mathcal{B}_1, \cdots, \mathcal{B}_s)$, $|\mathcal{B}_i| = n_i$, $V_i = \text{span}\mathcal{B}_i$ 是 T -不变子空间, 且 $[T_{V_i}]_{\mathcal{B}_i} = J_{n_i}(c_i) \Rightarrow T_{V_i}$ 准素循环. 从而 $V = \bigoplus_{i=1}^s V_i$ 是准素循环分解. 且 $f_{T_i} = p_{T_i} = (x - c_i)^{n_i}$ 是 T 的基本因子. 从而由基本因子的唯一性得到Jordan标准型唯一性. \square

从Jordan标准型可以看出很多 T 的性质

- 设 $\sigma(T) = \{c_1, \cdots, c_k\}$, 如果 c_i 在 $[T]_{\mathcal{B}}$ 的对角线上出现了 d_i 次, 则 $d_i = \dim \text{Ker}(T - c_i \text{id}_V)^n$ 称作属于特征值 c_i 的**广义特征子空间**, $f_T = \prod_{i=1}^k (x - c_i)^{d_i}$
- 设特征值为 c_i 的Jordan块的最大阶数为 r_i , 则 $p_T = \prod_{i=1}^k (x - c_i)^{r_i}$
- 特征值为 c_i 的Jordan块的个数 = $\dim V_{c_i}$ 即**几何重数**
- 可对角化等价于每个Jordan块的每个Jordan的尺寸全都是1.

设 F 是代数闭域, $T \in L(V)$, 存在 \mathcal{B} 使得 $[T]_{\mathcal{B}}$ 为Jordan形矩阵 J . 取 J_1 为 J 的对角部分, $J_2 = J - J_1$. 且 J_1, J_2 可交换. 因此将 T 分成了两个部分 $T = S + N$, 且 S 可对角化, N 幂零, $SN = NS$, 从而我们有下面的**Jordan分解**.

定理7.3.3 设 F 是代数闭域, $T \in L(V)$, 则存在唯一的 S, N 使得 $T = S + N$, S 可对角化, N 幂零. 且 $SN = NS$

在这个分解中, S 叫做 T 的**可对角化部分**, 或者**半单部分**. N 叫做 T 的**幂零部分**. 有很多性质, 比如 $f_S = f_T, \sigma(S) = \sigma(T)$

存在性已经证明, 下面证明唯一性.

证明 我们说明 J_1, J_2 均为 J 的多项式, 从而 S, N 都是 A 的多项式.

断言: 存在 $f, g \in F[x]$, 使得 $S = f(A), N = g(A), f + g = x$. 即 $J_1 = f(J), J_2 = g(J)$

在断言成立的情况下. 若 $S', N' \in F^{n \times n}$ 使得 $A = S' + N', S'N' = N'S'$, 下面证明 $S' = S, N' = N$. 事实上, 从而 S', A 可交换, 因此 S', S, N, N' 两两可交换.

又由于 $S - S' = N' - N$, 而 S, S' 可同时对角化, 从而 $S - S'$ 可对角化, 但由于 $N' - N$ 幂零, 从而只能 $S = S'$ 得证.

最后证明断言, 设 $p_A = \prod_{i=1}^k (x - c_i)^{r_i}$, 下面证明存在 $g_i, g_j \prod_{j \neq i} (x - c_j)^{r_j} \equiv (\text{mod } (x - c_i)^{r_i}) \implies f \equiv c_i (\text{mod } (x - c_i)^{r_i})$, 其实 $f(J) = J_1$. 事实上, $f(J_{n_1})(c_1) = c_1 I_1$, 从而得证. \square

7.4 Computation of Invariant Factors

7.5 Summary; Semi-Simple Operator

在Jordan分解中, 下面考虑不是代数闭域的情形. 若 $K \subset F, A \in K^{n \times n}$, 那么分解得到的 S, N 是否仍然为实矩阵. 事实上, 如果 $\text{char}(F) = 0$, 则答案是肯定的. 一般情况使只要 K 为完全域的时候则结论总成立. 特别地, 特征为0的域, 有限域, 代数闭域都是完全域. (对角化是指在 F 中可对角化, 此时的 S 就叫半单.)

下面对于 $K = \mathbb{R}, F = \mathbb{C}, A \in \mathbb{R}^{n \times n}$, 去证明 $S, N \in \mathbb{R}^{n \times n}$. 事实上 $A = S + N = \bar{S} + \bar{N}$, 从而 $S = \bar{S}, N = \bar{N}$
 下面推广这种方法, 复数域取共轭事实上可以看成 $\sigma: \mathbb{C} \rightarrow \mathbb{C}$ 的自同构, 并且 $\sigma(a) = a (a \in \mathbb{R})$

对于一般的 F , 也考虑 $\{\sigma: F \rightarrow F \text{ 是自同构} | \sigma(a) = a, \forall a \in \mathbb{R}\}$, 记作 $\text{Gal}(F/K)$, 叫域扩张的 Galois 群. 从而 $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \sigma\}$.

先取定一个 K , 将 F 看成 F 的代数闭包 \bar{K} , 满足 $K \subset \bar{K}$, 且 \bar{K}/K 是代数扩张. 即 $\forall c \in \bar{K}$, 存在 $f \in K[x]$, 使得 $f(c) = 0$, 且在域同构的意义下是唯一的. (如果 F 不是 K 的代数闭包, 则取一个小一点的域当作 F .)

命题 7.5.1 $\text{char} F = 0, F = \bar{K}, c \in K$ 的充分必要条件是 $\forall \sigma \in \text{Gal}(F/K), \sigma(c) = c$

一边是显然的, 而其实另一边也是对的. 即 $\forall c \in F - K$, 使得 $\sigma(c) \neq c$. 也就是说 Galois 群有充分多的映射来区分. (证明略)

若 $\text{char} F = 0$, 下面说明 $A \in K^{n \times n}$ 的半单部分和幂零部分仍在 K 中. 对任意的 $\sigma \in \text{Gal}(F/K), A = S + N = \sigma(S) + \sigma(N)$, 且 $\sigma(S)$ 也可对角化 $(\sigma(P))^{-1} \sigma(S) \sigma(P)$, 从而对任意 $\sigma, \sigma(S) = S, N = \sigma(N)$, 由命题 7.5.1, 从而成立

对于线性映射, 从而有

定理 7.5.1 设 $\text{char} K = 0, T \in L(V)$, 则存在唯一的 T_S, T_N 使得 $T = T_S + T_N, T_S T_N = T_N T_S$. 其中 T_S 半单, T_N 幂零

而半单就是指在代数闭包可对角化的刻画, 而在小域中应该定义成

定义 7.5.1 称 T 半单, $W \subset V, T$ -不变, 存在 $W' \subset V, T$ -不变, 使得 $V = W + W'$. 即任意不变子空间均存在不变补空间

- 取 $B, [T]_B$ 在 \bar{K} 上可对角化 $\Rightarrow T$ 半单
- $\text{char} K = 0, \Leftarrow$ 也对.

事实上, 对任意的域有 T 半单 $\Leftrightarrow p_T$ 无平方因子. 而 $[T]_B$ 在 \bar{K} 上可对角化 $\Leftrightarrow p_T$ 在 \bar{K} 上无重根.

这就给出了完全域的定义

定义 7.5.2 若 $K[x]$ 中的素多项式是在 \bar{K} 中总是无重根的, 则称 K 是完全域.

命题 7.5.2 $\text{char} K = 0$ 是完全域, 有限域也总是完全域, 代数闭域也是完全域.

而 $\mathbb{F}_p(t)$ 不是完全域, 考虑 $x^p - t = (x - c)^p$ 是素多项式但有重根.

最后说明代数闭包的存在性

证明 \bar{K} 是代数闭域 $\Rightarrow \bar{K}[x]$ 中的多项式在 \bar{K} 中总有根

命题 7.5.3 F 是代数闭域 $\Leftrightarrow F$ 没有非平凡的代数扩张.

证明 $\Rightarrow E/F$ 代数 $\Rightarrow \forall c \in E$, 存在 $f = \prod (x - c_i)$ 使得 $f(c) = 0 \Rightarrow c = c_i$

\Leftarrow 若 F 不是代数闭域, 存在 F 系数的素多项式 $p, \deg p \geq 2$, 使得 p 在 F 中没有根. 考虑 $F[x]/(p), (p)$ 为素理想从而为极大理想. 于是 $F[x]/(p)$ 是一个域. 而 F 看成 $F[x]/(p)$ 的子域. 从而这个扩张是非平凡的代数扩张. 事实上 $p(x + (p)) = 0$ 且是有限扩张, 即总是代数扩张. □

由上述命题, 只需证明 K 存在代数扩张 F/K 使得 F 没有非平凡的代数扩张.

考虑 K 的所有代数扩张构成 X , 满足 Zorn 引理的条件. 从而存在极大元. 于是它无非平凡的代数扩张. 从而 F 就是 K 的代数闭包. □

第八章 Inner Product Spaces

8.1 Inner Products

从本章开始我们将域取成实数域或者复数域即 \mathbb{R} 或 \mathbb{C}

定义8.1.1 设 V 是 F 线性空间, V 上的内积,指映射 $\langle \cdot, \cdot \rangle, V \times V \rightarrow F$ 使得

- (1) $\langle \alpha + \beta, \gamma \rangle$
- (2) $\langle c\alpha, \beta \rangle = c\langle \alpha, \beta \rangle$
- (3) $\langle \beta, \alpha \rangle = \overline{\langle \alpha, \beta \rangle}$
- (4) $\alpha \neq 0 \Rightarrow \langle \alpha, \beta \rangle$

从(3)可以推出 $\langle \gamma, \alpha + \beta \rangle = \langle \gamma, \alpha \rangle + \langle \gamma, \beta \rangle, \langle \alpha, c\beta \rangle = \bar{c}\langle \alpha, \beta \rangle$ 这种性质叫“一个半线性”, $\frac{1}{2}$ 线性(**sesqui-linear**)

对于(4),若为复数域,则要求 $\langle \alpha, \alpha \rangle$ 是实数且为正.这也是要求(3)的原因.即若为双线性,则 $\langle \alpha, \alpha \rangle$ 与 $\langle i\alpha, i\alpha \rangle$ 不能同时为正,则矛盾!

有内积的向量空间也叫**内积空间**.实数域上的有限维内积空间也叫**Euclid空间(Euclidean space)**,复的有限维线性空间也叫**酉空间(unitary space)**.

例8.1.1 $V = F^{n \times 1}, \alpha = (x_1, \dots, x_n)^t, \beta = (y_1, \dots, y_n)^t, \langle \alpha, \beta \rangle = \sum_{j=1}^n x_j \bar{y}_j$.这种内积称为**标准内积**.注意到 $\langle \alpha, \beta \rangle = \alpha^t \bar{\beta} = \bar{\beta}^t \alpha$.以后对于复矩阵,我们记 $A^* = \bar{A}^t$.

例8.1.2 设 $V = F^{m \times n}$,定义 $\langle A, B \rangle = \sum_{j,k} A_{jk} \bar{B}_{jk} = \text{tr}(AB^*) = \text{tr}(B^*A)$

定义8.1.2 $A \in F^{n \times n}$ 称为**Hermite矩阵(Hermitian matrix)**,如果 $A^* = A$.若进一步地,对任意 $X \in F^{n \times 1} \setminus \{0\}$,有 $X^*AX > 0$,则称 A 为**正定(positive)**矩阵

例8.1.3 $\forall Q \in GL_n(F), A = Q^*Q$ 则为正定矩阵.以后将证明每个正定都形如 Q^*Q

对于一个正定矩阵 A ,对于列向量 $\langle X, Y \rangle := Y^*AX$ 就是内积,另一方面,对于每个内积,其也可以写成一个正定矩阵.从而所有的内积和所有的正定矩阵有了一一对应.事实上,有下面的引理

引理8.1.1 设 $\dim V = n, \mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 记 $X = [\alpha]_{\mathcal{B}}, Y = [\beta]_{\mathcal{B}}$

- (1) 若 $A \in F^{n \times n}$ 为正定Hermite,则

$$\langle \alpha, \beta \rangle = Y^*AX = \sum_{j,k} A_{kj} x_j \bar{y}_k$$

是内积

- (2) 对于任意 V 上的内积 $\langle \cdot, \cdot \rangle$,存在唯一的正定Hermite矩阵 $A \in F^{n \times n}$,使得

$$\langle \alpha, \beta \rangle = Y^*AX = \sum_{j,k} A_{kj} x_j \bar{y}_k$$

. 我们将 A 称作内积在这组基下的矩阵.

证明 只证(2), (1)容易验证

先证唯一性. 若 A 满足要求, 取 $\alpha = \alpha_j, \beta = \alpha_k$, 得到 $A_{kj} = \langle \alpha_j, \alpha_k \rangle$.

存在性, 由上面, 我们只需证 $A_{kj} = \langle \alpha_j, \alpha_k \rangle$ 正定, 则 $\langle \alpha, \beta \rangle = \langle \sum x_j \alpha_j, \sum y_k \beta_k \rangle = \sum_{j,k} x_j y_k A_{kj} = Y^* A X$. 而由定义, 则 A 是Hermite矩阵, 而由于 $\langle X, X \rangle > 0$ 则得到 A 正定.

□

例8.1.4 考虑 $A = \begin{pmatrix} 1 & -1 \\ -1 & 4 \end{pmatrix}$, 设 $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $X^t A X = x_1^2 - 2x_1 x_2 + 4x_2^2 > 0$, 从而 A 正定.

从而设 $V = \mathbb{R}^{2 \times 1}$, $\langle \alpha, \beta \rangle = \beta^t A \alpha = \alpha^t A \beta = (x_1, x_2) A \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 y_2 - x_1 y_2 - x_2 y_1 + 4x_2 y_2$.

反过来, 这个内积在标准基下的矩阵就是 A .

例8.1.5 设 $T \in L(V, W)$ 是单射, 设 $\langle \cdot, \cdot \rangle_0$ 是 W 的内积, 则 $\langle \alpha, \beta \rangle = \langle T\alpha, T\beta \rangle_0$ 是 V 上的内积.

- 取 $V = W, \langle \cdot, \cdot \rangle_0$ 为标准内积. 对于可逆矩阵 $Q \in GL_n(F), T = L_Q$. 此时 $\langle \alpha, \beta \rangle = \langle Q\alpha, Q\beta \rangle_0 = (Q\beta)^* Q\alpha = \beta^* (Q^* Q)\alpha$. 从而 $Q^* Q$ 为内积的矩阵.
- 给定线性空间 V , 和 $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 是一组基. 有 $\Gamma_{\mathcal{B}}$ 为坐标映射, 取 $\langle \cdot, \cdot \rangle_0$ 是标准内积. 从而对应到此例当中, $\langle \alpha, \beta \rangle = \langle [\alpha]_{\mathcal{B}}, [\beta]_{\mathcal{B}} \rangle_0$, 若 $\alpha = \sum_j x_j \alpha_j, \beta = \sum_k y_k \alpha_k$, 从而 $\langle \alpha, \beta \rangle = \sum_j x_j \bar{y}_j$. 其在 \mathcal{B} 下的矩阵为单位矩阵.

有了内积之后, 就可以定义向量的长度, $\|\alpha\| = \langle \alpha, \alpha \rangle^{\frac{1}{2}}$. 从内积诱导出了一个长度函数 $\|\cdot\| : V \rightarrow [0, +\infty)$. 而内积是由长度函数唯一决定的. 事实上

$$(1) \text{ 若 } F = \mathbb{R}, \langle \alpha, \beta \rangle = \frac{1}{4} (\|\alpha + \beta\|^2 - \|\alpha - \beta\|^2)$$

$$(2) \text{ 若 } F = \mathbb{C}, \langle \alpha, \beta \rangle = \frac{1}{4} \sum_{k=1}^4 i^k \|\alpha + i^k \beta\|^2$$

这两个式子叫做叫做极化恒等式. 从这个式子可以判断一个范数函数是否为由内积诱导出来的.

下面讨论由内积诱导的长度(以后均讨论这种长度)的性质

引理8.1.2 (1) $\|c\alpha\| = |c|\|\alpha\|$

$$(2) \alpha \neq 0 \iff \|\alpha\| > 0$$

(3) $|\langle \alpha, \beta \rangle| \leq \|\alpha\| \|\beta\|$, 等号成立当且仅当 α, β 线性相关. 称作**Cauchy-Schwarz不等式**.

(4) $\|\alpha + \beta\| = \|\alpha\| + \|\beta\|$, 称作三角不等式.

其中只要某个函数满足(1), (2), (4), 则称作范数函数.

证明 (1), (2)显然. 考虑(3), 不妨设 $\alpha \neq 0$, 设 $\gamma = \beta - \frac{\langle \beta, \alpha \rangle}{\|\alpha\|^2} \alpha$. 利用几何意义, 即将 β 正交投影到 α^\perp 上. 则 $\langle \gamma, \alpha \rangle = 0$. 于是

$$0 \geq \|\gamma\|^2 = \langle \gamma, \beta - \frac{\langle \beta, \alpha \rangle}{\|\alpha\|^2} \alpha \rangle = \langle \gamma, \beta \rangle = \langle \beta, \beta \rangle - \frac{|\langle \alpha, \beta \rangle|^2}{\|\alpha\|^2}$$

从而(3)成立. 且等号成立当且仅当 $\gamma = 0$, 即线性相关

对于(4), 有

$$\|\alpha + \beta\|^2 = \|\alpha\|^2 + \|\beta\|^2 + 2\operatorname{Re}\langle \alpha, \beta \rangle \leq \|\alpha\|^2 + \|\beta\|^2 + 2|\langle \alpha, \beta \rangle| \leq \|\alpha\|^2 + \|\beta\|^2 + 2\|\alpha\| \|\beta\| \leq (\|\alpha\| + \|\beta\|)^2$$

□

定义8.1.3 记 $\alpha \perp \beta$,若 $\langle \alpha, \beta \rangle = 0$.若 $F = \mathbb{R}$,定义 $\angle(\alpha, \beta) = \arccos \frac{\langle \alpha, \beta \rangle}{\|\alpha\| \|\beta\|} \in [0, \pi]$.从而垂直即为 $\angle(\alpha, \beta) = \frac{\pi}{2}$

由于 z 与 \bar{z} 同时为0,从而 $\langle \alpha, \beta \rangle = 0 \iff \langle \beta, \alpha \rangle = 0$.从而 $\alpha \perp \beta \iff \beta \perp \alpha$

- 若 $S \subset V$ 中的向量两两正交,则称 S 为**正交集(orthogonal set)**.
- 若进一步 $\alpha \in S, \|\alpha\| = 1$,则称 S 为**标准正交集(orthonormal set)**.
- 是正交集的基称为正交基,称为标准正交集称为标准正交基.(注意正交集中有零向量,标准正交集中没有零向量,正交基中没有零向量)

例8.1.6 考虑 $F^{n \times 1}$ 的标准内积,其标准基就是标准正交基.

正交集还有一些性质

- 勾股定理: $\|\alpha + \beta\|^2 = \|\alpha\|^2 + \|\beta\|^2$,从而若 $\{\alpha_1, \dots, \alpha_m\}$ 是正交集,从而 $\sum_{i=1}^m \|\alpha_i\|^2 = \|\sum_{i=1}^m \alpha_i\|^2$
- 若 $\{\alpha_1, \dots, \alpha_m\}$ 是标准正交基.那么 $\langle \sum_{j=1}^n x_j \alpha_j, \sum_{k=1}^n y_k \alpha_k \rangle = \sum_{j=1}^n x_j \bar{y}_j$ 特别地, $\|\sum_{j=1}^n x_j \alpha_j\|^2 = \sum_{j=1}^n |x_j|^2$
- 不含0的正交集 S 线性无关,事实上,若 $\sum_{j=1}^n c_j \alpha_j = 0$,考虑 $\langle \alpha_k, \sum_{j=1}^n c_j \alpha_j \rangle = \bar{c}_k \langle \alpha_k, \alpha_k \rangle \Rightarrow c_k = 0$.从而一个不含零向量的正交集 S 是基 $\iff \text{span} S = V$

而在有限维的情况下,标准正交基一定存在

命题8.1.1 设 V 是有限维线性空间, $\{\beta_1, \dots, \beta_n\}$ 是空间的有序基

- (1) 存在空间的一组唯一的正交基 $\{\alpha_1, \dots, \alpha_n\}$ 和对角元为1的上三角矩阵 N ,使得

$$(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)N$$

- (2) 存在唯一的标准正交集 $\{\alpha'_1, \dots, \alpha'_n\}$ 和对角元大于0的上三角 N' ,使得

$$(\beta_1, \dots, \beta_n) = (\alpha'_1, \dots, \alpha'_n)N'$$

此时有 $\text{span}\{\beta_1, \dots, \beta_k\} = \text{span}\{\alpha_1, \dots, \alpha_k\} = \text{span}\{\alpha'_1, \dots, \alpha'_k\}$ 对任意 k 成立.

证明 以下的过程称作**Gram-Schmidt正交化**. 令由矩阵乘法可以得 $\beta_k = N_{1k}\alpha_1 + \dots + N_{k-1,k}\alpha_{k-1} + \alpha_k \Rightarrow \langle \beta_k, \alpha_j \rangle = N_{jk}\|\alpha_j\|^2 \Rightarrow N_{jk} = \frac{\langle \beta_k, \alpha_j \rangle}{\|\alpha_j\|^2}$.从而容易验证这样做满足条件且唯一

对于(2), 同样地可以说明 □

注意到,上面命题并不一定要求 $\{\beta_1, \dots, \beta_n\}$ 是0,若 β_i 是一组普通的向量.则若某个 $\alpha_j = 0$,则 $\{\beta_1, \dots, \beta_j\}$ 线性相关,若每个 $\alpha_j \neq 0$,则 $\{\beta_1, \dots, \beta_n\}$ 线性无关.

推论8.1.1 $\dim V < \infty$ 不含零向量的正交集总是可以扩充成正交基,任意一个标准正交集总可以扩充成标准正交基.

证明 先扩充成一组基,再做Schmidt正交化,而由于前面的部分正交,从而没变.类似地,任意一个标准正交集总可以扩充成标准正交基. □

下面考虑“正交”的好的性质.

命题8.1.2 设 $S = \{\alpha_1, \dots, \alpha_n\}$ 是不含0的正交集, $\beta \in \text{span}S$, 则

$$\beta = \sum_{k=1}^m \frac{\langle \beta, \alpha_k \rangle}{\|\alpha_k\|^2} \alpha_k$$

事实上, 设 $\beta = \sum_{k=1}^n c_k \alpha_k$, 与每个 α_i 作内积即可.

特别地, 若 S 是一组正交基, 则 $\forall \beta \in V$ 上面的式子均成立. 进一步, 若是标准正交基, 则 $\forall \beta$

$$\beta = \sum_{k=1}^m \langle \beta, \alpha_k \rangle \alpha_k$$

需要注意的是, β 只能在前面.

命题8.1.3 (Bessel不等式) 设 $\{\alpha_1, \dots, \alpha_m\}$ 是不含0向量的正交集, 则对任意 $\beta \in V$, 有

$$\sum_{k=1}^m \frac{|\langle \beta, \alpha_k \rangle|^2}{\|\alpha_k\|^2} \leq \|\beta\|^2$$

其中等号成立当且仅当 $\beta \in \text{span}S$

证明 将 S 扩充为正交基 $\{\alpha_1, \dots, \alpha_n\}$, 则

$$\beta = \sum_{k=1}^n \frac{\langle \beta, \alpha_k \rangle}{\|\alpha_k\|^2} \alpha_k$$

因此, 由勾股定理 $\|\beta\|^2 = \sum_{k=1}^n \left\| \frac{\langle \beta, \alpha_k \rangle}{\|\alpha_k\|^2} \alpha_k \right\|^2 = \sum_{k=1}^n \frac{|\langle \beta, \alpha_k \rangle|^2}{\|\alpha_k\|^2} \geq \sum_{k=1}^m \dots$ 而等号成立当且仅当 $\langle \beta, \alpha_{k+1} \rangle = 0 = \dots = \langle \beta, \alpha_n \rangle = 0 \iff \beta \in \text{span}S$ □

进一步, 若 S 是标准正交集, $\beta \in V$, 则 $\sum_k |\langle \beta, \alpha_k \rangle|^2 \leq \|\beta\|^2$

对于 $S \in V$, $S^\perp = \{\alpha \in V | \alpha \perp \beta \forall \beta \in S\}$ 是子空间. 且容易看出 $S^\perp = (\text{span}S)^\perp$

命题8.1.4 $\dim V < \infty$, 设 $W \subset V$ 是子空间, 则 $\dim W + \dim W^\perp = \dim V$

证明 取 W 的标准正交基 $\alpha_1, \dots, \alpha_m$, 扩充为全空间的标准正交基 $\{\alpha_1, \dots, \alpha_n\}$. 下面证明 $\{\alpha_{m+1}, \dots, \alpha_n\}$ 是 W^\perp 的基.

事实上, 对 $\forall \beta \in V$, $\beta = \sum_{k=1}^n \langle \beta, \alpha_k \rangle \alpha_k \iff \beta \in W^\perp \iff \langle \beta, \alpha_1 \rangle = \dots = \langle \beta, \alpha_m \rangle = 0 \iff \beta = \sum_{k=m+1}^n \langle \beta, \alpha_k \rangle \alpha_k \iff \beta \in \text{span}\{\alpha_{k+1}, \dots, \alpha_n\}$ □

推论8.1.2 $\dim W^\perp = \dim W^0$

事实上, 可以直接从零化子空间的性质来导出上述命题.

设 V 是 F 向量空间, 则内积诱导了一个 $V \rightarrow V^*$ 的同构 (复数域为不严格同构, 为复共轭线性同构). 考虑等同 $\beta \leftrightarrow \langle \cdot, \beta \rangle$. 严格来说, 考虑映射 $\Phi: V \rightarrow V^*$, $\Phi(\beta) \in V^*$ 满足 $\Phi(\beta)(\alpha) = \langle \alpha, \beta \rangle$

引理8.1.3 Φ 既单又满且共轭线性. 即 $\Phi(c\beta_1 + \beta_2) = \bar{c}\Phi(\beta_1) + \Phi(\beta_2)$

证明 为证单满, 只需证明对于 $\forall \beta \in V^*$, 存在唯一的 $\beta \in V$, 使得 $\Phi(\beta) = f$

事实上, 设 $\alpha_1, \dots, \alpha_n$ 是标准正交基, 对 $\beta = \sum_{j=1}^n c_j \alpha_j$, 从而 $\Phi(\beta) = f \iff \Phi(\beta)(\alpha_k) = f(\alpha_k) \iff \bar{c}_k = f(\alpha_k) \iff \beta = \overline{f(\alpha_j)} \alpha_j$. 从而 β 存在唯一的. 即 Φ 既单又满.

为证 Φ 共轭线性, 考虑 $\Phi(c\beta_1 + \beta_2)(\alpha)$ 容易验证其等于 $[\bar{c}\Phi(\beta_1) + \Phi(\beta_2)](\alpha)$

当 $F = \mathbb{R}$ 时, Φ 即为一个线性同构. 当 $F = \mathbb{C}$ 时, Φ 是实线性的.

通过“忘掉复结构”则可以用线性映射来直接说明这个问题 □

于是,可以直接证明上述推论.事实上,可以发现 $\Phi(S^\perp) = S^0$,由于 Φ 为实线性同构,忘掉复结构,从而 $\dim_{\mathbb{R}} W^\perp = \dim_{\mathbb{R}} W^0$.于是 $\dim W = \dim W^0$

最后说明 $\Phi(S^\perp) = S^0$,对 $\beta \in S^\perp \Leftrightarrow \langle \beta, \alpha \rangle = 0 (\forall \alpha \in S) \Leftrightarrow \phi(\beta)(\alpha) = 0 \forall \alpha \in S \Leftrightarrow \Phi(\beta) \in S^0$,在等同的意义下,这个 S^0 也可以叫做正交补.

推论8.1.3 $\dim V < \infty$,则 $(W^\perp)^\perp = W$

证明 显然 $W \subset (W^\perp)^\perp$,且维数相等,从而成立. \square

推论8.1.4 $V = W \oplus W^\perp$

证明 显然 $W \cap W^\perp = \{0\}$,由维数关系则结论成立. \square

有了直和分解之后,就可以考虑投影映射.对 $\forall \beta \in V$,存在唯一的分解 $\beta = \beta_1 + \beta_2, \beta_1 \in W, \beta_2 \in W^\perp$,定义 $P_W \in L(V)$ 满足 $P_W(\beta) = \beta_1$.称为到 W 上的正交投影.称 $P_W\beta$ 为 β 到 W 上的正交投影.

若 $\{\alpha_1, \dots, \alpha_m\}$ 为 W 的标准正交基,从而 $P_W\beta = \sum_{j=1}^m \langle \beta, \alpha_j \rangle \alpha_j$ 于是 $P_W + P_{W^\perp} = \text{id}_V$,下面考虑最佳逼近的问题.

命题8.1.5 设 $W \subset V$ 是子空间,则 $\forall \beta \in V, P_W\beta$ 是 β 在 W 中的最佳逼近.即函数 $W \rightarrow [0, +\infty), \alpha \mapsto \|\beta - \alpha\|$ 在且只在 $P_W\beta$ 处取得最小值.

证明 对 $\alpha \in W, \|\beta - \alpha\|^2 = \|\beta - \alpha + \alpha + P_W\beta\|^2 = \|\beta - \alpha\|^2 + \|P_W\beta - \alpha\|^2 \geq \|\beta - P_W\beta\|^2$,其中等号成立当且仅当 $\alpha = P_W\beta$ \square

在Schmidt正交化中,记 $W_k = \text{span}\{\beta_1, \dots, \beta_k\}$,则 $\alpha_k = P_{W_{k-1}^\perp} \beta_k$ 就是一个正交投影.

8.2 Adjoints

对 $T \in L(V)$ 有 $T^t \in L(V^*)$,则存在唯一的 $S \in L(V)$ 使得图表可交换.记为 T^* ,则 T^* 满足 $T^t \circ \Phi = \Phi \circ T^*$.则 $T^t(\Phi\beta) = \Phi(S\beta)$ 对任意 β .从而对任意 $\beta, \Phi(\beta) \circ T = \Phi(S\beta) \iff \forall \alpha \Phi(\beta)(T\alpha) = \Phi(S\beta)(\alpha) \forall \alpha, \beta$,从而 S 满足 $\langle T\alpha, \beta \rangle = \langle \alpha, S\beta \rangle \iff \langle \beta, T\alpha \rangle = \langle S\beta, \alpha \rangle$.

从而 T^* 满足 $\langle T^*\beta, \alpha \rangle = \langle \beta, T\alpha \rangle$.如果通过内积将 V, V^* 等同起来,则 T^t, T^* 是同一回事.即 $T^* = \Phi^* \circ T^t \circ \Phi^{-1}$ 取了两次复共轭则 T^* 无论如何都是线性映射.

定义8.2.1 上述定义的 T^* 为关于内积 $\langle \cdot, \cdot \rangle$ 的伴随变换.

这样的 T^* 也可以定义在两个不同的空间上,使得图表可交换.

设 $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ 是空间的标准正交基,则 $[T^*]_{\mathcal{B}} = [T_{\mathcal{B}}]^*$.

事实上 $\Phi(\mathcal{B}) = \{\Phi(\alpha_1), \dots, \Phi(\alpha_n)\}$ 是 \mathcal{B} 的对偶基 $\Rightarrow [T^t]_{\Phi(\mathcal{B})} = [T]_{\mathcal{B}}^t$ 设 T^* 在 \mathcal{B} 下的矩阵是 A ,则 $T^*\alpha_k = \sum_{j=1}^m A_{jk} \alpha_j$,取 Φ 从而

$$T^t(\Phi(\alpha_k)) = \Phi(T^*\alpha_k) = \sum_{j=1}^n \overline{A_{jk}} \Phi(\alpha_j)$$

从而 $[T^t]_{\Phi(\mathcal{B})} = \overline{A}$

例8.2.1 设 $V = F^{n \times 1}$ 取为标准内积, $T = L_A, A \in F^{n \times n}$,则 $L_A^* = L_{A^*} \iff \langle X, L_{A^*} Y \rangle = \langle L_A X, Y \rangle \iff \langle X, A^* Y \rangle = \langle AX, Y \rangle \iff (A^* Y)^* X = Y^* AX$ 确实是相等的.

命题8.2.1 (1) $(T + U)^* = T^* + U^*$

(2) $(cT)^* = \overline{c} T^*$

$$(3) (TU)^* = U^*T^*$$

$$(4) (T^*)^* = T$$

由以上四条,取 $*$ 是一个 \mathbb{C} 代数的共轭线性的反自同构.在算子代数中则称为 \mathbb{C}^* 代数.

定义8.2.2 若 $T^* = T$ 则称 T 是自伴的,即满足 $\langle T\alpha, \beta \rangle = \langle \alpha, T\beta \rangle$