

MATH 40003

LINEAR ALGEBRA

& GROUP

• vector space & field 注意, vector space 和 field 定义不同

$A = \{a_0 + a_1x + \dots + a_nx^n \mid a_0, a_1, \dots, a_n \in \mathbb{R}, n \in \mathbb{N}\}$ is a vector space

$B = \left\{ \frac{a_0 + a_1x + \dots + a_nx^n}{b_0 + b_1x + \dots + b_mx^m} \mid a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m \in \mathbb{R}, n, m \in \mathbb{N} \right\}$ is a field (考虑 $\forall x \in B, \exists x^{-1} \in B, x \cdot x^{-1} = x^{-1} \cdot x = 1$)

* so other example of field:

(1) $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, with addition and multiplication under modular prime p .

除号定义依据 field!

(2) $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}, i^2 = -1\}$

注意: field 中 inverse 证明要明确写出 inverse, 或证明存在!!!

• matrix notation

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}_{\mathbb{R}^{m \times n}} \times \begin{pmatrix} b_{11} & \dots & b_{1p} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{np} \end{pmatrix}_{\mathbb{R}^{n \times p}} = \begin{pmatrix} c_{11} & \dots & c_{1p} \\ \vdots & & \vdots \\ c_{m1} & \dots & c_{mp} \end{pmatrix}_{\mathbb{R}^{m \times p}}$$

注意下标!

$$(a_{ij})_{m \times n} (b_{kl})_{n \times p} = (c_{il})_{m \times p}, c_{il} = \sum_j a_{ij} b_{jl}$$

• subfield a subfield $F \subseteq E$ is a subset F of a field E , such that

• $0, 1 \in F$

• $\forall a, b \in F, a+b \in F, ab \in F, a+(0-a)=0$

• $\forall a \in F, \exists (-a), a^{-1}, a+(-a)=0, a \cdot a^{-1}=1$

• bilinear map

for V, U, W belongs to vector space over $\mathbb{F}$, there exist a bilinear map $f: V \times U \rightarrow W$ if following statements are satisfied:

(1) $f(\lambda v_1 + \mu v_2, u) = \lambda f(v_1, u) + \mu f(v_2, u)$

(2) $f(v, \lambda u_1 + \mu u_2) = \lambda f(v, u_1) + \mu f(v, u_2)$

注意: 它比 linear map 要更强! 其包含 linear map.

- echelon matrix
- (1) row-echelon matrix 将矩阵转化为 $\begin{pmatrix} 0 & 1 & 2 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
pivot 为 1 的矩阵, 且 pivot 不跨行出现
 - (2) reduced row-echelon matrix 在 row-echelon matrix 基础上, 所有含 pivot 的 column 仅 pivot 不为 0
 - (3) 将 augmented matrix 转化成 row-echelon matrix 进行解方程组. "the number of free parameters" = "free vectors" = the dimension of solution set.
- 注意: 在转化时, 有可能 the last column has a pivot. 此时方程无解

- (1) If $(A|B)$ is row-equivalent to $(A'|B')$, they have the same solutions.
- (2) $A, B \in \text{Mat}_{m,n}$ are row-equivalent if B can be obtained from A by applying the three elementary row operations:
- permuting rows
 - multiplying a row by a nonzero scalar
 - adding a multiple of a row to another row
- (3) if $(A|B)$ is row-equivalent to $(A'|B')$, they have the same solutions.
- (4) if $(A|B)$ and $(A'|B')$ are consistent and have the same solution, their row-equivalent rref forms are the same.
- (5) Given A , there is a unique ref matrix B row-equivalent to it.

proof:

对于 $A\vec{x} = \vec{b}$ consistent, 可根据 solution 列出 $(R|B)$

对于 $A\vec{x} = \vec{b}$ inconsistent, 考虑 $A\vec{x} = \vec{0}$ consistent.

inverse

- (1) assume $AX = I_n$, where $A \in M_{m,n}(\mathbb{F})$ and it has a right inverse. as a result, $m \leq n$.

proof:

prove by contradiction. if $m > n$, then we use echelon matrices:

$$AX = I \Rightarrow RX = C, \text{ where } R \text{ is the rref of } A$$

since $m > n$, in such a way, R will have some zero rows in the end as a result, to satisfy the equation, C will also have some zero rows in the end, which is impossible for any basic operations on I .

(2) if A is invertible on right and on left, then A is square, both right inverse and left inverse are the unique two-sided inverse

证明 B 是 A 的 inverse
而 $BA = AB = I$

proof:

$$\textcircled{1} m \leq n, n \leq m \Leftrightarrow m = n$$

$$\textcircled{2} X_L A X_R = X_L = X_R$$

if X_L, X_R are left/right inverse of A

$$\textcircled{3} A^{-1} A X_R = A^{-1} = X_R, X_L A A^{-1} = A^{-1} = X_L \text{ if } A^{-1} \text{ is two-sided inverse of } A$$

(1) for $\vec{v}_1, \dots, \vec{v}_n \in V, \lambda_1, \dots, \lambda_n \in \mathbb{F}$, their linear combination is linearly dependent
 $\lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n$

注意: n is finite!

(2) for $(\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n) \in V^n$ where $\vec{v}_i \in V$ for all i , it is linear dependent if there exists $\lambda_1, \dots, \lambda_n$ not all 0, such that
 $\lambda_1 \vec{v}_1 + \lambda_2 \vec{v}_2 + \dots + \lambda_n \vec{v}_n = \vec{0}$

注意 $\textcircled{1} \text{span}(\{\}) = \{\vec{0}\}, \{\} \text{ is linearly independent. } (\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n)$

$\textcircled{2} \lambda \vec{0} = \vec{0}$ for all $\lambda \in \mathbb{F}, \{\vec{0}\}$ is linearly dependent

$\textcircled{3}$ 判断 linearly dependent 可以用定义, 或行列式

(3) $\text{span}(\vec{v}_1, \dots, \vec{v}_n) = \{\text{all linear combination of } (\vec{v}_1, \dots, \vec{v}_n)\}$

注意: $\text{span}(\emptyset) = \{\vec{0}\}$ by definition.

(4) a basis of V is a linear independent spanning set

spanning 证明过程中写出组合方式

注意: $((v_1, \dots, v_n)$ is linear independent) $\Leftrightarrow$

$(\{v_1, \dots, v_n\})$ is linear independent and elements are distinct,

因为在 tuple 中元素不重复出现, set 中重复元素自动消去 e.g. $\{x, x\} = \{x\}$

(1) let $X \subseteq V$ be linearly independent and let $\vec{v} \in V \setminus \text{span}(X)$. then $X \cup \{\vec{v}\}$ is also linearly independent.

(2) let $X \subseteq V$ be spanning and let $\vec{x} \in X$ be such that $\vec{x} \in \text{span}(X \setminus \{\vec{x}\})$. then $X \setminus \{\vec{x}\}$ is still spanning.

(3) let $X \subseteq V$ and let $\vec{v} \in \text{span}(X)$ with $\vec{v} \neq 0$. suppose $\vec{v} = \lambda_1 \vec{x}_1 + \dots + \lambda_n \vec{x}_n$ for distinct $\vec{x}_1, \dots, \vec{x}_n \in X$ and all $\lambda_i \neq 0$. then for any index i : $\text{span}(X) = \text{span}((X \setminus \{\vec{x}_i\}) \cup \{\vec{v}\})$

(4) let $X \subseteq V$ be linearly independent and $Y \subseteq V$ be spanning, and suppose $|Y| < \infty$, then $|X| \leq |Y|$

proof:

① there exists a subset $Y' \subseteq X \cup Y$ such that $X \subseteq Y'$, $|Y'| = |Y|$ and $|Y'|$ is spanning.

- if $|X \setminus Y| = 0$, then take $Y' = Y$ to satisfy the conditions

- if $|X \setminus Y| = k > 0$, then choose $\vec{x} \in X \setminus Y$, since Y is spanning, we can write $\vec{x} = \lambda_1 \vec{y}_1 + \dots + \lambda_n \vec{y}_n$ for some $\vec{y}_1, \dots, \vec{y}_n \in Y$ and $\lambda_1, \dots, \lambda_n \in \mathbb{F}$, not all zero. WLOG, we discarding all 0 coefficients, so $\forall i = 1, \dots, n, \lambda_i \neq 0$. there exists at least one $\vec{y}_i \notin X$. if not, then $\vec{x}, \vec{y}_1, \dots, \vec{y}_n \in X$, and $\vec{x} - \lambda_1 \vec{y}_1 - \dots - \lambda_n \vec{y}_n = 0$, contradiction as X is linearly independent.

thus, let $Y' = (Y \setminus \{\vec{y}_i\}) \cup \{\vec{x}\}$. then $\text{span}(Y) = \text{span}(Y')$ and $|X \setminus Y'| = k - 1$

② then assume $|X| < \infty$, $|Y^{(n)}| = 0$

so there exists a spanning set $Y' \subseteq (X \cup Y)$ such that $X \subseteq Y'$ and $|Y| = |Y'|$, so $|Y| = |Y'| \geq |X|$.

② assume $|X| = \infty$, then we can find $|X'| = |Y| + 1$, which leads to contradiction. if finite case has been proved.

注意: V is finite dimensional if it has a finite spanning set. 这一条帮助我们证明 linearly independent set has finite elements

(5) every finite-dimensional vector space has a basis

proof:

prove by induction. if X is a spanning set.

① $|X| = 0$, then X itself is a basis

② assume $|X'| = k-1$ works, for $|X| = k$

- if X is linearly independent, then X itself is a basis

- if X is linearly dependent, so

$$\lambda_1 \vec{x}_1 + \dots + \lambda_n \vec{x}_n = 0 \text{ for } \vec{x}_1, \dots, \vec{x}_n \text{ distinct and } \lambda_1, \dots, \lambda_n \text{ not all } 0.$$

WLOG, if $\lambda_1 \neq 0$, then $\vec{x}_1 = \frac{\lambda_2}{\lambda_1} \vec{x}_2 + \dots + \frac{\lambda_n}{\lambda_1} \vec{x}_n$

$$\text{so } \text{span}(X \setminus \{\vec{x}_1\}) = \text{span}(X)$$

we turn this question into the condition of $|X \setminus \{\vec{x}\}| = k-1$
(6) $= k-1$, so we are done.

(6) 注意, 也就是说, every finite spanning set can be shrunk to a basis algorithmically.

(7) if V is a finite-dimensional vector space and $X \subseteq V$ is linearly independent, then X can be extended to a basis.

proof:

Cal PS4 9

if X not spanning, then $V \setminus \text{span}(X) \neq \emptyset$
we find $\vec{v} \in (V \setminus \text{span}(X))$, and make $X' = X \cup \{\vec{v}\}$,
repeat this process until $X^{(n)}$ is spanning.

(8) the following are equivalent for $B \subseteq V$, where V is a finite dimension vector space and $\dim V = n$.

① B is a basis

② B is linearly independent and $|B| = n$

③ B is spanning and $|B| = n$.

proof:

• if ① is true, then ②③ is true

• if ② is true

if $\text{span}(B) \neq V$, then we can find $\vec{v} \in (V \setminus \text{span}(B))$, and
 $B \cup \{\vec{v}\}$ is linearly independent.

this is impossible since otherwise $|B \cup \{\vec{v}\}| \leq |\text{basis of } V|$
 $n+1 \leq n$.

thus ② leads to ①, ① leads to ③

• if ③ is true

if B is not linearly independent, then we can find $B' \subsetneq B$
which is a basis.

but $|B'| < n$, which is impossible since $\dim V = n$.

thus ③ leads to ①, ① leads to ②

(9) if V is a finite-dimensional vector space, and $U \subseteq V$, then
 $\dim U \leq \dim V$

proof:

我们有两种证明方法:

① if $L \subseteq U \subseteq V$ is linear independent, then $|L| \leq \dim V$

if L doesn't span U , we can enlarge it gradually as 4

$L^{(n)} = L^{(n-1)} \cup \{\vec{u}\}$, where $\vec{u} \in U \setminus \text{span}(L^{(n-1)})$

iteratively, we will get either a basis of U , or a linearly independent set which $|L^{(n)}| > \dim V$

the latter is impossible, so $\dim U = |L^{(n)}| \leq \dim V$.

② we start with finding out the basis S of V . $|S| = \dim V$

we can then take any linearly independent set $L \subseteq U$, and modify S to contain L .

in such a way, we can either get:

- basis of $U \subseteq S$ ($\dim U \leq \dim V$)

- linear independent set of size $\dim V$ in U . $\geq S$ ($\dim U > \dim V$)

for the latter case; for V , S is spanning, so impossible
thus $\dim U \leq \dim V$.

(10) if $B \subseteq V$; V is a vector space

- if B is linearly independent, $\Leftrightarrow \forall \vec{v} \in V$, there is at most one expression $\vec{v} = \lambda_1 \vec{b}_1 + \dots + \lambda_m \vec{b}_m$, where $\vec{b}_i \in B$ are distinct and $\lambda_i \in \mathbb{R}$.

- if B is spanning $\Leftrightarrow \forall \vec{v} \in V$, there is at least one expression $\vec{v} = \lambda_1 \vec{b}_1 + \dots + \lambda_m \vec{b}_m$, where $\vec{b}_i \in B$ are distinct and $\lambda_i \in \mathbb{R}$.

(11) if $U, W \subseteq V$, and V is finite-dimensional, then $\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$

proof:

since $U \cap W \subseteq V$, $U \cap W$ is finite dimensional and it has basis

assume the basis of $U \cap W$ is $\{\vec{v}_1, \dots, \vec{v}_n\}$

we can extend it to get the basis of U : $\{\vec{v}_1, \dots, \vec{v}_n, \vec{u}_1, \dots, \vec{u}_m\}$

and the basis of W is $\{\vec{v}_1, \dots, \vec{v}_n, \vec{w}_1, \dots, \vec{w}_p\}$, and the basis

of $U+W$ is $\{\vec{v}_1, \dots, \vec{v}_n, \vec{u}_1, \dots, \vec{u}_m, \vec{w}_1, \dots, \vec{w}_p\}$

now, the only thing we need to prove is the basis of $U+W$ is true.

① $\text{span}\{\vec{v}_1, \dots, \vec{v}_n, \vec{u}_1, \dots, \vec{u}_m, \vec{w}_1, \dots, \vec{w}_p\} \supseteq \text{span}\{\vec{v}_1, \dots, \vec{v}_n, \vec{u}_1, \dots, \vec{u}_m\}$

so $\text{LHS} \supseteq U$, similarly, $\text{LHS} \supseteq W$, thus $\text{LHS} \supseteq U+W$

so it is spanning

② if $\lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n + \mu_1 \vec{u}_1 + \dots + \mu_m \vec{u}_m + \nu_1 \vec{w}_1 + \dots + \nu_p \vec{w}_p = \vec{0}$
 $\lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n + \mu_1 \vec{u}_1 + \dots + \mu_m \vec{u}_m = -(\nu_1 \vec{w}_1 + \dots + \nu_p \vec{w}_p)$

$\text{LHS} \in U$, $\text{RHS} \in W$, $\text{LHS} = \text{RHS}$, both side $\in U \cap W$.

call for $\vec{v} \in U \cap W$, then $\vec{v} = \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n$ is unique.

also, $\vec{v} \in U$, $\vec{v} \in W$, $\vec{v} = \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n + \mu_1 \vec{u}_1 + \dots + \mu_m \vec{u}_m$ is unique

$\vec{v} = \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n + \nu_1 \vec{w}_1 + \dots + \nu_p \vec{w}_p$ is unique

only possible if $\lambda_i = \nu_j = \nu_k = 0$

so it is linearly independent

4 key spaces (1) if A is row-equivalent to B , then their row spaces are the same.

proof: B is row of A is rows is combination

(2) if A and B are row equivalent, then $(\lambda_1 \vec{a}_1 + \dots + \lambda_n \vec{a}_n = \vec{0})$
 $\Leftrightarrow (\lambda_1 \vec{b}_1 + \dots + \lambda_n \vec{b}_n = \vec{0})$, their nullspace are the same.

proof:

$$M(\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n) = (\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n)$$

$$((\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n) \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \vec{0}) \Leftrightarrow (M(\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n) \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \vec{0})$$

$$\Leftrightarrow ((\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n) \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \vec{0})$$

(3) if A and B are row-equivalent, then the dimensions of their column spaces are the same.

proof:

$(\vec{a}_{i1}, \vec{a}_{i2}, \dots, \vec{a}_{in})$ is linearly independent $\Leftrightarrow$ same
 $(\vec{b}_{i1}, \vec{b}_{i2}, \dots, \vec{b}_{in})$ is linearly independent

and the basis is just the maximum linearly independent set.

(4) the dimensions of row space and column space of A are the same.

proof: 高斯消元之后只留pivot

(5) dimension of row space + dimension of nullspace = n for $A_{m \times n}$.

(6) nullspace is orthogonal to row space

(7) 如何寻找 row space basis: 用 Gauss-Jordan elimination 求 R . 因为 row space 不变, R 的 row space basis 即为 A 的 row space basis.

如何寻找 column space basis: ① transpose 化成 row space

② 用 Gauss-Jordan elimination 求 R , 并

找到 R 的 row space basis: $\vec{r}_{i1}, \vec{r}_{i2}, \dots$

$\vec{r}_{ik}$, 那么 A 的 column space basis 为

$\vec{a}_{i1}, \vec{a}_{i2}, \dots, \vec{a}_{ik}$ (independent correspondence unchanged)

(1) let $T: F^n \rightarrow F^m$ be a map, then $(T \text{ is linear}) \iff (\exists A \in M_{m \times n}(F) \text{ such that } T(\vec{v}) = A\vec{v} \text{ for all } \vec{v} \in F^n)$ linear algebra

and the matrix A is unique.

proof:

• assume T is linear, let $\vec{e}_1, \dots, \vec{e}_n$ be the standard basis of F^n .

$\vec{v} = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \lambda_1 \vec{e}_1 + \dots + \lambda_n \vec{e}_n$, $T(\vec{v}) = \lambda_1 T(\vec{e}_1) + \dots + \lambda_n T(\vec{e}_n)$

define $A = (T(\vec{e}_1) \ T(\vec{e}_2) \ \dots \ T(\vec{e}_n))$

• if $T(\vec{v}) = A\vec{v}$, then T is linear due to matrix multiplication is linear

• A is unique since $T(\vec{e}_i)$ are unique

Q) let V and W be finite-dimensional vector spaces over F . fix a basis $B = (\vec{v}_1, \dots, \vec{v}_n)$ for V , $C = (\vec{w}_1, \dots, \vec{w}_m)$ for W

① for any $\vec{v} \in V$, $[\vec{v}]_B = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$ if $\vec{v} = \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n$.

② similarly, for any $\vec{w} \in W$, $[\vec{w}]_C = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix}$ if $\vec{w} = \mu_1 \vec{w}_1 + \dots + \mu_m \vec{w}_m$

③ let $T: V \rightarrow W$ be linear, then there exists a unique matrix

${}_C T_B \in M_{m \times n}(F)$ such that for every $\vec{v} \in V$, $[T(\vec{v})]_C = {}_C T_B [\vec{v}]_B$. exactly, ${}_C T_B = ([T(\vec{v}_1)]_C \ [T(\vec{v}_2)]_C \ \dots \ [T(\vec{v}_n)]_C)$

proof: $V \xrightarrow{T} W$
 $\downarrow [\cdot]_B \quad \downarrow [\cdot]_C$
 $F^n \xrightarrow{\phi} F^m$
 ϕ is linear, so there exists a matrix A such that $\phi[\vec{v}]_B = A[\vec{v}]_B$
 assume $A = (A_1 \ A_2 \ \dots \ A_n)$, so $A_i = \phi(\vec{e}_i) = [T(\vec{v}_i)]_C$

在空间中有两种变化: 更换 basis 与 改变 vector point 的位置. 对于同一个位置的 vector point, 其位置的表示方法会因 basis 的不同而不同 (etc. $\vec{v}$ 与 $[\vec{v}]_B$ 均表示同一个 vector point). 对于同一个改变 vector point 的位置的变化, 其表示方法会因 basis 的不同而不同 (etc. T 与 ${}_C T_B$ 均表示同一个位置变化)

③ assume S, T are linear transformations, and $S: U \rightarrow V$, $T: V \rightarrow W$, the basis of U, V, W are B, C, D . thus, ${}_D [T \circ S]_B = {}_D [T]_C {}_C [S]_B$.

proof: take $\vec{u} \in U$.

$${}_D [T \circ S]_B [\vec{u}]_B = [T(S(\vec{u}))]_D = {}_D [T]_C [S(\vec{u})]_C = {}_D [T]_C {}_C [S]_B [\vec{u}]_B$$

(4) 有时为了方便运算, 会对 input 与 output 的表达形式进行转化

$${}_C [T]_B = [I]_C^A [T]_A [I]_A^B$$

(5) $\ker(T)$ is the nullspace of T , and $\text{im}(T)$ is the column space of T . assume $T: V \rightarrow W$, then $\text{im } T = W$ if and only if T is surjective.

$\ker(T) = 0$ if and only if T is injective

6

(6) let $T: V \rightarrow W$ be a linear map such that $\text{im } T$ is finite-dimensional
then define $\text{rk}(T) = \dim(\text{im}(T))$

(7) let $A \in M_{m,n}$ and $T_A: \mathbb{F}^n \rightarrow \mathbb{F}^m$ be the linear map $T_A(\vec{v}) = A\vec{v}$, then
 $\text{rk}(T_A) = \text{rk } A$

proof:

$$\text{im } T_A = \{A\vec{v} \mid \vec{v} \in \mathbb{F}^n\} = \text{span}(A\vec{e}_1, A\vec{e}_2, \dots, A\vec{e}_n) = \text{im } A$$

(8) let $T: V \rightarrow W$ be a linear map between finite-dimensional vector space V, W with bases B, C respectively, so $\text{rk}(c[T]_B) = \text{rk}(T)$

proof:

assume $B = (\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n)$ and $C = (\vec{w}_1, \vec{w}_2, \dots, \vec{w}_m)$, then the columns of $c[T]_B$ are $[T\vec{v}_1]_C, [T\vec{v}_2]_C, \dots, [T\vec{v}_n]_C$

$$\text{im } c[T]_B = \text{span}([T\vec{v}_1]_C, \dots, [T\vec{v}_n]_C) = [\text{im } T]_C$$

notice that $[\cdot]_C: W \rightarrow \mathbb{F}^m$ is an isomorphism, by the next conclusion we'll show: $\dim(\text{im } c[T]_B) = \dim [\text{im } T]_C = \dim(\text{im } T)$

(9) if $T: V \rightarrow W$ is an isomorphism, $\dim V = \dim W$

proof:

if B is the basis of V , then $T(B)$ is the basis of W , $\dim V = \dim W$

(10) if $T: V \rightarrow V$ to be linear, where V is finite dimensional, then:

$$\dim V = \text{rk } T + \dim \ker T$$

proof:

we first choose a basis for the kernel, assume it be $(\vec{v}_1, \dots, \vec{v}_m)$

we then extend it to the basis of V $(\vec{v}_1, \dots, \vec{v}_m, \vec{u}_1, \dots, \vec{u}_k)$

we can prove that $(T(\vec{u}_1), \dots, T(\vec{u}_k))$ is the basis of $\text{im } T$

(11) if $T: V \rightarrow W$ is linear, and V, W are finite-dimensional, then the following three statements are equivalent:

① T is bijective

- ① T is injective and $\dim V = \dim W$
- ② T is surjective and $\dim V = \dim W$

proof:

- if ①: it leads to injective and surjective. $\dim V = \dim W$ since T sends basis of V to basis of W .
- if ②: $\dim \text{Im } T + \dim \ker T = \dim V = \dim W$
since $\dim \ker T = 0$ due to T is injective
so $\dim \text{Im } T = \dim W$. since $\text{Im } T \subseteq W$, $\text{Im } T = W$
- if ③: $\dim \text{Im } T = \dim W$ due to T is surjective
 $\dim \ker T = 0$.

(II) assume $T: V \rightarrow W$ is linear and V, W are all finite-dimensional

① (T is injective) $\Leftrightarrow (\exists S: W \rightarrow V$ so $S \cdot T = I_V)$

② (T is surjective) $\Leftrightarrow (\exists S: W \rightarrow V$ so $T \cdot S = I_W)$

proof:

this can be proved by using the basis. assume $(\vec{v}_1, \dots, \vec{v}_k, \vec{u}_1, \dots, \vec{u}_m)$ is the basis of V , $(T\vec{v}_1, \dots, T\vec{v}_k, \vec{w}_1, \dots, \vec{w}_n)$ is the basis of W , and $(\vec{u}_1, \dots, \vec{u}_m)$ is the basis of $\ker T$

• if T is injective $S(T\vec{v}_i) = \vec{v}_i$, $S(\vec{u}_j) = 0$

• if T is surjective $n=0$, $S(T\vec{v}_i) = \vec{v}_i$

• double dual subspace

- (1) $V^* = \{T: V \rightarrow F \text{ linear}\}$ is the vector space of linear maps from V to F
the addition is $(f+g)(\vec{u}) = f(\vec{u}) + g(\vec{u})$, and the scalar multiplication is $(\lambda f)(\vec{u}) = \lambda f(\vec{u})$
more generally $\text{Hom}(V, W)$ denotes the vector space of linear maps from V to W .

(2) given a linear transformation $T: V \rightarrow W$, the dual transformation $T^*: W^* \rightarrow V^*$ is defined as $T^*(f) = f \circ T$. T^* is linear.

(3) given a composition $S: U \rightarrow V$, $T: V \rightarrow W$ in such a way, we have $(T \circ S)^* = S^* \circ T^*$.

proof:

$$(T \circ S)^*(f) = f \circ (T \circ S) = S^*(f \circ T) = S^* \circ T^*(f)$$

(4) if $T: V \rightarrow W$ is invertible, so is T^* . $(T^{-1})^* = (T^*)^{-1}$

[注意: 也就是说, 存在一个运算让我从 $T \mapsto T^*$]

(5) given a vector space V , we define the map $\iota: V \rightarrow (V^*)^*$ 其将 $\vec{v} \mapsto \iota\vec{v}$, where $\iota\vec{v}(f) = f(\vec{v})$

[注意: $(V^*)^* = \{V^* \rightarrow F \text{ is linear}\}$, 因此, 给定一个固定运算 ι (固定向量 $\vec{v}$), 从 V^* 中选取函数 f , 最后得到 $\iota\vec{v}(f) = f(\vec{v}) \in F$]

(6) the map ι is injective and linear (assume V is finite-dimensional)

proof:

$$\begin{aligned} \text{• linearity } \iota(\vec{v} + \vec{w})(f) &= f(\vec{v}) + f(\vec{w}) = \iota\vec{v}(f) + \iota\vec{w}(f) \\ \iota(\lambda\vec{v})(f) &= f(\lambda\vec{v}) = \lambda f(\vec{v}) = \lambda \iota\vec{v}(f) \end{aligned}$$

$$\begin{aligned} &\text{for } \vec{v}, \vec{w} \in V \\ &\text{for } \lambda \in F \end{aligned}$$

- injectivity: 我们要证明 if $v \in V$ nonzero, then $\tau v \neq 0$.
也就是说, 只要存在一个函数 f 使 $\tau v(f) \neq 0$ 即可
考虑 V 的 basis $\{v, v_1, v_2, \dots\}$, 并 define 一个函数 $f: V \rightarrow F$ by:
 $f(v) = 1, f(v_i) = 0$ for all i ;
so $f(\lambda v + \sum \lambda_i v_i) = \lambda$.
所以此时, $\tau v(f) = 1$.

(7) if $\dim V = n < \infty$, then $V \cong F^n \cong M_{n,1}$ (考虑 basis), so $V^* \cong F^n \cong M_{1,n}$, so $\dim V = \dim V^*$

since τ is injective and $\dim V = \dim V^* = \dim (V^*)^* < \infty$, τ is an isomorphism

(8) given a finite basis $(v_1, \dots, v_n)$ for a vector space V over F , let $\vec{v}_1^V, \dots, \vec{v}_n^V \in V^*$ be the functions $\vec{v}_i^V(\lambda_1 v_1 + \dots + \lambda_n v_n) = \lambda_i$. in particular, we have the useful formula

$$\vec{v}_i^V(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{otherwise} \end{cases}$$

the n -tuple $(\vec{v}_1^V, \dots, \vec{v}_n^V)$ of elements of V^* is a basis, and $f = \lambda_1 \vec{v}_1^V + \dots + \lambda_n \vec{v}_n^V$

proof:

• linearly independent: if $f = \lambda_1 \vec{v}_1^V + \dots + \lambda_n \vec{v}_n^V = 0$, then $f(v_i) = \lambda_i = 0$ for all i

• spanning: if $f \in V^*$, we claim that $f = f(v_1) \vec{v}_1^V + \dots + f(v_n) \vec{v}_n^V$

[注意: ① $v = \vec{v}_1^V(v) v_1 + \dots + \vec{v}_n^V(v) v_n$

② 本质上就是通过关注 basis 来得到结果, 对于 $f = \lambda_1 \vec{v}_1^V + \dots + \lambda_n \vec{v}_n^V$,

$\vec{v}_i^V$ 本身是一个函数, 且满足 $\vec{v}_i^V(v_j) = \delta_{ij}$, 用于判断 $\vec{v}$ 中 $\vec{v}_i$ 个数

λ_i 为一个基底向量 $\vec{v}_i^V$ 的系数, 即得到 $f(v_i) = \lambda_i$]

(9) taking double dual basis recovers the image under the isomorphism τ

• $B = \{v_1, \dots, v_n\}$ is the basis of V

• $B^V = \{\vec{v}_1^V, \dots, \vec{v}_n^V\}$ is the basis of V^*

• $B^{VV} = \{\vec{v}_1^{VV}, \dots, \vec{v}_n^{VV}\}$ is the basis of V^{**} , $\vec{v}_i^{VV} = \tau(\vec{v}_i^V)$

proof:

$$\tau \vec{v}_i^V(\vec{v}_j^V) = \vec{v}_j^V(v_i) = \delta_{ij} = \vec{v}_i^{VV}(\vec{v}_j^V)$$

[注意: $\vec{v}_i^{VV}$ depends on all of the $\vec{v}_j$, but $\vec{v}_i^V$ only depends on v_i]

事实上 double dual basis is just the original one under the isomorphism τ

(10) given $W \subseteq V$, we define $W^\perp \subseteq V^*$ by: $W^\perp = \{f \in V^* \mid \forall \vec{w} \in W, f(\vec{w}) = 0\}$

(11) if V is finite-dimensional, and $W \subseteq V$ is a subspace, then $\dim V = \dim W + \dim W^\perp$

proof:

assume the basis of W is $\{\vec{w}_1, \dots, \vec{w}_m\}$, we can expand it to the basis of V $\{\vec{w}_1, \dots, \vec{w}_m, \vec{v}_1, \dots, \vec{v}_{n-m}\}$

so $W^\perp = \text{span}\{\vec{v}_1^V, \dots, \vec{v}_{n-m}^V\}$, thus $\dim V = \dim W + \dim W^\perp$

(12) let V and W be finite dimensional vector space with bases B and C respectively. let $T: V \rightarrow W$ be a linear transformation, then

$$B^V[T^*]_C^V = C[T]_B^T$$

proof

write $B = \{\vec{v}_1, \dots, \vec{v}_n\}$, $C = \{\vec{w}_1, \dots, \vec{w}_m\}$

为证明两者相等, 需证明 $(B^T [T^*] C^T)_{ij} = (C^T [T] B)_{ji}$

LHS = $(T^* \vec{w}_j^T)(\vec{v}_i)$, 因为 $T^* \vec{w}_j^T = \lambda_1 \vec{v}_1^T + \dots + \lambda_n \vec{v}_n^T$

确定列, 取行元素

RHS = $\vec{w}_j^T (T \vec{v}_i)$ 因为 $\vec{w} = \lambda_1 \vec{w}_1 + \dots + \lambda_m \vec{w}_m$

取行元素, 确定列

LHS = RHS by definition.

• determinant

(1) $\det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij}$, $A \in M_n(F)$, $i=1, 2, \dots, n$

(2) •
$$\begin{vmatrix} \lambda a_{11} & \lambda a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix} = \lambda \begin{vmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix}$$

•
$$\begin{vmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix} + \begin{vmatrix} b_{11} & b_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix}$$

•
$$\begin{vmatrix} a_{11} & a_{12} & \dots \\ a_{11} & a_{12} & \dots \\ a_{31} & a_{32} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix} = 0$$

•
$$\begin{vmatrix} a_{21} & a_{22} & \dots \\ a_{11} & a_{12} & \dots \\ a_{31} & a_{32} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix} = - \begin{vmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ a_{31} & a_{32} & \dots \\ \vdots & \vdots & \ddots \end{vmatrix}$$

(3) if $A, B \in M_n(F)$, and they are row-equivalent, then $\det A = \beta \det B$ for some $\beta \neq 0$

(4) an elementary matrix is one that is obtained from I_n , with a single elementary row operation

$\det(EA) = \det E \det A$ for swapping, replacing and rescaling matrices

(5) proof: if $EA = B$, then A and B are row-equivalent, so $\det B = \beta \det A$

whereas $\det E = \det EI = \beta \det I = \beta$

so $\det EA = \det E \det A$

(6) suppose $A \in M_n(F)$, then following are equal:

① A is invertible ② A is non-singular

③ the rows of A are linear independent

④ A is row-equivalent to I ⑤ $\det A \neq 0$

proof: ④ $\rightarrow$ ⑤: $\det A = \beta \det I$, ⑤ $\rightarrow$ ④ by contradiction.

(6) suppose $A, B \in M_n(\mathbb{F})$, then:

① AB is singular if and only if at least one of A, B is singular.

② $\det AB = 0$ if and only if $\det A = 0$ or $\det B = 0$

proof: use 'not invertible'

(7) let $A, B \in M_n(\mathbb{F})$, then $\det AB = \det A \det B$

proof: if A or B is singular, then we are done.

if A and B are non-singular, then $A = \prod E_i, B = \prod E_j$

$$AB = \prod E_i \prod E_j, \det AB = \det(\prod E_i \prod E_j)$$

$$= \prod \det E_i \prod \det E_j$$

$$= \det(\prod E_i) \det(\prod E_j) = \det A \det B$$

(8) suppose $A \in M_n(\mathbb{F})$, then $\det A = \det A^T$

proof: $\det E = \det E^T$. if $A = \prod E_i$, $\det A = \prod \det E_i = \prod \det E_i^T = \det A^T$

(9) 范德蒙矩阵 $M = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}$, $\det M = \prod_{1 \leq i < j \leq n} (x_j - x_i)$

$$\det M = 0 \iff x_i = x_j \text{ for some } i, j$$

proof: 用 induction. 现在主要关注 iterative step

进行列运算: $\det M = \det \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ x_2 - x_1 & x_2(x_2 - x_1) & \dots & x_2^{n-1} - x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n - x_1 & x_n(x_n - x_1) & \dots & x_n^{n-1} - x_1^{n-1} \end{pmatrix}$

$$C_n \rightarrow C_n - x_1 C_1, C_{n-1} \rightarrow C_{n-1} - x_1 C_2, \dots$$

$$= \prod_{2 \leq i \leq n} (x_i - x_1) \begin{vmatrix} 1 & x_2 & \dots & x_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{n-2} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

(10) if $A = (a_{ij})$, then the cofactor matrix $C := (C_{ij})$, where $C_{ij} = (-1)^{i+j} \det(A_{ij})$.

we define $\text{Adj}(A) := C^T$, which is called the adjoint of A

notice that $\text{Adj}(A) \cdot A = \det(A) \cdot I$, so $A^{-1} = \frac{\text{Adj}(A)}{\det(A)}$

(11) let $T: V \rightarrow V$, and V is a finite-dimensional vector space over $\mathbb{F}$, then λ is an eigenvalue of T if $\exists \vec{v} \in V \setminus \{0\}$ such that $T(\vec{v}) = \lambda \vec{v}$

T is diagonalizable if and only if $\exists$ a basis B of eigenvectors over V .

• the eigenvalues of T are the same as those of $[T]_B$ (for some B)

• the character polynomial of a matrix is defined as $\det(xI - A)$
 $= \chi_A(x)$. (用 induction 证明是 polynomial)

[注意: 巧用 diagonalisation 来解 A^m]

• if $A \in M_n(\mathbb{F})$ and $\lambda \in \mathbb{F}$, let $E_\lambda = \{\vec{v} \in \mathbb{F}^n \mid A\vec{v} = \lambda \vec{v}\}$, this is the eigenspace of A for eigenvalue λ .

$\dim E_\lambda$ is called the geometric multiplicity of λ .

- multiplicity of λ as a root of $\chi_A(x)$ is called the algebraic multiplicity
- (A is diagonalisable) $\Leftrightarrow (\chi_A(x)$ factors into linear factor, and for all roots λ of $\chi_A(x)$, its geometric multiplicity = its algebraic multiplicity)

Proof: we need to prove some lemma first.

① V is a finite-dimensional vector space over $\mathbb{F}$, and $T: V \rightarrow V$.
suppose the eigenvectors $\vec{v}_1, \dots, \vec{v}_k$ has corresponding eigenvalues $\lambda_1, \dots, \lambda_k$. $\lambda_i \neq \lambda_j$ for $i \neq j$, then eigenvectors are linear independent

WTP: if $\alpha_1 \vec{v}_1 + \dots + \alpha_k \vec{v}_k = 0$, then $\alpha_1 = \dots = \alpha_k = 0$, by induction

case 1: true

inductive: if $\exists \alpha_i = 0$, true by eliminating $\vec{v}_i$

if $\forall \alpha_i \neq 0$, then $\frac{0}{\alpha_1} = \vec{v}_1 + \frac{\alpha_2}{\alpha_1} \vec{v}_2 + \dots + \frac{\alpha_k}{\alpha_1} \vec{v}_k = \vec{v}$

$$T(\vec{v}) = \lambda_1 \vec{v}_1 + \lambda_2 \alpha'_2 \vec{v}_2 + \dots + \lambda_k \alpha'_k \vec{v}_k$$

$$\therefore T(\vec{v}) - \lambda_1 \vec{v} = 0 - 0 = 0$$

$$\therefore \underbrace{(\lambda_2 - \lambda_1)}_{\text{non-zero}} \alpha'_2 \vec{v}_2 + \dots + \underbrace{(\lambda_k - \lambda_1)}_{\text{non-zero}} \alpha'_k \vec{v}_k = 0$$

so

so $\alpha'_2 = \alpha'_3 = \dots = \alpha'_k = 0$, $\alpha_1 = \alpha_2 = \dots = \alpha_k = 0$ contradict!

② for any eigenvalue λ of A , its geometric multiplicity $\leq$ algebraic multiplicity

assume the corresponding eigenvectors are $\vec{v}_1, \dots, \vec{v}_g$

we expand it to form a basis of V : $\{\vec{v}_1, \dots, \vec{v}_g, \vec{w}_{g+1}, \dots, \vec{w}_n\} = B$

notice that, in such a way, ${}_B[A]_B = \begin{pmatrix} \lambda I_g & 0 \\ 0 & D \end{pmatrix}$

since ${}_B[A]_B$ and A has same χ_A

$$\chi_A(x) = \det(xI - {}_B[A]_B) = (x - \lambda)^g q(x), \text{ done.}$$

then we just prove $\Rightarrow$

let B be basis of V , and B_{λ_i} be the set of basis of E_{λ_i}

since $B = B_{\lambda_1} + B_{\lambda_2} + \dots + B_{\lambda_a}$ and $B_{\lambda_i} \neq B_{\lambda_j}$ for $i \neq j$

$$|B| = |B_{\lambda_1}| + |B_{\lambda_2}| + \dots + |B_{\lambda_a}| = n.$$

by ②, done

(12) if $A \in M_n(\mathbb{F})$, A is diagonal and eigenvalues have their n^{th} roots for some $n \in \mathbb{N}$: then we can find a $C \in M_n(\mathbb{F})$ such that $C^n = A$, where $A = PDP^{-1}$,

$$C = PMP^{-1}, M^n = D.$$

(13) for an iterative equation system

9.

$$\begin{aligned} a_n &= \alpha a_{n-1} + \beta b_{n-1} \\ b_n &= \gamma a_{n-1} + \Omega b_{n-1} \end{aligned} \Rightarrow \begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \Omega \end{pmatrix} \begin{pmatrix} a_{n-1} \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \Omega \end{pmatrix}^n \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$$

随后用diagonalise即可简便运算

(14) assume A has eigenvalues $\lambda_1, \dots, \lambda_l$ and the corresponding basis of eigenspaces are $B_1, \dots, B_l$, then $\bigcup_{i=1}^l B_i$ is linearly independent set.

proof: if $0 = \sum_{i=1}^l \sum_{j=1}^{q_i} \alpha_{ij} v_{ij}$

then $\sum_{j=1}^{q_i} \alpha_{ij} v_{ij} = 0$ for all i

so $\alpha_{ij} = 0$ for all i, j

(15) for $A \in M_n(\mathbb{F})$, if $\chi_A(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + x^n$

then $\chi_A(A) = a_0 I + a_1 A + \dots + a_{n-1} A^{n-1} + A^n = 0$

orthogonality

(1) let $\vec{u}, \vec{v} \in \mathbb{R}^n$, then $\vec{u}, \vec{v}$ orthogonal if $\vec{u} \cdot \vec{v} = 0$, orthonormal if $\vec{u} \cdot \vec{v} = 0$ and $\|\vec{u}\|, \|\vec{v}\| = 1$

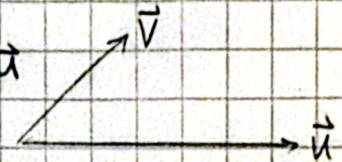
(2) $\|a\vec{u}\| = |a| \|\vec{u}\|$, $|\vec{u} \cdot \vec{v}| \leq \|\vec{u}\| \|\vec{v}\|$, $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$, $\|\vec{u} - \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$

proof: for $|\vec{u} \cdot \vec{v}| \leq \|\vec{u}\| \|\vec{v}\|$, consider minimise $\|\lambda \vec{u} - \vec{v}\|$.

$$\|\lambda \vec{u} - \vec{v}\|^2 = \lambda^2 \|\vec{u}\|^2 + \|\vec{v}\|^2 - 2\lambda(\vec{u} \cdot \vec{v}) \geq 0$$

$$\text{minimise when } \lambda = \frac{-b}{2a} = \frac{\vec{u} \cdot \vec{v}}{\|\vec{u}\|^2}, \text{proj}_{\vec{u}}(\vec{v}) = \frac{\vec{u} \cdot \vec{v}}{\|\vec{u}\|^2} \vec{u}$$

带入即得结果



(3) a matrix is orthonormal if $A^T A = I_n$

so $(A\vec{u}) \cdot (A\vec{v}) = \vec{u} \cdot \vec{v}$
 $(A\vec{u})^T (A\vec{v}) = \vec{u}^T \vec{v}$ } properties preserved by orthogonal transformation.

$$A^T = A^{-1}, \det(A) = \pm 1$$

(4) given a basis $\{\vec{v}_1, \dots, \vec{v}_n\}$, we can find $\{\vec{u}_1, \dots, \vec{u}_n\}$ orthogonal basis such that

$$\text{span}(\vec{v}_1, \dots, \vec{v}_i) = \text{span}(\vec{u}_1, \dots, \vec{u}_i)$$

$$\text{let } \vec{u}_1 = \vec{v}_1, \vec{u}_2 = \vec{v}_2 - \frac{(\vec{v}_1 \cdot \vec{v}_2)}{\|\vec{v}_1\|^2} \vec{v}_1, \dots, \vec{u}_n = \vec{v}_n - \sum_{i=1}^{n-1} \frac{\vec{v}_i \cdot \vec{v}_n}{\|\vec{v}_i\|^2} \vec{v}_i, \vec{u}_i = \frac{\vec{u}_i}{\|\vec{u}_i\|} \text{即归一化}$$

$\{\vec{u}_1, \vec{u}_2, \dots, \vec{u}_n\}$ are linearly independent

proof: if $\alpha_1 \vec{u}_1 + \alpha_2 \vec{u}_2 + \dots + \alpha_n \vec{u}_n = 0$, then $(\alpha_1 \vec{u}_1 + \dots + \alpha_n \vec{u}_n) \cdot \vec{u}_i = \alpha_i = 0$

(5) every real symmetric matrix is diagonalisable with an orthogonal transformation

$$A = A^T, \exists P \in O_n(\mathbb{R}), \text{ such that } P^T A P = D, P^T = P^{-1}$$

proof: lemma 1. all eigenvalues are real.

设 λ 为 eigenvalue, 则 $\bar{\lambda}$ 也是 eigenvalue. $A\vec{v} = \lambda\vec{v} \Rightarrow \bar{A}\vec{v} = \bar{\lambda}\vec{v}$

$$\lambda(\vec{v} \cdot \vec{v}) = (A\vec{v}) \cdot \vec{v} = (A\vec{v})^T \vec{v} = \vec{v}^T A^T \vec{v} = \vec{v}^T (\bar{A}\vec{v}) = \bar{\lambda}(\vec{v} \cdot \vec{v})$$

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

② lemma 2. if λ, μ are different eigenvalues with eigenvectors $\vec{u}, \vec{v}$, $\vec{u} \cdot \vec{v} = 0$

$$\lambda(\vec{u} \cdot \vec{v}) = (A\vec{u}) \cdot \vec{v} = (A\vec{u})^T \vec{v} = \vec{u}^T (A\vec{v}) = \mu(\vec{u} \cdot \vec{v})$$

③ lemma 3. for a $n \times n$ real symmetric matrix A , it has at least one eigenvectors $A\vec{v}_1 = \lambda_1 \vec{v}_1$.

we then find out $\vec{v}_2, \dots, \vec{v}_n$, such that $\vec{v}_i \cdot \vec{v}_j = 0$ for $i \neq j \in \{1, 2, \dots, n\}$

[考虑 1. 与 2. 同时成立, 1 与 2 实在不行考虑个例子]

then let $P = (\frac{\vec{v}_1}{\|\vec{v}_1\|}, \frac{\vec{v}_2}{\|\vec{v}_2\|}, \dots, \frac{\vec{v}_n}{\|\vec{v}_n\|})$, $P^T P = I_n$

notice $P^T A P = P^T A P$

$(P^T A P)^T = (P^T A P)^T = P^T A^T P$, so $A = A^T$

as $A = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & & \\ 0 & & B \end{pmatrix}$, B is symmetric as well

so we can use induction.

group

(1) $(G, *)$, where G is a set and $*: G \times G \rightarrow G$, is a group if

- $*$ is associative

- $\exists e \in G$ such that $g * e = e * g = g$

- $\forall g \in G, \exists h \in G$, such that $g * h = h * g = e$

proof: ① e is unique by considering $e = e e' = e'$

② h is unique for all g by considering $h_1 = e h_1 = (h_2 g) h_1 = h_2 (g h_1) = h_2$

(2) for a group $(G, *)$, $g, h \in G$

- if $xg = h$, $x = hg^{-1}$; if $gx = h$, $x = g^{-1}h$

- $(gh)^{-1} = h^{-1}g^{-1}$ by considering $(gh)(h^{-1}g^{-1}) = (h^{-1}g^{-1})gh = e$

(3) for a group $(G, *)$, it is abelian if $\forall g, h \in G$, $g * h = h * g$

(4) some special groups:

- cyclic group: $(G, *)$, where $G = \{\alpha^n | n \in \mathbb{Z}\}$ for $\alpha \in G$, α is generator.

[注意: 有限循环群: $(\{\xi^n | n \in \mathbb{Z}, \xi^m = 1\}, *)$

无限循环群: $(\mathbb{Z}, +) = (\{n \cdot 1 | n \in \mathbb{Z}\}, +)$

- let X be a set, $\alpha: X \rightarrow X$ is a permutation if α is bijection.

$\text{sym}(X) = \{\text{all permutations of } X\}$, and $(\text{sym}(X), \circ)$ is a group.

[注意: cycle 的表达形式分两种: $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ 或 (123) e.g.

every cycle $\alpha \in \text{sym}(X)$ factors uniquely as product of disjoint cycles]

(5) $(G, \circ)$ is a finite group if $|G| < \infty$, and $|G|$ is called the 'order' of G .
for $g \in G$, $o(g)$ is the smallest positive integer k such that $g^k = e$, and $o(g)$ is called the order of g .

① $\langle g \rangle = \{g^0, g^1, g^2, \dots\}$ is a group if $|G| < \infty$

② $o(g) \mid |G|$ (陪集分解进行证明)

(6) a subgroup of G is a subset $H \subseteq G$ such that it satisfies closure, the existence of identity, and invertible. this we write $H \leq G$.

若 $(G, \circ)$ is a group, then H is a

$$(1) H \neq \emptyset \quad (2) \forall h, h^{-1} \in H \quad (3) \forall h, h^{-1} \in H$$

[注意, subspace 的定义: if G is a vector space, and $H \subseteq G$, then H is a sub space if and only if

$$(1) \vec{0} \in H \quad (2) \forall \vec{h}, \vec{h}_1 \in H, \lambda_1, \lambda_2 \in \mathbb{F}, \lambda_1 \vec{h}_1 + \lambda_2 \vec{h}_2 \in H]$$

(1) suppose G is finite group, 我们可以更进一步精简上述条件

- every element of G has finite order
- if $H \subseteq G$ is a non-empty subset of G and for all $h, h_1 \in H$ we have $h, h_1 \in H$, then H is a subgroup of G

proof: (1) consider $g, g^2, g^3, \dots \in G$, as $|G|$ is finite, there exists $0 < m < l$ with $g^m = g^l$, then $\forall l > m$ and $g^{m-l} = e$

(2) we just need to show $\forall h \in H, \exists h^{-1} \in H$
assume $o(h) = k$, then $h^{k-1} = h^{-1} \in H$

(3) suppose $(G, \cdot)$ is a cyclic group and $G = \langle g \rangle$

- if $H \subseteq G$, then H is cyclic
- suppose $|G| = n$ ($o(g) = n$) and $m \in \mathbb{Z}$ let $d = \gcd(m, n)$, then

$$\square \langle g^m \rangle = \langle g^d \rangle$$

$$\square |\langle g^d \rangle| = \frac{n}{d}$$

$\square$ in particular, $\langle g^m \rangle = G$ if and only if $d = 1$

- if $|G| = h$ and $k \leq h$, then G has a subgroup of order k if and only if $k | h$. in this case, the subgroup is $\langle g^{\frac{h}{k}} \rangle$

proof: (1) we assume $H \neq \{e\}$, let d be the least element of $\{n \in \mathbb{N} : g^n \in H\}$
thus, $\langle g^d \rangle \subseteq H$

we now show $H \subseteq \langle g^d \rangle$. let $h \in H$, then $h = g^m$ for some $m \in \mathbb{Z}$ by definition of $G = \langle g \rangle$

so we write $m = qd + r$, for some $q, r \in \mathbb{Z}$ and $0 \leq r < d$

$$\text{then } h = g^{qd+r} = (g^d)^q g^r, g^r = h (g^d)^{-q} \in H$$

如果 $r > 0$, 则 $g^r \in H$ 违反 d be the least element of $\{n \in \mathbb{N} : g^n \in H\}$
so $r = 0$

(2) $\square$ to show $\langle g^m \rangle = \langle g^d \rangle$, we just need to show $g^m \in \langle g^d \rangle, g^d \in \langle g^m \rangle$
the first statement is true as $d | m$

for the second statement: $g^d = g^{km+ln} = g^{km} = (g^m)^k$, so $g^d \in \langle g^m \rangle$

(9) for $n \in \mathbb{N}$, the Euler totient function $\phi(n)$ is

$$|\{k \in \mathbb{N} \mid 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}|$$

for all $n \in \mathbb{N}$, we have $\sum_{1 \leq d \leq n, d | n} \phi(d) = n$

proof: if $d | n$, G has a unique subgroup G_d of order d , and it contains every element of G of order d , the subgroup is $\langle g^{\frac{n}{d}} \rangle$

[考虑上一条证明的2.1与3. 实在不行考虑个例子]

- 此时, G_d 中阶为 d 的元素个数为 $\phi(d)$ 这是因为 if $G_d = \langle h \rangle$, $\langle h^k \rangle = G_d$ if and only if $\gcd(k, d) = 1$. 所以在 G_d 中恰好有 $\phi(d)$ 个元素的阶为 d .
 - G 中总元素数为 $|G| = n$, 每个元素由阶 d 必整除 n , 且阶 d 对应 $\phi(d)$ 个元素
- $$\sum_{1 \leq d \leq n, d|n} \phi(d) = |G| = n.$$

(10) suppose $(G, \circ)$ is a group and $S \subseteq G$ is non-empty, let $S^{-1} = \{g^{-1} | g \in S\}$ and $\langle S \rangle = \{g, g, \dots, g_k | k \in \mathbb{N} \text{ and } g, g, \dots, g_k \in S \cup S^{-1}\}$, then

• $\langle S \rangle$ is a subgroup of G (proved by subgroup test)

• if $H \leq G$ and $S \subseteq H$, $\langle S \rangle \subseteq H$.

so $\langle S \rangle$ is the smallest subgroup of G containing S ; it is called the subgroup of G generated by S .

• if $S = \{x_1, \dots, x_n\}$, $\langle S \rangle = \langle x_1, \dots, x_n \rangle$

• if G is abelian, then $\langle x_1, \dots, x_n \rangle = \langle x_1^{k_1}, x_2^{k_2}, \dots, x_n^{k_n} | k_1, k_2, \dots, k_n \in \mathbb{Z} \rangle$

(11) Lagrange's theorem: suppose $(G, \cdot)$ is a finite group and H is a subgroup of G , then $|H| \mid |G|$.

(12) Fermat's Little theorem: suppose p is any prime, if $x \in \mathbb{Z}$ and $p \nmid x$, then $x^{p-1} \equiv 1 \pmod{p}$

Proof 陪集定理的证明:

assume $(G, \circ)$ is a group and $H \leq G$, then for $g \in G$, $gH = \{gh | h \in H\}$ is called a left coset of H in G .

• if $g, k \in G$, $gH \cap kH \neq \emptyset$, then $gH = kH$

◦ if $g = k h_0$, then $g h = k h_0 h$, $h_0 h \in H$, so $gH \subseteq kH$

• $k h = g h_0^{-1} h$, $h_0^{-1} h \in H$, so $kH \subseteq gH$

• so $gH = kH$

◦ if $g h_1 = k h_2$, $g = k h_2 h_1^{-1}$, $gH = kH$

• $|gH| = |H|$, because if $g h_1 = g h_2$, $h_1 = h_2$.

• $\bigcup_{g \in G} gH = G$, $|H| \mid |G|$.

费马小定理的证明: consider $\{\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times\}$

[注意] • 证明 if $a, b \in S_3$, $o(a) = 3$, $o(b) = 2$, then $\langle a, b \rangle = S_3$

这是因为 $\langle a, b \rangle \leq S_3$, so $|\langle a, b \rangle| \mid |S_3| = 6$

又因为 $o(a) = 3 \mid |\langle a, b \rangle|$, $o(b) = 2 \mid |\langle a, b \rangle|$, so $6 \mid |\langle a, b \rangle|$

so $|\langle a, b \rangle| = 6$, $\langle a, b \rangle = S_3$

• suppose p is a prime and G is group of order p , then G is cyclic. in fact, if $e \neq g \in G$, $\langle g \rangle = G$

because $|\langle g \rangle| \mid p$ but $|\langle g \rangle| \neq 1$, so $|\langle g \rangle| = p$.

(11) Assume $H \leq G$ are all finite groups, then the number of left cosets of H in G is called the index of H in G . $[G:H] = \frac{|G|}{|H|}$

[注意: 在找所有的 left cosets 时, 若选定了一个 left coset $\langle a \rangle$, 则找 β 使得 $\langle a, \beta \rangle = G$]

• Homomorphisms

(1) Suppose $(G, \cdot), (H, \cdot)$ are groups, a function $\phi: G \rightarrow H$ is a homomorphism

if $\forall g_1, g_2 \in G, \phi(g_1 g_2) = \phi(g_1) \phi(g_2)$

$\text{im } \phi = \{ \phi(g) \mid g \in G \}, \text{ker } \phi = \{ g \in G \mid \phi(g) = e_H \}$

(2) if the homomorphism ϕ is bijection, then ϕ is isomorphism.

We say groups G, H are isomorphic if there exists an isomorphism $\phi: G \rightarrow H$ in this case $G \cong H$.

(3) Suppose G, H are groups and $\phi: G \rightarrow H$ is a homomorphism, then

- $\phi(e_G) = e_H$

- $\phi(g^{-1}) = (\phi(g))^{-1} \forall g \in G$

- $\text{im } \phi \leq H, \text{ker } \phi \leq G$

(4) Suppose G, H, K are groups.

- a homomorphism $\phi: G \rightarrow H$ is injective if and only if $\text{ker } \phi = \{e_G\}$

- if $\phi: G \rightarrow H$ and $\psi: H \rightarrow K$ are homomorphism, then the composition

$\psi \circ \phi: G \rightarrow K$ is a homomorphism.

- if $\phi: G \rightarrow H$ is an isomorphism, then the inverse map $\phi^{-1}: H \rightarrow G$ is also an isomorphism

proof ① $\phi(e_G) = e_H$, so $e_G \in \text{ker } \phi$. by injectivity, $|\text{ker } \phi| \leq 1$, so $\text{ker } \phi = \{e_G\}$

(5) • Suppose G, H are cyclic groups of the same order, then there is an isomorphism $\alpha: G \rightarrow H$

- if V_1, V_2 are non-cyclic groups of order 4, then $V_1 \cong V_2$

proof: ① first assume G, H are finite, cycle of order n with $G = \langle g \rangle$ and $H = \langle h \rangle$, define $\alpha: G \rightarrow H$ by $\alpha(g^k) = h^k$ for $k \in \mathbb{Z}$
show it is well-defined

$$g^k = g^l \Leftrightarrow k = nm + l \Leftrightarrow h^k = h^l$$

it is also injective (equation above) and surjective (by definition)

thus, α is bijection if G, H are finite

② now assume G, H are infinite; we have

$$g^k = g^l \Leftrightarrow k = l \Leftrightarrow h^k = h^l$$

so it is well-defined, injective and surjective

- let $V_1 = \{e, a, b, c\}$. notice that since V_1 isn't cyclic, so $o(a), o(b), o(c) \neq 4$. also, $o(a), o(b), o(c) \mid 4$

thus $o(a) = o(b) = o(c) = 2$

we notice that $ab = ba = c$, $ac = ca = b$, $bc = cb = a$, otherwise $a, b, c = e$

if $V_2 = \{e', a', b', c'\}$, then V_2 has the similar properties.

so the map $e \mapsto e'$, $a \mapsto a'$, $b \mapsto b'$, $c \mapsto c'$ is an isomorphism from V_1 to V_2

S_n : (1) let $f, g \in S_n$ and $x \in [n] = \{1, 2, \dots, n\}$. we say that f fixes x if $f(x) = x$ and f moves x if $f(x) \neq x$. the support of f is $\{y \in [n] \mid f(y) \neq y\}$. this is denoted by $\text{supp}(f)$.

- we say f and g have disjoint supports (or are disjoint) if $\text{supp}(f) \cap \text{supp}(g) = \emptyset$

- note as f is a bijection, if $f(y) \neq y$, then $f(f(y)) \neq f(y)$, so $f(y) \in \text{supp}(f)$

- also $\text{supp}(f) = \text{supp}(f^{-1})$

(2) if $f, g \in S_n$ have disjoint supports, then

- $fg = gf$

- for all $m \in \mathbb{Z}$, we have $(fg)^m = f^m g^m$

(3) let $n \in \mathbb{N}$ and $r \leq n$, suppose $i_1, \dots, i_r \in [n]$ are distinct. if $f \in S_n$ fixes the other elements of $[n]$, then

$$f(i_1) = i_2, f(i_2) = i_3, \dots, f(i_{r-1}) = i_r, f(i_r) = i_1$$

then f is called an n -cycle or a cycle of length n , written as $(i_1, i_2, \dots, i_r)$.

(4) if $f = (i_1, i_2, \dots, i_r) \in S_n$, then f^{-1} is the r -cycle $g = (i_r, i_{r-1}, \dots, i_2, i_1)$

(5) if $f \in S_n$, there exists cycles $f_1, f_2, \dots, f_k \in S_n$ with disjoint supports such that $f = f_1 f_2 \dots f_k$. the combination is unique up to reordering.

proof: prove by induction on $m = |\text{supp}(f)|$ homomorphism $f: G \rightarrow S_n$

- if $m = 0$, $\text{supp}(f) = \emptyset$, $f = \tau$, $gh = hg$

- assume $m \leq k$ is true, consider $m = k + 1$

then take $i_1 \in \text{supp}(f)$, we have $i_2 = f(i_1)$, $i_3 = f(i_2)$, ...

choose r as small as possible such that $f(i_r) \in \{i_1, i_2, \dots, i_{r-1}\}$.

and $f(i_r) = i_1$ by contradiction. $f \in \langle g \rangle$ $g \cdot h = g \cdot h$, so $g_1 = g_2$

so it follows that $f = g f_1$, where $f_1 = (i_1, i_2, \dots, i_r)$, and g has supports $\text{supp}(f) \setminus \{i_1, i_2, \dots, i_r\}$ as $g = f f_1^{-1}$

so by hypothesis, done

to prove unique:

assume $f = f_1 f_2 \dots f_n = h_1 h_2 \dots h_m$ where f_i, h_j are cycles with distinct supports with f_i, h_j respectively

if $i_1 = \text{supp}(f_1) \cap \text{supp}(g_j)$, $f_1 = g_j$ by $(i_1, f_1(i_1), f_1^2(i_1), \dots, f_1^n(i_1))$

[注意: $(a_1, a_2, \dots, a_n) = (a_1, a_2)(a_2, a_3) \dots (a_{n-1}, a_n)$]

(6) the cycle shape of a permutation $f \in S_n$ is the sequence of cycle lengths in decreasing order, including repetitions and fixed points, which is written in disjoint cycle form.

(7) there are $\binom{n}{r} (r-1)!$ distinct r -cycle in a set of size $n \geq r$.

(8) suppose $g \in S_n$ is written in disjoint cycle form as $g = g_1 g_2 \dots g_k$ where g_i is an r_i -cycle (for $i=1, 2, \dots, k$) and $g_1, \dots, g_k$ are disjoint. if $m \in \mathbb{N}$, then:

- $g^m = g_1^m g_2^m \dots g_k^m$

- $(g^m = 1) \Leftrightarrow (g_i^m = 1 \text{ for all } i=1, 2, \dots, k)$

- the order of g is the lcm of length of disjoint cycles of g

- $g^{-1} = g_1^{-1} g_2^{-1} \dots g_k^{-1}$

(9) 任何有限群 G , 都存在 $n \in \mathbb{Z}$ such that injective homomorphism $\varphi: G \rightarrow S_n$.

proof: $\forall g \in G$, 都有映射 $\lambda_g: G \rightarrow G, \lambda_g(h) = gh$.

其中 λ_g 是从 G 到 G 的双射

因为每个 λ_g 都是 G 上的置换, $\lambda_g \in S_{|G|}$

所以同态 $\varphi: G \rightarrow S_{|G|}, \varphi(g) = \lambda_g$.

验证 φ injective: if $\varphi(g_1) = \varphi(g_2), \forall h \in G, g_1 h = g_2 h$, so $g_1 = g_2$.

(10) each permutations can be decomposed as a product of transpositions

proof: by induction $(a_1, a_2, \dots, a_n) = (a_1, a_2) (a_2, a_3) \dots (a_{n-1}, a_n)$

(11) for $n \geq 2$, we define D_{2n} as the group of symmetries of the regular n -gon. $|D_{2n}| = 2n$ and D_{2n} is 2-generated

example: $D_8 = \{1, (1 2 3 4), (1 4 3 2), (1 2)(3 4), (1 3), (2 4), (1 4)(2 3), (1 3)(2 4)\}$

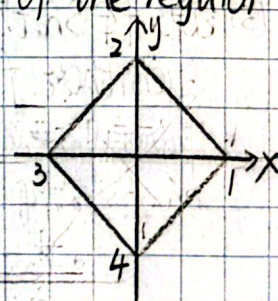
proof: 我们先证明 $|D_{2n}| \geq 2n$.

对于 odd n : 有 n 个 cycle 代表 $e^{i \frac{2\pi}{n}}$ 为旋转,

有 n 个 cycle 代表过某一点点对称.

对于 even n : 有 n 个 cycle 代表 $e^{i \frac{2\pi}{n}}$ 为旋转

有 n 个 cycle 代表 n 个对称轴变化



• 随后证明 $|D_{2n}| = 2n$.

we can find a finite group G acting on a set X such that

$\varphi: G \rightarrow \text{Symm}(X)$

define for fixed $x \in X$, orbit of x , $O(x)$, is $\{g \cdot x \mid g \in G\}$, where $g \cdot x = \varphi(g)(x)$.

then $O(x) = \frac{|G|}{|\text{stab}(x)|}$, where $\text{stab}(x) = \{g \in G \mid g \cdot x = x\}$, by considering the left coset of $\text{stab}(x)$ in G .

thus, D_{2n} acts on $\{1, 2, \dots, n\}$, $O(1) = \{1, 2, \dots, n\}$, $\text{stab}(1) = \{1, \tau\}$.

where T represents reflections with axis passing l .

$$n = \frac{|D_{2n}|}{2}, |D_{2n}| = 2n$$

• 最后证明其为 2-generated.

考虑 $a = (1)(2\ n)(3\ n-1)\dots$

$$b = (1\ n)(2\ n-1)\dots$$

$$ab = (1\ 2\ 3\ \dots\ n-1\ n)$$

and $D_{2n} = \langle a, b \rangle$. because $|a| = |b| = 2$, $|ab| = n$, $|\langle a, b \rangle| = 2n$.

(12) sign of permutation

recall that every permutation in S_n can be written as a product of 2-cycle. $(a_1, a_2, \dots, a_n) = (a_1, a_2)(a_2, a_3)\dots(a_{n-1}, a_n)$

the decomposition isn't unique, but the number of 2-cycles is either always odd or always even.

• let $n \in \mathbb{N}$ with $n \geq 2$. let $x_1, x_2, \dots, x_n$ be variables. if $P(x_1, x_2, \dots, x_n)$ is any polynomial in variables $x_1, x_2, \dots, x_n$ and $f \in S_n$, then we define $f(P)$ to be the polynomial $P(x_{f(1)}, x_{f(2)}, \dots, x_{f(n)})$.

• for all $f, g \in S_n$ and polynomial P in variables $x_1, x_2, \dots, x_n$, we have

① if $\alpha \in \mathbb{R}$, $f(\alpha P) = \alpha f(P)$

② $g(f(P)) = (gf)(P)$

proof: ③ $x_{g(f(x_i))} = x_{(gf)(x_i)}$

• focus on $\Delta = \Delta(x_1, x_2, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$

then for any $n \geq 2$ and $f \in S_n$, $f(\Delta) = \Delta$ or $-\Delta$.

We say $\text{sgn}(f) = 1$ if $f(\Delta) = \Delta$, $\text{sgn}(f) = -1$ if $f(\Delta) = -\Delta$.

• suppose $n \geq 2$ and $f, g \in S_n$.

① $\text{sgn}(fg) = \text{sgn}(f)\text{sgn}(g)$. so $\text{sgn}: S_n \rightarrow \pm 1$ is homomorphism.

② if f is a 2-cycle, $\text{sgn}(f) = -1$

③ if f is a r -cycle, $\text{sgn}(f) = (-1)^{r-1}$

proof: ④ $(fg)(\Delta) = f(g(\Delta)) = f(\text{sgn}(g)\Delta) = \text{sgn}(g)f(\Delta) = \text{sgn}(g)\text{sgn}(f)\Delta$

• a permutation $f \in S_n$ is even if $\text{sgn}(f) = 1$, is odd if $\text{sgn}(f) = -1$

the set of even permutations in S_n is a subgroup of S_n , called the alternative group A_n (the kernel of the homomorphism sgn). if $n \geq 2$ then the index of A_n in S_n is 2 (the two cosets of A_n are A_n and the set of odd permutations)

proof let $\sigma \in A_n$, $\text{sgn}(\tau) = -1$,

$\text{sgn}(\tau\sigma) = -1$, so, $\tau\sigma \in$ the set of odd permutations

- $\forall \text{sgn}(p) = -1, \text{sgn}(\tau^{-1}p) = 1$, so τ^{-1} the set of odd permutation $\subseteq A_n$.
- decomposition for each permutation isn't unique, but the sgn is.
- proof: if $f = f_{11} f_{12} \dots f_{1m} = f_{21} f_{22} \dots f_{2n}$, where f_{ij} are 2-cycles, then $e = f_{11} f_{12} \dots f_{1m} f_{2n}^{-1} \dots f_{22}^{-1} f_{21}^{-1}$, with sgn of 1. so both parts have sgn of 1 or -1.

- for every matrix $A = (a_{ij}) \in M_n(\mathbb{F})$, we have $\det A = \sum_{f \in S_n} \text{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)}$
- proof we firstly consider $\det' A = \sum_{f \in S_n} \text{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)}$

我们只需证明其满足 $\det A$ 的 D1 D2 D3 D4 四条法则即可

只关注 D3: assume row 1 and 2 of A are equal, so $a_{1j} = a_{2j}$ for $j \leq n$. let $g \in S_n$ be permutation (1 2), this is an odd permutation so

$S_n = A_n \cup A_n g$, thus

$$\begin{aligned} \det' A &= \sum_{f \in A_n} \text{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)} + \sum_{f \in A_n g} \text{sgn}(fg) a_{1fg(1)} a_{2fg(2)} \dots a_{nfg(n)} \\ &= \sum_{f \in A_n} \text{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)} - \sum_{f \in A_n} \text{sgn}(f) a_{1f(2)} a_{2f(1)} \dots a_{nf(n)} = 0. \end{aligned}$$

Since $g(1) = 2, g(2) = 1, g(3) = 3, \dots$

- ① (1) (Abelian) group: closure, (commutativity), associativity, inverse, identity
- (2) field: $(\mathbb{F}, +)$, $(\mathbb{F} \setminus \{0\}, \times)$ are Abelian groups, distributivity
- (3) vector space: $(V, +)$ is Abelian group, scalar multiplication: identity, associativity, distributivity
- (4) subfield: $0, 1 \in \mathbb{F}^*$, $\forall \vec{v}, \vec{u} \in \mathbb{F}^*$, $\vec{v}^{-1}$, $-\vec{v}$, $\vec{v} + \vec{u}$, $\vec{v}\vec{u} \in \mathbb{F}$
- (5) vector subspace: $0 \in V$, $\forall \vec{v}, \vec{u} \in V$, $\lambda \vec{v}$, $\vec{v} + \vec{w} \in V$ [证明要分开!]
- (6) linear map: $T(\lambda \vec{u} + \mu \vec{v}) = \lambda T(\vec{u}) + \mu T(\vec{v})$
- (7) bilinear map: $f(\lambda \vec{v}_1 + \mu \vec{v}_2, \vec{w}) = \lambda f(\vec{v}_1, \vec{w}) + \mu f(\vec{v}_2, \vec{w})$
 $f(\vec{v}, \lambda \vec{u}_1 + \mu \vec{u}_2) = \lambda f(\vec{v}, \vec{u}_1) + \mu f(\vec{v}, \vec{u}_2)$

② (1) 如何证明 inverse:

• $AB = BA = I$

(2) 如何证明 linear independent

• 老实找定义

• 行列式

• $B \subseteq V$ is spanning and $|B| = \dim V$

(3) 如何证明 spanning

• 老实找定义 (写出组合通式)

• $B \subseteq V$ is linearly independent and $|B| = \dim V$

(4) 3个关于 linearly independent 与 spanning 的基本操作

• linear independent sets extend

• spanning sets shrink

• element in set replacement

- $\{0\}$ is linearly dependent
- $\emptyset$ is linearly independent
- $\text{span}(\emptyset) = \{0\}$

注意 $|V| \neq \dim V$

$\text{rk } A = \dim(\text{im } A)$

if $X \subseteq V$ is linearly independent and $Y \subseteq V$ is spanning, $|X| \leq |Y|$, then $|X| \leq |Y|$

all finite-dimensional vector spaces have basis

$U \subseteq V$, U, V finite-dimensional vector spaces so $\dim U \leq \dim V$

$\dim(U+V) = \dim U + \dim V - \dim(U \cap V)$

③ (1) $A = MB$, A and B :

• same row space

• same nullspace

• same dimensional column space/left null space

(2) 如何找 row space basis: rref 形式直接写

(3) 如何找 column space basis: 对照 rref 形式的位置

④ linear algebra of linear map: ${}_B[T]_A = ([T(\vec{v}_1)]_B, [T(\vec{v}_2)]_B, \dots, [T(\vec{v}_n)]_B)$, $A = \{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$

• for $T: V \rightarrow W$, $\ker T = 0$ if T injective, $\text{im } T = W$ if T surjective

• for $T: V \rightarrow W$, $\text{rk } T = \dim(\text{im } T) = \dim(\{A\vec{v} \mid \vec{v} \in V\}) = \dim(\text{span}\{A\vec{e}_1, A\vec{e}_2, \dots\}) = \dim(\text{im } A)$

• isomorphism $\Rightarrow$ same dimensions

• for $T: V \rightarrow W$: (1) T is bijective

(2) T is injective and $\dim V = \dim W$

(3) T is surjective and $\dim V = \dim W$

$\left. \begin{matrix} (1) T \text{ is bijective} \\ (2) T \text{ is injective and } \dim V = \dim W \\ (3) T \text{ is surjective and } \dim V = \dim W \end{matrix} \right\} \text{任一成立} \Rightarrow \dim V = \text{rk } T + \dim \ker T$

• for $T: V \rightarrow W$: (1) $(T \text{ injective}) \Leftrightarrow (\exists S: W \rightarrow V, S \cdot T = I_V)$

(2) $(T \text{ surjective}) \Leftrightarrow (\exists S: W \rightarrow V, T \cdot S = I_W)$

⑤ double dual space

• dual transformation: for $T: V \rightarrow W$, $T^*: W^* \rightarrow V^*$, $T^*(f) = f \circ T$

for $S: U \rightarrow V$, $T: V \rightarrow W$, $(T \circ S)^* = S^* \circ T^*$

for $T: V \rightarrow W$ invertible, $(T^{-1})^* = (T^*)^{-1}$

for $U: V \rightarrow V^*$, $\vec{v} \mapsto \vec{v}^*$

$f = f(\vec{v}_1)\vec{v}_1^* + f(\vec{v}_2)\vec{v}_2^* + \dots + f(\vec{v}_n)\vec{v}_n^*$, $\vec{v} = (\vec{v}_1^* \cdot \vec{v})\vec{v}_1 + (\vec{v}_2^* \cdot \vec{v})\vec{v}_2 + \dots + (\vec{v}_n^* \cdot \vec{v})\vec{v}_n$

- basis of V $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$.
 basis of V^* $\{\vec{v}_1^*, \vec{v}_2^*, \dots, \vec{v}_n^*\}$ ← the same
 basis of V^{**} $\{\vec{v}_1^{**}, \vec{v}_2^{**}, \dots, \vec{v}_n^{**}\}$ ←
- given $W \subseteq V$, we have $W^\perp \subseteq V^*$, $\dim V = \dim W + \dim W^\perp$.
- $B^V[T^*]_{C^V} = {}^c[T]_B^T$

$x \rightarrow v$

$$\begin{aligned} (W-w) &= p\left(\frac{1}{1+x} = w\right) \\ &= p\left(1+x = \frac{1}{w}\right) \\ &= p\left(x = \frac{1}{w} - 1\right) \end{aligned}$$

$$\int_{\frac{1}{w}-1}^1 \frac{1}{x^2} dx$$

$$1 - \frac{1}{1-x} + \frac{2}{1-x} - 1$$

$$\int_0^{\frac{1}{w}} \frac{1}{x^2} dx$$

$$\frac{1}{w^2} - \frac{2}{w}$$

① determinant

• 范德蒙矩阵 $M = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}$, $\det M = \prod_{1 \leq i < j \leq n} (x_j - x_i)$

• adjoint of A : $\text{adj} A = C^T$, $(\text{adj} A) \cdot A = \det A \cdot I$

② diagonalisable

• eigenvector: $\vec{v} \in V \setminus \{\vec{0}\}$, such that $T(\vec{v}) = \lambda \vec{v}$

• diagonalisable if and only if:

- $\exists$ a basis B of eigenvectors over V

- for all eigenvalue: geometric multiplicity = algebraic multiplicity

• T and ${}_B[T]_B$ have same eigenvalues

• character polynomial: $\chi_A(x) = \det(xI - A)$

If eigenvalue recurrence enclosed form

③ orthogonal matrix

• for basis $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n\}$, derive orthonormal basis $\{\frac{\vec{u}_1}{\|\vec{u}_1\|}, \frac{\vec{u}_2}{\|\vec{u}_2\|}, \dots, \frac{\vec{u}_n}{\|\vec{u}_n\|}\}$ such that

$$\vec{u}_1 = \vec{v}_1$$

$$\vec{u}_2 = \vec{v}_2 - \frac{\vec{v}_2 \cdot \vec{u}_1}{\|\vec{u}_1\|^2} \vec{u}_1$$

$$\vec{u}_n = \vec{v}_n - \sum_{i=1}^{n-1} \frac{\vec{v}_n \cdot \vec{u}_i}{\|\vec{u}_i\|^2} \vec{u}_i$$

• $|\vec{u} \cdot \vec{v}| \leq \|\vec{u}\| \|\vec{v}\|$, $\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$

④ group

• 已知 G 是 group, 证明 $H \leq G$ 为 subgroup ($H \leq G$):

- $H \neq \emptyset$, $\forall h_1, h_2 \in H, h_1 h_2 \in H, h_1^{-1} \in H$

- 如果 G 为 finite group: $H \neq \emptyset, \forall h_1, h_2 \in H, h_1 h_2 \in H$

• G is a finite group and $g \in G$, then $\langle g \rangle \mid |G|$

- $H \leq G, |H| \mid |G|$

- $g \in G, \langle g \rangle$ is a group, $|\langle g \rangle| \mid |G|$

• 证明 groups 相同: $H = G$: $H \leq G$ and $|H| = |G|$

- $H \leq G, |H| = |G|$

- $\forall h \in H, h \in G; \forall g \in G, g \in H$

• cyclic group:

- assume $G = \langle g \rangle$, then: $H \leq G$ is cyclic

□ if $\phi(g) = n$ and $m \in \mathbb{Z}$, $d = \gcd(m, n)$, $\langle g^m \rangle = \langle g^d \rangle$

$|\langle g^d \rangle| = \frac{n}{d}$, $\langle g^m \rangle = G$ if and only if $d = 1$

- Euler Totient function: $\sum_{1 \leq d \leq n, d \mid n} \phi(d) = n$

[对于 cyclic group, $G_d = \langle g^{\frac{n}{d}} \rangle$ 中 order is d 的元素有 $\phi(d)$ 个]

- assume G is group and $S \subseteq G$, then $\langle S \rangle$ is the smallest subgroup containing

S . $\langle S \rangle = \{g_1 g_2 \dots g_k \mid k \in \mathbb{N} \text{ and } g_1, g_2, \dots, g_k \in S \cup S^{-1}\}$

4. homomorphism & isomorphism

- homomorphism: for groups G, H , $\phi: G \rightarrow H$, $g, g' \in G$, $\phi(gg') = \phi(g)\phi(g')$
- isomorphism: $\phi: G \rightarrow H$ is bijective, $\phi(f_1 f_2) = \phi(f_1)\phi(f_2)$
- for homomorphism $\phi: G \rightarrow H$: $\phi(e_G) = e_H$, $\phi(g^{-1}) = (\phi(g))^{-1} \forall g \in G$
 ϕ is injective if $\ker \phi = \{e_G\}$
- for isomorphism: cyclic groups of same order are isomorphic
 V_1, V_2 are non-cyclic and $|V_1| = |V_2| = 4$, $V_1 \cong V_2$

• permutation: S_n

- $\text{sym}(X) = \{\text{all permutations of } X\}$
- $\text{supp}(f) = \{x \in [n] \mid f(x) \neq x\}$; for f, g with disjoint supports, $fg = gf$
- if $f \in S_n$, $\exists$ cycles $f_1, f_2, \dots, f_k \in S_n$ with disjoint supports such that $f = f_1 f_2 \dots f_k$
 $\sigma(f) = \text{lcm}(\sigma(f_1), \sigma(f_2), \dots, \sigma(f_k))$
- each permutation can be produced as a product of transpositions (2-cycles)
- D_{2n} group of symmetries of regular n -gon, $|D_{2n}| = 2n$ and $D_{2n} = \langle \alpha, \beta \rangle$,
 $\alpha = (1)(2 \ n)(3 \ n-1) \dots$, $\beta = (1 \ n)(2 \ n-1)(3 \ n-2) \dots$
- if f is r -cycle, $\text{sgn}(f) = (-1)^{r-1}$, $\text{sgn}(f)$ is unique.
 $\text{sgn}(fg) = \text{sgn}(f)\text{sgn}(g)$
- f is even if $\text{sgn}(f) = 1$; f is odd if $\text{sgn}(f) = -1$
 alternative group A_n the set of all even permutation, if $n \geq 2$, $[S_n, A_n] = A_n$
- $\det A = \sum_{f \in S_n} \text{sgn}(f) a_{1f(1)} a_{2f(2)} \dots a_{nf(n)}$