

回忆 定理: 设 $A \in \mathbb{R}^{m \times n}$, $A \neq 0$

则以下断言等价

(i) $\text{rank}(A) = r$

(ii) A 中有一个 r 阶子式非零, 且所有大于 r 阶的子式都等于零

(iii) A 中有一个 r 阶子式非零, 且所有 $r+1$ 阶子式都等于零

证:

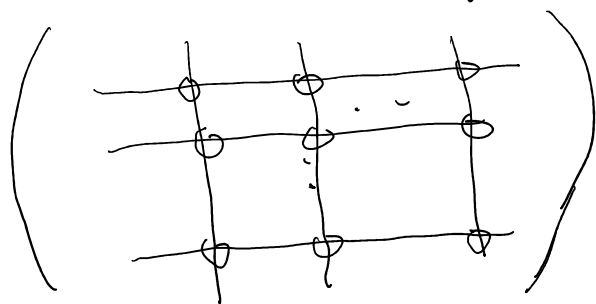
(i) $\Rightarrow$ (ii)

设 $\vec{A}_{i_1}, \dots, \vec{A}_{i_r}$ 线性无关

$\vec{A}^{(j_1)}, \dots, \vec{A}^{(j_r)}$ 线性无关

我们证明

$$M \begin{pmatrix} i_1 & \dots & i_r \\ j_1 & \dots & j_r \end{pmatrix} \neq 0$$



不妨设 $\vec{A}_1, \dots, \vec{A}_r$ 线性无关

$\vec{A}^{(1)}, \dots, \vec{A}^{(r)}$ 线性无关

且 $\dots$ 由其性质

$$\left(\begin{array}{ccc|ccc} \hline & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ \hline \end{array} \right) \} \text{由期中考试第10题可知}$$

$$M \begin{pmatrix} 1 & 2 & \cdots & r \\ & 1 & 2 & \cdots & r \end{pmatrix} \neq 0$$

$$\Rightarrow M \begin{pmatrix} i_1 & i_2 & \cdots & i_r \\ j_1 & j_2 & \cdots & j_r \end{pmatrix} \neq 0$$

设 $s > r$

$$M \begin{pmatrix} i_1 & i_2 & \cdots & i_s \\ j_1 & j_2 & \cdots & j_s \end{pmatrix} \neq 0$$

我们证明: $\vec{A}_{i_1}, \dots, \vec{A}_{i_s}$ 线性无关

$$\left(\begin{array}{ccc|ccc} \hline & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ \hline \end{array} \right) \begin{matrix} i_1 \\ i_2 \\ \vdots \\ i_s \end{matrix}$$



线性无关 但

是这些行延伸

$\therefore \vec{A}_{i_1}, \dots, \vec{A}_{i_s}$ 线性无关

$$\Rightarrow \text{rank}(A) \geq s > r \rightarrow \leftarrow$$

(ii) $\Rightarrow$ (iii) 证毕

(iii) $\Rightarrow$ (i)

设 A 中有一个 r 阶子式非零
且所有 $r+1$ 阶子式都等于零

要证 $\text{rank}(A) = r$

由 A 中有一个 r 阶子式非零可知

$$\text{rank}(A) \geq r$$

假定 $\text{rank}(A) = s$ 且 $s > r$

则 A 中有 $\vec{A}_{i_1}, \dots, \vec{A}_{i_r}, \vec{A}_{i_{r+1}}$ 线性无关

$$\text{设 } B = \begin{pmatrix} \vec{A}_{i_1} \\ \vec{A}_{i_2} \\ \vdots \\ \vec{A}_{i_{r+1}} \end{pmatrix}$$

$$\text{则 } \text{rank}(B) = r+1$$

于是 B 中有 $r+1$ 列线性无关

不妨设 $\vec{B}^{(j_1)}, \dots, \vec{B}^{(j_{r+1})}$ 线性无关

$$\text{令 } C = (\vec{B}^{(j_1)} \dots \vec{B}^{(j_{r+1})})_{r \times r}$$

$$\text{rank}(C) = r+1 \text{ 矛盾, } \det(C) \neq 0$$

$$\det(C) = M_A \begin{pmatrix} i_1, i_2, \dots, i_{r+1} \\ j_1, j_2, \dots, j_{r+1} \end{pmatrix} \neq 0 \rightarrow \leftarrow$$

$$A = \begin{pmatrix} \text{---} \\ \text{---} \\ \vdots \\ \text{---} \end{pmatrix} \begin{matrix} i_1 \\ i_2 \\ \vdots \\ i_{r+1} \end{matrix}$$

$$B = \left(\begin{array}{ccc|ccc} \circ & \circ & \cdots & \circ & \circ & \circ \\ \circ & \circ & \cdots & \circ & \circ & \circ \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \circ & \circ & \cdots & \circ & \circ & \circ \end{array} \right) \left. \vphantom{\begin{pmatrix} \circ & \circ & \cdots & \circ & \circ & \circ \end{pmatrix}} \right\} r+1$$

$j_1 \ j_2 \ \dots \ j_{r+1}$

$$C = \begin{pmatrix} \circ & \circ & \cdots & \circ \\ \circ & \circ & \cdots & \circ \\ \vdots & \vdots & \ddots & \vdots \\ \circ & \circ & \cdots & \circ \end{pmatrix}_{(r+1) \times (r+1)} \quad \text{且 } \det(C) \neq 0$$

矛盾.



定理说明. 我们只通过 n 个
和单法计算矩阵的秩

加也子式法.

例: Cramer's rule

设 $A \in M_n(\mathbb{R})$ 可逆, $\vec{b} \in \mathbb{R}^n$

$$A \vec{x} = \vec{b}$$

$$A \vec{x} = \vec{b}$$

$$\vec{x} = A^{-1} \vec{b}$$

$$x_i = \frac{\det(\vec{A}^{(1)} \dots \vec{A}^{(i-1)}, \vec{b}, \vec{A}^{(i+1)} \dots \vec{A}^{(n)})}{\det(A)}$$

$i=1, 2, \dots, n$

设 $A \in \mathbb{R}^{(n-1) \times n}$ $\square$ rank(A)=n-1

$$\dim(\text{sol}(A\vec{x}=\vec{0})) + n-1 = n$$

$$\Rightarrow \underline{\dim(\text{sol}(A\vec{x}=\vec{0})) = 1}$$

设 $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \neq \vec{0}$ 满足 $A\vec{x}=\vec{0}$ 则

则 $A\vec{x}=\vec{0}$ 的所有解是

$$\textcircled{a} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \lambda \in \mathbb{R}$$

$\textcircled{a}$ - (unique up to a multiplicative constant)

an additive constant

证法

$$\begin{pmatrix} |A_1| \\ -|A_2| \\ \vdots \end{pmatrix}$$

$\forall \vec{x} \neq \vec{0}$ 满足 $A\vec{x}=\vec{0}$ 则

$$\begin{pmatrix} -|A_1| \\ \vdots \\ (-1)^{n-1}|A_n| \end{pmatrix} \sim \begin{matrix} A \\ \text{非平凡解} \end{matrix}$$

其中 $A_j = (\vec{A}^{(1)}, \dots, \vec{A}^{(j-1)}, \vec{A}^{(j+1)}, \dots, \vec{A}^{(n)})$

证: 设 $M_i = \begin{pmatrix} A \\ \vec{A}_i \end{pmatrix}$

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \dots & a_{n-1,n} \\ \boxed{a_{i1}} & a_{i2} & \dots & \boxed{a_{in}} \end{pmatrix}_{n \times n}$$

$$i=1, 2, \dots, n-1$$

则 M_i 中第 i 行和第 n 行相同

故 $\det(M_i) = 0$

把 $\det(M_i)$ 按最后一行展开

$$a_{i1}(-1)^{n+1}|A_1| + a_{i2}(-1)^{n+2}|A_2| + \dots + a_{in}(-1)^{n+n}|A_n| = \det(M_i) = 0$$

$$\Rightarrow a_{i1}|A_1| + a_{i2}(-|A_2|) + \dots + a_{in}((-1)^{n-1}|A_n|) = 0$$

$$i=1, 2, \dots, n-1$$

$$\Rightarrow \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \dots & a_{n-1,n} \\ |A_1| & -|A_2| & \dots & (-1)^{n-1}|A_n| \end{pmatrix} \begin{pmatrix} |A_1| \\ -|A_2| \\ \vdots \\ (-1)^{n-1}|A_n| \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

(1) (1) (1)

故 $\vec{u} = \begin{pmatrix} |A_1| \\ -|A_2| \\ \vdots \\ (-1)^{n-1} |A_n| \end{pmatrix}$ 是 $A\vec{x} = \vec{0}$ 的解

$\therefore \text{rank}(A) = n-1$
 $\therefore A$ 中有一行 $n-1$ 阶子式非零
 而 $|A_1|, |A_2|, \dots, |A_n|$ 是 A 中
 所有 $n-1$ 阶子式, 故 $\vec{u} \neq \vec{0}$. $\square$

例: 设 $A \in \mathbb{R}^{m \times n}$, $B \in \mathbb{R}^{n \times m}$
 证: $\det(E_m + AB) = \det(E_n + BA)$
 [Sylvester 行列式恒等式]

证: 由 Sylvester 秩等式可知
 可取: 存在 $C_1, C_2, C_3, C_4 \in M_{m+n}(\mathbb{R})$

使得

$$\begin{pmatrix} E_m + AB & O \\ O & E_n \end{pmatrix} \begin{pmatrix} C_2 & C_4 \\ C_3 & C_1 \end{pmatrix} \\
= \begin{pmatrix} E_n & O \\ O & E_m + BA \end{pmatrix} \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}$$

$\therefore \det(C_1) = \det(C_2) = \det(C_3) = \det(C_4)$

$$C = \begin{pmatrix} E_m & * \\ * & E_n \end{pmatrix}$$

$$C_i = \begin{pmatrix} E_m & * \\ 0 & E_n \end{pmatrix}$$

由行列式乘法定理

$$\det \begin{pmatrix} E_m + AB & 0 \\ 0 & E_n \end{pmatrix}$$

$$= \det \begin{pmatrix} E_m & 0 \\ 0 & E_n + BA \end{pmatrix}$$

$$\Rightarrow \boxed{\det(\lambda E_m + AB) = \det(\lambda E_n + BA)}$$

{ ① 分块矩阵

{ ② 卷积定理 kernel image

摄动

第四章, 群、环和域简介

(抽象代数)

$\mathbb{R}^{m \times n}$

$\mathbb{R}^n$

$\mathbb{Q}^{m \times n}$

$\mathbb{Q}^n$ ✓

$\mathbb{C}^{m \times n}$

$\mathbb{C}^n$ ✓

在域上其子部是域的

在 $(\mathbb{Z})$ 上是平部空吗

↓

取

↓

解

§1 二元运算

§1.1 定义与基本性质

设 S 是集合, $f: S \times S \rightarrow S$
 $(x, y) \mapsto f(x, y)$

称 f 为 S 上的二元运算
 把结果 $f(x, y)$ 记为 $x \circ y$.

例: $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$
 $x, y \mapsto +(x, y)$
 $= x + y$

"+" 满足 交换律
 结合律
 加单位元 0
 加逆元 x 的加逆元 $(-x)$

例: $-$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$
 $x, y \mapsto -(x, y) = x - y$

例: 设 $S = \mathbb{Z} \cup \{-\infty\}$

$$+ : S \times S \rightarrow S$$
$$(x, y) \mapsto \max(x, y)$$

称 $+$ 为 "热带" 加法

$+$ 有交换律, 结合律

$$x + (-\infty) = \max(x, -\infty) = x$$

$\hookrightarrow$ " $+$ " 单位.

x 关于 $+$ 不一定有逆元

设 A, B 是列数相同的矩阵

$$A, B \mapsto \begin{pmatrix} A \\ B \end{pmatrix}$$

$$A \text{ vert cat } B = \begin{pmatrix} A \\ B \end{pmatrix}$$

$$\text{vert cat}(A, B) = \begin{pmatrix} A \\ B \end{pmatrix}$$

定义: 设 $*$ 是 S 上二元运算.

$$\text{如} \forall x, y, z \in S$$

$$x * (y * z) = (x * y) * z$$

则称 $*$ 满足结合律

则称 $*$ 满足结合律

满足结合律

定理 1.6 设 $*$ 是 S 的 n -元运算

$n \geq 3$, $x_1, \dots, x_n \in S$

设 $k, l \in \{1, 2, \dots, n-1\}$

$$\begin{aligned} & (x_1 * \dots * x_k) * (x_{k+1} * \dots * x_n) \\ &= (x_1 * \dots * x_l) * (x_{l+1} * \dots * x_n) \end{aligned}$$

证: 不妨设 $k > l$. 对 n 用归纳法

$n=3$, $k=2$, $l=1$

$$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$$

(结合律)

设 $n > 3$ 且假设对于 n 的值成立 考虑 n 的情况

$$\begin{aligned} & (x_1 * \dots * x_k) * (x_{k+1} * \dots * x_n) \\ &= \underbrace{(x_1 * \dots * x_l) * (x_{l+1} * \dots * x_k)}_{\text{归纳假设}} * (x_{k+1} * \dots * x_n) \\ &= (x_1 * \dots * x_l) * ((x_{l+1} * \dots * x_k) * (x_{k+1} * \dots * x_n)) \\ &= (x_1 * \dots * x_l) * \underbrace{(x_{l+1} * \dots * x_k * x_{k+1} * \dots * x_n)}_{\text{归纳假设}} \end{aligned}$$

(结合律)

定义 设 $x \in S, n \in \mathbb{Z}^+$,
 S 上 = 元运算 * 满足结合律

$$\text{则 } x^n = \underbrace{x * \dots * x}_n$$

若 S 中 = 元运算为 “+”

$$x + \dots + x = \underbrace{\quad}_n x$$

1.2 同余运算

设 n 是大于 1 的正整数

$$\forall x, y \in \mathbb{Z} \quad x \equiv_n y \Leftrightarrow n \mid (x - y)$$

$$\Leftrightarrow \exists k \in \mathbb{Z} \quad x = y + kn$$

$$\mathbb{Z}/\equiv_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

记为 $\mathbb{Z}_n$.

$$\text{card}(\mathbb{Z}_n) = n.$$

$$\text{定义: } +: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$(\bar{x}, \bar{y}) \mapsto \overline{x+y}$$

验证良定义:

设 $x', y' \in \mathbb{Z}$ 使得

$$\bar{x} = \bar{x}', \quad \bar{y} = \bar{y}'$$

$$\overline{x} = \overline{x'}, \quad \overline{y} = \overline{y'}$$

要证明: $\overline{x+y} = \overline{x'+y'}$

$$\because \overline{x} = \overline{x'} \quad \therefore x \equiv_n x'$$

$$\text{即 } \exists k \in \mathbb{Z}, \quad x = x' + kn$$

同理 $\exists l \in \mathbb{Z}$ 使得

$$y = y' + ln$$

$$x+y = (x'+y') + (k+l)n$$

$$\Rightarrow x+y \equiv_n x'+y'$$

$$\Rightarrow \overline{x+y} = \overline{x'+y'}$$

"+" 在 $\mathbb{Z}_n$ 上是良定义的 ✓

交换律 $\overline{x} + \overline{y} = \overline{x+y}$

$$\overline{y} + \overline{x} = \overline{y+x} = \overline{x+y}$$

结合律 满足

$$\overline{x} + \overline{0} = \overline{x+0} = \overline{x}$$

↪ 叫零元

$$\overline{x} + \overline{-x} = \overline{x+(-x)} = \overline{0}$$

↪ 叫逆元

例: $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

$$\overline{1+1} = \overline{1+1} = \overline{2} = \underline{0}$$

定义: $\cdot: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$
 $\overline{x}, \overline{y} \mapsto \overline{xy}$

验证良定义: 见讲义

例: $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

$$\overline{2} \cdot \overline{4} = \overline{2 \times 4} = \overline{8} = \overline{2}$$

$$\overline{2} \cdot \overline{3} = \overline{2 \times 3} = \overline{6} = \overline{0}$$

$$\overline{2} \cdot \overline{1} = \overline{2} \quad \checkmark$$

§1.3. 单位元和逆元

定义: 设 $*$ 是 S 上的二元运算
 如果 $\exists e \in S$ 满足: $\forall x \in S$
 $x * e = e * x = x$

则称 e 是关于 $*$ 的单位元

命题: 设 $*$ 是 S 上的二元运算
 $e, e' \in S$ 关于 $*$ 的单位元

$$\text{则 } e = e'$$

$$\text{证: } e * e' = e \Rightarrow e = e'$$

$$e * e' = e'$$

$$\text{vertcat}(A, B) = \begin{pmatrix} A \\ B \end{pmatrix}$$

$$\text{vertcat}(\square, B) = B$$

↪ 单位元

$$A := A_1 \quad \bigcirc$$

for i from 2 to 10 do

$$A := \text{vertcat}(A, A_i) \quad \bigcirc$$

end do

定义: 设 $*$ 是 S 上二元运算, 称

$x \in S$

如果 $\exists y \in S$ 使得

$$y * x = e, \text{ 则称 } x \text{ 有左逆}$$

如果 $\exists z \in S$ 使得

$$x * z = e, \text{ 则称 } x \text{ 有右逆}$$

如果 $\exists a \in S$ 使得

... ~

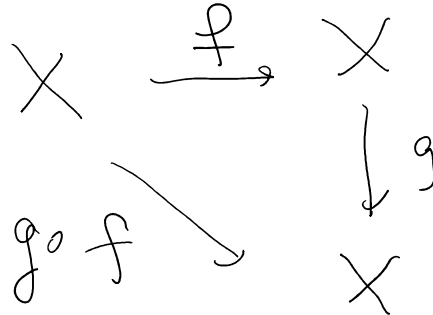
$$a * x = x * a = e$$

则称 x 是 S 中的可逆元且 a 称为 x 的逆.

例: 设 X 是非空集

$$S = \{ f: X \rightarrow X \}$$

$*$ 是 $\circ$



单射有左逆

满射有右逆

双射有逆

命题: 设 $*$ 是 S 上的二元运算
满足结合律有单位元 e , $x \in S$

如果 x 有左逆且有右逆

则 x 可逆.

证: 设 $a, b \in S$ 满足

$$a * x = e, x * b = e$$

我们只要证明 $a = b$ 即可

$$(a * x) * b = e * b$$

$$\Downarrow$$

$$a * (x * b) = b$$

$$a \times (x \times b) = b$$

$$a \times e \stackrel{\Downarrow}{=} b$$

$$\underline{a} = \underline{b}$$

□

注: 如果 $x \in S$ 可逆, 则逆是唯一的

命题: 设 $\bar{a} \in \mathbb{Z}_n$ 则

$\bar{a}$ 关于乘法可逆

$$\Leftrightarrow \gcd(a, n) = 1$$

证: $\Rightarrow$ 设 $\bar{b} \in \mathbb{Z}$ 满足

$$\bar{a} \bar{b} = \bar{1}$$

$$\text{则 } ab \equiv_n 1$$

$$\Rightarrow \exists k \in \mathbb{Z} \quad ab = 1 + kn$$

$$b \underline{a} + \underline{(kn)} = \underline{1}$$

$$\text{于是 } \gcd(a, n) = 1$$

$$\Leftarrow \text{ 设 } \gcd(a, n) = 1$$

由 Bezout 关系可知 $\exists u, v \in \mathbb{Z}$

$$ua + vn = 1$$

$$\Rightarrow \overline{ua + vn} = \bar{1}$$

$$\Rightarrow \underline{ua} + \underline{vn} = \underline{1} \quad \underline{vn} = \underline{0}$$

$$\Rightarrow \overline{ua} + \underbrace{\overline{0}} = \overline{1}$$

$$\Rightarrow \overline{ua} = \overline{1}$$

$$\Rightarrow \overline{ua} = \overline{1} \Rightarrow \overline{a} \stackrel{u}{=} \overline{a}$$

的逆 $\square$

例: 计算 $\mathbb{Z}_{15}$ 是关于加法的所有可逆元

$$\mathbb{Z}_{15} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{14}\}$$

可逆: $\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}$

逆元可由扩展 Euclid 算法