1

回忆：定理3.3 设 $A\in\mathbb{R}^{m\times n}$，则下列 ~~定理~~ 断言等价

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

(ii) $\forall k>r$，A的k阶子式都是零，且存在A的r阶子式非零

(iii) A的任意 $r+1$ 阶子式都为零，且存在A的r阶子式非零.

注：A的零阶子式定义为1

推论3.1 设 $A\in\mathbb{R}^{m\times n}$，则 $\operatorname{rank}(A)$ 等于A中非零子式的最大阶数.

定理3.4 设 $A\in\mathbb{R}^{m\times n}$，

$M_A\begin{pmatrix} i_1, \cdots & i_r \\ j_1, \cdots & j_r\end{pmatrix}\neq 0$

$\Longleftrightarrow$ $\vec{A}_{i_1}^{(行)},\ldots,\vec{A}_{i_r}^{(行)}$ 线性无关且 $\vec{A}^{(j_1)}\cdots\vec{A}^{(j_r)}$ 线性无关

证：$\Rightarrow$ 引理3.4

$\Leftarrow$ 设 $B=(\vec{A}^{(j_1)},\ldots,\vec{A}^{(j_r)})_{r\times n}$

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

$\therefore$ $\operatorname{rank}(B)=r$.

设 $k\in\{1,2,\ldots,m\}$

则 $\vec{A}_k$ 是 $\vec{A}_{i_1}^{(行)}\cdots\vec{A}_{i_r}^{(行)}$ 的线性组合

（$\because$ $\operatorname{rank}(A)=r$ 且 $\vec{A}_{i_1}^{(行)}\cdots\vec{A}_{i_r}^{(行)}$ 线性无关）

于是 $\vec{B}_k$ 是 $\vec{B}_{i_1}^{(行)}\cdots\vec{B}_{i_r}^{(行)}$ 的线性组合

由此可知

$$V_r(B)=\langle\vec{B}_{i_1}^{(行)},\ldots,\vec{B}_{i_r}^{(行)}\rangle$$

$\because$ $\dim V_r(B)=r$

$\therefore$ $\vec{B}^{(i_1)},\ldots\vec{B}^{(i_r)}$ 线性无关

于是 r阶行列式 $\det\begin{pmatrix}\vec{B}_{i_1}^{(行)}\\ \vdots \\ \vec{B}_{i_r}^{(行)}\end{pmatrix}\neq 0$

即 $M_A\begin{pmatrix} i_1,\ldots,i_r \\ j_1,\ldots,j_r\end{pmatrix}\neq 0$ ▨

例：$A=\begin{pmatrix}0&1&2\\3&4&5\\3&5&7\end{pmatrix}$

$\operatorname{rank}(A)=2$ $\quad(\because \vec{A}_3=\vec{A}_1+\vec{A}_2)$

$M_A\begin{pmatrix}1,2\\1,2\end{pmatrix}=\begin{vmatrix}0&1\\3&4\end{vmatrix}\neq 0$

问题：给定 $A\in\mathbb{R}^{m\times n}$，计算 $\operatorname{rank}(A)$ 和一个最大阶的非零子式

定义：设 $U=M_A\begin{pmatrix}i_1,\cdots i_k\\j_1,\cdots j_k\end{pmatrix}$ 是 A 的 k 阶子式，$s\in\{1,2,\cdots m\}$，$t\in\{1,2,\cdots,n\}$

则 $M_A\begin{pmatrix}i_1,\cdots i_k & s\\j_1,\cdots j_k & t\end{pmatrix}$ 称为 U 的一个加边子式

定理 3.5 设 ~~r=rank(A)~~ $A\in\mathbb{R}^{m\times n}$

则 $\operatorname{rank}(A)=r$

$\Leftrightarrow$ 存在 A 的一个 r 阶子式不为零 且该子式的加边子式都等于零.

证："$\Rightarrow$" 定理3.4

"$\Leftarrow$" 设 $N=M_A\begin{pmatrix}i_1,\cdots i_r\\j_1\cdots j_r\end{pmatrix}\neq 0$

且 $\forall$ ~~s,t 非(E)~~ $s\in\{1,2,\cdots m\}$，$t\in\{1,\cdots n\}$

$N_{st}=M_A\begin{pmatrix}i_1,\cdots i_r & s\\j_1,\cdots j_r, & t\end{pmatrix}=0$

则

$$N_{st}=\begin{vmatrix}a_{i_1,j_1}, & a_{i_1,j_2}, & \cdots & a_{i_1,j_r}, & a_{i_1,t}\\ a_{i_2,j_1}, & a_{i_2,j_2} & \cdots & a_{i_2,j_r}, & a_{i_2,t}\\ & \cdots & & & \\ a_{i_r,j_1}, & a_{i_r,j_2} & \cdots & a_{i_r,j_r}, & a_{i_r,t}\\ a_{s,j_1}, & a_{s,j_2}, & \cdots & a_{s,j_r}, & a_{s,t}\end{vmatrix}_{(r+1)}=0$$

按最后一列展开 N_{st}.

(*) $\alpha_{1s}a_{i_1,t}+\cdots+\alpha_{rs}a_{i_r,t}+Na_{s,t}=0$

其中 $\alpha_{1s},\cdots\alpha_{rs}$ 与 t 无关，N 与 $s.t$ 都无关

于是 (*) 对 $\forall t\in\{1,2,\cdots n\}$ 都成立

由此可知

$\alpha_{1s}(a_{i_1,1}, \cdots a_{i_1 n}) + \cdots +$

$\alpha_{rs}(a_{i_r,1}, \cdots a_{i_r,n}) + N(a_{s,1}, \cdots a_{s,n}) = 0$

即 $\alpha_{1s}\vec{A}_{i_1} + \cdots + \alpha_{rs}\vec{A}_{i_r} + N\vec{A}_s = 0$

$\because N \neq 0 \quad \therefore \vec{A}_s = \left(-\frac{\alpha_{1s}}{N}\right)\vec{A}_{i_1} + \cdots + \left(-\frac{\alpha_{rs}}{N}\right)\vec{A}_{i_r}$

即 $\vec{A}_s \in \langle \vec{A}_{i_1}, \cdots \vec{A}_{i_r} \rangle, \quad s = 1, 2, \cdots m$

于是 $V_r(A) = \langle \vec{A}_{i_1}, \cdots, \vec{A}_{i_r} \rangle$

$\cancel{\because N \neq 0} \Rightarrow \text{rank}(A) \leq r$

$\because N \neq 0 \quad \therefore \text{rank}(A) \geq r$

于是 $\text{rank}(A) = r$ ▨

例：计算

$$A = \begin{pmatrix} 2 & -1 & 3 & -2 & 4 \\ 4 & -2 & 5 & 1 & 7 \\ 2 & -1 & 1 & 8 & 2 \end{pmatrix}$$

计算 rank(A) 和给出一个 A 中~~最~~高阶的非零子式

解：$M_A\begin{pmatrix}1\\1\end{pmatrix} = 2 \neq 0$

加边 $M_A\begin{pmatrix}1 & \boxed{2}\\1 & \boxed{2}\end{pmatrix} = \begin{vmatrix} 2 & -1 \\ 4 & -2 \end{vmatrix} = 0$

$M_A\begin{pmatrix}1 & \boxed{2}\\1 & \boxed{3}\end{pmatrix} = \begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} \neq 0$

加边 $M_A\begin{pmatrix}1 & 2 & \boxed{3}\\1 & 3 & \boxed{2}\end{pmatrix} = \begin{vmatrix} 2 & 3 & -1 \\ 4 & 5 & -2 \\ 2 & 1 & -1 \end{vmatrix} = 0$

$M_A\begin{pmatrix}1 & 2 & \boxed{3}\\1 & 3 & \boxed{4}\end{pmatrix} = \begin{vmatrix} 2 & 3 & -2 \\ 4 & 5 & 1 \\ 2 & 1 & 8 \end{vmatrix} = 2\begin{vmatrix} 1 & 3 & -2 \\ 2 & 5 & 1 \\ 1 & 1 & 8 \end{vmatrix}$

$= 2\begin{vmatrix} 1 & 3 & -2 \\ 0 & -1 & 5 \\ 0 & -2 & 10 \end{vmatrix} = 0$

$M_A = \begin{pmatrix}1 & 2 & 3\\1 & 3 & 5\end{pmatrix} = \begin{vmatrix} 2 & 3 & 4 \\ 4 & 5 & 7 \\ 2 & 1 & 2 \end{vmatrix} = 2\begin{vmatrix} 1 & 3 & 4 \\ 2 & 5 & 7 \\ 1 & 1 & 2 \end{vmatrix}$

$= 2\begin{vmatrix} 1 & 3 & 4 \\ 0 & -1 & -1 \\ 0 & -2 & -2 \end{vmatrix} = 0$

$\Rightarrow M\begin{pmatrix}1 & 2\\1 & 3\end{pmatrix}$ 是最高阶非零子式．$\text{rank}(A) = 2$

§4 方阵对应的线性方程组

设 $A \in M_n$, $\vec{b} \in \mathbb{R}^n$, $\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

(L) $A\vec{x} = \vec{b}$ (H) $A\vec{x} = \vec{0}_n$

i) (L) 有解 $\Longleftrightarrow$ $\mathrm{rank}(A) = \mathrm{rank}(A \vdots \vec{b})$

ii) (L) 确定 $\Longleftrightarrow$ $\mathrm{rank}(A) = n$ $\Longleftrightarrow$ $\det(A) \neq 0$

iii) (H) 有非零 $\Longleftrightarrow$ $\mathrm{rank}(A) < n$ $\Longleftrightarrow$ $\det(A) = 0$

例：设 $p_i = (p_{i1}, \cdots p_{in}) \in \mathbb{R}^{1\times n}$, $i = 0, 1, \cdots n$

证明：$P_0, P_1, P_2, \cdots P_n$ 在同一超平面上

$$\Longleftrightarrow \det \begin{pmatrix} p_{01}, & p_{02}, & \cdots & p_{0n} & 1 \\ p_{11} & p_{12} & \cdots & p_{1n} & 1 \\ & & \cdots & & \\ p_{n,1} & p_{n2} & \cdots & p_{nn} & 1 \end{pmatrix} = 0$$

证：令 $P = \begin{pmatrix} p_{01} & p_{02} & \cdots & p_{0n} & 1 \\ p_{11} & p_{12} & \cdots & p_{1n} & 1 \\ & & \cdots & & \\ p_{n,1} & p_{n2} & \cdots & p_{nn} & 1 \end{pmatrix}_{(n+1)\times(n+1)}$

"$\Rightarrow$" 设 $P_0, P_1, \cdots P_n$ 在超平面

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b \text{ 上}$$

其中 $a_1, a_2, \cdots a_n, b \in \mathbb{R}$. 不全为零

则 $a_1 p_{i1} + a_2 p_{i2} + \cdots + a_n p_{in} = b$. $i = 0, 1, 2 \cdots n$

即 $a_1 p_{i1} + a_2 p_{i2} + \cdots + a_n p_{in} + (-b) = 0$

即 $P \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \\ -b \end{pmatrix} = 0$

$\Rightarrow \det(P) = 0$

"$\Leftarrow$" 设 $\det(P) = 0$ 则存在非零向量 $\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ 使得

$$P \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0 \quad (*)$$

设超平面 π 的方程是

$$\alpha_0 x_1 + \cdots + \alpha_n x_n + \alpha_{n+1} = 0$$

则由 $(*)$ 每个 P_i 在 π 上，$i = 1, 2 \cdots n+1$

$\boxed{}$

第4章 群、环、域

§1. 二元运算

定义：设 S 非空集合

$f: S \times S \longrightarrow S$ 称为 S 上的一个

二元运算

记号：$\forall x, y \in S$ $f(x,y)$ 记为 $x f y$.

例：$+$：
$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto x + y. \end{aligned}$$

满足交换律和结合律

$-$：
$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto x - y \end{aligned}$$

不满足交换律和结合律.

$\cdot$：
$$\begin{aligned} M_n \times M_n &\longrightarrow M_n \\ A, B &\longmapsto AB \end{aligned}$$

满足结合律但不满足交换律

$\star$：
$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto |x - y| \end{aligned}$$

则 $x \star y = y \star x$

$(1 \star 2) \star 4 = |1-2| \star 4 = 1 \star 4 = |1-4| = 3$

$1 \star (2 \star 4) = 1 \star |2-4| = 1 \star 2 = |1-2| = 1$

满足交换律，但不满足结合律.

定理1.1（广义结合律）：设 $*$ 是集合 S 上满足结合律的二元运算，设 $x_1, \ldots, x_n \in S$. $n > 2$

$k, l \in \{1, 2, \ldots, n-1\}$

则 $(x_1 * \cdots * x_k)(x_{k+1} * \cdots * x_n)$

$= (x_1 * \cdots * x_l) * (x_{l+1} * \cdots * x_n)$

其中 $x_1 * \cdots * x_k$，$x_{k+1} * \cdots * x_n$，$x_1 * \cdots * x_l$，$x_{l+1} * \cdots * x_n$ 的运算~~顺序~~可以~~任意~~按任意次序结合

证：对于 n 归纳

$n = 3$. $k, l \in \{1, 2\}$

$k=1,\ l=1$ $x_1 * (x_2 * x_3) = x_1 * (x_2 * x_3)$ ✓

$k=1,\ l=2$ $x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3$ （结合律）

$k=2,\ l=1$ 结合律

$k=2,\ l=2$ $(x_1 * x_2) * x_3 = (x_1 * x_2) * x_3.$ ✓

设当参与运算的元素个数小于 n 时定理成立. 设 $k, l \in \{1, 2, \dots n-1\}$

由归纳假设

$$x_1 * \dots * x_k, \quad x_{k+1} * \dots * x_n$$
$$x_1 * \dots * x_l, \quad x_{l+1} * \dots * x_n$$

都是唯一的

于是当 $k = l$ 时 定理成立

不妨设 $k > l$

$$(x_1 * \dots * x_l\, x_{l+1} * \dots * x_k) \cdot (x_{k+1} * \dots * x_n)$$

$$= [(x_1 * \dots * x_l) * (x_{l+1} * \dots * x_k)] * (x_{k+1} * \dots * x_n) \quad \text{归纳假设}$$

$$= (x_1 * \dots * x_l) * [(x_{l+1} * \dots * x_k) * (x_{k+1} * \dots * x_n)] \quad \text{结合律}$$

$$= (x_1 * \dots * x_l) * (x_{l+1} * \dots * x_k * x_{k+1} * \dots * x_n) \quad \text{归纳假设}$$

□

记号：当结合律满足时

$x_1 * x_2 * \dots * x_n$ 代表 n 个元素按任何方式进行运算后的唯一值. 特别地

$$\underbrace{x * x * \dots * x}_{n} = x^n$$

$n \geq 1$

例: X 是非空集合. T_X 代表 X 到 X 的所有映射的集合

$$\circ : T_X \times T_X \longrightarrow T_X$$
$$(f, g) \longmapsto f \circ g.$$

满足结合律.

特别地,

$$\circ : S_n \times S_n \longrightarrow S_n$$
$$(\sigma, \tau) \longmapsto \sigma \circ \tau.$$

同余运算　设 n 是大于 1 的整数

$\forall a, b \in \mathbb{Z}$　$a \equiv_n b$ 如果 $n \mid (a-b)$

$a \equiv_n b$ 也记作 $a \equiv b_n$

记 $\mathbb{Z}_n \equiv \mathbb{Z}/\equiv_n$

我们在 $\mathbb{Z}_n$ 上定义两个运算

为此 我们证明

引理 1.1 设 $a \equiv b \mod n$, $c \equiv d \mod n$

其中 $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{Z}^+ \setminus \{1\}$

则 $a + c \equiv b + d \mod n$, $ac \equiv bd \mod n$.

复习：定理1.1（广义结合律）

设 $*$ 是 S 上满足结合律的二元运算，$x_1, \cdots, x_n \in S$，$k, l \in \{1, \cdots, n-1\}$

则 $(x_1 * \cdots * x_k) * (x_{k+1} * \cdots * x_n)$

$= (x_1 * \cdots * x_l) * (x_{l+1} * \cdots * x_n)$

其中：$x_1 * \cdots * x_k$，$x_{k+1} * \cdots * x_n$，

$x_1 * \cdots * x_l$，$x_{l+1} * \cdots * x_n$

的运算次序可以按任意次序结合

回忆：引理1.1 设 $a, b, c, d \in \mathbb{Z}$

$n \in \mathbb{Z}^+$，$n > 1$，如果

$a \equiv b \mod n$，$c \equiv d \mod n$

则 $a + c \equiv b + d \mod n$

$ac \equiv b + d \mod n$

证: $a \equiv b \mod n \Rightarrow n \mid (a-b)$

$\Rightarrow \exists k \in \mathbb{Z} \quad a-b = kn$

同样 $\exists l \in \mathbb{Z} \quad c-d = ln$

$(a+c)-(b+d) = (k+l)n$

$\Rightarrow n \mid [(a+c)-(b+d)] \Rightarrow a+c \equiv b+d \mod n$

$ac = (b+kn)(d+ln)$

$= bd + (lb + kd + kln)n$

$\Rightarrow n \mid (ac-bd) \Rightarrow ac \equiv bd.$ ∎

定义: $+: \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$(\bar{a}, \bar{b}) \longmapsto \overline{a+b}$

记 $\bar{x} = \{ y \in \mathbb{Z} \mid x \equiv y \mod n \}$, 其中 $x \in \mathbb{Z}$

即 x 关于 $\equiv_n$ 的等价类

良定义: 设 $a \equiv c \mod n$, $b \equiv d \mod n$

$\bar{a} = \bar{c}$, $\bar{b} = \bar{d} \Rightarrow a \equiv c \mod n$, $b \equiv d \mod n$

$\bar{c} + \bar{d} = \overline{c+d} = \overline{a+b}$ (引理1.1.(i))

于是 $+$ 在 $\mathbb{Z}_n$ 上是良定义的.

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

$\bar{1} + \bar{1} = \bar{2} = \bar{0}$

$\bar{3} + \bar{5} = \bar{8} = \bar{0}$

定义: $\cdot: \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$(\bar{a}, \bar{b}) \longmapsto \overline{ab}$

验证良定义 设 $\bar{a} = \bar{c}$, $\bar{b} = \bar{d}$

$\bar{c} \cdot \bar{d} = \overline{cd}$

$a \equiv c \mod n.$ $b \equiv d \mod n$

由引理1.1.(ii) $ab \equiv cd \mod n$

即 $\overline{ab} = \overline{cd} \Rightarrow \bar{a} \cdot \bar{b} = \bar{c} \cdot \bar{d}.$

例: 在 $\mathbb{Z}_{10}$ 中计算 $\mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \cdots \bar{9}\}$

$\bar{2} \cdot \bar{5} = \overline{10} = \bar{0}$

$\overline{-8} \cdot \overline{11} = \overline{-88} = \cancel{\overline{100+(-12)}} = \overline{100+(-12)}$

$\cancel{= \overline{-12} = \overline{-20}} = \overline{(-90)+2} = \overline{-90} + \bar{2}$

$= \bar{2}$

验证：在 $\mathbb{Z}$ 上，"+" "·" 满足交换律和结合律.

$\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$

$(\bar{a}+\bar{b}) = \overline{a+b} = \overline{b+a} = \bar{b}+\bar{a}$

自己验证加法结合律和乘法交换律.

$(\bar{a}\cdot\bar{b})\cdot\bar{c} = \overline{ab}\cdot\bar{c} = \overline{(ab)\cdot c} = \overline{a(b\cdot c)}$

$= \bar{a}\cdot\overline{bc} = \bar{a}(\bar{b}\cdot\bar{c})$.

§2 群 (Group)

§2.1 群的定义

定义：设 S 是集合，$*$ 是 S 上的二元运算. 如果 $*$ 满足结合律，则称 S 是半群 (semi-group)，记为 $(S,*)$

例：设 S 是正偶数的集合

则 $(S,+)$ 是半群

例：$S=\{A\in M_n \mid \det(A)>1\}$

则 $(S,\cdot)$ 是非交换半群

~~$\det(A\cdot B)$~~

验证：运算的封闭性.

设 $A, B\in S$ $\quad \det(AB)=\det(A)\det(B)>1$

· 是 S 上的二元运算，结合律显然满足.

定义：设 S ~~是集合~~，$(S,*)$ 是半群

如果 $\exists e\in S$，使得

$\forall x\in S \quad x*e=e*x=x$

则称 $(S,*,e)$ 是含幺半群 (monoid)

引理2.1 设 $(S,*,e)$ 是含幺半群. $e'\in S$ 使得 $\forall x\in S$ $\quad xe'=e'x=x$

则 $e'=e$.

证：$e'\cdot e=e' \quad\Rightarrow e'=e$ □

$e'\cdot e=e$

称 e 是关于 $*$ 的单位元.

例. 设 S 是非负偶数的集合
$(S, +, 0)$ 是含幺半群

设 $S = \{A \in M_n \mid |A| \geq 1\}$
$(S, \cdot, E_n)$ 是含幺半群.

例: 设 T_X 是从集合 X 到 X 的所有映射. $e: X \to X$ 是恒同映射
则 $(T_X, \circ, e)$ 是含幺半群.

定义: 设 $(S, *, e)$ 是含幺半群.
$x \in S$. ~~如果存在~~ $y \in S$, 使得
$$x * y = y * x = e$$
则称 x 是可逆元. y 是 x 的一个逆

引理 2.2 设 $(S, *, e)$ 是含幺半群
$x \in S$ 可逆. 则它的逆唯一.

证: 设 y, z 是 x 的逆
$$xy = e$$
$$z(xy) = ze = z$$
$$\| $$
$$(zx) \cdot y = e \cdot y = y$$
$\Rightarrow z = y$ ☒

记 x 的逆为 x^{-1}

例: 设 $f \in T_X$ 是可逆元 $\Leftrightarrow f$ 是双射

证: 设 f 可逆. 设 $x_1, x_2 \in X$,
若 $f(x_1) = f(x_2)$
$\Rightarrow f^{-1} \circ f(x_1) = f^{-1} \circ f(x_2)$
$\Rightarrow e(x_1) = e(x_2) \Rightarrow x_1 = x_2$
f 是单射
设 $y \in X$. $z = f^{-1}(y)$
$f(z) = f(f^{-1}(y)) = f \circ f^{-1}(y) = e(y) = y$
f 是满射
反之设 f 是双射. 设 g 是 f 的逆映射
则 $f \circ g = g \circ f = e$ ☒

例：设 $f \in T_X$ 是单射，但不是满射

~~则~~ 令 $Y = X \setminus \mathrm{im}(f) \neq \emptyset$

定义：$g: X \longrightarrow X$

当 $x \in \mathrm{im}(f)$ 时，$\exists!\, z \in X$

使得 $f(z) = x$。此时定义 $g(x) = z$

取 $x_0 \in X$，当 $x \in Y$，$g(x) = x_0$

验证：$g \circ f = e$ $(\star)$

~~当 $x \in \mathrm{im}(f)$~~ $\forall u \in X$

$$g \circ f(u) = g(f(u)) = u.$$

$(\star)$ 成立

但 f 不可逆（引理2.2）

~~例 设 $f \in T$~~

引理2.3 设 $(S, *, e)$ 是含幺半群

$x \in S$，如果存在 $y, z \in S$

使得 $y * x = e$，$x * z = e$

则 $y = z$，即 $x^{-1} = y$.

证：
$$(y * x) * z = e * z = z$$
$$\|$$
$$y * (x * z) = y * e = y \qquad \square$$

由此可知，上例中 f 无右逆，即无 $h \in T_X$

使得 $f \circ h = e$.

例：设 $f \in T_X$ 是满射，但不是单射

则 $\forall x \in X$，$f^{-1}(x)$ 非空，取定其中一个

元素 u_x.

定义：$h: X \longrightarrow X$
$$x \longmapsto u_x$$

$$f \circ h(x) = f(u_x) = x$$

于是 $f \circ h = e$.

由引理2.3，f 不可能有左逆.

定义：设 $(G, *, e)$ 是半群

如果 $\forall g \in G$，g 都可逆，则称

$(G, *, e)$ 是群．

例：$(\mathbb{Z}, +, 0)$ 是群

$GL_n(\mathbb{R}) := \{ A \in M_n(\mathbb{R}) \mid |A| \neq 0 \}$

$(GL_n(\mathbb{R}), \cdot, E_n)$

称为 $\mathbb{R}$ 上的一般线性群

例：~~像~~ $(S_n, \circ, e)$ 是置换群

例：$(\mathbb{Z}_n, +, \overline{0})$ 是群

验证：~~$\mathbb{Z}_n$ $(\mathbb{Z}_n, +, \overline{0})$~~ $(\mathbb{Z}_n, +)$ 是半群

$(\mathbb{Z}_n, +, \overline{0})$ 是含幺半群

$\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$．

由加法交换律 $\overline{0} + \overline{a} = \overline{a}$

$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}$．

由加法交换律

$\overline{-a} + \overline{a} = \overline{0}$．

<u>群的等价定义</u>

设 $*$ 是集合 G 上的二元运算

如果满足

(i) 结合律 $\forall g_1, g_2, g_3 \in G$

$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$$

(ii) 单位元．$\exists e \in G$ 使得 $\forall g \in G$

$$g * e = e * g = g$$

(iii) 可逆元 $\forall g \in G$，$\exists h \in G$ 使得

$$g * h = h * g = e.$$

则称 ~~G是~~ $(G, *, e)$ 是群

由引理 2.1．2.2 可知．

群中单位元和逆元唯一．

注　设 $(G,*)$ 是群. 如果 $\forall g_1, g_2 \in G$

$$g_1 * g_2 = g_2 * g_1$$

则称 G 是交换群, 或阿贝尔 (Abelian) 群.

如果 $\mathrm{card}(G) < \infty$ 则称 G 是有限群

此时 $\mathrm{card}(G)$ 称为 G 的阶.

例: $(\mathbb{Z}_n, +, \bar{0})$ 是 n 阶交换群

$(S_n, \cdot, e)$ 是 $n!$ 阶非交换群.

引理 2.4　设 $(G, *; e)$ 是群. $a \in G$

$\forall g, h \in G$　$g * h$ 简记为 gh.

$$L_a: \begin{aligned} G &\longrightarrow G \\ g &\mapsto ag \end{aligned}, \qquad R_a: \begin{aligned} G &\longrightarrow G \\ g &\mapsto ga \end{aligned}$$

~~都是双射~~

注: L_a, R_a 称为 G 上关于 a 的左, 右平移.

证: 设 $g, h \in G$

$L_a(g) = L_a(h) \Rightarrow \cancel{ga}\ ag = ah$

$\Rightarrow a^{-1}(ag) = a^{-1}(ah)$

$\Rightarrow (a^{-1} \cdot a) g = (a^{-1} \cdot a) h$

$\Rightarrow e g = e h$

$\Rightarrow g = h$　　L_a 是单射

$\forall$ $L_a(\overset{a^{-1}g}{\cancel{ga^{-1}}}) = \cancel{ga^{-1}}\ a(a^{-1}g) = (aa^{-1})g$

$= eg = g$

L_a 是满射.

同理可证 R_a 是双射.　∎

另证:

$L_{a^{-1}} \circ L_a(g) = L_{a^{-1}}(ag) = a^{-1}(ag) = g$

$L_a \circ L_{a^{-1}}(g) = L_a(a^{-1}g) = a(a^{-1}g) = g$

于是 $L_{a^{-1}}$ 是 L_a 的逆映射.　∎

13

例 低阶群

1 阶 $G=\{e\}$

	e
e	e

实例：$(\{0\},+,0)$, $(\{1\},\cdot,1)$

$(\{E_n\},\cdot,E_n)$

它们看上去像一回事儿.

2 阶. $G=\{e,a\}$

	e	a
e	e	a
a	a	e

$a^2=e$

实例 $(\{1,-1\},\cdot,1)$, $(\{E_n,-E_n\},\cdot,E_n)$

$(\mathbb{Z}_2,+,\bar{0})$. $(\{(12),e\},\circ,e)$

$$\{(12),e\} = S_2$$

它们看上去像一回事儿

3 阶 $G=\{e,a,b\}$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

实例

$(\mathbb{Z}_3,+,\bar{0})$

$\mathbb{Z}_3=\{\bar{0},\bar{1},\bar{2}\}$

$G=\{e,a,a^2\}$ $a^3=e$

$$\left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\underbrace{\begin{pmatrix}-\frac{1}{2}&-\frac{\sqrt{3}}{2}\\\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix}}_{A},\underbrace{\begin{pmatrix}-\frac{1}{2}&\frac{\sqrt{3}}{2}\\-\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix}}_{A^2}\right\};\cdot,E_2\right)$$

$(\{e,(123),(123)^2\},\circ,e)$

一回事？

4 阶 $G=\{e,a,b,c\}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$G=\{e,a,b,c\}$

$a^2=b^2=c^2=e$

$ab=ba=c$

$ac=ca=b$

$cb=bc=a$

$(\mathbb{Z}_2\times\mathbb{Z}_2,+,(\bar{0},\bar{0}))$

$\{\cancel{1,-1,\sqrt{-1}}$

$(\bar{a},\bar{b})+(\bar{c},\bar{d})$

$=(\bar{a}+\bar{c},\bar{b}+\bar{d})$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\{e, b, \underset{= a}{b^2}, \underset{= c}{b^3}\}$

$b^4 = e$

$(\mathbb{Z}_4, +, \bar{0})$

$(\{$[illegible]$, -1, \sqrt{-1}, -\sqrt{-1}\}, \cdot, 1)$

好像不都是一回事儿