回忆：引理2.1 设 $A=(a_{ij})_{n\times n}$. 则

$\forall i,j\in\{1,\cdots,n\}$ (i) $\sum_{k=1}^{n} a_{ik}A_{jk}=\delta_{ij}|A|$

(ii) $\sum_{k=1}^{n} a_{ki}A_{kj}=\delta_{ij}|A|$.

证：设 $\vec{b}=(b_1,\cdots,b_n)$. $B=\begin{pmatrix}\vec{A}_1\\ \vdots\\ \vec{A}_{j-1}\\ \vec{b}\\ \vec{A}_{j+1}\\ \vdots\\ \vec{A}_n\end{pmatrix}$

由定理2.1

$\det(B)=b_1A_{j1}+\cdots+b_nA_{jn}$

特形1：设 $i\neq j$ 且 $\vec{b}=\vec{A}_i$

则 B 中有两行为 $\vec{A}_i$，则 $|B|=0$.

即 $a_{i1}A_{j1}+\cdots+a_{in}A_{jn}=0$

特形2. 设 ~~$\vec{b}=\vec{A}_j$ 且 $i\neq j$~~ $i\neq j$ 且 $\vec{b}=\vec{A}_i$

则 $\det(B)=\det(A)=a_{j1}A_{j1}+\cdots+a_{jn}A_{jn}$

$=\sum_{k=1}^{n} a_{ik}A_{jk}=\delta_{ii}\det(A)$

类似于证明(ii) 略

定义：设 $A=(a_{ij})_{n\times n}$. A的伴随矩阵 A^V 定义为

$$\begin{pmatrix}A_{11} & A_{21} & \cdots & A_{n1}\\ A_{12} & A_{22} & \cdots & A_{n2}\\ & & \cdots & \\ A_{1n} & A_{2n} & \cdots & A_{nn}\end{pmatrix}$$

定理2.4 设 $A\in M_n(\mathbb{R})$.

则 $AA^V=A^VA=|A|E_n$

证：设 $A^V=(a'_{ij})_{n\times n}$

$AA^V=(b_{ij})_{n\times n}$

则 $b_{ij}=\sum_{k=1}^{n} a_{ik}a'_{kj}=\sum_{k=1}^{n} a_{ik}A_{jk}$

$=\delta_{ij}|A|$ [引理2.1]

$\Rightarrow AA^V=|A|(\delta_{ij})=|A|E_n$.

同理 $A^VA = |A|E$. 图

注
$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} |A| & & & \bigcirc \\ & |A| & & \\ & & \ddots & \\ \bigcirc & & & |A| \end{pmatrix}$$

等矩阵秩的定理2.1和证明2.1.

例. 设 $A \in M_n(\mathbb{R})$. 证明 $|A^V| = |A|^{n-1}$

证: 由定理2.4和定理2.3

$$|A|\,|A^V| = |A|^n$$

当 $|A| \neq 0$ 时 $|A^V| = |A|^{n-1}$

当 $|A| = 0$ 时 $AA^V = O_{n\times n}$

于是 $A = O_{n\times n}$ 或 A^V 不满秩

还是两种情形下都有 $|A^V| = 0$ 且 $|A| = 0$

于是 $|A^V| = |A|^{n-1}$. 图

§3. 行列式的应用

§3.1 矩阵逆的公式

定理3.1 设 $A \in M_n(\mathbb{R})$. 则

A可逆 $\Leftrightarrow$ A^V 满秩

此时 $A^{-1} = \frac{1}{|A|}A^V$.

证: 由定理2.4

$$AA^V = |A|E$$

"$\Rightarrow$" 若A可逆 则 $|A| \neq 0$ 于是

$$\frac{1}{|A|}AA^V = E \Rightarrow A\left(\frac{1}{|A|}A^V\right) = E$$

$$\Rightarrow \frac{1}{|A|}A^V = A^{-1}$$

"$\Leftarrow$" 设 A^V 满秩. $\Rightarrow |A^V| \neq 0$ 由上例可知

$|A| \neq 0$ 于是 A可逆

A^{-1} 的公式已由"$\Rightarrow$"的证明给出.

§3.2 Cramer 法则

定理3.2 设 $A \in M_n(\mathbb{R})$ $\vec{x}=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$, $\vec{b}=\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix}$

则 $A\vec{x}=\vec{b}$ 有唯一解 $\Leftrightarrow$ A可逆

此时 解为

$$x_1=\frac{\det(\vec{b},\vec{A}^{(2)},\cdots,\vec{A}^{(n)})}{\det(A)},\ \cdots,\ x_n=\frac{\det(\vec{A}^{(1)},\cdots\vec{A}^{(n-1)}\vec{b})}{\det(A)}$$

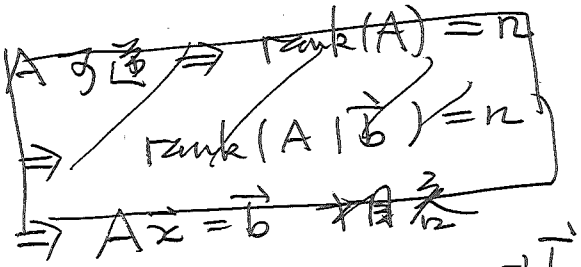
证: "$\Rightarrow$"

$A\vec{x}=\vec{b}$ 有唯一解 $\Rightarrow$ $A\vec{x}=\vec{0}$ 只有零解 (讲义2-4 p14 例)

$\Rightarrow$ A 列满秩 (第二章2.3节定理2)

$\Rightarrow$ A 可逆

"$\Leftarrow$"



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

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

$\Rightarrow x_i=(\vec{A^{-1}})_i\vec{b}$

设 A 可逆. 则 对 $\forall i=1,2,\cdots n$.

$$x_i=(\vec{A^{-1}})_i\vec{b}=\frac{1}{|A|}(\vec{A^*})_i\vec{b}$$

(定理3.1)

$$=\frac{1}{|A|}\left(b_1A_{1i}+\cdots+b_nA_{ni}\right)=\frac{1}{|A|}\det(\vec{A}^{(1)},\cdots\vec{A}^{(i-1)}\vec{b},\vec{A}^{(i+1)},\cdots\vec{A}^{(n)})$$ 证

注:

$$A^{-1}=\begin{pmatrix}\frac{A_{11}}{|A|} & \cdots & \frac{A_{n1}}{|A|}\\ & \cdots & \\ \frac{A_{1n}}{|A|} & \cdots & \frac{A_{nn}}{|A|}\end{pmatrix}$$

$$x_j=\frac{1}{|A|}\begin{vmatrix}a_{11}&\cdots a_{1j-1}&b_1&a_{1j+1}\cdots a_{1n}\\ a_{21}&\cdots a_{2j-1}&b_2&a_{2j+1}\cdots a_{2n}\\ &&\cdots&\\ a_{n1}&\cdots a_{nj-1}&b_n&a_{nj+1}\cdots a_{nn}\end{vmatrix}$$

$j=1,2,\cdots n$.

于是 当 $A\in M_n(\mathbb{Z})$ 且 A 可逆

A^{-1} 中的元素的分母都整除 $|A|$. 证

§3.3 行列式和矩阵的秩

定义：设 $A=(a_{ij})_{m\times n}$ $i_1,\cdots i_k\in\{1,\cdots m\}$

$j_1,\cdots j_k\in\{1,\cdots,n\}$. $i_1,\cdots i_k$ 不一定两两不同

$j_1,\cdots j_k$ 也不一定两两不同.

则 $\begin{vmatrix} a_{i_1,j_1} & \cdots & a_{i_1,j_k} \\ & \cdots & \\ a_{i_k,j_1} & \cdots & a_{i_k,j_k} \end{vmatrix}$ 称为 A 的

k 阶子式，记为 $M_A\begin{pmatrix} i_1,\cdots i_k \\ j_1,\cdots j_k \end{pmatrix}$

例：设 $A=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$

$M_A\begin{pmatrix}1&2\\1&2\end{pmatrix}=\begin{vmatrix}1&2\\5&6\end{vmatrix}$. $M_A\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{vmatrix}3&4\\7&8\end{vmatrix}$

$M_A\begin{pmatrix}2&1\\2&4\end{pmatrix}=\begin{vmatrix}6&8\\2&4\end{vmatrix}$ $M_A\begin{pmatrix}3&3\\R&4\end{pmatrix}=\begin{vmatrix}9&10\\9&10\end{vmatrix}$

引理3.1 设 $j_1,\cdots j_k\in\{1,\cdots,n\}$ 使得 ④

则 $\vec{A}^{(j_1)},\cdots\vec{A}^{(j_k)}$ 多半生无关 $\Longleftrightarrow$

则 对任 $i_1,\cdots i_k\in\{1,\cdots,m\}$. 使得

$$M_A\begin{pmatrix} i_1,\cdots i_k \\ j_1,\cdots j_k \end{pmatrix}\neq 0$$

证："$\Longrightarrow$" 令 $B=(\vec{A}^{(j_1)},\cdots\vec{A}^{(j_k)})_{m\times k}$

则 $\mathrm{rank}(B)=k$. 则对任 $i_1,\cdots i_k\in\{1,\cdots m\}$

使得 $\vec{B}_{i_1},\cdots\vec{B}_{i_k}$ 多半生无关. [第二章引理]

令 $B'=\begin{pmatrix}\vec{B}_{i_1}\\ \vdots \\ \vec{B}_{i_k}\end{pmatrix}_{k\times k}$. 则 B' 可逆满秩

于是 $|B'|\neq 0$. 而 $|B'|=M_A\begin{pmatrix} i_1,\cdots i_k \\ j_1,\cdots j_k \end{pmatrix}$.

"$\Longleftarrow$" 设 $\alpha_1,\cdots\alpha_k\in\mathbb{R}$ 满足

$$\alpha_1\vec{A}^{(j_1)}+\cdots+\alpha_k\vec{A}^{(j_k)}=\vec{0}$$

即 $\alpha_1\begin{pmatrix}a_{ij_1}\\ \vdots\\ a_{mj_1}\end{pmatrix}+\cdots+\alpha_k\begin{pmatrix}a_{ij_k}\\ \vdots\\ a_{m,j_k}\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$

$\Rightarrow \alpha_1\begin{pmatrix}a_{i_1,j_1}\\ \vdots\\ a_{i_k,j_1}\end{pmatrix}+\cdots+\alpha_k\begin{pmatrix}a_{i_1,j_k}\\ \vdots\\ a_{i_k,j_k}\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$

$\Rightarrow \alpha_1=\cdots=\alpha_k=0$ [因为 $\begin{pmatrix}a_{i_1,j_1}&\cdots&a_{i_1,j_k}\\ &\cdots&\\ a_{i_k,j_1}&\cdots&a_{i_k,j_k}\end{pmatrix}$ 满秩]

$\Rightarrow \vec{A}^{(j_1)},\cdots\vec{A}^{(j_k)}$ 线性无关

定理3.3 设 $A\in\mathbb{R}^{m\times n}$. 以下断言等价

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

(ii) A中有一个 r阶子式非零 而且任何大于r阶子式都是零

(iii) A中有一个 r阶子式非零. 而任何 r+1阶子式都是零

证: (i) $\Rightarrow$ (ii). 设 $\vec{A}^{(j_1)},\cdots\vec{A}^{(j_r)}$ 线性无关

由引理3.1 A中有一个 r阶子式非零

假设 $s>r$ 且 $M_A\begin{pmatrix}i_1,\cdots i_s\\ j_1,\cdots j_s\end{pmatrix}\neq 0$

由引理3.1 $\vec{A}^{(j_1)},\cdots\vec{A}^{(j_s)}$ 线性无关 $\rightarrow\leftarrow$

(ii) $\Rightarrow$ (iii) 显然.

(iii) $\Rightarrow$ (i) 由引理3.1. A中有 r列线性无关

于是 $\operatorname{rank}(A)\geq r$. 假如 $\operatorname{rank}(A)>r$

则 A中有 r+1列线性无关. 由引理3.1

A中有 r+1阶非零子式. 矛盾.

于是 $\operatorname{rank}(A)=r$.

注: 我们可以只用 $+,\times$ 来计算矩阵的秩.

§3.4 $\mathbb{R}^n$ 中的直线 (补充)

定理3.4 设 $A \in \mathbb{R}^{(n-1)\times n}$ 且 $\operatorname{rank}(A)=n-1$

则 (H) $A\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$ 的解空间

的一组基是 $\vec{W}=\begin{pmatrix}-D_1\\ D_2\\ \vdots\\ (-1)^{n-1}D_{n-1}\\ (-1)^n D_n\end{pmatrix}$，其中 D_j 是 A 去掉第 j 列后所得的矩阵的行列式，

证: 设 $B_i=\begin{pmatrix}\vec{A}_1\\ \vdots\\ \vec{A}_{n-1}\\ \vec{A}_i\end{pmatrix}$, $i=1,2,\cdots n-1$

$$0=|B_i|=a_{i1}(-1)^{n+1}D_1+a_{i2}(-1)^{n+2}D_2$$
$$+\cdots+a_{in}(-1)^{n+n}D_n$$

$$\Rightarrow a_{i1}(-D_1)+a_{i2}D_2+\cdots+a_{in}(-1)^n D_n=0$$

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

$$\Rightarrow x_1=-D_1,\quad x_2=D_2,\quad \cdots \quad x_n=(-1)^n D_n$$

是原方程组(H)的解. 又因为 $\operatorname{rank}(A)=n-1$

所以 $\dim V_A=1$ (对偶定理)

且 $D_1, D_2, \cdots D_n$ 中至少有一个非零 (定理3.3)

于是 $\vec{W}$ 是 V_A 的一组基 ∎

引理 3.2. 设 $\vec{u},\vec{v}\in\mathbb{R}^n$, $U,V\subset\mathbb{R}^n$ 是三个集合. 如果 $\vec{u}+U=\vec{v}+V$

则 $U=V$

证: $\because \vec{u}\in U \therefore \exists\, \vec{z}\in V$ 使得

$$\vec{u}=\vec{v}+\vec{z}$$

设 $\vec{x}\in U$. 则 $\exists\, \vec{y}\in V$ 使得

$$\vec{u}+\vec{x}=\vec{v}+\vec{y}$$

$$\Rightarrow \vec{v}+\vec{z}+\vec{x}=\vec{v}+\vec{y} \Rightarrow \vec{x}=\vec{y}-\vec{z}\in V$$

$$\Rightarrow U\subset V.$$

类似 $V\subset U$. ∎

定义：设 $\vec{u}\in\mathbb{R}^n$，$U\subset\mathbb{R}^n$ 是子空间

则 U 称为线性流形 $\vec{u}+U$ 的方向

$\dim U$ 称为线性流形 $\vec{u}+U$ 的维数

当 $\dim U=n-1$ 时 $\vec{u}+U$ 称为超平面

当 $\dim U=1$ 时，$\vec{u}+U$ 称为直线.

注：设 $\vec{u}=\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}$，$\dim U=1$，

且 $\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}$ 是 U 的一组基

则 $\vec{u}+U=\left\{\vec{u}+t\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}\mid t\in\mathbb{R}\right\}$

$=\left\{\begin{pmatrix}u_1+t\alpha_1\\ \vdots\\ u_n+t\alpha_n\end{pmatrix}\mid t\in\mathbb{R}\right\}$

于是直线 $\vec{u}+U$ 的参数方程是

$$\begin{cases}x_1=u_1+t\alpha_1\\ \quad\vdots\\ x_n=u_n+t\alpha_n\end{cases}$$

设 $U=V_A$ 其中 $A\in\mathbb{R}^{(n-1)\times n}$ $\operatorname{rank}(A)=n-1$

则 $\vec{u}+U$ 的参数方程是

$$\begin{cases}x_1=u_1-tD_1\\ x_2=u_2+tD_2\\ \quad\vdots\\ x_n=u_n+(-1)^n tD_n\end{cases}$$，其中 $D_1,D_2,\cdots D_n$ 如定理 3.4 给出.

例：证明：$\mathbb{R}^n$ 中的直线是

$\mathbb{R}^n$ 中 $n-1$ 个超平面的交.

证：设直线 $\vec{u}+U$，其中 $\vec{u}\in\mathbb{R}^n$

$U\subset\mathbb{R}^n$ 是 1 维子空间. 由定理 9.1

U 是某个 n 列的矩阵 A 的零空间对应

的齐次线性方程组的解空间 V_A

$\because\ \dim V_A=1\ \therefore\ \operatorname{rank}(A)=n-1$

于是不妨设 A 有 $n-1$ 行. [线性无关]

设 $A\vec{u}=\vec{v}$ 则 $\vec{u}+U$

是方程组 $A\vec{x}=\vec{v}$ 的解. 图

第四章 群、环、域 简介

§1. 二元运算

§1.1 广义结合律

定义：设 S 是非空集合，$f: S\times S\to S$ 称 f 为 S 上的一个（二元）运算.

记号 $\forall x,y\in S$ $f(x,y)$ 记为 xfy

例：(i) $+: \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$
$(a,b)\longmapsto a+b$ $[+(a,b)]$

(ii) $\cdot: M_n(\mathbb{R})\times M_n(\mathbb{R})\longrightarrow M_n(\mathbb{R})$
$(A,B)\longmapsto AB$

(iii) $*: \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$
$(x,y)\longmapsto |x-y|$

注：设 f 是 S 上的二元运算

如果 $\forall x,y\in S$，
如果 $f(x,y)=f(y,x)$ $[xfy=yfx]$
则称 f 满足交换律

$\forall x,y,z$
如果 $f(f(x,y),z)=f(x,f(y,z))$ $[(xfy)fz=xf(yfz)]$
则称 f 满足结合律.

在上述例子中
"+" 满足交换和结合律
$\cdot$ ------ 但不满足结合律
$*$ ------ 但不满足结合律

$(1*2)*4=|1-2|*4=1*4=|1-4|=3$
$1*(2*4)=1*|2-4|=1*2=|1-2|=1$

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
$x_1,\dots,x_n\in S$, $n\geq 2$, $k,l\in\{1,2,\dots,n+1\}$, $k\neq l$

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

证：对 n 归纳 $n=3$. 不妨设 $k=1$, $l=2$

$x_1*(x_2*x_3)=(x_1*x_2)*x_3$
[结合律]

设 $n>3$，且结论对参与运算的元素个数

少于 n 时都成立. 设 $k>l$

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

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

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

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

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

□

记号 设 $*$ 是 S 上满足结合律的

运算，则 $x_1 * \cdots * x_n$ 结果唯一

特别地 $\underbrace{x * \cdots * x}_{n \in \mathbb{Z}^+}$ 记为 x^n

我们有 $\forall\, n, m \in \mathbb{Z}^+$

$$(x^m) * (x^n) = x^{m+n}$$

当 $*$ 用 $+$ 取代时

$\underbrace{x + x + \cdots + x}_{n}$ 记为 nx

注意 nx 不是初等"n 乘以 x"

§1.2 同余运算

回忆：设 $n \in \mathbb{Z}^+$，$n>1$. $\forall a, b \in \mathbb{Z}$

$a \equiv_n b$ （或 $a = b \bmod n$）当且仅当 $n \mid (a-b)$.

$\mathbb{Z}/\equiv_n$ 记为 $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots \overline{n-1}\}$.

其中 $\bar{k} = \{ln+k \mid l \in \mathbb{Z}\}$

$\bar{0} = \overline{n} = \overline{2n} = \cdots$

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

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

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

验证良定义. 设 $\bar{a}=\bar{a'}$, $\bar{b}=\bar{b'}$

则 $a=a'+kn$, $b=b'+ln$, , $k,l\in\mathbb{Z}$

$$(a+b)=(a'+b')+(k+l)n$$

$$\Rightarrow \quad a+b \equiv a'+b' \mod n$$

$$\Rightarrow \quad \overline{a+b}=\overline{a'+b'}$$

自己验证 $\mathbb{Z}_n$ 上的 "+" 满足交换律和结律

例: $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$

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

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

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

定义: $\cdot$

$$\begin{aligned}\mathbb{Z}_n\times\mathbb{Z}_n &\longrightarrow \mathbb{Z}_n\\ \bar{a},\bar{b} &\longmapsto \overline{ab}\end{aligned}$$

验证: $\bar{a}=\bar{a'}$. $\bar{b}=\bar{b'}$

则 $a=a'+kn$. $b=b'+ln$

~~$ab=a'b'+a'ln+b'kn+kln$~~

$$ab=a'b'+a'ln+b'kn+kln^2$$

$$=a'b'+(a'l+b'k+kln)n$$

$$\Rightarrow \quad ab\equiv a'b' \mod n \quad \checkmark$$

$$\Rightarrow \quad \overline{ab}=\overline{a'b'}$$

自己验证 · 满足交换和结合律

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

$\bar{2}\cdot\bar{2}=\bar{4}=\bar{1}$ $\quad \bar{1}\cdot\bar{2}=\bar{2}$

$\bar{1}\cdot\bar{0}=\bar{0}$ $\quad \bar{1}\cdot\bar{1}=\bar{1}$

§1.3. 零指元和可逆元

定义: 设 $*$ 是 S 上的二元运算, $e\in S$

称 e 是 S 上关于 $*$ 的零位元, 若 $\forall x\in S$. $x*e=e*x=x$

则称 e 是 S 上关于 $*$ 的零位元.

例：0 是 $\mathbb{Z}$ 上 "$+$" 的单位元

E 是 $M_n(\mathbb{R})$ 上 "乘法" 的单位

$\overline{0}$ 是 $\mathbb{Z}_n$ 上 "$+$" 的单位.

$\overline{1}$ 是 $\mathbb{Z}_n$ 上 乘法 的单位

命题 1.1. 设 $*$ 是 S 上的二元运算

e 和 e' 是 S 中关于 $*$ 的单位. 则

$$e = e'$$

证：$e * e' = e$　　$e * e' = e' \Rightarrow e = e'$ □

定义：设 $*$ 是 S 上的二元运算

e 是 S 中关于 $*$ 的单位.

设 $x \in S$. 如果 $\exists y \in S$ 使得

$$x * y = y * x = e$$

则称 x 是 S 中关于 $*$ 的可逆元

例：$\mathbb{Z}$ 中关于 "$+$" 任何元素可逆

$M_n(\mathbb{R})$ 中关于 "乘法" 的可逆元是 所有满秩矩阵

$\mathbb{Z}_n$ 中关于 "$+$" 任何元素 可逆

命题 1.2 ~~设 $\mathbb{Z}_n$ 中~~ 设 $\overline{m} \in \mathbb{Z}_n$

则 $\overline{m}$ 关于 $\mathbb{Z}_n$ 中乘法可逆 $\Leftrightarrow \gcd(m,n)=1$

证："$\Leftarrow$" 由 Bezout 关系

$\exists a, b \in \mathbb{Z}$. 使得

$$am + bn = 1$$

$$am \equiv 1 \mod n$$

$$\overline{am} = \overline{1} \Rightarrow \overline{a}\,\overline{m} = \overline{1}$$

$$\overline{a}\,\overline{m} = \overline{m}\,\overline{a} = \overline{1}.$$

"$\Rightarrow$"　$\exists a \in \mathbb{Z}$.　$\overline{a}\,\overline{m} = \overline{1}$

$\Rightarrow am \equiv 1 \mod n$

$\Rightarrow \exists b \in \mathbb{Z}$　$am + nb = 1$

$\Rightarrow \gcd(m,n) = 1$.　(第一章定理 6.2) □

例：求 $\mathbb{Z}_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ 中的可逆元，

$\bar{1}=\bar{1}\cdot\bar{1}=\bar{1}$

$\bar{5}=\bar{5}\cdot\bar{5}=\overline{25}=\bar{1}$

例：设 $S^S=\{f:S\to S \mid f \text{ 映射}\}$ 复合。$\forall S$ 上满足结合律的二元运算

$id:S\to S$ 为恒同映射是 S 中关于"$\circ$"的单位元。$f\in S^S$ 可逆

$\Leftrightarrow f$ 是双射。

例：截断减法 $\dot{-}:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$

$(a,b)\mapsto \max(a-b,0)$

$\widetilde{\mathbb{Z}}=\mathbb{Z}\cup\{+\infty\}$

$\dot{+}:\widetilde{\mathbb{Z}}\times\widetilde{\mathbb{Z}}\to\widetilde{\mathbb{Z}}$

$(a,b)\mapsto \min(a,b)$

$\min(a,+\infty)=a$

$+\infty$ 是 $\widetilde{\mathbb{Z}}$ 中关于 $\dot{+}$ 的单位

$+\infty$ 是 $\widetilde{\mathbb{Z}}$ 中唯一的可逆元。

§2 群

§2.1 群的定义

定义：设 $*$ 是 S 上的二元运算

如果 $*$ 满足结合律，则称 $(S,*)$ 是半群。当"$*$"由上下文定义清楚时也称 S 为半群 (semi-group)

例：$(\mathbb{Z}^+,+)$ 是半群

$(M_n(\mathbb{R}),\cdot)$ 是半群

$(\mathbb{Z},\dot{+})$ 是半群

↳ 截断加法

当 $*$ 满足交换律时

半群 $(S,*)$ 称为交换半群。

定义：设 $*$ 是集合 M 上的二元运算

如果 $(M,*)$ 是有单位 e 的半群，则称 $(M,*,e)$ 或 M 是含幺半群 (monoid)

例：$(\tilde{\mathbb{Z}}, \dot{+}, +\infty)$ 是含幺半群

$(\mathbb{Z}_n, \cdot, \bar{1})$ 是含幺半群

$(M_n(\mathbb{R}), \cdot, E)$ 是含幺半群

命题2.1. 设 $(M,*,e)$ 是含幺半群，$x\in M$ 可逆

则 $\exists!\, y\in M$，使得 $xy=yx=e$.

证：设 $xy=yx=e$，$xz=zx=e$，其中 $y,z\in M$. 则

$$z(xy)=ze=z$$

结合律 $\longrightarrow$ $\|$

$$(zx)y=ey=y$$

$\Rightarrow y=z$

□

~~定义：设 $(G,*,e)$ 是含幺半群~~

~~如果 $\forall g\in G$~~

设 $x\in M$ ($\cdot$ 半群) x 的逆记为 x^{-1}

注：设 $x,y\in M$ 是可逆元，则 xy 仍可逆

且 $(xy)^{-1}=y^{-1}x^{-1}$.

验证：$(xy)(y^{-1}x^{-1})=x(yy^{-1})x^{-1}$

$=x(e)x^{-1}=xx^{-1}=e$.

$(y^{-1}x^{-1})(xy)=y^{-1}(x^{-1}x)y=y^{-1}ey=y^{-1}y=e$.

$\Rightarrow y^{-1}x^{-1}=(xy)^{-1}$.

定义：~~设 $*$ 是幺~~ 设 $(G,*,e)$ 是含幺半群，如果 $\forall g\in G$，g 都可逆，则称 $(G,*,e)$ 或 G 是群 (group)

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

令 $GL_n(\mathbb{R})=\{A\in M_n(\mathbb{R}) \mid A \text{ 可逆}\}$

则 $(GL_n(\mathbb{R}),\cdot,E)$ 是群，称为一般线性群 (General linear group)

设 X 是非空集合，$T_X=\{f: X\to X \mid f \text{ 双射}\}$

是 $(T_X, \circ, \mathrm{id}_X)$ 是群. 特别地

$(S_n, \circ, e)$ 是群. 称为 n 元置换群.

设 $\mathbb{R}^*=\{x\in\mathbb{R} \mid x\neq 0\}$. 则

$(\mathbb{R}^*, \cdot, 1)$ 是群.

命题2.2. 设 $\mathbb{Z}_n^*=\mathbb{Z}_n\setminus\{\bar{0}\}$. 则

$(\mathbb{Z}_n^*, \cdot, 1)$ 是群 $\Leftrightarrow$ n 是素数

证: 设 $a\in\{0,1,\cdots,n-1\}$. 注意到

$$\mathbb{Z}_n^*=\{\bar{1},\bar{2},\cdots,\overline{n-1}\}$$

由命题1.2. $\bar{a}$ 可逆 $\Leftrightarrow \gcd(a,n)=1$

"$\Rightarrow$" 由 $\gcd(a,n)=1 \Rightarrow a\nmid n \Rightarrow n$ 是素数

"$\Leftarrow$" 由 n 是素数 $\Rightarrow \gcd(a,n)=1 \Rightarrow \bar{a}$ 可逆 □

例: 求 $\mathbb{Z}_7^*=\{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$ 中

各元素的逆.

解: $\bar{1}\cdot\bar{1}=\bar{1}$. $\bar{2}\cdot\bar{4}=\bar{8}=\bar{1}$

$\bar{3}\cdot\bar{5}=\overline{15}=\bar{1}$. $\bar{6}\cdot\bar{6}=\overline{36}=\bar{1}$

注 设 $(G,*,e)$ 是群. 若"$*$"满足

交换律时称为交换群或阿贝尔群

(abelian groups). 否则称为非交换

(非阿贝尔群).

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

$(\mathbb{R}^*,\cdot,1)$ 是交换群

$(GL_n(\mathbb{R}),\cdot,E)$, $(S_n,\circ,e)$

不是交换群.

注：当 $\mathrm{card}(G)<\infty$ 时称 G 是有限群

否则称为无限群。$\mathrm{card}(G)$ 称为 G 的阶.

例：$(\mathbb{Z}_n, +, \bar{0})$ 是阶是 n. S_n 的阶是 $n!$

$(\mathbb{Z}, +, 0)$, $(GL_n(\mathbb{R}), \cdot, E)$

$(\mathbb{R}^*, \cdot, 1)$ 是无限群.

引理 2.1. 设 $(G, *, e)$ 是群, $a \in G$

则: $L_a: G \to G$, $g \mapsto a*g$; $R_a: G \to G$, $g \mapsto g*a$

都是双射

证: $L_{a^{-1}}: G \to G$, $g \mapsto a^{-1}*g$

$\forall\, g \in G$

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

$= (a*a^{-1})*g = e*g = g$

于是 $L_a \circ L_{a^{-1}} = id_G$. $\Rightarrow L_a$ 是双射 ⑮

反之 $L_{a^{-1}} \circ L_a = id_G$.

同理可证: R_a 是双射.

例 1 阶群.

$\mathrm{card}(G)=1$

$*$	e
e	e

实例: $(\{0\}, +, 0)$

$(\{1\}, \times, 1)$, $(\{E_n\}, \cdot, E_n)$

$\mathrm{card}(G)=2$ $G=\{e, a\}$

$*$	e	a
e	e	a
a	a	e

即 $a^2=e$

实例: $(\{1,-1\}, \cdot, 1)$

$(\mathbb{Z}_2, +, \bar{0})$, $(S_2, \circ, e)$

$\| $

$\{e, (12)\}$.