回忆： $A=(a_{ij})_{m\times n}\in \mathbb{R}^{m\times n}$.

$N=M_A\begin{pmatrix} i_1,\cdots,i_k \\ j_1,\cdots,j_k\end{pmatrix}$, A的k阶子式

设 $s\in\{1,\cdots,m\}$, $t\in\{1,\cdots n\}$. 称为

$M_A\begin{pmatrix} i_1,\cdots,i_k\ s \\ j_1,\cdots,j_k\ t\end{pmatrix}$ 称为 N 的一个加边式

例：

$$= \det\begin{pmatrix} a_{i_1j_1} & \cdots & a_{i_1j_k} & a_{i_1t} \\ \cdots & & & \\ a_{i_kj_1} & \cdots & a_{i_kj_k} & a_{j_kt} \\ a_{sj_1} & \cdots & a_{sj_k} & a_{st}\end{pmatrix}$$

$$\det\begin{pmatrix} a_{i_1j_1} & \cdots & a_{i_1t} & \cdots & a_{i_1j_k} \\ \cdots & & \cdots & & \cdots \\ a_{sj_1} & \cdots & a_{st} & \cdots & a_{sj_k} \\ \cdots & & \cdots & & \cdots \\ a_{i_kj_1} & \cdots & a_{i_kt} & \cdots & a_{i_kj_k}\end{pmatrix}$$

定理 3.4 设 $A\in\mathbb{R}^{m\times n}$, $A\neq O_{m\times n}$. ①

则 $\operatorname{rank}(A)=r$ $\Leftrightarrow$

(i) A 有一个 r 阶子式非零 N 非零

(ii) N 的所有加边子式都为零

证：“$\Rightarrow$” 定理 3.3

“$\Leftarrow$” 设 $N=M_A\begin{pmatrix} i_1,\cdots i_{r+1} \\ j_1,\cdots j_{r+1}\end{pmatrix}\neq 0$

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

$(\forall s\in\{1,\cdots,m\},\quad t\in\{1,\cdots n\})$

把 N_{st} 按最后一行展开.

$$(*):\ a_{sj_1}\alpha_{j_1,t}+\cdots+a_{sj_r}\alpha_{j_r,t}+N\,a_{st}=0$$

因为 $\alpha_{j_1,t},\cdots\alpha_{j_r,t}$ 与 s 无关.

所以 (*) 对 $s\in\{1,\cdots m\}$ 都成立

即 $\alpha_{j_1,t}\vec{A}^{(j_1)}+\cdots+\alpha_{j_r,t}\vec{A}^{(j_r)}+N\vec{A}^{(t)}=\vec{0}_m$

$$\Rightarrow \vec{A}^{(t)} = \left(\frac{-\alpha_{j_1,t}}{N}\right)\vec{A}^{(j_1)} + \cdots + \left(\frac{-\alpha_{j_r,t}}{N}\right)\vec{A}^{(j_r)}$$

$(\because N \neq 0)$

$$\Rightarrow \vec{A}^{(t)} \in \langle \vec{A}^{(j_1)}, \cdots, \vec{A}^{(j_r)} \rangle \quad \text{其中 } t \in \{1,2,\cdots\}$$

$$\Rightarrow \operatorname{rank}(A) \leq r.$$

由但 $N \neq 0$ 结合 $\operatorname{rank}(A) > r-1$ (定理3.3)

于是 $\operatorname{rank}(A) = r$. 图.

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

的秩和一个最大阶非零子式

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

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

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

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

$$M_A\begin{pmatrix}1&2&3\\1&3&4\end{pmatrix} = \begin{vmatrix}2&3&-2\\4&5&1\\2&1&8\end{vmatrix} = \begin{vmatrix}2&3&-2\\0&-1&5\\0&-2&10\end{vmatrix} = 0$$

$$M_A\begin{pmatrix}1&2&3\\1&3&5\end{pmatrix} = \begin{vmatrix}2&3&4\\4&5&7\\2&1&2\end{vmatrix} = \begin{vmatrix}2&3&4\\0&-1&-1\\0&-2&-2\end{vmatrix} = 0$$

且 $M_A\begin{pmatrix}1&2\\1&3\end{pmatrix} \neq 0$

$\Rightarrow \operatorname{rank}(A) = 2$

注：如果不用加边子式，可能要算 $\binom{3}{2}\binom{5}{2} = 30$ 个 二阶行列式

$\binom{5}{3} = 10$ 个 三阶行列式

用加边子式至多算

$\binom{2}{1}\binom{4}{1} = 8$ 个 二阶子式

$\binom{3}{1} = 3$ 个 三阶行列式.

注：行列式的应用在数学的很多分支中都出现.

例如：

数学分析：Jacobian，Hessian

微分方程：Wronskian.

初等代数：Sylvester's resultant

Discriminant.

其主要原因为 n个未知数，n个方程的线性方程组无处不在.

第4章 群、环、域简介

§1. 二元运算

定义：设 S 是非空集合，$f: S\times S\to S$ 称为 S 上的一个二元运算，即满足封闭性

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

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

满足交换律和结合律.

$\cdot: M_n(\mathbb{R})\times M_n(\mathbb{R})\to M_n(\mathbb{R})$，$(A,B)\mapsto AB$

满足结合律，但不满足交换律

$*: \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$，$(x,y)\mapsto |x-y|$

满足交换

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

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

不满足结合.

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，$x_1,\cdots,x_n\in S$，$n\geq 2$，$k,l\in\{1,2,\cdots,n-1\}$

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

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

证：对 n 归纳。

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

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

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

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

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

设 $n>3$ 且当参与运算的元素个数小于 n 时定理成立

设 $k, l \in \{1,2,\cdots,n-1\}$ 由归纳假设 ④

$x_1 * \cdots * x_k$, $x_{k+1} * \cdots * x_n$ 都是唯一的

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

特别地 当 $k=l$ 时 定理成立.

设 $k > l$

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

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

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

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

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

同理可以处理 $k < l$ 的情形 □

记号 设 $*$ 是 S 上的二元运算.

满足结合律, $x_1, \cdots x_n \in S$

则 $x_1 * x_2 * \cdots * x_n$ 有意义

特别. 当 $x \in S$, $n \in \mathbb{Z}^+$

x^n 代表 $\underbrace{x \cdots x}_{n}$

当 $m \in \mathbb{Z}^+$ $(x^n) * (x^m) = x^{m+n}$

更特别: 当 $*$ 用 "+" 来代表时

$\underbrace{x + x + \cdots + x}_{n}$ 用 nx 代表

但不是 n 乘以 x

例 **同余运算** 设 $n \in \mathbb{Z}^+$, $n > 1$

$a, b \in \mathbb{Z}$ 关于 n 同余. 如果

$n \mid (a-b)$

记为 $a \equiv_n b$ 或 $a \equiv b \bmod n$

"$\equiv_n$" 是等价关系.

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

$\mathbb{Z}_n = \{ \overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1} \}$

其中 $\overline{0} = \{ kn \mid k \in \mathbb{Z} \}$

$\overline{1} = \{ kn+1 \mid k \in \mathbb{Z} \}$

$\vdots$

$\overline{n-1} = \{ kn + n - 1 \mid k \in \mathbb{Z} \}$

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

$\overline{a} = \overline{a+kn}$, $k \in \mathbb{Z}$

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

$(\overline{a}, \overline{b}) \mapsto \overline{a+b}$, 其 $a, b \in \mathbb{Z}$

即 $\overline{a} + \overline{b} = \overline{a+b}$

良定义: 设 $\overline{a} = \overline{a'}$, $\overline{b} = \overline{b'}$

则 $a \equiv a' \bmod n$, $b \equiv b' \bmod n$

$a' = a + kn$. $b' = b + \ell n$, 其中,

k, ℓ 是某个整数

则 $a'+b' = a+kn+b+ln = a+b+(k+l)n$

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

$\Rightarrow \overline{a'+b'} = \overline{a+b}$. + 是良定义的

+ 满足交换律.

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

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

$\because a+b = b+a \quad \therefore \overline{a+b} = \overline{b+a}$

$\Rightarrow \bar{a}+\bar{b} = \bar{b}+\bar{a}$

自己验证: a "+" 满足结合律

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

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

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

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

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

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

$\overline{12}+\overline{24} = \overline{36} = \bar{0}$

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

"乘法": $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

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

即 $\bar{a}\cdot\bar{b} = \overline{ab}$

验证良定义: 设 $\bar{a} = \bar{a'}$ 且 $\bar{b} = \bar{b'}$

则 $a \equiv a' \mod n$, $b = b' \mod n$

$a' = a+kn$, $b' = b+ln$.

$a'b' = ab + (al+kb+lkn)n$

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

$\Rightarrow \overline{a'b'} = \overline{ab}$ 良定义 ✓

自己验证: $\bar{a}\bar{b} = \bar{b}\bar{a}$

验证结合律

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

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

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

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

例 $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{2} \cdot \bar{2} = \overline{4} = \bar{0}$, $\bar{3} \cdot \bar{3} = \overline{9} = \bar{1}$.

现在 $\mathbb{Z}_n$ 上有两个二元运算 $+$, $\cdot$

验证它们满足分配律

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

$= \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}$

单位元

设 $*$ 是集合 S 上的运算.

如果 $\exists e \in S$. 使得 $\forall x \in S$

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

则称 e 是关于 $*$ 的一个单位.

例: $\mathbb{Z}$ 上加法的单位是 0

$M_n(\mathbb{R})$ 乘法的单位是 E

$\mathbb{Z}_n$ 上加法的单位是 $\bar{0}$

$\mathbb{Z}_n$ 上乘法的单位是 $\bar{1}$

~~逆元~~ ~~设 $*$ 是集合~~

命题 1.1 设 e, e' 是 S 上运算 $*$ 的两个单位. 则 $e = e'$

证: $e * e' = e$ $e * e' = e'$

$\Rightarrow e = e'$

可逆元 设 $*$ 是 S 上的运算. e 是 $*$ 的单位. $x \in S$. 如果 $\exists y \in S$ 使得 $x * y = y * x = e$. 则称 x 是可逆元, y 是 x 的逆.

例, $\mathbb{Z}$ 上加法, 每个元素可逆

$M_n(\mathbb{R})$, 乘法. $A \in M_n(\mathbb{R})$ 是可逆元 $\Leftrightarrow$ A 满秩.

$\mathbb{Z}$，乘法中可逆元是 ± 1.

记：

命题 1.1 设 $n \in \mathbb{Z}$, $n > 1$., $m \in \mathbb{Z}$

则 $\bar{m} \in \mathbb{Z}_n$ 关于 $\mathbb{Z}_n$ 中乘法可逆

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

证：$\Rightarrow$ $\exists\ \bar{k} \in \mathbb{Z}_n$ 使得

$\bar{m}\,\bar{k} = \bar{1}$

即 $\overline{mk} = \bar{1}$ $\Rightarrow$ $mk \equiv 1 \bmod n$

$k \mid (mk - 1)$ $\Rightarrow$ $\exists\ l \in \mathbb{Z}$

使得 $mk - 1 = ln$

即 $km + (-l)n = 1$

由第一章定理 8.2. $\gcd(m, n) = 1$

"$\Leftarrow$" 由上述定理 $\exists\ a, b \in \mathbb{Z}$

使得 $am + bn = 1$

$\overline{am + bn} = \bar{1}$

$\bar{a}\bar{m} + \bar{b}\bar{n} = \bar{1}$ $\Rightarrow$ $\bar{a}\bar{m} = 1$.

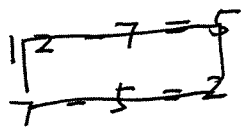
$\bar{m}$ 可逆

$\Rightarrow$ $\bar{m}\bar{a} = 1$.

例：列中 $\mathbb{Z}_{12}$ 中关于乘法的可逆元

$\bar{1}$, $\bar{5}$, $\bar{7}$ $\bar{11}$.

求 $\bar{7}$ 在 $\mathbb{Z}_{12}$ 中的逆



$12 = 7 + 5$

$7 = 5 + 2$

$5 = 2 \cdot 2 + 1$

$\bar{7} \cdot \bar{7} = \overline{49} = \overline{4 \times 12 + 1} = \overline{4 \times 12} + \bar{1} = \bar{1}$

在 $\mathbb{Z}_{15}$ 中 $\bar{2} \cdot \bar{8} = \overline{16} = \bar{1}$.

例：热带 加法：

$$\dot{+}: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a, b) \mapsto \max(a, b)$$

交换. 结合.

单位？ 设 $\widetilde{\mathbb{Z}} = \mathbb{Z} \cup \{-\infty\}$

$a \dot{+} (-\infty) = \max(a, -\infty) = a$.

回忆：命题 1.1. 设 $n \in \mathbb{Z}$, $n > 1$, $m \in \mathbb{Z}$

则 $\overline{m} \in \mathbb{Z}_n$ 关于 $\mathbb{Z}_n$ 中乘法可逆

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

证："$\Leftarrow$" $\gcd(m,n) = 1$

$\Rightarrow \exists u, v \in \mathbb{Z}$ 使得

$um + vn = 1$

$\Rightarrow \overline{um+vn} = \overline{1}$

$\because um + vn \equiv um \mod n$

$\therefore \overline{um+vn} = \overline{um}$

$\Rightarrow \overline{um} = \overline{1} \Rightarrow \overline{u}\,\overline{m} = \overline{1}$

$\Rightarrow \overline{m}$ 可逆

例：列出 $\mathbb{Z}_{15}$ 中关于乘法的可逆元 (8+)

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

求 $\overline{2}$ 的逆

$15 + 7 \cdot 2 = 1$

$\overline{15} + \overline{(-7)} \cdot \overline{2} = \overline{1}$ $\quad \overline{2}\,\overline{(-7)} = \overline{1}$

$\overline{(-7)}$ 是 $\overline{2}$ 的逆. $\overline{(-7)} = \overline{8}$.

例：热带加法：

$$\begin{aligned} \dot{+} : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\mapsto \max(a, b) \end{aligned}$$

交换，结合. 令 $\widetilde{\mathbb{Z}} = \mathbb{Z} \cup \{-\infty\}$

$$\begin{aligned} \dot{+} : \widetilde{\mathbb{Z}} \times \widetilde{\mathbb{Z}} &\longrightarrow \widetilde{\mathbb{Z}} \\ (a, b) &\mapsto \max(a, b) \end{aligned}$$

$a \dot{+} (-\infty) = -\infty \Rightarrow -\infty$ 为"加法"单位

$\dot{+}$ 中逆元只有 $-\infty$.

§2 群半群

§2.1 群半群的定义

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

例：$(\mathbb{Z}^+, +)$ 是半群，因为 "+" 定义在 $\mathbb{Z}^+$ 上

它是交换半群

定义：例：$S = \{A \in M_n(\mathbb{R}) \mid \det(A) > 1\}$

$(S, \cdot)$ 是半群

验证：$\cdot$ 封闭性：设 $A, B \in S$

$\det(AB) = \det(A)\det(B) > 1$

$\Rightarrow AB \in S$

$\Rightarrow \cdot$ 是 S 上的二元运算

结合律自然满足

定义：设 $(S, *)$ 是半群，如果 S 关于 $*$ 有单位元 e，则称 $(S, *, e)$ 是含么半群 (monoid)

例：$(\mathbb{Z}, +, 0)$ 是交换的含么半群

$(M_n(\mathbb{R}), \cdot, E)$ 是含么半群

例：设 S 是非空集合，

$S^S := \{f: S \to S \mid f \text{ 是映射}\}$

$(S^S, \circ, id)$ 是含么半群。

命题 2.1 设 $(S, *, e)$ 是含么半群，$x \in S$ 可逆，则 x 的逆唯一

证：设 y, z 是 x 的逆元

$yx = e$

$(yx)z = ez$

$y(xz) = z$ （结合律，单位元）

$y * e = z \Rightarrow y = z$ ☒

定义：设 $(G, *, e)$ 是含幺半群

如果 $\forall g \in G$，g 可逆，则称 $(G, *, e)$

是群 (Group)

例：$(\mathbb{Z}, +, 0)$ 是群（交换群，Abelian group）

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

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

验证：$(GL_n(\mathbb{R}), \cdot, E_n)$ 是群.

$A, B \in GL_n(\mathbb{R}) \Rightarrow AB$ 也可逆

（第二章 推论 5.2） $\Rightarrow AB \in GL_n(\mathbb{R})$

结合律，单位元和可逆自然可证.

思考

注：群 $\subset$ 含幺半群 $\subset$ 半群

群的等价定义：设 G 是非空集合

$*$ 是 G 上的二元运算

如果 (i) $\forall g_1, g_2, g_3 \in G$

$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$. (结合律)

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

$g * e = e * g = g$ (单位元)

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

$gh = hg = e$. (可逆)

则称 G 是群.

注：设 G 是群，$g \in G$

则 g 的逆唯一 (命题 2.1)

g 的逆记为 g^{-1}

注：设 $g, h \in G$

$(g*h)^{-1} = h^{-1} * g^{-1}$

验证：$(h^{-1} * g^{-1}) * (g * h)$

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

$= h^{-1} * (e * h) = h^{-1} * h = e$

自己验证 $(g*h)*(h^{-1}*g^{-1})=e$

例：X 非空集合

$T_X=\{f: X\to X \mid f$ 是双射$\}$

$(T_X, \circ, id)$ 是一个群，称为 X 上的变换群。这是因为双射的逆存在且仍是双射。

$(S_n, \cdot, e)$ 是群。

S_n 中以 $\{1,2,\cdots n\}$ 到 $\{1,2,\cdots n\}$ 的双射的集合

注 设 $(G,*,e)$ 是群，如果"$*$"满足交换律，则称 G 是交换群或阿贝尔群

如果 $\mathrm{card}(G)<\infty$，则称 G 是有限群，否则是无限群。$\mathrm{card}(G)$ 称为 G 的阶

例：$(\mathbb{Z}_n, +, \bar{0})$ 是 n 阶有限群

$(S_n, \cdot, e)$ 是 $n!$ 非交换群

$(\mathbb{Z}^{\mathbb{Z}}, +, 0)$ 是无穷阶交换群

$(M_n(\mathbb{R}), \bullet, E_n)$ 是 $\cdots$ 非交换群

引理 2.1 设 $(G,*,e)$ 是群，$a\in G$

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

都是双射

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

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

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

自己验证：$R_a\circ R_{a^{-1}}=R_{a^{-1}}\circ R_a=id$

例：1阶群

$G=\{e\}$

	e
e	e

实例：$(\{0\},+,0)$，$(\{1\},\times,1)$

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

但它们看上去是一回事儿

二阶 $G=\{e,a\}$

	e	a
e	e	a
a	a	e

$a^2=e$ 实例 $(\{1,-1\},\cdot,1)$

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

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

它们看上去是一回事儿

三阶 $G=\{e,a,b\}$

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

$ab=ba=e$，$a^2=b$，$b^2=a$

$b=a^2$，$a^3=e$

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

$a^3=e$

实例 $(\mathbb{Z}_3,+,\bar{0})=\{\bar{0},\bar{1},\bar{2}\}$ (12)

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

$\left(\{e,(123),(123)(123)\},\cdot,e\right)$

它们看上去是一回事儿吗？

四阶 $G=\{e,a,b,c\}$

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

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

$ab=ba=c$

$ac=ca=b$

$eb=bc=a$

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

$e=(\bar{0},\bar{0})$

$a=(\bar{1},\bar{0})$

$b=(\bar{0},\bar{1})$

$c=(\bar{1},\bar{1})$

$+:(\mathbb{Z}_2\times\mathbb{Z}_2)\times(\mathbb{Z}_2\times\mathbb{Z}_2)\to\mathbb{Z}_2\times\mathbb{Z}_2$

$((\bar{k},\bar{n}),(\bar{p},\bar{q}))\mapsto(\bar{k}+\bar{p},\bar{n}+\bar{q})$

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

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

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

$(\{1, -1, \sqrt{-1}, -\sqrt{-1}\}, \cdot, 1)$

$(\mathbb{Z}_4, +, \bar{0})$ 和 $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$

好像不是一回事儿.

实例：$G = (\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \}$

（依次记为 E_2，A，B，C）

$A^2 = B^2 = C^2 = E$

$AB = BA = C \quad AC = CA = B \quad CB = BC = A$

$(G, \cdot, E_2)$ 和 $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$

$(\mathbb{Z}_4, +, \bar{0})$ 和 $(\{1, -1, \sqrt{-1}, -\sqrt{-1}\}, \cdot, 1)$

是一回事.

§2.2 群同态和同构

定义：设 $(G, *, e)$，$(H, \star, \varepsilon)$ 是两个群：$\varphi: G \to H$ 称为是群同态

如果：$\forall\, g_1, g_2 \in G$

$$\varphi(g_1 * g_2) = \varphi(g_1) \star \varphi(g_2).$$

特别地 群同态

φ 是 $\begin{cases} \text{单射} \\ \text{满射} \\ \text{双射} \end{cases}$ 则称 φ 是(群) $\begin{cases} \text{单同态} \\ \text{满同态} \\ \text{同构.} \end{cases}$

引理 2.2（同态的基本性质）

设 $(G, *, e)$，$(H, \star, \varepsilon)$ 是两个群

$\varphi: G \to H$ 是群同态

则：(i) $\varphi(e) = \varepsilon$

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1} \quad (\forall g \in G)$

(iii) φ 是同构，则 φ^{-1} 也是

证: (i) $\varphi(e)=\varphi(e*e)=\varphi(e)\star\varphi(e)$

~~$\varphi(e)\neq\varphi(e)$~~

$\varphi(e)\star\varphi(e)^{-1}=\varphi(e)\star\varphi(e)\star\varphi(e)^{-1}$

$\varepsilon=\varphi(e)\star\varepsilon=\varphi(e)$

(ii) $\varepsilon=\varphi(e)=\varphi(g*g^{-1})$

$=\varphi(g)\star\varphi(g^{-1})$

$\varphi(g)^{-1}\star\varepsilon=\varphi(g)^{-1}\star\varphi(g)\star\varphi(g^{-1})$

$\varphi(g)^{-1}=\varphi(g^{-1})$

(iii) 设 $h_1,h_2\in H$. 则 $\exists!\ g_1,g_2\in G$

使得 $\varphi(g_1)=h_1\quad\varphi(g_2)=h_2$

$\varphi(g_1*g_2)=\varphi(g_1)\star\varphi(g_2)=h_1\star h_2$

$\varphi^{-1}(h_1\star h_2)=g_1*g_2=\varphi^{-1}(h_1)*\varphi^{-1}(h_2)$

于是 φ^{-1} 是群同态. 同时 φ^{-1} 是双射, 所以 φ^{-1} 是同构.

例: $\pi:\ \mathbb{Z}\longrightarrow\mathbb{Z}_n$

$a\longmapsto\bar{a}$

是 $(\mathbb{Z},+,0)$ 到 $(\mathbb{Z}_n,+,\bar{0})$ 的同态

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

例: 设 E 是偶数的集合 $(E,+,0)$ 也是群. 证明 $(\mathbb{Z},+,0)$ 和 $(E,+,0)$ 同构:

$\varphi:\ \mathbb{Z}\longrightarrow E$

$n\longmapsto 2n$

$\varphi(n+m)=2(n+m)$

$=2n+2m=\varphi(n)+\varphi(m)$

φ 显然是双射. …… 势相同

例: $(\mathbb{Z}_2,+,\bar{0})$ 与 $(\{-1,1\},\cdot,1)$

同构: $\varphi:\ \mathbb{Z}_2\longrightarrow\{-1,1\}$

$\bar{0}\longmapsto 1$

$\bar{1}\longmapsto -1$

$\varphi(\bar{0}+\bar{0})=\varphi(\bar{0})=1=1\cdot1=\varphi(\bar{0})\varphi(\bar{0})$

$\varphi(\bar{1}+\bar{0})=\varphi(\bar{1})=-1=(-1)\cdot1=\varphi(\bar{1})\varphi(\bar{0})$

$\varphi(\bar{1}+\bar{1})=\varphi(\bar{0})=1=(-1)(-1)=\varphi(\bar{1})\varphi(\bar{1})$

∴ $\mathbb{Z}_2$ 与交换群 ∴ 不需多验证

$\varphi(\bar{0}+\bar{1}) = \varphi(\bar{0})\,\varphi(\bar{1})$.

例：证明 $(\mathbb{Z}_2\times\mathbb{Z}_2, +, (\bar{0},\bar{0}))$ 与 $(\mathbb{Z}_4, +, \bar{0})$

不同构：

证明：反证：设 $\varphi: \mathbb{Z}_2\times\mathbb{Z}_2 \to \mathbb{Z}_4$

是同构，则 $\varphi((\bar{0},\bar{0})) = \bar{0}$

$\exists\ a \in \mathbb{Z}_2\times\mathbb{Z}_2$ 使得

$\varphi(a) = \bar{1}$

$\varphi(a+a) = \varphi(a)+\varphi(a) = \bar{1}+\bar{1} = \bar{2}$

$\forall\ a \in \mathbb{Z}_2\times\mathbb{Z}_2.\ a+a = (\bar{0},\bar{0})$

$\Rightarrow \varphi(a+a) = \bar{0} \Rightarrow \bar{0} = \bar{2}$ →← ☒

~~命题2.1 群同构~~

定义：设 $(G, *, e)$, $(H, \star, \varepsilon)$ 是两个群，如果存在 $\varphi: G \to H$ 是群同构，则称 G 和 H 同构，记为 $G \simeq H$.

引理2.3 设 $(G, *, e)$, $(H, \star, \varepsilon)$, $(K, \diamond, \lambda)$ 是三个群，

$\varphi: G \to H$, $\psi: H \to K$ 是群同态，则 $\psi\circ\varphi: G \to K$ 也是群同态.

证：设 $g_1, g_2 \in G$

$$\begin{aligned}\psi\circ\varphi(g_1 * g_2) &= \psi(\varphi(g_1 * g_2)) \\ &= \psi(\varphi(g_1)\star\varphi(g_2)) \\ &= \psi(\varphi(g_1)) \diamond \psi(\varphi(g_2)) \\ &= \psi\circ\varphi(g_1) \diamond \psi\circ\varphi(g_2).\end{aligned}$$

☒

命题2.1 群同构 "$\simeq$" 是等价关系

证：自反律，~~群同~~ 恒同映射是群同构

对称：引理2.2. (iii)

传递：引理2.3 和双射的复合仍是双射.

☒

群论基本问题：给定一类群
求这类群在"$\simeq$"下的等价类
并对每个等价类找出一个代表元。

例：一阶群：$(\{0\}, +, 0)$

$(\{0\}, +, 0) \simeq (\{1\}, \cdot, 1) \simeq \{\begin{pmatrix}1&0\\0&1\end{pmatrix}\}, \cdot, \begin{pmatrix}1&0\\0&1\end{pmatrix}\}$

二阶群

$(\mathbb{Z}_2, +, 0) \simeq (\{1,-1\}, \cdot, 1) \simeq (\{E_n, -E_n\}, \cdot, E_n)$

三阶群 $(\mathbb{Z}_3, +, 0)$ 是代表元（自己证）

四阶群：两个不同的同构类

$(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (\bar{0}, \bar{0}))$ 和 $(\mathbb{Z}_4, +, \bar{0})$

五阶群：都同构于 $(\mathbb{Z}_5, +, \bar{0})$。[以后证]

六阶群：有点麻烦。

例：$(\mathbb{Z}_6, +, \bar{0})$。 $S_3 = \{e, (12), (23), (13), (12)(23), (12)(13)\}$

不同构：因为 $\mathbb{Z}_6$ 是交换群

S_3 是非交换群

$[(12)(13) \neq (13)(12)]$

$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

记：设 $g \in G$，$n \in \mathbb{Z}^+$

$\underbrace{g^{-1} \cdots g^{-1}}_{n}$ 记为 g^{-n}.

当 $n=0$ 时 $g^n = e$.

自己验证：$\forall\, m, n \in \mathbb{Z}$

$g^{m+n} = g^m \cdot g^n$

当 $(G, +, 0)$ 是交换群时

$\forall\, n \in \mathbb{Z}^+$

$\underbrace{(-g) + \cdots + (-g)}_{n}$ 记为 $-ng$

自己验证 $\forall\, m, n \in \mathbb{Z}$

$(m+n)g = mg + ng$

结合律