

# 群论导引

Wang-Zhou Dai

## 1 引子

### 1.1 模 $m$ 剩余类与群的概念

回顾：模  $m$  同余是  $\mathbb{Z}$  上的一个等价关系。

$$a \equiv b \pmod{m} \leftrightarrow m \mid a - b$$

因此  $\mathbb{Z}/(\text{mod } m)$  包含  $m$  个等价类：

$$\begin{aligned} [0] &= \{x \mid x \equiv 0 \pmod{m}\} = \{km \mid k \in \mathbb{Z}\} \\ [1] &= \{x \mid x \equiv 1 \pmod{m}\} = \{km + 1 \mid k \in \mathbb{Z}\} \\ &\dots \\ [m-1] &= \{x \mid x \equiv m-1 \pmod{m}\} = \{km + (m-1) \mid k \in \mathbb{Z}\} \end{aligned}$$

同余模关系有如下性质：

**命题：**若  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ , 则

$$a + c \equiv c + d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

*Proof.* 根据定义，存在整数  $k, l$  使得

$$a - b = km, \quad c - d = lm$$

从而

$$\begin{aligned} (a + c) - (b + d) &= (a - b) + (c - d) = km + lm = (k + l)m, \\ ac - bd &= ac - bc + bc - bd = (a - b)c + (c - d)b = ck + bl)m. \end{aligned}$$

□

### 1.2 同构与同态

**定义：**我们称两个代数结构  $(S, *)$  与  $(S', *')$  **同构** (isomorphism) 当且仅当存在一个从  $S$  到  $S'$  的一一映射  $\phi$  使得

$$\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } x, y \in S$$

*homomorphism*

- 当没有一一映射条件时，上面的关系被称为**同态** (homomorphism)。
- 整数和加法、乘法构成的系统到模  $m$  剩余类与模  $m$  加法、乘法构成的系统，就构成一种同态。

#### 1.2.1 如何证明同构

对于两个代数结构  $(S, *)$  与  $(S', *')$ ，验证二者同构非常简单：

1. 定义映射  $\phi$ ，这个  $\phi$  一定要对于任意  $x \in S$  有定义；
2. 证明  $\phi$  是单射；
3. 证明  $\phi$  是满射；
4. 证明  $\phi$  保运算，即  $\phi(x * y) = \phi(x) *' \phi(y)$ 。

例子:  $(\mathbb{R}, +)$  与  $(\mathbb{R}^+, \cdot)$  同构。

1. 定义  $\phi(x) = e^x$ , 其定义域显然是满的;
2.  $\phi(x)$  显然是单射;
3.  $\phi(x)$  显然是满射;
4.  $\phi(x+y) = e^{(x+y)} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$ 。

### 1.2.2 如何证明不同构

例 1:  $(\mathbb{Q}, +)$  和  $(\mathbb{R}, +)$  不同构, 因为无法构造  $\mathbb{Q} \rightarrow \mathbb{R}$  的一一映射。

例 2:  $(\mathbb{Z}, \cdot)$  和  $(\mathbb{Z}^+, \cdot)$  不同构。虽然它们的基数都等于  $\aleph_0$ , 但在  $\mathbb{Z}$  中有两个元素令  $x \cdot x = 0$ , 在  $\mathbb{Z}^+$  中只有一个元素满足该条件 (注意到乘法是一样的), 所以不可能构建出保运算的一一映射函数。

所以, 代数结构更本质的是其内部结构的性质:

结构性性质 (structural property)	非结构性性质
集合有 4 个元素	集合里有 4
代数运算具有交换性	代数运算叫做“加法”
$x * x = x, \forall x \in S$	$S$ 中的元素都是方阵
$a * x = b$ 对任意 $a, b \in S$ 有解	$S \subset \mathbb{C}$

这类结构性性质才是抽象代数研究的主要对象。

## 2 群

### 2.1 代数方程求解

在代数系统中解方程:

$$\begin{aligned}
 5 + x &= 2 && \text{(given)} \\
 -5 + (5 + x) &= -5 + 2 && \text{(addition)} \\
 (-5 + 5) + x &= -5 + 2 && \text{(association)} \\
 0 + x &= -5 + 2 && \text{(inverse element)} \\
 x &= -5 + 2 && \text{(identity element)} \\
 x &= -3 && \text{(addition)}
 \end{aligned}$$

### 2.2 群的定义

定义: 设  $G$  是一个非空集合。如果在  $G$  上定义了一个代数运算 (通常称为乘法), 且满足:

1.  $\forall_{a,b,c \in G} [(ab)c = a(bc)]$
2.  $G$  中有一个元素  $e$  使得

$$\forall_{a \in G} (ea = ae = a)$$

称  $e$  为  $G$  的**单位元** (identity element)。

3.  $G$  中每个元素均存在**逆元** (inverse), 即

$$\forall_{a \in G} \exists_{b \in G} (ab = ba = e)$$

我们记  $b = a^{-1}$ 。

那么称  $(G, *)$  是一个群 (Group)。

- 如果只满足性质 1, 称为**半群** (semigroup);
- 如果满足性质 1, 2, 称为**含么半群**或者**独异点** (monoid);
- 注意: 虽然单位元和逆元对于乘法满足交换律, 但其他情况下不一定可交换;

如果群  $G$  的乘法还满足交换性

$$\forall_{a,b \in G} (ab = ba)$$

那么称  $(G, *)$  为**交换群**或**阿贝尔群** (Abelian group)。

- 同样的, 有交换半群和交换含么半群。

### 2.3 一些群的例子

- $n$  次单位根 ( $n^{\text{th}}$  roots of unity) 群 (见参考书目)。
- 模  $m$  的剩余类加上模  $m$  加法构成群  $(\mathbb{Z}_m, +_m)$ , 注意  $[a + b] = [a] + [b]$ 。
  1.  $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = ([a] + [b]) + [c]$
  2.  $[a] + [0] = [0] + [a] = [a]$
  3.  $[a] + [m - a] = [m] = [0]$
  4.  $[a] + [b] = [a + b] = [b + a] = [b] + [a]$
- $n \times n$  可逆方阵在矩阵乘法下构成群, 但没有可交换性:
  1. 矩阵乘法满足结合律;
  2. 可逆矩阵的乘积依然可逆, 因此有封闭性:  $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$ ;
  3. 单位元为  $I_n$ ;
  4. 有逆元;
- 模  $m$  的剩余类中与  $m$  互素的剩余类 (即约剩余系) 加上模  $m$  乘法构成阿贝尔群  $(\mathbb{Z}_m^*, *_m)$ 。

**定理 1:** 在  $\mathbb{Z}_m$  中,  $[a]$  是模  $m$  乘法可逆元当且仅当  $(a, m) = 1$ 。

*Proof.* ( $\Leftarrow$ ) 设  $(a, m) = 1$ , 则存在  $u, v \in \mathbb{Z}$ , 使得

$$au + mv = 1.$$

根据模  $m$  加法和乘法性质, 在  $\mathbb{Z}_m$  中

$$[1] = [a][u] +_m [m][v] = [a][u]$$

因此  $[u]$  就是  $[a]$  的逆元。

( $\Rightarrow$ ) 设  $[a]$  是可逆元, 其中  $0 < a < m$ 。假如  $(a, m) = d$  且  $d \neq 1$ 。则存在正整数  $0 < a_1, m_1 < m$  使得:

$$a = a_1d, m = m_1d$$

从而

$$am_1 = a_1dm_1 = a_1m$$

所以在  $\mathbb{Z}_m$  中有  $[a][m_1] = [a_1m] = [0]$ 。根据上面的假设,  $[a]$  是可逆元, 给左边等式两边同时左乘 (why?)  $[a]^{-1}$ :

$$[a]^{-1}([a][m_1]) = [a]^{-1}[0]$$

左边为  $([a]^{-1}[a])[m_1] = [1][m_1] = [m_1]$ ; 右边为  $[a]^{-1}[0] = [0]$ , 得到  $[m_1] = [0]$ , 与  $0 < m_1 < m$  矛盾。  $\square$

### 2.4 群的基本性质

**定理 2:** 若  $(G, *)$  是群, 那么它一定满足左右**消去律**, 即对任意  $a, b, c \in G$  有  $a * b = a * c \rightarrow b = c$  且  $b * a = c * a \rightarrow b = a$  成立。

*Proof.* 假设  $a * b = a * c$ , 由逆元存在性可知存在  $a'$  使得  $a * a' = a' * a = e$ , 其中  $e$  为  $(G, *)$  的单位元。

因此可以在  $a * b = a * c$  两边左乘  $a'$  得到  $b = e * b = a' * a * b = a' * a * c = e * c = c$ 。同理可证  $b * a = c * a \rightarrow b = a$ 。  $\square$

**定理 3:** 若  $(G, *)$  是群, 那么其中的线性方程  $a * x = b$  一定有唯一解。

**定理 4:** 若  $(G, *)$  是群, 那么它的单位元唯一, 且每个元素的逆元唯一, 且  $(a^{-1})^{-1} = a$ 。

**推论:** 若  $(G, *)$  是群, 那么对任意  $a, b \in G$  有  $(a * b)^{-1} = b^{-1} * a^{-1}$ 。

**例子:** 若  $(G, *)$  关于乘法满足结合律, 且  $G$  有左逆和左单位元, 求证  $G$  是群。

*Proof.* 由于有左单位和左逆, 所以  $\forall a \in G$  存在  $a^{-1}a = e_L$ 。且对  $a^{-1}$  有  $(a^{-1})^{-1}a^{-1} = e_L$ 。因此

$$aa^{-1} = e_L(aa^{-1}) = [(a^{-1})^{-1}a^{-1}](aa^{-1}) = (a^{-1})^{-1}(a^{-1}a)a^{-1} = (a^{-1})^{-1}e_La^{-1} = (a^{-1})^{-1}a^{-1} = e_L$$

因此  $a^{-1}$  也是右逆。同时

$$ae_L = a(a^{-1}a) = (aa^{-1})a = e_La$$

所以  $e_L$  也是右单位。因此  $G$  是群。 □

## 3 循环群

### 3.1 幂运算和阶

令  $a^n$  表示  $a * a * \dots * a$  共  $n$  个  $a$  相乘, 并规定

$$a^0 = e, a^{-n} = (a^{-1})^n, n \in \mathbb{N}^*$$

(一般  $\mathbb{Z}^+, \mathbb{R}^+$  表示正整数、实数;  $\mathbb{N}^*, \mathbb{Z}^*, \mathbb{R}^*$  表示不包含零的自然数、正整数、正实数集合)。

容易验证

$$a^m a^n = a^{m+n}, (a^m)^n = a^{mn}, m, n \in \mathbb{Z}$$

$G$  中元素的个数被称为它的**阶** (order), 接下来我们会看到为什么。

### 3.2 循环群与生成元

在模 9 即约剩余系群  $\mathbb{Z}_9^* = \{[1], [2], [4], [5], [7], [8]\}$  中

$$[2]^0 = [1], [2]^1 = [2], [2]^2 = [4], [2]^3 = [8], [2]^4 = [7], [2]^5 = [5].$$

因此

$$\mathbb{Z}_9^* = \{[2]^r \mid r = 0, 1, \dots, 5\}.$$

**定义:** 若  $(G, *)$  是群, 且  $G$  中的每一个元素都能写成  $G$  中某个元素  $a$  的整数次幂, 那么称  $G$  为**循环群** (cyclic group), 我们把  $a$  叫做  $G$  的一个**生成元** (generator), 并把  $G$  记为  $\langle a \rangle$ 。

- 若对任意  $n \in \mathbb{N}^*$  都有  $a^n \neq e$ , 则  $\langle a \rangle$  为如下无限循环群:

$$\{\dots, a^{-n}, \dots, a^{-1}, e, a, \dots, a^n, \dots\}$$

- 若存在某个  $n \in \mathbb{N}^*$  使得  $a^n = e$ , 则  $\langle a \rangle$  为  $n$  阶循环群:

$$\{e, a, \dots, a^{n-1}\}$$

- 循环群一定是阿贝尔群 (为什么?)。
- 在循环群中, 使得  $a^n = e$  的最小的正整数  $n \in \mathbb{N}^*$  被称为  $a$  的阶, 记作  $|a|$ 。例如 1 在  $(\mathbb{Z}, +)$  中为无穷阶元素;  $(\mathbb{Z}_9^*, *)$  中,  $[2]$  的阶为 6。

### 3.3 循环群的结构

**定义:** 如果群  $(G, *)$  到  $(G', *')$  有一个双射  $\sigma$ , 使得

$$\sigma(ab) = \sigma(a)\sigma(b), \forall a, b \in G,$$

那么称  $\sigma$  是  $(G, *)$  到  $(G', *')$  的一个群同构映射, 并称二者是同构的, 记作  $(G, *) \simeq (G', *')$ 。以后在不产生歧义的情况下我们简单记  $(G, *)$  和  $(G', *')$  为  $G$  和  $G'$ , 以及  $G \simeq G'$ 。

**定理 5:** 设  $\sigma$  是  $G$  到  $G'$  的同构映射, 则

1.  $\sigma(e) = e'$ ;
2.  $\sigma(a^{-1}) = \sigma(a)^{-1}, \forall a \in G$ ;
3.  $a$  与  $\sigma(a)$  阶相同。

*Proof.* (1)  $\sigma(e) = \sigma(ee) = \sigma(e)\sigma(e)$ , 记  $e'$  为  $G'$  的单位元, 则  $\sigma(g)\sigma(g)^{-1} = \sigma(g)^{-1}\sigma(g) = e'$ 。

对  $\sigma(e) = \sigma(e)\sigma(e)$  两边左乘  $\sigma(e)^{-1}$  得

$$e' = \sigma(e)^{-1}\sigma(e) = \sigma(e)^{-1}\sigma(e)\sigma(e) = e'\sigma(e) = \sigma(e)$$

得到  $e' = \sigma(e)$ 。

(2) 由于  $aa^{-1} = e$ , 因此  $\sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1}) = \sigma(e) = e'$ , 两边同时左乘  $\sigma(a)^{-1}$  得  $\sigma(a^{-1}) = \sigma(a)^{-1}$ 。

(3)  $\forall n \in \mathbb{N}^*$ , 由于  $\sigma$  是单射, 因此

$$a^n = e \Leftrightarrow \sigma(a^n) = e' \Leftrightarrow [\sigma(a)]^n = e'.$$

□

那么, 所有循环群组成的集合  $\Omega$  有多少个同构等价类?

**定理 6:**

1. 任意一个无限循环群都与  $(\mathbb{Z}, +)$  同构;
2. 对于  $m \in \mathbb{N}^*$ , 任意一个  $m$  阶循环群与  $(\mathbb{Z}_m, +_m)$  同构;
3. 1 阶循环群都与加法群  $\{0\}$  同构。

*Proof.* 1. 略。对于  $G = \langle a \rangle$ , 只需构造映射  $\sigma: G \rightarrow \mathbb{Z}$  为  $\sigma(a^k) = k$ , 并分布证明其为单射、满射且保运算即可。

2. 设  $G = \langle a \rangle$  为  $m$  阶循环群, 其中  $m > 1$ , 则

$$G = \{e, a, \dots, a^{m-1}\}$$

令

$$\begin{aligned} \tau: G &\rightarrow (\mathbb{Z}_m, +_m) \\ a^k &\mapsto [k], 0 \leq k < m. \end{aligned}$$

由于当  $0 \leq k, l < m$  时,  $a^k = a^l \Leftrightarrow k = l \Leftrightarrow [k] = [l]$ , 所以  $\tau$  是一个映射, 且是单射。任给  $[k] \in \mathbb{Z}_m$ , ( $0 \leq k < m$ ), 存在  $\tau(a^k) = [k]$ , 因此  $\tau$  是满射。从而  $\tau$  是双射。

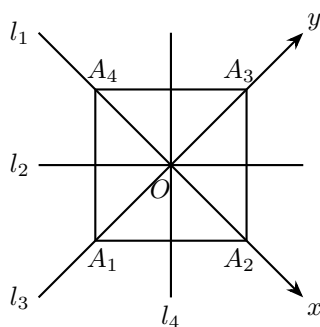
对于  $0 \leq k < m$ , 设  $k + l = qm + r$  ( $0 \leq r < m$ ), 则在  $\mathbb{Z}_m$  中,  $[k + l] = [r]$ 。由于  $G = \langle a \rangle$  的阶为  $m$ , 因此  $a$  的阶为  $m$ 。于是有

$$\tau(a^k a^l) = \tau(a^{k+l}) = \tau(a^{qm+r}) = \tau(a^r) = [r] = [k + l] = [k] +_m [l].$$

因此,  $\tau$  是一个从  $G$  到  $(\mathbb{Z}_m, +_m)$  的同构映射。

3. 显然  $\{e\} \simeq (\{0\}, +)$ 。

□



从上面的定理可以看到：

- 所有的无限循环群组成一个同构类，代表元为  $(\mathbb{Z}, +)$ ；
- 所有的  $m$  阶循环群组成一个同构类，代表元为  $(\mathbb{Z}_m, +_m)$ 。

## 4 二面体群

### 4.1 对称变换

**定义：**平面上（或空间中）的一个变换  $\sigma$  如果保持任意两点的距离不变，那么称  $\sigma$  是平面上（或空间中）的一个**正交点变换**（或保距变换）(isometry)。

- 显然，任意两个正交点变换的乘积仍然是正交点变换；
- 正交点变换的逆变换仍然是正交点变换。

**定义：**平面上（或空间中）的一个正交点变换  $\sigma$  如果让图形  $\Gamma$  的像与自身重合，那么称  $\sigma$  是  $\Gamma$  的**对称变换**。

### 4.2 图形对称群

如果把一个图形  $\Gamma$  的所有对称变换组成的集合叫做  $G$ 。那么，

- $G$  中任意两个对称变换的组合仍然是  $\Gamma$  的对称变换，即  $\forall \sigma_1, \sigma_2 \in G (\sigma_2 * \sigma_1 \in G)$ ；
- $\forall \sigma \in G$  有  $\sigma^{-1} \in G$ ；
- 显然，对称变换满足结合律；

所以这些变换构成一个群，我们称  $(G, *)$  为  $\Gamma$  **图形的对称群** (symmetric group)。

### 4.3 正方形的对称群

正方形的对称运算集合记作  $D_4$  它含有以下元素：

- 绕正方形中心  $O$  转角为  $\pi/2$  的旋转，记作  $\sigma$ ；
- 绕正方形中心  $O$  转角为  $\pi$  的旋转，记作  $\sigma^2$ ；
- 绕正方形中心  $O$  转角为  $3\pi/2$  的旋转，记作  $\sigma^3$ ；
- 绕正方形中心  $O$  转角为  $2\pi$  的旋转，记作  $\sigma^4 = I$ ；
- 关于  $l_1$  的反射，记作  $\tau_1$ ；
- 关于  $l_2$  的反射，记作  $\tau_2$ ；
- 关于  $l_3$  的反射，记作  $\tau_3$ ；
- 关于  $l_4$  的反射，记作  $\tau_4$ 。

因此有：

$$D_4 \supseteq \{I, \sigma, \sigma^2, \sigma^3, \tau_1, \tau_2, \tau_3, \tau_4\}$$

那么,  $D_4$  中还有没有其他运算? 它们是否满足封闭性? 是否构成一个群? (提示: 考虑上图的直角坐标系与旋转矩阵, 将  $\tau_i, i = 2, 3, 4$  用  $\tau_1$  和  $\sigma$  的乘积表示)

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

事实上,

$$D_4 = \{I, \sigma, \sigma^2, \sigma^3, \tau_1, \sigma\tau_1, \sigma^2\tau_1, \sigma^3\tau_1\}.$$

可以看出,  $D_4$  可以由两个元素  $\sigma$  和  $\tau_1$  生成, 且

$$\sigma^4 = I, \tau_1^2 = I.$$

由于  $(\sigma\tau_1)^2 = \tau_2^2 = I$ , 将  $(\sigma\tau_1)(\sigma\tau_1) = I$  两边左乘  $\sigma^{-1}$  得

$$\tau_1\sigma\tau_1 = \sigma^{-1}$$

有了已上公式, 任意两个元素的乘积都能计算出来, 例如:

$$\begin{aligned} \tau_1\sigma &= \sigma^{-1}\tau_1 = \sigma^3\tau_1 \\ (\sigma^2\tau_1)\sigma^3 &= \sigma^2(\tau_1\sigma)\sigma^2 = \sigma^2(\sigma^3\tau_1)\sigma^2 = \sigma(\tau_1\sigma)\sigma = \sigma(\sigma^3\tau_1)\sigma = \sigma^4(\tau_1\sigma) = \sigma^3\tau_1 \end{aligned}$$

因此,  $D_4$  有两个生成元  $\{\sigma, \tau_1\}$ , 我们记  $\tau_1 = \tau$ , 可以把  $D_4$  简洁地写成

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = I, \tau\sigma\tau = \sigma^{-1} \rangle.$$

其中的  $\sigma^4 = \tau^2 = I$  表明了  $\sigma$  和  $\tau$  自身的性质, 而  $\tau\sigma\tau = \sigma^{-1}$  可以被用来计算  $\tau$  和  $\sigma$  的乘积.

设正  $n$  边形中心为  $O$ , 用  $\sigma$  表示绕点  $O$  转角为  $2\pi/n$  的旋转, 用  $\tau$  表示关于正  $n$  边形的某条对称轴的反射, 则正  $n$  边形的对称群  $D_n$  为

$$D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = I, \tau\sigma\tau = \sigma^{-1} \rangle.$$

由于  $\tau\sigma = \sigma^{-1}\tau = \sigma^{n-1}\tau \neq \sigma\tau$ , 因此  $D_n$  是非阿贝尔群, 它们被称为**二面体群** (dihedral group).

上节课提到的**四元数群**同样可以用类似的方式表示出来:

$$Q = \langle i, j \mid i^4 = j^4 = I, iji = i^{-1} \rangle.$$

## 5 对称群

### 5.1 置换表示

除了图形的对称性, 还可以刻画其他事务的对称性. 考虑一元二次方程

$$ax^2 + bx + c = 0,$$

它的两个复根  $x_1, x_2$  满足

$$x_1 + x_2 = -b, x_1x_2 = c,$$

可以看到它们之间存在着某种对称性. 记  $\Omega = \{x_1, x_2\}$ , 令

$$\sigma: \Omega \rightarrow \Omega$$

$$x_1 \mapsto x_2$$

$$x_2 \mapsto x_1$$

此时仍然有  $x_2 + x_1 = -b, x_2x_1 = c$ , 因此形式化地描述了这一对称性: 对它们进行置换后, 运算结果保持不变. 我们可以将它表示为:

$$\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

同样的, 上面的  $D_4$  也可以表示为下面的形式:

$$\begin{aligned} I &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} & \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\ \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & \sigma^2\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\ \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} & \sigma^3\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \end{aligned}$$

**定义:** 当  $\Omega$  为有穷集合时,  $\Omega$  到自身的一个双射叫做  $\Omega$  上的一个**置换** (permutation)。

## 5.2 对称群的定义

令  $\Omega$  是一个非空集合,  $S_\Omega$  是  $\Omega$  上所有的置换 (这是一个  $\Omega \rightarrow \Omega$  的函数), 那么  $S_\Omega$  在函数复合运算  $\circ$  下构成群, 它被称为**对称群** (symmetry group), 它的子集被称为**置换群** (permutation group)。

*Proof.* 首先, 证明封闭性: 集合  $\Omega$  上两个置换  $\sigma, \tau$  的复合  $\sigma \circ \tau$  是如下映射:

$$\Omega \xrightarrow{\tau} \Omega \xrightarrow{\sigma} \Omega$$

由于  $\sigma$  和  $\tau$  都是双射, 因此  $\sigma\tau$  仍然是一个双射。

其次, 证明结合性: 由二元关系的结合性易得。

第三, 证明单位元存在: 恒等置换  $I$  使得  $\forall a \in \Omega (I(a) = a)$ , 所以对任意置换  $\sigma$  和任意  $a \in \Omega$  有  $I \circ \sigma(a) = I(\sigma(a)) = \sigma(a)$ , 且  $\sigma \circ I(a) = \sigma(I(a)) = \sigma(a)$ 。

最后, 证明对任意一个置换  $\sigma$  均存在其逆元  $\sigma^{-1}$ 。由于  $\sigma$  是  $\Omega$  上的双射, 因此反函数  $\sigma^{-1}$  必然存在, 且对任意  $a \in \Omega$  满足  $\sigma^{-1}(\sigma(a)) = \sigma(\sigma^{-1}(a)) = a$ , 即  $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = I$ 。

综上所述,  $S_\Omega$  构成一个群。 □

## 6 子群

从群的运算表中可以看出, 表中的内容实际上就是集合元素的一种重新排列。因此, 直觉上可以想像出置换群存在着某种结构上的一般性, 而凯莱定理就描述了这种一般性。为了介绍它, 我们首先要引入一个定义和一条引理。

**定义:** 令  $A \rightarrow B$  是一个函数, 且  $H$  是  $A$  的一个子集。我们定义  $f[H] = \{f(h) \mid h \in H\}$  为  $f$  在  $H$  上的像(image)。

**定义:** 如果  $G$  是一个群,  $H \subseteq G$  对于  $G$  中的运算封闭 (子代数) 且构成群, 那么称  $H$  是  $G$  的一个**子群** (subgroup), 记为  $H \leq G$  ( $H < G$  当  $H \neq G$ )。  $G$  自身和  $\{e\}$  被称为  $G$  的**平凡子群** (trivial subgroup), 其余的子群被称为**真子群** (proper subgroup)。

- 如果  $H$  是  $G$  的一个子群, 那么任意  $a, b \in H$  有  $ab \in H$ 。设  $e' \in H$  是  $H$  的单位元, 则  $e'e' = e'$ 。两边再同时乘以  $e'$  在  $G$  中的逆元得到  $e' = (e')^{-1}e'$ , 即  $e' = e$ 。因此子群  $H$  中的单位元就是  $G$  中的单位元。
- 任给  $b \in H$ , 设  $b$  在  $H$  中的逆元为  $b'$ , 则  $bb' = b'b = e$ 。该式在  $G$  中同样成立, 所以  $b$  在  $G$  中的逆元也是  $b'$ 。

**引理:** 令  $G$  和  $G'$  是群, 并令  $\phi: G \rightarrow G'$  是一个单射函数, 使得对任意  $x, y \in G$  有  $\phi(xy) = \phi(x)\phi(y)$ 。那么  $\phi[G]$  是  $G'$  的一个**子群**, 且  $\phi$  是  $G$  到  $\phi[G]$  的一个同构映射。

*Proof.* 首先, 证明  $\phi[G]$  的封闭性: 显然, 对于任意  $x', y' \in \phi[G]$  存在  $x, y \in G$  使得  $\phi(x) = x'$  且  $\phi(y) = y'$ , 且  $\phi(xy) = \phi(x)\phi(y) = x'y'$ , 说明  $x'y' \in \phi[G]$ 。

其次, 根据  $\phi$  的性质,  $\phi[G]$  中的运算显然满足结合律。

第三, 令  $e'$  表示  $\phi[G]$  中的单位元。那么有:

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e),$$

根据群运算的消去律, 得到  $e' = \phi(e)$ 。

第四, 证明任意  $x \in \phi[G]$  有逆元: 假设  $x' = \phi(x)$ , 那么有

$$e' = \phi(e) = \phi(x^{-1}x) = \phi(xx^{-1}) = \phi(x^{-1})\phi(x) = \phi(x)\phi(x^{-1}) = \phi(x^{-1})x' = x'\phi(x^{-1})$$



因此  $\phi(x^{-1})$  是  $x'$  的逆。因此  $\phi[G]$  是  $G'$  的子群。

最后, 由于  $\phi$  是单射, 因此  $\phi$  构成  $G \rightarrow \phi[G]$  的双射, 是二者之间的同构映射。□

## 7 凯莱定理

**定理 7 (Cayley's Theorem):** 任意一个群都与一个置换群同构。

*Proof.* 令  $G$  为一个群, 我们证明  $G$  与  $S_G$  的一个子群同构。根据上面的引理, 我们只需定义一个函数  $\phi: G \rightarrow S_G$  使得对于任意  $x, y \in G$  有  $\phi(xy) = \phi(x)\phi(y)$ 。

给定一个  $x \in G$ , 我们构造一个映射  $\lambda_x: G \rightarrow G$ , 使得对任意  $g \in G$  有  $\lambda_x(g) = xg$  (即对  $g$  左乘一个  $x$ ), 下面证明它是一个置换。

因为  $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$  对任意  $c \in G$  成立, 所以  $\lambda_x$  对  $G$  是映上的 (即一个满射)。又因为  $\lambda_x(a) = \lambda_x(b) \leftrightarrow xa = xb \leftrightarrow a = b$ , 所以  $\lambda_x$  是一个单射。所以  $\lambda_x$  是  $G$  上的一个置换 ( $G \rightarrow G$  的双射)。令  $\phi: G \rightarrow S_G$  为  $\phi(x) = \lambda_x, \forall x \in G$ 。

接下来需要证明  $\phi$  是一个从  $G$  到  $\phi[G]$  双射 (根据上面的引理, 只需要证明单射即可), 且保持  $G$  中的运算。

由于  $\phi(x) = \phi(y) \leftrightarrow \lambda_x = \lambda_y$  (注意这二者是函数) 在  $G$  中处处成立, 所以有  $\lambda_x(e) = \lambda_y(e) \leftrightarrow xe = ye \leftrightarrow x = y$ 。因此  $\phi$  是单射。

根据  $\phi$  的定义有  $\phi(xy) = \lambda_{xy}$ , 那么对于任意  $g \in G$  有  $\phi(xy)(g) = \lambda_{xy}(g) = xyg = x(yg) = x[\lambda_y(g)] = [\lambda_x\lambda_y](g)$  (置换的乘法即为函数复合运算), 因此  $\phi$  保运算。□

在证明中, 我们同样可以考虑由右乘诱导出的置换运算  $\rho_x(g) = gx$ , 甚至可以通过逆元诱导:  $\mu_x(g) = gx^{-1}$ 。关于凯莱定理的例子见 Fraleigh 的 83 页例 8.18。

## 8 子群和陪集

### 8.1 子群判定条件

**定理 8:** 群  $G$  的非空子集  $H$  是  $G$  的子群当且仅当对任意  $\forall a \forall b (a, b \in H \rightarrow ab^{-1} \in H)$ 。

*Proof.* ( $\Rightarrow$ ) 由于  $H < G$  是群, 所以  $a, b \in H \subseteq G$  意味着  $b^{-1} \in H$  且  $H$  对  $G$  中的乘法运算封闭, 因此  $ab^{-1} \in H$ 。

( $\Leftarrow$ ) 单位元存在: 由于  $H$  非空, 因此存在  $c \in H$ 。由已知条件得  $cc^{-1} \in H$ , 因此  $e \in H$ 。

逆元存在: 任给  $b \in H$ , 由已知条件 (其中的  $a$  替换为  $e$ ) 得  $eb^{-1} \in H$ , 因此  $b^{-1} \in H$ 。

\*  $\downarrow_H$  (乘法在  $H$  中的限制) 的结合律: 任给  $a, b \in H$ , 由已知条件和已证明的结论得  $a(b^{-1})^{-1} \in H$ , 即  $ab \in H$ 。因此  $H$  中的运算仍然保持  $G$  中的运算 (乘法表不变)。由于  $G$  是群, 因此该运算在  $H$  中依然满足结合律。□

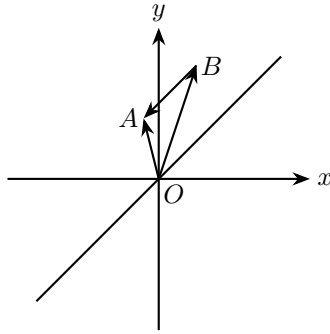
### 8.2 群的划分

子群可以用来研究群的结构, 一种最直接的方式就是利用子群  $H < G$  来构造  $G$  的一个划分。

考虑一个实数平面向量集合与向量加法构成的群  $G = (\mathbb{R}^2, +)$ , 穿过原点  $O$  的一条直线  $y = hx$  即是  $G$  中的一个子群, 我们记为  $H = \{(x, hx) \mid x \in \mathbb{R}\}$  (这里的  $h$  是一个  $\mathbb{R}$  上的常数), 它在向量加法上显然构成一个群:

- 封闭性: 对  $H$  中任意  $(x_1, hx_1)$  和  $(x_2, hx_2)$  有  $(x_1, hx_1) + (x_2, hx_2) = (x_1 + x_2, h(x_1, x_2)) \in H$ ;
- 结合律: 由实数加法结合律自然得出;
- 单位元: 易证  $(0, 0)$  是  $H$  中的单位元;

- 逆元: 对任意  $(x, hx) \in H$  易证  $(-x, -hx) \in H$  是其单位元。



从图中可以看到, 当  $A \notin H$  且  $\overrightarrow{OA} - \overrightarrow{OB} \in H$  时,  $A$  和  $B$  恰好位于一个与  $H$  平行的直线上。

这条与  $H$  平行的直线可以记为  $H' = \{(x, hx + b) \mid x \in \mathbb{R}\}$ , 其中  $h$  与  $H$  的斜率一样,  $b \neq 0$  是一个常数。容易验证  $H'$  也是  $G$  的一个子群。

我们记这里的  $\overrightarrow{OA} = a$ ,  $\overrightarrow{OB} = b$ , 向量加法为群的乘法 “ $*$ ” (无歧义时可省略)。这样一来, “ $\overrightarrow{OA}$  与  $\overrightarrow{OB}$  的差与  $H$  平行” 可以记为  $ab^{-1} \in H$ , 并且由它可以推出  $a$  和  $b$  属于同一个子群  $H'$ , 即同一个划分。根据划分与等价类的关系, 我们可以得到一种等价关系, 这可以表示为一条定理。

### 8.3 子群和等价类

**定理 8:** 若  $G$  为一个群, 且  $H < G$ 。那么  $G$  中存在等价关系  $\sim_L$  和  $\sim_R$ 。对任意  $a, b \in G$ , 它们的定义如下:

$$\begin{aligned} a \sim_L b &\leftrightarrow a^{-1}b \in H, \\ a \sim_R b &\leftrightarrow ab^{-1} \in H. \end{aligned}$$

*Proof.* 不失一般性, 这里只证明  $\sim_L$  是等价关系。

自反性: 根据  $H$  是子群有  $e \in H$ 。所以  $e \in H \leftrightarrow a^{-1}a \in H \leftrightarrow a \sim_L a$ 。

对称性: 根据  $H$  是子群有  $b^{-1}a = (a^{-1}b)^{-1} \in H$ 。所以  $a \sim_L b \leftrightarrow a^{-1}b \in H \leftrightarrow (a^{-1}b)^{-1} \in H \leftrightarrow b^{-1}a \in H \leftrightarrow b \sim_L a$ 。

传递性: 根据  $H$  是子群有  $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}c$ 。所以  $(a \sim_L b \wedge b \sim_L c) \leftrightarrow (a^{-1}b \in H \wedge b^{-1}c \in H) \leftrightarrow (a^{-1}b)(b^{-1}c) \in H \leftrightarrow a^{-1}c \in H \leftrightarrow a \sim_L c$ 。  $\square$

有了上述等价关系, 当给定一个子群  $H < G$  (例如  $\mathbb{R}^2$  的一条直线  $L$ ) 和任意一个  $a \in G$  时 (例如  $\mathbb{R}^2$  上的一个点  $A$ ), 其等价类 (例如过点  $A$  与  $L$  平行的直线) 即为:

$$[a] = \{x \in G \mid x \sim_L a\} = \{x \in G \mid a^{-1}x \in H\} = \{x \in G \mid a^{-1}x = h, h \in H\} = \{x \in G \mid x = ah, h \in H\} = \{ah \mid h \in H\}$$

同理可以得到  $\sim_R$  生成的等价类  $[a] = \{ha \mid h \in H\}$ 。

### 8.4 陪集

**定义:** 令  $H$  为  $G$  的子群。我们称集合  $aH = \{ah \mid h \in H\}$  为  $H$  关于  $a$  的左陪集 (left coset),  $Ha = \{ha \mid h \in H\}$  为  $H$  关于  $a$  的右陪集 (right coset),  $a$  为陪集代表元。 $H$  的所有左 (右) 陪集组成的集合是  $G$  的一个划分, 称为  $G$  关于子群  $H$  左 (右) 商集, 分别记做  $(G/H)_l$  和  $(G/H)_r$ 。

**命题:**  $a \in bH \leftrightarrow b^{-1}a \in H \leftrightarrow aH = bH$ 。

*Proof.*

$$a \in bH \leftrightarrow \exists h \in H (a = bh) \leftrightarrow \exists h \in H (b^{-1}a = h) \leftrightarrow b^{-1}a \in H$$

所以根据  $a \in bH$ , 存在  $h \in H$  使得  $b = ah^{-1}$  和  $a = bh$ , 那么存在  $h_1 \in H$  使得  $ah_1 = bhh_1 = b(hh_1)$ , 而由于  $h, h_1 \in H$  且  $H$  是子群 (关于乘法封闭), 所以  $hh_1 \in H$ , 因此得到任意  $ah = b(hh_1) \in bH$ , 根据集合包含关系定义有  $aH \subseteq bH$ . 同理可得

$$bh_2 = ah^{-1}h_2 \in aH \leftrightarrow bH \subseteq aH$$

因此  $aH = bH$ . □

**命题:** 左陪集与右陪集的基数相等。

*Proof.* 令

$$\begin{aligned} \sigma : (G/H)_r &\rightarrow (G/H)_l \\ aH &\rightarrow Ha^{-1} \end{aligned}$$

由于  $aH = cH$  说明  $c \sim_L a$ , 即  $c^{-1}a \in H$ , 这又等价于  $c^{-1}(a^{-1})^{-1} \in H$ , 因此有  $c^{-1} \sim_R a^{-1}$ , 即  $Hc^{-1} = Ha^{-1}$ , 因此  $\sigma$  是单射。

又因为任给  $Hb \in (G/H)_r$ , 有  $\sigma(b^{-1}H) = H(b^{-1})^{-1} = Hb$ , 所以  $\sigma$  是满射。

因此  $\sigma$  是双射, 且  $|(G/H)_l| = |(G/H)_r|$ . □

由这个命题可以引出以下概念:

**定义:** 设  $H$  是群  $G$  的一个子群, 把  $(G/H)_l$  或  $(G/H)_r$  的基数称为  $H$  在  $G$  中的**指数** (order), 记为  $[G : H]$ 。

## 9 拉格朗日定理

**命题:** 若  $H$  是  $G$  的子群, 那么  $G$  关于  $H$  的任意左、右陪集均和  $H$  等势, 即  $\forall a \in G (|H| = |aH| = |Ha|)$ 。

*Proof.* 构造映射  $\tau : H \rightarrow aH$ , 令  $\tau(h) = ah$ . 根据  $h_1 = h_2 \leftrightarrow ah_1 = ah_2$  可知其为单射; 且对于  $\forall ah \in aH$  有  $\tau(a^{-1}ah) = \tau(h) = ah$ , 所以它也是满射。因此  $\tau$  是  $H$  与  $aH$  间的双射。 □

由上面这些性质与定义, 可以得到下面这个简洁且重要的结论 (Never underestimate results that counts something!)

**定理 9:** 令  $H$  为一个有限群  $G$  的子群, 则

$$|G| = [G : H] \cdot |H|$$

*Proof.* 设  $[G : H] = r$ , 那么  $G$  的一个划分可以表示为:

$$G = H \cup a_1H \cup \cdots \cup a_{r-1}H,$$

其中  $H, a_1H, \dots, a_{r-1}H$  两两不相交。因此有

$$|G| = |H| + |a_1H| + \cdots + |a_{r-1}H| = |H| + |H| + \cdots + |H| = r|H|.$$

□

### 9.1 拉格朗日定理的应用

设  $G$  是有限群,  $a \in G$ . 设  $a$  的阶为  $s$ . 令

$$H = \{e, a, a^2, \dots, a^{s-1}\}$$

任给  $0 \leq i, j < s$ , 不妨设  $i \leq j$ , 我们有

$$a^i(a^j)^{-1} = a^{i-j} = a^{-(j-i)} = a^{s-(j-i)} \in H$$

$$a^j(a^i)^{-1} = a^{j-i} \in H$$

因此  $H$  是  $G$  的一个子群, 称  $H$  是由  $a$  生成的子群, 记作  $\langle a \rangle$ 。由  $H$  的定义可知,  $a$  的阶就是  $\langle a \rangle$  的阶。

**推论 1:** 设  $G$  是有限群, 则  $G$  的任一元素  $a$  的阶是  $G$  的阶的因数, 从而  $a^{|G|} = e$ 。

**推论 2:** 任意素数阶群一定是循环群。

*Proof.* 假设  $|G| = p$ , 且  $p$  为素数。令  $a \neq e$  为  $G$  中的一个非单位元。那么由  $a$  生成的子群  $H$  至少应该包括  $a$  和  $e$ 。然而根据拉格朗日定理,  $|H|$  可整除  $|G|$ 。因此当  $|H| \geq 2$  必有  $|H| = |G|$  且  $\langle a \rangle = G$ , 所以  $\langle a \rangle$  是循环群 (且  $a$  的阶为  $p$ )。□

### 9.1.1 欧拉定理和费马小定理

利用上面的推论, 可以给出欧拉定理和费马小定理的一个简短证明。

**欧拉定理:** 设  $m$  是大于 1 的整数, 若整数  $a$  与  $m$  互素, 则

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

*Proof.* 由于  $(a, m) = 1$ , 因此  $[a] \in \mathbb{Z}_m^*$ 。由于  $|\mathbb{Z}_m^*| = \varphi(m)$ , 因此由推论 1 得  $[a]^{\varphi(m)} = [1]$ 。

根据模  $m$  乘法的保运算性质, 有  $[a^{\varphi(m)}] = [1]$ , 即  $a^{\varphi(m)} \equiv 1 \pmod{m}$ 。□

**费马小定理:** 设  $p$  是素数, 则对于任意整数  $a$  有

$$a^p \equiv a \pmod{m}.$$

*Proof.* 若  $(a, p) = 1$ , 则根据欧拉定理得

$$a^{p-1} \equiv 1 \pmod{p}.$$

又有  $a \equiv a \pmod{p}$ , 根据模  $m$  乘法的性质将其与上式相乘, 有  $a^p \equiv a \pmod{p}$ 。□

### 9.1.2 循环群的结构

**定理 10:** 设  $G = \langle a \rangle$  是  $n$  阶循环群, 则

1.  $G$  的每一个子群都是循环群;
2. 对于  $G$  的阶  $n$  的每一个正因数  $s$ , 都存在唯一的一个  $s$  阶子群。除它们以外,  $G$  再也没有其他子群。

*Proof.* (1) 由于  $G$  的平凡子群  $\{e\}$  和  $G$  都是循环群, 所以只需证明  $G$  的任一非平凡子群都是循环群。

设  $H$  是  $G$  的非平凡子群, 则  $H$  中有  $G$  的非单位元。根据良序定理, 在  $H$  中存在幂指数最小的  $a$  的幂, 设为  $a^k$ , 其中  $k \neq 0$ 。任取  $a^q \in H$ , 设  $q = lk + r$ ,  $0 \leq r < k$ 。根据陪集等价类的定义, 有

$$a^r = a^{q-lk} = a^q (a^k)^{-l} \in H$$

如果  $r \neq 0$ , 那么  $r < k \wedge a^r \in H$  与  $a^k$  是  $H$  中  $a$  的最小幂元矛盾, 因此  $r = 0$ 。从而

$$a^q = (a^k)^l \in \langle a^k \rangle$$

由于对任意  $a^q \in H$  都有  $a^q \in \langle a^k \rangle$ , 故而  $H \subseteq \langle a^k \rangle$  (全称量词引入)。又由生成群的封闭性可知  $\langle a^k \rangle \subseteq H$ , 所以  $H = \langle a^k \rangle$ 。

因此  $G$  的所有子群都是循环群。

(2) 由 Lagrange 定理可知  $G$  的所有子群的阶均为  $n$  的因数。因此证明该命题只需证  $G$  的  $s$  阶子群存在且唯一, 其中  $s$  是  $n$  的因数。

设  $s$  是  $G$  的阶  $n$  的任意一个正因数, 则存在正整数  $d$  使得  $n = ds$ 。由于  $a$  的阶亦为  $n$ , 因此

$$|a^d| = \frac{n}{(n, d)} = \frac{n}{d} = s$$

于是  $\langle a^d \rangle$  是  $G$  的一个  $s$  阶子群, 存在性得证。

设  $H$  是  $G$  的任意一个  $s$  阶子群, 根据 (1) 的结论,  $H$  是循环群。设  $H = \langle a^k \rangle$ , 于是  $|a^k| = \frac{n}{(n,k)}$  (为什么?), 因此  $(n,k) = d$ , 因此存在整数  $u, v$  使得

$$un + vk = d,$$

于是

$$a^d = a^{un} a^{vk} = (a^k)^v \in \langle a^k \rangle = H$$

所以  $\langle a^d \rangle \subseteq H$ 。又由于  $|\langle a^d \rangle| = s = |H|$ , 所以  $\langle a^d \rangle = H$ 。这证明了  $G$  的  $s$  阶子群唯一。  $\square$

由上面的结论很容易可以得到:

**推论 3:** 若  $a$  是有限循环群  $G$  的生成元, 且  $|G| = n$ 。那么  $G$  的其他生成元是  $a^r$ ,  $(n,r) = 1$ 。

若  $r$  与  $n$  不互素,  $a^r$  生成出来的只能是  $G$  的子群。例如  $\mathbb{Z}_{18}$  的生成元有  $\{1, 5, 7, 11, 13, 17\}$ , 而

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\} \subset \mathbb{Z}_{18}.$$

[定理 10 的证明过程中用到的关于阶的引理如下]

**引理:** 设  $G$  是群, 且  $|a| = n$ , 则:

1. 对于正整数  $m$ , 有  $a^m = e \leftrightarrow n \mid m$ ;
2.  $\forall k \in \mathbb{N}^*$  有

$$|a^k| = \frac{n}{(n,k)}$$

*Proof.* (1) 设  $m = hn + r$ ,  $0 \leq r < n$ , 则

$$a^m = a^{hn} a^r = e a^r = a^r$$

由于  $a$  的阶为  $n$ , 所以  $a^m = e \leftrightarrow a^r = e \leftrightarrow r = 0 \leftrightarrow m = hn \leftrightarrow n \mid m$ 。

(2) 设  $a^k$  的阶为  $s$ , 则

$$e = (a^k)^s = a^{ks}$$

由于  $a$  的阶为  $n$ , 根据 (1) 中的结论有  $n \mid ks$ 。从而

$$\frac{n}{(n,k)} \mid \frac{k}{(n,k)} s.$$

由于  $(\frac{n}{(n,k)}, \frac{k}{(n,k)}) = 1$ , 因此  $\frac{n}{(n,k)} \mid s$ 。

欲证  $s \mid \frac{n}{(n,k)}$ , 考虑

$$(a^k)^{\frac{n}{(n,k)}} = (a^n)^{\frac{k}{(n,k)}} = e^{\frac{k}{(n,k)}} = e$$

所以, 根据 (1) 的结论有  $s \mid \frac{n}{(n,k)}$ , 得到  $s = \frac{n}{(n,k)}$ 。  $\square$

### 9.1.3 四阶群的同构类

根据 Lagrange 定理, 任给四阶群  $G$  (因数为 2 和 4), 则  $G$  中非单位元的阶只可能是 2 和 4。

**情形 1:**  $G$  中有 4 阶元, 则  $G = \langle a \rangle$ , 从而  $G \simeq (\mathbb{Z}_4, +)$ ;

**情形 2:**  $G$  中没有 4 阶元, 则  $G$  的三个非单位元  $a, b, c$  的阶均为 2, 即  $a = a^{-1} \wedge b = b^{-1} \wedge c = c^{-1}$ , 且  $ab \neq e$  (否则  $a = b^{-1} = b$ , 矛盾);  $ab \neq a$  (否则  $b = e$ , 矛盾);  $ab \neq b$  (否则  $a = e$ , 矛盾)。因此  $ab = c$ , 同理  $ba = c$ 。由于  $a, b, c$  是对称的, 所以还有  $ac = b = ca, bc = a = cb$ , 从而  $G$  是 Abel 群。令

$$\begin{aligned}\sigma: G &\rightarrow (\mathbb{Z}_2 \oplus \mathbb{Z}_2, +) \\ e &\mapsto ([0], [0]) \\ a &\mapsto ([0], [1]) \\ b &\mapsto ([1], [0]) \\ c &\mapsto ([1], [1])\end{aligned}$$

则  $\sigma$  是  $G$  到  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$  的一个双射。我们有

$$\sigma(ab) = \sigma(c) = ([1], [1]) = ([0], [1]) + ([1], [0]) = \sigma(a) + \sigma(b)$$

同理有

$$\sigma(ac) = \sigma(b) = ([1], [0]) = ([0], [1]) + ([1], [1]) = \sigma(a) + \sigma(c)$$

$$\sigma(bc) = \sigma(a) = ([0], [1]) = ([1], [0]) + ([1], [1]) = \sigma(b) + \sigma(c)$$

还有

$$\begin{aligned}\sigma(ea) &= \sigma(a), \dots \\ \sigma(a^2) &= \sigma(a) + \sigma(a) = \sigma(e), \dots\end{aligned}$$

因此  $\sigma$  是  $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$  的一个同构映射。综上所述, 四阶群只有两个同构类, 一个是模 4 加法群, 一个是  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ , 即 Klein four group。

## 10 商群、群同态基本定理

**定义:** 若群  $G$  到  $G'$  有一个映射  $\sigma: G \rightarrow G'$  使得

$$\sigma(ab) = \sigma(a)\sigma(b),$$

则称  $\sigma$  是群  $G$  到  $G'$  的一个同态映射 (homomorphism), 根据映射的种类可以定义满同态 (满射) 和同构 (双射)。

### 10.1 同态的基本性质

我们记  $G'$  中的元素比  $G$  中多一个单引号:

$$1. \sigma(e) = e'$$

$$a' = \sigma(a) = \sigma(ae) = \sigma(a)\sigma(e) = a'e'$$

$$2. \sigma(a^{-1}) = (a')^{-1}$$

$$e' = \sigma(e) = \sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1}) = a'\sigma(a^{-1}) \Rightarrow (a')^{-1} = \sigma(a^{-1})$$

3.  $G$  的子群  $H$  在  $\sigma$  下的像  $\sigma[H]$  也是  $G'$  的子群, 我们有时也记为  $\text{Im}G$

- 证明凯莱定理时的引理;

4. 若  $a \in G$  且  $a^n = e$ , 则  $(\sigma(a))^n = (a')^n = e'$ 。也就是说, 若  $a$  是  $G$  的  $n$  阶元, 则  $\sigma(a)$  的阶一定是  $n$  的因数。

$$e' = \sigma(e) = \sigma(a^n) = (\sigma(a))^n$$

### 10.2 核以及核的性质

**定义:** 设  $\sigma: G \rightarrow G'$  是一个同态, 则  $G'$  的单位元  $e'$  在  $G$  中的原像称为  $\sigma$  的核 (kernel), 记作  $\text{Ker}\sigma$ , 即

$$\text{Ker}\sigma = \{a \in G \mid \sigma(a) = e'\}.$$

核有如下性质:

**命题 1:** 若  $\sigma$  是  $G$  到  $G'$  的同态, 则  $\text{Ker}\sigma$  是  $G$  的一个子群。

*Proof.* 由于  $\sigma(e) = e'$ , 所以  $e \in \text{Ker}\sigma$ .

任意  $a, b \in \text{Ker}\sigma$  有  $\sigma(ab^{-1}) = \sigma(a)\sigma(b) = e'e' = e'$ . 于是  $ab^{-1} \in \text{Ker}\sigma$ , 所以  $\text{Ker}\sigma < G$ .  $\square$

**命题 2:** 若  $\sigma$  是  $G$  到  $G'$  的同态, 则  $\sigma$  是单射当且仅当

$$\text{Ker}\sigma = \{e\}$$

*Proof.* ( $\Leftarrow$ ) 设  $\sigma$  是单射, 则  $\forall a \in G (a \neq e \rightarrow \sigma(a) \neq e')$ , 因此  $\text{Ker}\sigma = \{e\}$ .

( $\Rightarrow$ ) 设  $\text{Ker}\sigma = \{e\}$ . 若  $a, b \in G$  使得  $\sigma(a) = \sigma(b)$ , 则  $\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = e'$ , 即  $ab^{-1} \in \text{Ker}\sigma$ . 由于  $\text{Ker}\sigma = \{e\}$ , 所以  $ab^{-1} = e$ , 即  $a = b$ . 因此  $\sigma$  是单射.  $\square$

**例子:** 设  $\sigma$  是  $G$  到  $G'$  的同态, 则  $\forall a \in G$  有

$$a(\text{Ker}\sigma) = (\text{Ker}\sigma)a.$$

*Proof.* 对  $\forall a \in G, \forall k \in \text{Ker}\sigma$  有

$$\sigma(aka^{-1}) = \sigma(a)\sigma(k)\sigma(a^{-1}) = a'e'(a')^{-1} = a'(a)^{-1} = e'$$

所以  $aka^{-1} \in \text{Ker}\sigma$ , 有  $ak = (aka^{-1})a \in (\text{Ker}\sigma)a$ . 故而  $a(\text{Ker}\sigma) \subseteq (\text{Ker}\sigma)a$ .

另一方面, 对任意  $k \in \text{Ker}\sigma$  有

$$\sigma(a^{-1}ka) = \sigma(a^{-1})\sigma(k)\sigma(a) = (a')^{-1}e'a' = (a)^{-1}a' = e'$$

即  $a^{-1}ka \in \text{Ker}\sigma$ , 所以有  $ka = a(a^{-1}ka) \in a(\text{Ker}\sigma)$ . 于是又有  $a(\text{Ker}\sigma) \supseteq (\text{Ker}\sigma)a$ .  $\square$

### 10.3 正规子群

上面这类子群被称为**正规子群** (Normal subgroup).  $H$  是正规子群的定义为:  $\forall a \in G$  有  $aH = Ha$ , 记作  $H \triangleleft G$ . 由上面的例子可知, 当  $\sigma$  是  $G \rightarrow G'$  的同态时,  $\text{Ker}\sigma \triangleleft G$ . 同样地,  $\{e\}$  也是  $G$  的 (平凡) 正规子群.

- 正规子群

**例子:** 证明  $H \triangleleft G \Leftrightarrow (\forall a \in G (aHa^{-1} = H))$ .

*Proof.*  $\forall a \in G$  有

$$\begin{aligned} aH = Ha &\Leftrightarrow (aH)a^{-1} = (Ha)a^{-1} \\ &\Leftrightarrow aHa^{-1} = H(aa^{-1}) \\ &\Leftrightarrow aHa^{-1} = H \end{aligned}$$

$\square$

**例子:** 证明若  $H < G$ , 且对任意  $a \in G, h \in H$  有  $aha^{-1} \in H$  则  $H \triangleleft G$ .

*Proof.* 对任意  $a \in G, h \in H$  有  $aha^{-1} \in H$ , 所以  $aHa^{-1} \subseteq H$ .

同理, 对  $a \in G, h \in H$  还有  $a^{-1}H(a^{-1})^{-1} \subseteq H$ , 即  $a^{-1}Ha \subseteq H$ .

那么我们就有  $a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1}$ , 即  $(aa^{-1})H(aa^{-1}) \subseteq aHa^{-1}$ , 所以有  $H \subseteq aHa^{-1}$ .

最终得到  $\forall a \in G (aHa^{-1} = H)$ , 即  $H \triangleleft G$ .  $\square$

**例子:** 证明若  $H < G$ , 且  $[G : H] = 2$ , 则  $H \triangleleft G$ .

*Proof.* 因为  $[G : H] = 2$ , 根据 Lagrange 定理,  $\exists a_1, a_2 \in G (a_1 \notin H \wedge a_2 \notin H)$  使得  $G$  存在两个划分:

$$G = H \cup a_1H \wedge G = H \cup Ha_2$$

因此  $a_1H = Ha_2$ , 得到  $a_1 \sim a_2$ , 故而可以用一个代表元  $a \sim a_1 \sim a_2$  代替. 因此有  $aH = Ha$ , 即  $H \triangleleft G$ .  $\square$

## 10.4 商群

Galois 发现正规子群对研究群的结构起着重要的作用。若  $N \triangleleft G$ , 则  $(G/N)_l = (G/N)_r$ , 记作  $G/N$ 。在  $G/N$  中我们规定运算

$$(aN) * (bN) = abN$$

若  $aN = cN$ ,  $bN = dN$ , 即  $a \sim c \wedge b \sim d$ , 则根据子群判定定理有  $c^{-1}a \in N \wedge d^{-1}b \in N$ , 从而

$$(cd)^{-1}(ab) = d^{-1}c^{-1}ab \in d^{-1}Nb$$

而由于  $N$  是正规子群, 所以有  $Nb = bN$ , 因此  $(cd)^{-1}(ab) \in d^{-1}Nb = d^{-1}bN = N$ , 因此  $(cd)N = (ab)N$ 。这表明  $(aN) * (bN)$  这两个陪集的乘法运算与代表元的选择无关, 因此运算的定义是合理的, 而且  $N$  的所有陪集关于该运算构成群。

*Proof.* 交换律:

$$\begin{aligned} [(aN)(bN)](cN) &= (abN)(cN) = [(ab)c]N, \\ (aN)[(bN)(cN)] &= (aN)(bcN) = [a(bc)]N = [(ab)c]N. \end{aligned}$$

单位元为  $N$  自身:

$$N(aN) = (eN)(aN) = eaN = aN, (aN)N = (aN)(eN) = aeN = aN$$

$aN$  的逆元为  $a^{-1}N$ :

$$(aN)(a^{-1}N) = aa^{-1}N = eN = N, (a^{-1}N)(aN) = a^{-1}aN = eN = N$$

□

所以, 若  $N \triangleleft G$ , 则  $G/N$  关于上面的运算构成一个群, 我们称它为  $G$  关于  $N$  的**商群** (quotient group)。

**命题:** 设  $G$  为有限群,  $N \triangleleft G$ , 则  $|G/N| = \frac{|G|}{|N|}$ 。

*Proof.* 根据 Lagrange 定理,  $|G| = [G : N]|N|$ , 因此  $|G/N| = [G : N] = \frac{|G|}{|N|}$ 。 □

**定理 11:** 设  $N$  是群  $G$  的一个正规子群, 令

$$\begin{aligned} \pi : G &\rightarrow G/N \\ a &\mapsto aN, \end{aligned}$$

则  $\pi$  是群  $G$  到商群  $G/N$  的一个满同态, 并且  $\text{Ker}\pi = N$ 。我们把  $\pi$  称为  $G$  的**自然同态** (natural homomorphism)。

*Proof.* 显然  $\pi$  是  $G$  到  $G/N$  的一个映射, 且  $\pi$  是满射。由于

$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b),$$

因此它是一个满同态, 又由于

$$x \in \text{Ker}\pi \Leftrightarrow \pi(x) = N \Leftrightarrow xN = N \Leftrightarrow x \in N$$

所以有  $\text{Ker}\pi = N$ 。 □

该定理表明, 若  $N$  是群  $G$  的正规子群, 则商群  $G/N$  是群  $G$  在自然同态下的像 ( $\text{Im}\pi$ ), 并且正规子群是自然同态的核。

再回到二元实数坐标系  $\mathbb{R}^2$  与过原点直线子群的例子。不失一般性, 我们假设该子群为  $N = \{(x, 0) \mid x \in \mathbb{R}\}$  ( $x$  轴), 并且能够构造一个从  $\mathbb{R}^2$  到  $N$  的同态 ( $x$  轴投影映射):

$$\begin{aligned} \sigma : \mathbb{R} &\rightarrow N \\ (a, b) &\mapsto (a, 0), \end{aligned}$$



很容易验证该同态满足保运算的性质，且  $\text{Im}\sigma = N$ 。但  $\sigma$  不是同构，因为它不是一一映射。由于  $N$  上关于加法的单位元为  $(0, 0)$ ，所以  $\text{Ker}\sigma = \{(0, b) \mid b \in \mathbb{R}\}$ ，即  $y$  轴。

同时， $\text{Ker}\sigma$  显然是一个正规子群，因为  $(a, b) + (0, \mathbb{R}) = (a, \mathbb{R} + b) = (a, b + \mathbb{R}) = (0, \mathbb{R}) + (a, b) = (a, \mathbb{R})$ 。

根据上面的定理 11，我们能够得到一个商群  $\mathbb{R}^2/\text{Ker}\sigma = \{(a, \mathbb{R}) \mid a \in \mathbb{R}\}$ ，并构造一个自然同态：

$$\begin{aligned}\pi : \mathbb{R} &\rightarrow \mathbb{R}/\text{Ker}\sigma \\ (a, b) &\mapsto (a, \mathbb{R}),\end{aligned}$$

明显，这个商群由平面上所有与  $y$  轴平行的直线组成，而且这个商群中的每个元素（直线）对应于  $N$  上的一个元素。受此启发，我们可以得到下面这条定理。

## 10.5 群同态基本定理

**定理 12 (Fundamental Theorem of Homomorphism in Groups):** 设  $\sigma$  是  $G \rightarrow G'$  的同态映射，则  $\text{Ker}\sigma$  是  $G$  的一个正规子群，且

$$G/\text{Ker}\sigma \simeq \text{Im}\sigma$$

*Proof.* 前面已证  $\text{Ker}\sigma \triangleleft G$ ，因此只需证明后面的部分。令

$$\begin{aligned}\psi : G/\text{Ker}\sigma &\rightarrow \text{Im}\sigma \\ a(\text{Ker}\sigma) &\mapsto \sigma(a)\end{aligned}$$

由于

$$\begin{aligned}a(\text{Ker}\sigma) = b(\text{Ker}\sigma) &\Leftrightarrow b^{-1}a \in \text{Ker}\sigma \Leftrightarrow \sigma(b^{-1}a = e') \\ &\Leftrightarrow \sigma(b^{-1})\sigma(a) = e' \Leftrightarrow \sigma(a) = \sigma(b)\end{aligned}$$

因此  $\psi$  是  $G/\text{Ker}\sigma$  到  $\text{Im}\sigma$  的映射，且它是单射。从  $\psi$  的定义可看出它是满射，所以它是双射。又由于

$$\begin{aligned}\psi[a(\text{Ker}\sigma)b(\text{Ker}\sigma)] &= \psi[ab(\text{Ker}\sigma)] = \sigma(ab) = \sigma(a)\sigma(b) \\ &= \psi[a(\text{Ker}\sigma)]\psi[b(\text{Ker}\sigma)]\end{aligned}$$

所以  $\psi$  是一个同构映射。 □

同态基本定理是抽象代数里**最基本**的定理之一 (FUNDAMENTAL!)。它的作用在于，如果想研究一个代数  $G'$  的结构，但我们对它知之甚少，这时便会带来许多麻烦。另一方面，我们对代数  $G$  有着较深刻的认识。此时，只要构造一个同态映射  $\sigma : G \rightarrow G'$  并找到  $\text{Ker}\sigma$ ，我们便可以在  $G$  的内部通过  $G/\text{Ker}\sigma$  研究  $G'$  的结构。因此“同构基本定理”不仅仅属于群论，它存在于所有的代数系统中，在代数几何、范畴论、代数拓扑等许多现代数学领域中都有着极大的作用，是用来帮助数学家探索未知，建立“未知与已知”之间联系的重要数学工具。下面是知乎一个答主关于同态基本定理在（泛函）分析和线性代数两个领域中如何体现的回答。



Phenomene Bizarre  
Lie theory and representations

+ 关注

专业 已有 2 人赠与了专业徽章 >

235 人赞同了该回答

如同YFan所说，可以从一般的Category角度定义Kernel，因此，只要是学代数类的课程，在教科书里都会遇到同态基本定理，比如Lie代数，抽象代数<sup>Q</sup>，表示论，高等代数。最初进入我们视线的，我想并非是群的同态基本定理<sup>Q</sup>，而应该是高等代数里线性空间<sup>Q</sup>范畴里的同态基本定理。我想在这个回答里说一说线性空间的同态基本定理。

最初学的时候我没发现，但后来回味的时候，发现线性空间的同态定理还是很有意思的，实际上它等价于线性方程组<sup>Q</sup>的解的结构定理。

考虑线性方程组 $AX=Y$ 的解，这里 $X \in \mathbb{R}^m$ ,  $Y \in \mathbb{R}^n$ , 是列向量,  $A$ 是系数矩阵<sup>Q</sup>, 那么这个方程组如果有解，则解的结构一定是某个特解加上对应的齐次方程组<sup>Q</sup>的解的形式，即一定是 $X_0 + T, T \in Ker A$ 的形式。如果你对商空间<sup>Q</sup>比较熟悉的话，这个解实际上是 $\mathbb{R}^m / Ker A$ 里的一个元素。如果你仔细想一想，这个解的结构定理实际上说的是： $\mathbb{R}^m / Ker A$ 和 $Im A$ 里的元素有一个1-1对应。

反之，抽象的线性空间同态定理<sup>Q</sup>可以通过取基底转化成线性方程组的求解问题。

2018年7月6日更新

之前举了个线性代数的例子，再举个微积分的例子。这个例子是在美国教微积分习题课的时候，琢磨出来的。当时有个同学问“为什么算不定积分的时候，后面要有个+C”。如果你憋着一肚子坏水儿，不怕低评价，不怕学生恨你的话，你可以按如下方式解释：

设 $C^1(\mathbb{R})$ 是定义在整个实数轴上所有一阶连续可微函数<sup>Q</sup>的集合，这是一个线性空间。那么通常意义下的求导数 $D = \frac{d}{dx} : C^1(\mathbb{R}) \rightarrow C^0(\mathbb{R})$ 就是一个线性映射<sup>Q</sup>。我们称一个函数 $f$ 是可积的，如果这个函数是某个函数的导数，换句话说 $f \in Im D$ （在这个例子里，像空间实际上就是所有连续函数<sup>Q</sup>，因为连续函数都可积嘛）。那么由第一同构定理<sup>Q</sup>，我们有 $C^1(\mathbb{R}) / Ker D \cong Im D$ ，这个同构映射<sup>Q</sup>的逆映射实际上就是求原函数<sup>Q</sup>。换句话说，一个函数的原函数是商空间 $C^1(\mathbb{R}) / Ker D$ 里的一个元素，作为商空间里的元素，我们通常习惯把它们写成陪集的形式，即 $F + Ker D$ 的形式，然后稍加思考，你就会发现 $Ker D = C$ ，正好就是常函数构成的一维子空间。所以，最后的结果就写成某个函数加上常数的形式了。

类似问题还有：“为什么某些类型的常微分方程<sup>Q</sup>的解一定是某个特解加上通解的形式？”诸如此类问题，你都可以这么解释。这是我刚到美国的时候，上助教课，觉得学生问的问题好无聊，触景生情琢磨出来的。当然了，我并没有这么去教他们。

编辑于 2019-02-24 00:37