近世代数

计算机科学与技术学院
苏敬勇

内容

第二章 群

- 群同态与同构的简单性质
- 正规子群和商群
- 群同态基本定理
- 群的同构定理
- 群的自同构群
- *Sylow定理
- *有限交换群

群同态与同构的简单性质

- 第一章中研究的同态、同构是在“代数系统”意义下进行的，我们希望通过群了解与其他代数系统，或者通过不同群的比较了解更多群里的结构和性质。。。
- “群之间的同态映射”---“同态映射” $\varphi: G \to \bar{G}$ $\varphi(ab)=\varphi(a)\varphi(b)$
- “群同态”---“同态” $G \sim \bar{G}$
- “群之间的同构映射”---“同构映射” $G \cong \bar{G}$
- “自同态映射”---“自同态” $\varphi: G \to G$ $\varphi(ab)=\varphi(a)\varphi(b)$
- “自同构映射”---“自同构” $\varphi: G \to G$ $\varphi(ab)=\varphi(a)\varphi(b)$

群同态与同构的简单性质

- **定理1：** 设G是一个群，$\bar{G}$ 是一个有代数运算（也称为乘法）的集合。如果 $G \sim \bar{G}$，则 $\bar{G}$也是一个群。

证明：首先，$\bar{G}$ 中乘法满足结合律。

其次，检查单位元和逆元。

设e是群G的单位元，$\bar{a}$ 是$\bar{G}$的一个元素，又设φ 是 G 到 $\bar{G}$ 的满同态，且在φ 之下

$$e \to \bar{e}, \quad a \to \bar{a}$$

于是

$$ea \to \bar{e} \cdot \bar{a}$$

但是$ea = a$，故 $\bar{e} \cdot \bar{a} = \bar{a}$，即 $\bar{e}$是 $\bar{G}$ 的单位元。

又设 $a^{-1} \to \overline{a^{-1}}$，则 $a^{-1}a \to \overline{a^{-1}}\,\bar{a}$

但是$a^{-1}a = e$，故 $\overline{a^{-1}}\,\bar{a} = \bar{e}$，即 $\overline{a^{-1}}$是 $\bar{a}$的逆元。

因此，$\bar{G}$ 也是一个群。

群同态与同构的简单性质

- **注：**本定理中的同态映射φ必须为满射。反例：设G为正有理数乘群,$\bar{G}$ 是全体正偶数对$a \circ b = 2$作成的半群。则有

$$\varphi : x \to 2 \qquad (\forall x \in G)$$

显然为G到$\bar{G}$的同态映射（但不是满射）。G是群，但$\bar{G}$并不是群。

- **推论：**设 φ 是群G到群$\bar{G}$ 的一个同态映射（不一定是满射）。则群G的单位元的像是群$\bar{G}$的单位元，G的元素a的逆元的像是a的像的逆元。即

$$\overline{a^{-1}} = \bar{a}^{-1} \quad \text{或} \quad \varphi(a^{-1}) = \varphi(a)^{-1}$$

- **注：**如果集合G与$\bar{G}$ 各有一个代数运算，且$G \sim \bar{G}$ ，则当$\bar{G}$ 为群时，G却不一定为群。

- **例1：**令G=｛全体正负奇数｝，代数运算为数的普通乘法；又$\bar{G} = \{1, -1\}$关于数的普通乘法作成群，令

$$\varphi : \text{正奇数} \to 1, \quad \text{负奇数} \to \text{-}1$$

易知φ是G到$\bar{G}$ 的同态满射,$G \sim \bar{G}$,$\bar{G}$是群，但G却不是群。

群同态与同构的简单性质

- **注：若G与 $\bar{G}$ 为各有一个代数运算的代数系统，且$G \cong \bar{G}$，则当G与$\bar{G}$ 中有一个是群时，另一个必然也是群。**
- **例2**：证明：$\bar{G}=\{0,1,2,3\}$ 对代数运算

$$a \circ b = r \qquad (r\text{为}a+b\text{用4除所得的余数})$$

作成一个群。

证明：令Z是整数加群，易知

$$\varphi: x \to x' \qquad (\forall x \in Z)$$

是Z到$\bar{G}$ 的一个同态满射，其中 x' 为整数 x 用4除所得余数。

由于Z是群，故由定理1知，$\bar{G}$ 也是群。

群同态与同构的简单性质

- **定理2**：设φ是群G到群$\bar{G}$的一个同态映射（不一定是满射），则

1）当$H \le G$时，有$\varphi(H) \le \bar{G}$，且$H \sim \varphi(H)$；

2）当$\bar{H} \le \bar{G}$时，有$\varphi^{-1}(\bar{H}) \le G$，且在$\varphi$之下诱导出$\varphi^{-1}(\bar{H})$到$\bar{H}$的一个同态映射。

证明：1）任取$\bar{a},\bar{b} \in \varphi(H)$，且在$\varphi$之下令

$$a \to \bar{a},\quad b \to \bar{b}\ ,$$

其中$a,b \in H$。由于$H \le G$，故$ab \in H$，且

$$ab \to \bar{a}\bar{b}\ 。$$

从而$\bar{a}\bar{b} \in \varphi(H)$。即$\varphi(H)$对$\bar{G}$的乘法封闭，且

$$H \sim \varphi(H)\ 。$$

但H是子群，从而$\varphi(H)$也是群且为$\bar{G}$的子群。

群同态与同构的简单性质

2）$\bar{H} \le \bar{G}$时，由于$\varphi^{-1}\left(\bar{H}\right)$显然非空，任取$a,b \in \varphi^{-1}\left(\bar{H}\right)$，在 φ 之下令

$$a \to \bar{a}, \quad b \to \bar{b}$$

则

$$ab^{-1} \to \bar{a}\bar{b}^{-1}$$

其中 $\bar{a},\bar{b} \in \bar{H}$ ，而$\bar{H} \le \bar{G}$，故$\bar{a}\bar{b}^{-1} \in \bar{H}$，从而

$$ab^{-1} \in \varphi^{-1}\left(\bar{H}\right)$$

即 $\varphi^{-1}\left(\bar{H}\right) \le G$ ，且显然 φ 诱导出$\varphi^{-1}\left(\bar{H}\right)$ 到 $\bar{H}$ 的同态映射。

群同态与同构的简单性质

- **定理3**：群G到群 $\bar{G}$ 的同态映射 φ 是单射的充分必要条件是，群 $\bar{G}$ 的单位元 $\bar{e}$ 的逆像只有e。

证明：必要性显然。

充分性：设 φ 是群G到群 $\bar{G}$ 的同态映射，且在 φ 之下 $\bar{e}$ 的逆像只有e，又设在 φ 之下

$$a \to \bar{a}, \quad b \to \bar{b} \text{ ，}$$

当 $a \neq b$ 时，必有 $\bar{a} \neq \bar{b}$，若否有 $\bar{a} = \bar{b}$，则由于

$$ab^{-1} \to \bar{a}\bar{b}^{-1} = \bar{e} \text{ 。}$$

故 $ab^{-1} = e$ ，$a = b$，矛盾。因此 φ 为单射。

群同态与同构的简单性质

- **例3**：设6阶群G不是循环群。证明：

$$G \cong S_3$$

证明：因为G不是循环群，故G没有6阶元。从而由Lagrange定理知，G必有2阶或3阶元。

除e外G中元素不能都是2阶元：若不然，则G为交换群。于是在G中任取互异的2阶元a,b，则易知

$$N = \{e, a, b, ab\} \leq G$$

这与Lagrange定理矛盾。

又除e外G中元素不能都是3阶元：若不然，则在G中任取3阶元a,b，可知G有子群

$$H = \{e, a, a^2\}, \quad K = \{e, b, b^2\}$$

其中 $b \notin H$，且 $H \cap K = \{e\}$。于是

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 9$$

这与 $|G| = 6$矛盾。

群同态与同构的简单性质

因此，G必有2阶元a和3阶元b。由此可知

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

且易知

$$\varphi: e\to(1), a\to(12), b\to(123),$$
$$ab\to(23), b^2\to(132), ab^2\to(13)$$

是G到对称群 S_3 的一个同构映射，故 $G\cong S_3$ 。

- **注**：这个例子说明在同构意义下6阶群只有两个：一个是6阶循环群，另一个是三元对称群S_3。

•结合联系3.1中习题3（4阶群G不是循环群则必与Klein四元群同构）可知，阶数小于7的群的结构已经完全清楚。

---1阶

---2\3\5素数阶群为循环群

---4阶群要么是循环群要么与Klein四元群同构；6阶如上例分析。

作业

- P56、3. 证明：4阶群G不是循环群则必与Klein四元群同构。