17.7 群的同态与同构

定义 称f为G_1到G_2的同态，如果

$f: G_1 \to G_2$, 且$\forall x, y \in G_1$，$f(xy)=f(x)f(y)$

实例: (1) 整数加群<Z, +>的自同态:

$f_c(x) = cx$，c为给定整数

(2) 模n加群<Z_n, ⊕>的自同态:

$f_p(x) = px \pmod{n}$, $p=0, 1,\ldots, n-1$

(3) G_1=<Z, +>, G_2=<Z_n, ⊕>, G_1到G_2的满同态

$f: Z \to Z_n$, $f(x)=x \pmod{n}$

说明: 将群看成代数系统<G, ∘, $^{-1}$, e>，则同态f满足: $f(e_1)=e_2$，$f(x^{-1})=f(x)^{-1}$

同态映射的性质

同态保持元素的性质

$f(e_1) = e_2, f(x^{-1}) = f(x)^{-1}$，满同态$f$将生成元映到生成元

$|f(a)|$整除$|a|$，同构条件下$|f(a)| = |a|$

同态保持子代数的性质

$H \leq G_1 \Rightarrow f(H) \leq G_2$

$H \trianglelefteq G_1$, f 为满同态，$f(H) \trianglelefteq G_2$

同态核的性质，$\mathbf{ker}f = \{x \in G | f(x) = e_2\}$

$\mathbf{ker}f = \{e_1\} \Leftrightarrow f$为单同态

$\mathbf{ker}f \trianglelefteq G_1, \forall a, b \in G_1, f(a) = f(b) \Leftrightarrow a\mathbf{ker}f = b\mathbf{ker}f$

同态基本定理

(1) N为G的正规子群，则G/N是G的同态像

(2) 若G'为G的同态像($f(G) = G'$)，则$G/\mathbf{ker}f \cong G'$.

同态核性质的证明

定理 1 若f为G_1到G_2的同态，则

(1) $\ker f \trianglelefteq G_1$

(2) $\forall a, b\in G_1, f(a)=f(b) \Leftrightarrow a\ker f = b\ker f$

证: (1) 证子群. 显然$\ker f$ 非空. $\forall a, b\in \ker f$,

$$f(ab^{-1}) = f(a)f(b)^{-1}=e_2e_2^{-1}=e_2 \Rightarrow ab^{-1}\in \ker f$$

正规性证明. $\forall g\in G_1, \forall a\in \ker f$,

$$f(gag^{-1})=f(g)f(a)f(g^{-1})=f(g)f(g^{-1})=f(e_1)=e_2$$

$$gag^{-1}\in \ker f$$

(2) $f(a)=f(b) \Leftrightarrow f(a)^{-1}f(b)=e_2 \Leftrightarrow f(a^{-1}b)=e_2$

$$\Leftrightarrow a^{-1}b\in \ker f \Leftrightarrow a\ker f = b\ker f$$

同态基本定理

定理2 设$N \trianglelefteq G$，则$G \overset{\tau}{\sim} G/N$.

即任何群均与其商群同态，或商群总是群的同态像。

证：在G与G/N之间建立映射如下：

$$\tau: G \to G/N\,, \tau(a) = aN,\ \forall a \in G$$

则显然τ是G到G/N的一个满射。又$\forall a, b \in G$，都

有$\tau(ab) = (ab)N = (aN)(bN) = \tau(a)\tau(b)$,

即τ是G到G/N的一个同态映射。

注：以后将上面的同态映射τ称为G到G/N的<u>自然同态</u>。

同态基本定理

定理3（同态基本定理） 设φ是群G到群$\overline{G}$的同态满射，则$N=\ker\varphi \trianglelefteq G$，且$G/N\cong\overline{G}$.

证： 由定理1可知，$N=\ker\varphi \trianglelefteq G$，在$G/N$与$\overline{G}$之间建立映射如下：

$$\sigma: G/N\to\overline{G},\ \sigma(aN)=\overline{a}=\varphi(a),\ \forall a\in G$$

(1) 设$aN=bN$，则$a^{-1}b\in N$，于是$\varphi\left(a^{-1}b\right)=\overline{e}$，

即 $\varphi(a)^{-1}\varphi(b)=\overline{a}^{-1}\overline{b}=\overline{e}$，从而$\overline{a}=\overline{b}$，

即G/N中的每个陪集在σ下的像唯一，因此σ确为G/N到$\overline{G}$的一个映射。

同态基本定理

(2) $\forall \bar{a} \in \bar{G}$，因为$\varphi$是满射，所以存在$a \in G$，使得$\varphi(a) = \bar{a}$，从而存在$aN \in G/N$，使得$\sigma(aN) = \bar{a}$，即$\sigma$是满射。

(3) 设$\sigma(aN) = \sigma(bN)$，即$\varphi(a) = \varphi(b) \Rightarrow \varphi(a)^{-1}\varphi(b) = \bar{e} \Rightarrow \varphi\left(a^{-1}b\right) = \bar{e}$，所以$a^{-1}b \in \ker\varphi = N$，从而$aN = bN$，即$\sigma$是单射。

(4) 又由于$\sigma(aN \cdot bN) = \sigma\big((ab)N\big) = \varphi(ab) = \varphi(a)\varphi(b) = \sigma(aN)\sigma(bN)$, 即$\sigma$是$G/N$到$\bar{G}$的一个同态映射。

综上所述，σ是G/N到$\bar{G}$的一个同构，所以$G/N \cong \bar{G}$。

同态基本定理

- 定理2表明，商群总是群的同态像
- 定理3表明，群的同态像一定与某个商群同构
- 因此同态基本定理表明，在同构意义下，

  群的同态像就是它的商群，

  因而确定群的全部同态像等价于找出该群的全部正规子群。

同态基本定理

推论 设G与$\overline{G}$是两个有限群，若存在满同态$\varphi: G \to \overline{G}$，则$|\overline{G}| \mid |G|$。

证：因为存在满同态$\varphi: G \to \overline{G}$，所以由定理3有

$$G/N \cong \overline{G}，其中 N = \ker\varphi。$$

从而$|\overline{G}| = |G/N|$。而由Lagrange定理，

$|G| = |N||G/N| \Rightarrow |G/N| \mid |G|$，所以 $|\overline{G}| \mid |G|$。

循环群的同态像

定理4 设G与$\overline{G}$是两个群(不必有限)且$\varphi: G \to \overline{G}$是满同态。则当$G$是循环群时，$\overline{G}$也是循环群。（等价的说法是：循环群的同态像还是循环群。）

证：设$G = \langle a \rangle$是由a生成的循环群，记$\varphi(a) = \overline{a}$。以下证明$\overline{G}$是由$\overline{a}$生成的循环群，即$\overline{G} = \langle \overline{a} \rangle = \langle \varphi(a) \rangle$。

事实上，显然$\langle \overline{a} \rangle \subseteq \overline{G}$。另一方面，$\forall \overline{x} \in \overline{G}$，因为$\varphi$是满射，所以$\exists x \in G$，使得$\varphi(x) = \overline{x}$。由于$G = \langle a \rangle$，故$x = a^m$，从而$\overline{x} = \varphi(a^m) = \varphi(a)^m = \overline{a}^m \in \langle \overline{a} \rangle$。由$\overline{x}$的任意性知，$\overline{G} \subseteq \langle \overline{a} \rangle$。

因此，$\overline{G} = \langle \overline{a} \rangle$是由$\overline{a}$生成的循环群，定理成立。

循环群的同态像

由同态基本定理，在同构意义下，群的同态像就是它的商群。再结合定理4得

推论 循环群的商群也是循环群。

综合有：

- 循环群的子群还是循环群；
- 循环群的同态像还是循环群；
- 循环群的商群也是循环群。

同态映射下子群间的关系

定理5 设$\varphi: G \to \overline{G}$是群$G$到群$\overline{G}$的满同态，$\ker\varphi = K$，则$G$的包含$K$的子群与$\overline{G}$的所有子群之间可以建立一个保持包含关系的双射。即，令

$$M = \{H | H \leq G, H \supseteq K\},\quad \overline{M} = \{\overline{H} | \overline{H} \leq \overline{G}\},$$

则M与$\overline{M}$之间可以建立一个保持包含关系的双射。

同态映射下子群间的关系

引理 设$\varphi: G \to \overline{G}$是群$G$到群$\overline{G}$的同态映射，$H \leq G$。如果$H \supseteq \ker\varphi$，则$\varphi^{-1}[\varphi(H)] = H$。

证: 首先显然有$H \subseteq \varphi^{-1}[\varphi(H)]$。

其次，$\forall x \in \varphi^{-1}[\varphi(H)]$，则$\varphi(x) \in \varphi(H)$。于是存在$h \in H$，使得$\varphi(x) = \varphi(h)$，从而有$\varphi(h)^{-1}\varphi(x) = \varphi\left(h^{-1}x\right) = \bar{e} \Rightarrow h^{-1}x \in \ker\varphi$。由假设$H \supseteq \ker\varphi$，得$h^{-1}x \in H$。又$h \in H \leq G$，所以$x \in H$，即有$\varphi^{-1}[\varphi(H)] \subseteq H$。

因此$\varphi^{-1}[\varphi(H)] = H$。

同态映射下子群间的关系

定理5的证明:

$M=\{H|H\leq G,\ H\supseteq K\}$, $\quad \bar{M}=\{\bar{H}|\bar{H}\leq \bar{G}\}$,

定义映射$f: M\rightarrow \bar{M}$, $f(H)=\varphi(H)$, $H\in M$。

以下验证f符合要求。

首先，f是M到$\bar{M}$的映射，因为若$H\leq G\Rightarrow \varphi(H)\leq \bar{G}$。

其次，f是单射：设$f(H_1)=f(H_2), H_1, H_2\in M$，得

$\varphi(H_1)=\varphi(H_2)$. 由引理得$H_1=\varphi^{-1}[\varphi(H_1)]=$

$\varphi^{-1}[\varphi(H_2)]=H_2$，所以$f$是单射。

同态映射下子群间的关系

f是满射:任给$\bar{H} \in \bar{M}$，令$H = \varphi^{-1}(\bar{H})$，则$H \leq G$. 显然$\bar{H} \supseteq \{\bar{e}\}$，从而$\varphi^{-1}(\bar{H}) \supseteq \varphi^{-1}(\bar{e})$，即$H \supseteq K$. 所以$H \in M$，且$f(H) = \bar{H}$。即$f$是满射，从而$f$是双射。

另外，若$H_1 \subseteq H_2$，则显然$\varphi(H_1) \subseteq \varphi(H_2)$，即$f(H_1) \subseteq f(H_2)$。反之，若$f(H_1) \subseteq f(H_2)$，即$\varphi(H_1) \subseteq \varphi(H_2)$，则$\varphi^{-1}[\varphi(H_1)] \subseteq \varphi^{-1}[\varphi(H_2)]$，由引理得$H_1 \subseteq H_2$, 定理得证。

同态映射下子群间的关系

从定理5的证明过程可以看出：把定理5中的子群改为正规子群，结论仍然成立。即

设$\varphi: G \rightarrow \bar{G}$是群$G$到群$\bar{G}$的满同态，$\ker\varphi = K$，则$G$的包含$K$的正规子群与$\bar{G}$的所有正规子群之间可以建立一个保持包含关系的双射。

群的第一同构定理

同态基本定理：设φ是群G到群$\overline{G}$的一个同态满射，则$G/\mathrm{ker}\varphi \cong \overline{G}$.

将同态基本定理推广就得到下面的第一同构定理。

定理6 (第一同构定理) 设φ是群G到群$\overline{G}$的一个满同态，且$\mathrm{ker}\varphi \subseteq N \trianglelefteq G$，记$\varphi(N) = \overline{N}$，则

$$G/N \cong \overline{G}/\overline{N}\text{，或}G/N \cong \varphi(G)/\varphi(N)$$

当$N = \mathrm{ker}\varphi$时，$\varphi(N) = \{\overline{e}\}$，$\overline{G}/\overline{N} = \overline{G}/\{\overline{e}\} \cong \overline{G}$，第一同构定理退化成同态基本定理。

群的第一同构定理

证：首先，由$N \trianglelefteq G$有$\overline{N}=\varphi(N) \trianglelefteq \overline{G}$。作映射:

$$\tau: G/N \to \overline{G}/\overline{N},$$

$$\tau(xN)=\varphi(x)\overline{N}, \qquad \forall xN \in G/N\text{。}$$

以下验证τ是G/N到$\overline{G}/\overline{N}$的一个同构映射。

(1) τ是映射：设$aN=bN$, $a,b \in G$，则$a^{-1}b \in N$，于是$\varphi(a)^{-1}\varphi(b)=\varphi\left(a^{-1}b\right) \in \varphi(N)=\overline{N}$，从而$\varphi(a)\overline{N}=\varphi(b)\overline{N}$, 即$G/N$中的每个陪集在$\tau$下的像唯一，因此$\tau$确为$G/N$到$\overline{G}/\overline{N}$的一个映射。

群的第一同构定理

(2) τ是满射：$\forall \bar{a}\bar{N} \in \bar{G}/\bar{N}$，$\bar{a} \in \bar{G}$，因为$\varphi$是满射，所以存在$a \in G$，使得$\varphi(a) = \bar{a}$，从而存在$aN \in G/N$，使得$\tau(aN) = \bar{a}\bar{N}$, 故$\tau$是满射。

(3) τ是单射：设$\tau(aN) = \tau(bN)$，即$\varphi(a)\bar{N} = \varphi(b)\bar{N}$，从而$\varphi\left(a^{-1}b\right) = \varphi(a)^{-1}\varphi(b) \in \bar{N}$。但$\tau$是满射且$\tau(N) = \bar{N}$，所以$\exists c \in N$，使得$\varphi\left(a^{-1}b\right) = \varphi(c) \Rightarrow \varphi\left(a^{-1}bc^{-1}\right) = \bar{e} \Rightarrow a^{-1}bc^{-1} \in \ker\varphi$. 于是由已知条件$\ker\varphi \subseteq N$得$a^{-1}bc^{-1} \in N \Rightarrow a^{-1}b = a^{-1}bc^{-1}c \in N$，从而$aN = bN$，即$\tau$是单射。

群的第一同构定理

(4) 又由于

$\boldsymbol{\tau(aN \cdot bN) = \tau\big((ab)N\big) = \varphi(ab)\overline{N} =}$
$\boldsymbol{\varphi(a)\varphi(b)\overline{N} = \varphi(a)\overline{N} \cdot \varphi(b)\overline{N} = \tau(aN)\tau(bN)}$，

所以$\boldsymbol{\tau}$是$\boldsymbol{G/N}$到$\boldsymbol{\overline{G}/\overline{N}}$的一个同态映射。

综上所述，$\boldsymbol{\sigma}$是$\boldsymbol{G/N}$到$\boldsymbol{\overline{G}/\overline{N}}$的一个同构，所以$\boldsymbol{G/N \cong \overline{G}/\overline{N}}$。

第一同构定理

定理 6（第一同构定理）设 φ 是群 G 到群 $\overline{G}$ 的一个满同态，且 $\ker\varphi \subseteq N \trianglelefteq G$，记 $\varphi(N)=\overline{N}$，则

$$G/N \cong \overline{G}/\overline{N}，或 \quad G/N \cong \varphi(G)/\varphi(N)$$

推论 设 $H \trianglelefteq G, N \trianglelefteq G$ 且 $N \subseteq H$，则

$$G/H \cong {}^{G/N}\Big/_{H/N}.$$

证：取自然同态 $\varphi: G \to G/N$，$\varphi(a) = aN$，其核 $\ker\varphi = N$。在第一同构定理中取 $\overline{G} = G/N$，取 N 为这里的 H，并注意 $\varphi(H) = H/N$，由第一同构定理得 $G/H \cong {}^{G/N}\Big/_{H/N}.$

群的第一同构定理

设$A,B\leq G$,则
$AB\leq G \Leftrightarrow AB=BA$

例1 设$H \trianglelefteq G, K \trianglelefteq G$，证明

$$G/HK \cong {}^{G/H}\!\big/_{HK/\mathrm{H}}$$

$HK=\cup\{hK|h\in H\}$
$=\cup\{Kh|h\in H\}$
$=KH$

证：由$H \trianglelefteq G, K \trianglelefteq G \Rightarrow HK \trianglelefteq G$。又显然$H \trianglelefteq HK$，直接由推论得

$$G/HK \cong {}^{G/H}\!\big/_{HK/H}。$$

注意：交换H,K的位置也可以

$$G/HK \cong {}^{G/K}\!\big/_{HK/K}$$

群的第二同构定理

设$A,B \le G$,则
$AB \le G \Leftrightarrow AB=BA$

定理7 (第二同构定理) 设G是群，$H \le G$，$N \trianglelefteq G$，则$H \cap N \trianglelefteq \mathrm{H}$，且$HN/N \cong H/(H \cap N)$.

证：由$H \le G, N \trianglelefteq G$有$HN \le G$，且$N \trianglelefteq HN$。作映射$\varphi: H \to HN/N, \varphi(x) = xN, \forall x \in H,$
则φ显然是H到HN/N的满同态。且
$\ker\varphi = \{x|x \in H, \varphi(x) = N\} =$
$\{x|x \in H, xN = N\} = \{x|x \in H, x \in N\} = H \cap N,$
于是由同态基本定理得

$$H/(H \cap N) \cong HN/N$$

群的第二同构定理

（第二同构定理）设G是群，$H\le G$，$N\trianglelefteq G$，则$H\cap N\trianglelefteq H$，且$HN/N\cong H/(H\cap N)$。

例 S_3, S_4设分别为3元、4元对称群，K_4是Klein四元群，证明：$S_4/K_4\cong S_3$。

$K_4=\{(1), (12)(34), (13)(24), (14)(23)\}$

证： 首先易验证$K_4\trianglelefteq S_4$。以下验证：$S_4=S_3K_4$且$S_3\cap K_4=\{(1)\}$，再用第二同构定理即可得证。事实上，把S_3中的每个置换看成保持4不动，则显然$S_3\cap K_4=\{(1)\}$成立。于是$|S_3K_4|=\frac{|S_3|\cdot|K_4|}{|S_3\cap K_4|}=6\times 4=24$。

习题33(1)

又$S_3K_4\subseteq S_4$且$|S_4|=24$，所以$S_4=S_3K_4$。于是由第二同构定理$S_4/K_4\cong S_3K_4/K_4\cong S_3/(S_3\cap K_4)\cong S_3/\{(1)\}\cong S_3$。

群的第三同构定理

(2) 若 L 是 G/N 的子群, 则存在 G 的子群 H, 使得 $N \subseteq H$ 且 $L = H/N$.

定理8 (第三同构定理) 设G是群，且$N \trianglelefteq G$，$\bar{H} \le G/N$，则

(1) 存在G的唯一子群$H \le G, H \supseteq N$，使得$\bar{H} = H / N$;

(2) 当$\bar{H} \trianglelefteq G/N$时，存在$G$的唯一正规子群$N \trianglelefteq G, \mathrm{H} \supseteq N$, 使得$\bar{H} = H/N$，且$G/H \cong {}^{G/N}/_{H/N}$

群的第一同构定理的推论

第三同构定理表明：商群G/N的子群仍为商群，且呈H/N的形式，其中$H \le G, H \supseteq N$；而且H是G的正规子群当且仅当H/N是G/N的正规子群。

群的第三同构定理

证：(1) 取自然同态$\varphi: G \to G/N, \varphi(a) = aN$，其核$\ker\varphi = N$. 由前面定理5知，在$G$的包含$N$的子群与$G/N$的所有子群之间可以建立一个保持包含关系的双射。因此当$\bar{H} \le G/N$时，必然存在G的唯一的子群$H \le G, H \supseteq N$与之对应，即$\varphi(H) = \bar{H}$。另一方面，根据φ的定义有$\varphi(H) = H/N$，所以$\bar{H} = H/N$.

(2) 还是由定理5，当$\bar{H} \trianglelefteq G/N$时，存在$G$的唯一的正规子群$H \trianglelefteq G, H \supseteq N$，使得$\bar{H} = H/N$。再由第一同构定理得$G/H \cong \varphi(G)/\varphi(H) \cong {}^{G/N}\big/_{H/N}$

自同态与自同构

End*G*： *G* 的自同态的集合

Aut*G*： *G* 的自同构的集合

Inn*G*： *G* 的内自同构的集合

内自同构 $f_x: G\to G,\ f_x(a)=xax^{-1}$

关系： $\mathrm{Inn}G \subseteq \mathrm{Aut}G \subseteq \mathrm{End}G$

End*G* 为独异点

Aut*G* 为群

Inn*G* 为 **Aut*G*** 的正规子群

$I_G=f_e$ 属于 **Inn*G***

实例

$Z_6=\{0, 1, 2, 3, 4, 5\}$， $G=<Z_6, \oplus>$,

$f_p: Z_6 \to Z_6$, $f_p(x)= px \pmod 6$

$f_0(x)=0$, $f_1=I_G$,

$f_2(0)=f_2(3)=0$, $f_2(1)=f_2(4)=2$, $f_2(2)=f_2(5)=4$

$f_3(0)=f_3(2)=f_3(4)=0$, $f_3(1)=f_3(3)=f_3(5)=3$

$f_4(0)=f_4(3)=0$, $f_4(1)=f_4(4)=4$, $f_4(2)=f_4(5)=2$

$f_5(0)=0$, $f_5(1)=5$, $f_5(2)=4$, $f_5(3)=3$, $f_5(4)=2$, $f_5(5)=1$

$\mathrm{End}G=\{f_0, f_1, \ldots, f_5\}$,

$\mathrm{Aut}G=\{f_1, f_5\}$

$\mathrm{Inn}G=\{f_1\}$