群的同态及其应用

◆郭　俊　李兴达　姚淑霞

（兰州城市学院数学学院　甘肃兰州　730070）

摘要：群的同态与同构是研究群与群之间关系的重要手段。本文基于群的同态与同构关系，结合教学经验，通过典型问题的分析阐明了群论中有关群的同态及同构问题的证明方法，为相关学者对这方面的学习和理解提供一定的帮助和指导作用.

关键词：群；同态；同构；同态映射

1 引言

群的同态与同构关系是群论中非常重要的内容，群论中关于子群、子群陪集、不变子群、商群及不变子群对群的分类问题等都与群的同态及同构有密切关系[1]。当所给的群是商群，或环是商环时，利用同态基本定理可以简化同态及同构问题的证明[2-4]。

同构映射是群之间关系最密切的映射，存在同构映射的两个群本质上可以不加区别，因为它们有相同的群结构，近世代数中最基本与最重要的研究内容就是搞清楚各种代数系统在同构意义下的分类，而同态映射只要求保持运算，显然它比同构映射更灵活，能够研究两个不同构的群之间的联系。

群的同态与同构是群论中非常重要的内容，而同态基本定理是群论中最为核心的结论，它告诉我们，两个群在同态满射的条件下蕴含着一个群同构关系($G/N\cong\overline{G}$)在处理一些同构问题时，我们也常常逆用这个定理，也就是说，先构造出同态满射，再利用该映射研究两个代数体系之间的关系。

为方便分析，将文中用到的相关概念做如下说明。

定义 1[5]若二元代数系统$<G,\circ>$满足：

（1）G 对 o 来说是封闭的，即$\forall a,b\in G$,都有 $a\circ b\in G$;

（2）o 在 G 中是可结合的，即

$\forall a,b,c\in G$,都有$(a\circ b)\circ c = a\circ(b\circ c)$;

（3）G 中至少存在关于 o 的单位元 e 即

$\exists e\in G$,使得$\forall a\in G$,都有 $e\circ a = a\circ e = a$;

（4）G 中每个元素 a 都有逆元 a^{-1} 即

$\forall a\in G$,都$\exists a^{-1}\in G$,使得$a\circ a^{-1} = a^{-1}\circ a = e$.

则称二元代数系统$<G,\circ>$为群（Group）。

定义 2[5] 如果群 G 的非空子集 H 对于群 G 的乘法运算也作成一个群，那么称 H 为 G 的子群，记作$H\leq G$.

一个群 G 的一个不空子集 H 作成 G 的一个子群的充要条件是：

(i)$\forall a,b\in H\Rightarrow ab\in H$,

(ii)$a\in H\Rightarrow a^{-1}\in H$;

推论：一个群 G 的一个不空子集 H 作成 G 的一个子群的充要条件是：$\forall a,b\in H\Rightarrow ab^{-1}\in H$.

定义 3[5] 设 G 是一个群，N 是其子群，若群中任意固定元的左陪集与右陪集总是相等的，则称 N 是 G 的正规子群(或不变子群)，记作$N\trianglelefteq G$

定义 4[5] 一个群 G 的一个不变子群 N 的所有左（右）陪集所做成的群叫做一个商群，用符号G/N表示.

定义 5[5] 设 G 与$\overline{G}$是两个群，如果存在一个映射φ：$G\rightarrow\overline{G}$，满足$\forall a\in G,\exists\overline{a}\in\overline{G}$使得$\varphi(a)=\overline{a}$,记为$a\rightarrow\overline{a}$,且$\forall a,b\in G$有

$\varphi(ab)=\varphi(a)\varphi(b)$.

则称φ为群 G 到群$\overline{G}$的一个同态映射。

当φ又是满射时，则称群 G 与群$\overline{G}$同态，记作$G\sim\overline{G}$.

当φ又是一一映射时，则称群 G 与群$\overline{G}$同构，记作$G\cong\overline{G}$.

为方便叙述，常记 a 在φ之下的象$\varphi(a)=\overline{a}$.

在群的同态与同构关系下，可以获得比较好的很多结论，下面就比较基础和重要的结论做一介绍。

2 群的同态与同构

引理 1[6]设 G 是一个群，$\overline{G}$是一个有二元运算(也称为乘法)的集合.如果$G\sim\overline{G}$.则$\overline{G}$也是一个群，并且，群 G 的单位元的象是群$\overline{G}$的单位元；G 的元素 a 的逆元的象是 a 的象的逆元，即

$\overline{a^{-1}}=\overline{a}^{-1}$或$\varphi(a^{-1}) = \varphi(a)^{-1}$.

证明：因为$G\sim\overline{G}$,G是群，其乘法满足结合律，所以$\overline{G}$的乘法也满足结合律。

设φ是 G 到$\overline{G}$的同态满射，e 是群 G 的单位元；

$\forall\overline{a}\in\overline{G}$ 令 $\overline{a}$ 在 φ 之下的原象是 a 则 $e\rightarrow\overline{e},a\rightarrow\overline{a}$, 于是 $ea\rightarrow\overline{e}\overline{a}$.但$ea=a$故$\overline{e}\overline{a}=\overline{a}$ 即$\overline{e}$是$\overline{G}$的单位元。

又$a^{-1}\rightarrow\overline{a^{-1}}$,则$a^{-1}a\rightarrow\overline{a^{-1}}\overline{a}$,

但$a^{-1}a=e$故$\overline{a^{-1}}\overline{a}=\overline{e}$即$\overline{a^{-1}}$是$\overline{a}$的逆元.

因此$\overline{G}$也是一个群.

应注意，本定理中的同态映射φ必须是满射. 如，G 是正有理数乘群，$\overline{G}$为有理数集对$a\circ b = a^2$ $(\forall a,b\in\overline{G})$作成的代数系统. 则$\varphi:x\rightarrow 1$ $(\forall x\in G)$。

是 G 到$\overline{G}$的一个同态映射(但不是满射)，虽然 G 是群，但$\overline{G}$对 o 不仅不是群,连半群也不是(因为其代数运算不满足结合律).

引理 2[6]设φ是群 G 到群$\overline{G}$的一个同态满射，则

(1)若$H\leq G$,则$\varphi(H)\leq\overline{G}$,且 $H\sim\varphi(H)$;

(2)若$\overline{H}\leq\overline{G}$,则$\varphi^{-1}(\overline{H})\leq G$,且在$\varphi$之下诱导出$\varphi^{-1}(\overline{H})$到$\overline{H}$的一个同态映射.

证明：(1) 任取 $\overline{a},\overline{b}\in\varphi(H)$ 且在 φ 之下 $\exists a,b\in H$ 使 $a\rightarrow\overline{a},b\rightarrow\overline{b}$,

由于 $H\leq G$ 故 $ab\in H$ 且 $\varphi(ab)=\overline{a}\overline{b}$ 从而 $\overline{a}\overline{b}\in\varphi(H)$ 即 $\varphi(H)$对$\overline{G}$的乘法封闭；又$H\sim\varphi(H)$且 H 是子群，从而$\varphi(H)$也是群，且是$\overline{G}$的子群.

(2)当$\overline{H}\leq\overline{G}$时，显然$\varphi^{-1}(\overline{H})$非空；

任取 $a,b\in\varphi^{-1}(\overline{H})$ 在 φ 之下令 $\varphi(a)=\overline{a},\varphi(b)=\overline{b}$. 则 $\varphi(ab^{-1})=\overline{a}\overline{b}^{-1}$, 而 $\overline{H}\leq\overline{G}$, 故 $\overline{a}\overline{b}^{-1}\in\overline{H}$, 从而 $ab^{-1}\in\varphi^{-1}(\overline{H})$即$\varphi^{-1}(\overline{H})\leq G$,显然,$\varphi$诱导出$\varphi^{-1}(\overline{H})$到$\overline{H}$的一个同态映射。

引理 3[5] 假定 G 和$\overline{G}$是两个群，并且 G 与$\overline{G}$同态，那么在这个同态满射之下，

G 的一个不变子群 N 的象$\overline{N}$是$\overline{G}$的不变子群；

$\overline{G}$的一个不变子群$\overline{N}$的逆象 N 是 G 的不变子群。

证明: (1)由 N 是 G 的一个不变子群，由定理 2 知$\overline{N}$是$\overline{G}$的一个子群。

$\forall\overline{a}\in\overline{G},\forall\overline{n}\in\overline{N}$，在 G 与$\overline{G}$的同态满射$\varphi$之下，令

$a\rightarrow\overline{a},n\rightarrow\overline{n}$ $(a\in G,n\in N)$，

则，在φ之下，$ana^{-1}\rightarrow\overline{a}\overline{n}\overline{a}^{-1}$,

但由于 N 是 G 的不变子群,$ana^{-1}\in N$,因此由$\overline{N}$是 N 在φ之下的象知，$\overline{a}\overline{n}\overline{a}^{-1}\in\overline{N}$.这样，$\overline{a}\in\overline{G},\overline{n}\in\overline{N}\Rightarrow\overline{a}\overline{n}\overline{a}^{-1}\in\overline{N}$..

因此，$\overline{N}$是$\overline{G}$的一个不变子群.

(2) $\overline{N}$既是$\overline{G}$的一个不变子群，由定理2知N是G的一个子群.

假定a是G的任意元，n是N的任意元，而且在φ之下，

$a \to \overline{a}, n \to \overline{n}$,

那么$\overline{a} \in \overline{G}, \overline{n} \in \overline{N}$,由$\overline{N}$是$\overline{G}$的不变子群知,$\overline{a}\overline{n}\overline{a}^{-1} \in \overline{N}$. 但在φ之下，$ana^{-1} \to \overline{a}\overline{n}\overline{a}^{-1}$,所以$ana^{-1} \in N$.这样，

$\forall a \in G, n \in N \Rightarrow ana^{-1} \in N$;

即N是G的一个不变子群.

定理4[5]（同态基本定理）假定G和$\overline{G}$是两个群，并且G与$\overline{G}$同态，那么这个同态满射的核 N 是 G 的一个不变子群，并且$G/N \cong \overline{G}$.

证明：假定a和b是N的任何两个元，那么在φ之下，

$a \to \overline{e}, b \to \overline{e}$,因此$ab^{-1} \to \overline{e}\overline{e}^{-1} = \overline{e}$,

这就是说，$a, b \in N \Longrightarrow ab^{-1} \in N$;

N 是 G 的一个子群. 假定$n \in N, a \in G$,而且在φ之下，$a \to \overline{a}$.那么在φ之下，

$a \to \overline{a}, n \to \overline{e}$,

$ana^{-1} \to \overline{a}\overline{e}\overline{a}^{-1} = \overline{e}$,

即，$n \in N, a \in G \Longrightarrow ana^{-1} \in N$;所以，N是G的一个不变子群.现在规定法则：$\psi: aN \to \overline{a} = \varphi(a)\ (a \in G)$;

我们说，这是一个G/N与G间的同构映射.因为：

(i) $aN = bN \Longrightarrow b^{-1}a \in N \Longrightarrow \overline{b}^{-1}\overline{a} = \overline{e} \Longrightarrow \overline{a} = \overline{b}$,

这就是说，在ψ之下G/N的元素只有一个唯一的象；

（ii）给了$\overline{G}$的一个任意元$\overline{a}$,在G里至少有一个元a满足条件$\varphi(a) = \overline{a}$由ψ的定义，$\psi: aN \to$给的$\overline{a}$,

这就是说，ψ是G/N到$\overline{G}$的满射；

(iii)$aN \neq bN \Longrightarrow b^{-1}a \overline{\in} N \Longrightarrow \overline{b}^{-1}\overline{a} \neq \overline{e} \Longrightarrow \overline{a} \neq \overline{b}$;

(iv)在ψ之下，$aNbN = abN \to \overline{ab} = \overline{a}\overline{b}$;这样$G/N \cong \overline{G}$.

同态基本定理告诉我们：如果群G同另一个群$\overline{G}$同态，则这个群$\overline{G}$在同构意义下是G的一个商群。

3 群的同态与同构的应用

3.1 群同态在循环群中的应用

应用1：设G与$\overline{G}$是两个群，且$G \sim \overline{G}$，若G是循环群，则$\overline{G}$也是循环群。

证明：设$G = \langle a \rangle$由于$G \sim \overline{G}$,设在此同态满射下，G的生成元a在$\overline{G}$中的象是$\overline{a}$下证 $\overline{G} = \langle \overline{a} \rangle$

显然 $\langle \overline{a} \rangle \subseteq G$ 另一方面，任取 $\overline{x} \in \overline{G}$ 令 $x \to \overline{x} (x \in G = \langle a \rangle)$,

则$x = a^m$于是$\overline{x} = \overline{a}^m \in \langle \overline{a} \rangle$故$\overline{G} \subseteq \langle \overline{a} \rangle$

因此$\overline{G} = \langle \overline{a} \rangle$结论得证。

应用2： 假定G是无限阶的循环群，$\overline{G}$是任何循环群，则G与$\overline{G}$同态。

证明：设$G = \langle a \rangle$是无限阶的循环群，$\overline{G} = \langle \overline{a} \rangle$是任一循环群，定义$\varphi: G \to \overline{G}, a^k \to \overline{a}^k, k \in \mathbb{Z}^*$.

下证φ是同态满射。

①因为$G = \langle a \rangle$是无限阶的循环群，所以$|a| = \infty$从而

$a^k = a^l \Leftrightarrow k = l$.

于是，若$a^k = a^l$则$\varphi(a^k) = \varphi(a^l)$故φ是映射；

② 给了 G 的一个任意元 y 则$\exists k \in \mathbb{Z}^*$, 使得$y = \overline{a}^k$, 从而$\exists a^k \in G$，使得$a^k \xrightarrow{\varphi} \overline{a}^k$,

故φ是g到$\overline{G}$的满射；

③在φ之下：

$\varphi: G \to \overline{G}, a^m \to \overline{a}^m, a^n \to \overline{a}^n, (m, n \in \mathbb{Z}^*)$,

故$a^m a^n = a^{m+n} \to \overline{a}^{m+n} = \overline{a}^m \overline{a}^n$;

从而φ是g到$\overline{G}$的同态映射；

综合以上三点可知，φ是g到$\overline{G}$的同态满射, 从而g与$\overline{G}$同态。

应用3: 假定G与$\overline{G}$是两个有限循环群，它们的阶各是n和m,证明，G与$\overline{G}$同态$\Leftrightarrow m \mid n$.

证明：设$G = \langle a \rangle$，$\overline{G} = \langle b \rangle$是两个有限循环群，$\circ(a) = n, \circ(b) = m$.

$\Rightarrow$）设$G \sim \overline{G}$且φ为其同态满射，N为同态满射φ的核，则$G/N \cong \overline{G}$. 但 $|G/N| = |G|/|N|, |\overline{G}| = |G/N|$，故$|\overline{G}|\,|\,|G|$,即$m \mid n$. $\Leftarrow$）若$m \mid n$，令

$\varphi: G \to \overline{G}, a^s \to b^r$,(其中$s = nq + r, q, r \in \mathbb{Z}$,且$0 \leq r < n$)

下证φ是同态满射.

①

$\forall a^x, a^y \in G$, 且令$x = nq_1 + r_1, y = nq_2 + r_2, (0 \leq r_1, r_2 < n)$;;

当$a^x = a^y$,即$a^{x-y} = a^{n(q_1 - q_2) + (r_1 - r_2)} = e$,

从而 $n|[n(q_1 - q_2) + (r_1 - r_2)]$, 必有$n|r_1 - r_2$，必有$n|r_1 - r_2$,但是$0 \leq |r_1 - r_2| < n$,

由n为a的阶知$r_1 - r_2 = 0$, 即 $r_1 = r_2$,从而

$\varphi(a^x) = b^{r_1} = b^{r_2} = \varphi(a^y)$;

故φ是群g到$\overline{G}$的映射；

②给了$\overline{G}$的一个任意元 y 则$\exists k \in \mathbb{Z}^*$, 使得$y = b$从而在g里，$\exists a^k \in G$,使得$a^k \xrightarrow{\varphi} b^k$,故φ是群g到$\overline{G}$的满射；

③因为

$\varphi: G \to \overline{G}, a^s \to b^r, a^k \to b^t$,

(其中$s = nq + r, k = nm + t, q, r, m, t \in \mathbb{Z}$,且$0 \leq r, t < n$),

故$\varphi(a^s a^k) = \varphi(a^{s+k}) = b^{r+t} = b^r b^t$.

从而φ是群g到$\overline{G}$的同态映射.

综合以上三点可得，φ是群G到$\overline{G}$的同态满射, 从而G与$\overline{G}$同态。

3.2 群的同态在普通数群中的应用

应用4：设G是正有理数乘群，$\overline{G}$是整数加群，证明：

$\varphi: 2^n \cdot \frac{b}{a} \to n$,

是群G到$\overline{G}$的一个同态满射，其中a,b是互素的正奇数，n是整数。

证明：显然φ是群G到群$\overline{G}$的满射.

当$(ab, 2) = 1, (cd, 2) = 1$时，显然有$(abcd, 2) = 1$且

$\varphi\left(2^n \cdot \frac{b}{a} \cdot 2^m \cdot \frac{d}{c}\right) = \varphi\left(2^{n+m} \cdot \frac{bd}{ac}\right) = n + m = \varphi\left(2^n \cdot \frac{b}{a}\right)\varphi\left(2^m \cdot \frac{d}{c}\right)$

从而φ是正有理数乘群G到整数加群$\overline{G}$的一个同态满射.

3.3 同态基本定理在群的同构中的应用

应用5：如果H和K是群G的子群且K是群G的不变子群，那么$(HK)/K \cong H(H \cap K)$[7].

证明：由$H \leq G, K \leq G$,则$H \cap K \leq G$ 又由 $K \trianglelefteq G$，知$\cap K \trianglelefteq G$,即$H/(H \cap K)$有意义。

定义$\varphi: hk \to h \cdot H \cap K$,其中h、k分别为H、K中的任意元。

（i）若$hk = h'k' \Longrightarrow kk'^{-1} = h^{-1}h' \Longrightarrow h^{-1}h' \in H \cap K$,

即有$h \cdot H \cap K = h' \cdot H \cap K \in H/(H \cap K)$,

故$\varphi(hk)$与$\varphi(h'k')$表示相同的陪集，因此φ是 HK 到$H/(H \cap K)$的映射；

（ii）对$H/(H \cap K)$中的任意元$h \cdot H \cap K$(其中$h \in H$)由于

$e \in K$ 故至少存在 HK 中的元 he=h 使得 $\varphi(he) = h \cdot H \cap K$ 所以 φ是 HK 到 $H/(H\cap K)$ 的满射；

（iii）因为 $K \trianglelefteq G$,所以对任意 $h' \in H$ 有 $Kh' = h'K$,于是，$\forall\, k \in K$ 存在 $k'' \in K$,使得 $kh' = h'k''$ 从而

$\varphi(hk \cdot h'k') = \varphi(hh' \cdot k''k') = hh' \cdot H \cap K$;

但由于 $hh' \cdot H \cap K = h \cdot (H \cap K) * h' \cdot (H \cap K)$,

故 $\varphi(hk \cdot h'k') = \varphi(hk) * \varphi(h'k')$,,

所以φ是群同态映射；

（iv）由于 $e \cdot H \cap K = H \cap K$ 是 $H/(H\cap K)$ 的单位元，因此

$\ker\varphi = \{hk \in HK | \varphi(hk) = H \cap K\}$,

又由于 $\varphi(hk) = h \cdot H \cap K$ 因此有 $h \cdot H \cap K = H \cap K$ 从而 $h \in H \cap K$,故 $\ker\varphi = \{hk \in HK | \varphi(hk) = H \cap K\} = (H \cap K) \cdot K = K$;

因此，由同态基本定理知：$(HK)/K \cong H/(H \cap K)$.

应用 6：设 $G = \{(a,b) | a,b \in R, a \neq 0\}$ 是对乘法 $(a,b)(c,d) = (ac, ad + b)$ 构成的群，$K = \{(1,b) | b \in R\}$, 则 $G/K \cong R^*$.(R^*表示正自然数)[8].

证明：对 $\forall a,b \in G$,设 $f: G \to R^*$ $(a,b) \to a$;

(1)显然 f 是 G 到 R^* 的映射；

(2)给了 R^* 的一个任意元 a,则在 G 里 $\exists (a,b) \in G$ 使得 $a \xrightarrow{f} (a,b)$;故 f 是 G 到 R^* 的满射；

(3)对 $\forall (a,b),(c,d) \in G$ 则

$f((a,b)(c,d)) = f(ac, ad + b) = ac = f(a,b)f(c,d)$,

所以 f 是 G 到 R^* 的同态映射；

综合 (1),(2),(3)知 f 是 G 到 R^* 的同态满射.

(4)同态满射的核

$f((a,b)(c,d)) = f(ac, ad + b) = ac = f(a,b)f(c,d)$,

因此，由同态基本定理知：$G/Kerf \cong R^*$,故 $G/K \cong R^*$.

本文通过群的同态与同构相关结论，结合教学经验，首先对群论中的同态与同构的一些重要结论给于分析和证明；其次，通过具体问题的分析了阐明了群的同态与同构在群论相关问题中的应用。

可以看出，寻找群 G 到群 $\overline{G}$ 的一个恰当对应法则成为解题的关键。要证明两个群同态时，首先要证明所给法则是一个映射，再说明它是满射，最后证明它满足 $\varphi(ab) = \varphi(a)\varphi(b)$,，即是同态映射就可以了。若要证明群 G 与群 $\overline{G}$ 的同构关系，需要在群同态基础上，计算同态满射的核 kerφ,最后应用群的同态基本定理获得 $G/\mathrm{Ker}\varphi \cong \overline{G}$.

因此，获得证明和求解群的同态与同构相关问题的解题思路如下：第一步：建立群 G 与群 $\overline{G}$ 的元素之间的对应关系φ并证明φ为映射；第二步：证明φ为群 G 到群 $\overline{G}$ 的满射；第三步：证明φ为群 G 到群 $\overline{G}$ 的同态映射；

从而获得群 G 与群 $\overline{G}$ 的同态关系；若需证明群 G 与群 $\overline{G}$ 同构，则继续进行

第四步：计算同态满射的核 kerφ;

第五步：应用群的同态基本定理得 $G/Ker\varphi \cong \overline{G}$.

参考文献：

[1]赵兴杰．子群陪集与群同态基本定理的一种几何模型[J]．数学杂志，2010，30(5):901-904．
[2]姚淑霞，赵传成．同态基本定理的应用之一——证明商群的同构[J]．现代经济信息，2008(4):100-101．
[3]陈国慧．同态基本定理的应用[J]．海南师范大学学报(自然科学版)，2002，15(2):18-20．
[4]金秀玲．同态基本定理的应用[J]．闽江学院学报，1999(6):1-3．
[5]张禾瑞.近世代数基础（修订版）[M].高等教育出版社,1978.
[6]杨子胥.近世代数[M].北京:中国矿业大学出版社,2008.
[7]陈国慧.同态基本定理的应用[J].湖南师范学院学报(自然科学版),2002.
[8]李倩倩,刘志刚,杨立英.群的基本同态定理的应用[J].广西师范学院学报(自然科学版),2005.

基金项目：甘肃省高等学校科研项目《时间离散的时滞反应扩散系统的行波解及其应用》(2016B-080)。

作者简介：郭俊（1997-），男，汉族，甘肃和政人，兰州城市学院数学学院。

通讯作者：姚淑霞（1980-），女，博士，副教授。