②

第 3 期　　华东师范大学学报(自然科学版)　　No.3
2000 年 9 月　　Journal of East China Normal University (Natural Science)　　Sep. 2000

文章编号:1000-5641(2000)03-0007-05

7—11

群上亚同态的一些例子

林　磊[1]，顾　沛[2]
(1. 华东师范大学数学系,上海　200062; 2. 南开大学数学系,天津　300071)

摘要: 该文给出群上亚同态的几个不同类型的例子,并确定了几个低阶群的亚同态集合。这表明"群上亚同态"这个概念具有广泛的意义,对说明亚同态的性质也有一定的作用。

关键词: 亚同态; 群; 例子　映射，群论
中图分类号: O152.7　**文献标识码**: A

群上的亚同态[1]是指群 G 上的这样一种映射,它满足如下的等式 $I(x,y)$:

$$I(x,\ y):\quad f(xyf(x)^{-1}) = f(x)f(y)f^2(x)^{-1},\ \forall x,\ y\in G$$

上式中 $f^2(x)^{-1}$ 表示 $[f^2(x)]^{-1}$。一般地,以 $f^n(x)^m$ 表示 $[f^m(x)]^m$,下同。它来源于集合上的 Yang-Baxter 方程的一个解。而集合上的 Yang-Baxter 方程的解的问题是九十年代菲尔兹奖获得者 V.G.Drinfeld 在[2]中提出来的。所以,群上亚同态的概念是有深刻背景的。

这个概念给出后,产生这样一个问题:关于群上的亚同态,除[1]中提到的"f 是 G 上的同态"及"$f(x)=x^{-1},\forall x\in G$"两个例子外,是否还能举出其它的例子?本文首先来回答这一问题。

设 G 是群。在本文中我们用 $Q(G)$ 来表示 G 上全体亚同态组成的集合,则我们有

定理 1　设 $Z(G)$ 是群 G 的中心,$a\in Z(G)$ 且 $a\neq e$(e 为 G 中单位元,下同),则由 a 决定的左平移 L_a[3]不是 G 上的同态,但 $L_a\in Q(G)$。

证　直接验证知对于 $f=L_a$,等式 $I(x,y)$ 成立,$\forall x,y\in G$。故 $L_a\in Q(G)$。当 $a\neq e$ 时,由于 $L_a(e)=a\neq e$,故 L_a 不是 G 上的同态。

定理 2　设 G 是群,$f\in Q(G)$,取 $n\in \mathbf{Z}$,定义 $g(x)=f(x)f(e)^n,\forall x\in G$,则 $g\in Q(G)$,且当 f 不是 G 上的同态时,g 一般也不是。

证　$n=0$ 时命题显然成立。而 $n>0$ 和 $n<0$ 两种情况,证明方法是类似的,所以我们只证明 $n>0$ 的情况。

据亚同态的定义,就是要证明

$$g(xyg(x)^{-1}) = g(x)g(y)g^2(x)^{-1},\ \forall x,\ y\in G. \tag{1}$$

注意到 f 是亚同态,考察(1),我们有

收稿日期:1998-06
基金项目:国家自然科学基金资助项目(19871028)
作者简介:林磊(1960—),男,副教授.

$$
\begin{aligned}
\text{左边} &= f(xy(f(x)f(e)^n)^{-1})f(e)^n = f(xyf(e)^{-n}f(x)^{-1})f(e)^n \\
&= f(x)f(yf(e)^{-n})f^2(x)^{-1}f(e)^n = f(x)f(eyf(e)^{-(n-1)}f(e)^{-1})f^2(x)^{-1}f(e)^n \\
&= f(x)f(e)f(yf(e)^{-(n-1)}f^2(e)^{-1}f^2(x)^{-1}f(e)^n \\
&= f(x)f(e)f(eyf(e)^{-(n-2)}f(e)^{-1})f^2(e)^{-1}f^2(x)^{-1}f(e)^n \\
&= f(x)f(e)f(e)f(yf(e)^{-(n-2)})f^2(e)^{-1}f^2(e)^{-1}f^2(x)^{-1}f(e)^n \\
&= \cdots\cdots \\
&= f(x)f(e)^nf(y)f^2(e)^{-n}f^2(x)^{-1}f(e)^n
\end{aligned}
$$

$$
\begin{aligned}
\text{右边} &= f(x)f(e)^nf(y)f(e)^n(f(f(x)f(e)^n)f(e)^n)^{-1} \\
&= f(x)f(e)^nf(y)f(f(x)f(e)^n)^{-1}.
\end{aligned}
$$

故(1)等价于

$$f^2(e)^{-n}f^2(x)^{-1}f(e)^n = f(f(x)f(e)^n)^{-1}, \forall x,y \in G.$$

也即

$$f(e)^{-n}f^2(x)f^2(e)^n = f(f(x)f(e)^n), \ \forall x,y \in G. \tag{2}$$

据[1]知,等式 $I(x,y)$ 对任何 $x,y\in G$ 成立等价于

$$f(x^{-1}yf(x)) = f(x)^{-1}f(y)f^2(x), \ \forall x,y \in G. \tag{3}$$

因此,f 满足(3),由此考察(2),有

$$
\begin{aligned}
\text{右边} &= f(e^{-1}f(x)f(e)^{n-1}f(e)) = f(e)^{-1}f(f(x)f(e)^{n-1})f^2(e) \\
&= f(e)^{-1}f(e^{-1}f(x)f(e)^{n-2}f(e))f^2(e) \\
&= f(e)^{-1}f(e)^{-1}f(f(x)f(e)^{n-2})f^2(e)f^2(e) \\
&= \cdots\cdots \\
&= f(e)^{-n}f(f(x))f^2(e)^n = \text{左边}.
\end{aligned}
$$

这证明了 g 是 G 上的亚同态,再用同态的定义直接计算可知,当 f 不是 G 上的同态时,g 一般不是 G 上的同态。

一般地,若 $g\in Q(G)$,$z\in G$,我们记使 $f(x)=g(x)z$,$\forall x\in G$ 的映射 f 为 g^z,则由上述定理可知:若 $f\in Q(G)$,而 $f(e)=z$,则必存在 $g\in Q(G)$,$g(e)=e$,使得 $f=g^z$。

定理 3 设 a 是群 G 中的任一元素,令 $f_{-1,a}(x)=x^{-1}a$, $\forall x\in G$,则 $f_{-1,a}\in Q(G)$.

一般地,对 $a\in G$,$n\in \mathbf{Z}$,我们可定义 G 上的映射 $f_{n,a}$: $f_{n,a}(x)=x^na$,$\forall x\in G$.

定理 4 设 G 是交换群,$a\in G$,$n\in \mathbf{Z}$,则由上述定义的 $f_{n,a}\in Q(G)$。

证 令 $f=f_{n,a}$,则 $\forall x,y\in G$,

$$
\begin{aligned}
f(xyf(x)^{-1}) &= f(xy(x^na)^{-1}) = f(xyx^{-n}a^{-1}) \\
&= (xyx^{-n}a^{-1})^na = x^ny^nx^{-n^2}a^{-n}a = x^{n-n^2}y^na^{1-n}.
\end{aligned}
$$

另一方面,

$$
\begin{aligned}
f(x)f(y)f^2(x)^{-1} &= f(x)f(y)f(x^na)^{-1} = x^nay^na((x^na)^na)^{-1} \\
&= x^ny^na^2(x^{n^2}a^{n+1})^{-1} = x^ny^na^2x^{-n^2}a^{-n-1} = x^{n-n^2}y^na^{1-n}.
\end{aligned}
$$

所以,对任何 $x,y\in G$,$I(x,y)$ 成立,即 $f_{n,a}\in Q(G)$。

定理 5 设 G 是群,$a\in G$,定义 $C_a(x)=a$,$\forall x\in G$,则 $C_a\in Q(G)$。

对于群 G,我们分别 $\mathrm{Aut}(G)$和 $\mathrm{End}(G)$表示 G 的自同构群以及 G 的全体自同态的集合,则显然我们有 $\mathrm{Aut}(G)\subset \mathrm{End}(G)\subset Q(G)$。

定理 6　设 G 是群,$f\in Q(G)$,$\varnothing\in \mathrm{Aut}(G)$,则 $\varnothing f\varnothing^{-1}\in Q(G)$。

证　令 $F=\varnothing f\varnothing^{-1}$,则对任何 $x,y\in G$

$$\begin{aligned}F(xyF(x)^{-1}) &= \varnothing f\varnothing^{-1}(xyF(x)^{-1}) = \varnothing f((\varnothing^{-1}x)(\varnothing^{-1}y)(\varnothing^{-1}F(x))^{-1})\\ &= \varnothing f((\varnothing^{-1}x)(\varnothing^{-1}y)f(\varnothing^{-1}x)^{-1}) = \varnothing[f(\varnothing^{-1}x)f(\varnothing^{-1}y)f^2(\varnothing^{-1}x)^{-1}]\\ &= \varnothing f\varnothing^{-1}(x)\varnothing f\varnothing^{-1}(y)(\varnothing f^2(\varnothing^{-1}x))^{-1} = F(x)F(y)F^2(x)^{-1}.\end{aligned}$$

所以,$\varnothing f\varnothing^{-1}\in Q(G)$。

推论　设 f 是群 G 上的映射,则 $f\in Q(G)$当有仅当存在一个 $\varnothing\in \mathrm{Aut}(G)$,使 $\varnothing f\varnothing^{-1}\in Q(G)$.

由上述定理,我们可以通过 $\varnothing\cdot f=\varnothing f\varnothing^{-1}$来定义 $\mathrm{Aut}(G)$在 $Q(G)$上的作用,并把 $Q(G)$按这一作用的轨道来进行分类。

下面,我们再就一类特殊的群来构造亚同态。

定理 7　设 H 是群 G 中指数为 2 的正规子群,若存在周期为 2 的元素 b,使 $G=H\cup Hb$. 定义 $f(h)=b$,$f(hb)=e$,$\forall h\in H$,则 $f\in Q(G)$,且 $f\notin \mathrm{End}(G)$.

证　对 x,y 属于 H 或 Hb 的情况分别验证 $I(x,y)$成立,从而 $f\in Q(G)$. 由于 $f(e)\neq e$,故显然 $f\notin \mathrm{End}(G)$。

满足定理 7 条件的群有很多,例如二面体群 D_n,n 次对群 S_n 以及正交群 $O_n(\mathbf{R})$等。

下面,我们对几个低阶的群 G 来确定集合 $Q(G)$。我们用 θ 来表示 G 上的零同态,即:$\theta(x)=e$,对所有 $x\in G$。而用 ι 来表示恒等映射。

定理 8　设 $G=\{e,a\}$是 2 阶循环群,则 $Q(G)=\{\theta,\iota,L_a,C_a\}$。

证　显然,$\theta,\iota\in \mathrm{End}(G)$,故 $\theta,\iota\in Q(G)$。又由定理 1,$L_a\in Q(G)$,由定理 5,$C_a\in Q(G)$。另一方面,G 到 G 的映射只有这 4 个,故得结论。

定理 9　设 $G=\{e,a,a^2\}$是 3 阶循环群,则 $Q(G)=\{L_x,C_x,f_{-1,x}\mid x\in G\}$。

证　设 $Q'(G)=\{L_x,C_x,f_{-1,x}\mid x\in G\}$,则由定理 1,定理 5 和定理 3 得:$Q'(G)\subset Q(G)$。另一方面,我们有 $Q'(G)=\{f:G\to G\mid |f(G)|=1$ 或 $3\}$. 所以只要证明若 f 是 G 上的映射,$|f(G)|=2$,则 $f\notin Q(G)$。由定理 2,我们还可假设 $f(e)=e$。

用反证法证明:假设 $f\in Q(G)$,若有 $x\in G$,$x\neq e$,使 $f(x)=e$。则由 $I(x,x)$得 $f(x^2)=e$,与$|f(G)|=2$ 的假设矛盾!从而可设 $f(a)=f(a^2)=x\neq e$。则由 $I(x^2,e)$得 $f(x)=e$,矛盾!这就证明了我们的结论,即 $Q(G)=Q'(G)$。

最后,我们来考察非交换群 $G=S_3=\{e,a,a^2,b,ab,a^2b\}$,其中 $a^3=b^2=e$,$bab=a^{-1}$。回忆一下 $\mathrm{Aut}(G)=\{\varnothing_x\mid x\in G\}$,其中 $\varnothing_x$ 是由 x 决定的内自同构,即 $\varnothing_x(y)=xyx^{-1}$,对所有 $y\in G$。$\mathrm{End}(G)=\mathrm{Aut}(G)\cup\{\varnothing_1=\theta,\varnothing_2,\varnothing_3,\varnothing_4\}$,其中 $\ker\varnothing_i=A_3$,$i=2,3,4$,$\varnothing_2(G)=\{e,b\}$,$\varnothing_3(G)=\{e,ab\}$,$\varnothing_4(G)=\{e,a^2b\}$。

定理 10　设 $G=S_3=\{e,a,a^2,b,ab,a^2b\}$. 则 G 的所有亚同态的集合为

$$Q(G)=\mathrm{End}(G)\cup\{\varnothing_2^{b},\varnothing_3^{ab},\varnothing_4^{a^2b},f_{-1,z},C_z\mid Z\in G\}。\tag{4}$$

证　首先我们记等式(4)的右边为 $Q'(G)$。由于 $S_3=A_3\cup A_3x$,$x\in\{b,ab,a^2b\}$,而

x 是周期为 2 的元素,故由定理 7 知,$\varnothing_2^b,\varnothing_3^{ab}$ 以及 $\varnothing_4^{a^2b}\in Q(G)$。而由定理 3 和定理 5 得 $f_{-1,z},C_z\in Q(G),\forall z\in G$. 所以,$Q'(G)\subset Q(G)$。

其次,我们来证明 $Q(G)\subset Q'(G)$。第一步我们先证明若 $f\in Q(G),f(e)=e$,则 $f\in \mathrm{End}(G)$或 $f=f_{-1,e}$。

(i)设 $f(a)=e$. 则由 $I(a,a)$得 $f(a^2)=e$。由 $I(a^j,b)$得 $f(a^jb)=f(b),j=1,2$。若 $f(b)=a^i(i=0,1,2)$,则由 $I(b,b)$得 $a^{2i}=e$,所以 $i=0$. 从而 $f(b)\in\{e,b,ab,a^2b\}$. 显然此时有 $f\in\mathrm{End}(G)$。

(ii)设 $f(a)=a$. 由 $I(a,y)$得

$$f(aya^{-1})=af(y)a^{-1},\forall y\in G. \tag{5}$$

所以

$$f(ab)=a^2f(b)a^{-2},\ f(a^2b)=af(b)a^{-1}. \tag{6}$$

设 $f(b)=a^\kappa(\kappa=0,1,2)$,则由(5)得 $f(a^2b)=f(ab)=f(b)=a^\kappa$。由 $I(b,a)$得 $f(a^\kappa)=a$,故 $\kappa\neq 0$。

若 $\kappa=1$,则由 $I(b,b)$得 $f(a^2)=a$,这导致 $I(a^2,e)$不成立。

若 $\kappa=2$,则由 $f(a^2)=a$ 同样导致$I(a^2,e)$不成立。所以,$f(b)\in\{b,ab,a^2b\}$。

若 $f(b)=b$,则由(6)得,$f(ab)=ab,f(a^2b)=a^2b$。由 $I(b,a^2)$得,$f(a^2)=a^2$,故 $f=\iota\in\mathrm{End}(G)$。

若 $f(b)=ab$,则 $f(ab)=a^2b$, $f(a^2b)=b$。同理由 $I(b,a^2)$,得 $f(a^2)=a^2$,所以 $f=\varnothing_{a^2}\in\mathrm{End}(G)$。

若 $f(b)=a^2b$,则 $f(ab)=b$、$f(a^2b)=ab$。由 $I(b,a^2)$以及 $I(a^2b,a^2)$,得 $f(a^2)=a^2$. 故 $f=\varnothing_a\in\mathrm{End}(G)$。

(iii)设 $f(a)=a^2$,由 $I(a,a)$得 $f(a^2)=a$。由 $I(a,y)$, 得 $f(aya)=a^2f(y)a^2$, $\forall y\in G$,由于 $a(a^ib)a=a^ib$, 故 $f(a^ib)=a^2f(a^ib)a^2$。而 $a^2a^ja^2=a^{j+1}\neq a^j$, 所以 $f(a^ib)\in\{b,\ ab,\ a^2b\}$, $i=0,1,2$。

当 $f(b)=b$ 时,由 $I(b,ab)$得

$$f(a^2b)=bf(ab)b. \tag{7}$$

若 $f(ab)=b$, 则 $I(ab,e)$不成立,若 $f(ab)=ab$, 则由(7)得,$f(a^2b)=a^2b$。此时 $f=f_{-1,e}$,若 $f(ab)=a^2b$, 则由(7)得 $f(a^2b)=ab$。此时 $f=\varnothing_b\in\mathrm{End}(G)$。

当 $f(b)=ab$ 时,由 $I(b,e)$得 $f(ab)=b$。又由 $I(b,\ a^2b)$及 $I(ab,\ a^2b)$得 $f(a^2b)=a^2b$,即 $f=\varnothing_{a^2b}\in\mathrm{End}(G)$。

当 $f(b)=a^2b$ 时,令 $g=\varnothing_bf\varnothing_b^{-1}$. 则 $g(a^i)=a^{-i}$, $g(b)=ab$。因此由上述讨论得 $g(ab)=b$, $g(a^2b)=a^2b$。所以 $f(ab)=ab$, $f(a^2b)=b$。即 $f=\varnothing_{ab}\in\mathrm{End}(G)$.

(iv)设 $f(a)=b$,由 $I(a,e)$得 $f(ab)=bf(b)^{-1}$。由 $I(a,\ ab)$得 $f(a^2)=f(b)^{-2}$。又由 $I(a,a^2)$得 $f(a^2)=bf(b)^2$。从而 $bf(b)^2=f(b)^{-2}$。得 $f(b)^4=b$. 矛盾!

(v)设 $f(a)=ab$,令 $g=\varnothing_af\varnothing_a^{-1}$。由于 $g(e)=e$, $g(a)=b$,故 g 满足(iv)的假设,所以 $g\notin Q(G)$, 由定理 6 的推论得 $f\notin Q(G)$。

(vi)设 $f(a)=a^2b$,则如上类似的讨论,由于 $\varnothing_{a^2}f\varnothing_{a^2}^{-1}\notin Q(G)$。故 $f\notin Q(G)$。

第二步，若 $f\in Q(G)$、$f(e)=z\neq e$，则存在 $g\in Q(G)$，而 $g(e)=e$，使得 $f=g^z$。

若取 $g=f_{-1,e}$，则 $g^z=f_{-1,z}\in Q'(G)$。下面我们对每个 $g\in \mathrm{End}(G)$ 以及 $z\in G$，$z\neq e$，来逐个验证是否 $f=g^z\in Q(G)$。

若 $g=\theta$，则 $g^z=C_z\in Q(G)$，而 $C_z\in Q'(G)$. 若 $g=\iota$、而 $f\in Q(G)$，则由 $I(x,e)$ 得 $zx=xz$，$\forall x\in G$. 即 $z\in Z(G)=\{e\}$，矛盾. 故对 $z\neq e$，$\iota^z\notin Q(G)$。对一般的 g，若 $f=g^z\in Q(G)$，则由 $I(e,e)$ 得 $f(z^{-1})=z^2f(z)^{-1}$。又由于 $f(z^{-1})=g(z^{-1})z=g(z)^{-1}z$，$f(z)=g(z)z$ 得，$g(z)z=zg(z)$，即 z 与 $g(z)$ 可交换。从而当 $z=b$ 时，$g=\varnothing_b$ 或 $\varnothing_2$；当 $z=ab$ 时，$g=\varnothing_{ab}$ 或 $\varnothing_3$；当 $z=a^2b$ 时，$g=\varnothing_{a^2b}$ 或 $\varnothing_4$。

而当 $f=\varnothing_b^b$ 时，由 $I(e,y)$ 得 $yb=by$，$\forall y\in G$，矛盾。故 $\varnothing_b^b\notin Q(G)$。又由于 $\varnothing_{ab}^{ab}=\varnothing_{a^2}\varnothing_b^b\varnothing_{a^2}^{-1}$，$\varnothing_{a^2b}^{a^2b}=\varnothing_a\varnothing_b^b\varnothing_a^{-1}$，故 $\varnothing_{ab}^{ab}$，$\varnothing_{a^2b}^{a^2b}\notin Q(G)$。另一方面，$\varnothing_2^b$、$\varnothing_3^{ab}$、$\varnothing_4^{a^2b}\in Q'(G)$。

最后，设 $f=\varnothing_q^a$，$q\in G$。则由 $I(x,e)$ 得 $xa=ax$，$\forall x\in G$，矛盾！从而 $\varnothing_q^a\notin Q(G)$. 而 $\varnothing_q^{a^2}=\varnothing_b\varnothing_x^a\varnothing_b^{-1}$，其中 $x=\varnothing_b(q)$。从而 $\varnothing_q^{a^2}\notin Q(G)$，于是我们证明了结论。

[参　考　文　献]

[1] 顾沛. 集合上的 Yang-Baxter 方程的又一个解与"群上的亚同态"[J]. 科学通报，1997，42(15)：1602～1605

[2] Drinfeld V G. On some unsolved problems in quantum group theory [J]. Lecture Notes in Math, 1992, 1510：1～8.

[3] 孟道骥. 代数学基础[M]. 天津：南开大学出版社，1992.

Some Examples of Metahomomorphisms on Groups

LIN Lei[1], GU Pei[2]

(1. *Department of Mathematics, East China Normal University, Shanghai* 200062, *China*;
2. *Department of Mathematics, Nankai University, Tianjin* 300071, *China*)

Abstract: In this paper we give some examples of metahomomorphisms on groups, which indicate the generality of the concept and are useful for understanding properties of metahomomorphisms. We also determine the sets of metahomomorphisms on some groups of lower orders.

Key words: metahomomorphism; group; example