第八讲同态基本定理

陈建文

November 10, 2022

定义1. 设$(G_1,\circ)$与$(G_2,*)$为两个群，如果存在一个从G_1到G_2的映射ϕ，使得$\forall a,b\in G_1$，

$$\phi(a\circ b)=\phi(a)*\phi(b)$$

则称G_1与G_2同态，ϕ称为从G_1到G_2的一个同态（*homomorphism*）。如果同态ϕ为满射，则称ϕ为从G_1到G_2的一个满同态，此时称G_1与G_2为满同态，并记为$G_1\sim G_2$。类似的，如果同态ϕ为单射，则称ϕ为单同态。

定理1. 设$(G_1,\circ)$与$(G_2,*)$为两个群，e_1和e_2分别为其单位元，ϕ为从G_1到G_2的同态，则

$$\begin{aligned}&\phi(e_1)=e_2\\&\forall a\in G_1\phi(a^{-1})=(\phi(a))^{-1}\end{aligned}$$

证明. 由$\phi(e_1)=\phi(e_1\circ e_1)=\phi(e_1)*\phi(e_1)$知$\phi(e_1)=e_2$。$\forall a\in G_1,\phi(a^{-1})*\phi(a)=\phi(a^{-1}\circ a)=\phi(e_1)=e_2$，从而$(\phi(a))^{-1}=\phi(a^{-1})$。 □

定理2. 设$(G_1,\circ)$为一个群，$(G_2,*)$为一个代数系。如果存在一个满射$\phi:G_1\to G_2$使得$\forall a,b\in G_1$

$$\phi(a\circ b)=\phi(a)*\phi(b)$$

则$(G_2,*)$为一个群。

证明. 验证$\forall x,y,z\in G_2,(x*y)*z=x*(y*z)$：由$\phi$为满射知$\exists a,b,c\in G_1$使得$\phi(a)=x,\phi(b)=y,\phi(c)=z$，从而$(x*y)*z=(\phi(a)*\phi(b))*\phi(c)=\phi(a\circ b)*\phi(c)=\phi((a\circ b)\circ c)$，$x*(y*z)=\phi(a)*(\phi(b)*\phi(c))=\phi(a)*\phi(b\circ c)=\phi(a\circ(b\circ c))$，$(x*y)*z=x*(y*z)$，这验证了在$G_2$中$*$运算满足结合律。

$\forall x\in G_2$，由ϕ为满射知$\exists a\in G_1$使得$\phi(a)=x$，于是$\phi(e)*x=\phi(e)*\phi(a)=\phi(e\circ a)=\phi(a)=x$。

$\forall x\in G_2$，由ϕ为满射知$\exists a\in G_1$使得$\phi(a)=x$，于是$\phi(a^{-1})*\phi(a)=\phi(a^{-1}\circ a)=\phi(e_1)$。 □

例. 设$n\in Z^+$，$Z_n'=\{0,1,\cdots,n-1\}$，在Z_n'上定义运算"$\oplus$"如下：$i\oplus j=(i+j)\bmod n$，令$f:Z\to Z_n'$，$\forall m\in Z,f(m)=m\bmod n$，则$f$为从$Z$到$Z_n'$的满射，并且$\forall a,b\in Z$，$f(a+b)=f(a)\oplus f(b)$，从而$(Z_n',\oplus)$为一个群。

证明. f显然为从Z到Z_n'的满射。要证$\forall a, b \in Z$，$f(a+b) = f(a) \oplus f(b)$，就是要证$(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$，此式显然成立。 □

定理3. 设ϕ为从群$(G_1, \circ)$到群$(G_2, *)$的同态，则

（*1*）如果H为G_1的子群，那么$\phi(H)$为G_2的子群；

（*2*）如果H为G_2的子群，那么$\phi^{-1}(H)$为G_1的子群；

（*3*）如果N为G_1的正规子群，那么$\phi(N)$为$\phi(G_1)$的正规子群；

（*4*）如果N为$\phi(G_1)$的正规子群，那么$\phi^{-1}(N)$为G_1的正规子群。

证明. 以下设G_1的单位元为e_1，G_2的单位元为e_2。

（1）$e_2 = \phi(e_1) \in \phi(H)$，从而$\phi(H)$非空。

$\forall x, y \in \phi(H)$，$\exists a, b \in H$使得$x = \phi(a)$，$y = \phi(b)$，则$x * y^{-1} = \phi(a) * \phi(b)^{-1} = \phi(a) * \phi(b^{-1}) = \phi(a \circ b^{-1}) \in \phi(H)$。

以上验证了$\phi(H)$为G_2的子群。

（2）由$\phi(e_1) = e_2 \in H$知$e_1 \in \phi^{-1}(H)$，从而$\phi^{-1}(H)$非空。

以下证明$\forall a, b \in \phi^{-1}(H)$，$a \circ b^{-1} \in \phi^{-1}(H)$，即$\phi(a \circ b^{-1}) \in H$。

$\forall a, b \in \phi^{-1}(H)$，则$\phi(a) \in H$，$\phi(b) \in H$，从而$\phi(a \circ b^{-1}) = \phi(a) * \phi(b^{-1}) = \phi(a) * \phi(b)^{-1} \in H$，于是$a \circ b^{-1} \in \phi^{-1}(H)$。

这验证了$\phi^{-1}(H)$为G_1的子群。

(3) $\phi(N)$显然为$\phi(G_1)$的子群。

以下证明$\forall h \in \phi(N), \forall g \in \phi(G_1), g * h * g^{-1} \in \phi(N)$。

$\forall h \in \phi(N)$，$\exists b \in N$使得$h = \phi(b)$，$\forall g \in \phi(G_1), \exists a \in G_1$，使得$g = \phi(a)$。于是，$g*h*g^{-1} = \phi(a)*\phi(b)*\phi(a)^{-1} = \phi(a \circ b)*\phi(a^{-1}) = \phi(a \circ b \circ a^{-1}) \in \phi(N)$，因此$\phi(N)$为$G_2$的正规子群。

（4）由（2）知$\phi^{-1}(N)$为G_1的子群。

要证$\phi^{-1}(N)$为G_1的正规子群，就是要证$\forall g \in \phi^{-1}(N), \forall a \in G_1, a \circ g \circ a^{-1} \in \phi^{-1}(N)$，而$\phi(a \circ g \circ a^{-1}) = \phi(a) * \phi(g) * \phi(a^{-1}) = \phi(a) * \phi(g) * \phi(a)^{-1} \in N$，从而$a \circ g \circ a^{-1} \in \phi^{-1}(N)$，结论得证。

□

定义2. 设ϕ为从群$(G_1, \circ)$到群$(G_2, *)$的一个同态，e_2为G_2的单位元，则G_1的子群$\phi^{-1}(\{e_2\})$称为同态ϕ的核，记为$Ker\phi$。$\phi(G_1)$称为在ϕ下G_1的同态像。

定理4. 设ϕ为从群$(G_1, \circ)$到群$(G_2, *)$的一个同态，则$Ker\phi$为群G_1的正规子群。

证明. 设群G_2的单位元为e_2，由$\{e_2\}$为群$\phi(G_1)$的正规子群知，$Ker\phi = \phi^{-1}(\{e_2\})$为$G_1$的正规子群。 □

定理5. 设N为G的一个正规子群，ϕ为从G到G/N的一个映射，$\forall x \in G \phi(x) = xN$，则$\phi$为从$G$到$G/N$的一个满同态，$Ker\phi = N$。

证明. $\forall x, y \in G, \phi(xy) = (xy)N = (xN)(yN) = \phi(x)\phi(y)$，这验证了$\phi$为从$G$到$G/N$的一个同态。

ϕ显然为从G到G/N的满射，因此ϕ为从G到G/N的满同态。

$\forall g \in G, g \in Ker\phi \Leftrightarrow \phi(g) = N \Leftrightarrow gN = N \Leftrightarrow g \in N$。 □

定理6 (群的同态基本定理)**.** 设ϕ为从群$(G_1, \circ)$到群$(G_2, *)$的同态，则$G_1/Ker\phi \cong \phi(G_1)$。

证明. 记$K=Ker\phi$。令$f:G_1/K\to\phi(G_1)$，$\forall gK\in G_1/K, f(gK)=\phi(g)$。

设G_1的单位元为e_1，G_2的单位元为e_2。$\forall g_1,g_2\in G_1$，如果$g_1K=g_2K$，则$g_1=g_1e_1\in g_1K=g_2K$，从而$\exists x\in K$使得$g_1=g_2\circ x$，于是$\phi(g_1)=\phi(g_2\circ x)=\phi(g_2)*e_2=\phi(g_2)$，所以$f(g_1K)=f(g_2K)$，这验证了$f$为映射。

f为单射，这是因为$\forall g_1K,g_2K\in G_1/K$，如果$f(g_1K)=f(g_2K)$，则$\phi(g_1)=\phi(g_2)$。设$g_1=g_2\circ x$，这里$x\in G_1$。于是，$\phi(g_1)=\phi(g_2)*\phi(x)$，由$\phi(g_1)=\phi(g_2)$知$\phi(x)=e_2$，所以$x\in K$。因此，$g_1K=(g_2\circ x)K=g_2(xK)=g_2K$。

f为满射，这是因为$\forall g_2\in\phi(G_1)$，$\exists g_1\in G_1$使得$\phi(g_1)=g_2$，于是$f(g_1K)=\phi(g_1)=g_2$。

$\forall g_1K,g_2K\in G_1/K$，$f((g_1K)(g_2K))=f((g_1\circ g_2)K)=\phi(g_1\circ g_2)=\phi(g_1)*\phi(g_2)=f(g_1K)*f(g_2K)$，因此$f$为从$G_1/K$到$\phi(G_1)$的同构。 □

课后作业题:

练习1. 设$(G,\circ)$为m阶循环群，$(\bar{G},\cdot)$为n阶循环群，试证：$G\sim\bar{G}$当且仅当$n|m$。

证明. 由$G\sim\bar{G}$往证$n|m$:

设ϕ为从G到$\bar{G}$的一个满同态，由群同态基本定理，$G/Ker\phi\cong\bar{G}$，于是$|G/Ker\phi|=|\bar{G}|$。由拉格朗日定理，$|G|=|G/Ker\phi||Ker\phi|$，这说明$|G/Ker\phi|||G|$，从而$|\bar{G}|||G|$，即$n|m$。

设$n|m$，往证$G\sim\bar{G}$:

设$G=(a)$，$\bar{G}=(b)$。

令$\phi:G\to\bar{G}$，$\forall i\in Z$，$\phi(a^i)=b^{i \bmod n}$。

$\forall i,j\in Z, i\neq j$，如果$a^i=a^j$，则$a^{j-i}=e$，从而$m|(j-i)$，由$n|m$知$n|(j-i)$，于是$i \bmod n=j \bmod n$，从而$b^{i \bmod n}=b^{j \bmod n}$，这验证了映射定义的合理性。

$\forall i,j\in Z$，$\phi(a^i\circ a^j)=\phi(a^{i+j})=b^{(i+j) \bmod n}=b^{(i \bmod n+j \bmod n) \bmod n}=b^{i \bmod n+j \bmod n}=b^{i \bmod n}\cdot b^{j \bmod n}=\phi(a^i)\cdot\phi(a^j)$。这证明了$\phi$为从$G$到$\bar{G}$的同态，$\phi$显然为满同态，于是$G\sim\bar{G}$。 □

练习2. 设G为一个循环群，H为群G的子群，试证：G/H也为循环群。

证明. 由G为循环群知G为交换群，从而H为G的正规子群。设$G=(a)$，$\forall x\in G/H$，存在自然数i使得$x=a^iH=(aH)^i$，于是$G/H=(aH)$，即G/H为循环群。 □