17.6 正规子群与商群

- 正规子群及判定
  - 定义
  - 判别定理
  - 判别法
- 商群
  - 定义及其实例
  - 性质

正规子群及其判定

正规子群：$H\le G$,，且$\forall a\in G$，$aH=Ha$. 记为$H\trianglelefteq G$.

判定定理： $N\le G$, 则下述条件等价

(1) N 是G 的正规子群

(2) $\forall g\in G, gNg^{-1}=N$

(3) $\forall g\in G, \forall n\in N, gng^{-1}\in N$

证： (1) $\Rightarrow$(2): $gN=Ng \Rightarrow gNg^{-1}=N$

(2) $\Rightarrow$(3): $gng^{-1}\in gNg^{-1}=N$

(3)$\Rightarrow$(1): $ng\in Ng\Rightarrow n\in N,g^{-1}\in G\Rightarrow g^{-1}ng\in N$

$\Rightarrow ng\in gN$

$gn\in gN\Rightarrow n\in N,g\in G\Rightarrow gng^{-1}\in N\Rightarrow gn\in Ng$

判定方法

判定方法

(1) 判定定理

(2) $|N|=t$, N 是G 的唯一t 阶子群

(3) 指数为2 的子群

证明

N是G的t 阶子群,且是唯一的t 阶子群,则N是G的正规子群.

证明 任取$g\in G$，则$gNg^{-1}\leq G$.（证明$N\approx gNg^{-1}$ ）

令$f:N\to gNg^{-1}$，$f(n)=gng^{-1}$，$\forall n\in N$

假若$f(n_1)=f(n_2)$,则有$gn_1g^{-1}=gn_2g^{-1}$,

从而推出 $n_1=n_2$，即f是单射。

任取$gng^{-1}\in gNg^{-1}$，则有$n\in N$且$f(n)=gng^{-1}$,

所以f是满射。从而$N\approx gNg^{-1}$。

由于G只有一个t阶子群，故$gNg^{-1}=N$。

$<N,*>$是$<G,*>$的正规子群。

证明（续）

N是G的子群，且$[G:N]=2$, 则N是G的正规子群.

证 $N\leq G$,且$[G:N]=2$.

则$G=N\cup Ng$, $\forall g\notin N$,

由于$N\cap Ng=\varnothing$，则有

$Ng=G-N$, $\forall g\notin N$.

同理可证$gN=G-N=Ng$, $\forall g\notin N$.

任取$g\in G$,若$g\in N$,则$Ng=N=gN$;

若$g\notin N$,则$Ng=G-N=gN$

从而$H\trianglelefteq G$.

举例

例 设$A=\{1,2,3\}$，$f_1,f_2,\ldots,f_6$是A上的双射函数。其中

$f_1=\{\langle 1,1\rangle,\langle 2,2\rangle,\langle 3,3\rangle\}$，　　$f_2=\{\langle 1,2\rangle,\langle 2,1\rangle,\langle 3,3\rangle\}$

$f_3=\{\langle 1,3\rangle,\langle 2,2\rangle,\langle 3,1\rangle\}$，　　$f_4=\{\langle 1,1\rangle,\langle 2,3\rangle,\langle 3,2\rangle\}$

$f_5=\{\langle 1,2\rangle,\langle 2,3\rangle,\langle 3,1\rangle\}$，　　$f_6=\{\langle 1,3\rangle,\langle 2,1\rangle,\langle 3,2\rangle\}$

令$G=\{f_1,f_2,\ldots,f_6\}$，则G关于函数的复合运算构成群。G的全体子群是：

$H_1=\{f_1\}$，　$H_2=\{f_1,f_2\}$，　$H_3=\{f_1,f_3\}$

$H_4=\{f_1,f_4\}$，$H_5=\{f_1,f_5,f_6\}$，$H_6=G$

H_1, H_6是平凡子群，故也是正规子群；

$[G:H_5]=2$,故H_5是正规子集。

H_2,H_3和H_4不是正规子群。

商群定义、性质

商群 $G/H = \{ Ha \mid a \in G \}$, $(Ha) \circ (Hb) = Hab$

说明:

良定义性质:

$$Ha=Hx,\ Hb=Hy \Rightarrow Hab=Hxy$$

商群G/H 就是商代数

$aRb \Leftrightarrow Ha=Hb \Leftrightarrow ab^{-1} \in H$

$aRb,\ cRd \Rightarrow ac\ R\ bd$

$aRb \Rightarrow a^{-1}Rb^{-1}$

性质: $|G/H|=[G:H]$，商群的阶是$|G|$的因子

保持群G 的性质：交换性，循环性等, 单位元

举例

例1 G 为Abel 群，$|G| = n$, 素数p 整除n, 则G 中有p 阶元.

证明思路：归纳法——商群满足条件推出原来群中性质.

归纳步骤. 假设$m<n$ 为真，证明对于n 为真.

设$|G| = n$, 取$a\in G$, $a \neq e$, $|a|\,|\,n$,寻找p 阶元.

① p 整除 $|a|$, 则$a^{|a|/p}$ 为p 阶元.

② p 不整除 $|a|$, 令$H = \langle a\rangle$, 构造G/H, $|G/H| = m$,

则$n=m|H|$，p不整除$|H|$，故p 整除m.

根据归纳假设，G/H 中必有p 阶元Hb, 导出b 与a 的关系

$$(Hb)^p = H \Rightarrow Hb^p = H \Rightarrow b^p\in H \Rightarrow b^p = a^t$$

$(a^{|a|})^t = e \Rightarrow (b^p)^{|a|} = e \Rightarrow (b^{|a|})^p = e \Rightarrow b^{|a|}$为$p$ 阶元

($b^{|a|}=e \ \Rightarrow (Hb)^{|a|}=H \Rightarrow p \mid |a|$,矛盾.)

17.7 群的同态与同构

定义 f 为G_1 到G_2 的同态当且仅当

$f: G_1 \to G_2$, 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$<Z_n,\oplus>$的自同态:

$f_p(x)=(px)\bmod n,\ p=0,1,\ldots,n-1$

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

$f: Z \to Z_n,\ f(x)=(x)\bmod n$

说明：将群看成代数系统$<G, \circ, ^{-1}, e>$，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

$f(e_1)=e_2$，$f(x^{-1})=f(x)^{-1}$，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

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

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

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

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

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

同态基本定理

(1) H 为G 的正规子群，则G/H 是G 的同态像

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

同态性质的证明

证明 (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) 显然$\ker f$非空. $\forall a,b\in \ker f$,

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

$\ker f$ 为G_1 的子群，下面证明正规性.

$\forall g\in G_1, \forall a\in \ker f$,

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

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

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

基本同态定理的证明

- f是G到G/H的满同态，$\forall a\in G$，$f(a)=Ha$，即$f(G)= G/H$
  $<G/H,\circ>$是$<G,*>$的同态像。
- 设φ是G到G'的满同态，$\ker\varphi \trianglelefteq G$，且
  $G/\ker\varphi=\{a\ker\varphi|a\in G)\}$
- 定义同于关系$R,\forall a,b\in G,aRb\Leftrightarrow \varphi(a)= \varphi(b)$
  商代数$G/R=\{[a]|a\in G\}$
- 证明G/R就是 $G/\ker\varphi$，或者两者同构
  $[a]=[b] \Leftrightarrow aRb \Leftrightarrow\varphi(a)= \varphi(b) \Leftrightarrow a\ker\varphi= b\ker\varphi$
  $[a]\circ[b]=[ab]$, $a\ker\varphi \circ b\ker\varphi=ab\ker\varphi$
- 根据同态基本定理有$G/R\cong G'$，从而$G/\ker\varphi\cong G'$

例9

例9 $<G,*>$是群，$<H,*>$和$<K,*>$是$<G,*>$的正规子群且$H\subseteq K$，证明 $G/K\cong(G/H)(K/H)$。

证明 定义 $\varphi: G/H\to G/K$， $\varphi(Ha)=Ka$，$\forall Ha\in G/H$，

则 $Ha=Hb \Rightarrow ab^{-1}\in H \Rightarrow ab^{-1}\in K \Rightarrow Ka=Kb$

所以φ是良定义的。易见φ是满射且$\forall Ha,Hb\in G/H$有

$\varphi(HaHb)=\varphi(Hab)=Kab=KaKb=\varphi(Ha)\varphi(Hb)$

于是φ是满同态 $\ker\varphi=K/H$。$<G/K,\circ>$的幺元是K,

$\varphi(Ha)=Ka=K\Leftrightarrow a\in K \Leftrightarrow \ker\varphi=\{Ha|a\in K\}=K/H$

根据同态基本定理， $G/K\cong(G/H)(K/H)$。

同态的分类

定义 设 f 是由 $G_1=\langle A, \bigstar\rangle$ 到 $G_2=\langle B,*\rangle$ 的一个同态,

(1) 如果 f 是从 A 到 B 的一个满射,则 f 称为**满同态**;G_2 是 G_1 的同态像.

(2) 如果 f 是从 A 到 B 的一个入射,则 f 称为**单一同态**;

(3) 如果 f 是从 A 到 B 的一个双射,则 f 称为**同构映射**,并称 $\langle A, \bigstar\rangle$ 和 $\langle B,*\rangle$ 是同构的,记作 $A\cong B$.

(4) 如果 $G_1=G_2$,则 f 称为**自同态**;若 $G_1=G_2$, f 是双射,则 f 称为**自同构**.

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

$$f_x: G\to G, f_x(a)=xax^{-1}$$

关系：

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$G$

总结

- 正规子群的定义和判定
- 商群的定义
- 同态性质及其应用
- 作业：习题十七 48、53、58

实例分析

例题1 $G_1=\langle R,+\rangle$是实数加群， $G_2=\langle R-\{0\},\cdot\rangle$是非零实数关于普通乘法构成的群，令

$$f: R\to R-\{0\}，f(x)=e^x$$

证明f是G_1到G_2的同态映射。

实例分析（续）

例题2 代数系统<*B*,⊕>和<*C*,*>都与 <*A*, ★>同构。

<*A*, ★>

★	*a*	*b*
a	*a*	*b*
b	*b*	*a*

<*B*, ⊕ >

⊕	偶	奇
偶	偶	奇
奇	奇	偶

<*C* * >

*	0^o	180^o
0^o	0^o	180^o
180^o	180^o	0^o

总结

形式上不同的代数系统，如果彼此同构，那么可抽象地把它们看作是本质上相同的代数系统，不同的只是所用的符号不同。

同构的逆仍是一个同构。

实例分析（续）

例题3 代数系统$<Z, \bullet>$, Z是整数集, $\bullet$为普通乘法.

$R=\{<a,b>|a,b\in Z$而且a,b的符号相同$\}$,

证明R是Z上的同余关系,并求$<Z, \bullet>$的同态像.

证 $\forall <a,b>,<c,d>\in R$，有三种情况：

(1) a,c 同号，有$<a \bullet c, b \bullet d>\in R$

(2) a,c异号，有$a \bullet c <0, b \bullet d <0$，即 $<a\bullet c, b\bullet d>\in R$

(3)a,b,c,d都为0，有$<a \bullet c$，$b \bullet d>\in R$

故R是Z上的同余关系。

实例分析（续）

$Z/R=B=\{$正整数集合，负整数集合，零$\}$

在B上定义二元运算如下

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

则$<B, \odot>$是$<Z, \bullet>$的同态象。

例题分析

例题4 设f_1, f_2都是从$<A, ★>$到$<B,*>$的同态.设映射

g：$A \to B$，$\forall a \in A$　　$g(a)=f_1(a)*f_2(a)$

证明：如果$<B,*>$是一个可交换半群，那么g是一个由$<A, ★>$到$<B,*>$的同态。

证 $\forall x,y \in A$，

$g(x★y)=f_1(x★y)*f_2(x★y)$

$=f_1(x)*f_1(y)*f_2(x)*f_2(y)$　（f是同态，且*满足结合律）

$=f_1(x)*f_2(x)*f_1(y)* f_2(y)$　（*满足交换律）

$=(f_1(x)*f_2(x))*(f_1(y) *f_2(y))$

$=g(x)*g(y)$　　得证

实例分析

例题5 设$G_1=\langle Q,+\rangle$是有理数加群，$G_2=\langle Q^*,\cdot\rangle$是非零有理数乘法群。证明不存在$G_2$到$G_1$的同构。

证明 假设φ是G_2到G_1的同构，那么有

$$\varphi: G_2 \to G_1,\ \varphi(1)=0\ (\text{幺元})$$

于是有

$$\varphi(-1)+\varphi(-1)$$

$$=\varphi((-1)(-1))$$

$$=\varphi(1)$$

$$=0$$

从而得$\varphi(-1)=0$，这与φ的单射性矛盾。

例题分析

例题6 循环群的同态象必定是循环群。

证明 设<G,*>是循环群，其生成元是a，同态映射为f，同态象为$<f(G), \cdot>$。则任取$a^m, a^n \in G$，有

$$f(a^m * a^n) = f(a^m) \cdot f(a^n)$$

下面证任意$f(a^l) \in f(G)$都可表示成$f(a)$的幂的形式。

当$m=1$时，有$f(a)=f(a)$

当$m=2$时，有$f(a^2)=f(a*a)=f(a) \cdot f(a)=f(a)^2$

假设$m=k\text{-}1$时$f(a^{k-1})=f(a)^{k-1}$，则

$$f(a^k)= f(a^{k-1}*a)= f(a^{k-1}) \cdot f(a)= f(a)^{k-1} \cdot f(a)=f(a)^k$$

因此$<f(G), \cdot>$是以$f(a)$为生成元的循环群。

实例分析

例题7 设$<G,\cdot>$是一个群，$<H,\cdot>$是$<G,\cdot>$的正规子群，$<K,\cdot>$是$<G,\cdot>$的子群，且$H\subseteq K\subseteq G$，若$<K/H,\circ>$是$<G/H,\circ>$的正规子群，则$<K,\cdot>$是$<G,\cdot>$的正规子群。

证 设f是G到G/H的自然同态，即$\forall g\in G$，有$f(g)=Hg$

因为$K\subseteq G$，故$\forall k\in K$，有$f(k)=Hk$，所以$f(K)=K/H$.

因为$<K/H,\circ>$是$<G/H,\circ>$的正规子群，

所以$\forall Hk\in K/H, Hg\in G/H$，有$Hg\circ Hk\circ Hg^{-1}\in K/H$

$Hg\circ Hk\circ Hg^{-1}=Hgkg^{-1}=f(gkg^{-1})\in K/H$

因此$gkg^{-1}\in K$，所以$<K,\cdot>$是$<G,\cdot>$的正规子群。