第十七章习题课—群的证明

- 规范证明的主要内容
  - 集合和二元运算构成群
  - 群G 的给定子集H构成子群
  - 群G 的给定子群是正规的
  - f是群G_1到G_2的同态映射
  - 证明群G_1同构于G_2
  - 证明群G_1不同构于G_2
- 比较灵活的证明
  - 群的基本性质的证明
  - 元素相等的证明
  - 与数的相等或者整除相关的证明
  - 子集相等

证明群或者子群

证明群: 验证下述条件之一

(1) 封闭性、结合律、单位元、每个元素有逆

(2) 封闭性、结合律、右单位元、每个元素有右逆

(3) 封闭性、结合律、方程有解

(4) 封闭性、结合律、有限、无零元、消去律

证明H是G的子群: 判定定理

前提: H是G的非空子集 (进行验证)

验证下述条件之一

(1) $\forall x, y \in H,\ xy \in H, x^{-1} \in H.$

(2) $\forall x, y \in H,\ xy^{-1} \in H$

(3) H有限, $\forall x, y \in H,\ xy \in H$

证明正规性或者同态

证明子群N 的正规性

验证下述条件之一：

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

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

(3) $|N|=n$, N是G的唯一的n阶子群

(4) $[G:N]=2$

证明f是G_1到G_2的同态

(1) 验证 $f: G_1\rightarrow G_2$（注意良定义性的验证）

(2) 验证$\forall x, y\in G_1$, $f(xy)=f(x)f(y)$

证明同构

方法一：证明$f: G_1 \to G_2$是同态，证明f为双射

方法二：同态基本定理：其中一个群是商群

例 1：设R是实数加群，则$R\times R=\{<a, b>|a, b\in R\}$ 关于分量的加法构成群。令$N=\{<0, b>|b\in R\}$。证明：N是$R\times R$的正规子群，且$(R\times R)/N\cong R$.

证：先证明N为正规子群（略）

定义$f: R\times R\to R$, $f(<a, b>)=a$, $\forall <a, b>\in R\times R$

验证f 为映射，满射，同态.

验证$\ker f =N$.

由同态基本定理$R\times R/N \cong R$.

证明不同构

反证法

例2 证明不存在$<Q^*, \cdot>$到$<Q, +>$的同构.

证 假设存在同构$f: Q^* \rightarrow Q$,

则$f(1)=0$,

$0 = f(1) = f((-1)(-1))$

$= f(-1)+f(-1) = 2f(-1)$,

从而$f(-1) = 0$

与f的单射性矛盾。

灵活的证明

- 群的基本性质的证明（略）
  - 证明有关元素的运算等式
  - 证明元素的阶相等
  - 证明交换性
- 和Lagrange定理有关的证明
  - 与群相关的数量结果
  - 证明数的整除或者相等
  - 证明群的其他性质
- 与同态性质相关的证明
  - 证明数的整除或者相等（与Lagrange定理联系）
  - 证明集合相等
  - 证明群的其他性质

与有限群相关的数量结果

(1) $|G| = [G:H]|H|$

$|G| = |G/H||H|$

$|a|\,|\,|G|,\ a \in G$

(2) $f: G \to G'$是满同态 $\Rightarrow |G'|\,|\,|G|$且$|G'| = |G/\ker f|$

(3) $|G| = n$, p为素数，$p|n$, G为Abel群

$\Rightarrow G$中含p阶元

(4) $|\overline{a}| = [G:N(a)]$ a 的正规化子$N(a)$ = $\{x \in G | xa=ax\}$

(5) A, B是G的子群，A, B有限，则 $|AB| = \dfrac{|A||B|}{|A \cap B|}$

证明

例 3 设A, B是G的子群，且A, B有限，则 $|AB| = \dfrac{|A||B|}{|A\cap B|}$

证：(1) 在$A\times B$上定义二元关系R，$<x, y>R<u, v> \Leftrightarrow xy=uv$

(2) 证明R为等价关系（略）

(3) 令$X=[<a, b>]=\{<x, y> \mid <a, b>R<x, y>\}$

$f: X\to A\cap B,\quad f(<x, y>)=a^{-1}x$

(4) f 为函数. $<x, y>R<a, b> \Rightarrow xy=ab \Rightarrow a^{-1}x=by^{-1}\in A\cap B$

f 单射. $f(<x, y>)=f(<u, v>) \Rightarrow a^{-1}x=a^{-1}u \Rightarrow x=u$

$\Rightarrow x=u, y=v \Rightarrow <x, y>=<u, v>$

f 满射. $\forall c\in A\cap B, \exists <ac, c^{-1}b>\in A\times B, <ac, c^{-1}b>\in X$

$f(<ac, c^{-1}b>)=a^{-1}ac=c$

(5) $|X|=|A\cap B|$, 有$|A\cap B|$个$<x, y>$使得xy相等，即

$|A||B|=|A\times B|=|A\cap B|\,|AB|$

证明

例 3 设A, B是G的子群，且A, B有限，则$|AB| = \dfrac{|A||B|}{|A \cap B|}$

证(II)：因为G的子集AB由形如$Ax\ (x \in B)$的A的右陪集的并组成，每个右陪集含有$|A|$个元素，故只需证明AB中含有$|B: A\cap B|$个A的右陪集。

根据$Ax=Ay \Leftrightarrow xy^{-1} \in A \Leftrightarrow xy^{-1} \in A\cap B \Leftrightarrow (A\cap B)x=(A\cap B)y$

知：AB中A的右陪集的个数$=B$中$A\cap B$的右陪集的个数$|B: A\cap B|$，故得证。

Lagrange定理的应用-1

证明整除

例4 G为n阶群，$a\in G, |\overline{a}|=k, C$为中心，$|C|=c$，则$k|(n/c)$.

证：$|\overline{a}|=[G:N(a)]\Longrightarrow k=[G:N(a)]$

$C\le N(a)\Longrightarrow |C|\,\big|\,|N(a)|\Longrightarrow c\,\big|\,|N(a)|$

$\Longrightarrow |N(a)|=cs$

$|G|=[G:N(a)]|N(a)|\Longrightarrow n=kcs, n/c=ks$

命题得证。

Lagrange定理的应用-2

确定子群或商群的阶

例 5 H_1, H_2为r, s 阶子群，$(r, s)=1$，则 $H_1 \cap H_2=\{e\}$

证明群的性质

$|G|=p^s, p$ 为素数，则 $p \mid |C|$.

例 6 证明p^2阶的群为Abel 群，其中p是素数.

证 取C, 则$|C|=p$或 p^2. (根据群方程，$|C|>1$). 若$|C|=p^2$, 得证.

若$|C|=p$, 作G/C, 则$|G/C|=p$, 由拉格朗日定理推论$G/C=\langle Cb\rangle$,

$\forall x, y \in G, Cx \in G/C \Rightarrow Cx = Cb^i \Rightarrow xb^{-i} \in C \Rightarrow x = c_1 b^i$

同理有$y = c_2 b^j$，于是

$$xy = c_1 b^i c_2 b^j = c_1 c_2 b^i b^j = c_1 c_2 b^{i+j}$$

$$yx = c_2 b^j c_1 b^i = c_2 c_1 b^{j+i}$$

$$\Rightarrow xy = yx$$

Lagrange定理的应用-3

例 7 设G是pm阶有限群，其中p是素数，m为正整数，且$m<p$，证明G的p阶子群是正规子群.

证：设$H=\{a_1=e, a_2, \ldots, a_p\}$是$G$的$p$阶子群. 取$x\in G$，令

$$xHx^{-1} = \{b_1=e, b_2, \ldots, b_p\}$$

(1) 若$xHx^{-1}=H$，则H是正规的.

(2) 若$xHx^{-1}\neq H$，则$xHx^{-1}\cap H$是H的子群，由Lagrange定理，$|xHx^{-1}\cap H| = p$或者1. 若$|xHx^{-1}\cap H| = p$，与$xHx^{-1}\neq H$ 矛盾；若$|xHx^{-1}\cap H| = 1$，则a_ib_j $(i, j=1,2,\ldots, p)$是G中p^2个互不相等的元素, 否则$a_ib_j=a_kb_l \Rightarrow a_k^{-1}a_i=b_lb_j^{-1} \in xHx^{-1}\cap H=\{e\} \Rightarrow a_k=a_i, b_j=b_l$，与$|G|=mp<p^2$ 矛盾。

同态的相关结果

(1) $f(xy) = f(x)f(y)$

$f(e) = e$

$f(x^{-1}) = f(x)^{-1}$

(2) G 交换 $\Rightarrow f(G)$交换

G 循环 $\Rightarrow f(G)$循环

(3) $H \leq G \Rightarrow f(H) \leq f(G)$

H正规，满同态 $\Rightarrow f(H)$正规

(4) ker$f$ 是G的正规子群

同态基本定理

同态证明题分析

证集合相等

例 8 设 f 为G_1到G_2的同态，则

$$f^{-1}(f(a)) = a\ker f$$

证 对一切$a\in G_1$,

$$\begin{aligned} x\in f^{-1}(f(a)) &\Leftrightarrow f(x) = f(a) \\ &\Leftrightarrow f(a)^{-1}f(x) = e_2 \\ &\Leftrightarrow f(a^{-1}x) = e_2 \\ &\Leftrightarrow a^{-1}x\in \ker f \\ &\Leftrightarrow x\in a\ker f \end{aligned}$$

同态与Lagrange定理

例 9 设$G_1=\langle a\rangle$, $G_2=\langle b\rangle$为m, n阶群，证明

G_2是G_1的同态像 $\Leftrightarrow n|m$

证 ($\Leftarrow$) 定义 $f(a^i)=b^i$, 则

$$a^i = a^j \Leftrightarrow m|(i-j) \Rightarrow n|(i-j) \Leftrightarrow b^i = b^j;$$

$$f\left(a^i a^j\right) = f\left(a^{i+j}\right) = b^{i+j} = b^i b^j = f\left(a^i\right) f\left(a^j\right);$$

另，显然f为满射。故f为满同态。

($\Rightarrow$) f是G_1到G_2的满同态，$G_2 \cong G_1/\ker f$,

$n=|G_2|=|G_1/\ker f|$, $|G_1/\ker f| \mid m \Rightarrow n|m$.

同态性质的应用

例 10 设H为有限群G的子群，N为G的正规子群。若 $(|H|, [G:N])=1$，证明H是N的子群。

证 令$g: G\to G/N$为自然同态，

则$g(H)\le G/N$

因此$|g(H)| \mid [G:N]$, 又$|g(H)| \mid |H|$

$(|H|,[G:N]) = 1 \Rightarrow |g(H)|=1$

所以$g(H)=\{N\}$

$x\in H \Rightarrow xN=g(x)=N \Rightarrow x\in N$

课后练习60

60. 设f是群G的满自同态，若G只有有限个子群，证明f是G的自同构。

证：由同态基本定理有$G/\mathrm{ker}f \cong G$，所以$G/\mathrm{ker}f$的子群与G的子群一一对应。$G/\mathrm{ker}f$的子群形式为$H/\mathrm{ker}f$，其中$\mathrm{ker}f \leq H \leq G$. 由于$G$只有有限个子群，所以$G/\mathrm{ker}f$只有有限个子群，设为$H_1/\mathrm{ker}f, \ldots, H_m/\mathrm{ker}f$，其中$\mathrm{ker}f \leq H_i \leq G$. 因此G至少有子群$H_1, \ldots, H_m$. 如果$\mathrm{ker}f$不是$\{e\}$，那么这些$H_i$至少包含两个元素。因此，$\{e\}$是$G$的，与这些$H_i$都不相同的子群，所以$G$的子群至少有$m+1$个，矛盾！因此$\mathrm{ker}f=\{e\}$, 即$f$为单同态，从而证明了$f$为自同构。