近世代数

计算机科学与技术学院
苏敬勇

内容

- 第一章 基本概念
- 第二章 群
- 第三章 正规子群和群的同态与同构
- 第四章 环与域
- 第五章 因子分解
- 第六章 域的扩张

多选题 1分

设置

以下关于同态同构叙述正确的是（ ）

两代数系统同态，前面的是群后边的也成群

两代数系统同态，后边的是群前边的也成群

两群之间有同态映射，就可保证单位元的像映为单位元

两群之间有同态映射，就可保证逆元的像映为像的逆元

提交

多选题 1分

设置

以下关于同态同构叙述正确的是（ ）

A 两代数系统同态，前面的是群后边的也成群

B 两代数系统同态，后边的是群前边的也成群

C 两群之间有同态映射，就可保证单位元的像映为单位元

D 两群之间有同态映射，就可保证逆元的像映为像的逆元

提交

第二章 群

- 群同态与同构的简单性质
- 正规子群和商群
- 群同态基本定理
- 群的同构定理
- 群的自同构群
- *Sylow定理
- *有限交换群

正规子群和商群

- **定义1**：设N是群G的一个子群。如果对G中每个元素 a都有

$$aN = Na，即 \ aNa^{-1} = N,$$

则称N是G的一个正规子群（或不变子群）。

就是说正规子群的**任何一个左陪集都是一个右陪集**，因此简称为**陪集**。

记为 $N \trianglelefteq G$；若N不是G的正规子群记为 $N \ntrianglelefteq G$。

若 $N \trianglelefteq G$ 且 $N \neq G$，则记为 $N \triangleleft G$。

•任意一个群G都至少有其平凡子群｛e｝与G本身是其正规子群，称为G的**平凡正规子群**。G的其他正规子群若存在的话称为G的**非平凡正规子群**。

•任意一个群G的中心是其正规子群，$C \trianglelefteq G$。

•交换群的任意一子群都是该群的正规子群。

•设$N \trianglelefteq G$，又 $N \leq H \leq G$，则 $N \trianglelefteq H$

正规子群和商群

- **例1：** $N=\{(1),(123),(132)\}$ 是三元对称群S_3 的一个正规子群。但是，S_3 的三个子群

$$H_1=\{(1),(12)\}，\quad H_2=\{(1),(13)\}，\quad H_3=\{(1),(23)\}$$

都不是 S_3的正规子群。

证明：对 S_3 中任意元素 σ 有

$$\sigma N\sigma^{-1}=\left\{(1),\sigma\left(123\right)\sigma^{-1},\sigma\left(132\right)\sigma^{-1}\right\}=N$$

故 $N\trianglelefteq S_3$。

但由于$\left(13\right)H_1\neq H_1\left(13\right)$，故$H_1\ntrianglelefteq S_3$。类似可证$H_2$ 和H_3也不是 S_3的正规子群

正规子群和商群

- **定理1**：设G是群，$N \leq G$。则 $N \trianglelefteq G \Leftrightarrow aNa^{-1} \subseteq N$ （$\forall a \in G$）。

证明：必要性显然。

充分性，设对G中任意元素a有$aNa^{-1} \subseteq N$，则

$$aNa^{-1}a \subseteq Na \text{，即} \quad aN \subseteq Na$$

又由 $a^{-1}Na \subseteq N$ 可得 $Na \subseteq aN$。因此，

$$aN = Na$$

即 $N \trianglelefteq G$ 。

- **注**：本定理也可改述为：G是群，$N \leq G$，则

$$N \trianglelefteq G \Leftrightarrow axa^{-1} \in N \quad (\forall a \in G, \forall x \in N)$$

正规子群和商群

- **例2**：n元交代群An是n元对称群Sn的一个正规子群。

证明：任意的n元置换σ 与其逆σ^{-1}具有相同的奇偶性，从而易知$\sigma A_n \sigma^{-1} \subseteq A_n$

故$A_n \trianglelefteq S_n$。

- **例3**：证明：Klein四元群

$$K_4 = \{(1),(12)(34),(13)(24),(14)(23)\}$$

是S_4的一个正规子群，因而也是交代群A_4的一个正规子群。

证明：K_4 中除了单位元外的三个元素是 S_4中仅有的阶为2的偶置换，任取其中一个，设为x，则对任意的4元置换 σ，乘积 $\sigma x \sigma^{-1}$ 仍是一个2阶偶置换，从而

$$\sigma x \sigma^{-1} \in K_4 \quad ,$$

故 $K_4 \trianglelefteq S_4$，于是 $K_4 \trianglelefteq A_4$ 。

正规子群和商群

- 又由于K_4是交换群，故

$$B_4=\{(1),(12)(34)\}\trianglelefteq K_4$$

从而有$B_4 \trianglelefteq K_4 \trianglelefteq S_4$，但是$B_4 \ntrianglelefteq S_4$：因有

$$(13)B_4 \neq B_4(13)$$ 。

- **注**：正规子群的正规子群不一定是原群的正规子群。即，正规子群不具有传递性。

- **定理2**：设 φ 是群G到群 $\bar{G}$ 的同态满射，则

1） $N \trianglelefteq G \Rightarrow \varphi(N) \trianglelefteq \bar{G}$ ；

2） $\bar{N} \trianglelefteq \bar{G} \Rightarrow \varphi^{-1}(\bar{N}) \trianglelefteq G$ 。

证明：1）因为$N \trianglelefteq G$，故由上节定理2可知，

$$\varphi(N) \leq \bar{G}$$

任取 $\bar{n} \in \varphi(N), \bar{a} \in \bar{G}$ ，由于 φ 是同态满射，可令

正规子群和商群

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

其中 $a \in G, n \in N$ ，于是

$$ana^{-1} \to \bar{a} \cdot \bar{n} \cdot \bar{a}^{-1} \quad 。$$

但是 $N \trianglelefteq G, ana^{-1} \in N$ ，故$\bar{a} \cdot \bar{n} \cdot \bar{a}^{-1} \in \varphi(N)$，从而

$$\bar{a} \cdot \varphi(N) \cdot \bar{a}^{-1} \subseteq \varphi(N) \quad , \quad \varphi(N) \trianglelefteq \bar{G} \text{ 。}$$

2）若$\bar{N} \trianglelefteq \bar{G}$，则任取$a \in G, n \in \varphi^{-1}(\bar{N})$，由于 φ是G到 $\bar{G}$的同态满射，故存在 $\bar{a} \in \bar{G}, \bar{n} \in \bar{N}$ 使得，

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

从而 $ana^{-1} \to \bar{a} \cdot \bar{n} \cdot \bar{a}^{-1}$，而 $\bar{a} \cdot \bar{n} \cdot \bar{a}^{-1} \in \bar{N}$，故 $ana^{-1} \in \varphi^{-1}(\bar{N})$

于是有

$$a\varphi^{-1}(\bar{N})a^{-1} \subseteq \varphi^{-1}(\bar{N}), \quad \varphi^{-1}(\bar{N}) \trianglelefteq G \text{ 。}$$

正规子群和商群

- **定理3**：群G的一个正规子群与一个子群的乘积是一个子群；两个正规子群的乘积仍是一个正规子群。

证明：1）设$N \trianglelefteq G, H \le G$，任取

$$nh \in NH \qquad (n \in N, h \in H),$$

由于 $Nh = hN$，故

$$nh \in Nh = hN \subseteq HN \qquad (n \in N, h \in H)$$

故 $NH \subseteq HN$，同理 $HN \subseteq NH$，于是有 $NH = HN$，故$NH \le G$。

实际上这一情况可以考察$(n_1h_1)(n_2h_2)^{-1} \in NH \qquad (\forall n_1h_1, n_2h_2 \in NH)$来实现。

而
$$\begin{aligned}(n_1h_1)(n_2h_2)^{-1} &= n_1h_1 \cdot h_2^{-1}n_2^{-1} \\ &= n_1\left(h_1h_2^{-1}\right)n_2^{-1} \\ &= n_1\,h_3n_2^{-1} \\ &= n_1\,n_3h_3 \\ &= n_4\,h_3 \in NH\end{aligned}$$

正规子群和商群

2)设 $N \trianglelefteq G, K \trianglelefteq G$，则由上知，$NK \le G$

对任意的 $a \in G$，有

$$a(NK) = (aN)K = (Na)K$$
$$= N(aK) = N(Ka) = (NK)a$$

故，$NK \trianglelefteq G$。

- **陪集乘法**：设N是群G的一个正规子群，任取二陪集 aN 与 bN，根据群中子集乘法有

$$(aN)(bN) = a(Nb)N = a(bN)N$$
$$= (ab)NN = abN$$

即 $(aN)(bN) = (ab)N$。我们称此为陪集的乘法。

•群G关于N的陪集集合在陪集乘法下作成一个代数系统；或者说陪集乘法是全体陪集的一个代数运算。

正规子群和商群

- **定理4**：群G的正规子群N的全体陪集对于陪集乘法作成一个群，称为G关于N的**商群**，记为G/N。

证明：首先，陪集乘法满足结合律。（原因最终归结与群中乘法满足结合律）

其次，考虑单位元和逆元的存在问题。N为单位元显然。

由于

$$\left(a^{-1}N\right)\left(aN\right)=a^{-1}aN=N,$$

故 $a^{-1}N$ 是 aN 的逆元，即 $\left(aN\right)^{-1}=a^{-1}N$。因此，G/N作成群。

•**注**：

1）$\left(aN\right)^{m}=a^{m}N \qquad \left(\forall m\in Z\right)$

2）$\left|G/N\right|=\left(G:N\right)$

3)Lagrange定理变形：$\left|G\right|=\left|N\right|\cdot\left(G:N\right)=\left|N\right|\cdot\left|G/N\right|$

$$\left|G/N\right|=\frac{\left|G\right|}{\left|N\right|}$$

正规子群和商群

- **定理5（A.L.Cauchy）**：设G是一个pn阶有限交换群，其中p是一个素数，则G有p阶元素，从而有p阶子群。

证明：对n用数学归纳法。

当n=1时，G的阶为p，由于p为一素数，故G为一循环群，有$G=\langle a\rangle$，生成元a的阶数就为p， 定理结论成立。

假定定理对阶为pk（$1\le k<n$）的交换群成立，下证对阶为pn的交换群G定理成立。（**目标找到G中某个元素，它的阶为p**）

在G中任取$a\neq e$，若$p\,\|a|$，令$|a|=ps$，则$|a^s|=p$，定理成立。

若$p\nmid|a|$，令$|a|=m>1$，则$(m,p)=1$，由于

$$m\,|\,pn,$$

故$m\,|\,n$。令$N=\langle a\rangle$，则由于G是交换群，故

$$|G/N|=p\cdot\frac{n}{m},\qquad 1\le\frac{n}{m}<n$$

于是由归纳假设，群G/N中有p阶元素，任取其一，设为bN，且$|b|=r$，则

正规子群和商群

$(bN)^r = b^r N = N$ 故有 $p|r$，于是可令 $r = pt$，则得 $|b^t| = p$ 。

•**注**：实际上，当G是非交换群时，这个定理仍成立。

•**推论**：pq（p，q为互异素数）阶交换群为循环群。

证明：由上定理知G有p阶元素a与q阶元素b，又因为p与q是互异素数，由第二章第2节定理4可知ab的阶为pq，即$|ab| = pq = |G|$。

实际上，首先 $(ab)^{pq} = a^{pq}b^{pq} = (a^p)^q (b^q)^p = e$，若有 $(ab)^r = a^r b^r = e$，则

$$p|r, q|r$$

但$(p,q)=1$，故有$pq|r$，故$|ab| = pq = |G|$。

•**更一般地**，阶为$p_1 p_2 \cdots p_s$ $(p_i\text{为互异素数})$的交换群必为循环群。

•注意这里的交换群是必要的，例如$6 = 2 \cdot 3$ 阶群 S_3就不是循环群。

多选题 1分

设置

以下关于正规子群和商群说法正确的是（ ）

正规子群是群中左右陪集相等的子群

有限群的商群的阶数是大群阶数的因子

有限群阶数为两互异素数乘积则其为循环群

群中正规子群与正规子群的乘积还是其正规子群

提交

多选题 1分

设置

以下关于正规子群和商群说法正确的是（ ）

A 正规子群是群中左右陪集相等的子群

B 有限群的商群的阶数是大群阶数的因子

C 有限群阶数为两互异素数乘积则其为循环群

D 群中正规子群与正规子群的乘积还是其正规子群

提交

正规子群和商群

•**定义2**：每个子群都是正规子群的非交换群，称为**哈密顿群**。

哈密顿（W.R.Hamilton，1805-1865）首先研究此群。

•**例4**：四元数群

$$G=\{1,i,j,k,-1,-i,-j,-k\}$$

是一个哈密顿群。

证明：首先，G是非交换群。其次，G的真子群只有

$$\langle -1\rangle,\quad \langle i\rangle,\ \langle j\rangle,\ \langle k\rangle.$$

而 $\langle -1\rangle \trianglelefteq G$显然。又令

$$N=\langle i\rangle, x\in G$$

由 $N=\{1,-1,i,-i\}$，故易知

$$\{x,-x,xi,-xi\}=\{x,-x,ix,-ix\}$$

即 $xN=Nx$，即得 $N\trianglelefteq G$。同理$\langle j\rangle$与$\langle k\rangle$也是G的正规子群。因此，G为哈密顿群。

正规子群和商群

- **注**：1、2、3、5、7阶群都是循环群，从而是交换群也就不是哈密顿群；4和6阶群也都不是哈密顿群，由上例可知4元数群（8阶）是阶数最小的哈密顿群。

实际上，4和6阶要么是循环群要么分别同构与 K_4 和 S_3 ，可知他们也非哈密顿群。

哈密顿群的研究很多...周期群、群中元素的阶有限。。。

•**定义3**：阶大于1且只有平凡正规子群的群，称为**单群**。

例如，素数阶群显然都是单群；

S_3不是单群；

A_4不是单群；A_2是单位元群；A_3 是单群。

特别当 $n \geq 5$时，可证明 A_n 是单群。

利用$n \geq 3$但$n \neq 4$ 时A_n 是单群，可得$S_n\left(n \neq 4\right)$ 的正规子群除去两个平凡正规子群$\{e\}$和 S_n外只有A_n 。

正规子群和商群

- 证明上结论：设$N \trianglelefteq S_n$，则$N \cap A_n \trianglelefteq A_n$。但 A_n是单群，故

$$N \cap A_n = A_n \quad 或 \quad N \cap A_n = \{(1)\}$$

当$N \cap A_n = A_n$ 时，$A_n \subseteq N$ 。由于置换群不是全由偶置换组成就是含奇、偶置换各一半，故

$$N = A_n \quad 或 \quad N = S_n 。$$

当$N \cap A_n = \{(1)\}$时，必有$N = \{(1)\}$:若否则可设N除了恒等置换外还包含有一个奇置换，设为τ 。于是

$$N = \{(1), \tau\} \trianglelefteq S_n 。$$

从而对S_n中任意σ ，必有$\sigma N \sigma^{-1} = N$，即

$$\sigma \tau \sigma^{-1} = \tau \quad 或 \quad \sigma \tau = \tau \sigma$$

亦即τ 是 S_n 的中心元。但当$n \geq 3$时S_n是无中心群，即其中心元只有(1)，故有$N = \{(1)\}$。

因此 S_n 的正规子群只有 $\{(1)\}, A_n, S_n$ 。

正规子群和商群

- **定理6**：有限交换群G为单群的充要条件是，$|G|$为素数。

证明：充分性显然。

必要性：设G是一个单群，且$|G|=n>1$。在G中任取元素 $a\neq e$。若 $|a|<n$

由G是交换群，故

$$\{e\}\trianglelefteq\langle a\rangle\trianglelefteq G$$

这与G是单群矛盾，故必有 $|a|=n=|G|$，从而$G=\langle a\rangle$ 为n阶循环群。再由G为单群可知，n必为素数。

•**有限单群是一类重要的群**：素数阶群、交代群 $A_n(n\geq 5)$、有限李型单群和26个零散单群。

•**每个有限单群都同其中的一个单群同构**。

作业：

- P62. 1、证明：指数是2的子群必是正规子群。
- 2、证明：若群G的n阶子群只有一个，则此子群必为G的正规子群。