近世代数

计算机科学与技术学院
唐琳琳

内容

第二章 群

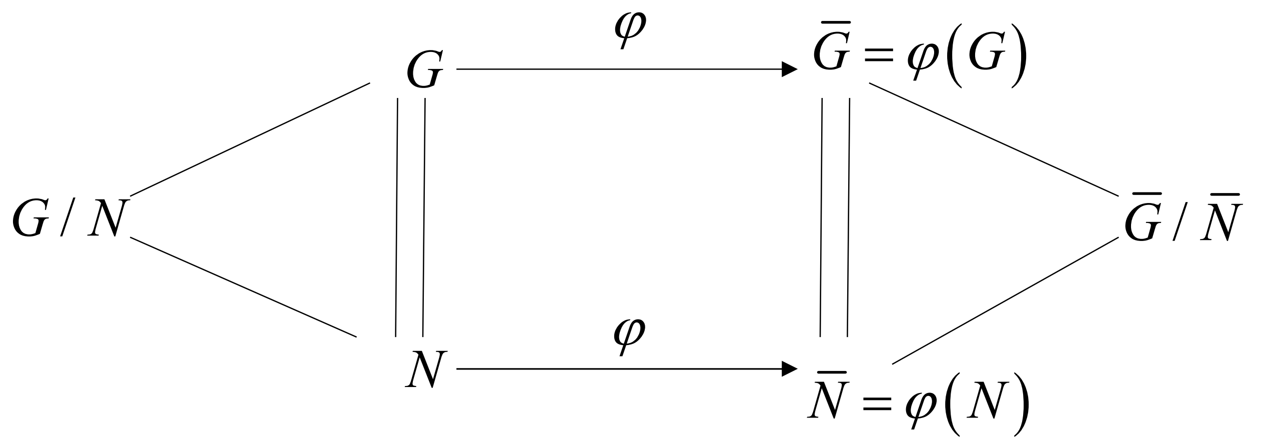
- 群同态与同构的简单性质
- 正规子群和商群
- 群同态基本定理
- 群的同构定理
- 群的自同构群
- *Sylow定理
- *有限交换群

群的同构定理

- **定理1（第一同构定理）：** 设φ是群G到群 $\bar{G}$ 的一个同态满射，又$Ker\varphi \subseteq N \trianglelefteq G$ ，$\bar{N}=\varphi(N)$，则

$$G/N \cong \bar{G}/\bar{N} \text{ 。}$$

证明：目标找到一个同构映射。首先给出一个结构图，体现几个群和正规子群、商群的关系。



群的同构定理

因为$N \trianglelefteq G$，φ 是满同态，故 $\bar{N}=\varphi(N)\trianglelefteq \bar{G}$ 。现在令

$$\tau: \quad G/N \to \bar{G}/\bar{N}$$
$$xN \to \varphi(x)\varphi(N) \qquad (\forall x \in G)$$

1）τ 是映射：设 $aN=bN(a,b\in G)$，则 $a^{-1}b\in N$，于是有

$$\varphi(a)^{-1}\varphi(b)=\varphi\left(a^{-1}b\right)\in\varphi(N)=\bar{N}$$

从而 $\varphi(a)\bar{N}=\varphi(b)\bar{N}$，故$\tau$ 是G/N到$\bar{G}/\bar{N}$ 的映射。

2）τ 是满射：任取$\bar{a}\bar{N}\in\bar{G}/\bar{N}\left(\bar{a}\in\bar{G}\right)$，则因$\varphi$ 是满同态，故有 $a\in G$，使$\varphi(a)=\bar{a}$

从而在τ 之下$\bar{a}\bar{N}$ 有逆象 aN，即τ 是满射。

3）τ 是单射：设$\varphi(a)\bar{N}=\varphi(b)\bar{N}$，则

$$\varphi\left(a^{-1}b\right)=\varphi(a)^{-1}\varphi(b)\in\bar{N}$$

故有$c\in N$ 使

$$\varphi\left(a^{-1}b\right)=\varphi(c)\text{或}\varphi\left(c^{-1}a^{-1}b\right)=\bar{e}$$

其中$\bar{e}$ 是$\bar{G}$的单位元。于是有 $c^{-1}a^{-1}b\in Ker\varphi$，故$c\cdot c^{-1}a^{-1}b\in N$，即得 $aN=bN$。

群的同构定理

也即τ为一单射。

故 τ 为一双射。

下证其保持运算。由于

$$aN\cdot bN=abN\to\varphi(ab)\bar{N}=\varphi(a)\varphi(b)\bar{N}=\varphi(a)\bar{N}\cdot\varphi(b)\bar{N}$$

故 τ 保持运算，它是 G/N 到$\bar{G}/\bar{N}$的同构映射。因此$G/N\cong\bar{G}/\bar{N}$ 。

•注：1）以上同构也可以写为 $G/N\cong\varphi(G)/\varphi(N)$ 。若形如定理1则 φ 必为满同态，N必为G的包含同态核的正规子群。

2）定理1的又一证法，利用上一节的“群同态基本定理”，考虑群$G\sim\bar{G}/\bar{N}$ ，也即$a\to\varphi(a)\bar{N}$，实际上此映射为同态满射，且同态核为N。

• 推论：设H，N是群G的两个正规子群，且$N\subseteq H$，则

$$G/H\cong G/N/H/N$$

证明：由自然同态知道$G\sim G/N$ ，同态核为N，从而根据定理1可得上结论成立

。

群的同构定理

- **例1**：设H，K是群G的两个正规子群。证明：

$$G/HK \cong G/H\,/\,HK/H$$

证明：因为$H \trianglelefteq G, K \trianglelefteq G$，故 $HK \trianglelefteq G$。又显然$H \trianglelefteq HK$，故直接由以上推论知上结论成立。

•**定理2（第二同构定理）**：设G是群，又$H \le G$，$N \trianglelefteq G$。则 $H \cap N \trianglelefteq H$，且

$$HN/N \cong H/(H \cap N)$$

证明：首先$HN \le G$，且$N \trianglelefteq HN$，易知

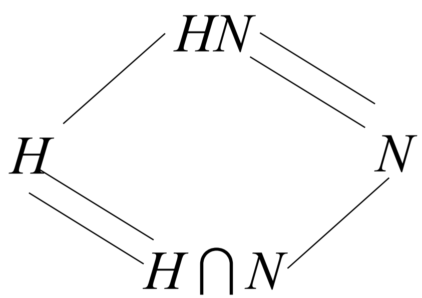
$$\varphi : x \to xN \qquad (\forall x \in H)$$

注：（$H \to HN/N$）

为一同态满射，且同态核为$H \cap N$，由群同态基本定理知：$H \cap N \trianglelefteq H$ 且

$$HN/N \cong H/(H \cap N)。$$

如右下图示：



群的同构定理

- **例2**：设S_3,S_4 分别为三、四元对称群，K_4 为Klein四元群。证明：

$$S_4/K_4\cong S_3$$

证明：因为 $S_3\le S_4$ （把 S_3 中每个置换 τ 视为$\tau(4)=4$），又$K_4\trianglelefteq S_4$ ，故

$$K_4\trianglelefteq S_3K_4\le S_4$$

而 $S_3\cap K_4=\{(1)\}$ 。从而

$$|S_3K_4|=\frac{|S_3|\cdot|K_4|}{|S_3\cap K_4|}=\frac{6\cdot 4}{1}=24$$

于是有 $S_3K_4=S_4$ ，由第二同构定理可得

$$S_4/K_4=S_3K_4/K_4\cong S_3/(S_3\cap K_4)\cong S_3$$

因此原结论成立：$S_4/K_4\cong S_3$ 。

群的同构定理

- **定理3（第三同构定理）：设G是群，又$N \trianglelefteq G$，$\bar{H} \le G/N$ 。则**

1）存在G得唯一子群$H \supseteq N$，且$\bar{H}=H/N$；

2）又当 $\bar{H} \trianglelefteq G/N$ 时，有唯一的$H \trianglelefteq G$ 使

$$\bar{H}=H/N \text{ 且 } G/H \cong G/N/H/N$$

证明：1）考虑自然同态

$$\tau : G \sim G/N$$

设$\bar{H}$在同态映射τ下的逆象为H 。则$N \subseteq H=\tau^{-1}\left(\bar{H}\right) \le G$，且由于$\tau$ 为一同态满射，故有

$$\tau\left(H\right)=\tau\left[\tau^{-1}\left(\bar{H}\right)\right]=\bar{H}$$

而 $\tau\left(H\right)=H/N$，故可得原求证结论成立$\bar{H}=H/N$。再分析，由于上节定理4可知G中包含N的不同的子群对应的像也是不同的，故H的存在是唯一的。

群的同构定理

2）继续考虑自然同态不难知道，当 $\bar{H}$为G/N的正规子群时，G有唯一的正规子群$H\supseteq N$，使得 $\bar{H}=H/N$。还是考虑自然同态，利用第一同构定理不难得到

$$G/H \cong G/N/H/N$$

原结论成立。

•注：该定理表明，商群G/N的子群仍为商群，且形如H/N，其中H为包含N的G的子群；H是G的正规子群当且仅当H/N为G/N的正规子群。

多选题 1分

设置

以下关于群同态基本定理和群的同构定理叙述正确的是（）

A 任一群在同构的意义下只能与自己的商群同态。

B 由群同态基本定理知道循环群的商群是循环群。

C 群的第一同构定理中的两群同态可以换成他们之间有一个同态映射，原结论仍成立。

D 由第二同构定理不难知道 $S_4/K_4 \cong S_3$。

提交

群的自同构群

- **定理1：**设M是有一个代数运算（叫做乘法）的代数系统，则M的全体自同构关于变换的乘法作成一个群，称为M的自同构群。

证明：封闭性：设 σ,τ 是M的任意两个自同构，则对M中的任二元素 a,b 有

$$\sigma\tau(ab)=\sigma[\tau(ab)]$$

$$=\sigma[\tau(a)\tau(b)]=\sigma\tau(a)\cdot\sigma\tau(b)$$

即$\sigma\tau$ 也是M的一个自同构。

逆元存在性：又因为对M的任意元素 x 有

$$\sigma\sigma^{-1}(x)=\sigma^{-1}\sigma(x)=x$$

考虑 σ^{-1}的保持运算性质，对于任意M中二元素如上a,b有

$$\sigma^{-1}(ab)=\sigma^{-1}\left[\sigma\sigma^{-1}(ab)\right]$$

$$=\sigma^{-1}\left[\sigma\sigma^{-1}(a)\cdot\sigma\sigma^{-1}(b)\right]$$

$$=\sigma^{-1}\left[\sigma\left(\sigma^{-1}(a)\cdot\sigma^{-1}(b)\right)\right]$$

$$=\sigma^{-1}(a)\cdot\sigma^{-1}(b)$$

群的自同构群

即 σ^{-1} 也是M的自同构。因此，M的自同构关于变换乘法作成群，也是$S(M)$的一个子群。

•**推论1**：群G的全体自同构关于变换乘法作成一个群。这个群称为群**G**的自同构群，记为**AutG**。

•**例1**：求Klein四元群

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

的自同构群。

解：分析：首先自同构把原群中的单位元映射为单位元，其他元素可能对应的情况数目成了自同构可能有的个数。

故，S_3即对应所有K_4的自同构，即$AutK_4=S_3$。

$$\begin{pmatrix} e & a & b & c \\ e & x & y & z \end{pmatrix}$$

群的自同构群

- **定理2**：无限循环群的自同构群是一个2阶循环群；n阶循环群的自同构群是一个$\varphi(n)$阶群，其中$\varphi(n)$为Euler函数。

证明：首先，无限循环群有两个生成元，生成元的个数即是可能的自同构的个数。故结论成立。

其次，因n阶有限循环群共有$\varphi(n)$个生成元，故其自同构群为$\varphi(n)$阶群。

•**推论2**：无限循环群的自同构群与3阶循环群的自同构群同构。

证明：无限群的自同构群为2阶循环群，3阶群的自同构群为2阶群，所有的2阶群阶为循环群且同构。故原结论成立。

群的自同构群

- **定理3**：设G是一个群，$a \in G$。则

1）$\tau_a : x \to axa^{-1} \quad (\forall x \in G)$ 是G的一个自同构，称为**G**的一个内自同构；

2）G的全体内自同构作成一个群，称为**G**的内自同构群，记为 $InnG$；

3）$InnG \trianglelefteq AutG$。

证明：1)τ_a 是双射变换，考虑其保运算性质。对任二元素 $x, y \in G$

$$\tau_a(xy) = a(xy)a^{-1} = a\left(xa^{-1}ay\right)a^{-1} = \left(axa^{-1}\right)\left(aya^{-1}\right)$$

即 $\tau_a(xy) = \tau_a(x) \cdot \tau_a(y)$，故 τ_a 为G的一个自同构。

2）设 τ_a, τ_b 为G的任二内自同构，则对G中的任意元素 x 有

$$\tau_a \tau_b(x) = \tau_a\left(bxb^{-1}\right) = abxb^{-1}a^{-1} = \tau_{ab}(x)$$

故 $\tau_a \tau_b$ 仍为一内自同构。再考虑逆元存在性。易知 $\tau_a^{-1} = \tau_{a^{-1}}$ 也是G的一个内自同构。故G的内自同构作成一个群，且有 $InnG \le AutG$。

群的自同构群

3）设σ为群G的任意一个自同构，τ_a 为G的任意一个内自同构，取 $x \in G$，令 $\sigma^{-1}(x)=y$，$\sigma(y)=x$ ，则

$$\begin{aligned}\sigma\tau_a\sigma^{-1}(x)&=\sigma\tau_a(y)=\sigma\left(aya^{-1}\right)\\&=\sigma(a)\sigma(y)\sigma\left(a^{-1}\right)\\&=\tau_{\sigma(a)}(x)\end{aligned}$$

即 $\sigma\tau_a\sigma^{-1}$ 仍为G的一个内自同构，故 $InnG \trianglelefteq AutG$ 。

•注：对于群G的正规子群来说，总有 $aNa^{-1}\subseteq N$或$\tau_a(N)\subseteq N$，其中 $\forall a\in G,\forall\tau_a\in InnG$，也就是说正规子群N是关于G的所有内自同构不变的子群，因此正规子群又常被称为不变子群。

群的自同构群

- **定义1**：对群G的所有自同构都不变的子群，亦即对G的任何自同构 σ，都有

$$\sigma(N)\subseteq N$$

的子群N，叫做G的一个特征子群。

•注：

1）群G和｛e｝都是群G的特征子群。

2）特征子群一定是正规子群，即特征子群一定是不变子群；反之不成立。例如，$N=\{(1),(12)(34)\}\lhd K_4$，但对于包含此非单位元位置的任意一个对换 σ，都会使得 $\sigma(N)\not\subseteq N$，故N虽然是不变子群但却不是特征子群。

群的自同构群

- **定义2**：设H群G的一个子群。如果H对G的每个自同态映射都不变，即对G的每个自同态映射φ都有

$$\varphi(H) \subseteq H,$$

则称H为群G的一个全特征子群。

•**注**：

1）G与｛e｝是群G的全特征子群。

2）是全特征子群一定是特征子群，但反之不成立。

•**例2**：群G的中心C是群G的一个特征子群。

证明：任取 $c \in C, x \in G, \sigma \in AutG$，则

$$\begin{aligned}\sigma(c)x &= \sigma(c)\cdot\sigma\left[\sigma^{-1}(x)\right] \\ &= \sigma\left[c\cdot\sigma^{-1}(x)\right] = \sigma\left[\sigma^{-1}(x)\cdot c\right] \\ &= \sigma\left[\sigma^{-1}(x)\right]\cdot\sigma(c) \\ &= x\sigma(c)\end{aligned}$$

群的自同构群

即$\sigma(c)\in C$，$\sigma(C)\subseteq C$，故群G的中心C为群G的一个特征子群。

•注：但群的中心并不一定是群的全特征子群。

•例3：有理数域Q上的2阶线性群 $G=GL_2(Q)$ 的中心（Q上所有2阶纯量矩阵）不是全特征群。

证明：任取 $A\in G$ ，即A为有理数域上2阶满秩方阵，则行列式$|A|$ 为一个有理数，故可令

$$|A|=\frac{b}{a}2^{n(A)},$$

其中a，b为奇数，$n(A)$是与A有关的整数。

由于 $|AB|=|A|\cdot|B|$ ，故有

$$n(AB)=n(A)+n(B)$$

于是易知

$$\varphi:\quad A\to\begin{pmatrix}1 & n(A)\\ 0 & 1\end{pmatrix}$$

是G到自身的一个映射，又由于

群的自同构群

$$\varphi(AB)=\begin{pmatrix}1 & n(AB)\\0 & 1\end{pmatrix}=\begin{pmatrix}1 & n(A)+n(B)\\0 & 1\end{pmatrix}$$

$$=\begin{pmatrix}1 & n(A)\\0 & 1\end{pmatrix}\begin{pmatrix}1 & n(B)\\0 & 1\end{pmatrix}=\varphi(A)\varphi(B)$$

故 φ 是群G的一个自同态映射。但是，φ 把G的中心元素 $\begin{pmatrix}2 & 0\\0 & 2\end{pmatrix}$ 变成了非中心元素 $\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}$ ，因此，G的中心不是全特征子群。

- **例4**：求证：循环群 $G=\langle a\rangle$ 的子群都是全特征子群。

证明：设 $H=\langle a^s\rangle\le G$，任取G的一个自同态 φ，则 $\varphi(a)=a^t$ ，于是

$$\varphi(a^s)=a^{st}\in H$$

从而 $\varphi(H)\subseteq H$ ，即H是群G的全特征子群。

- 注：全特征子群、特征子群、正规子群之间的关系如下：

$$\text{全特征子群}\subseteq\text{特征子群}\subseteq\text{正规子群}$$

群的自同构群

- **定理4**：设C是群G的中心，则

$$InnG \cong G/C$$

证明：设

$$\varphi: \quad a \to \tau_a \quad (\forall a \in G)$$

则易知φ为G到$InnG$的一个同态满射，故$G \sim InnG$。

若 τ_a为G的恒等自同构，即对G中任意的元素x都有$\tau_a(x)=x$，即

$$axa^{-1}=x, ax=xa$$

于是可知 $a \in C$。

反之，任取$c \in C$，显然 τ_c 是G的恒等自同构，故$C=Ker\varphi$。于是由群同态基本定理可得

$$InnG \cong G/C$$

证毕。

群的自同构群

- 注：

1）求群G的内自同构群，可通过找其中心

2）自同构没那么好发现，原因是群的自身性质有时并不能转移到其自同构群上

3）不同结构的群其自同构群可能同构

4）无中心群的自同构群也必为无中心群，从而当$n \geq 3$时$AutS_n$是无中心群。

作业

- P101. 2、设G是群，又 $K \leq H \trianglelefteq G$，$K \trianglelefteq G$。证明：若 G/K 是交换群，则 G/H 也是交换群。

P107. 1、证明：阶数 ≤ 7 的循环群的自同构群都是循环群。