近世代数之十五

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. 群的定义
2. Lagrange定理
3. 元素的阶

群

定义 (Cayley 1854)

二元组$(G,\cdot)$称为**群**，其中G为非空集合，**乘法**“$\cdot$”为二元运算

$$G \times G \to G, \quad (a,b) \mapsto a \cdot b$$

满足如下：

(G1) 结合律$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(G2) 有幺元$1_G = 1$

(G3) 有逆元（逆元唯一!）

注：有时简记为群G, 乘法运算$a \cdot b = ab$

注：公理(G3)最不平凡!

基本性质

引理

设G为群。

1. 乘法消去率: $ab = ac \Rightarrow b = c$
2. $(ab)^{-1} = b^{-1}a^{-1}$
3. 求逆运算$(-)^{-1}: G \to G, \quad g \mapsto g^{-1}$为双射。
4. 对于任何整数n, 定义幂次a^n。故, $a^{n+m} = a^n \cdot c^m$!

子群

定义

非空子集H称为**子群**，若$a \cdot b \in H$, $a^{-1} \in H$。记为$H \leq G$.

平凡子群：$\{1_G\}$, G.

基本例子:来自环

1. 给定环R，自然有三个群: **加法群**$(R,+)$，**单位群**$(U(R),\cdot)$，**自同构群**$(\mathrm{Aut}(Q),\circ)$
2. 取$R=\mathbb{Z},\mathbb{Z}_n,\mathbb{Z}[i]$等
3. 考虑域扩张K/k。则$\mathrm{Aut}(K/k)\leq \mathrm{Aut}(K)$

基本例子：群即对称

1. 一般线性群$\mathrm{GL}(n,\mathbb{C})$
2. 特殊线性群$\mathrm{SL}(n,\mathbb{C})$
3. $\mathrm{SO}_n \leq \mathrm{O}_n \leq \mathrm{GL}(n,\mathbb{R})$
4. 考虑$P \subseteq \mathbb{R}^n$，图形P的**对称群**

$$\Sigma(P) = \{g \in \mathrm{SO}_n(\text{或}\mathrm{O}_n) \mid g(P) = P\} \leq \mathrm{SO}_n$$

基本例子：群即置换

1. 抽象集X，其上的**置换** $\sigma\colon X \to X$双射
2. **对称群** $S(X) = \{X \text{ 上所有的置换}\}$
3. 例如：$\mathrm{Aut}(R) \leq S(R)$
4. Cayley定理（1878）：任何群“本质上”都是$S(X)$的子群!

Lagrange 定理

若$|G| < \infty$，称为**有限群**.

定理

设G为有限群，$H \leq G$。则: $|H|$整除$|G|$.

是否想起：$k \subseteq E \subseteq K$，则$\dim_k E | \dim_k K$?

Lagrange 定理的证明

1. $a \in G$，$aH = \{ah \mid h \in H\}$称为H的**左陪集**
2. $Ha = \{ha \mid h \in H\}$ 称为H的**右陪集**
3. 左、右陪集都与H一样大，它们都是G上某个等价关系的等价类。
4. 若有分拆$G = \bigcup_{i \in I} a_i H$，则称$\{a_i \mid i \in I\}$为$G$关于$H$的左陪集完全代表元系，$|I| = [G : H]$ 称为子群H的**指数**
5. 此时有，$G = \bigcup_{\in I} Ha_i^{-1}$。故，$\{a_i^{-1} \mid i \in I\}$恰为关于$H$的右陪集完全代表元系

Lagrange 定理，revisited

定理

设G为有限群，$H \leq G$。则有

$$|G| = |H| \cdot [G : H]$$

类比：$k \subseteq E \subseteq K$，则有

$$\dim_k K = \dim_k E \cdot \dim_E K!$$

注：对于含幺半群，该结论不成立。例如，$(\mathbb{Z}_8, \cdot)$，其含幺子半群$\{\bar{0}, \bar{1}, \bar{3}\}$。

元素的阶

定义

元素$a \in G$的**阶**，记为$\mathrm{ord}(a)$，是指最小的正整数d使得$a^d = 1_G$。若不存在这样的d，则记$\mathrm{ord}(a) = \infty$.

1. 若$|G| < \infty$，则任何元素a具有有限的阶。
2. 设$\mathrm{ord}(a) = d < \infty$。则$a^n = 1_G$当且仅当$d|n$。

阶（续）

命题

设$|G| < \infty$，$a \in G$。则

$$\mathrm{ord}(a) \text{ 整数} |G|$$

回想Fermat小定理：$a \in \mathbb{F}_p^\times$，$a^{p-1} \equiv 1 \pmod{p}$

群同态

定义

映射$f\colon G \to G'$称为**群同态**，若$f(a\cdot b) = f(a)\cdot f(b)$。双射群同态称为**群同构**。

注：群同态蕴含着$f(1_G) = 1_{G'}$以及$f(a)^{-1} = f(a^{-1})$。

例子

1. 子群$H \leq G$诱导包含同态$\mathrm{inc}\colon H \to G$
2. $\det\colon \mathrm{GL}(n,\mathbb{C}) \to \mathbb{C}^\times$
3. 单位根群$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$。则：有群同构

$$\mu_n \simeq (\mathbb{Z}_n, +)$$

4. 群$U(\mathbb{Z}_8)$与μ_4同构么？

群的直积

定义

设G，H为群。则$G \times H$上有自然的群结构，称为其**直积**。

1. 能找到G与$G \times H$之间的自然同态么？
2. 元素(g, h)的阶？
3. 设R, S为环。则$U(R \times S) \simeq U(R) \times U(S)$!
4. $\mu_2 \times \mu_2$同构于$U(\mathbb{Z}_8)$？**Klein四元群**(Vierergruppe)，记为V_4。