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 正规子群和有限群
- 第四章 环与域
- 第五章 因子分解
- 第六章 域的扩张

第二章 群

- 群的定义和初步性质
- 元素的阶
- 子群
- 循环群
- 变换群
- 置换群
- 陪集、指数和Lagrange定理
- 群在集合上的作用

循环群

- 设M是群G中的一个非空子集，G中包含M的子群总是存在，所有包含M的子群的交为 $\langle M\rangle$。则 $\langle M\rangle$ 仍为群G的一个子群，且G中任何一个子群只要包含M就会包含$\langle M\rangle$。所以 $\langle M\rangle$ 是群G中包含M的最小子群。

生成系

- **定义 1：**称 $\langle M\rangle$ 为群G中由子集M生成的子群，并把M叫做这个子群的**生成系。**
- **注：**

1. 一个群或子群可能有很多的生成系，甚至可以是无限多个生成系。
2. 集合M的元素可以是无限个，也可以是有限个。当M=｛$a_1,a_2,\ldots,a_n$｝时，把 $\langle M\rangle$ 简记为$\langle a_1,a_2,\ldots,a_n\rangle$。特别地，当$M=\{a\}$时，则记作$\langle M\rangle=\langle a\rangle$。

循环群

循环群

- **定义 2**：如果群G可以由一个元素a生成，即 $G=\langle a\rangle$ ，则称G为由a生成的一个**循环群**，并称a为G的一个**生成元**。

于是，$\langle a\rangle$ 是由一切形如

a^k （k是任意整数）

的元素作成的群，亦即

$$\langle a\rangle=\{\cdots,a^{-3},a^{-2},a^{-1},e,a^{1},a^{2},a^{3},\cdots\}$$

若改乘为加则此循环群可写为 $\langle a\rangle=\{\cdots,-3a,-2a,-a,0,a,2a,3a,\cdots\}$

•**注**：循环群必为交换群

循环群

- 例 1：整数加群Z是**无限循环群**。

证明：实际上如果可以找到此群的一个生成元，即可达到证明的目的。

$$Z=\langle 1\rangle$$

是否还有别的生成元呢？

- 例 2：n次单位根群U_n是**一个n阶循环群**。

证明：若设ε为n次单位原根，则有

$$U_n=\langle\varepsilon\rangle=\{1,\varepsilon,\varepsilon^2,\cdots,\varepsilon^{n-1}\}$$

这n个复数互异，对于任意整数k，ε^k必与这n个中的一个相等。

循环群

- **定理 1：** 设 $G=\langle a\rangle$ 为任一循环群，则

1）当 $|a|=\infty$ 时，$G=\langle a\rangle=\{\cdots,a^{-3},a^{-2},a^{-1},e,a^{1},a^{2},a^{3},\cdots\}$**为无限循环群，且与整数加群** Z **同构**。

2）当 $|a|=n$ 时，$G=\langle a\rangle=\{e,a^{1},a^{2},\cdots a^{n-1}\}$**为n阶循环群，且与n次单位根群**$U_n$**同构**。

证明：1）首先，由假设条件可知，任意两个元素不可能相等，得G为无限循环群。其次，需构造一个G与Z之间的同构映射：

$$\varphi:\quad a^{m}\to m$$

验证是双射并且保持运算。故有，$G\cong Z$ 。

2）首先，由假设条件 $|a|=n$可知，$e,a,a^{2},\cdots,a^{n-1}$ 互异，其次对于任意整数m， 可设

$$m=nq+r\quad (0\le r<n)$$

可推出 $a^{m}=(a^{n})^{q}\cdot a^{r}=a^{r}\in\{e,a,a^{2},\cdots,a^{n-1}\}$，故 $G=\langle a\rangle=\{\cdots,a^{-3},a^{-2},a^{-1},e,a,a^{2},a^{3},\cdots\}=\{e,a^{1},a^{2},\cdots a^{n-1}\}$

循环群

- 其次，需要构造出从G到U_n的一个同构变换，考虑

$$\varphi: \quad a^m \to \varepsilon^m$$（ε 为n次单位原根）

可验证其为一保持运算的双射，故$G \cong U_n$ 。

- **推论1**：n阶群是循环群 $\Leftrightarrow$ G有n阶元素。

证明：**必要性**：由定理1知n阶循环群的生成元是G中n阶元素。

充分性：若设G中有n阶元素a，则易知：

$$H = \left\{e, a, a^2, \cdots, a^{n-1}\right\}$$

是G的一个n阶子群，但G的阶也为n，则有

$$G = H = \langle a \rangle$$

- **注**：n阶循环群的元素是不是生成元，就看它的阶数是不是n。

循环群

- **定理2：** 无限循环群$\langle a\rangle$有两个生成元，即 a 与 a^{-1}；n阶循环群有 $\varphi(n)$ 个生成元，其中$\varphi(n)$ 为Euler函数。

证明：当 $|a|=\infty$时,$\langle a\rangle=\{\cdots,a^{-3},a^{-2},a^{-1},e,a,a^{2},a^{3},\cdots\}$，生成元为 a 和a^{-1}是显然的。

当 $|a|=n$ 时，元素 $a^{k}\,(0<k<n)$是$\langle a\rangle$的生成元当且仅当 a^{k} 的阶数为n，亦即（k,n）=1。从而$\langle a\rangle$ 有$\varphi(n)$ 个生成元。

例如：4，5，6阶循环群分别有

$$\varphi(4)=2,\quad \varphi(5)=4,\quad \varphi(6)=2$$

个生成元。

多选题 1分

设置

以下关于同构的两个群的单位元和逆元之间关系的描述正确的是（ ）

单位元映射为单位元

单位元不一定映射为单位元

逆元的像映射为其像的逆元

逆元的像不一定映射为其像的逆元

提交

多选题 1分

设置

以下关于同构的两个群的单位元和逆元之间关系的描述正确的是（ ）

A 单位元映射为单位元

B 单位元不一定映射为单位元

C 逆元的像映射为其像的逆元

D 逆元的像不一定映射为其像的逆元

提交

循环群

- **定理3**：循环群的子群仍为循环群。

证明：设H为循环群$\langle a\rangle$的一个子群。若H为平凡子群则结论显然。

若H不是平凡子群，则设H中最小的a的正数次幂为m，则 $a^m, a^{-m} \in H$，于是

$$\langle a^m \rangle \subseteq H$$

另一方面，对于$\forall a^s \in H$，令

$$s = mq + r, \qquad 0 \le r < m$$

由 $a^s, a^m \in H$，故

$$a^r = a^{s-mq} = a^s \cdot \left(a^m\right)^{-q} \in H$$

但a^m是H中具有最小正整数幂次的元素，故r=0，于是可知

$$a^s = \left(a^m\right)^q \in \langle a^m \rangle$$

即得 $H \subseteq \langle a^m \rangle$，因此 $H = \langle a^m \rangle$，即子群H也为一循环群。

循环群

- **定理4：**无限循环群G有无限多个子群；当 $G=\langle a\rangle$ 为n阶循环群时，对n的每个正因数k，G中有且只有一个k阶子群，这个子群为 $\langle a^{n/k}\rangle$ 。

证明：1）设 $|a|=\infty$，则易知

$$\langle e\rangle,\langle a\rangle,\langle a^2\rangle,\cdots$$

是G的全部互不相同的子群。且除 $\langle e\rangle$ 外都是无限循环群，从而彼此同构。

2）设 $|a|=n$ ，$k|n$ 且

$$n=kq$$

则 $|a^q|=k$，从而 $\langle a^q\rangle$ 是G的一个k阶子群。

又设H也是G的一个k阶子群，则由定理3，设 $H=\langle a^m\rangle$，则 $|a^m|=k$ 。而由于 a^m 的阶是 $\dfrac{n}{(m,n)}$，故

$$\frac{n}{(m,n)}=k,\quad n=k(m,n)$$

于是 $q=(m,n)$，$q|m$。从而 $a^m\in\langle a^q\rangle$，$\langle a^m\rangle\subseteq\langle a^q\rangle$。但是由于 $\langle a^q\rangle$ 与 $\langle a^m\rangle$ 同阶，故

$$H=\langle a^m\rangle=\langle a^q\rangle=\langle a^{n/k}\rangle$$

循环群

- 设n是大于1的整数，且

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

为n的标准分解式。易知n共有

$$T(n) = (k_1 + 1)(k_2 + 1)\cdots(k_m + 1)$$

个正因数。这里$T(n)$表示n的正因子数的个数。

- **推论2**：n阶循环群有且仅有$T(n)$ 个子群。

证明：利用定理4。

例如，4，5，6阶循环群分别有3，2，4个子群。

变换群

- **定义 1**：设M是一个非空集合。则由M的一些变换关于变换的乘法所作成的群，称为M的一个**变换群**；由M的若干个双射变换关于变换乘法作成的群，称为M的一个**双射变换群**；由M的若干个非双射变换关于变换乘法作成的群，称为M的**非双射变换群**。

- 例 1：设$|M|>1$，并取定$a\in M$。易知

$$\tau: \quad x \to a \quad (\forall x \in M)$$

是M的一个非双射变换，并且$\tau^2=\tau$ 。从而G=$\{\tau\}$作成M的一个非双射变换群。

- **定理1**：设M为任一非空集合,$S(M)$为由M的全体双射变换作成的集合。则$S(M)$关于变换的乘法作成一个群。

证明：变换乘法是其上的代数运算且满足结合律；恒等变换为$S(M)$上单位元；每个双射变换的逆变换也是双射变换，故$S(M)$关于变换的乘法作成群。

变换群

- **定义2**：称集合M的双射变换群$S(M)$为M上的**对称群，**当$|M|=n$，其上的对称群用S_n表示，并称为**n元对称群**。
- **注**：1）M上的对称群是M的最大双射变换群。

2）n元对称群S_n是一个阶为$n!$的有限群。

- **定理2**：设G是集合M的一个变换群，则

G是双射变换群 $\Leftrightarrow$ G中含有M的单（满）射变换。

证明：**必要性：**显然。

充分性：设G含有M的一个单射变换σ，则目标证G中每个元素均为M的双射变换。

首先。G的单位元必是M的恒等变换。设ε为G的单位元，于是$\sigma\varepsilon=\sigma$。从而

$$\sigma(\varepsilon(x))=\sigma\varepsilon(x)=\sigma(x) \qquad (\forall x\in M)$$

但σ是一个单射变换故有 $\varepsilon(x)=x \qquad (\forall x\in M)$，即得$\varepsilon$为M上的恒等变换。

变换群

其次，G中元素都是M上双射变换。

在G中任取元素 τ ，其逆元用τ^{-1} 表示，它是M的一个变换，且

$$\tau^{-1}\tau = \tau\tau^{-1} = \varepsilon$$

由此可得：若 $\tau(x)=\tau(y) \quad (x, y \in M)$，则必有

$$\tau^{-1}(\tau(x))=\tau^{-1}(\tau(y))\text{，即 } \tau^{-1}\tau(x)=\tau^{-1}\tau(y) \text{ ，}$$

从而 $\varepsilon(x)=\varepsilon(y), x=y$，即 τ 是M的单射变换。

又由于$\tau\left(\tau^{-1}(x)\right)=\tau\tau^{-1}(x)=\varepsilon(x)=x$，即M中任意元素$x$ 在τ 之下都有逆像，故τ又是M的满射变换。因此,τ 是M的双射变换。从而G是M的一个双射变换群。

- **推论1**：设G是集合M的一个变换群。则

G是双射变换群 $\Leftrightarrow$ G包含恒等变换。

证明：**必要性**：显然。

充分性：利用定理2。

变换群

•**注**：集合M的任何变换群中，不可能既含有M的双射变换又含有M的非双射变换。因此，不是双射变换群的变换群，必然是非双射变换群。

•如果$|M|>1$，则集合M的全体变换的集合 $T(M)$只能作成幺半群而不能作成群。

例 2：设M=｛1，2，3，4｝则M的以下二变换

$$\alpha=\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix},\quad \beta=\begin{pmatrix}1&2&3&4\\1&1&4&3\end{pmatrix}$$

作成M的一个非双射变换群。

证明：令G= $\{\alpha,\beta\}$ ，则易知

$$\alpha^2=\beta^2=\alpha,\qquad \alpha\beta=\beta\alpha=\beta$$

因此，G关于变换乘法封闭，且α 是G的单位元， α 与 β 的逆元为其自身，故G作成群。

α 与 β 都是M的非双射变换，故G是M的一个非双射变换群。

变换群

- 例 3：令 $M=\{(x,y)|x,y\in R\}$ ，且对任意实数 a 规定

$$\tau_a:\quad (x,y)\to(x+a,0)\quad (\forall (x,y)\in M)$$

则 $G=\{\tau_a|a\in R\}$作成M上的一个非双射变换群。

证明：τ_a 为M上的一个非双射变换。

封闭-----　$\tau_a\tau_b=\tau_{a+b}\in G$

单位元-----　τ_0

逆元-----　$\tau_a^{-1}=\tau_{-a}\in G$

- 例 4：设M为整数集。现对任意整数n规定

$$\tau_n:\quad x\to x+n\quad (\forall x\in M)$$

并令$G=\{\tau_n|n\in M\}$。则G是M的一个双射变换群，但非M上的对称群。

证明：首先，τ_n是M的一个双射变换，故$G\subseteq S(M)$。

变换群

其次，任取$\tau_s,\tau_t \in G$，则

$$\tau_s\tau_t(x) = \tau_s(x+t) = x+t+s = \tau_{s+t}(x) \quad (\forall x \in M),$$

即 $\tau_s\tau_t = \tau_{s+t} \in G$ 。又因为

$$\tau_{-n}\tau_n(x) = x \quad (\forall x \in M)$$

故 $\tau_{-n}\tau_n = \tau_0 = \varepsilon$ ，即 $\tau_n^{-1} = \tau_{-n} \in G$ 。因此，$G \leq S(M)$ 。从而G是M上的一个双射变换群。

但是考虑到 $\tau: \quad x \to -x$ 是M的一个双射变换，但是$\tau \notin G$，故G不是M上的对称群。

- **定理 3：**（A. Cayley, 1821-1895）**任何群都与一个（双射）变换群同构。**

证明：设G为任意一个给定的群。任取 $a \in G$，并令

$$\tau_a: \quad x \to ax \quad (\forall x \in G)$$

即 $\tau_a(x) = ax$ 。则 τ_a 是G的一个双射变换。

变换群

令 $\bar{G}=\{\tau_a | a\in G\}$，并取 $\tau_a,\tau_b\in\bar{G}$，则

$$\begin{aligned}\tau_a\tau_b(x)&=\tau_a(bx)=a(bx)\\&=(ab)x=\tau_{ab}(x)\qquad(\forall x\in G)\end{aligned}$$

因此，

$$\tau_a\tau_b=\tau_{ab}\in\bar{G}$$

从而 $\tau_{a^{-1}}\tau_a=\tau_e$， $\tau_a^{-1}=\tau_{a^{-1}}\in\bar{G}$ 。故 $\bar{G}\le S(G)$ 。即 $\bar{G}$ 是G的一个双射变换群。

又

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

即 $\varphi(a)=\tau_a$ 是G到 $\bar{G}$ 的一个双射，且 $\varphi(ab)=\varphi(a)\varphi(b)$ 。即 φ 是群G到 $\bar{G}$ 的一个同构映射，故 $G\cong\bar{G}$ 。

变换群

- **推论2**：任何n阶有限群都同n元对称群 S_n 的一个子群同构。

证明：同定理3。

- **注**：变换群，特别是n元对称群是一种相对具体的群。以上定理、推论表明任何一个抽象的群都可以找到一个具体的群与它同构。也就是说除了元素不同外，其代数性质完全一致。

作业

- P36. 1、设 $G=\langle a\rangle$ 为6阶循环群。给出 G 的一切生成元和 G 的所有子群。

- P39.1、设 $M=\{1,2,3,4\},H=\{\tau,\sigma\}$，其中

$$\tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 1 & 3 & 4\end{pmatrix},\qquad \sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 1 & 3 & 3\end{pmatrix}$$

问：H关于变换乘法是否作成有单位元的半群？是否作成群？