17.3 循环群

- 循环群的定义
- 循环群的分类
- 生成元
- 子群
- 循环群的实例

循环群的定义及其分类

定义 $G = \langle a \rangle = \{a^k \mid k \in \mathbf{Z}\}, a \in G$

称G为循环群，a为G的生成元.

分类：

生成元的阶无限，则 G 为无限循环群

生成元 a 为 n 阶元，则$G = \{e, a, a^2, \ldots, a^{n-1}\}$为$n$ 阶循环群

实例 $\langle \mathbf{Z}, + \rangle$为无限循环群

$\langle \mathbf{Z}_n, \oplus \rangle$为 n 阶循环群

循环群的生成元

定理1 $G=\langle a\rangle$是循环群

(1) 若 G 是无限循环群，则 G 的生成元是 a 和 a^{-1};

(2) 若 G 是 n 阶循环群，则 G 有 $\phi(n)$ 个生成元，

当 $n=1$时 $G=\langle e\rangle$ 的生成元为 e;

当 $n>1$时,$\forall r\,(r\in Z^{+}\wedge r<n)$, a^{r}是 G 的生成元 $\Leftrightarrow (n, r)=1$.

证明思路:

(1) 证明 a^{-1} 是生成元

证明若存在生成元 b，则 $b=a$ 或 a^{-1}.

(2) 只需证明 $(r, n)=1$, 则 a^{r} 是生成元

反之，若 a^{r} 是生成元，则 $(r, n)=1$.

证明

证 (1) a是生成元，$<a^{-1}> \subseteq G$,

任取 $a^l \in G$, $a^l = (a^{-1})^{-l} \in <a^{-1}> \Rightarrow G \subseteq <a^{-1}>$

假设 b为生成元，$b = a^j, a = b^t$,

$$a = b^t = (a^j)^t = a^{jt} \Rightarrow a^{jt-1} = e,$$

若 $jt-1 \neq 0$与 a 为无限阶元矛盾, 因此 $j = t = 1$ 或 $j = t = -1$

(2) $(n,r) = 1 \Leftrightarrow \exists\, u,v \in Z(un + rv = 1)$

$$\Rightarrow a = a^{un+rv} = (a^r)^v \Rightarrow a^r \text{为生成元}$$

反之，若a^r为生成元

$$(a^r)^{\frac{n}{(n,r)}} = e \Rightarrow |a^r| \,\Big|\, \frac{n}{(n,r)} \Rightarrow n \,\Big|\, \frac{n}{(n,r)} \Rightarrow (n,r) = 1$$

循环群的子群

定理2 $G=<a>$是循环群，那么

(1) G 的子群也是循环群

(2) 若G是无限阶，则 G 的子群除 $\{e\}$ 外也是无限阶

(3) 若G是 n 阶的，则 G 的子群的阶是 n 的因子，

对于 n 的每个正因子 d, 在 G 中有且仅有一个 d 阶子群.

证明思路：

(1) 子群 H 中最小正方幂元 a^m 为 H 的生成元

(2) 若子群 $H=<a^m>$有限，$a\neq e$, 则推出 $|a|$ 有限.

(3) $H=<a^m>$, $|H|=|a^m|$, $(a^m)^n=e$. 从而 $|a^m|$ 是 n 的因子.

(4) $<a^{n/d}>$是 d 阶子群，然后证明唯一性.

证明

证 (1) 设 H 是 $G=<a>$ 的子群，不妨设 $H \neq \{e\}$.

取 H 中最小正方幂元 a^m, $<a^m> \subseteq H$.

对于任意整数 i, $i = lm + r$, $r \in \{0, 1, \ldots, m-1\}$

$$a^i \in H \Rightarrow a^r = a^i (a^m)^{-l} \in H \Rightarrow r = 0 \Rightarrow a^i \in <a^m>$$

$H \subseteq <a^m>$

(2) 设 H 为 G 的子群，若 $H \neq \{e\}$, 必有 $H = <a^m>$,

a^m 为 H 中最小正方幂元.

假设 $|H| = t$, 则 $(a^m)^t = e \Rightarrow a^{mt} = e$，与 a 为无限阶元矛盾.

证明（续）

(3) 设 $G=\{e, a, \ldots, a^{n-1}\}$，$H=\{e\}$ 命题显然成立.

若 $H\neq\{e\}$, 必有 $H=<a^m>$, a^m为 H 中最小正方幂元.

设 $|H|=|a^m|=d$,

$$(a^m)^n=(a^n)^m=e\Rightarrow|a^m|\,|n\Rightarrow d\,|\,n$$

(4) 设 $d\,|\,n$，则 $H=<a^{n/d}>$ 是 G 的 d 阶子群.

若$H'=<a^m>$ 也是 G 的 d 阶子群，其中 a^m 为最小正方幂元.则

$$a^{md}=e\Rightarrow n\,|\,md\Rightarrow\frac{n}{d}\,|\,m\Rightarrow m=\frac{n}{d}t\Rightarrow a^m=(a^{\frac{n}{d}})^t\in H$$

$$H'\subseteq H,\,|H'|=|H|=d\Rightarrow H'=H$$

实例

例1 (1) $< Z_{12}, \oplus >$, 求生成元、子群.

生成元为与12 互质的数：1, 5, 7, 11
12 的正因子为 1, 2, 3, 4, 6, 12，
子群：<0>,<1>, <2>,<3>, <4>, <6>

(2) $G = < a^2 >$为12阶群，求生成元和子群.

生成元为 $a^2, a^{10}, a^{14}, a^{22}$
G的子群：$< e >, < a^2 >, < a^4 >, < a^6 >, < a^8 >, < a^{12} >$

(3) $< a >$为无限循环群，求生成元和子群.

生成元为a, a^{-1}；子群为$<a^i>$，$i = 0,1,2,\ldots$;

(4) $G = < Z, + >$，求生成元和子群.

生成元：1, –1；子群 nZ, $n = 0,1,\ldots$,

17.4 变换群与置换群

- 变换群
  - 变换群的定义
  - 变换群的实例
- n元置换群
  - 置换的表示
  - 置换的乘法和求逆运算
  - 置换群中元素的阶与子群
  - 置换群的实例

变换群

变换群的定义

A上的变换：　$f: A \to A$

A上的一一变换：　双射 $f: A \to A$

A上的一一变换群：$E(A) = \{ f \mid f: A \to A$为双射 $\}$

关于变换乘法构成群

A上的变换群G：　$G \subseteq E(A)$

实例

G为群，$a \in G$，令 $f_a: G \to G$, $f_a(x) = ax$，则 f_a 为一一变换.

$H = \{ f_a \mid a \in G \}$ 关于变换乘法构成 G 上的变换群.

$H \leq E(G)$

变换群的实例

例如 $G=\{e, a, b, c\}$,

$f_e=\{<e,e>,<a,a>,<b,b>,<c,c>\}$

$f_a=\{<e,a>,<a,e>,<b,c>,<c,b>\}$

$f_b=\{<e,b>,<a,c>,<b,e>,<c,a>\}$

$f_c=\{<e,c>,<a,b>,<b,a>,<c,e>\}$

$H=\{f_e, f_a, f_b, f_c\}$

思考：怎样证明 H 同构于 G

与独异点的表示定理进行比较

n元置换群

A上的 n 元置换：$|A| = n$ 时 A 上的一一变换

表示法

(1) 置换的表示法：令 $A = \{1, 2, \ldots, n\}$,

(2) 不交轮换的分解式：$\sigma = \tau_1\tau_2\ldots\tau_t$,

其中 $\tau_1,\tau_2, \ldots,\tau_t$ 为不交轮换

(3) 对换分解式：

对换 $(i\ j) = (j\ i)$

$(i_1\ i_2\ldots i_k) = (i_1\ i_k)\ (i_1\ i_{k-1})\ \ldots\ (i_1\ i_2)$

n元置换的轮换表示

定理1 任何n元置换都可以表成不交的轮换之积，并且表法是唯一的. 即：

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_t,\ \sigma = \tau_1 \tau_2 \cdots \tau_l \Rightarrow \{\sigma_1, \sigma_2, \ldots, \sigma_t\} = \{\tau_1, \tau_2, \ldots, \tau_l\}$$

证明思路

(1) σ 可以表成不交的轮换之积. 对改变的文字个数归纳证明.

(2) 唯一性. 假设

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_t,\quad \sigma = \tau_1 \tau_2 \cdots \tau_l.$$

令 $X = \{\sigma_1, \sigma_2, \ldots, \sigma_t\}$, $Y = \{\tau_1, \tau_2, \ldots, \tau_l\}$

任取 $\sigma_j \in X$, $\sigma_j = (i_1\, i_2 \ldots i_m)$, $m > 1$, 证明 $\exists \tau_s \in Y$ 使得 $\sigma_j = \tau_s$,

从而 $X \subseteq Y$. 同理 $Y \subseteq X$.

n元置换的轮换指数

轮换指数：$1^{C_1(\sigma)}2^{C_2(\sigma)}\cdots n^{C_n(\sigma)}$，$C_k(\sigma)$: k-轮换的个数

例如

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\5&2&3&8&7&6&1&4\end{pmatrix}=(1\,5\,7)(4\,8)$$

指数为 $1^3\,2^1\,3^1\,4^0\,5^0\,6^0\,7^0\,8^0=1^3\,2^1\,3^1$

不同指数的个数是如下方程的非负整数解的个数

$$x_1+2x_2+\ldots+nx_n=n$$

例如：

A={1,2,3}上的置换

σ_1=(1), σ_2=(1 2), σ_3=(1 3), σ_4=(2 3), σ_5=(1 2 3), σ_6=(1 3 2)

轮换指数为 1^3：σ_1； 1^12^1：$\sigma_2, \sigma_3, \sigma_4$； 3^1：σ_5, σ_6

*n*元置换的对换表示

- 任意轮换都可以表成对换之积

  对换可以有交

  表法不唯一，但是对换个数的奇偶性不变

- 奇置换、偶置换

  奇置换：表成奇数个对换之积

  偶置换：表成偶数个对换之积

  奇置换与偶置换之间存在一一对应，因此各有 $n!/2$ 个

置换的乘法与求逆

置换的乘法：函数的合成

例如：8元置换 $\sigma = (132)(5648)$，$\tau = (18246573)$，则

$$\sigma\tau = (15728)\,(3)\,(4)\,(6) = (15728)$$

置换求逆：求反函数

$$\sigma = (132)\,(5648)，\quad \sigma^{-1} = (8465)\,(231),$$

令S_n为$\{1, 2, \ldots, n\}$上所有n元置换的集合.

S_n关于置换乘法构成群，称为n元对称群.

S_n的子群称为n元置换群.

例　3元对称群 $S_3 = \{(1), (12), (13), (23), (123), (132)\}$

3元交代群 $A_3 = \{(1), (123), (132)\}$

置换群中元素的阶与子群

元素的阶

k 阶轮换 $(i_1\ i_2 \ldots i_k)$ 的阶为 k

$\sigma = \tau_1\tau_2\ldots\tau_l$ 是不交轮换的分解式，则 $|\sigma|=[|\tau_1|,|\tau_2|,\ldots,|\tau_l|]$

子群

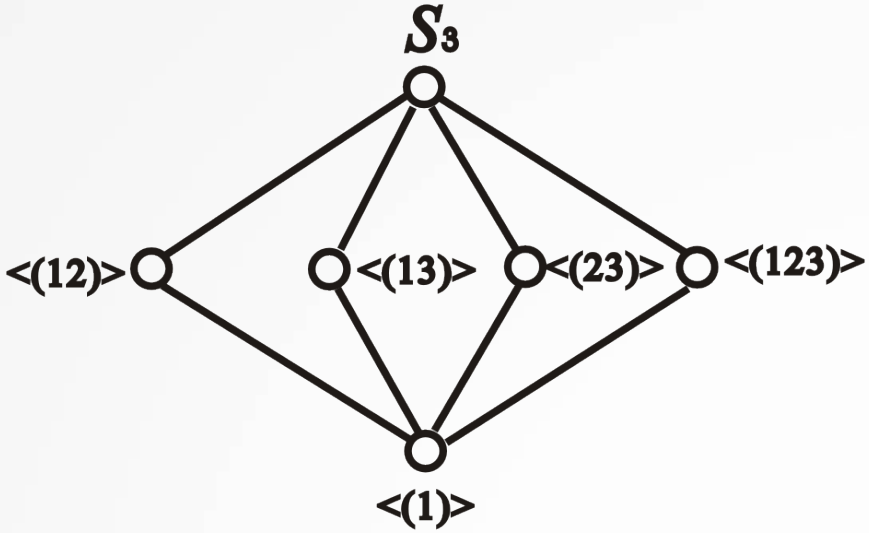
$\{(1)\}$，S_n，n元交代群A_n

例如 S_3，子群6个

$<(1)>, S_3,$

$<(12)>, <(13)>,$

$<(23)>, A_3 = <(123)>$

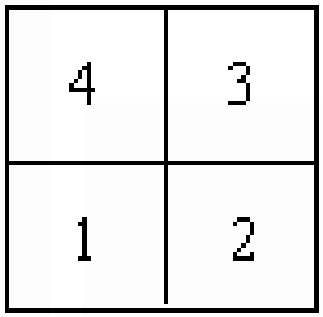


置换群的实例

Cayley 定理 每个群 G 都与一个变换群同构.

推论 每个有限群都与一个置换群同构

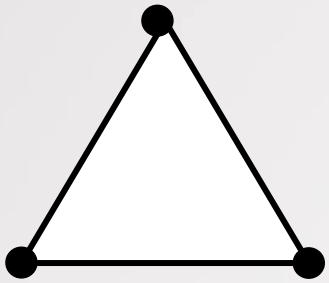
D_4，4×4 的方格图形，在空间旋转、翻转.



D_4= { (1), (1234), (13)(24), (1432), (12)(34),
(14)(23), (13)(2)(4), (24)(1)(3) }

$D_4 \leq S_4$

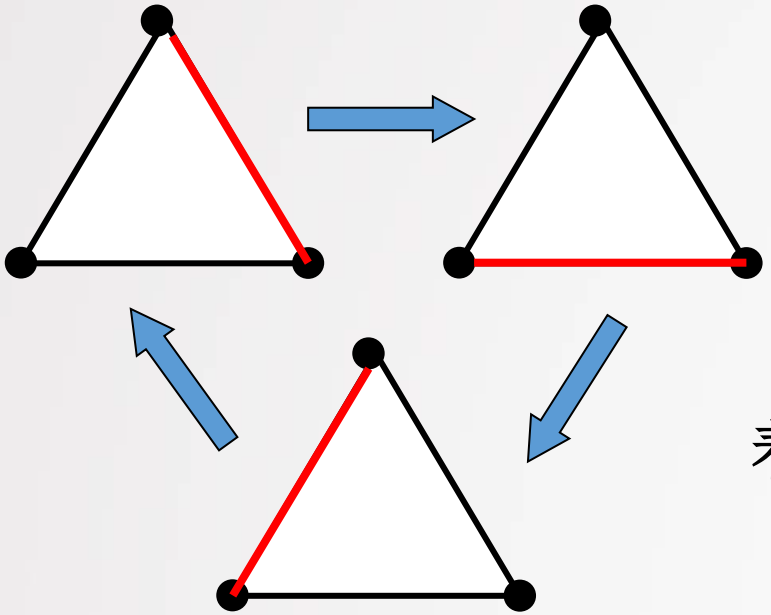
不同构的图的计数



$G = \{(1),(12),(13),(23),(123),(132)\}$

对三角形的边着黑红两色

方案数对应了3顶点不同构的图的个数



在G的作用下着色方案计数，

用Polya定理(第23章)

可以得到方案数等于4.

着色方案构成的轮换

冒泡排序算法分析

算法描述

输入: $L, n \geq 1$.

输出: 按非递减顺序排序的L.

算法 bubbleSort

1. $FLAG \leftarrow n$ // 标记被交换的最后元素位置
2. while $FLAG > 1$ do
3. $k \leftarrow FLAG - 1$
4. $FLAG \leftarrow 1$
5. for j=1 to k do
6. if $L(j) > L(j+1)$ then
7. $L(j) \leftrightarrow L(j+1)$
8. $FLAG \leftarrow j$

实例

5 7 2 6 9 3 1 8 4

5 2 6 7 3 1 8 4 9

2 5 6 3 1 7 4 8 9

2 5 3 1 6 4 7 8 9

2 3 1 5 4 6 7 8 9

2 1 3 4 5 6 7 8 9

1 2 3 4 5 6 7 8 9

1 2 3 4 5 6 7 8 9

特点：交换发生在相邻元素之间——对换

置换与逆序

每个输入是一个 n 元置换，其 逆序序列：

$b_1 = 0;\ \ b_2 = 0,1;\ \ \ldots\ ;\ b_n = 0,1,\ldots,n\text{-}1$

其中b_i表示在 i 后面且比 i 小的数的个数

置换与它的逆序序列构成一一对应

逆序数 置换中的逆序总数

$$b_1 + b_2 + \ldots + b_n$$

实例：置换 3 1 6 5 8 7 2 4

逆序序列为 (0, 0, 2, 0, 2, 3, 2, 3)

逆序数 12

排序算法的输入：n元置换，复杂度：比较次数

冒泡排序：每次相邻元素对换只能消除 1 个逆序

比较次数 ≥ 交换次数 ≥ 输入含有的逆序个数

复杂度分析

最坏情况分析 最大的逆序数是 $n(n-1)/2$, 最坏情况交换次数至少是 $n(n-1)/2$, 比较次数至少是 $n(n-1)/2$.

平均情况分析

设各种输入是等概率的

置换 α 的逆序序列是 $(b_1, b_2, \ldots, b_n)$,

置换 α' 的逆序序列为 $(0-b_1, 1-b_2, \ldots, n-1-b_n)$

α 与 α' 的逆序数之和为 $n(n-1)/2$

将$n!$个置换分成 $n!/2$个组，每组逆序之和为 $n(n-1)/2$，$n!$ 个排列平均逆序数 $n(n-1)/4$，平均的交换次数至少 $n(n-1)/4$

结论：冒泡排序的最坏和平均时间复杂性均为 $O(n^2)$