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$\}$

  关于变换合成构成群

  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.

$H\le E(G)$

变换群的实例

例如 $G=\{e, a, b, c\}$，

$$f_e=\{\langle e,e\rangle,\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle\}$$

$$f_a=\{\langle e,a\rangle,\langle a,e\rangle,\langle b,c\rangle,\langle c,b\rangle\}$$

$$f_b=\{\langle e,b\rangle,\langle a,c\rangle,\langle b,e\rangle,\langle c,a\rangle\}$$

$$f_c=\{\langle e,c\rangle,\langle a,b\rangle,\langle b,a\rangle,\langle c,e\rangle\}$$

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

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元置换的表示

A 上的n 元置换：$|A| = n$ 时A 上的一一变换

表示法

置换的表示法：令 A={ 1, 2, …, n },

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & \mathrm{n} \\ \sigma(1) & \sigma(2) & \cdots & \sigma(\mathrm{n}) \end{pmatrix}$$

如: 集合S＝{a,b,c,d}，将a映射到b, b映射到d, c映射到a，d 映射到c.这个置换可以表示为

$$\sigma = \begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

k阶轮换

- **定义** 设σ是$S=\{1,2,\ldots,n\}$上的n元置换。若

  $$\sigma(i_1)=i_2,\sigma(i_2)=i_3,\ldots,\sigma(i_{k-1})=i_k,\sigma(i_k)=i_1$$

  且保持S中的其他元素对应关系不变,则称σ为S上的**k阶轮换**,记作$(i_1i_2\ldots i_k)$.

  若k=2, 也称σ为S上的**对换**。
- **存在性**：对于任何S上的n元置换σ一定存在着一个有限序列$i_1,i_2,\ldots,i_k,k\geq 1$,使得

  $$\sigma(i_1)=i_2,\sigma(i_2)=i_3,\ldots,\sigma(i_{k-1})=i_k,\sigma(i_k)=i_1$$
- **不相交**：设$\sigma(i_1i_2\ldots i_k)$和$\tau\ (j_1j_2\ldots j_s)$是两个轮换，若$\{i_1i_2\ldots i_k\}\cap\{i_1i_2\ldots i_k\}=\varnothing$，则称σ和τ是**不相交的**.

不交轮换的分解式

- 令σ_1=（$i_1i_2\ldots i_k$）,它是从σ中分解出来的第一个轮换.
- 根据函数的复合定义可将σ写作$\sigma_1\sigma'$,其中σ′作用于S-$\{i_1,i_2,\ldots,i_k\}$ 上的元素。
- 继续对σ′进行类似的分解。由于S中只有n个元素,经过有限步以后,必得到σ的**轮换分解式** $\sigma=\sigma_1\sigma_2\ldots\sigma_t$
- 在上述分解中, 任何两个轮换都是**不交的**. 即

任何n元置换都可以表示成不交的轮换之积。

n元置换的分解式（举例）

例如5元置换

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

分别是4阶和2阶轮换

σ=（1 2 3 4）,τ=（1 3），其中τ也叫做对换。

n元置换的对换分解方法

- 设$S=\{1,2,\ldots,n\}$,$\sigma=(i_1i_2\ldots i_k)$是$S$上的$k$阶轮换,那么$\sigma$可以进一步表成对换之积,即

  $(i_1i_2\ldots i_k)=(i_1i_k)\ \ldots(i_1i_3)(i_1i_2)$

- 回顾关于n元置换的轮换表示,任何n元置换都可以唯一地表示成不相交的轮换之积,而任何轮换又可以进一步表示成对换之积,所以任何n元置换都可以表成对换之积。

举例

例 设$S=\{1,2,\ldots,8\}$,

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\5&3&6&4&2&1&8&7\end{pmatrix}\quad \tau=\begin{pmatrix}1&2&3&4&5&6&7&8\\8&1&4&2&6&7&5&3\end{pmatrix}$$

是8元置换。

解 两个置换的分解式为

$\sigma=(1\ 5\ 2\ 3\ 6)(4)(7\ 8)$

$\tau=(1\ 8\ 3\ 4\ 2)(5\ 6\ 7)$

其对换表示式分别为

$\sigma=(1\ 5\ 2\ 3\ 6)(7\ 8)=(1\ 6)(1\ 3)(1\ 2)(1\ 5)(7\ 8)$

$\tau=(1\ 8\ 3\ 4\ 2)(5\ 6\ 7)=(1\ 2)(1\ 4)(1\ 3)(1\ 8)(5\ 7)(5\ 6)$

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：

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

证明思路：

(1) σ可以表成不交的轮换之积. 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 $X=\{\sigma_1\sigma_2\cdots\sigma_t\},\quad Y=\{\tau_1\tau_2\cdots\tau_l\}$

任取 $\sigma_j\in X,\sigma_j=\{i_1i_2\cdots i_m\},m>1,$

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： $1^{C_1(\sigma)}\,1^{C_2(\sigma)}\cdots 1^{C_n(\sigma)}$

$C_k(\sigma)$: k-轮换的个数

例如 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 3 & 8 & 7 & 6 & 1 & 4 \end{pmatrix}$

$= \begin{pmatrix} 1 & 5 & 7 \end{pmatrix}\begin{pmatrix} 4 & 8 \end{pmatrix}$

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

轮换指数的性质

不同指数的个数是如下方程的非负整数解的个数

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

例如：

A={1,2,3}上的置换 (1),(1 2),(1 3),(2 3),(1 2 3),(1 3 2)

轮换指数为 1^3：σ_1； $1^1 2^1$：$\sigma_2,\sigma_3,\sigma_4$； 3^1：σ_5,σ_6

不同指数的个数为3,

$x_1 + 2x_2 + 3x_3 = 3$的非负整数解个数为3.

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,且表法不唯一,

  但是对换个数的奇偶性不变

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

$$= (1\ 7)(1\ 5)(4\ 8) = (5\ 7)(1\ 7)(4\ 8)$$

- 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

如：8 元置换σ=(132)(5648)，τ=(18246573), 则

$\sigma\tau$= (1)(28734) (5)(6) =(28734)

- **置换求逆**：求反函数

σ=(132)(5648)，σ^{-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

$\sigma = \tau_1\tau_2\cdots\tau_l$ 是不交轮换的分解式，则

$|\sigma| = [|\tau_1|, |\tau_2|, \cdots, |\tau_l|]$

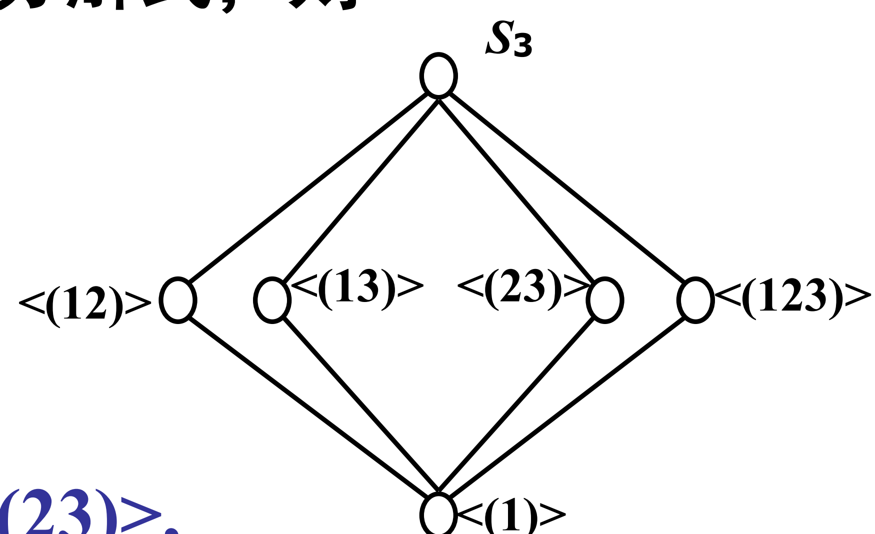
子群

$\{(1)\}$, S_n，n 元交代群A_n

例如 S_3的子群有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.

4	3
1	2

D_4={ (1), (1234), (13)(24), (1432), (12)(34),

(14)(23), (13)(2)(4), (24)(1)(3) }

$D_4 \le S_4$

17.5 群的分解

- 陪集及其性质
- Lagrange定理
- Lagrange定理的应用
- 共轭关系与共轭类
- 群的分类方程

陪集定义及其实例

陪集定义　G 为群，$H \le G$, $a \in G$,

右陪集　$Ha = \{ ha \mid h \in H \}$

Ha 中的a 称为该陪集的代表元素

实例：

S_3, $H=\{(1),(12)\}$, $H(1)=H(12)$

$H(13)=H(123)=\{(13),(123)\}$

$H(23)=H(132)=\{(23),(132)\}$

$V=\langle Z_6,+_6\rangle$, $H=\{0,2,4\}$

$H0=H2=H4=H$

$H1=H3=H5=\{1,3,5\}$

陪集的性质

定理 G 为群，H 是G 的子群，则

(1) $He=H$； (2) $a\in Ha$； (3) $Ha\approx H$；

(4) $b\in Ha \Leftrightarrow Ha=Hb \Leftrightarrow ba^{-1}\in H$

(5) 在G 上定义二元关系R, $aRb\Leftrightarrow ba^{-1}\in H$，则$R$ 为等价关系，且$[a]_R=Ha$

(6) $a,b\in G$, $Ha\cap Hb=\varnothing$ 或$Ha=Hb$，$\cup Ha=G$

说明 定义左陪集 $aH=\{ ah \mid h\in H \}$

性质类似 $b\in aH \Leftrightarrow aH=bH \Leftrightarrow a^{-1}b\in H$

陪集性质的证明

(4) $b \in Ha \Leftrightarrow Ha=Hb$

证 必要性. $b \in Ha \Leftrightarrow b=h'a \Leftrightarrow a=h'^{-1}b$

$ha \in Ha \Rightarrow ha=h'^{-1}hb \in Hb$

$hb \in Hb \Rightarrow hb=hh'a \in Ha$

充分性略.

(5) R是等价关系, $Ha=[a]$

证 $b \in [a] \Leftrightarrow aRb \Leftrightarrow ab^{-1} \in H$

$\Leftrightarrow Ha=Hb \Leftrightarrow b \in Ha$

右陪集　　左陪集

右陪集	左陪集
H的右陪集定义，即	H的左陪集定义，即
$Ha=\{ha \mid h\in H\}$，$a\in G$	$aH=\{ah \mid h\in H\}$，$a\in G$
右陪集的性质：	左陪集的性质：
1.$He=H$	1.$eH=H$
2.$\forall a\in G$，$a\in Ha$	2.$\forall a\in G$，$a\in aH$
3.$\forall a,b\in G$，$b\in Ha \Leftrightarrow ba^{-1}\in H \Leftrightarrow Ha=Hb$	3.$\forall a,b\in G$，$b\in aH \Leftrightarrow a^{-1}b\in H \Leftrightarrow aH=bH$
4.若在G上定义二元关系R，$\forall a,b\in G, \langle a,b\rangle\in R \Leftrightarrow ba^{-1}\in H$ 则R是G上的等价关系，且$[a]_R=Ha$。	4.若在G上定义二元关系R，$\forall a,b\in G, \langle a,b\rangle\in R \Leftrightarrow a^{-1}b\in H$ 则R是G上的等价关系，且$[a]_R=aH$。
5.$\forall a\in G$，$H\approx Ha$。	5.$\forall a\in G$，$H\approx aH$。

Lagrange定理的引理

引理 H 的左陪集数和右陪集数相等。

【分析】令$S=\{Hx|x\in G\}$,$T=\{xH|x\in G\}$,只需证明S≈T.

步骤：(1) 构造函数 $f: T\to S, f(Ha)=a^{-1}H$,

(2) f 的良定义性（ 单射性）

$Ha=Hb \Leftrightarrow ab^{-1}\in H \Leftrightarrow (a^{-1})^{-1}b^{-1}\in H$

$\Leftrightarrow a^{-1}H=b^{-1}H \Leftrightarrow f(Ha)=f(Hb)$

(3) f 的双射性.

注意：H 在G 中的指数$[G:H]=|S|=|T|$

H 在G 中的右（或者左）陪集数

Lagrange定理及其推论

lagrange 定理： $|G| = |H|\,[G:H]$

证明：令G 的不同的陪集为$Ha_1, Ha_2, \ldots, Ha_r$,

$$|G| = |Ha_1|+|Ha_2|+\ldots+|Ha_r| = |H|\,r = |H|\,[G:H]$$

说明： 适用于**有限群**，逆不一定为真.

推论

(1) 群的元素的阶是群的阶的因子.

证明：$\forall a\in G$, $\langle a\rangle$是G的子群，且$|\langle a\rangle| = |a|$.

(2) 素数阶群一定是循环群.

证明：$|G| = p$, $p>1$, 存在非单位元a,

$|a|$ 的阶是p 的因子，只能是 $|a| = p$.

故$G=\langle a\rangle$.

Lagrange定理的应用

例1 6阶群必含3 阶元.

证 由拉格朗日定理可知元素只能是1阶、2阶、3阶或6阶元。

1) 若存在a，$|a|=6$, 则a^2为3 阶元.

2) 假若没有6 阶元.假设没有3阶元，则$\forall a\in G$, $a^2 = e$, 则G为Abel群。取G中两个不同的2阶元a和b，令H={ a, b, ab, e },则H是子群，但$|H|=4$，$|G|=6$，与Lagrange 定理矛盾.

故一定存在3阶元。

Lagrange定理的应用（续）

例2 6阶群在同构意义上只有2个.

证明思路：

若G含6 阶元，是循环群.

若不含6 阶元，则含3 阶元a,

取$c\notin\{e, a, a^2\}$, 则c, ac, a^2c 两两不等（消去律）.

可以证明$G = \{e, a, a^2, c, ac, a^2c\}$ 同构于S_3.

先考察c, ca, ac，证明都是2阶元

构造运算表

- 推广

p是质数，$2p$ 阶群在同构意义下只有2个.

如10 阶群只有2个,4 阶群只有2个：循环群和Klein四元群.

Lagrange定理的应用（续）

例3 证明6阶可交换群是循环群。

思路：寻找其生成元，即G=<a>, $|a|=|G|=6$。

证明 设<G,*>是6阶可交换群，由例题1可知，存在$a\in G$，且$|a|=3$。

因为<G, *>是偶数阶群，所以G中必存在2阶元，

设2阶元为b，$|b|=2$。

因为2和3互质，且$a*b=b*a$，

所以$|a*b|=6$，且G= <$a*b$>，即<G,*>是循环群。

Lagrange定理的应用（续）

例4 证明阶小于6的群都是阿贝尔群。

证明 1阶群是平凡的，显然是阿贝尔群。

2阶,3阶和5阶群都是素数阶群，由拉格朗日定理的推论2可知都是循环群，也是阿贝尔群。

设G是4阶群，则G可能含有1阶，2阶或4阶元。

若G中含有4阶元a，则$G=\langle a\rangle$，G是阿贝尔群。

若G中不含4阶元，G中只含1阶和2阶元。

即$\forall x\in G$，$x^2=e$。则$\langle G,*\rangle$也是阿贝尔群。

共轭关系与共轭类

- **定义** 设G为群，定义G上二元关系R，

$$aRb \Leftrightarrow \exists x(x\in G,\ b=x^{-1}ax)$$

称R为G上的共轭关系

可以证明共轭关系是G上等价关系，等价类为**共轭类**

- **共轭类的性质：**
  - $a\in C \Leftrightarrow \bar{a}=\{a\}$，C是G的中心
  - $|\bar{a}|=[G:N(a)]$，其中

  a的正规化子：$N(a)=\{\, x \mid x\in G,\ xa=ax \,\}$是G的子群

证明见教材

群的分类方程

群的分类方程

G 为群，C 为中心，G 中至少含两个元素的共轭类有k 个，$a_1, a_2, ..., a_k$ 为代表元素，则

$|G| = |C| + [G:N(a_1)] + [G:N(a_2)] + \ldots + [G:N(a_k)]$

证明：$|C|=l,\ C=\{ a_{k+1}, a_{k+2}, \ldots, a_{k+l} \}$

$$\because \overline{a_{k+p}} = \{a_{k+p}\}, p = 1,2,\cdots,l$$

$$G = \overline{a_1} \cup \overline{a_2} \cup \cdots \cup \overline{a_k} \cup \{a_{k+1}\} \cup \{a_{k+2}\} \cup \cdots \cup \{a_{k+l}\}$$

$|G|=[G:N(a_1)]+[G:N(a_2)]+\ldots+[G:N(a_k)]+|C|$

注意：$N(a_i)<G$，

群分类方程的应用

例3 $|G|=p^s$, p 为素数，则$p|\ |C|$.

证明

$$|G| = |C|+[G:N(a_1)]+[G:N(a_2)]+\ldots+[G:N(a_k)]$$

对于$i = 1, 2, \ldots, k$,

$[G:N(a_i)]$是$|G|$的因子，$|G| = p^s$

$[G:N(a_i)] = p^t$ 或者 $[G:N(a_i)] = 1$

$[G:N(a_i)] = 1 \Rightarrow \bar{a}_i = \{a_i\} \Rightarrow a_i \in C$，矛盾

$p \mid [G:N(a_i)] \Rightarrow p \mid |C|$

作业

- 复习要点

  陪集定义

  陪集有哪些性质？

  Lagrange定理及其推论的内容

  Lagrange定理的应用

  与共轭关系相关的有哪些结果？

  了解群分类方程

- 书面作业：

  习题十七，27, 30, 32.