近世代数

计算机科学与技术学院
唐琳琳

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

置换群

- 最早被研究的群
- 每个有限的抽象群都和一个置换群同构
- **定义1**：n元对称群 S_n 的任意一个子群，都叫做一个**n元置换群**，简称为**置换群**。

注：研究有限集合置换，集合中的元素不重要。常表示为1,2,3,...n,并且一般都设n>1.

- **定义2**：一个置换 σ 如果把数码 i_1 变成 i_2，i_2 变成 i_3，…，i_{k-1} 变成 i_k，又把 i_k 变成 i_1，但别的数码（如果还有的话）都不变，则称 σ 是一个**k-轮换（循环）置换**，简称为**k-轮换（循环）**或**轮换（循环）**，并表示成：

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

例如：

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) = (321) = (213)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13) = (31)$$

置换群

• 注：1）**恒等变换**叫做1-轮换，记为

$$(1)=(2)=\cdots=(n)$$

2）2-轮换简称为**对换**，无公共数码的轮换称为**不相连轮换**。

• **定理1**：不相连轮换相乘时可以交换。

证明：设$\sigma=(i_1 i_2 \cdots i_k)$与$\tau=(j_1 j_2 \cdots j_k)$为两个不相连轮换，则由变换乘法知，乘积$\sigma\tau$与$\tau\sigma$都是集合$\{1,2,\cdots,n\}$的以下变换。

$$i_1 \to i_2, i_2 \to i_3, \cdots, i_{k-1} \to i_k, i_k \to i_1,$$
$$j_1 \to j_2, j_2 \to j_3, \cdots, j_{k-1} \to j_k, j_k \to j_1,$$

别的数码都不动。

因此易见，$\sigma\tau=\tau\sigma$。

置换群

- **定理2**：每个（非轮换）置换都可表为不相连轮换之积；每个轮换都可表为对换之积，因此，每个置换都可表为对换之积。

证明：1）任何一个置换都可以把构成一个轮换的所有数码按连贯顺序紧靠在一起，而把不动的数码放在最后。例如

$$\begin{pmatrix}1&2&3&4&5&6&7\\3&5&6&4&2&1&7\end{pmatrix}=\begin{pmatrix}1&3&6&2&5&4&7\\3&6&1&5&2&4&7\end{pmatrix}$$
$$=(136)(25)$$

一般地，对任意置换 σ 有

$$\sigma=\begin{pmatrix}i_1i_2\cdots i_k&\cdots&j_1j_2\cdots j_s&a\cdots b\\i_2i_3\cdots i_1&\cdots&j_2j_3\cdots j_1&a\cdots b\end{pmatrix}$$
$$=(i_1i_2\cdots i_k)(j_1j_2\cdots j_s)$$

即置换 σ 表示成了不相连轮换的乘积。

置换群

2）由置换乘法可知：$(1)=(12)(12)$，又

$$(i_1 i_2 \cdots i_k)=(i_1 i_k)(i_1 i_{k-1})\cdots(i_1 i_3)(i_1 i_2)$$

从而定理得证。

- **例1**：S_3 的6个置换用轮换表示出来就是：

$$(1),(12),(13),(23),(123),(132)$$

- **例2**：S_4 的24个置换用轮换或轮换的乘积表示出来就是：

(1);

$(12),(13),(14),(23),(24),(34)$;

$(123),(132),(124),(142),(134),(143),(234),(243)$;

$(1234),(1243),(1324),(1342),(1423),(1432)$;

$(12)(34),(13)(24),(14)(23)$.

- **注**：一个置换表示为对换的乘积时，表示法不是唯一的

置换群

- 例如：

$$(132)=(12)(13)$$
$$=(12)(23)(23)(13);$$
$$(1432)=(34)(13)(23)$$
$$=(23)(12)(14)$$
$$=(23)(13)(23)(13)(14)$$

虽然表示不同但是同一个置换的对换分解中，对换个数的奇偶性必然相同。

- **定理3：每个置换表示成对换乘积时，其对换个数的奇偶性不变。**

证明：设置换 σ 可表为m个对换 $\sigma_1,\sigma_2,\cdots\sigma_m$ 之积：

$$\sigma=\sigma_1\sigma_2\cdots\sigma_m \quad ,$$

则因为 σ 将排列 $12\cdots n$ 变成排列

$$\sigma(1)\sigma(2)\cdots\sigma(n) \quad ,$$

置换群

又由于 $\sigma=\sigma_1\sigma_2\cdots\sigma_m$ ，故连续施用对换$\sigma_m,\cdots,\sigma_2,\sigma_1$ 于$12\cdots n$ 也得一排列如上。但我们知道每个对换都改变排列的奇偶性...因此原置换决定的排列的奇偶性，也就决定了置换所能写称的对换的数量的奇偶性。

- **注：m与置换后的排列的奇偶性一致**。
- **定义3**：一个置换若分解成奇数个对换的乘积，则称为**奇置换**；否则称为**偶置换**。
- 特别，**恒等置换是偶置换**。
- σ奇（偶）置换 $\Leftrightarrow$ $\sigma(1)\sigma(2)\cdots\sigma(n)$为奇（偶）排列。
- n！个**n元对称群中奇偶置换各占一半**，各为$\frac{n!}{2}$ 个。
- n元对称群S_n 中奇、偶置换各占一半；恒等置换是偶置换，又任二偶置换乘积为偶置换，故S_n 中所有偶置换作成一个$\frac{n!}{2}$ 阶子群，记为A_n ，称为**n元交代（交错）群**。
- 任何置换群在奇偶性上都有这一特性。

置换群

- **例3**：求证：一个n元置换群G中的置换或者全是偶置换，或者奇、偶置换各占一半，且全体偶置换作成一个子群。

证明：若G中全部置换全是偶置换，结论已对；如果G中含有奇置换，任取其一，设为σ。并令A，B分别为G中全体奇、偶置换作成的集合，则由于σ与σ^{-1}都是奇置换，从而

$$\varphi: \qquad \tau \to \tau\sigma \qquad (\forall \tau \in A)$$

是A到B的一个双射。因此，$|A| = |B|$，即G中奇、偶置换的个数相等，各占一半（从而G的阶数为偶数）。

全体偶置换作成子群显然。（非空有限子集成子群）

单选题 1分

设置

以下关于置换的描述正确的是：（）

A 恒等置换是（1），因此为奇置换

B K-轮换当k为偶数时是奇置换

C 对换是偶置换

D K-轮换当k为奇数时是奇置换

提交

置换群

- **例4**：求证：

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

作成交代群A_4的一个交换子群。这个群（以及与其同构的群）称为Klein（C. F. Klein，1849-1925）四元群。

证明：

---对于置换乘法封闭

---结合律继承与A_4（不必验证）

---恒等置换（单位元存在）

---任意其他三个中的一个置换阶数为2（逆元是其本身）

置换群

- **置换的阶**
- **定理4**：k-轮换的阶为k；不相连轮换乘积的阶为各因子阶的最小公倍数。

证明：当$1 \le m < k$时有

$$(i_1 i_2 \cdots i_k)^m = (i_1 i_{m+1} \cdots) \neq (1),$$

而$(i_1 i_2 \cdots i_k)^k = (1)$，故$(i_1 i_2 \cdots i_k)$的阶是k。

其次，设$\sigma_1, \sigma_2, \cdots, \sigma_s$分别是阶为$k_1, k_2, \cdots, k_s$的不相连轮换，且

$$t = [k_1, k_2, \cdots, k_s],$$

则由于$k_i \mid t$，故$\sigma_i^t = (1)$。又因为不相连轮换相乘可交换，故

$$(\sigma_1 \sigma_2 \cdots \sigma_s)^t = \sigma_1^t \sigma_2^t \cdots \sigma_s^t = (1)$$

另一方面，若设$(\sigma_1 \sigma_2 \cdots \sigma_s)^r = (1)$，则同样有

$$\sigma_1^r \sigma_2^r \cdots \sigma_s^r = (\sigma_1 \sigma_2 \cdots \sigma_s)^r = (1)$$

只能是$\sigma_i^r = (1), \quad i = 1, 2, \cdots, s$，否则上式不可能为$(1)$。

置换群

但是我们知道σ_i的阶为k_i，故有$k_i \mid r$，于是$t \mid r$，即得$\sigma_1\sigma_2\cdots\sigma_s$的阶为

$$t=[k_1,k_2,\cdots,k_s]。$$

•注：此定理可以用来判断一个具体置换的阶。

例如：

(24)的阶是2，(153)的阶是3，

$(24)(153)$的阶是6，$(12)(34)$的阶是2。

而

$$\begin{pmatrix}1&2&3&4&5&6\\2&1&4&5&6&3\end{pmatrix}=(12)(3456)$$

的阶是4。

置换群

- **定理5**：设有n元置换 $\tau=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$，则对任意n元置换 σ，有

$$\sigma\tau\sigma^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{pmatrix}$$

证明：由于

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

故

$$\sigma\tau=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{pmatrix}$$

置换群

但是

$$\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}\sigma$$

$$=\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

$$=\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}=\sigma\tau$$

故

$$\sigma\tau\sigma^{-1}=\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}。$$

注：由此定理可知，当置换τ表示成轮换的乘积时，把出现在各轮换中的数码i换成$\sigma(i)$后即得$\sigma\tau\sigma^{-1}$。

置换群

- 例5：设 $\sigma=(14)(235),\tau=(153)(24)$ 。求 $\sigma\tau\sigma^{-1}=?$

解：

$$\sigma\tau\sigma^{-1}=(\sigma(1)\sigma(5)\sigma(3))(\sigma(2)\sigma(4))$$
$$=(425)(31)$$

多选题 1分

设置

以下关于置换群元素的阶数叙述正确的是：（）

A k-轮换的阶数是k

B 任一置换的阶数等于其可写成的不相连轮换的阶数的乘积

C 任一置换的阶数等于其可写成的不相连轮换的阶数的最小公倍数

D 偶置换的阶数为偶数，奇置换的阶数为奇数

提交

作业

- P65. 3、试求下列各置换的阶：

$$\tau_1=(1378)(24);\qquad \tau_2=(1372)(234)$$

$$\tau_3=\begin{pmatrix}1&2&3&4&5&6\\6&4&1&5&2&3\end{pmatrix};\qquad \tau_4=\begin{pmatrix}1&2&3&4&5&6&7\\5&7&6&3&1&4&2\end{pmatrix}$$

- 4、设 $\tau=(327)(26)(14),\ \sigma=(134)(57)$ 。试求：

$$\sigma\tau\sigma^{-1}=?\qquad \sigma^{-1}\tau\sigma=?$$

陪集、指数和Lagrange定理

• **定义1**：设H是群G的一个子群，$a \in G$。则称群G的子集

$$aH = \{ax \mid x \in H\}$$

为群G关于子群H的一个左陪集。而称

$$Ha = \{xa \mid x \in H\}$$

为群G关于子群H的一个右陪集。

•例如，$H = \{(1),(12)\}$ 是三元对称群 S_3 的一个子群，而

$$(13)H = \{(13),(123)\},\quad (23)H = \{(23),(132)\}$$

是H的两个左陪集；又

$$H(13) = \{(13),(132)\},\quad H(23) = \{(23),(123)\}$$

是H的两个右陪集。

•**注：左陪集 aH 与右陪集 Ha 一般不相等，特别当G是交换群时，他们相等。**

陪集、指数和Lagrange定理

- **左陪集性质**
- **1）** $a \in aH$
- **2）** $a \in H \Leftrightarrow aH = H$
- **3）** $b \in aH \Leftrightarrow aH = bH$
- **4）** $aH = bH$**，即a与b同在一个左陪集中** $\Leftrightarrow$ $a^{-1}b \in H$**（或** $b^{-1}a \in H$**）**

证明：设 $aH = bH$ ，则

$$a^{-1}aH = a^{-1}bH \text{，} H = a^{-1}bH$$

由性质2）可知 $a^{-1}b \in H$ 。反之，倒推即可。

- **5）若** $aH \bigcap bH \neq \Phi$ **，则** $aH = bH$

证明：设 $c \in aH \bigcap bH$ ，则 $c \in aH, c \in bH$ ，由性质3）知

$$aH = cH = bH$$

陪集、指数和Lagrange定理

- 把3）和4）联合起来就是：

$b \in aH$，即a, b属于同一个左陪集$\Leftrightarrow aH = bH \Leftrightarrow a^{-1}b \in H$（或$b^{-1}a \in H$）。

- 5）表明对任二左陪集来说，要么相等，要么无公共元素（交集为空）。
- 综合这些性质来看，群G中的元素必属于一个左陪集（性质1），且不会同时属于两个左陪集（性质5）。因此，群G的所有**左陪集**构成了G的一个**分类**，且两个元素在同一个类当且仅当$a^{-1}b \in H$（性质4）。

若$aH, bH, cH, \ldots$为群G关于子群H的所有不同左陪集，则有

$$G = aH \cup bH \cup cH \cup \cdots$$

称其为**群G关于子群H的左陪集分解**。而称$\{a, b, c, \ldots\}$为群G关于子群H的一个**左陪集代表系**。

- **注：**

1）由于H本身是G的一个左陪集，故其他的左陪集都不成群。

2）右陪集性质类似，只是性质4）改为$Ha = Hb \Leftrightarrow ab^{-1} \in H$(或$ba^{-1} \in H$)。

陪集、指数和Lagrange定理

- **定理1**：设H是群G的一个子群，又令

$$L=\{aH\,|\,a\in G\},\quad R=\{Ha\,|\,a\in G\}\ 。$$

则在L和R之间存在一个双射，从而左、右陪集的个数或者都为无限或者都有限且个数相等。

证明：在L和R之间建立映射：

$$\varphi:\qquad aH\to Ha^{-1}$$

单：若 $Ha=Hb$ ，则 $ba^{-1}\in H$ ，从而 $\left(b^{-1}\right)^{-1}a^{-1}\in H$ ，故有 $a^{-1}H=b^{-1}H$ 。

满：对任意 $Ha\in R$ ，总存在 $a^{-1}\in G$ 使得 $\varphi\left(a^{-1}H\right)=Ha$ ，故满。

- **注**：由此可知，由群G的一个**左陪集分解**

$$G=aH\cup bH\cup cH\cup\cdots \qquad \{a,b,c,...\}$$

可立即得到群G的一个**右陪集分解**：

$$G=Ha^{-1}\cup Hb^{-1}\cup Hc^{-1}\cup\cdots \qquad \left\{a^{-1},b^{-1},c^{-1},...\right\}$$

陪集、指数和Lagrange定理

- **例1**：取 S_3 的子群 $H=\{(1),(12)\}$，则

$$(1)H=\{(1),(12)\},\quad H(1)=\{(1),(12)\},$$
$$(13)H=\{(13),(123)\},\quad H(13)=\{(13),(132)\},$$
$$(132)H=\{(132),(23)\},\quad H(123)=\{(123),(23)\}.$$

于是

$$\begin{aligned} S_3 &= H\cup(13)H\cup(132)H \\ &= H\cup H(13)\cup H(123) \end{aligned}$$

它们分别是S_3关于子群H的左、右陪集分解。而 $\{(1),(13),(132)\}$与$\{(1),(13),(123)\}$分别为 S_3 关于子群H的左、右陪集代表系，而它们是不同的。

$$H\cup(13)H\cup(132)H\neq H\cup H(13)\cup H(132)$$

陪集、指数和Lagrange定理

- **定义2**：群G中关于子群H的互异的左（或右）陪集的个数叫做**H在G里的指数**，记为

$$(G:\ H)$$

- 例如，$(S_3:\ H)=3$。当然，指数可能无限也可能有限。
- **定理2**：（J. L. Lagrange, 1736-1813）设H是有限群G的一个子群，则

$|G|=|H|(G:H)$，即$(G:H)=\dfrac{|G|}{|H|}$。

从而任何子群的阶和指数都是群G的阶的因数。

证明：令$(G:H)=s$，且

$$G=a_1H\cup a_2H\cup\cdots\cup a_sH$$

是G关于子群H的左陪集分解。由于

$$\varphi:a_ih\ \rightarrow\ a_jh\quad(\forall h\in H)$$

是左陪集a_iH到a_jH的一个双射，从而$|a_iH|=|a_jH|$，于是有

陪集、指数和Lagrange定理

$$|a_1H| = |a_2H| = \cdots = |a_sH|$$

于是有$|G| = |H| \cdot s = |H|(G:H)$。

• **推论1**：有限群中每个元素的的阶都整除群的阶。

证明：设a是有限群G的一个n阶元素，则

$$|H| = \{e, a, \cdots, a^{n-1}\}$$

是G的一个n阶子群，故由定理2可知$n \mid |G|$。

•**注：素数阶群必为循环群**。

例2：由于$|S_3| = 6$，故三元对称群S_3 的子群及元素的阶都是6的因数。例如，子群

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

的阶是2，指数是3，且有$|S_3| = |H|(S_3:H)$，即$6 = 2 \cdot 3$。

陪集、指数和Lagrange定理

- **定理3**：设G是一个有限群，又 $K \le H \le G$，则

$$(G:H)(H:K)=(G:K)$$

证明：由Lagrange定理可知：

$$|G|=|H|(G:H)=|K|(G:K)$$

而 $|H|=|K|(H:K)$，可得结论成立。

•**注**：在此定理中若K=｛e｝，则定理3变为了Lagrange定理，可以看作是它的一个推论；另外当G为无限群而且 $A=\{a_1,a_2,\cdots\}$ 与 $B=\{b_1,b_2,\cdots\}$ 分别为G关于H和H关于K的左陪集代表系时，可以证明

$$AB=\{a_ib_j \mid a_i \in A, b_j \in B\}$$

是G关于K的一个左陪集代表系。因此，$(G:K)$ 无限当且仅当 $(G:H)$ 与 $(H:K)$ 至少有一个无限。

陪集、指数和Lagrange定理

- **定理4**：设H，K是群G的两个有限子群，则

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

证明：由于$H \cap K \leq H$，设 $\frac{|H|}{|H \cap K|} = m$，且

$$H = h_1(H \cap K) \cup h_2(H \cap K) \cup \cdots \cup h_m(H \cap K)\ ,$$

$$h_i \in H, \quad h_i^{-1} h_j \notin K, i \neq j\ ,$$

易知

$$HK = h_1 K \cup h_2 K \cup \cdots \cup h_m K\ ,$$

$$h_i K \cap h_j K = \Phi, \quad i \neq j\ ,$$

从而 $|HK| = m|K|$，即

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}\ 。$$

- **注：** HK **不一定是子群，又当H，K不是子群时，上等式一般不再成立。**

陪集、指数和Lagrange定理

• 由上定理可以看出，当且仅当子群H与K的交是单位元时才有

$$|HK| = |H| \cdot |K|$$

•**推论2**：设p，q是两个素数且p<q，则pq阶群G最多有一个q阶子群。

证明：设H，K是G的两个q阶子群，则由定理4可知，

$$|HK| = \frac{q^2}{|H \cap K|},$$

但 $H \cap K$ 整除q，而q是素数，故

$$|H \cap K| = 1 \text{或} q$$

若 $|H \cap K| = 1$，则由q>p知：$|HK| = q^2 > pq = |G|$，不可能。故 $|H \cap K| = q$，从而 $H = K$。

•**注**：1）以上的前提为“若有q阶子群”，以后会知道这样的群**必有且只有一个q阶子群**。

2）尽管q阶子群有且只有一个，然而p阶子群却可能有多个。例如 S_3 的2阶子群有3个。

作业：

• P71. 1、设G是n阶有限群。证明G中元素都满足方程 $x^n=e$

2、设H、K分别是群G的两个m与n阶子群。证明，若(m,n)=1，则 $H\cap K=\{e\}$。