第八章 群II

计算机系网络所：张小平

主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- **8.3 循环群 群的同构**
- 8.4 变换群和置换群 Cayley定理
- 8.5 陪集和群的陪集分解 Lagrange定理
- 8.6 正规子群与商群
- 8.7 群的同态、同态基本定理
- 8.8 群的直积

Tsinghua University

循环群 群的同构

- **定义8.3.1** 若群G中存在一个元素 a，使得G中的任意元素 g，都可以表示成 a 的幂的形式，即

$$G=\{a^k \mid k\in Z\},$$

则称G是**循环群**，记作 $G=\langle a\rangle$，a 称为G的**生成元**。

循环群 群的同构

- 思考：
  - 循环群和循环幺群的区别是什么？
  - 例：

$$(N,\ +)$$

$$(Z_m\ ,\bullet) \qquad Z_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$$

循环群 群的同构

- **定义** 对于循环群 $G=\langle a\rangle$，若生成元 a的阶数 $|a|=n$，则 $G=\langle a\rangle=\{e,a,a^2,\cdots,a^{n-1}\}$，称为$n$阶循环群；

  若$|a|$不存在，则 $G=\langle a\rangle=\{e,a,a^{-1},a^2,a^{-2},\cdots\}$ 也是无限的，称为无限阶循环群

清華大学 Tsinghua University

循环群 群的同构

- 思考：
  - 循环群的生成元有几个？
  - 例：
  - $(Z\ ,\ \ +)$ $\quad 1,\ \ -1$
  - $(Z_6\ ,\ \ \cdot)$ $\quad Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$

$(\bar{5})^0=\bar{0}$ $\quad (\bar{5})^2=\bar{4}$ $\quad (\bar{5})^4=\bar{2}$ $\quad (\bar{5})^6=\bar{0}$

$(\bar{5})^1=\bar{5}$ $\quad (\bar{5})^3=\bar{3}$ $\quad (\bar{5})^5=\bar{1}$

清華大學 Tsinghua University

循环群 群的同构

- **定理 8.3.1** 设 $G=\langle a\rangle$，则

1. 若 $O\langle a\rangle=\infty$，则 G 中只有生成元 a 或 a^{-1}
2. 若 $O\langle a\rangle=n$，则 G 中有 $\varphi(n)$ 个生成元

   – 其中 $\varphi(n)$ 是欧拉函数，它表示小于 n 且与 n 互素的正整数个数。

循环群 群的同构

- 证明：
  - 当$O\langle a\rangle=\infty$时，显然a是生成元。同时，$\forall a^k\in G$

    $a^k=\left(a^{-1}\right)^{-k}$，因此$a^{-1}$也是$G$的一个生成元
  - 假设还有另外一个生成元b，则不妨设$b=a^j$
  - 由于b也是生成元，则a可以写为$a=b^t$
  - 则必有$a=b^t=\left(a^j\right)^t=a^{jt}$，由消去律，$a^{jt-1}=e$
  - a为无限阶，则必有$jt-1=0$，故只能有

    $j=t=1$ 或 $j=t=-1$

证毕！

循环群 群的同构

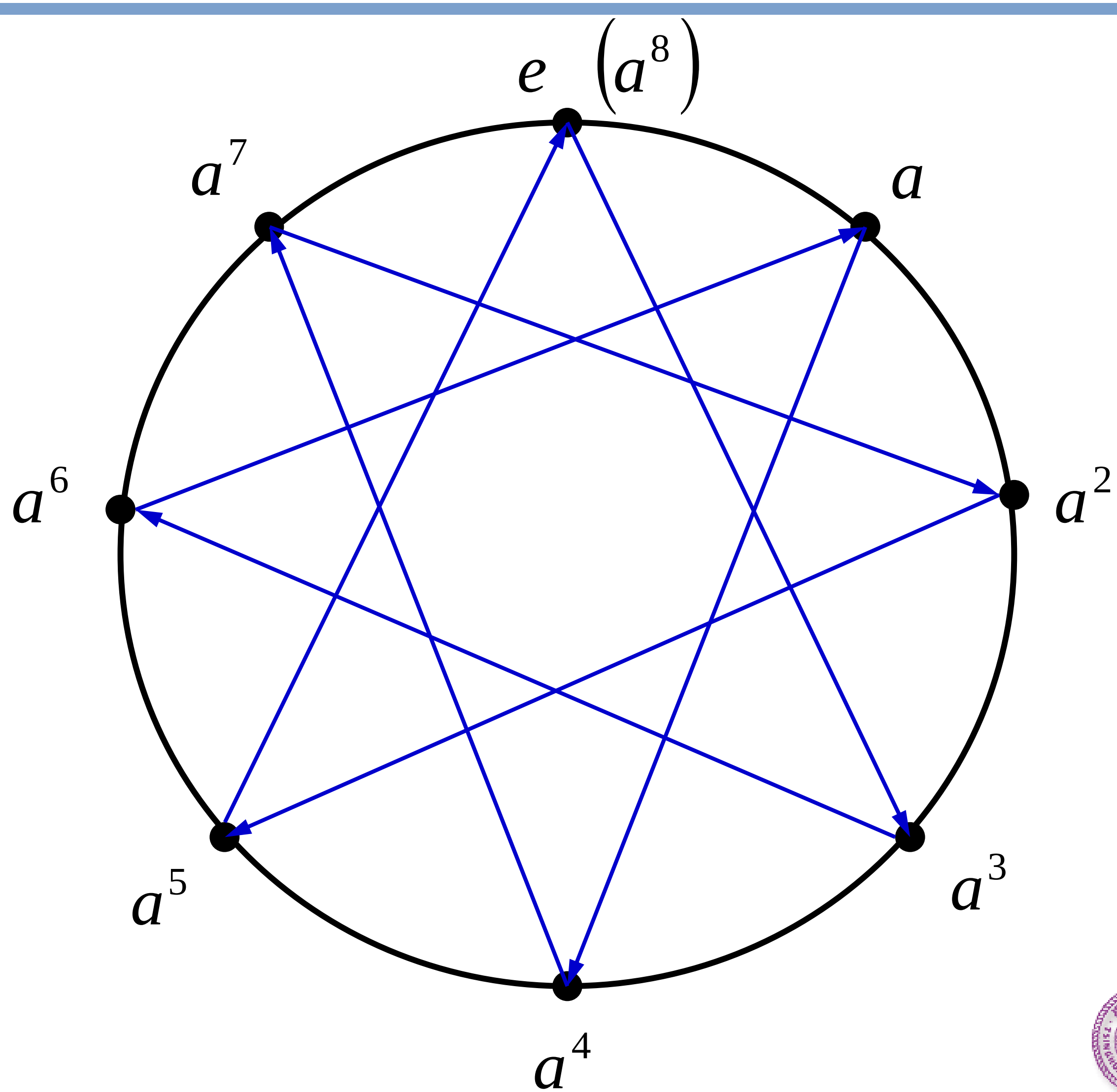
- 证明（续）：
  - 若 $G=\langle a\rangle=\langle a^r\rangle$，则存在 p 使 $a=(a^r)^p$，即 $a^{rp-1}=e$
  - 故存在 q，使得 $rp-1=qn$
  - 即 $(r,n)=1$

证毕！

Tsinghua University

循环群 群的同构

- 例：



循环群 群的同构

- 思考：
  - 循环群G的子群H是否仍然是循环群？
    - 分析：子群H的生成元？
    - G的子群H，可以写为 $H=\{e,a^{k_1},a^{k_2},\cdots,a^{k_m},\cdots\}$

不妨设H所有元素的幂次中，k_1 是最小正幂

则对于H中其他元素 a^{k_m} 幂次进行分析，一定有

$k_m = l \cdot k_1 + r$ ，其中 $0 \le r < k_1$ 。

故 $a^{k_m} = a^{r+l\cdot k_1} = a^r a^{l\cdot k_1} \Rightarrow a^r = a^{k_m}\left(a^{l\cdot k_1}\right)^{-1} \Rightarrow a^r \in H$

$r = 0$

循环群 群的同构

- 思考：
  - G为循环群时，G的子群是什么特征？
    - 若G为无限循环群：
    - 假设子群H生成元是 a^k，则该生成元的阶数一定为∞
    - 否则若存在正整数 q ，使得 $\left(a^k\right)^q = e$ ，将说明 a 为有限阶元，矛盾！

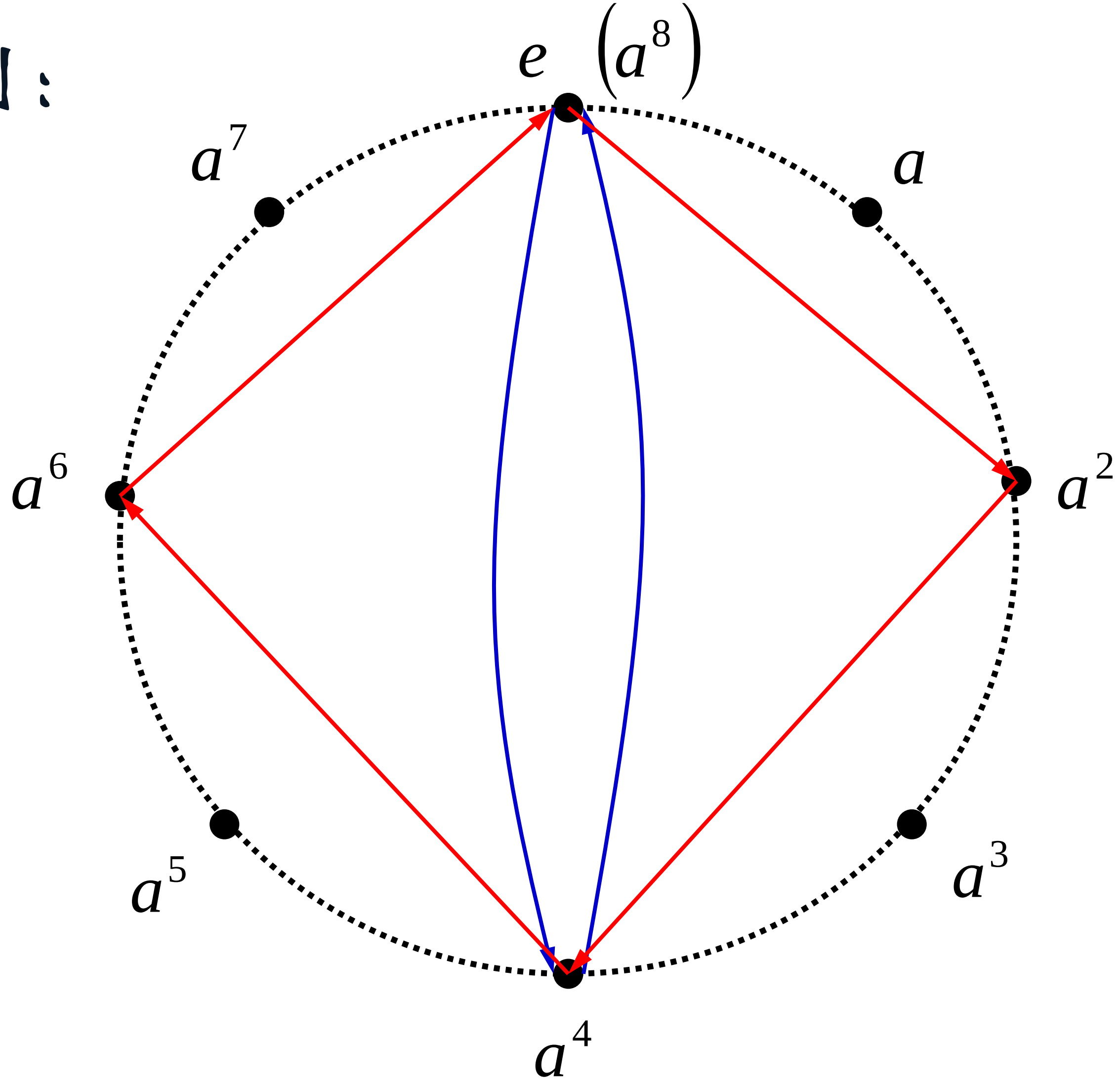
循环群 群的同构

- 思考：
  - G为循环群时，G的子群是什么特征？
    - 若G为n阶循环群：
    - 假设子群H生成元是a^{k_1}，设其阶数为 d
    - 自然，有$\left(a^{k_1}\right)^d = e$
    - 由于$\left(a^{k_1}\right)^n = (a^n)^{k_1} = (e)^{k_1} = e$ ，则必定有$d|n$

Tsinghua University

循环群 群的同构

- 例：



循环群 群的同构

- **定理 8.3.2** 设 $G=\langle a\rangle$ 是循环群，则

1. G的子群H都是循环群。

2. 若G是无限群，则子群 H $(H\neq\{e\})$ 也是无限群，若G是有限群时，设 $|G|=n$，且 a^k 是H中 a 的最小正幂，则 $|H|=n/k$ 。

循环群 群的同构

- 问题：
  - n阶循环群，对于n的某个因子，可有几个子群
  - 例如：10阶循环群，因子为2、5，则对应生成元阶为2的循环子群有几个？

循环群 群的同构

- **定理 8.3.3** 设G是n阶循环群，则对于 n 的每一个正因子d，G有且只有一个d 阶子群。

证明：

- 由于d为n的正因子，可知 $H=\left\langle a^{\frac{n}{d}}\right\rangle$ 是G的d阶子群。
- 假设存在$H_1=\langle a^m\rangle$也是G的d阶子群，且a^m是H_1中最小正幂元。

循环群 群的同构

- 证明（续）：
  - 显然，$a^{md}=(a^m)^d=e$，则有 $n\mid md$ ⇨ $\frac{n}{d}\mid m$
  - 令 $m=\frac{n}{d}\cdot t \quad (t\in Z)$ 则有：

$$a^m=a^{\frac{n}{d}\cdot t}=\left(a^{\frac{n}{d}}\right)^t\in H$$

  - 此时可以看出，a^m是H_1的生成元，但是却是H中的一个元素。因此必然有$H_1\subseteq H$。但是二者的阶数又相等，因而 $H_1=H$。

证毕！

Tsinghua University

- **定理 8.3.3** 设G是n阶循环群，则对于 n 的每一个正因子d，G有且只有一个d 阶子群。

循环群 群的同构

- 定义 8.3.2 设 $(G, \bullet)$ 和 $(G', *)$ 是两个群

  f： $G \to G'$ 是双射，如果 $\forall a, b \in G$ 都有

  $$f(ab) = f(a) * f(b)$$

  则称 f 是 G 到 G' 的一个同构，记作 $G \cong G'$

群同构的充分条件：1. 双射 2. 保持运算！

循环群 群的同构

- 例：设$G=(R^+, \times)$，$G'=(R, +)$，令$f: x\to \ln x$

  则 f 是从 G 到 G' 的一个双射，且 $\forall x,y\in G$

  $f(x\times y)=\ln(x\times y)=\ln x+\ln y=f(x)+f(y)$

  因此，$G\cong G'$

循环群 群的同构

- 定理8.3.4 设G是循环群，a为生成元

  1. 若$O\langle a\rangle=\infty$，则G与$(Z, +)$同构

  2. 若$O\langle a\rangle=n$，则G与$(Z_n, +)$同构

循环群 群的同构

- 证明： 1. 若$O\langle a\rangle=\infty$，则G与$(Z, +)$同构
  - 对于$O\langle a\rangle=\infty$，$\forall m,n\in Z\ (m\neq n)$，一定有$a^m\neq a^n$
  - 否则若 $a^m=a^n$ ，就有$a^{(m-n)}=e$
  - 无限循环群中，任何两个不等的元素幂次也不等

循环群 群的同构

- 证明（续）：1. 若$O\langle a\rangle=\infty$，则G与$(Z, +)$同构
  - 构造群G到Z的映射关系 $f: a^k \to k$
  - $\forall x \in G$， $f(x)=f\left(a^k\right)=k \in Z$ 说明 f 为映射
  - $\forall a^m, a^n \in G \ \left(a^m \neq a^n\right) \Rightarrow m \neq n \Rightarrow f\left(a^m\right) \neq f\left(a^n\right)$
  - $\forall k \in Z$， 必定$\exists a^k \in G$， 使得 $f\left(a^k\right)=k$
  - 因此 f 是双射！

循环群 群的同构

- 证明（续）：1. 若$O\langle a\rangle=\infty$，则G与$(Z，+)$同构
  - 群G到Z的映射关系 $f: a^k \to k$ 为双射！
  - 考察$\forall x,y\in G$，其中$x=a^m,y=a^n$

    $$f(xy)=f\left(a^m a^n\right)=f\left(a^{m+n}\right)=m+n=f(x)+f(y)$$

  - 因此f是G到Z的一个同构映射

$$G\cong Z$$

Tsinghua University

循环群 群的同构

- 证明（续）：2. 若$O\langle a\rangle = n$，则G与$(Z_n，+)$同构
  - 构造群G到Z的映射关系 $f：a^k \to \overline{k} \quad (0 \le k < n)$

  - 由于 $G = O\langle a\rangle$，故 G 中所有元素为 $e, a^1, a^2, \cdots, a^{n-1}$
  - Z_n 中所有元素为 $\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}$
  - 易证，映射 f 是从 G 到 Z_n 的双射！

循环群 群的同构

- 证明（续）：2. 若$O\langle a\rangle = n$，则G与$(Z_n, +)$同构
  - 存在群G到Z的双射关系 $f: a^k \to \overline{k} \quad (0 \le k < n)$

  - 考察 $\forall x, y \in G$，其中$x = a^{m_1}, y = a^{m_2} \quad (0 \le m_1 \le m_2 < n)$

$$f(xy) = f\left(a^{m_1}a^{m_2}\right) = f\left(a^{m_1+m_2}\right) = f\left(a^{(m_1+m_2) \bmod n}\right) = (m_1 + m_2) \bmod n$$
$$= f(x) + f(y)$$

  - 因此，f 是G 到 Z_n 的一个同构映射！

$$G \cong Z_n$$

证毕！

循环群 群的同构

- **定理 8.3.4** 设 G 是循环群，a 为生成元

  1. 若 $O\langle a\rangle=\infty$，则 G 与 $(Z, +)$ 同构
  2. 若 $O\langle a\rangle=n$，则 G 与 $(Z_n, +)$ 同构

循环群 群的同构

- 小结：
  - 循环群的定义
  - 生成元相关定理、性质
  - 子群相关定理、性质
  - 群的同构概念
  - 循环群的同构性质
  - 利用同构做群的判定

主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- **8.4 变换群和置换群 Cayley定理**
- 8.5 陪集和群的陪集分解 Lagrange定理
- 8.6 正规子群与商群
- 8.7 群的同态、同态基本定理
- 8.8 群的直积

变换群和置换群 Cayley定理

- 定义8.4.0 设 $A=\{a_1,a_2,\cdots\}$ 是一个非空集合，

A 到 A 的一个映射 f 称为 A 的一个**变换**，记做

$$f:\begin{bmatrix} a_1 & a_2 & \cdots \\ f(a_1) & f(a_2) & \cdots \end{bmatrix}$$

其中，恒等变换记为 I

变换群和置换群 Cayley定理

- 记集合A上全部变换的集合为$M(A)$
  - 若$|A|=n$，则$|M(A)|=n^n$

- 如果变换是双射的话，我们称之为**一一变换**。

变换群和置换群 Cayley定理

- 对于 A 中的两个变换 f，g，定义 A 的另一个变换 gf 为：

$$gf(a)=g\left(f(a)\right) \qquad \forall a\in A$$

称为变换 f 与 g 的乘积（或乘法运算）

- 对于代数系统 $(M(A),\cdot)$：
  - 变换乘法运算符合结合律
  - $fI=If=f$

清華大學 Tsinghua University

变换群和置换群 Cayley定理

- 定义 8.4.1 非空集合A的所有一一变换关于变换的乘法所作成的群叫做A的一一变换群，用 $E(A)$表示，$E(A)$的子群叫做 变换群

变换群和置换群 Cayley定理

- 当集合A为有限集合时，即$|A| = n$时，A中的一个一一变换称为一个n元置换，由置换构成的群称为置换群。

- 思考：
  - 置换群与变换群的区别？

变换群和置换群 Cayley定理

- 对于 n 元置换，可表示为：

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

- 显然，$\sigma(1),\sigma(2),\cdots,\sigma(n)$ 就是 $1\sim n$ 的一个排列。
- 反之，$1\sim n$ 的一个排列，唯一对应一个 n 元置换，则共有 $n!$ 个 n 元置换。
- 用 S_n 表示这 $n!$ 个 n 元置换的集合

变换群和置换群 Cayley定理

- 定义 8.4.2 S_n 对于置换乘法构成群，称为 n 次对称群。

  S_n 的子群称为 n 元置换群。

变换群和置换群 Cayley定理

- 对于一个置换 σ，如果满足

$$s(i_1)=i_2, \quad s(i_2)=i_3, \quad \cdots \quad ,s(i_l)=i_1$$

则称 $(i_1,i_2,\cdots,i_l)$是一个长度为 l 的轮换

当 $l=1$ 时，称为恒等置换

当 $l=2$ 时，称为对换

变换群和置换群 Cayley定理

- 例：
  - 置换 $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$

$$\sigma(1) = 3$$
$$\sigma(3) = 2$$
$$\sigma(2) = 4$$
$$\sigma(4) = 1$$

  - 因此，该置换可写为轮换的形式：$(1,3,2,4)$

$(3,2,4,1)$　$(2,4,1,3)$　$(4,1,3,2)$

变换群和置换群 Cayley定理

- 例：
  - 置换 $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 7 & 6 & 5 & 2 & 3 \end{bmatrix}$

$$\begin{cases} \sigma(1) = 4 \\ \sigma(4) = 6 \\ \sigma(6) = 2 \\ \sigma(2) = 1 \end{cases} \Rightarrow (4,6,2,1)$$

$$\begin{cases} \sigma(3) = 7 \\ \sigma(7) = 3 \end{cases} \Rightarrow (7,3)$$

$$\left[\sigma(5) = 5\right. \Rightarrow (5)$$

  - 因此，该置换可写为：$(4,6,2,1)(7,3)(5)$
  - 通常，恒等置换不写入置换的表达式中

变换群和置换群 Cayley定理

- 思考：
  - 置换和轮换的关系？
    - 轮换是某种特定形式的置换。
    - 轮换的乘积，仍然是置换。
    - 置换是否一定是轮换的乘积？
      - 如果是，有多少种表现形式？

变换群和置换群 Cayley定理

- **定义 8.4.3** 设 α,β 是 S_n 中的两个轮换，如果 α 和 β 中的元素都不相同，则称 α 和 β 是不相交的。

- **定理 8.4.1** 设 α,β 是两个不相交的轮换，则 $\alpha\beta=\beta\alpha$。（证明留做练习题）

变换群和置换群 Cayley定理

- 定理8.4.2： S_n中任意一个n元置换，一定可以表示成不相交轮换的乘积的形式，并且表示法是唯一的。即：$\forall\sigma\in S_n$, $\sigma=\sigma_1\sigma_2\cdots\sigma_t$

假如 $\sigma=\sigma_1\sigma_2\cdots\sigma_t=\tau_1\tau_2\cdots\tau_l$

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

定理的证明，留做选作作业题。提示：用数学归纳法

变换群和置换群 Cayley定理

- 事实上，一个置换如果写为可相交的轮换的乘积，表达式将是无穷多个

变换群和置换群 Cayley定理

- 引理8.4.1 设 $s=(i_1,i_2,\cdots,i_k)$ 是 S_n 上的 k 阶轮换

  $k>1$，则 $s=(i_1\quad i_k)(i_1\quad i_{k-1})\cdots(i_1\quad i_2)$

- 比如，任意一个轮换 σ，都可以表示为对换的乘积，且可以无穷多个。例如：

$$\sigma=(1\,2\,3\,4)=(2\;3)(3\;4)(4\;1)=(1\;4)(1\;3)(1\;2)\;\cdots\cdots$$

Tsinghua University

变换群和置换群 Cayley定理

- 对于一个 n 元置换：
  - 表示成不相交轮换的乘积时，表示法是唯一的
  - 表示为对换乘积时，表示法并不唯一
  - 对换的个数也不是确定的
- 问题：
  - 一个置换表示为对换乘积时，确定的是什么？

变换群和置换群 Cayley定理

- 定义8.4.4 设 $i_1 i_2 \cdots i_n$ 是 $1,2,\cdots,n$ 的一个排列，若 $i_k > i_l$ 且 $k<l$，则称 $i_k i_l$ 是一个**逆序**

  排列中逆序的总数称为这个排列的**逆序数**

- 例如：25431的逆序数？
  - 21，54，53，51，43，41，31共7个
  - 25431的逆序数为7

清華大學 Tsinghua University

变换群和置换群 Cayley定理

- 引理8.4.2 设 $\sigma \in S_n$ 且 $\sigma(j)=i_j$，$j=1,2,\cdots,n$，则在 σ 的对换表示中，对换个数的奇偶性与排列 $p=i_1i_2\cdots i_n$ 的逆序数奇偶性相同，记为 $N(\sigma)$
- 如果 $N(\sigma)$ 为奇数，则称 σ 为奇置换，否则称之为偶置换。

变换群和置换群 Cayley定理

- **定理8.4.3** n 次对称群 S_n 中所有偶置换的集合，对于 S_n 中的置换乘法构成子群，记为 A_n，称为交错群，若 $n \geq 2$，则 $|A_n| = \frac{1}{2}n!$

变换群和置换群 Cayley定理

- 小结：
  - 变换，所有变换构成的代数系统
  - 一一变换，一一变换群，变换群
  - 对称群，置换群
  - 置换：轮换，对换，恒等置换
  - 逆序、逆序数、置换的逆序数性质
  - 交错群

变换群和置换群 Cayley定理

- 定理 8.4.4 (Cayley定理)任意群 G 与一个变换群同构。

证明：首先构造一个变换群：

- 任取 $a \in G$ 定义 G 上的一个变换 f_a： $x \to ax, \forall x \in G$
- 定义 $\overline{G} = \{f_a | a \in G\}$，想办法证明其为变换群
- 再想办法证明$(G, \cdot) \cong (\overline{G}, \circ)$

Tsinghua University

变换群和置换群 Cayley定理

- 证明（续）：证 f_a： $x \to ax$ 是双射
  - 考察 $\forall b \in G$，是否存在 $x \in G$，使得 $f_a(x) = b$

    实际上，群G中方程 $ax = b$ 有唯一解
  - 因此 f_a 是满射。

  $\forall x_1, x_2 \in G$， $x_1 \neq x_2$

  $\Longrightarrow f_a(x_1) = ax_1 \neq ax_2 = f_a(x_2) \Longrightarrow f_a$ 是单射
  - 因此， f_a 是双射。

清華大学 Tsinghua University

变换群和置换群 Cayley定理

- 证（续）：证$\overline{G}=\{f_a|a\in G\}$关于变换乘法成群
  - $\forall f_a, f_b\in\overline{G}$, $(f_a f_b)(x)=f_a(f_b(x))=f_a(bx)=abx=f_{ab}(x)$
  - $\forall f_a, f_b\in\overline{G} \Leftrightarrow a,b\in G \Rightarrow ab\in G \Rightarrow f_{ab}\in\overline{G}$
  - $\forall f_a\in\bar{G}, f_a f_e=f_{ae}=f_a$，$f_e$是变换中的单位元
  - $\forall f_a\in\bar{G}$，$\exists f_{a^{-1}}\in\bar{G}$，$f_a f_{a^{-1}}=f_{a^{-1}}f_a=f_e$，因此

    $\forall f_a\in\bar{G}$ 存在逆元素 $f_a{}^{-1}=f_{a^{-1}}$

变换群和置换群 Cayley定理

- 证明（续）：证 $(G,\cdot)$和$(\bar{G},*)$同构
  - 构造映射关系 $\varphi: a \to f_a$
  - $\forall a,b,x \in G$，$a \neq b \Rightarrow ax \neq bx \Rightarrow f_a \neq f_b \Rightarrow \varphi(a) \neq \varphi(b)$
  - $\forall f_a \in \overline{G}$，一定存在 $a \in G$，使得 $\varphi(a) = f_a$
  - $\varphi(ab) = f_{ab} = f_a f_b = \varphi(a)\varphi(b)$
  - 因此，$(G,\cdot) \cong (\bar{G},*)$

证毕！

变换群和置换群 Cayley定理

- **定理 8.4.4** (Cayley定理)任意群 G 与一个变换群同构。

- 推论：设 G 是 n 阶有限群，则 G 与 S_n 的一个子群同构。

变换群和置换群 Cayley定理

- 小结：
  - Cayley定理

主要内容

- 8.1 半群
- 8.2 群、群的基本性质
- 8.3 循环群 群的同构
- 8.4 变换群和置换群 Cayley定理
- **8.5 陪集和群的陪集分解 Lagrange定理**
- 8.6 正规子群与商群
- 8.7 群的同态、同态基本定理
- 8.8 群的直积

Tsinghua University

陪集和群的陪集分解 Lagrange定理

- **定义8.5.1** 设 H 是群 G 的一个子群，对任意的 $a \in G$，集合

$$aH = \{ah \mid h \in H\}$$

称为子群 H 在 G 中的一个左陪集。同理，H 在 G 中的一个右陪集是

$$Ha = \{ha \mid h \in H\}$$

思考：左陪集和右陪集是否相等？

Tsinghua University

陪集和群的陪集分解 Lagrange定理

- **定理 8.5.1** 设H是G的子群，则H的左陪集具有下述性质

1. $H = eH, a \in aH$。

2. $|aH| = |H|$。

因H为G的子群，故消去律成立。则 $\forall h_1, h_2 \in H$，若 $h_1 \neq h_2$，则 $\forall a \in G$ 必定有 $ah_1 \neq ah_2$，故aH中没有共同元素，故 $|aH| = |H|$

3. $a \in H \Leftrightarrow aH = H$。

因为 $a \in H$，所以 $aH = \{ah \mid h \in H\} \subseteq H$

因为 $a \in H$，$\therefore a^{-1} \in H$，$\therefore \forall x \in H$，$a^{-1}x \in H$，$\therefore x = a(a^{-1}x) \in aH$

因此 $H \subseteq aH$ $\Rightarrow$ $aH = H$

4. $\forall x \in aH$，都有$xH = aH$，并叫a是aH的一个陪集代表

证明：

- $\forall x \in aH$，必定有$x = ah_1$，其中$h_1 \in H$
- $\forall xh \in xH$，有 $xh = (ah_1)h = a(h_1h) = ah'$，其中$h' \in H$
- 因此 $ah' \in aH$ 即$\forall xh \in xH$，有$xh \in aH$ 即$xH \subseteq aH$
- $\forall ah' \in aH$， $\because x = ah_1$， $\therefore a = xh_1^{-1}$
- 故 $ah' = (xh_1^{-1})h' = x(h_1^{-1}h') \in xH$ 即$aH \subseteq xH$

陪集和群的陪集分解 Lagrange定理

5. $aH = bH \Longleftrightarrow a \in bH$ 或 $b \in aH$

$$\Longleftrightarrow b^{-1}a \in H \text{ 或 } a^{-1}b \in H$$

证明：

- 充分性：由性质1可知，$a \in aH = bH$
- 故 $\exists h' \in H$，使得 $a = bh'$ 即 $b^{-1}a = h' \in H$
- 必要性：因 $b^{-1}a \in H$ 所以 $\exists h_1 \in H$ 使得 $b^{-1}a = h_1$
- 即 $a = bh_1$，即 $a \in bH$ 。由性质4， $bH = aH$
- 性质的另一半，显然！

思考：说明了什么？

Tsinghua University

陪集和群的陪集分解 Lagrange定理

6. $\forall a,b \in G$,若非 $aH = bH$,必有 $aH \cap bH = \phi$

证明：

- 假如 $aH \cap bH \neq \phi$，则必定 $\exists x \in aH \cap bH$
- 也就是 $x \in aH$ ，同时 $x \in bH$
- 则根据性质4，一定有 $xH = aH = bH$

陪集和群的陪集分解 Lagrange定理

- **定理 8.5.1** 设H是G的子群，则H的左陪集具有下述性质

1. $H = eH, a \in aH$ 2. $|aH| = |H|$ 3. $a \in H <=> aH = H$

4. $\forall x \in aH$, 都有$xH = aH$，并叫a是aH的一个陪集代表

5. $aH = bH <=> a \in bH$ 或 $b \in aH$

$<=> b^{-1}a \in H$ 或 $a^{-1}b \in H$

6. $\forall a, b \in G$,若非 $aH = bH$,必有 $aH \cap bH = \phi$

清華大學 Tsinghua University

陪集和群的陪集分解 Lagrange定理

- 定理8.5.2设G是有限群，H是G的子群，则存在一个正整数k，满足

$$G = a_1H \bigcup a_2H \bigcup \cdots \bigcup a_kH$$

其中 $a_iH \bigcap a_jH = \phi, \quad i \neq j, \quad i, j = 1, 2, \cdots, k$

- 思考：
  - 单位元e在那个陪集中？

陪集和群的陪集分解 Lagrange定理

- **定义8.5.2** 群G关于其子群H的左陪集的个数，称为H在G中的**指数**，记作$[G:H]$。

- 观察G的子群$H = \{e\}$：
  - H的左陪集个数为$|G|$
  - $[G:H] = [G:1] = |G|$

Tsinghua University

陪集和群的陪集分解 Lagrange定理

- **Lagrange定理** 设G是有限群，H是G的子群，则

$$[G:1]=[G:H][H:1]$$

陪集和群的陪集分解 Lagrange定理

- 推论1、设有限群 G 的阶为n，则 G 中任意元素a的阶都是n的因子，且适合 $a^n=e$

证明：

- $\forall a\in G$，可以得到G的循环子群 $H=\langle a\rangle$
- 则根据Lagrange定理，$p|H|=|G|=n$
- 又有 $a^{|H|}=e$ $\Longrightarrow$ $a^n=a^{p|H|}=\left(a^{|H|}\right)^p=e^p=e$

Tsinghua University

陪集和群的陪集分解 Lagrange定理

- 推论2　阶为素数p的群G是循环群。

  证明：

  - 对于任意一个非单位元的G中元素a
  - 根据推论1，a的阶为p的因子，因此只能为p
  - 故所有非单位元的元素阶均为p

Tsinghua University

陪集和群的陪集分解 Lagrange定理

- 推论3、设 A, B 是群 G 的两个有限子群，则

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

其中 $AB = \{ab \mid a \in A, b \in B\} = \bigcup_{a \in A} aB$。

陪集和群的陪集分解 Lagrange定理

证明：

G的子群
A的子群

- 因为 $B \le G$，所以 aB是B的左陪集
- 令 $S_1=\{aB \mid a \in A\}=\{a_1B,a_2B,\cdots,a_mB\}$，$D=A\cap B$
- 故 $A=\bigcup aD$，令 $S_2=\{aD \mid a \in A\}=\{a_1D,a_2D,\cdots,a_mD\}$
- 构造 S_1 与 S_2 的一一映射关系 σ： $a_iB \to a_iD$

$\forall a_i,a_j \in A,$ 若 $a_iB=a_jB,$ 必有 $a_i^{-1}a_j \in B$

且 $a_i^{-1}a_j \in A,$ 故 $a_i^{-1}a_j \in A\cap B = D \Leftrightarrow a_iD=a_jD$

陪集和群的陪集分解 Lagrange定理

证明（续）：$S_1=\{a_1B,a_2B,\cdots,a_mB\}$ $S_2=\{a_1D,a_2D,\cdots,a_mD\}$

- σ： $a_iB \to a_iD$ 为双射。
- 显然 $|S_1|=|S_2|=k$
- 因此 $|AB|=\left|\bigcup_{a\in A} aB\right|=k|B|$，同理，$|A|=k|D|$
- 两式合并，即得 $|AB|=\dfrac{|A||B|}{|A\cap B|}$

证毕！

陪集和群的陪集分解 Lagrange定理

- 推论 1、设有限群 G 的阶为n，则 G中任意元素a的阶都是n的因子，且适合 $a^n = e$
- 推论 2　阶为素数 p 的群G是循环群。
- 推论 3、设 A, B 是群 G 的两个有限子群，则

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

陪集和群的陪集分解 Lagrange定理

- 小结：
  - 左陪集
  - 左陪集6个性质
  - 群的陪集分解
  - Lagrange定理
  - 几个重要推论

作业

- 课后：
  - 13，14，21，25，27，30
- 选作：
  - 课件中的定理证明。
  - 23题
- 第三次习题课：
  - 6月3日
  - 报名截止时间：5月28日17:00，29日线上试讲