第八章 群

刘世霞
shixia@tsinghua.edu.cn

问题解答

- 请问书上例8.3.6（3）的 $\langle a, b\rangle$ 是什么意思
  - 指由元素a, b生成的最小的子群。该符号的定义在第8.3节的开头
- 计算陪集时怎么选择原群中的元素?
  - 应当遍历每一个元素以计算所有的陪集
  - 定理8.5.1说明，$a \in bH \Leftrightarrow aH = bH$，因此如果元素已经出现在已经计算过的陪集里，就无需重复计算
- (6 3 2 1)和(4 6)这种类型的轮换算相交吗
  - 算相交，$(6\ 3\ 2\ 1)(4\ 6) = (3\ 2\ 1\ 6\ 4)$

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。

求置换类型数目的一般解法

- 对于一个n阶置换，将其分解为不相交轮换的乘积，并记k-轮换出现的次数为c_k。
  - 例如，(1)(2)(3)(45)(6789)有3个1-轮换，1个2-轮换和1个4-轮换。
- 那么S_n中与之具有相同类型的置换个数为

$$\frac{n!}{1^{c_1}2^{c_2}3^{c_3}\cdots n^{c_n}\ \ c_1!\,c_2!\cdots c_n!}$$

- 证明：数字1~n 的全排列有 $n!$ 个
  - 每个k-轮换内部都有$(i_1 i_2 \cdots i_k) = (i_2 i_3 \ldots i_k i_1) = (i_k i_1 \ldots i_{k-2} i_{k-1})$，需要除$k$。因此一共需要除$1^{c_1}2^{c_2}3^{c_3}\ldots n^{c_n}$
  - c_k个k-轮换间彼此可以交换，例如$(i_1 i_2)(i_3 i_4)(i_5 i_6) = (i_1 i_2)(i_5 i_6)(i_3 i_4) = (i_3 i_4)(i_1 i_2)(i_5 i_6) = \cdots$，需要除$c_k!$。因此一共需要除$c_1!\,c_2!\cdots c_n!$

S_5中4个元素变的置换个数
$(ab)(cd)$形: $C_5^2 * C_3^2/2 = 15$个
$(abcd)$形: $A_5^4/4 = 30$个

⇨

S_5中4个元素变的置换个数
$(ab)(cd)$形: $\frac{5!}{1^1 2^2 1!2!} = 15$个
$(abcd)$形: $\frac{5!}{1^1 4^1 1!1!} = 30$个

第八章 群

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

8.5 陪集和群的陪集分解 Lagrange定理

- 群内的子群反映了群的结构和性质，因此我们需要进一步研究有关群内子群的性质
- G是一个群，H是G的一个子群，利用H可以在G的元素之间确定一个二元关系R

$$aRb \quad \text{当且仅当} \quad ab^{-1}\in H$$

R是G中的一个二元关系，是等价关系

因此由等价关系就可以确定G的一个划分，其划分块就是子群H的陪集

8.5 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

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

- 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

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

思考：左陪集和右陪集是否相等?

实例

设 $G=S_3$，H={e,(1 2)}，取a为e，(1 3)和(2 3)时，

$eH=H=\{e,(1\ 2)\}$,

$(1\ 3)H=\{(1\ 3),(1\ 2\ 3)\}$,

$(2\ 3)H=\{(2\ 3),(1\ 3\ 2)\}$,

$He=H$,

$H(1\ 3)=\{(1\ 3),(1\ 3\ 2)\}$,

$H(2\ 3)=\{(2\ 3),(1\ 2\ 3)\}$,

$G=eH\cup(1\ 3)H\cup(2\ 3)H$

(1 3)(1 2)= (3 1 2)

显然一般情况下

$$aH\neq Ha$$

轮换计算的一个小技巧

$\forall i, j,$ 当 $a_i \neq b_j$ 时

$$(a_1, \cdots a_n, c)(c, b_1, \cdots b_m) = (a_1, \cdots a_n, c, b_1, \cdots b_m)$$

- 例，计算(132)(13)(24)

$$(132)(13)(24) = (213)(13)(24) = (21)(13)(13)(24)$$

$$= (21)(24) = (12)(24) = (124)$$

实例

$G = (Z, +)$, $H = \{km \mid k \in Z\}$, H是G的子群，因为G是交换群，H的左、右陪集相等，它们是

$$0+H = H+0 = \{km \mid k \in Z\},$$

$$1+H = H+1 = \{1+km \mid k \in Z\},$$

$$2+H = H+2 = \{2+km \mid k \in Z\},$$

$$\ldots$$

$$m-1+H = H+m-1 = \{m-1+km \mid k \in Z\},$$

每个陪集正好与一个同余类对应

8.5 陪集和群的陪集分解 Lagrange定理

- 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$|aH| = |H|$

H的任意一个左陪集，其元素个数与H相同

3. $a \in H \Leftrightarrow aH = H$。

$\Rightarrow$: 因为$a \in H$，所以$aH = \{ah|h \in H\} \subseteq H$

$\forall h \in H, h = (aa^{-1})h = a(a^{-1}h) \in aH$ 故$H \subseteq aH$，故$aH = H$

$\Leftarrow$: $a = ae \in aH = H$

子群中任意一个元素和子群自身作用，得到的左陪集仍为子群自身

8.5 陪集和群的陪集分解 Lagrange定理

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

- 证明：左陪集中任意一个元素和子群H作用，得到的左陪集不变

$\forall x \in aH$，必定有$x = ah_1$，其中$h_1 \in H$

$\forall xh \in xH$，有$xh = (ah_1)h = a(h_1 h) = ah'$，其中$h' \in H$

因此$ah' \in aH$ 即$\forall xh \in xH$，有$xh \in aH$ 即$xH \subseteq aH$

$\forall ah' \in aH, \because x = ah_1, \therefore a = x{h_1}^{-1}$

故$ah' = \left(x{h_1}^{-1}\right)h' = x\left({h_1}^{-1}h'\right) \in xH$ 即$aH \subseteq xH$

8.5 陪集和群的陪集分解 Lagrange定理

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

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

- 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？

左陪集中任意一个元素和子群H作用，得到的左陪集不变

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

8.5 陪集和群的陪集分解 Lagrange定理

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

- 证明：
  - 假如 $aH \cap bH \neq \emptyset$，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$xH = aH = bH$

同一子群的两个左陪集要么相等、要么交集为空！

思考：该性质意味着什么？

$$G = \bigcup_{a \in G} aH$$

aH是G的一个划分

8.5 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. $|aH| = |H|$。

H的任意一个左陪集，其元素个数与H相同

3. $a \in H \Leftrightarrow aH = H$。

子群中任意一个元素和子群自身作用，得到的左陪集仍为子群自身

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

左陪集中任意一个元素和子群H作用，得到的左陪集不变

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

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

同一子群的两个左陪集要么相等、要么交集为空！

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

8.5 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

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

- 其中 $a_iH \cap a_jH = \emptyset, i \neq j, i, j = 1,2, \cdots, k$

- 思考：
  - 单位元e在哪个陪集中？

8.5 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$|G|$
  - $[G:H]=[G:1]=|G|$

8.5 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

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

$$G=a_1H\cup a_2H\cup\cdots\cup a_mH$$
$$|G|=m|H|=[G:H]|H|$$

有限群中，子群的阶只能是群的阶的因子！

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$[G:H]$。

8.5 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中任意元素的阶都是n的因子，且适合$x^n = e$。

- 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，$p|H| = |G| = n$（p为正整数）
  - 又有$a^{|H|} = e \Longrightarrow a^n = a^{p|H|} = (a^{|H|})^p = e^p = e$

$$\boxed{|G| = m|H| = [G:H]|H|}$$

8.5 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：
  - 取G 中一非单位元a，可以得到G的循环子群$H = \langle a \rangle$
  - 根据推论1，a的阶为p的因子，因此只能为p，所以 $O\langle a \rangle = p$
  - 所以$G = \langle a \rangle$

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

8.5 陪集和群的陪集分解 Lagrange定理

设A,B是群G的两个有限子群，则

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

推论3

- 证明:
  - 因为B是G的子群，所以aB是B的左陪集
  - 令$S_1 = \{aB|a \in A\} = \{a_1B, a_2B, \cdots, a_mB\}$，$D = A \cap B$
  - 故$A = \bigcup aD$，令$S_2 = \{aD|a \in A\} = \{a_1D, a_2D, \cdots, a_mD\}$
  - 构造S_1与S_2的一一映射关系$\sigma: a_iB \to a_iD$
  - $\forall a_i, a_j \in A$，若$a_iB = a_jB$，必有${a_i}^{-1}a_j \in B$（定理8.5.1）
  - 且${a_i}^{-1}a_j \in A$，故${a_i}^{-1}a_j \in A \cap B = D \Leftrightarrow a_iD = a_jD$
  - 故σ是映射，且是单射，也是满射

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

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

8.5 陪集和群的陪集分解 Lagrange定理

设A,B是群G的两个有限子群，则
$$|AB| = \frac{|A||B|}{|A\cap B|}$$

推论3

- 证明（续）：

$S_1 = \{a_1B, a_2B, \cdots, a_mB\}$ $S_2 = \{a_1D, a_2D, \cdots, a_mD\}$

  - $\sigma: a_iB \to a_iD$为双射。
  - 显然$|S_1| = |S_2| = k = [A:D] = |A|/|D|$
  - 因此$|AB| = |\cup_{a\in A} aB| = |S_1||B| = k|B|$，
  - 两式合并，即得$|AB| = \frac{|A||B|}{|A\cap B|}$ 证毕！

$$AB = \{ab|a \in A, b \in B\} = \cup_{a\in A} aB$$

8.5 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中任意元素的阶都是n的因子，且适合$x^n = e$。
- 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

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

利用Lagrange定理可以确定一个群内的可能存在的子群、元素的阶等，从而搞清一个群的结构

根据$|G|$的因子来确定可能存在子群的阶数或元素的阶数

Lagrange定理

- 设G是有限群，H是G的子群，则

$$[G:1] = [G:H][H:1]$$
$$G = a_1H \cup a_2H \cup \cdots \cup a_mH$$
$$|G| = m|H| = [G:H]|H|$$

设置

证明：6阶群一定存在一个3阶子群

提示：根据元素的阶分情况讨论

正常使用主观题需2.0以上版本雨课堂

作答

证明：6阶群一定存在一个3阶子群

- 对于6阶群G，非单位元的元素的阶只可能为$2,3,6$
- 如果存在6阶元a，则子群$\langle a^2 \rangle$为3阶子群
- 如果存在3阶元a，则子群$\langle a \rangle$为3阶子群
- 然后用反证法，证明G不能只由单位元和2阶元构成
  - 如果G只由单位元和2阶元构成，即每个元素的逆都是自身。则$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$，故$G$为交换群（上周作业题）
  - 此时取两个2阶元a, b，其生成的子群为$\{e, a, b, ab\}$ 为一个四阶子群。拉格朗日定理说明子群的阶一定是群的阶的因子。但4不是6的因子，矛盾
  - 因此，G不能只由单位元和2阶元构成
- 综上， 6阶群G必有3阶子群。

8.5 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

第八章 群

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

8.6 正规子群与商群

- 如果存在群G的一个子群H，根据它的左陪集可以完成群的分解。
- 事实上，子群H的右陪集，也有对称的性质
- 但是，在许多情况下，群G的子群的左右陪集并不相等
- 思考：
  - 任意给定一个群G，它是否存在子群H，使得其左右陪集相等？
  - 子群$\{e\}$，子群G

8.6 正规子群与商群

定义8.6.1

- 设H是G的一个子群，如果对任意的$a \in G$，都有$aH = Ha$，则称H是G的一个正规子群（亦称不变子群），用符号$H \lhd G$表示。
- 因此，对正规子群H就不必区分其左右陪集，而简称为H的陪集

8.6 正规子群与商群

定理8.6.1

- 设H是G的子群，则以下几个条件等价：

1. $H \lhd G$
2. $\forall g \in G, gHg^{-1} = H$
3. $\forall g \in G, gHg^{-1} \subseteq H$
4. $\forall g \in G, h \in H, ghg^{-1} \in H$

8.6 正规子群与商群

证明：1. $H \lhd G$ ⟹ 2. $\forall g \in G, gHg^{-1} = H$

- 因为H为正规子群，因此$\forall g \in G, gH = Hg$
- 因此

$$gHg^{-1} = (gH)g^{-1} = (Hg)g^{-1} = H(gg^{-1}) = He = H$$

8.6 正规子群与商群

证明：2. $\forall g \in G, gHg^{-1} = H$ $\Rightarrow$

3. $\forall g \in G, gHg^{-1} \subseteq H$

- $\forall g \in G, \quad gHg^{-1} = H$

$\Downarrow$

- $\forall g \in G, \quad gHg^{-1} \subseteq H$

8.6 正规子群与商群

证明：3. $\forall g \in G, gHg^{-1} \subseteq H$ $\Longrightarrow$

4. $\forall g \in G, h \in H, ghg^{-1} \in H$

- $gHg^{-1} \subseteq H$

$$\Downarrow$$

- $\forall g \in G, h \in H, \quad ghg^{-1} \in H$

8.6 正规子群与商群

证明：4. $\forall g \in G, h \in H, ghg^{-1} \in H \Longrightarrow 1.\ H \lhd G$

- 求证 $\forall g \in G,\quad gH = Hg$
- 据已知条件，$\forall g \in G, \forall h \in H$，都有$ghg^{-1} = h_1 \in H$
- 即$gh = h_1 g \in Hg$。因此$\forall g \in G, gH \subseteq Hg$
- 反之（取$\forall g^{-1} \in G$ ），易证 $\forall g \in G, Hg \subseteq gH$
- 因此 $\forall g \in G,\quad gH = Hg$

8.6 正规子群与商群

定理8.6.1

- 设H是G的子群，则以下几个条件等价：

  1. $H \lhd G$
  2. $\forall g \in G, gHg^{-1} = H$
  3. $\forall g \in G, gHg^{-1} \subseteq H$
  4. $\forall g \in G, h \in H, ghg^{-1} \in H$

8.6 正规子群与商群

定理8.6.2

- 设A,B是G的两个子群

  1. 若$A \lhd G, B \lhd G$，则$A \cap B \lhd G, AB \lhd G$

  2. 若$A \lhd G, B \leq G$，则$A \cap B \lhd B, AB \leq G$

8.6 正规子群与商群

证明：1. 若$A \lhd G, B \lhd G$，则$A \cap B \lhd G, AB \lhd G$

- 首先证明$A \cap B$是G的子群
- $\forall h \in A \cap B \implies h \in A, h \in B$
- $\forall g \in G,\ ghg^{-1} \in A,\ ghg^{-1} \in B$
- $\forall g \in G, \forall h \in A \cap B, ghg^{-1} \in A \cap B \implies A \cap B \lhd G$
- 首先证明AB是G的子群
- $\forall h \in AB \implies h = ab, a \in A, b \in B$
- $\forall g \in G, ghg^{-1} = gabg^{-1} = gag^{-1}gbg^{-1} = a'b' \in AB$
- $AB \lhd G$

$H \lhd G$

4.$\forall g \in G, h \in H, ghg^{-1} \in H$

8.6 正规子群与商群

证明：2. 若$A \lhd G, B \le G$，则$A \cap B \lhd B, AB \le G$

- $\forall h \in A \cap B \Longrightarrow h \in A, h \in B$
- $\forall g \in B \Longrightarrow ghg^{-1} \in A$ ($A \lhd G$且$B \le G$, 性质4), $ghg^{-1} \in B$
- $\forall g \in B, \forall h \in A \cap B, ghg^{-1} \in A \cap B \Longrightarrow A \cap B \lhd B$

$H \lhd G$

4.$\forall g \in G, h \in H, ghg^{-1} \in H$

8.6 正规子群与商群

证明：2. 若$A \lhd G, B \leq G$，则$A \cap B \lhd B, AB \leq G$

- $e \in A, e \in B \Rightarrow e \in AB$ 单位元！
- $\forall ab, a_1b_1 \in AB$

$A \lhd G \Rightarrow bA = Ab \Rightarrow ba = a'b$

- $(ab)(a_1b_1) = a(ba_1)b_1 = a(a_1{'}b)b_1 = (aa_1{'})(bb_1) \in AB$ 封闭性！
- $\forall ab \in AB, (ab)^{-1} = b^{-1}a^{-1} = (a^{-1})'b^{-1} \in AB$ 逆元素！
- $AB \leq G$ 证毕！

8.6 正规子群与商群

定理8.6.2

- 设A, B是G的两个子群

1. 若$A \lhd G, B \lhd G$，则$A \cap B \lhd G, AB \lhd G$
2. 若$A \lhd G, B \leq G$，则$A \cap B \lhd B, AB \leq G$

正规子群的乘积仍然是正规子群！
正规子群的交集仍然是正规子群！

正规子群与普通子群的乘积是普通子群！
正规子群与普通子群的交集是普通子群的正规子群！

8.6 正规子群与商群

- 定理8.6.3:设H是G的一个正规子群，G/H表示H的所有陪集构成的集合，即

$$G/H = \{gH|g \in G\}$$

- 则G/H关于陪集乘法作成群。称之为G关于H的商群
- 例：$G = (Z,+), H = (\{km\},+), G/H = (Z_m,+)$

> - G是一个群，H是G的一个子群，利用H可以在G的元素之间确定一个二元关系R
>
> $$a R b \text{ 当且仅当 } ab^{-1} \in H$$
>
> R是G中的一个二元关系，是等价关系
>
> 因此由等价关系就可以确定G的一个划分，其划分块就是子群H的陪集

8.6 正规子群与商群

证明：

陪集乘法对于G/H是一个二元运算

- $\forall aH, bH \in G/H, aHbH = \{ah_1bh_2 | h_1, h_2 \in H\}$
- $bH = Hb \Longrightarrow ah_1bh_2 = a(h_1b)h_2 = a(bh_1{}')h_2 = (ab)(h_1{}'h_2) \in abH$
- 故$aHbH \subseteq abH$
- 又$\forall h \in H, (ab)h \in abH$，$(ab)h = (ae)(bh) \in aHbH$
- 故$abH \subseteq aHbH$

二元运算！

- 因此$\forall aH, bH \in G/H, aHbH = abH = G/H$

关于乘法是封闭的

8.6 正规子群与商群

证明（续）： G/H对陪集乘法成群

- $\forall aH, bH, cH \in G/H$ 结合律！
  $(aHbH)cH = (abH)cH = (ab)cH = a(bc)H$
  $= aH(bc)H = aH(bHcH)$
- $eHaH = eaH = aH, aHeH = aeH = aH \Rightarrow eH = H$是单位元 单位元！
- $a^{-1}HaH = aa^{-1}H = eH$，因此$aH$的逆元为$a^{-1}H$

逆元素！

证毕！

8.6 正规子群与商群

定理8.6.3

- 设H是G的一个正规子群，G/H表示H的所有陪集构成的集合，即

$$G/H = \{gH|g \in G\}$$

- 则G/H关于陪集乘法作成群。称之为G关于H的商群。

8.6 正规子群与商群

小结

- 正规子群
- 正规子群的等价性质
- 正规子群与子群的交、乘积性质
- 商群

主观题 10分

设置

设G是群，$H_1 \le G, H_2 \le G$。证明$H_1 H_2 \le G \Leftrightarrow H_1 H_2 = H_2 H_1$

正常使用主观题需2.0以上版本雨课堂

作答

解答

设G是群，$H_1 \le G, H_2 \le G$。证明$H_1H_2 \le G \Leftrightarrow H_1H_2 = H_2H_1$

$\Rightarrow$: $\forall ab \in H_1H_2$，由$H_1H_2 \le G$,有$(ab)^{-1} = a_1b_1 \in H_1H_2$，故$ab = (a_1b_1)^{-1} = b_1^{-1}a_1^{-1} \in H_2H_1$，因此$H_1H_2 \subseteq H_2H_1$. 同理可证$H_2H_1 \subseteq H_1H_2$，故$H_1H_2 = H_2H_1$.

$\Leftarrow$: $\forall a_1b_1, a_2b_2 \in H_1H_2, (a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1}$

由H_2是子群，可知$b_1b_2^{-1} = b_3 \in H_2$ 上式变为$a_1b_3a_2^{-1}$

由$H_2H_1 = H_1H_2$，可知存在a', b',使得$b_3a_2^{-1} = a'b'$，上式变为$a_1a'b'$

由H_1是子群，可知$a_1a' \in H_1$，故$(a_1b_1)(a_2b_2)^{-1} = a_1a'b' \in H_1H_2$

所以H_1H_2是子群

主观题　10分

设置

1）证明，有限半群一定存在$x \in S$，满足$x^2 = x$
2）给出一个反例，说明其在无限半群中不成立

作答

解答

1）证明，有限半群一定存在$x \in S$，满足$x^2 = x$
2）给出一个反例，说明其在无限半群中不成立

- 考察集合$\{a, a^2, a^3, \dots, a^{|S|}, a^{|S|+1}\}$，含有$|S|+1$个元素，故必有$1 \le i < j \le |S|+1$使得$a^i = a^j$
- 对于任意$k \ge i$,均有$a^k = a^i a^{k-i} = a^j a^{k-i} = a^{k+j-i}$，进而$a^k = a^{k+(j-i)} = a^{k+2(j-i)} = \cdots$
- 因此只需选择合适的$k \ge i$，使得$2k = k + n(j-i)$。例如，取$x = a^{|S|(j-i)}$，满足$|S|(j-i) \ge |S| \ge i$，因此有$x = a^{|S|(j-i)} = a^{|S|(j-i)+|S|(j-i)} = x^2$。

- $(\mathbb{N}^+, +)$是一个反例，该半群不存在$x + x = x$的元素

设置

设$G=\langle M_2(\mathbb{Z}),+\rangle$是整数集$\mathbb{Z}$上全体二阶方阵关于矩阵加法构成的群。$A=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d\text{均为偶数}\right\}$. 证明

1)$A \le G$ 2) A是否是G的正规子群？若是，写出G/A的全体元素，若不是请说明理由。

正常使用主观题需2.0以上版本雨课堂

作答

解答

设$G=\langle M_2(\mathbb{Z}),+\rangle$是整数集$\mathbb{Z}$上全体二阶方阵关于矩阵加法构成的群。$A=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d\text{均为偶数}\right\}$. 证明1)$A\leq G$ 2) A是否是G的正规子群？若是，写出G/A的全体元素，若不是请说明理由。

(1) $\forall X,Y\in A$，有$X_{11},X_{12},X_{21},X_{22},Y_{11},Y_{12},Y_{21},Y_{22}$是偶数，则$-X_{11}+Y_{11}$，$-X_{12}+Y_{12}$，$-X_{21}+Y_{21},-X_{22}+Y_{22}$均为偶数。故$-X+Y\in A$。因此$A$是$G$的子群。

(2)由于矩阵的加法满足交换律，G为交换群，因此A自然是G的正规子群。

G/A共有16个元素，分别为$\{\begin{pmatrix} x & y \\ z & w \end{pmatrix}A \mid x,y,z,w=0{,}1\}$。

主观题 10分

设置

设G是一个群。$x, y \in G$，我们把所有形如$xyx^{-1}y^{-1}$的元素称为换位子。群G的所有换位子生成的子群称为G的换位子群G'。证明1)$G' \lhd G$ 2) G/G'是交换群.

正常使用主观题需2.0以上版本雨课堂

作答

解答

设G是一个群。$x, y \in G$，我们把所有形如$xyx^{-1}y^{-1}$的元素称为换位子。群G的所有换位子生成的子群称为G的换位子群H。证明1)$H \lhd G$ 2) G/H是交换群.

(1) 要证正规性，即证$\forall g \in G, h \in H$,有$ghg^{-1} \in H$。而$ghg^{-1} = (ghg^{-1}h^{-1})h$，$(ghg^{-1}h^{-1}) \in H, h \in H$. 故$ghg^{-1} \in H$

(2) G/H中的元素是$\{gH|g \in G\}$。要证交换群即证$\forall a, b \in G$，$aHbH = bHaH$。由正规性知$aHbH = abH$，$bHaH = baH$，因此只需证明$abH = baH$。而$a^{-1}b^{-1}ab = h \in H$，即$ab = bah$，$abH = bahH = baH$，证毕

离散数学2：代数结构部分总结

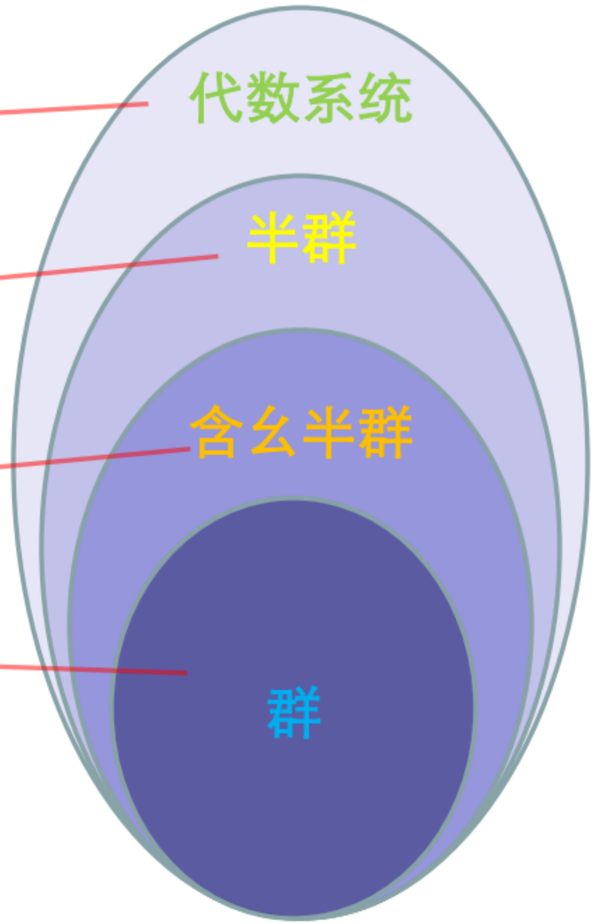
主要概念

非空集合+代数运算

非空集合+代数运算+结合律

非空集合+代数运算+结合律+单位元

非空集合+代数运算+结合律+单位元+逆元



群的定义

- 设G是非空集合，$\cdot$是G上的二元运算，若代数系统$(G,\cdot)$满足
  1. 适合结合律，即$\forall a,b,c \in G,$有$(ab)c = a(bc)$
  2. 存在单位元e，使得$\forall a \in G, ae = ea = a$
  3. G 中的元素都是可逆元。即 $\forall a \in G,$都$\exists a^{-1} \in G$，使得$aa^{-1} = a^{-1}a = e$
- 则称代数系统$(G,\cdot)$是一个群，或记为$(G,\cdot,e)$。
- 为了方便起见，常用G表示群$(G,\cdot,e)$

封结幺逆 → 凤姐咬你

半群

- 例： $(M_n(R),\times)$

  其中$M_n(R)$是全体$n\times n$实矩阵的集合

  $\forall A,B,C\in M_n(R)\qquad (A\times B)\times C=A\times(B\times C)$

  半群！　　幺群！

- 例：$(Z_m,\cdot)$

  设$Z_m=\{\overline{0},\overline{1},\cdots,\overline{m-1}\}$是模$m$同余的等价类集合，

$\cdot$是Z_m上的模m加法运算

半群！　　幺群！

半群

定义8.1.3

- 设$(M,\cdot,e)$是一个幺群，若$\cdot$适合交换律，则称M是交换幺群。

- 例：$(R,+)$

$$\forall a,b,c \in R \qquad (a+b)+c=a+(b+c)$$

$$\forall a \in R \qquad a+0=0+a=a$$

半群！ 幺群！ 交换幺群！

半群

- 例： $(M_n(R),\times)$

  其中$M_n(R)$是全体$n \times n$实矩阵的集合

  $\forall A, B, C \in M_n(R) \qquad (A \times B) \times C = A \times (B \times C)$

  半群！　　幺群！

- 例：$(Z_m,\cdot)$

  设$Z_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$是模$m$同余的等价类集合，

$\cdot$是Z_m上的模m加法运算

半群！　　幺群！　　交换幺群！

半群

定义8. 1. 4

- 设$(M,\cdot,e)$ 是一个幺群，若存在一个元素$g \in M$，使得任意的$a \in M$，a都可以写成g的方幂形式，即$a = g^m$（m是非负整数），则称$(M,\cdot,e)$ 是一个循环幺群，并且称g 是M的一个生成元。

半群

- 例： $(R,+)$

$$\forall a,b,c \in R \qquad (a+b)+c = a+(b+c)$$

$$\forall a \in R \qquad a+0 = 0+a = a$$

半群！ 幺群！ 交换幺群！ 循环幺群？ ×

- 例： $(N,+)$

循环幺群？ √

群的性质

性质1 设$(G, \cdot)$为群，则$\forall a \in G$，a的左逆元也是a的右逆元.

性质2 设$(G, \cdot)$为群，则G的左单位元e也是右单位元.

性质3 设$(G, \cdot)$为群，则$\forall a,b \in G$，方程$a \cdot x=b$和$y \cdot a=b$在G中的解唯一.

群的性质

性质4 设$(G, \cdot)$为群，则

(1) $\forall a \in G$，$(a^{-1})^{-1}=a$;

(2) $\forall a,b \in G$，$(a \cdot b)^{-1}=b^{-1} \cdot a^{-1}$.

性质5 群$(G, \cdot)$中的乘法满足消去律，即$\forall a,b,c \in G$ 有

(1) 若 $a \cdot b = a \cdot c$，则 $b = c$(左消去律)

(2) 若 $b \cdot a = c \cdot a$，则 $b = c$(右消去律)

群的性质

性质6 设G 为群，则G中的幂运算满足：

(1) $\forall a \in G$，$a^n a^m = a^{n+m}$，$n, m \in Z$

(2) $\forall a \in G$，$(a^n)^m = a^{nm}$，$n, m \in Z$

(3) 若G为交换群，则 $(ab)^n = a^n b^n$.

性质7 G为群，$a \in G$且 $|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当$r \mid k$.

(2) $O < a^{-1} > = O < a >$.

满足子群的条件

封闭性、单位元、逆元素

非空的

群、群的基本性质

定理8.2.6

- H是G的子群的充要条件是：
  1. H对G的乘法运算是封闭的，即$\forall a, b \in H$，都有$ab \in H$
  2. H中有单位元e'，且$e' = e$
  3. $\forall a \in H$，都有$a^{-1} \in H$，且a^{-1}是a在G中的逆元

群、群的基本性质

定理8.2.7

- G的非空子集H是G的子群的充要条件是$\forall a,b \in H$，都有$ab^{-1} \in H$

群、群的基本性质

例

- 设H_1, H_2是G的两个子群，则$H = H_1 \cap H_2$也是G的子群。

- 证明：
  - G单位元$e \in H_1, H_2$，所以$e \in H$，即H非空。
  - 任设$a, b \in H$，则$a, b \in H_1$， $a, b \in H_2$，由定理8.2.7有 $ab^{-1} \in H_1$，$ab^{-1} \in H_2$，因此$ab^{-1} \in H$，
  - 所以H是G的子群。

8.3 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

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

- 则称G是循环群，记作$G=\langle a\rangle$，a称为G的生成元。

由一个元素生成的群

8.3 循环群 群的同构

- 思考：
  - 循环群和循环幺群的区别是什么？
  - 例：

$$(N, +)$$

$$(Z_m, \cdot) \quad Z_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$$

8.3 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$|a|=n$，也可记为$O(a)$，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

关于循环群的一个结论

- 所有的循环群都同构于(Z,+)或$(Z_n, +)$

- 当$o(a)$=∞时， $G \cong$ (Z,+)无限循环群
- 当$o(a)$=n时， $G \cong (Z_n, +)$ n阶循环群

8.3 循环群 群的同构

- 思考：
  - 循环群的生成元有几个？
  - 例：

$(Z, +)$ $\qquad 1, \ -1$

$(Z_6, \ \bullet)$ $\qquad Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

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

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

8.3 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。

8.3 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$|H| = n/k$。

8.3 循环群 群的同构

定义8.3.2

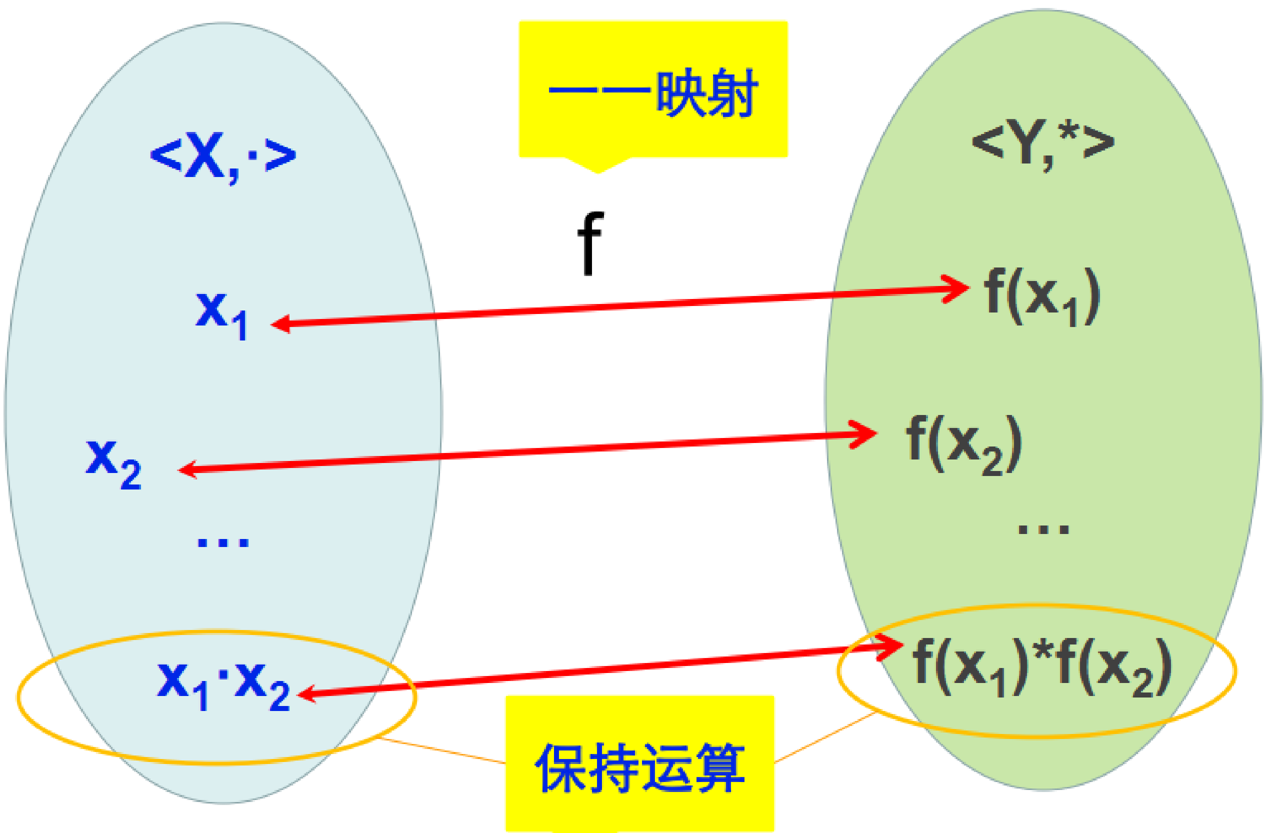
- 设$(G,\cdot)$和$(G',*)$是两个群，

  $f: G \to G'$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！

8.3 循环群 群的同构

同构示意图



8.3 循环群 群的同构

例：

- 设$G=(R^{+},\times),G'=(R,+)$，令$f: x\rightarrow lnx$

  则f是从G到G'的一个双射，且$\forall x,y\in G$

  $f(x\times y)=\ln(xy)=lnx+lny=f(x)+f(y)$

  因此，$G\cong G'$

8.3 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$(\mathrm{Z}, +)$同构
- 2. 若$O\langle a\rangle = n$，则G与$(Z_n, +)$同构

8.3 循环群 群的同构

定理8.3.5

- 设G是一个群，$(G',*)$是一个代数系统，如存在G到G'的双射f，且保持运算，即$\forall a, b \in G$，有
$$f(ab) = f(a) * f(b)$$
则G'也是一个群。

依据同构映射，可以做群的判定！

8.4 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

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

- 其中，恒等变换记为I

8.4 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。

8.4 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：

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

- 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
  - $fI = If = f$

8.4 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

8.4 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 一个集合A的一一变换所组成的群
  置换群 一个有限集合A的一一变换所组成的群

8.4 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

8.4 变换群和置换群 Cayley定理

- 例
  - $A=\{1,2,3\}$，则$S_3=\{\sigma_1,\sigma_2,\cdots,\sigma_6\}$，其中

$$\sigma_1=\begin{bmatrix}1&2&3\\1&2&3\end{bmatrix},\ \sigma_2=\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix},\ \sigma_3=\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix},$$

$$\sigma_4=\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix},\sigma_5=\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix},\ \sigma_6=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix},$$

  - 计算置换乘法$\sigma_2\sigma_4$： $i\rightarrow\sigma_2(\sigma_4(i))$
  - $\sigma_2\big(\sigma_4(1)\big)=\sigma_2(2)=3,\cdots$

$$\sigma_2\sigma_4=\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}=\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$$

8.4 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。

8.4 变换群和置换群 Cayley定理

- 对于一个置换σ，如果满足

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_l) = i_1$$

- 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

8.4 变换群和置换群 Cayley定理

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

$$\begin{cases}\sigma(1)=4\\\sigma(4)=6\\\sigma(6)=2\\\sigma(2)=1\end{cases} \Rightarrow (4,6,2,1) \qquad \begin{cases}\sigma(3)=7\\\sigma(7)=3\end{cases} \Rightarrow (7,3) \qquad [\sigma(5)=5 \Rightarrow (5)$$

  - 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

$$(4,6,2,1)(7,3)$$

8.4 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$\alpha\beta = \beta\alpha$。

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

- 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

8.4 变换群和置换群 Cayley定理

例

- S_4的全部置换可用轮换及其乘积表示为：
- 1. 都不变 : $e = (i)$
- 2. 两个元素变 : $(1\ 2), (3, 4), (1\ 3), (2\ 4), (1\ 4), (2\ 3)$
- 3. 三个元素变 : $(1\ 2\ 3), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 3),$
  $(1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3)$
- 4. 四个元素变： $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4),$
  $(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$
- 5. 四个元素变： $(12)(34), (13)(24), (14)(23)$

8.4 变换群和置换群 Cayley定理

引理8.4.1

- 设$\sigma=(i_1,i_2,\cdots,i_k)$是$S_n$上的$k$阶轮换，$k>1$，则

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

- 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：

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

8.4 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？

8.4 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

8.4 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$\sigma$的对换表示中，对换个数的奇偶性与排列$\pi = i_1 i_2 \cdots i_n$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。

8.4 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$|A_n| = \frac{1}{2}n!$

8.4 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

- 任何一个群G，都与一个变换群同构

推论：

- 设G是n阶有限群，则G与S_n的一个子群同构。
- 任何一个有限群G，都与一个置换群同构

8.5 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

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

- 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

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

思考：左陪集和右陪集是否相等？

8.5 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

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

有限群中，子群的阶只能是群的阶的因子！

8.5 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中任意元素的阶都是n的因子，且适合$x^n = e$。
- 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

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

利用Lagrange定理可以确定一个群内的可能存在的子群、元素的阶等，从而搞清一个群的结构
根据$|G|$的因子来确定可能存在子群的阶数或元素的阶数

8.6 正规子群与商群

定义8.6.1

- 设H是G的一个子群，如果对任意的$a \in G$，都有$aH = Ha$，则称H是G的一个正规子群（亦称不变子群），用符号$H \lhd G$表示。
- 因此，对正规子群H就不必区分其左右陪集，而简称为H的陪集

8.6 正规子群与商群

定理8.6.1

- 设H是G的子群，则以下几个条件等价：

  1. $H \lhd G$
  2. $\forall g \in G, gHg^{-1} = H$
  3. $\forall g \in G, gHg^{-1} \subseteq H$
  4. $\forall g \in G, h \in H, ghg^{-1} \in H$

定理8.6.2

- 设A, B是G的子群，则：

  1. $A \lhd G$，$B \lhd G$，则$A \cap B \lhd G$，$AB \lhd G$
  2. $A \lhd G$，$B \le G$，则$A \cap B \lhd B$，$AB \le G$

谢谢

shixia@tsinghua.edu.cn