第八章 群

刘世霞
shixia@tsinghua.edu.cn

主观题 10分

Setting

上节课有什么疑问吗？欢迎投稿。

Open Question is only supported on Version 2.0 or newer.

Answer

主观题 10分

Setting

为什么代数结构这部分的定义的代数结构、半群和群等概念均要求集合是非空的？欢迎投稿。

Open Question is only supported on Version 2.0 or newer.

Answer

习题课说明

- 图论部分
  - 时间：6月4日（本周日）第五大节
  - 地点：五教5105

- 代数结构部分
  - 时间：6月9日（下周五）第二大节
  - 地点：三教2101(随堂进行)

上次作业分析

- 整体完成情况较好，有两道证明题需要注意

15. 已知代数系统$(S,*)$和$(P,\cdot)$，其中 $S=\{a,b,c\}$，$P=\{1,2,3\}$，二元运算分别定义为：

•	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

•	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

试证它们是同构的。

- 证明代数系统$(S,*)$和$(P,\cdot)$同构，除了构造双射函数$f:S\rightarrow P$外，还需要验证**其保持运算，即$f(x*y)=f(x)\cdot f(y)$**

上次作业分析

2. 设$(S,\cdot)$是半群，证明$S\times S$对于下面规定的结合法·作成一个半群

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1\cdot b_1,a_2\cdot b_2),$$

当S有单位元时，$S\times S$也有单位元。

- 证明(e,e)是$S\times S$单位元时，需要同时验证(e,e)同时为左右单位元，即$\forall a,b\in S$，$(e,e)(a,b)=(a,b)$和$(a,b)(e,e)=(a,b)$

内容回顾：群的定义

封结幺逆

定义8.2.1

- 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$(G,\cdot,e)$

内容回顾：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.

内容回顾：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)

内容回顾：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 $\boldsymbol{G}$**为群，**$\boldsymbol{a\in G}$**且** $\boldsymbol{|a| = r}$**. 设**$\boldsymbol{k}$**是整数，则**

(1) $\boldsymbol{a^k = e}$**当且仅当**$\boldsymbol{r \mid k}$ **.**

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

内容回顾：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

内容回顾：满足子群的条件

封闭性、单位元、逆元素

非空的

封幺逆

内容回顾：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$ab^{-1} \in H$

Setting

关于群的元素的阶，下列说法正确的是

A 有限群的元素的阶都是有限的

B 所有元素的阶都是有限的群必为有限群

C 存在无限群，其元素的阶都是有限的

D 存在无限群，其元素的阶都是无限的

Submit

解答

- A: 有限群的元素的阶都是有限的
- B: 所有元素的阶都是有限的群必为有限群
- C: 存在无限群，其元素的阶都是有限的
- D: 存在无限群，其元素的阶都是无限的

解答

- A 正确，否则无限阶元的若干次幂就构成了一个无限集合
- B 错误 C正确，如($P(M)$,$\oplus$) ：除单位元外所有元素阶均为2的群
- D 错误，单位元的阶只能为1

内容回顾：循环群定义

- 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

内容回顾：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

内容回顾：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。

循环群中，若某元素的幂次与n互素，则可以作为另一生成元！

8.3 循环群 群的同构

定理8.3.1 若$o\langle a\rangle=\infty$，则G中只有生成元a或a^{-1}

- 证明：
  - 当$o\langle a\rangle=\infty$时，显然a是生成元。同时，$\forall a^k\in G$，$a^k=(a^{-1})^{-k}$，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$a=b^t=(a^j)^t=a^{jt}$，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$j=t=-1$

内容回顾：定理8. 3. 1

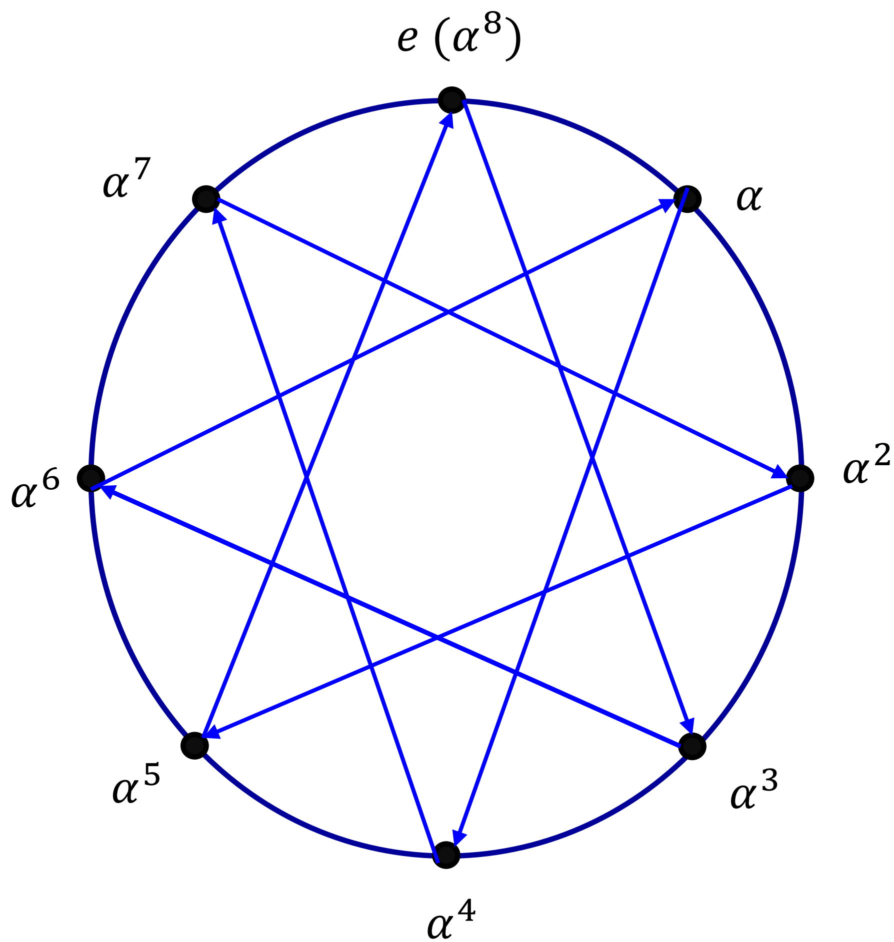
定理8. 3. 1 若$o\langle a\rangle = n$，则G中有$\varphi(n)$个生成元

- 证明（续）：
  - 当$o\langle a\rangle = n$时，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$rp - 1 = qn$　　裴蜀定理
  - 即$(r, n) = 1$　　证毕！

裴蜀定理：a, b互质的充分必要条件是存在整数x, y使ax+by=1

循环群中，若某元素的幂次与n互素，则可以作为另一生成元！

内容回顾：举例



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 循环群和群的同构:循环群的子群性质

- 思考:

循环群G的子群H是否仍然是循环群? YES!

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是最小值

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$a^{k_m}=a^{r+l\cdot k_1}=a^r a^{l\cdot k_1}$ ⟹ $a^r=a^{k_m}(a^{l\cdot k_1})^{-1}$ ⟹ $a^r\in H$

$r=0$

最小次幂是生成元

8.3 循环群和群的同构:循环群的子群性质

- 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$(a^k)^q = e$，将说明a为有限阶元，矛盾!

  – 若G为无限循环群，则其非平凡子群也为无限循环群!

8.3 循环群和群的同构:循环群的子群性质

- 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

    由于$(a^{k_1})^n = (a^n)^{k_1} = (e)^{k_1} = e$（定理8.2.5）

    则必定有$d|n$

  – 若G为n阶循环群，则其子群生成元阶数为n 因数！

定理8.2.5 设a是群G中的一个r阶元素，k是正整数，则

1. $a^k = e$，当且仅当 $r|k$

8.3 循环群和群的同构

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

定理8.3.2

- 证明：

  1. G的子群H都是循环群

  - H是G子群，则H中的元素可以表示成a的方幂的形式
  - 设a^k是H中a的最小正幂，任取$a^s \in H, s = pk + r(0 \le r < k)$,所以$a^r = a^{s-pk} = a^s a^{-pk} = a^s(a^k)^{-p} \in H$
  - a^k是最小正幂，故$r = 0$，即$a^s = (a^k)^p$，故$H = \langle a^k \rangle$

8.3 循环群 群的同构

定理8.3.2

- 证明：

  2. 若G是无限群，则$H(H \neq \{e\})$也是无限循环群
     - 反证法
     - 设$a^k(k \neq 0)$是H的一个生成元，且a^k是n阶元
     - $(a^k)^n = e$，即$a^{kn} = e$，与a是无限阶元矛盾
     - a^k是无限阶元
     - H是无限阶循环群

8.3 循环群 群的同构

定理8.3.2

- 证明：

  3. $|G| = n$, 且a^k是H中的a的最小正幂，则$|H| = n/k$

     - $O\langle a\rangle = n$，即$a^n = e$
     - a^k是循环群H中a的最小正幂（即$H = \langle a^k\rangle$）
     - 存在最小正整数m，使$(a^k)^m = e = a^n$，即$km = n$
     - a^k的阶$m = n/k$，即$|H| = n/k$。

8.3 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？

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$H=\langle a^{\frac{n}{d}}\rangle$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。

  显然，$a^{md}=(a^m)^d=e$，则有$n|md \Longrightarrow \frac{n}{d}|m$

  令$m=\frac{n}{d}\cdot t(t\in Z)$　则有：

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

  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$H_1=H$。

n阶循环群，n的因子有几个，子群就有几个！

多选题 1分

Setting

群$(Z_{14},+)$的子群为

A Z_{14}

B $\langle\overline{2}\rangle$

C $\langle\overline{7}\rangle$

D $\langle\overline{0}\rangle$

- 剩余类加群$(Z_{14},+)$中14的正因子有1,2,7,14，因此Z_{14}有4个子群：它自身，单位元群$\langle\overline{0}\rangle$, 以及$\langle\overline{2}\rangle$, $\langle\overline{7}\rangle$，其中$O\langle\overline{2}\rangle = 7, O\langle\overline{7}\rangle = 2$

Submit

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

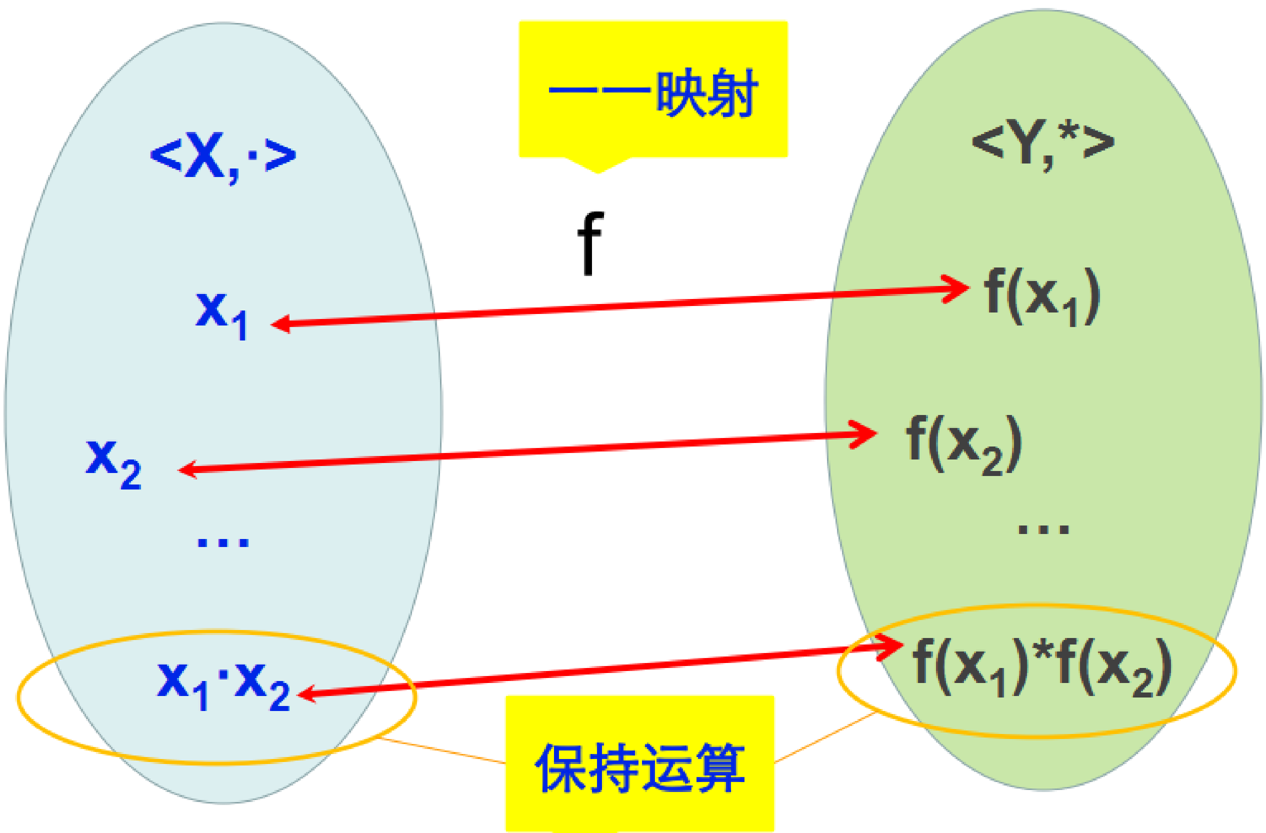
$$f(ab) = f(a) * f(b)$$

- 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$f: x \to lnx$

  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

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

8.3 循环群 群的同构

定理8.3.4

- 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$x=a^m,y=a^n$
    $f(xy)=f(a^m a^n)=f(a^{m+n})=m+n$
    $=f(x)+f(y)$
  - 因此f是G到Z的一个同构映射
  - $G\cong Z$

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

- 证明 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！
- 群G到Z_n的映射关系$f: a^k \to \overline{k}(0 \le k < n)$
- 考察$\forall x, y \in G$，其中$x = a^{m_1}, y = a^{m_2}(0 \le m_1 \le m_2 < n)$
- $f(xy) = f(a^{m_1}a^{m_2}) = f(a^{m_1+m_2}) = f\left(a^{(m_1+m_2) mod\, n}\right) = (m_1 + m_2) mod\, n = f(x) + f(y)$
- 因此，f是G到Z_n的一个同构映射！
- $G \cong Z_n$ 证毕！

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

任何两个阶相同的循环群同构！

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！

8.3 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

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

三维空间中有多少种正多面体

- 我们的证明方式是利用欧拉公式:

$$v+f-e=2$$

- 假设每个面的边数为n，每个顶点发射的边数为m:

$$\frac{vm}{2}=\frac{fn}{2}=e$$

- 因此带入v=2e/m以及f=2e/n，我们有:

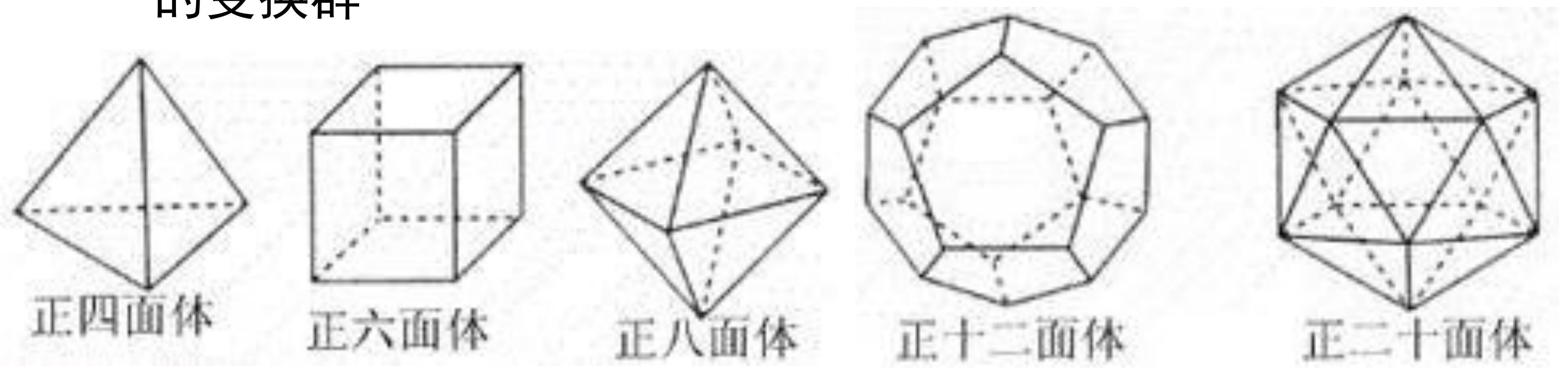
$$\frac{1}{n}+\frac{1}{m}=\frac{1}{2}+\frac{1}{e}>\frac{1}{2}$$

- 其中m,n>2，且为正整数

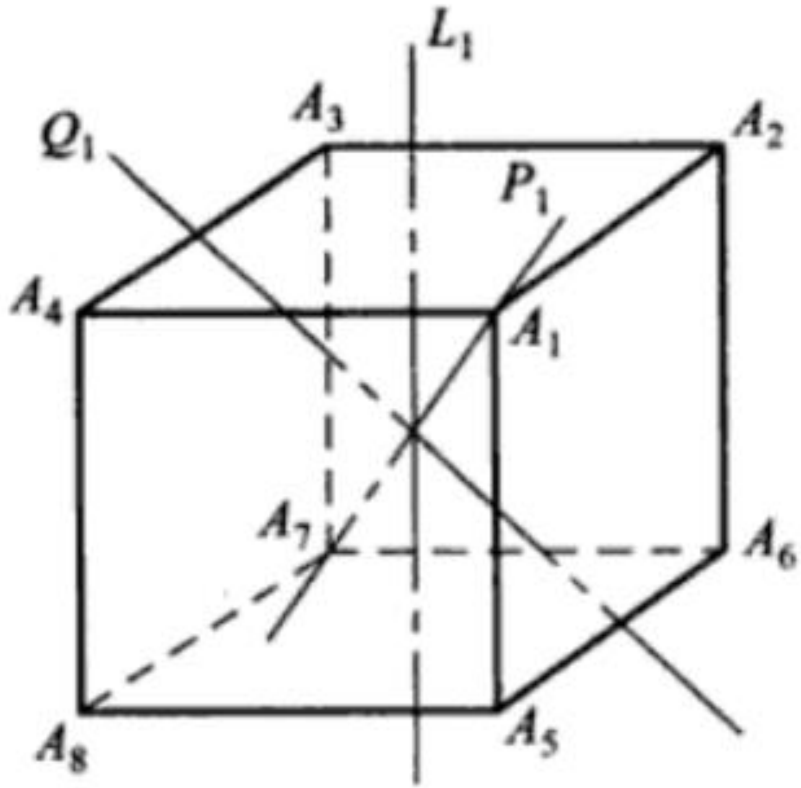
三维空间中有多少种正多面体

$$\frac{1}{n}+\frac{1}{m}=\frac{1}{2}+\frac{1}{e}>\frac{1}{2}$$

- 该方程解有限：(3, 3)，(3, 4)，(4, 3)，(3, 5)，(5, 3)
- 因此只有五种正多面体
- 在本节课中，我们将会学到正多面体的旋转群都是三维旋转群SO3的子群
- SO3是将三维物体绕一定旋转轴旋转一定角度的变换组成的变换群

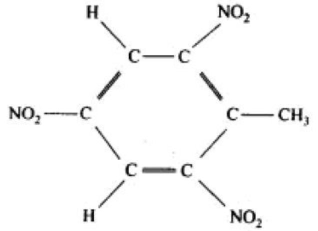


旋转



变换群的实际应用

- 排列组合里面的计数问题
  - 使用两种颜色的珠子串成含有五个珠子的项链，旋转72度或翻转后对应的是同一个项链，问一共有多少种不同的项链
  - 苯环上的碳原子可连接H、$\mathrm{CH_3}$或NO_2，问可形成多少种不同的物质



(TNT)

  - 求包含四个顶点且不同构的无向图个数

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

- 思考：

  变换有什么特点？

  – 定义域和值域为同一个集合

  – 如果变换是满射，则一定是单射吗？是双射吗？

有限集合上的变换，如果变换是满射，则一定是单射，也是是双射；无限集合上则不一定

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（了解）。
- S_n的子群称为n元置换群。

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

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

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

  - 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)

8.4 变换群和置换群 Cayley定理

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

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

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

  - 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

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

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

例

- $\alpha = (1\ 3\ 6), \beta = (2\ 5)$, 不相交
- 对于$\beta(i) = i, \alpha\beta(i) = \alpha(i), \beta\alpha(i) = \alpha(i)$
- 对于$\alpha(i) = i, \alpha\beta(i) = \beta(i), \beta\alpha(i) = \beta(i)$
- 对任意$i, \alpha\beta(i) = \beta\alpha(i), \alpha\beta = \beta\alpha$

8.4 变换群和置换群 Cayley定理

- 思考：

  置换群和轮换的关系？

  – 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？

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

$$\sigma=(i_2\ \ i_3)(i_3\ \ i_4)\cdots(i_{k-1}\ \ i_k)\ \ (i_1\ \ i_k)$$

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

- 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。

多选题 1分

设置

下面描述正确的

A 任意两个偶置换的乘积仍然是偶置换

B 任意两个奇置换的乘积是偶置换

C 任意两个奇置换的乘积是奇置换

D 一个奇置换和一个偶置换的乘积是奇置换

提交

8.4 变换群和置换群 Cayley定理

定理8.4.3

- n次交换群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8.4.3

- 证明：
  - S_n是有限群，任意两个偶置换的乘积仍然是偶置换
  - 由定理8.2.7得S_n中所有偶置换构成S_n的一个子群
  - 偶置换数n_1，奇置换数n_2
  - 某奇置换去乘不同偶置换，得到互异奇置换，$n_1 \le n_2$
  - 某奇置换去乘不同奇置换，得到互异偶置换，$n_1 \ge n_2$
  - $n_1 = n_2, A_n = \frac{1}{2}n!$

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$ab^{-1} \in H$

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。

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$(G,\cdot) \cong (\overline{G},\circ)$

一一变换？

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

定理8.4.4（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（有解）、单射（唯一解）⟶f_a是双射。

  – 以下证明$\overline{G} = \{f_a | a \in G\}$关于变换乘法成群

定理8.2.3：设$(G,\cdot)$是半群，如果对G中任意两个元素a, b，方程$ax = b$和$ya = b$在G中都有解，则G是一个群。

8.4 变换群和置换群 Cayley定理

定理8.4.4（Cayley定理）

- 证明（续）：证$\overline{G}=\{f_a|a\in G\}$关于变换乘法成群
  - $\forall f_a,f_b\in\overline{G},(f_af_b)(x)=f_a\big(f_b(x)\big)=f_a(bx)=abx=f_{ab(x)}$

封闭性 – $\forall f_a,f_b\in\overline{G}\ \Leftrightarrow a,b\in G\Longrightarrow ab\in G\Longrightarrow f_{ab}\in\overline{G}$

结合律 – 结合律自证

单位元 – $f_e: x\to ex$，是变换中的单位元

逆元素 – 由于f_a是一一变换，因此必定存在逆元素

$f_a{}^{-1}: x\to a^{-1}x \qquad f_a{}^{-1}=f_{a^{-1}}$

因此 $\overline{G}$ 关于变换乘法成群，即它是一个变换群！

8.4 变换群和置换群 Cayley定理

定理8.4.4（Cayley定理）

- 证明（续）：证G和$\overline{G}$同构
  - 构造映射关系$\varphi: a \rightarrow f_a$

单射 – $\forall a, b, x \in G, a \neq b \Longrightarrow ax \neq bx \Longrightarrow f_a \neq f_b \Longrightarrow \varphi(a) \neq \varphi(b)$

满射 – $\forall f_a \in \overline{G}$，一定存在$a \in G$，使得$\varphi(a) = f_a$

保持运算 – $\varphi(ab) = f_{ab} = f_a f_b = \varphi(a)\varphi(b)$

  - 因此，$G \cong \overline{G}$　　　　证毕！

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

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

- 小结：
  - 变换、一一变换
  - 一一变换群、变换群、对称群、置换群
  - 置换：轮换、对换、恒等变换
  - 逆序、逆序数、置换的逆序性质
  - Cayley定理

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

$$aRb \text{ 当且仅当 } ab^{-1}\in H$$

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

8.5 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？

单选题 1分

设置

判断题：左陪集和右陪集是否相等

A 相等

B 不相等

C 不一定

D 不确定

提交

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)},　　(1 3)(1 2)= (3 1 2)

(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)},

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

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

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$|aH| = |H|$

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$xh = (ah_1)h = a(h_1h) = ah'$，其中$h' \in H$

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

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

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！

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$A = \cup\, aD$，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$|AB| = |\bigcup_{a\in A} aB| = |S_1||B| = k|B|$，
 – 两式合并，即得$|AB| = \frac{|A||B|}{|A\cap B|}$ 证毕！

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

8.5 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

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

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

$$\Downarrow$$

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

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$A \cap B \lhd G, AB \lhd G$

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

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$A \cap B \lhd B, AB \leq G$

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

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！ 结合律！
- $\forall ab, a_1 b_1 \in AB$ $\boxed{A \lhd G \Rightarrow bA = Ab \Rightarrow ba = a'b}$
- $(ab)(a_1 b_1) = a(ba_1)b_1 = a(a_1{}'b)b_1 = (aa_1{}')(bb_1) \in AB$ 封闭性！
- $\forall ab \in AB, (ab)^{-1} = b^{-1}a^{-1} = (a^{-1})'b^{-1} \in AB$
- $AB \leq G$ 证毕！ 逆元素！

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

$\boxed{\text{陪集乘法对于}G/H\text{是一个二元运算}}$

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

$\boxed{G/H\text{对陪集乘法成群}}$

- $\forall aH, bH, cH \in G/H$

  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

谢谢

shixia@tsinghua.edu.cn