第八章 群

刘世霞
shixia@tsinghua.edu.cn

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. $H = eH, a \in aH$。

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$|aH| = |H|$

2. $|aH| = |H|$。

H的任意一个左陪集，其元素个数与H相同

3. $a \in H \Leftrightarrow aH = H$。

$\Rightarrow$: 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

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

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)},

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

显然一般情况下

$$aH \neq Ha$$

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

8.7 群的同态、同态基本定理

定义8.7.1

- 设G_1, G_2是两个群，f是G_1到G_2的一个映射。如果对任意的$a, b \in G_1$都有

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

- 则称f是G_1到G_2的一个同态映射，或简称同态。

8.7 群的同态、同态基本定理

- 若映射f分别是单射、满射、双射时，分别称之为G_1到G_2的单一同态、满同态、同构
- 用$G_1 \sim G_2$表示满同态，并称G_2是f作用下G_1的同态象

8.7 群的同态、同态基本定理

引理8.7.1

- 设H是G的正规子群，$\forall a \in G$令 $f: a \to aH$，则f是G到G/H的满同态。
- 证明：
  - 显然，f是G到G/H的一个映射
  - 同时，$\forall aH \in G/H$，总是$\exists a \in G$, 满足$f(a) = aH$
  - 因此f是G到G/H的一个满射

8.7 群的同态、同态基本定理

引理8.7.1

- 设H是G的正规子群，$\forall a \in G$令 $f: a \to aH$，则f是G到G/H的满同态。
- 证明（续）：
  - 由于$\forall a, b \in G, f(ab) = abH$
  - 且群G/H中的运算满足$aHbH = abH$（定理8.6.3）
  - 故$f(ab) = abH = aHbH = f(a)f(b)$ 保持运算！
  - 因此f是G到G/H的满同态

8.7 群的同态、同态基本定理

引理8.7.1

- 设H是G的正规子群，$\forall a \in G$令 $f: a \to aH$，则f是G到G/H的满同态。

8.7 群的同态、同态基本定理

定理8.7.1

- 若f是G_1到G_2的同态，g是G_2到G_3的同态，则gf是G_1到G_3的同态。
- 证明：显然gf是G_1到G_3的映射，以下只证明它保持运算，对任意$a, b \in G_1$

$$gf(ab) = g\big(f(ab)\big) = g\big(f(a)f(b)\big)$$
$$= g\big(f(a)\big)g\big(f(b)\big) = gf(a)gf(b)$$

- 因此gf是G_1到G_3的同态。

8.7 群的同态、同态基本定理

定理8.7.2

- 设G是一个群，$(G',\cdot)$是一个有二元运算的代数系统，若$f: G \to G'$是满射，且保持运算，则G'也是群，而且$G \sim G'$

群的同态象，仍然是群！

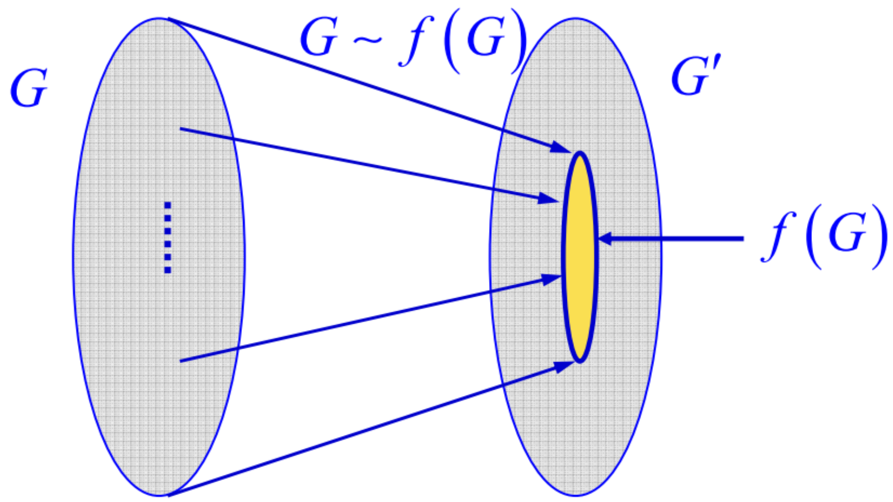
$G = (Z,+), G' = (Z_n,+), f(a) = a\ (mod)\ n$

8.7 群的同态、同态基本定理

引理8.7.2

- 设f是G到G'的同态，则G的象集$f(G)$是群G'的子群！

且f是G到$f(G)$的满同态



8.7 群的同态、同态基本定理

定理8.7.3

- 设f是G到G'的同态，则
  1. 若e和e'分别是G和G'的单位元，则$f(e)=e'$
  2. $\forall a\in G$，f将a的逆元映射到G'中的逆元，即 $f(a^{-1})=f^{-1}(a)$
  3. 如果H是G的子群，则H在f下的象$f(H)=\{f(a)|a\in H\}$是G'的子群，且$H\sim f(H)$

8.7 群的同态、同态基本定理

证明： 1.若e和e'分别是G和G'的单位元 $\Rightarrow$ $f(e)=e'$

- $f: G \sim f(G) \quad \forall a, b \in G, f(ab)=f(a)f(b)$
- $\forall a' \in f(G)$, 由于f为满射，因此必定$\exists a \in G$使得$f(a)=a'$
- 因此，$a'f(e)=f(a)f(e)=f(ae)=f(a)=a'$
- 同理，$f(e)a'=a'$。因此$f(e)$是$f(G)$中单位元
- 因为单位元唯一，故$f(e)=e'$

8.7 群的同态、同态基本定理

证明： 2. $\forall a \in G, f(a^{-1}) = f^{-1}(a)$

- $\forall a \in G$, 有$a^{-1} \in G$
- 因此，$f(aa^{-1}) = f(e) = e' = f(a)f(a^{-1})$
- 同理，$f(a^{-1}a) = f(e) = e' = f(a^{-1})f(a)$
- 故$f^{-1}(a) = f(a^{-1})$

8.7 群的同态、同态基本定理

证明： 3. $H \le G \Rightarrow f(H) \le G'$, 且$H \sim f(H)$

- $\forall a, b \in f(H)$，由于f为满射，因此必定存在$a', b' \in H$，使得$f(a') = a, f(b') = b$。
- 则$ab = f(a')f(b') = f(a'b') \in f(H)$ 封闭性！
- $e \in H \Rightarrow f(e) \in f(H)$ 单位元！

如果H是G的子群，则H在f下的象$f(H) = \{f(a) | a \in H\}$是$G'$的子群，且$H \sim f(H)$

8.7 群的同态、同态基本定理

证明： 3. $H \le G \Rightarrow f(H) \le G'$, 且$H \sim f(H)$

- $\forall a \in f(H)$，由于f为满射，因此必定$\exists a' \in H$, 使得$f(a') = a$
- 显然$(a')^{-1} \in H$，则$f((a')^{-1}) \in f(H)$
- $f\big((a')^{-1}\big)a = f\big((a')^{-1}\big)f(a') = f\big((a')^{-1}(a')\big) = f(e) = e'$
- 同理，$af\big((a')^{-1}\big) = e'$ 逆元素！
- 即$\forall a \in f(H)$，在$f(H)$中有逆元素

如果H是G的子群，则H在f下的象$f(H) = \{f(a)|a \in H\}$是G'的子群，且$H \sim f(H)$

8.7 群的同态、同态基本定理

证明： 3. $H \le G \Longrightarrow f(H) \le G'$，且$H \sim f(H)$

- $\forall a \in f(H)$，根据$f(H)$的定义，必定存在$a' \in H$，使得$f(a') = a$

满射！

- 说明f是从H到$f(H)$的满射！
- $\forall a, b \in H$，因为f是同态，所以

$$f(ab) = f(a)f(b) \in f(H)$$

保持运算！

- 故$H \sim f(H)$

如果H是G的子群，则H在f下的象$f(H) = \{f(a) | a \in H\}$是$G'$的子群，且$H \sim f(H)$

8.7 群的同态、同态基本定理

定理8.7.3

- 设f是G到G'的同态，则

1. 若e和e'分别是G和G'的单位元，则$f(e) = e'$

在同态映射下，单位元的象仍然是单位元

2. $\forall a \in G$，f将a的逆元映射到G'中的逆元，即

$f(a^{-1}) = f^{-1}(a)$ 在同态映射下，逆元素的象是象的逆元素

3. 如果H是G的子群，则H在f下的象$f(H) =$

$\{f(a)|a \in H\}$是G'的子群，且$H \sim f(H)$

在同态映射下，子群的象仍然是子群，且该同态映射形成二者之间的满同态

8.7 群的同态、同态基本定理

定理8.7.5

- 设f是G到G'的同态，e是G的单位元，令$K=\{a\in G|f(a)=f(e)\}$，则K是G的正规子群，K称为同态f的**核**，记作$Ker\ f$

$$G=(Z,+),G'=(Z_n,+),f(a)=a\ (mod)\ n$$
$$\mathrm{Ker}\ f=nZ=\{nk|k\in Z\}\lhd G$$

8.7 群的同态、同态基本定理

证明：

- 显然，e为K中的元素
- 由于f是同态，因此$f(e)=e'$是G'的单位元
- $\forall k,k_1\in K, f(kk_1)=f(k)f(k_1)=f(e)f(e)=e'=f(e)$
- $\forall k\in K, f(k^{-1})=f^{-1}(k)=f^{-1}(e)=e'=f(e) \Longrightarrow k^{-1}\in K$
- 因此，K为G的子群。

设f是G到G'的同态，e是G的单位元，令$K=\{a\in G|f(a)=f(e)\}$，则K是G的正规子群，K称为同态f的核，记作$Ker\ f$

8.7 群的同态、同态基本定理

证明：

- $\forall g \in G, \forall k \in K$
- $f(g^{-1}kg) = f(g^{-1})f(k)f(g) = f^{-1}(g)f(k)f(g) = f^{-1}(g)f(g) = e' = f(e)$
- 即$\forall g \in G, \forall k \in K, g^{-1}kg \in K$
- 因此，$K \lhd G$ 证毕！

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

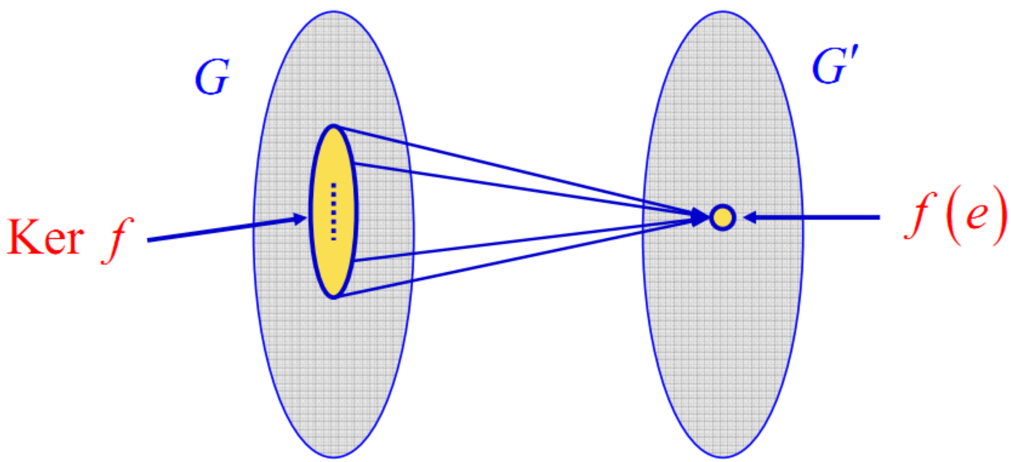
4.$\forall g \in G, h \in H, ghg^{-1} \in H$

设f是G到G'的同态，e是G的单位元，令$K = \{a \in G | f(a) = f(e)\}$，则$K$是$G$的正规子群，$K$称为同态$f$的核，记作$Ker\ f$

8.7 群的同态、同态基本定理

定理8.7.5

- 设f是G到G'的同态，e是G的单位元，令$K=\{a\in G|f(a)=f(e)\}$，则K是G的正规子群，K称为同态f的核，记作$Ker\ f$



8.7 群的同态、同态基本定理

- 定理8.7.6 设f是G到G'的同态，K是同态的核，那么对任意的$a, b \in G, f(a) = f(b)$的充要条件是$b \in aK$。

证明：

- 充分性：已知$b \in aK$ $\forall a, b \in G, f(a) = f(b)$
  - $\exists k \in K$,使得$b = ak$
  - $f(b) = f(ak) = f(a)f(k) = f(a)f(e) = f(a)$
- 必要性：已知$\forall a, b \in G, f(a) = f(b)$ $b \in aK$
  - $e' = f^{-1}(a)f(a) = f^{-1}(a)f(b) = f(a^{-1})f(b) = f(a^{-1}b)$
  - 说明$a^{-1}b \in K$, 即$b \in aK$

$f(a) = f(b) \Leftrightarrow a \equiv b (\mathrm{mod}\, n) \Leftrightarrow b \in aK$

8.7 群的同态、同态基本定理

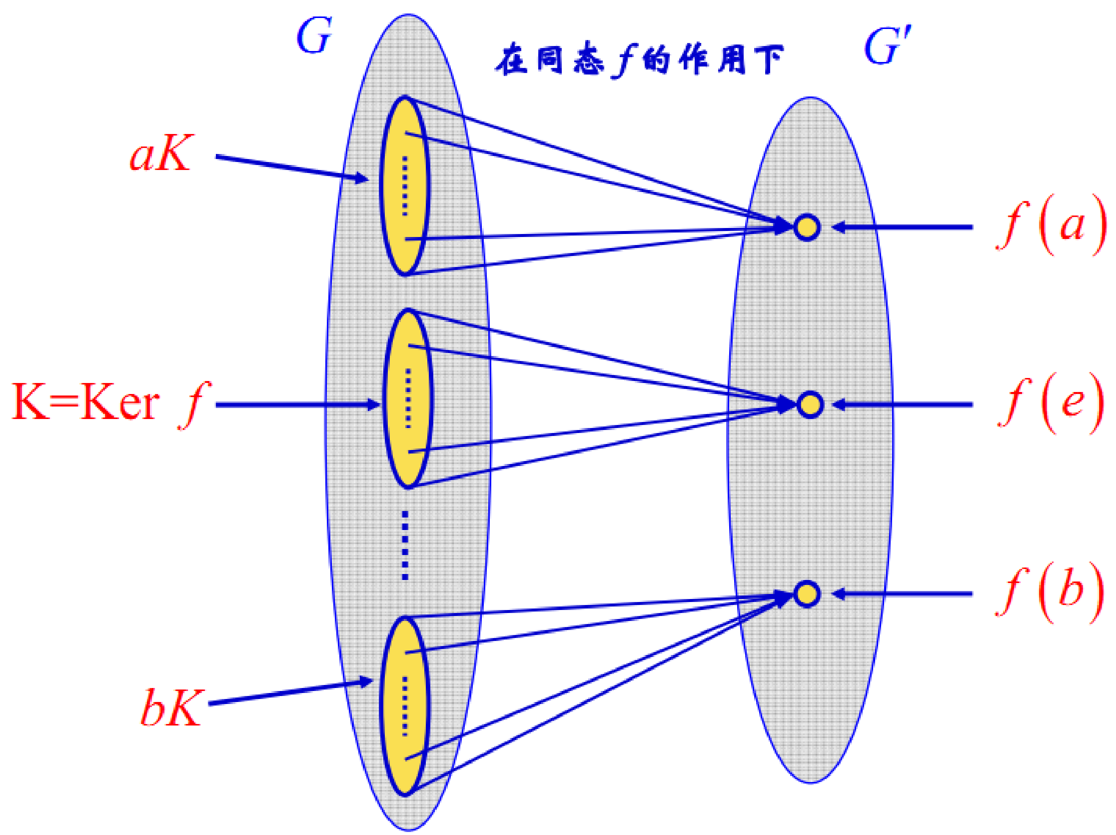
定理8.7.6

- 设f是G到G'的同态，K是同态的核，那么对任意的$a,b \in G, f(a) = f(b)$的充要条件是$b \in aK \quad a \in bK$

$$b \in aK \Leftrightarrow bK = aK$$

同态核的陪集所有元素映射到一个象！
同态核不同陪集的象一定不同！

8.7 群的同态、同态基本定理



$f(0) = f(6) = \cdots = \bar{0}; f(1) = f(7) = \cdots = \bar{1}$

8.7 群的同态、同态基本定理

定理8.7.7 设f是G到G'的同态，则f是单同态的充要条件是$Ker\ f=\{e\}$。

- 必要性：已知f为单同态 $Ker\ f=\{e\}$
  - G'中单位元e'在G中只有一个原象e, 即$Ker\ f=\{e\}$
- 充分性：已知$Ker\ f=\{e\}$ f为单同态
  - $\forall a,b\in G$，若$f(a)=f(b)$

  $f(a)f^{-1}(b)=f(a)f(b^{-1})=f(ab^{-1})=f(b)f^{-1}(b)=e'$
  - 由已知条件，$ab^{-1}=e$ $a=b$

证毕！

8.7 群的同态、同态基本定理

定理8.7.7

- 设f是G到G'的同态，则f是单同态的充要条件是$Ker\ f = \{e\}$。

推论

- 设f是G到G'的满同态，则f为同构的充要条件是$Ker\ f = \{e\}$。

8.7 群的同态、同态基本定理

同态基本定理

- 设G是一个群，则G的任一商群都是G的同态象；反之，若G'是G的同态象，f是G到G'的满同态，则$G' \cong G/K$，其中$K = Ker\ f$

$G = (Z, +), G' = (Z_n, +), f(a) = a\ (mod)\ n$
$K = \mathrm{Ker}\ f = nZ = \{nk | k \in Z\} \lhd G$
$G/K = (\{K, K+1, \dots, K+(n-1)\}, +)$
$G' \cong G/K : \bar{i} \leftrightarrow K + i$

8.7 群的同态、同态基本定理

证明： $G \sim G/H$

- G/H为任一商群，则$H \lhd G$ （商群的定义）
- 则可构造映射 $g: a \to aH(\forall a \in G)$
- 由引理8.7.1可知，g为满同态。
- 而G/H为G在g下的同态象
- 即$G \sim G/H$

引理8.7.1：设H是G的正规子群，$\forall a \in G$令$f: a \to aH$，则f是G到G/H的满同态。

8.7 群的同态、同态基本定理

证明： f是G到G'的满同态 $\longrightarrow$ $G/K \cong G'(K = Ker\ f)$

- 令$\varphi: aK \to f(a)$，显然符合映射条件
- $\forall x \in G'$, 由于f是满同态，因此必定$\exists a \in G$，使得$f(a) = x$，即$\varphi(aK) = f(a) = x$
- 因此φ是G/K到G'的满射
- 据定理8.7.6，$\varphi(aK) = \varphi(bK) \Leftrightarrow f(a) = f(b) \Leftrightarrow aK = bK$
- 因此φ是G/K到G'的单射

定理8.7.6：设f是G到G'的同态，K是同态的核，那么对任意的$a, b \in G, f(a) = f(b)$的充要条件是$b \in aK$。

8.7 群的同态、同态基本定理

证明：

f是G到G'的满同态 $\Longrightarrow$ $G/K \cong G'(K = Ker\ f)$

- $\varphi(aKbK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK)$
- 因此φ是G/K到G'的同构映射，即$G/k \cong G'$

8.7 群的同态、同态基本定理

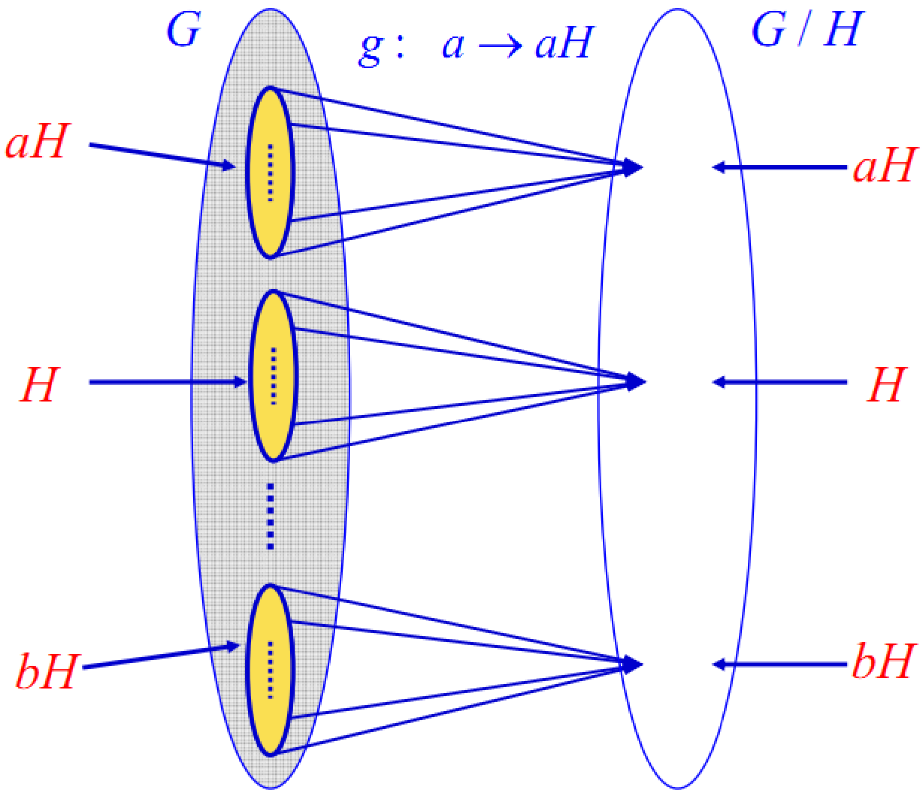
同态基本定理

- 设G是一个群，则G的任一商群都是G的同态象；反之，若G'是G的同态象，f是G到G'的满同态，则$G' \cong G/K$，其中$K = Ker\ f$

群的商群可以成为其同态象！

$G = (Z, +), H = nZ = \{nk|k \in Z\} \lhd G\ , f(a) = H + a$

8.7 群的同态、同态基本定理



8.7 群的同态、同态基本定理

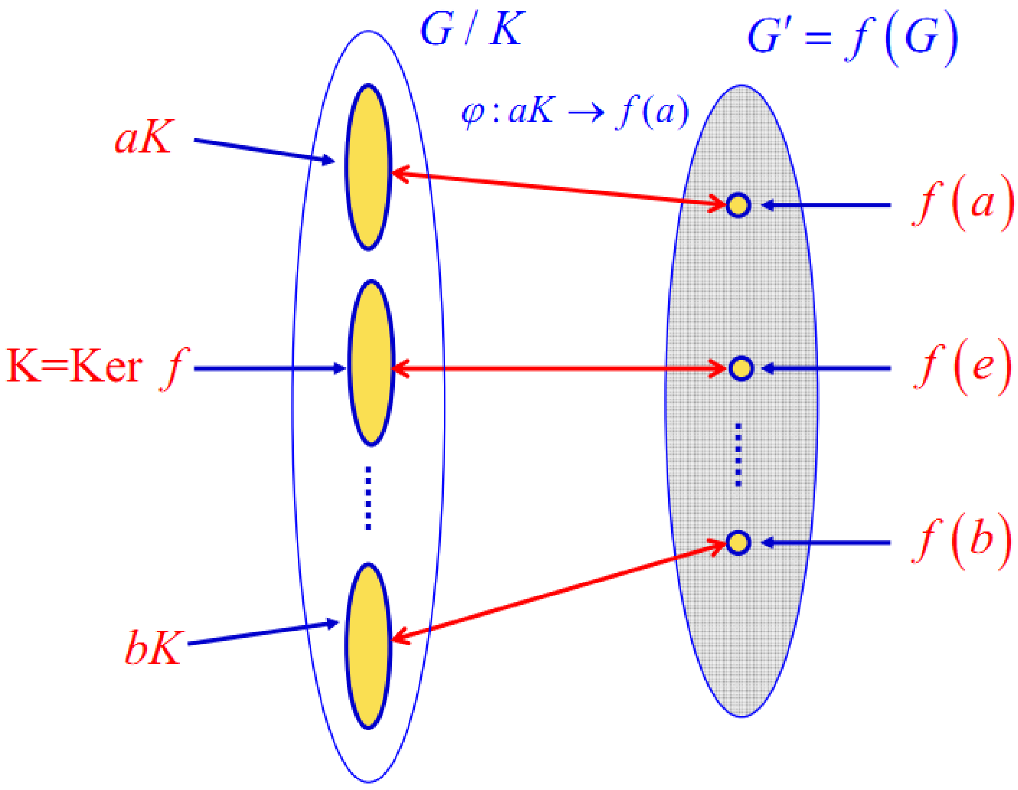
同态基本定理

- 设G是一个群，则G的任一商群都是G的同态象；反之，若G'是G的同态象，f是G到G'的满同态，则$G' \cong G/K$，其中$K = Ker\ f$

群（关于某个满同态）的同态象与该同态核的商群同构！

$G = (Z, +), G' = (Z_n, +), f(a) = a\ (mod)\ n$
$K = \mathrm{Ker}\ f = nZ = \{nk | k \in Z\} \lhd G$
$G/K = (\{K, K+1, \dots, K+(n-1)\}, +)$
$\boldsymbol{G' \cong G/K : \bar{i} \leftrightarrow K + i}$

8.7 群的同态、同态基本定理



8.7 群的同态、同态基本定理

几个经典的例子

- $G=(Z,+)$ 映射 $f: k\mapsto \bar{k}\quad (Z\to Z_n)$
  - 验证 f 是满同态
  - $K=\ker f=\langle n\rangle$
  - $Z/\langle n\rangle\cong Z_n$
- G 为全体n阶可逆实矩阵，对矩阵乘法构成群，取映射 $f: A\mapsto \det A\quad (G\to R^*)$
  - 验证 f 是满同态
  - $K=\ker f$ 为全体n阶行列式为1的可逆实矩阵
  - $G/K\cong R^*$

8.7 群的同态、同态基本定理

小结

- 群的同态、同态象
- 同态性质：单位元、逆元、子群
- 同态核，同态核性质
- 同态基本定理

离散数学2：代数结构部分期末总结

刘世霞
shixia@tsinghua.edu.cn

考试时间及考前答疑

- 考试时间
  - 6月15号 19:00-21:00
- 考试地点
  - 6A301,6A303
- 考前答疑：6月14号14:00-17:00
  - 陈莉：东主楼10-403
  - 刘世霞：东主楼10-407

6A301

2016010539	王世杰
2016012295	龙飘飘
2017011985	宗毅
2018010358	段祎然
2018010728	赵昀东
2018011855	褚驰
2018013371	何封越
2018013484	黄海天
2019010207	覃思中
2019010300	何承昱

2019010434	杨培文
2019011177	高嘉潞
2019012209	李奕杉
2019012282	王政
2019012480	方明洋
2019012490	程子睿
2019013260	蔡倬涵
2019013356	齐天亮
2019080151	梁兆麟
2019080302	辛馨

2020010108	徐浩博
2020010563	肖锦松
2020010896	刘天骐
2020010897	陈超帆
2020010906	武锦祀
2020010919	曹菡雯
2020010928	曹子尧
2020010936	姜迅驰
2020010940	叶舟桐
2020010970	陈顾骏

2020010971	王麒杰
2020010973	段津荣
2020010974	韩一松
2020010983	庞元喆
2020010987	容长荃
2020010988	牛天文
2020011004	罗柏霖
2020011010	孙桂宇
2020011011	杨天傲
2020011015	乔子卿

2020011089	徐潇悦
2020011093	闫天牧
2020011103	王子安

6A303

		2020012348	朱晗希	2020012387	张凯伦	2020012439	刘紫东
		2020012350	刘畅	2020012389	王集	2020012448	林碧澄
		2020012351	谭弈凡	2020012391	宋子瑄	2020012452	王军浩
2020011156	刘明道	2020012356	林欣涛	2020012392	张雨恬	2020012454	郑克寒
2020011466	刘志恒	2020012358	王宇航	2020012398	王双	2020012472	徐炜烨
2020011470	马越洲	2020012363	赵晨阳	2020012403	彭凌峰	2020012473	邓芮萱
2020011472	王子晨	2020012366	任自厚	2020012405	曾云帆	2020012479	王畅越
2020012345	申云溪	2020012375	汪静雅	2020012406	孙冯元	2020012493	蒲恒骏
2020012346	许德成	2020012383	陈睿柯	2020012408	沙之洲	2020050007	毛沐汐
2020012347	王秭祺	2020012385	陈启乾	2020012418	张凌华	2020080110	珍迪

考试内容

- 图论（70分）
- 代数结构（30分）

代数结构：第七章

7.1 集合与映射

7.2 等价关系

7.3 代数系统的概念

7.4 同构与同态

代数结构：第八章

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~~

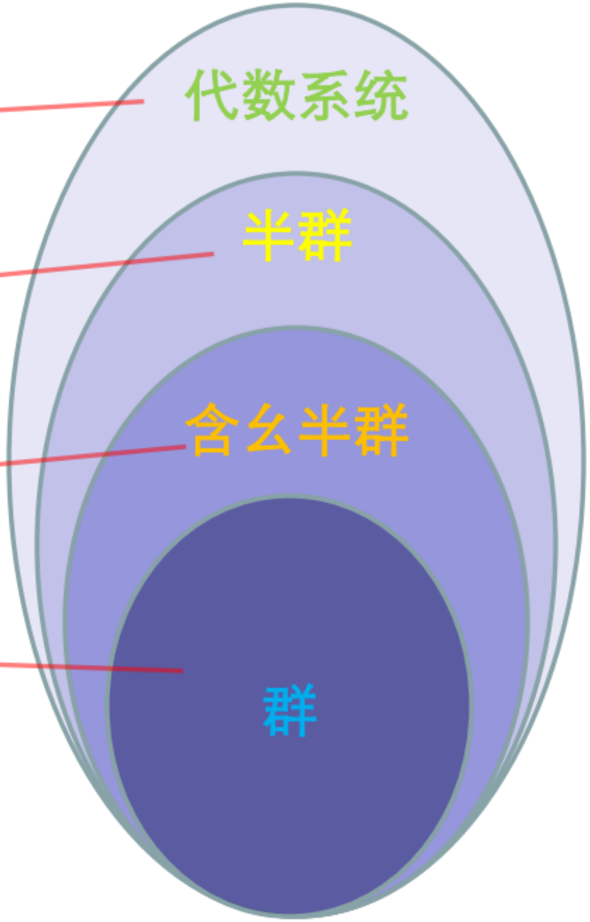
主要概念

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：

    $(N,+)$

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

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

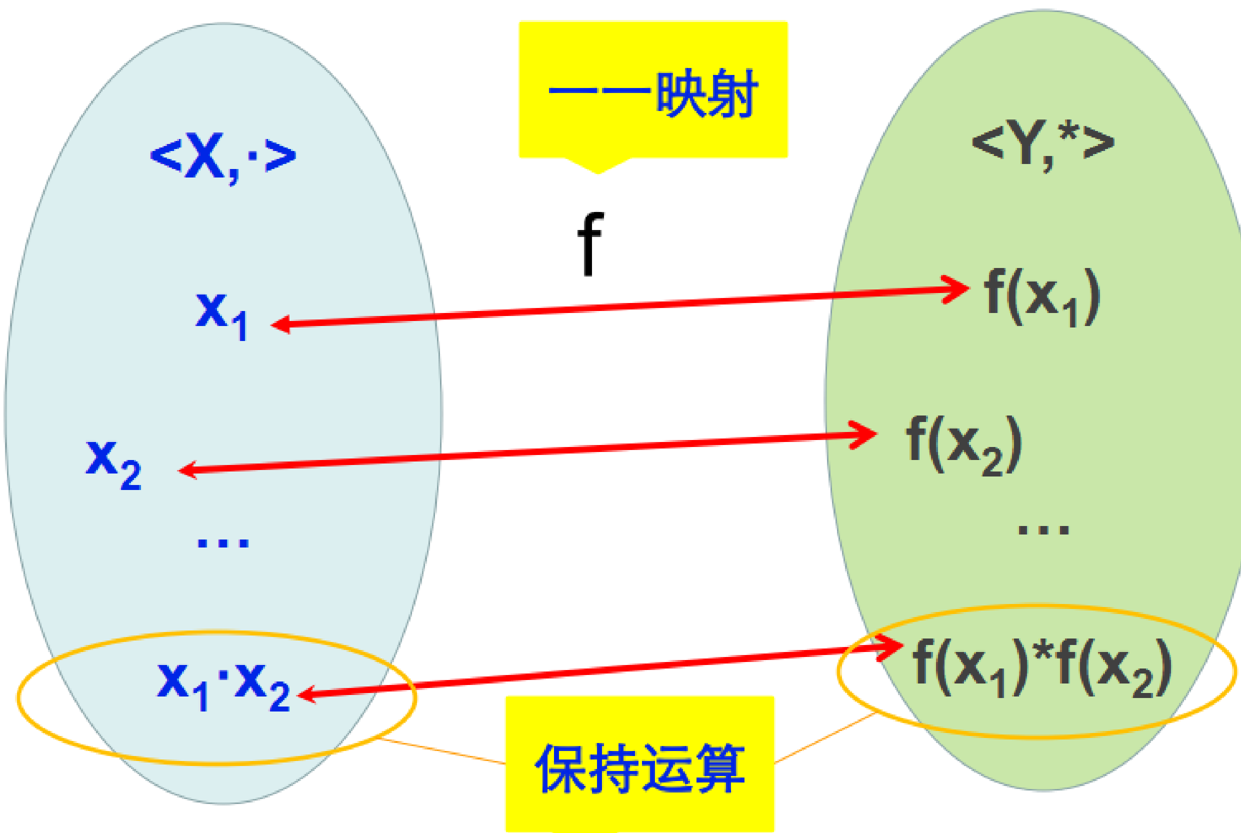
$$f(ab) = f(a) * f(b)$$

- 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$f:x\to lnx$

  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

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

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

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

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

$$\{\sigma(5)=5 \Rightarrow (5)$$

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

典型题目：选择题

多选题 1分

Setting

$(Z_m,\cdot)$

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

A 半群

B 幺群

C 交换幺群

D 都不是

提交

典型题目：判断题

（√）$(N,+)$是循环幺群

典型题目：填空题

（$Z,+$）的全部子群为 $\mathrm{H}_m = \{km \mid k \in \mathrm{Z}\}, m \geq 0$的整数

典型题目：填空题

（$Z_{12}, +$）的全部子群为

$\underline{\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle}$

$$< 0 > and < d >, d \mid n$$

一共有多少个子群？

（1）一个大于1的正整数N，如果它的标准分解式为：$N = P_1^{a_1} P_2^{a_2} \cdots P_n^{a_n}$ ，那么它的正因数个数为 $\sigma_0(N) = (1 + a_1)(1 + a_2) \cdots (1 + a_n)$ 。

8.3 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

    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 $r|k$

判断题

1. （ x ） $(N,+)$是循环群
2. （ √ ） $(Z,+)$是循环群
3. （ √ ） $(2Z,+)$是循环群 （$2Z$表示偶数集合）
4. （ √ ） $(Z_n,+)$是循环群
5. （ x ） $(Z_n^*,+)$是循环群（Z_n^*是$1\sim n$中与n互素元素组成的集合）
6. （ x ） $(Z_n^*,\times)$是循环群
7. （ x ） $(Q,+)$是循环群
8. （ √ ） $(\mathrm{Z},+)$ 和 $(2Z,+)$ 同构
9. （ x ） $(Q,+)$ 和 $(Z,+)$ 同构
10. （ x ） $(Q,+)$ 和 $(Q^+,\times)$ 同构
11. （ √ ） $(R,+)$ 和 $(R^+,\times)$ 同构
12. （ x ） $(R,+)$ 和 $(R^*,\times)$ 同构 （R^*表示$R-\{0\}$）

证明题

- 已知：在整数集 I 上的二元运算∗定义为：$a,b\in I$,

$$a * b=a+b-2$$

证明：$(I, *)$为群。

单位元：**2**

逆元：$x^{-1}=4-x$

1. 非空集合
2. 运算时封闭的
3. 满足结合律
4. 有单位元
5. 有逆元

证明：设G是群，证明对任意a，b有$O\langle ab\rangle=O\langle ba\rangle$

分析：令 $O\langle ab\rangle=n$ $O\langle ba\rangle = m$，然后利用阶的性质，证明n和m互相整除即可。

证：令 $O\langle ab\rangle=n$ $O\langle ba\rangle = m$，

由于$(ab)^n= abab...ab= a(ba)^{n-1}b= e$

$\Rightarrow$ $(ba)^n b= b$

$\Rightarrow$ $(ba)^n= e$

$\Rightarrow$ $m|n$

类似可得$n|m$

因而 $m=n$

此题的关键是把$(ab)^n$展开并变换成$(ba)^n$

证明题

- 已知：A, B 是群G的子群，试证$A \cup B$ 是G的子群当且仅当$A \subset B$ 或$B \subset A$ 。
- 证明：充分性显然。必要性反证：若不然，则存在$a \in A, a \notin B, b \in B, b \notin A$，此时$a, b \in A \cup B, ab \notin A \cup B$
- 该事实说明，群不能表示成两个真子群的并

- 是否存在群G可以表示成三个真子群的并？

谢谢

shixia@tsinghua.edu.cn