# 代 数 (二)

School of Computer Wuhan University

## 代数 (二) 内容

- ① 群的性质
  - 群的性质
  - 元素的阶
- ② 陪集和拉格朗日定理
  - 陪集的定义和性质
  - 拉格朗日定理
  - 陪集关系

### 群的性质

群

- 群是半群、含幺半群且每个元素都有逆元;
- 半群、含幺半群的所有性质在群中全部成立。

### 群的性质

#### 群

- 群是半群、含幺半群且每个元素都有逆元;
- 半群、含幺半群的所有性质在群中全部成立。

- 若群< G, \* >的单位元为e, ∀a, b ∈ G,
- ①  $(a^{-1})^{-1} = a$
- $(a*b)^{-1} = b^{-1}*a^{-1}$
- ① ::  $a * a^{-1} = e, a^{-1} * a = e,$ ::  $a \not\in a^{-1}$ 的左、右逆元, ::  $(a^{-1})^{-1} = a;$

- 若群< G, \* >的单位元为e, ∀a, b ∈ G,
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$ 证明:
- ①  $: a * a^{-1} = e, a^{-1} * a = e,,$  $:: a \not\in a^{-1}$  的左、右逆元,  $:: (a^{-1})^{-1} = a;$
- ②  $:: (a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$  $:: b^{-1}*a^{-1} \not\equiv a*b$  的左、右逆元、 $:: (a*b)^{-1} = b^{-1}*a^{-1}.$

- 若群< G, \* >的单位元为e, ∀a, b ∈ G,
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$ 证明:
- ① ::  $a * a^{-1} = e, a^{-1} * a = e,$ ::  $a \not\in a^{-1}$ 的左、右逆元, ::  $(a^{-1})^{-1} = a;$
- ②  $:: (a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$  $:: b^{-1}*a^{-1} \not = a*b$  的左、右逆元、 $:: (a*b)^{-1} = b^{-1}*a^{-1}.$

- 若群< G, \* >的单位元为 $e, \forall a, b \in G,$
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$  证明:
- ① ::  $a * a^{-1} = e, a^{-1} * a = e,$ ::  $a \not\in a^{-1}$ 的左、右逆元, ::  $(a^{-1})^{-1} = a;$
- ②  $:: (a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$  $:: b^{-1}*a^{-1} \not = a*b$  的左、右逆元、 $:: (a*b)^{-1} = b^{-1}*a^{-1}.$

- 若群< G, \* >的单位元为 $e, \forall a, b \in G,$
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$ 证明:
- ①  $\therefore a * a^{-1} = e, a^{-1} * a = e,$  $\therefore a \not\in a^{-1}$  的左、右逆元, $\therefore (a^{-1})^{-1} = a;$
- ②  $:: (a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$   $:: b^{-1}*a^{-1} \not\in a*b \not\in a*b \not\in a*b , : (a*b)^{-1} = b^{-1}*a^{-1}.$

- 若群< G, \* >的单位元为 $e, \forall a, b \in G,$
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$  证明:
- ①  $:: a * a^{-1} = e, a^{-1} * a = e,$  $:: a \not\in a^{-1}$ 的左、右逆元,  $:: (a^{-1})^{-1} = a;$
- ②  $:: (a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$  $:: b^{-1}*a^{-1} \not = a*b$  的左、右逆元、 $:: (a*b)^{-1} = b^{-1}*a^{-1}.$



- 若群< G, \* >的单位元为 $e, \forall a, b \in G,$
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$  证明:
- ①  $:: a * a^{-1} = e, a^{-1} * a = e,$  $:: a \not\in a^{-1}$ 的左、右逆元,  $:: (a^{-1})^{-1} = a;$
- ② ::  $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$  $\therefore b^{-1}*a^{-1} \not\equiv a*b$  的左、右逆元、∴  $(a*b)^{-1} = b^{-1}*a^{-1}$ .

- 若群< G, \* >的单位元为 $e, \forall a, b \in G,$
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$ 证明:
- ①  $:: a * a^{-1} = e, a^{-1} * a = e,$  $:: a \not\in a^{-1}$ 的左、右逆元,  $:: (a^{-1})^{-1} = a;$
- ② ::  $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$ ::  $b^{-1}*a^{-1} \not\ge a*b$  \text{ b. E. A \text{ if } \tau. ::  $(a*b)^{-1} = b^{-1}*a^{-1}$ .

- 若群< G, \* >的单位元为 $e, \forall a, b \in G,$
- ①  $(a^{-1})^{-1} = a$
- ②  $(a*b)^{-1} = b^{-1}*a^{-1}$ 证明:
- ①  $:: a * a^{-1} = e, a^{-1} * a = e,$  $:: a \not\in a^{-1}$  的左、右逆元、 $:: (a^{-1})^{-1} = a;$
- ②  $:: (a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = e,$   $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = e,$  $:: b^{-1}*a^{-1} \not\equiv a*b$  的左、右逆元,  $:: (a*b)^{-1} = b^{-1}*a^{-1}.$

- 若< G, \*>是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a=b; 证明:
- 2 同理可证。

- 若< G, \*>是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a = b;证明:
- ① 存在性:  $\diamondsuit x = a^{-1} * b$ , 则  $a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$ 惟一性: 若a \* x = b,
  则 $a^{-1} * (a * x) = a^{-1} * b$ ,  $\therefore (a^{-1} * a) * x = a^{-1} * b$ ,  $p x = a^{-1} * b$ .
- ② 同理可证。

- 若< G, \*>是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y,使得y\*a=b;
- ② 同理可证。

- 若< G, \*>是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a = b;证明:
- ① 存在性:  $\diamondsuit x = a^{-1} * b$ , 则  $a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$ ,
  惟一性: 若 a \* x = b,
  则 $a^{-1} * (a * x) = a^{-1} * b$ ,  $\therefore (a^{-1} * a) * x = a^{-1} * b$ ,  $\bowtie x = a^{-1} * b$ .
- 2 同理可证。

- 若< G, \*>是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a = b;证明:
- ① 存在性:  $\diamondsuit x = a^{-1} * b$ , 则  $a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$ ,
  惟一性: 若 a \* x = b,
  则 $a^{-1} * (a * x) = a^{-1} * b$ ,  $\therefore (a^{-1} * a) * x = a^{-1} * b$ , 即 $x = a^{-1} * b$ .
- 2 同理可证。

- 若< G, \*>是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a = b;证明:
- 2 同理可证。

- 若< G, \* >是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a = b;证明:
- 2 同理可证。

- 若< G, \* >是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a = b;证明:
- ① 存在性:  $\diamondsuit x = a^{-1} * b$ , 则  $a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$ ,
  惟一性: 若a \* x = b,
  则 $a^{-1} * (a * x) = a^{-1} * b$ ,  $\therefore (a^{-1} * a) * x = a^{-1} * b$ , 即 $x = a^{-1} * b$ .
- 2 同理可证。

- 若< G, \* >是群,则 $\forall a, b \in G,$
- ① 存在惟一的x, 使得a\*x=b;
- ② 存在惟一的y, 使得y\*a = b;证明:
- ① 存在性:  $\diamondsuit x = a^{-1} * b$ , 则  $a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$ ,
  惟一性: 若a \* x = b,
  则 $a^{-1} * (a * x) = a^{-1} * b$ ,  $\therefore (a^{-1} * a) * x = a^{-1} * b$ , 即 $x = a^{-1} * b$ .
- ② 同理可证。

### 性质

• 群中消去律成立。

证: 群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若x是幂等元,则,x = x \* x

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

②  $\mathbf{A}|\mathbf{G}| > 1$ ,且群 $\mathbf{G}$ 中有零元 $\theta$ ,

则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

#### 性质

• 群中消去律成立。

证: 群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若x是幂等元,则,x=x\*x

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ ,

则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

#### 性质

• 群中消去律成立。

证:群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若 $\times$ 是幂等元,则,x = x \* x

 $x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e$ 

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ ,

则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

#### 性质

• 群中消去律成立。

证: 群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若x是幂等元,则,x = x \* x

 $x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$ 

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ ,

则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

### 性质

• 群中消去律成立。

证:群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若 $\times$ 是幂等元,则, $\times = \times \times \times$ 

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ ,

则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

所以 $\theta$ 无逆元,与G是群矛盾。

#### 性质

• 群中消去律成立。

证: 群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若x是幂等元,则,x = x \* x

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ ,

则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

#### 性质

• 群中消去律成立。

证: 群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若×是幂等元,则, x = x \* x

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ , 则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

所以 $\theta$ 无逆元,与G是群矛盾。

#### 性质

• 群中消去律成立。

证:群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若x是幂等元,则,x = x \* x

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

● 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ ,

 $\text{NJ} \forall x \in G, x * \theta = \theta * x = \theta \neq e,$ 

### 性质

• 群中消去律成立。

证:群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若x是幂等元,则,x = x \* x

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

• 群中不可能有零元。

证: ① 若|G|=1,则唯一的元素视为单位元;

②  $\dot{\mathbf{z}}|G| > 1$ , 且群G中有零元 $\theta$ , 则 $\forall x \in G$ .  $x * \theta = \theta * x = \theta \neq e$ ,

所以 $\theta$ 无逆元、与G是群矛盾。

#### 性质

● 群中消去律成立。

证:群的每个元素都可逆,则每个元素都可约,所以消去律成立。

• 单位元是群中唯一的幂等元。

证: 若×是幂等元,则, x = x \* x

$$x = e * x = (x^{-1} * x) * x = x^{-1} * (x * x) = x^{-1} * x = e.$$

• 群中不可能有零元。

证: ① 若 |G| = 1, 则唯一的元素视为单位元;

② 若|G| > 1, 且群G中有零元 $\theta$ ,

则 $\forall x \in G, x * \theta = \theta * x = \theta \neq e$ ,

所以 $\theta$ 无逆元、与G是群矛盾。

### 性质

- 有限群 < G,\* > 的运算表中的每一行(列)是G中元素的一个置换。(有限集合S到S的一个双射,称为S的一个置换。)
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行,  $\forall b \in G$ ,则 $b = a*(a^{-1}*b)$ ,... b出现在a的那一行。 由a, b的任意性,得证;
- ② 再证:一个元素在运算表中的每一行(列)中不能出现两次(单射):假设元素k在a的那一行出现两次,
  - 即 $k = a * b_1 = a * b_2$ , 且 $b_1 \neq b_2$ , 但与群的可约性矛盾。
- ③ 因群G中有单位元, :任两行(列)均不相同。

### 性质

- 有限群 < G,\* > 的运算表中的每一行(列)是G中元素的一个置换。(有限集合5到5的一个双射,称为5的一个置换。)证:
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行,  $\forall b \in G$ ,则 $b = a*(a^{-1}*b)$ ,... b出现在a的那一行。 a,b的任意性,得证;
- ② 再证:一个元素在运算表中的每一行(列)中不能出现两次(单射):假设元素k在a的那一行出现两次,

即 $k = a * b_1 = a * b_2$ , 且 $b_1 \neq b_2$ , 但与群的可约性矛盾。

③ 因群G中有单位元, ::任两行(列)均不相同。

### 性质

- 有限群 < G,\* > 的运算表中的每一行(列)是G中元素的一个置换。(有限集合5到5的一个双射,称为5的一个置换。)证:
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行,

出d, D的任息性,行证,

② 再证:一个元素在运算表中的每一行(列)中不能出现两次(单射):假设元素k在a的那一行出现两次,

 $pk = a * b_1 = a * b_2$ , 且 $b_1 \neq b_2$ , 但与群的可约性矛盾。

③ 因群G中有单位元, 二任两行 (列) 均不相同。

### 性质

- 有限群 < G,\* > 的运算表中的每一行(列)是G中元素的一个置换。(有限集合5到5的一个双射,称为5的一个置换。)证:
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行, $\forall b \in G$ ,则 $b = a*(a^{-1}*b)$ ,... b出现在a的那一行。由a, b的任意性,得证:
- ② 再证:一个元素在运算表中的每一行(列)中不能出现两次(单射):假设元素k在a的那一行出现两次,

 $pk = a * b_1 = a * b_2$ , 且 $b_1 \neq b_2$ , 但与群的可约性矛盾。

③ 因群G中有单位元, ::任两行(列)均不相同。

### 性质

- 有限群< G,\*>的运算表中的每一行(列)是G中元素的一个置换。(有限集合5到5的一个双射, 称为5的一个置换。) 证:
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行,  $\forall b \in G$ ,则 $b = a*(a^{-1}*b)$ ,... b出现在a的那一行。 由a, b的任意性,得证;
- ② 再证:一个元素在运算表中的每一行(列)中不能出现两次(单射):假设元素k在a的那一行出现两次,

 $pk = a * b_1 = a * b_2$ , 且 $b_1 \neq b_2$ , 但与群的可约性矛盾。

③ 因群G中有单位元, ::任两行(列)均不相同。

### 性质

- 有限群< G,\*>的运算表中的每一行(列)是G中元素的一个置换。(有限集合S到S的一个双射,称为S的一个置换。)
   证:
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行,  $\forall b \in G$ ,则 $b = a*(a^{-1}*b)$ ,... b出现在a的那一行。 由a, b的任意性,得证;
- ② 再证:一个元素在运算表中的每一行(列)中不能出现两次(单射):假设元素k在a的那一行出现两次,

 $pk = a * b_1 = a * b_2$ , 且 $b_1 \neq b_2$ , 但与群的可约性矛盾。

③ 因群G中有单位元, ::任两行(列)均不相同。

### 性质

- 有限群< G,\*>的运算表中的每一行(列)是G中元素的一个置换。(有限集合S到S的一个双射,称为S的一个置换。)
   证:
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行,  $\forall b \in G$ ,则 $b = a*(a^{-1}*b)$ ,... b出现在a的那一行。 由a, b的任意性,得证;
- ② 再证: 一个元素在运算表中的每一行(列)中不能出现两次 (单射): 假设元素k在a的那一行出现两次, 即 $k=a*b_1=a*b_2$ ,且 $b_1\neq b_2$ ,但与群的可约性矛盾。
- ③ 因群G中有单位元, 二任两行(列)均不相同。

### 性质

- 有限群< G,\*>的运算表中的每一行(列)是G中元素的一个置换。(有限集合S到S的一个双射,称为S的一个置换。)
   证:
- ① 先证: 群G中的任一元素在运算表中的每一行(列)中均出现(满射): 考虑运算表中对应于元素a的那一行,  $\forall b \in G$ ,则 $b = a*(a^{-1}*b)$ ,... b出现在a的那一行。 由a, b的任意性,得证;
- ② 再证: 一个元素在运算表中的每一行(列)中不能出现两次 (单射): 假设元素k在a的那一行出现两次,  $p_k = a * b_1 = a * b_2$ ,且 $b_1 \neq b_2$ ,但与群的可约性矛盾。
- ③ 因群G中有单位元,∴任两行(列)均不相同。

## 有限群例子

Table: 一阶群



Table: 二阶群

*	e	a
e	e	a
a	a	e

Table: 三阶群

*	e	a	b
e	e	a	b
а	a	b	e
b	b	e	a

Table: 四阶群(1)

*	e	a	b	С
e	e	a	b	С
a	a	b	С	e
<b>b</b>	b	С	е	a
С	С	e	а	Ь

Table: 四阶群(2)

*	e	a	b	С
e	e	a	b	C
a	a	e	С	Ь
<b>b</b>	b	С	е	a
C∢	- C ∢	<b>∌</b>	<b>a</b> →	<b>e</b> ≘



- 群< G, \*>,  $\forall a \in G$ , 定义函数 $f_a : G \longrightarrow G$ ,  $x \longmapsto a * x$ , 则  $f_a$ 是双射。
- 证:

$$f_{a} \circ f_{a-1}(x)$$

$$= f_{a}(f_{a-1}(x))$$

$$= f_{a}(a^{-1} * x)$$

$$= a * a^{-1} * x = x$$

- $\therefore f_a \circ f_{a^{-1}} = \mathbb{I}_G$ ,同理, $f_{a^{-1}} \circ f_a = \mathbb{I}_G$ ,
- :. fa是双射。

- 群< G, \*>,  $\forall a \in G$ , 定义函数 $f_a : G \longrightarrow G$ ,  $x \longmapsto a * x$ , 则  $f_a$ 是双射。
- 证:

$$f_{a} \circ f_{a-1}(x)$$

$$= f_{a}(f_{a-1}(x))$$

$$= f_{a}(a^{-1} * x)$$

$$= a * a^{-1} * x = x$$

- $\therefore f_a \circ f_{a^{-1}} = \mathbb{I}_G$ ,同理, $f_{a^{-1}} \circ f_a = \mathbb{I}_G$ ,
- : f.是双射。

- 群< G, \*>,  $\forall a \in G$ , 定义函数 $f_a : G \longrightarrow G$ ,  $x \longmapsto a * x$ , 则  $f_a$ 是双射。
- 证:

$$f_a \circ f_{a^{-1}}(x)$$
  
=  $f_a(f_{a^{-1}}(x))$   
=  $f_a(a^{-1} * x)$   
=  $a * a^{-1} * x = x$ 

- $\therefore f_a \circ f_{a^{-1}} = \mathbb{I}_G$ ,同理, $f_{a^{-1}} \circ f_a = \mathbb{I}_G$ ,
- :. f.是双射。

#### 定理

- 群< G, \*>,  $\forall a \in G$ , 定义函数 $f_a : G \longrightarrow G$ ,  $x \longmapsto a * x$ , 则  $f_a$ 是双射。
- 证:

$$f_a \circ f_{a^{-1}}(x)$$
  
=  $f_a(f_{a^{-1}}(x))$   
=  $f_a(a^{-1} * x)$   
=  $a * a^{-1} * x = x$ 

$$\therefore f_a \circ f_{a^{-1}} = \mathbb{I}_G$$
,同理, $f_{a^{-1}} \circ f_a = \mathbb{I}_G$ ,

:. f.是双射。

#### 定理

- 群< G, \*>,  $\forall a \in G$ , 定义函数 $f_a : G \longrightarrow G$ ,  $x \longmapsto a * x$ , 则  $f_a$ 是双射。
- 证:

$$f_a \circ f_{a^{-1}}(x)$$
  
=  $f_a(f_{a^{-1}}(x))$   
=  $f_a(a^{-1} * x)$   
=  $a * a^{-1} * x = x$ 

$$\therefore f_a \circ f_{a^{-1}} = \mathbb{I}_G$$
,同理, $f_{a^{-1}} \circ f_a = \mathbb{I}_G$ ,

:. fa是双射。

### 例

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

 $\leftarrow$ 

若∀a, b∈ G, (a\*b)\*(a\*b) = (a\*a)\*(b\*b),  
∴ 
$$a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1}$$
,  
∴由结合律,  $b*a = a*b$ , 群< G,\*>是可交换群;

若群 < 
$$G$$
, \* >是可交换群,则 $\forall a, b \in G$ ,  $a * b = b * a$ ,  
∴  $a * (a * b) * b = a * (b * a) * b$   
∴  $(a * a) * (b * b) = (a * b) * (a * b)$ 

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

$$\leftarrow$$

若
$$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b),$$
∴  $a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1},$ 
∴由结合律, $b*a = a*b$ ,群 $< G, *>$ 是可交换群;

$$\Longrightarrow$$

若群
$$< G, *>$$
是可交換群,则 $\forall a, b \in G, a * b = b * a,$   
 $\therefore a * (a * b) * b = a * (b * a) * b$   
 $\therefore (a * a) * (b * b) = (a * b) * (a * b)$ 

### 例

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

 $\Leftarrow$ 

若
$$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b),$$
∴  $a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1},$ 
∴由结合律, $b*a = a*b$ ,群 $< G, *>$ 是可交换群;

若群< 
$$G$$
,\* >是可交换群,则 $\forall a,b \in G$ ,  $a*b=b*a$ ,  
∴  $a*(a*b)*b=a*(b*a)*b$   
∴  $(a*a)*(b*b)=(a*b)*(a*b)$ 

### 例

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

$$\leftarrow$$

**者**
$$∀a, b ∈ G, (a * b) * (a * b) = (a * a) * (b * b),$$

$$\therefore a^{-1} * (a * b) * (a * b) * b^{-1} = a^{-1} * (a * a) * (b * b) * b^{-1}$$

若群
$$< G, * >$$
是可交换群,则 $\forall a, b \in G, a * b = b * a,$ 

$$\therefore a * (a * b) * b = a * (b * a) * b$$

$$(a*a)*(b*b) = (a*b)*(a*b)$$

### 例

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

$$\leftarrow$$

者 
$$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b),$$
∴  $a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1},$ 
∴ 由结合律, $b*a = a*b$ ,群 $< G, *>$ 是可交换群;

若群< 
$$G$$
,\* >是可交换群,则 $\forall a,b \in G$ ,  $a*b=b*a$ ,  
∴  $a*(a*b)*b=a*(b*a)*b$   
∴  $(a*a)*(b*b)=(a*b)*(a*b)$ 

### 例

- 群< G, \*>是可交换群,iff,  $\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b).$
- 证:

 $\Leftarrow$ 

若
$$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b),$$
∴  $a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1},$ 
∴由结合律, $b*a = a*b$ ,群 $< G, *>$ 是可交换群;

若群
$$< G, *>$$
是可交换群,则 $\forall a, b \in G, a * b = b * a,$ 
∴  $a * (a * b) * b = a * (b * a) * b$ 
∴  $(a * a) * (b * b) = (a * b) * (a * b)$ 

### 例

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

$$\leftarrow$$

$$者 ∀a, b ∈ G, (a * b) * (a * b) = (a * a) * (b * b),$$

$$\therefore a^{-1} * (a * b) * (a * b) * b^{-1} = a^{-1} * (a * a) * (b * b) * b^{-1},$$

若群
$$< G, * >$$
是可交换群,则 $\forall a, b \in G, a * b = b * a,$ 

$$\therefore a * (a * b) * b = a * (b * a) * b$$

$$(a*a)*(b*b) = (a*b)*(a*b)$$

#### 例

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

$$\leftarrow$$

若
$$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b),$$
∴  $a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1},$ 
∴由结合律, $b*a = a*b$ ,群 $< G, *>$ 是可交换群;

若群
$$< G$$
, \* $>$ 是可交换群,则 $\forall a, b \in G$ ,  $a*b = b*a$ ,

$$\therefore a * (a * b) * b = a * (b * a) * b$$

$$(a*a)*(b*b) = (a*b)*(a*b)$$

#### 例

- 群 < G, \* > 是可交换群,iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

$$\leftarrow$$

若
$$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b),$$
∴  $a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1},$ 
∴由结合律, $b*a = a*b$ ,群 $< G, *>$ 是可交换群;

若群
$$< G, *>$$
是可交换群,则 $\forall a, b \in G, a * b = b * a,$ 
∴  $a * (a * b) * b = a * (b * a) * b$ 

### 例

- 群 < G, \* > 是可交换群, iff,  $\forall a, b \in G, (a * b) * (a * b) = (a * a) * (b * b).$
- 证:

$$\leftarrow$$

**若**
$$\forall a, b \in G, (a*b)*(a*b) = (a*a)*(b*b),$$

$$\therefore a^{-1} * (a * b) * (a * b) * b^{-1} = a^{-1} * (a * a) * (b * b) * b^{-1},$$

∴由结合律,
$$b*a=a*b$$
,群 $< G,*>$ 是可交换群;

若群
$$< G$$
,  $* >$ 是可交换群,则 $\forall a, b \in G$ ,  $a * b = b * a$ ,

$$\therefore a * (a * b) * b = a * (b * a) * b$$

$$(a*a)*(b*b) = (a*b)*(a*b)$$

- 设群< G, \*>,  $\forall a \in G$ , a的整数次幂可以归纳定义为:
  - ①  $a^0 = e$ ;
  - ②  $a^{n+1} = a^n * a, (n \in \mathbb{N});$
  - ③  $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质:

  - $(2 (a^m)^n = a^{mn}, (m, n \in \mathbb{Z})$

- 设群< G, \*>,  $\forall a \in G$ , a的整数次幂可以归纳定义为:
  - ①  $a^0 = e$ ;
  - ②  $a^{n+1} = a^n * a, (n \in \mathbb{N});$
  - ③  $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质:

- 设群< G, \*>,  $\forall a \in G$ , a的整数次幂可以归纳定义为:
  - ①  $a^0 = e$ ;
  - ②  $a^{n+1} = a^n * a, (n \in \mathbb{N});$
  - ③  $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质:

  - $(a^m)^n = a^{mn}, \quad (m, n \in \mathbb{Z})$

- 设群< G, \*>,  $\forall a \in G$ , a的整数次幂可以归纳定义为:
  - ①  $a^0 = e$ ;
  - ②  $a^{n+1} = a^n * a, (n \in \mathbb{N});$
  - ③  $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质:

  - $(2 (a^m)^n = a^{mn}, (m, n \in \mathbb{Z})$

- 设群< G, \*>,  $\forall a \in G$ , a的整数次幂可以归纳定义为:
  - ①  $a^0 = e$ ;
  - ②  $a^{n+1} = a^n * a, (n \in \mathbb{N});$
  - ③  $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质:
  - ①  $a^m * a^n = a^{m+n}$ .
  - $(2 (a^m)^n = a^{mn}, (m, n \in \mathbb{Z})$

- 设群< G, \*>,  $\forall a \in G$ , a的整数次幂可以归纳定义为:
  - ①  $a^0 = e$ ;
  - ②  $a^{n+1} = a^n * a, (n \in \mathbb{N});$
  - ③  $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质:
  - ①  $a^m * a^n = a^{m+n}$ ,
  - $(2 (a^m)^n = a^{mn}, (m, n \in \mathbb{Z})$

- 设群< G, \*>,  $\forall a \in G$ , a的整数次幂可以归纳定义为:
  - ①  $a^0 = e$ ;
  - ②  $a^{n+1} = a^n * a, (n \in \mathbb{N});$
  - ③  $a^{-n} = a^{-1} * a^{-1} * ... * a^{-1} = (a^{-1})^n, n \in \mathbb{N}_+$
- 性质:
  - ①  $a^m * a^n = a^{m+n}$ ,
  - $(a^m)^n = a^{mn}, (m, n \in \mathbb{Z})$

#### 定义-元素的阶

- 设< G, \*, e > 是群, $a \in G$ ,若存在正整数n,使得 $a^n = e$ ,满足上式的最小正整数n称为元素a的阶,并称元素a具有有限阶n,记为|a| = n.
- 若不存在这样的正整数n,则称元素a具有无限阶。

- 单位元e的阶为1, 且单位元是阶为1的唯一元素。
- 群 $< \mathbb{Z}, +, 0 >$ 中,除单位元0外,其余元素均为无限阶.
- $\bullet$  <  $\mathbb{N}_4$ , +4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.

#### 定义-元素的阶

- 设< G, \*, e > 是群, $a \in G$ ,若存在正整数n,使得 $a^n = e$ ,满足上式的最小正整数n称为元素a的阶,并称元素a具有有限阶n,记为|a| = n.
- 若不存在这样的正整数n,则称元素a具有无限阶。

- 单位元e的阶为1,且单位元是阶为1的唯一元素。
- 群 $< \mathbb{Z}, +, 0 >$ 中,除单位元0外,其余元素均为无限阶.
- $\bullet$  <  $\mathbb{N}_4$ , +4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.

#### 定义-元素的阶

- 设< G, \*, e > 是群, $a \in G$ ,若存在正整数n,使得 $a^n = e$ ,满足上式的最小正整数n称为元素a的阶,并称元素a具有有限阶n,记为|a| = n.
- 若不存在这样的正整数n,则称元素a具有无限阶。

- 单位元e的阶为1,且单位元是阶为1的唯一元素。
- 群< ℤ,+,0>中,除单位元0外,其余元素均为无限阶.
- $\bullet$  <  $\mathbb{N}_4$ , +4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.

#### 定义-元素的阶

- 设< G, \*, e > 是群, $a \in G$ ,若存在正整数n,使得 $a^n = e$ ,满足上式的最小正整数n称为元素a的阶,并称元素a具有有限阶n,记为|a| = n.
- 若不存在这样的正整数n,则称元素a具有无限阶。

- 单位元e的阶为1,且单位元是阶为1的唯一元素。
- 群 $< \mathbb{Z}, +, 0 >$ 中,除单位元0外,其余元素均为无限阶.
- $\bullet$  <  $\mathbb{N}_4$ , +4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.

#### 定义-元素的阶

- 设< G, \*, e > 是群, $a \in G$ ,若存在正整数n,使得 $a^n = e$ ,满足上式的最小正整数n称为元素a的阶,并称元素a具有有限阶n,记为|a| = n.
- 若不存在这样的正整数n,则称元素a具有无限阶。

- 单位元e的阶为1,且单位元是阶为1的唯一元素。
- 群 $< \mathbb{Z}, +, 0 >$ 中,除单位元0外,其余元素均为无限阶.
- $\bullet$  <  $\mathbb{N}_4$ , +4, 0 >, |0| = 1, |1| = 4, |2| = 2, |3| = 4.

### 定理

- $\# < G, *, e > \psi$ , |a| = n,  $\| a^k = e$ , iff, n | k.
- 证明:

 $\leftarrow$ 

若
$$n|k$$
,即  $k = mn, m \in \mathbb{Z}$ ,则 $a^k = a^{mn} = (a^n)^m = e^m = e$ .

-

若
$$a^k = e$$
, 设 $k = mn + t$ ,  $0 \leqslant t < n$ ,  $m \in \mathbb{Z}$ ,

$$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$$

$$\therefore$$
 n是使 $a^n = e$ 的最小正整数,又 $0 \le t < n$ ,

$$\therefore t = 0, k = mn.$$

### 定理

- $\# < G, *, e > \psi$ , |a| = n,  $\| a^k = e$ , iff, n | k.
- 证明:

 $\leftarrow$ 

若
$$n|k$$
,即  $k = mn, m \in \mathbb{Z}$ ,则 $a^k = a^{mn} = (a^n)^m = e^m = e$ .

 $\Longrightarrow$ 

 $\therefore$  n是使 $a^n = e$ 的最小正整数,又 $0 \le t < n$ ,  $\therefore t = 0, k = mn$ .

### 定理

- $\# < G, *, e > \psi$ , |a| = n,  $\| a^k = e$ , iff, n | k.
- 证明:

$$\leftarrow$$

若
$$n|k$$
,即  $k=mn, m \in \mathbb{Z}$ ,则 $a^k=a^{mn}=(a^n)^m=e^m=e$ .

 $\Longrightarrow$ 

若
$$a^k = e$$
, 设 $k = mn + t$ ,  $0 \le t < n$ ,  $m \in \mathbb{Z}$ ,  
 $a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e$ .

 $\therefore$  n是使 $a^n = e$ 的最小正整数,又 $0 \leqslant t < n$ ,

 $\therefore t = 0, k = mn.$ 

- $\# < G, *, e > +, |a| = n, M |a^k| = e, \text{ iff}, n|k.$
- 证明:

$$\leftarrow$$

若
$$n|k$$
,即  $k=mn, m \in \mathbb{Z}$ ,

则
$$a^{\kappa} = a^{mn} = (a^n)^m = e^m = e.$$

若
$$a^k = e$$
,设 $k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$ ,

$$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e.$$

:: 
$$n$$
是使 $a^n = e$ 的最小正整数,又 $0 \le t < n$ ,

$$\therefore t = 0, k = mn.$$

- 群 < G, \*, e >中,|a| = n,则  $a^k = e$ , iff, n|k.
- 证明:

$$\leftarrow$$

$$若n|k$$
,即  $k=mn, m \in \mathbb{Z}$ ,则  $a^k=a^{mn}=(a^n)^m=e^m=e$ .

$$\Longrightarrow$$

#### 定理

- $\# < G, *, e > +, |a| = n, M |a^k| = e, \text{ iff}, n|k.$
- 证明:

$$\leftarrow$$

若
$$n|k$$
,即  $k=mn, m \in \mathbb{Z}$ ,则  $a^k=a^{mn}=(a^n)^m=e^m=e$ .

 $\Longrightarrow$ 

#### 定理

- $\not$   $\mathbf{A} < G, *, e > \mathbf{p}$ , |a| = n,  $\mathbf{M}$   $a^k = e$ , iff, n | k.
- 证明:

$$\leftarrow$$

若
$$n|k$$
, 即  $k = mn, m \in \mathbb{Z}$ , 则 $a^k = a^{mn} = (a^n)^m = e^m = e$ .

$$\Longrightarrow$$

若
$$a^k = e$$
,设 $k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$ ,

$$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e.$$

 $\therefore$  n是使 $a^n = e$ 的最小正整数,又 $0 \le t < n$ ,

 $\therefore t = 0, k = mn.$ 

#### 定理

- $\# < G, *, e > +, |a| = n, M |a^k| = e, \text{ iff}, n|k.$
- 证明:

$$\leftarrow$$

若
$$n|k$$
, 即  $k = mn, m \in \mathbb{Z}$ , 则 $a^k = a^{mn} = (a^n)^m = e^m = e$ .

$$\Longrightarrow$$

 $\therefore t = 0, k = mn.$ 

- $\# < G, *, e > +, |a| = n, M |a^k| = e, \text{ iff}, n|k.$
- 证明:

$$\leftarrow$$

若
$$n|k$$
, 即  $k = mn, m \in \mathbb{Z}$ , 则 $a^k = a^{mn} = (a^n)^m = e^m = e$ .

$$\Longrightarrow$$

$$若 a^k = e$$
,设 $k = mn + t, 0 \leqslant t < n, m \in \mathbb{Z}$ ,
$$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e.$$

$$\therefore$$
 n是使 $a^n = e$ 的最小正整数,又 $0 \le t < n$ ,

$$\therefore t = 0, k = mn.$$

- $\not$   $\mathbf{A} < G, *, e > \mathbf{p}$ , |a| = n,  $\mathbf{M}$   $a^k = e$ , iff, n | k.
- 证明:

$$\leftarrow$$

若
$$n|k$$
, 即  $k = mn, m \in \mathbb{Z}$ ,

则
$$a^k = a^{mn} = (a^n)^m = e^m = e$$
.

$$\Longrightarrow$$

若
$$a^k = e$$
,设 $k = mn + t, 0 \leq t < n, m \in \mathbb{Z}$ ,

$$\therefore a^t = a^{k-mn} = a^k * (a^n)^{-m} = e * e^{-m} = e.$$

∴ 
$$n$$
是使 $a^n = e$ 的最小正整数,又 $0 \le t < n$ ,

$$\therefore$$
  $t = 0, k = mn$ .

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群 $< G, *, e > 中, a \in G$ ,

① 若元素a具有有限阶,设|a| = n,  $\therefore (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$ , 则 $a^{-1}$ 也具有有限阶,设为m,则 $m \le n$ , 又 $\therefore a^m = ((a^{-1})^m)^{-1} = e^{-1} = e$ ,  $\therefore n \le n$ 

所以m = n

② 若元素 a 具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群 $< G, *, e > 中, a \in G$ ,

① 若元素a具有有限阶,设|a|=n,  $\therefore (a^{-1})^n=a^{-1\cdot n}=(a^n)^{-1}=e^{-1}=e$ , 则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ , 又 $\therefore a^m=((a^{-1})^m)^{-1}=e^{-1}=e$ , $\therefore n \leq m$ , 所以 m=n

② 若元素 4具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a| = n,  $\therefore (a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$ , 则 $a^{-1}$ 也具有有限阶,设为m,则 $m \le n$ , 又 $\therefore a^m = ((a^{-1})^m)^{-1} = e^{-1} = e$ ,  $\therefore n \le m$ , 所以m = n;

② 若元素 a 具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e,$$
则 $a^{-1}$ 也具有有限阶,设为 $m$ ,则 $m \le n$ ,又 $(a^m)^m = ((a^{-1})^m)^{-1} = e^{-1} = e, (n \le m)$ 所以 $m = n$ :

② 若元素 4具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e,$$

则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ ,

$$\mathbf{X}$$
:  $a^m = ((a^{-1})^m)^{-1} = e^{-1} = e$ , :  $n \leq m$ ,

所以m=n;

② 若元素a具有无限阶、

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$$

则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ ,

**X**: 
$$a^m = ((a^{-1})^m)^{-1} = e^{-1} = e$$
, ∴  $n \leq m$ ,

所以m=n;

② 若元素 3具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

所以、元素。和其逆元有相同的阶。

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群
$$< G, *, e >$$
中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e,$$

则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ ,

$$X: a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, : n \leq m,$$

所以m=n;

② 若元素 3具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e,$$

则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ ,

$$X: a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, : n \leq m,$$

所以m=n;

② 若元素a具有无限阶、

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e,$$

则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ ,

$$\mathbf{X}$$
:  $a^m = ((a^{-1})^m)^{-1} = e^{-1} = e$ , :  $n \leq m$ ,

所以m=n;

② 若元素 具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e,$$

则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ ,

$$\mathbf{X}$$
:  $a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, : n \leq m,$ 

所以m=n;

② 若元素 4 具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ , 即 $a^{-1}$ 也具有无限 阶;

#### 定理

- 群中任一元素和其逆元具有相同的阶。
- 证明:

设群< G, \*, e >中,  $a \in G$ ,

① 若元素a具有有限阶,设|a|=n,

$$(a^{-1})^n = a^{-1 \cdot n} = (a^n)^{-1} = e^{-1} = e$$

则 $a^{-1}$ 也具有有限阶,设为m,则 $m \leq n$ ,

$$\mathfrak{X}$$
:  $a^m = ((a^{-1})^m)^{-1} = e^{-1} = e, : n \leq m,$ 

所以m=n;

② 若元素 具有无限阶,

易证不存在正整数m使得 $(a^{-1})^m = e$ ,即 $a^{-1}$ 也具有无限阶;

#### 定理

- 在有限群 $\langle G, *, e \rangle$ 中,设|G| = n,则任一元素具有有限阶,且阶至多为n.
- 证明:

 $\forall a \in G$ , 在序列 $a, a^2, a^3, ..., a^{n+1}$ 中至少有两个元素相等,不妨设 $a^r = a^s, 1 \le r < s \le n+1$ ,

则  $a^{-r} = a^{-s}$ ,

则  $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$ 

所以,元素a的阶至多为s-r ≤ n.

#### 定理

- 在有限群 $\langle G, *, e \rangle$ 中,设|G| = n,则任一元素具有有限阶,且阶至多为n.
- 证明:

 $\forall a \in G$ , 在序列 $a, a^2, a^3, ..., a^{n+1}$ 中至少有两个元素相等,不妨设 $a^r = a^s, 1 \le r < s \le n+1$ ,

则  $a^{-r} = a^{-s}$ ,

所以,元素a的阶至多为 $s-r \leq n$ .

#### 定理

• 在有限群 $\langle G, *, e \rangle$ 中,设|G| = n,则任一元素具有有限 阶、且阶至多为n.

所以、元素a的阶至多为 $s-r \leq n$ .

● 证明:

 $\forall a \in G$ , 在序列 $a, a^2, a^3, \dots, a^{n+1}$ 中至少有两个元素相等,

#### 定理

- 在有限群 $\langle G, *, e \rangle$ 中,设|G| = n,则任一元素具有有限阶,且阶至多为n.
- 证明:

 $\forall a \in G$ , 在序列 $a, a^2, a^3, ..., a^{n+1}$ 中至少有两个元素相等,不妨设 $a^r = a^s, 1 \le r < s \le n+1$ ,

则  $a^{-r} = a^{-s}$ ,

所以,元素a的阶至多为 $s-r \leq n$ .

#### 定理

- 在有限群 $\langle G, *, e \rangle$ 中,设|G| = n,则任一元素具有有限阶,且阶至多为n.
- 证明:

 $\forall a \in G$ , 在序列 $a, a^2, a^3, ..., a^{n+1}$ 中至少有两个元素相等,不妨设 $a^r = a^s, 1 \le r < s \le n+1$ ,则  $a^{-r} = a^{-s}$ ,

则  $a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$  所以,元素a的阶至多为 $s-r \le n$ .

#### 定理

- 在有限群 $\langle G, *, e \rangle$ 中,设|G| = n,则任一元素具有有限阶,且阶至多为n.
- 证明:

 $\forall a \in G$ , 在序列 $a, a^2, a^3, ..., a^{n+1}$ 中至少有两个元素相等,不妨设 $a^r = a^s, 1 \leqslant r < s \leqslant n+1$ ,

则 
$$a^{-r}=a^{-s}$$
,

$$M \ a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$$

所以,元素a的阶至多为 $s-r \leq n$ .

#### 定理

- 在有限群 $\langle G, *, e \rangle$ 中,设|G| = n,则任一元素具有有限阶,且阶至多为n.
- 证明:

 $\forall a \in G$ , 在序列 $a, a^2, a^3, ..., a^{n+1}$ 中至少有两个元素相等,不妨设 $a^r = a^s, 1 \leqslant r < s \leqslant n+1$ ,则  $a^{-r} = a^{-s}$ ,

则 
$$a^{s-r} = a^s * a^{-r} = a^s * a^{-s} = e$$
  
所以,元素a的阶至多为 $s-r \le n$ .

- 群 < G, \*, e >中,  $a \in G \ |a| = n$ ,则 $|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$ . 特别的, $|a^{-1}| = |a|$ .
- 证明:

- 群< G, \*, e >中, $a \in G \ |a| = n$ ,则 $|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$ . 特别的, $|a^{-1}| = |a|$ .
- 证明:

$$oldsymbol{\mathcal{B}}|a^k|=m$$
,则 $a^{km}=e$ ,  $\therefore n|km$ ,即 $\frac{n}{(k,n)}|\frac{km}{(k,n)}$ ,  $\overline{m}\frac{n}{(k,n)}$  与 $\frac{k}{(k,n)}$  互质,故 $\frac{n}{(k,n)}|m$ ,  $\mathcal{X}$   $\therefore (a^k)^{\frac{n}{(k,n)}}=(a^n)^{\frac{k}{(k,n)}}=e$ ,  $\therefore m|\frac{n}{(k,n)}$   $\mathcal{X}$   $m$ ,  $\frac{n}{(k,n)}\in\mathbb{Z}_+$ ,  $\therefore m=\frac{n}{(k,n)}$ .

- 群< G, \*, e >中, $a \in G |a| = n$ ,则 $|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$ . 特别的, $|a^{-1}| = |a|$ .
- 证明:

$$oldsymbol{\mathcal{U}}|a^k|=m$$
,则 $a^{km}=e$ ,  
 $\therefore n|km$ ,即 $\frac{n}{(k,n)}|\frac{km}{(k,n)}$ ,  
而 $\frac{n}{(k,n)}$ 与 $\frac{k}{(k,n)}$ 互质,故 $\frac{n}{(k,n)}|m$ ,  
又 $\therefore (a^k)^{\frac{n}{(k,n)}}=(a^n)^{\frac{k}{(k,n)}}=e$ ,  
 $\therefore m|\frac{n}{(k,n)}$   
又 $m,\frac{n}{(k,n)}\in\mathbb{Z}_+, \therefore m=\frac{n}{(k,n)}$ .

- 群< G, \*, e >中, $a \in G |a| = n$ ,则 $|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$ . 特别的, $|a^{-1}| = |a|$ .
- 证明:

$$\mathcal{E}|a^{k}| = m$$
,则 $a^{km} = e$ ,  
 $\therefore n|km$ ,即 $\frac{n}{(k,n)}|\frac{km}{(k,n)}$ ,  
而 $\frac{n}{(k,n)}$ 与 $\frac{k}{(k,n)}$ 互质,故 $\frac{n}{(k,n)}|m$ ,  
又 $\therefore (a^{k})^{\frac{n}{(k,n)}} = (a^{n})^{\frac{k}{(k,n)}} = e$ ,  
 $\therefore m|\frac{n}{(k,n)}$   
又 $m$ ,  $\frac{n}{(k,n)} \in \mathbb{Z}_{+}$ ,  $\therefore m = \frac{n}{(k,n)}$ .

- 群< G, \*, e >中, $a \in G |a| = n$ ,则 $|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$ . 特别的, $|a^{-1}| = |a|$ .
- 证明:

$$\mathfrak{X} \cdot (a^k)^{\frac{n}{(k,n)}} = (a^n)^{\frac{k}{(k,n)}} = e,$$

$$\therefore m|_{\frac{n}{(k,n)}}$$

$$\mathbf{X}m, \frac{n}{(k,n)} \in \mathbb{Z}_+, \therefore m = \frac{n}{(k,n)}.$$

- 群 < G, \*, e > 中,  $a \in G$  |a| = n, 则 $|a^k| = \frac{n}{(k,n)}$ ,  $(k \in \mathbb{Z})$ . 特别的,  $|a^{-1}| = |a|$ .
- 证明:

- 群< G, \*, e >中, $a \in G |a| = n$ ,则 $|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$ . 特别的, $|a^{-1}| = |a|$ .
- 证明:

设
$$|a^k|=m$$
,则 $a^{km}=e$ ,  
 $\therefore n|km$ ,即 $\frac{n}{(k,n)}|\frac{km}{(k,n)}$ ,  
而 $\frac{n}{(k,n)}$ 与 $\frac{k}{(k,n)}$ 互质,故 $\frac{n}{(k,n)}|m$ ,  
又 $\therefore (a^k)^{\frac{n}{(k,n)}}=(a^n)^{\frac{k}{(k,n)}}=e$ ,  
 $\therefore m|\frac{n}{(k,n)}$   
又 $m,\frac{n}{(k,n)}\in\mathbb{Z}_+, \therefore m=\frac{n}{(k,n)}$ .

- 群< G, \*, e >中, $a \in G |a| = n$ ,则 $|a^k| = \frac{n}{(k,n)}, (k \in \mathbb{Z})$ . 特别的, $|a^{-1}| = |a|$ .
- 证明:

设
$$|a^k|=m$$
,则 $a^{km}=e$ ,  $\therefore n|km$ ,即 $\frac{n}{(k,n)}|\frac{km}{(k,n)}$ ,  $\frac{n}{(k,n)}$  与 $\frac{k}{(k,n)}$  互质,故 $\frac{n}{(k,n)}|m$ ,又 $\therefore (a^k)^{\frac{n}{(k,n)}}=(a^n)^{\frac{k}{(k,n)}}=e$ , $\therefore m|\frac{n}{(k,n)}$  又 $m$ ,  $\frac{n}{(k,n)}\in\mathbb{Z}_+, \therefore m=\frac{n}{(k,n)}$ .

### 内容

- 1 群的性质
  - 群的性质
  - 元素的阶
- ② 陪集和拉格朗日定理
  - 陪集的定义和性质
  - 拉格朗日定理
  - 陪集关系

### 陪集

### 定义-左陪集(右陪集)

- 设< H, \* > 是群< G, \* > 的子群,
- 集合a\*H ≜ {a\*h|h∈H}为元素a∈G所确定的H的左陪集。
   左陪集a\*H可简记为aH.元素a为左陪集aH的表示元素.
- 集合 $H*a \triangleq \{h*a|h \in H\}$  为元素 $a \in G$ 所确定的H的右陪集。 右陪集H\*a可简记为Ha. 元素a为右陪集Ha的表示元素.

### 陪集

#### 定义-左陪集(右陪集)

- $\mathcal{C} < H, * > \mathcal{E} \not\subset G, * > 0$
- 集合a\*H ≜ {a\*h|h∈H}为元素a∈G所确定的H的左陪集。
   左陪集a\*H可简记为aH. 元素a为左陪集aH的表示元素.
- 集合H\*a = {h\*a|h∈H}为元素a∈G所确定的H的右陪集。
   右陪集H\*a可简记为Ha.元素a为右陪集Ha的表示元素。

### 陪集

#### 定义-左陪集(右陪集)

- 设< H, \* > 是群< G, \* > 的子群,
- 集合a\*H ≜ {a\*h|h∈H}为元素a∈G所确定的H的左陪集。
   左陪集a\*H可简记为aH.元素a为左陪集aH的表示元素.
- 集合H\*a ≜ {h\*a|h∈H}为元素a∈G所确定的H的右陪集。
   右陪集H\*a可简记为Ha.元素a为右陪集Ha的表示元素。

### 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, ($$
 $\mathring{k}$ 

$$\left(\begin{array}{ccc}
1 & 2 & 3 \\
1 & 3 & 2
\end{array}\right), \left(\begin{array}{ccc}
1 & 2 & 3 \\
3 & 2 & 1
\end{array}\right), \left(\begin{array}{ccc}
1 & 2 & 3 \\
2 & 1 & 3
\end{array}\right) (3)$$

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ ,  $H = \{I, d\}$ 是群 $S_3$ 的一个子群。

- $\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$   $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$   $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$   $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合 $\{[I, d], \{a, c\}, \{b, a^2\}\}$

## 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} \lambda \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
(翻转)

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ ,  $H = \{\mathbb{I}, d\}$ 是群 $S_3$ 的一个子群。

- $\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$   $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$   $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$   $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合{{I, d}, {a, c}, {b, a²}}

### 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} \lambda \xi \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} \lambda \xi \end{pmatrix}$$

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ ,  $H = \{\mathbb{I}, d\}$ 是群 $S_3$ 的一个子群。

- $\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$   $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$   $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$   $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合 $\{[I, d], \{a, c\}, \{b, a^2\}\}$

### 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ , $H = \{I, d\}$ 是群 $S_3$ 的一个子群。

- $\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$   $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$
- $cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$   $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$
- $bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$   $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$
- H的所有左陪集组成的集合 $\{[I,d],\{a,c\},\{b,a^2\}\}$

### 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} \lambda \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} \lambda \end{pmatrix} \begin{pmatrix} \lambda \end{pmatrix}$$

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ , $H = \{I, d\}$ 是群 $S_3$ 的一个子群。

### H的所有的左陪集为:

• 
$$\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$$
  $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$ 

• 
$$cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$$
  $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$ 

• 
$$bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$$
  $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$ 

• H的所有左陪集组成的集合 $\{[I, d], \{a, c\}, \{b, a^2\}\}$ 

### 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} \lambda \end{pmatrix}, \begin{pmatrix} \lambda \end{pmatrix} \right\}$$

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ ,  $H = \{\mathbb{I}, d\}$ 是群 $S_3$ 的一个子群。

### H的所有的左陪集为:

• 
$$\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$$
  $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$ 

• 
$$cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$$
  $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$ 

• 
$$bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$$
  $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$ 

• H的所有左陪集组成的集合 $\{[I,d],\{a,c\},\{b,a^2\}\}$ 

### 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\triangleq \left\{ \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \right\}$$

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ , $H = \{I, d\}$ 是群 $S_3$ 的一个子群。

### H的所有的左陪集为:

• 
$$\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$$
  $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$ 

• 
$$cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$$
  $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$ 

• 
$$bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$$
  $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$ 

● H的所有左陪集组成的集合{{I, d}, {a, c}, {b, a²}}

### 例 S3的左陪集

• 
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, ($$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, ($$

 $\triangleq \{\mathbb{I}, a, a^2, b, c, d\};$ 

• 3次对称群 $\langle S_3, \circ \rangle$ , $H = \{\mathbb{I}, d\}$ 是群 $S_3$ 的一个子群。

### H的所有的左陪集为:

• 
$$\mathbb{I}H = {\mathbb{I} \circ \mathbb{I}, \mathbb{I} \circ d} = {\mathbb{I}, d}$$
  $dH = {d \circ \mathbb{I}, d \circ d} = {d, \mathbb{I}}$ 

• 
$$cH = \{c \circ \mathbb{I}, c \circ d\} = \{c, a\}$$
  $aH = \{a \circ \mathbb{I}, a \circ d\} = \{a, c\}$ 

• 
$$bH = \{b \circ \mathbb{I}, b \circ d\} = \{b, a^2\}$$
  $a^2H = \{a^2 \circ \mathbb{I}, a^2 \circ d\} = \{a^2, b\}$ 

• H的所有左陪集组成的集合 $\{[I,d],\{a,c\},\{b,a^2\}\}$ 

### H的所有的右陪集为:

- $\bullet \ H\mathbb{I} = \{\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}\} = \{\mathbb{I}, d\} \quad Hd = \{\mathbb{I} \circ d, d \circ d\} = \{d, \mathbb{I}\}$
- $Hc = {\mathbb{I} \circ c, d \circ c} = {c, a^2}$   $Ha^2 = {\mathbb{I} \circ a^2, d \circ a^2} = {a^2, c}$
- $Hb = \{ \mathbb{I} \circ b, d \circ b \} = \{ b, a \}$   $Ha = \{ \mathbb{I} \circ a, d \circ a \} = \{ a, b \}$

- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- H的所有左陪集组成的集合{{I, d}, {a, c}, {b, a²}}

### H的所有的右陪集为:

- $H\mathbb{I} = {\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}} = {\mathbb{I}, d}$   $Hd = {\mathbb{I} \circ d, d \circ d} = {d, \mathbb{I}}$
- $Hc = {\mathbb{I} \circ c, d \circ c} = {c, a^2}$   $Ha^2 = {\mathbb{I} \circ a^2, d \circ a^2} = {a^2, c}$
- $Hb = {\mathbb{I} \circ b, d \circ b} = {b, a}$   $Ha = {\mathbb{I} \circ a, d \circ a} = {a, b}$

- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- H的所有左陪集组成的集合 $\{\{I, d\}, \{a, c\}, \{b, a^2\}\}$

### H的所有的右陪集为:

- $H\mathbb{I} = {\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}} = {\mathbb{I}, d}$   $Hd = {\mathbb{I} \circ d, d \circ d} = {d, \mathbb{I}}$
- $Hc = {\mathbb{I} \circ c, d \circ c} = {c, a^2}$   $Ha^2 = {\mathbb{I} \circ a^2, d \circ a^2} = {a^2, c}$
- $Hb = {\mathbb{I} \circ b, d \circ b} = {b, a}$   $Ha = {\mathbb{I} \circ a, d \circ a} = {a, b}$

- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- H的所有左陪集组成的集合 $\{\{I, d\}, \{a, c\}, \{b, a^2\}\}$

### H的所有的右陪集为:

- $H\mathbb{I} = {\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}} = {\mathbb{I}, d}$   $Hd = {\mathbb{I} \circ d, d \circ d} = {d, \mathbb{I}}$
- $Hc = {\mathbb{I} \circ c, d \circ c} = {c, a^2}$   $Ha^2 = {\mathbb{I} \circ a^2, d \circ a^2} = {a^2, c}$
- $Hb = {\mathbb{I} \circ b, d \circ b} = {b, a}$   $Ha = {\mathbb{I} \circ a, d \circ a} = {a, b}$

- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- H的所有左陪集组成的集合{{I, d}, {a, c}, {b, a²}}

### H的所有的右陪集为:

- $H\mathbb{I} = {\mathbb{I} \circ \mathbb{I}, d \circ \mathbb{I}} = {\mathbb{I}, d}$   $Hd = {\mathbb{I} \circ d, d \circ d} = {d, \mathbb{I}}$
- $Hc = {\mathbb{I} \circ c, d \circ c} = {c, a^2}$   $Ha^2 = {\mathbb{I} \circ a^2, d \circ a^2} = {a^2, c}$
- $Hb = {\mathbb{I} \circ b, d \circ b} = {b, a}$   $Ha = {\mathbb{I} \circ a, d \circ a} = {a, b}$

- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- H的所有左陪集组成的集合 $\{[I,d],\{a,c\},\{b,a^2\}\}$

### 定理

- 设< H,\* >是群< G,\* >的子群, aH和bH是任意两个左陪集, 则aH = bH, 或 $aH \cap bH = \emptyset$ .
- 证:

```
设aH \cap bH \neq \emptyset,则∃f \in aH \cap bH,
∴ ∃h_1, h_2 \in H,使得f = a*h_1 = b*h_2, ∴ a = b*h_2*h_1^{-1}
(证明aH \subseteq bH)
```

 $\because \forall x \in aH, \exists h \in H, \ x = a * h, \ , \ p x = b * h_2 * h_1^{-1} * h, \ \because H$ 是子群, $\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$  同理可证, $bH \subseteq aH$ ,paH = bH 或 $aH \cap bH = \emptyset$ 

- 设< H,\* >是群< G,\* >的子群, aHabH是任意两个左陪集, MaH = bH,  $A = \emptyset$ .
- 证:

### 定理

- 设< H,\* >是群< G,\* >的子群, aHnbH是任意两个左陪集, 则aH = bH, 或 $aH \cap bH = \emptyset$ .
- 证:

 $\boldsymbol{\mathcal{C}}_{a}H \cap bH \neq \emptyset, \, \, \boldsymbol{\mathcal{M}} \exists f \in aH \cap bH,$ 

∵∃h1, h2 ∈ H,使得f = a \* h1 = b \* h2, ∴ a = b \* h2 \* h11 (证明aH ⊆ bH)

 $\because \forall x \in aH, \exists h \in H, \ x = a * h, \ , \ ppx = b * h_2 * h_1^{-1} * h,$   $\because H$ 是子群, $\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$ 同理可证, $bH \subseteq aH$ ,ppaH = bH.

则aH = bH,或 $aH \cap bH = \varnothing$ .

### 定理

- 设< H,\* >是群< G,\* >的子群, aH和bH是任意两个左陪集, 则aH = bH, 或 $aH \cap bH = \emptyset$ .
- 证:

 $\boldsymbol{\mathcal{C}}_{a}H \cap bH \neq \emptyset, \, \, \boldsymbol{\mathcal{M}}\exists f \in aH \cap bH,$ 

 $\therefore \exists h_1, h_2 \in H$ ,使得 $f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$ (证明 $aH \subseteq bH$ )

 $\because \forall x \in aH, \exists h \in H, \ x = a * h, \ , \ ppx = b * h_2 * h_1^{-1} * h,$   $\because H$ 是子群, $\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$ 同理可证, $bH \subseteq aH$ ,ppaH = bH.

### 定理

- 设< H,\* >是群< G,\* >的子群, aH和bH是任意两个左陪集, 则aH = bH, 或 $aH \cap bH = \emptyset$ .
- 证:

 $\therefore \exists h_1, h_2 \in H$ ,使得 $f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$ (证明 $aH \subseteq bH$ )

 $\therefore \forall x \in aH, \exists h \in H, \ x = a * h, \ , \ \mathbb{P} x = b * h_2 * h_1^{-1} * h, \ \therefore H$ 是子群, $\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$  同理可证, $bH \subseteq aH$ , $\mathbb{P} aH = bH$ . 则aH = bH. 或 $aH \cap bH = \emptyset$ .

### 定理

- 设< H,\* >是群< G,\* >的子群, aHabH是任意两个左陪集, 则aH = bH, 或 $aH \cap bH = \emptyset$ .
- 证:

 $\therefore \exists h_1, h_2 \in H$ ,使得 $f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$ (证明 $aH \subseteq bH$ )

 $\because \forall x \in aH, \exists h \in H, \ x = a * h, \ , \ \mathbf{p}x = b * h_2 * h_1^{-1} * h,$   $\because H$ 是子群,  $\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$ 同理可证,  $bH \subseteq aH$ ,  $\mathbf{p}aH = bH$ .

### 定理

- 设< H,\* >是群< G,\* >的子群, aHabH是任意两个左陪集, 则aH = bH, 或 $aH \cap bH = \emptyset$ .
- 证:

设 $aH \cap bH \neq \emptyset$ ,则 $\exists f \in aH \cap bH$ ,

- $\therefore \exists h_1, h_2 \in H$ ,使得 $f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$ (证明 $aH \subseteq bH$ )
- $\therefore \forall x \in aH, \exists h \in H, \ x = a * h, \ , \ \mathsf{EP} x = b * h_2 * h_1^{-1} * h,$
- $\therefore$  H是子群, $\therefore$   $h_2*h_1^{-1}*h\in H, \therefore$   $x\in bH, \therefore$   $aH\subseteq bH$ .
- 同理可证,  $bH \subseteq aH$ , paH = bH.
- 则aH = bH, 或 $aH \cap bH = \emptyset$ .

### 定理

- 设< H,\*>是群< G,\*>的子群, aH和bH是任意两个左陪集,则aH=bH,或aH∩bH=∅.
- 证:

- $\therefore \exists h_1, h_2 \in H$ ,使得 $f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$ (证明 $aH \subseteq bH$ )
- $\because \forall x \in aH, \exists h \in H, \ x = a * h, \ , \ \mathbf{p}x = b * h_2 * h_1^{-1} * h,$   $\because H$ 是子群,  $\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH.$
- い 「大丁料,  $:: n_2 * n_1 * n \in n, :: X \in Dn, :: an \subseteq Dn$

同理可证,  $bH \subseteq aH$ , paH = bH.

则aH = bH, 或 $aH \cap bH = \emptyset$ 

### 定理

- 设< H,\*>是群< G,\*>的子群, aH和bH是任意两个左陪集,则aH=bH,或aH∩bH=∅.
- 证:

- $\therefore \exists h_1, h_2 \in H$ ,使得 $f = a * h_1 = b * h_2, \therefore a = b * h_2 * h_1^{-1}$ (证明 $aH \subseteq bH$ )
- $\forall x \in aH, \exists h \in H, \ x = a * h, \ , \ \mathbb{P} x = b * h_2 * h_1^{-1} * h,$
- $\therefore$  H是子群,  $\therefore h_2 * h_1^{-1} * h \in H, \therefore x \in bH, \therefore aH \subseteq bH$ .

同理可证,  $bH \subseteq aH$ , paH = bH.

则aH = bH, 或 $aH \cap bH = \emptyset$ .

- 设< H, \* >是群< G, \* >的子群,则 $G = \bigcup aH$ .
- 证:

$$(1) \ G \subseteq \bigcup_{a \in G} aH$$

$$: H \leqslant G, : e \in H,$$

$$orall a \in G, \ a = a * e \in aH, \$$
所以 $G \subseteq \bigcup_{i \in G} aH;$ 

(2) 
$$\bigcup_{a \in G} aH \subseteq G$$

$$\forall a \in G, \forall h \in H, \ a * h \in G, \therefore aH \subseteq G$$

$$\therefore \bigcup aH \subseteq G$$

- $\mathcal{U} < H, * > \mathcal{E} \mathcal{A} < G, * > \mathsf{OPP} \mathcal{A}$ ,  $\mathcal{M} G = \bigcup_{a \in \mathcal{A}} \mathcal{A} \mathcal{A}$ .
- 证:

(1) 
$$G \subseteq \bigcup_{a \in G} aH$$
  
 $\because H \leqslant G, \therefore e \in H,$   
 $\forall a \in G, \ a = a * e \in aH, 所以 $G \subseteq \bigcup_{a \in G} aH$$ 

(2) 
$$\bigcup_{a \in G} aH \subseteq G$$
  
 $\forall a \in G, \forall h \in H, \ a * h \in G, \therefore aH \subseteq G$   
 $\therefore \bigcup_{a \in G} aH \subseteq G$ 

### 定理

- $\mathcal{U} < H, * > \mathcal{E} \mathcal{A} < G, * > \mathsf{OPP} \mathcal{A}$ ,  $\mathcal{M} G = \bigcup_{a \in \mathcal{A}} \mathcal{A} \mathcal{A}$ .
- 证:

$$(1) \ \ G \subseteq \bigcup_{a \in G} aH$$

$$\therefore H \leqslant G, \therefore e \in H$$

$$\forall a \in G, \ a = a * e \in aH, \$$
所以 $G \subseteq \bigcup_{a \in G} aH;$ 

(2) 
$$\bigcup aH \subseteq G$$

 $\forall a \in G, \forall h \in H, \ a * h \in G, :: aH \subseteq G$ 

$$\therefore \bigcup aH \subseteq G$$

- 设< H, \* >是群< G, \* >的子群,则 $G = \bigcup_{a \in G} aH$ .
- 证:

(1) 
$$G \subseteq \bigcup_{a \in G} aH$$
  
 $\therefore H \leqslant G, \therefore e \in H,$   
 $\forall a \in G, \ a = a * e \in aH,$  所以 $G \subseteq \bigcup_a H$ 

(2) 
$$\bigcup_{a \in G} aH \subseteq G$$
  
 $\forall a \in G, \forall h \in H, \ a * h \in G, \therefore aH \subseteq G$   
 $\therefore \bigcup_{a} aH \subseteq G$ 

- 设< H, \* >是群< G, \* >的子群,则 $G = \bigcup_{a \in G} aH$ .
- 证:

(1) 
$$G \subseteq \bigcup_{a \in G} aH$$
  
 $\therefore H \leqslant G, \therefore e \in H,$   
 $\forall a \in G, \ a = a * e \in aH, \ 所以 $G \subseteq \bigcup_{a \in G} aH;$$ 

(2) 
$$\bigcup_{a \in G} aH \subseteq G$$
  
 $\forall a \in G, \forall h \in H, \ a * h \in G, \therefore aH \subseteq G$   
 $\therefore \bigcup_{a \in G} aH \subseteq G$ 

- 设< H, \* >是群< G, \* >的子群,则 $G = \bigcup_{a \in G} aH$ .
- 证:

(1) 
$$G \subseteq \bigcup_{a \in G} aH$$
  
 $\therefore H \leqslant G, \therefore e \in H,$   
 $\forall a \in G, \ a = a * e \in aH, \ 所以G \subseteq \bigcup_{a \in G} aH;$ 

(2) 
$$\bigcup_{a \in G} aH \subseteq G$$
  
 $\forall a \in G, \forall h \in H, \ a * h \in G, : aH \subseteq G$   
 $\therefore \bigcup_{a} aH \subseteq G$ 

- 设< H, \* >是群< G, \* >的子群,则 $G = \bigcup_{a \in G} aH$ .
- 证:

(1) 
$$G \subseteq \bigcup_{a \in G} aH$$
  
 $\therefore H \leqslant G, \therefore e \in H,$   
 $\forall a \in G, \ a = a * e \in aH, \ 所以G \subseteq \bigcup_{a \in G} aH;$ 

(2) 
$$\bigcup_{a \in G} aH \subseteq G$$
  
 $\forall a \in G, \forall h \in H, \ a * h \in G, \therefore aH \subseteq G,$   
 $\therefore \bigcup_{a \in G} aH \subseteq G$ 

- 设< H, \* >是群< G, \* >的子群,则 $G = \bigcup_{a \in G} aH$ .
- 证:

(1) 
$$G \subseteq \bigcup_{a \in G} aH$$
  
 $\therefore H \leqslant G, \therefore e \in H,$   
 $\forall a \in G, \ a = a * e \in aH, \ 所以 $G \subseteq \bigcup_{a \in G} aH;$$ 

(2) 
$$\bigcup_{a \in G} aH \subseteq G$$
  
 $\forall a \in G, \forall h \in H, \ a * h \in G, \therefore aH \subseteq G,$   
 $\therefore \bigcup_{a \in G} aH \subseteq G$ 

### 定理

- 设< H,\*>是群< G,\*>的子群, H的任意的陪集的大小 (基数) 是相等的。
- 证:

设a是群G中的任一元素, $h_1, h_2$ 是子群H中的元素,若 $h_1 \neq h_2$ ,则 $a * h_1 \neq a * h_2$ (消去律)。

所以,aH中没有相同的元素,即aH和H的基数一样,且H的 所有陪集基数相等。

 $\mathbb{R}P \forall a \in G, |aH| = |Ha| = |H|.$ 

#### 定理

- 设< H,\*>是群< G,\*>的子群, H的任意的陪集的大小 (基数) 是相等的。
- 证:

设a是群G中的任一元素, $h_1, h_2$ 是子群H中的元素,若 $h_1 \neq h_2$ ,则 $a*h_1 \neq a*h_2$ (消去律)。

所以,aH中没有相同的元素,即aH和H的基数一样,且H的 所有陪集基数相等。

 $\operatorname{\mathfrak{P}}\forall a\in \mathit{G},\ |aH|=|Ha|=|H|.$ 

### 定理

- 设< H,\*>是群< G,\*>的子群, H的任意的陪集的大小 (基数) 是相等的。
- 证:

设a是群G中的任一元素, $h_1, h_2$ 是子群H中的元素,

所以,aH中没有相同的元素,即aH和H的基数一样,且H的 所有陪集基数相等。

 $\operatorname{\mathfrak{P}} \forall a \in G, \ |aH| = |Ha| = |H|.$ 

### 定理

- 设< H,\*>是群< G,\*>的子群, H的任意的陪集的大小 (基数) 是相等的。
- 证:

设a是群G中的任一元素, $h_1$ ,  $h_2$ 是子群H中的元素,若 $h_1 \neq h_2$ ,则 $a*h_1 \neq a*h_2$ (消去律)。

所以,aH中没有相同的元素,即aH和H的基数一样,且H的 所有陪集基数相等。

 $\operatorname{\mathfrak{PP}} \forall a \in \mathit{G}, \ |aH| = |Ha| = |H|.$ 

#### 定理

- 设< H,\*>是群< G,\*>的子群, H的任意的陪集的大小 (基数) 是相等的。
- 证:

设a是群G中的任一元素, $h_1,h_2$ 是子群H中的元素,若 $h_1 \neq h_2$ ,则 $a*h_1 \neq a*h_2$ (消去律)。 所以,aH中没有相同的元素,即aH和H的基数一样,且H的所有陪集基数相等。

 $\operatorname{\mathfrak{PP}} \forall a \in \mathit{G}, \ |aH| = |Ha| = |H|.$ 

### 定理

- 设< H,\*>是群< G,\*>的子群, H的任意的陪集的大小 (基数) 是相等的。
- 证:

设a是群G中的任一元素, $h_1, h_2$ 是子群H中的元素,若 $h_1 \neq h_2$ ,则 $a * h_1 \neq a * h_2$ (消去律)。

所以,aH中没有相同的元素,即aH和H的基数一样,且H的 所有陪集基数相等。

 $\operatorname{\mathfrak{P}} \forall a \in \mathit{G}, \ |aH| = |Ha| = |H|.$ 

#### 定理

设< H, \* >是群< G, \* >的子群,

- aH和bH是任意两个左陪集,则aH = bH,或aH∩bH = Ø.
- $G = \bigcup_{a \in G} aH$ . (所有左陪集的并集即为G)
- H的任意两个陪集的大小相等, 都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且, 划分中的块 (即各个左陪集) 的大小相等。
- 即: G的大小=左陪集的个数×H的大小

#### 定理

设< H, \* >是群< G, \* >的子群,

- aH和bH是任意两个左陪集,则aH = bH,或aH∩bH = Ø.
- $G = \bigcup_{a \in G} aH$ . (所有左陪集的并集即为G)
- H的任意两个陪集的大小相等,都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且, 划分中的块 (即各个左陪集) 的大小相等。
- 即: G的大小=左陪集的个数×H的大小

#### 定理

设< H, \* >是群< G, \* >的子群,

- aH和bH是任意两个左陪集,则aH = bH,或aH∩bH = Ø.
- $G = \bigcup_{a \in G} aH$ . (所有左陪集的并集即为G)
- H的任意两个陪集的大小相等, 都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且, 划分中的块 (即各个左陪集) 的大小相等。
- 即: G的大小=左陪集的个数×H的大小

#### 定理

设< H, \* >是群< G, \* >的子群,

- aH和bH是任意两个左陪集,则aH = bH,或aH∩bH = Ø.
- $G = \bigcup_{a \in G} aH$ . (所有左陪集的并集即为G)
- H的任意两个陪集的大小相等,都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且, 划分中的块 (即各个左陪集) 的大小相等。
- 即: G的大小=左陪集的个数×H的大小

#### 定理

设< H.\*>是群< G.\*>的子群、

- aH和bH是任意两个左陪集、则aH = bH、或aH∩bH = Ø.
- $G = \bigcup aH.$  (所有左陪集的并集即为G)  $a \in G$
- H的任意两个陪集的大小相等、都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且、划分中的块(即各个左陪集)的大小相等。

#### 定理

设< H, \* >是群< G, \* >的子群,

- aH和bH是任意两个左陪集,则aH = bH,或aH∩bH = Ø.
- $G = \bigcup_{a \in G} aH$ . (所有左陪集的并集即为G)
- H的任意两个陪集的大小相等, 都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且, 划分中的块 (即各个左陪集) 的大小相等。
- 即: G的大小=左陪集的个数×H的大小

#### 定理

设< H, \* >是群< G, \* >的子群,

- aH和bH是任意两个左陪集,则aH = bH,或aH∩bH = Ø.
- $G = \bigcup_{a \in G} aH$ . (所有左陪集的并集即为G)
- H的任意两个陪集的大小相等, 都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且, 划分中的块 (即各个左陪集) 的大小相等。
- 即: G的大小=左陪集的个数×H的大小

#### 定理

设< H, \* >是群< G, \* >的子群,

- aH和bH是任意两个左陪集,则aH = bH,或aH∩bH = Ø.
- $G = \bigcup_{a \in G} aH$ . (所有左陪集的并集即为G)
- H的任意两个陪集的大小相等,都等于H的大小。
- H的左、右陪集的个数相等。(Th8.5.3)

- H的所有左陪集集合,构成G的一个划分;
- 并且, 划分中的块 (即各个左陪集) 的大小相等。
- 即: G的大小=左陪集的个数×H的大小

## Lagrange定理

#### 定理

- 引入记号[G:H]:设<H,\*>是群<G,\*>的子群,称H的左
   (右)陪集的个数为H在G中的指数,记为[G:H].
- Lagrange定理 设< H,\*>是有限群< G,\*>的子群,则
   |H|整除|G|,且|G|=|H|⋅[G:H]

#### 注意

• 注意: Lagrange定理的逆定理不成立。即,如果|G|=n, m整除n,则阶为m的子群未必存在。但是,对于循环群却成立。

# Lagrange定理

#### 定理

- 引入记号[G: H]: 设< H,\*>是群< G,\*>的子群, 称H的左
   (右) 陪集的个数为H在G中的指数,记为[G: H].
- Lagrange定理 设< H,\*>是有限群< G,\*>的子群,则
   |H|整除|G|,且|G|=|H|⋅[G:H]

#### 注意

• 注意: Lagrange定理的逆定理不成立。即,如果|G|=n,m整除n,则阶为m的子群未必存在。但是,对于循环群却成立。

# Lagrange定理

#### 定理

- 引入记号[G: H]: 设< H,\*>是群< G,\*>的子群, 称H的左
   (右) 陪集的个数为H在G中的指数,记为[G: H].
- Lagrange定理 设< H,\*>是有限群< G,\*>的子群,则
   |H|整除|G|,且|G|=|H|⋅[G:H]

### 注意

• 注意: Lagrange定理的逆定理不成立。即,如果|G|=n,m整除n,则阶为m的子群未必存在。但是,对于循环群却成立。

#### 推论

● 在有限群G中,每个元素的阶能整除|G|.

```
证: 设a \in G, |a| = r, 则a^r = e. \{e, a, a^2, a^3, \dots, a^{r-1}\}, *> \mathcal{L} < G, *> 的子群, 即< a > \le G, \therefore |< a > |整除|G|, 即|a|整除|G|.
```

### 推论

• 质数阶段群必为循环群。

证: 设
$$|G| = p$$
,  $p$ 是质数,  $\forall a \in G$ ,  $|a|$ 整除 $p$ ,  $\exists a \neq e$ , 则 $|a| = p$ , 设 $H = \{e, a, a^2, ......, a^{p-1}\}$ ,  $< H, * >$ 构成群,则 $H \le G$ ,  $|H| = p$ , 即 $G = H = < a >$ .

### 推论

● 在有限群G中,每个元素的阶能整除 G.

证:设 $a \in G$ , |a| = r, 则 $a^r = e$ .

### 推论

• 质数阶段群必为循环群。

证:设
$$|G| = p$$
,  $p$ 是质数, $\forall a \in G$ ,  $|a|$ 整除 $p$ , 若 $a \neq e$ , 则 $|a| = p$ , 设 $H = \{e, a, a^2, ......, a^{p-1}\}$ ,  $< H, * >$ 构成群,则 $H \leqslant G$ ,  $|H| = p$ , 即 $G = H = < a >$ .

### 推论

● 在有限群G中,每个元素的阶能整除|G|.

证: 设
$$a \in G$$
,  $|a| = r$ , 则 $a^r = e$ .  $< \{e, a, a^2, a^3, \dots, a^{r-1}\}, *> \mathcal{E} < G, *> 的子群,$  即 $< a > < G, : | < a > |$  整除 $|G|$ , 即 $|a|$  整除 $|G|$ .

### 推论

• 质数阶段群必为循环群。

证:设
$$|G| = p$$
,  $p$ 是质数, $\forall a \in G$ ,  $|a|$ 整除 $p$ , 若 $a \neq e$ ,则 $|a| = p$ , 设 $H = \{e, a, a^2, ......, a^{p-1}\}$ ,  $< H, * >$ 构成群,则 $H \le G$ ,  $|H| = p$ , 即 $G = H = < a >$ .

### 推论

● 在有限群G中,每个元素的阶能整除 G.

证: 设
$$a \in G$$
,  $|a| = r$ , 则 $a^r = e$ .  $< \{e, a, a^2, a^3, \dots, a^{r-1}\}, *> \mathcal{E} < G, *>$ 的子群,  $P < a > \leqslant G$ , ∴  $| < a > |$  整除 $|G|$ ,  $|P| = a$  整除 $|G|$ .

### 推论

• 质数阶段群必为循环群。

证: 设
$$|G| = p$$
,  $p$ 是质数,  $\forall a \in G$ ,  $|a|$ 整除 $p$ ,  $\exists a \neq e$ , 则 $|a| = p$ , 设 $H = \{e, a, a^2, ......, a^{p-1}\}$ ,  $< H, * >$ 构成群,则 $H \le G$ ,  $|H| = p$ , 即 $G = H = < a >$ .

### 推论

• 在有限群G中,每个元素的阶能整除 G.

证: 设
$$a \in G$$
,  $|a| = r$ , 则 $a^r = e$ .  $\{e, a, a^2, a^3, \dots, a^{r-1}\}, *> \mathbb{E} \{G, *> \mathbf{6}\}$  即 $\{a > \{G, \dots, a^r\}, *> \mathbb{E} \{G, *> \mathbf{6}\}\}$  [G].

### 推论

• 质数阶段群必为循环群。

证: 设
$$|G| = p$$
,  $p$ 是质数,  $\forall a \in G$ ,  $|a|$ 整除 $p$ , 若 $a \neq e$ , 则 $|a| = p$ , 设 $H = \{e, a, a^2, ......, a^{p-1}\}$ ,  $< H, * >$ 构成群,则 $H \le G$ ,  $|H| = p$ , 即 $G = H = < a >$ .

#### 推论

● 在有限群G中,每个元素的阶能整除 G.

证: 设
$$a \in G$$
,  $|a| = r$ , 则 $a^r = e$ .  $\{e, a, a^2, a^3, \dots, a^{r-1}\}, *> \mathbb{E} \{G, *> \mathbf{6}\}$  即 $\{a > \{G, \dots, a^r\}, *> \mathbb{E} \{G, *> \mathbf{6}\}\}$  [G].

### 推论

• 质数阶段群必为循环群。

证:设
$$|G| = p$$
,  $p$ 是质数, $\forall a \in G$ ,  $|a|$ 整除 $p$ ,  $\exists a \neq e$ ,  $y \mid a| = p$ , 设 $y \mid a| = p$ , 设 $y \mid a| = p$ ,  $y \mid a| = p$ ,

### 推论

● 在有限群G中,每个元素的阶能整除|G|.

证: 设
$$a \in G$$
,  $|a| = r$ , 则 $a^r = e$ .  $\{e, a, a^2, a^3, \dots, a^{r-1}\}, *> \mathcal{E} < G, *>$ 的子群,  $p < a > \leqslant G$ ,  $\therefore |a| \leq a > |a|$  整除 $|G|$ ,  $p |a|$  整除 $|G|$ .

### 推论

• 质数阶段群必为循环群。

证: 设
$$|G| = p$$
,  $p$ 是质数,  $\forall a \in G$ ,  $|a|$ 整除 $p$ ,  $\exists a \neq e$ , 则 $|a| = p$ , 设 $H = \{e, a, a^2, ....., a^{p-1}\}$ ,

< H,\*>构成群,则H≤G, |H|=p,即G=H=<a>.

### 推论

● 在有限群G中,每个元素的阶能整除 G.

证: 设
$$a \in G$$
,  $|a| = r$ , 则 $a^r = e$ .  
  $< \{e, a, a^2, a^3, \dots, a^{r-1}\}, *>$ 是 $< G, *>$ 的子群, 即 $< a>$  $\le G$ ,  $\therefore |< a> |$  整除 $|G|$ , 即 $|a|$  整除 $|G|$ .

### 推论

• 质数阶段群必为循环群。

证:设
$$|G| = p$$
,  $p$ 是质数, $\forall a \in G$ ,  $|a|$ 整除 $p$ , 若 $a \neq e$ ,则 $|a| = p$ , 设 $H = \{e, a, a^2, ......, a^{p-1}\}$ ,  $< H, * >$ 构成群,则 $H \leqslant G$ ,  $|H| = p$ , 即 $G = H = < a >$ .

### 推论

● 在有限群 G中,每个元素的阶能整除 G.

证: 设
$$a \in G$$
,  $|a| = r$ , 则 $a^r = e$ .  
 $\{e, a, a^2, a^3, \dots, a^{r-1}\}, *> \mathbb{E} \{G, *> \mathbf{6} \}$  即 $\{a > \{G, \dots, a^r\}, *> \mathbb{E} \{G, *> \mathbf{6} \}$  即 $\{a > \{G, \dots, a^r\}, *> \mathbb{E} \{G, \dots, a^r\},$ 

### 推论

• 质数阶段群必为循环群。

证:设
$$|G| = p$$
,  $p$ 是质数, $\forall a \in G$ ,  $|a|$ 整除 $p$ , 若 $a \neq e$ , 则 $|a| = p$ , 设 $H = \{e, a, a^2, ......, a^{p-1}\}$ ,  $< H, * >$ 构成群,则 $H \leqslant G$ ,  $|H| = p$ , 即 $G = H = < a >$ .

# 左(右) 陪集关系

#### 陪集等价关系

设< H, \* >是群< G, \* >的子群,

- H的所有左(右) 陪集的集合是G的一个划分;
- 由这个划分可以诱导出一个G上的等价关系,称之为子群 H的左(右) 陪集等价关系;
- 这个等价关系的每一个等价类就是H的一个左(右) 陪集。

# 左(右) 陪集关系

#### 陪集等价关系

设< H, \* >是群< G, \* >的子群,

- H的所有左(右) 陪集的集合是G的一个划分;
- 由这个划分可以诱导出一个G上的等价关系,称之为子群 H的左(右) 陪集等价关系;
- 这个等价关系的每一个等价类就是H的一个左(右)陪集。

# 左(右) 陪集关系

#### 陪集等价关系

设< H, \* >是群< G, \* >的子群,

- H的所有左(右) 陪集的集合是G的一个划分;
- 由这个划分可以诱导出一个G上的等价关系,称之为子群 H的左(右) 陪集等价关系;
- 这个等价关系的每一个等价类就是H的一个左(右)陪集。

### 左陪集关系

- $\mathcal{C} < H, * > \mathcal{E} \not = \langle G, * \rangle$  **6**  $\mathcal{C} < H, * \rangle$  **7**  $\mathcal{C} < H, * \rangle$  **8**  $\mathcal{C} < H, * \rangle$  **9**  $\mathcal{C} < H, * \rangle$  **1**  $\mathcal{C} < H, * \rangle$  **1**  $\mathcal{C} < H, * \rangle$  **1**  $\mathcal{C} < H, * \rangle$  **2**  $\mathcal{C} < H, * \rangle$  **3**  $\mathcal{C} < H, * \rangle$  **4**  $\mathcal{C} < H, * \rangle$  **5**  $\mathcal{C} < H, * \rangle$  **6**  $\mathcal{C} < H, * \rangle$  **7**  $\mathcal{C} < H, * \rangle$  **9**  $\mathcal{C} < H$
- 证:  $x \in aH \iff \exists h \in H, \ x = a * h \iff \exists h = a^{-1} * x \in H,$  因此,  $\forall x, \ x \in aH \iff a^{-1} * x \in H.$
- 描述了左陪集aH中的元素x。

- 同理 $\forall x, x \in Ha \iff x * a^{-1} \in H$ .
- 描述右陪集Ha中的元素x。

#### 左陪集关系

- $\mathbf{i}\mathbf{x}: \mathbf{x} \in \mathbf{a}\mathbf{H} \iff \exists \mathbf{h} \in \mathbf{H}, \mathbf{x} = \mathbf{a} * \mathbf{h} \iff \exists \mathbf{h} = \mathbf{a}^{-1} * \mathbf{x} \in \mathbf{H},$   $\mathbf{B}\mathbf{k}, \forall \mathbf{x}. \mathbf{x} \in \mathbf{a}\mathbf{H} \iff \mathbf{a}^{-1} * \mathbf{x} \in \mathbf{H}.$
- 描述了左陪集aH中的元素x。

- 同理 $\forall x, x \in Ha \iff x * a^{-1} \in H$ .
- 描述右陪集Ha中的元素x。

### 左陪集关系

- $\mathcal{U} < H, * > \mathcal{E} \mathcal{A} < G, * > \mathbf{0} \mathcal{F} \mathcal{A}, \quad \mathbb{M}$  $\forall x, x \in \mathcal{A} H \iff a^{-1} * x \in \mathcal{H}.$
- 证:  $x \in aH \iff \exists h \in H, \ x = a * h \iff \exists h = a^{-1} * x \in H,$ 因此,  $\forall x, \ x \in aH \iff a^{-1} * x \in H.$
- 描述了左陪集aH中的元素x。

- 同理 $\forall x, x \in Ha \iff x * a^{-1} \in H$ .
- 描述右陪集Ha中的元素x。

### 左陪集关系

- $\mathcal{U} < H, * > \mathcal{E} \mathcal{A} < G, * > \mathbf{0} \mathcal{F} \mathcal{A}, \quad \mathbb{M}$  $\forall x, x \in \mathcal{A} H \iff a^{-1} * x \in \mathcal{H}.$
- 证:  $x \in aH \iff \exists h \in H, \ x = a * h \iff \exists h = a^{-1} * x \in H,$  因此,  $\forall x, \ x \in aH \iff a^{-1} * x \in H.$
- 描述了左陪集aH中的元素x。

- 同理 $\forall x, x \in Ha \iff x * a^{-1} \in H$ .
- 描述右陪集Ha中的元素x。

### 左陪集关系

- 证:  $x \in aH \iff \exists h \in H, \ x = a * h \iff \exists h = a^{-1} * x \in H,$  因此,  $\forall x, \ x \in aH \iff a^{-1} * x \in H.$
- 描述了左陪集aH中的元素x。

- 同理 $\forall x, x \in Ha \iff x * a^{-1} \in H$ .
- 描述右陪集Ha中的元素x。

#### 左陪集关系

- 证:  $x \in aH \iff \exists h \in H, \ x = a * h \iff \exists h = a^{-1} * x \in H,$  因此,  $\forall x, \ x \in aH \iff a^{-1} * x \in H.$
- 描述了左陪集aH中的元素x。

- 同理 $\forall x, x \in Ha \iff x * a^{-1} \in H$ .
- 描述右陪集Ha中的元素×。

- 设< H,\*>是群< G,\*>的子群, 定义G上的二元关系 R:  $< a,b>\in R$ , iff,  $a^{-1}*b\in H$ . 称R为H的左陪集关系。
- · R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - **对称性**:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH \colon x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$
  - $@aH \subseteq [a]_R: \ \forall x \in aH, \ \exists h \in H, \ x = a * h,$

- 设< H,\*>是群< G,\*>的子群, 定义G上的二元关系 R:  $< a,b> \in R$ , iff,  $a^{-1}*b \in H$ . 称R为H的左陪集关系。
- · R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - 对称性:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$   $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH \colon x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$  $\vdots x = a * (a^{-1} * x) \in aH : [a]_R \subseteq aH$
  - $@aH \subseteq [a]_R: \ \forall x \in aH, \ \exists h \in H, \ x = a * h,$

- 设< H,\*>是群< G,\*>的子群,定义G上的二元关系
   R: < a,b>∈ R, iff, a<sup>-1</sup>\*b∈ H. 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - **对称性**:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH \colon x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$  $\vdots x = a * (a^{-1} * x) \in aH : [a]_R \subseteq aH$
  - $@aH \subseteq [a]_R: \ \forall x \in aH, \ \exists h \in H, \ x = a * h,$

- 砂< H,\*>是群< G,\*>的子群,定义G上的二元关系  $R: \langle a, b \rangle \in R$ , iff,  $a^{-1} * b \in H$ .  $\Re A \to B$ .
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ :
  - 对称性:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$

$$\iff b^{-1} * a \in H \iff bRa$$

- -传递性:  $aRb \land bRc \iff a^{-1} * b \in H \land b^{-1} * c \in H$
- $\bullet$   $[a]_R = aH$

- 设< H,\* >是群< G,\* >的子群,定义G上的二元关系 R: < a, b >  $\in$  R, iff,  $a^{-1}$  \* b  $\in$  H. 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - **对称性**:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH \colon x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$  $\vdots x = a * (a^{-1} * x) \in aH : [a]_R \subseteq aH$
  - $@aH \subseteq [a]_R: \forall x \in aH, \exists h \in H, x = a * h,$ 
    - $\mathbb{R}^n h = a^{-1} * x \in H. \quad \times Ra, \quad x \in [a]_{\mathcal{B}}, \quad aH \subseteq [a]_{\mathcal{B}}$

- 设< H,\*>是群< G,\*>的子群,定义G上的二元关系
   R: < a,b>∈ R, iff, a<sup>-1</sup>\*b∈ H. 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - 对称性:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \land bRc \Longleftrightarrow a^{-1} * b \in H \land b^{-1} * c \in H$

$$\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$$

- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH \colon x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$   $\vdots \quad x = a * (a^{-1} * x) \in aH \quad \vdots \quad [a]_R \subseteq aH$
  - $\bigcirc aH \subseteq [a]_R$ :  $\forall x \in aH$ ,  $\exists h \in H$ , x = a \* h,

- 设< H,\*>是群< G,\*>的子群, 定义G上的二元关系 R:  $< a,b> \in R$ , iff,  $a^{-1}*b \in H$ . 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - **对称性**:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH \colon x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$   $\vdots x = a * (a^{-1} * x) \in aH : [a]_R \subseteq aH$
  - $@aH \subseteq [a]_R: \forall x \in aH, \exists h \in H, x = a * h,$

### 左陪集等价关系的定义

- 设< H,\* >是群< G,\* >的子群,定义G上的二元关系 R: < a, b >  $\in$  R, iff,  $a^{-1}$  \* b  $\in$  H. 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - **对称性**:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH \colon x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$  $\vdots x = a * (a^{-1} * x) \in aH : [a]_R \subseteq aH$
  - $@aH \subseteq [a]_R: \ \forall x \in aH, \ \exists h \in H, \ x = a * h,$

### 左陪集等价关系的定义

- 设< H,\*>是群< G,\*>的子群,定义G上的二元关系
   R: < a,b>∈ R, iff, a<sup>-1</sup>\*b∈ H. 称R为H的左陪集关系。
- R是等价关系
  - -自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - 対称性:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH: x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$
  - $\textcircled{a}H \subseteq [a]_R$ :  $\forall x \in aH$ ,  $\exists h \in H$ , x = a \* h,

### 左陪集等价关系的定义

- 设< H,\*>是群< G,\*>的子群, 定义G上的二元关系 R:  $< a,b>\in R$ , iff,  $a^{-1}*b\in H$ . 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - 対称性:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 
  - $\textcircled{1}[a]_R \subseteq aH: \ x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$   $\therefore x = a * (a^{-1} * x) \in aH, \ \therefore [a]_R \subseteq aH;$
  - $\textcircled{a}H \subseteq [a]_R$ :  $\forall x \in aH$ ,  $\exists h \in H$ , x = a \* h,

 $\mathbb{P}h = a^{-1} * x \in H$ . xRa.  $x \in [a]_{P}$ .  $aH \subseteq [a]_{P}$ 

### 左陪集等价关系的定义

- 设< H,\* >是群< G,\* >的子群,定义G上的二元关系 R: < a, b >  $\in$  R, iff,  $a^{-1}$  \* b  $\in$  H. 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - 対称性:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 

  - $@aH \subseteq [a]_R: \ \forall x \in aH, \ \exists h \in H, \ x = a * h,$

### 左陪集等价关系的定义

- 设< H,\*>是群< G,\*>的子群,定义G上的二元关系
   R: < a,b>∈ R, iff, a<sup>-1</sup>\*b∈ H. 称R为H的左陪集关系。
- R是等价关系
  - 自反性:  $e = a^{-1} * a \in H \iff aRa$ ;
  - 対称性:  $aRb \iff a^{-1} * b \in H \iff (a^{-1} * b)^{-1} \in H$  $\iff b^{-1} * a \in H \iff bRa$
  - -传递性:  $aRb \wedge bRc \iff a^{-1} * b \in H \wedge b^{-1} * c \in H$  $\implies (a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \iff aRc.$
- $\bullet$   $[a]_R = aH$ 
  - $\mathbb{O}[a]_R \subseteq aH: x \in [a]_R \Leftrightarrow xRa \Leftrightarrow aRx \Leftrightarrow a^{-1} * x \in H,$  $\therefore x = a * (a^{-1} * x) \in aH, \therefore [a]_R \subseteq aH;$

 $\mathbb{P}h = a^{-1} * x \in H$ .  $xRa, x \in [a]_{\mathcal{P}}, aH \subseteq [a]_{\mathcal{P}}$ .

 $@aH \subseteq [a]_R: \ \forall x \in aH, \ \exists h \in H, \ x = a * h,$ 

#### 小结

- 设< H, \* >是群< G, \* >的子群,则H可以诱导出一个由H的 左(右)陪集集合构成的对G的划分;
- 由这个划分可以诱导出G的一个左(右) 陪集等价关系;
- 左陪集等价关系: ∀a,b属于同一个左陪集←⇒ a,b属于同一个左陪集等价关系的等价类←⇒ a<sup>-1</sup> \* b ∈ H.
  - $\Rightarrow$ :  $a \in aH$ ,  $b \in bH$ , M aH = bH;
  - □且, a, b有左陪集关系,  $pa^{-1}*b \in H$ .

#### 例

#### 小结

- 由这个划分可以诱导出G的一个左(右) 陪集等价关系;
- 左陪集等价关系: ∀a,b属于同一个左陪集⇔ a,b属于同一个左陪集等价关系的等价类⇔ a<sup>-1</sup> \* b ∈ H.
  - ightharpoonup 
    ightharpoonup aH,  $b \in bH$ , ightharpoonup aH = bH;
  - □且, a, b有左陪集关系,  $pa^{-1}*b \in H$ .

#### 例

#### 小结

- 设< H, \*>是群< G, \*>的子群,则H可以诱导出一个由H的 左(右)陪集集合构成的对G的划分;
- 由这个划分可以诱导出G的一个左(右) 陪集等价关系;
- 左陪集等价关系: ∀a, b属于同一个左陪集←⇒ a, b属于同一个左陪集等价关系的等价类←⇒ a<sup>-1</sup> \* b ∈ H.
  - Arr :  $a \in aH$ ,  $b \in bH$ , Arr aH = bH;
  - □且, a, b有左陪集关系,  $pa^{-1}*b \in H$ .

#### 例

#### 小结

- 由这个划分可以诱导出G的一个左(右) 陪集等价关系;
- 左陪集等价关系: ∀a,b属于同一个左陪集←⇒ a,b属于同一个左陪集等价关系的等价类←⇒ a<sup>-1</sup> \* b ∈ H.
  - $\Rightarrow$ :  $a \in aH$ ,  $b \in bH$ , M aH = bH;
  - ➡且, a, b有左陪集关系, 即 $a^{-1}*b \in H$ .

#### 例

#### 小结

- 设< H, \* >是群< G, \* >的子群,则H可以诱导出一个由H的 左(右)陪集集合构成的对G的划分;
- 由这个划分可以诱导出G的一个左(右) 陪集等价关系;
- 左陪集等价关系: ∀a,b属于同一个左陪集←⇒ a,b属于同一个左陪集等价关系的等价类←⇒ a<sup>-1</sup> \* b ∈ H.
  - $\Rightarrow$ :  $a \in aH$ ,  $b \in bH$ , M aH = bH;
  - □且, a, b有左陪集关系, 即 $a^{-1}*b \in H$ .

#### 例

- 3次对称群 $< S_3, \circ, \mathbb{I} >, S_3 = {\mathbb{I}, a, a^2, b, c, d},$
- $H = \{I, d\}$  是群  $S_3$  的一个子群;
- H的所有左陪集组成的集合{{I, d}, {a, c}, {b, a²}}
- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

- 3次对称群 $< S_3, \circ, \mathbb{I} >, S_3 = \{\mathbb{I}, a, a^2, b, c, d\},$
- $H = \{I, d\}$  是群 $S_3$ 的一个子群;
- H的所有左陪集组成的集合{{I,d}, {a, c}, {b, a²}}
- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

- 3次对称群 $< S_3, \circ, \mathbb{I} >, S_3 = {\mathbb{I}, a, a^2, b, c, d},$
- $H = \{\mathbb{I}, d\}$  是群  $S_3$  的一个子群;
- H的所有左陪集组成的集合 $\{[I,d],\{a,c\},\{b,a^2\}\}$
- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

- 3次对称群 $< S_3, \circ, \mathbb{I} >, S_3 = {\mathbb{I}, a, a^2, b, c, d},$
- $H = \{I, d\}$  是群 $S_3$ 的一个子群;
- H的所有左陪集组成的集合 $\{\{I,d\},\{a,c\},\{b,a^2\}\}$
- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

- 3次对称群 $< S_3, \circ, \mathbb{I} >, S_3 = {\mathbb{I}, a, a^2, b, c, d},$
- $H = \{I, d\}$  是群 $S_3$ 的一个子群;
- H的所有左陪集组成的集合 $\{[I,d],\{a,c\},\{b,a^2\}\}$
- H的所有右陪集组成的集合 $\{[I,d],\{c,a^2\},\{a,b\}\}$
- 则由H诱导的左、右陪集等价关系也不同。

- 设< H, \* >是群< G, \* >的子群,称 $H \rightarrow G$ 的不变子群(正规子群), $iff, \forall a \in G, aH = Ha, 记为<math>H \triangleleft G$ .
- 注:  $\forall a \in G, aH = Ha \iff \forall a \in G, \exists h_1, h_2 \in H, a * h_1 = h_2 * a.$
- 对于正规子群,左右陪集对应相等,aH = Ha,可简称为陪集。左右陪集关系相同,简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

- 设< H, \* >是群< G, \* >的子群,称 $H \rightarrow G$ 的不变子群(正规子群), $iff, \forall a \in G, aH = Ha, 记为<math>H \triangleleft G$ .
- $\mathbf{i}: \forall a \in G, aH = Ha \Longleftrightarrow$   $\forall a \in G, \exists h_1, h_2 \in H, a * h_1 = h_2 * a.$
- 对于正规子群,左右陪集对应相等,aH = Ha,可简称为陪集。左右陪集关系相同,简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

- 设< H, \* >是群< G, \* >的子群,称 $H \rightarrow G$ 的不变子群(正规子群), $iff, \forall a \in G, aH = Ha, 记为<math>H \triangleleft G$ .
- 注:  $\forall a \in G$ ,  $aH = Ha \iff$  $\forall a \in G$ ,  $\exists h_1, h_2 \in H$ ,  $a * h_1 = h_2 * a$ .
- 对于正规子群,左右陪集对应相等,aH = Ha,可简称为陪集。左右陪集关系相同,简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

- 设< H, \* >是群< G, \* >的子群,称 $H \rightarrow G$ 的不变子群(正规子群), $iff, \forall a \in G, aH = Ha, 记为<math>H \triangleleft G$ .
- 注:  $\forall a \in G, aH = Ha \iff \forall a \in G, \exists h_1, h_2 \in H, a * h_1 = h_2 * a.$
- 对于正规子群,左右陪集对应相等, aH = Ha,可简称为陪集。左右陪集关系相同,简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

- 设< H, \* >是群< G, \* >的子群,称 $H \rightarrow G$ 的不变子群(正规子群)、 $iff, \forall a \in G, aH = Ha, 记为<math>H \triangleleft G$ .
- 注:  $\forall a \in G, aH = Ha \iff \forall a \in G, \exists h_1, h_2 \in H, a * h_1 = h_2 * a.$
- 对于正规子群,左右陪集对应相等, aH = Ha,可简称为陪集。左右陪集关系相同,简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

- 设< H, \* >是群< G, \* >的子群,称 $H \rightarrow G$ 的不变子群(正规子群), $iff, \forall a \in G, aH = Ha, 记为<math>H \triangleleft G$ .
- 注:  $\forall a \in G$ ,  $aH = Ha \iff$  $\forall a \in G$ ,  $\exists h_1, h_2 \in H$ ,  $a * h_1 = h_2 * a$ .
- 对于正规子群,左右陪集对应相等, aH = Ha,可简称为陪集。左右陪集关系相同,简称为陪集关系。
- 所有可交换群的子群都是正规子群。
- 所有平凡子群都是正规子群。

### 定理

- $H \triangleleft G$ ;
- $\forall a \in G, \ a * H * a^{-1} = H;$
- $\bullet \ \forall a \in G, \ a * H * a^{-1} \subseteq H;$
- $\bullet \ \forall a \in G, \ \forall h \in H, \ a * h * a^{-1} \in H;$

#### 定理

- $H \triangleleft G$ ;
- $\forall a \in G, \ a * H * a^{-1} = H;$
- $\bullet \ \forall a \in G, \ a * H * a^{-1} \subseteq H;$
- $\bullet \ \forall a \in G, \ \forall h \in H, \ a * h * a^{-1} \in H;$

### 定理

- $H \triangleleft G$ ;
- $\forall a \in G, \ a * H * a^{-1} = H;$
- $\forall a \in G$ ,  $a * H * a^{-1} \subseteq H$ ;
- $\bullet \ \forall a \in G, \ \forall h \in H, \ a * h * a^{-1} \in H$

### 定理

- $H \triangleleft G$ ;
- $\forall a \in G, \ a * H * a^{-1} = H;$
- $\forall a \in G$ ,  $a * H * a^{-1} \subseteq H$ ;
- $\forall a \in G$ ,  $\forall h \in H$ ,  $a * h * a^{-1} \in H$ ;

## 同余关系

### 定义-同余关系

- < A,\*>是一个代数系统, R是A上的等价关系, 称等价关系 R在运算\*下具有置换性质, iff,
  - if  $\forall$  < a, b > $\in$  R $\land$  < c, d > $\in$  R, then < a \* c, b \* d > $\in$  R.
- 将一个运算数置换为等价类中的另一个元素,不会改变运算 结果的等价类,即,等价关系R在运算\*下仍然保持。
- 若等价关系R在运算\*下具有置换性质,则称R为< A,\*>上 的同余关系。

### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
  - a1是aH中的任一元素。b1是bH中的任一元素。 现证任意的a1 \* b1都在H的同一陪集中。

#### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,

$$a_1$$
是 $a$ H中的任一元素, $b_1$ 是 $b$ H中的任一元素,现证任意的 $a_1*b_1$ 都在 $B$ H的同一陪集中。 设  $a_1=a*h_1,b_1=b*h_2,\ h_1,h_2\in B$ H, $a_1*b_1=(a*h_1)*(b*h_2)$   $=(a*h_1)*(h_3*b)$   $=a*h_4*b$   $=(a*b)*h_5$   $(h_i\in B)$ 

 $\therefore \forall a_1 * b_1 \in (a * b) H.$ 

### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,

 $a_1$ 是aH中的任一元素, $b_1$ 是bH中的任一元素,

现证任意的a1\*b1都在H的同一陪集中。

谈  $a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H$ ,

$$a_1 * b_1 = (a * h_1) * (b * h_2)$$
  
=  $(a * h_1) * (h_3 * b)$ 

$$= (a * b) * br (b: \in H)$$

 $\therefore \forall a_1 * b_1 \in (a * b) H.$ 

### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,
   a<sub>1</sub>是aH中的任一元素,b<sub>1</sub>是bH中的任一元素,
   现证任意的a<sub>1</sub>\*b<sub>1</sub>都在H的同一陪集中。

波 
$$a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H$$
,
 $a_1 * b_1 = (a * h_1) * (b * h_2)$ 
 $= (a * h_1) * (h_3 * b)$ 
 $= a * h_4 * b$ 
 $= (a * b) * h_5 \quad (h_i \in H)$ 

 $\therefore \forall a_1 * b_1 \in (a * b)H.$ 

#### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,
   a<sub>1</sub>是aH中的任一元素,b<sub>1</sub>是bH中的任一元素,
   现证任意的a<sub>1</sub> \* b<sub>1</sub>都在H的同一陪集中。

设  $a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H,$ 

$$a_1 * b_1 = (a * h_1) * (b * h_2)$$
  
=  $(a * h_1) * (h_3 * b)$   
=  $a * h_4 * b$   
=  $(a * b) * h_5$   $(h_i \in H)$ 

 $\therefore \forall a_1 * b_1 \in (a * b)H.$ 

### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集, a<sub>1</sub>是aH中的任一元素,b<sub>1</sub>是bH中的任一元素, 现证任意的a<sub>1</sub> \* b<sub>1</sub>都在H的同一陪集中。
   设 a<sub>1</sub> = a \* h<sub>1</sub>, b<sub>1</sub> = b \* h<sub>2</sub>, h<sub>1</sub>, h<sub>2</sub> ∈ H,

後 
$$a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H_1$$
  
 $a_1 * b_1 = (a * h_1) * (b * h_2)$   
 $= (a * h_1) * (h_3 * b)$   
 $= a * h_4 * b$ 

 $\therefore \forall a_1 * b_1 \in (a * b) H.$ 

### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,
   a<sub>1</sub>是aH中的任一元素,b<sub>1</sub>是bH中的任一元素,

现证任意的 $a_1*b_1$ 都在H的同一陪集中。

设 
$$a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H$$
,

$$a_1 * b_1 = (a * h_1) * (b * h_2)$$
  
=  $(a * h_1) * (h_3 * b)$ 

$$= a * h_4 * h$$

$$= (a*b)*h_5 \qquad (h_i \in H)$$

 $\therefore \forall a_1 * b_1 \in (a * b)H.$ 

### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,

 $a_1$ 是aH中的任一元素, $b_1$ 是bH中的任一元素,

现证任意的 $a_1 * b_1$ 都在H的同一陪集中。

设 
$$a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H$$
,

$$a_1 * b_1 = (a * h_1) * (b * h_2)$$
  
=  $(a * h_1) * (h_3 * b)$   
=  $a * h_4 * b$ 

$$= (a*b)*h_5 \qquad (h_i \in H)$$

 $\therefore \forall a_1 * b_1 \in (a * b)H.$ 

### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,

 $a_1$ 是aH中的任一元素, $b_1$ 是bH中的任一元素,

现证任意的 $a_1*b_1$ 都在H的同一陪集中。

谈 
$$a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H$$
,

 $= (a * b) * h_5 (h_i \in H)$ 

$$a_1 * b_1 = (a * h_1) * (b * h_2)$$
  
=  $(a * h_1) * (h_3 * b)$   
=  $a * h_4 * b$ 

$$\therefore \forall a_1 * b_1 \in (a * b)H.$$

#### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,
   a₁是aH中的任一元素,b₁是bH中的任一元素,

现证任意的 $a_1*b_1$ 都在H的同一陪集中。

後 
$$a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H,$$

$$a_1 * b_1 = (a * h_1) * (b * h_2)$$
  
=  $(a * h_1) * (h_3 * b)$   
=  $a * h_4 * b$ 

$$= (a*b)*h_5 \qquad (h_i \in H)$$

$$\therefore \ \forall a_1 * b_1 \in (a * b) H.$$

## 正规子群和同余关系(一)

#### 定理

- 群G的正规子群的陪集关系是G上的同余关系。
- 证:设aH和bH是群G的两个陪集,
   a<sub>1</sub>是aH中的任一元素,b<sub>1</sub>是bH中的任一元素,

现证任意的 $a_1*b_1$ 都在H的同一陪集中。

波 
$$a_1 = a * h_1, b_1 = b * h_2, h_1, h_2 \in H$$
,  
 $a_1 * b_1 = (a * h_1) * (b * h_2)$   
 $= (a * h_1) * (h_3 * b)$   
 $= a * h_4 * b$   
 $= (a * b) * h_5 (h_i \in H)$ 

$$\therefore \forall a_1 * b_1 \in (a * b)H.$$

同时陪集关系是等价关系,所以由正规子群H诱导出的陪集 关系是同余关系。

### 定义

设< H,\*,e>是群< G,\*,e>的正规子群。H的陪集关系R
 (是同余关系,具有置换性质),则< G/H,®,H>是群,其中:

```
G/H = G/R = \{aH | a \in G\};
aH \circledast bH = (a * b)H;
[aH]^{-1} = a^{-1}H;
H是单位元.
```

• R是H的陪集关系,习惯也记为 $< G/R, \circledast, H>$ ,称为群G关于正规子群H的商群。

### 定义

• 设< H, \*, e > 是群< G, \*, e > 的正规子群。H的陪集关系R (是同余关系,具有置换性质),则< G/H,  $\circledast$ , H > 是群,其中:

$$G/H = G/R = \{aH | a \in G\};$$
  
 $aH \circledast bH = (a * b)H;$   
 $[aH]^{-1} = a^{-1}H;$   
 $H$ 是单位元。

• R是H的陪集关系,习惯也记为 $< G/R, \circledast, H>$ ,称为群G关于正规子群H的商群。

#### 定义

设< H,\*,e>是群< G,\*,e>的正规子群。H的陪集关系R
 (是同余关系,具有置换性质),则< G/H,⊛,H>是群,其中:

$$G/H = G/R = \{aH | a \in G\};$$
  
 $aH \circledast bH = (a * b)H;$   
 $[aH]^{-1} = a^{-1}H;$   
 $H 是 单位元。$ 

● R是H的陪集关系,习惯也记为< G/R, ®, H>, 称为群G关于正规子群H的商群。

#### 定义

 设< H,\*,e>是群< G,\*,e>的正规子群。H的陪集关系R (是同余关系,具有置换性质),则< G/H, $\circledast$ ,H>是群,其 中:

$$G/H = G/R = \{aH | a \in G\};$$
  
 $aH \circledast bH = (a * b)H;$   
 $[aH]^{-1} = a^{-1}H;$   
 $H 是 单位元$ 

• R是H的陪集关系,习惯也记为 $< G/R, \circledast, H>$ ,称为群G关

#### 定义

• 设< H, \*, e > 是群< G, \*, e > 的正规子群。H的陪集关系R (是同余关系,具有置换性质),则< G/H,  $\circledast$ , H > 是群,其中:

```
G/H = G/R = \{aH | a \in G\};

aH \circledast bH = (a * b)H;

[aH]^{-1} = a^{-1}H;

H是单位元.
```

• R是H的陪集关系,习惯也记为 $< G/R, \circledast, H>$ ,称为群G关于正规子群H的商群。

### 定义

• 设< H, \*, e > 是群< G, \*, e > 的正规子群。H的陪集关系R (是同余关系,具有置换性质),则< G/H,  $\circledast$ , H > 是群,其中:

```
G/H = G/R = \{aH | a \in G\};

aH \circledast bH = (a * b)H;

[aH]^{-1} = a^{-1}H;

H是单位元.
```

● R是H的陪集关系,习惯也记为 $< G/R, \circledast, H>$ ,称为群G关于正规子群H的商群。

# 商群的例子

#### 定义

● (有限群的) 商群的阶等于群G的阶除以子群H的阶,即H在G中的指数。

### 例

- 群 $< \mathbb{Z}, +, 0 >$ ,  $4\mathbb{Z} \triangleleft \mathbb{Z}$ , **商群为**  $< \{4\mathbb{Z}, 4\mathbb{Z} + 1, 4\mathbb{Z} + 2, 4\mathbb{Z} + 3\}, \oplus, 4\mathbb{Z} >$

# 商群的例子

### 定义

● (有限群的) 商群的阶等于群G的阶除以子群H的阶,即H在G中的指数。

### 例

- $\mathbf{\mathcal{Z}}$  + , 0 > ,  $4\mathbb{Z} \triangleleft \mathbb{Z}$  ,  $\mathbf{\mathcal{Z}}$   $\mathbf{\mathcal{Z}}$   $\mathbf{\mathcal{Z}}$   $\mathbf{\mathcal{Z}}$   $\mathbf{\mathcal{Z}}$   $\mathbf{\mathcal{Z}}$  + 3},  $\oplus$  ,  $4\mathbb{Z} >$
- 群 $< S_3, \circ, \mathbb{I} >, \{\mathbb{I}, a, a^2\} \triangleleft S_3$ , 商群为  $< \{\{\mathbb{I}, a, a^2\}, \{b, c, d\}\}, \circledast, \{\mathbb{I}, a, a^2\} >.$

# 商群的例子

### 定义

● (有限群的) 商群的阶等于群G的阶除以子群H的阶,即H在G中的指数。

### 例

- $\mathbf{\mathcal{Z}}$  + , 0 >  $, 4\mathbb{Z} \triangleleft \mathbb{Z}$   $, \mathbf{\vec{n}}\mathbf{\vec{n}}\mathbf{\vec{n}}$   $< \{4\mathbb{Z}, 4\mathbb{Z} + 1, 4\mathbb{Z} + 2, 4\mathbb{Z} + 3\}, \oplus, 4\mathbb{Z} >$
- 群 $< S_3, \circ, \mathbb{I} >, \{\mathbb{I}, a, a^2\} \triangleleft S_3$ , 商群为  $< \{\{\mathbb{I}, a, a^2\}, \{b, c, d\}\}, \circledast, \{\mathbb{I}, a, a^2\} >.$

- 设R是群< G, \* >上的同余关系,则 $[e]_R \triangleleft G$ ,且R就是G关于 正规子群 $[e]_R$ 的陪集关系。
- 证: (略)
  - (1)  $[e]_R \leqslant G$ ;
  - (2)  $[e]_R \triangleleft G$ ;
  - (3)  $[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

- $\partial R \neq G$ , \* > L的同余关系,则[e]<sub>R</sub>  $\triangleleft G$ ,且R就是G关于正规子群[e]<sub>R</sub>的陪集关系。
- 证: (略)
  - $(1) [e]_R \leqslant G;$
  - (2)  $[e]_R \triangleleft G$ ;
  - (3)  $[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

- $\partial R \neq G$ , \* > L的同余关系,则[e]<sub>R</sub>  $\triangleleft G$ ,且R就是G关于正规子群[e]<sub>R</sub>的陪集关系。
- 证: (略)
  - (1)  $[e]_R \leq G$ ;
  - (2)  $[e]_R \triangleleft G$ ;
  - (3)  $[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

- $\partial R \neq G$ , \* > L的同余关系,则[e]<sub>R</sub>  $\triangleleft G$ ,且R就是G关于正规子群[e]<sub>R</sub>的陪集关系。
- 证: (略)
  - (1)  $[e]_R \leq G$ ;
  - (2)  $[e]_R \triangleleft G$ ;
  - (3)  $[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

- 设R是群< G, \* >上的同余关系,则 $[e]_R \triangleleft G$ ,且R就是G关于正规子群 $[e]_R$ 的陪集关系。
- 证: (略)
  - (1)  $[e]_R \leq G$ ;
  - (2)  $[e]_R \triangleleft G$ ;
  - (3)  $[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

- 设R是群< G, \* >上的同余关系,则 $[e]_R \triangleleft G$ ,且R就是G关于正规子群 $[e]_R$ 的陪集关系。
- 证: (略)
  - (1)  $[e]_R \leq G$ ;
  - (2)  $[e]_R \triangleleft G$ ;
  - (3)  $[a]_R = a * [e]_R$
- 由G上的同余关系可以诱导G的正规子群。

- 设h是群< G, \*, e >到群< H, o, I >的同态,则:
  - (1) h诱导的G上的等价关系 $=_h$ 是同余关系,  $\forall a, b \in G, \ a =_h b \iff h(a) = h(b)$
  - (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$
  - (3) K的陪集关系 (正规子群的陪集关系) 就等于上述同余关系=h。

#### 定理

- 设h是群< G, \*, e>到群< H, o, I>的同态,则:
  - (1) h诱导的G上的等价关系=h是同余关系,

 $\forall a, b \in G, \ a =_h b \iff h(a) = h(b)$ 

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I} \}$
- (3) K的陪集关系(正规子群的陪集关系)就等于上述同余关系=h。

- 设h是群< G, \*, e >到群< H, o, I >的同态,则:
  - (1) h诱导的G上的等价关系=h是同余关系,

$$\forall a, b \in G, \ a =_h b \iff h(a) = h(b)$$

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I} \}$
- (3) K的陪集关系(正规子群的陪集关系)就等于上述同余关系=h。

#### 定理

- 设h是群< G, \*, e>到群< H, o, I>的同态,则:
  - (1) h诱导的G上的等价关系=h是同余关系,  $\forall a, b \in G, a = h, b \iff h(a) = h(b)$
  - (2) h的同态核K是< G, \*, e >的正规子群,

 $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$ 

(3)K的陪集关系(正规子群的陪集关系)就等于上述同 余关系=h。

### 定理

- $\mathfrak{g}h$   $\mathbb{Z}$   $\mathbb{Z}$   $G, *, e > \mathfrak{I}$   $\mathbb{Z}$   $\mathbb{Z}$ 
  - (1) h诱导的G上的等价关系=h是同余关系,

$$\forall a, b \in G, \ a =_h b \iff h(a) = h(b)$$

(2) h的同态核K是< G, \*, e >的正规子群,

$$K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$$

(3)K的陪集关系(正规子群的陪集关系)就等于上述同 余关系=h。

#### 定理

- 设h是群< G, \*, e>到群< H, o, I>的同态,则:
  - (1) h诱导的G上的等价关系=h是同余关系,

$$\forall a, b \in G, \ a =_h b \iff h(a) = h(b)$$

(2) h的同态核K是< G,\*,e>的正规子群,

$$K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$$

(3) K的陪集关系(正规子群的陪集关系)就等于上述同余关系 $=_h$ 。

#### **Proof**

• (1) h诱导的G上的等价关系=h是同余关系,

$$\forall a, b \in G, \ a =_h b \iff h(a) = h(b)$$

• 证:

#### **Proof**

• (1) h 诱导的G上的等价关系=h是同余关系, $\forall a, b \in G, a = h, b \iff h(a) = h(b)$ 

• 证:

#### **Proof**

- (1) h 诱导的G上的等价关系= $_h$ 是同余关系,  $\forall a, b \in G, a =_h b \iff h(a) = h(b)$
- 证:

#### **Proof**

• (1) h 诱导的G上的等价关系=h是同余关系,  $\forall a, b \in G, a = h, b \iff h(a) = h(b)$ 

#### **Proof**

• (1) h 诱导的G上的等价关系=h是同余关系, $\forall a, b \in G, a = h, b \iff h(a) = h(b)$ 

#### **Proof**

• (1) h 诱导的G上的等价关系 $=_h$ 是同余关系,  $\forall a, b \in G, a =_h b \iff h(a) = h(b)$ 

#### **Proof**

• (1) h 诱导的G上的等价关系 $=_h$ 是同余关系,  $\forall a, b \in G, a =_h b \iff h(a) = h(b)$ 

#### **Proof**

• (1) h 诱导的G上的等价关系=h是同余关系,  $\forall a, b \in G, a = h b \iff h(a) = h(b)$ 

### **Proof**

(2) h的同态核K是< G,\*,e>的正规子群,

$$K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$$

- · 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K, \quad \not \exists h(k_1) = h(k_2) = \mathbb{I},$$
 $\vdots \quad h(k_1 * k^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I}$ 

$$\kappa_1 * k_2^{-1} \in K, \therefore K \leqslant G.$$

② K < G:

$$\forall a \in G, k \in K$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h$$
  
=  $h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

 $\therefore a^{-1} * k * a \in K, K \triangleleft G.$ 

#### **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$
- 证:
- ①  $K \leqslant G$ :  $\forall k_1, k_2 \in K, \quad \mathsf{有} h(k_1) = h(k_2) = \mathbb{I},$   $\therefore h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   $k_1 * k_2^{-1} \in K, \quad \therefore K \leqslant G.$
- $^{\circ}$   $K \triangleleft G$ :

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

### **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$
- 证:
- ①  $K \leqslant G$ :  $\forall k_1, k_2 \in K, \quad$ 有 $h(k_1) = h(k_2) = \mathbb{I},$   $\therefore h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   $k_1 * k_2^{-1} \in K, \therefore K \leqslant G.$
- $\bigcirc$   $K \triangleleft G$

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
  
=  $h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

#### **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$ 
  - 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K, \quad \mathbf{\pi} h(k_1) = h(k_2) = \mathbb{I},$$
  
 $\therefore \quad h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   
 $k_1 * k_2^{-1} \in K, \quad \therefore \quad K \leqslant G.$ 

② K < G:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

#### **Proof**

- (2) h的同态核K是< G,\*,e>的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$ 
  - 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K, \quad \not a h(k_1) = h(k_2) = \mathbb{I},$$
  
 $\therefore h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   
 $k_1 * k_2^{-1} \in K, \quad \therefore K \leq G.$ 

② K ⊲ G:

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
  
=  $h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

#### **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$ 
  - 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K, \quad f_1(k_1) = h(k_2) = \mathbb{I},$$

$$\therefore \quad h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$$

$$k_1 * k_2^{-1} \in K, \quad K \leq G.$$

② K < G:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
  
=  $h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

## **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$
- 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K$$
,  $f_1h(k_1) = h(k_2) = \mathbb{I}$ ,  
∴  $h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   
 $k_1 * k_2^{-1} \in K$ , ∴  $K \leq G$ .

② K < G:

$$\forall a \in G, \ k \in K,$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
  
=  $h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

 $\therefore a^{-1} * k * a \in K, K \triangleleft G.$ 

## **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$ 
  - 证:
- ①  $K \leqslant G$ :  $\forall k_1, k_2 \in K, \quad fh(k_1) = h(k_2) = \mathbb{I},$  $\therefore \quad h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$

$$k_1 * k_2^{-1} \in K$$
,  $K \leqslant G$ .

$$\forall a \in G, k \in K$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
  
=  $h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

$$\therefore a^{-1} * k * a \in K, K \triangleleft G.$$

## **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$
- 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K$$
,  $f_1h(k_1) = h(k_2) = \mathbb{I}$ ,  
∴  $h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   
 $k_1 * k_2^{-1} \in K$ , ∴  $K \leq G$ .

$$\forall a \in G, k \in K$$

$$h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$$
$$= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$$

## **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$
- 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K$$
,  $f_1h(k_1) = h(k_2) = \mathbb{I}$ ,  
∴  $h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   
 $k_1 * k_2^{-1} \in K$ , ∴  $K \leq G$ .

$$\forall a \in G, \ k \in K,$$
  
 $h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$   
 $= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

## **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$ 
  - 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K$$
,  $f_1h(k_1) = h(k_2) = \mathbb{I}$ ,  
∴  $h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   
 $k_1 * k_2^{-1} \in K$ , ∴  $K \leq G$ .

$$\forall a \in G, \ k \in K,$$
  
 $h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$   
 $= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 

## **Proof**

- (2) h的同态核K是< G, \*, e >的正规子群, $K = ker(h) \triangleq \{a | a \in G \land h(a) = h(e) = \mathbb{I}\}$ 
  - 证:
- ① *K* ≤ *G*:

$$\forall k_1, k_2 \in K$$
,  $f_1h(k_1) = h(k_2) = \mathbb{I}$ ,  
∴  $h(k_1 * k_2^{-1}) = h(k_1) \circ h(k_2)^{-1} = \mathbb{I} \circ \mathbb{I} = \mathbb{I}$   
 $k_1 * k_2^{-1} \in K$ , ∴  $K \leq G$ .

$$\forall a \in G, k \in K,$$
 $h(a^{-1} * k * a) = h(a^{-1}) \circ h(k) \circ h(a) = h(a^{-1}) \circ \mathbb{I} \circ h(a)$ 
 $= h(a^{-1}) \circ h(a) = h(a)^{-1} \circ h(a) = \mathbb{I}$ 
 $\vdots a^{-1} * k * a \in K, K \triangleleft G.$ 

### **Proof**

- (3) K陪集关系 (正规子群的陪集关系) 就等于上述同余 关系=h。
- 证: a, b有K陪集关系 $\Longleftrightarrow a, b$ 也有同余关系 $=_h$ :  $\forall a, b \in G$ ,  $a =_h b \Longleftrightarrow h(a) = h(b)$   $\iff h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$   $\iff a^{-1} * b \in K$ ,

#### **Proof**

- (3) K陪集关系 (正规子群的陪集关系) 就等于上述同余 关系=h。
- 证: a, b有K陪集关系
   a, b也有同余关系=h:

 $\forall a, b \in G$ ,  $a =_h b \iff h(a) = h(b)$   $\iff h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$  $\iff a^{-1} * b \in K$ ,

### **Proof**

- (3) K陪集关系 (正规子群的陪集关系) 就等于上述同余 关系=h。
- 证: a, b有K陪集关系⇔ a, b也有同余关系=h:
   ∀a, b ∈ G,
   a = h b ⇔ h(a) = h(b)

$$\iff h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$$
  
$$\iff a^{-1} * b \in K.$$

#### **Proof**

- (3) K陪集关系 (正规子群的陪集关系) 就等于上述同余 关系=h。
- 证:  $a, b \in K$  陪集关系  $\Longrightarrow$   $a, b \in A$  同余关系  $=_h$ :  $\forall a, b \in G,$   $a =_h b \iff h(a) = h(b)$   $\iff h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$   $\iff a^{-1} * b \in K.$

### **Proof**

- (3) K陪集关系 (正规子群的陪集关系) 就等于上述同余 关系=h。
- 证: a, b有 K 陪集关系  $\iff$  a, b 也有同余关系 $=_h$ :  $\forall a, b \in G$ ,  $a =_h b \iff h(a) = h(b)$   $\iff h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$   $\iff a^{-1} * b \in K$

### **Proof**

- (3) K陪集关系 (正规子群的陪集关系) 就等于上述同余 关系=h。
- 证: a, b有 K 陪集关系  $\iff$  a, b 也有同余关系 $=_h$ :  $\forall a, b \in G$ ,  $a =_h b \iff h(a) = h(b)$   $\iff h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$   $\iff a^{-1} * b \in K$ .

### **Proof**

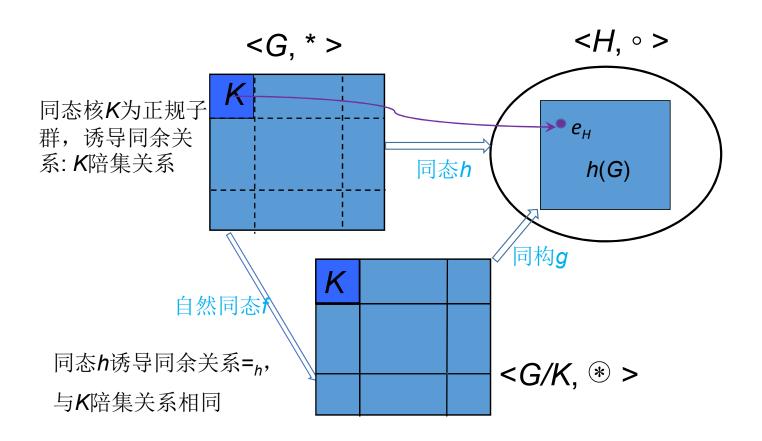
- (3) K陪集关系 (正规子群的陪集关系) 就等于上述同余 关系=h。
- 证: a, b有 K 陪集关系  $\iff$  a, b 也有同余关系 $=_h$ :  $\forall a, b \in G$ ,  $a =_h b \iff h(a) = h(b)$   $\iff h(a^{-1} * b) = h(a^{-1}) \circ h(b) = h(a^{-1}) \circ h(a) = \mathbb{I}$   $\iff a^{-1} * b \in K$ .

# 群同态基本定理

### 定理

• 设h是从群< G, \*>到群 $< H, \circ>$ 的同态,K是同态核,则 < G/K, \*>同构于 $< h(G), \circ>$ .

■ 群同态基本定理:设h是从群〈G,\*〉到群〈H,。〉的同态,K是同态h的核,则〈G/K,\*〉同构于〈h(G),。〉.



## 小结

- 1 群的性质
  - 群的性质
  - 元素的阶
- ② 陪集和拉格朗日定理
  - 陪集的定义和性质
  - 拉格朗日定理
  - 陪集关系