

# 群理论

# Group theory

上节可的内容:

**7+4+6**

**7中运算规律:**封闭性, 交换律。。。

**4个特出元素:**单位元, 逆元, 。。。

**6类运算保持:**满同态保持结合律, 。。。

### 课堂练习1

设  $\langle A, * \rangle$  和  $\langle B, \circ \rangle$  是代数系统， $f: A \rightarrow B$  是函数； $f$  是满同态的必要条件之一是：  $|A| < |B|$

- ☐ A 上述说法是正确的
- ☒ B 上述说法是错误的

提交

## 课堂练习2

以下 \*运算的单位元是 [填空1]。没有单位元填写0

*	a	b	c
a	c	a	b
b	a	b	c
c	a	c	b

正常使用填空题需3.0以上版本雨课堂

作答

以下哪种判断正确。

- ☐ A 运算1满足等幂律
- ☐ B 运算2满足等幂律
- ☒ C 运算3满足等幂律
- ☐ D 运算4满足等幂律

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

运算 1

*	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

运算 2

*	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

运算 3

*	a	b	c
a	a	b	c
b	b	b	c
c	c	c	b

运算 4

提交

任意给定两个代数系统 $\langle A, * \rangle$ 和 $\langle B, \circ \rangle$ ，要么二者是单同态的，要么是满同态的，要么是同构的。

- ☐ A 上述论述正确
- ☒ B 上述论述错误

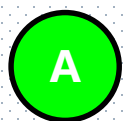
提交

给定代数系统 $\langle A, * \rangle$ ，单位元 $e$ 一定就是幂等元，任何幂等元也一定就是单位元。

- ☐ A 上述论述正确
- ☒ B 上述论述错误

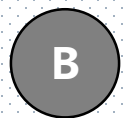
提交

设  $f$  是  $\langle A, * \rangle$  到  $\langle B, \circ \rangle$  的同构映射。 $e_A$  是  $\langle A, * \rangle$  的单位元， $e_B$  是  $\langle B, \circ \rangle$  的单位元，则  $f^{-1}(e_B) = e_A$ 。



A

上述论述正确



B

上述论述错误

提交





--伽罗瓦

1811-1832

# 伽罗瓦

- 伽罗瓦是法国数学家，群论的创建者。1811年10月25日生于拉赖因堡，1832年5月31日卒于巴黎。
- 于18岁时发表了第一篇论文。
- 伽罗瓦很早就开始了方程理论的研究，并提出了群的理论
- 伽罗瓦在解决代数方程的根式解问题中提出的群论，开辟了代数学的一个崭新的天地。

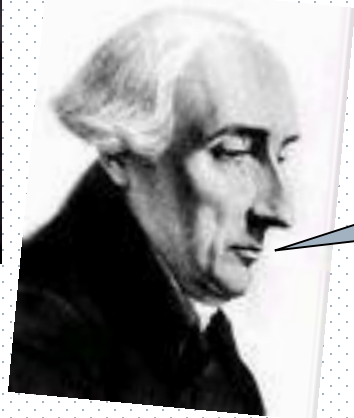


# 天才的童年

- 伽罗瓦的双亲都受过良好的教育。在父母的熏陶下，伽罗瓦童年时代就表现出有才能、认真、热心等良好的品格。
- 1823年10月伽罗瓦年满12岁时**，离开了双亲，考入有名的路易·勒·格兰皇家中学。从他的老师们保存的有关他在中学生活的回忆录和笔记中，记载着伽罗瓦是位具有“杰出的才干”，“举止不凡”，但又“**为人乖僻、古怪、过分多嘴**”性格的人。

# 数学世界的顽强斗士

- 伽罗瓦通过改进数学大师拉格朗日的思想，即设法绕过拉氏预解式，但又从拉格朗日那里继承了问题转化的思想，即把预解式的构成同置换群联系起来的的思想，并在阿贝尔研究的基础上，进一步发展了他的思想，把全部问题转化或归结为置换群及其子群结构的分析。



拉格朗日

阿  
尔



# 天才的陨落

□ 伽罗瓦诞生在拿破仑帝国时代，经历了波旁王朝的复辟时期，又赶上路易·腓力浦朝代初期，他是当时最先进的革命政治集团——共和派的秘密组织“人民之友”的成员，

•伽罗瓦敢于对政治上的动摇分子和两面派进行顽强的斗争，年轻热情的伽罗瓦对师范大学教育组织极为不满。

•在监狱中伽罗瓦一方面与官方进行不妥协的斗争，另一面他还抓紧时间刻苦钻研数学。尽管牢房里条件很差，生活艰苦，他仍能静下心来在数学王国里思考。

# 群论——跨时代的创造

- 伽罗瓦最主要的成就是提出了群的概念，并用群论彻底解决了根式求解代数方程的问题，而且由此发展了一整套关于群和域的理论，为了纪念他，人们称之为伽罗瓦理论。正是这套理论创立了抽象代数学，把代数学的研究推向了一个新的里程。正是这套理论为数学研究工作提供了新的数学工具——群论。它对数学分析、几何学的发展有很大影响，并标志着数学发展现代阶段的开始。

$\langle A, * \rangle$

代数系统

半群

含么半群

群 (环, 域)

群, 环, 域  
格

# Chapter 5

## 群 Group theory



## § 5.1 半群

(1)

### 5.1.1 半群的定义

**定义：**

设  $\langle S, * \rangle$  是一个代数系统，如果  $*$  运算满足结合律，则称  $\langle S, * \rangle$  是一个半群。

举例：  $\langle \mathbf{N}, + \rangle, \langle \mathbf{N}, \times \rangle, \langle \mathbf{Z}, + \rangle, \langle \mathbf{Z}, \times \rangle, \langle \mathbf{R}, + \rangle$

$\langle \mathbf{N}, - \rangle, \langle \mathbf{N}, \div \rangle, \langle \mathbf{Z}, - \rangle,$

## § 5.1 半群

举例： $\langle M_n(R), + \rangle$ ，**n**是大于等于**1**的正整数。

举例： $\langle M_n(R), \bullet \rangle$ ，**n**是大于等于**1**的正整数。

举例： $\langle \mathbf{P(S)}, \oplus \rangle$ ，**S**非空集合， $\oplus$ 是集合的对称差。

举例： $\langle A^A, \circ \rangle$ ，**A**非空集合， $\circ$ 是函数的复合运算。

以上系统都可以组成半群。

## § 5.1 半群

(2)

例：假设 $S=\{a,b,c\}$ ，在 $S$ 上定义运算 $\Delta$ ，如运算表给出。证明 $\langle S, \Delta \rangle$ 是半群。

$\Delta$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

验证 $\Delta$ 运算是可结合的。

$$(a \Delta b) \Delta c = a \Delta c = c$$

$$a \Delta (b \Delta c) = a \Delta c = c$$

$$(a \Delta b) \Delta c = a \Delta (b \Delta c)$$

$$(b \Delta a) \Delta c = b \Delta (a \Delta c) \text{等}$$

## § 5.1 半群

(2)

例:  $\langle \mathbf{N}, \circ \rangle$ , 在 $\mathbf{N}$ 上定义运算 $\circ$ , 如下:

$\mathbf{a} \circ \mathbf{b} = \mathbf{a} + \mathbf{b} + \mathbf{a} * \mathbf{b}$ , 证明 $\langle \mathbf{N}, \circ \rangle$  是半群;

定义如下:  $\mathbf{a} \circ \mathbf{b} = \mathbf{a} + \mathbf{b} - \mathbf{a} * \mathbf{b}$ , 如何?

$$(a \circ b) \circ c = (a \circ b) + c + (a \circ b) * c$$

$$= (a + b + a * b) + c + (a + b + a * b) * c$$

$$= a + b + c + a * b + a * c + b * c + a * b * c$$

$$a \circ (b \circ c) = \dots = (a \circ b) \circ c$$

$$(a \circ b) \circ c = (a \circ b) + c - (a \circ b) * c$$

$$= (a + b - a * b) + c + (a + b - a * b) * c$$

$$= a + b + c - a * b + a * c + b * c - a * b * c$$

$a \circ (b \circ c) = ?$  封闭性

## § 5.1 半群

(3)

### 5.1.1 半群的定义

**定义：**

假设  $\langle S, * \rangle$  是一个半群， $a \in S$ ， $n$  是正整数，则  $a^n$  表示  $n$  个  $a$  的计算结果，即  $a^n = a * a * \dots * a$   
对任意的正整数  $m, n$ ,

$$a^m * a^n = a^{m+n}, (a^m)^n = a^{mn}$$

## § 5.1 半群

(4)

### 5.1.2 交换半群

定义：

如果半群  $\langle S, * \rangle$  中的  $*$  运算满足交换律，则称  $\langle S, * \rangle$  为交换半群。

在交换半群  $\langle S, * \rangle$  中，若  $a, b \in S$ ， $n$  是任意正整数，则  $(a * b)^n = a^n * b^n$

## § 5.1 半群 (5)

### 5.1.3 独异点 (含幺半群)

定义:

假设  $\langle S, * \rangle$  是一个半群, 如果  $\langle S, * \rangle$  中有单位元, 则称  $\langle S, * \rangle$  是独异点, 或含幺半群。

$\langle \mathbf{N}, + \rangle, \langle \mathbf{N}, \times \rangle, \langle \mathbf{Z}, + \rangle, \langle \mathbf{Z}, \times \rangle, \langle \mathbf{R}, + \rangle$  是独异点吗?

$\langle \mathbf{N} - \{0\}, + \rangle, \langle \mathbf{N} - \{0\}, \times \rangle$  是独异点吗?

# 独异点（含幺半群）

举例： $\langle M_n(R), + \rangle$ ，**n**是大于等于**1**的正整数。

举例： $\langle M_n(R), \bullet \rangle$ ，**n**是大于等于**1**的正整数。

举例： $\langle A^A, \circ \rangle$ ，**A**非空集合， $\circ$ 是函数的复合运算。



练习：< $P(S)$ ,  $\oplus$ >,  $S$ 非空集合,  $\oplus$ 是集合的对称差, 则 $\oplus$ 运算的单位元是 **[填空1]**。

< $P(S)$ ,  $\cap$ >, 则 $\cap$ 运算的单位元是 **[填空2]**。

< $P(S)$ ,  $\cup$ >, 则 $\cup$ 运算的单位元是 **[填空3]**。

## § 5.1 半群

(6)

### 5.1.3 独异点 (含么半群)

**定理:** 假设  $\langle S, * \rangle$  是独异点, 如果  $a, b \in S$ , 并且  $a, b$  有逆元  $a^{-1}, b^{-1}$  存在, 则:

$$(1) (a^{-1})^{-1} = a;$$

$$(2) (a * b)^{-1} = b^{-1} * a^{-1}.$$

证明:  $\langle S, * \rangle$  是独异点, 单位元一定存在  $e \in S$ ,

$a^{-1}a = a a^{-1} = e$ ; 所以有  $(a^{-1})^{-1} = a$

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

## § 5.1 半群

(7)

### 5.1.4 子半群

定义：

假设  $\langle S, * \rangle$  是一个半群，若  $T \subseteq S$ ，且在  $*$  运算下也构成半群，则称  $\langle T, * \rangle$  是  $\langle S, * \rangle$  的子半群。

## § 5.1 半群

假设  $A = \{a, b\}$ ,  $\langle P(A), \cap \rangle$  是一个含么半群

若  $B = \{a\}$  则  $P(B) \subseteq P(A)$

并且  $\langle P(B), \cap \rangle$   
构成半群, 是  $\langle P(A), \cap \rangle$  的子  
半群。

还有否?

若  $B = \{b\}$ , 则  $P(B) \subseteq P(A)$

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{a, b\}$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$

## § 5.1 半群

(9)

### 5.1.4 子半群

**定义：**

设  $\langle S, * \rangle$  是含幺半群，若  $\langle T, * \rangle$  是它的子半群，并且  $\langle S, * \rangle$  的单位元  $e$  也是  $\langle T, * \rangle$  单位元，则称  $\langle T, * \rangle$  是  $\langle S, * \rangle$  的子含幺半群。

设  $\langle S, * \rangle$  是可交换的含么半群， $T = \{a \mid a \in S, \text{ 且 } a * a = a\}$ ，  
证明  $\langle T, * \rangle$  是  $\langle S, * \rangle$  的子含么半群。

## § 5.1 半群

(10)

例：设  $\langle S, * \rangle$  是可交换的含幺半群， $T = \{a \mid a \in S, \text{ 且 } a * a = a\}$ ，则  $\langle T, * \rangle$  是  $\langle S, * \rangle$  的子含幺半群。

解：

(1) 封闭  $\because a, b \in T \quad a * a = a, \quad b * b = b, \quad (a * b) * (a * b) = a * \textcolor{red}{a} * \textcolor{red}{b} * b = a * b$   
 $\therefore a * b \in T$

(2) 可结合  $*$  本来就是可结合的

(3) 单位元与  $S$  是同一个  $\because e * e = e; \therefore e \in T$

## § 5.2 群的概念及其性质

(1)

### 5.2.1 群的基本概念

定义：

设  $\langle G, * \rangle$  是一代数系统，如果满足以下几点：

(1) 运算是可结合的；

(2) 存在单位元  $e$ ；

(3) 对任意元素  $a$  都存在逆元  $a^{-1}$ ；

则称  $\langle G, * \rangle$  是一个群。 $|G|$ 表示群的阶



例：  $\langle \mathbf{R}, + \rangle$ ,  $\langle \mathbf{R} - \{0\}, \times \rangle$ , 构成群

(1) 运算是封闭的

(2) 运算是可结合的;

(3) 存在单位元  $e$ ;

(4) 对任意元素  $a$  都存在逆元  $a^{-1}$ ;

举例： $\langle M_n(R), + \rangle$ ，**n**是大于等于**1**的正整数。     √

举例： $\langle M_n(R), \bullet \rangle$ ，**n**是大于等于**1**的正整数。     ×

举例： **$\langle P(S), \oplus \rangle$** ，**S**非空集合， $\oplus$ 是集合的对称差。     √

举例： **$\langle P(S), \cap \rangle$** ， **$\langle P(S), \cup \rangle$**      ×

举例： **$\langle A^A, \circ \rangle$** ，**A**非空集合， $\circ$ 是函数的复合运算。后续分析

## § 5.2 群的概念及其性质

(2)

例：假设  $R = \{0, 60, 120, 180, 240, 300\}$  表示平面几何上图形绕形心顺时针旋转的角度集合。 $*$  是定义在  $R$  上的运算。定义如下：对任意的  $a, b \in R$ ， $a * b$  表示图形顺时针旋转  $a$  角度，再顺时针旋转  $b$  角度得到的总旋转度数。并规定旋转  $360$  度等于原来的状态，即该运算是模  $360$  的。整个运算可以用运算表表示。

## § 5.2 群的概念及其性质

*	0	60	120	180	240	300
0	0	60	120	180	240	300
60	60	120	180	240	300	0
120	120	180	240	300	0	60
180	180	240	300	0	60	120
240	240	300	0	60	120	180
300	300	0	60	120	180	240

设  $\langle R, * \rangle$  是一代数系统，满足以下几点：

- (1) 运算  $*$  “顺时针旋转的角度”是封闭的
- (2) 运算  $*$  “顺时针旋转的角度”是可结合的；
- (3) 存在单位元  $e=0$ ；
- (4) 对任意元素  $a$  都存在逆元  $a^{-1}$ ；

$$0*0=0; 60*300=0;$$

$$120*240=0; 180*180=0$$

$$0^{-1}=0; 60^{-1}=300; 120^{-1}=240; 180^{-1}=180$$

$\langle G, * \rangle$  是一个群。  $|G|=6$ ，六阶群

## § 5.2 群的概念及其性质

例：**A**是非空集合， $F = \{f \mid f : A \rightarrow A\}$ ，双射集

运算“ $\circ$ ”是函数的复合运算，

则 $\langle \mathbf{F}, \circ \rangle$ 是群

例1：  $A=\{1,2,3\}$

解： 双射的个数 **3!**，  $F=\{f_1, f_2, f_3, f_4, f_5, f_6\}$ ,

$$\begin{aligned} f_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \\ f_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ f_5 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{aligned}$$

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$

$$f_2 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_6$$

$$f_3 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5$$

$$f_4 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$



$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$

(1) 运算是可结合的;

(2) 存在单位元  $e$ ;  **$f_1 = I_A$**

(3) 对任意元素  $a$  都存在逆元  $a^{-1}$ ;

$f_1, f_2, f_3, f_4$  自身为逆元,  $f_5, f_6$  互为逆元

## § 5.2 群的概念及其性质

### 5.2.1 群的基本概念

一个群如果运算满足交换律，则称该群为交换群，或Abel群（阿贝尔）。

$$\forall a, b \in G \text{ 有 } \mathbf{a*b=b*a}$$

勒让德、拉普拉斯、傅立叶、泊松、柯西。

例  $\langle \mathbf{Z}_5, +_5 \rangle$  是可交换群。  $\langle \mathbf{Z}_m, +_m \rangle$  也是可交换群

$$(1) \forall [i], [j], [k] \in \mathbf{Z}_5$$

$$([i] +_5 [j]) +_5 [k] = \\ [i] +_5 ([j] +_5 [k]) = \\ [(i+j+k) \bmod 5]$$

$$(2) e = [0]$$

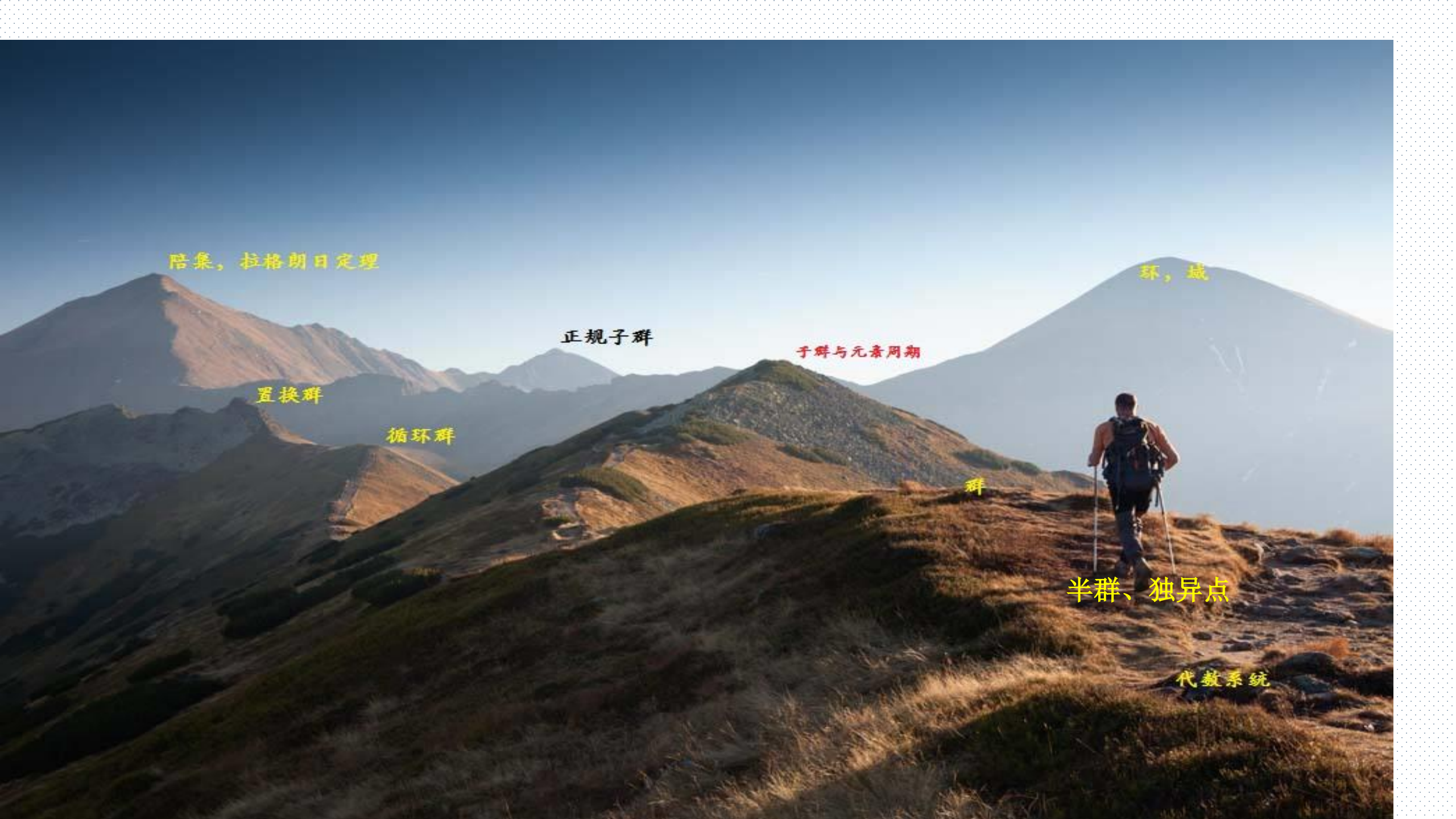
$$(3) \forall [i] \in \mathbf{Z}_5$$

$$[i]^{-1} = [-i] = [5-i]$$

$$(4) \forall [i], [j] \in \mathbf{Z}_5$$

$$[i] +_5 [j] = [j] +_5 [i] = [(i+j) \bmod 5]$$

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]



陪集, 拉格朗日定理

正规子群

子群与元素周期

环, 域

置换群

循环群

群

半群、独异点

代数系统

## § 5.2 群的概念及其性质

(5)

### 5.2.2 群的性质

- (1) 任何群都没有零元。
- (2) 设  $\langle G, * \rangle$  是群，则  $G$  中消去律成立。
- (3) 设  $\langle G, * \rangle$  是群，单位元  $e$  是  $G$  中的唯一幂等元。

## § 5.2 群的概念及其性质

(6)

### 5.2.2 群的性质

- (4) 设  $\langle G, * \rangle, \langle H, \circ \rangle$  是群,  $f$  是  $G$  到  $H$  的同态, 若  $e$  为  $\langle G, * \rangle$  的单位元, 则  $f(e)$  是  $\langle H, \circ \rangle$  的单位元, 并且对任意  $a \in G$ , 有  $f(a^{-1}) = f(a)^{-1}$ 。
- (5) 设  $\langle G, * \rangle$  是群,  $\langle H, \circ \rangle$  是任意代数系统, 若存在  $G$  到  $H$  的满同态映射, 则  $\langle H, \circ \rangle$  必是群。

## § 5.2 群的概念及其性质

(9)

### 5.2.4 有限群的性质

**定理：**

设  $\langle G, * \rangle$  是一个  $n$  阶有限群，它的运算表中的每一行（每一列）都是  $G$  中元素的一个全排列。

## § 5.2 群的概念及其性质

(10)

### 5.2.4 有限群的性质

*	e
e	e

一阶群

*	e	a
e	e	a
a	a	e

二阶群

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

三阶群

??



## § 5.2 群的概念及其性质

### 5.2.4 有限群的性质

填**e**

*	e	a	b
e	e	a	b
a	a	e	?
b	b	?	e

×

填**b**

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

✓

填**a**

*	e	a	b
e	e	a	b
a	a	a	?
b	b	?	?

×

三阶群（唯一）

# § 5.2 群的概念及其性质

(11)

## 5.2.4 有限群的性质

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



每个元素自身为逆元

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

*	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e



两个元素（包括 $\mathbf{e}$ ）自身为逆元  
另两个元素互为逆元

## § 5.2 群的概念及其性质

例:  $\langle \mathbf{G}, * \rangle$  是可交换(**ABEL**)群的充要条件是  $\forall a, b \in \mathbf{G}$  有  $(a*b)*(a*b)=(a*a)*(b*b)$

解: 充分性  $\forall a, b \in \mathbf{G}$  有  $(a*b)*(a*b)=(a*a)*(b*b)$   
则  $\langle \mathbf{G}, * \rangle$  是可交换(**ABEL**)群。

必要性  $\langle \mathbf{G}, * \rangle$  是可交换(**ABEL**)群则有  $\forall a, b \in \mathbf{G}$  有  $(a*b)*(a*b)=(a*a)*(b*b)$

例：任何阶数是**1,2,3,4**阶的群都是可交换  
(**ABEL**)群。

**1**阶群是可交换(**ABEL**)群， $G=\{e\}$

**2**阶群是可交换(**ABEL**)群， $G=\{e,a\}$

**3**阶群是可交换(**ABEL**)群， $G=\{e,a,b\}$

若 $a*b=a$  则 $a^{-1}*a*b=a^{-1}*a=e, b=e$

若 $a*b=b$  则 $a*b*b^{-1}=b*b^{-1}=e, a=e$

只有  $a*b=e, b*a=b*a*e=b*a*(b*b^{-1})$   
 $=b*(a*b)*b^{-1}=b*e*b^{-1}=b*b^{-1}=e$

$a*b=b*a$

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

**4阶的群都是可交换(ABEL)群。**

**4阶群是可交换(ABEL)群,  $G=\{e,a,b,c\}$**

**(1)  $a,b,c$  自为逆元,**

**则  $a*b=b*a=c$ ;  $b*c=c*b=a$ ;**

**$c*a=a*c=b$  交换律满足**

**(2)  $a,b,c$  两个元素互为逆元, 如  $a,b$  互为逆元**

**若  $a*b=b*a=e$**

**则  $c*c=e$ ,  $a*c \neq e$ ,  $a*c=b$**

**同理  $c*a=b$  所以  $a*c=c*a$ ,**

**同理  $b*c=c*b$**

## § 5.2 群的概念及其性质

例：假设  $\langle G, * \rangle$  是一个二阶群，则  $\langle G \times G, * \rangle$  是一个Klein群。且是可交换（**abel**）群。

$$G = \{e, a\}$$

$$G \times G = \{ \langle e, e \rangle, \langle e, a \rangle, \langle a, e \rangle, \langle a, a \rangle, \}$$

$$\langle e, e \rangle * \langle e, e \rangle = \langle e * e, e * e \rangle = \langle e, e \rangle$$

$$\langle e, e \rangle * \langle e, a \rangle = \langle e * e, e * a \rangle = \langle e, a \rangle$$

$$\langle a, a \rangle * \langle a, a \rangle = \langle a * a, a * a \rangle = \langle e, e \rangle$$

# § 5.2 群的概念及其性质

*	<e,e>	<e,a>	<a,e>	<a,a>
<e,e>	<e,e>	<e,a>	<a,e>	<a,a>
<e,a>	<e,a>	<e,e>	<a,a>	<a,e>
<a,e>	<a,e>	<a,a>	<e,e>	<e,a>
<a,a>	<a,a>	<a,e>	<e,a>	<e,e>

同构  
 $\cong$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$G \rightarrow G \times G$ ; 定义如下双射  
 $e \rightarrow \langle e,e \rangle, a \rightarrow \langle e,a \rangle,$   
 $b \rightarrow \langle a,e \rangle, c \rightarrow \langle a,a \rangle$

## § 5.2 群的概念及其性质

(7)

### 5.2.3 半群与群

(1) 假设  $\langle G, * \rangle$  是半群, 并且

①  $\langle G, * \rangle$  中有一左单位元  $e$ , 使得对任意的  $a \in G$ , 有  $e * a = a$ ;

②  $\langle G, * \rangle$  中任意元素  $a$  都有“左逆元”  $a^{-1}$ , 使得  $a^{-1} * a = e$ 。

则  $\langle G, * \rangle$  是群。

$$a^{-1} * a = e, \text{ 有 } a^{-1} \in G, \quad (a^{-1})^{-1} \in G$$

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

$$a e = a(a^{-1}a) = ea = e$$



## § 5.2 群的概念及其性质

(8)

### 5.2.3 半群与群

(2) 有限半群，如果消去律成立，则必为群。

*	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

任何群中都有单位元 $e$ ,且单位元是群中的唯一幂等元。

- ☒ A 上述论述正确。
- ☐ B 上述论述错误。

提交

一阶群 $\langle A, * \rangle$ 中有单位元 $e$ ，即 $e \in A$ ，而一阶群 $|A|=1$ ，也就是说集合 $A$ 中只有一个元素，所以单位元 $e$ 的逆元不存在。

- ☐ A 上述论述正确。
- ☒ B 上述论述错误。

提交

设 $\mathbf{G}=\mathbf{R}\times\mathbf{R}$ ， $\mathbf{R}$ 是实数集， $\mathbf{G}$ 上的二元运算定义如下：

$\forall \langle x, y \rangle \in \mathbf{R}\times\mathbf{R}$ 代表平面坐标系中的一点，定义 $+$ 运算

$$\langle x_1, y_1 \rangle + \langle x_2, y_2 \rangle = \langle x_1 + x_2, y_1 + y_2 \rangle$$

则 $\langle \mathbf{G}, + \rangle$  是群。

A

上述论述正确。

B

上述论述错误。

提交

设  $G = R \times R$ ,  $R$  是实数集,  $G$  上的二元运算定义如下;

$\forall \langle x, y \rangle \in R \times R$  代表平面坐标系中的一点, 定义  $+$  运算

$\langle x_1, y_1 \rangle + \langle x_2, y_2 \rangle = \langle x_1 + x_2, y_1 + y_2 \rangle$ , 则  $\langle G, + \rangle$  构成群。

设  $H = \{ \langle x, y \rangle \mid y = 2x \}$ , 则  $\langle H, + \rangle$  是  $G$  的子群。



A

上述论述正确。



B

上述论述错误。

提交

代数系统 $\langle \mathbf{R}, + \rangle$ ,  $\langle \mathbf{R} - \{0\}, \times \rangle$ 都可以构成群。 $+$ 的单位元是 **【填空1】**； $\times$ 的单位元是 **【填空2】**。

## § 5.3 子群与元素周期

### 5.3.1 子群

定义：

设  $\langle G, * \rangle$  是一个群，非空集合  $H \subseteq G$ 。如果  $H$  在  $G$  的运算下也构成群，则称  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的子群。

## § 5.3 子群与元素周期

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$H_0 = \{e\}$$

$$H_1 = \{e, a\}$$

$$H_2 = \{e, b\}$$

$$H_3 = \{e, c\}$$

$H_4 = \{e, a, b\}$  ? 不能构成  $G$  的子群



## § 5.3 子群与元素周期

(2)

### 5.3.1 子群

**定理：**

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的子群，则

(1)  $\langle H, * \rangle$  的单位元  $e_H$  一定是  $\langle G, * \rangle$  的单位元，即

$$e_H = e_G.$$

(2) 对  $a \in H$ ， $a$  在  $H$  中的逆元  $a'$ ，一定是  $a$  在  $G$  中的逆元。

## § 5.3 子群与元素周期

(3)

### 5.3.2 由子集构成子群的条件

(1) 设  $H$  是群  $\langle G, * \rangle$  中  $G$  的非空子集, 则  $H$  构成  $\langle G, * \rangle$  子群的充要条件是:

① 对  $\forall a, b \in H$ , 有  $a * b \in H$ ;

② 对  $\forall a \in H$ , 有  $a^{-1} \in H$ 。

由① 对  $\forall a, b \in H$ , 有  $a * b \in H$ ; ② 对  $\forall a \in H$ , 有  $a^{-1} \in H$ 。  
 $a * a^{-1} \in H; e \in H$

## § 5.3 子群与元素周期

(4)

### 5.3.2 由子集构成子群的条件

#### (2) 推论 (子群的判定条件)

假设  $\langle G, * \rangle$  是群,  $H$  是  $G$  的非空子集, 则  
 $\langle H, * \rangle$  是  $\langle G, * \rangle$  子群的充要条件是:

对  $\forall a, b \in H$ , 有  $a * b^{-1} \in H$ 。

对  $\forall a, b \in H$ , 有  $a * b^{-1} \in H$ 。

有  $a * a^{-1} \in H$ ;  $e \in H$ ;  $a * b = a * (b^{-1})^{-1} \in H$

## § 5.3 子群与元素周期

(5)

### 5.3.2 由子集构成子群的条件

#### (3) (子群的判定条件)

假设  $\langle G, * \rangle$  是一个群,  $H$  是  $G$  的非空有限子集,  
则  $\langle H, * \rangle$  是  $\langle G, * \rangle$  子群的充要条件是:

对  $\forall a, b \in H$ , 有  $a * b \in H$ 。

分析证明。多种思路

## § 5.3 子群与元素周期

假设  $\langle G, * \rangle$  是一个群,  $H$  是  $G$  的非空有限子集, 则  $\langle H, * \rangle$  是

$\langle G, * \rangle$  子群的充要条件是: 对  $\forall a, b \in H$ , 有  $a * b \in H$ 。

证明: 充分性,  $H \neq \emptyset$ ,  $H \subseteq G$ , 且  $|H| = m$ , 若  $a \in H$

则  $a * a \in H, a * a * a \in H \dots \dots$

即  $a, a^2, \dots, a^m, a^{m+1} \in H (a^0 = e)$ , 而  $H$  只有  $m$  个元素,

$\therefore a$  的  $m+1$  个幂元素中至少有两个相等, 不妨设  $a^t = a^s (1 \leq t < s \leq m+1)$ ,

$$\therefore a^t = a^s = a^{s-t} * a^t$$

即  $a^0 * a^t = a^{s-t} * a^t$  根据消去率有,  $a^{s-t} = a^0 (e) \in H$  (有单位元)

设  $r = s - t$  则  $e = a^r = a^{r-1} * a = a * a^{r-1}$

则  $a$  与  $a^{r-1}$  互为逆元

$\therefore H$  为  $G$  的子群

必要性: 略

## § 5.3 子群与元素周期

(6)

### 5.3.3 元素的周期

#### (1) 群中元素的幂运算

假设  $\langle G, * \rangle$  是一个群,  $a \in G$ 。

则  $a^0 = e$ ;  $a^{i+1} = a^i * a$ ;

$$\begin{aligned}(a^i)^{-1} &= a^{-i} = (a^{-1})(a^{-1}) \dots (a^{-1}) \\ &= (a^{-1})^i \quad (i \geq 0);\end{aligned}$$

$$a^m * a^n = a^{m+n};$$

$$(a^m)^n = a^{mn} \quad (m, n \text{ 为整数})。$$

## § 5.3 子群与元素周期

(7)

### 5.3.3 元素的周期

#### (2) 元素的周期

**定义：** 设  $\langle G, * \rangle$  是一个群， $a \in G$ 。若存在正整数  $n$ ，使得  $a^n = e$ ，则将满足该条件的最小正整数  $n$  称为元素  $a$  的周期或阶。若这样的  $n$  不存在，则称元素  $a$  的周期无限。元素  $a$  的周期记为：  $|a|$

## § 5.3 子群与元素周期

例：  $\langle \mathbb{Z}_4, +_4 \rangle$  是一个群，其中  $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ ，其运算表如右图。

$$[0]^1 = [0] \quad |[0]| = 1$$

$$[1]^4 = [0] \quad |[1]| = 4$$

$$[2]^2 = [0] \quad |[2]| = 2$$

$$[3]^4 = [0] \quad |[3]| = 4$$

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

元素的周期有三种值 **1**， **2**， **4**



## § 5.3 子群与元素周期

例： $\langle \mathbb{Z}_5, +_5 \rangle$ 是一个群，其中 $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ ，其运算表如右图。

$$[0]^1 = [0] \quad |[0]| = 1$$

$$[1]^5 = [0] \quad |[1]| = 5$$

$$[2]^5 = [0] \quad |[2]| = 5$$

$$[3]^5 = [0] \quad |[3]| = 5$$

$$[4]^5 = [0] \quad |[4]| = 5$$

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

元素的周期有三种值**1**，**5**

## § 5.3 子群与元素周期

例：群 $\langle \mathbb{Z}_4, +_4 \rangle$ 的子群。

子群： $\langle \mathbb{Z}_1, +_4 \rangle$ ,  $\langle \mathbb{Z}_4, +_4 \rangle$

$$\mathbb{Z}_1 = \{[0]\},$$

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$$

子群： $\langle \mathbb{Z}_2, +_4 \rangle$

$$\mathbb{Z}_2 = \{[0], [2]\}$$

元素的周期有三种值**1**, **2**, **4**;

有三种阶的子群

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

## § 5.3 子群与元素周期

例：群 $\langle \mathbb{Z}_5, +_5 \rangle$ 的子群。

子群： $\langle \mathbb{Z}_1, +_5 \rangle$ ,  $\langle \mathbb{Z}_5, +_5 \rangle$

$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ ,

$\mathbb{Z}_1 = \{[0]\}$ ,

元素的周期有亮种值**1**, **5**；也有两种阶的子群

$\mathbb{Z}_2 = \{[0], [2]\}$  ?  $\langle \mathbb{Z}_2, +_5 \rangle$ , 不封闭所以不是！

## 定义：循环群(下节)

设  $\langle G, * \rangle$  是一个群，若在  $G$  中存在一个元素  $a$ ，使得  $G$  中任意元素都由  $a$  的幂组成，即  $G = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$ ，则称该群为循环群，元素  $a$  称为循环群的生成元。

例:  $\langle \mathbb{Z}_4, +_4 \rangle$  群

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\},$$

循环(子)群

$$\mathbb{Z}_1 = \{[0]\} = ([0]) = \{[0]^0\},$$

$$\begin{aligned}\mathbb{Z}_2 &= ([2]) = \{[2]^0, [2]^1\} \\ &= \{[0], [2]\}\end{aligned}$$

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$$[1]^1 = [1], [1]^2 = [2], [1]^3 = [3], [1]^4 = [0]$$

$$([1]) = \{[1]^1, [1]^2, [1]^3, [1]^4\} = \mathbb{Z}_4, [1] \text{ 是 } \mathbb{Z}_4 \text{ 生成元}$$

例:  $\langle \mathbb{Z}_5, +_5 \rangle$  是一个群,

其中  $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ ,

$$[1]^1 = [1], [1]^2 = [2], [1]^3 = [3], [1]^4 = [4], [1]^5 = [0]$$

$([1]) = \{[1]^1, [1]^2, [1]^3, [1]^4, [1]^5\} = \mathbb{Z}_5$ ,  $[1]$  是生成元

$$[2]^1 = [2], [2]^2 = [4], [2]^3 = [1], [2]^4 = [3],$$

$[2]^5 = [0]$  所以  $([2]) = \mathbb{Z}_5$   $[2]$  是生成元

$$([3]) = \mathbb{Z}_5 \quad ([4]) = \mathbb{Z}_5$$

对  $\langle \mathbb{Z}_5, +_5 \rangle$  群除  $[0]$  外其它元素都是生成元

例:  $\langle \mathbb{Z}_4, +_4 \rangle$  群

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ ,

循环(子)群

$([0]) = \{[0]\}$ , 一阶群;  $|[0]| = 1$  元素 $[0]$ 的周期是1

$([2]) = \{[0], [2]\}$  二阶群;  $|[2]| = 2$  元素 $[2]$ 的周期是1

$|[0]| = [0]$  元素的周 = 1  $|([0])| =$  元素 $[0]$ 生成的循环群的阶为1

所以有  $|[0]| = |([0])| = 1$

同样有  $|[2]| = |([2])| = 2$

结论:  $a$  的周期等于  $a$  生成的循环子群 $(a)$   
的阶。 即  $|a| = |(a)|$ ;

例：群  $R = \{0, 60, 120, 180, 240, 300\}$

$$(60) = R,$$

$$(120) = \{120^0, 120^1, 120^2\} = \{0, 120, 240\}$$

$$|60| = 6, |(60)| = 6, |120| = 3, |(120)| = 3$$

$$|60| = |(60)| = 6$$

$$|120| = |(120)| = 3$$

满足：a 的周期等于 a 生成的循环子群(a)  
的阶。 即  $|a| = |(a)|$ ;



例：

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$$\mathbf{b^1=b, \quad b^2=b*b=a}$$

$$\mathbf{b^3=a*b=c}$$

$$\mathbf{b^4=c*b=e}$$

$$\mathbf{(b)=\{b^1,b^2,b^3,b^4\}} \\ \mathbf{=\{b, a, c, e \}}$$

所以有  $|b|=|(b)|=4$

## § 5.3 子群与元素周期

### 5.3.3 元素的周期

#### (3) 元素周期的性质

设  $\langle G, * \rangle$  是一个群,  $a \in G$ 。

①  $a$  的周期等于  $a$  生成的循环子群  $\langle a \rangle$  的阶。

即  $|a| = |\langle a \rangle|$ ;

② 若  $a$  的周期为  $n$ , 则  $a^m = e$  的充分必要条件是  $n|m$ 。

## § 5.3 子群与元素周期

设 $\langle G, * \rangle$ 是一个群,  $a \in G$

①  $a$ 的周期等于  $a$  生成的循环子群 $(a)$ 的阶。 即  $|a| = |(a)|$

设 $a$ 的周期为有限 $n$ , 即 $|a| = n$ ,  $(a) = \{a^0, a^1, a^2, \dots, a^{n-1}\}$

$\forall a^i \in (a)$ , 则 $i = kn + r$ , 其中 $k, r \in \mathbb{Z}$ ,  $0 \leq r < n$

$$a^i = a^{kn+r} = a^{kn} a^r = (a^n)^k a^r = (e^n)^k a^r = a^r$$

$$a^i \in \{a^0, a^1, a^2, \dots, a^{n-1}\} \quad (a) \subseteq \{a^0, a^1, a^2, \dots, a^{n-1}\}$$

又因为 $\{a^0, a^1, a^2, \dots, a^{n-1}\} \subseteq (a)$  所以 $\{a^0, a^1, a^2, \dots, a^{n-1}\} = (a)$

## § 5.3 子群与元素周期

$$\{a^0, a^1, a^2, \dots, a^{n-1}\} = (a) \quad |a|=n, |(a)|=n ?$$

若  $a^i = a^j, 0 \leq i, j < n, i \neq j$

则  $a^{i-j} = e, 0 < i-j < n$ , 与  $a$  的周期为  $n$  矛盾

所以  $a^0, a^1, a^2, \dots, a^{n-1}$  互不相同

$$|(a)|=n, \text{ 又 } |a|=n$$

$$|(a)| = |a|$$

## § 5.3 子群与元素周期

设 $\langle G, * \rangle$ 是一个群,  $a \in G$

①  $a$ 的周期等于  $a$  生成的循环子群 $\langle a \rangle$ 的阶。 即  $|a| = |\langle a \rangle|$

② 若  $a$  的周期为  $n$ , 则  $a^m = e$  的充分必要条件是  $n|m$ 。

必要性: 若  $n|m$ , 有  $a^m = e$

若  $n|m$ , 设 $m=kn, k \in \mathbf{Z}$

所以  $a^m = (a^k)^n = (a^n)^k = e^k = e$

充分性:  $a^m = e$ , 则 $n|m$ ,

设 $m=kn+r$ , 其中  $k \in \mathbf{Z}, 0 \leq r < n$

所以  $a^m = (a^k)^n a^r = (a^n)^k a^r = e^k a^r = a^r$

$a^r = e, 0 \leq r < n$ , 因为 $a$ 的周期为 $n$ ,

所以只能 $r=0$ , 即 $n|m$

## § 5.3 子群与元素周期

### 5.3.3 元素的周期

#### (3) 元素周期的性质

**推论：**

设  $\langle G, * \rangle$  是一个群， $a \in G$ 。若  $a$  的周期为  $n$ ，则

$$(a) = \{a^0, a^1, \dots, a^{n-1}\}。$$

## § 5.3 子群与元素周期

例1 假设 $\langle G, * \rangle$ 是一个群， $|G|=2n$ ，证明 $G$ 中至少有一个周期为2的元素。  
(在偶数阶群中至少有一个周期为2的元素)

$$G = \{\text{元素与元素的逆元不同}\} \cup \{\text{元素与元素的逆元相同}\}$$

证明：因为群 $\langle G, * \rangle$ 中的元素互逆，即元素 $a$ 的逆元是 $a^{-1}$ ， $a^{-1}$ 的逆元是 $a$ 。因而 $G$ 中逆元不等于自身的元素必为偶数个（包括零个）。

但是 $G$ 有偶数个元素，因此 $G$ 的逆元等于自身的元素个数也必为偶数个，而 $G$ 的单位元 $e$ 的逆元是其本身，所以 $G$ 中至少还有另一个元素 $a$ 其逆元是它本身，即 $a^{-1}=a$ 。

从而  $a^2 = a * a = a * a^{-1} = e$ ，并且 $e \neq a$ 。即  $a$ 是一个周期为2 的元素

所以至少存在一个周期为2的元素。

## § 5.3 子群与元素周期

例2 假设 $\langle G, * \rangle$ 是可交换群,  $a, b \in G$ ,  $|a|=2, |b|=3$

证明  $|a*b|=6$

证明: 因为 $(a*b)^6 = a^6 * b^6 = (a^2)^{*3} * (b^3)^{*2} = e$

故  $a*b$  必有有限周期

设  $|a*b|=n$ , 则  $n|6$

故  $n$  有4种可能, 即  $n=1, 2, 3, 6$

若  $n=1$ , 则  $a*b=e$ , 所以  $b=a^{-1}$ ,  $b^2=(a^{-1})^2=(a^2)^{-1}=e$ ,  $b^2=e$  矛盾

若  $n=2$ , 则  $(a*b)^2=a^2*b^2=b^2=e$ ,  $b^2=e$  矛盾

若  $n=3$ , 则  $(a*b)^3=a^3*b^3=a^3=a*a^2=a=e$ ,  $a=e$  矛盾

因此,  $n=6$ 。



## § 5.3 子群与元素周期

例3  $\langle G, * \rangle$ 是群,  $a \in G$ , 则元素 $a$ 的周期与 $a^{-1}$  的周期相同。

证明: 设元素 $a$ 的周期为 $r$ , 元素 $a^{-1}$ 的周期为 $t$ ,  $a^r = e$ ,  $(a^{-1})^t = e$

则  $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$ ; 因为元素 $a^{-1}$ 的周期为 $t$ ,  
所以  $t \leq r$  另  $t | r$

又有  $a^t = (a^{-t})^{-1} = ((a^{-1})^t)^{-1} = e^{-1} = e$ , 因为元  
素 $a$ 的周期为 $r$ , 所以  $r \leq t$  另  $r | t$

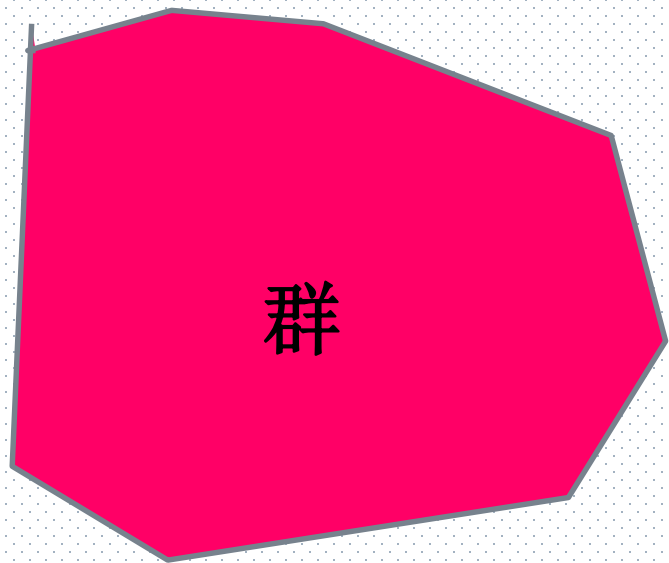
所以  $r = t$

在 $\langle \mathbb{Z}_5, +_5 \rangle$ 群中，其中 $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ ，各元素的周期分别为。元素 $[0]$ 的周期为 [填空1] ,元素 $[1]$ 的周期为 [填空2] ,元素 $[2]$ 的周期为 [填空3] ,元素 $[3]$ 的周期为 [填空4] ,元素 $[4]$ 的周期为 [填空5] 。

正常使用填空题需3.0以上版本雨课堂

作答

$\langle \mathbf{A}, * \rangle$



1、群的阶  $|\mathbf{G}|$  有限/无限

2、子群  $\mathbf{S} \subseteq \mathbf{G}$  如  $\mathbf{S} = \{\mathbf{e}\}$

3、群中元素的周期  $\forall a \in \mathbf{G} \quad |a| = n$   
 $n$  可以是自然数（奇，偶数）也可能是无限

4、 $\langle \mathbf{G}, * \rangle$  群中，  $\forall a \in \mathbf{G} \quad |a| = |(a)|$

$|a| = |a^{-1}|$ ，在偶数阶群中至少有一个周期为2的元素。

。。

？，群中任何元素的周期一定是群的阶的正因子？  
循环群，置换群，群同态？

## § 5.4 循环群

(1)

### 5.4.1 定义

设  $\langle G, * \rangle$  是一个群，若在  $G$  中存在一个元素  $a$ ，使得  $G$  中任意元素都由  $a$  的幂组成，即  $G = (a) = \{a^i \mid i \in \mathbb{Z}\}$ ，则称该群为循环群，元素  $a$  称为循环群的生成元。

例：群 $R=\{0,60,120,180,240,300\}$   
 $(60)=R$ ,生成元是60

例：  $\langle \mathbb{Z}_n, +_n \rangle$  ,生成元是1,  $([1])=\mathbb{Z}_n$  还有其它生成元？

例：

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$$\mathbf{a^0=e}$$

$$\mathbf{a^1=a}$$

$$\mathbf{a^2=b}$$

生成元是**a或b**  
 $(a)=G; (b)=G$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

生成元是**b或c**  
 $(b)=G; (c)=G$

**a为什么不是生成元。**

例： $\langle G, \times_7 \rangle$ 是一个群，即 $\langle \mathbb{Z}_7 - \{[0]\}, \times_7 \rangle$

其中 $G = \{[1], [2], [3], [4], [5], [6]\}$ ，其运算表如图。

是否是循环群？生成元是什么？

$\times_7$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

$$[3]^0 = [1] \text{ (e)}$$

$$[3]^1 = [3]$$

$$[3]^2 = [2]$$

$$[3]^3 = [6]$$

$$[3]^4 = [4]$$

$$[3]^5 = [5]$$

还有其它生成元吗？

例:  $\langle G, \times_7 \rangle$  是一个群, 即  $\langle \mathbb{Z}_7 - \{[0]\}, \times_7 \rangle$

其中  $G = \{[1], [2], [3], [4], [5], [6]\}$ , 其运算表如图。

- ☒ A **[5]** 是群的生成元
- ☐ B **[6]** 是群的生成元
- ☐ C **[5], [6]** 都是群的生成元
- ☐ D **[5], [6]** 都不是群的生成元

$\times_7$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

提交

例:  $\langle \mathbb{Z}, + \rangle$  是循环群, 生成元有几个?

解:  $(1) = \{i \mid i \in \mathbb{Z}\} = \mathbb{Z}$

$$1^0 = 0 \text{ (e)}, \quad 1^\infty = 0 \text{ (e)}$$

$$\forall m \in \mathbb{Z}, m = 1 + 1 + \dots + 1 = 1^m \text{ (是一种表示方式)}$$

$$\forall -m \in \mathbb{Z},$$

$$\begin{aligned} -m &= (-1) + (-1) + \dots + (-1) = (-1)^m \\ &= (1^{-1})^m = 1^{-m} \end{aligned}$$

$(2) = \{2i \mid i \in \mathbb{Z}\} \neq \mathbb{Z}$  所以 **1** 不是生成元

另外 **-1** 是生成元吗?



$$(-1)^0 = 0(e), \quad (-1)^\infty = 0(e)$$

$$1^{-1} = (-1)$$

$\forall m \in \mathbf{Z}, m = 1 + 1 + \dots + 1 = 1^m = (1^{-1})^{-m}$  是一种表示方式

$$\exists -m \in \mathbf{Z},$$

$$-m = (-1) + (-1) + \dots + (-1) = (-1)^m$$

$(2) = \{2i \mid i \in \mathbf{Z}\} \neq \mathbf{Z}$  所以 2 不是生成元

生成元有 2 个, **1**, **-1** ( $\langle \mathbf{Z}, + \rangle$  是无限循环群)

## § 5.4 循环群

### 5.4.2 循环群的性质

(1) 设  $\langle G, * \rangle$  是一个循环群。

① 若  $\langle G, * \rangle$  是  $n$  阶有限群循环群，

则  $\langle G, * \rangle \cong \langle \mathbb{Z}_n, +_n \rangle$ ;

② 若  $\langle G, * \rangle$  是无限群循环群，则

$\langle G, * \rangle \cong \langle \mathbb{Z}, + \rangle$ 。

## § 5.4 循环群

(1) 设  $\langle G, * \rangle$  是一个循环群。

① 若  $\langle G, * \rangle$  是  $n$  阶有限群, 则

$$\langle G, * \rangle \cong \langle \mathbb{Z}_n, +_n \rangle;$$

$G$  是  $n$  阶有限循环群, 则一定存在生成元  $a$ ,  $G = (a) = \{a^i \mid i \in \mathbb{N}\} = \{a^0, a^1, \dots, a^{n-1}\}$

定义映射  $f: [i] \rightarrow a^i, \forall [i] \in \mathbb{Z}_n$

显然  $f$  是满射.

若  $i \neq j$  即  $[i] \neq [j]$ , 并有  $a^i \neq a^j$  所以  $f$  也是单射

所以  $f$  是双射

$$f([i] +_n [j]) = f([i+j]) = a^{i+j} = a^i * a^j = f([i]) * f([j])$$

所以  $G$  与  $\mathbb{Z}_n$  同构 ( $G \cong \mathbb{Z}_n$ )

无限循环群同构于整数加群。证明类似

## § 5.4 循环群

### 5.4.2 循环群的性质

#### (2) 循环群的子群必为循环群

例:  $\langle \mathbb{Z}_6, +_6 \rangle$  群  $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ ,

循环(子)群:

$$([0]) = \{[0]\},$$

$$([2]) = \{[0], [2], [4]\} = \{[2]^0, [2]^1, [2]^2\}$$

## § 5.4 循环群

证明：循环群的子群必为循环群

$G$ 是循环群,则一定存在生成元 $a$ ,  $G = \langle a \rangle$

设 $H$ 是其子群,

(1) 若 $H = \{e\} = \{a^0\}$ ,  $e$ 是 $H$ 的生成元

(2) 若 $H \neq \{e\}$  则 $H = \{a^{n_1}, a^{n_2}, a^{n_3}, \dots\}$

令 $i_0 = \min\{n_i \mid a^{n_i} \in H, n_i > 0\}$  (只要证明 $H = \langle a^{i_0} \rangle$ )

对于 $\forall a^i \in H, i > i_0$

则  $i = ki_0 + r, 0 \leq r < i_0, k \in \mathbb{N}$

## § 5.4 循环群

$$a^i = a^{ki_0+r} = a^{ki_0} a^r$$

$$a^r = a^{-ki_0} a^i \quad \text{由封闭性可知 } a^r \in H$$

因为  $0 \leq r < i_0$  且  $i_0$  是最小正指数，所以  $r=0$

$$a^i = a^{ki_0} = (a^{i_0})^k \quad \text{所以 } H = \langle a^{i_0} \rangle$$

## § 5.4 循环群

### 5.4.2 循环群的性质

(3) 设  $\langle G, * \rangle$  是  $n$  阶循环群,  $m$  是正整数, 并且  $m \mid n$ , 则  $G$  中存在唯一一个  $m$  阶子群。

例:  $\langle \mathbb{Z}_6, +_6 \rangle$  群  $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ , 其子群:

六阶循环群必有1阶、2阶、3阶、6阶(循环)子群。

$$([0]) = \{[0]\},$$

$$([2]) = \{[0], [2], [4]\}$$

其**2**阶子群是谁?  $\{[0], [3]\}$

## § 5.4 循环群

### 5.4.2 循环群的性质

设  $\langle G, * \rangle$  是  $n$  阶循环群,  $m$  是正整数, 并且  $m \mid n$ , 则  $G$  中存在唯一一个  $m$  阶子群。

因为  $m \mid n$ , 设  $n = dm$ ,  $(a^d)^m = a^{dm} = a^n = e$ , ( $a^d$  的周期是  $m$ ?)

对于  $\forall h \in \mathbb{N}$ , 若  $0 < h < m$  则  $0 < dh < dm = n$

$(a^d)^h = a^{dh} \neq e$ , 所以  $a^d$  的周期是  $m$  (说明  $m$  是最小的)

所以  $a^d$  作为生成元生成的是  $m$  阶子群,  $A = \langle a^d \rangle$ ,  $|A| = m$ ; 找到了  $m$  阶子群, 唯一吗?



## § 5.4 循环群

设 $H$ 是 $G$ 的另一 $m$ 阶子群, 即  $H = \langle a^i \rangle$ ,  $(a^i)^m = a^{im} = e$

所以有 $n \mid im$  即  $dm \mid im$  所以有 $d \mid i$

设 $i = kd$ ,  $a^i = a^{kd} = (a^d)^k$

所以有 $a^i \in A$ , 对于 $j \in \mathbb{Z}$ ,  $(a^i)^j \in A$

$H \subseteq A$ , 因为 $H$ 和 $A = \langle a^d \rangle$ 均有 $m$ 个元素,  $H = A$ ,  $H = \langle a^d \rangle$

设  $\langle G, * \rangle$  是  $n$  阶循环群,  $m$  是正整数, 并且  $m \mid n$ , 则  
 $G$  中存在唯一一个 $m$ 阶子群。

对于 $n$ 的每个正因子 $m$ 都存在唯一一个 $m$ 阶子群。

$n$ 阶循环群的子群个数恰为 $n$ 的正因子数。

## § 5.4 循环群

例1 证明循环群的同态像必为循环群。

解：  $\langle G, * \rangle$  是循环群， $a$ 是生成元， $f$ 是同态映射，则 $\langle f(G), * \rangle$ 是同态像

$\forall a^n, a^m \in G$ , 有 $f(a^n * a^m) = f(a^n) * f(a^m)$

$n=1$ 时  $f(a) = f(a)$

$n=2$ 时  $f(a^2) = f(a) * f(a) = (f(a))^2$

$n=k-1$ 时  $f(a^{k-1}) = (f(a))^{k-1}$

$f(a^k) = f(a^{k-1} * a) = f(a^{k-1}) * f(a) = (f(a))^{k-1} * f(a) = (f(a))^k$

所以 $f(G)$ 中的每个元都可以表示成 $f(a)$ 的若干次幂

即  $\langle f(a) \rangle = f(G)$

## § 5.4 循环群

例2  $\langle G, * \rangle$  是无限循环群, 则只有两个生成元  $a$  和  $a^{-1}$ 。

解:  $\forall b \in G = \langle a \rangle$ , 则  $\exists n \in \mathbb{Z}$ , 有  $b = a^n$

$b = (a^{-n})^{-1} = (a^{-1})^{-n} = (a^{-1})^{n_1}$  其中  $n_1 = -n \in \mathbb{Z}$

$a^{-1}$  也是群的生成元

若  $c$  是另一生成元, 则  $\exists k, m \in \mathbb{Z}$   $c = a^k$  (1)  $a = c^m$  (2)

(2) 代入 (1) 所以  $c = c^{km}$  即  $c^{km-1} = e$

若  $km \neq 1$  则有消去律可知  $c$  的阶是有限的, 这与  $G$  是无限阶群矛盾

若  $km = 1$   $k=m=1$  或  $k=m=-1$

所以  $c=a$  或  $c=a^{-1}$

群只有两个生成元  $a$  和  $a^{-1}$

## § 5.5 置换群

### 5.5.1 置换及其运算

(1) 有限集  $S$  到其自身的双射称为  $S$  上的一个置换。当  $|S| = n$  时,  $S$  上的置换称为  $n$  次置换。

## § 5.5 置换群

### 5.5.1 置换及其运算

(2) 定义：设  $S$  上有如下置换

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_{i-1} & a_i & a_{i+1} & \cdots & a_n \\ a_2 & a_3 & \cdots & a_i & a_1 & a_{i+1} & \cdots & a_n \end{pmatrix}$$

称该置换为循环置换，记为  $(a_1, a_2, \dots, a_i)$ ， $i$  为循环长度。当  $i=2$  时称为对换。

单位置换，即恒等映射也视为循环置换，记为  $(1)$  或  $(n)$ 。

## § 5.5 置换群

### 5.5.2 置换群

(1) **定义：** 一个阶为 $n$ 的有限集合 $S$ 上所有的置换所组成的集合 $S_n$ 及其复合运算 $\circ$ 构成群,称  $\langle S_n, \circ \rangle$  为  $n$  次对称群(Symmetric group of degree  $n$ ), 而  $\langle S_n, \circ \rangle$  的任意子群称为  $n$  次置换群。

$n$  次对称群的阶?  $|S_n| = ? \quad n!$

## § 5.5 置换群

### 5.5.2 置换群

**例1:** 假设  $S=\{1,2,3\}$ , 写出  $S$  的 3 次对称群和所有的 3 次置换群。

解:  $S_3=\{f_1, f_2, f_3, f_4, f_5, f_6\}$ , 并且

$$f_1=(1), f_2=(1,2), f_3=(1,3), f_4=(2,3),$$

$$f_5=(1,2,3), f_6=(1,3,2)$$

$$f_1 = (1) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_2 = (1,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$f_3 = (1,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f_4 = (2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$f_5 = (1,2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_6 = (1,3,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$



$\mathbf{f}_1$ 是单位元,  $(\mathbf{f}_1) = \{\mathbf{f}_1\}$

群中元素 $\mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$ 的阶是**2**,

$$(\mathbf{f}_2) = \{\mathbf{f}_2, f_2^2\} = \{\mathbf{f}_1, \mathbf{f}_2\}$$

$$(\mathbf{f}_3) = \{\mathbf{f}_3, f_3^2\} = \{\mathbf{f}_1, \mathbf{f}_3\}$$

$$(\mathbf{f}_4) = \{\mathbf{f}_4, f_4^2\} = \{\mathbf{f}_1, \mathbf{f}_4\}$$

元素 $\mathbf{f}_5, \mathbf{f}_6$ 的阶是**3**,

$$(\mathbf{f}_5) = \{\mathbf{f}_5, f_5^2, f_5^3\} = \{\mathbf{f}_1, \mathbf{f}_5, \mathbf{f}_6\}$$

$$(\mathbf{f}_6) = \{\mathbf{f}_6, f_6^2, f_6^3\} = \{\mathbf{f}_1, \mathbf{f}_5, \mathbf{f}_6\}$$

$\{\mathbf{f}_1\}, \{\mathbf{f}_1, \mathbf{f}_2\}, \{\mathbf{f}_1, \mathbf{f}_3\}, \{\mathbf{f}_1, \mathbf{f}_4\}$

$\{\mathbf{f}_1, \mathbf{f}_5, \mathbf{f}_6\}$  是子群, 即**3次**置换群

但**3次**置换群的阶有**1, 2, 3**阶

例：有那些置换群是可交换群（**ABEL**群）？

解：{**f**<sub>1</sub>} , {**f**<sub>1</sub>, **f**<sub>2</sub>} , {**f**<sub>1</sub>, **f**<sub>3</sub>} , {**f**<sub>1</sub>, **f**<sub>4</sub>}

{**f**<sub>1</sub>, **f**<sub>5</sub>, **f**<sub>6</sub>} 是子群，即**3**次置换群

$$(\mathbf{f}_1) = \{\mathbf{f}_1\}$$

$$(\mathbf{f}_2) = \{\mathbf{f}_1, \mathbf{f}_2\}$$

$$(\mathbf{f}_3) = \{\mathbf{f}_1, \mathbf{f}_3\}$$

$$(\mathbf{f}_4) = \{\mathbf{f}_1, \mathbf{f}_4\}$$

$$(\mathbf{f}_5) = \{\mathbf{f}_1, \mathbf{f}_5, \mathbf{f}_6\}$$

$$(\mathbf{f}_6) = \{\mathbf{f}_1, \mathbf{f}_5, \mathbf{f}_6\}$$

◦	f <sub>1</sub>	f <sub>2</sub>	f <sub>3</sub>	f <sub>4</sub>	f <sub>5</sub>	f <sub>6</sub>
f <sub>1</sub>	f <sub>1</sub>	f <sub>2</sub>	f <sub>3</sub>	f <sub>4</sub>	f <sub>5</sub>	f <sub>6</sub>
f <sub>2</sub>	f <sub>2</sub>	f <sub>1</sub>	f <sub>6</sub>	f <sub>5</sub>	f <sub>4</sub>	f <sub>3</sub>
f <sub>3</sub>	f <sub>3</sub>	f <sub>5</sub>	f <sub>1</sub>	f <sub>6</sub>	f <sub>2</sub>	f <sub>4</sub>
f <sub>4</sub>	f <sub>4</sub>	f <sub>6</sub>	f <sub>5</sub>	f <sub>1</sub>	f <sub>3</sub>	f <sub>2</sub>
f <sub>5</sub>	f <sub>5</sub>	f <sub>3</sub>	f <sub>4</sub>	f <sub>2</sub>	f <sub>6</sub>	f <sub>1</sub>
f <sub>6</sub>	f <sub>6</sub>	f <sub>4</sub>	f <sub>2</sub>	f <sub>3</sub>	f <sub>1</sub>	f <sub>5</sub>

都是可交换群（**ABEL**群）

## § 5.5 置换群

### 5.5.2 置换群

(2) 性质：（Cayley 凯利定理）

任意  $n$  阶群必同构于一个  $n$  次置换群。

群

循环群

非循环群

- ① 若  $\langle G, * \rangle$  是  $n$  阶有限群循环群，  
则  $\langle G, * \rangle \cong \langle \mathbb{Z}_n, +_n \rangle$ ;
- ② 若  $\langle G, * \rangle$  是无限群循环群，则  
 $\langle G, * \rangle \cong \langle \mathbb{Z}, + \rangle$ 。

任意  $n$  阶群必同构于一个  $n$  次置换群  
( $n$  次对称群的某子群)。

任何有限阶群都是循环群。

☐ A 正确

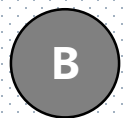
☒ B 错误

提交

在偶数阶群中至少有一个周期为**2**的元素，也可以有**3**个周期为**2**的元素，但周期为**2**的元素不能为偶数个。



正确



错误

提交

$n$  次对称群的阶一定是 $n$ 。

A 正确

B 错误

提交

$n$  次置换群的阶一定是 $n$ 。

- ☐ A 正确
- ☒ B 错误

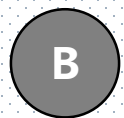
提交



任何循环群的子群一定还是循环群。



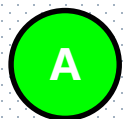
正确



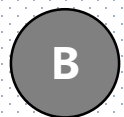
错误

提交

任何循环群一定是可交换群（**ABEL**群）。



正确

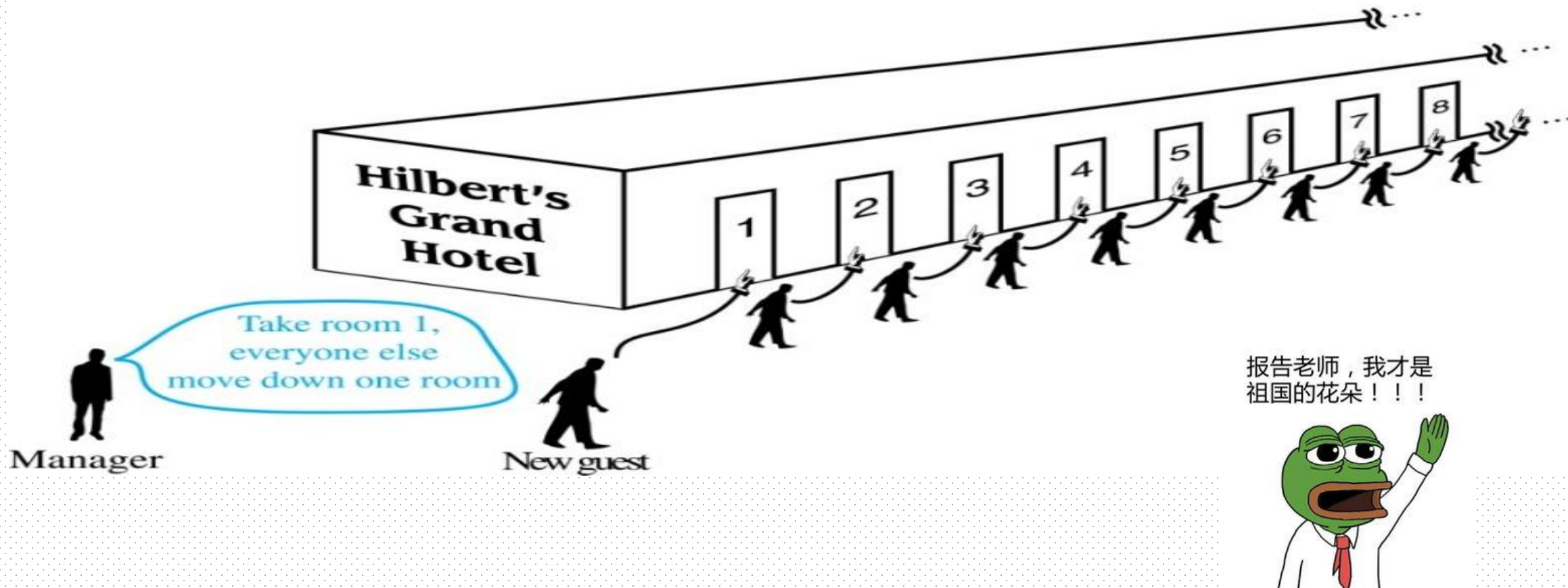


错误

提交

问：什么是无穷  $(-\infty, +\infty)$  ？

答：无穷就是....,....



## § 5.6 陪集

(1)

### 5.6.1 左同余关系（左陪集关系）

定义：

设  $\langle G, * \rangle$  是一个群， $\langle H, * \rangle$  是其子群。利用  $H$  在  $G$  上定义关系：

$$R_H = \{ \langle a, b \rangle \mid a, b \in G, b^{-1} * a \in H \}$$

$$R'_H = \{ \langle a, b \rangle \mid a, b \in G, a * b^{-1} \in H \}$$

则称  $R_H$  为  $G$  上的模  $H$  左同余关系（左陪集关系）； $R'_H$  为  $G$  上的模  $H$  右同余关系（右陪集关系）。

## § 5.6 陪集 (2)

### 5.6.1 左同余关系 (左陪集关系)

**定理:**

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群, 则  $G$  中模  $H$  左同余关系是等价关系。

**(1)**自反 **(2)**对称 **(3)**传递  $R_H = \{ \langle a, b \rangle \mid a, b \in G, b^{-1} * a \in H \}$

$\langle a, a \rangle \in R_H, a^{-1} * a \in H$   $H$  是子群

$\langle a, b \rangle \in R_H, b^{-1} * a \in H$   $H$  是子群,  $(b^{-1} * a)^{-1} \in H$   $a^{-1} * b \in H$   $\langle b, a \rangle \in R_H,$

$\langle a, b \rangle \in R_H$   $\langle b, c \rangle \in R_H$   $b^{-1} * a \in H, c^{-1} * b \in H, c^{-1} * a \in H$   $\langle a, c \rangle \in R_H$

## § 5.6 陪集

(3)

### 5.6.2 左陪集

定义：

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，则  $a \in G$  为代表元的模  $H$  同余关系的等价类  $[a] = \{a * h \mid h \in H\}$ ，称为  $H$  在  $G$  内由  $a$  确定的左陪集。

简记为： $aH = [a] = \{\dots\}$ 。 陪集着实有些抽象！

## § 5.6 陪集

(3)

例1: 设 $\mathbf{G}=\mathbf{R}\times\mathbf{R}$ ,  $\mathbf{R}$ 是实数集,  $\mathbf{G}$ 上的二元运算定义如下;

$\forall \langle x, y \rangle \in \mathbf{R}\times\mathbf{R}$  代表平面坐标系中的一点,

$$\langle x_1, y_1 \rangle + \langle x_2, y_2 \rangle = \langle x_1 + x_2, y_1 + y_2 \rangle$$

则 $\langle \mathbf{G}, + \rangle$  是群。

设 $\mathbf{H}=\{\langle x, y \rangle \mid y=2x\}$ ,  $\mathbf{H}$ 是 $\mathbf{G}$ 的子群。

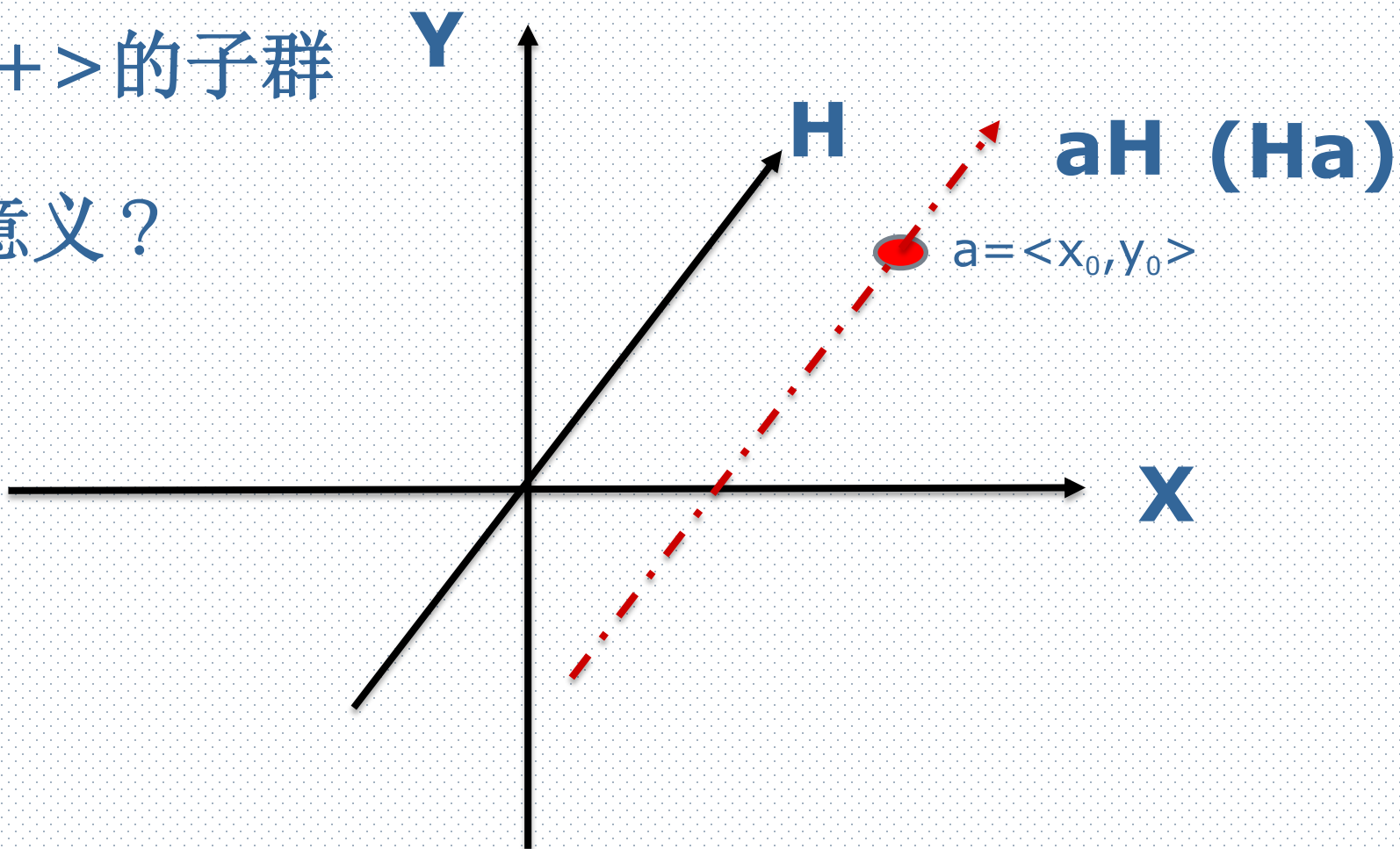
取 $a=\langle x_0, y_0 \rangle$ ,  $a\mathbf{H}, \mathbf{H}a$ 的意义是什么?

## § 5.6 陪集

(3)

$\langle H, + \rangle$  是  $\langle G, + \rangle$  的子群

陪集的几何意义？





## § 5.6 陪集

(5)

### 5.6.2 左陪集

例2:  $G = \{e, a, b, c, d, e, f\}$ 。

- 1、写出子群  $\langle a \rangle$
- 2、证明  $\langle a \rangle * c = c * \langle a \rangle$
- 3、找出所有两个元素的子群
- 4、求  $\langle d \rangle$  的右陪集

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

## § 5.6 陪集

1、写出子群  $\langle a \rangle = \{a^0, a^1, a^2\} = \{e, a, b\}$

2、证明  $\langle a \rangle * c = c * \langle a \rangle$

$$\langle a \rangle * c = \{e, a, b\} * c = \{c, d, f\}$$

$$c * \langle a \rangle = c * \{e, a, b\} = \{c, d, f\}$$

3、找出所有两个元素的子群  $\{e, c\}, \{e, d\}, \{e, f\}$

4、求  $\langle d \rangle$  的右陪集  $\langle d \rangle = \{e, d\}$

$$\langle d \rangle * a = \{e, d\} * a = \{a, c\}$$

$$\langle d \rangle * d = \{e, d\} * d = \{e, d\}$$

$$\langle d \rangle * b = \{e, d\} * b = \{b, f\}$$

$$\langle d \rangle * e = \{e, d\} * e = \{e, d\}$$

$$\langle d \rangle * c = \{e, d\} * c = \{a, c\}$$

$$\langle d \rangle * f = \{e, d\} * f = \{b, f\}$$

$$\langle d \rangle * a = \{e, d\} * c = \{a, c\}$$

$$\langle d \rangle * b = \{e, d\} * f = \{b, f\}$$

$$\langle d \rangle * c = \{e, d\} * e = \{e, d\}$$

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

$\langle d \rangle$  的右陪集六个结果只有三个不同的集合  
且是G的划分。

## § 5.6 陪集

(5)

### 5.6.2 左陪集

例3：设 $\langle \mathbb{Z}_6, +_6 \rangle$ 是一个群， $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ ，试写出 $\langle \mathbb{Z}_6, +_6 \rangle$ 中每个子群及相应的左陪集。

$$H_1 = \{[0]\}$$

$$H_2 = \{[0], [3]\}$$

$$H_3 = \{[0], [2], [4]\}$$

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

## § 5.6 陪集

### 5.6.2 左陪集

$$H_1 = \{[0]\}$$

$$H_2 = \{[0], [3]\}$$

$$H_3 = \{[0], [2], [4]\}$$

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$$H_1 = \{[0]\},$$

H<sub>1</sub>有6个不同的陪集

$$\text{左陪集: } [0]H_1 = \{[0]\}, [1]H_1 = \{[1]\},$$

$$[2]H_1, [3]H_1, [4]H_1, [5]H_1 = \{[2]\}, \{[3]\}, \{[4]\}, \{[5]\}$$

H<sub>2</sub>有3个不同的陪集

$$H_2 = \{[0], [3]\},$$

$$\text{左陪集: } [0]H_2 = \{[0], [3]\}, [3]H_2 = \{[0], [3]\},$$

$$[1]H_2 = [4]H_2 = \{[1], [4]\}, [2]H_2 = [5]H_2 = \{[2], [5]\}$$

H<sub>3</sub>有2个不同的陪集

$$H_3 = \{[0], [2], [4]\}$$

$$\text{左陪集: } \{[0]H_3, [1]H_3, [2]H_3, [3]H_3, [4]H_3, [5]H_3\}$$

$$[0]H_3 = [2]H_3 = [4]H_3 = \{[0], [2], [4]\},$$

$$[1]H_3 = [3]H_3 = [5]H_3 = \{[1], [3], [5]\}$$

## § 5.6 陪集

(4)

### 5.6.2 左陪集

定理:

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群, 则:

(1)  $eH = H$ ;

(2) 对  $\forall a, b \in G$ ,  $aH = bH \Leftrightarrow b^{-1} * a \in H$

(3) 对  $\forall a \in G$ ,  $aH = H \Leftrightarrow a \in H$

**证明：** 设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，则：

(1)  $eH = H$ ;  $\forall x \in eH, \exists h_1 \in H$  有  $x = eh_1 = h_1 \in H$ ,  
所以有  $eH \subseteq H$ ; 又  $H \subseteq eH$  , 所以  $eH = H$

**证明：** 设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，则：

$$\begin{aligned} (2) \text{ 对 } \forall a, b \in G, \quad aH = bH &\Leftrightarrow b^{-1} * aH = b^{-1} * bH \\ &\Leftrightarrow b^{-1} * aH = eH \Leftrightarrow b^{-1} * aH = H \Leftrightarrow b^{-1} * a \in H \end{aligned}$$

另法  $\forall a, b \in G, \quad aH = bH$  则  $\exists h_1, h_2 \in H$  有  $ah_1 = bh_2$

$$a = bh_2h_1^{-1} \text{ 所以 } b^{-1} * a = b^{-1}bh_2h_1^{-1} = eh_2h_1^{-1} = h_2h_1^{-1} \in H$$

$$b^{-1} * a \in H \text{ 设 } b^{-1} * a = h_1 \text{ 所以 } a = bh_1$$

$$\forall ah \in aH \quad ah = bh_1h = bh_2 \in bH \quad aH \subseteq bH \quad \text{同理 } bH \subseteq aH$$

$$\text{所以 } aH = bH$$

**证明：** (3) 对  $\forall a \in G$ ,  $aH = H \Leftrightarrow a \in H$

则  $\exists h_1, h_2 \in H$  有  $ah_1 = h_2$   $a = h_2h_1^{-1} \in H$   $a \in H$

若  $a \in H$  由运算封闭性  $aH = H$

另法 利用(1)(2)  $aH = H = eH \Leftrightarrow e^{-1} * a \in H \Leftrightarrow a \in H$



## § 5.6 陪集 (4)

定理:

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群, 则:

(1)  $eH = H$ ;

(2) 对  $\forall a, b \in G$ ,  $aH = bH \Leftrightarrow b^{-1} * a \in H$

(3) 对  $\forall a \in G$ ,  $aH = H \Leftrightarrow a \in H$

**(1)** 单位元的陪集还是子群自身

**(2)** 两个元素的陪集相同, 则两个元素有模 **H** 左同余关系 (等价关系)

**(3)** 某元素的陪集与子群相同, 则该元素一定是子群中的元素。

## § 5.6 陪集

(6)

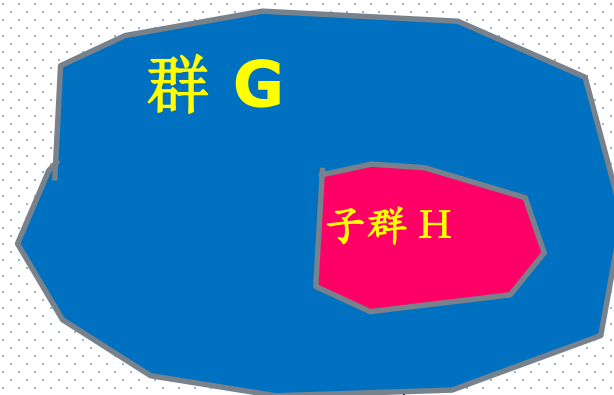
### 5.6.3 左商集和右商集

定义:

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群, 由  $H$  所确定的  $G$  上所有元素的左陪集构成的集合称为  $G$  对  $H$  的左商集, 记为:  $S_L = \{ aH \mid a \in G \}$ ; 所有右陪集构成的集合称为  $G$  对  $H$  的右商集, 记为:  $S_R = \{ Ha \mid a \in G \}$ 。

## § 5.6 陪集

设  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的子群。



(1) 利用  $H$  定义  $G$  上的关系

$$R_H = \{ \langle a, b \rangle \mid a, b \in G, b^{-1} * a \in H \}$$

$$R'_H = \{ \langle a, b \rangle \mid a, b \in G, a * b^{-1} \in H \}$$

则称  $R_H$  和  $R'_H$  分别为  $G$  上的模  $H$  左同余关系（左陪集关系）和右同余关系（右陪集关系）。

为什么？

(2)  $H$  在  $G$  内由  $a$  确定的左、右陪集简记为：

$$aH = [a] = \{ a * h \mid h \in H \} = \{ ah \mid h \in H \}$$

$$Ha = [a] = \{ h * a \mid h \in H \} = \{ ha \mid h \in H \}$$

(3) 左、右商集  $S_L = \{ aH \mid a \in G \}$ 、 $S_R = \{ Ha \mid a \in G \}$

## § 5.6 陪集

(5)

例:  $G = \{e, a, b, c, d, f\}$ 。

求  $(d)$  的右陪集、 $(d)$  的左陪集, 左商集  $S_L$ , 右商集  $S_R$

$$(d) = \{e, d\}$$

右陪集:

$$(d) * a = (d) * c = \{a, c\}$$

$$(d) * b = (d) * f = \{b, f\}$$

$$(d) * e = (d) * d = \{e, d\}$$

左陪集:

$$a * (d) = f * (d) = \{a, f\}$$

$$c * (d) = b * (d) = \{b, c\}$$

$$e * (d) = d * (d) = \{d, e\}$$

$$\text{右商集 } S_R = \{\{a, c\}, \{b, f\}, \{e, d\}\}$$

$$\text{左商集 } S_L = \{\{a, f\}, \{b, c\}, \{d, e\}\}$$

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

$S_L \neq S_R$   $|S_L| = |S_R|$  商集不同但商集等势

例：设  $\langle \mathbb{Z}_6, +_6 \rangle$  是一个群， $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ ，  
运算表如下：

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$$H1 = \{[0]\}$$

$$H2 = \{[0], [3]\}$$

$$H3 = \{[0], [2], [4]\}$$

$$H_1 = \{[0]\},$$

$$\begin{aligned} S_L &= \{[0]H_1, [1]H_1, [2]H_1, [3]H_1, [4]H_1, [5]H_1\} \\ &= \{\{[0]\}, \{[1]\}, \{[2]\}, \{[3]\}, \{[4]\}, \{[5]\}\} \end{aligned}$$

$$\begin{aligned} S_R &= \{H_1[0], H_1[1], H_1[2], H_1[3], H_1[4], H_1[5]\} \\ &= \{\{[0]\}, \{[1]\}, \{[2]\}, \{[3]\}, \{[4]\}, \{[5]\}\} \end{aligned}$$

$$S_L = S_R \quad |S_L| = |S_R|$$

$$H_2 = \{[0], [3]\},$$

$$\begin{aligned} S_L &= \{[0]H_2, [1]H_2, [2]H_2, [3]H_2, [4]H_2, [5]H_2\} \\ &= \{\{[0], [3]\}, \{[1], [4]\}, \{[2], [5]\}\} \end{aligned}$$

$$\begin{aligned} S_R &= \{H_2[0], H_2[1], H_2[2], H_2[3], H_2[4], H_2[5]\} \\ &= \{\{[0], [3]\}, \{[1], [4]\}, \{[2], [5]\}\} \end{aligned}$$

$$S_L = S_R \quad |S_L| = |S_R|$$

$$H_3 = \{[0], [2], [4]\}$$

$$\begin{aligned} S_L &= \{[0]H_3, [1]H_3, [2]H_3, [3]H_3, [4]H_3, [5]H_3\} \\ &= \{\{[0], [2], [4]\}, \{[1], [3], [5]\}\} \end{aligned}$$

$$\begin{aligned} S_R &= \{H_3[0], H_3[1], H_3[2], H_3[3], H_3[4], H_3[5]\} \\ &= \{\{[0], [2], [4]\}, \{[1], [3], [5]\}\} \end{aligned}$$

$$S_L = S_R \quad |S_L| = |S_R|$$

## § 5.6 陪集

(7)

### 5.6.3 左商集和右商集

定理:

设  $\langle H, * \rangle$  是任意群  $\langle G, * \rangle$  的子群,  
则  $G$  关于  $H$  的左、右商集必等势。

定义映射  $f: S_L \rightarrow S_R$ ,

$$\text{对 } \forall a \in G, f(aH) = Ha^{-1}$$

## § 5.6 陪集

(8)

### 5.6.3 左商集和右商集

**定义：** 设  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的子群， $S_L$  的基数称为  $H$  在  $G$  内的**指数**。记为：

$$[G:H] = |S_L| \quad \text{或} \quad [G:H] = |S_R|$$



例:  $G = \{e, a, b, c, d, f\}$ 。

求  $(d)$  的右陪集、 $(d)$  的左陪集, 左商集  $S_L$ , 右商集  $S_R$

$$(d) = \{e, d\}$$

右陪集:

$$(d) * a = (d) * c = \{a, c\}$$

$$(d) * b = (d) * f = \{b, f\}$$

$$(d) * e = (d) * d = \{e, d\}$$

左陪集:

$$a * (d) = f * (d) = \{a, f\}$$

$$c * (d) = b * (d) = \{b, c\}$$

$$e * (d) = d * (d) = \{d, e\}$$

$$\text{右商集 } S_R = \{\{a, c\}, \{b, f\}, \{e, d\}\}$$

$$\text{左商集 } S_L = \{\{a, f\}, \{b, c\}, \{d, e\}\}$$

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

$$[G:H] = [G:(d)] = |S_L| = 3$$

例：设  $\langle Z_6, +_6 \rangle$  是一个群， $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$ ，  
运算表如下：

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$$H_1 = \{[0]\}$$

$$H_2 = \{[0], [3]\}$$

$$H_3 = \{[0], [2], [4]\}$$

$$[Z_6 : \{[0]\}] = \mathbf{6}$$

$$H_1 = \{[0]\},$$

$$[Z_6 : H_1] = |S_L| = 6$$

$$S_L = \{\{[0]\}, \{[1]\}, \{[2]\}, \{[3]\}, \{[4]\}, \{[5]\}\}$$

$$S_R = \{\{[0]\}, \{[1]\}, \{[2]\}, \{[3]\}, \{[4]\}, \{[5]\}\}$$

$$[Z_6 : H_2] = 3 \quad [Z_6 : H_3] = 2$$

## § 5.6 陪集

(9)

### 5.6.3 左商集和右商集

定理：

设  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的子群， $H$  的任意左陪集（右陪集）与  $H$  等势。

$$\forall a \in G, |aH| = |H| \text{ 或 } |Ha| = |H|$$

## § 5.6 陪集

(10)

### 5.6.4 Lagrange 定理

定理：

假设  $\langle G, * \rangle$  是有限群， $\langle H, * \rangle$  是  $\langle G, * \rangle$  的子群，则  $H$  的阶必整除  $G$  的阶，并且  $|G| = [G:H]|H|$ 。

$n$  阶群的子群的阶一定是  $n$  的因子。

## § 5.6 陪集

(11)

### 5.6.4 Lagrange 定理

- (1) 任何素数阶的群不可能有非平凡<sub>非平凡</sub>的子群。
- (2) 素数阶的群必为循环群。
- (3) 假设  $\langle G, * \rangle$  是  $n$  阶有限群, 则对  $\forall a \in G, |a| \mid n$  (形象表述?)。
- (4) 假设  $\langle G, * \rangle$  是  $n$  阶有限群, 则对  $\forall a \in G, a^n = e$ 。

## § 5.6 陪集

(11)

(1) 任何素数阶的群不可能有非平凡

的子群  $S \subseteq G, S = G$ , 或  $S = \{e\}$

由拉格朗日定理得，素数阶群的子群的阶只能是1或素数自身，所以。。。

## § 5.6 陪集

(11)

(3) 假设  $\langle G, * \rangle$  是  $n$  阶有限群, 则对  
 $\forall a \in G, |a| \mid n$  (形象表述?)。

$n$  阶有限群中任意元素的周期一定整除  $n$ ;

$n$  阶有限群中任意元素的周期只能是  $n$  的正因子;

## § 5.6 陪集

(11)

(4) 假设  $\langle G, * \rangle$  是  $n$  阶有限群, 则对  
 $\forall a \in G, a^n = e$ 。

$\forall a \in G$ , 由拉格朗日定理得  $|a|$  整除  $|G|$   
设  $|a| = m, |G| = n, n = km$   
 $a^n = a^{km} = (a^m)^k = e^k = e$



## § 5.6 陪集

(11)

**例1：**证明素数阶循环群的每个非单位元都是生成元。（素数阶的群必为循环群）

证明：设 $\langle G, * \rangle$ 是 $p$ 阶循环群， $p$ 是素数。  
对 $G$ 中任一非单位元 $a$ 。设 $a$ 的阶为 $k$ , 则 $k \neq 1$

由拉格朗日定理， $k$ 是 $p$ 的正整数因子。因为 $p$ 是素数，故 $k=p$ 。 $a$ 的阶就是 $p$ ，即群 $G$ 的阶。  
故 $a$ 是 $G$ 的生成元。

## § 5.6 陪集

(11)

**例1:** 证明素数阶循环群的每个非单位元都是生成元。（素数阶的群必为循环群）

证明:  $|G|=n$  且  $p$  是素数,  $p>1$ ,  $a \in G$   $a \neq e$   
设  $|(a)|=m$ , 则  $m>1$  由拉格朗日定理知  $m|p$   
因为  $p$  是素数, 所以  $m=p$ ,  $(a)$  是  $p$  阶循环群  
即  $G$  的  $p$  个元素都在  $(a)$  中,  $(a) = G$

**例2：**证明**9**阶群必有**3**阶子群。

证明，设**a**是**9**阶群的一个非单位元元素  
则**a**的周期只能是**3**或**9**

如果**a**的周期是**3**，则  $\langle \mathbf{a} \rangle = \{a^1, a^2, a^3\}$  是**3**阶子群

如果**a**的周期是**9**，则  $\langle \mathbf{a}^3 \rangle = \{a^3, a^6, a^9\}$   
 $= \{a^3, (a^3)^2, (a^3)^3\}$  是**3**阶子群

**例3：G是有限群，K是G的子群，H是K的子群**  
**则  $[G:H]=[G:K][K:H]$**

证明，K是G的子群， $|G|=[G:K]|K|$

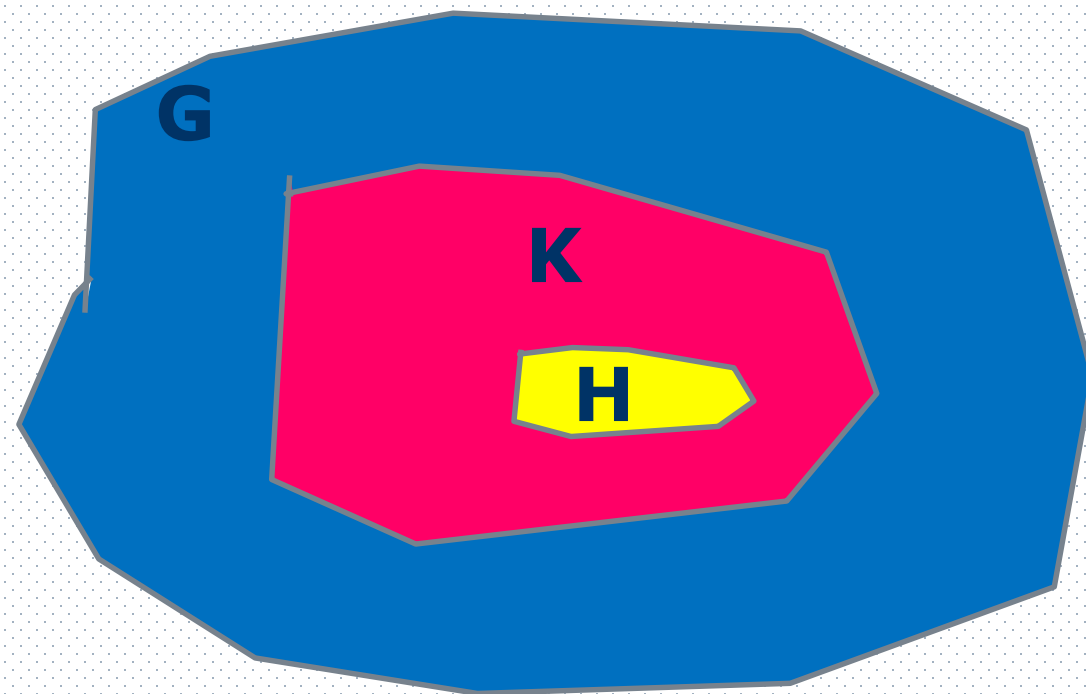
又H是K的子群

$$|K|=[K:H]|H|$$

又H是G的子群

$$|G|=[G:H]|H|$$

则  $[G:H]=[G:K][K:H]$



例4:  $\mathbf{G}$ 是群,  $\mathbf{H}$ 是 $\mathbf{G}$ 的子群,  
令 $\mathbf{M}=\{\mathbf{x}|\mathbf{x} \in \mathbf{G}, \mathbf{xHx}^{-1}=\mathbf{H}\},$   
则 $\mathbf{M}$ 也是 $\mathbf{G}$ 的子群

$$\mathbf{M}=\{\mathbf{x}|\mathbf{x} \in \mathbf{G}, \mathbf{xHx}^{-1}=\mathbf{H}\},$$

证明: (1) $\mathbf{M} \neq \Phi$ , 因为  $e \in G$ , 且  $eHe^{-1}=H$ ,  $e \in \mathbf{M}$

(2) $\forall x, y \in M$ , 有  $M$  的定义得,  $xHx^{-1}=H$ ,  $yHy^{-1}=H$

$$x^{-1}Hx=H, y^{-1}Hy=H$$

$$xy^{-1}H(xy^{-1})^{-1}=xy^{-1}H(y^{-1})^{-1}x^{-1}=xy^{-1}Hyx^{-1}=XHX^{-1}=H$$

$$\therefore xy^{-1} \in M$$

$M$  是  $G$  的子群,

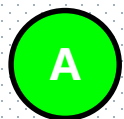
素数阶的群必为循环群，而偶数阶的群一定不是循环群。

☐ A 正确

☒ B 错误

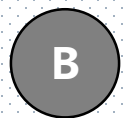
提交

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，则单位元  $e$  关于  $H$  的左，右陪集都等于  $H$ 。



A

正确



B

错误

提交

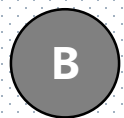


设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，群中两个元素的左陪集相同，则两个元素一定具有模  $H$  左同余关系。



A

正确



B

错误

提交

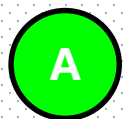
设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，则对  $\forall a \in G$ ，  
都有  $aH = H$ 。

☐ A 正确

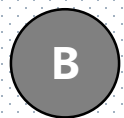
☒ B 错误

提交

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群, 对  $\forall a \in G$ , 若  $aH = H$   
 $\Leftrightarrow a^{-1} \in H$



正确



错误

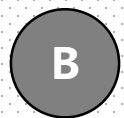
提交

设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，子群  $H$  中任意两元素的左陪集都等于  $H$ 。即若  $\forall a, b \in H$ ，则  $aH = bH = H$



A

正确



B

错误

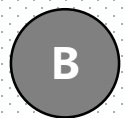
提交

设  $\langle H, * \rangle$  是任意群  $\langle G, * \rangle$  的子群，则  $G$  关于  $H$  的左、右商集可以不同，但  $H$  的左、右商集必等势。



A

正确



B

错误

提交

假设  $\langle G, * \rangle$  是有限群， $\langle H, * \rangle$  是  $\langle G, * \rangle$  的子群，则  $H$  的阶整除  $G$  的阶所得到的商称为  $H$  在  $G$  内的指数。

即  $|G| = |H| \cdot |G/H|$



A

正确



B

错误

提交

## § 5.7 正规子群

(1)

### 5.7.1 正规子群的定义

设  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的子群，如果对  $\forall a \in G$  有  $aH = Ha$ ，则称  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的正规子群（不变子群）。

例：假设  $S=\{1,2,3\}, S_3=\{f_1, f_2, \dots, f_6\}$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$



$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\langle \{f_1\}, o \rangle, \langle \{f_1, f_2\}, o \rangle, \langle \{f_1, f_3\}, o \rangle, \langle \{f_1, f_4\}, o \rangle,$$

$$\langle \{f_1, f_5, f_6\}, o \rangle, \langle S_3, o \rangle$$

是三次置换群，是三次对称群的子群，是否为正规子群？

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$

$H_1 = \{f_1\}, \forall a \in S_3$  是否都有  $aH_1 = H_1a$

$H_1 = \{f_1\}$  是  $S_3$  的正规子群

$H_2 = \{f_1, f_2\}, \forall a \in S_3$  是否都有  $aH_2 = H_2a$

$$f_1\{f_1, f_2\} = \{f_1, f_2\} = f_2\{f_1, f_2\},$$

$$\{f_1, f_2\}f_1 = \{f_1, f_2\} = \{f_1, f_2\}f_2$$

$$f_3\{f_1, f_2\} = \{f_3, f_5\} = f_5\{f_1, f_2\},$$

$$\{f_1, f_2\}f_3 = \{f_3, f_6\} = \{f_1, f_2\}f_6$$

$$f_4\{f_1, f_2\} = \{f_4, f_6\} = f_6\{f_1, f_2\},$$

$$\{f_1, f_2\}f_4 = \{f_4, f_5\} = \{f_1, f_2\}f_5$$

$$f_3\{f_1, f_2\} = \{f_3, f_5\} \neq \{f_3, f_6\} = \{f_1, f_2\}f_3$$

$$f_4\{f_1, f_2\} = \{f_4, f_6\} \neq \{f_4, f_5\} = \{f_1, f_2\}f_4$$

$H_2 = \{f_1, f_2\}$  不是  $S_3$  的正规子群, 但  $H_2$  是可交换群。

## § 5.7 正规子群

(4)

### 5.7.2 判定正规子群的条件

**定理：**

设  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的一个子群，则以下条件等价：

(1) 对  $\forall a \in G, aH = Ha$

(2) 对  $\forall a \in G, h \in H$ , 必存在  $h' \in H$ , 使  
$$h * a = a * h'$$

(3) 对  $\forall a \in G, h \in H, a * h * a^{-1} \in H$ , 或者  
$$a^{-1} * h * a \in H.$$

设  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的一个子群, 则以下条件等价:

(1) 对  $\forall a \in G, aH = Ha$

(2) 对  $\forall a \in G, h \in H$ , 必存在  $h' \in H$ , 使  
 $h * a = a * h'$

(3) 对  $\forall a \in G, h \in H, a * h * a^{-1} \in H$ ,

(1)  $\rightarrow$  (2) 对  $\forall a \in G, h \in H, h * a \in Ha, aH = Ha, h * a \in aH$   
 $\exists h' \in H$ , 所以  $h * a = a * h'$

(2)  $\rightarrow$  (3) 对  $\forall a \in G, h \in H, \exists h' \in H, aH = Ha, a * h * a^{-1} = Haa^{-1}$ , 所以  
 $a * h * a^{-1} \in H$

## § 5.7 正规子群

(3)

### 5.7.2 判定正规子群的条件

**定理：**

群  $\langle G, * \rangle$  的子群  $\langle H, * \rangle$  是正规子群的充要条件是：

对  $\forall a \in G, h \in H$  有  $a * h * a^{-1} \in H$ ,


或者  $a^{-1} * h * a \in H$ 。

$\Rightarrow$  对  $\forall a \in G, h \in H$  有  $a * h * a^{-1} \in H$ ,

$\forall x \in aH, \exists h \in H, x = ah, x = ah(a^{-1}a) = (aha^{-1})a = h'a$

$\therefore x \in Ha$

$aH \subseteq Ha$  同理  $Ha \subseteq aH \therefore Ha = aH$

  $Ha = aH$  对  $\forall a \in G, h \in H, ah \in aH, aH = Ha,$   
 $ah \in Ha, \exists h' \in H, \therefore ah = h'a$   
 $h' = aha^{-1}, \therefore aha^{-1} \in H$

## § 5.7 正规子群

(3)

### 5.7.3 商群

**定义：**

子群  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的正规子群在  $G/H$  上

定义新的运算  $\circ$ ：

对  $\forall a, b \in G$ , 有  $aH \circ bH = (a * b)H$ ,

称为  $G$  对  $H$  的商群。

**$G/H = \{\text{不同陪集作为元素}\}$**

(1) 封闭性  **$aH \circ bH = (a * b)H$**

(2) 可结合  **$(aH \circ bH) \circ cH = aH \circ (bH \circ cH)$   
 **$= (a * b * c)H$****

(3) 单位元  **$eH$   $eH \circ bH = (e * b)H = bH$**

(4) 逆元  **$aH$  的逆元  $a^{-1}H$   $aH \circ a^{-1}H = (a * a^{-1})H = eH$**



## § 5.7 正规子群

(4)

### 5.7.3 商群

例:  $\langle \mathbf{N}_6, +_6 \rangle$ ,  $\mathbf{H} = \{0, 2, 4\}$ ,  $\mathbf{H}$  为  $\mathbf{N}_6$  的正规子群, 故有商群

$$\mathbf{N}_6 / \mathbf{H} = \langle \{0\mathbf{H}, 1\mathbf{H}\}, \circ \rangle$$

$$0\mathbf{H} = 0 +_6 \{0, 2, 4\} = \{0, 2, 4\} = \mathbf{H} (=2\mathbf{H}, 4\mathbf{H});$$

$$1\mathbf{H} = 0 +_6 \{0, 2, 4\} = \{1, 3, 5\} (3\mathbf{H}, 5\mathbf{H})$$

其运算如下:  $(0\mathbf{H}) \circ (0\mathbf{H}) = (0 +_6 0)\mathbf{H} = 0\mathbf{H};$

$$(1\mathbf{H}) \circ (1\mathbf{H}) = 2\mathbf{H} = 0\mathbf{H};$$

$$(0\mathbf{H}) \circ (1\mathbf{H}) = (1\mathbf{H}) \circ (0\mathbf{H}) = 1\mathbf{H};$$

$$(0\mathbf{H})^{-1} = 0^{-1}\mathbf{H} = 0\mathbf{H};$$

$$(1\mathbf{H})^{-1} = 1^{-1}\mathbf{H} = 5\mathbf{H} = 1\mathbf{H}.$$

$\circ$	$0\mathbf{H}$	$1\mathbf{H}$
$0\mathbf{H}$	$0\mathbf{H}$	$1\mathbf{H}$
$1\mathbf{H}$	$1\mathbf{H}$	$0\mathbf{H}$

## § 5.7 正规子群

### 5.7.3 商群

例：三次置换群  $\langle \{f_1, f_5, f_6\}, \circ \rangle$  所产生的商

集  $S_3/H_3 = \{f_1H_3, f_2H_3\}$ ,

$$H_3 = \{f_1, f_5, f_6\}$$

$$f_1H_3 = f_1 \circ \{f_1, f_5, f_6\} = H_3$$

$$f_2H_3 = f_2 \circ \{f_1, f_5, f_6\} = \{f_2, f_3, f_4\}$$

$$f_3H_3 = f_3 \circ \{f_1, f_5, f_6\} = \{f_2, f_3, f_4\}$$

$$f_4H_3 = f_4 \circ \{f_1, f_5, f_6\} = \{f_2, f_3, f_4\}$$

$$f_5H_3 = f_4 \circ \{f_1, f_5, f_6\} = \{f_1, f_5, f_6\}$$

$$f_6H_3 = f_4 \circ \{f_1, f_5, f_6\} = \{f_1, f_5, f_6\}$$

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$

## § 5.7 正规子群

### 5.7.3 商群

三次置换群 $\langle \{f_1, f_5, f_6\}, o \rangle$ 所产生的商集

$S_3/H_3 = \{f_1H_3, f_2H_3\}$  关于运算  $\Delta$  构成一个商群。

在 $S_3/H_3$ 上所定义的运算如右表所示:

$\Delta$	$f_1H_3$	$f_2H_3$
$f_1H_3$	$f_1H_3$	$f_2H_3$
$f_2H_3$	$f_2H_3$	$f_1H_3$

例：设  $\langle \mathbb{Z}_6, +_6 \rangle$  是一个群， $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ ，  
 运算表如下：  $H = \{[0], [3]\}$  是其子群

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$$H = \{[0], [3]\},$$

左陪集：  $[0]H = \{[0], [3]\}, [3]H = \{[0], [3]\},$

$$[1]H = [4]H = \{[1], [4]\}, [2]H = [5]H = \{[2], [5]\}$$

右陪集：  $H[0] = \{[0], [3]\}, H[3] = \{[0], [3]\},$

$$H[1] = H[4] = \{[1], [4]\}, H[2] = H[5] = \{[2], [5]\}$$

满足  $aH = Ha$  是正规子群

$$\mathbb{Z}_6/H = \{[0]H, [1]H, [2]H\}$$

对  $\forall a, b \in \mathbb{Z}_6/H$ ，有  $aH \circ bH = (a +_6 b)H$

$$[0]H \circ [1]H = ([0] +_6 [1])H = [1]H \quad [0]H \circ [2]H = ([0] +_6 [2])H = [2]H$$

$$[1]H \circ [2]H = ([1] +_6 [2])H = [3]H \quad [2]H \circ [1]H = ([2] +_6 [1])H = [3]H$$

$\circ$	0H	1H	2H
0H	0H	1H	2H
1H	1H	2H	0H
2H	2H	0H	1H

[0]H自身为逆元 [1]H, [2]H互为逆元

构造了一个三阶商群,  $\langle \mathbf{Z}_6/\mathbf{H}, \circ \rangle$   
 商群的运算对象是陪集。

## § 5.7 正规子群

(5)

### 5.7.4 子集的乘积

#### (1) 定义

假设  $\langle G, * \rangle$  是一个群,  $A, B$  是  $G$  的子集, 集合

$$\{ab \mid a \in A, b \in B\}$$

称为  $A, B$  的乘积, 记为  $A*B$  或  $AB$ 。

## § 5.7 正规子群

(6)

### 5.7.4 子集的乘积

#### (2) 性质

(I) 子集的乘积满足结合律。即

$$(A*B)*C=A*(B*C)$$

(II) 在子集的运算下，任何子群都为幂等元，即 $HH=H$ 。

## § 5.7 正规子群

(7)

### 5.7.4 子集的乘积

**定理：**

设  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的正规子群，  
则对  $\forall a, b \in G$ ,  $aH * bH = (a * b)H$



$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$

$H_2 = \{f_1, f_2\}$  不是  $S_3$  的正规子群

对  $\forall a, b \in G$ ,  $aH * bH = (a * b)H$  不一定成立

$$H_2 = \{f_1, f_2\}$$

$$f_1 \{f_1, f_2\} \circ f_2 \{f_1, f_2\} = \{f_1, f_2\}$$

$$f_1 \circ f_2 \{f_1, f_2\} = f_2 \{f_1, f_2\} = \{f_1, f_2\}$$

$$f_3 \{f_1, f_2\} \circ f_5 \{f_1, f_2\} = \{f_3, f_5\} \circ \{f_3, f_5\} = \{f_1, f_2, f_4, f_6\}$$

$$f_3 \circ f_5 \{f_1, f_2\} = f_2 \{f_1, f_2\} = \{f_1, f_2\}$$

$$\therefore f_3 \{f_1, f_2\} \circ f_5 \{f_1, f_2\} \neq f_3 \circ f_5 \{f_1, f_2\}$$

1、任何正规子群不一定是可交换群（**ABEL**）。



正确



错误

提交

2、三次置换群 $\langle \{f_1, f_2\}, \circ \rangle$ 是三次对称群 $\langle S_3, \circ \rangle$ 的子群,  
 $\langle \{f_1, f_2\}, \circ \rangle$ 是正规子群吗?

A

是

B

不是

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$

提交

3、因为三次置换群 $\langle \{f_1, f_4\}, \circ \rangle$ 虽是三次对称群 $\langle S_3, \circ \rangle$ 的子群，但不满足正规子群的条件，所以 $\langle \{f_1, f_4\}, \circ \rangle$ 不是正规子群，但是可交换群。

A

正确

B

错误

$\circ$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_1$	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$
$f_2$	$f_2$	$f_1$	$f_6$	$f_5$	$f_4$	$f_3$
$f_3$	$f_3$	$f_5$	$f_1$	$f_6$	$f_2$	$f_4$
$f_4$	$f_4$	$f_6$	$f_5$	$f_1$	$f_3$	$f_2$
$f_5$	$f_5$	$f_3$	$f_4$	$f_2$	$f_6$	$f_1$
$f_6$	$f_6$	$f_4$	$f_2$	$f_3$	$f_1$	$f_5$

提交

4、子群  $\langle H, * \rangle$  是群  $\langle G, * \rangle$  的任意正规子群，在  $\mathbf{G/H}$  上定义新的运算  $\circ$ ，对  $\forall a, b \in G$ ，有  $\mathbf{aH \circ bH = (a * b)H}$ ，则商群  $\langle \mathbf{G/H}, \circ \rangle$  的单位元是（ ）。

- ☐ A  $\mathbf{H}$
- ☐ B  $\mathbf{1H}$
- ☒ C  $\mathbf{eH}$
- ☐ D  $\mathbf{GH}$

提交

5、 $\langle \mathbf{N}_6, +_6 \rangle$ ,  $\mathbf{H} = \{0, 2, 4\}$ ,  $\mathbf{H}$  为  $\mathbf{N}_6$  的正规子群, 存在商群  $\mathbf{N}_6/\mathbf{H} = \langle \{0\mathbf{H}, 1\mathbf{H}\}, \circ \rangle$ , 下列哪些论述正确 (多选题)。

A

$\mathbf{H} = 0\mathbf{H} = 2\mathbf{H} = 4\mathbf{H}$

B

$1\mathbf{H}$  为商群  $\langle \mathbf{N}_6/\mathbf{H}, \circ \rangle$  的单位元

C

$e\mathbf{H}$  为商群  $\langle \mathbf{N}_6/\mathbf{H}, \circ \rangle$  的单位元

D

$0\mathbf{H}$  的逆元是自身,  $1\mathbf{H}$  的逆元也是自身

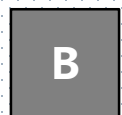
提交

6、设  $\langle H, * \rangle$  是  $\langle G, * \rangle$  的一个子群，对某个  $a \in G$ ， $a$  在满足下列哪个条件下左陪集  $aH$  一定可以构成群（多选题）。



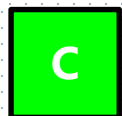
A

$a=e$  ( $e$  是群  $G$  的单位元)



B

$a \in G$



C

$a \in H$

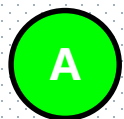


D

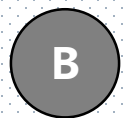
对  $a \in G$ ,  $\exists b \in G$ , 都有  $b^{-1} * a \in H$

提交

7、任何循环群的子群一定是可交换群。



正确



错误

提交



8、任何素数阶循环群只有两个生成元， $a \in G$ , 它们分别是 $a$ 和 $a^{-1}$ 。

☐ A 正确

☒ B 错误

提交

9、任何无限群 $G$ 有且仅有两个生成元 $a$ 和 $a^{-1}$ 。 $(a \in G)$

☐ A 正确

☒ B 错误

提交

10、因为在有限群中任何元素的周期一定是群的阶的正因子，所以偶数阶群中一定没有奇数阶的元素。

☐ A 正确

☒ B 错误

提交

11、 $\langle G, \times_7 \rangle$ 是一个群，即 $\langle \mathbb{Z}_7 - \{[0]\}, \times_7 \rangle$   
其中 $G = \{[1], [2], [3], [4], [5], [6]\}$ ，其运算表如图。下列哪些论述正  
确（多选题）

- ☐ A **[2]**是群的生成元
- ☒ B **[3]**是群的生成元
- ☐ C **[4]**是群的生成元
- ☒ D **[5]**是群的生成元
- ☐ E **[6]**是群的生成元

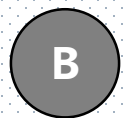
$\times_7$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

提交

12、给定群 $\langle G, * \rangle$  的任意正规子群  $\langle H, * \rangle$ ,  
则商群 $\langle G/H, \circ \rangle$ 一定是唯一的。



上述论述正确



上述论述错误

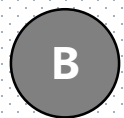
提交

13、 $\langle H, * \rangle$ 是群 $\langle G, * \rangle$ 的子群，如果 $\langle H, * \rangle$ 是可交换群，则 $\langle H, * \rangle$ 不一定是 $\langle G, * \rangle$ 的正规子群。



A

上述结论正确



B

上述结论错误

提交

14、假设  $\langle G, * \rangle$  是一个群， $H$  是  $G$  的非空子集，则  $\langle H, * \rangle$  是  $\langle G, * \rangle$  子群的充要条件是：  
对  $\forall a, b \in H$ ，有  $a * b \in H$ 。

- ☐ A 上述论述正确
- ☒ B 上述论述错误

15、假设  $\langle G, * \rangle$  是  $n$  阶有限群，则对  
 $\forall a \in G, |(a)| \mid n$ 。

A

上述论述正确

B

上述论述错误

提交



# 第五章 作业

习题一 1, 3

习题二 2, 5, 6

习题三 3, 4, 6, 7

习题四 1, 2, 4

习题五 1, 3

习题六 1, 3, 5, 7

习题七 1, 3, 5

$$\langle 2 \rangle \mathbf{M}_R \ddot{\cdot}^2 \langle , \rangle \cup \cap \neg$$

$$\Leftrightarrow \Rightarrow \emptyset \subseteq \rightarrow \exists \in \wedge \vee \forall x A_n$$

$$\textcircled{6} \textcircled{7} \textcircled{8} \textcircled{9} \textcircled{10} \textcircled{11} \textcircled{12} \textcircled{13} \textcircled{14} \dots \therefore \ddot{\cdot} A^2 \cup \cap \in$$

$$\Leftrightarrow \Rightarrow \exists$$

$$\textcircled{1} \textcircled{2} \textcircled{3} \textcircled{4} \textcircled{5} \forall x \rightarrow \epsilon^{-1} \neq \emptyset \epsilon \rightarrow \vee \wedge \Leftrightarrow$$

$$\exists \leq \subseteq \not\subseteq \not\rightarrow p \approx \equiv \pm \cdot ' \infty \not\approx 0 \neg \times_n \langle , \rangle \leftrightarrow^\circ$$

$$\oplus \oplus \wedge \vee \sim \cong \cdot \sqrt{\pi}_+ \Delta \leq \not\in A_n$$

$\forall \exists \emptyset \cap \cup \subseteq \subset \not\subseteq \notin \forall \in \leq \geq \dots \aleph \Sigma \{ \} \equiv \pm^\circ \infty$   
 $\alpha \beta \sigma \rho \varsigma \omega \zeta \psi \eta \delta \epsilon \varphi \lambda \mu \pi \Delta \theta \pm \prod \wedge \vee \forall \} \therefore$   
 $\sqrt{\supset}$

$\cong \approx \sim \infty \supseteq \cap \cup ^\circ \mathbf{C} \% _0 \geq \leq \therefore \prod \in \Sigma \nless \frac{1}{2} \frac{1}{4} \S$   
 $\yen \{ \} ? \pm \qquad \leftrightarrow \vee \wedge \neg \rightarrow \leftarrow \Rightarrow \Leftrightarrow$   
 $\downarrow \uparrow \Lambda \oplus \neq \odot - \langle \rangle$   
 $\star \blackstar \nabla \nless \frown \therefore \therefore \therefore \cup \cap \neq - - - //$   
 $// \therefore \therefore \therefore \perp \searrow \nearrow \swarrow \nwarrow \times \checkmark$   
 $\langle \lceil - \rceil \div \cdot ^\circ \cdot \langle 2, \mathbf{b} \rangle \rightsquigarrow \smile \Phi$