

# 第一周作业总结

作业批改要求较为宽松，具体如下：交了质量不错10分；交了且质量总体还可以，9分；有少做题或质量不太好，8分；少做的题较多或做错很多题，7分。

大概来说：错2题或者多题无合理清晰的过程的，9分；错四题或错四题以下且多题无合理清晰的过程的，8分；以此类推，此次提交完整作业的，7分最低。也可能出现因错的题目为大题，出现一道题影响1分的情况。

因此，本次作业获得10分的，并不代表全对且过程完全清晰合理，请大家注意核对各题答案。

本PPT分为重点分析题部分以及答案公布部分。答案均截取自被提交作业内被认为是完美的答案。

## 第一周作业重点分析题：

12.1.(5)

13.1.(3)

13.4.(3)、(4)

13.6

以上各题出错人数均达5人以上。

### 12.1.5 正确答案示例

(5)  $[S; \oplus]$ , 其中  $S = \{[1], [2], [3]\}$ ,  $[i] \oplus [j] = [ij]$ .

$\forall a, b \in S, a = [x], b = [y] : x, y = 1, 2, 3$

$$a \oplus b = [x] \oplus [y] = [xy]$$

situation 1:  $x, y$  中至少有一个为 1, 不妨令  $x=1$

$$\text{则 } [xy] = [y] \in S$$

situation 2:  $x, y$  全不为 1

$$x = y = 2 \text{ 时: } [xy] = [4] = [0] \notin S.$$

$\therefore$  运算封闭).

$\therefore [S; \oplus]$  不是代数系统.

### 13.1.3 正确答案示例

$\nexists$ :  $\forall A, B \in P(S)$ , 有  $(A \cup B) \cup C = A \cup (B \cup C)$ . 故是半群

又对  $\forall A \in P(S)$ , 有  $\emptyset \cup A = A \cup \emptyset = A$  且  $\emptyset \in P(S)$

∴  $\emptyset$  是  $[P(S); \cup]$  的单位元

$\therefore [P(S); \cup]$  是半群

### 13.4.(3)、(4)正确答案示例

13) 1的n次根(包含复数与实根)关于乘法·的运算

if: 1的n次根为  $e^{i\frac{2\pi x}{n}}$ ,  $x=0, 1, \dots, n$

①结合律:  $(e^{i\theta_1} \cdot e^{i\theta_2}) \cdot e^{i\theta_3} = e^{i(\theta_1 + \theta_2 + \theta_3)} = e^{i\theta_1} \cdot (e^{i\theta_2} \cdot e^{i\theta_3})$

②单位元: 单位元为 1

③逆元:  $e^{i\theta} \cdot e^{i\theta'} = e^{i2\pi} \Rightarrow \theta' = 2\pi - \theta$ . 逆元为  $e^{i(2\pi - \theta)}$

④交换律:  $e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1 + \theta_2)} = e^{i\theta_2} \cdot e^{i\theta_1}$

∴ 为交换群

14) 1的所有正整数次根关于乘法运算 同(3)

13.6 求证:  $S \neq \emptyset$ ,  $T_S$  为所有  $S \rightarrow S$  的一一对应所围成的集合, 关于映射的复合运算。

## 13.6 正确答案示例

$S^S$  为所有  $S \rightarrow S$  的映射组成的集合, 则  $[T_S; \circ]$  为群,  $[S^S; \circ]$  不是群

证明: (1) 对  $\forall f, g, h \in T_S$ ,  $\forall a \in S$ , 设  $h(a) = b, g(b) = c, f(c) = d$  ( $b, c, d \in S$ )

$$((f \circ g) \circ h)(a) = (f \circ g)(h(a)) = (f \circ g)(b) = f(g(b)) = f(c) = d$$

$$(f \circ (g \circ h))(a) = f((g \circ h)(a)) = f(g(h(a))) = f(g(b)) = f(c) = d$$

∴ 满足结合律。

又自身映射  $I \in T_S$ , 对  $\forall f \in T_S$ , 有  $I \cdot f = f \circ I = f$

∴ 有单位元  $I$

对  $\forall f \in T_S$ , 有  $f^{-1} \in T_S$  满足  $f \circ f^{-1} = f^{-1} \circ f = I$

即逆元为反映射

综上,  $[T_S; \circ]$  为群

(2)  $S^S$  为所有映射组成的群, 则非双射无反映射, 无逆元

∴  $[S^S; \circ]$  不是群

# 第一周作业答案公布：

12.1.(4)

(4)  $[S; \oplus]$  其中  $S = \{[0], [1], [2], [3]\}$ ,  $[i] \oplus [j] = [i+j]$

$$[0] = \{4k\}, k \in \mathbb{Z}$$

$$[1] = \{1+4k\}, k \in \mathbb{Z}$$

....

$\therefore \forall a, b \in S$ , 令  $a = [x], b = [y]; x, y = 0, 1, 2, 3$

则  $a \oplus b = [x] \oplus [y] = [x+y]$

若  $x+y < 4$ : 则  $[x+y]$  即  $a \oplus b$  仍属于  $S$

若  $x+y \geq 4$ : 则  $[x+y] = [x+y - 4k]$ , 其中  $k \in \mathbb{Z}, x+y - 4k \in [0, 3]$ .

$\therefore a \oplus b \in S$ , 运算满足封闭性.

$\therefore [S; \oplus]$  是代数系统

12.2.(1)

运算 "+": 单位元为 0;  $\forall a \in \mathbb{R}$ ,  $a+x=0$ ,  $x=-a \in \mathbb{R}$   
 $\therefore$  逆元为  $-a$ ;  $a+x=x$ ,  $\therefore$  无零元.

运算 ".":  $\forall a \in \mathbb{R}$ :  $a \cdot x = a$ ,  $x=1$   $\therefore$  单位元为 1;

$$a \cdot x = 1, x = \frac{1}{a} (a \neq 0)$$

$\therefore$  除 0 以外, 元素  $a$  的逆元为  $\frac{1}{a}$ .

$$ax = x, x = 0. \text{ 零元 } \neq 0.$$

12.2.(2)

运算“+”：单位元： $M_{nn}(0)$ ；

$\forall a \in M_{nn}(\mathbb{Q})$ ：其逆元为 $-a$ 。

无零元。

运算“.”：单位元： $E_n$ ；

$\forall a \in M_{nn}(\mathbb{Q})$ ，若 $|a| \neq 0$ ，其逆元为其逆阵，否则无逆元；

零元为 $M_{nn}(0)$ 。

12.3

解：不一定唯一，反例：

$$\begin{matrix} * & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 \\ 2 & 1 & 2 & 3 \\ 3 & 1 & 2 & 3 \end{matrix}$$

易知该代数系统中 1、2、3 都是石单位元。

但无石单位元，且石单位元不唯一。

只有石单位元的情况同理。

12.4

证明：对  $\forall [a]=[b] \in \tilde{S}$ ,  $[c]=[d] \in \tilde{S}$

$$\text{有 } a-b=k_1n, c-d=k_2n, k_1, k_2 \in \mathbb{Z}$$

$$\therefore axc - bxd = (k_1n+b)(k_2n+d) - bd$$

$$= k_1k_2n^2 + k_1dn + k_2bn$$

$$= kn, k \in \mathbb{Z} \quad \text{即 } axc \sim bxd$$

$$\therefore [axc] = [bxd]$$

$\therefore$   $\otimes$ 的运算结果与等价类的选取无关

12.7.  $\forall a \in S$ .

12.7

$$\varphi(a * e) = \varphi(a) = \varphi(a) \circ \varphi(e)$$

$$\varphi(e * a) = \varphi(a) = \varphi(e) \circ \varphi(a)$$

$\because a$  的任意性, 且  $\varphi(e) \in T$

$\therefore \varphi(e)$  为  $T$  的单位元.

$$\textcircled{2} \quad \varphi(a * a^{-1}) = \varphi(e) = \varphi(a) \circ \varphi(a^{-1})$$

$$\varphi(a^{-1} * a) = \varphi(e) = \varphi(a^{-1}) \circ \varphi(a)$$

$\therefore \varphi(e)$  为  $T$  的单位元.

$\therefore \varphi(a^{-1})$  为  $\varphi(a)$  的逆元.

反例:  $[R - \{0\}; \cdot] \xrightarrow{\varphi} [\{1, 0, -1\}; \cdot]$ .

$$\begin{cases} \forall a \in R - \{0\}, \varphi(a) = \begin{cases} 1, & a > 0 \\ 0, & a < 0 \end{cases} \end{cases}$$

在  $[\{1, 0, -1\}; \cdot]$  中, 1 为单位元, 而  $\forall a \in R, a < 0$ .  $\varphi(a) = \varphi(a^{-1}) = 0$   
 $\varphi(a) \cdot \varphi(a^{-1}) = 0 \neq 1 \quad \therefore \varphi(a^{-1})$  不为  $\varphi(a)$  之逆元.

## 12.5

[ $\mathbb{Z}; +$ ]:  $\forall a, b, c, d \in \mathbb{Z}, a \sim b, c \sim d.$

设  $a = n_1k + i_1, b = n_2k + i_1, c = m_1k + i_2, d = m_2k + i_2$

$$\begin{aligned} a+c &= k(n_1+m_1) + i_1+i_2 & (a+c)\%k &= i_1+i_2 \\ b+d &= k(n_2+m_2) + i_1+i_2 & (b+d)\%k &= i_1+i_2 \end{aligned} \Rightarrow \begin{aligned} (a+c)\%k &= i_1+i_2 \\ (b+d)\%k &= i_1+i_2 \end{aligned} \therefore a+c \sim b+d$$

[ $\mathbb{Z}; \times$ ]:  $\forall a, b, c, d \in \mathbb{Z}, a \sim b, c \sim d.$

设  $a = n_1k + i_1, b = n_2k + i_1, c = m_1k + i_2, d = m_2k + i_2$

$$\begin{aligned} a \times c &= (n_1k + i_1)(m_1k + i_2) & (a \times c)\%k &= i_1i_2 \\ b \times d &= (n_2k + i_1)(m_2k + i_2) & (b \times d)\%k &= i_1i_2 \end{aligned} \Rightarrow \begin{aligned} (a \times c)\%k &= i_1i_2 \\ (b \times d)\%k &= i_1i_2 \end{aligned} \therefore a \times c \sim b \times d.$$

$\therefore$  同余关系与整数的“+”，“ $\times$ ”是相容的。

12.6

证明：易知  $S$  和  $T$  中的元素都可用  $(a, b)$  ( $a, b \in \mathbb{C}$ ) 来唯一表示。

构造映射  $\varphi: S \rightarrow T$ , 对  $\forall (a, b) \in S$ ,  $\varphi(a+ib) = a+i\sqrt{b} \in T$ .

$\therefore \exists \forall (a, b), (c, d) \in S$ ,  $\varphi((a, b)) = a+i\sqrt{b}$ ,  $\varphi((c, d)) = c+i\sqrt{d}$

$$\therefore \varphi((a, b)) + \varphi((c, d)) = (a+c) + i\sqrt{(b+d)}$$

$$\varphi((a, b) + (c, d)) = \varphi((a+c) + i(b+d)) = (a+c) + i\sqrt{(b+d)}$$

$\therefore \varphi$  是从  $[S; +]$  到  $[T; +]$  的同态映射。

$$\text{又 } \varphi(s) = T$$

$\therefore \varphi$  是满同态映射。

$$\exists \forall \psi(\varphi(a+ib) = \psi(c+id)), \exists \forall a+i\sqrt{b} = c+i\sqrt{d}$$

$$\therefore a=c, b=d \quad \text{即 } a+ib = c+id$$

$\therefore \varphi$  是一一对应的。

$\therefore [S; +]$  和  $[T; +]$  是同构的。

13.1.(1)

(1)  $[z; -]$

答: 整数上的减法不满足结合律, 故不是半群

13.1.(2)

(2)  $[c; x]$

答: 复数上的乘法满足结合律, 又有单位元 1.

故  $[c; x]$  是 似群

13.1.(4)

$\forall A, B, C \in M_{m,n}(\mathbb{Q})$ , 有  $(A+B)+C = A+(B+C)$ , 故是半群

又  $0 \in M_{m,n}(\mathbb{Q})$ ,  $\forall A \in M_{m,n}(\mathbb{Q})$ , 有  $0+A=A+0=A$

$\therefore [M_{m,n}(\mathbb{Q}); +]$  有单位元 0.

$\therefore [M_{m,n}(\mathbb{Q}); +]$  是加法群

13.1.(5)

$\checkmark$ : 对  $\forall [a], [b], [c] \in \mathbb{Z}_n$ , 有知  $[a] \oplus [b] \oplus [c] = [a] \oplus ([b] \oplus [c])$

$\therefore$  满足结合律, 故是群

又  $[0] \in \mathbb{Z}_n$ , 对  $\forall [a] \in \mathbb{Z}_n$ , 有  $[0] \oplus [a] = [a] \oplus [0] = [a]$

$\therefore [0]$  是  $[\mathbb{Z}_n; \oplus]$  的单位元

$\therefore [\mathbb{Z}_n; \oplus]$  是双群

13.4.(1)

①结合律:  $\forall a, b, c \in \mathbb{Z}, (a \circ b) \circ c = (a+b-2) \circ c = a+b+c-4$

$$a \circ (b \circ c) = a \circ (b+c-2) = a+b+c-4$$

$\therefore (a \circ b) \circ c = a \circ (b \circ c)$ , 满足结合律

②单位元:  $\forall a \in \mathbb{Z}$ , 设  $\exists e \in \mathbb{Z}$ , s.t  $a \circ e = a + e - 2 = a \Rightarrow e = 2$

$$\therefore e \circ a = e + a - 2 = a = a \circ e$$

$\therefore [\mathbb{Z}; \circ]$  有单位元  $e = 2$

③逆元:  $\forall a \in \mathbb{Z}$ , 设  $\exists a' \in \mathbb{Z}$ , s.t  $a \circ a' = e$ . If  $a + a' - 2 = 2 \Rightarrow a' = 4 - a$

$$\therefore a' \circ a = 4 - a + a - 2 = 2 = e = a \circ a'$$

$\therefore [\mathbb{Z}; \circ]$  中每个元素都有逆元

④交换律:  $\forall a, b \in \mathbb{Z}$ , 有  $a \circ b = a + b - 2 = b + a - 2 = b \circ a$

$\therefore [\mathbb{Z}; \circ]$  满足交换律

综上,  $[\mathbb{Z}; \circ]$  是交换群

13.4.(2)

①结合律:  $(a \circ b) \circ c = (a + b - ab) \circ c = a + b - ab + c - ac - bc + abc$

$$a \circ (b \circ c) = a \circ (b + c - bc) = a + b + c - bc - ab - ac + abc$$

$$\therefore (a \circ b) \circ c = a \circ (b \circ c) \quad \text{满足结合律}$$

②单位元:  $a \circ e = a + e - ae = a \Rightarrow e = 0$

$$\therefore e \circ a = 0 + a - 0 = a$$

$$\therefore \text{有单位元 } e = 0$$

③逆元:  $a \circ a' = a + a' - a \cdot a' = e = 0$

$$a = a a' - a' = (a-1)a'$$

$$\therefore a' = \frac{a}{a-1} \quad (a \neq 1)$$

$\therefore$  不是所有元素都有逆元

综上,  $[Z; \circ]$  构成拟群

13.4.(5)  $[R - \{0\}; *]$ ,  $*: a * b = a^2 b^2$

$$\forall a, b, c \in R^*: a * (b * c) = a^2 (b^2 c^2)^2 = a^2 b^4 c^4$$

$$(a * b) * c = a^4 b^4 c^2$$

$\therefore [R - \{0\}; *]$  不是群

13.4.(6)

$\text{证:}$  为知  $[F[x], +]$  符合结合律. 单位元为 0. 符合交换律

$$\forall F[x], F[x] + F[y] = 1 \Rightarrow F[y] = -a_0 - a_1 x - \dots - a_n x^n$$

$\therefore [F[x], +]$  为交换群

13.4.(7)  $\forall$ : 易知满足结合律, 交换律, 单位元为 0, 逆元为  $-a - \sqrt{2}b$

$\therefore$  为交换群

13.4.(8)  $\exists$ : 令  $a$  为单位元, 且满足交换律

$\because$  包含  $a$  的三个数相乘 满足交换律

$\therefore$  只需验证:  $(b \cdot c) \cdot d = d \cdot d = c$ ,  $b \cdot (c \cdot d) = b \cdot b = c$

$$(b \cdot d) \cdot c = a \cdot c = c, b \cdot (d \cdot c) = b \cdot b = c$$

$\therefore$  满足结合律

$\therefore$  为交换群

13.10

证明] (1)  $\Rightarrow (ab)^2 = (ab)(ab) = (aa)(bb) = a^2 b^2$

(2)  $\Leftarrow (ab)^2 = abab = a^2 b^2 = aabb$

设  $a \cdot b$  的逆元为  $a^{-1}, b^{-1}$

$\therefore a^{-1}abab b^{-1} = a^{-1}aabb b^{-1}$

即  $ba = ab$

$\therefore [G; \cdot]$  是可交换的

综上，得证

13.11

证:  $\exists a \in G$ , s.t.  $a! = a^{-1}$

否则若  $\forall a \in G$ ,  $a = a^{-1}$

$\forall x, y \in G$ .  $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$ , 矛盾

$\therefore \exists b = a^{-1}$ ,  $\therefore b \neq a$  且  $a \neq e \neq b$ , 且  $ab = ba$

$\checkmark$ : (1) 结合律:  $\forall a, b, c \in \mathbb{Z}, (a * b) * c = (a + b - 1) * c = a + b + c - 2$

## 补充题

$$a * (b * c) = a * (b + c - 1) = a + b + c - 2 = (a * b) * c$$

$\therefore$  满足结合律

(2) 单位元:  $\forall a \in \mathbb{Z}, \exists e \in \mathbb{Z}, \text{st } a * e = a + e - 1 = a \Rightarrow e = 1$

$$\therefore e * a = 1 + a - 1 = a = a * e$$

$\therefore$  有单位元  $e = 1$

(3) 逆元:  $\forall a \in \mathbb{Z}, \exists a' \in \mathbb{Z}, \text{st } a * a' = a + a' - 1 = e = 1$

$$\therefore a' = 2 - a$$

$$\therefore a' * a = a' + a - 1 = 2 - a + a - 1 = 1 = e$$

$\therefore \forall a \in \mathbb{Z}, \text{存在逆元 } a' = 2 - a$

(4) 交换律:  $\forall a, b \in \mathbb{Z}, \text{有 } a * b = a + b - 1 = b + a - 1 = b * a$

$\therefore$  满足交换律

综上,  $[\mathbb{Z}; *]$  是交换群



# 第三四讲作业讲解

张政锋

邮箱 : 19210240021@fudan.edu.cn

# 01

---

第三讲

---



## 本次作业评分准则

**10分：**思路比较清晰，允许错漏**1题**与一些证明不严谨

**9分：**部分题目证明过程不严谨，错**两问~三问**

**8分：**错漏题达**3~4题**

**6, 7分：**错漏题**4题以上**

## 题目：

**易错题：** **13. (2) (3)** （循环置换的概念）

**较难题：** **33. (3) 、补充题2、补充题4**

13.12 将下述置换分解为不含公共元的循环置换，然后再将其分解成对换的乘积。

(2)  $\begin{pmatrix} 3 & 7 & 6 & 5 & 2 & 1 & 4 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$

(3)  $\begin{pmatrix} a & b & c & d & e & f \\ f & a & e & d & c & b \end{pmatrix}.$

13.12  
(2).  $\sigma = \begin{pmatrix} 3 & 7 & 6 & 5 & 2 & 1 & 4 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 7 & 6 & 5 & 4 \\ 2 & 3 & 7 & 6 & 5 & 4 & 1 \end{pmatrix}$   
 $= (1237654) = (12)(23)(37)(76)(65)(54)$

(3)  $\sigma = \begin{pmatrix} a & b & c & d & e & f \\ f & a & e & d & c & b \end{pmatrix} = \begin{pmatrix} a & f & b & c & e & d \\ f & b & a & e & c & d \end{pmatrix}$   
 $= (afb)(ce) = (af)(fb)(ce)$



13.13 已知置换:  $\delta = (1 \ 2 \ \dots \ n)$ ,  $S = (1 \ 2 \ 3)(4 \ 5)$ ,  $T = (1 \ 4)(3 \ 2)(1 \ 6)$ , 求:

(1)  $\delta^{-1}$ , (2)  $S^2 \cdot T$ , (3)  $(S \cdot T)^{-1}$ .

(1)  $\delta = (12)(23)(34)\cdots(n-1 \ n)$

$$\begin{aligned}\delta^{-1} &= (n-1 \ n) \cdots (21) = (n \ n-1)(n-1 \ n-2) \cdots (21) \\ &= (n \ n-1 \ \cdots \ 2 \ 1)\end{aligned}$$

(2)  $S^2 \cdot T = (123)(45)(123)(45) \cdot (14)(32)(16)$

$$\begin{aligned}&= (123)(123) \cdot (14)(32)(16) \\ &= (123)(231)(14)(32)(16)\end{aligned}$$

$$= (123)(2314)(32)(16)$$

$$= (123)(1423)(32)(16)$$

$$= (123)(142)(23)(32)(16)$$

$$= (123)(421)(16)$$

$$\begin{aligned}&= (123)(4216) = (312)(2164) = (31)(12)(21)(16)(64) \\ &= (3164)\end{aligned}$$

$$= (1643).$$

(3):  $(S \cdot T)^{-1}$  先化简  $S \cdot T$

$$S \cdot T = (123)(45)(14)(32)(16) = (16542)$$

$$(S \cdot T)^{-1} = (16542)^{-1} = (24561)$$



13.18 群  $G$ ,  $a, b, c$  是  $G$  中任意元素, 证明

- (1) 元素  $ab$  与  $ba$  同阶。
- (2) 元素  $abc, bca$  与  $cab$  同阶。

解: (1) 设  $ab$  的阶为  $n$ . (有限).

$$(ab)^n = e \Rightarrow (ab)^n = a(ba)^{n-1}b = e$$

由群  $G$   $b^{-1}$  存在. 则:

$$ba(ba)^{n-1}b = (ba)^n b = be = b$$

$$\Rightarrow (ba)^n = e. \text{ 设 } ba \text{ 的阶为 } n'. \text{ 则 } n' \leq n.$$

由  $(ba)^{n'} = e$ . 同理可得:  $(ab)^{n'} = e \Rightarrow n \leq n'$

$\therefore n = n'$ . 即  $ab$  与  $ba$  同阶.

(2) 由(1)知  $ab$  与  $ba$  同阶.

设  $bc = \beta$  则  $a\beta$  与  $\beta a$  同阶. 即  $abc$  与  $bca$  同阶.

设  $ca = \gamma$ . 则  $\gamma b$  与  $b\gamma$  同阶. 即:  $bca$  与  $cab$  同阶

02

## 第四讲



13.20  $G$  为群,  $a, b \in G$ , 已知  $ab = ba$ ,  $a$  的阶为  $n$ ,  $b$  的阶为  $m$ , 证明

(1)  $(n, m) = 1$  时,  $ab$  的阶为  $nm$ 。

(2)  $(n, m) \neq 1$ , 且  $(a) \cap (b) = \{e\}$  时,  $ab$  的阶为  $n, m$  之最小公倍数  $\text{LCM}(n, m)$ 。

(1).  $(n, m) = 1$  时,  $ab$  阶为  $mn$ . 已知  $ab = ba$

设  $ab$  的阶为  $p$ . 由  $(ab)^{mn} = a^{mn} b^{mn} = (a^n)^m (b^m)^n = e$   
 $\Rightarrow p | mn$ .

另一方面  $a^p b^p = (ab)^p = e \Rightarrow a^p = b^{-p}$ .

$a^p$  阶为  $d_1 = (n, p)$ . 则有  $a^{pd_1} = e = b^{-pd_1}$

$b^{-1}$  阶与  $b$  的阶相同  $\Rightarrow m | pd_1$ . 又  $(m, n) = 1 \Rightarrow m | p$ .

同理可得:  $n | p \quad \left. \begin{matrix} \\ (m, n) = 1 \end{matrix} \right\} \Rightarrow mn | p$

$\therefore p = mn$ . 即  $p$   $ab$  的阶为  $mn$ .

13.20  $G$  为群,  $a, b \in G$ , 已知  $ab = ba$ ,  $a$  的阶为  $n$ ,  $b$  的阶为  $m$ , 证明

(1)  $(n, m) = 1$  时,  $ab$  的阶为  $nm$ 。

(2)  $(n, m) \neq 1$ , 且  $(a) \cap (b) = \{e\}$  时,  $ab$  的阶为  $n, m$  之最小公倍数  $\text{LCM}(n, m)$ 。

(2) 设  $ab$  的阶为  $p$ . 由  $a, b$  阶分别为  $n, m$ ,  $a^n = b^m = e$ .

又  $(a) \cap (b) = \{e\}$ . 则  $\forall \alpha, \beta \in \mathbb{N}$  且  $a^\alpha = b^\beta$ . -是有  
 $n | \alpha$  且  $m | \beta$ .

又  $(b) = (b^{-1})$  则  $a^\alpha = b^{-\beta}$  时有:  $n | \alpha$  且  $m | \beta$ .

由  $(ab)^p = a^p b^p = e \Rightarrow a^p = b^{-p}$  故有:

$n | p$  且  $m | p$ .  $\Rightarrow \text{LCM}(m, n) | p$ .

另一方面  $(ab)^{\text{LCM}(m, n)} = a^{\text{LCM}(m, n)} b^{\text{LCM}(m, n)} = e \Rightarrow p | \text{LCM}(m, n)$

故  $p = \text{LCM}(m, n)$ . 即  $ab$  的阶为  $\text{LCM}(m, n)$ .

### 13.25 证明：任一无限群必有无限多的子群。

25、证明：设无限群  $[G]$  .

①  $G$  中有一个元素  $a$  的阶为无限.

$$\text{取 } H_1 = \{e, a^1, a^{-1}, a^2, a^{-2}, \dots\}.$$

$$H_2 = \{e, a^2, a^{-2}, a^4, a^{-4}, \dots\}.$$

--- ---

$$H_n = \{e, a^n, a^{-n}, a^{2n}, a^{-2n}, \dots\}.$$

--- ---

则  $H_1, H_2, \dots, H_n, \dots$  都是  $G$  的子群.  $G$  有无限多个子群.

②  $G$  中每个元素的阶均有限，则这些元素的个数无限.

记这些元素为  $\{a_1, a_2, \dots, a_n, \dots\}$ .

$$\text{取 } H_1 = \langle a_1 \rangle, H_2 = \langle a_2 \rangle, \dots, H_n = \langle a_n \rangle, \dots$$

则  $H_1, H_2, \dots, H_n, \dots$  都是  $G$  的子群.  $G$  有无限多个子群.

综上， $G$  有无限多个子群.

### 13.33 求陪集。

- (1)  $[R;+]$  关于子群  $[Q;+]$ 。
- (2)  $[C^*; \cdot]$  关于子群  $U = \{x \mid x \in C^*, \|x\| = 1\}$ 。
- (3)  $S_n$  关于  $n$  固定不变的置换子群。
- (4) 平面向量加法群，关于  $x$  轴向量子群。

解: (1) 全  $H = [Q; +]$ ,  $G = [R; +]$

$$\begin{aligned} \forall g \in G, gH &= \{gh \mid h \in H\} = G \\ Hg &= \{hg \mid h \in H\} = G \end{aligned}$$

∴ 陪集为  $[R; +]$

$$(2) \quad \forall g = r \cos \theta + ir \sin \theta \in C^*, \quad r \neq 0, \theta \in [0, 2\pi).$$

$$\forall x = \cos \alpha + i \sin \alpha \in U, \alpha \in [0, 2\pi)$$

$$gx = (r \cos \theta + ir \sin \theta)(\cos \alpha + i \sin \alpha)$$

$$= r(\cos \theta \cos \alpha - \sin \theta \sin \alpha) + i r (\sin \theta \cos \alpha + \cos \theta \sin \alpha)$$

$$= r \cos(\theta + \alpha) + i r \sin(\theta + \alpha)$$

又显然  $gx = xg$ . 由  $x$  的任意性.

$$\therefore gC^* = C^*g = \{x \mid x \in C^*, \|x\| = |g|\}. \quad (|g| = r.)$$

$$(3) \forall \sigma_s = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_{s(1)} & \sigma_{s(2)} & \cdots & \sigma_{s(n)} \end{pmatrix} \in S_n.$$

设  $S_n'$  为  $n$  固定不变的子群.  $\forall \sigma_{s'} = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma_{s'(1)} & \sigma_{s'(2)} & \cdots & \sigma_{s'(n-1)} & n \end{pmatrix} \in S_n'$

$$\begin{aligned} \sigma_s \cdot \sigma_{s'} &= \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_{s(1)} & \sigma_{s(2)} & \cdots & \sigma_{s(n)} \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma_{s'(1)} & \sigma_{s'(2)} & \cdots & \sigma_{s'(n-1)} & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma_s(\sigma_{s'(1)}) & \sigma_s(\sigma_{s'(2)}) & \cdots & \sigma_s(\sigma_{s'(n-1)}) & \sigma_s(n) \end{pmatrix} \end{aligned}$$

$\therefore$  由  $\sigma_s \cdot S_n'$  是固定  $n$  变化为  $\sigma_{s(n)}$  的置换子群.

$$\therefore \sigma_s \cdot S_n' = S_n' \cdot \sigma_s.$$

同理  $S_n' \cdot \sigma_s$  也是固定  $n$  变化为  $\sigma_{s(n)}$  的置换子群.

$$(4) \text{ 设关于 } x \text{ 轴向量子群 } H = \{(x, 0) \mid x \in \mathbb{R}\}$$

$$\text{平面向量加法群 } [G; +]. \quad G = \{(x, y) \mid x, y \in \mathbb{R}\}.$$

$$\forall g = (x, y) \in G.$$

$$\begin{aligned} gH &= \{(x+a, y) \mid a \in \mathbb{R}\} = \{(y, x+a) \mid a \in \mathbb{R}\} = Hg. \\ \therefore gH &= Hg = \{(x, y) \mid x, y \in \mathbb{R} \text{ 且 } y \text{ 为定值}\} \end{aligned}$$





13.36  $H$  为  $G$  的正规子群，在  $G$  上定义二元关系  $\rho$ ：对任  $x, y \in G$ ， $x\rho y$  当且仅当  $xH = yH$ ，记为  $x \equiv y \pmod{H}$ ，证明

(1)  $\rho$  是等价关系。

(2)  $\rho$  关于  $G$  的运算相容，即当  $x \equiv y \pmod{H}$ ,  $x' \equiv y' \pmod{H}$  时， $xx' \equiv yy' \pmod{H}$ 。

(3)  $x\rho y$  当且仅当  $x^{-1}y \in H$ 。

(1)  $\forall x \in G$ ,  $xH = xH$   
 $\therefore x \rho x$  (自反的)  
 $\therefore \rho$  是自反的  
 $\forall x, y \in G$ , 若  $x \rho y$ , 则  $xH = yH$   
 $\therefore yH = xH$ ,  $y \rho x$   
 $\therefore \rho$  是对称的  
 $\forall x, y, z \in G$ , 若  $x \rho y$ ,  $y \rho z$   
则  $xH = yH = zH$   
 $\therefore x \rho z$   
 $\therefore \rho$  是传递的  
 $\therefore \rho$  是等价关系

(2) 由  $x \equiv y \pmod{H}$ ,  $x' \equiv y' \pmod{H}$  可得

对  $\forall h \in H$ ,  $xh = yh$ ,  $x'h = y'h$

由于  $H$  是正规子群 故  $\forall a \in G$ ,  $aH = Ha$

则  $hx = hy$

由消去性得  $xx'h = xy'h$ ,  $hx'y' = hy'y$   $\Rightarrow$   $xy'h = yy'h$

故  $xx'h = yy'h$ , 即  $xx' \equiv yy' \pmod{H}$ .

$$(3) x \rho y \Rightarrow x^{-1}y \in H.$$

$$\because x, y \in G. \quad xH = yH.$$

$$\therefore \text{必然 } \exists h_1, h_2 \in H. \text{ s.t. } xh_1 = yh_2.$$

$$\text{又 } h_1^{-1} \in H \quad \therefore h_1 h_2^{-1} = x^{-1}y$$

$$\therefore h_1 h_2^{-1} \in H$$

$$\therefore x^{-1}y \in H$$

$$x^{-1}y \in H \Rightarrow x \rho y$$

$$\forall h \in H. \text{ 必有 } g \in G. \text{ s.t. } x \cdot h = y \cdot g.$$

$$\therefore g = y^{-1} \cdot (xh) = (y^{-1}x) \cdot h = (x^{-1}y)^{-1} \cdot h$$

$$\text{又 } x^{-1}y \in H. \quad \therefore (x^{-1}y)^{-1} \in H \quad \therefore g \in H.$$

$$\text{由 } h \text{ 的任意性. 有 } \{xh \mid h \in H\} = \{y g \mid g \in H\} = \{yh \mid h \in H\}.$$

$$\therefore xH = yH. \text{ 即 } x \rho y.$$

03

## 四道补充题

补充:1.群G是阶为偶数的有限群,则G中阶为2的元素个数一定是奇数.

设 $a$ 的阶为 $p$ , 则 $a^p = e$ . 设 $a^{-1}$ 的阶数为 $k$ .

$$(a^{-1})^p = (a^p)^{-1} = e \text{ 故 } k \leq p.$$

$$\text{再考虑 } a^k = (a^{-1})^{-k} = ((a^{-1})^k)^{-1} = e, \text{ 则 } p \leq k$$

综上,  $p = k$ .

易知 阶数为1的元素只有 $e$ ; 当 $a \neq a^{-1}$ 时,  $a$ 与 $a^{-1}$ 的阶数大于2

故 G 中阶数不为2的元素有奇数个

又有 G 的阶为偶数, 故 G 中阶为2的元素个数一定是奇数

2. 设  $G$  是  $rs$  阶循环群,  $(r,s)=1$ ,  $H_1$  和  $H_2$  分别为  $G$  的  $r$  和  $s$  阶子群, 证明:  $G = H_1 H_2 = \{h_1 h_2 | h_1 \in H_1, h_2 \in H_2\}$

思路一: 易知  $H_1 H_2 \subseteq G$ , 证  $|H_1 H_2| = |G|$

易知  $H_1 H_2 \subseteq G$ , 证  $|H_1 H_2| = |G|$

$$|H_1| = r, |H_2| = s \quad \text{设 } H_1 = \{h_1, h_2, \dots, h_r\}$$

由引理 13.1  $\forall h_1 \in H_1, |h_1 H_2| = |H_2| = s$

由引理 13.2 对  $h_1 \in H_1, h_2 \in H_1, h_1 \neq h_2$  时,  $h_1 H_2 \cap h_2 H_2 = \emptyset \quad ((r,s)=1)$

$$\therefore |H_1 H_2| = |\{h_1 H_2 \cup h_2 H_2 \cup \dots \cup h_r H_2\}| = |H_1| |H_2| = rs$$

$\because H_1, H_2$  为  $G$  的子群  $\therefore H_1 H_2 \subseteq G$  且  $|H_1 H_2| = |G| = rs$

$$\therefore G = H_1 H_2$$

$H, H_2$  为  $G$  的子群,  $\therefore$  对  $\forall h_1 \in H, h_2 \in H_2$ , 有  $h_1 \in H, h_2 \in H_2$   
 $\therefore h_1 h_2 \in G$  即  $H_1 H_2 \subseteq G$ .

$\because G$  为  $r, s$  阶循环群, 该  $a$  为其中一个生成元  $\therefore G = \{a^0, a^1, \dots, a^{rs-1}\}$

$\forall g \in G, \exists k \in [0, rs-1]$ , 有  $g = a^k \quad \therefore (r, s) = 1$ .

①  $r, s$  中至少有一个为 1, 结论显然成立.

②  $r, s$  均不为 1, 则  $r \neq s$  不妨设  $r, s$  中较大数为  $r$ .

$\because (r, s) = 1$ .  $k$  可唯一表示成  $k = mr + ns$  的形式.

且  $mr + ns < rs$  即  $m < s, n < r$ .

$\therefore \forall g \in G, g = a^k = a^{mr+ns} = a^{mr} \cdot a^{ns} = (a^r)^m \cdot (a^s)^n$

$\therefore H_1, H_2$  分别为  $G$  的  $r$  阶和  $s$  阶子群

$\therefore H_1 = \{a^0, a^s, \dots, a^{(s-1)s}\}, H_2 = \{a^0, a^r, \dots, a^{(r-1)r}\}$

$\therefore (a^r)^m \in H_2, (a^s)^n \in H_1$  即  $g \in H_1 H_2 \quad \therefore G \subseteq H_1 H_2$

综上,  $G = H_1 H_2$ . 得证

思路二: 易知  $H_1 H_2 \subseteq G$ , 证  $G \subseteq H_1 H_2$

严谨的思路：

下证  $H_1, H_2$  是  $G$  的循环子群. 由  $G$  是循环群. 则  $H_1$  中的元素均可表示为  $a^n$ .  $a$  为  $G$  的生成元.

对  $d > 0$ . 设  $d$  为  $a^d \in H_1$  的最小  $d$ . 对  $\forall a^p \in H_1$ .

$\exists \alpha, \beta \in \mathbb{Z}$ , 使  $d\alpha + p\beta = (d, p)$ .

而  $a^{d\alpha + p\beta} = (ad)^\alpha \cdot (ap)^\beta \in H_1 \Rightarrow a^{(d, p)} \in H_1$ .

又  $d$  为最小的整数.  $\Rightarrow (d, p) \geq d$ . 而  $(d, p) \leq d$ .

$\Rightarrow (d, p) = d$ . 则  $a^p = (ad)^r$ .

故  $\forall a^p \in H_1$ ,  $a^p$  可表示为  $(ad)^r$ . 则  $H_1$  为循环群. 同理可证  $H_2$  为循环群.

又  $H_1$  为  $r$  阶循环群.  $H_1$  可写作  $H_1 = \{h_1^1, h_1^2, \dots, h_1^r\}$ .

$H_1$  的单位元  $e = h_1^r$  为  $G$  的单位元  $a^{rs}$ .  $\Rightarrow h_1 = a^s$ .

復旦大學  $\therefore H_1 = \{a^s, a^{2s}, \dots, a^{rs}\}$ . 同理  
 $H_2 = \{a^r, a^{2r}, \dots, a^{rs}\}$ .

构造  $G' \rightarrow G$  的映射:  $\varphi(h_1, h_2) = \varphi(a^{m_s} a^{n_r}) = a^{ms+nr}$

而  $G'$  中, 若有  $a^{m's} \cdot a^{n'r} = a^{ms} \cdot a^{nr}$   $m, m' \in \{1, 2, \dots, r\}$

即:  $a^{(m-m')s+(n-n')r} = a^{krs}$   $n, n' \in \{1, 2, \dots, s\}$ .

$$m-m' < r, \quad n-n' < s.$$

$$\Rightarrow (m-m')s + (n-n')r = krs.$$

$$\Rightarrow rs \mid (m-m')s + (n-n')r \quad \text{又 } (r, s) = 1 \text{ 且 } r \nmid (m-m'), s \nmid (n-n')$$

$$\Rightarrow m-m'=0 \quad n=n'$$

即  $H_1, H_2$  中两两相乘结果互不相同.  $\Rightarrow |G'| = |H_1||H_2| = rs$ .

又  $\varphi$  为  $G' \rightarrow G$  的映射.  $\Rightarrow G'$  与  $G$  同构且  $\varphi$  为恒等映射.

$G'$  与  $G$  同构. 又  $\forall g' \in G$ .  $g' = h'_1 h'_2$ .  $h'_1 \in H_1, h'_2 \in H_2$ .

$$\Rightarrow g' \in G.$$

即  $G'$  中元素一定是  $G$  中的元素. 故  $G = G'$ . 即  $G = H_1 H_2$ .

### 3. $[H_1; \cdot]$ 和阶 $[H_2; \cdot]$ 是群 $[G; \cdot]$ 的子群, $[H_1 \cup H_2; \cdot]$ 是否是群 $[G; \cdot]$ 的子群? 说明理由

举例子 由例 13.9 所给出的  $S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$  及其运算表, 根据定理 13.16, 关于 $\circ$ 运算封闭的子集所有

$$\begin{aligned}H_1 &= \{e, \sigma_1\} \\H_2 &= \{e, \sigma_2\} \\H_3 &= \{e, \sigma_3\} \\H_4 &= \{e, \sigma_4, \sigma_5\}\end{aligned}$$

这 4 个都是  $S_3$  的子群, 其中  $H_4 = A_3$ 。

例 13.17 找出  $[Z_{12}; \oplus]$  的所有子群。

根据同余类加法运算的定义, 可知下述几个都是  $Z_{12}$  的子群,

$$\begin{aligned}H_1 &= \{[0], [2], [4], [6], [8], [10]\} \\H_2 &= \{[0], [4], [8]\} \\H_3 &= \{[0], [3], [6], [9]\} \\H_4 &= \{[0], [6]\}\end{aligned}$$

这 4 个子群都是循环群, 例如  $H_1 = ([2])$  等。

4. 设  $H_1, H_2$  是  $G$  的子群, 证明  $H_1H_2$  是  $G$  的子群当且仅当  $H_1H_2 = H_2H_1$ , 其中  $H_1H_2 = \{h_1h_2 | h_1 \in H_1 \text{ 并且 } h_2 \in H_2\}$ ,  $H_2H_1 = \{h_2h_1 | h_1 \in H_1 \text{ 并且 } h_2 \in H_2\}$

(必要性)  $H_1H_2$  是  $G$  的子群, 证:  $H_1H_2 = H_2H_1$

已知  $H_1, H_2$  是  $G$  子群,  $H_1H_2$  是  $G$  子群, 证明:  $H_1H_2 = H_2H_1$

$\forall h_1 \in H_1, h_2 \in H_2, h_1h_2 \in H_1H_2, \text{ 则 } (h_1h_2)^{-1} \in H_1H_2$

$$(h_1h_2)^{-1} = h_2^{-1}h_1^{-1} \in H_2H_1$$

$\therefore \forall (h_1h_2)^{-1} \in H_1H_2, \text{ 有 } h_2^{-1}h_1^{-1} \in H_2H_1$

$\therefore H_1H_2 \subseteq H_2H_1$  同理  $H_2H_1 \subseteq H_1H_2$

$$\therefore H_1H_2 = H_2H_1$$

(充分性)  $H_1H_2 = H_2H_1$ , 证:  $H_1H_2$  是  $G$  的子群 (解法一)

已知  $H_1, H_2$  是  $G$  子群,  $H_1H_2 = H_2H_1$ , 证明:  $H_1H_2$  是  $G$  子群

由定理 13.14 出发, 证明 ①  $H_1H_2$  关于  $G$  的运算封闭

$$\textcircled{2} \quad \forall h_1, h_2 \in H_1H_2, (h_1h_2)^{-1} \in H_1H_2$$

① 取  $h_1, h_2 \in H_1H_2$ ,  $h'_1, h'_2 \in H_1H_2$ , 证  $h_1h_2 \cdot h'_1h'_2 \in H_1H_2$

$$h_1h_2h'_1h'_2 = h_1(h_2h'_1)h'_2 \quad \because H_2H_1 = H_1H_2$$

$$= h_1h_{11}h_{22}h'_2 \quad \because H_1, H_2 \text{ 为 } G \text{ 的子群}$$

$$= h_{11}h_{222} \in H_1H_2$$

② 取  $h_1, h_2 \in H_1H_2$ , 考虑  $(h_1h_2)^{-1}$

$$(h_1h_2)^{-1} = h_2^{-1}h_1^{-1} \quad (\because H_1, H_2 \text{ 为 } G \text{ 的子群且 } H_2H_1 = H_1H_2)$$

$$= h'_1h'_2 \quad (\therefore \exists h_1' \in H_1, h_2' \in H_2 \text{ 使 } h_1'h_2' = h_2^{-1}h_1^{-1})$$

$$\therefore (h_1h_2)^{-1} \in H_1H_2$$

(充分性)  $H_1H_2 = H_2H_1$ , 证:  $H_1H_2$  是  $G$  的子群 (解法二)

已知  $H_1, H_2$  是  $G$  子群,  $H_1H_2 = H_2H_1$ , 证明:  $H_1H_2$  是  $G$  子群

由定理 13.15 出发, 证明  $\forall h_1, h_2, h'_1, h'_2 \in H_1H_2, h_1h_2(h'_1h'_2)^{-1} \in H_1H_2$

$$\begin{aligned} h_1h_2(h'_1h'_2)^{-1} &= h_1h_2h_2'^{-1}h_1'^{-1} && (\exists h_{22} \in H_2 \text{ 使 } h_{22} = h_2h_2'^{-1}) \\ &= h_1h_{22}h_1'^{-1} && (h_{22}h_1'^{-1} \in H_2H_1, \& H_2H_1 = H_1H_2) \\ &= h_1h_{11}h_{222} && (\exists h_{11} \in H_1, h_{222} \in H_2, \text{ 使 } h_{11}h_{222} = h_{22}h_1'^{-1}) \\ &= h_{111}h_{222} \in H_1H_2 && (\exists h_{111} \in H_1 \text{ 使 } h_{111} = h_1h_{11}) \end{aligned}$$



謝謝  
THANK YOU

# 第五六讲作业詳解

茹港徽

邮箱：19210240196@fudan.edu.cn

## 本次作业评分准则

**10分：**思路比较清晰，允许错漏**2**题与一些证明不严谨

**9分：**部分题目证明过程不严谨，错3-4问

**8分：**错漏题达**5-6**题

**6, 7分：**错漏题**6**题以上

## 错的较多的题目：

13. 28、13. 35、13. 40的部分证明题、13. 41的部分题

13.27 设  $G = \langle a \rangle$ ,  $|G| = n$ , 证明

- (1) 它的任一子群是循环群。
- (2) 它的任一元的阶可以整除  $n$ 。
- (3) 设  $d$  为  $n$  的因子, 则  $G$  必存在唯一一个阶为  $d$  的子群。

(1) 设  $G = \{a, a^2, \dots, a^n = e\}$   $H = \{a^{m_1}, a^{m_2}, \dots, a^{m_k}\}$   $d = \min\{m_1, m_2, \dots, m_k\}$

反证, 若  $H$  不是循环群, 则  $\exists m_i$  使  $a^{m_i} \notin \langle a^d \rangle$  那  $m_i = rd + s$ ,  $r \in \mathbb{Z}$ ,  $0 < s < d$   
由于  $a^d \in H$  故  $a^{-rd} \in H$ ,  $a^{-rd} \cdot a^{m_i} \in H$  故  $a^{-rd} \cdot a^{m_i} = a^s \in H$   
 $\Rightarrow d = \min\{m_1, m_2, \dots, m_k\}, 0 < s < d$ , 故假设不成立

(2) ① 对单位元  $e = a^n$ , 其阶为 1, 整除  $n$ .

② 对其它元素  $a^\alpha$ ,  $\alpha = 1, \dots, n-1$ , 设其阶为  $p_\alpha$ .

$$\Rightarrow (a^\alpha)^{p_\alpha} = e \Rightarrow n | \alpha p_\alpha, \alpha = 1, \dots, n-1, \alpha < n$$

且若  $(\alpha, n) = 1$ , 则  $n | p_\alpha$ , 此时  $a^\alpha$  阶为  $p_\alpha = n$ .  $p_\alpha | n$

③ 若  $(\alpha, n) \neq 1$ , 则  $\frac{n}{(\alpha, n)} \mid \frac{\alpha}{(\alpha, n)} p_\alpha$

$$\text{且 } \left( \frac{n}{(\alpha, n)}, \frac{\alpha}{(\alpha, n)} \right) = 1 \Rightarrow \frac{n}{(\alpha, n)} \mid p_\alpha.$$

此时  $a^\alpha$  阶为  $\frac{n}{(\alpha, n)} = p_\alpha$ .  $p_\alpha | n$

综上: 群  $G$  任一元的阶整除  $n$ .

(3) 由(1)知,  $G$  的子群为循环群, 故阶为  $d$  的子群可表示为

$$H = \{b, b^2, \dots, b^d = e\}, \text{ 且 } b^d = a^n = e \Rightarrow b = a^{n/d}$$

$d$  为  $n$  的因子, 则  $d | n$ . 故

$$H = \{a^{n/d}, a^{2n/d}, \dots, a^n\} \text{ 唯一.}$$

13.28 设  $G = \langle a \rangle$ ,  $b = a^k$ ,  $|G| = n$ , 讨论当  $b$  为  $G$  的生成元时,  $k$  具有什么性质? 当  $b$  为  $G$  的一个子群的生成元时,  $k$  又具备什么性质?

$\because b$  为  $G$  的生成元  $\therefore b = a^k$  的阶为  $n$ .

令  $d = (n, k)$ .  $\therefore k = k_1 \cdot d$ .  
则  $(a^k)^{n/d} = (a^{k_1 \cdot d})^{n/d} = a^{k_1 \cdot n} = e$ .  
 $\therefore n | n/d \Rightarrow d = 1$ .

$\therefore b$  为  $G$  的生成元时  $(n, k) = 1$ .

设  $H$  为  $G$  的一个子群.  $H$  的阶为  $p$ .

则由 Lagrange 定理.  $r = |G| / |H|$ . 则  $n = pr$ .  
 $b$  为  $H$  的生成元  $\Rightarrow b^p = (a^k)^p = e \Rightarrow n | kp \Rightarrow \frac{n}{p} | k \Rightarrow r | k$ .  
 $\therefore (k, n) = r = |G| / |H|$ .

13.29 证明：指数为 2 的子群，一定是正规的。

设  $G$  为群， $H$  为  $G$  的子群。

$\because H$  指数为 2.  $\therefore H$  有 2 个不同的左 (右)陪集。

$$\therefore He = eH = H.$$

$\therefore H, G - H$  为  $H$  的两个陪集。

$\forall g \in G$ . 若  $g \in H$ . 则  $gH = Hg = H$ .

若  $g \notin H$ . 则  $gH \neq H$ .  $Hg \neq H$ .  
 $\therefore gH = G - H = Hg$ .

$\therefore \forall g \in G$ . 有  $gH = Hg$ .

$\therefore H$  是正规子群。

13.30  $G$  为群,  $C \subseteq G$ ,  $C = \{x \mid x \in G \text{ 且对 } \forall g \in G, xg = gx\}$ , 称  $C$  为  $G$  的中心, 证明它是正规子群。

对  $e \in G$ ,  $\forall x \in G$ . 显然  $ex = xe = x \Rightarrow e \in C$ .  
 $\therefore C$  非空.

$\forall a, b \in C$ .  $(ab)x = a(bx) = (ax)b = x(ab) \Rightarrow ab \in C$ .  
 $\therefore$  满足封闭性.

$\forall a \in C$ . 则对于  $a^{-1} \in G$ .  $a \cdot a^{-1} = a^{-1} \cdot a = e \Rightarrow a^{-1} \in C$ .  
 $\therefore$  对  $\forall a \in C$ .  $a^{-1} \in C$ .

$\therefore C$  是  $G$  的子群.

又  $\forall g \in G$ .  $gC = \{gx \mid x \in C\} = \{xg \mid x \in C\} = Cg$ .  
 $\therefore C$  是  $G$  的正规子群.

13.31 群  $G$  中的所有与给定元  $a \in G$  可换的元素全体  $N(a) = \{x \in G \mid xa = ax\}$  构成  $G$  的一个子群；循环群  $(a)$  是  $N(a)$  的正规子群。

对  $\forall a \in G$ . 显然  $e \in N(a)$ .

$\forall x, y \in N(a)$ .  $(xy)a = x(ya) = (xa)y = a(xy) \Rightarrow xy \in N(a)$ .

$\therefore N(a)$  满足封闭性.

$\forall x \in N(a)$  则对其逆元  $x^{-1} \in G$ .  $x \cdot x^{-1} = x^{-1} \cdot x = e$ .

$\therefore \forall x \in N(a)$  有  $x^{-1} \in N(a)$

$\therefore N(a)$  是  $G$  的一个子群.

$$\begin{aligned}\forall g \in N(a) \quad a^x \in (a). \quad & g \cdot a^x \cdot g^{-1} = (g \cdot a) \cdot a^{x-1} \cdot g^{-1} \\ &= a \cdot (g \cdot a^{x-1}) \cdot g^{-1} \\ &= \dots = a^x \cdot g \cdot g^{-1} \\ &= a^x \cdot (g \cdot g^{-1}) = a^x \in (a).\end{aligned}$$

$\therefore (a)$  是  $N(a)$  的正规子群.

13.32 证明：两个正规子群的交仍为正规子群。

设  $H_1, H_2$  是  $G$  的两个正规子群  $H = H_1 \cap H_2$ .

$\forall a, b \in H \quad \begin{cases} a, b \in H_1 & \therefore ab \in H_1 \\ a, b \in H_2 & \therefore ab \in H_2 \end{cases} \Rightarrow ab \in H_1 \cap H_2 \Rightarrow ab \in H.$

$\therefore$  满足封闭性.

$\forall a \in H \quad \begin{cases} a \in H_1 & \therefore a^{-1} \in H_1 \\ a \in H_2 & \therefore a^{-1} \in H_2 \end{cases} \Rightarrow a^{-1} \in H_1 \cap H_2 \Rightarrow a^{-1} \in H.$

$\therefore \forall a \in H \quad \therefore a^{-1} \in H.$

$\therefore H$  是  $G$  的一个子群.

$\forall g \in G \quad h \in H \quad \begin{cases} ghg^{-1} \in H_1 & \therefore ghg^{-1} \in H_1 \\ ghg^{-1} \in H_2 & \therefore ghg^{-1} \in H_2 \end{cases} \therefore ghg^{-1} \in H.$

$\therefore H$  是正规子群.

13.34 证明交换群  $G$ , 关于子群  $H$  的商群  $G/H$  是交换群。

$$\forall Hg, Hg' \in G/H.$$

$$Hg \circ Hg' = Hgg' = Hg'g \quad (\text{由 } G \text{ 是交换群}) \\ = Hg' \circ Hg$$

$\therefore G/H$  是交换群。

### 13.35 求商群。

(1)  $R^* = R - \{0\}$  乘法群关于  $D = \{x > 0 \mid x \in R\}$  子群。

(2)  $[R; +]$  关于  $[Z; +]$  子群。

(3)  $[C^*; \cdot]$  关于  $[D; \cdot]$  子群。

(4)  $[U; \cdot]$  关于  $[U_n; \cdot]$  子群, 其中  $U = \{a + ib \mid a, b \in R, \|a^2 + b^2\| = 1\}$ ,  $n$  为给定自然数,  $U$  的

子群:  $U_n = \{x \mid x \in U, x^n = 1\}$ 。

(1) 商集中包含  $\{x > 0 \mid x \in R\}$  和  $\{x < 0 \mid x \in R\}$  两个陪集, 关于  $\odot$  运算构成群。

(2) 商群为  $\{[x] \mid x \in R, x \in [0, 1]\}$ ,  $[x] = \{x + k \mid k \in \mathbb{Z}\}$

(3) 商群为  $\{[e^{i\theta}] \mid \theta \in [0, 2\pi)\}$ ,  $[e^{i\theta}] = \{pe^{i\theta} \mid p > 0, p \in R\}$

(4)  $U = \{e^{i\theta} \mid \theta \in [0, 2\pi)\}$ ,  $U_n = \{e^{i(\frac{2k\pi}{n})} \mid k \in N \text{ 且 } k < n\}$

商群为  $\{[e^{i\varphi}] \mid \varphi \in [0, \frac{2\pi}{n})\}$ ,  $[e^{i\varphi}] = \{e^{i\varphi + i \cdot \frac{2k\pi}{n}} \mid k \in N \text{ 且 } k < n\}$

13.37  $\phi: G \rightarrow G'$  是群  $G$  与  $G'$  的同态映射, 证明

(1)  $\phi(G) \subseteq G'$  是  $G'$  的子群。

$$\forall x \in G, \quad \phi(e) \circ \phi(G) = \phi(G) \circ \phi(e) = \phi(e \cdot G) = \phi(G) \Rightarrow \phi(e) \text{ 是 } \phi(G) \text{ 的单位元.}$$

$$\forall a, b \in G, \quad \phi(a) \circ \phi(b) = \phi(ab)$$

$\because ab \in G, \quad \therefore \phi(ab) \in \phi(G) \subseteq G' \Rightarrow \text{满足封闭性.}$

$\forall a \in G, \quad a^{-1}$  为  $a$  在  $G$  中逆元.

$$\phi(a) \circ \phi(a^{-1}) = \phi(a \cdot a^{-1}) = \phi(e).$$

$\therefore \forall \phi(a) \in \phi(G), \quad \exists \phi(a^{-1}) = (\phi(a))^{-1} \in \phi(G).$

$\therefore \phi(G) \subseteq G'$  是  $G'$  的子群.

### 13.40 证明

- (1)  $[D; \cdot] \cong [R; +]$ 。
- (2)  $[Q_+; \cdot]$  与  $[Q; +]$  不同构, 其中  $Q_+ = \{x \in Q \mid x > 0\}$ 。
- (3)  $Z_4$  不同构于  $K_4$  (四元克莱茵群)。
- (4)  $G$  与  $G'$  同态,  $\phi$  为其同态映射,  $G$  与  $G'$  同构, 当且仅当  $K = \{e\}$ 。

(1) 令  $\varphi(x) = 2^x$ . 显然  $\varphi: R \rightarrow D$  是一个双射  
 则  $\forall a, b \in R$ . 有  $\varphi(a) \cdot \varphi(b) = 2^a \cdot 2^b = 2^{a+b} = \varphi(a+b)$   
 $\therefore \varphi$  是  $[R; +]$  到  $[D; \cdot]$  的一个满同态映射.  
 $\therefore [D; \cdot] \cong [R; +]$ .

(2) 反证. 若  $[Q_+; \cdot]$  与  $[Q; +]$  同构. 则必然存在同构映射  $\varphi: Q \rightarrow Q_+$   
 使得  $\exists a \in Q$ . 使  $\varphi(a) = 2$ .  
 又  $2 = \varphi(a) = \varphi(\frac{a}{2} + \frac{a}{2}) = \varphi(\frac{a}{2}) \cdot \varphi(\frac{a}{2}) \Rightarrow \varphi(\frac{a}{2}) = \sqrt{2} \notin Q_+$ . 矛盾.  
 $\therefore [Q_+; \cdot]$  与  $[Q; +]$  不同构.

(3) 设  $\Sigma_4 = \{[0], [1], [2], [3]\}$ ,  $K_4 = \{e, \alpha, \beta, \gamma\}$  若存在同构映射  $\varphi$  则  $\varphi([0]) = e$   
 对于  $\forall [x], [x]^{-1} \in \Sigma_4$ ,  $\varphi([x][x]^{-1}) = \varphi([x]) * \varphi([x]^{-1}) = e$   
 由  $K_4$  的性质知  $\varphi([x]) = \varphi([x]^{-1})$  由  $\varphi$  是双射知  $[x] = [x]^{-1}$   
 故不存在此映射

(4) ① 设  $G$  和  $G'$  同构,

由同态映射的性质知  $\varphi(e_G) = e_{G'}$ , 又  $\varphi$  为双射, 只有  $e_G$  的像为  $e_{G'}$

$$\therefore K = \{e\}$$

② 设  $K = \{e\}$ ,

$\because G$  与  $G'$  同态  $\therefore \varphi$  为满射,  $\varphi(G) = G'$   $\therefore G/K \cong G'$

~~又  $G/K \cong G$ , 故  $G \cong G'$~~  易证  $[G : \cdot] \cong [G/K : \cdot]$ : 构造  $\varphi: G \rightarrow G/K$ ,  $\forall g \in G$

易知  $\varphi$  为双射且满足同态等式

$$\therefore G \cong G/K \cong G'$$

13.41 证明:  $C^*, D, U, U_n$  图如 13.35 所示。

- (1)  $R/Z \cong U$ 。
- (2)  $C^*/D \cong U$ 。
- (3)  $C^*/U \cong D$ 。
- (4)  $U/U_n \cong U$ 。
- (5)  $C^*/U_n \cong C^*$ 。

ii) 对  $\forall x \in R$ . 设  $\varphi(x) = e^{i \cdot 2\pi x}$

$$\because U = \{a+ib \mid a, b \in R, \|a^2 + b^2\| = 1\} = \{x \mid x = \cos \theta + i \sin \theta, \theta \in R\} = \{x \mid x = e^{i\theta}, \theta \in R\}.$$

$\therefore$  显然  $\varphi(R) \subseteq U$ .

$\forall a, b \in R$ .  $\varphi(a+b) = e^{i \cdot 2\pi(a+b)} = e^{i \cdot 2\pi a} \cdot e^{i \cdot 2\pi b} = \varphi(a) \cdot \varphi(b)$

$\therefore \varphi$  是  $R \rightarrow U$  的同态映射。

对  $\exists U$ . 设  $e' = \cos \alpha + i \sin \alpha$  为  $U$  的单位元。

$\forall u = \cos \theta + i \sin \theta \in U$ .  $e' \cdot u = u \Rightarrow e' = 1$ .

$\forall u \in U$ .  $u \cdot e' = u \cdot 1 = u \quad \therefore e'$  是单位元。

$$K = \{x \in R \mid \varphi(x) = e'\} = \{x \in R \mid e^{i \cdot 2\pi x} = 1\} = \{x \in R \mid \cos(2\pi x) + i \sin(2\pi x) = 1\}.$$

$$= \{x \in R \mid \cos(2\pi x) = 1\} \Rightarrow K = \mathbb{Z}.$$

$\therefore R/\mathbb{Z} \cong \varphi(R)$ .

$\forall x \in R$ .  $\therefore 2\pi x \in R$ .  $\therefore$  显然  $\varphi(R) = U$ . 即  $\varphi$  是满同态映射。

$\therefore R/\mathbb{Z} \cong U$ .

12)  $\forall x = r\cos\theta + ir\sin\theta = r \cdot e^{i\theta} \in C^*$ ,  $r \in \mathbb{R}^+$ ,  $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ .  $\varphi(x) = \frac{x}{|x|} = \frac{x}{|r|} = \frac{r}{|r|} \cdot e^{i\theta}$ .

显然  $\varphi(C^*) = U$ . 又  $\forall a, b \in C^*$ ,  $\varphi(ab) = (r_1, r_2) \cdot e^{i(\theta_1+\theta_2)} = (r_1 \cdot e^{i\theta_1}) \cdot (r_2 \cdot e^{i\theta_2}) = \varphi(a)\varphi(b)$

即  $\varphi$  是  $C^*$  到  $U$  的满同态映射.  $\Rightarrow C^*/K \cong U$ .

$\because U$  的单位元为  $e' = 1$ .

$$\begin{aligned} K &= \{x \in C^* \mid \varphi(x) = e'\} = \left\{x \in C^* \mid \frac{rcos\theta + irsin\theta}{|r|} = 1\right\} = \left\{x \in C^* \mid rcos\theta = |r|\right\} \\ &= \left\{x \in C^* \mid r > 0, \theta = 0\right\} \Rightarrow K = D. \\ \therefore C^*/D &\cong U. \end{aligned}$$

(3). 构造  $C^* \rightarrow D$  的映射.  $\phi: x^* \rightarrow D: \forall re^{i\theta} \in C^*, \phi(re^{i\theta}) = ye^{i\theta} \in D$ ,

易知  $\phi$  为满射.  $\forall r_1 e^{i\theta_1}, r_2 e^{i\theta_2} \in C^*, r_1 > 0, r_2 > 0$ .

$$\phi(r_1 e^{i\theta_1} r_2 e^{i\theta_2}) = \phi(r_1 r_2 e^{i(\theta_1+\theta_2)}) = r_1 r_2 = \phi(r_1 e^{i\theta_1}) \phi(r_2 e^{i\theta_2})$$

$\phi$  满足同态等式. 故  $C^*$  与  $D$  同态.

$\forall u = e^{i\theta} \in U, \phi(u) = 1 = e_D, \forall u \in \text{ker}(\phi)$ .

又当  $\phi(re^{i\theta}) = 1 = e_D$  时,  $r = 1, re^{i\theta} \in U \Rightarrow \text{ker}(\phi) \subseteq U$ .

$\Rightarrow U = \text{ker}(\phi)$ . 故有  $C^*/U \cong D$ .

(4) 构造  $U \rightarrow U$  的映射  $\phi: U \rightarrow U$ ,  $\forall u = e^{i\theta}$ ,  $\phi(u) = (e^{i\theta})^n = e^{in\theta} \in U$ .

① 当  $n=0$  时,  $U_0 = \{x \in U \mid x^0 = 1\} \Rightarrow U_0 = U$ .

此时  $U/U = \{U\}$ . 此时  $U/U$  不与  $U$  同构.

② 当  $n \neq 0$  时,  $\phi$  为满射.  $\forall e^{i\theta_1}, e^{i\theta_2} \in U$ .

$$\phi(e^{i\theta_1} \cdot e^{i\theta_2}) = e^{i(n(\theta_1 + \theta_2))} = e^{in\theta_1} \cdot e^{in\theta_2} = \phi(e^{i\theta_1}) \phi(e^{i\theta_2})$$

$\therefore U$  与  $U$  同态.  $\forall u_R = e^{i\frac{2k\pi}{n}} \in U_n$ .  $\phi(u_R) = e^{i\frac{2k\pi}{n} \cdot n} = 1 = e_U$ .

$\Rightarrow U_n \subseteq \text{ker}(\phi)$ . 当  $\phi(u) = e^{in\theta} = 1$  时  $\theta = \frac{2k\pi}{n}$ .  $u \in U_n$ .

$\Rightarrow \text{ker}(\phi) \subseteq U_n$ .

故  $U_n = \text{ker}(\phi)$  则  $U/U_n \cong U$ .

(5)  $\forall x = r e^{i\theta} \in C^*$   $r > 0$ ,  $\theta \in R$ .

$$\therefore \varphi(x) = x^n = r^n e^{in\theta}$$

$$r > 0, \theta \in R \Rightarrow r^n > 0, n\theta \in R$$

$$\therefore \varphi(C^*) = C^*$$

$$\begin{aligned} \forall a, b \in U. \quad \varphi(ab) &= \varphi(r_1 e^{i\theta_1} \cdot r_2 e^{i\theta_2}) = \varphi((r_1 r_2) e^{i(\theta_1 + \theta_2)}) \\ &= (r_1 r_2)^n e^{in(\theta_1 + \theta_2)} = r_1^n e^{in\theta_1} \cdot r_2^n e^{in\theta_2} = \varphi(a) \varphi(b) \end{aligned}$$

$\therefore \varphi$  是  $C^* \rightarrow C^*$  的满同态映射.

对  $[C^*, \cdot]$ . 设  $e'$  为其单位元.  $\forall x \in C^*$ .  $d \cdot x = x \Rightarrow e' = 1$

$$x \cdot e' = x \cdot 1 = x \Rightarrow e' = 1 \text{ 为 } C^* \text{ 的单位元.}$$

$$\begin{aligned} K &= \left\{ x \in C^* \mid \varphi(x) = e' \right\} = \left\{ x \in C^* \mid x^n = 1 \right\} = U_n. \\ \therefore C^*/U_n &\cong C^*. \end{aligned}$$

13.42 证明  $[Z_2 \times Z_2; +]$  同构于  $K_4$ ，其中运算+定义为各分量模 2 加。

(用反证)

13.42. 证明：4 阶群只有两种结构。设  $G$  为 4 阶群，则  $\forall g \in G$ ,  $g$  的阶又能为 1, 2, 4.

① 当  $g$  的阶为 4 时,  $G$  为 4 阶循环群。

② 当  $g$  的阶不为 4 时, 单位元  $e$  的阶为 1, 其余元素阶为 2, 即  $K_4$  群。

记  $Z_2 \times Z_2$  的元素为  $[a, b]$ .  $\forall [a, b], [c, d] \in Z_2$ .

$$[a, b] + [c, d] = [(a+c) \bmod 2, (b+d) \bmod 2]$$

则除  $[0, 0]$  阶为 1, 其余元素  $[a, b]$  阶为 2. 即  $[a+b] + [a, b] = [0, 0] = e$ .

$\therefore Z_2 \times Z_2$  不为 4 阶循环群. 故  $Z_2 \times Z_2$  与  $K_4$  同构.

补充1.  $j$  为群  $[G; *] \otimes [G'; \cdot]$  的同态映射，则  $j$  为一对一当且仅当  $K = \{e_G\}$ ，这里  $K$  为同态核。

2. 设  $j$  是群  $G$  到  $G'$  的同态映射，证明：

(1) 若  $H$  是  $G$  的子群，则  $j(H)$  也是  $G'$  的子群。

(2) 若  $H$  是  $G$  的正规子群，且  $j$  是满同态映射，则  $j(H)$  也是  $G'$  的正规子群。

1. 证明：① 当  $j$  为一对一时，有  $K = \{e_G\}$ 。

$j$  为  $[G; *]$  到  $[G'; \cdot]$  的同态映射， $\forall g_1, g_2 \in G$ ， $g_1 \neq g_2$  有  $j(g_1) \neq j(g_2)$ 。

$$\forall g \in G, j(g)j(e_G) = j(g) = j(g)e_{G'}$$

$\Rightarrow j(e_G) = e_{G'}$ . 即  $e_G \in K$ .  $j$  为一对一映射，则  $e_{G'}$  只有一个原像，则  $K = \{e_G\}$ .

② 当  $K = \{e_G\}$  时， $j$  为一对一映射。

若  $\exists g_1, g_2 \in G$ ，且  $g_1 \neq g_2$ ， $j(g_1) = j(g_2) = e_{G'}$

$$\Rightarrow j(g_1)j(g_2)^{-1} = j(g_1g_2^{-1}) = e_{G'} \quad j(g_2)^{-1} = e_{G'}$$

$\Rightarrow g_1g_2^{-1} \in K$ . 又  $g_1 \neq g_2$ ，则  $g_1g_2^{-1} \neq e_G$ ，与  $K = \{e_G\}$  矛盾。

$\therefore j$  为一对一映射。

综上：当  $j$  为一对一映射当仅当  $K = \{e_G\}$

补充2：设  $[G, \cdot]$ ,  $[G', *]$

(1)  $\forall x \in H$ ,  $\varphi(x) \in G'$ , 故  $\varphi(H) \subseteq G'$

$\forall x, y \in H$ ,  $\varphi(x), \varphi(y) \in \varphi(H)$ ,  $\varphi(x) * \varphi(y) = \varphi(x \cdot y) \in \varphi(H)$

$\forall x, x^{-1} \in H$ ,  $\varphi(x) * \varphi(x^{-1}) = \varphi(x \cdot x^{-1}) = \varphi(e) = e'$  故  $\varphi(x)$  有逆元  $\varphi(x^{-1})$

因此  $\varphi(H)$  是  $G'$  的子群

(2) 由(1)知  $\varphi(H)$  是子群,

$\forall \varphi(g) \in G'$ , 由于  $\varphi$  是满同态的, 故  $\exists g \in G$  使  $\varphi(g) \in G'$  成立

$\forall \varphi(x) \in \varphi(H)$ ,  $x \in H$ ,  $\varphi(g) * \varphi(x) = \varphi(gx)$

而  $H$  正规, 故  $\exists x' \in H$  使  $gx = x'g$  且  $\varphi(g) * \varphi(x) = \varphi(x'g) = \varphi(x') * \varphi(g)$

故  $\varphi(H)$  是正规子群