

# Discrete Mathematics.

---

高迅老师的离散课笔记

2018.1.4 - 2018.1.7

---

---

---

---

---

---

---



# 代数系统

## 1. 代数运算的定义

$S \times S$  到  $S$  为一个映射，为  $S$  上的一个二元代数运算（简运算）

例：

$\triangleright S = \{a, b\}$ , 则  $S \times S = \{(a, a), (a, b), (b, a), (b, b)\}$

映射  $f$  为：  
 $(a, a) \rightarrow a$   
 $(a, b) \rightarrow a$   
 $(b, a) \rightarrow b$   
 $(b, b) \rightarrow b$

$f$  称为  $S$  的一个二元代数运算，有

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

也可表示为：

$a * a = a, a * b = a, b * a = b, b * b = b$

18

## 2. 代数运算的性质

① 交换律  $a, b \in S, a * b = b * a$  成立，称  $*$  是交换律。

② 结合律  $a, b, c \in S, (a * b) * c = a * (b * c)$  成立，称  $*$  是结合律。

③ 零等律  $0 \in S, a * 0 = a, 0$  为零等元，若  $S$  中每个元素都是关于零等元，称  $*$  满足零等律

例： $a^n$  不是  $a$  的  $n$  次幂，是对于  $a$  的  $n$  次幂

例： $S$  非空， $p(S)$  为  $S$  的幂集，则  $\cup, \cap$  满足零等律

④ 分配律  $a, b, c \in S, a * (b + c) = (a * b) + (a * c)$

⑤  $(b + c) * a = (b * a) + (c * a)$ , 称  $*$  对  $+$  的分配律

注：要求④⑤都成立，因  $*$  必须满足交换律

例：设  $A = \{\alpha, \beta\}$ , 二元运算\*, + 定义如下：问分配律成立否？

*	$\alpha$	$\beta$
$\alpha$	$\alpha$	$\beta$
$\beta$	$\beta$	$\alpha$

+	$\alpha$	$\beta$
$\alpha$	$\alpha$	$\alpha$
$\beta$	$\beta$	$\alpha$

解答：① 该运算+对\* 满足分配律，因为

$$x + (y * z) = (x + y) * (x + z);$$

$$(y * z) + x = (y + x) * (z + x); \quad \alpha \quad \alpha$$

$$\text{证明: } \begin{cases} \text{若 } x = \alpha \text{ 时, } x + (y * z) = \alpha. & \underline{(x+y)*(\underline{x+z})} = \alpha. \\ \text{若 } x = \beta \text{ 时, } x + (y * z) = y * z & \underline{(x+y)*(\underline{x+z})} = y * z. \end{cases}$$

同理验证右分配律成立。

② 该运算\* 对该运算+ 不可分配。

$$\begin{cases} \text{若 } x = \alpha \text{ 时, } x * (y + z) = y + z. \end{cases}$$

$$(x * y) + (x * z) = y + z.$$

$$\begin{cases} x = \beta \\ y = \alpha \\ z = \beta \end{cases} \quad \underline{x * (\underline{y+z})} = \beta$$

$$\begin{cases} x = \beta \\ y = \alpha \\ z = \beta \end{cases} \quad \frac{(x * y) + (x * z)}{\beta} = \beta + \alpha = \alpha.$$

故不成立。

⑤ 吸收律  
 $a, b \in S$      $a^*(a+b) = a$ ,     $a + (a^*b) = a$ .  
 又  $\textcircled{*}$  和  $\textcircled{+}$  满足吸收律

➤ 例：定义自然数集合  $N$  上的运算 \* 和 + 如下：

对于任意  $a, b \in N$ , 有  $a^*b = \max\{a, b\}$ ,  
 $a+b = \min\{a, b\}$ , 则 \* 和 + 是  $N$  上的二元代数运算, 且满足吸收律。

$$a^*(a+b) = \max\{a, \min\{a, b\}\} = a$$

$$a + (a^*b) = \min\{a, \max\{a, b\}\} = a$$

26

⑥ 消去律.     $a, b, c \in S$ .

$$\textcircled{1} \quad a^*b = a^*c \quad \text{且} \quad b = c$$

$$\textcircled{2} \quad b^*a = c^*a. \quad \text{且} \quad b = c$$

称 \* 满足消去律.

$a$  的左消. 可以消

### 3. 代数系统的意义

$S$  非空集合 + 基于  $S$  上的代数运算 = 代数系统  
 记为  $(S, f_1, \dots, f_n)$ .

例：

➤ 设  $S$  是一个非空集合,  $\rho(S)$  是  $S$  的幂集, 则  $(\rho(S), \cap, \cup)$  为代数系统。

➤ 设  $\wedge, \vee$  是真值集合  $\{0, 1\}$  上的合取与析取运算, 则  $(\{0, 1\}, \wedge, \vee)$  是代数系统。

# 群的定义

1. 半群的定义： $G$  非空、 $\cdot$  为  $G$  上的二元运算且满足 结合律，称  $(G, \cdot)$  为半群  
(Z+)

2. 群的定义：半群满足如下条件：

① 单位元元素： $e \in G$  使得  $a \cdot e = e \cdot a = a$

② 逆元素： $\forall a \in G$  存在  $a^{-1} \in G$  使得  $a \cdot a^{-1} = a^{-1} \cdot a = e$  (Z+)

注：这个数叫做左逆元，称为左逆群；反之为右逆群

$$S = \{0, 1, 2, \dots, m-1\}$$

$$a \oplus b = \begin{cases} a+b & \text{if } a+b < m \\ a+b-m & \text{if } a+b \geq m \end{cases}$$

$\Rightarrow (S, \oplus)$  称为 模  $m$  加法群

证：单位元  $0 \oplus a = a \oplus 0 = a$

逆： $a \oplus (m-a) = (m-a) \oplus a = 0$

问题：

设  $S = \{a, b\}$ ，使用乘法表定义  $S$  上的运算。如下：

.	a	b
a	a	b
b	b	a

问  $(S, \cdot)$  是否为群？

① 单位元：

$$a \cdot e = e \cdot a = a \quad e = a$$

$$b \cdot e = e \cdot b = b \quad e = a$$

$a \oplus$  单位元

② 逆

$$a \cdot a^{-1} = a^{-1} \cdot a = a \quad a^{-1} = a$$

$$b \cdot b^{-1} = b^{-1} \cdot b = b \quad b^{-1} = b$$

都在左边。

- 设 $\mathbb{R}$ 是实数， $\cdot$ 是数的普通乘法，定义 $\mathbb{R}$ 上的一个运算 $*$ ，对 $\mathbb{R}$ 中任意元素 $a, b$ ，有 $a*b=|a|\cdot b$ ，问 $(\mathbb{R}, *)$ 上是否有单位元？
- 答：没有。

设单位元为 $e$ .  $a \cdot e = a$   
 $\Rightarrow a \cdot e = |a| \cdot e \neq a$ .

### 3. 理解群的意义

① 单位元是群中唯一的零等元

即 $\exists e \in (\mathbb{G}, \cdot)$ 是群 单位元为 $e$ .  $\forall x \in \mathbb{G} \quad e \cdot x = x \quad e^n = e$

$\therefore e$ 是零等元

设 $x \in (\mathbb{G}, \cdot)$ 的零等元.  $\exists x^{-1} \in \mathbb{G} \quad x \cdot x^{-1} = e$

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

② 群中不可同时有零元 ( $a \cdot 0 = 0 \cdot a = 0 \neq 1$ )

$$x \cdot 0 = 0 \cdot x = 0 \neq 1.$$

$\therefore 0$ 无逆元。

③ 满足结合律

$$a \cdot b = a \cdot c$$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad i \cdot b = i \cdot c \quad \nabla \quad b = c.$$

問

(G.)  $(a \cdot b)^{-1}$  是否等于  $a^{-1} \cdot b^{-1}$ ?

$$\text{解: } (a \cdot b)^{-1} \cdot (a \cdot b) = e = a^{-1} \cdot a \cdot b^{-1} \cdot b$$

$$\text{若 } (a \cdot b)^{-1} = a^{-1} \cdot b^{-1} \quad (2) \quad a \cdot b^{-1} \cdot b = a^{-1} \cdot b^{-1} \cdot b$$

又, 集合中元素不重複成立.  $\therefore (a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$

4. 集合的性质

(1). 單位元素唯一. 沒有元素而空集不是

結論 ①  $(a^{-1})^{-1} = a$ . ②  $(a \cdot b)^{-1} = b^{-1} \cdot a$ , ③  $1^{-1} = 1$

\* 元素為 1 的群也只有一個

*	e
e	e

$$a + e = a$$

\* 元素為 2 的群也只有一個

*	e	a
e	e	a
a	a	e

$$a \times a = e$$

(2). 性質 ① ② ③ 成立. 即

① 有左逆

② 有右逆

A 是 B 的充要條件

$A \rightarrow B$ . 充分性

$B \rightarrow A$ . 必要性

(3). 集合之於而 ① ② ③ 成立的除法群  $\Leftrightarrow$  滿足  $a \cdot b \neq 0 \Rightarrow a \cdot b^{-1} \in G$

定理. ① 先证必要性(群中可除条件成立.)

$$\forall a, \exists x, y \in G, x \cdot a = e, y \cdot a = b$$

$$\text{同理可得 } y = a \cdot b^{-1} \Rightarrow ya = b$$

② 再证必要性.(可除条件的推出 (1)(2))

$$\forall c \in G, \exists x, y \in G, x \cdot c = c \text{ 且 } y \cdot c = c$$

$$\text{对任意 } a, \exists x, y \in G, x \cdot a = a$$

$$\text{及 } e \cdot a = e, c \cdot c \cdot y = c \cdot y = a$$

及 (1) 成立.

又:  $a^{-1}$  为适合  $x \cdot a = e$  的  $x$ .

$$x_1 | a^{-1} \cdot a = e$$

及 (2) 成立

(4). 设  $G$  是一个群.  $\forall a_1, \dots, a_n \in G$  有  $a_1 \cdots a_n = a_n \cdots a_1$  成立

$$(5). \begin{cases} \text{若 } a^m, a^n \in G, & a^m \cdot a^n = a^{m+n}. \\ \text{若 } (a^m)^n \in G, & (a^m)^n = a^{mn} \end{cases} \text{成立}$$

$$\text{若 } (a \cdot b)^m \in G, (a \cdot b)^m = a^m \cdot b^m \text{ 成立}$$

$$\boxed{-\text{假设 } (a \cdot b)^m = a^m \cdot b^n \text{ 不成立}} \quad \text{Abel 脱落法}$$

5. Abel 群 (交换群). 没足交换之群而群

(1). 设  $(G, \cdot)$  是一个群.  $(G, \cdot)$  成 Abel 群的充要条件是  $\forall a, b \in G$

$$(a \cdot b)^2 = a^2 \cdot b^2$$

$$\text{证. } \text{先证 必要性} \quad (a \cdot b)^2 = a \cdot b \cdot a \cdot b = a \cdot (b \cdot a) \cdot b \\ = a \cdot (a \cdot b) \cdot b = a^2 b^2$$

② 再论充分性

$$(a \cdot b)^2 = a^2 \cdot b^2 \text{ 充分}$$

$$a^{-1} \cdot (a \cdot b) \cdot (a \cdot b) \cdot b^{-1} \Rightarrow b \cdot a = a \cdot b$$

故  $(G, \cdot)$  成 Abel 群

6. Abel 群的性质

(1). 在一个 Abel 群中任意两个元素的乘积因数分解唯一

$$(2). \text{第} = \text{所有} \text{素数成之} \quad (a \cdot b)^n = a^n \cdot b^n$$

# 置换群

## 1. 置换的定义

» 定义6.2.4 设 $M$ 是一个非空的有限集合， $M$ 的一个一对一变换称为一个置换。

设 $M=\{a_1, a_2, \dots, a_n\}$ ，则 $M$ 的置换 $\sigma$ 可简记为

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}, \quad b_i = \sigma(a_i), \quad i=1, 2, \dots, n$$

» 结论： $M$ 的置换共有 $n!$ 个。

»  $M$ 上的置换也称为n元置换。特别地，

若 $\sigma(a_i) = a_i, \quad i=1, 2, \dots, n$ ，则 $\sigma$ 为n元恒等置换。

S<sub>n</sub> : n! 个置換作成的集合。

$a_1, a_2, \dots, a_n$  in 一个  
n元置换到  $A^m$   $A^m = m!$

## 2. 置换的乘法

注意两个 G, T 满足  $G(Ta) = G(T(a))$

$$G = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$GT = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

## 3. 置换乘法的性质

① 满足结合律  $(GT)p = G(Tp) \quad G, T, p \in S_n$

②  $S_n$  中有单位元 (n元恒等置换)

③ 每个 n 元置换有逆元素  $\left(\begin{matrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{matrix}\right)^{-1} = \left(\begin{matrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{matrix}\right)$

## ①. $n$ 次对称群

$n$  元置换的全体  $S_n$ . 为置换乘法. 作成一个群

>  $n=1$ ,  $M=\{a\}$ ,  $S_1=\{\begin{pmatrix} a \\ a \end{pmatrix}\}$  在置换的乘法下作成1次对称群, 为**Abel**群。

>  $n=2$ ,  $M=\{a, b\}$ ,  $S_2=\{\begin{pmatrix} a & b \\ a & b \end{pmatrix}, \begin{pmatrix} a & b \\ b & a \end{pmatrix}\}$  在置换的乘法下作成2次对称群, 为**Abel**群。

> 当  $n \geq 3$  时,

$$\begin{pmatrix} 1 & 2 & 3 \cdots n \\ 2 & 1 & 3 \cdots n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \cdots n \\ 3 & 2 & 1 \cdots n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \cdots n \\ 3 & 1 & 2 \cdots n \end{pmatrix}$$

$S_n$  不是**Abel**群。

$$\begin{pmatrix} 1 & 2 & 3 \cdots n \\ 3 & 2 & 1 \cdots n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \cdots n \\ 2 & 1 & 3 \cdots n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \cdots n \\ 2 & 3 & 1 \cdots n \end{pmatrix}$$

## 5. 置换的轮换表示法.

$G$  为  $M$  的置换. 将  $\bar{m}$  变到  $m$  的元素  $a_1, \dots, a_r$

$(\begin{matrix} a_1 & a_2 & \cdots & a_r \\ a_2 & a_3 & \cdots & a_1 \end{matrix})$ . 而  $G$  不变  $M$  中其余元素. 则  $G$  为

一个 轮换

例:  $G = (\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{matrix}) = (\begin{matrix} 1 & 3 & 4 \end{matrix})(\begin{matrix} 3 & 4 & 1 \end{matrix}) = (\begin{matrix} 4 & 1 & 3 \end{matrix})$

轮换.

① 设  $(a_1 \cdots a_r)$  为  $M$  的轮换. 则  $(a_1 \cdots a_r)^{-1} = (a_r \cdots a_1)$

$$(\begin{matrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{matrix})^{-1} = (\begin{matrix} 4 & 3 & 1 \\ 3 & 1 & 4 \end{matrix})$$

## 6. 不相容轮换.

1. 定义: 两个轮换中而元素都不相同

$$\text{例 } M = \{1 2 3 4 5 6 7\}, (134) \text{ 与 } (637) \text{ 相容, } (134) \text{ 与 } (25) \text{ 不相容.}$$

习题. 计算  $(12345)(23456)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 6 & 3 \end{pmatrix} \\ = (124)(356)$$

练习.

①  $G, T$  为两个不相容轮换 则  $GT = TG$

② 任意一个轮换可以写成不相容轮换的乘积

$$\text{例 } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 4 & 2 & 8 & 7 & 6 \end{pmatrix} = (1352)(68)(7)$$

去掉单轮换  $(1352)(68)$

习题  $(134)(51)(314)(412)$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$

$$\begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 \\ 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 4 & 1 & 2 \\ 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 3 \end{pmatrix} \\ = \cancel{(124)} \cancel{(35)}$$

## 7. 对称：长度为2的轮换

结论：该轮换可以写成对换的乘积

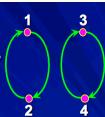
推论：任意置换，有一法而将每一个对换的乘积

$$(6) \quad (132) = (12)(13)$$

$$(a_1 \dots a_r) = (a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_3)(a_1 a_2)$$

## 8. 通过顺时针圆圈表示

- 先把置换表成不相杂轮换之乘积，然后用一组顺向圈来表示。
- 每个顺向圈的长度，即圈上所含的元素个数，就是该圈所表示的轮换的长度。
- 一个n元置换对应一组顺向圈，这组圈的长度之总和为n；反之，一组顺向圈表示一置换，置换的元素个数就是组中各图长度之总和。



23

► n元置换σ对应图形表达式(图型)

$$G_\sigma = \sum_{i=1}^k a_i z_i = a_1 z_1 + a_2 z_2 + \dots + a_n z_n$$

$z_i$ 表示长度为i的圈， $a_i$ 表示如此的 $z_i$ 的个数；  
诸 $a_i$ 为非负整数， $0 \leq a_i \leq n$ ，  
 $a_i = 0$ 或1；

$$\therefore a_1 + 2a_2 + \dots + na_n = n$$

► 例： $M = \{1, 2, 3, 4, 5, 6, 7, 8\}$ ,

$$\sigma = (1 \ 6)(3 \ 4 \ 5)(2 \ 8),$$

$$\therefore G_\sigma = z_1 + 2z_2 + z_3, \quad 1 \times 1 + 2 \times 2 + 3 \times 1 = 8$$

24

## 9. 置换的奇偶性

- 设σ表为k个不相杂的轮换的乘积(包括长度为1的轮换在内)，长度分别为 $r_1, r_2, \dots$ ，

$\sum_{j=1}^k (r_j - 1)$ 若 $= n - k$ 为奇数(偶数)，则称σ为

奇置换(偶置换)。

► 例如： $\sigma = (1 \ 2 \ 3 \ 4 \ 5 \ 6)(3 \ 2 \ 4 \ 1 \ 5 \ 6) = (134)(2)(5)(6)$ 是偶置换

$T = (1 \ 2 \ 3 \ 4 \ 5 \ 6)(3 \ 2 \ 5 \ 6 \ 1 \ 4) = (135)(46)(2)$ 是奇置换

25

► 结论：奇置换可表为奇数个对换之积，偶置换可表为偶数个对换之积。

$$(T^n) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 2 & 9 & 7 & 8 & 4 & 5 \end{pmatrix} = (1\ 3\ 6\ 7\ 8\ 4\ 2)(5\ 9)$$

$\therefore n-1=9-2=7$ . おおきい置換で 15 通りの対称形がある。

$$= (1\ 8)(1\ 4)(1\ 8)(1\ 7)(1\ 6)(1\ 3)(5\ 9) \quad (7 \text{ 个})$$

G.T と G.T' は GT との関係性の関係。

$$\text{証明 } ① \frac{E}{G} \times \frac{G}{G'} = 1^{\frac{P}{P}} \quad 1^{\frac{P}{P}} \times (G' \times \frac{G}{G}) = 1^{\frac{P}{P}}$$

$$\frac{E}{G} \times (G' \times \frac{G}{G}) = \frac{E}{G'} \quad (G' \times \frac{G}{G}) \times \frac{E}{G} = \frac{E}{G'}$$

証明 ② 一般に  $n$ ,  $n \geq 1$ , 2 つの置換の個数と置換の個数が相等。

(a) 置換の逆像数

定義: 置換の逆像数  $n-1$

# 子群及其性质

## 1. 子群的定义

› 定义6.3.1 设 $(G, \cdot)$ 是一个群,  $H \subseteq G$ , 如果 $(H, \cdot)$ 仍是一个群, 则 $(H, \cdot)$ 叫做 $(G, \cdot)$ 的子群。如果 $G$ 的一个子群 $H$ 不等于 $G$ , 即  $H \subset G$ , 则 $(H, \cdot)$ 叫做 $(G, \cdot)$ 的真子群。

› 注:  $G$ 的子群 $H$ 的运算必须与 $G$ 的运算一样。比如,  $(C^*, \cdot)$ 不是 $(C, +)$ 的子群。

## 2. 单元子群

除单位元素组成的子群, 除自身组成的子群

## 3. 子群的判别条件

(1) ①  $a \in H, b \in H, \text{则 } ab \in H$

②  $a \in H \text{ 且 } a^{-1} \in H$

③  $H$ 非空

(2) ① ② 互换为  $ab^{-1} \in H$ .

(3) 若 $H$ 是有限非空子集, 则证明封闭性即由  $a \in H, b \in H \Rightarrow ab \in H$

### 3. 循环群

1.  $a$  为  $G$  的元素,  $\{a^n\}$  有界即生成  $G$  一个子群, 由  $a$  生成的循环群

证明: 由刻别条件(二)

① ( $a$ ) 有元, 令  $a^0 = 1 \in G$

②  $a^m, a^n \in G$  则  $(a^m) \cdot (a^n) = a^{m+n} \in G$

2. 定义: 若  $G$  可由它的一个元素生成, 即存在  $G$  使  $G = \langle a \rangle$

则  $G$  为循环群.

例如整数加法群  $(\mathbb{Z}, +)$ , 由 1 生成

### 3. 元素的周期

看由元素  $a$  所生成的循环群  $\langle a \rangle$ :

$\dots, a^{-2}, a^{-1}, a^0, a, a^2, \dots$  (1)

情形 1<sup>0</sup> 如果(1)中所有元素都彼此不同, 则称  $a$  的周期为无穷大或 0。此时, 对任意两个不同的整数  $s$  与  $t$ ,  $a^s \neq a^t$ 。

情形 2<sup>0</sup> 如果(1)中出现重复的元素, 即有整数  $s \neq t$ , 使  $a^s = a^t$ 。不妨设  $s > t$ , 于是  $s - t > 0$  且  $a^{s-t} = 1$ , 即有正整数  $m$  使  $a^m = 1$ 。

若  $n$  为适合  $a^n = 1$  的最小正整数, 则称  $a$  的周期为  $n$ 。

21

结论一: 群中任一元素的周期为 |

结论二: 群中任一元素和它的逆具有同样的周期

## 四、群的性质

- 定理6.3.5 若群G中元素a的周期为n，则
- 1)  $a, a^2, a^3, \dots, a^{n-1}$  为n个不同元素；
  - 2)  $a^m=1$  当且仅当  $n | m$ ；
  - 3)  $a^s=a^t$  当且仅当  $n | (s-t)$ 。

## 练习

- 设a为群G的一个元素，
- 1) 如果a的周期为无穷大，则(a)是无限循环群，(a)由彼此不同的元素 $\dots, a^2, a^{-1}, 1, a, a^2, \dots$ 组成。
  - 2) 如果a的周期为n，则(a)为n元循环群，它由n个不同的元素 $1, a, a^2, a^3, \dots, a^{n-1}$ 组成。

28

4. 群的子群而生成元素。

$$\varphi(20) = 20 \times \frac{1}{2} \times \frac{1}{5}$$

$$\begin{aligned}\varphi(20) &= \frac{20}{2} \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\ &= 8\end{aligned}$$

$$\begin{array}{r} 13 \ 17 \ 11 \ 13 \ 9 \\ \hline 17 \ 19 \end{array}$$

### ► 定理6.3.6

- 1) 无限循环群(a)一共有两个生成元： $a$ 及 $a^{-1}$ 。
- 2) n元循环群(a)中， $a^k$ 是(a)的生成元的充要条件是  $(n, k)=1$ 。所以(a)一共有  $\varphi(n)$  个生成元素。

問 9 の 復習

$$1 \quad \underbrace{a^0 \ a^1 \ a^2 \ a^3 \ a^4 \ a^5 \ a^6 \ a^7 \ a^8}_{\text{1つめの } n=9} \quad n=9$$

$$\begin{aligned} \text{1つめの } n &= 1 \quad (c = 1, 2, 5, 7) \\ &\underline{\quad a^8 \ a^4 \ a^1 \ a^2 \ a^5 \ a^7 \ a^8 \quad} \text{ 2つめの } n \\ &\quad \end{aligned}$$

$$\varphi(a) = \varphi(q) = 3^2 = q \times \left(1 - \frac{1}{3}\right)$$

$$(a^4)^0 = a^0 = 1$$

$$(a^4)' = a^4$$

$$(a^4)^2 = a^8$$

$$(a^4)^3 = a^{12-9} = a^3$$

$$(a^4)^4 = a^7$$

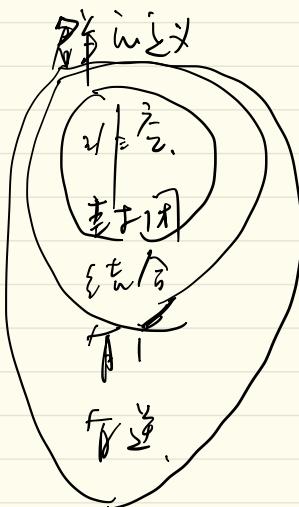
$$(a^4)^5 = a^2$$

$$(a^4)^6 = a^6$$

$$(a^4)^7 = a$$

$$(a^4)^8 = a^5$$

$$(a^4)^9 = 1$$



27.

$$a^0 \ a^1 \ \dots \ a^n \quad n=10.$$

Enter  $\rightarrow f_2$

$$\varphi(n).$$

①  $\Rightarrow$  算出  $n$  个数

$n$  位同或不同

$$3 \ n \times (1 - \frac{1}{p_1}) (1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_n}).$$

5.  $\begin{cases} 3 \\ \overline{m} \end{cases}$

$$\begin{cases} 3 \\ \overline{m} \end{cases} \quad a/m = n \dots 0. \quad a \equiv b \pmod{m}.$$

除以  $m$  余  $a$ , 不等于  $b$  但  $a \equiv b \pmod{m}$

因为  $m$  有  $m$  个类, 每个类有  $m$  个数  $\pmod{m}$  在  $m$  个类

$$(123)^0 = 1$$

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

$$(123)^1 = (123)$$

$$(123)(123)^2 = \left( \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array} \right) = (132)$$

$$(123)^3 = (123)(132) = \underbrace{(1)(3)(2)}_{\cancel{1}\cancel{2}\cancel{3}} = 1$$

$$\begin{array}{c} \uparrow a \quad \uparrow b \quad \nearrow c \\ (12) = (12)I \end{array}$$

$$(23) = (12)(123)^H$$

$$(12)(132) = (13)\cancel{(23)}$$

$$\uparrow \quad \quad \quad (123)I = \underline{(123)}$$

$$\underline{(123)} \underline{(123)} = (132)$$

同理  
G 与 H 互为同构

例：设  $G$  是三次对称群： $G=\{I, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)\}$ ， $H$  是由  $(1 2 3)$  生成的子群  $H=\{I, (1 2 3), (1 3 2)\}$ 。

因为有  $I \in H$ ，使得  $(1 2) = (1 2)I$ ，所以  $(1 2) \equiv (1 2) \pmod{H}$ 。

因为有  $(1 2 3) \in H$ ，使得  $(2 3) = (1 2)(1 2 3)$ ，所以  $(2 3) \equiv (1 2)(\text{右} \pmod{H})$ 。

可验证： $(1 2) \equiv (2 3) \pmod{H}$ ，

$$(1 2) \equiv (1 3) \pmod{H}$$

$$(1 3) \equiv (1 2) \pmod{H}$$

$$(1 3) \equiv (2 3) \pmod{H}$$

$$(2 3) \equiv (1 3) \pmod{H}$$

$H$  中元素互相合同。

$$(1 2)I = (1 2)$$

$$(1 2)(1 2 3) = \cancel{(1 2)}(2 3)$$

$$(1 2)(1 3 2) = (1 3)\cancel{(2 3)}$$

$$\left\{ (1 2)(1 2 3)(1 3 2) \right\}$$

$$\left\{ I, (1 2 3), (1 3 2) \right\}$$

$$\left\{ (1 2) \right\}$$

$$\left\{ (1 2) \right\}$$

$$\left\{ (1 2) \right\}$$

$$\frac{|G|}{|H|} = 2$$

$(\exists +)$

$$0 + \alpha = \alpha$$

G.

-2 -1 0 1 2 ...

1, -1.

$\rightarrow 0 2 4 \dots H.$

$I + H = \underline{\text{奇数}}$

高  
度

$H = \underline{\text{偶数}}$

力矩. 滚动摩擦. 右右滚动  
轨迹

例：

设  $G$  是 3 次对称群：

~~$\{(1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$~~

$H : \{(1, 2)\}$ ,

$H$  有三个右陪集：

$\{(1, 2)\}, \{(1, 3), (1, 2, 3)\}, \{(2, 3), (1, 3, 2)\}$

$H$  有三个左陪集：

$\{(1, 2)\}, \{(2, 3), (1, 2, 3)\}, \{(1, 3), (1, 3, 2)\}$

右陪集

$(1, 3) \underline{1} = \underline{(1, 3)}$

$(1, 3)(1, 2) = \underline{(1, 2, 3)}$

$(2, 3) \underline{1} = (2, 3)$

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

故  $H$  的右陪集有：  $\boxed{H}, \boxed{\{(1, 2)\}}, \boxed{\{(1, 3), (1, 2, 3)\}}, \boxed{\{(2, 3), (1, 3, 2)\}}$

$$\frac{|G|}{|H|} = 3$$

右陪集

同理

① いざなう  $aH = H \rightarrow a \in H$

$\because 1 \in H \therefore a \cdot 1 \rightarrow a \quad a \in aH$

② いざなう  $a \in H \rightarrow aH = H$  左右積分の定義 群の集合的性質

(1).  $aH \subseteq H$  はるかに

いざなう  $b \in aH \quad b = ah \quad (h \in H)$

$\leftarrow aH \subseteq G$  はるかに  $a \in H \quad h \in H \rightarrow b \in H$

$\therefore aH \subseteq H$  はるかに

(2)  $H \subseteq aH$  はるかに

説明

いざなう  $x \in H \quad$  いざなう.

$$\begin{aligned} x &= (a \cdot a^{-1})x \\ &= \underline{a}^{\text{左}} (\underline{a^{-1}} x) \end{aligned}$$

$\therefore x \in aH$

(3).  $aH = bH$  はるかに  $a^{-1}b \in H$

説明. いざなう

$$b \in bH \quad aH = bH \Rightarrow b \in aH$$

いざなう

$$b \in aH \Rightarrow aH = bH \quad a^{-1}b \in H$$

$$b \in bH$$

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

正规群.

$a \in G$ .  $H^g = G$  這是群.  $aH = Ha$ ,  $\forall h \in H$  這  
是群.

定義 1: 半直積 - 這是正規子群

定義 2: Abel 群的直積是正規子群.

$$\begin{array}{l} g \in G \\ a \in G \end{array} \quad \begin{array}{l} \text{正規子群} \\ \therefore ag \in G \\ \underline{ga \in G} \end{array}$$

∴ 正規子群不是滿足交換律.

滿足交換律的子群 - 這是正規子群

定理 3. 若  $H$  是  $G$  的正规子群.  $\forall g \in G$  則  $gHg^{-1} \subseteq H$

證明. ① 必要性  $H$  是  $G$  的正规子群  $\rightarrow$  待證

$$\therefore g \in G \text{ 當且 } gH = Hg \Rightarrow gHg^{-1} = Hg g^{-1}$$

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

② 充分性:  $g \in G, gHg^{-1} \subseteq H \rightarrow H$  是正规子群

$$\text{取 } g \in G. \rightarrow gH = Hg.$$

$$gHg^{-1}g \subseteq Hg \quad gH \subseteq Hg.$$

$$g^{-1}CG : \underline{g^{-1}Hg} \subseteq H \quad Hg \subseteq gH$$

$$Hg \subseteq gH$$

定理 4.  $H$  是  $G$  的正规子群.  $a \in G$ . 則

$$\underline{\underline{a^{-1}Ha}} = H$$

Lagrange 逆元定理 < 研究之陪集的个数  
 $G$  为群.  $H$  为  $G$  的子群.  $a \in G$  且  $a$  在  $H$  中的陪集中. 则存在  $b \in H$  使得  $a^{-1}b \in H$ .

$H$  在  $G$  中的阶数. ( $G:H$ )  $|G|_H =$  左右陪集的个数

设  $G$  为有限群. 之阶为  $n$ . 对任意  $a \in G$ . 则  $a^n = 1$

$$\text{若 } a. \text{ 则 } a^m \rightarrow (a). \quad \frac{m}{\cancel{m}} \mid n.$$

$$\therefore n \equiv 0 \pmod{m}. \quad \boxed{a^n = 1}$$

問：若  $b$  在  $\mathbb{Z}_m$  一定有同餘方程之解。

設  $b$  在  $\mathbb{Z}_m$  为  $G$ .  $\text{且 } |G| = b$

$\exists H$  为  $G$  的子群  $\Rightarrow$   $|H| \equiv 0 \pmod{|G|}$

$$G = \langle a^0, \dots, a^5, x \rangle$$

若  $a^0, a, a^4$

若  $a^1, a^5$  ( $\exists 2+3 \not\in H$ )

若  $a^0 \rightarrow [a^0]$

$a^2 \rightarrow (a^2, a^4, a^0)$

$a^3 \rightarrow (a^3, a^0)$

$a^4 \rightarrow (a^4, a^2, a^0)$

$b = 1 \times 5$

$b \sim 2+3$

$b \times (\frac{1}{2}) \times (\frac{2}{3}) = 2$

$q_{cm} = 1 \times 2 = b$

*	a
a	a

→ 雖然

x	e	b
e	e	b
b	b	e

→ 逆元

x	e	a	b
e	e	a	b
a	a	e b	b e
b	b	b e	x a

$$a^{-1} = a'$$

$$a \cdot a = e.$$

四元體群

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

$$\underline{b \cdot a = b \cdot a = c}$$

$$a \cdot a = e$$

$$a^3 = a$$

6元群

$a^n$

① 一个群不简单

该群的阶数  $\varphi(6) = 2$

$$(6 \cdot 1) = 1 \quad (6 \cdot 5) = 1.$$

$a^0 \ a^1 \cdots a^5$

6个元素  $\{1, 2, 3, 6\}$  元素的阶数是  $1, 2, 3, 6$

$a^1$  和  $a^5$  互为逆元. 6

1 是  $a^0 \rightarrow (a^0)$  1

$a^2 \rightarrow (a^2, a^4, a^0)$ . 3

$a^3 \rightarrow (a^3, a^0)$ . 2

$a^4 \rightarrow (a^4, a^2, a^0)$ . 3

- 互为逆元为3元素

$ab = ba$ .

3 非简单群

$a^- = a$ . 121  
Abel 群.

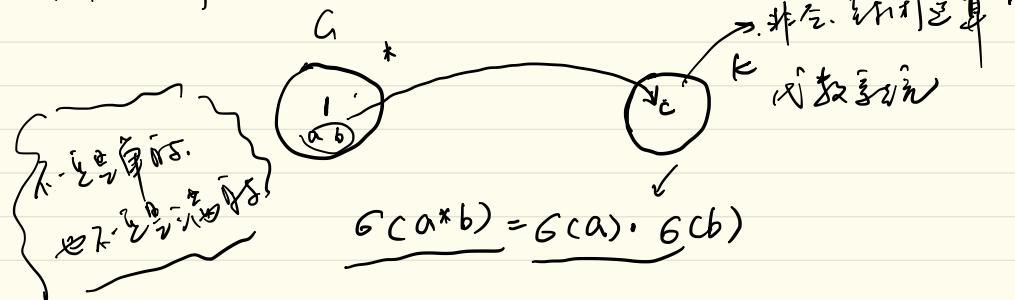
不是简单群

(1) 若所有之素数阶数为 2, 3  $a^2 = 1$ .  $G_1 \cong A$  为简单.

在  $G_1 \cong A$ .  $a, b \in G_1$   $\{1, a, b, ab\} = H$   $H \cong G_1$  为简单

由  $a, b \in G_1$   $a \neq 1$ ,  $b \neq 1$

[T] 感想



① 由定理

⇒ 形式成立

(b) 2

$$\text{证毕. } G(a+b) = G(a) \oplus G(b) \rightarrow b \pmod{n}$$

$$a+b \pmod{n} = a \pmod{n} \oplus b \pmod{n}$$

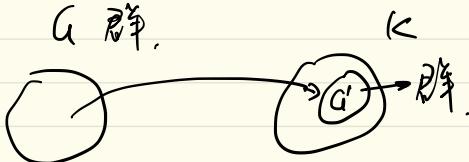
[T] 3

$$G(x_1 + x_2) = -(x_1 + x_2) = -x_1 + (-x_2)$$

$$G(x_1) = -x_1 = -x_1 + (-x_2)$$

$$+ G(x_2) = -x_2$$

[T] 4



单元素相同

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

数学研究

$i \rightarrow \gamma$

$m, n \in \mathbb{Z}$ .

$$G(m+n) = i^{m+n}$$

$$\begin{aligned} G(m) &= i^m & \rightarrow G(m+n) &= G(m) \cdot G(n), \\ G(n) &= i^n & \text{由上式得} \end{aligned}$$

$$\left. \begin{array}{l} i^0 = 1 \\ i^1 = i \\ i^2 = -1 \\ i^3 = -i \end{array} \right\} \quad \underbrace{(1, i, -1, -i)}_{G'} \subseteq (C^*, \cdot)$$

①  $i^2 = -1$

$$i^4 = 1 \quad (p(4) = 1 \cdot 3)$$

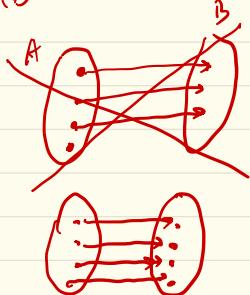
$$\underline{\textcircled{2}} \quad G(a^{-1}) = (G(a))^{-1}$$

$$G(-1) = i^{-1} = \frac{1}{i} = -i$$

$$G(1) = i$$

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

单射、不同元映射到同同  
满射，B中元都在A中都有



## 例2：

› 群 $(\mathbf{R}, +)$ 和 $(\mathbf{R}^+, \cdot)$ 是同态的，因为若令  
 $\sigma : x \rightarrow e^x, x \in \mathbf{R}$ , 则 $\sigma$ 是 $\mathbf{R}$ 到 $\mathbf{R}^+$ 的1-1映  
射，且对任意 $x_1, x_2 \in \mathbf{R}$ , 有  
 $\sigma(x_1+x_2) = e^{x_1+x_2} = e^{x_1} \cdot e^{x_2} = \sigma(x_1) \cdot \sigma(x_2)$ ,  $\sigma$   
是 $(\mathbf{R}, +)$ 到 $(\mathbf{R}^+, \cdot)$ 的满同态映射。

$$G(x_1+x_2) = e^{x_1+x_2} = e^{x_1} \cdot e^{x_2} = G(x_1) \cdot G(x_2)$$

## 定理6.4.1

› 设 $\mathbf{G}$ 是一个群， $\mathbf{K}$ 是一个乘法系统， $\sigma$ 是 $\mathbf{G}$ 到 $\mathbf{K}$ 中的一个同态映射， $\mathbf{G}'=\sigma(\mathbf{G})$ ，则  
1) $\mathbf{G}'$ 是一个群；  
2) $\mathbf{G}'$ 的单位元 $1'$ 就是 $\mathbf{G}$ 的单位元 $1$ 的映像  
 $\sigma(1)$ ，即 $1'=\sigma(1)$ ；  
3)对任意 $a \in \mathbf{G}$ ,  $\sigma(a^{-1})=(\sigma(a))^{-1}$ 。  
› 称 $\mathbf{G}$ 和 $\mathbf{G}'$ 同态，记为 $\mathbf{G} \sim \mathbf{G}'$ 。

① 非空、1'是否在 $\mathbf{G}'$   
且 $G(a) \in \mathbf{G}'$ 、 $\mathbf{G}'$ 非空

② 封闭 ( $\forall a, b \in \mathbf{G}', a \cdot b \in \mathbf{G}'$ )

$$\begin{aligned} &G(a) \in \mathbf{G}' \\ &G(b) \in \mathbf{G}' \end{aligned}$$

$$\text{Q.E.D. } \underline{G(a) \cdot G(b) \in \mathbf{G}'}$$

$$G(a \cdot b) \in \mathbf{G}'$$

$$\text{③ } \left\{ \begin{array}{l} \text{1'} \in \mathbf{G}' \\ \underline{G(a) \cdot G(b) \cdot G(c) = G(a) \cdot (G(b) \cdot G(c))} \end{array} \right.$$

$$G(a \cdot b) \cdot G(c) = G(a \cdot b \cdot c)$$

$$G(a) \cdot G(b \cdot c) = G(a \cdot b \cdot c)$$

$$\textcircled{④} \quad \overline{G(a) \cdot G(c)} = \overline{G(a \cdot c)} = \underline{\underline{G(a)}}$$

$G(a) \cdot \underline{G(c)}$

$$\textcircled{⑤} \quad \overline{G(a) \cdot \underline{(G(a))^{-1}}} = \overline{G(a) \cdot G(a^{-1})} \\ = \underline{\underline{G(1)}}$$

同様  $1-1$  映射は  $\textcircled{④}$  の意味で成り立つ。

$$\underline{\underline{R^+}} \quad \begin{array}{l} a \in R^+ \\ b \in R^- \end{array} \quad G(a \cdot b) = \log_2 a \times b = \underline{\log_2 a + \log_2 b} \\ = G(a) + G(b)$$

$1-1$  映射。満足する条件を満たす。

矛盾:  $x_1 \neq x_2$  で  $\log x_1 \neq \log x_2$ ,  $\therefore G(x_1) \neq G(x_2)$ .

満足:  $\forall x \in R^+$   $\exists \underline{\log x \in R}$

$\lambda$  为  $R^k$  中的元素.

$(R^k, \cdot)$  为  $(R, +)$  的  $\lambda$ -倍数.

例 1. 线性法.

设  $G$  为  $R^k$  到  $R^k$  中的 可逆映射.

令  $\lambda \in R$  有  $G(1) \rightarrow 0$   $G(-1) \rightarrow a$

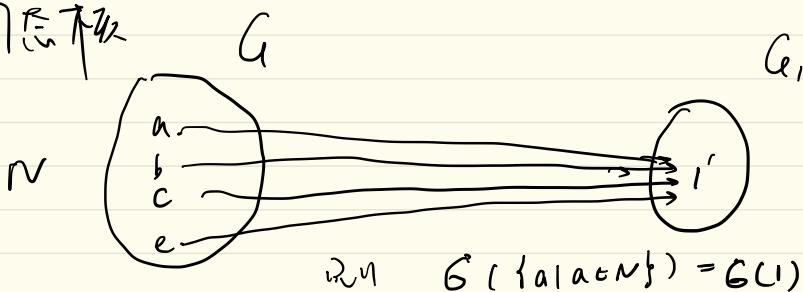
$$\begin{aligned} \text{从 } G & \quad G(1) = G((1) \cdot (-1)) = G(-1) + G(-1) \\ & = a + a = 2a \end{aligned}$$

若  $a \neq 0$ , 则  $G(1) \rightarrow 0$  为矛盾

|线性法

无限制环路. 例初等整数加法原理

同态映射



$$G^{-1}(l') \rightarrow N$$

且  $N$  为  $G$  的子集

$$G' = G(0) = 0 \pmod{3} = \bar{0}$$

$$\underbrace{G'(0)}_{\text{def}} = \{0, 3, 6, \dots\} = 3G$$

$G \{ \}$  H は 3 倍群。

$$\frac{|H|}{|Ha|} = \frac{a \in G}{a \notin H}$$

$$|G| / |H| \neq$$

$$\frac{|G|}{|H|} = \frac{|G|}{|ab^{-1}|}$$

群論 - 例題

①  $I' \rightarrow$  原始素数の同型核  $\rightarrow$  正規子群

②  $G(a') \rightarrow$  是  $N \in G$  の  $a'$  で  $a' \in N$

群  $\oplus$  ① 非空  $G(I) = I' \cap N$

$\Rightarrow a \in N, b \in N \Rightarrow ab^{-1} \in N$

$$\text{群} G(ab^{-1}) = I' \Rightarrow G(ab^{-1}) = G(a) * G(b^{-1})$$

$$= I' * I' = I'$$

$\therefore ab^{-1} \in N$

$\therefore N \in G$  の子群

$$N = \{ab^{-1} \mid ab^{-1} \in H\}$$

$$N = \{ab^{-1} \mid a \in H, b \in H\}$$

$$a \in H, b \in H$$

(2). 再証する部分は既に証明

既に証明済み

要す:  $g \in G$ .

既に

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

$gH = HG$

$$\boxed{gNg^{-1} \subseteq N}$$

( $\forall a \in gNg^{-1}$ . 既に  $N_0 \in N$ .  $a = gN_0g^{-1}$ )

$$G(a) = G(g) \left( \underbrace{G(N_0)}_{= 1'} \cdot G(g^{-1}) \right) = G(g) \cdot G(g^{-1})$$

$$\begin{aligned} \therefore a \in N. & \quad \therefore 1' \\ & = G(g \cdot g^{-1}) = G(1) \\ & = 1' \end{aligned}$$

(3). さて  $G'$ .  $G(a) = a'$ . 今証

$$G(b)(a')^H = 1'$$

$$\boxed{G^+(a') = Na}$$

$$G(b) G(a)^{-1} = 1'$$

$$b \in G. \quad \boxed{G(b) = a'}$$

$$\begin{aligned} G(b) G(a^{-1}) & = G(b \cdot a^{-1}) \\ & = 1' \end{aligned}$$

$$b \cdot a^{-1} \in N$$

$$\boxed{b \in Na.}$$

$$\boxed{G(a') \in Na.}$$

$\exists, \forall$  1  $N$  是環. ② 1  $\{A, B\} \subset N$  是半群.

② 1  $AB$  也是  $N$  中半群.

$$a \in G \quad A = Na.$$

$$b \in G \quad B = Nb.$$

$$\begin{aligned} AB &= NaNb = \underline{N} \underline{Na} \underline{b} \\ &= Nc \end{aligned}$$

$$\begin{array}{l} ab \in G. \\ c \in G \end{array}$$

$$N = \{-10, -5, 0, 5, 10\}.$$

$$a \in \mathbb{I}$$

$$a \equiv 1 \pmod{5}$$

$$\underline{N+a} \quad \underline{\{ -9, -4, 1, 6 \}} \quad \overline{1}$$

环论之2

- ① 非空
- ② 二运算
- ③ 封闭

} 2个半群.

~~加法和乘法满足 Abel 算律~~

$$\textcircled{1} a+b = b+a$$

$$\textcircled{2} (a+b)+c = a+(b+c)$$

④ 加法有1

⑤ 加法有逆

⑥ 乘法~~满足结合律~~  $a+b \times c = a \times (b \times c)$

⑦ 乘法对加法分配律  $a \times (b+c) = ab+ac$

加法构成加法群 (Abel)

乘法构成乘法群

$$(a+b)^n = \underline{C_a^0 a^0 b^0 + C_a^1 a^{n-1} b^1 + \dots + C_a^n a^0 b^n}$$

= 二式之和

› 定理6.5.1 环R的子集S作成子环必要而且

只要,

1) S非空;

2) 若 $a \in S$ ,  $b \in S$ , 则 $a-b \in S$ ;

3) 若 $a \in S$ ,  $b \in S$ , 则 $ab \in S$ .

10

☆ 令1环. — 1. N<sup>i</sup>-环. 而且能找到由环扩充

☆ 互换律. — 本法满足互换律.

☆ 与环律1与环律1不一定一致. 但群律一致的

☆ 清去律  $a \in R$ ,  $b \in R$   $a \cdot b \neq 0$   $ab = 0$

即  $a, b$  为零因子. 若没有零因子, 则称清去律

不

$$\textcircled{1} \quad axb = a \times c \Rightarrow b = c$$

$$\textcircled{2} \quad b \times a = c \times a \Rightarrow b = c$$

| 清去律的加法逆元是群 |

消去环的性质

① 消去环满足消去律

② 在消去环  $R$  中, 不为 0 的元素在加法下是可逆的  
[即存在]

① 若周期为  $a$  则有  $a^n = 0$ . (无限循环进位制)

② 若  $a$  与  $b$  周期  $\neq 0$ ,  $b$  与  $a$  周期  $n \neq 0$ .

$$\begin{cases} ma = 0 \\ nb = 0 \end{cases} \text{ or } m = n$$

$$(a \cdot m)b = 0$$

$$a \neq 0, mb = 0 \Rightarrow n \mid m$$

$$(b \cdot n)a \cdot b$$

$$a \cdot nb = 0$$

$$b \neq 0 \Rightarrow a \cdot n = 0 \Rightarrow m \mid n.$$

$$\boxed{m = n}$$

③ 在消去环  $R$  中, 不为 0 的元素在乘法下是有周期的  
且  $\neq 0$ . 或者质数

密度

有理数圆周率及根号不

( $\pi \times +$ )

[合1. 有理数圆周率及根号不]

无理数不

如图示

①  $\sqrt{2}$

③ 重读有理数圆周率及根号不

$$\begin{array}{c} \overline{0 \ 1 \ 2 \ 3} \\ \hline \Delta \quad \Delta \end{array}$$

$$\begin{array}{r} 3 \times 2 = 2 \\ 1 \times 2 = 2 \end{array}$$

(本)

设  $R$  为实数，若  $R$  为有理数，则  $R$  为整数。

而元素若能构成等差数列，则  $R$  为本 (无理数)

(本不是整数，因为不是等差数列。)

本无理数。

如图示。  $q + r$  (下述)

(本不是整数)

本不是整数

( $R, +, \cdot$ )

本不是整数

本不是整数

不等式解集： $a < b$  时去集 .  $a \geq b$  时保集.

$$\frac{a \cdot b \neq 0}{}$$

无零因式  $\rightarrow$  去集之去集.

有零因式  $\rightarrow$  保集.  
无零因式保集.

★ 成、 $\boxed{3 \leq R < 1}$

★ 成  $\rightarrow$  去集. 同时下同去之保集.

★ 不成特例是成

不等式解集  $\neq$  空集.

$$a < b \neq 0 \quad \begin{matrix} a \neq 0 \\ b \neq 0 \end{matrix}$$

$$ab = ac$$

- 理想  $N \triangleq 3 \geq n$

①  $a \in N$   $\rightarrow$  加法封闭.  
 ②  $a-b \in N$ .  $\rightarrow$  减法封闭.

\* ③  $a \in N, x \in R$   $\rightarrow$  乘法封闭.  
 $ax \in N, xa \in N$

理想  $\neq \emptyset$   
非空  $\Leftrightarrow$  3 性质

$a \in N, b \in N$   
 $ab \in N$

| 是整数环,  $m \in S \in R$ ,  $S$  是理想

①. 非空  
 ②  $a \in m$ .  $\rightarrow \exists i_1$  使得  $a = m_{i_1}$   
 $| \exists i_2 \quad b = m_{i_2}$

$\therefore a-b = m(\underbrace{i_1-i_2}) \in m$

③  $a \in m!$  ② 1.  $\exists i_0$  s.t.  $a = m_{i_0}$

$\forall x \in I.$  ② 1.  $ax = \underline{m_{i_0}!} \in N$

$x \cdot a = 1 \cdot m_{i_0} = m_{i_0} \in N$

8 27.

①  $\frac{a}{b} \in \mathbb{Z}$

③  $a - b \in N$

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$$

③  $a \times b \in N$

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

③  $\forall x \in \mathbb{R} \notin N.$   $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$

$$ax = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$x \cdot a = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin N$$

① 定義  $R$  只有半單理想 ( $D, \text{否}$ )

即  $R$  中理想  $N$

若  $N = \{0\}$ , 則  $\exists$ .

否則 設  $N = R$

則  $N \neq \{0\}$ . 但  $a \in N$ .  $\Rightarrow a \neq 0$

$a$  有逆元  $a^{-1}$ .  $\forall n \in N$ .  $a^{-1}a \in N$ .  
 $1 \in N$

即  $\forall x \in R$   $x = 1x \in N$

$\Rightarrow R \subseteq N$

② 两个理想  $n$  之交必为理想

$aR$  是  $R$  在交换环  $A$  中的子理想,  $a \in R, (R)$   $aR = \{ar | r \in R\}$

$aR$  是  $R$  的理想, 且包含  $a$ .

由  $a$  生成的理想

想

①  $a|0$

②  $a - b \in aR$ .

$(0) = \{0\}$

③  $\forall aR, r \in R$

$(1) = R$ .

$aR$  是  $a$  生成的 理想

$aR \cup bR$  (包含两个理想)

同余关系.

$R, N, a, b \in R, n \in N, a \equiv b \pmod{N}$

$a \equiv b \pmod{N} \quad \text{Def} \quad a \equiv b + n \quad (n \in N)$

性质 1:  $a \equiv b \quad c \equiv d \quad a + c \equiv b + d$

性质 2:  $a \equiv b \quad c \equiv d \quad a \times c \equiv b \times d$

逐塊地圖是相同的。

① AIR IN

$$\textcircled{2} \quad \underline{G(a+b) = G(a) + G(b)}, \quad \underline{G(ab) = G(a)G(b)}$$

(b) 材料 1-1 版行.

► 设  $\mathbf{R}$  是一个环,  $\mathbf{S}$  是一个有加法和乘法的运算系统。若  $\sigma$  是  $\mathbf{R}$  到  $\mathbf{S}$  中的一个同态映射, 则:

$R$ 的映象 $R'=\sigma(R)$ 也是一个环,

$\sigma(0)$ 就是 $R'$ 的零 $0'$ ,

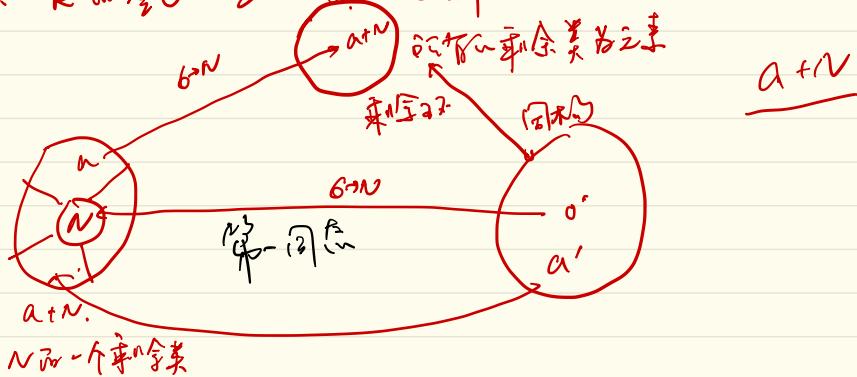
$$\sigma(-a) = -\sigma(a).$$

若  $R$  有壹而  $R'$  不只有一个元素，则  $R'$  有壹，而且  $\sigma(1)$  就是  $R'$  的壹 $1'$ ；

若 $a \in R$ 有逆，则 $\sigma(a)$ 在 $R'$ 中有逆而且 $\sigma(a^{-1})$ 就是 $\sigma(a)^{-1}$ 。

1

同様 R'm' と並んで (只解説用)



非极性分子

$$(a+N) + (b+N) = (a+b) + N$$

$$(a+N)(b+N) = ab + N$$



$R \xrightarrow{\text{分解}} \text{原子}$  (本)

$R \xrightarrow{\text{分解}} N$  (本)

单分子不极性分子理想

(3). 单分子理想  $\xrightarrow{\text{单分子理想}} \text{单分子理想}$

$$P(X \text{理想}) = \frac{1}{4} + \left\{ 0, 1, 2, 3, 4 \right\} = \left\{ 0, 1, 2, 3, 4 \right\}$$

找子群  $\xrightarrow{\text{找子群}}$

极大理想

$\exists R$  一个理想  $N$  是一个极大理想. 即  $N \subsetneq R$

$(PR \neq N)$  之间没有别的理想 (极大理想不是一)

① 极大理想与单纯环的关系.

$N \subset R$

$N$  是  $R$  的极大理想  $\Leftrightarrow$  它是单纯环:

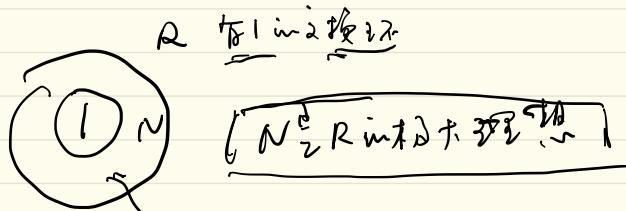
$R/N$  是单纯环.

② 若有  $1$  的倍数, 则单纯  $\Rightarrow R$  是一个域

$$a \in R, \quad a \neq 0, \quad aR = R \quad \exists a_0, \quad a_0 \cdot a = 1 \\ a_0 = a^{-1}$$

③ (无素域) 若有  $1$  的倍数在单纯环里不

④



$R/N$  域  
(即  $R/N$  是单纯环)

(有邊緣的算子不是理想)

① 有1元零元  $\Rightarrow$  该理想是整环. 整环的性质理想是主理想. 因此为主理想环.

整数环是主理想环



整环

$\forall N \in \mathbb{Z}$ :

$0 \cdot 1 = N$ , 故  $N$  是理想

(2). 若  $N$  中不只一个元素, 则  $\exists a \in N$  使得  $a$  是  $N$  中所有非零元素的最小正整数. 设  $b \in N$

$$(a) = a\mathbb{Z} \subseteq N$$

$$\exists b \in N \quad \exists b = aq + r \quad 0 \leq r < |a|$$

$$r = b - aq \in N. \quad \because r = 0$$

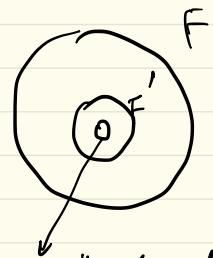
$$\therefore b = aq, \quad b \in a\mathbb{Z} \Rightarrow N \subseteq a\mathbb{Z}$$

$\therefore N = a\mathbb{Z}$ . 故  $N$  是主理想

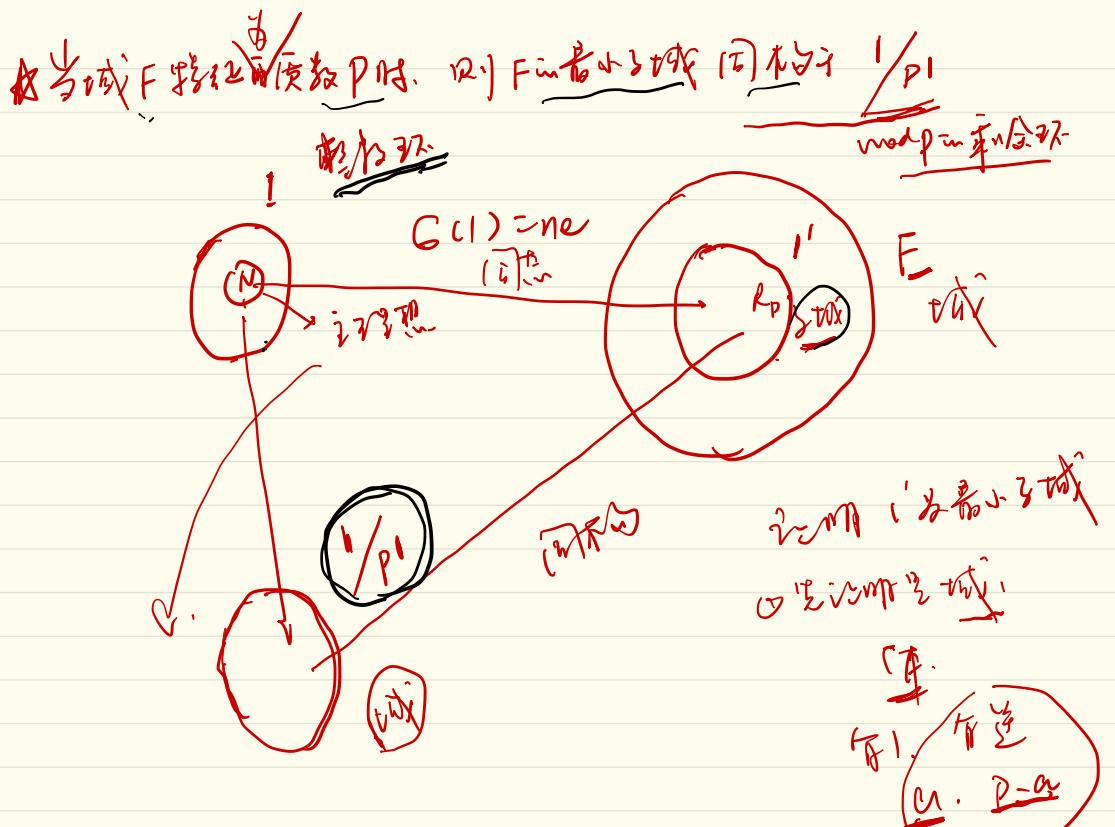
非零  
 $a, b \in N$ .  
 $a \neq 0, b \neq 0$   
 $ab \in N, ba \in N$

$b \in a\mathbb{Z}$

最小正整数

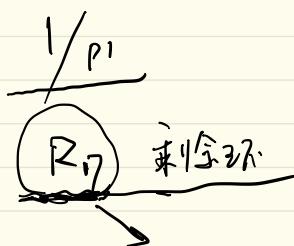


$F'$  不能包含  
最小正整数



★ 当域  $F$  中不存在质数时, 域  $F$  中含有无限小的域同构于有理数域  $\mathbb{Q}$

$\mathbb{Q}$  在域  $F$  中是最大的域



$$\frac{1}{p} = 3 \times \frac{1}{13}$$

$$4 \times x = 1$$

$$x = 13$$

$$39 \text{ mod } 17 = 5$$

本原多项式 整数环

(无重根的多项式) 和一个整系数多项式相乘  
整系数多项式与本原多项式相乘

\* Eisenstein 定理.

对于一个质数  $p$ .  $p$  不整除  $a_0$ .  $\underline{p \mid a_1 \dots p \mid a_n}$   
 $\underline{p^2 \nmid a_n}$ .  $f(x) \in \mathbb{Z}[x]$  上有  $\bar{p}$ .

重数论.

①  $f(x)$  是本原多项式.  $f(x)$  在  $\mathbb{R}$  上不可约, 则  $f(x)$  在  $\mathbb{C}$  上也不可约.

上也不可约.

② 整系数  $f(x)$ .  $\underline{x \in \mathbb{R}}$  不可约. 则  $\underline{x \in \mathbb{C}}$  不可约

③ 整系数  $f(x) \in \mathbb{R}[x]$ . 若  $a_0$  不是  $f(x)$  的根.

则  $f(x)$  在  $\mathbb{R}$  上不可约. 因为  $\mathbb{R}$  上不可约  $\underline{f_p(x)}$ .

④  $f(x) \in \mathbb{R}$  上不可约

$$ax^4 + bx^2 + \frac{ax}{x} + 1$$

$$\overline{y} \sqrt{x^2 - 1}$$

$$3x^3 - \frac{3}{2}x^2 + \left(b + \frac{3}{4}\right)x + \left(a - \frac{b}{2} - \frac{3}{8}\right)$$

$$2x+1$$

$$\sqrt{bx^4 + 0x^3 + 2bx^2 + 2ax + 2}$$

$$\cancel{bx^4} + 3x^3$$

$$- 3x^3 + 2bx^2$$

$$- - 3x^3 - \frac{3}{2}x^2$$

$$(2b + \frac{3}{2})x^2 + 2ax$$

$$(b + \frac{3}{4})x$$

$$(2a - b - \frac{3}{4})x + 2$$

$$a - \frac{b}{2} - \frac{3}{8}$$

$$\frac{b}{2} + \frac{13}{8} - a$$

$$R_0 \xrightarrow{f_p} R_p \xrightarrow{2x^2 - 8} \underline{\underline{R_3}}.$$

$\Rightarrow f(x)$  在  $R_0$  上不是  $P$  的倍数.

但  $f(x)$  在  $R_p$  上是  $P$  的倍数.

$$\underline{\underline{2x^2 - 8}} \Rightarrow \underline{\underline{2(x+2)(x-1)}} = 0$$

$$a, b, c \in \{0, 1, 2\}$$

$$a + bx + cx^2$$

$$b=1, \quad a=1$$

$$\begin{cases} x=2 \\ x=-1 \end{cases}$$

$\Rightarrow$  故  $R_0$  上有 1 次因式, 2 次因式.

但  $R_p$  上只有 1 次因式

$$x^2 + 1 = 0$$

故  $R_0$  上有

3 个

+ 但  $R_p$  是 2 的倍数. 但  $R_0$  上不可约.

$$\textcircled{1} \text{ 设 } f(x) = x^5 + 5x^2 + 15 \quad \text{per R}_0 \text{ 中不约分}$$

若设  $P$  为 Eisenstein 之质数,  $P=5$ ,  $P \nmid a_0$ ,  $f(x)$  在  $\mathbb{F}_5[x]$

$$P^2 \nmid a_2 \quad \therefore x^5 + 5x^2 + 15 \in \mathbb{F}_5[x] \text{ 中不约分}$$

o 1 2

$$\textcircled{2} \text{ } x^5 + 7x^2 - 3 \quad \text{设 } f(x) \text{ 在 } \mathbb{F}_7[x] \text{ 上不约分}$$

$\exists$   $f(x) \in \mathbb{F}_7[x]$  使  $f(x)$  在  $\mathbb{F}_7[x]$  上不约分, 则  $f(x)$  在  $\mathbb{F}_7[x]$  上不约分

$$f(x) = x^5 + x^2 + 1$$

$$\begin{array}{l} \text{④ 设 } f(x) \text{ 为一二次因式} \\ f(0) = 1 \quad \therefore f(x) \in \mathbb{F}_7[x] \text{ 不含 } P \\ f(1) = 3 \end{array}$$

⑤ 设  $f(x)$  为一二次因式.

$$f(x) = (x^3 + x^2)(x^2 + x + 1) + 1$$

$$\therefore f(x) = \underbrace{(x^3 + x^2)}_{\text{因式}} + \underbrace{(x^2 + x + 1)}_{\text{因式}}$$

$$\begin{aligned} & x^2 + ax + b \\ & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\ & \begin{pmatrix} x^2 \\ x^2 + x \end{pmatrix} = x^2 - (x+1)(x+1) \\ & \quad = (x+1)^2 \end{aligned}$$

$x^2 + x + 1$  (因式)

⑥ 因此  $f(x)$  在  $\mathbb{F}_7[x]$  上不约分

综上,  $f(x)$  在  $\mathbb{F}_7[x]$  上不约分.

n次单根复数上

~~( $\times$ )~~  $-1 = 0$ . in  $\mathbb{R}$ , n次单根

设  $r(\cos\omega + i\sin\omega)$

两步级相乘  $rs [\cos(\omega+0) + i\sin(\omega+0)]$

$\therefore$  1重n次根. 若为n次单根. 则有  $\omega \neq 0$

$$\left( \cos \frac{\omega}{n} + i \sin \frac{\omega}{n} \right)^k$$

而. 所有n次单根都在复平面上以原点为圆心的圆周上

由  $\infty$  级成  $n$  个单根.  $\sqrt[n]{1}$  有  $n$  个

$\varphi(n)$  为元. 本元  $n$  次生成元

$$\Phi_n(x) = (x - \varphi_1)(x - \varphi_2) \cdots (x - \varphi_{\varphi(n)})$$
 称为 1包围式

$$\Phi_1(x) = (x-1)$$

$$\Phi_2(x) = (x+1)$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

而  $\Phi$ . 为  $\mathbb{Z}_n$  的生成元. 在  $\mathbb{C}$  中

$$x^8 - 1 = \prod_{d|8} \Phi_d(x) = \underbrace{\Phi_1(x)}_{\text{only } 1 \text{ term}} \underbrace{\Phi_2(x) \Phi_4(x) \Phi_8(x)}_{\text{3 terms}}$$

$\Phi_7 \text{ is omitted}$

$d = 1, 2, 4, 8$

找  $\Phi_{24}(x)$ .

$$\therefore x^{24} - 1 = \prod_{d|24} \Phi_d(x) = \underbrace{\Phi_1}_{x+1} \underbrace{\Phi_2}_{x-1} \underbrace{\Phi_3}_{x^2+x+1} \underbrace{\Phi_4}_{x^3-1} \underbrace{\Phi_6}_{x^6-1} \underbrace{\Phi_8}_{x^8-1} \underbrace{\Phi_{12}}_{x^{12}-1} \underbrace{\Phi_{24}}_{x^{24}-1}$$

$$\Phi_1 = x-1$$

$$\Phi_2 = x+1$$

$$\Phi_3 = x^2+x+1$$

$$\Phi_4 = x^3-1$$

$$\begin{array}{r} x^8 - x^4 + 1 \\ \hline x^4 + 1 \sqrt{x^{12} + x^8 + 1} \\ \underline{-x^8 - 1} \\ \hline -x^8 - \end{array}$$

$$x^4 + 1$$

$$\begin{aligned} \therefore \frac{x^{24}-1}{x^{12}-1} &= \Phi_{24} \cdot \Phi_8 \\ \frac{x^8-1}{x^4-1} &= \Phi_8 = x^4+1 \\ \therefore \Phi_{24} &= \frac{(x^{24}-1)(x^4+1)}{x^{12}-1} \\ &= \frac{(x^{12}+1)(x^8+1)}{x^4+1} \end{aligned}$$

$$\frac{x^{24}+1}{x^{12}-1} = \Phi_{24} \Phi_8$$

$$\cancel{\Phi_1} = \Phi_1 \Phi_2 \Phi_4 \cancel{\Phi_6} \Phi_8$$

$$\therefore \Phi_8 = \frac{x^8-1}{(x+1)(x-1)(x^2+1)} = \frac{x^8-1}{x^4-1} = x^4+1$$

# 重根 in 域

在域上  
 n 次多项式  
 不是单根 in 域  
 是单根 in 域  
 没有重根  
 $n = kp^m$   
 $x^n - 1 = (x^{k-1})^{p^m}$   
 $45 = 9 \times 5^1$   
 $x^{45} - 1 = (x^8 - 1)^5$

$$x^{45} - 1 = 0 \quad \text{在 } R_9 上 \text{ 有重根 in 域}$$

$$9 | 45 \rightarrow 45 = 9 \times 5^1 \Rightarrow k=9 \quad m=1$$

∴ 根为  $\underline{(x^9 + 1)^5}$  5 重根

例.  $R_2 = \{0, 1\}$  上的4个矩阵:

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

作成的集合  $F = \{0, 1, a, b\}$  在矩阵加法、乘法下作成一个域。则在  $F$  上求4次单位根就是求方程  $x^4 - 1 = 0$ ,

即  $x^4 - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$  的根。

该域的特征是2,  $4=2^2$ , 因此  $x^4 - 1 = (x-1)^4 = 0$ 。1是该方程的2<sup>2</sup>=4重根。

$x^n - 1 = 0$  在域上是否有  
n重根?

设问:

① n 不是单根 in 域

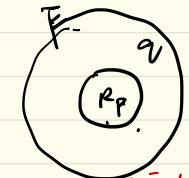
② 0 在 F 上有根

则解成 n 重根不成立 ( $n \neq 0$ )  
元素不是  $\Phi_n$  in F

$$x^n - 1 = 0$$

有限域论 Galois.

$$|F| = q$$



$q-1$  个非零元. 互质且单.

$$x^{q-1} + \dots = 0 \text{ in } F$$



$R_p[x]$  在  $F$  上一个多项式环.

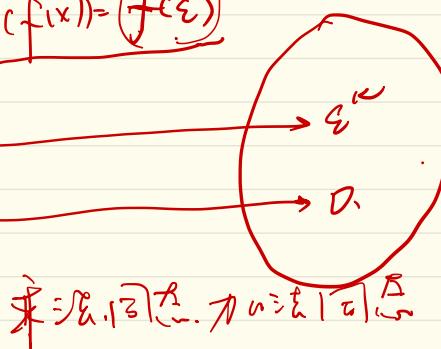
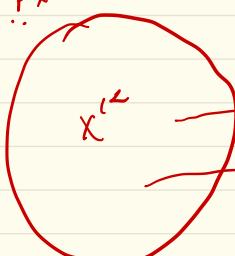


$\Phi(q-1)$  个生成元素 却是  $\Phi_{q-1}(x)$  在  $F$  上

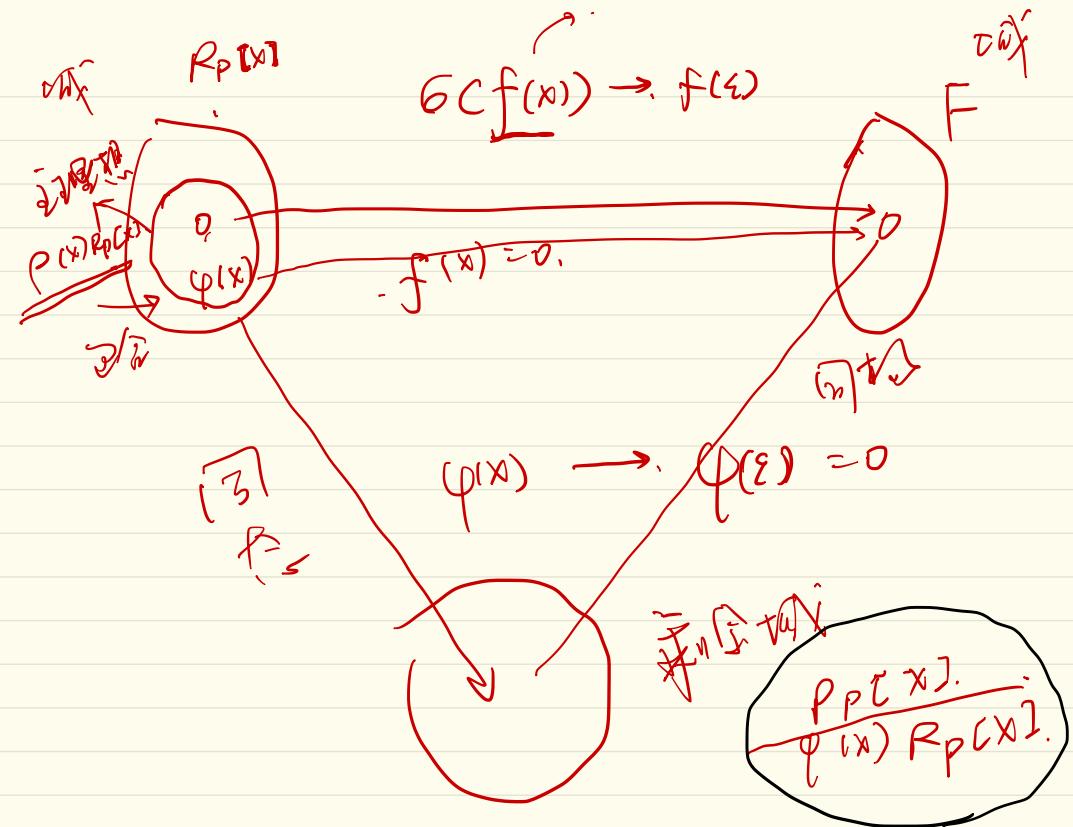
$R_p[x]$  上  $F$  上一个多项式环.  
 $\Phi_{q-1}(x)$  在  $F$  上的因式  $\Phi(x)$ .  
 $\Phi(x)$  是  $F$  上的有理数.

$R_p[x]$

$$G(f(x)) = f(\xi)$$



F



两个映射.

$$\underline{\phi(x)} \perp \underline{P(x)}$$

$\phi(x)$  与  $P(x)$  不平行

$\phi(x)$  与  $P(x)$  相交 或者 垂直.

{ $\phi$  与  $P(x)$

有限域

F中元素个数一定是  $p^n$

→ 域的特征

元素相同时限域必互同构

$\Phi_{p^{m-1}}$  在  $R[x]$  中任意质因式  $4(x)$  的  $\frac{1}{2} m$  次方

$\frac{1}{2}$

$$z^{2-1} \mid z^4 - 1 \quad \Rightarrow 3 \mid 15 = 1.$$

$t \in \mathbb{F}_{p^m}$

$t^2 \in \mathbb{F}_{p^m}$

$m \mid n$

極限下限極

(8元)

$$P=2 \quad M=3$$

$\varphi(x)$  是 3 次 3 改式

$R_{\geq 1}$

$$\textcircled{1} \text{ 且 } \Phi_{P^{M-1}} = \Phi_7$$

$$x^7 - 1 = \Phi_1 \Phi_7$$

$$\textcircled{2} \quad \Phi_7 = \frac{x^7 - 1}{x - 1} = \underbrace{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1}_{\text{1}}$$

$$\therefore \varphi(x) = \underbrace{x^3 + x + 1}_{\text{1}}$$

$$\frac{R_2[x]}{\varphi(x) R_2[x]} = \frac{R_2[x]}{\varphi(x) R_2[x]}$$

$$\begin{array}{r} x^3 + x^2 + x + 1 \\ \textcircled{1} \quad 1 \quad 0 \quad 0 \quad 0 \\ \hline \end{array} \quad \textcircled{1}$$

$$x^3 + 1$$

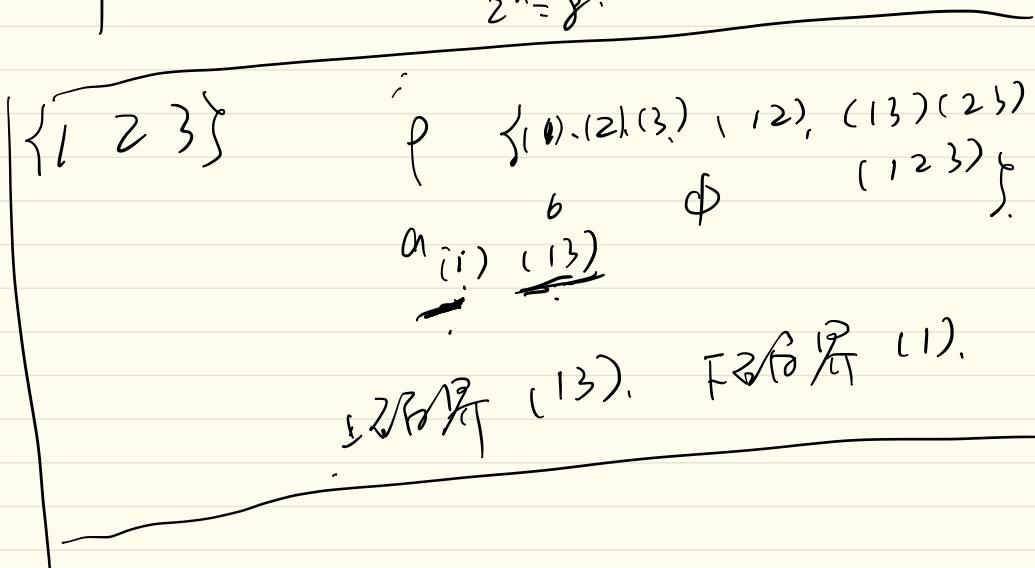
=

$\{a_0 \dots a_n\}$ .

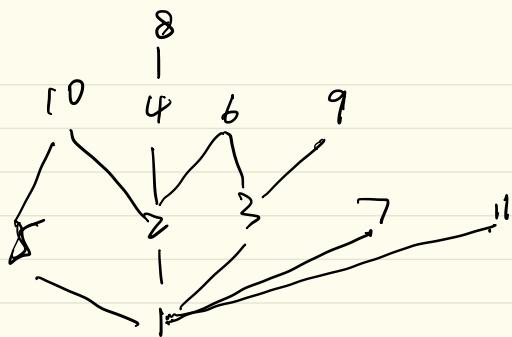
$(a_0 a_1) \leq 0$ .

補.  $P(S)$  は  $S$  の部分集合.

[R1] 部分集合  $(P(S), \subseteq)$  は一个木.

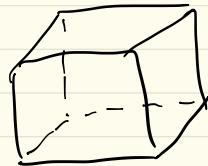


半序



部分序关系

a, b



性质：选择结合吸收



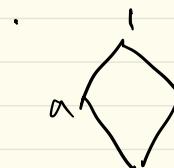
选择属性

$$\underline{a * (a \oplus b)} = a \quad \begin{matrix} \nearrow \text{最大公因数} \\ \searrow \text{最小公倍数} \end{matrix}$$

选择。

选择  $a, b$ . ( $L = \{x, \emptyset, 0, 1\}$ )

分配律 分配律成立

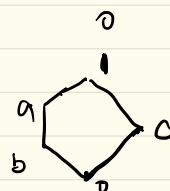


$$axb = 0$$

$$a \oplus b = 1$$

(半序) 选择律

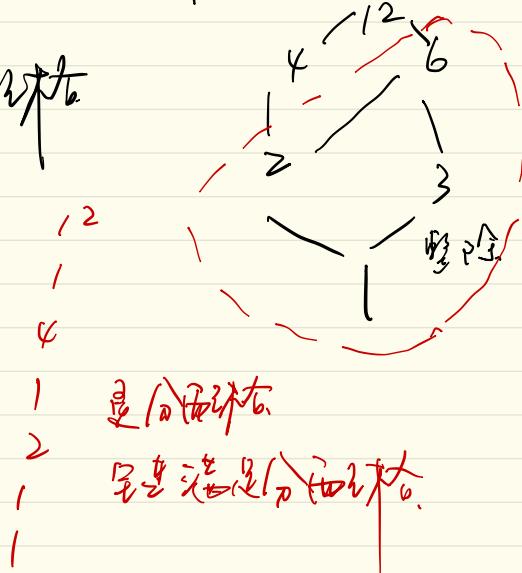
(半序) 选择律



选择公理

有余数. 每个元素都有余元素.

分配律



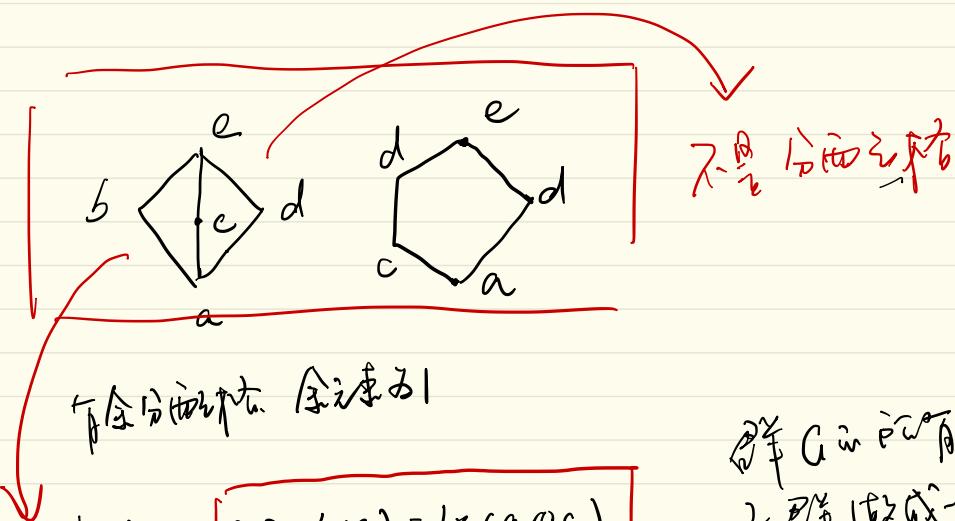
18 题 2

$$\underline{2 \times (4 \oplus 6)}.$$

$$= 2 \times 4 \oplus 2 \times 6$$

$$(4 \oplus 6) \times 2$$

$$4 \times 2 \oplus 6 \times 2$$



有余数. 余元素

模乘法.

$$\boxed{a \oplus (b \otimes c) = b \times (a \oplus c)}$$

$$a \otimes c = b \oplus c \\ \downarrow n=b$$

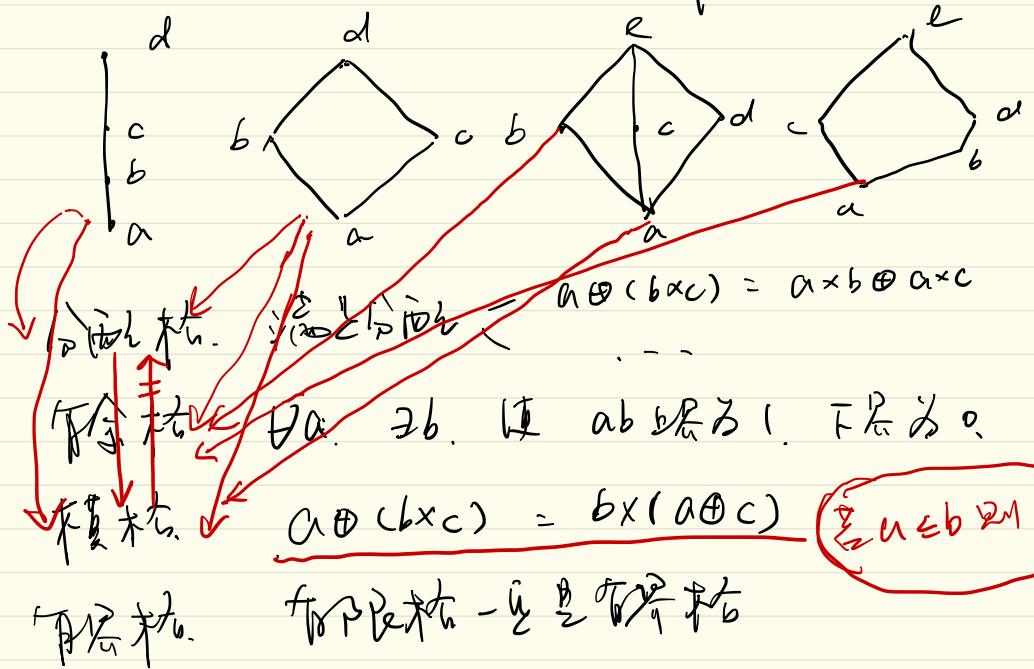
解  $a \otimes c = b$  且  $c$

与  $b$  改成一个数.

是下集. 答.

半直和  $b$ .  $a \cdot b$ . 1.  $a \cdot b$ .  $\uparrow$  上. T

代数和 微分/微分. 变换率.  $\sqrt{A} w^2$ .



平行四边形是模様.

模様 - 也是平行四边形.

$$\underline{c \oplus (b \times c) = b \times c} \underline{c \oplus a} \underline{a}$$

布尔代数：有余分项的逻辑表达式

$$(B, \cdot, +, -, 0, 1)$$

且 上下取反

Huntington 定理

$$\underline{k_1 s_1} + \underline{k_2 s_2}$$

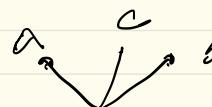
① 交换律  $a \cdot b = b \cdot a$      $a+b = b+c$

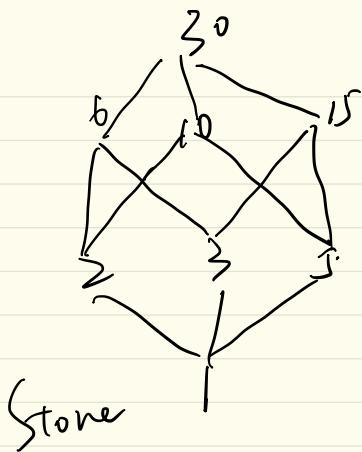
② 分配律  $a \cdot (b+c) = a \cdot b + a \cdot c$      $a+(b+c) = (a+b) \cdot (a+c)$

③  $a \cdot 1 = a$      $a \cdot 0 = 0$

④  $\bar{\bar{a}} = a$      $a \cdot \bar{a} = 0$      $a + \bar{a} = 1$

极小元： $a \cdot x$  的值为 0  
或称本身

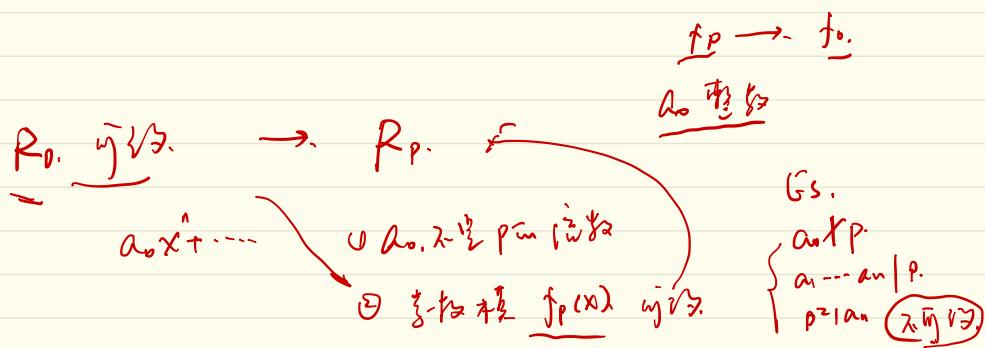




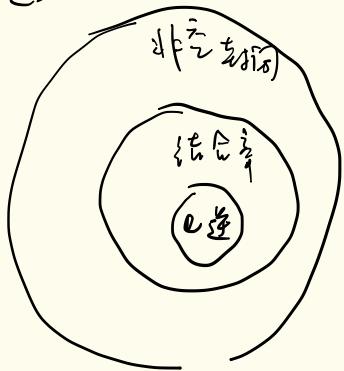
所以邊為 2, 3, 5.

$$b_0 = 2$$

所有外角之和都為某個  $\frac{1}{3}$  合成  $\frac{10}{3}$  之倍數



分子



原 子

$\rightarrow$   $n$

$n:$

$\frac{1}{2} \frac{3}{4}$

分子对称性

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

原 子 电子 对称

分子对称性  
分子对称性

分子对称性  
分子对称性

分子对称性

分子对称性

①  $a^{\text{GH}}$   
 $a^{\text{GH}}$

②  $a^{\text{GH}} b^{\text{GH}}$

③  $a^{\text{GH}} a^{\text{GH}}$

$\frac{1}{2} \frac{3}{4}$

$a^{\text{GH}} b^{\text{GH}}$

$a^{\text{GH}}$

(3)  $\frac{1}{2} \frac{3}{4} + \frac{1}{2} \frac{3}{4}$

$a^{\text{G}}$   $a^{\text{GH}}$

$a^{\text{GH}}$  in  $\frac{1}{2} \frac{3}{4}$

周期

$$a^n = e$$

D

- ① ~~无理数的根号是无理数，  
0. 无理数~~  $\rightarrow \underline{\alpha} \quad \underline{\alpha^{-1}}$   
含无理根号的数是无理数
- ② 无理数不等于有理数.

无理数

$\varphi(n)$ . 无理数

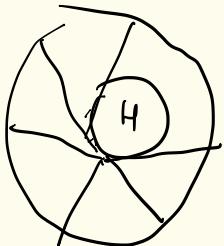
$$\text{无理数} \quad n \times (1 - p_1) (1 - p_2) \dots$$

$\exists \gamma \in \mathbb{R}$  使得  $\gamma$

$$G = \{x_1, x_2, x_3\}$$

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

G. H



划分 G 为不相交的集合

在 rear > 一个数集合

在 arr

之积数  $\prod_{i=1}^n r_i = R$

$$\alpha + H = \{1, 4\}$$

$$= \{2, 5\}$$

$$\frac{\{0, 3\} \cup \{1, 4\} \cup \{2, 5\}}{}$$

子集的并

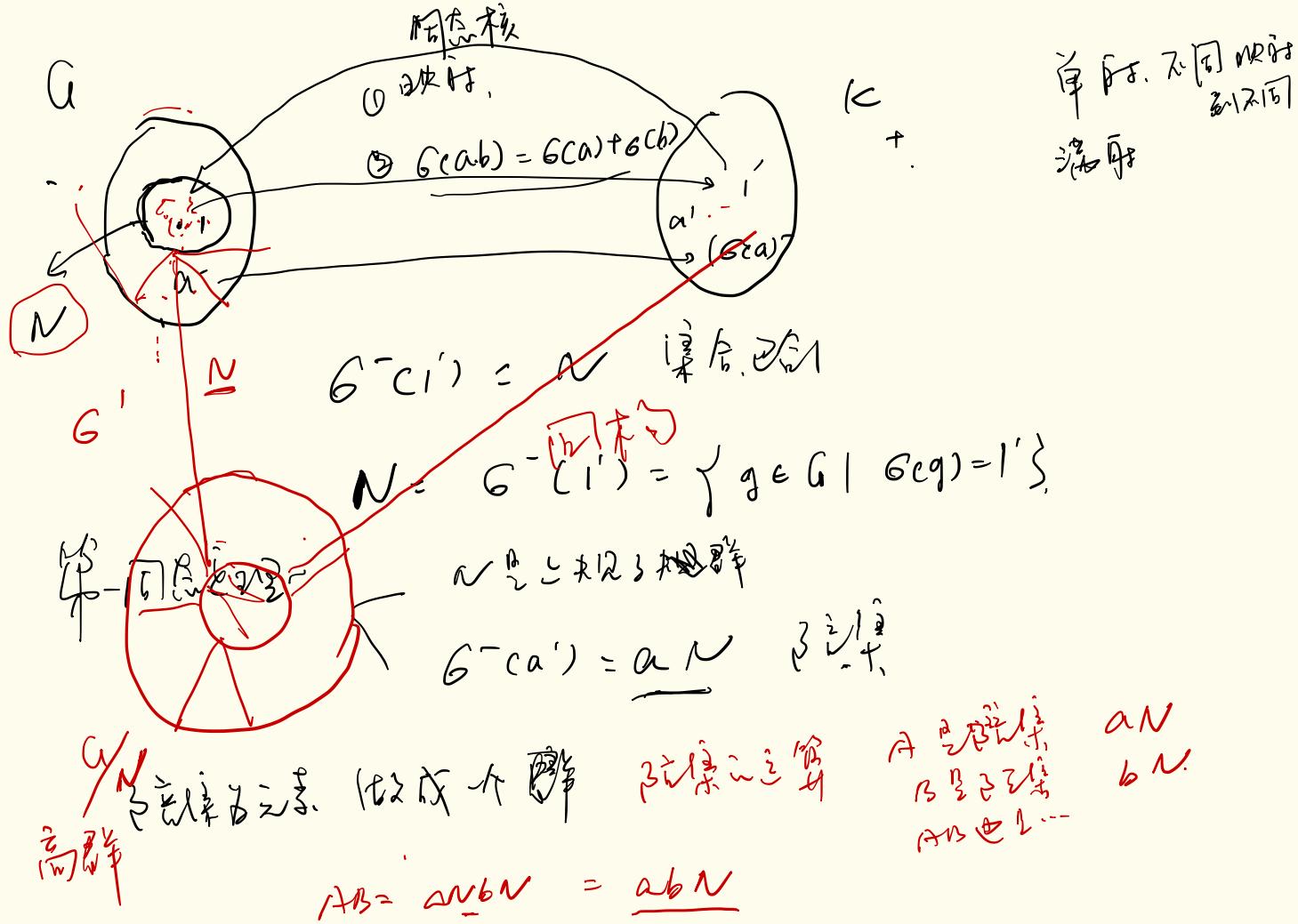
~~$$\frac{|G|}{|H|} = 1$$~~

之积数  $\prod_{i=1}^n A_i$

$$\alpha H = Ha$$

之积数  $\prod_{i=1}^n A_i$

$$\text{且 } \underbrace{\alpha H}_{\text{之积数}} \subseteq H$$



$G \in \text{子群} \subseteq G' \text{ 的子群}$

大对大 小对小

$\mathbb{Z}_{\ell^2} \times \mathbb{Z}_{\ell^2}$

环  $\mathcal{A}$  法 群 + 交换律

半群 结合律

半群 对加法 交换律.

环  $\mathcal{A}$  满足交换律的子群

半群 无交换律,

$a \in G, b \in G \neq 0$

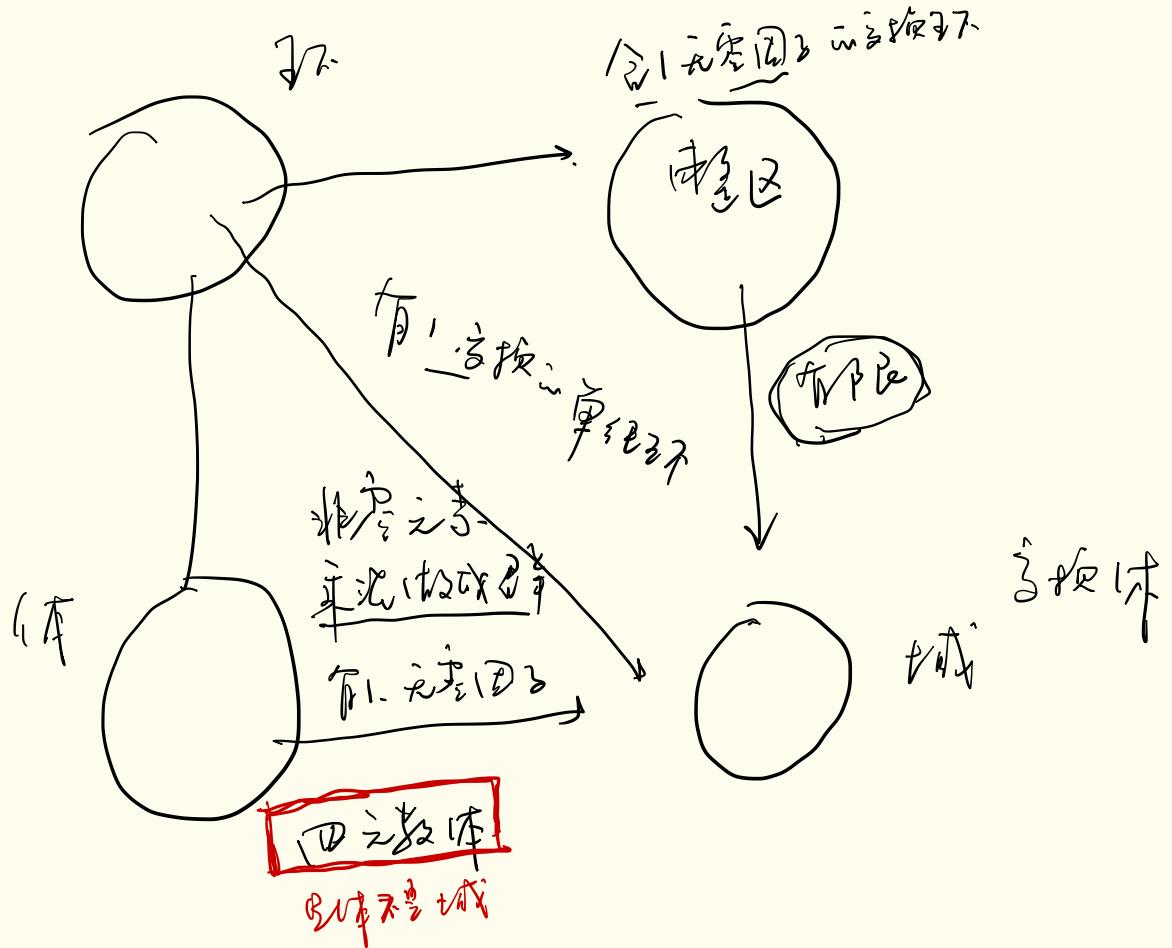
消去律  $ab = 0$ .

半群 非消去律.

半群

半群 不满足 结合律

半群



高级单片机 演讲  
云课堂

简单

加法器与减法器  
乘法器

乘法器  
除法器

(Z, +, -)

整数

进位溢出

1本  
指针

121

乘法器

二进制数

无符号数

$$\begin{aligned} & (a \in R, b \in R) \neq 0 \\ & ab = 0 \end{aligned}$$

例：无符号数  
与负数

+有限

乘法器完成部分  
无符号数

少主频

121

支持本

~~0xe = 0~~

~~0xa = 0~~

~~0xb = 0~~

乘法器不为0

① 溢出情况

② 同期取值。0. 定义

理想.

$N$

①  $\exists \exists \forall$   $a \in N, b \in N$

$\exists a - b \in N$ . 有法

③  $a \in N, b \in G$ .

$ab \in N$   $ba \in N$

非理想  $\{0\}, \{R\}$

非基本

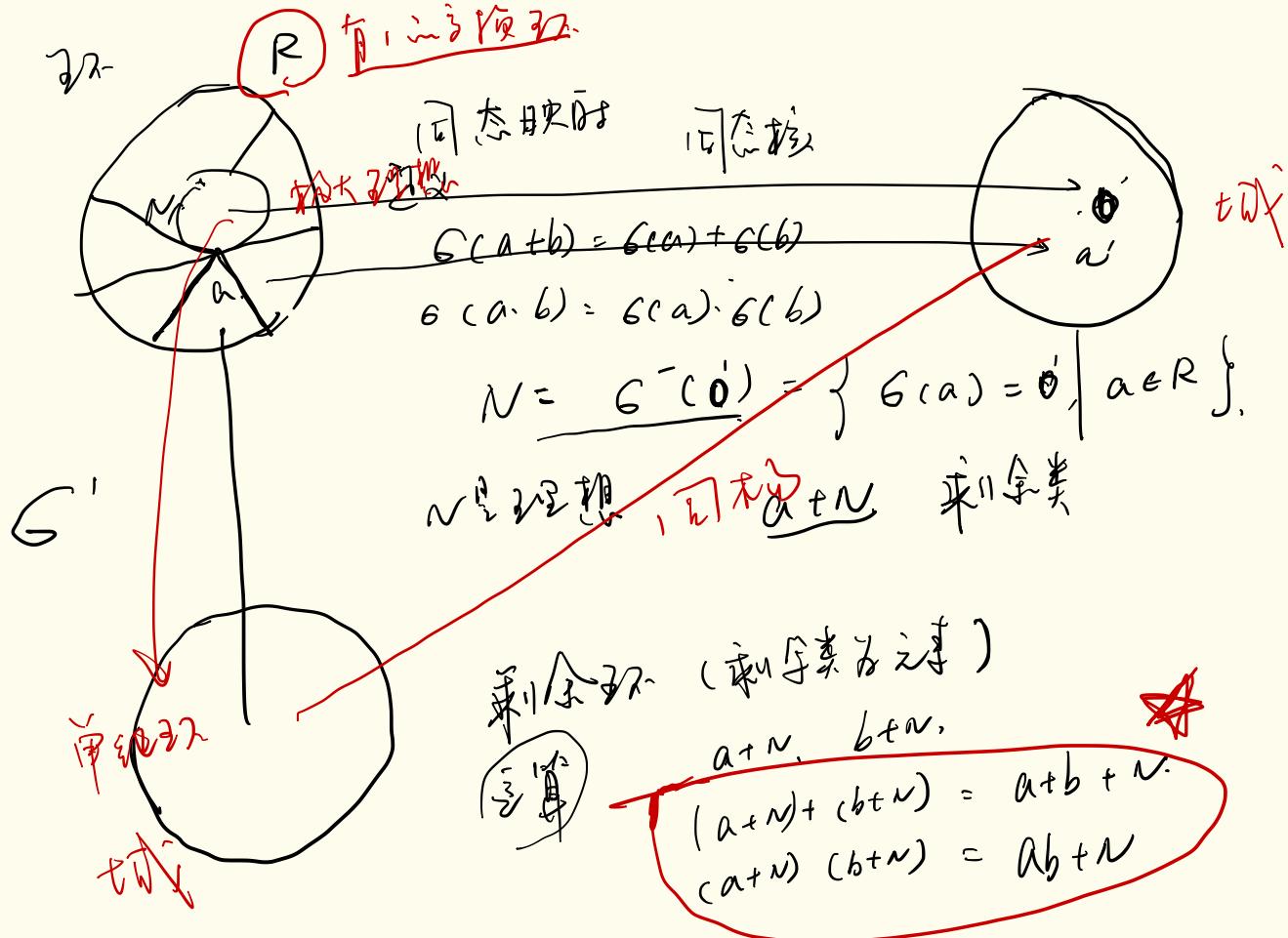
awl.

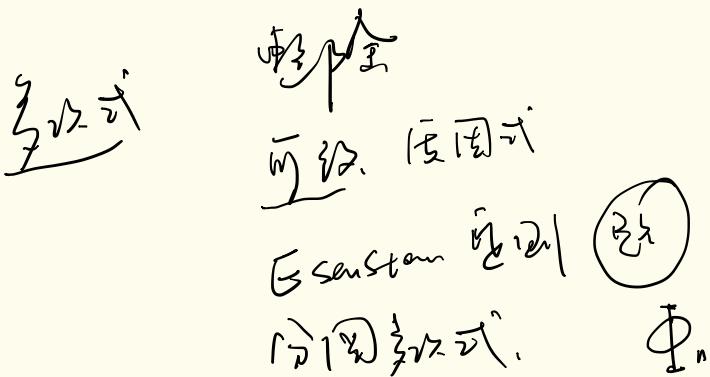
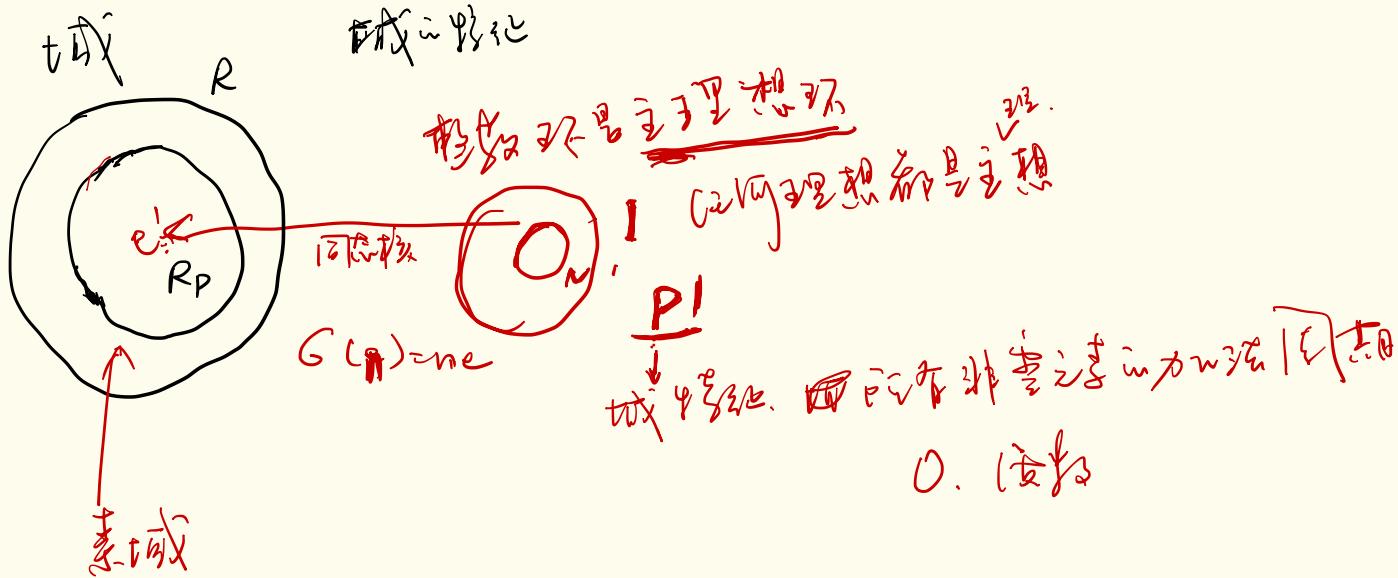
非交换

理想

$R$  有反換元  $a \in R$ .

$aR = \{ar, ra\}$





1. 由  $x^n - 1$  的因式分解.

$n > 2$  时有

$$x^n - 1 = 0.$$

由  $x^n - 1$  的因式分解.

$$\Phi(n) \cdot \Phi = (x - \varepsilon_1)(x - \varepsilon_2) \cdots (x - \varepsilon_{n-1})$$

$\Rightarrow \Phi(\varepsilon_i)$ .

由  $x^n - 1$  的因式分解.

$$\text{设 } \Phi_1 = x - 1$$

$$\Phi_3 = x^2 + x + 1$$

$$x^{n-1} = \prod_{d|n} \Phi_d(x).$$

$$\Phi_2 = x + 1$$

$$\Phi_4 = x^2 + 1$$

$$x^{24} - 1 = \Phi_1(1) \Phi_2(2) \Phi_3(3) \Phi_4(4)$$

$$\Phi_6(6) \Phi_8(8) \Phi_{12}(12) \Phi_{24}(24)$$

由  $x^n - 1$  的因式分解.

由  $x^n - 1$  的因式分解.

$n$  不是  $p$  的倍数.  $n$  是  $p$  的倍数.

$n$  是  $p$  的倍数.  $(x^k - 1)^p \rightarrow (x^q - 1)^s$

$$n = 45 \quad p = 5. \quad n = q \times 5^1$$

问题: 为什?

由  $x^n - 1$  的因式分解.



① 由  $x^n - 1$  的因式分解.

②  $n = q \times 5^1$  由  $x^n - 1$  的因式分解.

由  $x^n - 1$  的因式分解.  $n$  不是  $p$  的倍数.

$$x^n - 1$$

在域  $P_p$  上

$$\begin{matrix} x \\ x^9 \end{matrix} \rightarrow$$

$$(P_3)$$

$$\frac{x^3}{(x-1)^9} = \frac{1}{x^9 P^m}$$

$$\frac{x^9}{q+1 P^m}$$

題目

去掉 0,  $x^{q-1} \rightarrow 0.$

$\Rightarrow \varphi(q-1).$

$\Phi_{q-1}$ .

$R_p[x]$  上的零次式

$\Phi_{q-1}$ .  $R_p$  上的一个不可约因式

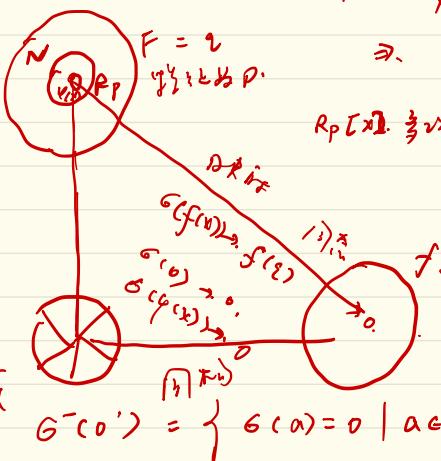
$\varphi(x)$ ,  $f(x)$ ,  $\epsilon$  成立.



$\chi^m$  的一个零次式

由  $\chi^m$  是不可约的  
且  $P^m$  不是

剩  
下



$P(x)$   $R_p$  上成  $P(x)$  与  $f(x)$  相通.

$$\Rightarrow \frac{R_p(x)}{\varphi(x) f_p(x)}$$

證明. ①  $F$  中元素必為  $p^m$  的倍數

②  $R_{p^n}$   $F_{p^m}$ .  $n \mid m$

$$\textcircled{3} \quad f^{m-1} \mid f^n - 1$$

④  $F$  中元素為  $n$  個.  $R_{p^n}$  有  $n$  個互質的元素  $\epsilon$  使得  $\epsilon^m \equiv 1$   
即  $\epsilon^{p^m-1} \equiv 1$

極点の定義

$$\textcircled{1} \quad q(x) = x^3 \quad p=3 \quad m=2$$

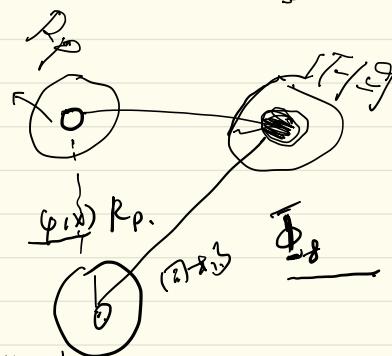
$$x^8 - 1 = \Phi_1 \Phi_2 \Phi_4 \Phi_8$$

$$\Rightarrow \Phi_1 = \frac{x^8 - 1}{(x+1)(x-1)(x^2+1)} = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1$$

$$4(x) \text{ は } 2\sqrt{2} \neq 2$$

$$\text{左側} \quad \cancel{(x^2 - x - 1)} \quad (x^2 + x - 1)$$

$$\frac{x^2 + x + 1}{1 \quad 0} \quad \textcircled{1}$$



$$\therefore R_3 \quad (\psi_1(x) R_3(x))$$

$$\text{が } \psi_1(x) \text{ は } \frac{1}{2}\pi \text{ の}$$

$$\frac{a_1 x + b_1}{2} \quad \stackrel{\circlearrowleft}{\frac{1}{2}}$$

$$\Rightarrow \left\{ \begin{array}{l} \bar{1}, \bar{2}, \bar{0}, \bar{x}+1, \bar{x}+2 \\ \bar{2x}, \bar{2x}+1, \bar{2x}+2, \dots \end{array} \right\}$$

$$\therefore \bar{x} = \varepsilon. \quad \text{R.1 } q(\bar{x}) \text{ は } \begin{cases} \bar{1}, \bar{2}, \bar{0}, \bar{\varepsilon}+1, \bar{\varepsilon}+2, \bar{2\varepsilon}, \bar{2\varepsilon}+1 \\ \bar{2x}+2, \dots \end{cases}$$

$$\text{入元方程式} \quad (x^3 + x^2 + 1)(x^2 + x + 1)$$

$$f(z) = P(z) Q(z) \text{ で } (x^2 - x - 1)(x^2 + x + 1)$$

$$16 \text{ 番目 } P(z) Q(z) \quad (x^4 + x^3 + 1)(x^4 + x + 1)$$

positive  $\varepsilon$   
 $\{ \bar{1}, \bar{2}, \varepsilon, \varepsilon+1, \varepsilon+2, 2\varepsilon, 2\varepsilon+1 \}$   
 $2\varepsilon+2, 0 \}$

$\varepsilon$	0	1	-1	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
0	0	1	-1	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
1	1	-1	0	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
-1	-1	0	1	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon+2$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon+1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+2$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon-1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon+1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon-1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon+1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon-1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$

$\varepsilon$	0	1	-1	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
0	0	0	0	0	0	0	0	0	0
1	1	1	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon-1$
-1	1	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon+2$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon+1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+2$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon-1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon+1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon-1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$
$\varepsilon$	$\varepsilon$	$\varepsilon-1$	$\varepsilon+1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$	$\varepsilon$	$\varepsilon+1$	$\varepsilon-1$

$$\begin{array}{c}
 \textcircled{-} \\
 \left( \begin{array}{ccccc}
 0 & 1 & -1 & \varepsilon & \varepsilon+1 \\
 1 & 0 & 1 & \varepsilon-1 & \varepsilon \\
 -1 & 1 & 0 & \varepsilon+1 & \varepsilon-1 \\
 \varepsilon & \varepsilon-1 & \varepsilon+1 & 0 & 1 \\
 \varepsilon+1 & \varepsilon+1 & \varepsilon & -1 & 0 \\
 \varepsilon-1 & \varepsilon-1 & \varepsilon-1 & 1 & -1
 \end{array} \right) \xrightarrow{\text{row } 5 \leftrightarrow \text{row } 1} \\
 \xrightarrow{\text{row } 1 \leftrightarrow \text{row } 2} \quad \xrightarrow{\text{row } 2 \leftrightarrow \text{row } 3} \quad \xrightarrow{\text{row } 3 \leftrightarrow \text{row } 4} \quad \xrightarrow{\text{row } 4 \leftrightarrow \text{row } 5} \quad \xrightarrow{\text{row } 5 \leftrightarrow \text{row } 6}
 \end{array}$$

$$\begin{aligned}
 \varphi(x) &= \underline{x^2 + 1} \\
 (\varepsilon+1)(-\varepsilon+1) &= \underline{-\varepsilon^2 + 1}
 \end{aligned}$$

分子の次数が2より大きい場合.

$$\textcircled{1}, \quad g = 2^>, \quad \Rightarrow p=2, \quad m=3.$$

$$\Rightarrow \frac{\Phi_1}{\Phi_2}$$

$$R^1 \quad x^2 - 1 = \Phi_1 \cdot \Phi_2$$

$$\Rightarrow \frac{\Phi_1}{\Phi_2} \cdot \frac{x^2 - 1}{x - 1} = \underline{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} =$$

ここで  $\Phi_1(x)$  が  $\Phi_1$  のもとで  $R_2$  上で  $m-1$  次式であることを示す.

$$m=3, \quad \lambda \sqrt{a} \text{ が } \boxed{x^3 + x + 1} \quad a x^3 + b x^2 + c x + 1$$

$$\Phi_1(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$$

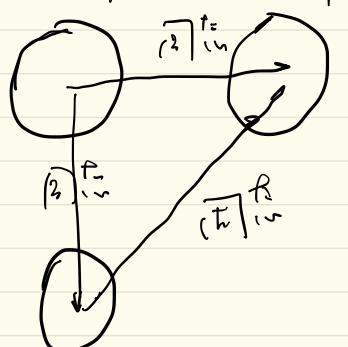
$$= \underline{x^6 + x^5 + x^3} + \underline{x^6 + x^5 + x^3} + \underline{x^2 + x} + \underline{x + 1}$$

$$= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\therefore \frac{R_p(x)}{\Phi(x) R_p(\Phi)} = \left\{ \frac{a_0 + a_1 x + a_2 x^2}{\underset{i}{\overset{i}{\underset{i}{|}}}} \mid a_0, a_1, a_2 \in R_2 \right\}.$$

$$= \left\{ \overline{0}, \overline{1}, \overline{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x+1}, \overline{x^2+x} \right\}$$

$$\text{ゆえに } z = \overline{x} \Rightarrow \{ 0, 1, z, z+1, z^2, z^2+1, z^2+z+1, z^2+z \}$$



( $\forall$ )  $a \rightarrow b$  是半論子

$$a - b = n \in N$$