

群

- ① 结合律
 $(ab)c = a(bc)$
- ② 有单位元
 $ea = ae = a$
 $e+a = a+e = a$
- ③ 可逆
 $a \cdot a' = a'a = e$
- ④ 封闭

环

- ① 对于加法是交换群
- ② 对于乘法封闭
- ③ 满足结合律
- ④ 满足分配律
 $a(b+c) = ab+ac$

域

- ① 有单位元
- ② 每个非零元都有可逆元

从群出发定义

- ① 加法交换群
- ② 非零元乘法交换群
- ③ 分配律

判断是否子群

$\forall a, b \in H, H \leq G$
有 $a \cdot b^{-1} \in H$

是否子除环

$\forall a, b \in S$
 $a \cdot b \in S, a \cdot b^{-1} \in S$

子群的陪集

$H \leq G, \forall a \in G$
 $aH = \{ah \mid h \in H\}$
左陪集

整环:

- 1) 交换环
- 2) 存在单位元
- 3) 无零因子

商群

H 在 G 中不同左(右)
陪集组成的新集合
 $G/H = \{aH \mid a \in G\}$

除环

- 1) 有非零元
- 2) 非零元构成乘法群

环理论 类似陪集

有限域例证

例 2 求 $\mathbf{F}_{2^4} = \mathbf{F}_2[x]/(x^4 + x + 1)$ 中的生成元 $g(x)$, 并计算 $g(x)^t$, $t = 0, 1, \dots, 14$ 和所有生成元.

解 因为 $|\mathbf{F}_{2^4}^*| = 15 = 3 \cdot 5$, 所以满足

$$g(x)^3 \not\equiv 1 \pmod{x^4 + x + 1}, \quad g(x)^5 \not\equiv 1 \pmod{x^4 + x + 1}$$

的元素 $g(x)$ 都是生成元.

对于 $g(x) = x$, 有

$$x^3 \equiv x^3 \not\equiv 1 \pmod{x^4 + x + 1}, \quad x^5 \equiv x^2 + x \not\equiv 1 \pmod{x^4 + x + 1},$$

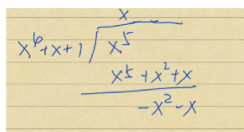
所以 $g(x) = x$ 是 $\mathbf{F}_2[x]/(x^4 + x + 1)$ 的生成元.

对于 $t = 0, 1, 2, \dots, 14$, 计算 $g(x)^t \pmod{x^4 + x + 1}$:

$$\begin{aligned} g(x)^0 &\equiv 1, & g(x)^1 &\equiv x, & g(x)^2 &\equiv x^2, \\ g(x)^3 &\equiv x^3, & g(x)^4 &\equiv x + 1, & g(x)^5 &\equiv x^2 + x, \\ g(x)^6 &\equiv x^3 + x^2, & g(x)^7 &\equiv x^3 + x + 1, & g(x)^8 &\equiv x^2 + 1, \\ g(x)^9 &\equiv x^3 + x, & g(x)^{10} &\equiv x^2 + x + 1, & g(x)^{11} &\equiv x^3 + x^2 + x, \\ g(x)^{12} &\equiv x^3 + x^2 + x + 1, & g(x)^{13} &\equiv x^3 + x^2 + 1, & g(x)^{14} &\equiv x^3 + 1. \end{aligned}$$

所有生成元为 $g(x)^t$, $(t, 15) = 1$

$$\begin{aligned} g(x)^1 &= x, & g(x)^2 &= x^2, & g(x)^4 &= x + 1, \\ g(x)^7 &= x^3 + x + 1, & g(x)^8 &= x^2 + 1, & g(x)^{11} &= x^3 + x^2 + x, \\ g(x)^{13} &= x^3 + x^2 + 1, & g(x)^{14} &= x^3 + 1. \end{aligned}$$



$$\begin{array}{r} x \\ x^4 + x + 1 \overline{) x^5} \\ \underline{x^4 + x^2 + x} \\ -x^2 - x \end{array}$$

椭圆曲线

$$x^2 \equiv 2 \pmod{401}$$

$$x^2 + y^2 = p \pmod{p} ?$$

二次拟系数

$$\left(\frac{2}{401} \right)$$

不可约多项式

$$2^6 + 2^4 + 1$$

$$64 + 16 + 1$$

$$2^6 \quad 64$$

$$+ 16$$

$$\hline 80$$

27 m

$$\frac{1}{8} \cdot \frac{1}{2} \cdot 81$$

$$(11) \quad (8+4+1)$$

$$(2+4)(2)+1$$

$$(8+4)+1$$

$$(12+1)13$$

$$(8+3)$$

$$6+$$

$$\begin{array}{r} 13 \overline{) 81} \\ 2 \end{array} \quad \begin{array}{r} 13 \\ \times \end{array}$$

A C B D D

(1)
(2)
(4)

(2)
(4)

不确定

C C C B D

(1)
(3)

二. (H)

1. (1) n 是奇数, 对任意 b , $b^{n-1} \equiv 1 \pmod{n}$
A. 否

5x2.

$$(2) m = 1105 = 5 \times 13 \times 17$$

$$\frac{\phi}{\phi} (a, m) = 1, (R) \quad (a, 5)(a, 13)(a, 17) = 1$$

证法2.

$$\begin{cases} a^4 \equiv 1 \pmod{5} \\ a^{12} \equiv 1 \pmod{13} \\ a^{16} \equiv 1 \pmod{17} \end{cases}$$

$$a^{\frac{1105}{\cancel{1105}}} = \begin{cases} (a^4)^{276} \equiv 1 \pmod{5} \\ (a^{12})^{92} \equiv 1 \pmod{13} \\ (a^{16})^{69} \equiv 1 \pmod{17} \end{cases}$$

$\therefore 1105$ 是合数.

3.

$$\left(\frac{3}{p}\right) = 1 \left(\frac{5}{p}\right) = 1$$

$$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{p-1}{2}} \frac{p}{3}$$

$$= (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p = 4k+1 \\ -1 & p \neq 4k+1 \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & p = 3k+1 \\ -1 & \end{cases}$$

$$\therefore \underline{(p = 3k+1) \text{ and } (p = 4k+1)}$$

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

$$\left(\frac{p}{5}\right) = \begin{cases} 1 \\ -1 \end{cases} \quad p \equiv 1 \pmod{5}$$

$$p = 5k + 1$$

$$\Leftrightarrow \begin{cases} p \equiv 1 \pmod{3} \\ p \equiv 1 \pmod{4} \\ p \equiv 1 \pmod{5} \end{cases}$$

$$p \equiv 1 \pmod{60}$$

$$p. \quad (1250) = \underline{2 \times 5^4} \quad 2, p^{\alpha} \text{ 有原根}$$

$$\varphi(1250) = 1250 \times \frac{1}{5} \times \frac{4}{5} = 500.$$

$$\therefore \frac{500}{2} = 250 \quad \frac{500}{5} = 100$$

验证. $g^{250} \neq 1$, $g^{100} \neq 1 \pmod{1250}$

从 $g=2$ 开始. 验证...

~~200~~ ~~100~~

找到 g . g^d 是原根. 则

$$(d, \varphi(m)) = 1$$

共有 $\frac{\varphi(\varphi(m))}{\varphi(500)}$

5.

$\mathbb{Z}/(p-1)\mathbb{Z}$ 是加群

有限群同构乘积类加群?

$$\mathbb{Z}/(p-1)\mathbb{Z} = \{ \overline{0}, \overline{1}, \overline{2}, \overline{3} \dots \overline{p-2} \}$$

易记明是加群

$$\mathbb{F}_p^* = \mathbb{F}_p / \{0\} = \{1, 2, 3, \dots, p-1\}$$

同构 \downarrow 为

$$f(ab) = f(a) \cdot f(b).$$

不太会

6.

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

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

$$= (1) (243)$$

7. $x^3 + x + 1$ 不可约.

证明: $GF(2)$ 不可约, 次数 ≤ 1 为

$$1, x, x+1$$

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

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

$$\begin{cases} x^3+x+1 \nmid x \\ x^3+x+1 \nmid x+1 \end{cases}$$

\therefore 不可约

$$(2) F_2^3 = F_2[x] / (x^3+x^2+1)$$

$$x^3-1 = 1$$

... ..

$$\begin{array}{r} x^6 + x^3 + x^2 + 1 \\ x^3 + x^2 + 1 \overline{) x^6 + x^3 + x^2 + 1} \\ \hline x^3 + x^2 + x^2 \end{array}$$

$$72 \quad g(x) = x$$

$$x^7 \equiv 1 \pmod{(x^3 + x^2 + 1)}$$

\therefore 是原根.

$$\begin{array}{r} x^6 + x^6 \\ x^6 + x^5 + x^3 \\ \hline x^5 + x^6 + x^3 \\ x^5 + x^6 + x^2 \\ \hline x^3 + x^2 \\ x^3 + x^2 \\ \hline \end{array}$$

$$g(x)^t \equiv 1 \pmod{(x^4 + x + 1)}$$

$$(t, 7) = 1 \quad \text{共 } \phi(7) = 6 \text{ 个}$$

$$8. \quad y^2 = x^3 + x + 2 \quad (\mathbb{F}_7) \pmod{7}$$

$$x=0 \quad \bar{y}_0$$

$$x=1 \quad y=2, 5$$

$$x=2 \quad \bar{y}_0$$

$$x=3 \quad y=2, 5$$

$$x=4 \quad y=0, 7$$

$$x=5 \quad \bar{y}_2$$

$$x=6 \quad 0, 7$$

$$12) \quad P = (1, 2) \text{ find } 2P, \quad y^2 = x^3 + x + 2$$

$$2P = P + P, \quad \begin{cases} x_1 = 1 \\ y_1 = 2 \end{cases}$$

$$\therefore x_1 = x_2$$

$$\therefore \lambda = \frac{3x_1^2 + a_4}{2y_1} = \frac{3+1}{4} = 4 \cdot 4^{-1} \pmod{7}$$

$$= 4 \times 2 \\ = 1 \pmod{7}$$

$$x_3 = \lambda - x_1 - x_2$$

$$= 1 - 1 - 1$$

$$= -1 \pmod{7}$$

$$= 6$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$= 1(1 - 6) - 2$$

$$= -7 \pmod{7}$$

$$= 0$$

$\therefore (6, 0)$