# 第8、10、11、13章

## 第8章 群

### (4)

#### Question

设 $G$ 是 $n$ 阶有限群. 证明：对任意元 $a \in G$，有 $a^n = e$.

#### Answer

**证明：**

$G$ 是 $n$ 阶有限群，设 $H$ 为 $G$ 的 $m$ 阶交换群.

由拉格朗日定理得 $m \mid n$，只需证 $a^m = e$.

设 $a_1, a_2, \cdots, a_k$ 为 $H$ 内不同元素，则 $aa_1, aa_2, \cdots, aa_k$ 也为 $H$ 内不同元素.

而 $e \cdot a_1 a_2 \cdots a_k = a_1 \cdot a_2 \cdots a_k = aa_1 \cdot aa_2 \cdots aa_k = a^k a_1 a_2 \cdots a_k$

即 $a^k = e = a^m$，得证.

### (5)

#### Question

证明：群 $G$ 中的元素 $a$ 与其逆元 $a^{-1}$ 有相同的阶.

#### Answer

**证明：**

设 $\operatorname{ord}(a) = n \neq m = \operatorname{ord}(a^{-1})$

$\therefore\ a^n = e$

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

$\therefore\ m \mid n$

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

$\therefore\ n \mid m$

从而 $n = m$，得证.

## (10)

### Question

给出 $\boldsymbol{F}_7$ 中的加法表和乘法表.

### Answer

**解：**

$\boldsymbol{F}_7 = \boldsymbol{Z}/7\boldsymbol{Z} = \{0,1,2,3,4,5,6\}.$

**加法表**

| $\oplus$ | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| **1** | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| **2** | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| **3** | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| **4** | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| **5** | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| **6** | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

**乘法表 ($\boldsymbol{F}_7^*$)**

| $\otimes$ | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| **1** | 1 | 2 | 3 | 4 | 5 | 6 |
| **2** | 2 | 4 | 6 | 1 | 3 | 5 |
| **3** | 3 | 6 | 2 | 5 | 1 | 4 |
| **4** | 4 | 1 | 5 | 2 | 6 | 3 |
| **5** | 5 | 3 | 1 | 6 | 4 | 2 |

| $\otimes$ | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| **6** | 6 | 5 | 4 | 3 | 2 | 1 |

## (11)

### Question

求出 $\boldsymbol{F}_{23}$ 的生成元.

### Answer

**解：**

23 是素数，则 $\boldsymbol{F}_{23}$ 是循环群，$\varphi(23) = 22 = 2 \times 11$.

$\text{ord}_{23}(-1) = 2, \qquad 2^{11} \equiv 1 \pmod{23} \Rightarrow \text{ord}_{23}(2) = 11, \qquad (2,\ 11) = 1$

$\therefore \text{ord}_{23}(-2) = 2 \times 11 = 22, \qquad \therefore -2(21)$ 为一个生成元.（或查原根表得 5 是 23 的一个原根，即为一个生成元）.

找 $p - 1 = 22$ 的完全剩余系，枚举得 $1, 3, 5, 7, 9, 13, 15, 17, 19, 21$ 符合条件（检验共 $\varphi(22) = \varphi(2) \times \varphi(11) = 1 \times 10 = 10$ 个，正确）

$(-2)^1 = -2 \equiv 21 \pmod{23} \quad (-2)^3 = -8 \equiv 15 \pmod{23}$

$(-2)^5 = -32 \equiv 14 \pmod{23} \quad (-2)^7 = -128 \equiv 10 \pmod{23}$

$(-2)^9 = -512 \equiv 17 \pmod{23} \quad (-2)^{13} = -8192 \equiv 19 \pmod{23}$

$(-2)^{15} = -32768 \equiv 7 \pmod{23} \quad (-2)^{17} = -131072 \equiv 5 \pmod{23}$

$(-2)^{19} \equiv 20 \pmod{23} \quad (-2)^{21} \equiv 11 \pmod{23}$

$\therefore\ \boldsymbol{F}_{23}$ 的所有生成元为 $5, 7, 10, 11, 14, 15, 17, 19, 20, 21$.

## (12)

### Question

证明：$\mathbf{Z}/n\mathbf{Z}$ 中的可逆元对乘法构成一个群，记作 $\mathbf{Z}/n\mathbf{Z}^*$.

### Answer

**证明：**

对 $\boldsymbol{Z}/n\boldsymbol{Z}$ 中任意元素均有结合律，且存在单位元.

其中任意可逆元 $a$ 满足 $a^{-1}\cdot a=a\cdot a^{-1}=e$.

则构成群.

# 第10章 环与理想

## (6)

### Question

证明集合 $\mathbf{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Z}\}$ 对于通常的加法和乘法构成一个整环.

### Answer

**证明：**

1. $\mathbf{Z}[\sqrt{2}]$ 对于加法有
$$(a+b\sqrt{2})\oplus(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$$
构成交换加群，零元为 $0$. 对任意 $(a+b\sqrt{2})$ 的负（逆）元为 $-(a+b\sqrt{2})$.
2. $\mathbf{Z}[\sqrt{2}]$ 对于乘法有
$$(a+b\sqrt{2})\otimes(c+d\sqrt{2})=(ac)+2\cdot(bd)+(ad+bc)\sqrt{2}$$
满足结合律和分配律，且满足交换律，有单位元 $1$.
3. 可以找到 $3,2+\sqrt{2}$ 为不可约元，$2=(2+\sqrt{2})(2-\sqrt{2})$ 为可约元.
4. 若 $a+b\sqrt{2}\neq 0$ 是零因子，则存在非零元 $c+d\sqrt{2}$ 使
$$(a+b\sqrt{2})\otimes(c+d\sqrt{2})=(ac+2\cdot bd)+(ad+bc)\sqrt{2}=0$$
则 $ac+2bd=0,\ ad+bc=0\Rightarrow ac^2=(-2bd)c=2ad^2\Rightarrow a(c^2-2d^2)=0.$
$\therefore\ c^2=2d^2.$
$\therefore\ c=\sqrt{2}d.$
而 $c$，$d$ 是整数，$\therefore\sqrt{2}d$ 不为整数，矛盾. $\therefore$ 无零因子.

因此 $\mathbf{Z}[\sqrt{2}]$ 对于通常的加法和乘法构成一个整环.

## (15)

### Question

设 $D$ 是无平方因数的整数. 证明集合 $\mathbf{Q}[\sqrt{D}]=\{a+b\sqrt{D}\mid a,b\in\mathbf{Q}\}$ 对于通常的加法和乘法构成一个域.

### Answer

**证明:**

1. $\mathbf{Q}[\sqrt{D}]$ 对于加法有

$$(a+b\sqrt{D})\oplus(c+d\sqrt{D})=(a+c)+(b+d)\sqrt{D}$$

   构成交换加群，零元为 $0$. 对任意 $(a+b\sqrt{D})$ 的负（逆）元为 $-(a+b\sqrt{D})$.
2. $\mathbf{Q}[\sqrt{D}]$ 对于乘法有

$$(a+b\sqrt{D})\otimes(c+d\sqrt{D})=(ac)+2\cdot(bd)+(ad+bc)\sqrt{D}$$

   $\mathbf{Q}^*[\sqrt{D}]=\mathbf{Q}[\sqrt{D}]/\{0\}$，有单位元 $1$. 对任意 $(a+b\sqrt{D})$ 的逆元为

$$(a+b\sqrt{D})^{-1}=\frac{a}{a^2-b^2D}+\big(-\frac{b}{a^2-b^2D}\big)\sqrt{D}\quad(a\neq 0,b\neq 0)$$

因此集合 $\mathbf{Q}[\sqrt{D}]=\{a+b\sqrt{D}\mid a,b\in\mathbf{Q}\}$ 对于通常的加法和乘法构成一个域.

# 第11章 多项式环

## (3)

### Question

设 $a(x)$，$b(x)$ 是数域 $\boldsymbol{F}_2$ 上的多项式，试计算 $s(x)$，$t(x)$ 使得

$$s(x)\cdot a(x)+t(x)\cdot b(x)=(a(x),b(x)).$$

① $a(x)=x^2+x+1,\ b(x)=x^8+x^4+x^3+x+1.$

② $a(x)=x^3+x+1,\ b(x)=x^8+x^4+x^3+x+1.$

③ $a(x)=x^4+x+1,\ b(x)=x^8+x^4+x^3+x+1.$

### Answer

**解:**

① $a(x) = x^2 + x + 1,\ b(x) = x^8 + x^4 + x^3 + x + 1.$

1. $b(x) = q_0(x) \cdot a(x) + r_0(x), \quad q_0(x) = x^6, \quad r_0(x) = x^7 + x^6 + x^4 + x^3 + x + 1$
2. $a(x) = q_1(x) \cdot r_0(x) + r_1(x), \quad q_1(x) = 0, \quad r_1(x) = x^2 + x + 1$
3. $r_0(x) = q_2(x) \cdot r_1(x) + r_2(x), \quad q_2(x) = x^5, \quad r_2(x) = x^5 + x^4 + x^3 + x + 1$
4. $r_1(x) = q_3(x) \cdot r_2(x) + r_3(x), \quad q_3(x) = 0, \quad r_3(x) = x^2 + x + 1$
5. $r_2(x) = q_4(x) \cdot r_3(x) + r_4(x), \quad q_4(x) = x^3, \quad r_4(x) = x + 1$
6. $r_3(x) = q_5(x) \cdot r_4(x) + r_5(x), \quad q_5(x) = x, \quad r_5(x) = 1$

$$\begin{aligned}
1 = r_5(x) &= q_5(x)(q_4(x) \cdot r_3(x) + r_2(x)) + r_3(x) \\
&= (x^4 + 1)(q_3(x) \cdot r_2(x) + r_1(x)) + (x) \cdot r_2(x) \\
&= (x)(q_2(x) \cdot r_1(x) + r_0(x)) + (x^4 + 1) \cdot r_1(x) \\
&= (x^6 + x^4 + 1)(q_1(x) \cdot r_0(x) + a(x)) + (x) \cdot r_0(x) \\
&= (x)(q_0(x) \cdot a(x) + b(x)) + (x^6 + x^4 + 1) \cdot a(x) \\
&= (x^7 + x^6 + x^4 + 1)(a(x)) + (x) \cdot b(x)
\end{aligned}$$

$$\therefore\ s(x) = x^7 + x^6 + x^4 + 1, \quad t(x) = x.$$

② $a(x) = x^3 + x + 1,\ b(x) = x^8 + x^4 + x^3 + x + 1.$

1. $b(x) = q_0(x) \cdot a(x) + r_0(x), \quad q_0(x) = x^5, \quad r_0(x) = x^6 + x^5 + x^4 + x^3 + x + 1$
2. $a(x) = q_1(x) \cdot r_0(x) + r_1(x), \quad q_1(x) = 0, \quad r_1(x) = x^3 + x + 1$
3. $r_0(x) = q_2(x) \cdot r_1(x) + r_2(x), \quad q_2(x) = x^3, \quad r_2(x) = x^5 + x + 1$
4. $r_1(x) = q_3(x) \cdot r_2(x) + r_3(x), \quad q_3(x) = 0, \quad r_3(x) = x^3 + x + 1$
5. $r_2(x) = q_4(x) \cdot r_3(x) + r_4(x), \quad q_4(x) = x^2, \quad r_4(x) = x^3 + x^2 + x + 1$
6. $r_3(x) = q_5(x) \cdot r_4(x) + r_5(x), \quad q_5(x) = 1, \quad r_5(x) = x^2$
7. $r_4(x) = q_6(x) \cdot r_5(x) + r_6(x), \quad q_6(x) = x, \quad r_6(x) = x^2 + x + 1$
8. $r_5(x) = q_7(x) \cdot r_6(x) + r_7(x), \quad q_7(x) = 1, \quad r_7(x) = x + 1$
9. $r_6(x) = q_8(x) \cdot r_7(x) + r_8(x), \quad q_8(x) = x, \quad r_8(x) = 1$

$$
\begin{aligned}
1 = r_8(x) &= q_8(x)(q_7(x)\cdot r_6(x) + r_5(x)) + r_6(x) \\
&= (x+1)(q_6(x)\cdot r_5(x) + r_4(x)) + (x)\cdot r_5(x) \\
&= (x^2)(q_5(x)\cdot r_4(x) + r_3(x)) + (x+1)\cdot r_4(x) \\
&= (x^2+x+1)(q_4(x)\cdot r_3(x) + r_2(x)) + (x^2)\cdot r_3(x) \\
&= (x^4+x^3)(q_3(x)\cdot r_2(x) + r_1(x)) + (x^2+x+1)\cdot r_2(x) \\
&= (x^2+x+1)(q_2(x)\cdot r_1(x) + r_0(x)) + (x^4+x^3)\cdot r_1(x) \\
&= (x^5)(q_1(x)\cdot r_0(x) + a(x)) + (x^2+x+1)\cdot r_0(x) \\
&= (x^2+x+1)(q_0(x)\cdot a(x) + b(x)) + (x^5)\cdot a(x) \\
&= (x^7+x^6)(a(x)) + (x^2+x+1)\cdot b(x)
\end{aligned}
$$

$$
\therefore\ s(x) = x^7 + x^6, \quad t(x) = x^2 + x + 1.
$$

③ $a(x) = x^4 + x + 1,\ b(x) = x^8 + x^4 + x^3 + x + 1.$

$$
\begin{array}{llll}
1. & b(x) = q_0(x)\cdot a(x) + r_0(x), & q_0(x) = x^4, & r_0(x) = x^5 + x^3 + x + 1 \\
2. & a(x) = q_1(x)\cdot r_0(x) + r_1(x), & q_1(x) = 0, & r_1(x) = x^4 + x + 1 \\
3. & r_0(x) = q_2(x)\cdot r_1(x) + r_2(x), & q_2(x) = x, & r_2(x) = x^4 + x + 1 \\
4. & r_1(x) = q_3(x)\cdot r_2(x) + r_3(x), & q_3(x) = x, & r_3(x) = x^3 + 1 \\
5. & r_2(x) = q_4(x)\cdot r_3(x) + r_4(x), & q_4(x) = 1, & r_4(x) = x^2 \\
6. & r_3(x) = q_5(x)\cdot r_4(x) + r_5(x), & q_5(x) = x, & r_5(x) = 1
\end{array}
$$

$$
\begin{aligned}
1 = r_5(x) &= q_5(x)(q_4(x)\cdot r_3(x) + r_2(x)) + r_3(x) \\
&= (x+1)(q_3(x)\cdot r_2(x) + r_1(x)) + (x)\cdot r_2(x) \\
&= (x^2)(q_2(x)\cdot r_1(x) + r_0(x)) + (x+1)\cdot r_1(x) \\
&= (x^3+x+1)(q_1(x)\cdot r_0(x) + a(x)) + (x^2)\cdot r_0(x) \\
&= (x^2)(q_0(x)\cdot a(x) + b(x)) + (x^3+x+1)\cdot a(x) \\
&= (x^6+x^3+x+1)(a(x)) + (x^2)\cdot b(x)
\end{aligned}
$$

$$
\therefore\ s(x) = x^6 + x^3 + x + 1, \quad t(x) = x^2.
$$

## (5)

### Question

设 $a(x),\ b(x)$ 是数域 $\boldsymbol{F}_2$ 上的多项式，试计算它们的最大公因式 $(a(x), b(x))$.

① $a(x) = x^{15} + 1,\ b(x) = x^8 + x^4 + x^3 + x + 1.$

② $a(x) = x^7 + 1,\ b(x) = x^8 + x^4 + x^3 + x + 1.$

## Answer

**解：**

① $a(x) = x^{15} + 1,\ b(x) = x^8 + x^4 + x^3 + x + 1.$

$$
\begin{array}{llll}
1. & a(x) = q_0(x) \cdot b(x) + r_0(x), & q_0(x) = x^7, & r_0(x) = x^{11} + x^{10} + x^8 + x^7 + 1 \\
2. & b(x) = q_1(x) \cdot r_0(x) + r_1(x), & q_1(x) = 0, & r_1(x) = x^8 + x^4 + x^3 + x + 1 \\
3. & r_0(x) = q_2(x) \cdot r_1(x) + r_2(x), & q_2(x) = x^3, & r_2(x) = x^{10} + x^8 + x^6 + x^4 + x^3 + 1 \\
4. & r_1(x) = q_3(x) \cdot r_2(x) + r_3(x), & q_3(x) = 0, & r_3(x) = x^8 + x^4 + x^3 + x + 1 \\
5. & r_2(x) = q_4(x) \cdot r_3(x) + r_4(x), & q_4(x) = x^2, & r_4(x) = x^8 + x^5 + x^4 + x^2 + 1 \\
6. & r_3(x) = q_5(x) \cdot r_4(x) + r_5(x), & q_5(x) = 1, & r_5(x) = x^5 + x^3 + x^2 + x \\
7. & r_4(x) = q_6(x) \cdot r_5(x) + r_6(x), & q_6(x) = x^3, & r_6(x) = x^6 + x^2 + 1 \\
8. & r_5(x) = q_7(x) \cdot r_6(x) + r_7(x), & q_7(x) = 0, & r_7(x) = x^5 + x^3 + x^2 + 1 \\
9. & r_6(x) = q_8(x) \cdot r_7(x) + r_8(x), & q_8(x) = x, & r_8(x) = x^4 + x^3 + x^2 + x + 1 \\
10. & r_7(x) = q_9(x) \cdot r_8(x) + r_9(x), & q_9(x) = x, & r_9(x) = x^4 + x + 1 \\
11. & r_8(x) = q_{10}(x) \cdot r_9(x) + r_{10}(x), & q_{10}(x) = 1, & r_{10}(x) = x^3 + x^2 \\
12. & r_9(x) = q_{11}(x) \cdot r_{10}(x) + r_{11}(x), & q_{11}(x) = x, & r_{11}(x) = x^3 + x + 1 \\
13. & r_{10}(x) = q_{12}(x) \cdot r_{11}(x) + r_{12}(x), & q_{12}(x) = 1, & r_{12}(x) = x^2 + x + 1 \\
14. & r_{11}(x) = q_{13}(x) \cdot r_{12}(x) + r_{13}(x), & q_{13}(x) = x, & r_{13}(x) = x^2 + 1 \\
15. & r_{12}(x) = q_{14}(x) \cdot r_{13}(x) + r_{14}(x), & q_{14}(x) = 1, & r_{14}(x) = x \\
16. & r_{13}(x) = q_{15}(x) \cdot r_{14}(x) + r_{15}(x), & q_{15}(x) = x, & r_{15}(x) = 1
\end{array}
$$

$$\therefore\ (a(x), b(x)) = 1.$$

② $a(x) = x^7 + 1,\ b(x) = x^8 + x^4 + x^3 + x + 1.$

$$
\begin{array}{llll}
1. & a(x)=q_0(x)\cdot b(x)+r_0(x), & q_0(x)=x, & r_0(x)=x^4+x^3+1 \\
2. & b(x)=q_1(x)\cdot r_0(x)+r_1(x), & q_1(x)=x^3, & r_1(x)=x^6+x^3+1 \\
3. & r_0(x)=q_2(x)\cdot r_1(x)+r_2(x), & q_2(x)=0, & r_2(x)=x^4+x^3+1 \\
4. & r_1(x)=q_3(x)\cdot r_2(x)+r_3(x), & q_3(x)=x^2, & r_3(x)=x^5+x^3+x^2+1 \\
5. & r_2(x)=q_4(x)\cdot r_3(x)+r_4(x), & q_4(x)=0, & r_4(x)=x^4+x^3+1 \\
6. & r_3(x)=q_5(x)\cdot r_4(x)+r_5(x), & q_5(x)=x, & r_5(x)=x^4+x^3+x^2+x+1 \\
7. & r_4(x)=q_6(x)\cdot r_5(x)+r_6(x), & q_6(x)=1, & r_6(x)=x^2+x \\
8. & r_5(x)=q_7(x)\cdot r_6(x)+r_7(x), & q_7(x)=x^2, & r_7(x)=x^2+x+1 \\
9. & r_6(x)=q_8(x)\cdot r_7(x)+r_8(x), & q_8(x)=1, & r_8(x)=1
\end{array}
$$

$$
\therefore\ (a(x),b(x))=1.
$$

## (9)

### Question

证明 $f(x)=x^8+x^4+x^3+x+1$ 是数域 $\boldsymbol{F}_2$ 上的不可约多项式，从而 $\boldsymbol{R}_{2^8}=\boldsymbol{F}_2[x]/(f(x))$ 是一个域.

### Answer

**证明：**

$\deg f=8.$

对于 $\deg p\le\frac{1}{2}\deg f=4$ 的不可约多项式，

$p(x)=x,x+1,x^2+x+1,x^3+x+1,x^3+x^2+1,x^4+x+1,x^4+x^3+1,x^4+x^3+x^2+x+1.$

经检验，对这些 $p(x)$ 均有 $p(x)\nmid f(x)$，则 $f(x)$ 为不可约多项式.

## (10)

### Question

设 $a(x)=x^6+x^4+x^2+x+1$，$b(x)=x^7+x+1$. 在 $\boldsymbol{R}_{2^8}=\boldsymbol{F}_2[x]/(x^8+x^4+x^3+x+1)$ 中计算 $a(x)+b(x)$，$a(x)\cdot b(x)$，$a(x)^2$，$a(x)^{-1}$，$b(x)^{-1}$.

### Answer

**解：**

$a(x) + b(x) = x^7 + x^6 + x^4 + x^2 \pmod{p(x)}.$

$a(x) \cdot b(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \equiv x^7 + x^6 + 1 \pmod{p(x)}.$

$(a(x))^2 = x^{12} + x^8 + x^4 + x^2 + 1 \equiv x^7 + x^5 + x^2 + 1 \pmod{p(x)}.$

$a(x)^{-1}:$

$$\begin{aligned}
p(x) &= x^2 \cdot a(x) + (x^6 + 1) \\
a(x) &= 1 \cdot (x^6 + 1) + x^4 + x^2 + x \\
x^6 + 1 &= x^2 \cdot (x^4 + x^2 + x) + x^4 + x^3 + 1 \\
x^4 + x^2 + x &= 1 \cdot (x^4 + x^3 + 1) + x^3 + x^2 + x + 1 \\
x^4 + x^3 + 1 &= x \cdot (x^3 + x^2 + x + 1) + x^2 + x + 1 \\
x^3 + x^2 + x + 1 &= x \cdot (x^2 + x + 1) + 1
\end{aligned}$$

$$\begin{aligned}
1 &= x \cdot (x \cdot (x^3 + x^2 + x + 1) + x^4 + x^3 + 1) + x^3 + x^2 + x + 1 \\
&= (x^2 + 1) \cdot (1 \cdot (x^4 + x^3 + 1) + x^4 + x^2 + x) + x \cdot (x^4 + x^3 + 1) \\
&= (x^2 + x + 1) \cdot (x^2 \cdot (x^4 + x^2 + x) + x^6 + 1) + (x^2 + 1) \cdot (x^4 + x^2 + x) \\
&= (x^4 + x^3 + 1) \cdot (1 \cdot (x^6 + 1) + a(x)) + (x^2 + x + 1) \cdot (x^6 + 1) \\
&= (x^4 + x^3 + x^2 + x) \cdot (x^2 \cdot a(x) + p(x)) + (x^4 + x^3 + 1) \cdot a(x) \\
&= (x^6 + x^5 + 1) \cdot a(x) + (x^4 + x^3 + x^2 + x) \cdot p(x)
\end{aligned}$$

$$\therefore\ a(x)^{-1} = x^6 + x^5 + 1.$$

$b(x)^{-1}:$

$$\begin{aligned}
p(x) &= x \cdot b(x) + (x^4 + x^3 + x + 1) \\
b(x) &= x^3 \cdot (x^4 + x^3 + x + 1) + x^6 + x^4 + x^3 + x + 1 \\
x^6 + x^4 + 3 + x + 1 &= x^2 \cdot (x^4 + x^3 + x + 1) + x^5 + x^4 + x^3 + x + 1 \\
x^5 + x^4 + x^2 + x + 1 &= x \cdot (x^4 + x^3 + x + 1) + 1
\end{aligned}$$

$$\begin{aligned}
1 &= b(x) + (x^4 + x^3 + x + 1)(x^3 + x^2 + x) \\
&= b(x) + (p(x) + x \cdot b(x)) \cdot (x^3 + x^2 + x) \\
&= (x^3 + x^2 + x) \cdot p(x) + (x^4 + x^3 + x^2 + 1) \cdot b(x)
\end{aligned}$$

$$\therefore\ b(x)^{-1} = x^4 + x^3 + x^2 + 1.$$

# 第13章 域的结构

## (2)

### Question

求 $\boldsymbol{F}_{2^4} = \boldsymbol{F}_2[x]/(x^4+x^3+1)$ 中的生成元 $g(x)$，并计算 $g(x)^t$，$t=0,1,\cdots,14$ 和所有生成元.

### Answer

**解：**

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

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

的元素 $g(x)$ 都是生成元.

对于 $g(x)=x$，有

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

所以 $g(x)=x$ 是 $\boldsymbol{F}_2[x]/(x^4+x^3+1)$ 的生成元.

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

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

所有生成元为 $g(x)^t$，$(t,\varphi(15))=1$.

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

## (3)

### Question

证明 $x^8+x^4+x^3+x+1$ 是 $\boldsymbol{F}_2$ 上的不可约多项式，从而 $\boldsymbol{F}_2[x]/(x^8+x^4+x^3+x+1)$ 是一个 $\boldsymbol{F}_{2^8}$ 域.

### Answer

**证明：**

$\because$ $\boldsymbol{F}_2[x]$ 中的所有次数 $\leq 2$ 的不可约多项式为 $x, x+1, x^2+x+1$，且

$$
\begin{aligned}
x^8+x^4+x^3+x+1 &= x\cdot(x^7+x^3+x^2+1)+1 \\
&= (x+1)\cdot(x^7+x^6+x^5+x^4+x^2+x)+1 \\
&= (x^2+x+1)(x^6+x^5+x^3)+x+1
\end{aligned}
$$

$$
\begin{aligned}
\therefore x &\nmid x^8+x^4+x^3+x+1, \\
x+1 &\nmid x^8+x^4+x^3+x+1, \\
x^2+x+1 &\nmid x^8+x^4+x^3+x+1.
\end{aligned}
$$

$\therefore$ $x^8+x^4+x^3+x+1$ 是 $\boldsymbol{F}_2[x]$ 中的不可约多项式.

因此 $\boldsymbol{F}_2[x]/(x^8+x^4+x^3+x+1)$ 是一个 $\boldsymbol{F}_{2^8}$ 域.

## (9)

### Question

求出 $\boldsymbol{F}_3[x]$ 中的所有（一个）$4$ 次 $3$ 项和 $5$ 项不可约多项式。

### Answer

**解：**

对 $\boldsymbol{F}_3[x]$ 的元素数域用 $-1,0,1$ 记，先只考虑首一多项式.

1. 对 $1$ 次有 $x, x+1, x-1$.

对 $2$ 次及以上，常数项只能为 $1$ 或 $-1$，以保证不被 $x$ 整除.

2. 设 $f(x)=x^2+ax+1$，$f(1)=a-1$，$f(-1)=-a-1$.
$\therefore$ $a=\pm1$ 时分别被 $x\mp1$ 整除，只有 $f(x)=x^2+1$ 不可约.
再设 $f(x)=x^2+ax-1$，$f(\pm1)=\pm a, a=\pm1$ 时不可约，故有 $x^2+1, x^2+x-1, x^2-x-1$ 不可约.

3. 对 $3$ 次，讨论 $f(x)=x^3+ax^2+bx+1$，代入 $\pm1\Rightarrow\begin{cases}a+b-1\neq0\\a-b\neq0\end{cases}$.
列举得 $x^3-x^2+1, x^3-x^2+x+1, x^3-x+1, x^3+x^2-x+1$.
常数项为 $-1$ 对应 $x^3+x^2-1, x^3+x^2+x-1, x^3-x-1, x^3-x^2-x-1$.

4. 对 $4$ 次，不可约则不含 $1,2$ 次因子.
讨论 $f(x)=x^4+ax^3+bx^2+cx+1$，代入 $\pm1\Rightarrow\begin{cases}a+b+c-1\neq0\\-a+b-c-1\neq0\end{cases}$.
   i. 对 $3$ 项有：
   $\begin{cases}a=0\\b=-1\\c=0\end{cases}$ 或 $\begin{cases}a=0\\b=0\\c=0\end{cases}$
   得 $\begin{cases}x^4+1\\x^4-x^2+1\end{cases}$,
   常数项为 $-1$ 对应 $\begin{cases}x^4-1\\x^4+x^2-1\end{cases}$.
   除去首一限制有：
   $\pm(x^4+1),\pm(x^4-x^2+1)$,
   $\pm(x^4-1),\pm(x^4+x^2-1)$.
   ii. 对 $5$ 项有：
   $\begin{cases}a=1\\b=1\\c=-1\end{cases}$ 或 $\begin{cases}a=-1\\b=1\\c=-1\end{cases}$
   得 $\begin{cases}x^4+x^3+x^2-x+1\\x^4-x^3+x^2-x+1\end{cases}$,
   常数项为 $-1$ 对应 $\begin{cases}x^4+x^3-x^2-x-1\\x^4-x^3-x^2-x-1\end{cases}$.
   除去首一限制有：
   $\pm(x^4+x^3+x^2-x+1),\pm(x^4-x^3+x^2-x+1)$,
   $\pm(x^4+x^3-x^2-x-1),\pm(x^4-x^3-x^2-x-1)$.