习题 8.4

(5) 证明：群G中的元素 a 与其逆元 a^{-1} 有相同的阶.

证：设 $|a|=n$，则 $a^n=e$. 又 $(a^{-1})^n=(a^n)^{-1}=e^{-1}=e$.

∴ $|a^{-1}|=n$，故G中元素 a 与其逆元 a^{-1} 有相同的阶

(9) 每个循环群都是交换群.

证：设 G 为循环群 ~~|G|=n~~ 则 $G=\langle a\rangle$

设 ~~a,b,c~~ i, j, ~~是~~ 为群中任意元素，则有 $\begin{cases} i=a^{p_1}, \\ j=a^{p_2} \end{cases}$ ~~p_1, p_2~~.

则 $i\cdot j=a^{p_1}\cdot a^{p_2}=a^{p_1+p_2}=a^{p_2}\cdot a^{p_1}=j\cdot i$

则群G为交换群

(10) F_7 中的加法表和乘法表

加法表：

	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：

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(11) 求 F_{23} 的生成元.

解：F_{23} 是一个素数域，对于加法构成加法群 $\langle F_{23},+\rangle$，并且群阶 $=23$，是一个素数阶群，进而是循环群，其中任意一个非单位元都是生成元.

对于乘法 $(F_{23}/\{0\},\times)$ 构成一个乘法群，群阶为22

根据原根 g 的性质 $(g^0, g^1, \cdots, g^{\varphi(23)-1})$ 构成模23的简化剩余系，22有2、11两个等因子，从2、3、5、6…中试算.

$2^2=4$, $2^{11}=1 \pmod{23}$

$3^2=9$, $3^4=12$, $3^8=6$, $3^{10}=1 \pmod{23}$

$5^2=2$, $5^4=4$ $5^8=16$, $5^{10}=9$ $5^{11}=-1 \pmod{23}$

则 5 是模23的一个原根，也为 F_{23} 的一个生成元.

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

封闭性：对于两个元素 $\forall a,b\in(\mathbb{Z}/n\mathbb{Z})^*$，我们要证明 $a\cdot b$ 也是可逆元，

∵ a,b 为可逆元 ∴ $\begin{cases}a\cdot a^{-1}\equiv 1 \pmod n\\ b\cdot b^{-1}\equiv 1 \pmod n\end{cases}$ 考虑 $a\cdot b$：$a\cdot b\,b^{-1}\cdot a^{-1}$

$=a\cdot b\cdot b^{-1}\cdot a^{-1}=1 \pmod n$，则 ab 的逆元为 $b^{-1}a^{-1}$，因此 $a,b\in(\mathbb{Z}/n\mathbb{Z})^*$

结合性：$a,b,c\in\mathbb{Z}/n\mathbb{Z}$，有 $(a\cdot b)c=a\cdot(b\cdot c)\pmod n$

单位元：存在单位元 1

可逆元：设 $a\in(\mathbb{Z}/n\mathbb{Z})^*$，则意味着 $(a,n)=1$，故 $ax+ny=1$

则在模 n 的意义下，有 $ax\equiv 1 \pmod n$，故 x 为 a 的单位元。

3.4

1) $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 6 & 1 & 5 \end{pmatrix}$

$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 1 & 2 \end{pmatrix}$ $\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 6 & 1 & 5 \end{pmatrix}$

$\sigma_1^{-1} = \begin{pmatrix} 2 & 3 & 4 & 5 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

(4) 素数阶群一定是循环群

证: 设 G 为素数阶群.

$|G| = p$, p 为素数. 由拉格朗日定理, G 的子群阶一定为 1 或 p.

则除 G 中的单位元以外, 其他非单位元生成的阶均为 p, 即 $a^p = e$.

又 $\langle a \rangle$ 阶也为 p, 则 $\langle a \rangle = G$, 故素数阶的群一定是循环群且每个非单位元都是生成元.

(7) p 为素数. 证明: $\mathbb{Z}/p^2\mathbb{Z}$ 中的可逆元对乘法构成一个循环群, 并求其阶.

$\mathbb{Z}/p^2\mathbb{Z}$ 中除了加法单位元 0 以外 $(\mathbb{Z}/p^2\mathbb{Z})/\{0\}$ 含有 p^2-1 个元.

设 a、b 为 $(\mathbb{Z}/p^2\mathbb{Z})/\{0\}$ 中的两个可逆元, 则有 $a \cdot a^{-1} = e$

则 $ab \cdot b^{-1} \cdot a^{-1} = e$, 则 ab 的可逆为 $b^{-1}a^{-1}$ 即 $ab \cdot b^{-1} = e$.

满足封闭性.

又 $(ab) \cdot c = a(bc)$ 满足结合律 有乘法单位元 e. 每个元素都有可逆元.

$\mathbb{Z}/p^2\mathbb{Z}$ 中的可逆元满足 $(a, p^2) = 1$, p 为素数, 则 a 不能为 p 的倍数.

则 $G = \mathbb{Z}/p^2\mathbb{Z}/\{kp\}$ $k = 0, 1, \cdots$ 共有

其中共有 $p^2 - p$ 个元素、G 在乘法下构成一个群 $|G| = p^2 - p$

10.7.

(6) 证明集合 $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$ 对于通常加法和乘法构成一个整环。

证明：对于通常加法 $a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2}=(a_1+a_2)+(b_1+b_2)\sqrt{2}$，构成一个加法交换群，存在零元 0，$a+b\sqrt{2}$ 存在负元 $-a-b\sqrt{2}$。

对于通常乘法，$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$ 满足结合律和分配律，有单位元 1，满足交换律，假设存在零因子。

使得 $(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}=0$

即 $a_1,b_1,a_2,b_2\neq 0$，$a_1,b_1,a_2,b_2\in\mathbb{Z}$；

$$\begin{cases}a_1a_2+2b_1b_2=0\\ a_1b_2+a_2b_1=0\end{cases}\Rightarrow\begin{cases}a_1a_2=-2b_1b_2\\ a_1b_2=-a_2b_1\end{cases}\Rightarrow\begin{cases}\frac{a_1}{b_1}=-2\frac{b_2}{a_2}\\ \frac{a_1}{b_1}=-\frac{a_2}{b_2}\end{cases}$$

则有 $-2\frac{b_2}{a_2}=-\frac{a_2}{b_2}$ 则有 $a_2^2=2b_2^2$ 则 $\frac{a_2}{b_2}=\pm\sqrt{2}$，$\frac{a_1}{b_1}=\pm\sqrt{2}$，显然与 a_1,b_1,a_2,b_2 均为整数矛盾，故不存在零因子。

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

证明：$\mathbb{Q}$ 对于加法：$a_1+b_1\sqrt{D}+a_2+b_2\sqrt{D}=(a_1+a_2)+(b_1+b_2)\sqrt{D}$ 构成一个加法满交换群，存在零元 0，$a+b\sqrt{D}$ 存在负元，$-a-b\sqrt{D}$，$(a,b\in\mathbb{Q})$

$\mathbb{Q}$ 对于乘法：首先 D 为无平方因数的整数则 $\sqrt{D}$ 为无理数，

$(a_1+b_1\sqrt{D})(a_2+b_2\sqrt{D})=(a_1a_2+Db_1b_2)+(a_1b_2+a_2b_1)\sqrt{D}$ 满足结合律、分配律、交换律，有单位元 1，对于每个非零元，$a+b\sqrt{D}$ 若存在可逆元 $a'+b'\sqrt{D}$ 则满足 $(a+b\sqrt{D})(a'+b'\sqrt{D})=(aa'+Dbb')+(ab'+a'b)\sqrt{D}=1$

则有 $\begin{cases}aa'+Dbb'=1\\ ab'+a'b=0\end{cases}$ 解得一可逆元为 $\frac{a-b\sqrt{D}}{a^2-b^2D}$ 有 $(a+b\sqrt{D})\left(\frac{a-b\sqrt{D}}{a^2-b^2D}\right)=1$

其中 $a^2-b^2D\neq 0$，因为 D 为无平方因数，a,b 不同时为 0，

故 $\mathbb{Q}(\sqrt{D})$ 对于通常加法乘法构成一个域

若 $a^2-b^2D=0$ 则 $\left(\frac{a}{b}\right)^2=D$，$D$ 为有理数的平方，这与 D 为无平方因数的整数矛盾

11.8. (3) $a(x), b(x)$ 是 F_2 上多项式. 试计算 $s(x), t(x)$, 使 $s(x)a(x)+t(x)b(x)=(a(x),b(x))$

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

解: $b(x)=x^8+x^4+x^3+x+1 = (x^6+x^5+x^3)a(x)+x+1$

$2+1+0 \mid 8+4+3+1+0$; $6+5+3$

$8+6+5$

$7+6+4+3+1+0$

$7+6+5$

$5+4+3+1+0$

$5+4+3$

$1+0$.

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

$x+1=(x+1)\cdot 1+0$

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

$1 = a(x) - x(x+1)$

$= a(x) - x(b(x)-(x^6+x^5+x^3)a(x))$

$= (x^7+x^6+x^4+1)a(x) - x\,b(x)$

$s(x)=(x^7+x^6+x^4+1)$, $t(x)=x$

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

$b(x)=x^8+x^4+x^3+x+1=(x^5+x^3+x^2+1)\cdot a(x)+x^2$

$3+1+0 \mid 8+4+3+1+0$; $5+3+2+0$

$8+6+5$

$6+5+3+1+0$

$6+4+3$

$2+1+0$

$2+1+0$

$3+2+1+0$

$3+1+0$

2

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

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

$x+1=1\cdot x+1$

$1=x+1-x$

$=x+1-(x^2-x(x+1))$

$=(x+1)(x+1)-x^2$

$=[a(x)-x^2](x+1)-x^2$

$=(x+1)(a(x))-x\cdot x^2$

$=(x+1)(a(x))-x\cdot(b(x)-(x^5+x^3+x+1)a(x))$

$=(x^6+x^4+x^3+1)(a(x))-x\,b(x)$

$s(x)=(x^6+x^4+x^3+1)$

$t(x)=-x$

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

$b(x)=(x^4+x)\cdot a(x)+x^3+x^2+1$

$4+1+0 \mid 8+4+3+1+0$; $4+1$

$8+4+1$

$5+3+1+0$

$5+2+1$

$3+2+0$.

$3+2+0 \mid 1+0$; $4+3+1$

$3+0$

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

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

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

$=x^3+x^2+1-(x+1)(a(x)-(x+1)(x^3+x^2+1))$

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

$=x^2(b(x)-(x^4+x)\cdot a(x))-(x+1)a(x)$

$=x^2\cdot b(x)-(x^6+x^3+x+1)a(x)$

$s(x)=x^2$

$t(x)=x^6+x^3+x+1$

用辗转相除法求 $(a(x), b(x))$. $a(x)=x^{15}+1$, $b(x)=x^8+x^6+x^3+x^2+1$

$15+3+2+1$ | $8+4+3+2+0$ | $7+0$

$15+11+10+9+7$

$11+10+9+7+0$ | $7+3+2+1$ | $3+0$

$11+7+6+5+3$

$10+9+6+5+3+0$ | $8+5+4+3+2+0$ | $5+2+1+0$

$10+6+5+4+2$

$8+4+3+2+0$ | $8+5+4+3+1$ | $5+2+1+0$

$5+2+1+0$ | $5+2+1+0$ | 1

$a(x)=(x^7+x^3+x^2+x)\cdot b(x)+x^3+x^2+x+1$

$b(x)=(x^3+1)\cdot(x^5+x^2+x+1)+1$

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

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

② $a(x)=x^7+1$, $b(x)=x^8+x^6+x^3+x+1$

$7+0$ | $1+x$ | $8+x+3+1+0$

$8+1$

$4+3+0$ | $2+2+1+0$ | $4+3+0$

$7+0$ | $7+6+3$

$6+3+0$ | $6+5+2$

$5+3+2+0$ | $5+4+1$

$4+3+2+1+0$ | $4+3+0$ | $2+1$

$b(x)=x\cdot a(x)+x^6+x^3+1$

$a(x)=(x^3+x^2+x+1)\cdot(x^4+x^3+1)+x^2+1$

$x^4+x^3+1=(x^2+x+1)(x^2+1)+x$

$2+1+0$ | $4+3+0$ | $4+2$

$3+2+0$ | $3+1$

$2+1+0$ | $2+0$ | 1

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

故 $(a(x), b(x))=1$

证明：$f(x)=x^8+x^4+x^3+x+1$ 为数域 F_2 上的不可约多项式. 只需对 $\deg \le 4$ 的不可约多项式进行试除，即对 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, $x^4+x^3+x^2+x+1$ 进行试除，结果发现均不可整除

则 $f(x)=x^8+x^4+x^3+x+1$ 为数域 F_2 上的不可约多项式

则 $F_2[x]/f(x)$ 确为域. 证毕.

1101. 设 $a(x) = x^6 + x^4 + x^2 + x + 1$　$b(x) = x^7 + x + 1$.

在 $R_2^8 = F_2[x]/(x^8 + x^4 + x^3 + x + 1)$ 中计算 $a(x) + b(x)$, $a(x) \cdot b(x)$.

$a(x)^2$, $a(x)^{-1}$, $b(x)^{-1}$

解: $a(x) + b(x) = x^7 + x^6 + x^4 + x^2$

$a(x) \cdot b(x) = x^{13} + x^7 + x^6 + x^{11} + x^5 + x^4 + x^9 + x^3 + x^2 + x^8 + x^2 + x + x^7 + x + 1$

$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 = x^7 + x^6$.

$5+3$
$8+4+3+1+0 \mid 13+11+9+8+6+5+4+3$
$13+9+8+6+5$
$11+4+3$
$11+7+6+4+3$
$7+6$

$a(x)^2 = x^{12} + x^8 + x^4 + x^2 + 1$

$= x^7 + x^5 + x^2 + 1$

4
$8+4+3+1+0 \mid 12+8+4+2+0$
$12+8+7+5+4$
$7+5+2+0$

$9+7+5+3$
$+8+6+4+2$
$1+0$
$8+4+3+1+0 \mid 9+8+7+6+5+4+3+2$
$9+5+4+2+1$
$8+7+6+3+1$
$8+4+3+1+0$
$7+6+4+2+1+0$

$x^8 + x^4 + x^3 + x + 1 = (x^6 + x^4 + x^2 + x + 1)(x^2+1) + x^4$

$2+0$
$6+4+2+1+0 \mid 8+4+3+1+0$
$8+6+4+3+2$
$6+2+1+0$
$6+4+2+1+0$
4

$x^6 + x^4 + x^2 + x + 1 = (x^2+1) \cdot x^4 + x^2 + x + 1$

$x^4 = (x^2+x)(x^2 + x + 1) + x$

$2+1$
$2+1+0 \mid 4$
$4+3+2$
$3+2$
$3+2+1$

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

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

$= (x^2 + x + 1) - (x+1)(x^4 - (x^2+x)(x^2 + x + 1))$

$= (x^3 + x + 1)(x^2 + x + 1) - (x+1) x^4$

$\therefore a(x)^{-1} = (x^5 + x^3 + x^2 + x + 1)$

$x^8 + x^4 + x^3 + x + 1 = x \cdot (x^7 + x + 1) + x^4 + x^3 + x^2 + 1$

$= (x^3 + x + 1)(x^6 + x^4 + x^2 + x + 1) - (x^2+1) x^4)$

$- (x+1) x^4$

$x^7 + x + 1 = (x^3+x^2+x)(x^4 + x^3 + x^2 + 1) + x$

$3+2+1$
$4+3+2+0 \mid 7+1+0$
$7+6+5+3$
$6+5+3+1+0$
$6+5+4+2$
$4+3+2+1+2$

$(x^4 + x^3 + x^2 + 1) = (x^3 + x^2 + x) \cdot x + 1$

$= (x^3 + x + 1)(x^6 + x^4 + x^2 + x + 1) - (x^5 + x^2) \cdot x^4$

$1 = x^4 + x^3 + x^2 + 1 - (x^3 + x^2 + x) \cdot x$

$= (x^3 + x + 1)(x^6 + x^4 + x^2 + x + 1) - (x^4+x^2)(x^8 + x^4 + x^3 + x + 1 - (x^6 + x^4 + x^2 + x + 1))$

$= (x^4 + x^3 + x^2 + 1) - (x^7 + x + 1 - (x^3 + x^2 + x)(x^4 + x^3 + x^2 + 1))(x^3 + x^2 + x)$

$= (x^5 + x^3 + x^2 + x + 1)(x^6 + x^4 + x^2 + x + 1) - (x^5 + x^2)(x^8 + x^4 + x^3 + x + 1)$

$= (x^6 + x^4 + x^2 + 1)(x^4 + x^3 + x^2 + 1) - (x^3 + x^2 + x)(x^7 + x + 1)$

$= (x^6 + x^4 + x^2 + 1)(x^8 + x^4 + x^3 + x + 1 - x(x^7 + x + 1)) - (x^3 + x^2 + x)(x^7 + x + 1)$

$= (x^6 + x^4 + x^2 + 1)(x^8 + x^4 + x^3 + x + 1) - (x^3 + x^2)(x^4 + x^4 + x^2 + 1)(x^7 + x + 1)$

$\therefore b(x)^{-1} = x^7 + x^6 + x^4 + x^3 + \dots$

13.5 求 $F_2[x]/(x^4+x^3+1)$ 中生成元 $g(x)$，并计算 $g(x)^t$, $t=0,1,\cdots,14$.

加法的有生成元。$2^4-1=15$ 次方，有许因子 3、5：

设 $g_1(x)=x$, $g_1(x)^3=x^3$ 非 $|g_1(x)^5=x^5=x^3+x+1$ 非 $|$

$$\begin{array}{r|l} & x+1 \\ \hline x^4+x^3+1 & x^5 \\ & x^5+x^4+x \\ \hline & x^4+x \\ & x^4+x^3+1 \end{array}$$

故 $g_1(x)=x$ 是生成元，

$g(x)^0=1$ $g(x)^1=x$, $g(x)^2=x^2$, $g(x)^3=x^3$, $g(x)^4=x^3+1$.

$g(x)^5=x^3+x+1$, $g(x)^6=x^3+x^2+x+1$ $g(x)^7=x^2+x+1$.

$g(x)^8=x^3+x^2+x$ $g(x)^9=x^2+1$ $g(x)^{10}=x^3+x$. $g(x)^{11}=x^3+x^2+1$

$g(x)^{12}=x+1$ $g(x)^{13}=x^2+x$ $g(x)^{14}=x^3+x^2$

$\varphi(15)=\varphi(3)\times\varphi(5)=2\times 4=8$，共有8个生成元，

结论：$g_1(x)=x$, $g_2(x)=x^2$, $g_3(x)=x^3+1$, $g_4(x)=x^2+x+1$.

$g_5(x)=x^3+x^2+x$, $g_6(x)=x^3+x^2+1$, $g_7(x)=x^2+x$. $g_8(x)=x^3+x^2$

证：要证 $x^8+x^4+x^3+x+1$ 是 $F_2[x]$ 中的不可约多项式，

即证 当 $\deg\le 4$ 时，对于所有的不可约多项式进行试除，

即 对，x, x^2+1, x^3+x+1, x^3+x^2+1, x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$ 试除，发现 均不可整除，则 $x^8+x^4+x^3+x+1$ 是不可约多项式，从而 $F_2[x]/(x^8+x^4+x^3+x+1)$ 是一个 F_{2^8} 域。