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。