1. 设$G=\{a,b,c,d\}$，在 G 上定义的二元运算$*$如下表,

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(1) 证明$\langle G,*\rangle$是一个群；并找出幺元，及每个元素的逆元。

(2) 判断$\langle G,*\rangle$是否为循环群，若是，则指出该循环群的生成元。

（1） 显然运算是封闭的、可结合的。a 为幺元，b、c、d 的逆元分别为 d、c、b. 所以$\langle G,*\rangle$是一个群。

(2) $\langle G,*\rangle$是循环群，生成元为 b，d.

2. 设$Z_6=\{0,1,2,3,4,5\},+_6$为模 6 加法，即$i+_6 j=(i+j)mod\ 6$, 其中$+$是普通加法运算。

(1) 证明$\langle Z_6,+_6\rangle$是一个循环群，并找出生成元。

(2) 判断$\langle Z_6,+_6\rangle$是否有 4 阶子群，并说明理由。

(1) 显然运算是封闭的；

由于$(x+_6 y)+_6 z=x+_6(y+_6 z)=(x+y+z)mod\ 6$, 所以运算$+_6$是可结合的；

由于对于任意$x\in Z_6, x+_6 0=0+_6 x=x$，所以存在幺元 0；

2 和 4 互为逆元，1 和 5 互为逆元，3 的逆元是自身，所以$\langle Z_6,+_6\rangle$是一个群。经验证，1 是$\langle Z_6,+_6\rangle$的生成元，因此$\langle Z_6,+_6\rangle$是一个循环群。生成元为 1,5.

(2) $\langle Z_6,+_6\rangle$的阶为 6，由拉格朗日定理，子群的阶数应该整除群的阶数，4 不能整除 6，因此没有 4 阶子群。

3. 已知$G=\{1,2,3,4\}$， $\times_5$为模 5 乘法,即$i\times_5 j=(i\cdot j)mod\ 5$, 其中$\cdot$是普通乘法运算，

(1) 证明$\langle G,\times_5\rangle$是一个群；并找出幺元，及每个元素的逆元；

(2) 判断$\langle G,\times_5\rangle$是否为循环群；若是，则指出该循环群的生成元。

(1) 证明：显然运算是封闭的；

由于$(x\times_5 y)\times_5 z=x\times_5(y\times_5 z)=(x\cdot y\cdot z)mod\ 5$, 所以运算$\times_5$是可结合的；

由于对于任意$x \in G, 1 \times_5 x = x \times_5 1 = x$，*所以存在幺元* 1；

2 和 3 互为逆元，1 和 4 的逆元是自身，所以$\langle G, \times_5 \rangle$是一个群

(2) $\langle G, \times_5 \rangle$是循环群，生成元是 2，3。

4. 设$G = \{a, b, c, d\}$，在 G 上定义的二元运算$*$如下表,$\langle G, * \rangle$是群，

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

(1) 找出群的幺元，逆元，并说明理由；

(2) 判断$\langle G, * \rangle$是否为循环群；若是，则指出该循环群的生成元。

(1) 由于对于任意$x \in G, a * x = x * a = x$，*所以幺元为*$a$；

由于$c * d = d * c = a$，$a * a = b * b = a$,所以 c 和 d 互为逆元，a 和 b 的逆元是自身

(2) 判断$\langle G, * \rangle$是否为循环群；若是，则指出该循环群的生成元。

是循环群。

$c = c^1, b = c * c = c^2, d = b * c = c^3, a = d * c = c^4,$

$d = d^1, b = d * d = d^2, c = b * d = d^3, a = c * d = d^4$

所以 c 和 d 是生成元

5. 设$G = \{a, b, c\}$，在 G 上定义的二元运算$*$如下表：

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(1) 证明$\langle G, * \rangle$是一个群；

(2) 判断$\langle G, * \rangle$是否为循环群，若是，则指出该循环群的生成元。

(1) 由运算表可知，$*$运算在 G 上是封闭的；因为$\forall x, y, z \in G, (x * y) * z = x * (y * z)$，所以$*$运算在 G 上可结合的；根据运算表，$a$为 G 中关于$*$运算的幺元；$b, c$

互为逆元。因此⟨G, ∗⟩是一个群。

(2) ⟨G, ∗⟩是循环群，生成元为b或者c.

6. $\mathcal{P}$(A)是有限集合A的幂集，证明< $\mathcal{P}$(A),⊕>是群

① $\oplus$在$p(A)$上是封闭的.

即$\forall A_1, A_2 \in p(A)$. $A_1 \oplus A_2 \in p(A)$

② $\oplus$在$p(A)$上是可结合的.

即$\forall A_1, A_2, A_3 \in p(A)$

$(A_1 \oplus A_2) \oplus A_3 = A_1 \oplus (A_2 \oplus A_3)$

③ 存在幺元 ϕ

即$\forall A_1 \in p(A)$，$A_1 \oplus \phi = \phi \oplus A_1 = A_1$

④ $\forall A_1 \in p(A)$，存在逆元 A_1

∴ $< p(A), \oplus >$ 是群.