p365

1.

证明:
∀(a,b), (c,d), (e,f) ∈ S,
((a,b) o (c,d)) o (e,f) = (ac,ad + b) o (e, f) = (ace,acf + ad + b),
(a,b) o ((c,d) o (e,f)) = (a,b) o (ce, cf + d) = (ace, acf + ad +b),
即((a,b) o (c,d)) o (e,f) = (a,b) o ((c,d) o (e,f))所以 o 运算在 S 上满足结合律。 故(S,o)是半群。
∀(a,b) ∈ S, (a,b) o (1,0) = (a,b), (1,0) o (a,b) = (a,b), 因此(1,0)是 (S,o)的幺元。 ∀(a,b) ∈ S, (1/a,a - b/a) o (a,b) = (1,0),故对于每个 S 中元素, 都存在左逆元。
故由群的定义知, (S,o)构成群。

2.

∀a,b∈ Un,an = 1, bn = 1 所以$(ab)n$ = 1, 所以 ab∈ Un, 满足运算封闭性, 且复数运算满足 结合律, 所以Un是一个半群, 1 是Un的幺元, 每个元素的逆元为本身的 n-1 次方幂, 所以 Un对通常的复数乘法构成一个群

5.

证明:
设 G 中矩阵从左到右依次为 A_1, A_2, A_3, A_4,则它们在矩阵乘法上得到的结果为

矩阵乘法	A_1	A_2	A_3	A_4
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_1	A_4	A_3
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_3	A_2	A_1

由此可见,矩阵乘法在 G 上封闭,并且满足结合律,具有幺元(A_1),每个元素都有逆元,故 G 对矩阵乘法是一个群。

P369

1.

证明:
abab = $(ab)_2$ =a_2b_2 = aabb,由群 G 满足消去律知, ba = ab。

2.

证明：
$\forall a,b \in G$，$(ab)(ab) = e = aa$,根据消去律，$bab = a$。故
$bbab = ba$，而 $bbab = eab = ab$，故 $ba = ab$。即$\forall a,b \in G$，$ab = ba$，因此群
G 是交换群。

3.

证明:令 G 为四阶群,令 G={a,b,c,e},其中 e 是 G 中的幺元,任取 G 中一个非幺元元素,不妨设为 a　则对于非幺元元素 b，令 ab=c,ba=e　设 b 不是 a 的逆元,若 a 为 a 的逆 aa=e 因为 ba=e,a=b，与假设矛盾　若 C 是 a 的逆元,ca=e,ba=e,b=c，也矛盾，所以 b 是 a 的逆元，故 ab=ba:所以 G 是交换群。

4.

证明：
设 O（G） >2，(G,o)是非交换群。e 是其上的幺元。假设$\forall a \in G$，$a \circ a = e$，
则$\forall a,b \in G$ 且 a，$b \neq e$，$(a \circ b) \circ (a \circ b) = e = e \circ e = a \circ a \circ b \circ b$，由群满足的
消去律知，$b \circ a = a \circ b$，即(G,o)是交换群，与已知矛盾。因此$\exists a \in G$，$a \circ a \neq e$，即 $a \neq a^{-1}$，因此$\exists a,a^{-1} \in G$ 使得 $a,a^{-1} \neq e$ 且 $a \neq a^{-1}$，此时 $a \circ a^{-1} = a^{-1} \circ a$。故对于非交换的阶大于 2 的群，必有两个非单位元的运算可交换。

5.

证明：
设（G,o） 是有限群，幺元为 e。设 $M = \{x|O(x) > 2, x \in G\}$，$\forall a \in M$，有 $a^n = e$，$n > 2$，而 $a^n = a^{n-1} \circ a = e$，即 $a^{n-1} = a^{-1}$。若 $a^{n-1}=a$，则 $a \circ a = e$ 即 $O(e) = 2$，与 $O(a) > 2$ 矛盾，因此 a^{n-1} 与 a 不相等，在 M 中是互异的元素。
设 $b = a^{n-1}$，则 $b \circ a = e$，也就是说 $a = b^{-1}$。而 $a^{n+1} = a^n \circ a = e \circ a = a$。取
$k = (n-1)(n-1) = (n-2)n + 1$,则 $a^k = b^{n-1}$。而 $a^k = a^{(n-2)n+1} = e^{(n-2)} \circ a = a$，故
$b^{n-1} = a$，即 $b \circ b^{n-1} = e$,故 $O(b) \leq n$。由于 n-1>1，故 $O(b) > 2$，因此 $b \in M$。由此可知，若有某个元素属于 M，则与其互异的其逆元素也必定属于 M，因此 M 中的元素可以划分成对，故 M 中元素必定为偶数。

6.

证明：
由题 5 的证明，可知有限群中阶大于 2 的元素个数必为偶数。偶数阶的群必为有限群，故可使用此结论。由于幺元 e 不在阶大于 2 的元素之集合中，且 $O(e) = 1$，故 e 不在阶为 2 的元素之集合中。偶数阶的群除去幺元和阶大于 2 的元素，剩余元素即为阶为 2 的元素。由于阶大于 2 的元素个数为偶数，幺元仅有一个，故剩余元素的个数为偶数-偶数-1，为奇数。

7.

证明：
a 为幺元时，结论显然成立。 a 不为幺元时， 由阶的定义知 $m \geq n$。假设 n 不能整除 m， 则 $m = kn + c$， 其中 $k \in N_+$， $c \in \{1,2,\dots,n-1\}$， 此时 $a^m = (a^n)^k a^c = e^k a^c = a^c$，而 $c<n$， $O(a) = n$，故 $a^c \neq e$，因此 $a^m = a^c \neq e$，这与已知条件矛盾，因此假设不成立， n 可以整除 m。

8.

证明：
偶数阶群满足第六题的条件，故可用第 6 题的结论。根据第六题结论， 偶数阶群的阶为 2 的元素个数为奇数，这说明阶为 2 的元素个数至少为 1，故至少存在一个阶为 2 的元素。

9.

证明：
设 G 中幺元为 e， 设 $b_n = a_1a_2\dots a_n$， 若$\exists b_m = e$， 则取 $p = 1$， $q = m$， 符合要求； 否则， 由运算的封闭性， $b_n \in G/\{e\}$。 由鸽巢原理知， $\exists 1 \leq m_1 < m_2 \leq n$， 满足 $b_{m_1} = b_{m_2}$。等式两侧同时与$(b_{m_1})^{-1}$进行右 o 运算，则 $(b_{m_1})^{-1}b_{m_1} = (b_{m_1})^{-1} b_{m_2}$ 即 $e = a_{m_1}^{-1}\dots a_2^{-1}a_1^{-1}a_1a_2\dots a_{m_2} = a_{m+1}a_{m+2}\dots a_n$。 因此取 $p = m+1$， $q = n$，符合要求。 综上所述， 总是$\exists 1 \leq p \leq q \leq n$ 使得 $a_p\dots a_q = e$。

p373

2.

假设 G1 和 G2 互相不包含，那么$\exists a \in G1$ 且$a \notin G2$，$\exists b \in G2$ 且$b \notin G1$ 那么$ab \notin G1$，$ab \notin G2$，但是$a \in G$, $b \in G$，$ab \in G$，与假设矛盾，故 G1 和 G2 互相包含，$G1 \subseteq G2$ $G2 \subseteq G1$。

5.

证明：
设 $\varphi^{-1}(e_2) = M$， e_1 为 G_1 的幺元。 对于$\forall a \in G_1$， $\varphi(a) * \varphi(e_1) = \varphi(a \circ e_1) = \varphi(a)$， 故 $\varphi(e_1) = e_2$， 故 $e_1 \in M$。 对于$\forall a,b \in M$， $\varphi(a \circ b) = \varphi(a) * \varphi(b) = e_2 * e_2 = e_2$， 故 $a \circ b \in M$， 因此 $\circ$ 在 M 上运算封闭。 由于 $M \subseteq G_1$， G_1 是群满足结合律， 故 M 是半群。 由于 $e_1 \in M$， 故 M 中有幺元 e_1。
对$\forall a \in M$， 设其在 G_1 中的逆元为 a^{-1}， 则 $\varphi(a) * \varphi(a^{-1}) = \varphi(a \circ a^{-1})$， 亦即 $e_2 * \varphi(a^{-1}) = \varphi(e_1) = e_2$， 故 $\varphi(a^{-1}) = e_2$， 故 $a^{-1} \in M$。 由于 $a^{-1} \circ a = a \circ a^{-1} = e_1$， 故 M 中存在 a 的逆元。 于是 M 是群。 由于 $M \subseteq G_1$， 故 M 是 G 的子群。

8.

证明：
设三阶群 G = {1,2,3}。 sym(S)={$\varphi_1 \ldots \varphi_6$}， 其中
(1 2 3/1 2 3) (1 2 3/ 1 3 2) (1 2 3/ 2 1 3) (1 2 3/2 3 1) (1 2 3/ 3 1 2) (1 2 3 / 3 2 1)则 sym(S)的全部子群如下：
{φ_1}、 {φ_1， φ_2}、 {φ_1， φ_3}、 {φ_1， φ_4}、 {Φ_1， φ_5， φ_6}、
{φ_1、 φ_2、 φ_3、 φ_4、 φ_5、 φ_6}