# 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 A1， A2， A3， A4，则它们在矩阵乘法上得到的  
结果为

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 矩阵乘法 | A1 | A2 | A3 | A4 |
| A1 | A1 | A2 | A3 | A4 |
| A2 | A2 | A1 | A4 | A3 |
| A3 | A3 | A4 | A1 | A2 |
| A4 | A4 | A3 | A2 | A1 |

由此可见，矩阵乘法在 G 上封闭，并且满足结合律，具有幺元（A1），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 =a2b2 = aabb,由群 G 满足消去律知， ba = ab。

# 2.

证明：  
∀a,b∈ G， (ab)(ab) = e = aa,根据消去律， bab = a。 故  
bbab = ba， 而 bbab = eab = ab， 故 ba = ab。 即∀a,b∈ 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中的么元,任取G中一个非么元元素,不妨设为a 则对于非么元元素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∀a∈ G， a o a = e，  
则∀a,b∈ G 且 a， b≠e， (a o b) o( a o b) = e = e o e = a o a o b o b， 由群满足的  
消去律知， b o a = a o b， 即(G,o)是交换群， 与已知矛盾。 因此∃a∈ G， a o a ≠  
e， 即 a ≠ a-1， 因此∃a,a-1∈ G 使得 a,a-1≠e 且 a ≠ a-1， 此时 a o a-1 = a-1 o  
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∈ G}， ∀a∈ M， 有 an  
= e， n > 2，而 an = an-1 o a = e，即 an-1 = a-1。 若 an-1=a，则 a o a = e 即 O(e)  
= 2，与 O(a) >2 矛盾，因此 an-1 与 a 不相等，在 M 中是互异的元素。  
设 b = an-1，则 b o a = e，也就是说 a = b-1。 而 an+1 = an o a = e o a = a。取  
k = (n-1)(n-1) = (n-2)n +1,则 ak = bn-1。而 ak = a(n-2)n + 1 = e(n-2) o a = a，故  
bn-1 = a，即 b o bn-1 = e,故 O(b) ≤ n。由于 n-1>1，故 O(b) > 2，因此 b∈  
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 ≥ n。假设 n  
不能整除 m， 则 m = kn + c， 其中 k∈ N+， c∈ {1,2,…n-1}， 此时 am =  
(an)kac = ekac = ac，而 c<n， O(a) = n，故 ac ≠e，因此 am = ac ≠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 bn = a1a2…an， 若∃bm = e， 则取 p = 1， q = m， 符合要  
求； 否则， 由运算的封闭性， bn∈ G/{e}。 由鸽巢原理知， ∃1≤m1<m2≤n， 满  
足 bm1 = bm2。等式两侧同时与(bm1)-1进行右 o 运算，则 (bm1)-1bm1= (bm1)-1  
bm2即 e = am1-1… a2-1a1-1a1a2…am2 = am+1am+2…. an。 因此取 p = m+1， q = n，  
符合要求。 综上所述， 总是∃1≤p≤q≤n 使得 ap…aq = e。

# p373

# 2.

假设 G1 和 G2 互相不包含，那么∃𝑎 ∈ 𝐺1*且*𝑎 ∉ 𝐺2*，*∃𝑏 ∈ 𝐺2*且*𝑏 ∉ 𝐺1那么𝑎𝑏 ∉

𝐺1*，*𝑎𝑏 ∉ 𝐺2，但是𝑎𝜖𝐺, 𝑏 ∈ 𝐺*，*𝑎𝑏 ∈ 𝐺，与假设矛盾，故 G1 和 G2 互相包含， G1⊆G2 G2⊆G1。

# 5.

证明：  
设φ -1(e2) = M， e1 为 G1的幺元。 对于∀a∈ G1， φ (a) \*φ (e1) = φ (a o e1)  
=φ (a)， 故φ (e1) = e2， 故 e1∈ M。 对于∀a,b∈ M， φ (a o b) =φ (a) \*φ (b) = e2  
\* e2 = e2， 故 a o b∈ M， 因此 o 在 M 上运算封闭。 由于 M⊆G1， G1是群满足结  
合律， 故 M 是半群。 由于 e1∈ M， 故 M 中有幺元 e1。  
对∀a∈ M， 设其在 G1中的逆元为 a-1， 则φ (a) \*φ (a-1) = φ (a o a-1)， 亦即  
e2 \* φ (a-1) = φ (e1) = e2， 故φ (a-1) = e2， 故 a-1 ∈ M。 由于 a -1 o a = a o a-1 =  
e1， 故 M 中存在 a 的逆元。 于是 M 是群。 由于 M⊆G1， 故 M 是 G 的子群。

# 8.

证明：  
设三阶群 G = {1,2,3}。 sym(S)={φ 1…φ 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}