P374

1、

根据变换群的定义：若 G 为 Sys（S）上的一个子群，则它是 R 上的变换群。
显然，f 是 R 上单位的一一对应的映射关系。只需证明 G 是 Sys（S）的子群即可。
①、任意 f1=a1x+b1,f2=a2x+b2 属于 G, f1f2=a2(a1x+b1)+b2=a1a2x+(b1a2+b2),也在 G 上。
②、任意 f=ax+b∈G，f^-1=1/ax+(-b/a)也∈G。
所以 G 是 Sys(x)的一个子群。
得证。

P384

1、

设 n 次单位根之集 G={a,a^-1,a^-2,……a^-n},根据定义，显然每个元素都是 a^-n 的乘方。
根据循环群的定义，它是一个循环群。

3、

因为 r 和 n 互质，则只需证（a^r）^k=a^(r*k)=a^(r*k%n)均可找到 a^m 与之相等。(k,m 属于自然数，且属于[1，n])。
只需证：对于一个大于 2 的自然数 n，任取一个与它互质的素数 r,r*[1,n]%n 分别与[1,n]一一对应。
数学归纳法：
当 r 为 2 时，n 必为奇数。设 k 属于[1,n],当 k 小于 n/2 时，r*k 为偶数，当 k 大于 n/2 时，r*k%n 为奇数，显然成立。
当 r 为 m 时成立，往证 r 为 m+1 时成立。设 r*k%n 余 a，(k 为 r*k 小于 n 的最大值+1)，即将问题转化为(r*k+a)%n,即为 a 对 n 的相同问题，显然 a 小于 r，即转化为假设已经得证了的子问题。所以成立。
得证。

5、

r 和 n 的最大公约数为 d，a^（r*k）当 k=n/d 时，a^(r*k%n)=a^r,所以 a^r 共有 n/d 项，所以阶为 n/d。

P387

1、

取六阶群的单位元，任意元素及其逆元构成一个三阶群，证明该群为六阶群子群即可。设三阶群的元素分别为 a,a^-1,e;任取两元素，其运算后仍在三阶群内：
取 a，a^-1:a。a^-1=a^-1。a=e
取 a,e：a。e=e。a=a;
a^-1 同理。
同时 a 在其中且 a^-1 也在其中，所以它是六阶群的子群。得证。

4、

不一定。
左陪集与右陪集相等是元素相等。ah=ha 只是陪集相等的特殊情况。可能左陪集的元素与原来元素存在一种一一对应关系，右陪集的元素与原来的元素存在另一种一一对应关系，而它们映射的结果都是
同一个群，这样会导致 aH=Ha，但是 ah≠ha。