# 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。