作业4

CINTA作业四、证明、编程

1、写出完整证明，虽然课堂上讲了。群$\mathbb{G}$ 的非空子集$\mathbb{H}$是$\mathbb{G}$ 的子群，当且仅当$\mathbb{H} \neq \emptyset$，且对任意$a, b \in \mathbb{H}$， $ab^{-1} \in \mathbb{H}$。

2、证明：任意群$\mathbb{G}$的两个子群的交集也是群$\mathbb{G}$的子群。

3、证明或证伪：任意群$\mathbb{G}$的两个子群的并集也是群$\mathbb{G}$的子群。

4、编程完成以下工作：给定一个素数p，返回 Z_p^*的一个子群。据此，能否找出子群的阶与Z_p^*的阶之间的关系？特别是，课堂上提到的两种方法：对所有元素做平方、立方，所得到子群的阶有什么规律？请尝试不同的素数，得到自己的结论。

1.证明

(1)充分性:

非空子集H是群G的子群，所以群H满足群的所有公理

我们任意选取元素a、b∈ H，一定有a的逆元a^{-1}、和b的逆元b^{-1}都属于群H，

根据群的封闭性原理，任意群H中的元素之间进行操作后仍然落在群H的集合内，有

$$a \in H\text{ , }b \in H\text{ , }ab \in H\text{ , 且 }ab^{-1} \in H$$

因为H是非空子集，所以H必定不能为空

(2)必要性

对任意元素a、b∈H，有$ab^{-1} \in H$，且H不为空

欲证明H是G的子群，根据定义，从以下3个方面证明：

1.封闭性：取a=a b=b^{-1} ，根据$ab^{-1} \in H$，有

$$a(b^{-1})^{-1} \in H \Rightarrow ab \in H$$

故非空集合H满足封闭性

2.单位元：取a=a b=a ，根据$ab^{-1} \in H$，有

$$ab^{-1} \in H \quad and \quad b = a \quad \Rightarrow aa^{-1} = e \in H$$

故非空集合H有单位元

3.逆元：取a=单位元e b=a，根据$ab^{-1} \in H$ 以及 上面证得的 $aa^{-1} \in H$，有

$$ea^{-1} = a^{-1} \in H$$

故非空集合H有逆元

因此H是群G的子群

2.证明：任意群G的两个子群的交集也是G的子群

任取群G的两个子群H_1、H_2，$\forall a,b \in H_1 \cap H_2$，

因为 $a \in H_1$，H_1是群，所以 存在逆元 $a^{-1} \in H_1$，b同理存在 $b^{-1} \in H_1$

又因为 $a \in H_2$，H_2是群，所以 存在逆元 $a^{-1} \in H_2$，b同理存在 $b^{-1} \in H_2$

所以，有

$$ab \in H_1 \quad and \quad ab \in H_2$$
$$ab \in H_1 \cap H_2$$

同理也有

$$b^{-1}a^{-1} \in H_1 \quad and \quad b^{-1}a^{-1} \in H_2$$
$$b^{-1}a^{-1} \in H_1 \cap H_2$$

集合$H_1 \cap H_2$ 操作继承H1和H2,具有封闭性，且存在单位元$aa^{-1} = e \in H_1 \cap H_2$

存在逆元 $a^{-1} \in H_1$ 并且 $a^{-1} \in H_2$，即得到$a^{-1} \in H_1 \cap H_2$

故集合$H_1 \cap H_2$ 也是群G的一个子群，即$H_1 \cap H_2 \leq G$

3.证明：任意群G的两个子群的并集不是G的子群

任取群G的两个子群H_1、H_2，任取$h_1 \in H_1 \quad and \quad h_1 \notin H_2$，$h_2 \in H_2 \quad and \quad h_2 \notin H_1$，

假设 $h_1h_2 \in H_1$

因为H_1 是群G的子群，所以存在元素h的逆元 $h_1^{-1} \in H_1$

由群H_1的定义可知

$$h_2 = (h_1^{-1}h_1)h_2 = h_1^{-1}(h_1h_2) \in H_1$$

可是这与我们的假设$h2 \notin H_1$ 矛盾，因此 $h_1h_2 \notin H_1$

同理，假设有$h_1h_2 \in H_2$,利用与上面的证明相同的方法可得

$$h_1 = (h_2^{-1}h_2)h_1 = h_2^{-1}(h_2h_1) \in H_2$$

与我们的假设$h1 \notin H_2$ 矛盾，因此 $h_1h_2 \notin H_2$

因为 $h_1h_2 \notin H_2 \quad and \quad h_1h_2 \notin H_1$，所以 $h_1h_2 \notin H_1 \cup H_2$，不满足群的封闭性，不构成群，自然也就不构成群G的子群

4.编程

```
#include<stdio.h>
#include<set>
#include<iostream>
using namespace std;
set<int> ans;
int shu[10000];
int num=0;
void subgroup(int p)   //i^2，对群元素做平方运算得到的子群
{
    for(int i=1;i<p;i++)
```

```
    {
        int c=(i*i)%p;    //立方的情况则在乘以一个i
        if(ans.find(c)==ans.end())
        {
            ans.insert(c); //不含相同元素的集合
        }
        shu[num++]=c;   //含有相同元素的集合
    }
}
int main()
{
    int p;
    cin>>p;
    subgroup(p);
    set<int>::iterator it=ans.begin();
    while(it!=ans.end())
    {
        cout<<*it<<" ";
        it++;
    }
    cout<<endl;
    for(int i=0;i<num;i++)
        cout<<shu[i]<<" ";
    return 0;
}
```

关系：子群的阶是 群Z_p^* 的阶的一个约数，设群Z_p^* 的阶为n，它的子群的阶为m，有m | n

Z_p^* 的阶为 p-1 ，对元素进行平方和立方得到的子群的阶仍然是 p-1 ，只不过子群里有等价类出现，例如p=7时，有

[1]、[2]、[4]三个等价类，共有六个元素，和Z_p^* 的元素个数一致，即阶相同且能相互整除。