**第一次小测试**

**郝裕玮**

**18329015**

1. **等价关系需要满足哪几个条件？写出集合的所有划分和对应的所有等价关系（6+30分）。**

解：（1）等价关系需要满足3个条件：反身性，对称性，传递性；

（2）如果A划分为1个子集，则有P1={1,2,3,4};

（3）如果A划分为2个子集,则有

P2={{1},{2,3,4}},P3={{1,2},{3,4}},P4={{1,3},{2,4}},

P5={{1,4},{2,3}},P6={{1,2,3},{4}},P7={{1,2,4},{3}},

P8={{2},{1,3,4}};

（4）如果A划分为3个子集，则有

P9={{1},{2},{3,4}},P10={{1},{3},{2,4}},

P11={{1},{4},{2,3}},P12={{2},{3},{1,4}},

P13={{2},{4},{1,3}},P14={{3},{4},{1,2}};

（5）如果A划分为4个子集，则有P15={{1},{2},{3},{4}};

所以A共有15种不同的等价关系：

={1~1,2~2,3~3,4~4,1~2,2~1,1~3,3~1,1~4,4~1,2~3,3~2,2~4,4~2,3~4,4~3}

={1~1,2~2,3~3,4~4,2~3,3~2,2~4,4~2,3~4,4~3}

={1~1,2~2,3~3,4~4,1~2,2~1,3~4,4~3}

={1~1,2~2,3~3,4~4,1~3,3~1,2~4,4~2}

={1~1,2~2,3~3,4~4,1~4,4~1,2~3,3~2}

={1~1,2~2,3~3,4~4,1~2,2~1,1~3,3~1,2~3,3~2}

={1~1,2~2,3~3,4~4,1~2,2~1,1~4,4~1,2~4,4~2}

={1~1,2~2,3~3,4~4,1~3,3~1,1~4,4~1,3~4,4~3}

={1~1,2~2,3~3,4~4,3~4,4~3}

={1~1,2~2,3~3,4~4,2~4,4~2}

={1~1,2~2,3~3,4~4,2~3,3~2}

={1~1,2~2,3~3,4~4,1~4,4~1}

={1~1,2~2,3~3,4~4,1~3,3~1}

={1~1,2~2,3~3,4~4,1~2,2~1}

={1~1,2~2,3~3,4~4}

1. **构成群要满足的四个条件是什么？证明所有行列式为1的阶整数矩阵组成的集合关于矩阵乘法构成群，判断是否为交换群（8+12+2分）。**

解：（1）4个条件为：封闭性；群中元素的代数运算满足结合律；具有单位元E；群中每一个元素都有自己的逆元且它们的代数运算等于单位元。

（2）对于(Z):

因为S=A X B且满足|S|=1，所以S∈(Z)，所以满足封闭性；

因为(A X B) X C = A X (B X C)，所以群中元素的代数运算满足结合律；

易证群中具有单位元E；

又因为对任意A∈(Z)，存在且||=，所以A\*=1，且∈(Z)，所以群中每一个元素都有自己的逆元，且它们的代数运算等于单位元。

1. **在整数集合上定义运算：，证明构成群，写出元素3的逆元（16+4分）。**

解：（1）对任意a,b∈Z，都有ab=a+b-2属于Z，满足封闭性；

（2）对于a,b,c∈Z,(ab)c=(a+b-2)c=a+b-2+c-2=a+b+c-4

abc)=a(b+c-2)=a+b+c-2-2=a+b+c-4

所以易证满足结合律；

（3）同时存在单位元E=2，对任意a∈Z，有aE=a+2-2=a

（4）同时对任意a∈Z，有逆元=4-a,使得a=a+4-a-2=2=单位元E

所以构成群，并易知3的逆元为4-3=1

1. **为了对消息进行加密，RSA加密方案选取两个素数并计算，利用加密密钥进行密文的计算，对密文解密时是用私钥进行的计算。请计算出私钥、密文的具体值，验证该密文的解密过程(10+6+6分)。**

解：

因为

= 6

加密过程：c==mod77=31

私钥：=

解密过程：