# 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$\mathbf{A=\{1，2，3，4\}}$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：

$\sim_1$={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}

$\sim_2$={1~1,2~2,3~3,4~4,2~3,3~2,2~4,4~2,3~4,4~3}

$\sim_3$={1~1,2~2,3~3,4~4,1~2,2~1,3~4,4~3}

$\sim_4$={1~1,2~2,3~3,4~4,1~3,3~1,2~4,4~2}

$\sim_5$={1~1,2~2,3~3,4~4,1~4,4~1,2~3,3~2}

$\sim_6$={1~1,2~2,3~3,4~4,1~2,2~1,1~3,3~1,2~3,3~2}

$\sim_7$={1~1,2~2,3~3,4~4,1~2,2~1,1~4,4~1,2~4,4~2}

$\sim_8$={1~1,2~2,3~3,4~4,1~3,3~1,1~4,4~1,3~4,4~3}

$\sim_9$={1~1,2~2,3~3,4~4,3~4,4~3}

$\sim_{10}$={1~1,2~2,3~3,4~4,2~4,4~2}

$\sim_{11}$={1~1,2~2,3~3,4~4,2~3,3~2}

$\sim_{12}$={1~1,2~2,3~3,4~4,1~4,4~1}

$\sim_{13}$={1~1,2~2,3~3,4~4,1~3,3~1}

$\sim_{14}$={1~1,2~2,3~3,4~4,1~2,2~1}

$\sim_{15}$={1~1,2~2,3~3,4~4}

**2. 构成群要满足的四个条件是什么？证明所有行列式为 1 的n阶整数矩阵组成的集合$SL_n(Z)$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$SL_n$(Z):

因为 S=A X B 且满足|S|=1，所以 S∈$SL_n$(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∈$SL_n$(Z)，$A^{-1}$存在且|$A^{-1}$|=$\frac{1}{|A|}$，所以 A*$A^{-1}$=1，且 $A^{-1}$∈$SL_n$(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。

**3. 在整数集合Z上定义运算⊕：$\mathbf{a \oplus b = a + b - 2}$，证明$(Z，\oplus)$构成群，写出元素 3 的逆元（16+4 分）。**

解：（1）对任意 a,b∈Z，都有 a⊕b=a+b-2 属于 Z，满足封闭性；

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

a⊕ (b⊕c)=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 a⊕E=a+2-2=a

（4）同时对任意 a∈Z，有逆元$a^{-1}$=4-a,使得 a⊕ $a^{-1}$=a+4-a-2=2=单位元 E

所以$(Z，\oplus)$构成群，并易知 3 的逆元为 4-3=1

**4. 为了对消息$m=3$进行加密，RSA 加密方案选取两个素数$p=7,q=11$并计算$n=p\times q,\psi(n)=(p-1)(q-1)$，利用加密密钥$e=7$进行密文的计算$c=m^e\ mod\ n$，对密文解密时是用私钥$d=e^{-1}\ mod\ \psi(n)$进行$c^d\ mod\ n$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$n = p \times q = 7 \times 11 = 77$

$\psi(n) = (p-1)(q-1) = 6 \times 10 = 60$

加密过程：c=$m^e \bmod n$=$3^7$mod77=31

私钥：$d = e^{-1} \bmod \psi(n)$=$7^{-1} mod 60 = 43$

解密过程：$c^d \bmod n = 31^{43} mod 77 = 3$