**2019级离散数学第5次作业**

**学号： 姓名： 班级： 总分：**

一、(每问5分，共10分)

设，*Q*是有理数集，\*为*S*上的二元运算，有：



(1) \*运算在*S*上是否可交换、可结合？是否为幂等？

(2) \*运算是否有单位元、零元？如果有，请指出，并求出*S*中所有可逆元素的逆元。.

解：

(1) 因为，

而，所以，不具有交换律。

对任意的，有

，且

。因此，满足结合律。

因为，所以不是幂等的。

(2)

因为没有交换律，所以要求单位元，需要先求出左单位元，右单位元，当左单位元和右单位元相等的时候，那么就称为单位元。零元也是一样，没有交换律，就要先求出左零元和右零元，如果左右零元相等，就叫做零元。

**求零元：**假设左零元为<*a*, *b*>.那么根据左零元的定义，对任意的，有

，

由于对任意的都成立，所以左零元为.但是，对任意的，显然，因此，不是右零元。即左零元不等于右零元。从而，没有零元。

**求单位元：**假设左单位元为，那么根据左单位元的定义，对任意的有

，

从而有。

又因为，所以也是右单位元。因此，单位元为。

二、(每题5分，共20分)

设，问下面定义的运算能否与*S*构成代数系统.如果能构成代数系统，那么请说明\*运算是否满足交换律、结合律，请求出\*运算的单位元和零元。

(1) 是*x*与*y*的最大公约数；

(2) 是*x*与*y*的最小公倍数；

(3) *x*\**y*=大于等于*x*和*y*的最小整数；

(4) *x*\**y*=质数*p*的个数，其中.

解：(1) 因为运算具有封闭性，所以能构成代数系统。运算具有交换律和结合律，无单位元，零元是1。

(2) 运算不具有封闭性，所以不能构成代数系统。比如：

(3) 因为运算具有封闭性，所以能构成代数系统。运算具有交换律和结合律，单位元是1，零元是10。

(4) 因为运算不具有封闭性，所以不能构成代数系统。比如：

三、(10分)

设,在上定义二元运算,对任意的.现设字母和数字之间有对应关系如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 | 1 | 2 | … | 25 |
| A | B | C | … | Z |

设函数(*k*是某个固定值,且),将某句英文变换为UVWHKBUGSXKPKEAPL.

请解出相应的原文,并给出C代码.(提示：需要人工观察输出的字符串来找到原文,C代码中长度不超过25行。精简做法, 最核心的代码只有1行)

参考答案：ILOVEDISCRETEMATH

参考代码：

#include <stdio.h>

#include <string.h>

int main(void)

{

int k, j, len;

char str[] = "UVWHKBUGSXKPKEAPL", str1[] = "UVWHKBUGSXKPKEAPL";

len = strlen(str);

for (k = 1; k < 26; k++)

{

for (j = 0; j < len; j++)

{

{

str1[j] = k \* (str[j] - 'A') % 26 + 'A';//核心

}

}

printf("k = %d, %s\n",k, str1);//可以不用输出k的值

}

return 0;

}

四、(16分)

设*Z*为整数集，在*Z*上定义的二元运算\*如下：



问：*Z*关于\*运算是否构成群？请说明理由。

解：

(1) 对任意的，可得



即，运算满足结合律。

(2) 对任意的，有

，即，运算具有单位元，为e=2。

(3) 对任意的，有

，

即Z中的任意元素*x*对于运算存在逆元，且。

综合(1),(2),(3)可得整数集Z关于运算构成群。

五、(16分)

设,证明*G*关于矩阵普通乘法构成一个群。

**证明**：令



且矩阵乘法用表示，则*G*中元素的运算表为

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | A | B | C | D |
| A | A | B | C | D |
| B | B | A | D | C |
| C | C | D | A | B |
| D | D | C | B | A |

有运算表可知，运算具有封闭性，单位元，每个元素的逆元是它自己。又根据线性代数可知，矩阵的乘法具有结合律。从而，*G*关于矩阵的乘法构成一个群。

六、(每问6分，共12分)

设,定义*Z*10上的二元运算⊕，其满足对,则可知是一个群。(其中：*x* mod 10表示*x*除以10的余数)

(1) 求出群中所有元素的阶；

(2) 求出中元素10086的阶。

解：容易知道，群Z10中⊕运算的单位元是0.

(1) 根据元素的阶的定义,容易知道110=0,即元素1的阶等于10,即|1|=10.同理可求得其它元素的阶分别为：

|1|=|3|=|7|=|9|=10，|2|=|4|=|6|=|8|=5，|5|=2，|0|=1.

(2) 容易知道，群的单位为是0，根据群的阶的定义，计算出元素10086的阶是18181.

七、(每问8分，共16分)

设,定义上的二元运算，其满足对,那么可知是一个群。(其中：*x* mod 11表示*x*除以11的余数)

(1) 求群中所有元素的阶；

(2) 求中元素18178,18179,18180的阶。(提示：需要编程来计算)

(设，则使得成立的最小正整数*k*，称为元素*a*的阶)

编写函数：int multMod(int a, int k, int p);

函数功能：判断对于上述两个群中的运算, 是否成立；如果成立，则函数返回1，否则返回非1.

提示：.例如：*p*=11或者18181

计算举例：

显然群的单位元为1,并且。可按以下步骤计算:

① 

② 

③ 

④ 

从而, ,所以，式

，可以通过函数

multMod(4, 5, 11)来计算，计算方法如①②③④所示。因此函数multMod(4, 5, 11)的返回值等于1,即在群

中，元素4的阶等于5.

解：

(1) 容易知道，群 中运算的单位元是1.

根据元素的阶的定义,计算可知, 而,所以元素2的阶等于10,即|2|=10.同理可求得其它元素的阶分别为：

|2|=|6|=|7|=|8|=10，|3|=|4|=|5|=|9|=5，|10|=2，|1|=1.

(2) 容易知道，群的单位为是1，根据群的阶的定义，计算出元素18178,18179,18180的阶分别是|18178|=9090,|18179|=18180,|18180|=2.

参考代码

/\*

函数功能：判断群在中,运算是否成立, 若成立则函数的返回值为1,否则函数的返回值不等于1

\*/

参考代码一：

int mulMod(int x, int n, int p)

{

int c = 1;

for (; n != 0; n = n >> 1)

{

if (n & 1)

{

c = (c \* x) % p;

}

x =( x \* x) % p;

}

return c;

}

参考代码二：

int mulMod(int x, int n, int p)

{

int i, c = 1;

for (i = 1; i <= n; i++)

{

c = c \* x % p;

}

return c;

}