Домашнее задание 2. Часть 1. Курс "Алгебра". 2018-2019 уч. год. БПИ183. Вариант 30

Андрей Шан

4 марта 2019 г.

1	2	3	4	5	6	7	8	9	10	$\sum$

1 Задание

В циклической группе $G{=}\langle a \rangle$

1.1 (α) все элементы g такие, что $g^{114}{=}1$

Элементы g имеют вид a^n, также извснетно что $a^{570}{=}1$ необходимо найти такие n, что $a^{n\times 114}{=}1$, так-же $1{=}1^k{=}a^{570\times k}$, где $k{\in}\mathbb{N}$

т.е. необходимо найти такие k, что $a^{n\times 114}{=}a^{570\times k}$, следовательно $n{\times}114{=}570{\times}k \Rightarrow n{=}5{\times}k$, значит n это числа кратные 5 из промежутка $[0;569]$. т.е.

n=(0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100, 105, 110, 115, 120, 125, 130, 135, 140, 145, 150, 155, 160, 165, 170, 175, 180, 185, 190, 195, 200, 205, 210, 215, 220, 225, 230, 235, 240, 245, 250, 255, 260, 265, 270, 275, 280, 285, 290, 295, 300, 305, 310, 315, 320, 325, 330, 335, 340, 345, 350, 355, 360, 365, 370, 375, 380, 385, 390, 395, 400, 405, 410, 415, 420, 425, 430, 435, 440, 445, 450, 455, 460, 465, 470, 475, 480, 485, 490, 495, 500, 505, 510, 515, 520, 525, 530, 535, 540, 545, 550, 555, 560, 565), 114 элементов

1.2 (β) элементы g порядка 114

порядок это минимальное такое m, что $g^m{=}1$, значит 114 это минимальная степень в котрую надо возвести g чтоб получить 1. $a^{s\times 114}{=}1{=}a^{570\times h}$, где h не кратно 2,3,19.

$\Rightarrow s{\times}2{\times}3{\times}19{=}h{\times}2{\times}3{\times}5{\times}19 \;\Rightarrow\; s{=}h{\times}5$.

Значит s=(5,25, 35, 55, 65, 85, 115,125, 145, 155, 175, 185, 205, 215, 235, 245, 265, 275, 295, 305, 325, 335, 355, 365, 385, 395, 415, 425, 445, 455, 485, 505, 515, 535, 545, 565), 36 элементов

Ответ: α) 114 элементов a^n, где n это числа кратные 5 из промежутка $[0;569]$,

β) 36 элементов a^s, где s это числа не кратные 2,3,19 из промежутка $[1;113]$ умножененные на 5

2 Задание

Порядок элемента (d,s,z) Группы $D_3 \times S_4 \times \mathbb{Z}_4$ равен НОК(ord(d),ord(s),ord(z)), также по условию он равен 4. т.е. НОК(ord(d),ord(s),ord(z))=4. Найдем в группе каждого множителя все элементы порядка 1,2,4. (Мы выбрали именно такие порядки т.к. НОК $\geq$ чем элементы для которых он считается и по определению эти элементы делители НОК)

В группе D_3 1 элемент порядка 1 - это тождественное преобразование. 3 элемента порядка 2 - это все отражения. И 0 элементов порядка 4.

В группе S_4 1 элемент порядка 1 - это тождественная перестановка. 9 элементов порядка 2 - это циклы (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3).(Все перестановки сосотоящие из одного цикла длиной 2 и все перестеновки состоящие из 2 циклов длиной 2). И 6 элементов порядка 4 - это циклы (1,2,3,4), (1,2,4,3), (1,3,2,4), (1,3,4,2), (1,4,2,3), (1,4,3,2).

В группе Z_4 1 элемент порядка 1 - это 0. 1 элемент порядка 2 - это 2. И 1 элемент порядка 4 - это 1

Рассмотрим при каких порядках элементов d,s,z НОК(d,s,z)=4. Для начала скажем, что в каждой тройке порядков хотя-бы один элемент должен быть равен 4, так-как никакая комбинация порядков 2 и 1 не даст НОК=4. У группы D_3 нет элемента с порядком 4 $\Rightarrow$ тройка (4,4,4) невозможна.

Дальнейшая нотация маска - кол-во элементов. (_,4,4)$-4\times6\times1=24$, (_,_,4)$-4\times10\times1=40$, (_,4,_)$-4\times6\times2=48$. (вместо пропусков можно подставить элементы с порядком 1 или 2)

Ответ: 112 элементов.

3 Задание

Проверить совместность можно найдя решение неоднородной слау. Используем для этого обратную матрицу. Для решения уравнения Ax=b, используем метод гаусса

$$\begin{pmatrix} 12 & 9 & 8 & 1 & 16 \\ 4 & 1 & 15 & 0 & 6 \\ 5 & 18 & 16 & 2 & 13 \\ 17 & 8 & 5 & 3 & 10 \end{pmatrix} = \begin{pmatrix} 12 & 9 & 8 & 1 & 16 \\ 4 & 1 & 15 & 0 & 6 \\ 5 & 18 & 16 & 2 & 13 \\ 0 & 17 & 6 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 12 & 15 & 1 & 15 \\ 4 & 1 & 15 & 0 & 6 \\ 5 & 18 & 16 & 2 & 13 \\ 0 & 17 & 6 & 6 & 7 \end{pmatrix} =$$

$$\begin{pmatrix} 5 & 12 & 15 & 1 & 15 \\ 0 & 17 & 6 & 6 & 7 \\ 5 & 18 & 16 & 2 & 13 \\ 0 & 17 & 6 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 12 & 15 & 1 & 15 \\ 0 & 17 & 6 & 6 & 7 \\ 0 & 6 & 1 & 1 & 17 \\ 0 & 17 & 6 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 12 & 15 & 1 & 15 \\ 0 & 17 & 6 & 6 & 7 \\ 0 & 6 & 1 & 1 & 17 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} =$$

$$\begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 & x_5 & \end{matrix} \\ \left(\begin{array}{cccc|c} 5 & 12 & 15 & 1 & 15 \\ 0 & 17 & 6 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \end{array}$$

Найдем частное решение неоднородной слау, положим что $x_3{=}0, x_4{=}0$, тогда $17x_2{+}6{\times}0{+}6{\times}0{=}7 \Rightarrow 17x_2{=}7 \Rightarrow x_2{=}6$
$5x_1{+}12{\times}6{+}15{\times}0{+}1{\times}0{=}15 \Rightarrow 5x_1{+}15{=}15 \Rightarrow x_1{=}0$

Найдем ФСР соответствующей однородной СЛАУ $\left(\begin{array}{cccc|c} 5 & 12 & 15 & 1 & 0 \\ 0 & 17 & 6 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$, найдем линейно независимые решения данной СЛАУ, их 2 т.к. размерность матрицы 4, а Ранг 2. Для этого в первом случае обозначим $x_4{=}1$, $x_3{=}0 \Rightarrow x_2{=}3$, $x_1{=}5$, а во втором $x_4{=}0$, $x_3{=}1 \Rightarrow x_2{=}3$, $x_1{=}4$

Найдя частное решение неоднородной СЛАУ и ФСР соответствующей однородной СЛАУ запишем решение СЛАУ в векторном виде $x{=}\begin{pmatrix} 0 \\ 6 \\ 0 \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} 5 \\ 3 \\ 0 \\ 1 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 3 \\ 1 \\ 0 \end{pmatrix}$

Ответ: т.к. было найдено решение СЛАУ совместна. Решение СЛАУ в векторном виде

$x{=}\begin{pmatrix} 0 \\ 6 \\ 0 \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} 5 \\ 3 \\ 0 \\ 1 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 3 \\ 1 \\ 0 \end{pmatrix}$, ФСР соответствующей однородной СЛАУ $= t_1 \begin{pmatrix} 5 \\ 3 \\ 0 \\ 1 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 3 \\ 1 \\ 0 \end{pmatrix}$

4 Задание

Необходимо найти M, известно (p,q,y)=(139,53,47), x=52, (a,b)=(92,44)

Вычислим $M=b(a^x)^{-1} \mod p \Rightarrow M=44\times(92^{52})^{-1} \mod 139=44\times(92^{139-1-52}) \mod 139=20$

Ответ: M=20

5 Задание

Необходимо найти m, известно c=1564

5.1 Закрытый ключ Кортаны:(N=20711,d=1715).

m=1564^{1715} mod 20711=99

5.2 Открытый ключ Алисы:(N=12317,d=181).

Он не нужен для дешифровки

Ответ: В таблице ASCII коды 99 соотвествуют символу c

6 Задание

$f(x)=x^3+x^2+11x+6$, $g(x)=x^3+2x^2+15$ Для нахождения НОД сначала найдем частное и остаток приделение g(x)/f(x) $\Rightarrow$ 1 и остаток x^2+8x+9, теперь поделим f(x)/x^2+8x+9, и получим $x+12$ и остаток $x+12$, далее $x^2+8x+9/x+12 = x+15$ и остаток 0. А это значит что предыдущий остаток это НОД. Т.е. НОД($fx^3+x^2+11x+6$,x^3+2x^2+15)$=x+12$

Далее найдем такие $u(x)$,$v(x) \in \mathbb{Z}_{19}[x]$, что $u(x)f(x)+v(x)g(x)=$НОД(f,g)
Распишем 2 и 1 деление с остатком $f(x)=(x^2+8x+9)(x+12)+(x+12)$, $g(x)=f(x)+(x^2+8x+9) \Rightarrow$ $f(x)=(g(x)-f(x))(x+12)+(x+12) \Rightarrow f(x)+f(x)(x+12)+g(x)(18x+7)=$НОД $\Rightarrow$

$$f(x)(x+13)+g(x)(18x+7)=GCD$$

Ответ: НОД(f,g)$=x+12$, $u(x)=x+13$, $v(x)=18x+7$

7 Задание

Рассмотрим поле $F{=}\mathbb{F}_5[x]/\langle x^2{+}3x{+}3\rangle$, и смежный класс $\overline{f}{=}f{+}\langle x^2{+}3x{+}3\rangle{\in}F$

Преобразуем выражение

$$\frac{2x^2{+}4x{+}2}{x^6{+}2x^5{+}4x^4{+}x^3{+}2x^2{+}3}{+}(4x^5{+}2x^2{+}4x{+}2)(4x^4{+}4x^3{+}3x^2{+}2x{+}1){-}\frac{2x^3{+}3x{+}2}{x{+}1}$$

, для начала найдем многочлены обратные к $x^6{+}2x^5{+}4x^4{+}x^3{+}2x^2{+}3$ и $x{+}1$

Обозначим $f(x){=}x^2{+}3x{+}3$, $g(x){=}x^6{+}2x^5{+}4x^4{+}x^3{+}2x^2{+}3$, $h(x){=}x{+}1$, известно НОД(a,b)$=ax{+}by$, а в случае если один из аргументов НОДа $f(x)$, то множитель с данным аргументом занулиться. Для нахождения коэфицентов x, y применим Алгоритм Еклида и пойдем в обратную сторону.

$g(x)/f(x){=}x^4{+}4x^3{+}4x^2{+}2x{+}4$ и остаток $2x{+}1$ $\Rightarrow$ $f(x)/(2x{+}1){=}3x$ и остаток 3 $\Rightarrow$ $(2x{+}1)/3{=}4x{+}2$ и остаток 0.

Пойдем обртано по алгоритму. $f(x){=}3x(2x{+}1){+}3 \Rightarrow$
$f(x){=}3x(g(x){-}f(x)(x^4{+}4x^3{+}4x^2{+}2x{+}4)){+}3 \Rightarrow f(x){+}f(x)(x^4{+}4x^3{+}4x^2{+}2x{+}4){+}2x(g(x)){=}3$ члены содержащие $f(x)$ занулятся (т.к. мы работаем в поле F) $\Rightarrow 2x(g(x)){=}3$ домножим обе части на 2 $\Rightarrow$

$$4x(g(x)){=}1$$

Проделаем тоже самое для $h(x)$ $f(x)/h(x){=}x{+}2$ с остатком 1 $\Rightarrow$ $h(x)/1{=}x{+}1$ с остатком 0. Пойдем обратно по алгоритму $f(x){=}h(x)(x{+}2){+}1 \Rightarrow f(x){+}h(x)(4x{+}3){=}1$ член содержащий $f(x)$ занулится (т.к. мы работаем в поле F) $\Rightarrow$

$$(4x{+}3)h(x){=}1$$

Домножим и разделим соответствующие дроби на обратные к их знаменателям

$$\frac{2x^2{+}4x{+}2}{x^6{+}2x^5{+}4x^4{+}x^3{+}2x^2{+}3}\frac{4x}{4x}{+}(4x^5{+}2x^2{+}4x{+}2)(4x^4{+}4x^3{+}3x^2{+}2x{+}1){-}\frac{2x^3{+}3x{+}2}{x{+}1}\frac{4x{+}3}{4x{+}3}{=}$$

$$\frac{(2x^2{+}4x{+}2)4x}{1}{+}(4x^5{+}2x^2{+}4x{+}2)(4x^4{+}4x^3{+}3x^2{+}2x{+}1){-}\frac{(2x^3{+}3x{+}2)(4x{+}3)}{1}{=}$$

$$(2x^2{+}4x{+}2)4x{+}(4x^5{+}2x^2{+}4x{+}2)(4x^4{+}4x^3{+}3x^2{+}2x{+}1){+}(2x^3{+}3x{+}2)(x{+}2){=}$$

$$x^9{+}x^8{+}2x^7{+}x^6{+}3x^5{+}2x^4{+}x^3{+}4x{+}1$$

Разделим полученное выражение на $x^2{+}3x{+}3$

$$\frac{x^9{+}x^8{+}2x^7{+}x^6{+}3x^5{+}2x^4{+}x^3{+}4x{+}1}{x^2{+}3x{+}3}{=}(4x{+}1){+}(x^7{+}3x^6{+}2x^4{+}2x^3)(x^2{+}3x{+}3)$$

Ответ:$\overline{f}{=}4x{+}1$

8 Задание

Дано множество матриц G вида $\begin{pmatrix} x_1 & x_2 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & x_4 & x_3 \end{pmatrix}$, где $x_i \in \mathbb{R}$ с операциями матричного умножения и сложения

Для того чтобы доказать что это кольцо с данными операциями надо доказать что данное множество матриц и сложение образуют абелеву группу и данное множество матриц и умножение образуют полугруппу, а также обладает двусторонней дистрибутивностью $\times$ относительно $+$.

8.1 Докажем что это абелева групп по сложению

8.1.1 Докажем операция не выводит за пределы множества

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 & 0 & 0 \\ 0 & a_1+a_2 & 0 & 0 \\ 0 & 0 & c_1+c_2 & 0 \\ 0 & 0 & d_1+d_2 & c_1+c_2 \end{pmatrix} \in G$$

8.1.2 Докажем ассоциативность

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} + \left(\begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} \right) = \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} +$$
$$\begin{pmatrix} a_2+a_3 & b_2+b_3 & 0 & 0 \\ 0 & a_2+a_3 & 0 & 0 \\ 0 & 0 & c_2+c_3 & 0 \\ 0 & 0 & d_2+d_3 & c_2+c_3 \end{pmatrix} = \begin{pmatrix} a_1+a_2+a_3 & b_1+b_2+b_3 & 0 & 0 \\ 0 & a_1+a_2+a_3 & 0 & 0 \\ 0 & 0 & c_1+c_2+c_3 & 0 \\ 0 & 0 & d_1+d_2+d_3 & c_1+c_2+c_3 \end{pmatrix}$$
$$\left(\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} \right) + \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 & 0 & 0 \\ 0 & a_1+a_2 & 0 & 0 \\ 0 & 0 & c_1+c_2 & 0 \\ 0 & 0 & d_1+d_2 & c_1+c_2 \end{pmatrix} +$$
$$\begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} = \begin{pmatrix} a_1+a_2+a_3 & b_1+b_2+b_3 & 0 & 0 \\ 0 & a_1+a_2+a_3 & 0 & 0 \\ 0 & 0 & c_1+c_2+c_3 & 0 \\ 0 & 0 & d_1+d_2+d_3 & c_1+c_2+c_3 \end{pmatrix}$$

8.1.3 Найдем нейтральный элемент

$$\begin{pmatrix} a & b & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & d & c \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & d & c \end{pmatrix} = \begin{pmatrix} a & b & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & d & c \end{pmatrix}$$

8.1.4 Найдем обратный элемент

$$\begin{pmatrix} a & b & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & d & c \end{pmatrix} + \begin{pmatrix} -a & -b & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & -c & 0 \\ 0 & 0 & -d & -c \end{pmatrix} = \begin{pmatrix} -a & -b & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & -c & 0 \\ 0 & 0 & -d & -c \end{pmatrix} + \begin{pmatrix} a & b & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & d & c \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = e$$

8.1.5 Докажем абелевость

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 & 0 & 0 \\ 0 & a_1+a_2 & 0 & 0 \\ 0 & 0 & c_1+c_2 & 0 \\ 0 & 0 & d_1+d_2 & c_1+c_2 \end{pmatrix}$$

$$\begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} + \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 & 0 & 0 \\ 0 & a_1+a_2 & 0 & 0 \\ 0 & 0 & c_1+c_2 & 0 \\ 0 & 0 & d_1+d_2 & c_1+c_2 \end{pmatrix}$$

8.2 Докажем что это полугруппа по умножению

8.2.1 Докажем что операция не выводит за пределы множества

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times \begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_2b_1+a_1b_2 & 0 & 0 \\ 0 & a_1a_2 & 0 & 0 \\ 0 & 0 & c_1c_2 & 0 \\ 0 & 0 & c_2d_1+c_1d_2 & c_1c_2 \end{pmatrix} \in G$$

8.2.2 Докажем ассоциативность

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times \left(\begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} \times \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} \right) = \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times$$

$$\begin{pmatrix} a_2a_3 & a_3b_2+a_2b_3 & 0 & 0 \\ 0 & a_2a_3 & 0 & 0 \\ 0 & 0 & c_2c_3 & 0 \\ 0 & 0 & c_3d_2+c_2d_3 & c_2c_3 \end{pmatrix} = \begin{pmatrix} a_1a_2a_3 & a_2a_3b_1+a_1\left(a_3b_2+a_2b_3\right) & 0 & 0 \\ 0 & a_1a_2a_3 & 0 & 0 \\ 0 & 0 & c_1c_2c_3 & 0 \\ 0 & 0 & c_2c_3d_1+c_1\left(c_3d_2+c_2d_3\right) & c_1c_2c_3 \end{pmatrix}$$

$$\left(\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times \begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} \right) \times \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_2b_1+a_1b_2 & 0 & 0 \\ 0 & a_1a_2 & 0 & 0 \\ 0 & 0 & c_1c_2 & 0 \\ 0 & 0 & c_2d_1+c_1d_2 & c_1c_2 \end{pmatrix}$$

$$\begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} = \begin{pmatrix} a_1a_2a_3 & a_3\left(a_2b_1+a_1b_2\right)+a_1a_2b_3 & 0 & 0 \\ 0 & a_1a_2a_3 & 0 & 0 \\ 0 & 0 & c_1c_2c_3 & 0 \\ 0 & 0 & c_3\left(c_2d_1+c_1d_2\right)+c_1c_2d_3 & c_1c_2c_3 \end{pmatrix} =$$

$$\begin{pmatrix} a_1a_2a_3 & a_2a_3b_1+a_1\left(a_3b_2+a_2b_3\right) & 0 & 0 \\ 0 & a_1a_2a_3 & 0 & 0 \\ 0 & 0 & c_1c_2c_3 & 0 \\ 0 & 0 & c_2c_3d_1+c_1\left(c_3d_2+c_2d_3\right) & c_1c_2c_3 \end{pmatrix}$$

Но конечно же некоторые пункты можно было взять из свойств матриц

8.3 Докажем дистрибутивность в обе стороны

8.3.1 Докажем в одно сторону

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times \left(\begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} \right) =$$

$$\begin{pmatrix} a_1(a_2+a_3) & (a_2+a_3)b_1+a_1(b_2+b_3) & 0 & 0 \\ 0 & a_1(a_2+a_3) & 0 & 0 \\ 0 & 0 & c_1(c_2+c_3) & 0 \\ 0 & 0 & (c_2+c_3)d_1+c_1(d_2+d_3) & c_1(c_2+c_3) \end{pmatrix}$$

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times \begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} + \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} =$$

$$\begin{pmatrix} a_1a_2+a_1a_3 & a_2b_1+a_3b_1+a_1b_2+a_1b_3 & 0 & 0 \\ 0 & a_1a_2+a_1a_3 & 0 & 0 \\ 0 & 0 & c_1c_2+c_1c_3 & 0 \\ 0 & 0 & c_2d_1+c_3d_1+c_1d_2+c_1d_3 & c_1c_2+c_1c_3 \end{pmatrix}$$

8.3.2 Докажем в другую

$$\left(\begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} \right) \times \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} =$$

$$\begin{pmatrix} a_1(a_2+a_3) & (a_2+a_3)b_1+a_1(b_2+b_3) & 0 & 0 \\ 0 & a_1(a_2+a_3) & 0 & 0 \\ 0 & 0 & c_1(c_2+c_3) & 0 \\ 0 & 0 & (c_2+c_3)d_1+c_1(d_2+d_3) & c_1(c_2+c_3) \end{pmatrix}$$

$$\begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} \times \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 & 0 & 0 \\ 0 & a_3 & 0 & 0 \\ 0 & 0 & c_3 & 0 \\ 0 & 0 & d_3 & c_3 \end{pmatrix} \times \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} =$$

$$\begin{pmatrix} a_1a_2+a_1a_3 & a_2b_1+a_3b_1+a_1b_2+a_1b_3 & 0 & 0 \\ 0 & a_1a_2+a_1a_3 & 0 & 0 \\ 0 & 0 & c_1c_2+c_1c_3 & 0 \\ 0 & 0 & c_2d_1+c_3d_1+c_1d_2+c_1d_3 & c_1c_2+c_1c_3 \end{pmatrix}$$

8.4 Найдем делители нуля

Данное кольцо коммутативно по умножению $\Rightarrow$ неважно с какой стороны умножается делитель нуля

$$\begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & a_1 & 0 & 0 \\ 0 & 0 & c_1 & 0 \\ 0 & 0 & d_1 & c_1 \end{pmatrix} \times \begin{pmatrix} a_2 & b_2 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & c_2 & 0 \\ 0 & 0 & d_2 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_2b_1+a_1b_2 & 0 & 0 \\ 0 & a_1a_2 & 0 & 0 \\ 0 & 0 & c_1c_2 & 0 \\ 0 & 0 & c_2d_1+c_1d_2 & c_1c_2 \end{pmatrix}$$

Найдем такие $a_1, b_1, c_1, d_1 \neq 0 : \exists a_2, b_2, c_2, d_2 \neq 0$ такие что, $a_1a_2 = a_2b_1 + a_1b_2 = c_1c_2 = c_2d_1 + c_1d_2 = 0$ в данном случае нам важно только нулевой элемент или нет. т.е. можно перебрать 15 вариантов (исключая когда все равны 0) и выбрать такие для которых существуют такие элементы 2 матрицы которые не все нулевые. С помощью магии ПрОгРаМмИрОвАнИя я нашел 11 таких наборов

$$\begin{pmatrix}a&0&0&0\\0&a&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\begin{pmatrix}a&0&0&0\\0&a&0&0\\0&0&0&0\\0&0&d&0\end{pmatrix},\begin{pmatrix}0&b&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\begin{pmatrix}0&b&0&0\\0&0&0&0\\0&0&0&0\\0&0&d&0\end{pmatrix},\begin{pmatrix}a&b&0&0\\0&a&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\begin{pmatrix}a&b&0&0\\0&a&0&0\\0&0&0&0\\0&0&c&0\end{pmatrix},$$

$$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&c&0\\0&0&0&c\end{pmatrix},\begin{pmatrix}0&b&0&0\\0&0&0&0\\0&0&c&0\\0&0&0&c\end{pmatrix},\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&c&0\\0&0&d&c\end{pmatrix},\begin{pmatrix}0&b&0&0\\0&0&0&0\\0&0&c&0\\0&0&d&c\end{pmatrix},\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&d&0\end{pmatrix}$$

Ответ: Записан строчками выше.

9 Задание

Выпишим элементы группы $S_2 \times D_4$:

1)(e,R_0)	2)(e,R_{90})	3)(e,R_{180})	4)(e,R_{270})
5)(e,u_0)	6)(e,u_1)	7)(e,u_2)	8)(e,u_3)
9)$((1,2),R_0)$	10)$((1,2),R_{90})$	11)$((1,2),R_{180})$	12)$((1,2),R_{270})$
13)$((1,2),u_0)$	14)$((1,2),u_1)$	15)$((1,2),u_2)$	16)$((1,2),u_3)$

Найдем по теореме Кэли перестановку $\in S_{16}$ которая соответствует $(e,R_9 0)$ будем использовать номера элементов вместо их записи

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	3	4	1	6	7	8	5	10	11	12	9	14	15	16	13

Ответ: элемент (e,R_{90}) соответствует перестановке

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 & 10 & 11 & 12 & 9 & 14 & 15 & 16 & 13 \end{pmatrix}$$

10 Задание

Заполним таблицу Кэли из условия с учетом того что она представляет группу

	p	q	r	s	t	u	v	w
p	w	v	u	r	s	t	p	q
q	v	w	s	t	u	r	q	p
r	u	s	v	q	w	p	r	t
s	r	t	q	w	p	v	s	u
t	s	u	r	p	v	q	t	w
u	t	r	p	v	q	w	u	s
v	p	q	w	s	t	u	v	r
w	q	p	t	u	r	s	w	v

Всего 5 групп (с точностью до изоморфизма) порядка 8. и из них подходит только группа $Z_4 \times Z_2$

Ответ: $Z_4 \times Z_2$