Assignment-02

7AU0935
Hrudaya Jinna

① Let a and b be the permulations defined in the above handout on permutations

ⓐ Using the 2X11 representation of permutations, compute the 2X11 representation of the permutation ba.

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 11 & 7 & 8 & 10 & 2 & 1 & 5 & 3 & 4 & 6 \end{pmatrix}$$

and

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 6 & 3 & 10 & 2 & 11 & 1 & 5 & 4 & 9 & 8 \end{pmatrix}$$

$$b \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 6 & 3 & 10 & 2 & 11 & 1 & 5 & 4 & 9 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 11 & 7 & 8 & 10 & 2 & 1 & 5 & 3 & 4 & 6 \end{pmatrix}$$

$$= \left(\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1\to 9\to 4 & 2\to 11\to 8 & 3\to 7\to 1 & 4\to 8\to 5 & 5\to 10\to 9 & 6\to 2\to 6 & 7\to 1\to 7 & 8\to 5\to 2 \\ 4 & 8 & 1 & 5 & 9 & \cancel{8} =6 & 7 & \cancel{5}\,2 \end{array} \right.$$

$$\left. \begin{array}{ccc} 9 & 10 & 11 \\ 9\to 3\to 3 & 10\to 4\to 10 & 11\to 6\to 11 \\ 3 & \underline{40} =10 & \cancel{6}\,11 \end{array} \right)$$

So finally

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 8 & 1 & 5 & 9 & 6 & 7 & 2 & 3 & 10 & 11 \end{pmatrix}$$

(b) Using the product of disjoint cycles representation of permutations a and b, compute the product ba in the product of disjoint cycles form

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 11 & 7 & 8 & 10 & 2 & 1 & 5 & 3 & 4 & 6 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 6 & 3 & 10 & 2 & 11 & 1 & 5 & 4 & 9 & 8 \end{pmatrix}$$

If we write product of cycles

$$b = (1,7)\ (2,6,11,8,5)\ (4,10,9)$$

$$a = (1,9,3,7)\ (2,11,6)\ (4,8,5,10)$$

$$b \circ a = [(1,7)(2,6,11,8,5)(4,10,9)]\ [(1,9,3,7)(2,11,6)(4,8,5,10)]$$

$$= (1,4,5,9,3\cancel{7})\ (2,8)\ \overset{(7)}{(6)}(10)(11)$$

$$= (1,4,5,9,3)\ (2,8)$$

(c) Using the 2×11 representation of b, compute the 2×11 representation of the permutation b^{-1}

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 6 & 3 & 10 & 2 & 11 & 1 & 5 & 4 & 9 & 8 \end{pmatrix}$$

$$b^{-1} = \begin{pmatrix} 7 & 6 & 3 & 10 & 2 & 11 & 1 & 5 & 4 & 9 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{pmatrix}$$

~~To check~~ write the 2 row to top and compare the values)

$$b \circ b^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1\to 7 & 2\to 5 & & & & & & & & & \\ 7 & 5 & 3 & 9 & 8 & 2 & 1 & 11 & 10 & 4 & 6 \end{pmatrix}$$

To check the b^{-1} values

$$b \circ b^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 6 & 3 & 10 & 2 & 11 & 1 & 5 & 4 & 9 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 5 & 3 & 9 & 8 & 2 & 1 & 11 & 10 & 4 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1\to 7\to 1 & 2\to 5\to 2 & 3\to 3 & 4\to 9 & 5\to 8 & 6\to 2 & 7\to 1 & 8\to 11 & 9\to 10 & 10\to 4 & 11\to 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{pmatrix}$$

$$= \underline{1}$$

So $b^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 5 & 3 & 9 & 8 & 2 & 1 & 11 & 10 & 4 & 6 \end{pmatrix}$

(a) Using the product of disjoint cycles representation of the permutation b.
Compute the inverse b^{-1} in product of disjoint cycles representation form.

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 6 & 3 & 10 & 2 & 11 & 1 & 5 & 4 & 9 & 8 \end{pmatrix}$$

$$b = (1\ 7)(2, 6, 11, 8, 5)(3)(4, 10, 9)$$

$$b^{-1} = ?$$

$$= ((1\ 7)(2, 6, 11, 8, 5)(3)(4, 10, 9))^{-1}$$

$$= (7\ 1)(5, 8, 11, 6, 2)(3)(9, 10, 4)$$

Arrange to normalized form

$$= (1\ 7)(2, 5, 8, 11, 6)(3)(4, 9, 10)$$

② Construct the addition and multiplication tables for the ring $R = \mathbb{Z}_{15}$ = mod 15. List all the units in R. List all the non-trivial divisors of zero in R.

For addition table

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15%15 = 0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15%15 = 0	16%15 = 1
3	3	4	5	6	7	8	9	10	11	12	13	14	15%15 = 0	16%15 = 1	17%15 = 2
4	4	5	6	7	8	9	10	11	12	13	14	15%15 = 0	16%15 = 1	17%15 = 2	18%15 = 3
5	5	6	7	8	9	10	11	12	13	14	0	1	2	3	19%15 = 4
6	6	7	8	9	10	11	12	13	14	0	1	2	3	4	20%15 = 5
7	7	8	9	10	11	12	13	14	0	1	2	3	4	5	21%15 = 6
8	8	9	10	11	12	13	14	0	1	2	3	4	5	6	22%15 = 7
9	9	10	11	12	13	14	0	1	2	3	4	5	6	7	23%15 = 8
10	10	11	12	13	14	15%15 = 0	1	2	3	4	5	6	7	8	24%15 = 9
11	11	12	13	14	15%15 = 0	1	2	3	4	5	6	7	8	9	25%15 = 10
12	12	13	14	0	1	2	3	4	5	6	7	8	9	10	26%15 = 11
13	13	14	15%15 = 0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15%15 = 0	= 1	2	3	4	5	6	7	8	9	10	11	12	28%15 = 13

For multiplication table

·	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	16%15 =1	18%15 =3	20%15 5	22%15 =7	24%15 =9	26%15 =11	28%15 =13
3	0	3	6	9	12	15%15 =0	8%15 =3	21%15 =6	24%15 =9	27%15 =12	30%15 =0	33%15 =3	36%15 =6	39%15 =9	42%15 =12
4	0	4	8	12	16%15 =1	20%15 =5	24%15 =9	28%15 =13	32%15 =2	36%15 =6	40%15 =10	44%15 =14	48%15 = 3	52%15 =7	56%15 =11
5	0	5	10	15%15 =0	20%15 =5	25%15 =10	30%15 =0	35%15 =5	40%15 =10	45%15 =0	50%15 =5	55%15 =10	60%15 =0	65%15 =5	70%15 =10
6	0	6	12	18%15 =3	24%15 =9	30%15 =0	36%15 =6	42%15 =12	48%15 =3	54%15 =9	60%15 =0	66%15 =6	72%15 =12	78%15 =3	84%15 =9
7	0	7	14	21%15 =6	28%15 =13	35%15 =5	42%15 =12	49%15 =4	56%15 =11	63%15 = 3	70%15 =10	77%15 =2	84%15 =9	91%15 =1	98%15 =8
8	0	8	16%15 =1	24%15 =6	32%15 =2	40%15 =10	48%15 =3	56%15 =11	64%15 =4	72%15 =12	80%15 = 5	88%15 =13	96%15 =6	104%15 =14	112%15 =7
9	0	9	18%15 =3	27%15 =12	36%15 =6	45%15 =0	54%15 =9	63%15 =3	72%15 =12	81%15 =6	90%15 =0	99%15 =9	108%15 =3	117%15 =12	126%15 =6
10	0	10	20%15 =3	30%15 =0	40%15 =10	50%15 =5	60%15 =0	70%15 =10	80%15 =5	90%15 =0	100%15 =10	110%15 =5	120%15 =0	130%15 =10	140%15 =5
11	0	11	22%15 =7	33%15 =3	44%15 =14	55%15 =10	66%15 =6	77%15 =2	86%15 =13	99%15 =9	110%15 =5	120/15 =1	132%15 =12	143%15 =8	154%15 =4
12	0	12	24%15 =9	36%15 =6	48%15 =3	60%15 =0	72%15 =12	84%15 =9	96%15 =6	108%15 =3	120%15 =0	132%15 =12	144%15 =9	156%15 =6	168%15 =3
13	0	13	26%15 =11	39%15 =9	52%15 =7	65%15 =5	78%15 =3	91%15 =1	104%15 =14	117%15 =12	130%15 =10	143%15 =8	156%15 =6	169%15 =4	182%15 = 2
14	0	14	28%15 =13	42%15 =12	56%15 =11	70%15 =10	84%15 =9	98%15 =8	112%15 =7	126%15 =6	140%15 =5	154%15 =4	168%15 =3	182%15 =2	196%15 =1

Scanned with CamScanner

From the multiplication table we get

$3 \cdot 5 = 0$

$3 \cdot 10 = 0$

$\cancel{3 \cdot 11 = 0}$

$5 \cdot 3 = 0$

$5 \cdot 6 = 0$

$5 \cdot 9 = 0$

$5 \cdot 12 = 0$

$6 \cdot 5 = 0$

$6 \cdot 10 = 0$

$9 \cdot 5 = 0$

$9 \cdot 10 = 0$

$10 \cdot 3 = 0$

$10 \cdot 6 = 0$

$10 \cdot 9 = 0$

$10 \cdot 12 = 0$

$12 \cdot 5 = 0$

$12 \cdot 10 = 0$

The nontrivial divisors of zero in Z are

$3, 5, 6, 9, 10, 12$

③ The integers modulo 13 form a finite field of 13 elements GF(13). Find the multiplicative inverse of each of the non-zero elements of GF(13)

soln Given modulo 13 of GF(13)

From 0 to 12

•	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	14%13 =1	16%13 =3	18%13 =5	20%13 =7	22%13 =9	24%13 =11
3	0	3	6	9	12	15%13 =2	18%13 =5	21%13 =8	24%13 =11	27%13 =1	30%13 =4	33%13 =7	36%13 =10
4	0	4	8	12	16%13 =3	20%13 =7	24%13 =11	28%13 =2	32%13 =6	36%13 =10	40%13 =1	44%13 =5	48%13 =9
5	0	5	10	15%13 =2	20%13 =7	25%13 =12	30%13 =4	35%13 =9	40%13 =1	45%13 =6	50%13 =11	55%13 =3	60%13 =8
6	0	6	12	18%13 =5	24%13 =11	30%13 =4	36%13 =10	42%13 =3	48%13 =9	54%13 =2	60%13 8	66%13 =1	72%13 =7
7	0	7	14%13 =1	21%13 =8	28%13 =2	35%13 =9	42%13 =3	49%13 =10	56%13 =4	63%13 =11	70%13 5	77%13 =12	84%13 =6
8	0	8	16%13 =3	24%13 =11	32%13 =6	40%13 =1	48%13 =9	56%13 =4	64%13 =12	72%13 =7	80%13 =2	88%13 =10	96%13 =5
9	0	9	18%13 =5	27%13 =1	36%13 =10	45%13 =6	54%13 =2	63%13 =11	72%13 =7	81%13 =3	90%13 =12	99%13 =8	108%13 =4
10	0	10	20%13 =7	30%13 =4	40%13 =1	50%13 =11	60%13 =8	70%13 =5	80%13 =2	90%13 12	100%13 =9	110%13 =6	120%13 =3
11	0	11	22%13 =9	33%13 =7	44%13 =5	55%13 =3	66%13 =1	77%13 =12	88%13 =10	99%13 =8	110%13 =6	121%13 =4	132%13 =2
12	0	12	24%13 =11	36%13 =10	48%13 =9	60%13 =8	72%13 =7	84%13 =6	96%13 =5	108%13 4	120%13 3	132%13 2	144%13 1

Scanned with CamScanner

From the table we can conclude that

Multiplicative inverse of 1 is 1 $\Rightarrow 1 \cdot 1 = 1$
Multiplicative inverse of 2 is 7 $\Rightarrow 2 \cdot 7 = 1$
Multiplicative inverse of 3 is 9 $\Rightarrow 3 \cdot 9 = 1$
Multiplicative inverse of 4 is 10 $\Rightarrow 4 \cdot 10 = 1$
Multiplicative inverse of 5 is 8 $\Rightarrow 5 \cdot 8 = 1$
Multiplicative inverse of 6 is 11 $\Rightarrow 6 \cdot 11 = 1$
Multiplicative inverse of 7 is 2 $\Rightarrow 7 \cdot 2 = 1$
Multiplicative inverse of 8 is 5 $\Rightarrow 8 \cdot 5 = 1$
Multiplicative inverse of 9 is 3 $\Rightarrow 9 \cdot 3 = 1$
Multiplicative inverse of 10 is 4 $\Rightarrow 10 \cdot 4 = 1$
Multiplicative inverse of 11 is 6 $\Rightarrow 11 \cdot 6 = 1$
Multiplicative inverse of 12 is 12 $= 12 \cdot 12 = 1$

4) (20pts) Construct the addition and multiplication tables for the ring $R= GF(2)[x] \bmod x^3+1=0$. List all the units n R. List all the non-trivial divisors of zero in R .

Solution:
For addition $x^3=1$

+	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

For multiplication

*	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	001	011	101	110
011	000	011	110	101	101	110	011	000
100	000	100	001	101	010	110	011	111
101	000	101	011	110	110	101	101	000
110	000	110	101	011	011	101	110	000
111	000	111	111	000	111	000	000	111

For the multiplication

011*111=000

101*111=000

110*111=000

111*011=000

111*101=000

111*110=000

Therefore non trivial divisors of 0 are 011,111,110,101

Hence the non trivial divisors of zero in R are:

$x+1$, x^2+x+1 , x^2+x , x^2+1;

There are 4 non trivial zeros for the above R.

5)Costruct the addition and multiplication tables for the ring

R= GF(2)[x] mod x^4+1=0 . List all the units n R.

List all the non-trivial divisors of zero in R .

Sol:Here we consider x^4=1

For addition

+	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0001	0001	0000	0011	0010	0101	0100	0111	0110	1001	1000	1011	1010	1101	1100	1111	1110
0010	0010	0011	0000	0001	0110	0111	0100	0101	1010	1011	1000	1001	1110	1111	1100	1101
0011	0011	0010	0001	0000	0111	0110	0101	0100	1011	1010	1001	1000	1111	1110	1101	1100
0100	0100	0101	0110	0111	0000	0001	0010	0011	1100	1101	1110	1111	1000	1001	1010	1011
0101	0101	0100	0111	0110	0001	0000	0011	0010	1101	1100	1111	1110	1001	1000	1011	1010
0110	0110	0111	0100	0101	0010	0011	0000	0001	1110	1111	1100	1101	1010	1011	1000	1001
0111	0111	0110	0101	0100	0011	0010	0001	0000	1111	1110	1101	1100	1011	1010	1001	1000
1000	1000	1001	1010	1011	1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0110	0111

100 1	100 1	100 0	101 1	101 0	110 1	110 0	111 1	111 0	000 1	000 0	001 1	001 0	010 1	010 0	011 1	010 0
101 0	101 0	101 1	100 0	100 1	111 0	111 1	110 0	110 1	001 0	001 1	000 0	000 1	011 0	011 1	010 0	010 1
101 1	101 1	101 0	100 1	100 0	111 1	111 0	110 1	110 0	001 1	001 0	000 1	000 0	011 1	011 0	010 1	010 0
110 0	110 0	110 1	111 0	111 1	100 0	100 1	101 0	101 1	010 0	010 1	011 0	011 1	000 0	000 1	001 0	001 1
110 1	110 1	110 0	111 1	111 0	100 1	100 0	101 1	101 0	010 1	010 0	011 1	011 0	00 01	00 00	001 1	001 0
111 0	111 0	111 1	110 0	110 1	101 0	101 1	100 0	100 1	011 0	011 1	010 0	010 1	001 0	001 1	000 0	000 1
111 1	111 1	111 0	110 1	110 0	101 1	101 0	100 1	100 0	011 1	011 0	010 1	010 0	001 1	001 0	000 1	000 0

For multiplication table

*	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
0001	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0000	0010	0100	0110	1000	0110	1100	1110	0001	0011	0101	0111	1001	1101	1011	1111
0011	0000	0011	0110	0101	1100	1111	1010	1001	1001	1010	1111	1100	0101	0110	0011	0000
0100	0000	0100	1000	1100	0001	0101	1001	1101	0010	0110	0110	1110	0011	0111	1011	1111
0101	0000	0101	0110	1111	0101	0000	1111	1010	1010	1111	0000	0101	1111	1010	0101	0000
0110	0000	0110	1100	1010	1001	1111	1101	1111	0011	0110	1111	1111	1011	1011	1111	1111
0111	0000	0111	1110	1001	1101	1010	1111	0100	1011	1100	0101	0010	0010	0001	1000	1111
1000	0000	1000	0001	1001	0010	1010	0011	1011	0100	1100	0101	1101	0110	1110	0111	1111
1001	0000	1001	0011	1010	0110	1111	0110	1100	1100	0101	1111	1100	1010	0011	1001	0000
1010	0000	1010	0101	1111	0110	0000	1111	0101	0101	1111	0101	1111	1111	1111	1111	1111
1011	0000	1011	0111	1100	1110	0101	1111	0010	1101	1100	1111	0001	0011	1000	0100	1111
1100	0000	1100	1001	0101	0011	1111	1011	0110	0110	1010	1111	0011	0101	1001	1100	0000
1101	0000	1101	1101	0110	0111	1010	1011	0001	1110	0011	1111	1000	1001	1111	1111	1111
1110	0000	1110	1011	0011	1011	0101	1111	1000	0111	1001	1111	0100	1100	1111	0001	1111

1111	0000	1111	1111	0000	1111	0000	1111	1111	1111	0000	1111	1111	0000	1111	1111	0000

From the above table non trival zeros of R are:
0011*1111=0000
0101*0101=0000
0101*1010=0000
0101*1111=0000
1001*1111=0000
1010*1111=0000
1100*1111=0000
1111*0011=0000
1111*0101=0000
1111*1001=0000
1111*1100=0000
1111*1111=0000
Therefore non trivial divisors of zeros are 0011, 0101, 1001, 1010, 1100, 1111

Hence the non trivial divisors of zero in R are:

$x+1$, x^2+1 , x^3+1, x^3+x, x^3+x^2 , x^3+x^2+x+1;
There are 6 non trivial divisors of zeros for the above R.