Assignment - 3

1)

*	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	b	a
d	c	d	a	b

* b must be the identity element since $b^2 = b$
* Hence we can fill the rows and columns with b in it.
* Filling in the rest using sudoku rules gives us the table on the left.
* Since $a^2 = b^2 = c^2 = d^2 = 1^2$, we can conclude that $\{a, b, c, d\}$ is isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, with $b = (0,0)$ and $a, c, d = (0,1), (1,0)$, and $(1,1)$ symmetrically

~~* $b^2 = b$~~

~~$\Rightarrow b = 0$ or 1~~

~~* $a^2 = b = 0$ or 1~~

~~$\Rightarrow a = 0, 2, 1, 3$~~

~~* $c * d = a$~~

2) * To show a set is a group, we ~~to~~ show the 4 properties below :-

1) <u>Closure</u> :- $x_1, x_2 \in S \Rightarrow x_1 x_2 \in S$.

$$x_1^d = x_2^d = e$$

$$\Rightarrow x_1^d x_2^d = e$$

$$\Rightarrow x_1 x_1 x_1 \cdots x_1 x_2 x_2 \cdots x_2 = e$$

$$* \Rightarrow x_1 x_2 x_1 x_2 \cdots x_1 x_2 = e$$

$$\Rightarrow (x_1 x_2)^d = e$$

$$\Rightarrow (x_1 x_2) \in S$$

Note that the starred step (*) can only be performed if G is commutative.

$\therefore$ G has to be an abelian group.

2) <u>Associativity</u> :- Since G is a group, for any $g_1, g_2, g_3 \in G$,

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$$

Hence S is also associative.

3) Identity: $e^d = e$

$\Rightarrow e \in S$.

4) Inverse: For any $x \in S$,

$x^d = e$

$\Rightarrow x^d x^{-d} = x^{-d}$

$\Rightarrow e = (x^{-1})^d$

$\Rightarrow (x^{-1})^d = e$

$\therefore \forall x \in S, x^{-1} \in S$.

* There for any Abelian Group $(G, *)$, the set $S = \{x \in G \mid x^d = e\}$ forms a subgroup of G.

3) * We know that any permutation $p \in S_n$ can be represented as a product of disjoint cycles.

$\therefore$ It is enough to prove that any cycle $\sigma = (a_1 a_2 \dots a_k) \in \langle \pi_1, \pi_2 \rangle$,

where $\pi_1 = (1\ 2)$ and $\pi_2 = (1\ 2\ \dots\ n)$

* First, we claim that $\forall\ i$, $(1\ i) \in \langle \pi_1, \pi_2 \rangle$ using induction on

$(1\ i), (2\ \dots\ i{-}1\ 1\ i\ \dots\ n) \in \langle \pi_1, \pi_2 \rangle$

P<u>roof</u> by I<u>nduction</u>:

→ Base case is trivially true

→ Assume that the statement is true for ~~$\forall\ i \in n$~~ some i.

* $\Rightarrow (1\ i)(2\ \dots\ i{-}1\ 1\ i\ \dots\ n) = (2\ \dots\ i\ 1\ i{+}1\ \dots\ n)$

$\Rightarrow (2\ \dots\ i\ 1\ i{+}1\ \dots\ n) \in \langle \pi_1, \pi_2 \rangle$

* Since S_n is a finite group,

$\forall\ a \in \langle \pi_1, \pi_2 \rangle$, $a^{-1} \in \langle \pi_1, \pi_2 \rangle$

* $\Rightarrow (2\ \dots\ i\ 1\ i{+}1\ \dots\ n)^{-1}(1\ i)(2\ \dots\ i\ 1\ i{+}1\ \dots\ n) = (1\ i{+}1)$

$\therefore (1\ i{+}1) \in \langle \pi_1, \pi_2 \rangle$

* $\therefore$ By induction, we have $\forall\ i$, $(1\ i) \in \langle \pi_1, \pi_2 \rangle$

* Since $(1\ i) \in \langle \pi_1, \pi_2 \rangle \ \forall i$

$\Rightarrow (i\ j) = (1\ i)(1\ j)(1\ i) \in \langle \pi_1, \pi_2 \rangle$

$\Rightarrow (i\ j) \in \langle \pi_1, \pi_2 \rangle \ \forall i, j$

* $\therefore$ ~~any~~ $\forall\ \sigma = (a_1 a_2 \dots a_k)$, we have

$\Rightarrow \sigma = (a_k\ a_1)(a_{k-1}\ a_1) \dots (a_2\ a_1)$

$= \prod (i\ j)$

$\Rightarrow \sigma \in \langle \pi_1, \pi_2 \rangle \ \forall \sigma$

H.P.

* Since any permutation $\pi \in S_n$ can be represented as above, we have

$S_n \subseteq \langle \pi_1, \pi_2 \rangle$ and $\langle \pi_1, \pi_2 \rangle \subseteq S_n$

$\Rightarrow \langle \pi_1, \pi_2 \rangle = S_n$

H.P.

i) * Given that $M \in GL_2(\mathbb{Z}_p)$, the set of all 2×2 non singular matrices

* $GL_2(\mathbb{Z}_p)$ forms a group under multiplication since it satisfies

→ Closure :- $\forall\, A, B \in GL_2(\mathbb{Z}_p)$, if $|A| \neq 0$ & $|B| \neq 0$, $\Rightarrow |AB| \neq 0$. $\therefore AB \in GL_2(\mathbb{Z}_p)$

→ Associativity :- $\forall\, A, B, C \in GL_2(\mathbb{Z}_p)$, $A\cdot(B\cdot C) = (A\cdot B)\cdot C$.

→ Identity : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $\forall\, A \in GL_2(\mathbb{Z}_p)$, $I\cdot A = A\cdot I = A$ & $|I| \neq 0$. $\Rightarrow I \in GL$

→ Inverse :- By definition $\forall\, A \in GL_2(\mathbb{Z}_p)$, $\exists\, B \in GL_2(\mathbb{Z}_p)$ s.t. $AB = I$, i.e. $B = A^{-1}$

* Let $A \in GL_2(\mathbb{Z}_p)$

$\Rightarrow A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\Rightarrow |A| = ad - bc$.

$\Rightarrow$ Number of ways to choose a, b, c, d s.t. $|A| \neq 0$ is $p^4 - p^3$.

$\Rightarrow |GL_2(\mathbb{Z}_p)| = p^4 - p^3$

(1) * Now since $GL_2(\mathbb{Z}_p)$ is a finite group, by Lagrange's Th^m, we have

$$\forall\, M \in GL_2(\mathbb{Z}_p),\ M^{|GL_2(\mathbb{Z}_p)|} = I$$

$$\Rightarrow M^{p^4 - p^3} = I \quad \forall\, M \in GL_2(\mathbb{Z}_p).$$

(2) * $\therefore n = p^4 - p^3$

5) * We know that

$$x^{p^q} - x = \prod_{d \mid q} \left(\prod \text{irreducable polynomials of degree } d\right)$$

$$\Rightarrow x^{p^q} - x = \cancel{\prod_{d \neq q}} \left(\prod_{d=1} \text{polynomials}\right)\left(\prod_{d=q} \text{irreducable polynomials}\right)$$

p irreducible polynomials of degree 1.

$$\Rightarrow \text{degree}\left(\prod_{d=q} \text{irreduciable polynomials}\right) = p^q - p$$

$$\Rightarrow \text{no. of irreducible polynomials of degree } q = \frac{p^q - p}{q}$$

6) * We can see that $f(x) = x^2 + x + 2$ is an irreducible polynomial of degree 2 in $\mathbb{Z}_5$. since none of $f(0), f(1), f(2), f(3), f(4) = 0$.

* $\Rightarrow \mathbb{Z}_5[x] / f(x)$ is a finite field of order 25
* $\Rightarrow x^{24} \equiv 1 \pmod{f}$ (Using Fermat's Little Th^m)

$\Rightarrow x^{2022} \equiv x^6 \pmod{f}$

* $x^2 + x + 2 \equiv 0 \pmod{f}$

$\Rightarrow x^2 \equiv (-x-2) \pmod{f}$

$\Rightarrow x^4 \equiv (3x+2) \pmod{f}$

$\therefore x^6 \equiv (3x+2)(-x-2) \pmod{f}$

$\Rightarrow x^6 \equiv 2 \pmod{f}$

$\therefore x^{2022} \equiv 2 \pmod{f}$ in $\mathbb{Z}_5$

7) Any Finite Field $\mathbb{F}$ of order p^k and generator α can be represented as

$$\mathbb{F}_q = \{0, \alpha, \alpha^2, \dots, \alpha^{p^k-1} = 1\} \qquad -①$$

(a) Using ①, we have

$$\sum_{a \in \mathbb{F}_q} a = 0 + \sum_{i=1}^{p^k-1} \alpha^i$$
$$= \frac{(\alpha - \alpha^{p^k})}{(1-\alpha)}$$
$$= \frac{(\alpha - \alpha)}{1-\alpha} \qquad \text{(By Lagrange's Th}^m \text{ (Since } |F| = p^k))$$
$$= 0$$

(b) Since $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, using ①, we have

$$\prod_{a \in \mathbb{F}_q^*} a = \prod_{i=1}^{p^k-1} \alpha$$
$$= \alpha^{\sum_{i=1}^{p^k-1} i}$$
$$= \alpha^{\frac{(p^k-1)p^k}{2}}$$
$$= \left(\alpha^{\frac{p^k-1}{2}}\right)^{p^k}$$
$$= (-1)^{p^k} \qquad \left(\text{Since } \alpha^{p^k-1} = 1, \Rightarrow \alpha^{\frac{p^k-1}{2}} = 1 \text{ or } -1. \text{ But } \alpha^{\frac{p^k-1}{2}} \neq 1 \text{ since } \alpha \text{ is a generator} \Rightarrow \alpha^{\frac{p^k-1}{2}} = -1\right)$$
$$= -1$$

(c) $$\sum_{a \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_q, a \neq b} ab = \sum_{a \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_q} ab - \sum_{a \in \mathbb{F}_q} a^2$$
$$= \sum_a a \sum_b b - \sum_a a^2$$
$$= \left(\sum_a a\right)^2 - \sum_a a^2$$
$$= 0 - \sum_{a \in \mathbb{F}_q} a^2 \qquad \text{(Using (a))}$$

Using ①,

$$\sum_{a \in \mathbb{F}_q} a^2 = 0 + \sum_{i=1}^{p^k-1} \alpha^{2i}$$
$$= \frac{(\alpha^2 - \alpha^{2p^k})}{(1-\alpha^2)} \qquad ((1-\alpha^2)^{-1} \text{ exists } \forall\, q > 3)$$
$$= \frac{(\alpha^2 - \alpha^2)}{(1-\alpha^2)} = 0 \qquad \text{(By Lagrange's Th}^m)$$

$$\therefore \sum_{a \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_q, a \neq b} ab = 0 - 0 = 0$$