Name: Rojat Rajesh Shetty
CWID: 10477484

Assignment-4

Exercise 4.1: consider a cartesian product $G = \mathbb{Z} \times \mathbb{Z} = \{(\alpha, x) \mid \alpha, x \in \mathbb{Z}\}$ and a binary operation $\cdot$ on G defined as follows:

$$(\alpha_1, x_1) \cdot (\alpha_2, x_2) = (\alpha_1 + \alpha_2, (-1)^{\alpha_2} x_1 + x_2)$$

(1) prove that $(G, \cdot)$ is a group.

The properties of a group are

① $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for $a, b, c \in G$.

② has a Identity element :

③ There is a inverse. a has inverse b s.t $a^{-1}b$, $ab = 1$.

① Lets check for associative.

$\Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$ * both sides by (α_3, x_3)

$$((\alpha_1, x_1) \cdot (\alpha_2, x_2)) \cdot (\alpha_3, x_3) = (\alpha_1 + \alpha_2, (-1)^{\alpha_2} x_1 x_2) \cdot (\alpha_3, x_3)$$

$$= (\alpha_1 + \alpha_2 + \alpha_3, (-1)^{\alpha_3} ((-1)^{\alpha_2} x_1 + x_2) + x_3)$$

$$(\alpha_1, x_1) \cdot ((\alpha_2, x_2) \cdot (\alpha_3, x_3)) = (\alpha_2 + \alpha_3, (-1)^{\alpha_3} x_2 + x_3) \cdot (\alpha_1, x_1)$$

$$(\alpha_1, x_1) \cdot (\alpha_2 + \alpha_3, (-1)^{\alpha_3} x_2 + x_3) = (\alpha_1 + \alpha_2 + \alpha_3, (-1)^{\alpha_2 + \alpha_3} x_1 + (-1)^{\alpha_3} x_2 + x_3)$$

$$(\alpha_1 + \alpha_2 + \alpha_3, (-1)^{\alpha_3} ((-1)^{\alpha_2} x_1 + x_2) + x_3) = (\alpha_1 + \alpha_2 + \alpha_3, (-1)^{\alpha_2 + \alpha_3} x_1 + (-1)^{\alpha_3} x_2 + x_3)$$

$\therefore$ It is associative.

2. <u>Identity element</u>

so Lets assume (d, e) as identity element.

ST $(\alpha_1, x_1) \cdot (d, e) = (\alpha_1, x_1)$

$(\alpha_1 + d, (-1)^d x_1 + e) = (\alpha_1, x_1)$

$\alpha_1 + d = \alpha_1$ $\rightarrow$ so we can say that $d = 0$

$(-1)^d x_1 + e = x_1$ since $d = 0$ so $e = 0$

$e = x - x = 0$

$\therefore (d, e) = (0, 0)$.

It has identity element.

---

3. <u>Inverse check</u>. $(\alpha_1, x_1) \cdot (\alpha_1, x_1) = (e, f)$

$a \cdot b = 0$. so b is a^{-1}.

$(\alpha_1, x_1)^{-1}$ or

$(\alpha_1, x_1) \cdot (\alpha_1^{-1}, x_1^{-1}) = (0, 0)$

~~so it~~

$(\alpha_1 + \alpha_1^{-1}, (-1)^{\alpha_1^{-1}} x_1 + x_1^{-1}) = (0, 0)$

so to prove this to be true,

$\alpha_1 + \alpha^{-1} = 0$ so $\alpha^{-1} = -\alpha$

$(-1)^{\alpha^{-1}} x_1 + x_1^{-1} = 0$ so $x_1^{-1} = -(-1)^{\alpha} x_1$

To verify if this is true,

$(\alpha_1, x_1) \cdot (-\alpha_1, -(-1)^{-\alpha} x_1) = (\alpha_1 + -\alpha_1, (-1)^{-\alpha_1} x_1 + -(-1)^{\alpha} x_1)$

$= \alpha - \alpha = 0$

$(-1)^{-\alpha_1} x_1 + -(-1)^{\alpha_1} x_1 = 0$.

so, inverse exists.

$\therefore (G, \cdot)$ is a group.

and since $G = \mathbb{Z} \times \mathbb{Z}$ it is closed. as product is also in $\mathbb{Z}$.

(checking commutative group).

2] is $(G, \circ)$ abelian?

To prove $(G, \circ)$ is abelian, we need to show

$$a \cdot b = b \cdot a$$

$$(\alpha_1, x_1) \cdot (\alpha_2, x_2) = (\alpha_2, x_2) \cdot (\alpha_1, x_1)$$

$$(\alpha_1 + \alpha_2, (-1)^{\alpha_2} x_1 + x_2) \neq (\alpha_1 + \alpha_2, (-1)^{\alpha_1} x_2 + x_1)$$

so, from this we can say that it is <u>not</u> abelian

---

3) Is $(G, \cdot)$ finite? $\quad g \in G \cdot g^n = e$.

$(G, \cdot)$ is not finite as $G = \mathbb{Z} \cdot \mathbb{Z}$ & $\mathbb{Z}$ is infinite.

so, the answer is <u>no</u>. $(G, \cdot)$ is not finite.

4.) Prove that every cyclic group is abelian. Then use (2) to prove $(G, \cdot)$ is not cyclic.

To prove that it is cyclic, $G = \{(\alpha, x)^n ; n \in \mathbb{Z}\}$

so $(\alpha, x)^2 = (\alpha, x) \cdot (\alpha, x)$ $\qquad (\alpha, x)^n \to$ for some (α, x) that generates center G.

$$= (\alpha + \alpha, (-1)^{\alpha} x + x)$$

if $n = \alpha$ $\left(n\alpha, (-1)^{(n-1)\alpha (n-2)\alpha} + (-1) \ldots (-1)^{\alpha} + (-1)^{\alpha}\right)$

so from this we can say, every cyclic group is abelian

since G is not even abelian, $\therefore$ G is not cyclic,

inverse of it can be true or false.

$\therefore$ $(G, \cdot)$ is not cyclic.

---

5) Does $(G, \cdot)$ have torsion?

So, to have torsion, we should have some $n \{n \in \mathbb{Z}\}$

s.t. $(\alpha, x)^n = (0, 0)$ $\qquad$ so we can say

non trivial elements have finite order

But, in this case, only $(0, 0)^n = (0, 0)$.

$\therefore$ we can say that $(G, \cdot)$ doesnot have torsion //

(6) Is $\pi_1 : G \to \mathbb{Z}$ defined by $(\alpha, x) \xrightarrow{\pi_1} \alpha$ a homomorphism?

$\Rightarrow$ $\pi_1 : G \to \mathbb{Z}$ where $(\alpha, x) \xrightarrow{\pi_1} \alpha$.

$G : \{ (\alpha, x) \mid \alpha_1, x \in \mathbb{Z} \}$

$= (\alpha_1 + \alpha_2, (-1)^{\alpha_2} x_1 + x_2)$

for some $a, b \in G$.

$\pi_1 [(a_1 a_2) \cdot (b_1, b_2)] = \pi (a_1, a_2) + \pi (b_1, b_2)$

$\pi [a_1 + b_1, (-1)^{b_1} a_2 + b_2] = \pi (a_1, a_2) + \pi (b_1, b_2)$

$\underline{a_1 + b_1 = a_1 + b_1}$

This tell us it is homomorphism

---

(7). is $\pi_2 : G \to \mathbb{Z}$ defined by $(\alpha, x) \xrightarrow{\pi_2} x$ a homomorphism

$\pi_2 : G \to \mathbb{Z}$ where we know $(\alpha, x) \xrightarrow{\pi_2} x$ for some $a, b \in G$

$\pi_2 ((a_1, a_2) \cdot (b_1, b_2)) = \pi_2 (a_1, a_2) + \pi (b_1, b_2)$

$\pi_2 (a_1 + b_1, (-1)^{b_1} a_2 + b_2) = \pi_2 (a_1, a_2) + \pi_2 (b_1, b_2)$

$(-1)^{b_1} a_2 + b_2 \neq a_2 + b_2$.

so it is not homomorphism.

4.2 Exercise

$\Rightarrow$ Find $|2|$ in U_{67}.

we know that value of $n = 67$,

so Lets calculate $\phi(n) = n - 1 = 67 - 1 = 66$.

we have to calculate PPF $(66) = 2 \times 3 \times 11$.

$\frac{66}{2} = 33$

$2^{33} \equiv_{67} 66 \neq 1$

$\frac{66}{3} = 22$

$2^{33} \bmod 67$

$= 8589934592 \bmod 67$

$= \underline{\underline{66}}$

$2^{22} \equiv_{67} 33 \neq 1$

$\frac{66}{11} = 6$

$2^6 \equiv_{67} 64 \neq 1$

$2^{22} \bmod 67$

$= 4194304 \bmod 67$

$\Rightarrow 33$.

since none of the above values give remainder of 1, we can conclude

$\underline{|2| = 66}$

$2^6 \bmod 67 = 64$.

Exercise 4.3.

Is 2 a primitive root modulo 31?

* To check if a is a primitive root modulo n.

① we need to check $\gcd(a, n) = 1$ must be true.

② compute $PPF(\varphi(n)) = p_1^{a_1} \cdots p_k^{a_k}$

③ check if $a^{\frac{\varphi(n)}{p_i}} \equiv_n 1$ (each must be false)

④ if all conditions are satisfied, then output yes.

$\therefore$ ① $\gcd(2, 31) = 1$

② $PPF(30) = 2 \cdot 3 \cdot 5$.

$2^{\frac{30}{2}} \equiv_{31} 1$

$2^{\frac{30}{3}} \equiv_{31} 1$

$2^{\frac{30}{5}} \equiv_{31} 2$

the output is false.

$\therefore$ 2 is not primitive root modulo 31.

Exercise 4.4

consider a set $G = \{x_1, x_2, \cdots x_8\}$ of eight elements equipped with a binary operation $\cdot$ defined by the multiplication table shown below. $(G, \cdot)$ is a group.

$\cdot$	x_4	x_3	x_7	x_1	x_2	x_6	x_5	x_6
x_4	x_2	x_6	x_5	x_8	x_4	x_3	x_7	x_1
x_3	x_1	x_4	x_8	x_7	x_3	x_2	x_1	x_+
x_7	x_5	x_1	x_4	x_6	x_7	x_8	x_2	x_3
x_1	x_8	x_5	x_3	x_4	x_1	x_7	x_6	x_2
x_2	x_4	x_3	x_7	x_1	x_2	x_6	x_5	x_8
x_6	x_3	x_2	x_1	x_5	x_6	x_4	x_8	x_7
x_5	x_7	x_8	x_2	x_3	x_5	x_1	x_4	x_6
x_8	x_1	x_7	x_6	x_2	x_8	x_5	x_9	x_4

(1) which element is the identity of G?

x_2 is the identity element

(2) Is G abelian? why.

we know that for abelian, it should satisfy

$(a \cdot b) = (b \cdot a)$

$x_3 \cdot x_7 = x_4$

$x_7 \cdot x_3 = x_1$

so it is abelian.

so $x_4 \neq x_1$.

(3) Find $|x_3|$

$|x_3| = x_3 \cdot x_3$

$= x_4$.

$x_4 \cdot x_3 = x_6$

$x_6 \cdot x_2 = x_2$

Hence, we can conclude $n=4$.

$\therefore$ order of $|x_3| = 4$

(4) find $\langle x_4 \rangle$.

so: $x_4 \cdot x_4 = x_2$.

$x_2 \cdot x_4 = x_4$.

$\{x_4, x_2\}$

$\boxed{\begin{array}{l} a \cdot i = a \\ i a = a \end{array}}$

$\langle x \rangle$ is the minimal subgroup of G containing x.

$\langle a \rangle$ is the minimal subgroup of G containg a.

(5) find the coset $x_6 \cdot \langle x_4 \rangle$

$\langle x_4 \rangle = \{ x_6, x_2)$

$x_6 \cdot \{ x_4, x_2 \}$

$\therefore x_6 \cdot x_4 = x_3$

$\& \; x_6 \cdot x_2 = x_6$

$\therefore \{ x_3, x_6 \}$ //

---

(6) Find x_5^{-1}

$\boxed{a^{-1} = b}$ $\boxed{a \cdot b = b \cdot a = e}$

so satisfying this, we can say that

$x_5 \cdot x_7 = x_2$ & $x_7 \cdot x_5 = x_2$

~~where x_2 is the identity element~~

---

(7) Is x_7 a primitive element?

$x_7 \cdot x_7 = x_4$

$x_4 \cdot x_7 = x_5$

$x_5 \cdot x_7 = x_2$

$x_2 \cdot x_7 = x_7$

From this, we can conclude x_7 is not primitive.

---

(8) is G cyclic?

$x_4 = x_4 \cdot x_4 = x_2$

$x_2 = x_4 = x_4$

$x_7 = x_7 \cdot x_7 = x_4$

$x_4 \cdot x_7 = x_5$

$x_5 \cdot x_7 = x_2$

$x_2 \cdot x_7 = x_7$

$x_3 = x_3 \cdot x_3 = x_4$

$x_4 \cdot x_3 = x_6$

$x_6 \cdot x_3 = x_2$

$x_2 \cdot x_3 = x_3$

$x_1^2 = x_1 \cdot x_1 = x_4$

$x_4 \cdot x_1 = x_8$

$x_8 \cdot x_1 = x_2$.

$x_2 \cdot x_1 = x_1$.

$x_2^2 = x_2 \cdot x_2 = x_2$.

$x_5^2 = x_5 \cdot x_5 = x_4$

$x_4 \cdot x_5 = x_7$

$x_7 \cdot x_5 = x_2$

$x_2 \cdot x_8 = x_5$.

$x_6^2 = x_6 \cdot x_6 = x_4$

$x_4 \cdot x_6 = x_3$

$x_3 \cdot x_6 = x_2$

$x_2 \cdot x_6 = x_6$

$x_8^2 = x_8 \cdot x_8 = x_4$

$x_4 \cdot x_8 = x_1$

$x_1 \cdot x_8 = x_2$

$x_2 \cdot x_8 = x_8$.

so, From the above result we can say that,
since, none of the element generate G,

G is not cyclic