* Show that $(\{1, 0, -1, 2\}, +)$ is not group.

* Is $(\{1, 0, -1, 2\}, +)$ group?

proof: Let $A = (\{1, 0, -1, 2\})$

$(A, *) = (A, +)$ is not closure, since

$1 + 2 = 3 \notin (A, +)$.

or

$2 \in A$, but $-2 \notin A$,

$\therefore (A, +)$ is not group.

* Is $(\mathbb{Z}, *)$ group, such that $a * b = a + b + 2 \; \forall a, b \in \mathbb{Z}$

proof:

① closure $\Longrightarrow \forall a, b \in \mathbb{Z} \Longrightarrow a + b + 2 \in \mathbb{Z}$.

② Associative: $\forall a, b, c \in \mathbb{Z}$

$$(a * b) * c = a * (b * c)$$
$$(a + b + 2) * c = a * (b + c + 2)$$
$$a + b + 2 + c + 2 = a + (b + c + 2) + 2$$
$$a + b + c + 4 = a + b + c + 4.$$

③ Identity: $a * e = e * a = a$

$a * e = a + e + 2 = a \Longrightarrow e = -2$

$e * a = e + a + 2 = a \Longrightarrow e = -2$

④ Inverse: $a * \bar{a}^{1} = \bar{a}^{1} * a = e$, let b the inverse of a.

$a * b = a + b + 2 = -2 \Longrightarrow a + b = -4 \Longrightarrow b = -4 - a$.

$b * a = b + a + 2 = -2 \Longrightarrow b + a = -4 \Longrightarrow b = -4 - a$.

Theorem: Let G be a group, then the following are equivalent

1. G is abelian
2. $(a*b)^{-1} = a^{-1} * b^{-1}$
3. $(a*b)^2 = a^2 * b^2$

proof: ① $\longrightarrow$ ②

$(a*b)^{-1} = b^{-1} * a^{-1}$ ④, since G is abelian

$\therefore (a*b)^{-1} = b^{-1} * a^{-1} = a^{-1} * b^{-1}$

② $\longrightarrow$ ③

$$(a*b)^2 = (a*b)(a*b) = a*(b*a)*b.$$

$$= a*((b*a)^{-1})^{-1}*b \quad [\, a = (a^{-1})^{-1} \,].$$

$$= a*(a^{-1}*b^{-1})^{-1}*b = a*(a^{-1})^{-1}*(b^{-1})^{-1}* = a*a*b*b \; [b$$

$$= a^2 * b^2$$

③ $\longrightarrow$ ① $(a*b)^2 = a^2 * b^2$

$$a*b*a*b = a*a*b*b$$

$$b*a = a*b$$

$\therefore G$ is abelian

* $a \equiv b \pmod n \Longrightarrow a - b = nk ; k \in \mathbb{Z}$

$x \equiv a \pmod n \Longrightarrow x - a = nk \Longrightarrow x = a + nk$.

* Find $[1], [3], [2], [-2], [5]$ if $n = 4$.

$[1] = \{ x \in \mathbb{Z} ; x = 1 + 4k \} ; k \in \mathbb{Z} = \{ 0, \pm 1, \pm 2, \ldots$

$[1] = \{ \ldots, -11, -7, -3, 1, 5, 9, 13, \ldots \}$

$[3] = \{ x \in \mathbb{Z} ; x = 3 + 4k ; k \in \mathbb{Z} \}$

$= \{ \ldots, -1, 3, 7, \ldots \}$

$[2] = \{ x \in \mathbb{Z} ; x = 2 + 4k ; k \in \mathbb{Z} \}$.

$= \{ \ldots, -10, -6, -2, 2, 6, 10, \ldots \}$

$[-2] = \{ x \in \mathbb{Z} ; x = -2 + 4k ; k = 0, \pm 1, \pm 2, \ldots \}$

$= \{ \ldots, -10, -6, -2, 2, 10, \ldots \}$

$[5] = \{ x \in \mathbb{Z} ; x = 5 + 4k ; k \in \mathbb{Z} \}$.

$= \{ \ldots, -3, 1, 5, 9, 13, \ldots \}$.

① The identity element of a group $(G,*)$ (abelian) is unique

Proof:

Let e, e' be the identity element.

$\therefore e'$ is identity element, then $e*e'=e$

$\therefore e$ is identity element, then $e'*e=e'$

$\therefore G$ abelian group.

$\therefore e*e'=e'*e$

$e=e'$

$\therefore$ The identity unique element.

② The inverse element of each element of a group $(G,*)$ is unique.

Proof: If a', a'' the inverse of a, then

$$a*a'=a'*a=e$$

and

$$a*a''=a''*a=e$$

$$\therefore a'*a=e=a''*a$$

$$\therefore a'=a''$$

$\therefore$ The inverse of a is unique.

③ Let G be a group and $a \in G$, then $(a^{-1})^{-1} = a$.

proof:- a inverse of a^{-1}

a^{-1} inverse of $(a^{-1})^{-1}$

but the inverse is unique $\Rightarrow a = (a^{-1})^{-1}$.

④ $(a*b)^{-1} = b^{-1} * a^{-1}$ $\forall$ $a, b \in G$.

proof:- $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b$

$= b^{-1}*e*b = b^{-1}*b = e$.

$(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1}$

$= a*a^{-1} = e$.

$\therefore b^{-1}*a^{-1}$ is inverse of $a*b$, but

$(a*b)^{-1}$ is inverse of $a*b$,

but the inverse is unique.

$\therefore (a*b)^{-1} = b^{-1}*a^{-1}$.

Theorem: Let $(G, *)$ be a group, then for each $a, b \in G$.

1- If $a * b = a * c$, then $b = c$

proof:- G is a group $\Longrightarrow \bar{a}^1 \in G$

$\bar{a}^1 * (a * b) = \bar{a}^1 * (a * c)$, as $*$ is associative,

so we have $(\bar{a}^1 * a) * b = (\bar{a}^1 * a) * c$. Thus,

$e * b = e * c$ which implies that $b = c$.

2- If $b * a = c * a$, then $b = c$.

proof:- G is a group $\Longrightarrow \bar{a}^1 \in G$.

$\therefore (b * a) * \bar{a}^1 = (c * a) * \bar{a}^1$, since G is associative,

then $b * (a * \bar{a}^1) = c * (a * \bar{a}^1)$

$b * e = c * e$ which implies that $b = c$.