Theorem: let $(G,*)$ is group and Let H a nonempty subset of G, Then H is a subgroup of G if ab^{-1} is in H for every $a,b \in H$.

---

example: Let $G=\{1,-1,i,-i\}$, $(G,\cdot)$ group
H be a nonempty subset of G such that:
$H=\{x \in G: x^2=e\}$, Prove that $(H,\cdot)$ is a subgroup of $(G,\cdot)$, $e=1$.

Solution: (We will prove $(H,\cdot)$ is a subgroup of $(G,\cdot)$ by above theorem)

here we have $e^2=e \Rightarrow e \in H \Rightarrow H \neq \emptyset$

Let $a,b \in H \Rightarrow a^2=e$ and $b^2=e$

Now we have to prove that $(ab^{-1})^2=e$

$\because (ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1}$
$= e\,e^{-1} = e$

$\therefore (ab^{-1})^2=e \Rightarrow ab^{-1} \in H$

$\therefore (H,\cdot)$ is a subgroup of $(G,\cdot)$

ملاحظة: لا يوجد زمرة لا تحتوي على زمرة جزئية لانه على الاقل يوجد زمر جزئية تافهة مثال على ذلك الزمرة $(Z_5-\{0\},\cdot)$ فان الزمر الجزئية تكون فقط

$H_1=\{1\}$
$H_2=(Z_5-\{0\})$

Example: $(\mathbb{Z}_{12},+)$ be a group and

$H_1 = \{0\}$

$H_2 = \mathbb{Z}_{12}$

$H_3 = \{0,2,4,6,8,10\}$, $H_4 = \{0,3,6,9\}$

$H_5 = \{0,4,8\}$, $H_6 = \{0,6\}$

Note that :

$H_3 \cup H_4 = \{0,2,3,4,6,8,9,10\}$ not ~~group~~ subgroup

$\because$ $8,3 \in H_3 \cup H_4 \Rightarrow 8+3 = 11 \notin H_3 \cup H_4$

$H_4 \cup H_5 = \{0,3,6,9,4,8\}$ not subgroup

$\because$ $6,4 \in H_4 \cup H_5 \Rightarrow 6+4 = 10 \notin H_4 \cup H_5$

Also note that:

$H_3 \cap H_4 = \{0,6\}$ is subgroup

$H_6 \cap H_3 = \{0,6\}$ is subgroup

$H_5 \cap H_3 = \{0,4,8\}$ is subgroup

Theorem: If $(H_1,*)$ and $(H_2,*)$ are subgroups of a group $(G,*)$ then $(H_1 \cup H_2,*)$ is a subgroup Iff $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

* المبرهنة بدون برهان.

ولكن للتحقيق على صحة المبرهنة انظر المثال أعلاه.

في $(\mathbb{Z}_{12},+)$ نلاحظ أن $H_5 \subseteq H_3$ وعليه يكون $H_5 \cup H_3$ subgroup of $(G,*)$

23

[redacted]

Theorem: If $(H_1, *)$ and $(H_2, *)$ are subgroups of a group $(G, *)$ then $(H_1 \cap H_2)$ is a subgroup of $(G, *)$

Proof:

$\because H_1 \neq \emptyset , H_2 \neq \emptyset$ ($\because H_1, H_2$ subgroups)

$\therefore H_1 \cap H_2 \neq \emptyset$

Let $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ and $a, b \in H_2$

$\because H_1$ is subgroup $\Rightarrow ab^{-1} \in H_1$

$\because H_2$ is subgroup $\Rightarrow ab^{-1} \in H_2$

$\therefore ab^{-1} \in H_1 \cap H_2$

$\therefore (H_1 \cap H_2, *)$ subgroup of $(G, *)$

H.W / ① find all subgroups of a group $(\mathbb{Z}_{24}, +)$

② find all subgroups of $(\mathbb{Z}_8, +)$

③ Prove that $H = \{0, 2, 4\}$ is subgroup of $(\mathbb{Z}_6, +)$

④ find the order of the group $(\mathbb{Z}_{12}, +)$ and find order each element in this group.

⑤ find the order of the group $(\mathbb{Z}_7, +)$ and the order of each element in this group.

Example: Let $G=\{e,a,b,c\}$ with $a^2=b^2=c^2=e$, $ab=c$, $ac=b$, $cb=a$, show that $(G,\cdot)$ be a group.

Solution:-

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

① $\forall a,b \in G \Rightarrow a\cdot b \in G$, G Closed

② $\forall a,b,c \in G \Rightarrow a\cdot(b\cdot c)=(a\cdot b)\cdot c$

③ $e=e$ $(\because e \in G)$

④ $(a)^{-1}=a$, $(b)^{-1}=b$, $(c)^{-1}=c$

Note: that the above group G is comm. group.

*الزمرة هنا تسمى (Klein 4-group)

Q/ find all subgroups of $G=\{e,a,b,c\}$

Sol:- $H_1=\{e\}$

$H_2=G$

$H_3=\{a^n : n\in\mathbb{Z}\}$

$=\{a^1, a^2, a^3, \dots\}$

$=\{a, e\}$

$H_4=\{b^n : n\in\mathbb{Z}\}=\{b, e\}$

$H_5=\{c^n : n\in\mathbb{Z}\}=\{c, e\}$

Definition:- Let H and K are subgroups of a group G. Then $H * K = \{ h * k : h \in H, k \in K \}$

For example in $(\mathbb{Z}_6, +)$, we have

$H_1 = \{0\}$

$H_2 = \mathbb{Z}_6$

$H_3 = \{0, 2, 4\}$

$H_4 = \{0, 3\}$, H_1, H_2, H_3, H_4 are all subgroups of $(\mathbb{Z}_6, +)$

$H_3 + H_4 = \{ h + k : h \in H_3, k \in H_4 \}$

$= \{ 2+3, 2+0, 4+3, 4+0, 0+3, 0+0 \}$

$= \{ 5, 2, 1, 4, 3, 0 \} = \mathbb{Z}_6$

Ex: Let $G = \{ e, a, a^2, a^3, \dots, a^7 \}$, $(G, \cdot)$ be a group. such that $a^8 = e$.

$H_1 = \{e\}$, $H_2 = G$

$H_3 = \{ e, a^2, a^4, a^6 \}$

$H_4 = \{ e, a^4 \}$

$\therefore H_3 \cdot H_4 = \{ e.e, e.a^2, e.a^4, e.a^6, a^4.e, a^4.a^2, a^4.a^4, a^4.a^6 \}$

$\Rightarrow H_3 \cdot H_4 = \{ e, a^2, a^4, a^6 \}$

ضرب تجمع الأسس

Definition:- Let $(G,*)$ be a group. The Center of G is the set:

$$\text{Cent}.G = \{a \in G : ax = xa, \forall x \in G\}$$

ex: find center of $(\mathbb{Z}_6, +)$

Sol^n:-

Note that $(\mathbb{Z}_6, +)$ Comm. group

$\therefore$ for any $a, b \in \mathbb{Z}_6$

$$\Rightarrow a+b = b+a$$

$$\Rightarrow \text{Cent}.G = \mathbb{Z}_6$$

ملاحظة: اذا كانت الزمرة ابدالية فان Center لتلك الزمرة هو الزمرة نفسها.

** . $\mathbb{Z}_n$ سواء كانت مع الضرب أو الجمع فان Cent $\mathbb{Z}_n$ يساوي $\mathbb{Z}_n$ نفسها لانها ابدالية مع الضرب والجمع.

Q/ find center of $(S_3, \circ)$

Sol^n:- $\text{Cent}(S_3) = \{f_1\}$, $f_1 \circ f_i = f_i \circ f_1$; $i = 1:6$

$\because$ f_1 ابدالي مع كل العناصر في S_3 .

ex/ find Center of $G = \{1, -1, i, -i\}$

Sol^n: Since this group is Comm. group

$\therefore$ $\text{Cent}.G = G$

27

Theorem :- Let $(G, *)$ be a group, Then

$$Cent(G) = G \Longleftrightarrow G \text{ is Commutative group}$$

Proof:-

$(\Rightarrow)$ $\forall a \in G \Rightarrow a \in Cent(G)$

$\therefore a * x = x * a \;,\; \forall x \in G$

$\therefore a * x = x * a \;,\; \forall x, a \in G$

$\therefore G$ is Commutative

$(\Leftarrow)$ suppose that G is Comm. group T.P $cent(G) = G$

(i.e, T.P $Cent(G) \subseteq G \wedge G \subseteq cent(G)$)

By definition of $Cent(G)$ we have $cent(G) \subseteq G$

Now T.P $G \subseteq Cent(G)$

Let $x \in G$, G is Commutative group.

$\Rightarrow x * a = a * x \;,\; \forall a \in G$

$\therefore x \in Cent(G)$

$\therefore G \subseteq cent(G)$

$\therefore cent(G) = G$

H.W: find Center of a group $(\mathbb{Z}_{100}, +)$?

Cyclic Group :- الزمرة الدوارة

Definition:- Let $(G,*)$ be a group and $a \in G$, the cyclic subgroup of G generated by the element a is denoted by $\langle a \rangle$ and defined as

$$\langle a \rangle = \{ a^K : K \in \mathbb{Z} \} = \{ \dots, a^{-1}, a^0, a^1, \dots \}$$

Definition:- A group $(G,*)$ is called cyclic group generated by a iff $\exists\, a \in G$ such that

$$G = \langle a \rangle = \{ a^K : K \in \mathbb{Z} \}$$

* تسمى الزمرة دائرية أو دوارة اذا أمكن توليدها من عنصر واحد او اذا وجد عنصر يولدها.

Example:- In $(\mathbb{Z}_9, +)$ find the cyclic subgroup generated by $2, 3, 1$

Sol^n:-

$$\langle 2 \rangle = \{ a^K : K \in \mathbb{Z} \} = \{ \dots, (2)^{-3}, (2)^{-2}, (2)^{-1}, (2)^0, (2)^1, (2)^2, \dots \}$$

$$= \{ \dots, 3, 5, 7, 0, 1, 2, \dots \}$$

$$= \{ 0, 1, 2, \dots, 8 \} = \mathbb{Z}_9$$

$\therefore (\mathbb{Z}_9, +)$ is cyclic generated by 2

$$\langle 3 \rangle = \{ \dots, (3)^{-2}, (3)^{-1}, (3)^0, (3)^1, (3)^2, (3)^3, \dots \}$$

$= \{ 0, 3, 6 \}$ is cyclic subgroup of $\mathbb{Z}_9$

$$\langle 1 \rangle = \{ \dots, (1)^{-2}, (1)^{-1}, (1)^0, (1)^1, (1)^2, \dots \}$$

$$= \{ \dots, 6, 7, 8, 0, 1, 2, 3, \dots \}$$

$$= \{ 0, 1, 2, 3, 4, 5, 6, 7, 8 \} = \mathbb{Z}_9$$

$\therefore (\mathbb{Z}_9, +)$ is cyclic generated by 1.

Example: In $(\mathbb{Z},+)$ find cyclic group generated by $1, -1$

Solution:-

$$\langle 1\rangle = \{1^k : k\in\mathbb{Z}\} = \{\dots, 1^{-3}, 1^{-2}, 1^{-1}, 1^{0}, 1^{1}, 1^{2}, 1^{3}, \dots\}$$
$$= \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$
$$= \mathbb{Z}$$

$$\langle -1\rangle = \{(-1)^k : k\in\mathbb{Z}\}$$
$$= \{\dots, (-1)^{-3}, (-1)^{-2}, (-1)^{-1}, (-1)^{0}, (-1)^{1}, (-1)^{2}, (-1)^{3}, \dots\}$$
$$= \{\dots, 2, 1, 0, -1, -2, \dots\} = \mathbb{Z}$$

$\therefore$ $(\mathbb{Z},+)$ is cyclic group generated by $1, -1$.

Example:- consider $(\mathbb{Z}_6, +)$

$\langle 1\rangle = \{1, 2, 3, 4, 5, 0\}$, it's subgroup generated by 1 (cyclic subgroup)

$\langle 2\rangle = \{2, 4, 0\}$ it's cyclic subgroup generated by 2.

$\langle 3\rangle = \{3, 0\}$, cyclic subgroup generated by 3

$\langle 4\rangle = \{4, 2, 0\}$, cyclic subgroup generated by 4

$\langle 5\rangle = \{5, 4, 3, 2, 1, 0\}$; cyclic subgroup generated by 5.

note that $(\mathbb{Z}_6, +)$ cyclic group generated by $1, 5$, since $\langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6$

Theorem:- Every cyclic group is Commutative

Proof:- Let $(G,*)$ be a cyclic group

$\therefore \exists\, a \in G$ such that $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$

T.P G is Commutative group

Let $x, y \in G$, (T.P $x * y = y * x \ \forall\, x, y \in G$)

$\because x \in G = \langle a \rangle \Rightarrow x = a^m, m \in \mathbb{Z}$

and $y \in G = \langle a \rangle \Rightarrow y = a^n, n \in \mathbb{Z}$

$\therefore x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$

$\therefore G$ is Commutative group.

Note: the Converse of above theorem is not true. for example:-

Let $G = \{e, a, b, c\}$, $(G, \circ)$ with $a^2 = b^2 = c^2 = e$

in this group We have

$\forall\, a, b \in G \Rightarrow a \circ b = b \circ a$

$\therefore (G, \circ)$ is Comm. group.

But $(G, \circ)$ is not cyclic group Since

$\langle e \rangle = \{e\} \neq G$

$\langle a \rangle = \{a^k ; k \in \mathbb{Z}\} = \{e, a\} \neq G$

$\langle b \rangle = \{b^k : k \in \mathbb{Z}\} = \{e, b\} \neq G$

$\langle c \rangle = \{c^k : k \in \mathbb{Z}\} = \{e, c\} \neq G$

there no element in G such that element generate a group G.

$\therefore$ Comutative group $\not\Rightarrow$ cyclic group

Theorem:- $\langle a \rangle = \langle a^{-1} \rangle \, , \forall a \in G$

Proof:

$$\langle a \rangle = \{ a^{k} : k \in \mathbb{Z} \} = \{ (a^{-1})^{-k} , : -k \in \mathbb{Z} \}$$

$$= \{ (a^{-1})^{m} : m = -k \in \mathbb{Z} \}$$

$$= \langle a^{-1} \rangle$$

Theorem: If $(G, *)$ is a finite group of order n generated by a, then $G = \langle a \rangle = \{ a^{k} : k \in \mathbb{Z} \}$

$$= \{ a^{1}, a^{2}, \dots, a^{n} = e \} ,$$

Such that n is least positive integer, $a^{n} = e$

$o(a) = oG$ (رتبة العنصر الذي يولد الزمرة = رتبة الزمرة)

Example: Show that $(\mathbb{Z}_n, +)$ is cyclic group.

Solution: Since $\mathbb{Z}_n$ is finite group and $o(\mathbb{Z}_n) = n$, To prove that $\mathbb{Z}_n = \langle 1 \rangle$

$$\langle 1 \rangle = \{ (1)^{k} : k \in \mathbb{Z} \} = \{ (1)^{1}, (1)^{2}, (1)^{3}, \dots, (1)^{n} = e \}$$

$$= \{ 1, 2, 3, \dots, n = 0 \} = \mathbb{Z}_n$$

$\therefore \mathbb{Z}_n = \langle 1 \rangle$ and $o(\mathbb{Z}_n) = o(1) = n .$

خوارزمية القسمة

Definition:- (Division Algorithm for $\mathbb{Z}$)
If a and b are integers with $b>0$, then there is a unique Pair of integers q and r such that:-

$a = bq + r$, (the number q is called the quotient and r is called the reminder when n is divided by b)
$0 \leq r < b$

example:- Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Solⁿ:- We have $a = 38$, $b = 7$

$\because a = bq + r$ $0 \leq r < b$

$\therefore 38 = 7(5) + 3$ $0 \leq 3 < 7$

$\therefore q = 5$, $r = 3$

example: Let $a = 15$, $b = 2$, Find q and r

Solution:- We have

$a = bq + r$, $0 \leq r < b$

$\therefore 15 = 2(7) + 1$ $0 \leq 1 < 2$

$\therefore q = 7$, $r = 1$