Group Theorey

أستاذ المادة :أ.م.د.ريم عمران رشيد

المادة الدراسية جبر الزمر

عدد الساعات : ٢ نظري . ١ مناقشة

لغة التدريس : الانكليزية

عدد الوحدات : ٥ وحدات

جامعة تكريت

كلية التربية طوزخورماتو

قسم الرياضيات

المرحلة الثانية

الموضوع	عدد الأسابيع
النظام الرياضي , شبه الزمرة , الزمرة , أمثلة , الزمر المنتهية وغير المنتهية , زمرة التناظر , زمرة التناوب , زمرة التناظر للمربع , التطابق , خوارزمية القسمة , بعض خواص الزمر , قوانين الحذف , رتبة الزمر المنتهية , رتبة عناصر الزمرة	٥
الزمر الجزئية , أمثلة , نظريات , جداء الزمر الجزئية , مركز الزمرة , الزمر الدائرية , أمثلة , نظريات , القاسم المشترك الأعظم , المشاركات اليسرى (اليمنى) للزمر الجزئية , الدليل , نظرية لاكرانج , نتائج نظرية لاكرانج	٦
ترافق العناصر في الزمرة , ترافق الزمر الجزئية , منظم العنصر , منظم الزمر الجزئية , الزمر الجزئية السوية , الزمر البسيطة , زمرة القسمة , نظريات , المبادل	٦
التشاكلات الزمرية , أمثلة , نظريات , التماثل الزمري , نواة التشاكل , النظرية الأساسية الثالثة في التشاكل الزمري , السلسلة , السلسلة التركيبية , الزمر الجزئية السوية العظمى , نظرية جوردون – هولدر , الزمر الأولية , نظرية سايلو , الجداء الداخلي لزمرتين جزئيتين , الجداء الخارجي لزمرتين	٧
مفهوم الحلقة مع أمثلة شاملة , المثاليات , حلقات القسمة , أنواع معينة من المثاليات , حلقة الحدوديات , الحلقات البوولية وجبر بوولين	٣

References:

1- Introduction to group theory by Walter Ledermann Alam J. Weir.

2- Introduction to modern abstract algebra By David M. Burton.

3- Group theory By M. Suzuki.

4- مقدمة في الجبر الحديث تأليف ديفيد بيرتون وترجمة عبد العال كاظم

وهناك الكثير الكثير من الكتب والمصادر العلمية في هذا الموضوع

: بسم الله الرحمن الرحيم :

"Group theory"

⊛ Chapter One:-

Binary operations:

Definition: Let G be a non-empty set. Any function from $G \times G \to G$ is called a Binary operations on G iff:-

خاصية الانغلاق

1- $a * b \in G \quad , \forall a, b \in G$ [closure].

2- $a, b, c, d \in G$ s.t. $(a,b) = (c,d)$ then $a*b = c*d$

معرف بشكل جيد [well-define].

Examples:- ①

Show that $*$ is a binary operation on N, where

$a*b = ab+2 \quad \forall a, b \in N$.

Sol. Let $h, k \in N$

① $h*k = hk+2 \in N$

② Let $h, k, n, m \in N$ s.t. $(h,k) = (n,m)$

$h*k = hk+2 = nm+2 = n*m$. $\therefore \Rightarrow *$ is a B.O. on N.

EX.②:- Show that "$-$" is not binary operation on N.

but "$-$" is binary operation on Z.

Sol. Let $9, 12 \in N$

(1) $9 - 12 = -3 \notin N$.

$\therefore$ $-$ is not B.O. on N.

○ Let $n, m \in Z$

(1) $n - m \in Z \quad \forall\, n, m \in Z$.

(2) $n, m, h, k \in Z$ s.t. $(n, m) = (h, k)$

$n - m = h - k$

$\therefore$ $-$ is B.O. on Z. ⊠

Exa(3):- Let $a * b = a + b + 2$, $\forall\, a, b \in Z^+$. Is $*$ a B.O. on Z^+?

Solu.

(1) Let $h, k \in Z^+$

$h * k = \underbrace{h + k}_{\in Z^+} + 2 \in Z^+$

(2) Let $n, m, h, k \in Z^+$ s.t. $(n, m) = (h, k)$

$n * m = n + m + 2 = h + k + 2 = h * k$.

$\therefore$ $*$ is B.O. on Z^+. ⊠

Exa.(4):- Let $a * b = a^b$, $a, b \in Z$. Show that '$*$' is B.O.? on Z.

Sol.: Let $a = 2$, $b = -2$, $2, -2 \in Z$.

(1) $a * b = 2^{-2} = \frac{1}{2^2} = \frac{1}{4} \notin Z$.

$\therefore$ $*$ is not B.O. on Z. ⊠

Exa. 5. Is The Union a B.O. on $P(X)$? $P(X)$ هي مجموعة القوى
Power(X)

تذكر $P(X)$?

$A=\{a,b\}$, Find $P(A)$?

$P(A)=\{\phi, A, \{a\}, \{b\}\}$.

لنعود للمثال

Sol. Let $A, B \in P(X)$

① $A \cup B \in P(X)$ ✓ لا نخرج من كمية

② Let $A, B, C, D \in P(X)$ s.t. $(A,B)=(C,D)$

$A \cup B = C \cup D$ ✓ تحقق التعريفان

$\therefore$ The Union is a B.O. on $P(X)$. ☒

Example 6:- Is the Intersection (التقاطع) is a B.O. on $P(X)$?

Sol.:- yes becouse:-

Let $A, B \in P(X)$

① $A \cap B \in P(X)$

② Let $A, B, C, D \in P(X)$ s.t. $(A,B)=(C,D)$.

$A \cap B = C \cap D$.

$\therefore \cap$ is B.O. on $P(X)$. ☒

* A properties of a Binary operations:-

Def.:- A B.O. $G*G \to G$ is:-

1- Commutative if $a*b = b*a$ $\forall a,b \in G$.

2- associative if $a*(b*c) = (a*b)*c$, $\forall a,b,c \in G$.

Exa. Show that "+" is a Commutative and associative on R.

Sol. Let $n,m \in R$

① $n+m = m+n \Rightarrow \therefore$ + is Comm. on R.

② Let $n,m,k \in R$

$\Rightarrow n+(m+k) = (n+m)+k \Rightarrow \therefore$ + is assoc. on R. ⊠

Exa. show that "−" is asso. on R and Z or not?

Sol. Let $a=1$, $b=2$, $c=3$ $\therefore a,b,c \in R$ and Z

$1-(2-3) \overset{?}{=} (1-2)-3$

$1+1 \overset{?}{=} (-1)-3$

$2 \overset{?}{\neq} -4 \Rightarrow \therefore$ "−" is not asso. on R and Z

Example:- Let R be a set of real numbers and $*$ is a B.O. defined as $a*b = a+b-ab$, then $*$ is comm. and asso.?

Sol.:- ① $a*b = a+b-ab = b+a-ba = b*a \Rightarrow *$ is Comm.

② Let $a,b,c \in R$, then:-

$a*(b*c) \stackrel{?}{=} (a*b)*c$

$a*(b*c) = a*(b+c-bc) = a+b+c-bc-ab-ac+abc$ --- ①

$(a*b)*c = (a+b-ab)*c = a+b-ab+c-ac-bc+abc$ --- ②

$\Rightarrow 1 = 2$

$\therefore$ $*$ is asso. on R. ⊠

Example:- Let $H = \{n^2 \mid n \in Z^+\} \subset Z$. show that H is closed under multiplication. Is H closed under additions?

Sol:- Let $x, y \in H$ s.t. $x = n_1^2$, $y = n_2^2$, $n_1^2, n_2^2 \in Z^+$

$xy = n_1^2 \cdot n_2^2 = (n_1 \cdot n_2)^2 \in H$

$\therefore$ H is closed under multiplication.

Now:-

$x+y = n_1^2 + n_2^2 \notin H$ becouse

Let $x = 1 = 1^2$, $y = 4 = 2^2$, $x, y \in H$

$x+y = 1^2 + 2^2 = 5 \notin H$

$\therefore$ H is not closed under additions. ⊠

Note:-

1- addition and multiplication are associative binary operations in Z, but subtraction is not associative.

2- Matrix addition and Matrix multiplication are assoc. b.o. in $M_n(R)$.

Problem:- Let F be the set of all functions from a set S into S. Show that composition of function is an (assoc. b.o.) on F. Give an example to show that composition of functions need not be commutative.

Solu.

Let $f, g, h \in F$. Note that: $f \circ g$ defined as:

$$(f \circ g)(x) = f(g(x)), \forall x \in S \Rightarrow (f \circ g) \in F$$

we have, $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))), \forall x \in S$ --- ①

and $(f \circ (g \circ h))(x) = (f(g \circ h)(x)) = f(g(h(x))), \forall x \in S$ --- ②

$$1 = 2 \Rightarrow ((f \circ g) \circ h) = (f \circ (g \circ h)).$$

$\therefore$ $\circ$, is an (asso. b.o.) in F.

Now:-

Let $f, g : R \rightarrow R$ be defined as $f(x) = \sin x$ and $g(x) = 2x$.

Then: $(f \circ g)(x) = f(2x) = \sin(2x)$ --- ①

$(g \circ f)(x) = g(\sin x) = 2\sin(x)$ --- ②

$1 \neq 2$ $\therefore$ $\circ$ is not comm. ⊠

Definition:- Mathematical system: النظام الرياضي

A (M.S.) is a non-empty set of elements with one or more binary operations defined on this set.

Examples:-

$(R,+)$, $(R,\cdot)$, $(R,-)$, $(R^*,\div)$, $(N,+)$, $(R,+,\times)$, ... are M.S.

but: $(N,-)$, $(R,\div)$, $(Q,+,-)$ are not M.S..

Definition:- Semigroup شبه الزمرة

A semigroup is a pair $(S,*)$ in which S is an empty set and $*$ is a (B.O.) on S with assoc. law.

i.e.: $(S,*)$ is semi group $\Leftrightarrow$ ① $S \neq \varphi$
② $*$ is a binary O.
③ $a*(b*c) = (a*b)*c \quad \forall a,b,c \in S$

Examples:-

1- $(Z,+)$, $(Z,\times)$, $(R,+)$, $(R^*,\div)$, $(N,+)$ are Semigroup.

2- $(N,-)$, $(Ze,+)$, ... are not S.g.

Definition:- Identity element. العنصر المحايد

Let $(S,*)$ be a (M.S.). An element $e \in S$ is an (I.E.) for $*$ if $e*a = a*e = a \quad \forall a \in S$.

Example:- (I.E.) of $(Z,+)$ is 0 because

$$a+0 = 0+a = a \quad \forall a \in Z.$$

Remark:- مهمة جداً — العنصر المحايد وحيد.

A (M.S.) $(S,*)$ has at most one identity element.

i.e. : if the identity element exists, it is unique.

Problem:-

On $Z \times Z$ define the (b.o.) $\circ$ by $(a,b)\circ(c,d) = (ac, bc+d)$.

Is $\circ$ comm.? assoc.? Find the Identity element?

Solu

① Let $(1,2)\circ(3,4) = (3,10)$ and $(3,4)\circ(1,2) = (3,6)$

$\therefore \circ$ is not comm.

② $((a,b)\circ(c,d))\circ(e,f) = (ac, bc+d)\circ(e,f) = ace, (bc+d)e+f$

$= ace, bce+de+f$ --- ①

$(a,b)\circ((c,d)\circ(e,f)) = (a,b)\circ(ce, de+f))$

$= ace, bce+de+f$ --- ②

$\Rightarrow$ ① = ② $\therefore \circ$ is assoc.

③ Let $e = (x,y)$ be the identity element for $\circ$, Then

$(a,b)\circ(x,y) = (x,y)\circ(a,b) = (a,b)$

$\Rightarrow (ax, bx+y)) = (xa, ya+b) = (a,b)$

$\Rightarrow ax = xa = a \Rightarrow ax = a \Rightarrow \underline{x = 1}$

$bx+y = b$ or $ya+b = b$

$\Rightarrow bx+y = b \Rightarrow b.1+y = b \Rightarrow \underline{y = 0}$

$\Rightarrow (x,y) = \underline{(1,0)}$ is the identity element of $\circ$. ☒

⊛ **Definition:-** The Inverse element, العنصر النظير

Let $(S,*)$ be a $(M.S.)$ and $a,b \in S$. Then b is called an inverse of a if $a*b = b*a = e$.

Example:- في المثال السابق

$(a,b)\circ(c,d) = (ac, bc+d)$, $e = (1,0)$, Find Inverse element of (a,b).?

Sol

$(a,b)\circ(c,d) = e = (c,d)\circ(a,b)$

$\therefore (a,b)\circ(c,d) = (1,0)$

$= (ac, bc+d) = (1,0)$

$\Rightarrow ac = 1 \Rightarrow c = \frac{1}{a}$

$bc+d = 0 \Rightarrow b\cdot\frac{1}{a} + d = 0 \Rightarrow d = \frac{-b}{a}$.

$\therefore (a,b)^{-1} = \left(\frac{1}{a}, \frac{-b}{a}\right)$.

$(c,d)\circ(a,b) = (1,0)$

$(ca, da+b) = (1,0)$

$\Rightarrow ca = 1 \Rightarrow a = \frac{1}{c}$

$da+b = 0 \Rightarrow d\cdot\frac{1}{c} + b = 0 \Rightarrow b = \frac{-d}{c}$

$\therefore (c,d)^{-1} = \left(\frac{1}{c}, \frac{-d}{c}\right)$. ⊠

* Definition:- The Group:

A group $(G,*)$ is a set G, closed under a binary operati-on $*$, such that the following axioms are satisfied.

1- Associativity: $(a*b)*c = a*(b*c)$, $\forall a,b,c \in G$.

2- Existence of Identity element: There is an element e in G such that $e*x = x*e = x$, $\forall x \in G$.

3- Existence of Inverse element: There is an element a^{-1} or $a' \in G$ s.t. $a*a' = a'*a = e$ $\forall a \in G$.

Here a' is called the inverse of a.

بشكل مبسط لتعريف الزمرة.

$(G,*)$ زمرة

$(G,*)$ closed. $a*b \in G$	$(G,*)$ assoc. $(a*b)*c = a*(b*c) \in G$	$(G,*)$ Identity element e $a*e = e*a = a$ $\forall a \in G$	Inverse element a' $a*a' = a'*a = e$ $\forall a \in G$.

(Group) اربعة شروط

(*) **Definition:-** A group G is abelian if its binary operation is commutative (ابدالية).

* A group that is not abelian is called nonabelian (ليست ابدالية).

Remark:-

In a group G, the identity element and inverse of each element are unique. (العنصر المحايد والنظير وحيد)

Examples:-

1- The sets Z, Q, R and $\mathbb{C}$ under <u>addition</u> (الجمع) are <u>abelian gp.</u>

2- The sets Q^+, R^+, R^*, Q^*, and $\mathbb{C}^*$ under <u>multiplication</u> are <u>abelian groups.</u>

(*) (يعني هذه المجاميع مع عملية الضرب هي زمر ابدالية)

3- The set Z^+ under addition is <u>not a group</u>. Since it has no identity element ($(Z^+, +)$ ليست زمرة لعدم وجود العنصر المحايد)

4- The set $Z^+ \cup \{0\}$ under addition is <u>not a group</u>, even if it has an identity element 0, but no inverse for 1.

* ($(Z^+ \cup \{0\}, +)$ ليست زمرة لأنها تحتوي على العنصر المحايد ولكن لا تملك العنصر النظير)

5- The set $M_n(R)$ under matrix addition is an <u>abelian group</u>. The Zero matrix is the identity elements.

(*) ($(M_n(R), +)$ مجموعة المصفوفات مع عملية الجمع هي زمرة ابدالية والعنصر المحايد هو المصفوفة الصفرية)

6- The set $M_n(\mathbb{R})$ under matrix multiplication is not a group since the zero matrix has no multiplicative inverse.

($M_n(R), \cdot$) مجموعة المصفوفات مع عملية الضرب ليست زمرة لأن المصفوفة الصفرية لا تملك معكوس ضربي)

* Reversal Law: (قانون الانعكاس)

Let $(G, *)$ be a group. For $a, b \in G$, prove that:

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

Sol

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

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

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

Since the inverse of any element in a group is unique, this shows that $(a*b)^{-1} = b^{-1}*a^{-1}$. ⊠

* problem:-

Let $*$ be defined on $\mathbb{Q}^+$ by $a*b = \frac{ab}{2}$. Prove that $\mathbb{Q}^+$ is an abelian group under $*$?

Sol

1- It is clear that $\mathbb{Q}^+$ is closed under $*$ because $a*b = \frac{ab}{2} \in \mathbb{Q}^+$ $\forall a, b \in \mathbb{Q}^+$.

2- Also $(a*b)*c = a*(b*c) = \frac{abc}{4}$, $\forall a, b, c \in \mathbb{Q}^+$.

$\Rightarrow$ $*$ is associative.

3- $*$ is commutative, since $a*b = \frac{ab}{2} = \frac{ba}{2} = b*a$. $\forall a, b \in \mathbb{Q}^+$

4- If e is the identity element for $*$, then

$$a*e=a \Rightarrow \frac{ae}{2}=a \Rightarrow \underline{\underline{e=2}} \in Q^+.$$

5- Finally, computation shows that:

$$a*a^{-1}=e=\frac{a \cdot a^{-1}}{2}=2$$

$$\Rightarrow a^{-1}=\frac{4}{a}, \forall a \in Q^+.$$

$\therefore (Q^+,*)$ is abelian group. ⊠

⊛ **Problem**:- Let $G=\{1,-1,i,-i\}$ be a set and "$\cdot$" be a binary operation. Is $(G,\cdot)$ a group?

Sol

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

1- Closure is true.

2- Assoc. Law is true.

3- ① is the identity element.

4- $1^{-1}=1$, $-1^{-1}=-1$

$i^{-1}=-i$, $-i^{-1}=i$

$\therefore (G,\cdot)$ is a group. and Comm. group because $a \cdot b=b \cdot a$ $\forall a,b \in G$. ⊠

⊛ **Problem**: Let $G=Z$, $a*b=a+b+2$. Show that $(G,*)$ is a Comm. group?

Sol

1- Closure:- Let $a,b \in Z$, then $a*b=a+b+2 \in Z$ $\forall a,b \in G$

$\therefore$ Closure is true.

2- Let $a,b,c \in G$, then

$(a*b)*c = a*(b*c)$

$(a+b+2)*c \overset{?}{=} a*(b+c+2)$

$a+b+2+c+2 \overset{?}{=} a+b+c+2+2$

$= a+b+c+4 = a+b+c+4. \Rightarrow *$ is assoc. in G.

3- Let $e \in G \ni a*e = e*a = a$, then

$a*e = a \Rightarrow a+e+2 = a \Rightarrow e = \underline{\underline{-2}} \in G$.

4- Let $a^{-1} \in G \ni a^{-1}*a = e$, then

$a^{-1}+a+2 = -2 \Rightarrow a^{-1} = -(4+a) \in G$.

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

5- $a*b = a+b+2 = b+a+2 = b*a$.

$\therefore a*b = b*a. \Longrightarrow (G,*)$ is a comm. group. $\boxtimes$.

Problem: Let $G = \{f_1, f_2, f_3, f_4\}$, where f_1, f_2, f_3, f_4 are mapping on $\mathbb{R}\setminus\{0\}$, s.t. $f_1(x) = x$, $f_2(x) = -x$, $f_3 = \frac{1}{x}$, $f_4 = \frac{-1}{x}$.
Show that $(G, \circ)$ is a group.?

Solution

1- Closure is true.

For example:

$f_1 \circ f_4(x) = f_1(f_4(x))$

$= f_1\left(\frac{-1}{x}\right) = \frac{-1}{x} = f_4$

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

$f_2 \circ f_3 = f_2(f_3(x)) = f_2\left(\frac{1}{x}\right) = \frac{-1}{x} = f_4$

$f_3 \circ f_4 = f_3(f_4(x)) = f_3\left(\frac{-1}{x}\right) = -x = f_2$

$f_2 \circ f_2 = f_2(f_2(x)) = f_2(-x) = x = f_1$

$\vdots$

وهكذا

$\therefore$ closure is true.

2- Associ is true because:-

$(a * b) * c = a * (b * c) \ \forall \ a, b, c \in G$

example:-

$(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$

$= (f_1(f_2)) \circ f_3 \overset{?}{=} f_1 \circ (f_2(f_3))$

$= (f_1(-x)) \circ f_3 \overset{?}{=} f_1 \circ \left(f_2\left(\frac{1}{x}\right)\right)$

$f_2 \circ f_3 \overset{?}{=} f_1 \circ f_4$

$f_2(f_3) \overset{?}{=} f_1(f_4)$

$f_2\left(\frac{1}{x}\right) \overset{?}{=} f_1\left(\frac{-1}{x}\right)$

$\frac{-1}{x} = \frac{-1}{x} = f_4$. $\therefore \circ$ is associ $\forall f_i \in G$.

3- The identity element of G is f_1 since

$f_1 \circ f_1 = f_1$, $f_1 \circ f_2 = f_2$, $f_1 \circ f_3 = f_3$, $f_1 \circ f_4 = f_4$.

4- The inverse element of G is:-

$f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$.

$\therefore (G, \circ)$ is a group. ⊠

⊛ Theorem ①: Cancellation Laws قوانين الاختزال

In a group G, with binary operation $*$, the left and right cancellation laws holds.

(i.e.), $a*b = a*c \Rightarrow b=c$ and $b*a = c*a \Rightarrow b=c$, $\forall a,b,c \in G$.

Proof:-

suppose $a*b = a*c$. Multiplying from the left with a^{-1} on both sides, we get:

$a^{-1}*(a*b) = a^{-1}*(a*c)$. Using Associativity,

$(a^{-1}*a)*b = (a^{-1}*a)*c \Rightarrow e*b = e*c \Rightarrow b=c$.

Similarly, from $b*a = c*a$, we get $b=c$. ⊠

⊛ Theorem ②:

If G is a group with binary operation $*$, and if $a,b \in G$ The linear equations $a*x=b$ and $y*a=b$ have unique solution, x, y in G.

حل وحيد

Proof:

If possible x_1 and x_2 are the solution of $a*x=b$.

Then $a*x_1 = b$ and $a*x_2 = b$

Hence $a*x_1 = a*x_2$ implies $x_1 = x_2$ (By left Cancelation law)

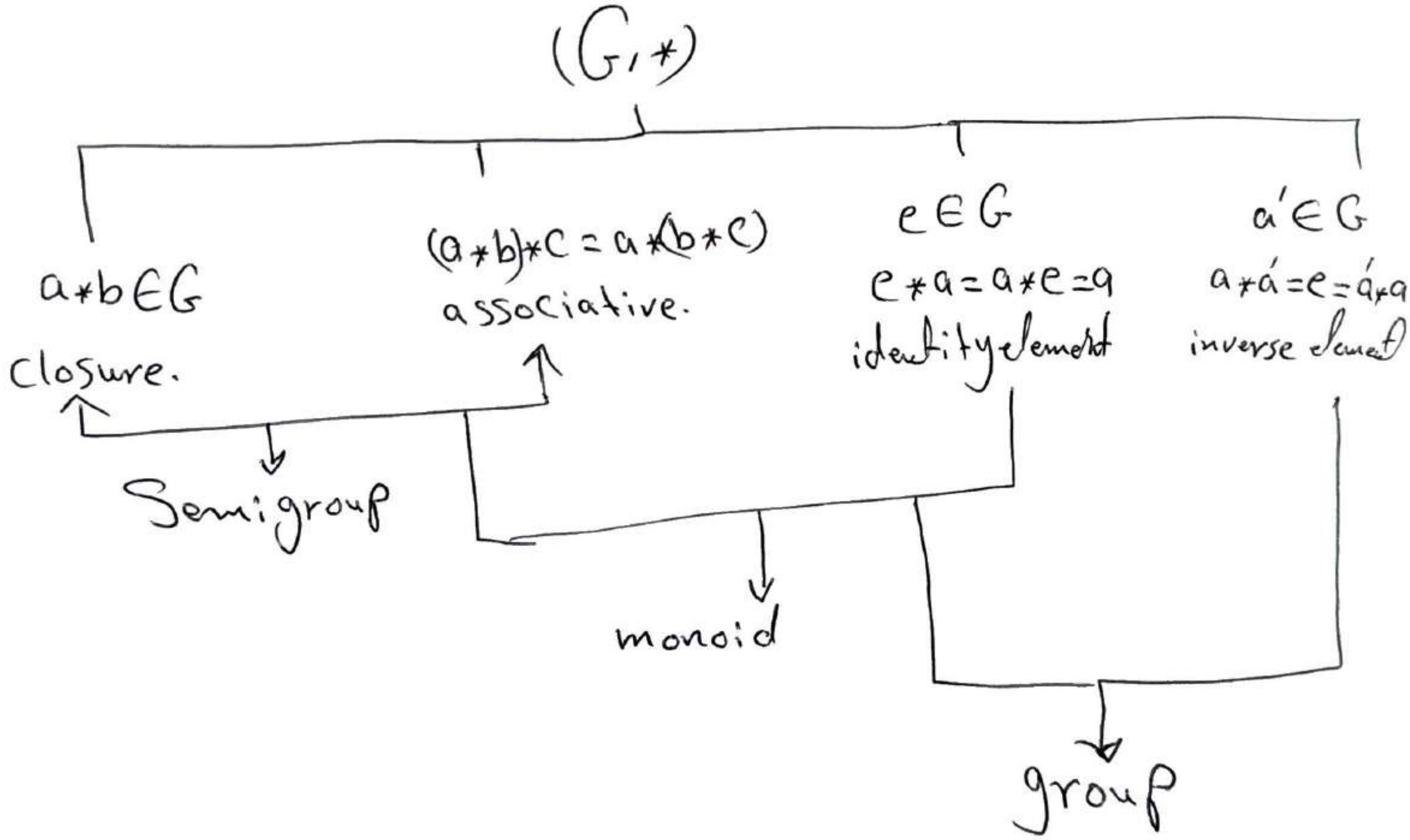
⊛ Try The other yourself! H.w الشطارة في اختبره بنفسك ⊛

* Remark:

* A set together with an associative binary operation is called a <u>Semigroup</u>.

* A <u>monoid</u> is a semigroup that has an identity element for the binary operation.

* Note that a group is both a <u>semigroup</u> and a <u>monoid</u>.



* Problem:-

Let $S = \mathbb{R} \setminus \{-1\}$. Define $*$ on S by $a * b = a + b + ab$.

ⓐ Show that $*$ is a binary operation on S.

ⓑ Show that $(S, *)$ is a group.

ⓒ Find the solution of the equation $2 * x * 3 = 7$ in S.

Solve

ⓐ We must show that S is closed under $*$, that is, that

$a + b + ab \neq -1$ for $a, b \in S$.

Now: $a + b + ab = -1$ iff $0 = ab + a + b + 1$

$= (a+1)(b+1)$.

This is the case iff either $a = -1$ or $b = -1$, whis is not the case for $a, b \in S$. ⊠

ⓑ We have $a * (b * c) = a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc)$

$= a + b + c + ab + ac + bc + abc$ --- ①

and $(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c$

$= a + b + c + ab + ac + bc + abc$ --- ②

$1 = 2 \Rightarrow *$ is assoc. on S.

Now: Let $e \in S$ $e \neq \{-1\}$

$a * e = a \Rightarrow a + e + ae = a \Rightarrow e + ae = 0 \Rightarrow$

$e(1 + a) = 0 \Rightarrow e = \underline{\underline{0}}$

$\therefore$ identity element $e = 0 \in S$.

Since $a * 0 = 0 * a = a$.

Also, $\frac{-a}{a+1}$ acts as inverse of a, for $a * a' = a' * a = e$

$a + a' + aa' = 0 \Rightarrow a'(1+a) = -a \Rightarrow a' = \frac{-a}{1+a}$.

$\therefore a * \frac{-a}{1+a} = 0 = a + \frac{-a}{1+a} + a \cdot \frac{-a}{1+a} = 0$

$= \frac{a(1+a) - a - a^2}{(1+a)} = 0 = \frac{a + a^2 - a - a^2}{1+a} = \frac{0}{1+a} = 0.$

Thus $(S, *)$ is a group. ⊠

(c) Because the operation is comm. $2 * x * 3 = 2 * 3 * x = 11 * x$.

$2 * x * 3 = (2 + x + 2x) * 3$

$= 2 + x + 2x + 3 + (2 + x + 2x)3$

$= 5 + 3x + 6 + 3x + 6x = 11 + 12x = 11 + x + 11x$

$= 11 * x$.

Now by inverse of 11 is $\frac{-a}{1+a} = \frac{-11}{12}$, by (b).

(باستخدام المعكوس)

From $11 * x = 7$ we obtain

$x = \frac{-11}{12} * 7 = \frac{-11}{12} + 7 + \frac{-11}{12} \cdot 7 = \frac{-11 + 84 - 77}{12} = \frac{-4}{12} = \boxed{\frac{-1}{3}}$

$\therefore x = \frac{-1}{3}$. ⊠

⊛ Problem:-

Show that if $(a*b)^2 = a^2 * b^2$ for all a,b in a group G, then G is abelian.

Sol:

we have $(a*b)*(a*b) = (a*a)*(b*b)$, so

$$a*[b*(a*b)] = a*[a*(b*b)] \text{, and left canc. law.}$$

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

Then $(b*a)*b = (a*b)*b$, and right canc. law,

$b*a = a*b$. Thus G is abelian. ⊠.

⊛ Definition: (The integral powers of a)

Let $(G,*)$ be a group. The integral powers of a, $a \in G$ is defined by:

1- $a^n = \underbrace{a*a*a*\cdots*a}_{n\text{-times}}$

2- $a^0 = e$

3- $a^{-n} = (a^{-1})^n$, $n \in \mathbb{Z}^+$

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

⊛ Example:- ① In $(\mathbb{R},+)$, $a=3$

1- $3^4 = 3+3+3+3 = 12$

2- $3^0 = 0$

3- $3^{-2} = (3^{-1})^2 = (-3)+(-3) = -6$

4- $0 = 0^2 = (3+3^{-1})^2 = 3^2+(3^{-1})^2$
$= 3+3+(-3+-3)$
$= 0 = e$. ⊠

② In $(\mathbb{R},\cdot)$, $a=2$

1- $2^3 = 2\cdot2\cdot2 = 8$

2- $2^0 = 1$

3- $2^{-4} = (2^{-1})^4 = (\frac{1}{2})^4 = \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{16}$

4- $1 = 1^3 = (2\cdot2^{-1})^3 = 2^3\cdot(2^{-1})^3 = 2\cdot2\cdot2\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}$
$= 1 = e.$

③ In $(G=\{1,-1,i,-i\},\cdot)$, $a=i$

1- $i^0=1$

2- $i^2=-1$

3- $i^{-2}=(i^{-1})^2=(-i)^2=-i\cdot-i=\underline{\underline{-1}}$, 4- $1=1^3=(i\cdot i^{-1})^3=i^3\cdot(i^{-1})^3=i\cdot i\cdot i\cdot -i\cdot -i\cdot -i=-i\cdot +i=1=\underline{\underline{e}}$

⊛ Theorem:-

Let $(G,*)$ be a group and $a\in G$, $m,n\in \mathbb{Z}$, then:

1- $a^n * a^m = a^{n+m}$ $\forall n,m\in \mathbb{Z}$.

2- $(a^n)^m = a^{nm}$ $\forall n,m\in \mathbb{Z}^+$.

3- $a^{-n}=(a^n)^{-1}$ $\forall n\in \mathbb{Z}^+$.

4- $(a*b)^n = a^n * b^n$ $\forall n\in \mathbb{Z} \Leftrightarrow G$ is comm. group.

⊛ Definition: Order of a group: رتبة الزمرة

The number of elements of a group (finite or infinite) is called its **order**. We will use $|G|$ to denote the order of G.

⊛ Example:- ① $(\mathbb{Z},+)$ the group of integers under addition has infinite order (i.e) $|\mathbb{Z}|=\infty$.

② $(G=\{1,-1,i,-i\},\cdot) \Rightarrow |G|=4$ (finite group).

⊛ Definition:- Order of an Element رتبة العنصر

The **order** of an element g in a group G is the smallest positive integer n s.t. $\underline{\underline{g^n=e}}$. (In additive notation, this would be $ng=0$.) If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$.

Example:- Let $(G=\{1,-1,i,-i\},\cdot)$. Find the order of elements to G?

Sol

1- $|1|=1$

2- $|-1|=2$ because $(-1)^2=-1\cdot-1=1$

3- $|-i|=4$ because $(-i)^4=-i\cdot-i\cdot-i\cdot-i=1$

4- $|i|=4$ because $(i)^4=i\cdot i\cdot i\cdot i=1$

Some types of groups

1- Z_n group
2- permutation group
3- Symmetric group.

The group of integers modulo n Z_n:

زمرة الأعداد الصحيحة بمعيار n Z_n:

شرح مبسط لـ $(Z_n, +_n)$.

زمرة الأعداد الصحيحة بمعيار n رمزها هو $(Z_n, +_n)$

$$Z_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

* n عدد صحيح موجب
* $+_n$ هو الجمع المعياري
* العنصر المحايد له هو $\bar{0}$
* نظير العنصر k هو n-k.
* لا نقصد بالأعداد التي في Z_n الأعداد الصحيحة الاعتيادية ولكن نقصد بها صفوف التكافؤ بمعيار n.
* في هذه الزمرة تكون العناصر عبارة عن صفوف تكافؤ $[a]$ تم كتابتها $\bar{a}$ للسهولة في هذا المثال.

In Example: $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$= \{[0], [1], [2], [3], [4], [5]\}$

نلاحظ أن: مضاعفات الستة

اضافة 6 للعدد

$$[0] = [6] = [-6] = [12] = \cdots$$

$$[1] = [7] = [-5] = \cdots$$

$$[2] = [8] = [-4] = \cdots$$

$$[3] = [9] = [-3] = \cdots$$

$$[4] = [10] = [-2] = \cdots$$

$$[5] = [11] = [-1] = \cdots$$

$$[6] = [12] = [0]$$

وهكذا نعود للبداية.

Example:- In Z_{10}, Find $(9 +_{10} 6)^{-1}$ و $(5^{-2}) +_{10} 6^3$?

(1) $9 +_{10} 6 = 15 \equiv 5$

(*) عند جمع $9 +_{10} 6$ يكون الناتج أكبر من 10 نطرح 10 والباقي هو الناتج .

$\Rightarrow (5)^{-1} = 5^{-1} = 10 - 5 = \underline{\underline{5}}$

(*) حسب قاعدة النظير $\underline{\underline{n-k}}$
$n = 10, k = 5$, $k^{-1} = 5$.

(2) $5^{-2} +_{10} 6^3$

$= (5^2)^{-1} +_{10} 6^3$

$= 5^2 = 5+5 = 10 = 0 \Rightarrow (0)^{-1} = \bar{0} \in Z_{10}$

$6^3 = 6+6+6 = 18 \equiv 8 \quad \in Z_{10}$

$\therefore 5^{-2} +_{10} 6^3 = \bar{0} +_{10} \bar{8} = \underline{\underline{\bar{8}}} \in Z_{10}$.

(*) الآن : رتبة العناصر في Z_n

(*) order elements in $\underline{\underline{Z_n}}$

لإيجاد رتبة العنصر في Z_n نحن نعلم بأن رتبة الزمرة Z_n هو n

$\therefore Z_n = \{\bar{0}, \bar{1}, \dots \overline{n-1}\}$

$|Z_n| = n$, Let $a \in Z_n$

$$|a| = \frac{n}{g.c.d(a, n)}$$

(*) Example:- In Z_{18}, Find $|6|$?

$\Rightarrow |6| = \frac{18}{g.c.d(18, 6)} = \frac{18}{6} = \underline{\underline{3}}$.

⊛ The generated of Z_n. ⊛ المولدات في Z_n.

$Z_n = \{\bar{0}, \bar{1}, \cdots \overline{n-1}\}$ يكون العنصر $a \in Z_n$ مولد للزمرة Z_n اذا كان g.c.d(n,a) مساوي للواحد

$g.c.d(n,a) = 1 \Rightarrow$ أي

a generated to Z_n group.

⊛ Example:- In $Z_8 = \{\bar{0}, \bar{1} \cdots \bar{7}\}$, Find the generated to Z_8?

Now: $g.c.d(8,1) = 1$

$g.c.d(8,2) = 2$

$g.c.d(8,3) = 1$

$g.c.d(8,4) = 2$

$g.c.d(8,5) = 1$

$g.c.d(8,6) = 2$

$g.c.d(8,7) = 1$

∴ The Set of generated to $Z_8 = \{1, 3, 5, 7\}$.

⊛ Example:- In $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, Find the set of generated to Z_5?

sol

$$\left.\begin{array}{l} g.c.d(5,1) = 1 \\ g.c.d(5,2) = 1 \\ g.c.d(5,3) = 1 \\ g.c.d(5,4) = 1 \end{array}\right\} \Rightarrow S = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

ملاحظة

⊛ اذا كانت Z_n و n عدد اولي فان المولدات هي جميع الاعداد ماعدا الصفر.

"The group of integers modulo n Z_n"

⊛ Definition:-

تطابق   معيار

Let $a, b \in Z$, $n > 0$. Then a is congruent to b modulo n if: $a - b = nk$, $k \in Z$ and denoted by $a \equiv b$ or $b \equiv a \pmod{n}$.

⊛ Examples:-

1- $17 \equiv 5 \pmod{6}$, since $17 - 5 = 12 = (6)\cdot(2)$

2- $8 \equiv 4 \pmod{2}$, since $8 - 4 = 4 = (2)\cdot(2)$

3- $-12 \equiv 3 \pmod{3}$, since $-12 - 3 = -15 = (3)\cdot(-5)$

4- $5 \not\equiv 2 \pmod{2}$, since $5 - 2 = 3 \neq (2)\cdot(K)$, $\forall K \in Z$.

تكافؤ

⊛ Theorem: The congruence module n is an equivalence relation on the set of integers.

علاقة التكافؤ

reflexive انعكاسية   Symm. متناظرة   tran. متعدية

Proof:-

Let $a, b, c \in Z$, $n > 0$

1- $a - a = 0 = (n)(0)$

$\therefore a \equiv a \pmod{n} \Rightarrow$ reflexive is true.

2- if $a \equiv b \pmod{n} \Rightarrow a - b = (n)k$, $k \in Z$

So, $b - a = -nk = (n)(-k)$, $-k \in Z$

$\therefore a \equiv b \pmod{n} \Rightarrow$ symmetric is true.

3- if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, To prove $a \equiv c \pmod{n}$

since $a \equiv b \pmod{n}$, then $a - b = nk_1$ --- (1)

and $b \equiv c \pmod{n}$, then $b - c = nk_2$ -- (2)

By adding $\Rightarrow$ $a - c = n(k_1 + k_2)$, $k_1 + k_2 \in \mathbb{Z}$

$\therefore$ $a \equiv c \pmod{n}$ $\Rightarrow$ Transitive is true.

$\therefore$ The congruence modulo n is an equivalence relation. ⊠.

صنف التكافؤ

(*) Define:- Let $a \in \mathbb{Z}$, $n > 0$. The congruence class of a modulo n, denoted by $[a]$ is the set of all integers that are congruent to a modulo n.

(*) صنف التكافؤ: هو مجموعة من الأعداد الصحيحة المتكافئة بمعيار n.

i.e.

$$[a] = \{z \in \mathbb{Z} : z \equiv a \pmod{n}\}$$
$$= \{z \in \mathbb{Z} : z = a + kn, k \in \mathbb{Z}\}$$

(*) Example:- (1) If $n = 2$, find $[0]$, $[1]$.

sol:-

$$[0] = \{z \in \mathbb{Z} : z \equiv 0 \pmod{2}\}$$
$$= \{z \in \mathbb{Z} : z = 0 + 2k, k \in \mathbb{Z}\}$$
$$= \{0, \mp 2, \mp 4, \mp 6, \ldots\} \ldots ⊠$$

$$[1] = \{z \in \mathbb{Z} : z \equiv 1 \pmod{2}\}$$
$$= \{z \in \mathbb{Z} : z = 1 + 2k, k \in \mathbb{Z}\}$$
$$= \{\mp 1, \mp 3, \mp 5, \ldots\}. ⊠$$

Example: (2) If $n=3$, find $[1]$, $[7]$.

Sol.

$$[1] = \{z \in \mathbb{Z} : z \equiv 1 \pmod 3\}$$
$$= \{z \in \mathbb{Z} : z = 1 + 3k, k \in \mathbb{Z}\}$$
$$= \{1, -2, 4, 7, -5, \cdots\}$$

$$[7] = \{z \in \mathbb{Z} : z \equiv 7 \pmod 3\}$$
$$= \{z \in \mathbb{Z} : z = 7 + 3k, k \in \mathbb{Z}\}$$
$$= \{7, 10, 4, 1, 13, \cdots\}.$$

Definition:-

مجموعة صفوف التكافؤ مقياس n

The set of all congruence classes modulo n is denoted by $\mathbb{Z}_n$ (which is read $\mathbb{Z}$ mod n). Thus:

$$\mathbb{Z}_n = \{[0], [1], [2], \cdots, [n-1]\} \text{ or}$$

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots \overline{n-1}\}$$

* $\mathbb{Z}_n$ has n elements.

$\mathbb{Z}_n$ تمتلك n من العناصر

Example:-

$$\mathbb{Z}_1 = \{\bar{0}\}$$
$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$$
$$\mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \cdots \bar{9}\}$$
$$\mathbb{Z}_{50} = \{\bar{0}, \bar{1}, \cdots \overline{49}\}$$
$$\vdots$$

وهكذا

(*) Definition:-

علاقة اولية

Two integers a and b are relatively Prime iff

$g.c.d(a,b) = 1.$

يقال عن العددين (a,b) لهما علاقة اولية اذا كان القاسم المشترك الاعظم لهما يساوي للواحد.

Example:-

Let $a=2, b=4, c=7$

$g.c.d(2,4)=2$ not relatively Prime.

but $g.c.d(2,7)=1$ relatively Prime.

$\Rightarrow g.c.d(4,7)=1$ ...

(*) Theorem:-

Let n be a positive integer and Z_n be as defined above

Then:-

① For each $[a] \in Z_n$, $[a] \neq \phi$.

② If $[a] \in Z_n$ and $b \in [a]$, then $[a]=[b]$, That is any element of the congruence class $[a]$ determines the class.

③ For any $[a],[b] \in Z_n$ where $[a] \neq [b]$, $[a] \cap [b] = \phi$
either $[a]=[b]$ or $[a] \cap [b] \neq \phi$.

④ $\bigcup \{[a] : [a] \in Z_n\} = Z$, Z_n is a partition of the set Z.

① صف التكافؤ لا يساوي ϕ

② $[a]$ يحوي على العنصر b هذا يؤدي الى أن $[a]=[b]$ لا كلاهما متشابهين.

③ اذا كان لدينا $[a] \neq [b]$ صفين تكافؤ فأن تقاطعهم يساوي لـ ϕ او اذا كان $[a]=[b]$ فأن تقاطعهم لا يساوي ϕ.

④ اتحاد صفوف التكافؤ يشكل المجموعة Z وان Z_n هو جزء من Z [illegible]

⊛ Now, we define addition on Z_n (write $+_n$) by the following:-

For any $[a], [b] \in Z_n$, $[a] +_n [b] = [a+b]$, $\forall [a], [b] \in Z_n$

⊛ Similarly, we define multiplication on Z_n (write $\cdot_n$) by the following:

$$[a] \cdot_n [b] = [a \cdot b], \forall [a], [b] \in Z_n.$$

⊛ **Theorem:-** For each positive integer n the System $(Z_n, +_n)$ forms a comm. group, know as the group of integers modulo n.

النظام $(Z_n,+_n)$ هو زمرة ابدالية تسمى بالزمرة العيارية في الأعداد الصحيحة بمعيار n.

Proof:- Let $[a], [b], [c] \in Z_n$.

$$\begin{aligned} [a] +_n ([b] +_n [c]) &= [a] +_n [b+c] \\ &= [a+b+c] \\ &= [a+b] +_n [c] \\ &= ([a] +_n [b]) +_n [c] \end{aligned}$$

$\therefore$ $+_n$ is assoc. binary operation on Z_n.

By definition of $+_n$ if it is clear that $[0]$ is the identity element of Z_n.

If $[a] \in Z_n$, then $[n-a] \in Z_n$, and

$$[a] +_n [n-a] = [a+n-a] = [n] = [0]$$

$\therefore$ $[a]^{-1} = [n-a]$. Thus $(Z_n, +_n)$ is a group.

Now $[a] +_n [b] = [a+b] = [b+a] = [b] +_n [a]$.

$\therefore$ $(Z_n, +_n)$ is a comm. group. ⊠

Examples:- Construct the operation tables for the group $(Z_4, +_4)$.

sol: $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ or $\{[0], [1], [2], [3]\}$

$+_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$e = \bar{0} = \bar{4}$ لاحظ أن

$1^{-1} = 3, \; 2^{-1} = 2, \; 3^{-1} = 1$

Example:- $(Z_7, +_7)$

$Z_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$+_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$e = \bar{0} = \bar{7}$ العنصر المحايد

العنصر النظير

$1^{-1} = 6$

$2^{-1} = 5$

$3^{-1} = 4$

$4^{-1} = 3$

$5^{-1} = 2$

$6^{-1} = 1$

$0^{-1} = 0$

* Example:- $(Z_4, \cdot_4)$

Sol

$\cdot_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Now: it is clear that we cannot have a group. since the number $\bar{1}$ is the identity but the numbers $\bar{0}$ and $\bar{2}$ have no inverse. it follows that $(Z_4, \cdot_4)$ is not a group, but it is a semigroup.

يعني أنه نلاحظ أن العنصر المحايد في $(Z_4, \cdot_4)$ هو $\bar{1}$
لكن العنصرين $\bar{2}$ و $\bar{0}$ لا يمتلكان عنصر نظير.
وهنا فأن الـ $(Z_4, \cdot_4)$ ليست زمرة لكنها شبه زمرة.

* Example:- Find the order of elements 8, 7 in $(Z_{10}, +_{10})$.

Sol

In addition the order $= na = 0$

$Z_{10} = \{\bar{0}, \bar{1}, \dots, \bar{9}\}$, $|Z_{10}| = 10$

$|\bar{8}| = n \cdot 8 = 0 \Rightarrow n = \underline{5}$. or $\frac{10}{g.c.d(10,8)} = \frac{10}{2} = 5$.

$|\bar{7}| = n \cdot 7 = 0 \Rightarrow n = 10$ or $\frac{10}{g.c.d(10,7)} = \frac{10}{1} = 10$.

نلاحظ أن الرتبة لـ $\bar{7}$ هي رتبة الزمرة وهذا يعني أن العناصر الأولية على رتبة تساوي رتبة الزمرة

(*) In $Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \dots \bar{7}\}$

(*) الزمـــ .

Addition modulo 8

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication Modulo 8

$\cdot_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

من الجدولين نلاحظ أن Z_8 مع $+_8$ تمثل زمرة لكن مع $\cdot_8$ لا تمثل زمرة لكن

نلاحظ أن العناصر 0 و 2 و 4 و 6 لا يحققون شروط الزمرة فنلغيهم من الجدول فيصبح الجدول

$\cdot_8$	0	1	2	3	4	5	6	7
~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~	~~0~~
1	~~0~~	1	~~2~~	3	~~4~~	5	~~6~~	7
~~2~~	~~0~~	~~2~~	~~4~~	~~6~~	~~0~~	~~2~~	~~4~~	~~6~~
3	~~0~~	3	~~6~~	1	~~4~~	7	~~2~~	5
~~4~~	~~0~~	~~4~~	~~0~~	~~4~~	~~0~~	~~4~~	~~0~~	~~4~~
5	~~0~~	5	~~2~~	7	~~4~~	1	~~6~~	3
~~6~~	~~0~~	~~6~~	~~4~~	~~2~~	~~0~~	~~6~~	~~4~~	~~2~~
7	~~0~~	7	~~6~~	5	~~4~~	3	~~2~~	1

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

وهذه المجموعة نطلق عليها مجموعة Unit modulo n

$U(8) = \{1, 3, 5, 7\}$

والتي تحقق الشروط الأربعة

Consider the set of integers m meeting the following conditions:

① : $1 \leq m < 8$

هذه المجموعة اذا حققت الشروط الاتية :- D

② : m and 8 are relative prime.

(i.e.) $g.c.d(8, m) = 1$

, $g.c.d(8,1) = 1$
$g.c.d(8,3) = 1$
$g.c.d(8,5) = 1$
$g.c.d(8,7) = 1$

$\Longrightarrow U(8) = \{1, 3, 5, 7\}$, (Unite modulo 8), $\cdot_8$)

(*) Example:-

IS $(U(8), \cdot_8)$ a group?

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

نتاكد من :-

1- Closure ✓
2- Assoc. ✓
3- Identity (1) ✓
4- Inverse.

. $1^{-1} = 1$, $3^{-1} = 3$, $5^{-1} = 5$, $7^{-1} = 7$.

$\therefore (U(8), \cdot_8)$ is a group.

* **Example:-** The set $U(10)=\{1,3,7,9\}$ under multiplication modulo 10. Is The $(U(10),\cdot)$ a group?

Sol:

ملاحظة: هذه المجموعة هي مجموعة جزئية من Z_{10} والتي تعني كل العناصر التي تكون علاقتها أولية أي أن $g.c.d(n,a)=1$.

$\because$ $n=10$, $Z_{10}=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9}\}$

$g.c.d(10,0)=0$

$g.c.d(10,1)=1$

$g.c.d(10,2)=2$

$g.c.d(10,3)=1$

$g.c.d(10,4)=2$

$g.c.d(10,5)=5$

$g.c.d(10,6)=2$

$g.c.d(10,7)=1$

$g.c.d(10,8)=2$

$g.c.d(10,9)=1$

$\Rightarrow$ نستخرج $U(n)=\{1,3,7,9\}$ مع العملية المعطاة وهي $(U(10),\cdot)$.

لنتحقق أن $(U(10),\cdot)$ زمرة نكون الجدول

$\cdot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

نلاحظ من الجدول :-

① الانغلاق متحققة

② التجميعية متحققة

③ وجود العنصر المحايد وهو 1

④ وجود العنصر النظير وهو

$\bar{1}^{-1}=1$

$\bar{3}^{-1}=7$, $\bar{7}^{-1}=3$

$\bar{9}^{-1}=9$

$\therefore$ $(U(10),\cdot)$ هي زمرة .

ولإيجاد الرتبة بالنسبة للزمرة $U(10)$ ورتبة عناصرها :-

$|U(10)| = 4$

$|1| = 1$, $|3| =$ $\qquad$ $3^n = 1$ نلاحظ للحصول على

$3^1 = 3$, $3^2 = 9$, $3^3 = 7$, $3^4 = 1 \Rightarrow \therefore |3| = 4$

$|7| =$

$7^1 = 7$, $7^2 = 9$, $7^3 = 3$, $7^4 = 1 \Rightarrow \therefore |7| = 4$

$|9| =$

$9^1 = 9$, $9^2 = 1 \Rightarrow \therefore |9| = 2$.

Example:- Consider $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under mult. modulo 15. This group has order $\underline{\underline{8}}$. Find the order of all elements of $U(15)$.

Sol:

$|1| = 1$

$|2| \Rightarrow 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 1 \Rightarrow |2| = \underline{\underline{4}}$

$|4| \Rightarrow 4^1 = 4, 4^2 = 1 \Rightarrow |4| = \underline{\underline{2}}$

$|7| \Rightarrow 7^1 = 7, 7^2 = 4, 7^3 = 13, 7^4 = 1 \Rightarrow |7| = \underline{\underline{4}}$

$|8| \Rightarrow 8^1 = 8, 8^2 = 4, 8^3 = 2, 8^4 = 1 \Rightarrow |8| = \underline{\underline{4}}$

$|11| \Rightarrow 11^1 = 11, 11^2 = 1 \Rightarrow |11| = 2$

$|13| \Rightarrow 13^1 = 13, 13^2 = 4, 13^3 = 7, 13^4 = 1 \Rightarrow |13| = \underline{\underline{4}}$

$|14| \Rightarrow 14^1 = 14, 14^2 = 1 \Rightarrow |14| = \underline{\underline{2}}$.

هنالك طريقة أخرى لإيجاد الرتبة وبطريقة أسهل أحد أمرها بالاعتماد على الفصل التكافئ أعلاه :.

$14 = -1 \mod 15$
$13 = -2 \mod 15$
$11 = -4 \mod 15$
$8 = -7 \mod 15$

$\therefore |14| = |-1| = (-1)^1 = -1,\ (-1)^2 = 1 \Rightarrow |14| = \underline{\underline{2}}$

$|13| = |-2| = (-2)^1 = -2,\ (-2)^2 = 4,\ (-2)^3 = 8,\ (-2)^4 = 1 \Rightarrow |13| = \underline{\underline{4}}$

$|11| = |-4| = (-4)^1 = -4,\ (-4)^2 = 1 \Rightarrow |11| = \underline{\underline{2}}$

$|8| = |-7| = (-7)^1 = -7,\ (-7)^2 = 4,\ (-7)^3 = -13,\ (-7)^4 = 1 \Rightarrow |8| = \underline{\underline{4}}.$

Example:- In $(Z_{10}, +_{10})$.

$Z_{10} = \{\bar{0}, \bar{1}, \dots \bar{9}\},\ \Rightarrow |Z_{10}| = 10,$

$|0| = 1,\ |1| = 10$
$|2| = 5,\ |3| = 10$
$|4| = 5,\ |5| = 2$
$|6| = 5,\ |7| = 10$
$|8| = 5,\ |9| = 10$

since $1\cdot 2 = 2,\ 2\cdot 2 = 4,\ 3\cdot 2 = 6,\ 4\cdot 2 = 8$
$5\cdot 2 = 0 \Rightarrow |2| = \underline{\underline{5}}$

$1\cdot 4 = 4,\ 2\cdot 4 = 8,\ 3\cdot 4 = 2,\ 4\cdot 4 = 6,\ 4\cdot 5 = 0$
$\Rightarrow |4| = 5$

$1\cdot 3 = 3,\ 2\cdot 3 = 6,\ 3\cdot 3 = 9,\ 4\cdot 3 = 2,\ 5\cdot 3 = 5$
$6\cdot 3 = 8,\ 7\cdot 3 = 1,\ 8\cdot 3 = 4,\ 9\cdot 3 = 7,\ 10\cdot 3 = 0$
$\Rightarrow |3| = 10$

$1\cdot 7 = 7,\ 2\cdot 7 = 4,\ 3\cdot 7 = 1,\ 4\cdot 7 = 8,\ 5\cdot 7 = 5,\ 6\cdot 7 =$
$2,\ 7\cdot 7 = 9,\ 8\cdot 7 = 6,\ 9\cdot 7 = 3,\ 10\cdot 7 = \underline{\underline{0}}$
$|7| = \underline{\underline{10}}$

$1\cdot 6 = 6,\ 2\cdot 6 = 2,\ 3\cdot 6 = 8,\ 4\cdot 6 = 4,\ 5\cdot 6 = 0$
$|6| = 5$

$1\cdot 5 = 5,\ 2\cdot 5 = 0 \Rightarrow |5| = \underline{\underline{2}}$

توضيح : نلاحظ أن رتب
الأعداد الأولية العلاقة
ترتبط مساوية لرتبة
الزمرة
والأخرى تحسب حسب
القاعدة $ng = 0,\ +$
بالنسبة للجمع.

Permutations groups (زمر التباديل)

*** Definition:-**

Let S be a set of n elements, a one-to-one mapping S onto S is called permutation on S.

The set of all permutation is denoted by S_n.

Let $S=\{a_1,a_2,\dots,a_n\}$ and $f: S\to S$ is defined by

$f(a_1)=b_1, f(a_2)=b_2, \dots f(a_n)=b_n$ $\{b_i\in S\ i=1,\dots n\}$

then

$$g_n=\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n)\end{pmatrix} \quad [g\in S_n]$$

$$=\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n\end{pmatrix}$$

where g is a permutation and S_n is a set of all permutations.

when S contain n elements the possible permutation is given by $n!$.

*** Example:-** If S contains 3 elements $S=\{1,2,3\}$, then $S_n\to S_3$, $3!=3\cdot2\cdot1=6$ elements in S_3, S_3 has 6 permutation

$$S_3=\{f_1,f_2,f_3,f_4,f_5,f_6\} \Rightarrow |S_3|=3!=6$$

اي أن عدد العناصر هو $\underline{\underline{6}}$

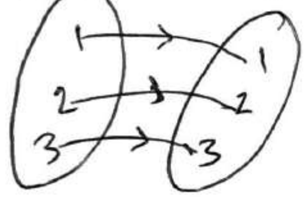
$\dots (312)\ (213)\ -\ (132)$ not comm

$$S_3 = \left\{ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

then in element f_1, the function f is defined by follow

$f: S \to S$, s.t. $f(1) = 1$, $f(2) = 2$, $f(3) = 3$

$f: S \to S$



$\therefore$ f is one-to-one and onto

and we can defined f for all elements in S_3.

⊛ **Definition:-** Let S be a set of n elements. The set of all one-to-one, onto permutation with binary operation ($\circ$) (compositions) is formed a group wich is called Symmetric group.

⊛ **Example:-** Let

$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, Find $f_2 \circ f_3$ and

$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $f_3 \circ f_5$, $f_5 \circ f_3$?

$$f_2 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$f_5 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$f_3 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \Longrightarrow f_3 \circ f_5 \neq f_5 \circ f_3 \Rightarrow \circ \text{ is not comm.}$$

وليست ابدالية

Example:-

Is S_3 with composition operation form a group? (S_3, o)?

conseder S_3

$$S_3 = \left\{ \begin{matrix} f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} & f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{matrix} \right\}$$

$$f_1 o f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$f_1 o f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2$$

$$f_1 o f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_3$$

$$f_1 o f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4$$

$$f_1 o f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_5$$

$$f_1 o f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_6$$

$$f_2 \circ f_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = f_2$$

$$f_2 \circ f_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = f_3$$

$$f_2 \circ f_3 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = f_1$$

$$f_2 \circ f_4 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = f_6$$

$$f_2 \circ f_5 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = f_4$$

$$f_2 \circ f_6 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = f_5$$

$$f_3 \circ f_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = f_3$$

$$f_3 \circ f_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = f_1$$

$$f_3 \circ f_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = f_2$$

$$f_3 \circ f_4 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = f_5$$

$$f_3 \circ f_5 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = f_6$$

$$f_3 \circ f_6 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = f_4$$

$$f_4 \circ f_1 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = f_4$$

$$f_4 \circ f_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = f_5$$

$$f_4 \circ f_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = f_6$$

$$f_4 \circ f_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = f_1$$

$$f_4 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2$$

$$f_4 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_3$$

$$f_5 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_5$$

$$f_5 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_6$$

$$f_5 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4$$

$$f_5 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_3$$

$$f_5 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$f_5 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2$$

$$f_6 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_6$$

$$f_6 \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ & & \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4$$

$$f_6 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_5$$

$$f_6 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2$$

$$f_6 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_3$$

$$f_6 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

Now we can put this result in table

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

then S_3 is a group and the identity is $f_1 \in S_3$

and the inverce of all elements $\in S_3$

$(f_1)^{-1} = f_1$, $(f_2)^{-1} = f_3$, $(f_3)^{-1} = f_2$, $(f_4)^{-1} = f_4$

$(f_5)^{-1} = f_5$, $(f_6)^{-1} = f_6$

and we can see that S_3 is not commutative group since $(f_3 \circ f_4 = f_5) \neq (f_4 \circ f_3 = f_6)$

S_n is commutative when $n < 3$

There is another way to find the idintity in S_3 and we can use it in S_n when $(n=1,2,\cdots)$

for example in S_3 if want to know the identity for any element such as f_4

$$f_4 \circ I = I \circ f_4 = f_4$$

$$\therefore \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{\text{the function here is } f} \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ x & y & z \end{pmatrix}}_{\text{the function here is } g} = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{\text{here of course } f \circ g}$$

to fined x

$g(1) = x$, $f(1) = 3$, $(f \circ g)(1) = f(g(1)) = f(x) = 3$

$\therefore x = f^{-1}(3)$

$\therefore x = 1$

$g(2) = y$, $f(2) = (2)$, $(f \circ g)(2) = f(g(2)) = f(y) = 2$

$\therefore y = f^{-1}(2)$

$y = 2$

$g(3) = z$, $f(3) = (1)$, $(f \circ g)(3) = f(g(3)) = f(z) = 1$

$\therefore z = f^{-1}(1)$

$z = 3$

$$\therefore I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

and we can use it for all elements

And by the same way we can fined the inverse

as example if we want to fined the inverse of f_3 we can write

$f_3 \circ f_3^{-1} = f_3^{-1} \circ f_3 = f_1$, $(f_1 = I)$

$$\therefore f_3 \circ f_3^{-1} = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{f} \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ x & y & z \end{pmatrix}}_{g} = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{f \circ g}$$

$g(1) = x$, $f(1) = 2$, $(f \circ g)(1) = f(g(1)) = f(x) = 1$

$\therefore x = f^{-1}(1) = 3$

$g(2) = y$, $f(2) = 3$, $(f \circ g)(2) = 2 \Rightarrow f(g(2)) = f(y) = 2$

$y = f^{-1}(2) = 1$

$g(3) = z$, $f(3) = 1$, $(f \circ g)(3) = f(g(3)) = f(z) = 3$

$\therefore z = f^{-1}(3) = 2$

$$\therefore f_3^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2$$

and we can find the inverse for all elements by the same way.

المدار

The Orbits

Let σ be a permutation of a set A. Then the relation on A defined by

$$a \sim b \iff b = \sigma^n(a) \text{ for } n \in Z^+$$

is an equivalence relation

Definition

The equivalence classes determind by the above equivlence relation the orbits of σ

Example: Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$

To fined the orbit containing 1 we apply σ repetedly

$\underbrace{1 \to 3 \to 6 \to}_{\text{orbit}} 1 \to 3 \to 6 \to \cdots$

$\underbrace{2 \to 8 \to}_{\text{orbit}} 2 \to 8 \to \cdots$

$\underbrace{4 \to 7 \to 5}_{\text{orbit}} \to 4 \to 7 \to \cdots$

$\therefore$ there are three orbits in σ $\{1,3,6\}$, $\{2,8\}$, $\{4,7,5\}$

we can right the permutation by it's orbits
بالإمكان كتابة التبديل بدلالة المدار

if $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (12)(345)$

the length (طول) of Permutation is the number of elements in the largest cycle (اكبر دورة)

in A the length is 3

Example:-

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix} \in S_6 = \underbrace{(124)}_{\text{دورة}}\underbrace{(56)}_{\text{دورة}} \Rightarrow$

دورات منفصلة

Joint and dis Joint permutation

let f and g are two permutations, if the intersection of there cycle equal to $\emptyset$ then f and g are disjoint. And if the intersection of them not equal to $\emptyset$ then f and g are not disjoint

example

① let $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2)$ $\quad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3)$

$f \cap g = (1\,2) \cap (1\,3) = 1 \neq \emptyset$

$\therefore$ f and g are not disjoint متصلة

② let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = (1\;3\;2)$

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (4\;5)$

$f \cap g = (1\;3\;2) \cap (4\;5) = \emptyset$

$\therefore$ f and g are disjoint منفصلة

ملاحظات :

١- اذا كانت العناصر بداخله الى نفسه لا يكتب ضمن الدورة .

٢- الدورات المنفصلة هي التي لا يوجد اتصال بينهم .

٣- الدورات المتصلة " " يوجد " "

Example:-

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix} \in S_6$

$= \underbrace{(1\,2\,4)}_{\text{دورة}}\underbrace{(5\,6)}_{\text{دورة}}$

دورة منفصلة

$\mu = (1\,2\,3)(3\,4\,6) \in S_6$

دورات متصلة

تركيب ان يطلع متصلة

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 6 & 5 & 1 \end{pmatrix}$$

$$= (1\,2\,3\,4\,6)$$ دورة منفصلة

وايضاً طريقة سهلة لايجاد معكوس التبديل.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ f(1) & f(2) & \cdots & & & f(n) \end{pmatrix}$$

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

بعدها نرتب f^{-1} بحيث تكون بشكل:

$$f^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ - & - & - & - \end{pmatrix}$$

Example:- $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$, Find f^{-1}?

الخطوة الأولى: نقلب الأسطر:

$$f^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \xleftarrow{\text{بعدها نرتب}} f^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Example:-

اذا كانت التباديل مكتوبة على شكل دورات

$f = (1\,4\,3\,5\,6) \in S_6$, Find f^{-1}!

① نثبت العنصر الأول

② ثم نقلب العناصر الباقية.

$$f^{-1} = (1\,6\,5\,3\,4)$$

أما اذا كانت الدورات منفصلة: نستخدم نفس الطريقة السابقة وهي تثبيت العنصر الأول ونقلب الباقي

$$f = (1\,5\,6)(2\,8) \in S_8$$

$$f^{-1} = (1\,6\,5)(2\,8)$$

(47)

(*) حساب القوى للتبديل f^n

(*) Example:-

$f=(1\,2\,3\,4\,5\,6) \in S_6$, Find f^2, f^3, f^4, f^5, f^6 ?

ملاحظة:-

① نلاحظ أن

Sol

$f=(1\;\;2\;\;3\;\;4\;\;5\;\;6)$

$f^2=(1\,3\,5)(2\,4\,6) = \left.\begin{matrix}1\to3\\3\to5\\5\to1\\2\to4\\4\to6\\6\to2\end{matrix}\right\}$

دورتين منفصلة

يعني نتخطى ٣ خطوات

$f^3=(1\,4)(2\,5)(3\,6)$ $\quad \left\{\begin{matrix}f=(1\,2\,3\,4\,5\,6)\\ f^3=(1\,4)(2\,5)(3\,6)\end{matrix}\right.$ $\quad \left.\begin{matrix}1\to4\\4\to1\\2\to5\\5\to2\\3\to6\\6\to3\end{matrix}\right\}$

$f^4=(1\,5\,3)(2\,6\,4)$ $\quad \left\{\begin{matrix}f=(1\,2\,3\,4\,5\,6)\\ f^4=(1\,5\,3)(2\,6\,4)\end{matrix}\right.$ $\quad \left.\begin{matrix}1\to5\\5\to3\\3\to1\\2\to6\\6\to4\\4\to2\end{matrix}\right\}$

$f^5=(1\,6\,5\,4\,3\,2) = \left.\begin{matrix}1\to6\\6\to5\\5\to4\\4\to3\\3\to2\\2\to1\end{matrix}\right)$

$f^6 = I = \left.\begin{matrix}1\to1\\2\to2\\3\to3\\4\to4\\5\to5\end{matrix}\right)$

(*) Example:-

$f=(1\,2\,4\,5)(3\,6) \in S_6$. Find f^3, f^4 ?

Sol

$f^3=(1\,5\,4\,2)(3\,6) = \left.\begin{matrix}1\to5\\5\to4\\4\to2\\2\to1\\3\to6\\6\to3\end{matrix}\right\}$

$f^4=(I) = \left.\begin{matrix}1\to1\\2\to2\\3\to3\\4\to4\\5\to5\\6\to6\end{matrix}\right)$

The order of Permutation:-   رتبة التباديل:

① نكتب التباديل على صورة دورات منفصلة

$$f = \underbrace{(\;---\;)}_{l_1 \text{ ذات طول}}\underbrace{(\;---\;)}_{l_2}\underbrace{(\;---\;)}_{l_3} \;----\; \underbrace{(\;---\;)}_{L_n}$$

$$|f| = \text{l.c.m}(l_1, l_2, l_3, \ldots L_n)$$

$$= \boxed{\frac{L_1 \cdot L_2 \cdot L_3 \cdot \ldots \cdot L_n}{\text{g.c.d}(L_1, L_2 L_3, \ldots L_n)}}$$

Example:- $f = (\underbrace{1\,4\,5}_{3})(\underbrace{2\,3}_{2}) \in S_5$. Find $|f|$

$$|f| = \text{l.c.m}(3, 2)$$

$$= \frac{2 \cdot 3}{\text{g.c.d}(2 \cdot 3)} = \frac{6}{1} = \underline{\underline{6}}$$

$\therefore |f| = \underline{\underline{6}}$ رتبة التبديل $= \underline{\underline{6}}$

Example:- $f = (1234)(2435) \in S_5$

① نحولها إلى دورات منفصلة ثم نجد $|f|$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$= (\underbrace{1\,2}_{2})(\underbrace{3\,5}_{2})$$

$$\therefore |f| = \text{l.c.m}(2, 2)$$

$$= \frac{2 \cdot 2}{\text{g.c.d}(2, 2)} = \frac{4}{2} = \underline{\underline{2}} \Rightarrow |f| = \underline{\underline{2}}$$

لو طلب هنا ايجاد f^{-13} مثلاً :-

$$f^{-13} = (f^{13})^{-1} = (f^{12+1})^{-1} = (f^{12} \circ f^{1})^{-1}$$

$$= f^{12} = I \Rightarrow f^{-13} = \underline{\underline{f^{-1}}}$$

للمثال السابق

$f = (1\,4\,5)(2\,3)$

$|f| = \underline{\underline{6}} \Rightarrow f^{12} = I$ مضاعفات الستة

$f^{-1} = (1\,5\,4)(2\,3)$

ملاحظة مهمة جداً جداً :-

رتبة S_n هو $n!$ أي عدد التبديلات في الزمرة مثلاً :-

$|S_3| = 3! = 6$

$|S_4| = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$

$|S_6| = 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$

وهكذا .

(50)

∴ The order elements of $(S_n, \circ)$ group تذكر

(٩) رتبة العناصر في $(S_n, \circ)$ الزمرة التناظرية.

$$(S_3, \circ) = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

$$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

الآن نجد رتبة العنصر $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

أولاً: نكتب التبديل على شكل دورة منفصلة

$$: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

(*) رتبة العنصر هو طول الدورة.

$$\therefore o(f_5) = \underline{2}$$

(*) **Example:-** $(S_6, \circ) = 6! = 720$ هذا عدد او رتبة (S_6)

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix}, \text{Find the order of } (f)?$$

(*) أولاً: نحولها الى دورات منفصلة

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix} = \underset{3}{\underline{(145)}}\,\underset{2}{\underline{(23)}}$$

دورتين منفصلة

رتبة f هو المضاعف المشترك الأصغر للدورتين

$$\therefore o(f) = \text{L.C.M}(3,2) = \underline{6}.$$

(*) **Example:-** Find the order of f, where

$$f = (1\,2\,3)(4\,5\,3) \in S_5.$$

في هذا المثال نلاحظ أن الدورات متصلة وليست منفصلة.
يجب أن نحولها الى منفصلة لكي نجد الرتبة لـ f.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (\underbrace{1\,2\,3\,4\,5}_{5})$$

$\therefore o(f) = \underline{\underline{5}}$

Example:- Find the order of f and σ where:

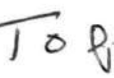
$$\left.\begin{aligned} f &= (1\,2)(2\,4\,3) \in S_4 \\ \sigma &= (5\,4\,3\,2)(1\,6) \in S_6. \end{aligned}\right\} \quad \text{H.W}$$

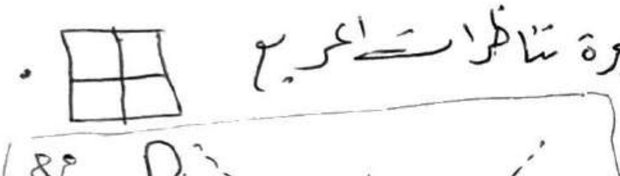
Symmetric group — زمرة التناظر حول المربع

(*) **Definition:-** The symmetric group is a spacial part (حالة خاصة) of the permutation groups (من زمرة التبادل) for describing images similar to geometric shaps (اشكال) such as triangle and squar (مربع).

And it takes all the property at permutation. مما تأخذ جميع خصائص التباديل.

To prove that the symmetric is a group :- برهنة أن التناظر زمرة

يجب ان نوضح بعض الأشياء الخاصة بزمرة تناظرات المربع  .



الشكل العام له هو:

المجموعة هي:

$$G_s = \{R_{90}, R_{180}, R_{270}, R_{360}, H, V, D_1, D_2\}$$

R_{90} : دوران خانة واحدة باتجاه عقارب الساعة

R_{180} : " خانتين " "

R_{270} : " ثلاث خانات " "

R_{360} : " اربع خانات (وهي العنصر المحايد)

H : انعكاس حول المحور الأفقي.

V : انعكاس حول المحور العمودي.

D_1 : انعكاس على القطر الرئيسي

D_2 : انعكاس على القطر الثانوي

(*) ملاحظة :- الدورات يكون باتجاه عقارب الساعة

(*) **Examples:-**

$$\begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix} \xrightarrow{R_{90}} \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix} \xrightarrow{R_{180}} \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix} \xrightarrow{V} \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix} \xrightarrow{D_2} \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{R_{270}}\begin{bmatrix}2&3\\1&4\end{bmatrix}$$

هذه الأشكال كل دورانه وانعكاسها .

$$\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{R_{360}}\begin{bmatrix}1&2\\4&3\end{bmatrix}=I$$ العنصر المحايد

$$H\;\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{H}\begin{bmatrix}4&3\\1&2\end{bmatrix}$$

$$D_1\;\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{D_1}\begin{bmatrix}3&2\\4&1\end{bmatrix}$$

العملية المعرفة على هذه المجموعة هي التركيب .

للسهولة بالإمكان كتابتها * والتي تعني ∘.

* Examples:-

1- $R_{180} * D_1$ حركتين باتجاه عقارب الساعة

$$\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{D_1}\begin{bmatrix}3&2\\4&1\end{bmatrix}\xrightarrow{R_{180}}\begin{bmatrix}1&4\\2&3\end{bmatrix}=D_2$$ وهذا تقابل

D_2

2- $D_1 * H$

$$H\;\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{H}\begin{bmatrix}4&3\\1&2\end{bmatrix}\xrightarrow{D_1}\begin{bmatrix}2&3\\1&4\end{bmatrix}=R_{270}$$

3- $H * R_{180}$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{R_{180}}H\;\begin{bmatrix}3&4\\2&1\end{bmatrix}\xrightarrow{H}\begin{bmatrix}2&1\\3&4\end{bmatrix}=V$$

V

4- $D_2 * H$

$$H\;\begin{bmatrix}1&2\\4&3\end{bmatrix}\xrightarrow{H}\begin{bmatrix}4&3\\1&2\end{bmatrix}\xrightarrow{D_2}\begin{bmatrix}4&1\\3&2\end{bmatrix}=R_{90}$$

D_2

وهكذا ...

شرح مبسط لزمرة التناظر حول المربع: "Symmetric group"

* عناصر هذه الزمرة هي عبارة عن مجموعة دورانات ومجموعة انعكاس

* الدورانات متكونة من: $R_{360}, R_{90}, R_{180}, R_{270}$ حيث:

$$\underset{R_{360}}{\begin{bmatrix}1&2\\4&3\end{bmatrix}},\quad \underset{R_{90}}{\begin{bmatrix}4&1\\3&2\end{bmatrix}}\quad \underset{R_{180}}{\begin{bmatrix}3&4\\2&1\end{bmatrix}}\quad \underset{R_{270}}{\begin{bmatrix}2&3\\1&4\end{bmatrix}}$$

* الانعكاس متكون من: V, H, D_1, D_2 حيث:

$$\underset{V}{\begin{bmatrix}2&1\\3&4\end{bmatrix}}\quad \underset{H}{\begin{bmatrix}4&3\\1&2\end{bmatrix}}\quad \underset{D_1}{\begin{bmatrix}3&2\\4&1\end{bmatrix}}\quad \underset{D_2}{\begin{bmatrix}1&4\\2&3\end{bmatrix}}$$

* العملية المعرفة على هذه المجموعة هي التركيب وللسهولة نكتب *

مثال:

$R_{90} * R_{180}$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{R_{180}} \begin{bmatrix}3&4\\2&1\end{bmatrix} \xrightarrow{R_{90}} \begin{bmatrix}2&3\\1&4\end{bmatrix} = R_{270}$$

$R_{180} * V$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{V} \begin{bmatrix}2&1\\3&4\end{bmatrix} \xrightarrow{R_{180}} \begin{bmatrix}4&3\\1&2\end{bmatrix} = H$$

$H * R_{90}$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{R_{90}} \begin{bmatrix}4&1\\3&2\end{bmatrix} \xrightarrow{H} \begin{bmatrix}3&2\\4&1\end{bmatrix} = D_1$$

$D_1 * V$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{V} \begin{bmatrix}2&1\\3&4\end{bmatrix} \xrightarrow{D_1} \begin{bmatrix}4&1\\3&2\end{bmatrix} = R_{90}$$

→ هذه الزمرة ليست ابدالية

$V * D_1$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{D_1} \begin{bmatrix}3&2\\4&1\end{bmatrix} \xrightarrow{V} \begin{bmatrix}2&3\\1&4\end{bmatrix} = R_{270}$$

نلاحظ هناك عدة حالات في التركيب وهي:

١- دوران * دوران : في هذه الحالة نقوم بجمع الزوايا أي

$$R_x * R_y = R_{x+y}$$ حيث R_{360} هي العنصر المحايد

$$R_{90} * R_{180} = R_{270}$$

$$R_{180} * R_{270} = R_{90} \Longrightarrow \begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{R_{270}} \begin{bmatrix}2&3\\1&4\end{bmatrix} \xrightarrow{R_{180}} \begin{bmatrix}4&1\\3&2\end{bmatrix} = R_{90}$$

وهكذا .

٢- دوران * انعكاس : في هذه الحالة تحرك الانعكاس عكس اتجاه عقارب الساعة بحركات مساوية للدوران الموجود حيث أن

R_{90} = حركة واحدة

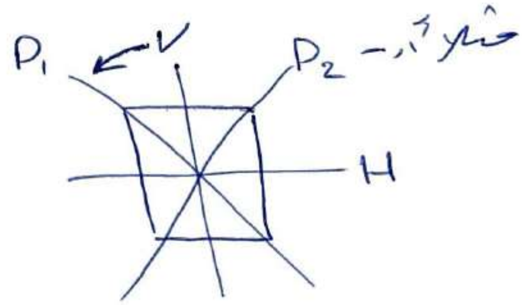
R_{180} = حركتين

R_{270} = ثلاث حركات

R_{360} = ٤ حركات

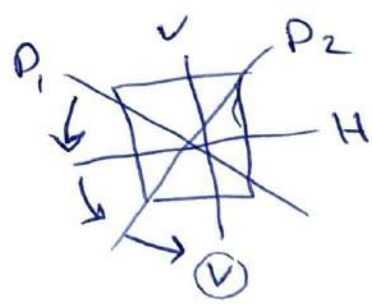
$$R_{90} * V$$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{V} \begin{bmatrix}2&1\\3&4\end{bmatrix} \xrightarrow{R_{90}} \begin{bmatrix}3&2\\4&1\end{bmatrix} = D_1$$



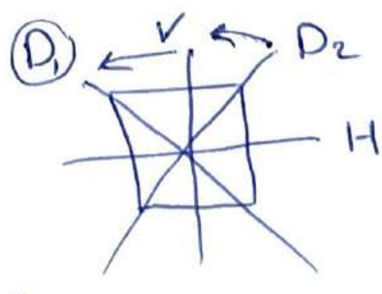
$$R_{270} * D_1$$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{D_1} \begin{bmatrix}3&2\\4&1\end{bmatrix} \xrightarrow{R_{270}} \begin{bmatrix}2&1\\3&4\end{bmatrix} = V$$



$$R_{180} * D_2$$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{D_2} \begin{bmatrix}1&4\\2&3\end{bmatrix} \xrightarrow{R_{180}} \begin{bmatrix}3&2\\4&1\end{bmatrix} = D_1$$

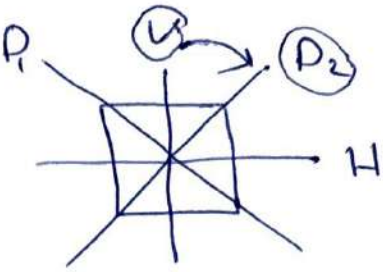


وهكذا !

٣- انعكاس * دوران: في هذه الحالة نحرك الانعكاس مع عقارب الساعة وأحياناً حسب الحركات المذكورة سابقاً مثلاً:

$V * R_{90}$

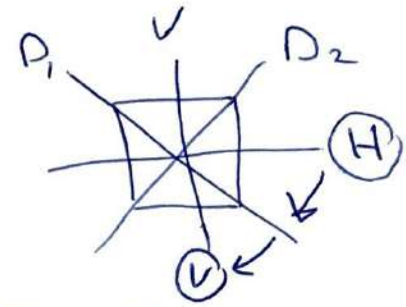
$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{R_{90}} \begin{bmatrix}4&1\\3&2\end{bmatrix} \xrightarrow{V} \begin{bmatrix}1&4\\2&3\end{bmatrix} = D_2$$



حركة واحدة

$H * R_{180}$

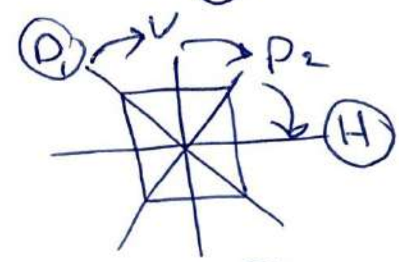
$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{R_{180}} \begin{bmatrix}3&4\\2&1\end{bmatrix} \xrightarrow{H} \begin{bmatrix}2&1\\3&4\end{bmatrix} = V$$



حركتين

$D_1 * R_{270}$

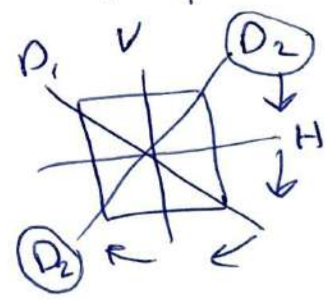
$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{R_{270}} \begin{bmatrix}2&3\\1&4\end{bmatrix} \xrightarrow{D_1} \begin{bmatrix}4&3\\1&2\end{bmatrix} = H$$



ثلاث حركات

$D_2 * R_{360}$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{R_{360}} \begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{D_2} \begin{bmatrix}1&4\\2&3\end{bmatrix} = D_2$$

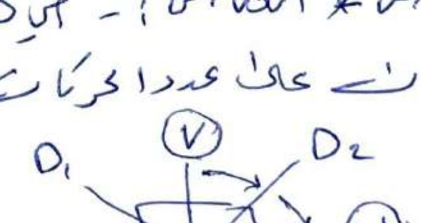


وهكذا .....

٤- انعكاس * انعكاس: - أي هذه الحالة يكون الناتج دائماً دوران ويكون على عدد الحركات المحصورة بين الانعكاسين مثلاً
ومع عقارب الساعة

$V * H$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{H} \begin{bmatrix}4&3\\1&2\end{bmatrix} \xrightarrow{V} \begin{bmatrix}3&4\\2&1\end{bmatrix} = R_{180}$$



حركتين
R_{180}

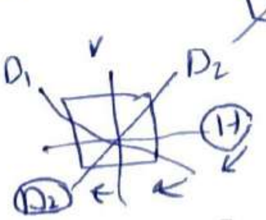
$D_1 * H$

$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \xrightarrow{H} \begin{bmatrix}4&3\\1&2\end{bmatrix} \xrightarrow{D_1} \begin{bmatrix}2&3\\1&4\end{bmatrix} = R_{270}$$

ثلاث حركات
R_{270}

$H * D_2$

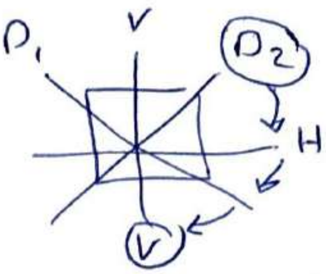
$$\begin{bmatrix}1&2\\4&3\end{bmatrix} \rightarrow \begin{bmatrix}1&4\\2&3\end{bmatrix} \longrightarrow \begin{bmatrix}2&3\\1&4\end{bmatrix} = R_{270}$$



ثلاث حركات
R_{270}

$D_2 * V$

$\boxed{\begin{smallmatrix}1&2\\4&3\end{smallmatrix}} \xrightarrow{V} \boxed{\begin{smallmatrix}2&1\\3&4\end{smallmatrix}} \xrightarrow{D_2} \boxed{\begin{smallmatrix}2&3\\1&4\end{smallmatrix}} = R_{270}$



تمثل حركات
R_{270}

وهكذا.....

* رتبة الزمرة $(Sy, \circ)$ هو $|Sy| = 8$ لأن

$$Symmetric = \{R_{90}, R_{180}, R_{270}, R_{360}, V, H, D_1, D_2\}$$

العنصر المحايد لهذه الزمرة هو R_{360}.

* رتبة العناصر هي :-

$|R_{360}| = 1$

$|R_{90}| = 4 = |R_{270}|$

$|R_{180}| = 2$

$|V| = 2 = |H| = |D_1| = |D_2|$

* وأيضاً : معكوس العناصر هو

$R_{360}^{-1} = R_{360}$

$R_{90}^{-1} = R_{270}$, $R_{270}^{-1} = R_{90}$, $R_{180}^{-1} = R_{180}$

$V^{-1} = V$, $H^{-1} = H$, $D_1^{-1} = D_1$, $D_2^{-1} = D_2$

* امثلة متنوعة :-

بالاعتماد على رتبة العناصر والحركات والدورانات والانعكاسات

$$\left(R_{90}^{-15} * V^{9}\right)^{3} * H^{3}$$

$$\left(\left(R_{90}^{12+3}\right)^{-1} * V^{8+1}\right)^{3} * H^{2+1}$$

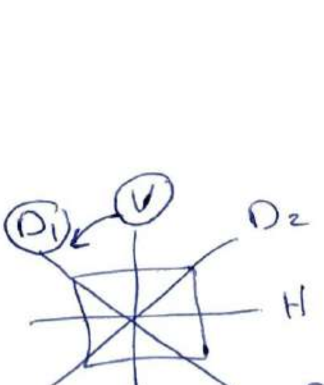
$$= \left(\left(R_{90}^{3}\right)^{-1} * V\right)^{3} * H$$

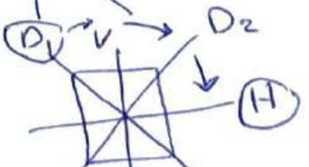
$$= \left(\left(R_{270}\right)^{-1} * V\right)^{3} * H$$

$$= \left(R_{90} * V\right)^{3} * H$$

$$= \left(D_1\right)^{3} * H$$

$$= D_1^{2+1} * H = D_1 * H = R_{270}$$





$\boxed{\begin{smallmatrix}1&2\\4&3\end{smallmatrix}} \xrightarrow{H} \boxed{\begin{smallmatrix}4&3\\1&2\end{smallmatrix}} \xrightarrow{D_1} \boxed{\begin{smallmatrix}2&3\\1&4\end{smallmatrix}} = R_{270}$

* رتبة عناصر زمرة تناظرات المربع $\boxed{\begin{matrix}1 & 2\\ 4 & 3\end{matrix}}$ (order):

$|R_{360}| = 1$, $|R_{270}| = |R_{90}| = 4$, $|R_{180}| = 2$

ورتبة أي انعكاس = 2

$|V| = |H| = |D_1| = |D_2| = \underline{\underline{2}}$

لأنه:

$(R_{270})^4 = R_{270} * R_{270} * R_{270} * R_{270} = \underline{\underline{R_{360}}} \Rightarrow |R_{270}| = 4$

$(R_{180})^2 = R_{180} * R_{180} = R_{360} \Rightarrow |R_{180}| = 2$

$(R_{90})^2 = R_{90} * R_{90} * R_{90} * R_{90} = R_{360} \Rightarrow |R_{90}| = 4$

$(R_{360})^1 = R_{360}. \Rightarrow |R_{360}| = 1$

وأن

$(V)^2 = V * V = R_{360} \Rightarrow |V| = 2$

$(D_1)^2 = D_1 * D_1 = R_{360} \Rightarrow |D_1| = 2$

$(D_2)^2 = D_2 * D_2 = R_{360} \Rightarrow |D_2| = 2$

$(H)^2 = H * H = R_{360} \Rightarrow |H| = 2$

نلاحظ أن مجموعة التناظرات مع عملية $\circ$ هي زمرة لأنه تحقق شروط الزمرة الأربعة وهي

(1) closur.

(2) Assoc.

(3) Identity $= R_{360}$

(4) Inverse. $\Rightarrow R_{90}^{-1} = R_{270}$, $R_{270}^{-1} = R_{90}$, $R_{180}^{-1} = R_{180}$, $R_{360}^{-1} = R_{360}$.

$V^{-1} = V$, $H^{-1} = H$, $D_1^{-1} = D_1$, $D_2^{-1} = D_2$.

حل مجموعة اسئلة :

Q1/ Let $G = \{(a,b) : a,b \in \mathbb{R},\ a \neq 0\}$, define the operation $*$ on G by:- $(a,b)*(c,d) = (ac, bc+d)$. Is $(G,*)$ form a group?

Sol//

1- $*$ is closed: This is clear that $*$ is closed by definition.

2- let $(a,b), (c,d), (e,f) \in G$

$$[(a,b)*(c,d)]*(e,f) = (ac, bc+d)*(e,f)$$
$$= ((ac)e, (bc+d)\cdot e + f)$$
$$= a(ce), b(ce) + (de+f)$$
$$= (a,b)*(ce, de+f)$$
$$= (a,b)*[(c,d)*(e,f)]$$

$\therefore$ $*$ is associative.

3- Let $e = (g,h)$, $g,h \in \mathbb{R}$ and $g \neq 0$

$\therefore e*(a,b) = (a,b)*e = (a,b)$ $\quad \forall (a,b) \in G$

$(g,h)*(a,b) = a,b$

$\Rightarrow (ga, (ha+b)) = (a,b)$

$\Rightarrow ga = a \Rightarrow g = 1$, $ha+b = b \Rightarrow ha = 0 \Rightarrow h = \underline{0}$

$\therefore (g,h) = (1,0) = e$ The identity element of G.

4- let $(a,b)^{-1} = (k,l)$, $k,l \in \mathbb{R}$, $k \neq 0$

$\therefore (a,b)*(k,l) = (g,h) \Rightarrow (a,b)*(k,l) = (1,0)$

$\Rightarrow (ak, bk+l) = (1,0)$

$\Rightarrow ak = 1 \Rightarrow \boxed{k = 1/a}$, $bk + l = 0 \Rightarrow bk = -l$

$\Rightarrow l = -b \cdot 1/a = \boxed{-b/a}$

$\therefore$ The inverse element of (a,b) in G is $(1/a, -b/a)$ ②

$\therefore$ The system $(G,*)$ form a groups.

Q/ Is $(G,*)$ a comm. group. ?

Sol: No, because:- if $(1,5)*(3,0)=(3,15)$

but $(3,0)*(1,5)=(3,5) \neq (3,15)$.

Q2/ Show that $(Z_e,+)$ is a form group?

Sol: 1- let $a,b \in Z_e$. <To prove $a+b \in Z_e$>

$\because a,b \in Z_e$, $\therefore a=2n$, $b=2m$ for some $n,m \in Z_e$

$a+b=2n+2m=2(n+m)=2k \in Z_e$ for some $k=n+m \in Z$

$\therefore Z_e$ is closed under $+$.

2- Let $a,b \in Z_e$

$\therefore a=2n$, $b=2m$, $c=2k$ for some $n,m,k \in Z$

$$(a+b)+c=(2n+2m)+2k = 2(n+m)+2k$$
$$=2(n+m+k)$$
$$=2n+2(m+k)$$
$$=a+(b+c)$$

$\therefore +$ is associative.

3- The identity element of Z_e is 0

4 The inverse element of $a \in Z_e$ is $-a \in Z_e$, where $a=2n$ for some $n \in Z$.

$-a=-2n$

5- $a+b=2n+2m$
$=2(n+m)=2(m+n)=2m+2n=b+a$

$\therefore (Z_e,+)$ is a comm. group.

Q3/ let $X \neq \phi$, $P(X) = \{A : A \subseteq X\}$. The power set of X. (2)

Is $(P(X), \cap)$ form a group?

Sol/ ① let $A, B \in P(X)$. < To Prove $A \cap B \in P(X)$

$\because A, B \in P(X) \Rightarrow A \subseteq X \wedge B \subseteq X$

$\Rightarrow A \cap B \subseteq X$

$\Rightarrow A \cap B \in P(X)$

$\therefore P(X)$ is closed under $\cap$.

2- let $A, B, C \in P(X)$

$(A \cap B) \cap C = \{x : x \in A \cap B \wedge x \in C\}$

$= \{x : (x \in A \wedge x \in B) \wedge x \in C\}$

$= \{x : x \in A \wedge (x \in B \wedge x \in C)\}$

$= \{x : x \in A \wedge (x \in B \cap C)\}$

$= A \cap (B \cap C)$. $\therefore \cap$ is associative.

3- $X \in P(X)$ s.t. $\forall A \in P(X) \Rightarrow A \subseteq X$

$\Rightarrow A \cap X = X \cap A = A$

$\therefore$ The identity element of $P(X)$ is X.

4- let $A \in P(X)$

if $A = X \Rightarrow X \cap X = X \Rightarrow X^{-1} = X$

if $A \neq X \Rightarrow A \subseteq X$

$\Rightarrow A \cap B \neq X$, $\forall B \in P(X)$.

$\therefore A$ has no inverse

$\therefore (P(X), \cap)$ is not a group. ⊛

Q4/ let $M_2^*(R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in R , ad - bc \neq 0 \right\}$. show that

$(M_2^*(R), \cdot)$ form a group?

Sol: 1- Let $A, B \in M_2^*(R)$ s.t. $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$

To Prove $A \cdot B \in M_2^*(R)$

$$A \cdot B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix} \in M_2^*(R).$$

$\therefore M_2(R)$ is closed under $\cdot$

2- (To Prove $A \cdot I = I \cdot A = A$)

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$\Rightarrow ax + bz = a$ --- (1)

$ay + bw = b$ --- (2)

$cx + dz = c$ --- (3)

$cy + dw = d$ --- (4)

$x = \dfrac{a - bz}{a}$ --- (1) $\qquad x = \dfrac{c - dz}{c}$ --- (3)

$y = \dfrac{b - bw}{a}$ --- (2) $\qquad y = \dfrac{d - dw}{d}$ --- (4)

من (1) و (3)

$$\frac{a - bz}{a} = \frac{c - dz}{c} \Rightarrow c(a - bz) = a(c - dz)$$

$$= \cancel{ca} - bzc = \cancel{a}c - dza$$

$$= adz - bzc = 0 \Rightarrow z(ad - bc) = 0$$

$z = 0 \Leftarrow$ بالفرض $(ad - bc) \neq 0$ علماً بأن

بالتعويض

$\Rightarrow \boxed{x = 1}$

من (2) و (4)

$$\frac{b - bw}{a} = \frac{d - dw}{c} \Rightarrow c(b - bw) = a(d - dw) = cb - cbw = ad - adw$$

$= cb(1 - w) = ad(1 - w)$

$= cb(1-w) - ad(1-w) =$

$(1 - w)(cb - ad) = 0$

$= (w - 1)(ad - cb) = 0$

علماً بأن

$\boxed{w = 1} \Leftarrow w - 1 = 0 \Leftarrow$ بالفرض $(ad - cb) \neq 0$

بالتعويض $\boxed{y = 0/a = 0}$

$\boxed{\therefore x = 1, y = 0, z = 0, w = 1}$ $\quad \therefore I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_2^*$

(5) تابعه

4- $A \cdot A^{-1} = I$

لإيجاد A^{-1} نوجد Adj A

$$A^{-1} = \frac{\operatorname{Adj} A}{|A|}$$

$$\operatorname{Adj} A = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \Rightarrow A^{-1} = \frac{\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}} = \frac{\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}}{(ad-cb)} \neq 0$$ بالفرض

$$\therefore A^{-1} = \begin{bmatrix} \frac{d}{(ad-cb)} & \frac{-b}{(ad-cb)} \\ \frac{-c}{(ad-cb)} & \frac{a}{(ad-cb)} \end{bmatrix}$$

$$\therefore A \cdot A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \frac{d}{(ad-cb)} & \frac{-b}{(ad-cb)} \\ \frac{-c}{(ad-cb)} & \frac{a}{(ad-cb)} \end{bmatrix} = \begin{bmatrix} \frac{ad-cb}{ad-cb} & \frac{-ab+ab}{ad-cb} \\ \frac{cd-cd}{ad-cb} & \frac{-ca+ad}{ad-cb} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore (M_2^*(R), \cdot)$ is a form group.

but it is not comm group because

let $A = \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 1 \\ 2 & 4 \end{bmatrix}$

$A \cdot B = \begin{bmatrix} 10 & 2 \\ 11 & 13 \end{bmatrix}$, $B \cdot A = [\ 11$

تكفي

$\therefore A \cdot B \neq B \cdot A$.

$\therefore (M_2^*(R), \cdot)$ is not comm-group.

* Problem:-

Let $S = \mathbb{R} \setminus \{-1\}$. Define $*$ on S by $a*b = a+b+ab$.

(a) Show that $*$ is a binary operation on S.

(b) Show that $(S,*)$ is a group.

(c) Find the solution of the equation $2*x*3=7$ in S.

Solve

(a) We must show that S is closed under $*$, that is, that

$a+b+ab \neq -1$ for $a,b \in S$.

Now: $a+b+ab=-1$ iff $0 = ab+a+b+1$

$= (a+1)(b+1)$.

This is the case iff either $a=-1$ or $b=-1$, whis is not the case for $a,b \in S$. ⊠

(b) We have $a*(b*c) = a*(b+c+bc) = a+(b+c+bc)+a(b+c+bc)$

$= a+b+c+ab+ac+bc+abc$ --- (1)

and $(a*b)*c = (a+b+ab)*c = (a+b+ab)+c+(a+b+ab)c$

$= a+b+c+ab+ac+bc+abc$ --- (2)

$1 = 2 \Rightarrow *$ is assoc. on S.

Now: Let $e \in S$ $e \neq \{-1\}$

$a*e = a \Rightarrow a+e+ae = a \Rightarrow e+ae=0 \Rightarrow$

$e(1+a)=0 \Rightarrow e=\underline{\underline{0}}$

$\therefore$ identity element $e=0 \in S$.

Since $a * 0 = 0 * a = a$.

Also, $\frac{-a}{a+1}$ acts as inverse of a, for $a * a' = a' * a = e$

$a + a' + aa' = 0 \Rightarrow a'(1+a) = -a \Rightarrow a' = \frac{-a}{1+a}$. c

$\therefore a * \frac{-a}{1+a} = 0 = a + \frac{-a}{1+a} + a \cdot \frac{-a}{1+a} = 0$

$$= \frac{a(1+a) - a - a^2}{(1+a)} = 0 = \frac{a + a^2 - a - a^2}{1+a} = \frac{0}{1+a} = \underline{\underline{0}}.$$

Thus $(S, *)$ is a group. ⊠

(c) Because the operation is comm. $2 * x * 3 = 2 * 3 * x = 11 * x$.

$$2 * x * 3 = (2 + x + 2x) * 3$$

$$= 2 + x + 2x + 3 + (2 + x + 2x)3$$ فسبه عليه

$$= 5 + 3x + 6 + 3x + 6x = 11 + 12x = 11 + x + 11x$$

$$= 11 * x.$$

Now by inverse of 11 is $\frac{-a}{1+a} = \frac{-11}{12}$, by (b).

(باستخدام المعكوس)

From $11 * x = 7$ we obtain

$$x = \frac{-11}{12} * 7 = \frac{-11}{12} + 7 + \frac{-11}{12} \cdot 7 = \frac{-11 + 84 - 77}{12} = \frac{-4}{12} = \boxed{\frac{-1}{3}}$$

$\therefore x = \frac{-1}{3}$. ⊠.

Chapter Two:-
Subgroups and Cyclic groups
"الزمر الجزئية والزمر الدائرية"

Definition(1): Let $(G,*)$ be a group and $H \subseteq G$, H is a non-empty subset of G. Then $(H,*)$ is a subgp of $(G,*)$ if $(H,*)$ is itself a group.

Definition(2):-

Let $(G,*)$ be a group and $H \subseteq G$, then $(H,*)$ is a subgroup of G if:

1- $\forall a,b \in H \Rightarrow a*b \in H$

2- The identity element of G is an element of H (i.e.) $e \in G \Rightarrow e \in H$.

3- $\forall a \in H \Rightarrow a^{-1} \in H$.

مهمة جداً جداً

Remark(1):-

Each group $(G,*)$ has at least two subgroups $(\{e\},*)$ and $(G,*)$, these subgroups are known trivial subgroup and improper, any subgroup different from these subgroups known a proper subgroups.

تافهة

غير فعلية

فعلية

Examples:-

1- $(\mathbb{Z},+)$ is a proper subgroup of $(\mathbb{R},+)$.

2- $H=\{1,-1\} \subseteq \{1,-1,i,-i\}$, then $(H,\cdot)$ is a subgroup of $(\{1,-1,i,-i\},\cdot)$.

3- $H=\{\bar{0},\bar{2}\} \subseteq \mathbb{Z}_4$

$(H,+_4)$ is a proper subgroup of $(\mathbb{Z}_4,+_4)$. But $\{\bar{0},\bar{3}\}$ is not subgroup of $(\mathbb{Z}_4,+_4)$.

4- $(\mathbb{Q}^*,\cdot)$ is a subgroup of $(\mathbb{R}^*,\cdot)$.

Theorem (1):- Let $(G,*)$ be a group and $\phi \neq H \subseteq G$. Then $(H,*)$ is a subgroup of $(G,*)$ iff $a*b^{-1} \in H \ \forall a,b \in H$.

Proof:-

$(\Rightarrow)$ Let $(H,*)$ be a subgroup and $a,b \in H$, then

$a,b^{-1} \in H \Rightarrow a*b^{-1} \in H$ (Since $*$ closure).

$(\Leftarrow)$ Let $a*b^{-1} \in H$. To prove $(H,*)$ is a subgroup.

(1) Since $H \neq \phi \Rightarrow \exists\, b \in H$ s.t. $b*b^{-1} \in H \Rightarrow e \in H$.

(2) since $b \in H$ and $e \in H \Rightarrow e*b^{-1} \in H \Rightarrow b^{-1} \in H$

(3) Let $a \in H$ and $b^{-1} \in H$ (by 2) $\Rightarrow a*(b^{-1})^{-1} \in H \Rightarrow a*b \in H$

$\therefore$ By definition (2) $(H,*)$ is a subgroup of $(G,*)$. $\boxtimes$

Example (2):- Let $(Z,+)$ be a group and $H=\{5a : a\in Z\}$, show that $(H,+)$ is a subgroup of $(Z,+)$.

Sol. By Theorem ①, Let $x+y \in H$. To Prove $x+y^{-1} \in H$

$$x\in H \Rightarrow x=5a,\ a\in Z,\quad y\in H \Rightarrow y=5b,\ b\in Z$$

$$x+y^{-1} = 5a+(5b)^{-1} = 5a+5(-b)$$
$$= 5(\underbrace{a-b}_{\in Z}) \in H$$

$\Rightarrow (H,+)$ is a subgp of $(Z,+)$. ⊠

⊛ The operationes of Subgroups:

العمليات على الزمر الجزئية:

① The Intersection of subgroups: تقاطع الزمر الجزئية.

Theorem ②:- If $(H_i,*)$ are the collection of subgroups of $(G,*)$, then $(\cap H_i,*)$ is also subgroup of $(G,*)$.

Proof:-

① Since $\exists e\in H_i,\ \forall i \Rightarrow e\in \cap H_i \Rightarrow \cap H_i \neq \phi$.

② Let $x,y\in \cap H_i$. T.P. $x*y^{-1}\in \cap H_i$

Since $x,y\in \cap H_i \Rightarrow x,y\in H_i,\ \forall i$

$\Rightarrow x*y^{-1}\in H_i,\ \forall i$ (Since H_i Subgroups)

$\Rightarrow x*y^{-1}\in \cap H_i$.

$\therefore (\cap H_i,*)$ is a subgp of $(G,*)$. ⊠

② The Union of Subgroups:- الاتحاد في الزمر الجزئية:

Theorem (3):- Let $(H_1,*)$ and $(H_2,*)$ are two subgroups of $(G,*)$ then $(H_1 \cup H_2,*)$ is a subgroup of $(G,*)$ iff $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proof: ($\Rightarrow$) Let $(H_1 \cup H_2,*)$ is a subgroup, T.P. $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Suppose that $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$

$\therefore \exists\, a \in H_1,\ a \notin H_2$ and $b \in H_2,\ b \notin H_1$

$\therefore a*b \in H_1 \cup H_2 \Rightarrow a*b^{-1} \in H_1 \cup H_2$

$\Rightarrow a*b^{-1} \in H_1$ or $a*b^{-1} \in H_2$

$\Rightarrow a,b \in H_1$ or $a,b \in H_2$ C! (تناقض).

$\therefore H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

($\Leftarrow$) Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$, T.P. $(H_1 \cup H_2,*)$ is a subgroup.

If $H_1 \subseteq H_2 \Rightarrow H_1 \cup H_2 = H_2$ is a subgp.

If $H_2 \subseteq H_1 \Rightarrow H_1 \cup H_2 = H_1$ is a subgp.

$\therefore (H_1 \cup H_2,*)$ is a subgp. ⊠.

Remark:- ملاحظة

$(H_1 \cup H_2,*)$ need not be a subgroup of $(G,*)$.

For example:- In $(Z_6,+_6)$, $H_1=\{\bar{0},\bar{2},\bar{4}\}$, $H_2=\{\bar{0},\bar{3}\}$

$H_1 \cup H_2=\{\bar{0},\bar{2},\bar{3},\bar{4}\}$, $\bar{2},\bar{3} \in H_1 \cup H_2$ but $\bar{2}+_6\bar{3}=\bar{5} \notin H_1 \cup H_2$. ⊠

$\therefore (H_1 \cup H_2,+_6)$ is not subgp.

(3)- The Product of Subgps:- مبادئ الزمر الجزئية :.

$H*K$:- Let $(G,*)$ be a group and $(H,*)$, $(K,*)$ are two subgps of G. Then the product of H and K is the set : $H*K = \{h*k : h \in H, k \in K\}$.

Example :- In $(Z_6, +_6)$, $H = \{\bar{0}, \bar{2}, \bar{4}\}$, $K = \{\bar{0}, \bar{3}\}$

$$H +_6 K = \{\bar{0} +_6 \bar{0}, \bar{0} +_6 \bar{3}, \bar{2} +_6 \bar{0}, \bar{2} +_6 \bar{3}, \bar{4} +_6 \bar{0}, \bar{4} +_6 \bar{3}\}$$

$$= \{\bar{0}, \bar{3}, \bar{2}, \bar{5}, \bar{4}, \bar{1}\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = Z_6.$$

Notes:-

1- $H*H$ is write H^2

2- If $H = \{a\}$, then $H*K = a*K$, If $K = \{b\}$, then $H*K = H*b$.

3- $H \cup K \subseteq H*K$.

Theorem (4):- Let $(G,*)$ be a group and $(H,*)$, $(K,*)$ are Two subgroups of G, then:-

1- $H*K \neq \phi \wedge H*K \subseteq G$.

2- $H \subseteq H*K$ and $K \subseteq H*K$.

3- $(H*K, *)$ is a subgp of G iff $H*K = K*H$.

4- If $(G,*)$ is a comm. gp, then $(H*K, *)$ is a subgp of G.

Proof:

(1) $\because e \in H \wedge e \in K \Rightarrow e * e = e \in H*K$

$\therefore H*K \neq \phi$

And let $x \in H*K \Rightarrow x = a*b \ni a \in H \subseteq G$ and $b \in K \subseteq G$

$\Rightarrow a \in G \wedge b \in G$

$\Rightarrow a*b = x \in G$

$\therefore H*K \subseteq G$

(2) Let $x \in H \Rightarrow x = x*e \in H*K$

$\Rightarrow x \in H*K$

$\therefore H \subseteq H*k$

Similarly $K \subseteq H*K$

(3) $(\Rightarrow)$ suppose $(H*K,*)$ is asubgroup of $(G,*)$ T.P. $H*K=K*H$

(i.e.) $H*K \subseteq K*H \wedge K*H \subseteq H*K$

Let $x \in H*K \Rightarrow x = a*b \ni a \in H \wedge b \in K$

Since $H*K$ is subgroupof $G \Rightarrow x^{-1} \in H*K$

Let $x^{-1} = c*d \ni c \in H \wedge d \in K$

$x = (x^{-1})^{-1} = (c*d)^{-1} = d^{-1}*c^{-1} \ni d^{-1} \in K \wedge c^{-1} \in H$

$\therefore x = d^{-1}*c^{-1} \in K*H$

$\therefore H*K \subseteq K*H$

$K*H \subseteq H*K$ **(H.W.)**

$(\Leftarrow)$ Let $H*K=K*H$ T.P.$(H*K,*)$ is subgroup of$(G,*)$

$H*K \neq \phi$and $H*K \subseteq G$ (by 1)

Let $x,y \in H*K$ T.P.$x*y^{-1} \in H*K$

$x \in H*K \Rightarrow x = a*b \ni a \in H \wedge b \in K$

$y \in H*K \Rightarrow y = c*d \ni c \in H \wedge d \in K$

$x*y^{-1} = (a*b)*(c*d)^{-1}$

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

$= a*(\underbrace{b*d^{-1}}_{\in K})*\underbrace{c^{-1}}_{\in H}$

$\therefore (b*d^{-1})*c^{-1} \in K*H = H*K$

$\therefore (b*d^{-1})*c^{-1} \in H*K$

$\Rightarrow \exists\, p \in H,\ \ell \in K \ni (b*d^{-1})*c^{-1} = p*\ell$

$\therefore a*(b*d^{-1})*c^{-1} = \underbrace{a*p}_{\in H} * \underbrace{\ell}_{\in K} \in H*K$

$\therefore x*y^{-1} \in H*k$

$\therefore (H*K,*)$ is subgroup of $(G,*)$

(4) If $(G,*)$ is commutative group, then $(H*K,*)$ is subgroup of $(G,*)$

Proof: $H*K \neq \phi$ and $H*K \subseteq G$ (by 1)

Let $x,y \in H*K$ T.P. $x*y^{-1} \in H*K$

$x \in H*K \Rightarrow x = a*b \ni a \in H \wedge b \in K$

$y \in H*K \Rightarrow y = c*d \ni c \in H \wedge d \in K$

$x*y^{-1} = (a*b)*(c*d)^{-1}$

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

$= (a*b)*(c^{-1}*d^{-1})$ (since G is commutative)

$= a*(b*)*d^{-1}$ ($*$ is associative)

$= (a*c^{-1})*(b*d^{-1})$ ($*$ is commutativeand associative)

$\therefore x*y^{-1} \in H*K$

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

Notes:-

1- $H * K \neq K * H$

2- $(H*K, *)$ need not be a subgroup of $(G,*)$. $\boxed{H.w}$.?

* Definition:- Center of a group * مركز الزمرة

The center of a group $(G,*)$, denoted by $Cent(G)$ or $C(G)$ is the set:

$$C(G) = \{ c \in G ; c*x = x*c, \forall x \in G \}$$

Note:-

$C(G) \neq \varphi$, since $\exists e \in G$ s.t.
$e*x = x*e \quad \forall x \in G \Rightarrow e \in C(G)$.

Example:- In symmetric group $(S_y, \circ)$

$$S_y = \{ R_{360}, R_{90}, R_{180}, R_{270}, V, H, D_1, D_2 \}$$

$C(S_y) = R_{360}$ because:

$$C(S_y) = \{ f \in S_y : f \circ g = g \circ f \quad \forall g \in S_y \} = R_{360}.$$

2- In $(Z_6, +_6)$, The $C(Z_6) = Z_6$ because:

$\bar{0} + \bar{0} = 0$, $\bar{0} + \bar{1} = \bar{1} + 0$, $0 + 2 = 2 + 0$ ---- $\bar{5} + \bar{0} = \bar{0} + \bar{5}$

$\bar{5} + \bar{1} = \bar{1} + \bar{5}$

$\bar{1} + \bar{0} = \bar{0} + 1$ ----

⋮

$\bar{5} + \bar{5} = \bar{5} + \bar{5}$. ⊠

$\bar{5} + \bar{0} = \bar{0} + \bar{5}$ ------

Theorem(5):- Let $(G,*)$ be a group. Then $(Cent(G),*)$ is a subgroup of $(G,*)$.

Proof:-

$Cent(G) \neq \phi$ because $e \in Cent(G)$ (by Note ⊛)

$C(G) = \{a \in G : x*a = a*x,\ \forall x \in G\} \subseteq G$.

Let $a, b \in Cent(G)$. T.P. $a*b^{-1} \in Cent(G)$

$a \in Cent(G) \Rightarrow a*x = x*a \quad \forall x \in G$

$b \in Cent(G) \Rightarrow b*x = x*b \quad \forall x \in G$

T.P. $(a*b^{-1})*x = x*(a*b^{-1}) \quad \forall x \in G$.

$$
\begin{aligned}
(a*b^{-1})*x &= a*(b^{-1}*x) \\
&= a*(x^{-1}*b)^{-1} \\
&= a*(b*x^{-1})^{-1} \quad (\text{since } b \in Cent(G)) \\
&= a*(x*b^{-1}) \\
&= (a*x)*b^{-1} \\
&= (x*a)*b^{-1} \quad (\text{since } b \in Cent(G)). \\
&= x*(a*b^{-1})
\end{aligned}
$$

$\therefore (a*b^{-1}) \in Cent(G)$.

$\therefore (Cent(G),*)$ is a subgroup of $(G,*)$. ⊠.

Theorem (6) :- Let $(G,*)$ be a group. Then

$$Cent(G) = G \Leftrightarrow G \text{ is a comm. group.}$$

Proof :-

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

$\therefore a * x = x * a \quad \forall x \in G$

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

$\therefore G$ is Comm. gp.

$(\Leftarrow)$ 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 $Cent(G) \subseteq G$.

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

Let $x \in G$, G is comm. group $\Rightarrow x * a = a * x \quad \forall x \in G$.

$\therefore x \in Cent(G) \Rightarrow G \subseteq Cent(G)$.

$\therefore Cent(G) = G$.

تكملة

①

Subgroups and Cyclic groups

Define:- ① + ② + ③ هنالك ثلاث تعاريف للزمرة الجزئية

$$\text{Subgp} \Rightarrow H \subseteq G$$

		حسب الجبرية
$(H,*)$	$(H,*)$	$(H,*)$
$H \neq \Phi \subseteq G$	① $a*b \in H$	$a,b \in H$
$(H,*)$ is it self a group	② $e \in H$	$\Rightarrow a*b^{-1} \in H$
يعني تحقق الشروط الأربعة	③ $a^{-1} \in H$	

① $a,b \in H \Rightarrow a*b \in H$

② $a,b,c \in H \Rightarrow (a*b)*c = a*(b*c)$

③ $e \in H \Rightarrow a*e = e*a = a$

④ $a^{-1} \in H \Rightarrow a*a^{-1} = a^{-1}*a = e$

Example:- if $G = (\mathbb{Z},+)$ be a group, and $H = \{7a : a \in \mathbb{Z}\}$
Show that $(H,+)$ is a subgp of $(\mathbb{Z},+)$.

بين انه $(H,+)$ هي زمرة جزئية للزمرة $(\mathbb{Z},+)$

Sol: الحل:- لديك عدة مقترحات للإجابة ١- اما ان تبرهن انه $(H,+)$ زمرة بحد ذاتها اي تحقق الشروط الأربعة عليها

٢- او تحقق الشروط الثلاثة (الانغلاق + e + a^{-1})

٣- او حسب الجبرية $a,b \in H \Rightarrow a*b^{-1} \in H$

* نأخذ واحدة هي حسب الجبرية

$\because x, y \in H \;, x = 7a \;, y = 7b$

$\Rightarrow x + y \in H \Rightarrow 7a + 7b \Rightarrow 7\underbrace{(a+b)}_{\in \mathbb{Z}} \Rightarrow 7c \in H \,,\; c = (a+b)$

$x + y^{-1} = 7a + (7b)^{-1} \Rightarrow 7a + 7(-b) = 7\underbrace{(a-b)}_{\in \mathbb{Z}} = 7k \in H \,,\; k = (a-b)$

$\therefore x + y^{-1} \in H \Rightarrow (H,+)$ is a subgp of $(\mathbb{Z},+)$

وهكذا تكون الزمر الجزئية بالنسبة لـ $(\mathbb{Z},+)$ وهي $\underline{\underline{(n\mathbb{Z},+)}}$

حيث $(n\mathbb{Z},+)$ هي $(1\mathbb{Z},+),(2\mathbb{Z},+),(3\mathbb{Z},+)$ ....

وبنفس الخطوات جميعها.

: The operation of subgps,,

العمليات على الزمر الجزئية.

① Intersection: التقاطع

If $(H_i,*)$ is the collection of subgps of $(G,*)$, then $(\cap H_i,*)$ is also subgp. of $(G,*)$.

نص القاعدة تقاطع أي عدد من الزمر الجزئية المنتهية هو زمرة جزئية وحسب البرهنة الموجودة.

__Example:-__ Let $(\mathbb{Z}_8,+_8)$ is a gp.

$\mathbb{Z}_8,+_8$

1.8 2.4

order

$\langle \bar{1} \rangle = \mathbb{Z}_8 \Longrightarrow o(\bar{1}) = 8$

$\langle \bar{8} \rangle = \langle \bar{0} \rangle = \{\bar{0}\}$ $o(\bar{0}) = 1$

$\langle \bar{2} \rangle = \{\bar{0},\bar{2},\bar{4},\bar{6}\}$ $o(\bar{2}) = 4$

$\langle \bar{4} \rangle = \{\bar{0},\bar{4}\}$ $o(\bar{4}) = 2$

طريقة إيجاد الزمر الجزئية للزمرة $\mathbb{Z}_n$ $\Longleftarrow$

لو لاحظنا الطريقة التقليدية هي

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \{\bar{0},\bar{1},\bar{2},\bar{3},\cdots\bar{7}\} = \mathbb{Z}_8$

$\langle \bar{2} \rangle = \{\bar{0},\bar{2},\bar{4},\bar{6}\}$

$\langle \bar{3} \rangle = \{\bar{0},\bar{3},\bar{6},\bar{1},\bar{4},\bar{7},\bar{2}\} = \mathbb{Z}_8$

$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}\}$

$\langle \bar{5} \rangle = \{\bar{0}, \bar{5}, \bar{2}, \bar{7}, \bar{4}, \bar{1}, \bar{6}\} = Z_8$

$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \bar{4}, \bar{2}\} = \langle \bar{2} \rangle$

$\langle \bar{7} \rangle = \{\bar{0}, \bar{7}, \bar{6}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}\} = Z_8$

نلاحظ أنه اذا كانت العلاقة ما بين n والعدد علاقة أولية
أي القاسم المشترك الأعظم هو 1 فأن الزمرة الجزئية هي
الزمرة الأم مثلاً

$g.c.d(8,1) = 1 = Z_8$

$g.c.d(8,3) = 1 = Z_8$

$g.c.d(8,5) = 1 = Z_8$

$g.c.d(8,7) = 1 = Z_8$

لكن

$g.c.d(8,2) = 2 = \langle \bar{2} \rangle$

$g.c.d(8,4) = 4 = \langle \bar{4} \rangle$

$g.c.d(8,6) = 2 = \langle \bar{2} \rangle$

وهذه القاعدة لجميع الزمر الجزئية من النوع Z_n

* الآن : تقاطع الزمر الجزئية

$\langle \bar{2} \rangle \cap \langle \bar{4} \rangle = \{\bar{0}, \bar{4}\}$

$\langle \bar{2} \rangle \cap \langle \bar{3} \rangle = \langle \bar{2} \rangle$

$\langle \bar{3} \rangle \cap \langle \bar{5} \rangle = Z_8$

$\vdots$

وهكذا نلاحظ جميع التقاطعات
تمثل زمرة جزئية موجودة في
الزمر الجزئية.

2- Union ($\cup$)   ($\cup$) الاتحاد

فيما يتعلق بالاتحاد للزمر الجزئية فانه ليس بالضرورة ان تكون اتحاد الزمر الجزئية هو زمرة جزئية كما في المثال:

Example :- Let $(Z_{12}, +_{12})$ be a gp and $H_1 = (\langle \bar{2} \rangle, +_{12})$

$H_2 = (\langle \bar{3} \rangle, +_{12})$

$$H_1 \cup H_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} \cup \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$$
$$= \{\bar{0}, \bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}\}$$

نلاحظ أن $H_1 \cup H_2$ لا يمثل زمرة جزئية وذلك لأنه

$\bar{2}, \bar{3} \in H_1 \cup H_2 \Rightarrow \bar{2} +_{12} \bar{3} = \bar{5} \notin H_1 \cup H_2$

$\bar{3}, \bar{4} \in H_1 \cup H_2 \Rightarrow \bar{3} +_{12} \bar{4} = \bar{7} \notin H_1 \cup H_2$

وهكذا للكثير من القيم.

$(H_1 \cup H_2, +_{12})$ is not subgp. ⊠

(*) هناك حالة يصبح فيها الاتحاد زمرة جزئية وهو عندما تكون احد الزمر الجزئية جزئية من الأخرى أي

$$H_1 \subseteq H_2 \text{ or } H_2 \subseteq H_1$$

مثال:-

$(Z_{12}, +_{12})$ is a gp , $Z_{12} = \{\bar{0}, \bar{1}, \bar{2}, \dots \bar{11}\}$

1.12   2.6   3.4

$\langle \bar{1} \rangle = Z_{12}$

$\langle \bar{12} \rangle = \langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$

$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$

هذه هي الزمر الجزئية الفعلية لـ Z_{12}

وباقي الزمر الجزئية كلها اما مساوية لـ Z_{12} او مساوية لبعض الزمر الجزئية الفعلية.

لأن ـــ تكون

Let $H_1 = \langle \bar{3} \rangle$, $H_2 = \langle \bar{6} \rangle \Rightarrow \boxed{H_2 \subseteq H_1}$

$H_1 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $H_2 = \{\bar{0}, \bar{6}\}$

$H_1 \cup H_2 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} = \langle \bar{3} \rangle$ is a subgp of $(Z_{12}, +_{12})$

and Let $H_1 = \langle \bar{4} \rangle$, $H_2 = \langle \bar{2} \rangle \Rightarrow \boxed{H_1 \subseteq H_2}$

$H_1 = \{\bar{0}, \bar{4}, 8\}$, $H_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$

$H_1 \cup H_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} = \langle \bar{2} \rangle$ is a subgp of $(Z_{12}, +_{12})$

العملية الأخرى ـــ هي:

3- Product: $H * K$

Let $(G, *)$ be a gp and $(H, *)$, $(K, *)$ are two subgps of G. Then the product of H and K is the set

$$H * K = \{h * k : h \in H, k \in K\}$$

Example:-

In $(Z_8, +_8)$, $H_1 = \langle \bar{2} \rangle$, $H_2 = \langle \bar{4} \rangle$

$Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$, $\langle \bar{4} \rangle = \{\bar{0}, \bar{4}\}$

$H_1 +_8 H_2 = \{\bar{0} +_8 \bar{0}, \bar{0} +_8 \bar{4}, \bar{2} +_8 \bar{0}, \bar{2} +_8 \bar{4}, \bar{4} + \bar{0}, \bar{4} + \bar{4}, \bar{6} + \bar{0}, \bar{6} + \bar{4}\}$

$= \{\bar{0}, \bar{4}, \bar{2}, \bar{6}, \bar{4}, \bar{0}, \bar{6}, \bar{2}\} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \langle \bar{2} \rangle$. ☒

Notes:- ملاحظات :-

1. $H*H$ is write H^2
2. If $H=\{a\}$, then $H*K=a*K$. If $K=\{b\}$, then $H*K=H*b$
3. $\boxed{H\cup K\subseteq H*K}$

Theorem:- Let $(G,*)$ be a gp and $(H,*),(K,*)$ are two subgps of G, then:-

1- $H*K\neq\phi \wedge H*K\subseteq G$

2- $H\subseteq H*K$ and $K\subseteq H*K$

3- $(H*K,*)$ is a subgp of G iff $H*K=K*H$

4- If $(G,*)$ is a Comm. gp then $(H*K,*)$ is a subgp of G.

البراهين موجودة في الملزمة. (مطلوبة طبعاً).

ملاحظات :-

Notes:- Let $(H,*)$ and $(K,*)$ be two subgps of $(G,*)$ then:-

1- $H*K\neq K*H$

2- $(H*K,*)$ need not be subgp of $(G,*)$. H.W ?

Example:-

1. Let $G=(S_3,\circ)$, $H_1=(I,(12))$, $H_2=(I,(13))$

$H_1\circ H_2=\{I\circ I,\ I\circ(13),\ (12)\circ I,\ (12)\circ(13)\}$

$H_1\circ H_2=\left\{I,\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$

$=\left\{I,(13),(12),\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}=\{I,(13),(12),(132)\}$

* **Now:** $H_2 \cdot H_1 = \{I \cdot I, I \cdot (12), (13) \cdot I, (13) \cdot (12)\}$

$$= \{I, (12), (13), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$$

$$= \{I, (12), (13), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\}$$

$$= \{I, (12), (13), (123)\} \neq H_1 \cdot H_2 . \boxtimes$$

Define:- The Center of a gp $(G, *)$ denoted by Cent(G) or $C(G)$ is the set

$C(G) = \{c \in G : c * x = x * c, \forall x \in G\}$ العناصر التي تتبادل مع كل عناصر الزمرة تسمى المركز

Note:-

$C(G) \neq \phi$, since $\exists e \in G$ s.t.

$e * x = x * e \quad \forall x \in G \Rightarrow e \in C(G)$.

Examples:-

1- The group $G = (S_3, o) = \{I, (12), (13), (123), (132), (23)\}$

$C(S_3) = I$ because: $C(S_3) = \{f \in S_3 : f o g = g o f \ \forall g \in S_3\} = I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

2- The group $G = (Z_4, +_4) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$C(Z_4) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = Z_4$ because:-

1. $\bar{0} + \bar{0} = 0$, $\bar{0} + \bar{1} = \bar{1} + 0$, $\bar{0} + \bar{2} = \bar{2} + \bar{0}$, $\bar{0} + \bar{3} = \bar{3} + \bar{0}$
2. $\bar{1} + \bar{0} = \bar{0} + 1$, $\bar{1} + \bar{1} = \bar{1} + \bar{1}$, $\bar{1} + \bar{2} = \bar{2} + 1$, $\bar{1} + \bar{3} = \bar{3} + 1$
3. $\bar{2} + \bar{0} = \bar{0} + 2$, $\bar{2} + 1 = \bar{1} + 2$, $\bar{2} + \bar{2} = \bar{2} + 2$, $\bar{2} + \bar{3} = \bar{3} + 2$
4. $\bar{3} + \bar{0} = \bar{0} + \bar{3}$, $\bar{3} + \bar{1} = \bar{1} + \bar{3}$, $\bar{3} + \bar{2} = \bar{2} + \bar{3}$, $\bar{3} + \bar{3} = \bar{3} + \bar{3}$

(3)- The group $G=(\{1,-1,i,-i\},\cdot)$ The center G is:-

- $1\cdot 1=1\cdot 1$, $1\cdot -1=-1\cdot 1$, $1\cdot i=i\cdot 1$, $-i\cdot 1=1\cdot(-i)$

- $-1\cdot 1=1\cdot -1$, $-1\cdot -1=-1\cdot -1$, $-1\cdot i=i\cdot -1$, $-1\cdot -i=-i\cdot -1$

3- $i\cdot 1=1\cdot i$, $i\cdot -1=-1\cdot i$, $i\cdot i=i\cdot i$, $i\cdot -i=-i\cdot i$

. $-i\cdot 1=1\cdot -i$, $-i\cdot -1=-1\cdot -i$, $-i\cdot i=i\cdot -i$, $-i\cdot -i=-i\cdot -i$.

$\therefore\ C(G)=\{1,-1,i,-i\}$

(4)- The group $G=(\mathbb{R}\setminus\{0\},\cdot)$

$C(\mathbb{R})=\mathbb{R}$ since $\mathbb{R}$ with multiplication is comm.

(5) **Theorem:** Let $(G,*)$ be a gp. Then the Cent G ((Cent $G,*$) is a subgp of $(G,*)$.

(*) مركز الزمرة هو زمرة جزئية من الزمرة.

البرهان مطلوب وموجود في الملزمة.

(*) **Theorem:** Let $(G,*)$ be a gp. then

$\mathrm{Cent}(G)=G \Leftrightarrow G$ is a comm. gp.

(*) مركز الزمرة = الزمرة نفسها $\Longleftrightarrow$ اذا كانت الزمرة ابدالية.

البرهان مطلوب وموجود في الملزمة.

The Cyclic group

الزمرة الدوارة

*** Definition:- (cyclic group).**

Let $(G,*)$ be a group, then G is called cyclic group if $\exists\, a \in G$ such that $G = (a) = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ and a is called generator of a group G.

i.e. G is generated by $a \in G$ if $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Notes:-

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

2- $|(a)| = |a|$.

3- If G is a cyclic group generated by $a \in G$ [i.e. $G = \langle a \rangle$] and $b \in G$, then $\exists\, k \in \mathbb{Z}$, s.t. $b = a^k$.

4- If $a \in \mathbb{Z}$, then $\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{a \cdot n : n \in \mathbb{Z}\}$.

Examples:-

1- $(\mathbb{Z},+)$, since $\exists\, 1 \in \mathbb{Z}$, s.t. $\langle 1 \rangle = \{1^n : n \in \mathbb{Z}\} = \{1 \cdot n : n \in \mathbb{Z}\}$
$= \{0, \mp 1, \mp 2, \mp 3, \ldots\} = \mathbb{Z}$

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

2- $(\mathbb{Z}_e,+)$, since $\exists\, 2 \in \mathbb{Z}_e$, s.t. $\langle 2 \rangle = \{2^n : n \in \mathbb{Z}\}$
$= \{2n : n \in \mathbb{Z}\} = \{0, \mp 2, \mp 4, \ldots\} = \mathbb{Z}_e$

$\therefore \mathbb{Z}_e$ is cyclic group generated by $2, -2$. $\boxtimes$

3- $(Q,+)$ is not cyclic, since $\nexists\, a \in Q$, s.t. $\langle a \rangle = \{a^n, n \in Z\} = Q$.

4- In general. $(S_n, \circ)$ is not cyclic group, $n \geq 3$.

* **Theorem:-** If $(G,*)$ is a finite cyclic group of order n generated by a. Then $G = \langle a \rangle = \{a^0, a^1, a^2, \dots a^n = e\}$. $(a^0 = e = a^n)$

⊛ مهمة جداً

Notes:-

1- The generators of a group $(Z_p, +_p)$, where p is a prime number all elements of Z_p except 0.

مركب

2- The generators of a group $(Z_n, +_n)$, where n is composite number is $a \in Z_n$ if $\boxed{g.c.d(a,n) = 1.}$

* **Examples:-** Find the generators of the following gp:-

1- $(Z_5, +_5)$.

2- $(Z_6, +_6)$.

3- $(Z_9, +_9)$

4- $(G = \{1,-1,i,-i\}, \cdot)$, wher $i^2 = -1$.

Sol. (1) <To Find the generators of $(Z_5, +_5)$>?

$\because Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, and since 5 is a prime number, then the generators of a group Z_5 are $\bar{1}, \bar{2}, \bar{3}, \bar{4}$. Since.

$$\langle \bar{1} \rangle = \{\bar{1}^n : n \in Z\} = \{\bar{1} \cdot n : n \in Z\} = \{\bar{1}^0, \bar{1}^1, \bar{1}^2, \bar{1}^3, \dots\}$$
$$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = Z_5.$$

$\langle \bar{2} \rangle = \{ \bar{2}^n : n \in Z \} = \{ \bar{2} \cdot n : n \in Z \} = \{ \bar{2}^1, \bar{2}^2, \bar{2}^3, \bar{2}^4, \ldots \} = \{ 2, 4, 1, 3, 0 \} = Z_5$

$\langle \bar{3} \rangle = \{ \bar{3}^n : n \in Z \} = \{ \bar{3} \cdot n : n \in Z \} = \{ \bar{3}^1, \bar{3}^2, \bar{3}^3, \ldots \} = \{ \bar{3}, \bar{1}, \bar{4}, \bar{2}, \bar{0} \} = Z_5$

$\langle \bar{4} \rangle = \{ \bar{4}^n : n \in Z \} = \{ \bar{4} \cdot n : n \in Z \} = \{ \bar{4}^1, \bar{4}^2, \bar{4}^3, \ldots \} = \{ \bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{0} \} = Z_5$.

Solu ②: < To find the generators of $(Z_6, +_6)$ >? مركز

$\because Z_6 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$ and since 6 is a composite order.

$\Rightarrow Z_6$ generated by $\bar{1}, \bar{5}$, since g.c.d$(6,1) = 1$ and g.c.d$(6,5) =$

The following to show that:-

$\langle \bar{1} \rangle = \{ \bar{1}^n : n \in Z \} = \{ \bar{1} \cdot n : n \in Z \} = \{ \bar{1}^1, \bar{1}^2, \bar{1}^3, \ldots \} = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{0} \} = Z_6$.

$\langle \bar{5} \rangle = \{ \bar{5}^n : n \in Z \} = \{ \bar{5} \cdot n : n \in Z \} = \{ \bar{5}^1, \bar{5}^2, \bar{5}^3, \ldots \} = \{ \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}, 0 \} = Z_6$.

$\therefore Z_6$ generated by $\bar{1}, \bar{5}$.

but

$\langle \bar{2} \rangle = \{ \bar{2}^n : n \in Z \} = \{ \bar{2} \cdot n : n \in Z \} = \{ \bar{2}^1, \bar{2}^2, \bar{2}^3, \ldots \} = \{ \bar{2}, \bar{4}, \bar{0} \} \neq Z_6$.

$\langle \bar{3} \rangle = \{ \bar{3}^n : n \in Z \} = \{ \bar{3} \cdot n : n \in Z \} = \{ \bar{3}^1, \bar{3}^2, \bar{3}^3, \ldots \} = \{ \bar{3}, \bar{0} \} \neq Z_6$

$\langle \bar{4} \rangle = \{ \bar{0}, \bar{2}, \bar{4} \} = \langle \bar{2} \rangle \neq Z_6$.

$\therefore Z_6$ is not generated by $\bar{2}, \bar{3}, \bar{4}$. ⊠

Solu ③: < To find the generators of $(Z_9, +_9)$ >?

بنفس الطريقة السابقة.

$\because Z_9 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8} \}$

g.c.d$(9, \bar{1}) = 1$, g.c.d$(9,2) = 1$, g.c.d$(9,3) = 3$

g.c.d$(9,4) = 1$, g.c.d$(9,5) = 1$, g.c.d$(9,6) = 3$

g.c.d$(9,7) = 1$, g.c.d$(9,8) = 1$.

$\therefore Z_9$ generated by $\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}$. ⊠

Soln (4) $G = (\{1, -1, i, -i\}, \cdot)$

$\langle 1 \rangle = \{1^n : n \in \mathbb{Z}\} = \{1^1, 1^2, 1^3, \ldots\} = \{1, 1, \ldots\} \neq G$. (1) not generator

$\langle -1 \rangle = \{(-1)^n : n \in \mathbb{Z}\} = \{(-1)^1, (-1)^2, (-1)^3, \ldots\} = \{1, -1\} \neq G$. (-1) not generator.

$\langle i \rangle = \{(i)^n : n \in \mathbb{Z}\} = \{(i)^1, (i)^2, (i)^3, (i)^4, \ldots\} = \{i, -1, -i, 1\} = G$. (i) generator

$\langle -i \rangle = \{(-i)^n : n \in \mathbb{Z}\} = \{(-i)^1, (-i)^2, (-i)^3, (-i)^4, \ldots\} = \{-i, -1, i, 1\} = G$. (-i) generator

$\therefore$ G is cyclic group generated by $i, -i$. ⊠

(*) **Theorem:-** Every cyclic group is a commutative group

But the converse is not. (*) العكس غير صحيح.

Proof:-

Let $(G, *)$ be a cyclic group generated by a (i.e. $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$)

< T.P. G is a comm. group (i.e. we must to prove) $x * y = y * x$ $\forall x, y \in G$ >.

Let $x, y \in G$ and since G is cyclic gp generated by a.

$\Rightarrow x = a^n$ and $y = a^m$, for some $n, m \in \mathbb{Z}$

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

Therefore, G is a comm. group. ⊠

(*) ملاحظة مهمة جداً :-

عكس النظرية اعلاه ليس من الضروري صحيح أي أن علينا ان تكون الزمرة ابدالية ولكنها ليست دائرية . المثال الآتي يوضح ذلك .

⊛ **Example:-**

$(\mathbb{Q},+)$ is a comm. group but not cyclic, since $\nexists\, a \in \mathbb{Q}$, s.t.

$$\mathbb{Q} = \langle a \rangle . \quad \boxtimes$$

⊛ **Theorem:-**

Every subgroup of a cyclic group is cyclic.

⊛ **Examples:-** Find all cyclic subgroups of the following groups:-

1- $(Z_{12}, +_{12})$

2- $(Z_{26}, +_{26})$

Sol ①:- The cyclic subgroups of the group $(Z_{12}, +_{12})$ are:-

Z_{12},

1·12   2·6   3·4

$Z_{12} = \{\bar{0}, \cdots \overline{11}\}$

$H_1 = \langle \bar{1} \rangle = (Z_{12}, +_{12}) \implies |\langle \bar{1} \rangle| = 12.$ } trivial subgp.

$H_2 = \langle \bar{0} \rangle = (\{\bar{0}\}, +_{12}) \implies |\langle \bar{0} \rangle| = 1.$

$H_3 = \langle \bar{2} \rangle = (\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}, +_{12}) \implies |\langle \bar{2} \rangle| = 6.$ } Proper subgroup

$H_4 = \langle \bar{6} \rangle = (\{\bar{0}, \bar{6}\}, +_{12}) \implies |\langle \bar{6} \rangle| = 2.$

$H_5 = \langle \bar{3} \rangle = (\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}, +_{12}) \implies |\langle \bar{3} \rangle| = 4.$

$H_6 = \langle \bar{4} \rangle = (\{\bar{0}, \bar{4}, \bar{8}\}, +_{12}) \implies |\langle \bar{4} \rangle| = 3.$

but

$\langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \overline{11} \rangle = \langle \bar{1} \rangle$

$\langle \bar{2} \rangle = \langle \bar{8} \rangle = \langle \overline{10} \rangle,$

$\langle \bar{3} \rangle = \langle \bar{9} \rangle .$

Sol. ②:- The cyclic subgroups of the group $(\mathbb{Z}_{26}, +_{26})$ are:-

$$\mathbb{Z}_{26}$$

1.26   2.13

$$\left.\begin{array}{ll} \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \cdots \overline{25}\} = \mathbb{Z}_{26} & \Rightarrow |\langle \bar{1} \rangle| = 26 \\ \langle \bar{0} \rangle = \{\bar{0}\} & \Rightarrow |\langle \bar{0} \rangle| = 1 \end{array}\right\} \text{trivial subgp}$$

$$\left.\begin{array}{ll} \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \cdots \overline{24}\} & \Rightarrow |\langle \bar{2} \rangle| = 13 \\ \langle \overline{13} \rangle = \{\bar{0}, \overline{13}\} & \Rightarrow |\langle \overline{13} \rangle| = 2 \end{array}\right\} \text{proper subgp}$$

but :-

$$\langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 15 \rangle = \langle 17 \rangle = \langle 19 \rangle = \langle 21 \rangle = \langle 23 \rangle = \langle 25 \rangle$$

$$= \langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 12 \rangle = \langle 14 \rangle = \langle 16 \rangle = \langle 18 \rangle = \langle 20 \rangle = \langle 22 \rangle = \langle 24 \rangle$$

$$\langle \bar{2} \rangle = \langle \bar{4} \rangle = \langle 6 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 12 \rangle = \langle 14 \rangle = \langle 16 \rangle = \langle 18 \rangle = \langle 20 \rangle = \langle 22 \rangle = \langle 24 \rangle$$

* ملاحظة مهمة جداً :-

عكس النظرية السابقة ليس من الضروري صحيح أي أنه توجد زمرة جزئية دائرية من زمرة ليست دائرية والمثال الآتي يوضح ذلك.

④ Example:- Given example cyclic subgp in a group is not cyclic

Sol.

A subgroup $(H = \{e, (12)\}, \circ)$ of a group $(S_3, \circ)$ is a cyclic subgroup generated by (12). Since.

$$\begin{aligned} \langle (12) \rangle &= \{(12)^n : n \in \mathbb{Z}\} \\ &= \{(12)^1, (12)^2, (12)^3, \cdots\} \\ &= \{(12), e, (12), e, \cdots\} \\ &= \{(12), e\} = H \end{aligned}$$

But $(S_3, \circ)$ is not cyclic group ⊠.

"Cyclic Groups: (الزمر الدوارة (الدائرية)"

Definition:- Let $(G,*)$ be a gp and $a \in G$, The cyclic subgroup generated by an element a denoted by

$\langle a \rangle = \{a^n \mid n \in Z\}$. ⊛ هذه زمرة دائرية غير منتهية

If there is $b \in G$ s.t. $\langle b \rangle = G$ then $(G,*)$ is called a cyclic group and b is called a generator for G.

⊛ An Infinit cyclic gp generated by a is $\langle a \rangle = \{a^n \mid n \in Z\}$, but a finit cyclic gp generated by a is $\langle a \rangle = \{a^0, a^1, \dots, a^n\}$, $a^n = e$. ⊛

Notes:-

① $O(a) = n$

② $a^n = e$

③ $a^{n-1} = a^{-1}$

Notes:-

* Every cyclic gp is abelian (comm.) group.

كل زمرة دائرية هي زمرة ابدالية

Examples:-

1- $(Z_n, +_n)$ is cyclic gp $\Rightarrow (Z_n, +_n)$ is abelian gp.

2- $(Z, +)$ is cyclic gp $\Rightarrow (Z, +)$ is abelian gp

Q_x/ Find the generated of acyclic gp $(Z_8, +_8)$?

جد جميع المولدات للزمرة الدائرية $(Z_8, +_8)$

$Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

$\langle\bar{0}\rangle = \{\bar{0}\}$

$\underline{\langle\bar{1}\rangle} = \{\bar{1}^0, \bar{1}^1, \bar{1}^2, \bar{1}^3, \bar{1}^4, \bar{1}^5, \bar{1}^6, \bar{1}^7\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\} = Z_8$

$\langle\bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

$\underline{\langle\bar{3}\rangle} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\} = Z_8$

$\langle\bar{4}\rangle = \{\bar{0}, \bar{4}\}$

$\underline{\langle\bar{5}\rangle} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\} = Z_8$

$\langle\bar{6}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \langle\bar{2}\rangle$

$\underline{\langle\bar{7}\rangle} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\} = Z_8$

$\therefore$ The generated of Z_8 are: $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

وبطريقة اخرى اذا كانت العلاقة اولية مابين ال n والعدد a أي $g.c.d(n, a) = 1$ فهي تولد الزمرة نلاحظ

$g.c.d(8, 1) = \underline{1}$, $g.c.d(8, 3) = \underline{1}$, $g.c.d(8, 5) = \underline{1}$, $g.c.d(8, 7) = \underline{1}$

Example:-

Find the generated of Cyclic gp $(Z, +)$.?

In $(Z, +)$, Find the generated of Cyclic gp $(Z, +)$?

جد مولدات الزمرة الدائرية $(Z, +)$.

Sol

$\langle 1\rangle = \{1^k \mid k \in Z\} = \{0, \mp 1, \mp 2, \mp 3, \dots\} = Z$

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

$\therefore \{1, -1\}$ are generated $(Z, +)$. $\boxtimes$

Example :- Is $(S_3, \circ)$ cyclic gp ?

Sol:- $S_3 = \left\{ \begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 3&2&1 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix} \right\}$

$= \{ I, (132), (123), (23), (13), (12) \}$

① $\langle I \rangle = \{ I^k \mid k \in \mathbb{Z} \} = I \neq S_3$

② $\langle (132) \rangle = \{ (132)^k \mid k \in \mathbb{Z} \} = \{ (132)^0, (132)^1, \cdots \}$

$(132)^0 = I \quad , \quad (132)^1 = (132)$

$(132)^2 = (132) \circ (132) = \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix} \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix} = \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} = (123)$

$(132)^3 = (132)^2 \circ (132) = \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix} = \begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix} = I$

$\therefore \langle (132) \rangle = \{ I, (132), (123) \} \neq S_3$

③ $\langle (123) \rangle = \{ (123)^0, (123)^1, (123)^2, \cdots \}$

$(123)^2 = \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} \circ \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} = \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix} = (132)$

$(123)^3 = (123)^2 \circ (123) = \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix} \circ \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} = \begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix} = I$

$\therefore \langle (123) \rangle = \{ I, (123), (132) \} = \langle (132) \rangle \neq S_3$

④ $\langle (23) \rangle = \{ (23)^0, (23)^1, (23)^2, \cdots \}$

$(23)^2 = \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix} \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix} = \begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix} = I$

$\therefore \langle (23) \rangle = \{ I, (23) \}$

⑤ $\langle (13) \rangle = \{ (13)^0, (13)^1, (13)^2, \cdots \}$

$(13)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\therefore \langle (13) \rangle = \{ I, (13) \} \neq S_3$

⑥ $\langle (12) \rangle = \{ (12)^0, (12)^1, (12)^2, \dots \}$

$(12)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\langle (12) \rangle = \{ I, (12) \} \neq S_3$

$\therefore (S_3, \circ)$ is not cyclic gp. $\boxtimes$

Example:- Is $G = \{1, -1, i, -i\}$ a cyclic gp ?

Sol

$\langle 1 \rangle = \{ 1^0, 1^1, 1^2, 1^3, \dots \} = 1 \neq G$

$\langle -1 \rangle = \{ -1^0, -1^1, -1^2, \dots \} = \{1, -1\} \neq G$

$\langle i \rangle = \{ i^0, i^1, i^2, i^3, \dots \} = \{ 1, i, -1, -i \} = G$

$\langle -i \rangle = \{ -i^0, -i^1, -i^2, -i^3, \dots \} = \{ -1, -i, 1, i \} = G$

$\therefore$ The generated of $(G, \cdot)$ are $\{ i, -i \}$

$\therefore (G, \cdot)$ is cyclic gp. $\boxtimes$

Definition:- (Division Algorithm for $\mathbb{Z}$) خوارزمية القسمة

If a and b are integers with $\underline{b>0}$, then there is a unique (زوج وحيد) pair of integers $\underline{q}$ and $\underline{r}$ s.t.

$$a = bq + r \quad , \text{where } 0 \leq r < b$$

The number $\underline{q}$ is called the quotient (ناتج القسمة) and $\underline{r}$ is called the remainder (الباقي) when $\underline{a}$ is divided (يقسم) by $\underline{b}$

Examples:-

① Find the quotient and remainder r when 38 divided by 7 according to the (division algorithm)

Sol: $a = bq + r$

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

$\Rightarrow q = 5 \; , \; r = \underline{3}$

② $a = 103 \; ; \; b = 9$

$a = bq + r$

$103 = 9(11) + 4 \Rightarrow q = 11 \; , \; r = 4 \qquad 0 \leq 4 < 9$

③ $a = 43 \; , \; b = 4$

$a = bq + r$

$43 = 4(10) + 3 \qquad , \; q = 10 \; , \; r = 3 \; , \; 0 \leq 3 < 10$

(*) مهمة جداً

Theorem:- A subgroup of a cyclic group is cyclic.

الزمرة الجزئية من زمرة دائرية تكون دائرية

Corollary:- If $(G,*)$ is a finite cyclic gp of order n generated by a, then every subgp of G is cyclic generated by $a^m \ni m|n$.

اذا كانت $(G,*)$ زمرة دائرية منتهية وعددها (n) وتتولد بواسطة a فان اي زمرة جزئية من G هي زمرة جزئية دائرية متولدة بواسطة a^m بحيث m يقسم n.

Example:- Find all subgps of $(Z_{21}, +_{12})$?

Z_{21}

$1 \cdot 21 \qquad 3 \cdot 7$

$1|21,\ 21|21,\ 3|21,\ 7|21$

$\langle \bar{1} \rangle = Z_{21}$

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}, \bar{18}\}$

$\langle \bar{7} \rangle = \{\bar{0}, \bar{7}, \bar{14}\}$

(*) الامثلة السابقة جميعها تبين الزمر الجزئية الدائرية.

Corollary:- If $(G,*)$ is finite cyclic gp of prime order, then G has no proper subgps.

الزمر الدائرية المنتهية ذات الرتبة الأولية لا تمتلك زمر جزئية فعلية.

Example:- $(Z_7,+_7)$, $(Z_5,+_5)$ --- $(Z_p,+_p)$

هذه الزمر جميعها لا تمتلك زمر جزئية فعلية فقط التافهة وهي الزمرة نفسها والعنصر المحايد.

Definition:- G.C.d (x,y) القاسم المشترك الأكبر

A positive integer c is said to be a greatest common divisor of two non-zero numbers x, y. iff :-

يقسم

① $c|x \wedge c|y$

② if $a|x \wedge a|y \Rightarrow a|c$ $\Rightarrow$ g.c.d $(x,y) = c$. $\boxtimes$

Example:- Find g.c.d $(12,18)$

Sol: g.c.d $(12,18) = 6$ since

① $6|12 \wedge 6|18$

② $3|12 \wedge 3|18$

or $1|12 \wedge 1|18$

or $2|12 \wedge 2|18$.

$\Rightarrow$ g.c.d $(12,18) = \underline{6}$. $\boxtimes$

Remark:- If $(G,*)$ is finite cyclic gp of order $\underline{\underline{n}}$ generated by a, then the generators of G is $\underline{\underline{a^k}}$ such that $g.c.d(k,n)=1$.

Example:- $(Z_6,+_6)$, $Z_6=\{\bar{0},\bar{1},\dots\bar{5}\}$

1.6 2.3

$\langle\bar{1}\rangle = Z_6 \longrightarrow g.c.d(1,6)=\underline{\underline{1}}$

$\langle\bar{0}\rangle=\{\bar{0}\}$

$g.c.d(2,6)=2$

$\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4}\}$, $\langle\bar{3}\rangle=\{\bar{0},\bar{3}\}$. $g.c.d(3,6)=\underline{\underline{3}}$

$\langle\bar{4}\rangle=\{\bar{0},\bar{4},\bar{2}\}$ $g.c.d(4,6)=2$

$\langle\bar{5}\rangle=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}=Z_6$ $g.c.d(5,6)=\underline{\underline{1}}$

Theorem:- If $(G,*)$ is an infinite cyclic gp generated by a, then:-

① a and a^{-1} are only generators of G.

② Every subgp of G except $\{e\}$ is an infinite subgp.

ابدا

⊛ شرح مبسط على الزمر الجزئية :-

① تعريف الزمرة الجزئية :- لتكن $(G,*)$ زمرة و $\phi \neq H \subseteq G$ ، تكون $(H,*)$ زمرة جزئية من G اذا كانت $(H,*)$ زمرة.

⊛ أي يجب ان تحقق بديهيات الزمرة (شروط الزمرة).

⊛ يجب ان تكون العملية $*$ هي نفس العملية للزمرة G .

⊛ نكتب $H \leq G$ أو $(H,*) \leq (G,*)$.

⊛ امثلة بسيطة :-

$(Z,+) \leq (R,+)$ أو $Z \leq R$

$(Q^*,\cdot) \leq (R^*,\cdot)$ أو $Q^* \leq R^*$

مثال :- لتكن $H=\{\bar{0},\bar{5},\bar{10},\bar{15}\} \subseteq Z_{20}$ ، أثبت أن $H \leq Z_{20}$ or $(H,+_{20}) \leq (Z_{20},+_{20})$

الحل :-

$Z_{20}=\{\bar{0},\bar{1},\dots,\bar{19}\}$, $|Z_{20}|=20$

نلاحظ أن :-

$\phi \neq H=\{\bar{0},\bar{5},\bar{10},\bar{15}\} \subseteq Z_{20}$

عمل جدول كيلي :-

$+_{20}$	$\bar{0}$	$\bar{5}$	$\bar{10}$	$\bar{15}$
$\bar{0}$	$\bar{0}$	$\bar{5}$	$\bar{10}$	$\bar{15}$
$\bar{5}$	$\bar{5}$	$\bar{10}$	$\bar{15}$	$\bar{0}$
$\bar{10}$	$\bar{10}$	$\bar{15}$	$\bar{0}$	$\bar{5}$
$\bar{15}$	$\bar{15}$	$\bar{0}$	$\bar{5}$	$\bar{10}$

من الجدول نلاحظ أن

⊛ الانغلاق متحقق

⊛ المحايد هو $\bar{0}$

⊛ النظير موجود لكل عنصر

$\bar{5}^{-1}=\bar{15}$, $\bar{10}^{-1}=\bar{10}$, $\bar{15}^{-1}=\bar{5}$

⊛ ايضاً شرط الابدالية متحقق.

$\therefore (H,+_{20}) \leq (Z_{20},+_{20})$ أي $H \leq Z_{20}$. ⊠

مثال :

Let $G = S_3$, $H = \{(1), (12)\}$. Is $H \leq G$?

Sol

$G = S_3$, $* = \circ \Rightarrow (S_3, \circ) = \{I, (12), (13), (23), (123), (132)\}$

$\phi \neq H = \{(1), (12)\} \subseteq S_3$

نحقق شروط الزمرة عن طريق جدول كيلي

$\circ$	(1)	(12)
(1)	(1)	(12)
(12)	(12)	(1)

من الجدول :

- الانغلاق متحقق
- العنصر المحايد (1)
- العنصر النظير $(1)^{-1} = (1)$, $(12)^{-1} = (12)$
- العملية تبديلية هنا في هذه الزمرة.

$\therefore H \leq S_3$ or $(H, \circ) \leq (S_3, \circ)$.

ملاحظة مهمة جداً جداً

1- اذا كانت الزمرة ابدالية فان الزمرة الجزئية ابدالية ايضاً.

2- اذا كانت الزمرة الجزئية ابدالية فانه ليس بالضرورة ان تكون الزمرة ابدالية وكما في المثال اعلاه.

$(S_3, \circ)$ ليست ابدالية لكن $(H, \circ)$ ابدالية.

مثال :

Let $G = S_3$, $H = \{(1), (123), (132)\}$. Is $H \leq S_3$ or not. Is H a comm. or not?

Sol

$\circ$	(1)	(123)	(132)
(1)	(1)	(123)	(132)
(123)	(123)	(132)	(1)
(132)	(132)	(1)	(123)

✓ Closure
✓ Identity
✓ Inverse
✓ comm.

$\therefore H \leq S_3$ or $(H, \circ) \leq (S_3, \circ)$.

⊛ الزمرتان التافهتان : Trivial subgroups.

اذا كانت $(G,*)$ زمرة فأن :

$$(G,*) \leq (G,*)$$

and $(\{e\},*) \leq (G,*)$

مبرهنة : لتكن G زمرة و $\phi \neq H \subseteq G$ فأن $H \leq G$ اذا وفقط اذا كان لكل $x,y \in H$ فأن $xy^{-1} \in H$.

البرهان :

[$\Leftarrow$] نفرضنا $H \leq G$ و $x,y \in H$

وكون H زمرة جزئية $\Leftarrow$ $y^{-1} \in H$

$\therefore$ $xy^{-1} \in H$ (شرط الانغلاق) . ⊠

[$\Rightarrow$] نفرضنا انه لكل $x,y \in H$ ، $xy^{-1} \in H$.

$\because$ $H \neq \phi$ اذن يوجد على الاقل $e \in H$

$e \in H \to x \cdot x^{-1} \in H$ [عنصر محايد] ✓

$e \cdot x^{-1} \in H \to x^{-1} \in H$ [عنصر نظير] ✓

لكل $x,y \in H \to y^{-1} \in H$

$\Rightarrow x \cdot (y^{-1})^{-1} \in H \to xy \in H$ [الانغلاق] ✓

أما شرط التجميعية فهي متحققة من (الزمرة G الام)

$\therefore$ $H \leq G$. ⊠

⊛ ملاحظة : ١- هذه المبرهنة مهمة جدا جدا لانها تختصر علينا اثبات الزمر الجزئية .

٢ استخدام الطريقة الكلاسيكية اذا كانت المجموعة منتهية العناصر

٣ استخدام المبرهنة اذا كانت المجموعة غير منتهية العناصر .

⊛ **Example:-** Prove that $H \leq Q^*$ such that $H = \{2^n : n \in Z\}$. (اثبت أن H زمرة جزئية من Q^* بحيث أن)

لاحظ أن المجموعة غير منتهية اذن نستخدم المبرهنة.

Sol:

Let $x, y \in H$ s.t. $x = 2^n$, $y = 2^m$, $n, m \in Z$

$$x \cdot y^{-1} = 2^n \cdot (2^m)^{-1} = 2^n \cdot 2^{-m} = \underline{\underline{2^{(n-m)}}} \in Z \in H$$

$\therefore H \leq Q^*$. ⊠

⊛ **Example:-** $H = \{f \in S_n : f(k) = k\}$, show that $H \leq S_n$.

⊛ اثبت أن مجموعة H والتي هي مجموعة التباديل $f(k)=k$ هي زمرة جزئية من S_n،

Sol:

معنى $f(k)=k$ أي مثلاً في S_3، $f(2)$ هي تثبيت 2 أي

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ وهكذا.

الحل الأول: Let $f, g \in H$ T.P. $f \circ g^{-1} \in H$

$f(k) = k$, $g(k) = k$

$$f \circ g^{-1}(k) = f(g^{-1}(k)) = f(k) = k$$

⊛ طريقة مبسطة للمعكوس

$g(k) = k \Rightarrow \cancel{g^{-1}g}(k) = g^{-1}(k)$

$\boxed{k = g^{-1}(k)}$

$\therefore f \circ g^{-1}(k) = k \in H \Rightarrow H \leq S_n$. ⊠

⊛: **Example:-** Prove that $(H,*) \leq (G,*)$ s.t. $G=\mathbb{R}^*\times\mathbb{R}$ where
$(a,b)*(c,d)=(ac,bc+d)$ and $H=\{(a,0): a>0\}$.

Sol

⊛ بالبداية يجب ان نستخرج العنصر المحايد لـ G والعنصر النظير لـ G .

$(a,b)*(e_1,e_2)=(a,b)$

$(ae_1, be_1+e_2)=(a,b)$

$\Rightarrow ae_1=a \Rightarrow e_1=1$

$b.1+e_2=b \Rightarrow e_2=0$

$\Rightarrow \boxed{(e_1,e_2)=(1,0)}$ Identity of G

$(a,b)*(c,d)=(1,0)$

$=(ac, bc+d)=(1,0)$

$\Rightarrow c=\frac{1}{a}, d=\frac{-b}{a} \Rightarrow \boxed{(a,b)^{-1}=(\frac{1}{a},\frac{-b}{a})}$ inverse of G.

Now:

Let $(a,0),(b,0)\in H$ s.t. $a,b>0$

$(a,0)*(b,0)^{-1}=(a,0)*(\frac{1}{b},0)$

$=(\frac{a}{b}, 0+0)=(\frac{a}{b},0)\in H$

$\Rightarrow H\leq G.$ ⊠

⊛: Example :- $(H*K, *)$ is not necessary subgroup

Let $H=(\{e,(12)\},\circ)$ and $K=(\{e,(23)\},\circ)$ be two sub groups of group $(S_3,\circ)$

$H\circ K=\{e\circ e,\ e\circ(23),\ (12)\circ e,\ (12)\circ(23)\}$

$=\{e,\ (23),(12),\ \underline{(123)}\}$ $\quad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$\therefore$ $H\circ K$ is not sub group of a group S_3. Since $(23),(12) \in H\circ K$ but $(23)\circ(12)=\underline{(132)} \notin H\circ K \Rightarrow H\circ K$ is not closed under $\circ$.

$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$.

شرح مبسط لكيفية ايجاد الزمرة الجزئية :

① كيفية ايجاد الزمر الجزئية بالنسبة للزمر الغير منتهية أي بشرط مساوية للعمليات الجمعية .

$(Z,+), (Q,+), (R,+), \ldots$

جميعها زمر غير منتهية

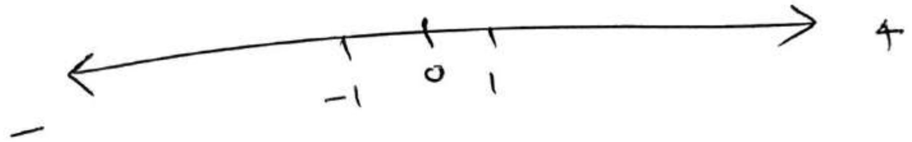
$\Rightarrow (Z,+) \subseteq (Q,+) \subseteq (R,+)$

ولاحظنا

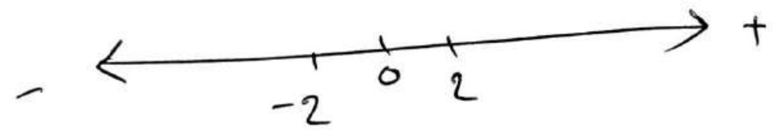
$(Z,+) \leq (Q,+) \leq (R,+)$

* السؤال هل أنه للـ $(Z,+)$ زمر جزئية ؟ الجواب نعم وهي :

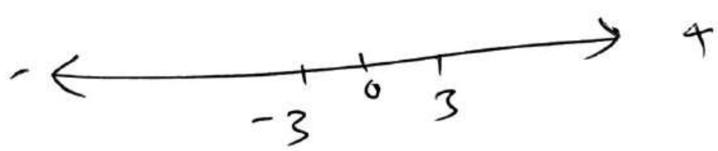
$(Z,+)$



$(2Z,+)$



$(3Z,+)$



$\vdots$

جميع هذه الزمر هي زمر جزئية للزمرة $(Z,+)$.

* بصورة عامة :

الزمر الجزئية للزمرة $(Z,+)$ هي $(nZ,+)$

والزمر الجزئية للزمرة $(2Z,+)$ هي $(n\cdot 2Z,+)$

" " " $(KZ,+)$ هي $(n\cdot KZ,+)$

* اعطِ أمثلة لدينا الزمرة الرباعية :

$$G=(\{1,-1,i,-i\},\cdot) \Rightarrow |G|=\underline{4}$$

هذه الزمرة ذات رتبة $\underline{4}$ عناصرها هي :

$|1|=1$

$|-1|=2\ ,\ |i|=\underline{4}\ ,\ |-i|=\underline{4}$

الزمر الجزئية لها هي :

$$\underset{\text{تافهة}}{\underline{\{1\}}}\ ,\ \underset{\text{فعلية}}{\underline{\{1,-1\}}}\ ,\ \underset{\text{تافهة}}{\underline{\{i,-i,1,-1\}}}\ ,\ \underset{\text{تافهة}}{\underline{\{-i,i,1,-1\}}}$$

العنصر (-1) رتبته $\underline{2}$ أي العنصر نظيره . وهي زمرة جزئية فعلية

$$\langle -1\rangle=\{-1,1\}$$

* الزمرة $(Z_n,+_n)$

رتبة هذه الزمرة هي n

$$Z_n=\{\bar{0},\bar{1},\dots,\overline{n-1}\} \Rightarrow |Z_n|=\underline{n}$$

نعطي مثال لتوضيح كيفية ايجاد الزمر الجزئية .

$$g.c.d(n,a) \Rightarrow \frac{n}{g.c.d(n,a)}$$

$(Z_{12},+_{12})$

$1\cdot 12$	$2\cdot 6$	$3\cdot 4$
trivial	Pro.	Pro.

$g.c.d(12,5)=1 \Rightarrow \frac{12}{1}=12$

$7)=1 \Rightarrow \frac{12}{1}=1$

$8)=4 \Rightarrow \frac{12}{4}=3$

$9)=3 \Rightarrow \frac{12}{3}=4$

$10)=2 \Rightarrow \frac{12}{2}=6$

$11)=1 \Rightarrow \frac{12}{1}=12$

وتعتمد جميعها على الرتبة .

$\langle\bar{0}\rangle=\{\bar{0}\}$

$\langle\bar{1}\rangle=\{\bar{0},\bar{1},\dots,\overline{11}\} \Rightarrow |\bar{1}|=\overline{12}=\underline{Z_{12}}$

$\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\} \Rightarrow |\bar{2}|=\underline{6}$

$\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6},\bar{9}\} \Rightarrow |\bar{3}|=4$

$\langle\bar{4}\rangle=\{\bar{0},\bar{4},\bar{8}\} \Rightarrow |\bar{4}|=3$

$\langle\bar{6}\rangle=\{\bar{0},\bar{6}\} \Rightarrow |\bar{6}|=2$

باقي العناصر هي :

$\langle\bar{0}\rangle \leftarrow$ تافهة

$\left.\begin{array}{l}\langle\bar{1}\rangle=\langle\bar{5}\rangle=\langle\bar{7}\rangle=\langle\overline{11}\rangle\ ,\ \langle\bar{2}\rangle=\langle\overline{10}\rangle\\ \langle\bar{3}\rangle=\langle\bar{9}\rangle\ ,\ \langle\bar{4}\rangle=\langle\bar{8}\rangle\\ \langle\bar{6}\rangle\end{array}\right\}$ فعلية

أما إذا كانت $(Z_p, +_p)$ أي العدد أولي فإن جميع الزمر الجزئية المتولدة لها زمرة جزئية تافهة لأنه عدد أولي :-

$(Z_5, +_5)$

$\langle \bar{0} \rangle = \{\bar{0}\} \Rightarrow |\bar{0}| = 1,$

$Z_5 = \langle \bar{1} \rangle = \langle \bar{2} \rangle = \langle \bar{3} \rangle = \langle \bar{4} \rangle$ because $g.c.d(5, a) = 1 \ \forall a = 1, -4$

أي أن $\{1, 2, 3, 4\}$ هم مولدات لـ Z_5 .

(*) اما في حالة زمرة التباديل permutation group (S_n, o) ايضاً نعتمد على الرتبة وكما يلي في المثال :-

$(S_3, o) \Rightarrow |S_3| = 3! = 6$

$S_3 = \{ I, \underset{L=2}{\underline{(12)}}, \underset{2}{\underline{(13)}}, \underset{2}{\underline{(23)}}, \underset{3}{\underline{(123)}}, \underset{3}{\underline{(132)}} \}$

الزمر الجزئية هي :-

I, S_3 تافهة

$\left.\begin{array}{l} \langle (12) \rangle = \{ I, (12) \} \\ \langle (13) \rangle = \{ I, (13) \} \\ \langle (23) \rangle = \{ I, (23) \} \end{array}\right\}$ مختلفة ذات رتبة $\underline{2}$ $\Rightarrow$ كل عنصر رتبته $\underline{2}$ يساوي نظيره

$\left.\begin{array}{l} \langle (123) \rangle = \{ I, (123), (132) \} \\ \langle (132) \rangle = \{ I, (132), (123) \} \end{array}\right\} \Rightarrow \langle (123) \rangle = \langle (132) \rangle$ ذات رتبة $\underline{3}$

متساوية

نظير

نظير

(*) اذا كانت الزمرة (S_4, o) فبنفس الطريقة ايضاً نعتمد على الرتبة واسهل الزمر الجزئية الفعلية التي رتبتها $\underline{2}$ أي :-

$|S_4| = 4! = 4 \cdot 3 \cdot 2 \cdot = \underline{24}$

$\langle (12) \rangle, \langle (13) \rangle, \langle (14) \rangle, \langle (23) \rangle, \langle (24) \rangle, ----$

وايضاً الزمر الجزئية الفعلية ذات الرتبة $\underline{3}$ وهي :-

$\langle (123) \rangle, \langle (132) \rangle, \langle (234) \rangle, \langle (243) \rangle, \langle (124) \rangle, \langle (142) \rangle$ ----

وايضاً الزمر الجزئية الفعلية ذات الرتبة 4 وهي :-

$\langle (1234) \rangle, \langle (1432) \rangle, \langle (1342) \rangle, \langle (1243) \rangle,$ ----

$$\langle (12) \rangle = \{ I, (12) \}$$

$$\langle (123) \rangle = \{ I, (123), (132) \}$$

$$\langle (1234) \rangle = \{ I, \underset{L=4}{\underline{(1234)}}, \underset{L=4}{\underline{(1432)}}, \underset{L_1 = \underline{\underline{2}}, L_2 = 2}{\underline{(13)(24)}} \}$$

$\vdots$

وهكذا.

⊛ أما في حالة زمرة التناظر:

$Sy(\square) \Leftarrow$ Symmetric gp

وهي أيضاً نفس الطريقة نعتمد على الرتبة:

$$|Sy| = \underline{\underline{8}}$$

$$Sy = \{ \underset{I}{\underline{\underline{R_0}}}, R_{90}, R_{180}, R_{270}, V, H, D_1, D_2 \}$$

ونعلم بأنه كل عنصر له رتبة وهي:

$$|R_{90}| = 4 = |R_{270}|$$

$$|R_{180}| = 2$$

$$|V| = |H| = |D_1| = |D_2| = \underline{\underline{2}}$$

الزمر الجزئية هي:

$$V = \{ I, V \}, \; H = \{ I, H \}, \; D_1 = \{ I, D_1 \}, \; D_2 = \{ I, D_2 \}.$$

$$\{ I, R_{180}, R_{90}, R_{270} \}, \; \{ I, R_{180}, D_1, D_2 \}, \; \{ I, R_{180}, V, H \}$$ أيضاً

جميعها زمر جزئية فعلية.

Cyclic gp

الزمرة الدائرية أو الدوارة: هي زمرة $(G,*)$ وتحتوي عنصر a بحيث علينا أن نكتب جميع عناصر الزمرة بدلالة هذا العنصر بالشكل التالي

$$\langle a\rangle=\{a^0,a^1,a^2,\dots\}$$ اذا كانت غير منتهية

أو

$$\langle a\rangle=\{a^0,a^1,a^2,\dots,a^{n-1}\}$$ اذا كانت منتهية

حيث $a^n=e$ و $a^0=e$.

أمثلة:

* $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$

نلاحظ أن $(\mathbb{Z},+)$ فقط هي زمرة دائرية متولدة بواسطة 1 و -1

أيضاً

$(2\mathbb{Z},+)$ cyclic generated by $(2,-2)$

$(3\mathbb{Z},+)$ " " " $(3,-3)$

$(7\mathbb{Z},+)$ " " " $(7,-7)$

نلاحظ أن العنصر المولد يكون هو ونظيره

* الزمرة $(\{1,-1,i,-i\},\cdot)$ رتبتها 4 نبحث عن عناصر رتبتها 4 والعناصر هي $(i$ و $-i)$
* الزمرة $(\mathbb{Z}_n,+_n)$ التي رتبتها n نبحث عن العناصر التي رتبتها n هي التي تولد هذه الزمرة
* الزمرة $(\mathbb{Z}_p,+_p)$ رتبتها p العناصر التي تولدها هي كل العناصر ما عدا $\bar{0}$.

(*) زمرة التبادل $(S_n, \circ)$ رتبتها $n!$ هذه الزمرة لا تمتلك عناصر رتبتها مساوية لـ $n!$ مثلاً $(S_3, \circ)$ لا يوجد عنصر رتبته $\underline{6}$ لذا فهي ليست دائرية ،

لكن في حالة $(S_2, \circ)$ لاحظ أن $n = \underline{\underline{2}}$ أي

$$S_2 = \{I, \underset{2}{(12)}\}$$

هذه الزمرة دائرية لأن رتبة العنصر (12) هو $\underline{2}$.

∴ بصورة عامة زمرة التبادل ليست دائرية فقط عندما $\boxed{n \leq 2}$ تكون دائرية .

(*) زمرة التناظر $(S_4, \circ)$ رتبتها (8) ، وهذه الزمرة ايضاً لا تمتلك أي عنصر رتبته 8 .

ملاحظات :

1. أي عنصر مولد في الزمرة يجب ان يكون النظير ايضاً مولد .
2. الزمرة التي لا تحوي عناصرها على رتبة مساوية لرتبة الزمرة تكون غير دائرية
3. زمرة التبادل هي زمرة ليست دائرية فقط عندما $\boxed{n \leq 2}$.
4. اي زمرة دائرية تكون ابدالية والعكس غير صحيح .
مثل الزمرة $(Q, +)$ هي زمرة ابدالية ولكنها ليست دائرية.

⊛ الزمرة الدائرية ممكن أن تكتب بصورة عامة بدلالة العنصر a.
ممكن أن نستخرج رتبة العناصر بدلالة $\underline{a}$ مثلاً:-

Example:- If $(G,*)$ is a cyclic gp of order $\underline{15}$ generated by a. Find $|a^7|$, $|a^9|$, $|a^{12}|$.?

Sol

$$G=\{a^0,a^1,a^2,\dots,a^{14}\}\Rightarrow |G|=\underline{15}$$

$$|a^k|=\frac{n}{g.c.d(n,k)}\Rightarrow |a^7|=\frac{15}{g.c.d(15,7)}=\frac{15}{1}=\underline{15}$$

$\therefore a^7$ is generated of G.

$$\rightarrow |a^9|=\frac{15}{g.c.d(15,9)}=\frac{15}{3}=\underline{5}$$

$$\langle a^9\rangle=\{a^0,a^3,a^6,a^9,a^{12}\}$$

$$|a^{12}|=\frac{15}{g.c.d(15,12)}=\frac{15}{3}=\underline{5}$$

$$\langle a^{12}\rangle=\{a^0,a^3,a^6,a^9,a^{12}\}=\langle a^9\rangle$$

Example:- $|G|=60$, Find $|a^{15}|$, $|a^{24}|$, $|a^{11}|$?

$$|a^{15}|=\frac{60}{g.c.d(60,15)}=\frac{60}{15}=\underline{4}$$

$$\langle a^{15}\rangle=\{a^0,a^{15},a^{30},a^{45}\}$$

$$|a^{24}|=\frac{60}{g.c.d(60,24)}=\frac{60}{6}=10$$

$$\langle a^{24}\rangle=\{a^0,a^6,a^{12},a^{18},a^{24},a^{30},a^{36},a^{42},a^{48},a^{54}\}.$$

$$|a^{11}|=\frac{60}{g.c.d(60,11)}=\frac{60}{1}=60\Rightarrow \underline{\langle a^{11}\rangle} \text{ generated of } G. \boxtimes$$

⊛ الزمر الجزئية بدلالة a^k هي قياساً :-

Example:- $|G| = 10$, Find all subgp of G.?

$G = \{a^0, a^1, \dots, a^9\}$

$$10 \begin{cases} 1\cdot 10 & \text{trivial} \\ 2\cdot 5 & \text{Proper} \end{cases}$$

$\langle a^0 \rangle = \{a^0 = e\}$

$\langle a^1 \rangle = \{a^0, a^1, \dots, a^{11}\} = G.$

$\langle a^2 \rangle = \{a^0, a^2, a^4, a^6, a^8\}$

$\langle a^5 \rangle = \{a^0, a^5\}$ والباقي كما جئنا بها سابقاً.

$g.c.d(10,3) = 1 \Rightarrow \frac{10}{1} = 10$ ✓

$g.c.d(10,4) = 2 \Rightarrow \frac{10}{2} = 5$

$g.c.d(10,6) = 2 \Rightarrow \frac{10}{2} = 5$

$,7) = 1 \Rightarrow \frac{10}{1} = 10$ ✓

$8) = 2 \Rightarrow \frac{10}{2} = 5$

$9) = 1 \Rightarrow \frac{10}{1} = 10$ ✓

$\langle a^1 \rangle = \langle a^3 \rangle = \langle a^7 \rangle = \langle a^9 \rangle$

نظير

نظير

$\langle a^2 \rangle = \langle a^4 \rangle = \langle a^6 \rangle = \langle a^8 \rangle.$ ⊠

وهكذا كما تم شرحه مسبقاً.

Normal subgroups — الزمرة الجزئية الناظمية

***Define:-** Let $(H,*)$ be a subgroup of the group $(G,*)$ and let $a \in G$. The set :-

مصاحبات يسارية

$a*H = \{a*h : h \in H\}$ is called a $\boxed{\text{left coset}}$ of H in G.

The element a is a representative of $a*H$. and the set

مصاحبات يمينية

$H*a = \{h*a : h \in H\}$ is called a $\boxed{\text{right coset}}$ of H in G.

ليس بالضرورة

Note:- It is not necessarily $\boxed{a*H = H*a}$.

Example:- Let $H = \{\bar{0}, \bar{4}, \bar{8}\}$, $G = (Z_{12}, +_{12})$. Find $a*H$, $H*a$.

Sol.

$0 +_{12} H = \{\bar{0}, \bar{4}, \bar{8}\}$

$1 +_{12} H = \{\bar{1}, \bar{5}, \bar{9}\}$

$2 +_{12} H = \{\bar{2}, \bar{6}, \bar{10}\}$

$3 +_{12} H = \{\bar{3}, \bar{7}, \bar{11}\}$

$4 + H = \{\bar{4}, \bar{8}, \bar{0}\} = 0+H = 8+H$

$5 + H = \{\bar{5}, \bar{9}, \bar{1}\}$

$6 + H = \{\bar{6}, \bar{10}, \bar{2}\}$

$7 + H = \{\bar{7}, \bar{11}, \bar{3}\}$

$8 + H = \{\bar{8}, \bar{0}, \bar{4}\}$

$9 + H = \{\bar{9}, \bar{1}, \bar{5}\}$

$10 + H = \{\bar{10}, \bar{2}, \bar{6}\}$

$11 + H = \{\bar{11}, \bar{3}, \bar{7}\}$

مكررة

$H+0 = \{0, 4, 8\} = H+4 = H+8$

$H+1 = \{1, 5, 9\} = H+5 = H+9$

$H+2 = \{2, 6, 10\} = H+6 = H+10$

$H+3 = \{3, 7, 11\} = H+7 = H+11$

ملاحظة: نلاحظ أن عدد المصاحبات هو

$0+H,\ 1+H,\ 2+H,\ 3+H$

أربع مصاحبات وان

$H = \{0, 4, 8\}$

الفترة ما بين الـ $[0,4)$ هو عدد المصاحبات والباقي مكررة جميعها.

Example:- If $(G,\cdot)$ is cyclic group of order $\underline{4}$, and $H=\langle a^2\rangle$ is a subgroup of G generated by a^2. Find $a*H$ and $H*a$ of H in G.

Sol:

$$G=\{e,a,a^2,a^3\},\ |G|=4 \Rightarrow a^4=e.$$ لأن الزمرة دائرية ورتبتها $\underline{4}$

$$H=\langle a^2\rangle=\{e,a^2\}.$$

$a*H=$

$e*H=\{e,a^2\}=a^2*H$

$a*H=\{a,a^3\}=a^3*H$

$a^2*H=\{a^2,e\}$

$a^3*H=\{a^3,a\}$

$\therefore a*H=\{e*H,a*H\}$

$H*a=$

$H*e=\{e,a^2\}$

$H*a=\{a,a^3\}$

$H*a^2=\{a^2,e\}$

$H*a^3=\{a^3,a\}$

$H*a=\{H*e,H*a\}$

$\therefore H*a=a*H.$ $\boxtimes$.

Example:- Let $G=(Z_4,+_4)$, $H=\langle 2\rangle=\{\bar{0},\bar{2}\}$, Find $a*H$, $H*a$

$a*H$:

$\bar{0}+H=\{\bar{0},\bar{2}\}$

$\bar{1}+H=\{\bar{1},\bar{3}\}$

$\bar{2}+H=\{\bar{2},\bar{0}\}$

$\bar{3}+H=\{\bar{3},\bar{1}\}$

$\therefore a*H=\{0+_4H,1+_4H\}$

$H*a$:

$H+\bar{0}=\{\bar{0},\bar{2}\}$

$H+\bar{1}=\{\bar{1},\bar{3}\}$

$H+\bar{2}=\{\bar{2},\bar{0}\}$

$H+\bar{3}=\{\bar{3},\bar{1}\}$

$\therefore H*a=\{H+\bar{0},H+\bar{1}\}$

$\therefore a*H=H*a.$ $\boxtimes$

Example:- Let $G = (\mathbb{Z}_{12}, +_{12})$, $H = \langle 6 \rangle = \{\bar{0}, \bar{6}\}$, Find $a * H$, $H * a$.

Sol

$a * H =$

$0 + H = \{\bar{0}, \bar{6}\}$

$1 + H = \{\bar{1}, \bar{7}\}$

$2 + H = \{\bar{2}, \bar{8}\}$

$\bar{3} + H = \{\bar{3}, \bar{9}\}$

$4 + H = \{\bar{4}, \bar{10}\}$

$5 + H = \{\bar{5}, \bar{11}\}$

$6 + H = \{\bar{6}, \bar{0}\} = 0 + H$

$7 + H = \{\bar{7}, \bar{1}\} = 1 + H$

$8 + H = \{\bar{8}, \bar{2}\} = 2 + H$

$9 + H = \{\bar{9}, \bar{3}\} = 3 + H$

$10 + H = \{\bar{10}, \bar{4}\} = 4 + H$

$\bar{11} + H = \{\bar{11}, \bar{5}\} = 5 + H$

$\therefore a * H = \{0 + H, 1 + H, 2 + H, 3 + H, \bar{4} + H, \bar{5} + H\}$

$H * a =$

$H + 0 = \{\bar{0}, \bar{6}\}$

$H + 1 = \{\bar{1}, \bar{7}\}$

$H + 2 = \{\bar{2}, \bar{8}\}$

$H + 3 = \{\bar{3}, \bar{9}\}$

$H + 4 = \{\bar{4}, \bar{10}\}$

$H + 5 = \{\bar{5}, \bar{11}\}$

$H + 6 = \{\bar{6}, \bar{0}\} = H + 0$

$H + 7 = \{\bar{7}, \bar{1}\} = H + 1$

$H + 8 = \{\bar{8}, \bar{2}\} = H + 2$

$H + 9 = \{\bar{9}, \bar{3}\} = H + 3$

$H + 10 = \{\bar{10}, \bar{4}\} = H + 4$

$H + 11 = \{\bar{11}, \bar{5}\} = H + 5$

$\therefore H * a = \{H + 0, H + 1, H + 2, H + 3, H + 4, H + 5\}$

$H * a = a * H$

نلاحظ ان

$\boxtimes$

Remarks:-

1- If $(G,*)$ is a Commutative group then:-
$$a*H = H*a. \quad \forall a \in G.$$

2. If e is the identity element of $(G,*)$. Then
$$e*H = \{e*h : h \in H\} = \{h : h \in H\} = H.$$

3- $|a*H| = |H|$. i.e. $o(a*H) = o(H)$.

4- $a*H$ is not subgp in general. (H.w.)

5- $a*H \neq H*a$ in general. For example:-

Example:- In (S_3, o), $H = \langle(12)\rangle$

$$S_3 = \{I, (123), (132), (12), (13), (23)\}$$

$H = \langle(12)\rangle = \{I, (12)\}$ where $(12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$a*H =$

$$I \circ H = \{I \circ I, I \circ (12)\} = \{I, (12)\} = H$$

$$(123) \circ H = \{(123) \circ I, (123) \circ (12)\} = \{(123), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$= \{(123), (13)\}.$$

$$H \circ (123) = \{I \circ (123), (12) \circ (123)\} = \{(123), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\},$$

$\therefore a*H \neq H*a \Longrightarrow \quad = \{(123), (23)\} \neq \{(123), (13)\}.$ $\boxtimes$

Definition:- A Subgroup H of a group G is called a $\boxed{\text{normal subgp}}$ of G if:-

$$\boxed{Ha = aH \quad \forall a \in G.}$$

Example:- Let $G = (\{1, -1, i, -i\}, \cdot)$ and $H = (\{1, -1\}, \cdot)$

is H a normal subgroup or not.?

Sol:

$a * H =$

$1 \cdot H = \{1, -1\}$

$-1 \cdot H = \{-1, 1\}$

$i \cdot H = \{i, -i\}$

$-i \cdot H = \{-i, i\}$

$H * a =$

$H \cdot 1 = \{1, -1\}$

$H \cdot (-1) = \{-1, 1\}$

$H \cdot (i) = \{i, -i\}$

$H \cdot (-i) = \{-i, i\}$

$$a * H = H * a = \{H, i \cdot H\}$$

$\therefore$ H is a normal subgp of G. ⊠.

Theorem:- A subgroup H of a group G is normal in G iff $\boxed{g^{-1}Hg = H}$ for all $g \in G$. تعريف ثاني

Proof:- Let H be a normal subgp in G, then صحيحة مهمة

$$Hg = gH \quad \forall g \in G$$

$$\Rightarrow g^{-1}Hg = g^{-1}(gH) = (g^{-1}g)H = H$$

Conversely, let $g^{-1}Hg = H \quad \forall g \in G$.

Then $g(g^{-1}Hg) = gH$

$$\Rightarrow (gg^{-1})Hg = gH \Longrightarrow Hg = gH \quad \text{Hence } H \text{ is normal.} ⊠$$

Theorem:- Let $(H,*)$ be a subgp of $(G,*)$ and $a \in G$

Then:-

1- H is itself left coset of H in G.

الزمرة الجزئية H هي نفسها مصاحبات يسارية من H للزمرة G .

2- If $(G,*)$ is abelian group, then $a*H = H*a$.

Proof ①:-

$e \in H$, $e*H = \{e*h \mid h \in H\} = H$.

Proof ②:-

$a*H = \{a*h : h \in H\} = \{h*a : h \in H\} = H*a$.

Note:- $\boxed{\text{The Converse is not true.}}$ العكس غير صحيح .

Example:- $(S_3, \circ)$, $H = \langle (123) \rangle$

$S_3 = \{I, (123), (132), (12), (23), (13)\}$

$\langle (123) \rangle = \{I, (123), (132)\}$

$a*H \Rightarrow$ if $a = (132)$

$$(132)\circ H = \left\{ \begin{array}{l} (132)\circ I, (132)\circ(123), (132)\circ(132) \\ = (132), I, (123) \end{array} \right\}.$$

$\Rightarrow a*H = \{I, (123), (132)\}$

$$H*a = \left\{ \begin{array}{l} I\circ(132), (123)\circ(132), (132)\circ(132) \\ = (132), I, (123) \end{array} \right\}$$

Now: $a * H = H * a$ in $(S_3, \circ)$ if $H = \{I, (123), (132)\}$

$\boxed{\text{but}}$ $(S_3, \circ)$ is not abelian gp. $\boxtimes$.

Remark:- Every coset (Left or Right) of a Subgp H of a group $(G, *)$ has the sane number of element as G.

ملاحظة:-

اي مصاحبات (يسارية او يمينية) عددها مساوي لعدد العناصر الموجودة في G.

Example:- In $(Z_6, +_6)$, $H = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$

$a * H =$	$H * a =$
$\bar{0} + H = \{\bar{0}, \bar{3}\}$	$H + \bar{0} = \{\bar{0}, \bar{3}\}$
$\bar{1} + H = \{\bar{1}, \bar{4}\}$	$H + \bar{1} = \{\bar{1}, \bar{4}\}$
$\bar{2} + H = \{\bar{2}, \bar{5}\}$	$H + \bar{2} = \{\bar{2}, \bar{5}\}$
$\bar{3} + H = \{\bar{3}, \bar{0}\} = \bar{0} + H$	$H + \bar{3} = \{\bar{3}, \bar{0}\} = H + \bar{0}$
$\bar{4} + H = \{\bar{4}, \bar{1}\} = \bar{1} + H$ مكررة	$H + \bar{4} = \{4, \bar{1}\} = H + \bar{1}$ مكررة
$\bar{5} + H = \{\bar{5}, \bar{2}\} = \bar{2} + H$	$H + \bar{5} = \{\bar{5}, \bar{2}\} = H + \bar{2}$
$\therefore a * H = \{\bar{0} + H, \bar{1} + H, \bar{2} + H\}$	$\therefore H * a = \{H + \bar{0}, H + \bar{1}, H + \bar{2}\}$

$\Longrightarrow a * H = H * a \Longrightarrow H$ is normal Subgp.

Remark:- $(a * H) \cap (b * H) = \phi$ or $a * H = b * H$.

* يعني :- تقاطع المصاحبات المختلفة مساوي لـ ϕ أو المصاحبات متساوية.

كما في امثلة اعلاه :-

$\bar{0} + H \cap \bar{1} + H = \phi$

✓ $\bar{1} + H = \bar{4} + H$.

Remark:- If $(H,*)$ is a subgp of G, then the Left (Right) cosets of H in G forms a partition.

ملاحظة:- المصاحبات اليمينية (اليسارية) تقسم G.

Example:- In $(Z_6, +_6)$, $H = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$

$a*H =$

$$\left.\begin{aligned}
\bar{0}+H &= \{\bar{0},\bar{2},\bar{4}\}\\
\bar{1}+H &= \{\bar{1},\bar{3},\bar{5}\}\\
\bar{2}+H &= \{\bar{2},\bar{4},\bar{0}\} = \bar{0}+H\\
\bar{3}+H &= \{\bar{3},\bar{5},\bar{1}\} = \bar{1}+H\\
\bar{4}+H &= \{\bar{4},\bar{0},\bar{2}\} = \bar{0}+H\\
\bar{5}+H &= \{\bar{5},\bar{1},\bar{3}\} = \bar{1}+H
\end{aligned}\right\} \text{مكررة}$$

$H*a =$

$$\left.\begin{aligned}
H+0 &= \{\bar{0},\bar{2},\bar{4}\}\\
H+1 &= \{\bar{1},\bar{3},\bar{5}\}\\
H+2 &= \{\bar{2},\bar{4},\bar{0}\} = H+0\\
H+3 &= \{\bar{3},\bar{5},\bar{1}\} = H+1\\
H+4 &= \{\bar{4},\bar{0},\bar{2}\} = H+0\\
H+5 &= \{\bar{5},\bar{1},\bar{3}\} = H+1
\end{aligned}\right\} \text{مكررة}$$

$\therefore a*H = \{\bar{0}+H, \bar{1}+H\}$, $H*a = \{H+\bar{0}, H+\bar{1}\}$

$\Longrightarrow a*H = H*a$

نلاحظ الآتي:-

① عدد المصاحبات الناتجة هو $\underline{\underline{2}}$ لأن $o(Z_6)=6$

و $o(H)=3 \Longleftarrow 2 = \frac{6}{3}$ عدد المصاحبات

$\boxed{\therefore \text{قانون:- عدد المصاحبات} = \dfrac{\text{رتبة الزمرة}}{\text{رتبة الزمرة الجزئية}}}$ مهم جداً

$$\boxed{\therefore \text{The number of Cosets} = \frac{o(G)}{o(H)}.}$$

ونلاحظ ذلك من خلال جميع الأمثلة السابقة.

Definition:- Let $(H,*)$ be a subgp of a group $(G,*)$. The number of Left (Right) cosets of H in G is called the $\boxed{\text{index}}$ of H in G and denoted by $[G:H]$.

Note:- If $H=\{e\}$, then $[G:H]=\frac{o(G)}{o(H)}=\frac{n}{1}=n=o(G)$.

Example:- In $(Z_{12},+_{12})$ and $H=\{\bar{0},\bar{4},\bar{8}\}$,

$$[G:H]=\frac{o(G)}{o(H)}=\frac{12}{3}=4 \,//$$

عدد المصاحبات هو $\underline{4}$.

Example:- In $(Z_{18},+_{18})$, $H=\{\bar{0},\bar{6},\bar{12}\}$.

$$[G:H]=\frac{o(G)}{o(H)}=\frac{18}{3}=6 \,//$$ عدد المصاحبات هو 6

$$\left.\begin{aligned}
\bar{0}+H &= \{\bar{0},\bar{6},\bar{12}\}\\
\bar{1}+H &= \{\bar{1},\bar{7},\bar{13}\}\\
\bar{2}+H &= \{\bar{2},\bar{8},\bar{14}\}\\
\bar{3}+H &= \{\bar{3},\bar{9},\bar{15}\}\\
\bar{4}+H &= \{\bar{4},\bar{10},\bar{16}\}\\
\bar{5}+H &= \{\bar{5},\bar{11},\bar{17}\}
\end{aligned}\right\} \Longrightarrow$$ عدد المصاحبات $= \underline{\underline{6}}$

بعدها تكون مكررة

$\boxed{\text{ملاحظة: حيلة رياضية}}$

عدد المصاحبات يكون محصور بين العدد بين الأول والثاني من H مغلق من الأول ومفتوح من الثاني مثلاً:

$$H=\{\bar{0},\bar{6},\bar{12}\} \Rightarrow [\bar{0},\bar{6})=\{\underline{\underline{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}}}\}$$

وهكذا!

Theorem: "Lagrange Theorem" مبرهنة لاگرانج

((The order and index of any subgroup of a finite group divide the order of the group.))

رتبة الزمرة الجزئية و تقسم رتبة الزمرة.
الدليل

Proof:-

Let $(G,*)$ be a finite group and $(H,*)$ be a subgp of $(G,*)$ and let $o(G)=n$, $o(H)=k$, $[G:H]=r$

<we want to prove $k \backslash n$ and $r \backslash n$> | الرمز \ يعني يقسم

i.e. $\boxed{o(H) \backslash o(G)}$ and $\boxed{[G:H] \backslash o(G)}$.

Let $a_1 * H, a_2 * H, \ldots, a_r * H$ be the distinct Left Cosets of H in G

$\therefore a_1 * H \cup a_2 * H \cup \cdots \cup a_r * H = G$

$\Rightarrow |a_1 * H \cup a_2 * H \cup \cdots \cup a_r * H| = |G| = n$

$\Rightarrow |a_1 * H| + |a_2 * H| + \cdots + |a_r * H| = |G| = n$

$\because |a_i * H| = |H| = k \quad \forall\, i = 1, \ldots, r$

$\Rightarrow k + k + \cdots + k = n$

$\Rightarrow rk = n$, $\therefore r \backslash n$ and $k \backslash n$. ⊠

(*) طريقة اخرى في البرهان.

or $o(G) = [G:H] \cdot o(H)$

$|G| = [G:H] \cdot |H|$

$n = r \cdot k$

$\Rightarrow r \backslash n$ and $k \backslash n$. ⊠

Example:- In $(Z_{24}, +_{24})$, $H_1 = \langle \bar{3} \rangle$, $H_2 = \langle \bar{4} \rangle$.

$$[G : H_1] = \frac{o(G)}{o(H_1)} = \frac{24}{8} = 3.$$

$H_1 = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}, \bar{18}, \bar{21}\} \Rightarrow o(H_1) = 8$

$H_2 = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}\} \Rightarrow o(H_2) = 6$

$$[G : H_2] = \frac{24}{6} = \underline{\underline{6}}$$

$\Rightarrow o(G) = [G : H] \cdot o(H)$

$\Rightarrow o(G) = [G : H_1] \cdot o(H_1)$

$24 = 3 \cdot 8 \Rightarrow 3 \backslash 24$ and $8 \backslash 24$

$o(G) = [G : H_2] \cdot o(H_2)$

$24 = 6 \cdot 6 \Rightarrow 6 \backslash 24.$ ⊠

Corollary (17):- If $(G, *)$ is finite group, then, the order of any element of G divides the order of G.

نتيجة :- اذا كانت $(G,*)$ زمرة منتهية فان ترتيب اي عنصر في G يقسم ترتيب الزمرة اي

$o(a) \backslash o(G).$

Example:- $In(Z_4, +_4) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$o(\bar{0}) = 1$ because $(\bar{0}) = \{\bar{0}\}$

$o(\bar{1}) = 4$ " $(\bar{1}) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$o(\bar{2}) = 2$ " $(\bar{2}) = \{\bar{0}, \bar{2}\}$

$o(\bar{3}) = 4$ " $(\bar{3}) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

ملاحظة :-

$o(a) \backslash o(G) \quad \forall a \in G$

$1 \backslash 4$

$4 \backslash 4$

$2 \backslash 4$

$4 \backslash 4$

Corollary ② : If $(G, *)$ is a finite group, then

$$a^{o(G)} = e \quad , \forall a \in G.$$

نتيجة: اذا كانت $(G,*)$ زمرة منتهية فان

$$\boxed{a^{o(G)} = e \quad \forall a \in G}$$

Proof:-

Suppose that $o(G) = n$,

Let $a \in G$, $\ni o(a) = m$.

By corollary ① of Lagrange theorem $\Rightarrow o(a) \backslash o(G). \Rightarrow m \backslash n$

$\Rightarrow n = mk$

$a^{o(G)} = a^n = (a^m)^k = e^k = e$

$\therefore a^{o(G)} = e \quad \forall a \in G. \boxtimes$

Example:- In $(Z_4, +_4) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $o(Z_4) = 4$.

$\bar{0}^4 = \bar{0}$, $\bar{1}^4 = \bar{0}$, $\bar{2}^4 = \bar{0}$, $\bar{3}^4 = \bar{0}$.

Corollary ③:- Every group of Prime order is cyclic.

$\boxed{\text{نتيجة: كل زمرة ذات رتبة اولية دائرية}}$

Proof:- Let $(G, *)$ be finite

$\ni o(G) = p$.

By corollary ① of Lagrange theorem $\Rightarrow o(a) \mid p \quad \forall a \in G$.

$\Rightarrow o(a) = 1$ or p

If $o(a) = 1 \Rightarrow a = e$

If $o(a) = p \Rightarrow o(a) = o(G) \Rightarrow G = \langle a \rangle$

$\therefore (G, *)$ is cyclic group. ⊠.

Example:- In $(Z_5, +_5) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} \Rightarrow o(Z_5) = \underline{5}$.

5 is a prime number

$\Rightarrow o(\bar{0}) = 1$ because $(\bar{0}) = \{\bar{0}\}$

$o(\bar{1}) = 5$ " $(\bar{1}) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$o(\bar{2}) = 5$ " $(\bar{2}) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$o(\bar{3}) = 5$ " $(\bar{3}) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$o(\bar{4}) = 5$ " $(\bar{4}) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\langle \bar{1} \rangle = \langle \bar{2} \rangle = \langle \bar{3} \rangle = \langle \bar{4} \rangle$, because g.c.d $(5,1) = 1$

$(5,2) = 1$

تولد relative prime $(5,3) = 1$

$\Rightarrow \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ generated Z_5. $(5,4) = 1$

Z_5 clic. ⊠

Definition:- Simple group الزمرة البسيطة

The group $(G,*)$ is called a Simple group if $(G,*)$ has no normal subgps other than the two trivial ones.

Example:- $(Z_7,+_7)$ is a simple group.

Note:- The finite cyclic groups of prime order are Simple groups.

Definition: Commutator المبادل

Let $(G,*)$ be a group and $a,b \in G$, the Commutator of a and b is defined to be the Product:

$a*b*a^{-1}*b^{-1}$, it will be denoted by $[a,b]$

i.e. $[a,b] = a*b*a^{-1}*b^{-1}$.

Remark:-

1- If $(G,*)$ is a Comm. gp. then $[a,b]=e \ \forall a,b \in G$.

because: $[a,b] = a*b*a^{-1}*b^{-1} = a*a^{-1}*b*b^{-1} = e$.

2- If $[a,b]=e \ \forall a,b \in G$, Then $(G,*)$ is a Comm. gp.

Proof: Let $a,b \in G$.

$\because [a,b]=e \Rightarrow a*b*a^{-1}*b^{-1}=e$

$\Rightarrow a*b*a^{-1}*b^{-1}*b = e*b \Rightarrow a*b*a^{-1} = b$

$\Rightarrow a*b = b*a$. ⊠

Example:- Let $G = \{1, -1, i, -i\}$, $a = -1$, $b = i$, Find $[a,b]$?

Sol:

$[a,b] = a * b * a^{-1} * b^{-1} = -1 \cdot i \cdot -1 \cdot -i = -i \cdot i = \underline{\underline{1}}$

وهناك طريقة اخرى ، وهي :-

$\because G$ is a Comm. gp, then $[a,b] = e = \underline{\underline{1}}$

Example:- Let $G = (S_3, \circ)$, $a = (12)$, $b = (123)$, Find $[a,b]$?

Sol:

$[a,b] = a * b * a^{-1} * b^{-1} \Longrightarrow (12) \circ (123) \circ (12)^{-1} \circ (123)^{-1}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$= \underline{\underline{(13)}} \neq I$ because $(S_3, \circ)$ is not Comm. $\boxtimes$

Factor Groups or Quotient group

Factor groups:-

Let N be a normal subgroup of a group $(G,*)$. We define the set G/N to be the set of all Left (or, right) Cosets of N in G, i.e.,

$G/N = \{a*N : a \in G\}$. we define the binary operation on G/N, $\otimes$ as follows:

$a*N \otimes b*N = (a*b)*N$. where $a*N, b*N \in G/N$.

Definition: Factor groups:

For any group G, Let N be a normal subgroup of G. Then, the set of all left (or, right) cosets of N in G, is also a group it self, known as factor group of G by N (or the quotient group of G by N).

Notation: The factor group of G by H is denoted by G/H. And, $G/H = \{a*H \mid a \in G\}$.

Theorem:- Let $(H, *)$ be a normal subgroup of the group $(G, *)$. Then $(G/H, \otimes)$ forms a group called the $\boxed{\text{quotient group}}$ of G by H.

Proof:- 1- <To show $\otimes$ is associative on G/H>.

Let $a*H, b*H, c*H \in G/H$.

$$\Rightarrow [(a*H)\otimes(b*H)]\otimes(c*H) = ((a*b)*H)\otimes(c*H)$$
$$= ((a*b)*c)*H$$
$$= (a*(b*c))*H$$
$$= (a*H)\otimes[(b*H)\otimes(c*H)]. \boxtimes$$

2- <To show $e*H$ is the identity element on $\otimes$>.

$$(a*H)\otimes(e*H) = (a*e)*H = a*H$$
$$(e*H)\otimes(a*H) = (e*a)*H = a*H. \boxtimes$$

3- <To show $a^{-1}*H$ is the inverse element of $a*H$>.

$$(a*H)\otimes(a^{-1}*H) = (a*a^{-1})*H = e*H = H$$
$$(a^{-1}*H)\otimes(a*H) = (a^{-1}*a)*H = e*H = H. \boxtimes$$

$\therefore (G/H, \otimes)$ is a group called quotient group of G by H. $\boxtimes$.

Remark:-

If $(G, *)$ is a Comm. group, then $(G/H, \otimes)$ is also a Comm.

Proof:- $(a*H)\otimes(b*H) = (a*b)*H$

$$= (b*a)*H$$

$$= (b*H)\otimes(a*H). \boxtimes$$

Examples:-

1- Find the quotient group $(\mathbb{Z}_8/\{\bar{0},\bar{4}\}, \otimes)$, and construct the operation table.?

Sol

$\mathbb{Z}_8 = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7}\}$, $H = \{\bar{0},\bar{4}\}$.

$$\mathbb{Z}_8/H = \{\bar{0}+H, \bar{1}+H, \bar{2}+H, \bar{3}+H\}$$

$$= \{\{\bar{0},\bar{4}\}, \{\bar{1},\bar{5}\}, \{\bar{2},\bar{6}\}, \{\bar{3},\bar{7}\}\}$$

$\otimes$	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$	$\bar{3}+H$
$\bar{0}+H$	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$	$\bar{3}+H$
$\bar{1}+H$	$\bar{1}+H$	$\bar{2}+H$	$\bar{3}+H$	$\bar{0}+H$
$\bar{2}+H$	$\bar{2}+H$	$\bar{3}+H$	$\bar{0}+H$	$\bar{1}+H$
$\bar{3}+H$	$\bar{3}+H$	$\bar{0}+H$	$\bar{1}+H$	$\bar{2}+H$

2- Since $(Z,+)$ is an abelian group, $4Z$ is normal Subgp. of Z. Find the factor group $Z/4Z$.?

Solu

$Z/4Z = \{a+4Z \mid a \in Z\} = \{0+4Z, 1+4Z, 2+4Z, 3+4Z\}$.

(using the fact that:

$0+4Z = 4+4Z = 8+4Z = \cdots$

$1+4Z = 5+4Z = 9+4Z = \cdots$

$2+4Z = 6+4Z = 10+4Z = \cdots$

$3+4Z = 7+4Z = 11+4Z = \cdots$

$\otimes$	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$0+4Z$	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$1+4Z$	$1+4Z$	$2+4Z$	$3+4Z$	$0+4Z$
$2+4Z$	$2+4Z$	$3+4Z$	$0+4Z$	$1+4Z$
$3+4Z$	$3+4Z$	$0+4Z$	$1+4Z$	$2+4Z$. ☒

3- Let $|G| = 16$, $|H| = 4$, G generated by a. Find the factor of G/H.?

Solu : $G = \{a^0, a^1, \cdots, a^{15}\}$, $H = \{a^0, a^4, a^8, a^{12}\}$

$G/H = \{a^0 * H, a^1 * H, a^2 * H, a^3 * H\}$

$\otimes$	$a^0 * H$	$a^1 * H$	$a^2 * H$	$a^3 * H$
$a^0 * H$	$a^0 * H$	$a^1 * H$	$a^2 * H$	$a^3 * H$
$a^1 * H$	$a^1 * H$	$a^2 * H$	$a^3 * H$	$a^0 * H$
$a^2 * H$	$a^2 * H$	$a^3 * H$	$a^0 * H$	$a^1 * H$
$a^3 * H$	$a^3 * H$	$a^0 * H$	$a^1 * H$	$a^2 * H$

. ☒

4- Let $G = \{1, -1, i, -i\}$, $H = \{1, -1\}$. Find $(G/H, \times)$?

Sol

$G/H = \{1*H, i*H\}$ because $1*H = -1*H$

$i*H = -i*H$

and by Lagrange theorem $\frac{|G|}{|H|} = \frac{4}{2} = 2$ عدد المصاحبات

$\times$	$1*H$	$i*H$
$1*H$	$1*H$	$i*H$
$i*H$	$i*H$	$1*H$

. $\boxtimes$

ملاحظات مهمة :-

١- يجب ان تكون الزمرة الجزئية زمرة ناظمية عند حسابه زمرة القسمة أي ان $H \trianglelefteq G$.

٢- اذا كان عدد المصاحبات مساوي لـ 2 فان الزمرة الجزئية تكون زمرة جزئية ناظمية أي

$$[G:H] = \frac{o(G)}{o(H)} = 2 \Rightarrow H \trianglelefteq G$$

٣- اذا كانت الزمرة ابدالية هذا يؤدي الى ان زمرة القسمة ابدالية ايضاً.

٤- اذا كانت الزمرة الجزئية ناظمية فليس بالضرورة ان تكون الزمرة ابدالية.

٥- تقاطع الزمر الجزئية الناظمية هو زمرة جزئية ناظمية.

٦- يقال عن الزمرة بأنها زمرة بسيطة اذا كانت لا تحتوي على زمرة جزئية ناظمية فعلية غير الزمر الجزئية الناظمية التافهة.

٧- المبادل مساوي للمحايد بالنسبة للزمرة اذا كانت الزمرة ابدالية. $\boxtimes$

Chapter 4

Homomorphisms

"Homomorphisms" التشاكلات

Definition:- Let $(G,*)$ and $(G',\circledast)$ be two groups. A homomorphism from G into G' is a mapping:

$$f:(G,*)\longrightarrow(G',\circledast) \text{ such that:}$$

$$f(a*b)=f(a)\circledast f(b). \text{ for all } a,b\in G.$$

التعريف: لتكن $(G,*)$ و $(G',\circledast)$ زمرتان و f دالة من G الى G' فان f تشاكل اذا وفقط اذا

$$f(a*b)=f(a)\circledast f(b). \quad \forall\, a,b\in G.$$

Examples:-

1- Let $(G,*)$ be any group define: $f:G\longrightarrow G$ by:-

$f(a)=e \quad \forall a\in G$. Is f a homomorphism?

Sol: Let $a,b\in G \Rightarrow f(a)=e,\ f(b)=e$.

$$\Rightarrow f(a*b)=e$$
$$=e*e$$
$$=f(a)*f(b). \quad \therefore f \text{ is a homomorphism.}$$

Note: $f:G\to G,\ f(a)=e$ is called a trivial homomorphism

التشاكل التافه

كما في المثال ①

2- $f:G\longrightarrow G$, s.t. $f(a)=a$. Is f a homo.?

Sol: let $a,b\in G\Rightarrow f(a)=a,\ f(b)=b$

$$\Rightarrow f(a*b)=a*b\Rightarrow f(a)*f(b). \therefore f \text{ homo.} \boxtimes$$

3- Let $(\mathbb{Z},+)$ be a group, define $f: \mathbb{Z} \to \mathbb{Z}$ by:
$f(a)=7a \quad \forall a \in \mathbb{Z}$. IS f a homo.?

Sol

Let $a,b \in \mathbb{Z}$, s.t. $f(a)=7a$, $f(b)=7b$.

$$
\begin{aligned}
f(a+b) &= 7(a+b) \\
&= 7a+7b \\
&= f(a)+f(b).
\end{aligned}
$$

$\therefore f$ is homo. $\boxtimes$

4- Let $(G,*)$ and $(G',\circledast)$ be two groups with identity elements e and e' respectively.

Define $f: G \longrightarrow G'$ by:
$f(a)=e' \quad \forall a \in G$. IS f a homo.?

Sol

Let $a,b \in G$, s.t. $f(a)=e'$, $f(b)=e'$.

$$
\begin{aligned}
f(a*b) &= e' \\
&= e' * e' \\
&= f(a) * f(b).
\end{aligned}
$$

$\therefore f$ homo. $\boxtimes$.

5- Let $(R,+)$ and $(R-\{0\},\cdot)$ be two groups.

Define : $f: R \longrightarrow (R-\{0\})$ by:

$f(a) = 5^a \quad \forall a \in R$. Is f a homo.?

Sol:

let $a,b \in R$, s.t. $f(a) = 5^a$, $f(b) = 5^b$.

$$f(a+b) = 5^{a+b}$$

$$= 5^a \cdot 5^b$$

$$= f(a) \cdot f(b).$$ $\therefore f$ is a homo. $\boxtimes$

6- let $(Z,+)$ be a group, define $f: Z \longrightarrow Z$ by:

$f(a) = a+1$, $\forall a \in Z$. Is f a homo.?

Sol:

Let $a,b \in Z$, s.t. $f(a) = a+1$, $f(b) = b+1$

$f(a+b) = (a+b)+1$ --- (1)

$f(a)+f(b) = a+1 + b+1 = (a+b)+2$ --- (2)

$1 \neq 2$.

$\therefore f$ is not homo. $\boxtimes$

7- Let $f: \mathbb{Z} \to \mathbb{Z}_n$ s.t. $f(a) = [a]$, $\forall a \in \mathbb{Z}$. Is f a homo.?

Sol:

Let $a, b \in \mathbb{Z}$, s.t. $f(a) = [a]$, $f(b) = [b]$.

$$
\begin{aligned}
f(a+b) &= [a+b] \\
&= [a] +_n [b] \\
&= f(a) +_n f(b).
\end{aligned}
$$

$\therefore f$ is a homo. $\boxtimes$

8- Let $\varphi: (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$, s.t. $\varphi(a) = |a|$, $\forall a \in \mathbb{R}^*$. Is φ a homo.?

Sol:

Let $a, b \in \mathbb{R}^*$, s.t. $\varphi(a) = |a|$, $\varphi(b) = |b|$.

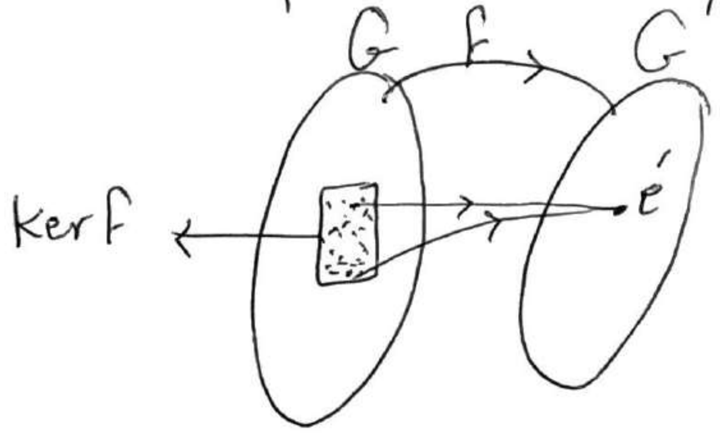
$$
\begin{aligned}
\varphi(a \cdot b) &= |a \cdot b| \\
&= |a| \cdot |b| \\
&= \varphi(a) \cdot \varphi(b).
\end{aligned}
$$

$\therefore \varphi$ is a homo. $\boxtimes$

Kernel النواة

Define:- Let f be a homomorphism from the group $(G,*)$ into the group $(G',\oplus)$. The $\boxed{\text{Kernel}}$ of f, denoted by Kerf, is the set:

$$\operatorname{Ker} f = \{ a \in G : f(a) = e' \} \subseteq G$$



Example:- Let $f : (\mathbb{Z},+) \to (\mathbb{Z}_4, +_4)$ defined by:
$f(a) = [a] \quad \forall a \in \mathbb{Z}$. Is f a homo. and find the ker f.?

Sol:
Let $a,b \in \mathbb{Z}$, s.t. $f(a) = [a]$, $f(b) = [b]$

$$\begin{aligned} f(a+b) &= [a+b] \\ &= [a] +_4 [b] \\ &= f(a) +_4 f(b). \end{aligned} \qquad \therefore f \text{ is homo.}$$

Now:

$$\begin{aligned} \operatorname{Ker} f &= \{ a \in \mathbb{Z} : f(a) = e' \} \\ &= \{ a \in \mathbb{Z} : f(a) = [0] \} \end{aligned}$$

$\because \mathbb{Z}_4 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \} \Longrightarrow \bar{0} = \bar{4} = \bar{8} = \cdots$
$\bar{1} = \bar{5} = \bar{9} = \cdots$

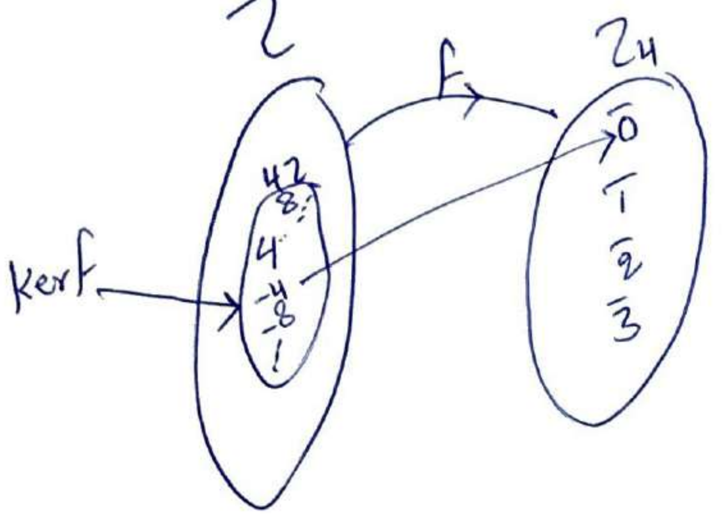
$\bar{2} = \bar{6} = \overline{10} = \cdots$

$\bar{3} = \bar{7} = \overline{11} = \cdots$

$\therefore \ker f = \{ a \in \mathbb{Z} : [a] = [0] \}$

$= \{ a \in \mathbb{Z} : a = 4k , k \in \mathbb{Z} \}$

$= 4\mathbb{Z} = \{ \ldots, -8, -4, 0, 4, 8, 12, \ldots \}$



2- Let $f : (\mathbb{R}^{+}, \cdot) \to (\mathbb{R}, +)$, s.t. $f(a) = \ln(a)$ $\forall a \in \mathbb{R}^{+}$.

IS f a homo, find the $\ker f$.?

Sol

Let $a, b \in \mathbb{R}^{+}$, s.t. $f(a) = \ln(a)$, $f(b) = \ln(b)$

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

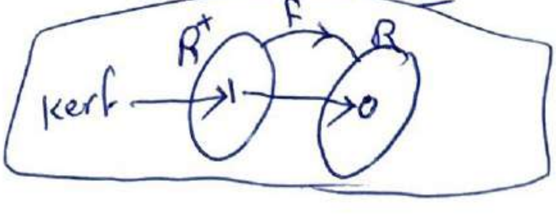
$= \ln(a) + \ln(b)$

$= f(a) + f(b)$. $\therefore f$ is a homo.

$\ker f = \{ a \in \mathbb{R}^{+} : f(a) = 0 \}$

$= \{ a \in \mathbb{R}^{+} : \ln(a) = 0 \}$ $\qquad \ln(1) = 0$ العنصر الوحيد الذي

$\ker f = \{ 1 \}$. $\boxtimes$



3- $f:(R,+) \longrightarrow (R^*,\cdot)$, s.t. $f(x)=e^x \ \forall x \in R$.

IS f a homo. and find the $\ker f$.? (H.w.)

Sol

Let $a,b \in R$, s.t. $f(a)=e^a$, $f(b)=e^b$.

$$f(a+b)=e^{a+b}$$

$$=e^a \cdot e^b$$

$$=f(a)\cdot f(b)$$. $\therefore f$ is a homo.

$$\ker f=\{a \in R : f(a)=e'\}$$

$$=\{a \in R : e^a=1\}$$ $e^a=1$ العدد الوحيد الذي هو $a=0$

$$\ker f=\underline{\underline{\{0\}}}.$$

Theorem :- 1

If f is a homo. from the group $(G,*)$ into the group $(G',\circledast)$, then:-

1- $\boxed{f(e)=e'}$, where e is the identity element of G and e' is the identity element of G'.

2- $\boxed{f(a^{-1})=f(a)^{-1}}$.

Proof: 1 :- Let $a \in G \Rightarrow f(a) \in G'$

$$\therefore f(a) * e' = f(a)$$
$$= f(a * e)$$
$$= f(a) \circledast f(e) \quad (f \text{ is a homo.})$$

$\therefore f(e) = e'$ (by cancelation law). ☒

Proof 2 :- let $a \in G \Rightarrow a^{-1} \in G$ and $f(a) \in G'$

$$f(a) * f(a^{-1}) = f(a * a^{-1}) \quad (f \text{ is a homo.})$$
$$= f(e)$$
$$= e' \Rightarrow f(a)^{-1} = f(a^{-1}).$$

$$f(a^{-1}) * f(a) = f(a^{-1} * a) \quad (f \text{ is a homo.})$$
$$= f(e)$$
$$= e' \Longrightarrow f(a^{-1}) = f(a)^{-1}. \quad ☒$$

Theorem ②:-

If f is a homo. from the group $(G,*)$ into the group $(G',\circledast)$, then $\boxed{\ker f}$ is a $\boxed{\text{normal subgroup}}$ of $(G,*)$.

Proof:

توضيح: نريد أن نبرهن أن Kerf هو زمرة جزئية ناظمية حيث اننا نبرهن أولاً انه زمرة جزئية ثم نبرهن انه ناظمية.

$\because f$ is a homo. and $f(e)=e'$

$\therefore e \in \ker f$, $\therefore \ker f \neq \phi$

Let $a,b \in \ker f$

$\Rightarrow f(a)=e'$, $f(b)=e'$. <To show $a*b^{-1} \in \ker f$>

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

$$= f(a) \circledast f(b)^{-1} \quad (f \text{ is a homo.})$$

$$= e' \circledast (e')^{-1}$$

$$= e' \circledast e' = e'$$

$\therefore a*b^{-1} \in \ker f$.

$\therefore (\ker f, *)$ is a subgroup of $(G,*)$.

Now: For normality, Let $k \in \ker f$ and $a \in G$.

<To show $a*\ker f*a^{-1} \subseteq \ker f$> حسب تعريف الناظمية

Let $a*k*a^{-1} \in a*\ker f*a^{-1}$

$$f(a*k*a^{-1}) = f(a)\circledast f(k)\circledast f(a^{-1}) \quad (f \text{ is a homo.})$$

$$= f(a)\circledast f(k)\circledast f(a)^{-1}$$

$= f(a) \circledast e' \circledast f(a)^{-1}$

$= f(a) \circledast f(a)^{-1}$

$= e'$

$\therefore a * k * a^{-1} \in \ker f$

$\therefore a * \ker f * a^{-1} \subseteq \ker f$

$\therefore (\ker f, *)$ is a normal subgroup of $(G, *)$. ⊠

Theorem ③ :-

A homo. from a group $(G, *)$ into a group $(G', \circledast)$ is one-to-one $\boxed{(1-1)}$ iff $\boxed{\ker f = \{e\}}$.

Definition:- ISomorphism (التشاكل)

A group $(G, *)$ is said to be isomorphic to group $(G', \circledast)$, denoted by $(G, *) \simeq (G', \circledast)$ if there exist:-

1- $f : G \longrightarrow G'$ is a homo.

2- f is 1-1 متباين

3- f is onto شامل

شامل متباين تشاكل

i.e. f is isomorphism $\longleftrightarrow$ f: homo. + 1-1 + onto.

Example:- Let $(Z_4, +_4)$ and $(\{1,-1,i,-i\}, \cdot)$ be two groups, where $\boxed{i^2=-1}$. Define $f: Z_4 \to \{1,-1,i,-i\}$ by:

$$f(a) = i^a \quad \forall\, a \in Z_4 .\ \text{Is } (Z_4, +_4) \cong (\{1,-1,i,-i\}, \cdot)?$$

Sol.

1- To show f is a homo.

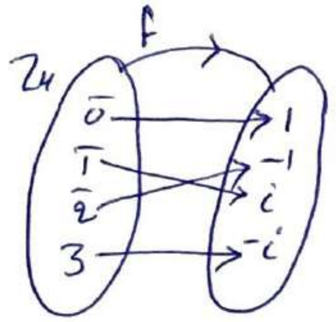
Let $a, b \in Z_4 \Rightarrow f(a) = i^a$, $f(b) = i^b$

$f(a+b) = i^{a+b} = i^a \cdot i^b = f(a) \cdot f(b)$. $\therefore f$ is a homo. $\boxtimes$

2- To show f is 1-1.

$f(\bar{1}) = i^1$, $f(\bar{2}) = i^2$, $f(\bar{3}) = i^3$, $f(\bar{0}) = i^0$

$\Rightarrow f(\bar{1}) = i$, $f(\bar{2}) = -1$, $f(\bar{3}) = -i$, $f(\bar{0}) = 1$



$\Rightarrow f$ is 1-1 متباينة

3- To show f is onto.

$f(Z_4) = \{f(a) : a \in Z_4\} = \{f(\bar{0}), f(\bar{1}), f(\bar{2}), f(\bar{3})\} = \{1, -1, i, -i\}$.

$\therefore f$ is onto. شامل

$\therefore (Z_4, +_4) \cong (\{1,-1,i,-i\}, \cdot)$. $\boxtimes$

Example:- $f: G \longrightarrow G$, defined by $f(x) = x \quad \forall x \in G$.

IS $G \simeq G$?

Sol:

1- To show f is a homo.

Let $x, y \in G$, s.t. $f(x) = x$, $f(y) = y$.

$f(xy) = xy = f(x) \cdot f(y) \Rightarrow f$ is a homo.

2- To show f is 1-1.

Let $f(x) = f(y)$

$\Rightarrow \quad x = y \Longrightarrow f$ is 1-1.

3- To show f is onto.

Let $y \in G$

$\Rightarrow f(y) = y \Longrightarrow G \simeq G$. $\boxtimes$.

Example: Let $\varphi: (\mathbb{Z}_8, +_8) \longrightarrow (\{1, -1, i, -i\}, \cdot)$. defined by $\varphi(n) = i^n$, is φ a homo., Find the $\ker \varphi$, IS φ 1-1, onto?

Sol:

(1) Let $\bar{n}, \bar{m} \in \mathbb{Z}_8 \Rightarrow \varphi(\bar{n}) = i^n$, $\varphi(\bar{m}) = i^m$

$\varphi(\bar{n} +_8 \bar{m}) = i^{n+m} = i^n \cdot i^m = \varphi(i^n) \cdot \varphi(i^m)$ $\therefore \varphi$ is a homo.

(2) $\ker \varphi = \{ \bar{n} \in \mathbb{Z}_8 : \varphi(\bar{n}) = 1 \}$

$= \{ \bar{n} \in \mathbb{Z}_8 : i^n = 1 \}$

$= \{ \bar{0}, \bar{4} \}$. $\therefore \varphi$ is not 1-1. ليست متباينة

③ IS ϕ is onto

Now: $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \cdots \bar{7}\}$

$\phi(\bar{4}) = \phi(\bar{0}) = i^0 = 1$

$\phi(\bar{5}) = \phi(\bar{1}) = i^1 = i$

$\phi(\bar{6}) = \phi(\bar{2}) = i^2 = -1$

$\phi(\bar{7}) = \phi(\bar{3}) = i^3 = -i$

نلاحظ عناصر المجال المقابل جميعها موجودة $\{1, -1, i, -i\}$

$\therefore \phi$ is onto.

أي أنه: لكل عنصر y في G يوجد عنصر مثل x في $\mathbb{Z}_8$ بحيث أن $\phi(x) = y$.

Example:- $f : (\mathbb{Z}, +) \to (\mathbb{Z}_e, +)$, s.t. $f(a) = 2a \ \forall a \in \mathbb{Z}$.

Prove that f is an isomorphism.?

Sol:

① Let $a, b \in \mathbb{Z}$, s.t. $f(a) = 2a$, $f(b) = 2b$.

$f(a+b) = 2(a+b) = 2a + 2b = f(a) + f(b)$. $\therefore f$ is homo.

② $\ker f = \{a \in \mathbb{Z} : f(a) = 0\}$

$= \{a \in \mathbb{Z} : 2a = 0\} \Rightarrow \ker f = \{0\}$ $\therefore f$ is 1-1.

③ f is onto?

Let $x \in \mathbb{Z}$, $\boxed{\mathbb{Z}_e = \{2a, a \in \mathbb{Z}\}}$

$\Rightarrow f(x) = 2a$

$\Rightarrow 2x = 2a$

$\Rightarrow x = a \Rightarrow f(a) = 2a$

$\Rightarrow f$ is onto. $\Rightarrow \mathbb{Z} \simeq \mathbb{Z}_e$. $\boxtimes$

Example:- Let $f:(\mathbb{R}^*,\cdot) \longrightarrow (\mathbb{R}^+,\cdot)$, defined by

$f(x)=|x|$, $\forall x\in \mathbb{R}^*$. Is f an isomorphism

Sol//

1- Let $x,y \in \mathbb{R}^*$, s.t. $f(x)=|x|$, $f(y)=|y|$

$$f(x\cdot y)=|x\cdot y| = |x|\cdot|y|$$
$$=f(x)\cdot f(y) \Rightarrow f \text{ is a homo.}$$

2- $\ker f = \{x\in \mathbb{R}^* : f(x)=e'\}$

$= \{x \in \mathbb{R}^* : |x|=1\}$, $\boxed{|x|=1 \Rightarrow x=\mp 1}$

$=\{1,-1\}$

$\therefore f$ is not 1-1.

$\therefore f$ is not isomor. $\boxtimes$.

Is f an onto?

Let $y\in \mathbb{R}^+ \Longrightarrow y>0$

- يجب ان نحصل على عنصر في المجال صورته y

$$\left.\begin{array}{l} x\in \mathbb{R}^*,\ f(x)=y \\ |x|=y \\ \Rightarrow x=\mp y \\ y\in \mathbb{R}^*,\ f(y)=|y|=y \\ \text{عدد موجب} \\ -y\in \mathbb{R}^*,\ f(-y)=|-y|=y \\ \text{ايضاً عدد موجب} \end{array}\right\} \Rightarrow f \text{ is onto.}$$

Definition:- Let $(G,*)$ and $(G',\circ)$ are groups, and $f: G \longrightarrow G'$ be homomorphism, then:-

1- f is called $\boxed{\text{monommorphism}}$ iff f is $\boxed{1-1}$.

2- f is called $\boxed{\text{epimorphism}}$ iff f is $\boxed{\text{onto}}$.

3- f is called $\boxed{\text{isomorphism}}$ iff f is $\boxed{1-1}$ and $\boxed{\text{onto}}$.

تكافؤ

4- f is called $\boxed{\text{endomorphism}}$ iff $\boxed{G = G'}$.

5- f is called $\boxed{\text{automorphism}}$ iff f is $\boxed{\text{isomorphism}}$ and $\boxed{G = G'}$ $\boxed{(1\text{-}1, \text{onto}, \text{homo}, G = G')}$.

وحدة حبايب
هم زوا السكاريك

Example:- $f: \mathbb{Z} \longrightarrow \mathbb{Z}_3$, s.t. $f(a) = [a]$ or $f(a) = \bar{a}$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$f(0) = [0]$ or $\bar{0}$

$f(1) = \bar{1}$

$f(2) = \bar{2}$

$f(3) = \bar{0} \Rightarrow 3 \neq 0$

$f(4) = \bar{1} \Rightarrow 4 \neq 1$

$f(5) = \bar{2} \Rightarrow 5 \neq 2$

$\vdots$

وهكذا

$\therefore$ Therefore f is not 1-1, So f is not monommorphism

2- For all $\bar{a} \in Z_3$, $\exists a \in Z \ni f(a) = \bar{a}$. hence f is onto.

hence f is $\boxed{\text{epimorphism}}$

3- hence f is onto but not 1-1, (hence f is not isomorphism).

4- hence f is not endomorphism.

5- f is not automorphism f is not (1-1), (not isomo),

since $G \neq G'$.

types of homomorphism

مهمة جداً جداً

f	types	Relation	
$G \to G'$	homomorphism	$f(a*b) = f(a) \circ f(b)$	تشاكل
$G \to G'$	monomorphism	f is $\boxed{\text{homo}}$ + $\boxed{1-1}$	تشاكل + شامل
$G \to G'$	epimorphism	f is $\boxed{\text{homo.}}$ + $\boxed{\text{onto}}$	تشاكل + متباين
$G \to G'$	isomorphism (تماثل)	f is $\boxed{\text{homo.}}$ + $\boxed{1-1}$ + $\boxed{\text{onto}}$	التماثل = تشاكل + شامل + متباين
$\boxed{G \to G}$	endomorphism	f is $\boxed{\text{homo.}}$ + $\boxed{G = G'}$	تشاكل + الزمرة نفسها
	automorphism	f is $\boxed{\text{isomorphism}}$ + $\boxed{\text{endo morphism}}$ Or f is $\boxed{\text{homo.}}$ + $\boxed{1-1}$ + $\boxed{\text{onto}}$ + $\boxed{G = G'}$	

Example :- Let $f : (G, *) \to (R^*, \cdot)$, s.t.

مع $\boxed{G = R - \{1\} \ , \ a * b = a + b + ab,}$

$f(a) = a + 1 \ , \ \forall a \in G$. Show that f is homo,

Find $\ker f$, and if f is 1-1 , onto.?

Soul

(1) Let $a, b \in G$ s.t. $f(a) = a+1$, $f(b) = b+1$

$$f(a * b) = f(a + b + ab) = a + b + ab + 1 \quad \cdots (1)$$

$$f(a) \cdot f(b) = (a+1) \cdot (b+1)$$

$$= ab + a + b + 1 \quad \cdots (2)$$

$$1 = 2 \implies f \text{ is homo.}$$

(2) $\ker f = \{a \in G : f(a) = e'\}$

$= \{a \in G : \underline{a+1} = 1\} = \underline{\underline{\{0\}}} = e$ of G العنصر المحايد لـ

من الفصل الأول

$\therefore f$ is 1-1.

or Let $f(a) = f(b)$

$\implies a + 1 = b + 1 \implies a = b \Big\}$ 1-1 طريقة ثانية لـ

(3) لإثبات أن f شاملة نلاحظ أن المجال مستثنى منه (1)

والمجال المقابل مستثنى منه $\{0\}$.

لكي تكون شاملة نختار عنصر من المجال المقابل بحيث نلقى عنصر ،

من المجال صورته هذا العنصر أي أن :

$x \in G : \quad f(x) = y \quad , y \in R^*$

$\Rightarrow x+1=y \Rightarrow \boxed{x=y-1}$

نلاحظ أن $y \in R^*$ ماعدا الصفر، فإن المجال هو جميع الأعداد R ماعدا $\{1\}$

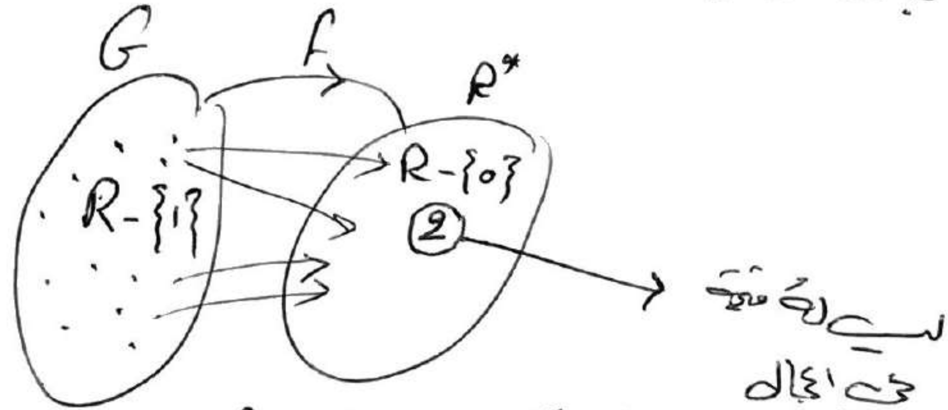
أي أن $x \neq 1$.

أما إذا كان $x=1$ وظهر لنا قيمة $y=0$ فليس هناك مشكلة

أما إذا كان $x=1$ وظهر لنا قيمة y وهي y أي

$x=y-1 \Rightarrow 1=y-1 \Rightarrow \boxed{y=2}$

ظهر لنا أن القيمة 2 في المجال المقابل ليس لها عنصر في المجال ومعنى هذا أن الدالة ليست شاملة



لذا تصبح الدالة f ليست شاملة

not onto. ☒

Example:- Let $(G,*)$ be a group and a is a fixed element in G. Define a function:

$$f^a : G \to G \text{ by: } f^a(x) = a * x * a^{-1} \quad \forall x \in G.$$

Show that $(G,*)$ isomorphic to $(G,*)$.

Sol:

1- Let $x, y \in G$, s.t. $f^a(x) = a * x * a^{-1}$, $f^a(y) = a * y * a^{-1}$

$$\begin{aligned} f^a(x*y) &= a * (x*y) * a^{-1} \\ &= a * (x * e * y) * a^{-1} \\ &= a * (x * a^{-1} * a * y) * a^{-1} \\ &= (a * x * a^{-1}) * (a * y * a^{-1}) \\ &= f^a(x) * f^a(y). \Rightarrow f^a \text{ is homo.} \end{aligned}$$

2- Let $f^a(x) = f^a(y)$, $\forall x, y \in G$.

$$\begin{aligned} &\Rightarrow a * x * a^{-1} = a * y * a^{-1} \\ &\Rightarrow a^{-1} * a * x * a^{-1} = a^{-1} * a * y * a^{-1} \\ &\Rightarrow e * x * a^{-1} = e * y * a^{-1} \\ &\Rightarrow x * a^{-1} * a = y * a^{-1} * a \\ &\Rightarrow x * e = y * e \Rightarrow x = y \Rightarrow f^a \text{ is } \underline{1-1} \end{aligned}$$

3- $f^a(G) = \{ f^a(x) : \forall x \in G \}$

$$= \{ a * x * a^{-1} : x \in G \} = G.$$

$\therefore f^a$ is onto $\Longrightarrow (G,*) \simeq (G,*)$. $\boxtimes$

Example:- prove that the group $(\mathbb{Z},+)$ is not isomorphic to the group $(\mathbb{Q}^*,\cdot)$, i.e. $(\mathbb{Z},+) \not\cong (\mathbb{Q}^*,\cdot)$.

Prove:- Let $(\mathbb{Z},+) \cong (\mathbb{Q}^*,\cdot)$ — لكي نبرهن أنه ليست تماثل نبرهن بالتناقض أي

$\therefore \exists f : \mathbb{Z} \to \mathbb{Q}^*$ s.t. — ∴ يوجد دالة من $\mathbb{Z}$ الى $\mathbb{Q}^*$

f is a homo. onto and 1-1 — وهذه الدالة هي تشاكل ومتباينة وشاملة

$\because -1 \in \mathbb{Q}^*$ and f is onto — وبما أن (-1) ينتمي الى $\mathbb{Q}^*$ والدالة شاملة

$\therefore \exists x \in \mathbb{Z}$, s.t. $f(x) = -1$ — اذن يوجد x ينتمي الى $\mathbb{Z}$ بحيث أن $f(x)=-1$

$$\Rightarrow f(2x) = f(x+x)$$
$$= f(x)\cdot f(x) \quad (f \text{ is homo.})$$
$$= (-1)\cdot(-1)$$
$$= \underline{\underline{1}}$$

لكن $f(0)=1$ لأن الدالة تشاكل ومتباينة

But $f(0)=1$ (because f is a homo and $f(e)=e'$).

$\because 1$ is unique $\Rightarrow f(2x) = f(0)$ — وبما أن 1 عنصر وحيد

$\because f$ is 1-1 $\Rightarrow 2x = 0 \Rightarrow x = 0$ — $\Leftarrow \boxed{x=0}$

So $f(0)=-1$, $f(0)=1$, C! تناقض

because f is 1-1.

$\therefore (\mathbb{Z},+) \not\cong (\mathbb{Q}^*,\cdot)$. $\boxtimes$

Example:- prove that the group $(Z,+)$ is not isomorphic to the group $(Q^*,\cdot)$, i.e. $(Z,+) \not\cong (Q^*,\cdot)$.

Prove:- Let $(Z,+) \cong (Q^*,\cdot)$ لكي نبرهن أنها ليست تماثل نبرهن التناقض أي

$\therefore \exists f: Z \to Q^*$ s.t. ∴ يوجد دالة من Z الى Q^*

f is a homo. onto and 1-1 وهذه الدالة هي تشاكل ومتباينة وشاملة

$\because -1 \in Q^*$ and f is onto وبما أن (-1) ينتمي الى Q^* والدالة شاملة

$\therefore \exists x \in Z$, s.t. $f(x) = -1$ اذن يوجد x ينتمي الى Z بحيث أن $f(x) = -1$

$$\Rightarrow f(2x) = f(x+x)$$

$$= f(x) \cdot f(x) \quad (f \text{ is homo.})$$

$$= (-1) \cdot (-1)$$

$$= \underline{\underline{1}}$$

لكن $f(0) = 1$ لأن الدالة تشاكل ومتباينة

But $f(0) = 1$ (because f is a homo and $f(e) = e'$).

$\because 1$ is unique $\Rightarrow f(2x) = f(0)$ وبما أن 1 عنصر وحيد

$\because f$ is 1-1 $\Rightarrow 2x = 0 \Rightarrow x = 0$ $\Leftarrow$ $\boxed{x=0}$

So $f(0) = -1$, $f(0) = 1$, C! تناقض

because f is 1-1.

$\therefore (Z,+) \not\cong (Q^*,\cdot)$. $\boxtimes$

Example:- Let $f:(\mathbb{Z},+)\to(\mathbb{R}^*,\cdot)$ defined by:-

$$f(x)=\begin{cases}1 & x\in \mathbb{Z}_e\\ -1 & x\in \mathbb{Z}_o\end{cases}$$

① Show that f is a homo.

② Find the $\mathrm{Ker}(f)$ and $f(\mathbb{Z})$.

Sol/

Let $a,b\in\mathbb{Z}$ s.t. $f(a)=\begin{cases}1 & a\in\mathbb{Z}_e\\ -1 & a\in\mathbb{Z}_o\end{cases}$,

$$f(b)=\begin{cases}1 & b\in\mathbb{Z}_e\\ -1 & b\in\mathbb{Z}_o\end{cases}$$

Now:-

(i) If a,b are both even, then $a+b$ is even

$f(a+b)=1=1\cdot1=f(a)\cdot f(b)$.

(ii) If a,b are both odd, then $a+b$ is even

$f(a+b)=1=(-1)\cdot(-1)=f(a)\cdot f(b)$.

(iii) If one of them is even and the other is odd so that we suppose a is even and b is odd.

$f(a+b)=-1$ -- ①

$f(a)\cdot f(b)=1\cdot(-1)=-1$ --- ②

$\therefore f(a+b)=f(a)\cdot f(b)\Rightarrow f$ is homo.

2- $Ker(f) = \{a \in Z : f(a) = 1\}$

$= \{a \in Z : a \text{ is even} = 1\} = Ze.$

$f(Z) = \{1, -1\}.$

$\cdot$	1	-1
1	1	-1
-1	-1	1

تحقق النص

Theorem:-

Let $(H,*)$ be a normal subgroup of the group $(G,*)$. Then the mapping $\boxed{nat_H : G \to G/H}$ defined by:- $\boxed{nat_H(a) = a * H}$, is a homomorphism from $(G,*)$ onto the quotient group $(G/H, \otimes)$; the $\boxed{Ker(nat_H) = H}$.

ملاحظة:-
الزمرة الجزئية الناظمية $(H,*)$ من الزمرة $(G,*)$ والدالة
المعرفة بالنص التالي $nat_H : G \to G/H$ ، $nat_H(a) = a * H$ هي تشاكل من $(G,*)$ الى زمرة القسمة $(G/H, \otimes)$ وأن النواة $\boxed{Ker(nat_H) = H}$ هي H نفسها.

Theorem:

(*) مهمة منها النص

1- Every finite cyclic group of order $n>0$ is isomorphic to $(Z_n, +_n)$

2- Every infinite cyclic group is isomorphic to $(Z, +)$.

ملاحظة :-

١- أي زمرة دائرية منتهية ذات رتبة $n>0$ تكون متماثل مع الزمرة الاعتيادية $(Z_n, +_n)$.

٢- اي زمرة دائرية غير منتهية تكون متماثلة مع زمرة الأعداد الصحيحة $(Z, +)$.

Corollary:- Any two cyclic groups of the same order are isomorphic.

نتيجة :- أي زمرتين دائريتين لهما نفس الرتبة يكونان متماثلتان.

Define:- Let $(G, *)$ be a group and $a \in G$, define a function $f_a : G \to G$ by: $f_a(x) = a * x$ for all $x \in G$, then F_G is the set $F_G = \{f_a : a \in G\}$.

Remark:- $(F_G, \circ)$ is a group, where $\circ$ is the composition of function.

Proof:- ① Let $f_a, f_b \in F_G$, $a, b \in G$. <To Prove $f_a \circ f_b \in F_G$>.

Let $x \in G$

$$(f_a \circ f_b)(x) = f_a(f_b(x))$$
$$= f_a(b * x)$$
$$= a * b * x$$
$$= (a * b) * x = f_{a*b}(x) \Rightarrow f_a \circ f_b = f_{a*b}$$

$\because a, b \in G \Rightarrow a * b \in G$ (G is a group).

$\therefore f_{a*b} \in F_G$.

$\therefore F_G$ is closed under $\circ$.

2- Let $f_a, f_b, f_w \in F_G$, $a, b, w \in G$.

Let $x \in G$.

$$((f_a \circ f_b) \circ f_w)(x) = (f_a \circ f_b)(f_w(x))$$
$$= f_{a*b}(w * x)$$
$$= (a * b) * (w * x)$$

$= a * ((b * w) * x)$

$= f_a((b * w)(x))$

$= f_a((f_b \circ f_w)(x))$

$= (f_a \circ (f_b \circ f_w))(x)$

$\Rightarrow (f_a \circ f_b) \circ f_w = f_a \circ (f_b \circ f_w)$.

$\therefore \circ$ is associative on F_G.

3- $\because e \in G \Rightarrow F_e \in F_G$. <To prove $f_e \circ f_a = f_a \circ f_e = f_a$>.

Let $x \in G$.

$(f_e \circ f_a)(x) = f_e(f_a(x)) = f_e(a * x) = e * (a * x)$

$= (e * a) * x$

$= (a * e) * x$

$= (a * x) = f_a(x)$.

$\therefore f_e \circ f_a = f_a * f_e = f_a$ (f_e is the identity element of F_G):

4- Let $f_a \in F_G \Rightarrow a \in G,\ a^{-1} \in G \Rightarrow f_{a^{-1}} \in F_G$.

Let $x \in G$.

$(f_a \circ f_{a^{-1}})(x) = f_a(f_{a^{-1}}(x))$

$= f_a(a^{-1} * x)$

$= a * (a^{-1} * x)$

$= (a * a^{-1}) * x$

$= e * x$

$= f_e(x) \longrightarrow$

$\therefore (f_a \circ f_{a^{-1}})(x) = f_e(x)$

$(f_{a^{-1}} \circ f_a)(x) = f_{a^{-1}}(f_a(x))$

$= f_{a^{-1}}(a * x)$

$= a^{-1} * (a * x)$

$= (a^{-1} * a) * x$

$= e * x = f_e(x)$.

$\therefore f^{-1}(a) = f_{a^{-1}}$.

There fore $(F_G, \circ)$ is a group. $\boxtimes$

Theorem :- "Cayley's Theorem"

مهمة جداً
مقرر النص والبرهان

Let $(G,*)$ be a group, then:

$$(G,*) \cong (F_G, \circ), \text{ where } F_G = \{f_a : a \in G\}$$

$$f_a : G \to G \text{ s.t. } f_a(x) = a * x \quad \forall x \in G.$$

Proof:- Let $g : G \to F_G$ defined by

$$g(a) = f_a \quad \forall a \in G.$$

1- Let $a, b \in G$.

$g(a*b) = f_{a*b} = f_a \circ f_b = g(a) \circ g(b)$

$\therefore$ g is a homo.

2- Let $g(a) = g(b)$ $\forall a, b \in G$

$\Rightarrow f_a = f_b$

$\Rightarrow f_a(x) = f_b(x) \quad \forall x \in G$

$\Rightarrow a * x = b * x$ (by cancellation law).

$\Rightarrow a = b \Longrightarrow \therefore g$ is 1-1.

3- $g(G) = \{g(a) : a \in G\} = \{f_a : a \in G\} = F_G$.

$\therefore$ g is onto.

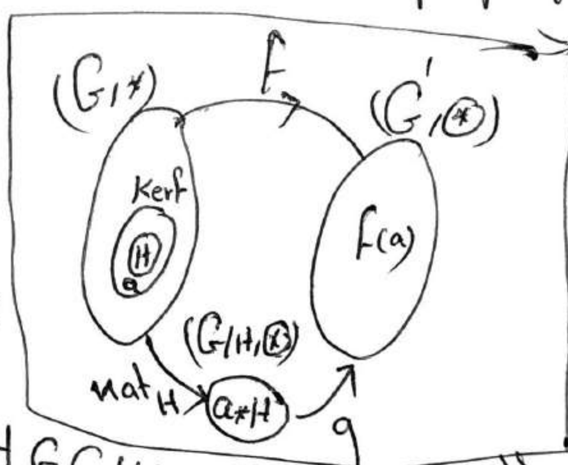
$\therefore (G,*) \cong (F_G, \circ)$. $\boxtimes$

Theorem (2): Factorization of Homomorphism

حفظ النص والبرهان

Let f be a homo. from the group $(G,*)$ onto the group $(G',\circledast)$, and let $(H,*)$ be a normal subgroup of $(G,*)$, such that $H \subseteq \ker f$. Then there exists a unique homo. $g : G/H \to G'$ with property that $f = g \circ nat_H$.

Proof:-



توضيح الطريقة

Let $g : G/H \to G'$ defined by:

$g(a*H) = f(a) \quad \forall a \in G,\ a*H \in G/H.$

Or: توضيح أكثر

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "nat_H"'] & & G' = f(G) \\ & G/H \arrow[ur, "g"'] & \end{tikzcd}$$

<To show g is well defined function>.

Let $a*H,\ b*H \in G/H$ s.t.

$a*H = b*H$

$\Rightarrow a^{-1}*b \in H$

$\because H \subseteq \ker f$

$\Rightarrow f(a^{-1}*b) = e'$, ($e'$ is the identity in G')

$\Rightarrow f(a^{-1}) \circledast f(b) = e'$

$\Rightarrow f(a)^{-1} \circledast f(b) = e'$

$\Rightarrow f(a) = f(b)$

$\Rightarrow g(a*H) = g(b*H)$

$\therefore g$ is well defined function.

Now : <To prove g is a homo.>

Let $a*H, b*H \in G/H \quad \forall a, b \in G$.

$$g((a*H)*(b*H)) = g((a*b)*H)$$
$$= f(a*b)$$
$$= f(a) \circledast f(b)$$
$$= g(a*H) \circledast g(b*H).$$

$\therefore g$ is a homo.

<To prove $f = g \circ nat_H$>

Let $a \in G$.

$$f(a) = g(a*H)$$
$$= g(nat_H(a))$$
$$= (g \circ nat_H)(a)$$

$\therefore f = g \circ nat_H$.

<To Prove g is Unique>

Let $h : G/H \to G$ s.t. $f = h \circ nat_H$

Let $a * H \in G/H$

$$\Rightarrow h(a*H) = h(nat_H(a))$$
$$= (h \circ nat_H)(a)$$
$$= f(a)$$
$$= (g \circ nat_H)(a)$$
$$= g(nat_H(a))$$
$$= g(a*H)$$

$\therefore g = h \Rightarrow g$ is Unique. $\boxtimes$.

Corollary:- 1- $g: G/H \longrightarrow G$ is onto.

2- If $\ker f = H$, then g is 1-1.

Proof ①:- $g(G/H) = \{ g(a*H) : a*H \in G/H, a \in G \}$

$= \{ f(a) : a \in G \}$

$= f(G) = G'$

$\therefore g$ is onto. $\boxtimes$

Proof ②:-

$\ker g = \{ a*H : g(a*H) = e' \}$

$= \{ a*H : f(a) = e' \}$

$= \{ a*H : a \in \ker f \}$

$= \{ a*H : a \in H \}$

$= \{ H \} = \{ e*H \}.$

$\therefore g$ is 1-1. $\boxtimes$.

Theorem 3 :- Fundamental Homomorphism Theorem

If f is a homo. from the group $(G,*)$ onto the group $(G',\circledast)$. Then $(G/\ker f, \otimes) \simeq (G', \circledast)$.

Proof:- Let $g : G/\ker f \to G'$ defined by:

$$g(a*\ker f) = f(a) \quad \forall a \in G,\ a*\ker f \in G/\ker f.$$

1- <To prove g is well define.>

Let $a*\ker f, b*\ker f \in G/\ker f$ s.t.

$a*\ker f = b*\ker f$.

$\Rightarrow a^{-1}*b \in \ker f$

$\Rightarrow f(a^{-1}*b) = e'$ (e' is the identity of G')

$\Rightarrow f(a^{-1}) \circledast f(b) = e'$

$\Rightarrow f(a)^{-1} \circledast f(b) = e' \Rightarrow f(a) = f(b) \Rightarrow g(a*\ker f) = g(b*\ker f)$

$\Rightarrow g$ is well define.

2- <To show g is a homo.>.

Let $a*\ker f, b*\ker f \in G/\ker f$

$\Rightarrow g(a*\ker f \otimes b*\ker f) = g((a*b)*\ker f)$

$= f(a*b)$

$= f(a) \circledast f(b) \Rightarrow g(a*\ker f) = g(b*\ker f)$

$\therefore g$ is a homo.

3- <To prove g is 1-1>.

Let $a*\ker f, b*\ker f \in G/\ker f$ s.t.

$g(a*\ker f) = g(b*\ker f)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow f(a) \circledast f(b)^{-1} = e'$

$\Rightarrow f(a) \circledast f(b^{-1}) = e'$

$\Rightarrow f(a*b^{-1}) = e'$

$\Rightarrow a*b^{-1} \in \ker f$

$\Rightarrow a*\ker f = b*\ker f$.

$\therefore g$ is 1-1.

4- <To prove g is onto.>.

$$g(G/\ker f) = \{g(a*\ker f) : a*\ker f \in G/\ker f, a \in G\}$$
$$= \{f(a) : a \in G\} = G'.$$

$\therefore g$ is onto.

$\therefore g$ is isomorphism.

$\therefore (G/\ker f, \circledast) \cong (G', \circledast)$. $\boxtimes$

4

Theorem: Correspondence Theorem

Let f be a homo. from the group $(G,*)$ onto the group $(G',\circledast)$. Then there is an one-to-one correspondence between the subgroup $(H,*)$ of $(G,*)$ s.t. $Ker f \subseteq H$ and the set of all subgroup $(H',\circledast)$ of $(G',\circledast)$.

Proof:- Let $(H',\circledast)$ be a subgp of $(G',\circledast)$.

we must take $H = f^{-1}(H')$ with $Ker f \subseteq H'$, s.t. $f(H) = H'$

$\because f$ is a homo. $\Rightarrow (f^{-1}(H'),*)$ is a subgroup of $(G,*)$, also $Ker f = f^{-1}(e') \subseteq f^{-1}(H')$.

$\because f$ is onto $\Rightarrow f(f^{-1}(H')) = H'$

suppose that $(H_1,*)$ and $(H_2,*)$ are subgroups of $(G,*)$ with $Ker f \subseteq H_1$ and $Ker f \subseteq H_2$, and
$f(H_1) = f(H_2)$

By using the Lemma: (If $(H,*)$ is any subgroup of $(G,*)$ s.t. $Ker f \subseteq H$, then $H = f^{-1}(f(H))$.) we get.

$H_1 = f^{-1}(f(H_1)) = f^{-1}(f(H_2)) = H_2$. $\boxtimes$

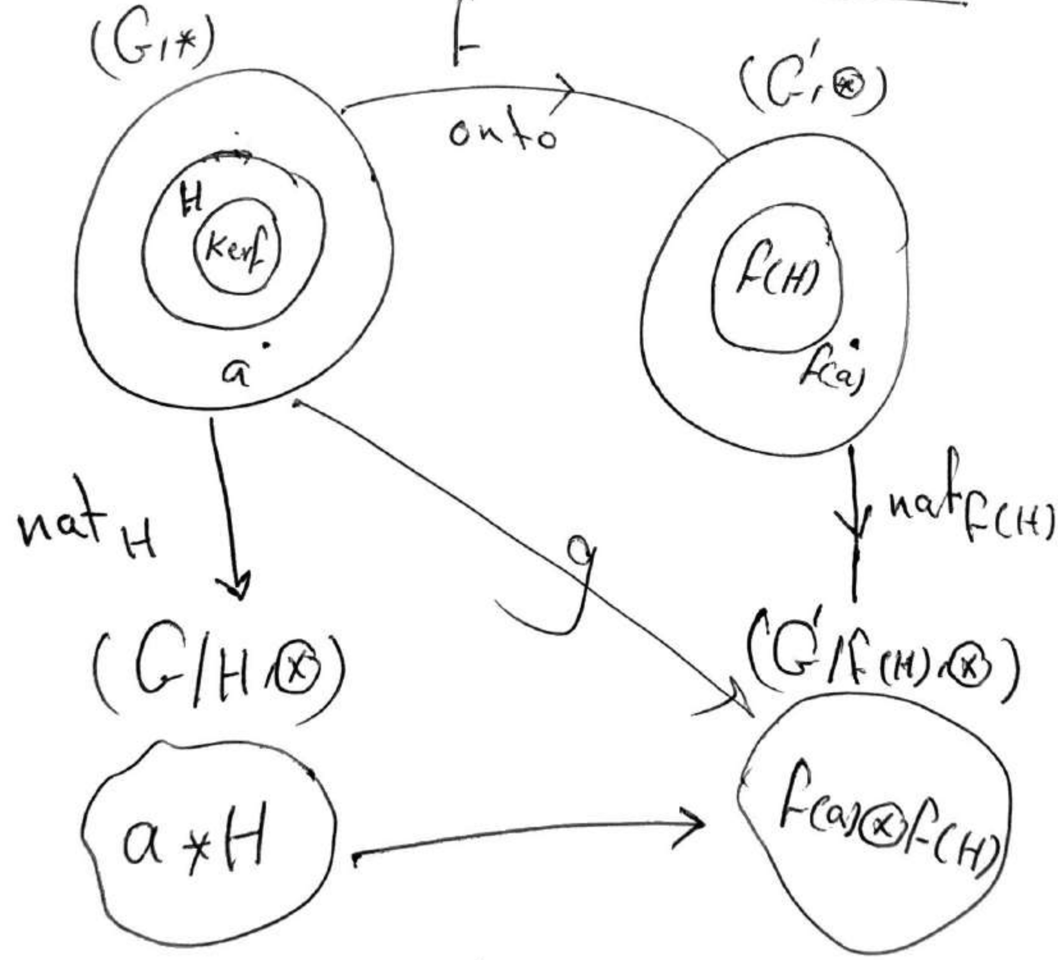
Theorem ⑤ :-

ضغط الخطأ على الصفر فقط

Let f be a homo. from the group $(G, *)$ onto the group $(G', \circledast)$ and let $(H, *)$ be a normal subgroup of $(G, *)$. If $\ker f \subseteq H$, then

$$(G/H, \otimes) \simeq (G'/f(H), \otimes).$$

الإعطاء



مقطع الخطأ على المبرهنة

5

Theorem:

If $(H,*)$ and $(K,*)$ are subgroups of the group $(G,*)$, with $(K,*)$ normal in $(G,*)$, then

$$\left(\frac{H}{H\cap K}, \otimes\right) \simeq \left(\frac{H*K}{K}, \otimes'\right)$$

$$\begin{tikzcd}
H \arrow[r, "I_H"] \arrow[dr, "\alpha"'] & H*K \arrow[d, "nat_K"] \\
 & H*K/K
\end{tikzcd}$$

I_H : is the inclusion map from H onto $H*K$ because: $H \subseteq H*K$ and nat_K is the natural map from $H*K$ onto $H*K/K$.

$\alpha : H \longrightarrow H*K/K$

Fundamental theorem

تطبيقات المبرهنة الأساسية

Theorem ③: If f is a homo. from the group $(G,*)$ onto group $(G',\circledast)$. Then:

$$(G/\ker f, \otimes) \simeq (G', \circledast).$$

المبرهنة الأساسية للتشاكل :-

اذا كان $f:(G,*)\to(G',\circledast)$ تشاكل زمري شامل فأن :-

$$(G/\ker f, \otimes) \simeq (G', \circledast).$$

تطبيقات على المبرهنة :-

Example:- Let $f:(Q^*,\cdot)\to(Q^+,\cdot)$. s.t. $f(x)=|x|$. Show that f is a homo. and applay the Fundamental theorem.

Proof

Let $a,b\in Q^*$ s.t. $f(a)=|a|$, $f(b)=|b|$

① $f(a\cdot b)=|a\cdot b|=|a|\cdot|b|=f(a)\cdot f(b)$. $\therefore f$ is homo.

② $f(Q^*)=\{f(a): a\in Q^*\}$

$=\{|a| : a\in Q^*\}$

$=Q^+$ $\therefore$ f is onto.

③ $\ker(f)=\{a\in Q^*: f(a)=1\}$

$=\{a\in Q^*: |a|=1\}=\{1,-1\}$

عدد عناصر مجموعة kerf هو 2 والتي تكافئ $\boxed{Z_2}$

نطبق المبرهنة الرئيسية

$$(G/\ker f, \otimes) \simeq (G', \circledast)$$

$$\Rightarrow (Q^*/\{1,-1\}, \otimes) \simeq (Q^+, \cdot)$$

$$\Rightarrow \boxed{Q^*/\{1,-1\} \simeq Q^+} \quad \text{or} \quad \boxed{Q^*/Z_2 \simeq Q^+}$$

على الشكل الصحيح.

Example: (2)

$f: Z_{12} \longrightarrow Z_3$, $f(n)=n$. نفس المطلب السابق

Sol

Let $a,b \in Z_{12}$ s.t. $f(a)=a$, $f(b)=b$

(1) $f(a+b)=a+b=f(a)+f(b) \Rightarrow f$ is a homo.

(2) $Z_3=\{\bar{0},\bar{1},\bar{2}\}$, $f(0)=0$, $f(1)=1$, $f(2)=2$

$\Rightarrow f$ is onto.

(3) $\ker f=\{n\in Z_{12} : f(n)=0\}$

$=\{n\in Z_{12} : n=0\}$

$=\{0,3,6,9\}$ ⇐ (*) عدد عناصر الـ kerf مساوية للـ (4) أربعة

$|\ker f|=4$ وهنا عائدة Z_4 لأنه عدد العناصر 4

(4) حسب (*) لتطبيق المبرهنة $\ker f \simeq Z_4$

$(Z_{12}/\{0,3,6,9\}, \otimes) \simeq (Z_3, +_3)$

أي $(Z_{12}/\langle 3\rangle, \otimes) \simeq (Z_3, +_3)$ or $(Z_{12}/Z_4) \simeq (Z_3)$.

Cayles theorem تطبيقات مبرهنة كلي

Theorem: G any group $\Rightarrow G \simeq F_G$

$F_G = \{f_a, f_e, \dots\}$, $f_a(x) = a * x$

Example:- Let $(Z_5^*, \cdot_5)$, Find a subgroup in $S_4 \simeq Z_5^*$

Soul

$Z_5^* = \{1, 2, 3, 4\}$

$f_1 : f_1(1) = 1\cdot 1$, $f_1(2) = 1\cdot 2$, $f_1(3) = 1\cdot 3$, $f_1(4) = 1\cdot 4$

$f_1 = (1)(2)(3)(4) = \underline{\underline{(1)}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$f_2 : f_2(1) = 2\cdot 1 = 2$, $f_2(2) = 2\cdot 2 = 4$, $f_2(3) = 1$, $f_2(4) = 3$

$f_2 = (1\ 2\ 4\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

$f_3 : f_3(1) = 3\cdot 1 = 3$, $f_3(2) = 3\cdot 2 = 1$, $f_3(3) = 4$, $f_3(4) = 2$

$f_3 = (1\ 3\ 4\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

$f_4 : f_4(1) = 4\cdot 1 = 4$, $f_4(2) = 4\cdot 2 = 3$, $f_4(3) = 2$, $f_4(4) = 1$

$f_4 = (1\ 4)(2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

$\therefore H = \{f_1, f_2, f_3, f_4\} \subseteq S_4$

$H \simeq Z_5^*$. $\boxtimes$

Jorden-Holder Theorem

Define:- A chain for a group $(G,*)$ is a finite sequence of subgroups of $(G,*)$:

$$G = H_0 \supset H_1 \supset H_2 \cdots \supset H_{n-1} \supset H_n = \{e\}$$

descending with proper inclusions from G to $\{e\}$.
تنازلي

⊛ The Length of the chain is the integer $\underline{\underline{n}}$، طول السلسلة

⊛ The normal chain: The chain for $(G,*)$ is called normal chain if all subgroups $(H_i,*)$ are normal.

Example:- The following are normal chain for the comm. group $(Z_{24}, +_{24})$:-

1- $Z_{24} \supset \langle \bar{2} \rangle \supset \langle \bar{4} \rangle \supset \langle \bar{8} \rangle \supset \langle \bar{0} \rangle$ of the length 4//.

2- $Z_{24} \supset \langle \bar{2} \rangle \supset \langle \bar{4} \rangle \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$ " " " 4//.

3- $Z_{24} \supset \langle \bar{2} \rangle \supset \langle \bar{6} \rangle \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$ " " " 4//.

4- $Z_{24} \supset \langle \bar{3} \rangle \supset \langle \bar{6} \rangle \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$ " " " 4//

5- $Z_{24} \supset \langle \bar{4} \rangle \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$

6- $Z_{24} \supset \langle \bar{2} \rangle \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$ " " " 3//

7- $Z_{24} \supset \langle \bar{8} \rangle \supset \langle \bar{0} \rangle$, 8- $Z_{24} \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$ " " " 3// 2

توضيح :-

$$\mathbb{Z}_{24} = \{\bar{0}, \bar{1}, \ldots, \overline{23}\}$$

1 . 24 — trivial Subgp

2 - 12   3 . 8   4 . 6 — Proper Subgps

$\langle \bar{0} \rangle = \{0\}$

$\langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \ldots, \overline{23}\} = \mathbb{Z}_{24}$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}\}$

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}\}$

$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}, \overline{12}, \overline{16}, \overline{20}\}$

$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}\}$

$\langle \overline{12} \rangle = \{\bar{0}, \overline{12}\}$

$\langle \bar{8} \rangle = \{\bar{0}, \bar{8}, \overline{16}\}$

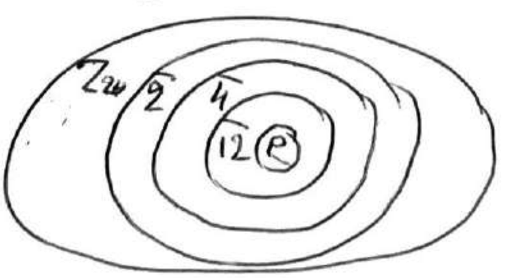
هذه هي جميع الزمر الجزئية الفعلية

$\{\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \overline{12}\}$

نلاحظ منه :

$\mathbb{Z}_{24} \supset \langle \bar{2} \rangle \supset \langle \bar{4} \rangle \supset \langle \overline{12} \rangle \supset \{\bar{0}\}$

الزمرة $\mathbb{Z}_{24}$ تحوي على $\langle \bar{2} \rangle$ و $\langle \bar{2} \rangle$ تحوي $\langle \bar{4} \rangle$ و $\langle \bar{4} \rangle$ تحوي على $\langle \overline{12} \rangle$ و $\langle \overline{12} \rangle$ تحوي $\langle \bar{0} \rangle$ وطولها هو $\underline{\underline{4}}$ أي كم زمرة جزئية تحوي السلسلة



Example:- In the group $(S_4, \circ)$, the sequence

$$S_4 \supset \{R_0, R_{180}, V, H\} \supset \{R_0, H\} \supset \{R_0\}$$

In normal chain of length 3

Since:

$\{R_0, R_{180}, V, H\}$ is a normal subgp of $(S_4, \circ)$

and $\{R_0, H\}$ is a normal subgp of $\{R_0, R_{180}, V, H\}$

also, $\{R_0\}$ is a normal subgp of $\{R_0, H\}$.

but:- $S_4 \supset \{R_0, H\} \supset \{R_0\}$ is not normal chain subgp

because: $\{R_0, H\}$ is not normal subgp of $(S_4, \circ)$.

Example:- In the group $(Z_{12}, +_{12})$, the following chains are normal chain:-

$$Z_{12} \supset \langle 6 \rangle \supset \{\bar{0}\}$$

$$Z_{12} \supset \{0\}$$

$$Z_{12} \supset \langle 2 \rangle \supset \langle 4 \rangle \supset \{0\}$$

$$Z_{12} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \{0\}$$

$$Z_{12} \supset \langle 2 \rangle \supset \langle 6 \rangle \supset \{0\}$$

since every subgp of the group $(Z_{12}, +_{12})$ is normal subgp, because $(Z_{12}, +_{12})$ is comm.

Note:- If $|G| \geq 2$, then the normal chain $G \supset \langle e \rangle$ is called trivial chain of length 1.

Define:- In the group $(G,*)$, the descending sequence of sets:

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$$

forms a composition chain for $(G,*)$ if:-

1- H_i is a subgp of $(G,*)$.

2- H_i is a normal subgroup of H_{i-1}.

The inclusion $H_{i-1} \supseteq K \supseteq H_i$, where K is a normal subgroup of H_{i-1}, implies that either:

$K = H_{i-1}$ or $K = H_i$.

Example:- In the group $(Z_{24}, +_{24})$

1- $Z_{24} \supset \langle \bar{2} \rangle \supset \langle \bar{4} \rangle \supset \langle \bar{8} \rangle \supset \langle \bar{0} \rangle$

2- $Z_{24} \supset \langle \bar{3} \rangle \supset \langle \bar{6} \rangle \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$

1+2 are both composition chains for $(Z_{24}, +_{24})$.

but

$Z_{24} \supset \langle \bar{2} \rangle \supset \langle \bar{12} \rangle \supset \langle \bar{0} \rangle$, is not a composition chain because

$$\langle \bar{2} \rangle \supset \underline{\langle \bar{6} \rangle} \supset \langle \bar{12} \rangle$$

Definition:- a normal subgp $(H,*)$ is called <u>maximal normal subgp</u> of the group $(G,*)$ if:-

1- $H \neq G$.

اي لا يوجد زمرة جزئية ناظمية

2- there exist no normal subgp $(K,*)$ s.t. $\boxed{H \subset K \subset G}$

Example:- In the group $(Z_{24}, +_{24})$ the subgps $(\langle 2 \rangle, +_{24})$ and $(\langle 3 \rangle, +_{24})$ are maximal normal subgp.

Remark:- a chain

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$$

is composition chain if each subgp $(H_i, *)$ is maximal subgp of $(H_{i-1}, *)$.

Example:- In $(Z_{24}, +_{24})$

$Z_{24} \supset \langle 4 \rangle \supset \langle 8 \rangle \supset \{0\}$ is not composition chain because $\langle 4 \rangle$ is not maximal normal subgp of $(Z_{24}, +_{24})$ since there exist $\langle 2 \rangle$ as maximal normal subgp of $(Z_{24}, +_{24})$ and $Z_{24} \supset \underline{\underline{\langle 2 \rangle}} \supset \langle 4 \rangle$

where:

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$$

$$\langle 4 \rangle = \{0, 4, 8, 12, 16, 20\} \Longrightarrow \underline{\underline{\langle 2 \rangle \supset \langle 4 \rangle}}$$

Definition:- A group is simple if it has no non-trivial proper normal subgp. (تعريف مجاني)

Example:-

1- $(Z_{2u}, +_{2u})$ is not simple.

2- $(Z_p, +_p)$ is simple-

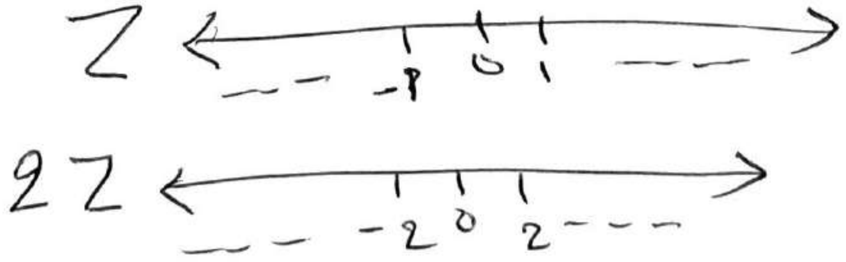
Theorem:- A normal subgp $(H,*)$ of the group $(G,*)$ is maximal if and only if the quotient group $(G/H, \otimes)$ is simple-

ملاحظة :- الزمرة الجزئية الناظمية $(H,*)$ للزمرة $(G,*)$ هي عظمى اذا وفقط اذا زمرة القسمة $(G/H, \otimes)$ بسيطة.

Example:- In the group $(Z,+)$ the subgp $(Z_e,+)$ is maximal normal subgp since:-

$Z/Z_e = \{Z_o, Z_e\}$ and since the order of $Z/Z_e = 2$

Then $(Z/Z_e, \otimes)$ is simple and hence $(Z_e,+)$ is maximal normal subgp of the group $(Z,+)$.



$Z \supset 2Z$

$Z/Z_e = \{Z_o, Z_e\}$ $\quad$ 2 = مجموعة عناصرها

Note:- G/H is simple if $|G/H| = p$, where p is prime number.

Example:- In $(Z_{24}, +_{24})$

$\because \left| Z_{24}/\langle \bar{2} \rangle \right| = \frac{24}{12} = 2$

$\Rightarrow \langle \bar{2} \rangle$ is maximal normal subgp of $(Z_{24}, +_{24})$

$\left| Z_{24}/\langle \bar{3} \rangle \right| = \frac{24}{8} = 3$

$\Rightarrow \langle \bar{3} \rangle$ is maximal normal subgp of $(Z_{24}, +_{24})$

but

$\left| Z_{24}/\langle \bar{4} \rangle \right| = \frac{24}{6} = 4$ is not prime.

$\Rightarrow \langle \bar{4} \rangle$ is not maximal normal subgp of $(Z_{24}, +_{24})$

$\left| Z_{24}/\langle \bar{8} \rangle \right| = \frac{24}{3} = 8$ is not prime.

$\Rightarrow \langle \bar{8} \rangle$ is not maximal normal subgp of $(Z_{24}, +_{24})$

imp

Remark:- A normal chain

$$G \supset H_0 \supset H_1 \cdots \supset H_{n-1} \supset H_n = \{e\}$$

is composition chain if the quotient groups $\left(H_{i-1}/H_i \right)$ is simple. $\forall\, i = 0, \ldots, n$.

مهمة جداً جداً

<u>Example:</u> show that the chain

$$\mathbb{Z}_{80} \supset \langle \bar{2} \rangle \supset \langle \bar{4} \rangle \supset \langle \overline{20} \rangle \supset \langle \overline{40} \rangle \supset \langle \bar{0} \rangle$$

is <u>composition chain</u> for $(\mathbb{Z}_{80}, +_{80})$.

<u>Proof:</u> ① $\because \left| \frac{\mathbb{Z}_{80}}{\langle \bar{2} \rangle} \right| = \frac{|\mathbb{Z}_{80}|}{|\langle \bar{2} \rangle|} = \frac{80}{40} = \underline{\underline{2}}$ is prime number

$\therefore \frac{\mathbb{Z}_{80}}{\langle \bar{2} \rangle}$ is simple $\Longrightarrow \langle \bar{2} \rangle$ is maximal in $\mathbb{Z}_{80}$.

② $\because \left| \frac{\langle \bar{2} \rangle}{\langle \bar{4} \rangle} \right| = \frac{|\langle \bar{2} \rangle|}{|\langle \bar{4} \rangle|} = \frac{40}{20} = 2$ is prime number

$\therefore \frac{\langle \bar{2} \rangle}{\langle \bar{4} \rangle}$ is simple $\Longrightarrow \langle \bar{4} \rangle$ is maximal in $\langle \bar{2} \rangle$.

③ $\because \left| \frac{\langle \bar{4} \rangle}{\langle \overline{20} \rangle} \right| = \frac{|\langle \bar{4} \rangle|}{|\langle \overline{20} \rangle|} = \frac{20}{4} = 5$ is prime number

$\therefore \frac{\langle \bar{4} \rangle}{\langle \overline{20} \rangle}$ is simple $\Longrightarrow \langle \overline{20} \rangle$ is maximal in $\langle \bar{4} \rangle$.

4. $\left| \frac{\langle \overline{20} \rangle}{\langle \overline{40} \rangle} \right| = \frac{|\langle 20 \rangle|}{|\langle 40 \rangle|} = \frac{4}{2} = 2$ is prime number

$\therefore \frac{\langle \overline{20} \rangle}{\langle \overline{40} \rangle}$ is simple $\Longrightarrow \langle \overline{40} \rangle$ is maximal in $\langle \overline{20} \rangle$

5- $\left| \frac{\langle \overline{40} \rangle}{\langle \bar{0} \rangle} \right| = \frac{|\langle \overline{40} \rangle|}{|\langle \bar{0} \rangle|} = \frac{2}{1} = 2$ is prime number

$\therefore \frac{\langle \overline{40} \rangle}{\langle \bar{0} \rangle}$ is simple $\Longrightarrow \langle \bar{0} \rangle$ is maximal in $\langle \overline{40} \rangle$.

$\therefore \mathbb{Z}_{80} \supset \langle \bar{2} \rangle \supset \langle \bar{4} \rangle \supset \langle \overline{20} \rangle \supset \langle \overline{40} \rangle \supset \langle \bar{0} \rangle$

is composition chain for $(\mathbb{Z}_{80}, +_{80})$. $\boxtimes$

Theorem:- Every finite group $G \neq \{e\}$ has a Composition Chain.

(كل زمرة منتهية تحتوي على أكثر من عنصر واحد لها سلسلة تركيبية).

حفظ النص

Theorem: (Jordan-Holder)

In a finite group with more than one elements, Any two composition chains are equivalent.

(في الزمرة المنتهية التي تحتوي على أكثر من عنصر واحد، اي سلسلتين تركيبية تكون متكافئة)

Example:- In group $(Z_{24}, +_{24})$ the chains:-

$$Z_{24} \supset \langle 2 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\} \quad --- (1)$$

and

$$Z_{24} \supset \langle 3 \rangle \supset \langle 6 \rangle \supset \langle 12 \rangle \supset \{0\} \quad --- (2)$$

are equivalent.

The quotient group of the first chain are:-

(1) $\left|\frac{Z_{24}}{\langle 2 \rangle}\right| = \frac{24}{12} = 2$ is prime

(2) $\left|\frac{\langle 2 \rangle}{\langle 6 \rangle}\right| = \frac{|\langle 2 \rangle|}{|\langle 6 \rangle|} = \frac{12}{4} = 3$ is prime

(3) $\left|\frac{\langle 6 \rangle}{\langle 12 \rangle}\right| = \frac{|\langle 6 \rangle|}{|\langle 12 \rangle|} = \frac{4}{2} = 2$ is prime.

(4) $\left|\frac{\langle 12 \rangle}{\langle \bar{0} \rangle}\right| = \frac{|\langle 12 \rangle|}{|\langle \bar{0} \rangle|} = \frac{2}{1} = 2$ is prime

The quotient groups of the second chain are:

① $\left|\frac{Z_{24}}{<\bar{3}>}\right| = \frac{|Z_{24}|}{|<\bar{3}>|} = \frac{24}{8} = 3$ is Prime

② $\left|\frac{<\bar{3}>}{<\bar{6}>}\right| = \frac{|<\bar{3}>|}{|<\bar{6}>|} = \frac{8}{4} = 2$ is Prime

③ $\left|\frac{<\bar{6}>}{<\bar{12}>}\right| = \frac{|<\bar{6}>|}{|<\bar{12}>|} = \frac{4}{2} = 2$ is Prime

④ $\left|\frac{<\bar{12}>}{<\bar{0}>}\right| = \frac{|<12>|}{|<\bar{0}>|} = \frac{2}{1} = 2$ is Prime.

By theorem (Any two finite cyclic groups have the same order are isomorphic).

$\Rightarrow (Z_{24}/<3>, \otimes) \simeq (<2>/<\bar{6}>, \otimes$ ...

$(<3>/<6>, \otimes) \simeq (Z_{24}/<\bar{2}>, \otimes)$

and $(<6>/<12>, \otimes) \simeq (<6>/<12>, \otimes)$

also $(<12>/\{0\}, \otimes) \simeq (<12>/\{0\}, \otimes)$

So the composition chains are equivalent. $\boxtimes$

Solvable groups:-

Definition:- A group $(G,*)$ is called solvable if it has a normal chain (Possibly of length 1).

$$G = H_0 \supset H_1 \supset H_2 \cdots \supset H_{n-1} \supset H_n = \{e\}$$

In which every quotient group $(H_{i-1}/H_i, \circledast)$ where $(i=1,2,\cdots n)$ is commutative.

Example:- $(S_3, \circ)$ is solvable group since there exist a normal chain:

$$S_3 \supset \{I, (123), (132)\} \supset \{I\},$$

take $H_0 = S_3$, $H_1 = \{I, (123), (132)\}$, $H_2 = \{I\}$.

Then:-

$(H_0/H_1, \circledast)$ and $(H_1/H_2, \circledast)$ are commutative, Since.

$\left|\frac{H_0}{H_1}\right| = \frac{6}{3} = 2$ is prime order and hece it is cyclic, So it Comm.

Also:

$|H_1/H_2| = \frac{3}{1} = 3$ is prime order and hence it cyclic, so it commutative.

We note that H_1 is normal in S_3 and H_2 is normal in H_1.

Remark:- Every commutative group with more than one element is solvable since the trivial chain $G \supset \{e\}$ is solvable chain.

Example:- The group $(S_4, \circ)$ is solvable group since the chain: $S_4 \supset \{R_0, R_{90}, R_{180}, R_{270}\} \supset \{R_0, R_{180}\} \supset \{R_0\}$ Is normal chain, and

$(H_2/H_3, \otimes), (H_1/H_2, \otimes), (H_0/H_1, \otimes)$ are commutative, where:

$H_0 = S_4$, $H_1 = \{R_0, R_{90}, R_{180}, R_{270}\}$, $H_2 = \{R_0, R_{180}\}$, $H_3 = \{R_0\}$.

توضيح

① $\left|\frac{H_0}{H_1}\right| = \frac{8}{4} = 2$ is prime order and it is cyclic, so it comm

② $\left|\frac{H_1}{H_2}\right| = \frac{4}{2} = 2$ 〃 〃 〃 and it is cyclic, so it comm

③ $\left|\frac{H_2}{H_3}\right| = \frac{2}{1} = 2$ 〃 〃 〃 and it is cyclic, so it comm

Definition:- A group $(G,*)$ is said to be P-group if the order of each element of $(G,*)$ is a power of a fixed prime p.

i.e. a finite group $(G,*)$ is called p-group (where P is prime number) if:

$$\boxed{\forall a \in G, \quad O(a) = |a| = p^k \text{ , for some } K \geq 0 .}$$

Example:-

1- the group $(S_y, \circ)$ is 2-group

$S_y = \{R_0, R_{180}, R_{270}, R_{90}, V, H, D_1, D_2\}$

$\Rightarrow |S_y| = 8 = 2^3$.

$|R_0| = 1 = 2^0$

$|R_{180}| = 2$

$|R_{90}| = |R_{270}| = 4 = 2^2$

$|H| = |V| = |D_1| = |D_2| = 2^1$

نلاحظ ان كل عناصر S_y رتبها 2^k وان الزمرة نفسها

رتبتها 2^3 . لهذا فان الزمرة

$(S_y, \circ)$ is a 2-group.

2- The group $(Z_8, +_8)$ is 2-group

$Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

$|Z_8| = 8 = 2^3$, $|\bar{3}| = 8 = 2^3$

$|\bar{0}| = 1 = 2^0$ $|\bar{4}| = 2 = 2^1$

$|\bar{1}| = 8 = 2^3$ $|\bar{5}| = 8 = 2^3$

$|\bar{2}| = 4 = 2^2$ $|\bar{6}| = 4 = 2^2$

$|\bar{7}| = 8 = 2^3$

$\therefore$ The order of each element in Z_8 is a power of $\underline{\underline{2}}$

$\Rightarrow (Z_8, +_8)$ is 2-group.

3- The group $(Z_9, +_9)$ is 3-group.

$Z_9 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}$

$o(\bar{0}) = 1 = 3^0$, $o(\bar{5}) = 9 = 3^2$

$o(\bar{1}) = 9 = 3^2$ $o(\bar{6}) = 3$

$o(\bar{2}) = 9 = 3^2$ $o(\bar{7}) = 9 = 3^2$

$o(\bar{3}) = 3$ $o(\bar{8}) = 9 = 3^2$

$o(\bar{4}) = 9 = 3^2$

$\therefore$ The order of each element in Z_9 is a power of 3 //

$\Rightarrow (Z_9, +_9)$ is 3-group.

Remark:- If $|G| = p^k$, where p is a prime number, then G is p-group.

Example:- ① The group $(Z_{25}, +_{25})$ is 5-group because $|Z_{25}| = 5^2$.

② The group $(Z_9, +_9)$ is 3-group becuse $|Z_9| = 3^2$.

③ The group $(Z_8, +_8)$ is 2-group becaus $|Z_8| = 2^3$.

④ The group $(S_4, \circ)$ is 2-group because $|S_4| = 2^3$.

⑤ The group $(Z_{16}, +_{16})$ is 2-group because $|Z_{16}| = 2^4$.

Remark:- Every group of prime order is p-group.

Example:- $(Z_5, +_5)$ is 5-group because $|Z_5| = 5^1$.

Theorem:- If $(G, *)$ is p-group and $(H, *)$ is a subgp of $(G, *)$, then $(H, *)$ is p-group.

Theorem:- If $(G, *)$ be a p-group of order $\boxed{p^2}$ then $(G, *)$ is commutative.

Remark:- Not every p-group is commutative.

Example:- The group $(S_4, \circ)$ is 2-group but $(S_4, \circ)$ is not commutative.

Sylow P- Subgroup

<u>Definition:</u>- Let $(G,*)$ be a finite group and P is a Prime number, a Subgroup $(H,*)$ of $(G,*)$ is Said to be Sylow P-Subgroup if:-

1- $(H,*)$ is a P-group.

2- $(H,*)$ is not contained in any other P-subgroup of $(G,*)$ for Some Prime P.

<u>Example:</u>- $(Z_{24}, +_{24})$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}, \bar{18}, \bar{20}, \bar{22}\}$

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}, \bar{18}, \bar{21}\}$

$\langle \bar{4} \rangle = \{\bar{0}, \bar{4}, 8, 12, 16, 20\}$

$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \bar{12}, \bar{18}\}$

$\langle \bar{8} \rangle = \{\bar{0}, \bar{8}, \bar{16}\}$

$\langle \bar{12} \rangle = \{\bar{0}, \bar{12}\}$

$\boxed{o(\bar{2}) = 12 = 2^2 \cdot 3}$, $o(8) = 3^1$

(*) $o(3) = 8 = 2^3$ (*) $o(12) = 2^1$

$\boxed{o(4) = 6 = 2^1 \cdot 3}$

(*) $o(6) = 4 = 2^2$

The 2-Subgroup of $(\mathbb{Z}_{24}, +_{24})$ are:-

$\langle \bar{3} \rangle, \langle \bar{6} \rangle, \langle \overline{12} \rangle$

$\because \langle \bar{3} \rangle \nsubseteq \langle \bar{6} \rangle$ and $\langle \bar{3} \rangle \nsubseteq \langle \overline{12} \rangle$

$\therefore (\langle \bar{3} \rangle, +_{24})$ is a Sylow 2-Subgp.

The 3-Subgroup of $(\mathbb{Z}_{24}, +_{24})$ is only $(\langle \bar{8} \rangle, +_{24})$ which is not contained in any other 3-Subgp.

$\therefore (\langle \bar{8} \rangle, +_{24})$ is a Sylow 3-Subgp.

تم بحمده تعالى

بالتوفيق للجميع ان شاء الله