التاريخ: ١٢ / ١٠ / ٢٠١٥ الموضوع :

بسم الله الرحمن الرحيم

الفصل الاول

جبر الزمر

The Group

Def A binary operation $(*)$ on a non empty set (G) is a function from the set proudct $G \times G$ into G we denoted the image of a Pair (x,y) under the binary operation $*$ by

$$*(x,y) = x * y, \forall x, y \in G$$

حاصل ضرب عنصرين في العملية الثنائية الناتج هو عنصر ينتمي للمجموعة

The above Property is called the (Closure Property), and if this is satisfied, we ~~get~~ say that G is (Closed) under the operation

الموضوع : ______________ التاريخ : / /

A mathematical system النظام الرياضي

Def is a non empty set G and a binary operation defined on G and denoted by $(G, *)$ which satisfy the closure property تحقق شرط الانغلاق

Ex ① $(N, +)$ is a mathematical system

② $(N, \cdot)$ 〃 〃 〃
عملية الضرب

③ $(N, -)$ is not mathematical system
مع عملية الطرح

Since $(5, 2) \in N$
and $(2-5) = -3 \notin N$

Def The binary operation $(*)$ on a non empty set G is called

التجميع (associative) if

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

Ex $(Z, +)$ is associative since $\forall\, a, b, c \in Z$

الاعداد الصحيحة
(+ و -)

عبارة عن نظام رياضي تتحقق فيه شرط الاغلاق والتجميع

Semi group شبه الزمرة

Def The mathimatical system $(G, *)$ is called (a semi-group)

if the binary operation on G is associative

1. G is closed under $*$
2. $*$ is associative

Ex $(Z, \cdot)$ is a semi group

(+ و - و ·) عملية الضرب

شبه زمرة ~~لانه~~ اذا تحقق الانغلاق والتجميع

$(Z, +)$ is semi group

$(Z, \div)$ is not semi group

$(2, 3) \in Z, \left(\frac{2}{6} = \frac{1}{3}\right) \notin Z$

اذا لم يتحقق احد الشروط
∴ ليست شبه زمرة

The identity [illegible] العنصر المحايد

Def An identity for the binary operation $(*)$ on a non empty set G is an element $e$ven in G

اعداد زوجيه

$a * e = e * a = a$

Ex $(Z, +)$ the identity is (Zero 0)

الاعداد الموجبه الزوجيه

The inverse المعكوس

هو عنصر ينتمي للمجموعة بحيث اذا تفاعل مع عنصر آخر ينتج المعكوس

Def. if the binary operation on anon empty set (G) have an identity e, then the inverse for an element

$x \in G$ is $x^{-1} \in G$ such that
$x * x^{-1} = x^{-1} * x = e$

Ex $(Z, +) \Rightarrow \exists\, x^{-1} \in Z \quad \forall x \in Z$

$(Z, \cdot) \Rightarrow \nexists\, x^{-1} \in Z \quad \forall x \in Z$

$(5, \frac{1}{5}) = 1 \in R \rightarrow$ (الاعداد الحقيقية (+و- والنسبية)

الزمرة: المجموعة الخالية مع العملية الرياضية تدعى زمرة اذا تحققت فيها الصفات

① تكون مغلقة ② تجميعية ③ وجود العنصر المحايد
④ وجود معكوس لكل عنصر

Def: A non empty set G with a binary operation $(*)$ is called (a group) denoted by $(G, *)$ if satisfied:

① Closure Property
$\forall a, b \in G \Rightarrow a * b \in G$

② Associative Low
$\forall a, b, c \in G$
$(a * b) * c = a * (b * c)$

③ Existence of identity
$\exists e \in G$ s.t $a * e = e * a = a$ $\forall a \in G$

④ Existtence of invers
$\forall x \in G, \exists x^{-1} \in G$ s.t
$x * x^{-1} = x^{-1} * x = e$

Ex $(Z, +)$

① $\forall a, b \in Z \Rightarrow a+b \in Z$

$\therefore$ Z is closed under $(+)$

② $\forall a, b, c \in Z \Rightarrow (a+b)+c = a+(b+c)$

$\therefore$ + is asso on Z

③ $\exists\, 0 \in Z$ such that $a+0 = 0+a = a$

$\forall a \in Z$

$\therefore \exists$ identity

④ $\forall x \in Z, \exists x^{-1} \in Z$

such that $x + x^{-1} = x^{-1} + x = 0$

$\therefore \exists x^{-1} \; \forall x \in Z$ $\quad \therefore (Z, +)$ is a group

التاريخ : / / الموضوع :

Ex $(M_{2\times 2}, +)$

$a + b \qquad\qquad b + a$

① $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$

② $(a+b)*c = a*(b+c)$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left[\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right]$$

③ $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a^{-1} & b^{-1} \\ c^{-1} & d^{-1} \end{bmatrix} = \cancel{e} = e \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

④ $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

التاريخ: / /　　　　الموضوع :

Commutative group الزمرة الابدالية

هي التي تحقق عملية الابدال في العملية الرياضية
مثال/ (Z) عاكس عملية الجمع
كل رقمين بعملية الجمع (عملية ابدالية)

Def A group $(G, *)$ is said to be abinary or commutative group if the binary operation $*$ is commutative

i.e يعني $a * b = b * a, \forall a, b \in G$

Ex $(Z, \cdot)$ is a commutative group
since $\forall a, b \in Z, a.b = b.a$

Ex $(N, +)$ is a comm group
since $\forall a, b \in N \quad a+b = b+a$

Ex $(Z, +), a, b \in Z, a+b = 2a+b$ ضعف الاول + الثاني

~~is not group~~ is not comm group
$b+a = 2b+a$
لان الارقام تختلف في حالة وحده اذا كانت متساوية

$(2a+2b)+c = 2a+(b+c)$

التجميع لا يتحقق لأن الطرفين غير متساويين

الزمرة المحددة: نطلقها على الكروب الذي يحوي مجموعة عناصر محددة

Def: We shall call group $(G,*)$ a finite if the set G is finite

Ex: $(Z,+)$, $(R-\{0\},\cdot)$, $(Q,+)$ — is infinite group

but $(C_3,\cdot)$ is finite group

الموضوع : وحدة العنصر المحايد   التاريخ : / /

Theorem (1.1) النظرية الاولى

(Uniqness of identity)

[نص النظريه → The identity element in group is uniqe]

Proof Let $(G, *)$ is a group

Let $e, \acute{e}$ are two identity element

then $e * \acute{e} = \acute{e} * e = e$

Since (e) is identity

and $e * \acute{e} = \acute{e} * e = e$

Since e is identity

$\therefore e = \acute{e}$

$\therefore$ The identity is uniqe

الموضوع : التاريخ : / /

النظرية الثانية (وحدانية المعكوس)

لكل عنصر له معكوس واحد

Theorem (1.2)
(uniqness of inverse

نص النظريه ~~"Each element of a group has a uniqe invers"~~

نفرض عنصر (a) له معكوسين (b, c)

Proof Let $(G, *)$ be a group and $a \in G$ and

Let (b) as well as (C) be an inverse of نفسه (b) $a*c = c*a = e$

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

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

$\therefore b = c$

$\therefore$ the inverse is uniqe

الموضوع : ______ التاريخ : / /

النظرية الثالثة (معكوس المعكوس) هو العنصر نفسه

Theorem (1.3) If $(G, *)$ is a group and a be any element of G then $(a^{-1})^{-1} = a$

Proof Let e be the identity element in G then

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

نضرب طرفي المعادلة ب $(a^{-1})^{-1}$

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

$$\left((a^{-1})^{-1} * a^{-1}\right) * a = (a^{-1})^{-1}$$

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

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

النظرية الرابعة } اذا كانت الكروب تحتوي (٣ عناصر) (a, b, c) فيمكن تحقيق الاختصار من جهة اليمين واليسار

Theorem (1.4)

قوانين الاختصار

The Cancelation Lous hold in group

Proof $a * b = a * c$

اختصار من جهة اليمين $a^{-1} * (a * b) = a^{-1} * (a * c)$

العنصر في معكوسه يعطينا identity $(a^{-1} * a) * b = (a^{-1} * a) * c$

$$e * b = e * c$$

$$b = c$$

and if $b * a = c * a$

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

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

$$b * e = c * e$$

$$b = c$$

Theorem 1-5   النظرية الخامسة

If $(G, *)$ is a group then
$(a*b)^{-1} = b^{-1} * a^{-1}$ → معكوس الثاني × معكوس الاول
$\forall a, b \in G$

Proof:

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

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

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

نأخذ الطرف الثاني $(b^{-1} * a^{-1}) * (a*b)$

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

$$= b^{-1} * e * b \qquad = b^{-1} * b = e$$

$\therefore (b^{-1} * a^{-1})$ is the inverse of $(a*b)$

but $(a*b^{-1})$ is also the inverse of $(a*b)$

by (Theorem 1.2)

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

التاريخ : / /   الموضوع :

Theorem (1.6)   النظرية السادسة

If a, b are any two element of a group $(G, *)$ then the equation ~~$(a*x)$~~ $(a * x = b)$ and $(y * a = b)$ have uniqe solution in G

Proof $\quad a * x = b \qquad$ نضرب بـ a^{-1}

$$a^{-1} * a * x = a^{-1} * b$$

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

$$x = a^{-1} * b$$

Since $(a^{-1} \in G, b \in G \Rightarrow a^{-1} * b \in G$

Let x_1, x_2 are two solutions of equation $a * x = b$

$$\Rightarrow a * x_1 = b \quad \text{and} \quad a * x_2 = b$$

$$\therefore a * x_1 = a * x_2$$

$$a^{-1} * a * x_1 = a^{-1} * a * x_2$$

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

$\therefore$ The equation $a * x = b$ have uniqe Solution in G

simelarly in equation $y * a = b$

Theorem (1.7)   النظريه السابقة 7

Any non Commutative group has at least Six elements

اي زمرة غير ابدالية تحوي على الاقل (٦) عناصر في المجموعة الموجودة فيها

Proof

If $(G, *)$ is a non commutative group it must have an identity element (e) and a pair of a non commutative elements a and b

نفرض كروب ليس ابدالي

such that $a * b \neq b * a$

$\therefore$ Now the set G is $\{a, b, a*b, b*a\}$

T.P the element $a*a$ is defrent from each element of G

~~(1) if $a*a = b$ implies~~

(1) if $a*a = a$ implies $a = e$ C! تناقض

(2) if $a*a = b$ implies $a*b$

$= a * (\overset{\text{نعوض}}{a*a}) = \cancel{(a*a)}\ (a*a)*a$

$= b*a$ C! تناقض

③ if $a*a = a*b$ implies $a=b$

④ if $a*a = b*a$ implies $a=b$

either $a*a \neq e$ then $a*a \in G$

or $a*a = e$

In this latter we show

$(a*b*a)$ is (distinct) from G

عنصر مختلف من عندي يا

Now $a*(a*b*a) = (a*a)*(b*a)$

عنصر مختلف

$= e*(b*a) = b*a$

⑤ $a*b*a = e \Rightarrow b*a = a*(a*b*a)$

$= a*e = a$

⑥ $a*b*\cancel{a} = \cancel{a} \Rightarrow a*b = e$ Ci تناقض

⑦ $a*b*a = b \Rightarrow a*b = a*(a*b*a)$

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

$= a*(b*a)$

$= e*b*a = b*a$ Ci

الموضوع : ________ التاريخ : / /

(8) $a*b*a = a*b \Rightarrow a=e$ Ci

(9) $a*b*a = b*a \Rightarrow a=e$ Ci تناقض

order group ترتيب الكروب

Def Let $(G,*)$ be a finite group the order of G is the number of it's elements and we denoted by $|G|$

هو عدد العناصر الموجودة في مجموعة الكروب المحدد بعناصر ثابتة محددة

Ex A group $(C_3, .)$ where $C_3 = \{1, w, w^2\}$

٣ عناصر

$$|G| = |C_3| = 3$$

- A group $(G, .)$ where $G = \{1, -1, i, -i\}$

$$\therefore |G| = 4$$

Def Let $(G, *)$ be a group, the order of an element $a \in G$ is the least Positive integer (m) such $a^m = e$

We denoted by $\overset{\text{order}}{O}(a) = m$

Ex A group $(C_3, \cdot)$

$O(1) = 1$ since $1^1 = 1$

$O(w) = 3$ since $w^3 = 1$ $(w \times w \times w) = 1$

$O(w^2) = 3$ since $(w^2)^3 = 1$

Ex A group $(G, \cdot)$, $C = \{1, -1, i, -i\}$

$O(1) = 1$

$O(-1) = 3$

$O(i) = 4$

$O(-i) = 4$

التاريخ: ١٨/ ١١ / ٩٥ الموضوع :

Theorem (1.8) النظرية الثامنة

The order of an element of a group is the same of it's inverse

proof Let $a \in G$ such that

$$\text{order}(a) = m \text{ and } O(a^{-1}) = n$$

$\because$ order $(a) = m \Rightarrow a^m = e \Rightarrow (a^m)^{-1} = e^{-1} = e$

$\Rightarrow (a^{-1})^m = e \Rightarrow O(a^{-1}) = m$ —— ①

$\because O(a^{-1}) = n \Rightarrow \left((a^{-1})^n\right)^{-1} = (e)^{-1} \Rightarrow (a^n)^{-1} = e$] نأخذ inverse للطرفين

$a^n = e^{-1} = e \Rightarrow O(a) = n$ —— ②

From ① and ② then

$$m = n \Rightarrow \text{order}(a) = O(a^{-1})$$

التاريخ : / /　　　　　الموضوع :

Theorem (1.9)　　　النظرية التاسعة

If a and b are any two element of agroup G, then $O(a) = O(b^{-1} * a * b)$

Proof Let $O(a) = m$

$$\therefore a^m = e$$

Now $(b^{-1} * a * b)^m = b^{-1} * a * b * b^{-1} * a * b \text{ --- } b^{-1} * a * b$

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

$$= b^{-1} * a * e * a * e * a \text{ -- } * e * a * b$$

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

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

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

التاريخ: / /　　　　　　　　الموضوع :

Theorem (1.10)
نظرية القسمة

النظرية العاشرة

Division algrothem

if $\overset{5,2}{a,b} \in \mathbb{Z}$ with $b \neq 0$

then there exist uniqe

$q, r \in \mathbb{Z}$ such that:

$a = q\,b + r_{(1)}$, $0 \leq r < |b|$

$5 = q(2) + 1$

الفصل الثاني

Symetric and integer module n groups

Def: A one-one mapping of a finite set S of n elements onto itself is called a permutation of degree n.

$$f = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ f(a_1) & f(a_2) \cdots f(a_n) \end{pmatrix}$$

Ex: Let $S = \{a, b, c\}$ and the Permutation define as $f(a) = b$, $f(b) = c$, $f(c) = a$

then $f \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$

Remark The set of all Permutation is called the Symmetric Set denote by (S_n) and $|S_n| = n!$

Ex Let $S = \{1, 2, 3\}$ find S_3

$$S_3' = \left\{ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\right.$$

$$\left. f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$f = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix},\quad g = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$$

$$f \circ g(a) = f(\underbrace{g(a)}_{\text{تأثير (g) على (a)}}) = \underbrace{f(c)}_{\text{تأثير (c) بـ f}} = d$$

$$g \circ f(a) = g(f(a)) = g(b) = d$$

$$f^{-1} = \begin{pmatrix} f(a_1) & \cdots & f(a_n) \\ a_1 & \cdots & a_n \end{pmatrix}$$

ينقلب السطر ~~الاول~~ الثاني
الى السطر الاول

Theorem 2.1   النظرية الاولى

Let S be a finite set containing n distinct element then the symmetric set of all ~~the~~ Pormutations of degree n on S froms a finite group of order $n!$ and denoted by (S_n, o)

Proof:

① Clouser Property if f, g, $g \in S_n$ then $f o g \in S_n$

② Associative law: since the Composite on mapping is associative so it associative on Permutations

تبديلي

③ Existence of identity: the identity Permutation

$$f = \begin{pmatrix} a_1 & \cdots & a_n \\ a_1 & \cdots & a_n \end{pmatrix}$$

④ Existence of invers: $f = \begin{pmatrix} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \end{pmatrix}$

$$f^{-1} = \begin{pmatrix} b_1 & \cdots & b_n \\ a_1 & \cdots & a_n \end{pmatrix}$$

$$f o f^{-1} = \begin{pmatrix} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \end{pmatrix} o \begin{pmatrix} b_1 & \cdots & b_n \\ a_1 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & \cdots & b_n \\ b_1 & \cdots & b_n \end{pmatrix} = I$$

$f^{-1} o f =$

الموضوع :   التاريخ : / /

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

Def: A Permutation f of sets is a cycle of length n (or n-) if there exist $a_1, a_2, \ldots a_n \in S$ s.t $f(a_1) = a_2$

$f(a_2) = a_3$

$f(a_{n-1}) = a_n$, $f(a_n) = a_1$ and $f(x) = x$

Theorem 2.2

The Product of disjoint cycles is Commutative

Proof: Let S be a finite set and f, g be any two disjoint cycles on S_n Then f and g have no comm element.

التاريخ : / /

الموضوع :

Ex $f = (1, 2, 3)$ $g = (3, 4, 6)$

$f \circ g = (1,$ $(5, 4, 6)$

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

نظرية 2 :- اذا كانت الدالتين

The Product of disjoint is Commutative

Exc $f=(1\ 2\ 5)\ ,\ g=(3\ 4\ 6)$

$fog=(1\ 2\ 5)(3\ 4\ 6) \Rightarrow fog = gof$

يعني ناتج ضربهم نفس الناتج

$gof=(3\ 4\ 6)(1\ 2\ 5)$

Theorem (2.3)

The symetric group $(S_n, \circ)$ is non-Commutative for $n \geqslant 3$

دائرة

$S_2 \rightarrow 2\ (1, 2)$ (2 تروح للواحد)

$S_3=\{I, (1,2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

Proof: Exc

Theorem (2.4) Every Permutation Can be expressed as a composite of disjoint cycles

Corollary: Every Permutation Can be expressed as a Composite of transpositios
تبديل
اي تبديلي يمكن ان تكتبه بتركيبة الانتقالات

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

Ex $f = (2\ 5\ 6\ 4) = (2\ 4) \circ (2\ 6) \circ (2\ 5)$

يعرف التبديل على انه زوجي اوفردي حسب عدد الانتقالات

Def: A Permutation of a finite set is even (odd) if the number of transpositions is (even) odd

Ex/ $f = (1\ 2)(3\ 4\ 6) = (1\ 2)(3\ 6)(3\ 4)$: odd
زوجي لان ٣ مجموعات

$f = (2\ 5\ 6\ 4) = (2\ 4)(2\ 6)(2\ 5)$
f is odd

الموضوع : ______ التاريخ: ١٦ / ١٢ / ٢٠١٠

2.5

Theorem (5) A Cycle of length n is an even (odd) Permutation according as n is odd (even)

(Proof) Let $f = (a_1, a_2 --- a_n)$

$$= (a_1, a_n) \circ (a_1, a_{n-1}) \circ --- \circ (a_1, a_2)$$

i.e f is Proudct of $(n-1)$ transPositions
الانتقالات

عدد العناصر

if n is odd then $(n-1)$ is even and (f is even)

f n is even then $(n-1)$ is odd and (f is odd)

Remarks:

① اذا كان لدينا انتقالات
Everey transPositions is odd Permutation

مثل $(1\ 2)$ الانتقال بينهما واحد يعني odd)

$(1\ 2)(1\ 3) = (1\ 2\ 3)$
① ② even ← (٣) طولها

② The identity is even Permutation

Ex. Find x, y if $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & x & y & 6 \end{pmatrix}$

when (1) f is even (2) f is odd

(1) if f is even, $f = (1\ 3\ 2) = (12)(13)$ الواحد انتقل للـ (3)

الـ(2) انتقلت للـ(1) بس فنكرر الواحد

$\therefore x = 4 \ , \ y = 5$

(2) if f is odd $f = (1\ 3\ 2)(4\ 5) = (12)(13)(45)$

$\therefore x = 5 \ , \ y = 4$

$S_4 = \{1, 2, 3, 4\}$

هو زوجي بس تبديل فردي

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

فردي

الرقم الرابع لنفسه منكتبه

التاريخ : / /

الموضوع :

Theorem (6):

① The Product of two even Permutations is an even Permutation

② The Product of two odd Permutations is an even Permutation

③ The Product of an even Permutations and an odd Permutation is an odd Permutations

Proof

11 / 10 / 001 الموضوع :

Def The set of all even permutations of degree (n) is called Alternating set denoted by (A_n) and its order $= \frac{n-1}{2}$

Ex in $S_3 = \{I, (12), (13), (23) (123) (132)\}$

even permutations $= \{I, (123)(132)\} = A_3$

odd permutations $= \{(12), (13), (23)\}$

Theorem 7 (A_n, o) is a group

Proof ① $\forall f, g \in A_n$, $f o g \in A_n$

حاصل تركيبهم يكون زوجي ∴ ينتمي الى (A_n) ∴ شرط الانغلاق تحقق

② $\forall h, f, g \in A_n \therefore h, f, g \in S_n$

S_n is a group and $A_n \subseteq S_n$

∴ خاصية التجميع متحققة في A_n

③ $I \in A_n$

④ $\forall f \in A_n \Rightarrow f^{-1} \in A_n$ $f = (1\,2\,3) \Rightarrow f^{-1} = (3\,2\,1)$

$\therefore (A_n, o)$ is a group

منآخذ البرهان

الموضوع : التاريخ: ٢١ / ١٢ / ٢٠١٥

نأخذ المنطوق فقط

Theorem 2.9

تعريف

كل الاعداد الصحيحة التي تكون مع (a) نسمي تطابق صفيا مع (a)

Ex For $n = 3$ → نعمل ٣ صفوف

$[0] = \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\}$

الصف الاول للصفر $= \{x \in \mathbb{Z} : x = 0 + \underbrace{3K}_{\text{مضاعفات الرقم ٣}}, K \in \mathbb{Z}\}$

$= \{\ldots, -9, -6, -3, 0, 3, \overset{2\times 3}{6}, 9, \ldots\}$

$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\}$

الصف الثاني للواحد $= \{x \in \mathbb{Z} : x = 1 + 3K, K \in \mathbb{Z}\}$

$\{\ldots, -5, -2, 1, 4, 7$

الموضوع : ______________ التاريخ : / /

$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}$

$[3] = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}$

$Z_3 = \{[0], [1], [2]\}$

$Z_4 = \{[0], [1], [2], [3]\}$

$Z_n = \{[0], [1], \dots, [n-1]\}$

Theorem 2.10 Let n be a positive integer then.

① for every $[a] \in Z_n$, $[a] \neq \emptyset$

صف تطابق

لازم $\neq \emptyset$

$Z_4 = \{[0], [1], [2], [3]\}$

$-8, -4, 0, 4, 8, \dots$

يعني انزيد 4 لان Z_4

$-5, 1, 5, 9$

② if $[a] \in Z_n$ and $b \in [a]$ then $[b] = [a]$

اذا كان صف التطابق $[a]$

Z_n معناها انزيد فوق الصف رقم (n) النظيراه

③ for any $[a], [b] \in Z$

فرض $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$

$[a] \cap [b] \neq \emptyset$

نفرض عنصر موجود

④ $\cup \{[a] : a \in Z\} = Z$

اتحاد كل الاجزاء يعطينا (Z)

كل الصفوف التكافؤ التي يعطينا (Z)

التاريخ: ٢٨ / ١٢ / ٢٠١٥ الموضوع :

~~Theorem~~

الجمع بالنسبة لـ (n)

Def Abinary operation ($+_n$) defined on Z_n by ; if $[a], [b] \in Z_n$ then

$$[a] +_n [b] = [(a+b) \bmod n]$$

عندما تصل القيمة الناتج نطرح من (n)

Ex in Z_5 → من الصفر الى ٤

الرقم من خارجها

$[2] +_5 [4] = [1]$

$[0] +_5 [1] = [1]$

$[3] +_5 [4] = [2] \Rightarrow 3+4 = 7-5 = [2]$

$[3] +_5 [2] = [0] \Rightarrow 3+2 = 5-5 = 0$

من (5) وفوق الناتج

انقص بس 1, 2, 3, 4 منقص

طش

التاريخ: ١٠/٤/ /   الموضوع:

Theorem 11

مهم

تحقق خمس شروط

الزمرة (٤) شروط و الشرط (٥) من (الابدال)

The math. sys $(Z_n, +_n)$ forms a com. group, known as the group of integers modulo n.

Proof $Z_n \neq \emptyset$

حتى نعرف انه com لازم تحقق ⑤ شروط

① by above defi → التعريف في الصفحة السابقة

② $\forall [a], [b], [c] \in Z_n$ ⟵ a, b, c لكل العناصر

$([a] +_n [b]) +_n [c] =$

$(a+b) +_n [c] = (a+b+c)$

$= [a+(b+c)] = [a] +_n (b+c)$ تجزئة

$= [a] +_n ([b] +_n [c])$

③ the identity is $[0] = [n]$

④ the inverse of $[a] = [n-a]$

$S.t\ [a] +_n [n-a] = [\cancel{a}+n-\cancel{a}] = [n] = [0]$

$(Z_{10}, +_{10})$

الشرط الخامس

الموضوع :   التاريخ : / /

⑤ $\forall [a], [b] \in Z_n$

$[a] +_n [b] = (a+b) = (b+a) = [b] +_n [a]$

$\therefore (Z_n, +_n)$ is com. group

Ex) $(Z_4, +_4)$ is comm group

① $\forall [a], [b] \in Z_4 \quad [a] +_4 [b] = [(a+b) \bmod 4] \in Z_4$

② $\forall [a], [b], [c] \in Z_4$

$([a]$ نفس برهان النظرية

فقط نكتب $\begin{pmatrix} +_4 \\ Z_4 \end{pmatrix}$

③ $[0] = [4]$

④ invers $[a] = [4-a]$

s.t $[a] +_4 [4-a]$

بمكان كل (n) نكتب 4

التاريخ : / /　　　　الموضوع :

Ex Find invers $[a]^{-1}$ of all element of Z_5

$$Z_5 = \{[0],[1],[2],[3],[4]\}$$

$[a]$	$[a]^{-1}$
$[0]$	$[0]$
$[1]$	$[4]$
$[2]$	$[3]$
$[3]$	$[2]$
$[4]$	$[1]$

$[0] +_5 [0] = [0]$
$[1] +_5 [4] = [0]$

$[o -]$

الفصل الثالث

The sub group

Def) A non empty subset H of a group $(G, *)$ is called a sub group if $(H, *)$ is a group

Ex) Let $(Z, *)$ is a group show that $(Z_e, +)$ is sub group

even الاعداد الزوجية من ضمنها الصفر

Solution) $Z_e \neq \phi$

① for all $(a, b) \in Z_e$ s.t $a + b \in Z_e$

② Since asso. is hold تتحقق in Z then its hold تتحقق in Z_e also

③ identity $0 \in Z_e$ s.t $0 + a = a + 0 = a \ \forall a \in Z_e$

④ $\forall a \in Z_e$, $\exists a^{-1} = -a \in Z_e$ s.t $(a + (-a) = (-a) + a = 0$

$+2 + -2 = 0$

$\therefore (Z_e, +)$ is sub group

Ex) Let $G=\{1,-1,i,-i\}$, $(G,\cdot)$ is a group and $\underline{\underline{H}}=\{1,-1\}$, show that $(H,\cdot)$ is a sub group of a group $(G,\cdot)$
زمرة جزئية

Sol/ $H\neq\phi$

① $\forall\ a,b\in H$ s.t $(a.b)\in H$:تحقق شرط الإغلاق

② asso is hold
تتحقق

③ identity $\Rightarrow 1\in H$ s.t $1.a=a.1=a,\ \forall a\in H$

$\therefore$ 1 is the identiy of H

④ $\forall a\in H\ \exists\ a^{-1}\in H$ s.t $a.a^{-1}=a^{-1}.a=1$

$1\cdot -1=-1\cdot -1=1$

$\therefore (H,\cdot)$ is subgroup

Ex Let $(S_4, \circ)$ is a group show that $(A_4, \circ)$ is sub group

Sol $A_4 \neq \emptyset$ {لان يوجد عناصر بـ A_4}

① $\forall f, g \in A_4$ s.t $f \circ g \in A_4$

تركيب الدالة الزوجية مع الدالة الزوجية الاخرى ينتمي الى A_4 الاعداد الزوجية

② asso is hold in S_4 then its hold in A_4

③ $I \in A_4$ s.t $I \circ f = f \circ I = f$ $\forall f \in A_4$

④ $\forall f \in A_4$ $\exists f^{-1} \in A_4$ s.t $f \circ f^{-1} = f^{-1} \circ f = I$

$\therefore (A_4, \circ)$ is a subgroup

Ex) Let $(Z_{12}, +_{12})$ is a group

$$H = \{[0], [2], [4], [6], [8], [10]\}$$

Show that $(H, +_{12})$ is a subgroup of a group $(Z_{12}, +_{12})$

sol $H \neq \phi$

① $\forall [a], [b] \in H$ s.t $[a] +_{12} [b]$

$$= [(a+b) \bmod 12)] \in H$$

② ass is hold in Z_{12} then its hold in H

③ $[0] \in H$ S.t $[0] +_{12} [a] = [a] +_{12} [0] = [a]$

$\forall a \in H$

④ inverse

$\forall [a] \in H \ \exists [a]^{-1} = [n-a] \in H$

s.t $[a] +_{12} [a]^{-1} = [a]^{-1} +_{12} [a] = [0]$

$\therefore (H, +_{12})$ is a subgroup

of a group $(Z_{12}, +_{12})$

نظرية (٣) برهانها غير مطلوب

الموضوع : التاريخ : / /

Remark Every group $(G, *)$ has two sub group namely G and $[e]$, thes subgroups are called (trivial subgroup), other than trivial is called a proper sub group

١) العنصر المحايد في الزمرة الجزئية هو نفسه الموجود في الزمرة الرئيسية
٢) معكوس اي عنصر في sub group هو نفسه في الزمرة الرئيسة
٣) ترتيب اي عنصر في المجموعة الجزئيه هو نفسه ترتيب العنصر في الزمره الرئيسية

Remarks

① Every subgroub of an abelian group is abelian

كل مجموعة جزئية من كروب ابدالي تكون ابدالية

② A non - abelian group may have an abelian subgroub

الزمرة الرئيسيه غير ابدالية ممكن احتوائها على زمرة ابدالية مثل A_3

Ex A group $(S_3, \circ)$ is non abelian but a sub group $(A_3, \circ)$ is a ~~beline~~ abelian

③ A non-abelian group may have a nonabelian supgroup

زمرة الجداول

Ex A non-abelian group $(S_4, \circ)$ has a non abelian sub group $(A_4, \circ)$

الجزء الأول

Th. 3.1 If $(G, *)$ is a group then $(H, *)$ is a subgroup iff $a * b^{-1} \in H, \forall a, b \in H$

الجزء الثاني

Proof: $\Rightarrow$ suppose that $(H, *)$ is a subgroup

T.P $a * b^{-1} \in H, \forall a, b \in H$

$\because a \in H, b \in H \Rightarrow b^{-1} \in H$

$\therefore a * b^{-1} \in H, \forall a, b \in H$

$\Leftarrow$ suppose that $a * b^{-1} \in H$

$\forall a, b \in H$, T.P $(H, *)$ is a subgroup

① $a \in H, b \in H \Rightarrow a \in H, b^{-1} \in H$

$\Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$

② ass hold in G then its hold in H

③ $\because a \in H \Rightarrow a^{-1} \in H \Rightarrow a * a^{-1} \in H \Rightarrow e \in H$

④ $a * b^{-1} \in H, \forall a, b \in H$

$a \in H, b^{-1} \in H, \forall a, b \in H$

$\therefore \forall b \in H, \exists b^{-1} \in H$ $\therefore (H, *)$ is a group

$\therefore (H, *)$ is a subgroup

زمرة جزئية (G)

الموضوع :   التاريخ : / /

تشكيله تقاطعات

Th. 3.2 The intersection of any collection of subgroups of a group $(G, *)$ is a subgroup of G

Proof: Let $\{H_i ; i \in I\}$ be a collection of subgroups of a group G

$\bigcap \{H_i ; i \in I\} \neq \phi$ since $\exists\, e \in H$

$\therefore e \in \bigcap H_i$

Let $a, b \in \bigcap H_i$ T.P $a * b^{-1} \in \bigcap H_i \quad \forall i \in I$

زمرة جزئية

$\Rightarrow a, b \in H_i, \forall i \in I$

$\therefore a * b^{-1} \in H_i, \quad \forall i \in I$

$\therefore a * b^{-1} \in \bigcap H_i, \quad \forall i \in I$ (by Th 3.1)

$\therefore (\bigcap_{i \in I} H_i, *)$ is sub group

3.3 النظرية

التاريخ: ١٤ / ١ / ٢٠١٦ الموضوع:

اذا اعطانا بالسؤال (if only if) يعني لازم انبرهن بالاتجاهين

Th. 3.3 The union of two subgroups of a group $(G, *)$ is a subgroup iff one contained in the other

Proof $\Leftarrow$

Let $(H_1, *)$, $(H_2, *)$ be two subgroup of G

Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

T.P $H_1 \cup H_2$ is subgroup

Since $H_1 \subseteq H_2 \Rightarrow H_1 \cup H_2 = H_2$

Since H_2 is subgroup $\Rightarrow H_1 \cup H_2$ is subgroup

الحالة الثانية

since $H_2 \subseteq H_1 \Rightarrow H_1 \cup H_2 = H_1$

Since H_1 is subgrup $\Rightarrow H_1 \cup H_2$ is subgroup

تكملة النظرية

التاريخ: ١٤ / ١ / ٢٠١٦ المرضوع :

الاتجاه الثاني $\Rightarrow$ Let H_1 and H_2 be a subgroups of G and $H_1 \cup H_2$ 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 $\exists b \in H_2, b \notin H_1$

$\because a \in H_1 \Rightarrow a \in H_1 \cup H_2$

$\because b \in H_2 \Rightarrow b \in H_1 \cup H_2$

$\because H_1 \cup H_2$ is subgroup

$\therefore a * b \in H_1 \cup H_2$

$\Rightarrow a * b \in H_1$ or $a * b \in H_2$

$\because H$ is subgroup

$\Rightarrow a \in H_1 \Rightarrow a^{-1} \in H_1 \Rightarrow a * b \in H_1$

$\Rightarrow \underbrace{a^{-1} * a}_{e} * b \in H_1 \Rightarrow b \in H_1$ C تناقض لانا بالفرضيه $b \notin H_1$

$\because a * b \in H_2$ and H_2 is subgroup

$b \in H_2 \Rightarrow b^{-1} \in H_2$, $a * \underbrace{b * b^{-1}}_{e} \in H_2 \Rightarrow a \in H_2$ C!

$\therefore H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

التاريخ: ١٨ / ١ / ٢٠١٦
الاثنين

الموضوع :

عملية ضرب بين مجموعتين او (معالجة)

Def: Let H and K be two subgroups of a group G, Then the Product of H and K denoted by $H * K$ is defined by $H * K = \{h * k : h \in H, k \in K\}$

Remark

① $H^{-1} = \{h^{-1} : h \in H\} = H$

② $(H * K) * L = H * (K * L)$

③ $H * (K \cup L) = H * K \cup H * L$

④ $H * (K \cap L) \subseteq H * K \cap H * L$

⑤ $(H * K)^{-1} = K^{-1} * H^{-1}$ حاصل ضرب مجموعتين يعطينا المعكوس للمجموعة
عالتعريف

⑥ $H * H^{-1} = H \rightarrow$ نستخدم المجموعة كاملة من ضمنها (identity)

$K * K^{-1} = K$ $\quad H * H^{-1} = H$

التاريخ: / / الموضوع:

Theorem 3.4: If (H, K) are subgroups of G then $H*K$ is subgroup iff $H*K = K*H$

تحقق شرط الابدال

Proof $\Rightarrow$ suppose that $H*K$ is subgroup

T.P $H*K = K*H$

$\because H*K$ is subgroup

$(H*K)^{-1} = H*K$

$\therefore K^{-1}*H^{-1} = H*K$

$\therefore K*H = H*K$

$\Leftarrow$ suppose that $H*K = K*H$

T.P $H*K$ is subgroup

To show $\underbrace{(H*K)}_{\text{subgroup}} * \underbrace{(H*K)^{-1}}_{\text{معكوسها}} = \underbrace{H*K}_{\text{نفسها المجموعة}}$

$(H*K)*(H*K)^{-1} = H*\underbrace{K*K^{-1}}_{K}*H^{-1} = H*K*H^{-1}$

$= \overbrace{K*H}^{H}*H^{-1} = K*H = H*K$

$\therefore H*K$ is subgroup

$\mathbb{Z} \bmod 12$

التاريخ: 2016 / 1 / 18 صفوف تطابق

الموضوع :

Ex) $(Z_{12}, +_{12}) = \{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\}$

is a group, $H_1 = \{[0],[6]\}$, $H_2 = \{[0],[4],[8]\}$

2) $H_1 * H_2 = \{0, 6\} +_{12} \{0, 4, 8\}$ كل عنصر بالمجموعة الاولى نجمع مع كل عناصر المجموعة الثانية

$= \{0 +_{12} 0, 0 +_{12} 4, 0 +_{12} 8, 6 +_{12} 0, 6 +_{12} 4, 6 +_{12} 8\}$

$= \{[0],[4],[8],[6],[10],[2]\}$ اذا الناتج اكبر من (١٢) نطرح من المجموع ١٢

ترتيب من عندي $= \{0, 2, 4, 6, 8, 10\}$

١) الانغلاق عند جمع اي عنصرين الناتج يكون موجود في المجموعة

1) $\forall$ all $[a],[b] \in S$. s.t $[a] +_{12} [b]$

$= [(a+b) \bmod_{12}] \in S$

2) asso تتحقق $([a]*[b])*[c]$

3) identity $\{[0]_* \in S\}$

4) inverse كل عنصر نجمعه مع معكوسه يعطينا

$\forall [a] \in S, \exists\ [a]^{-1} = [n-a] \in S$

s.t $[a] +_{12} [a]^{-1} = [a]^{-1} +_{12} [a] = [0]$

الموضوع : مركز الزمرة

التاريخ : ٢٠ / ١ / ٢٠١٦

العناصر التي تحقق خاصية الابدال مع كل عناصر الزمرة نجمعها و نسميها (مركز الزمرة)

Def: The Center of group $(G, *)$ denoted by $C(G)$ is the set ~~C(G) = {a ∈ G~~

Center group $C(G) = \{a \in G : a * b = b * a, \forall b \in G\}$ احفظ

Ex in the groups

$(Z, +) \Rightarrow C(Z)$

$(Z, +_{10}) \Rightarrow C(Z_{10}) = Z_{10}$

مجموعة التباديل من (٤) عناصر $(S_4, o) \Rightarrow C(S_4) = \{I\}$

تباديل زوجية من (S_4) $(A_4, o) \Rightarrow C(A_4) = \{I\}$

$(S_3, o) \Rightarrow C(S_3) = \{I\}$

$(A_3, o) \Rightarrow C(A_3) = A_3$

تباديل زوجية من (S_3)

الاربعاء

2016/ 1/20 التاريخ: الموضوع :

Theorem 3.5: If $(G, *)$ is a group then $(C(G), *)$ is a sub group

Proof:- $e * a = a * e$, $\forall a \in G$

$\therefore e \in C(G) \Rightarrow C(G) \neq \emptyset$

Let $a, b \in C(G)$

$\therefore a * x = x * a$ and $b * x = x * b$, $\forall x \in G$

Then if $y \in G$, T.P $(a * b^{-1}) \in C(G)$

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

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

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

حقق شرط الابدال

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

$\therefore (a * b^{-1}) \in C(G)$ by Th.(3.1)

$\therefore (C(G), *)$ is Subgroup

الموضوع : ―――――――― التاريخ: ٢٥ / ١ / ٢٠١٦

تعريف cyclic

Def / A group $(G, *)$ is Said to be cyclic group, if $\exists\, a \in G$ s.t $\forall\, b \in G \Rightarrow b = a^n$, $n \in Z$, the element a is Called the generator of G, and we write $G = (a)$

Ex: A group $(Z, +)$ is Cyclic group generated by 1 (مولدة بواسطة), $(1)^1 = 1$, $(Ze, +)$ is cyclic group generated by 2 (مولدة بواسطة)

$1^2 \Rightarrow 1+1 = 2$

$1^3 \Rightarrow 1+1+1 = 3$

Ex: A group $(C_3, \cdot)$ (عملية الضرب) where C_3 is the set of all Cube roots of unity

Sol: $C_3 = \{1, w, w^2\}$

$C_3 = (w)$ since

$w^1 = w$	$(w^2)^1 = w^2$
$w^2 = w^2$	$(w^2)^2 = w$
$w^3 = 1$	$(w^2)^3 = 1$

$\therefore (C_3, \cdot)$ is cyclic group

عملية الضرب

$(w)^6 = 6$

تحذف عناصر عوامل الـ(٦) تبقى مفردة 1

التاريخ : / / الموضوع :

جدول زمرة جزئية

Ex $(Z_4, +_4)$ is a group find all subgroups

ج) $Z_4 = \{[0], [1], [2], [3]\}$

$[0]^1 = [0]$, $[0]^2 = [0]$

$[1]^1 = [1]$

$[1]^2 = [1] +_4 [1] = [2]$

$[1]^3 = [1] +_4 [1] +_4 [1] = [3]$

$[1]^4 = [1] +_4 [1] +_4 [1] +_4 [1] = [4] - 4 = [0]$

$(([2]) = \{[2], [4]\}$

$([3]) = \{[3], [2], [1], [0]\} = Z_4$

$Z_4 = ([1]) = ([3])$

$[3]^1 = [3] \rightarrow n = 1$

$[3]^2 = [2]$ $\quad [3] +_4 [3] = [6-4] = [2]$

$[3]^3 = [1]$ $\quad [3] +_4 [3] +_4 [3] = 6-4 = 2+3 = 5-4 = [1]$

$[3]^4 = [0]$

$\therefore (Z_4, +_4)$ is cyclic group

all the subgroups is $(([0]), +_4)$

$(([1]), +_4)$, $(([2]), +_4)$

$(S_n, \circ) \rightarrow$ is not cyclic group

Theorem 3.6 Every cyclic group is commutative.

Proof Let $G = (a)$ be a cyclic group generated by a.

Let $x, y \in G \Longrightarrow x = a^m, y = a^n$, $m, n \in \mathbb{Z}$

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

$$= a^n * a^m = y * x$$

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

Remark A Com. group is not always a cyclic group

Ex. $(\mathbb{R}, +)$ is Com. group but not Cyclic

Remark

① If an element a is generator of cyclic group G, then a^{-1} is also generator of G

② The order of cyclic group is the same of the order of its generator

التاريخ : / / الموضوع :

Theorem 3.7 Every Subgroup of cyclic group is cyclic.

Proof Let $(G=(a), *)$ is cyclic group generated by a

Let $(H, *)$ is a subgroup of G

if $H = G$ and $H=\{e\}$ then H is cyclic

if $H \neq G$ and $H \neq \{e\}$, if $a^m \in H$, $m \in Z$ then $a^{-m} = H$

hence H Contain Positive integer Power of a

Let n be the Smalest Positive integer

S.t. $a^n \in H$

To Show $H = (a^n)$

T.P $H \subseteq (a^n)$

Let $a^k \in H$, $K \in Z$

التاريخ : / /　　　　　　　　　　　　الموضوع :

by divition algorithem then

$\exists\, q, r \in \mathbb{Z}$ S.t $K = qn + r$, $0 \leq r < n$

$\because a^n, a^K \in H$ then

$a^r = a^{K-qn} = a^K * (a^n)^{-q} \in H$

if $r > 0$ C! Since $r < n$ and (n) is the

Smalest Positive integer S.t $a^n \in H$

$\therefore r = 0$ and $K = qn$

$\therefore a^K \in (a^n)$　　　$\therefore H \subseteq (a^n)$

Now T.P $(a^n) \subseteq H$

Let $(a^n)^m \in (a^n)$

$\because a^n \in H$ and H is Closed Under $*$

لان (G) هي زمرة تحقق الشروط الاربعه بيها

و (H) هي جزء من G

$\therefore (a^n)^m \in H$

$\therefore (a^n) \subseteq H$

$\therefore H = (a^n) \Rightarrow \therefore (H, *)$ is Cyclic subgroup

التاريخ : / /   الموضوع :

Ex $(\mathbb{Z}_8, +_8)$ is Cyclic group $\mathbb{Z}_8 = ([1])$

$$H = \{[0], [2], [4], [6]\}$$

$(H, +_8)$ is Cyclic Subgroup.

$[0]^1 = [0]$

$[0]^2 = [0] +_8 [0] = [0]$

$[2]^1 = [2]$

$[2]^2 = \cancel{[4]}\ [2] +_8 [2] = 4$

$[2]^3 = [6]$

$[2]^4 = [8] = 0$

2016/2/1 التاريخ: الموضوع: ______

Ex) find all Subgroups and generators of a group $(Z_{12}, +_{12})$

Solution)

$Z_{12} = \{[0], [1], [2], \dots [11]\}$

$([0]) = \{[0]\}$

$([1]) = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [0]\}$

$([2]) = \{[2], [4], [6], [8], [10], [0]\}$

$([3]) = \{[3], [6], [9], [0]\}$

$([4]) = \{[4], [8], [0]\}$

$([5)] = \{[5], [10], [3], [8], [1], [6], [11], [4], [9], [2], [7], [0]\} = Z_{12}$

$([6]) = \{[6], [0]\}$

-12

$+7 \quad +7$

$([7]) = \{[7], [2], [9], [4], [11], [6], [1], [8], [3], [10], [5], [0]\} = Z_{12}$

$7+7=14-12=$

التاريخ : / /   الموضوع :

$8+8=16 \xrightarrow{-12}$

$([8]) = \{[8], [4], [0]\}$

$([9]) = \{[9], [6], [3], [0]\}$

$([10]) = \{[10], [8], [6], [4], [2], [0]\}$

$([11]) = \{[11], [10], [9], [8], [7], [6], [5],$
$[4], [3], [2], [1], [0]\} = Z_{12}$

$\therefore$ The Subgroup of $(Z_{12}, +_{12})$ is

$([0]), +_{12})$, $(([1]), +_{12})$, $(([2]), +_{12})$

$(([3]), +_{12})$, $(([4]), +_{12})$, $(([6]), +_{12})$

المجموعات المتشابهة لا تتكرر
مثل $([8]) = ([4])$

تعطينا فقط الصفر المحايد

$\oplus$ The trevial Subgroups is
$(([0]), +_{12})$ and $(([1]), +_{12})$
(1) يعطينا عناصر Z_{12}

$\oplus$ The Proper Subgroups is
$(([2]), +_{12})$, $(([3]), +_{12})$, $(([4]), +_{12})$

$(([6]), +_{12})$

The generators of $(Z_{12}, +_{12})$ is $\{[1], [5], [7], [11]\}$

الموضوع : ______ التاريخ : / /

Ex $(Z_{10}, +_{10})$ is a group

$H = \{[0], [2], [4], [6], [8]\}$

$K = \{[0], [5]\}$ find $K +_{10} H$

$K +_{10} H = \{[0] +_{10} [0], [0] +_{10} [2], [0] +_{10} [4], [0] +_{10} [6], [0] +_{10} [8],$
$[5] +_{10} [0], [5] +_{10} [2], [5] +_{10} [4], [5] +_{10} [6],$
$[5] +_{10} [8]\}$

$= \{[0], [2], [4], [6], [8], [5], [7], [9], [1], [3]\}$

طلعت عناصر (Z_{10})

التاريخ: 2016 / 2 / 22 — الموضوع :

Proposition: If $(G, *)$ is a finite cyclic group of prim order then G has no proper subgroup

Def: Let $(H, *)$ be a subgroup of group $(G, *)$ and $a \in G$, the the set $a * H = \{a * h : h \in H\}$ is called a left coset of H in G.

تعريف

the element a is a representative of $a * H$ In a similar way we can define the right coset

$$H * a = \{h * a : h \in H\}$$

Remarks:

① Since $e \in H \Rightarrow a * e \in a * H$
$= a \in a * H$

$\therefore a * H \neq \emptyset$

② In general $a * H = H * a$ if G is Commutative group.

Ex: A group $(G, \cdot)$ where $G = \{i, -i, 1, -1\}$
and $H = \{-1, 1\}$

$i \cdot H = \{i(-1), i(1)\} = \{-i, i\}$

$i \cdot H = H$

$-1 \cdot H = \{-1(-1), -1(1)\} = \{1, -1\} = H$

$-i \cdot H = \{-i(-1), -i(1)\} = \{i, -i\}$

الموضوع: ______ التاريخ: / /

Ex A group $(Z,+)$, Let $H=\{3n : n \in Z\}$
مضاعفات العدد (٣)

$Z + H$

$0 + H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$1 + H = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$2 + H = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

$Z = (0+H) \cup (1+H) \cup (2+H)$

Ex The ~~syme~~ symetric group (S_3, o)

where $H = \{I, (123), (132)\}$ is a subgroup of G.

$(12) o H = \{(12), (23), (13)\}$

$= (13) o H = (23) o H$

معكوسه

$(123) o H = \{(123), (\boxed{132}), I\} = (132) o H$

اذا ناخذها مع H نقطينا نفس هذا الناتج نفس المجموعه

$(12) o (123)$

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

$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$

$S_3 = \{I, (12)(13)(23), (123), (132)\}$

2016 / 2 / 24 :التاريخ   الموضوع :

Ex Let $K = \{I, (12)\}$

$(23) \circ K = \{(23), (132)\}$

$\cancel{K \circ H}$ $K \circ (23) = \{(23), (123)\}$

$\therefore (23) \circ K \neq K \circ (23)$

Th. 3.8: If $(H, *)$ is a subgroup of a group G then $a * H = H$ iff $a \in H$

proof: $\Rightarrow$ Let $a * H = H$, T.P $a \in H$

Let $a * e \in a * H \Rightarrow a \in H$

$\Leftarrow$ Let $a \in H$, T.P $a * H = H$

Let $x \in a * H \Rightarrow x = a * h, h \in H$

$\Rightarrow x \in H \Rightarrow a * H \subseteq H$

and Let $y \in H \Rightarrow e * y = (a * a^{-1}) * y$

$= a * (a^{-1} * y) \in a * H \Rightarrow y \in a * H$

$\therefore H \subseteq a * H$

$\therefore a * H = H$

2016/ 2 / 24 :التاريخ   الموضوع :

Th. 3.9 if $(H, *)$ is a Subgroup of a group G and $a, b \in G$, then $a*H = b*H$ iff $a^{-1}*b \in H$

Proof $\Rightarrow$ Let $a*H = b*H$, T.P $a^{-1}*b \in H$

Let $x \in a*H \Rightarrow x = a*h$, $h \in H$

$\because x \in b*H \Rightarrow x = b*h_1$, $h_1 \in H$

$\therefore b*h_1 = a*h$

$a^{-1}*b = h*h_1^{-1} \in H$ $\therefore a^{-1}*b \in H$

$\Leftarrow$ Let $a^{-1}*b \in H$, T.P $a*H = b*H$

$\because a^{-1}*b \in H$

$\therefore a^{-1}*b = h$, $h \in H$

$\therefore b = a*h$

$\therefore b*H = (a*h)*H = a*(h*H) = a*H$

by Th. 3.8

التاريخ : / /   الموضوع :

Th 3.10 if $(H, *)$ is a subgroup of a group G, $a, b \in G$, then either $a * H$ and $b * H$ are disjoint or else $a * H = b * H$

Proof Let $a * H \cap b * H \neq \phi$

$\therefore \exists x \in a * H \cap b * H$

$\Rightarrow x \in a * H$ and $x \in b * H$

$\therefore x = a * h_1$ and $x = b * h_2$, $h_1, h_2 \in H$

$\therefore a * h_1 = b * h_2$

$a^{-1} * b = h_1 * h_2^{-1} \in H$

$\Rightarrow a^{-1} * b \in H$ by Th. 3.9

$\Rightarrow a * H = b * H$

Th. 3.11 (~~Lagrange~~)

The order and index of any subgroup of a finite group divides the order of the group.

Proof: Let H be a subgroup of a finite group G, then H is finite

Let $|H| = m$ and $|G| = n$

Let $H = \{h_1, h_2, \dots, h_m\}$ where h is ~~distinct~~ are distinct, Now Let $a \in G$

مختلفة العناصر

~~distin~~

then $a * H = \{a*h_1, \dots, a*h_m\}$

all element of $a*H$ are distinct

$\therefore |a*H| = m$

$\Leftarrow$

Now if G Contain K distinct Cosets of H in G

$\because |G| = n$ and $\frac{|G|}{|H|} = K$

$\therefore n = mK$

$\therefore$ the order of H and index of H in G divisor the order of G

index → K

Ex) If $H = \{0, 6, 12, 18\}$ is cyclic subgroup of $(Z_{24}, +_{24})$ find No of all distinct Left Coset of H in Z_{24}

Sol) $|Z_{24}| = 24$, $|H| = 4$

$\therefore \frac{|G|}{|H|} = \frac{24}{4} = 6$

Ex Let $H=\{I,(123),(132)\}$ be a subgroup of S_3 find index H

Sol $\frac{|S_3|}{|H|} = \text{index } H$

$\therefore \text{index}.H = \frac{6}{3} = 2$

Ex if $H=\{[0],[3],[6],[9]\}$ be a subgroup of a group G and index $H=3$ find $|G|$

Sol $\frac{|G|}{|H|} = \text{index } H$

$\therefore |G| = |H| \text{ index}.H = 4 \cdot 3 = 12$

2016 / 3 / 2 التاريخ : الموضوع :

نتيجة

Corollary (1) The order of every element of finite group is divisor of the order of the group

Proof Let G be a finite group of order (n) and $a \in G$, $O(a)$ is finite $\forall a \in G$

Let $O(a) = m$

Let $H = \{a, a^2, a^3, \ldots, a^m = e\}$ where all ~~a's~~ a_i's are distinct

$\therefore |H| = m$

by lagrang th. $\Rightarrow |H|$ is a divisor of $|G|$

$\therefore \exists K \in Z^+$ s.t $\frac{n}{m} = K \Rightarrow \frac{|G|}{O(a)} = K$

i.e the order of element a divisor of order G.

التاريخ: / /   نتيجة ②   الموضوع :

Corollary 2 For an element a of a finite group G then $a^{|G|} = e$

proof: Let G be a finite group $|G| = n$

and $a \in G \Rightarrow O(a) = m$, $a^m = e$

by Corollary ① $\Rightarrow O(a)$ divisor of $|G|$

i.e. m is divisor of n

s.t $n = mK$, $K \in Z^+$ (اي رقم)

$$a^{|G|} = a^n = a^{mK} = (a^m)^K = e^K = e$$

$$\therefore a^{|G|} = e$$

Ex Let a finite group $(Z_4, +_4)$

$Z_4 = \{[0], [1], [2], [3]\}$

$[0]^4 = [0] +_4 [0] +_4 [0] +_4 [0] = [0]$

$[1]^4 = [1] +_4 [1] +_4 [1] +_4 [1] = [0]$

$[2]^4 = [2] +_4 [2] +_4 [2] +_4 [2] = [0]$

$[3]^4 = [3] +_4 [3] +_4 [3] +_4 [3] = [0]$

Chapter Four

2016 / 3 / 7 التاريخ : الموضوع :

Def: A subgroup $(H, *)$ of a group $(G, *)$ is said to be a normal subgroup iff $a * H = H * a \ \forall a \in G$

Ex In the group $(S_3, \circ)$ and
$H = \{I, (123), (132)\}$

Sol Since $\forall f \in S_3 \Rightarrow f \circ H = H \circ f$

$\therefore$ H is normal subgroup

but $H = \{I, (23)\}$, $S_3 = \{I, (12), (13), (23), (123), (132)\}$

$(12) \circ H = \{(12), (123)\}$

$H \circ (12) = \{(12), (132)\}$

$(12) \circ H \neq H \circ (12)$

$\therefore$ H is not normal subgroup

Ex In the group $(Z_{12}, +_{12})$ and

$H = \{[0], [3], [6], [9]\}$

ابدالي عملية الجمع (ابدالية)

Sol Since $\forall [a] \in Z_{12} \Rightarrow [a] +_{12} H = H +_{12} [a]$

$\therefore$ H is normal subgroup

الكروب الدوري كل كروب بداخله هو normal

Remark Every cyclic group is Com. group if follow that every subgroup of cyclic group.

٢٠١٦ / ٣ / ٨ التاريخ : الموضوع :

Theorem 4.1 A subgroup H of a group $(G, *)$ is normal iff $a*H*\bar{a}^{1} \subseteq H$, $\forall a \in G$.

proof: $\Rightarrow$ Let H be normal subgroup of a group G T.P $a*H*\bar{a}^{1} \subseteq H$ $\forall a \in H$

$\therefore a*H = H*a, \forall a \in G$ if $h \in H \Rightarrow$

$a*H = h_1 * a$ for same $h_1 \in H$ نضرب بـ $\bar{a}^{1}$

~~$a*h$~~ $\therefore a*h*\bar{a}^{1} = h_1 \in H$

$\therefore a*H*\bar{a}^{1} \subseteq H, \forall a \in G$

$\Leftarrow$ Now Let H be a subgroup of G s.t $a*H*\bar{a}^{1} \subseteq H, \forall a \in G$

T.P H is normal

i.e $a*H = H*a$. if $a \in G$, $h \in H$

$\Rightarrow a * h * a^{-1} \in H$

$a * h \in a * H$

$\therefore a * h = a * h * a^{-1} * a$

$= (a * h * a^{-1}) * a \in H * a$

$\therefore a * H \subseteq H * a$ —— ①

Let $h * a \in H * a$

$\therefore h * a = a * a^{-1} * h * a$

$= a * (a^{-1} * h * a) \in a H$

$\therefore H * a \subseteq a * H$ —— ②

From ①, ② We get

$a * H = H * a$

$\therefore (H, *)$ is normal Subgroup.

Remarks If $(G, *)$ is a group then

① $C(G)$ is normal Subgroup

② $\{e\}$ and G are normal Subgroup

Proof: by Th. 3.1 $(C(G), *)$ is Subgroup

Let $x \in G$ and $a \in C(G)$

$$x * a * x^{-1} = (x * a) * x^{-1}$$

$$= (a * x) * x^{-1}$$

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

$$= a \in C(G)$$

$\therefore x * a * x^{-1} \in C(G)$

$\therefore x * C(G) * x^{-1} \subseteq C(G)$ by Th. 4.1

$\therefore C(G)$ is normal Subgroup

الموضوع : ______________ التاريخ : / /

التاريخ: ١٤ / ٣ / ٢٠١٦
الموضوع: تعريف العناصر المترابطة

Def: An element a of group$(G, *)$ is said to be conjugate element to $b \in G$ $\exists x \in G$ s.t $\boxed{a = x^{-1} * b * x}$

Ex: I a symmetric group (S_3, o)

Let $a = (132)$, $b = (123)$ and $x = (12)$, $x^{-1} = (12)$ s.t

$$\underset{a}{(132)} = \underset{x^{-1}}{(12)}\, \underset{o}{o}\, \underset{b}{(123)}\, \underset{o}{o}\, \underset{x}{(12)}$$

$$= (12)\, o\, (13) = (132)$$

$\therefore$ a Conjugate to b

$a = (12)$, $b = (23)$, $x = (13)$, $x^{-1} = (13)$

$$(12) = (13)\, o\, (23)\, o\, (13)$$

$$= (13)\, o\, (123) = (12)$$

$\therefore$ a Conjugate b

Def : Let $(G,*)$ be a group and $a \in G$ then the Conjugate class of a is denoted by $C(a)$ and defined by

$$C(a) = \{b \in G : b = x * a * x^{-1}\}$$
$$= \{x * a * x^{-1}, \forall x \in G\}$$

Ex : Find all Conjugate class of each element in $(G,*)$ where $G = \{1, -1, i, -i\}$

Sol : $C(-i) = \{x * (-i) * x^{-1}, \forall x \in G\}$

$$= \{1 * (-i) * (1)^{-1}, -1 * (-i) * (-1)^{-1}, i * (-i) * i^{-1}, -i * (-i) * (-i)^{-1}\}$$

$$= \{-i, -i, -i, -i\} = \{-i\}$$

$$C(i) = \{i\}$$

التاريخ : / /　　　　الموضوع :

Ex: In a group $(Z_3, +_3)$ find $C([2])$

$$C([2]) = \{x * [2] * x^{-1}, \forall x \in Z_3\}$$

$$= \{[0] +_3 [2] +_3 [0]^{-1}, [1] +_3 [2] +_3 \underbrace{[1]^{-1}}_{[2]}, [2] +_3 [2] +_3 \underbrace{[2]^{-1}}_{[1]}\}$$

$$= \{[2], [2], [2]\} = \{[2]\}$$

H.W: find all $C([a]), \forall [a] \in Z_4$

$C[0]$ $+_4$

Def Let H and K be two Subgroups of a group $(G, *)$, then K is Said to be Conjugate Subgroup to H if $\exists\, x \in G$ st $H = x * K * x^{-1}$

Ex In a group (S_3, o), Let $H = \{I, (12)\}$ and $K = \{I, (13)\}$ are two Subgroups of S_3. Is H Conjugate to K.

Sol

$$H = x * K * x^{-1}$$

if $= (2\,3)$, $H = (2\,3) o \{I, (1\,3)\} o (2\,3)$

$= (2\,3) o \{(2\,3), (1\,3\,2)\}$

if $x = (12)$ $= \{I, (1\,3)\} = K$

التاريخ : / /　　　　الموضوع :

$H = (12) \circ \{I, (13)\} \circ (12)$

$= (12) \circ \{(12), (123)\}$

$= \{I, (23)\}$

if $x = (13)$, $H = (13) \circ \{I, (13)\} \circ (13)$

$= (13) \circ \{(13), I\}$

$= \{I, (13)\} = K$

if $x = (123)$, $H = (123) \circ \{I, (13)\} \circ (132)$

$= (123) \circ \{(132) \circ (23)\}$

$= \{I, (12)\} = H$

$\therefore \exists (123) \in S_3$ s.t $\boxed{H = \underset{x}{(123)} \circ \underset{k}{K} \circ \underset{x^{-1}}{(132)}}$

$\therefore H$ Conjugate to K.

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

للتوضيح

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

Ex In a group $(Z_8, +_8)$, Let

$$H = ([2]) = \{[0],[2],[4],[6]\}$$

$$K = ([4]) = \{[0],[4]\}$$ IS H Conjugate K.

Sol if $x = [0]$, $H = x +_8 \{[0],[4]\} +_8 x^{-1}$

$$= [0] +_8 \{[0],[4]\} +_8 [0]$$

$$= [0] +_8 [0] +_8 \{[0],[4]\} = \{[0],[4]\} \neq H$$

if $x = [1]$, $H = [1] +_8 \{[0],[4]\} +_8 [7]$ معكوس (١) حتى يعطينا الصفر $0 = 8 - 8 = 1 + 7$

$$= [1] +_8 [7] +_8 \{[0],[4]\}$$

$$= \{[0],[4]\} = K$$

$\therefore \exists\, [a] \in Z_8$ S.t $H = [a] +_8 K +_8 [a]^{-1}$

$\therefore$ H Conjugate to K.

الموضوع :   التاريخ: /   /

Propositions خواص

① A Subgroups $(H, *)$ of group $(G, *)$ is said to be Self Conjugate iff $C(H) = H$

② A Subgroup $(H, *)$ of a group $(G, *)$ is Self Conjugate iff H is normal Subgroup of G

H is Conjugate with Self

$H = x * H * x^{-1}$

$\Leftrightarrow H * x = x * H$

$\therefore$ H is normal Sub.

التاريخ: / /   الموضوع:

Def. A group $(G,*)$ s.t. $G \neq \{e\}$ is said to be a simple group if it has no proper normal subgroup.

Ex A group $(Z_7, +_7)$ is simple group since Z_7 has no proper normal subgroup

Ex $(Z_{10}, +_{10})$ is not a simple group. Since $([2], +_{10})$ is a proper normal subgroup

Remark Every group of prime order is simple

Ex A group $(S_3, \circ)$ is not simple group since $A_3 = \{I, (123), (132)\}$ is proper normal subgroup of S_3.

/ / التاريخ: الموضوع :

Def Let $(H,*)$ be anormal Subgroup of agroup $(G,*)$ We define G/H by
$G/H=\{a*H : a\in G\}$ and $\otimes$ on G/H by

$a*H \otimes b*H = a*b*H$, $\forall$ $a*H$ and $b*H \in G/H$

Theorem 4.2 if $(H,*)$ is normal sub of agroup $(G,*)$ then $(G/H,\otimes)$ is agroup Called quotient group or Factor group

Proof $G/H=\{a*H : a\in G\}$

$\because e\in G \Rightarrow e*H\in G/H \Rightarrow G/H\neq\emptyset$

Now Let $a*H=c*H$ and $b*H=d*H$

T.P $a*b*H=c*d*H$

$\because a*H=c*H \Longrightarrow a*c^{-1}\in H$

$b*H=d*H \Longrightarrow b*d^{-1}\in H$

Now $(a*b)*(c*d)^{-1}=a*b*d^{-1}*c^{-1}$

$\because a*c^{-1}\in H$, $b*d^{-1}\in H$ and H normal

$\therefore a*(b*d^{-1})*a^{-1}\in H$

التاريخ : / /　　　　　　　　　　　　　　　　　　الموضوع :

$\Rightarrow a*(b*d^{-1})*a^{-1}*(a*c^{-1})\in H$

$\Rightarrow (a*b)*(c*d)^{-1}\in H$

$\Rightarrow a*b*H = c*d*H$

$\therefore \otimes$ is well define

① Let $a*H$ and $b*H \in G/H$

$a*H \otimes b*H = a*b*H \in G/H$

$\therefore a*H \otimes b*H \in G/H$

② Let $a*H,\ b*H,\ c*H \in G/H$

$((a*H)\otimes(b*H))\otimes(c*H)$

$=(a*b*H)\otimes(c*H)$

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

$=(a*H)\otimes((b*c)*H)$

$=(a*H)\otimes((b*H)\otimes(c*H))$

تكملة → المنظومة

الموضوع : التاريخ : / /

(3) The coset $H = e * H \in G/H$ is the identity element s.t. $(e*H) \otimes (a*H) = e*a*H = a*H$

and $(a*H) \otimes (e*H) = a*e*H = a*H$

(4) $\forall a*H \in G/H \Rightarrow \exists a^{-1}*H \in G/H$ s.t.
$(a*H) \otimes (a^{-1}*H) = a*a^{-1}*H = e*H = H$

and $(a^{-1}*H) \otimes (a*H) = a^{-1}*a*H = e*H = H$

$\therefore (G/H ; \otimes)$ is a group

Ex: A group $(S_3, \circ)$ and a normal subgroup $(A_3, \circ)$ then $(S_3/A_3, \circ)$ is the quotient group

Where $S_3/A_3 = \{A_3, (13) \circ A_3\}$.

Note: Every quotient group is com. group.

Def :- Let $(G, *)$ be a group and $a, b \in G$ the Commutator of a and b denoted by $[a, b]$ is defined by

$$[a, b] = a * b * a^{-1} * b^{-1}$$

Ex) In the group $(Z_6, +_6)$, find $[[2], [5]]$

Sol) $[[2], [5]] = [2] +_6 [5] +_6 [2]^{-1} +_6 [5]^{-1}$

$= [2] +_6 [5] +_6 [4] +_6 [1]$

$= [0]$

Ex) In the group $(S_3, \circ)$ find $[(12), (13)]$

Sol) $[(12), (13)] = (12) \circ (13) \circ (12)^{-1} \circ (13)^{-1}$

$= (12) \circ (13) \circ \underbrace{(12) \circ (13)}$

$= (12) \circ \underbrace{(13) \circ (132)}$

$= (12) \circ (23) = (123)$

Remarks:

① if $(G,*)$ is Com. group then $[a,b]=e$.

② The inverse of commutator is again a Commutator, s.t $[a,b]^{-1}=[b,a]$

Def Let $(G,*)$ be a group, then the derived subgroup or Commutater subgroup of $(G,*)$ denoted by $([G,G],*)$ where

$$[G,G]=\{\Pi[a_i,b_i] : a_i, b_i \in G\}$$

Where Π denoted to a Products of finitly many Commutators of G

$$f \circ g(x)=f(g(x))$$

التاريخ: / /　　　　　　　　　　الموضوع :

Theorem 4.3: The group $([G,G],*)$ is a normal subgroup of a group $(G,*)$

Proof: $e \in G \Rightarrow [e,e] \in [G,G]$

$\therefore [G,G] \neq \phi$

Let $x,y \in [G,G]$

$\Rightarrow x = [a_1,b_1]*[a_2,b_2]* \cdots *[a_n,b_n]$

and $y = [c_1,d_1]*[c_2,d_2]* \cdots *[c_n,d_n]$

$x*y^{-1} = [a_1,b_1]* \cdots *[a_n,b_n]*[c_1,d_1]^{-1}* \cdots *[c_n,d_n]^{-1}$

$= [a_1,b_1]* \cdots *[a_n,b_n]*[d_1,c_1]* \cdots *[d_n,c_n]$

$\therefore x*y^{-1} \in [G,G]$

$\therefore ([G,G],*)$ is subgroup

T.P $([G,G],*)$ is normal

تكملة في الصفحة التالية

تكملة النظرية

التاريخ : / /

الموضوع :

Let $x \in [G, G]$

T.P $x * [G, G] * x^{-1} \subseteq [G, G]$

Let $a \in \cancel{x} * [G, G] * x^{-1}$

$\therefore a = x * c * x^{-1}, \ c \in [G, G]$

$= x * c * x^{-1} * e$

$= \underline{x * c * x^{-1} * c} * c$

$= [x, c] * c \in [G, G]$

$\therefore a \in [G, G]$

$\therefore ([G, G], *)$ is normal Subgroup.

التاريخ : / /   الموضوع :

Theorem 4.4 Let $(H,*)$ be a normal subgroup of a group $(G,*)$ then $(G/H, \otimes)$ is commutative iff $[G,G] \subseteq H$

Proof. Let $a*H, b*H \in G/H$

which is commutative

$\therefore (a*H)\otimes(b*H) = (b*H)\otimes(a*H)$

$\Leftrightarrow (a*b)*H = (b*a)*H$

$\Leftrightarrow (a*b)*(b*a)^{-1} \in H$

$\Leftrightarrow [a*b] \in H$

$\Leftrightarrow [G,G] \subseteq H$

التاريخ : / /　　　　الموضوع :

Chapter five

Group Homomorphisms

تشاكلات الزمر

Def: Let $(G, *)$ and $(\acute{G}, \acute{*})$ be two groups, then a mapping $f:(G, *) \to (\acute{G}, \acute{*})$ is called a homomorphisms iff

$$f(a * b) = f(a) \acute{*} f(b), \forall a, b \in G$$

Ex: Let $f:(Z, +) \to (Z_e, +)$ s.t $f(n) = 2n$ $\forall n \in Z$ is f hom. or not

Sol: Let $n, m \in Z$

$$f(n+m) = 2(n+m) = 2n + 2m$$

$$= f(n) + f(m)$$

$\therefore f$ is hom.

الموضوع : ________ التاريخ : / /

Ex Let $f:(\mathbb{R},+) \to (\mathbb{R}^*,\cdot)$ s.t

$f(a)=e^a, \forall \in \mathbb{R}$ is f hom.

Sol Let $a,b \in \mathbb{R}$

$$f(a+b)=e^{a+b}=e^a\cdot e^b=f(a)\cdot f(b)$$

$\therefore f$ is homo.

Ex Let $f:(\mathbb{Z},+) \to (\mathbb{Z},+)$ s.t

$f(a)=2a+5 \quad \forall a \in \mathbb{Z}$, is f hom.

Sol Let $a,b \in \mathbb{Z}$

$$f(a+b)=2(a+b)+5$$

$$=2a+2b+5$$

$$f(a)+f(b)=2a+5+2b+5$$

$$\therefore f(a+b) \neq f(a)+f(b)$$

$\therefore f$ is not hom.

(٢)

Ex: Let $f:(\mathbb{Z},+) \longrightarrow (\mathbb{Z}_n, +_n)$

$f(a)=[a]$, $\forall a \in \mathbb{Z}$, is f hom.

Sol: Let $a, b \in \mathbb{Z}$

$f(a+b) = [a+b] = [a] +_n [b]$

$= f(a) +_n f(b)$ $\therefore f$ is hom.

الموضوع : ______ التاريخ : / /

Ex Let $f : (\mathbb{Z}, +) \to (\mathbb{R} - \{0\}, \cdot)$ defined by

$$f(n) = \begin{cases} 1 & \text{if } n \in \mathbb{Z}_e \\ -1 & \text{if } n \in \mathbb{Z}_{odd} \end{cases}$$

Show that f is hom.

Sol Let $n, m \in \mathbb{Z}$ then

① n and m are even.

$f(n+m) = 1 = 1 \cdot 1 = 1 = f(n) \cdot f(m)$

$\therefore f$ is hom.

② n and m are odd.

$1 + 3 =$ زوجي

$f(n+m) = 1$ (صورة العدد الزوجي في $f(n)$ هي (1)) ~~$f(n) \cdot f(m)$~~

$= (-1) \cdot (-1) = 1$ $\therefore f$ is hom.

$= f(n) \cdot f(m)$

~~③ n and m~~

③ one of them is even and other is odd

صوره العدد الفردي في السؤال (-1)

$f(n+m) = -1 = 1 \cdot (-1) = f(n) \cdot f(m)$ if n ev, (m) odd

$= (-1) \cdot 1 = f(n) \cdot f(m)$ $\therefore f$ is hom.

if n odd (m) even

Ex) Let $f = (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$, $f(a) = \ln a$

is f hom.

Sol) Let $a, b \in \mathbb{R}^+$

$$f(a \cdot b) = \ln(a \cdot b) = \ln(a) + \ln(b)$$
$$= f(a) + f(b)$$

$\therefore f$ is homo.

Ex) Let $f: (G, *) \to (G, *)$

$f(a) = x * a * x^{-1} \ \forall a \in G$ is f hom.

Sol) Let $a, b \in G$

$$f(a * b) = x * a * b * x^{-1}$$
$$= x * a * e * b * x^{-1}$$
$$= x * a * x^{-1} * x * b * x^{-1}$$
$$= f(a) * f(b) \quad \therefore f \text{ is hom.}$$

2016 / 4 / 4 :التاريخ الموضوع :

Theorem 5.7

if $f : (G, *) \longrightarrow (\acute{G}, \acute{*})$ is hom then

الجزء الأول (i) $f(e) = \acute{e}$, where e and $\acute{e}$ are identi[ties]
of G and $\acute{G}$ respectively.

الجزء (2) (ii) $f(a^{-1}) = f(a)^{-1}$

Proof (i) $a * e = a \Longrightarrow f(a * e) = f(a)$

$$\Rightarrow f(a) \acute{*} f(e) = f(a)$$

$$f(a)^{-1} \acute{*} f(a) \acute{*} f(e)$$

$$= f(a)^{-1} \acute{*} f(a)$$

$$\acute{e} \acute{*} f(e) = \acute{e} \; \cancel{\Rightarrow}$$

$$\Rightarrow f(e) = \acute{e}$$

٢

الجزء ②

(ii) $\because a * a^{-1} = e \Rightarrow f(a * a^{-1}) = f(e)$

$\Rightarrow f(a) \acute{*} f(a^{-1}) = \acute{e}$

$f(a^{-1}) \acute{*} f(a^{-1}) = \acute{e}$

$f(a^{-1}) \acute{*} f(a) \acute{*} f(a^{-1}) = f(a)^{-1} \acute{*} \acute{e}$

$\Rightarrow \acute{e} \acute{*} f(a^{-1}) = f(a^{-1}) \Rightarrow f(a^{-1})$

$= f(a)^{-1}$

Theorem 5.2 if $f : (G, *) \to (\acute{G}, \acute{*})$ is hom. then

الجزء الأول (i) if $(H, *)$ is a subgroup of G then $(f(H), \acute{*})$ is a subgroup of $\acute{G}$

Proof الجزء ① $f(H) = \{f(h) : h \in H\}$

Let $f(h_1) \acute{*} f(h_2)^{-1}$

$= f(h_1 * h_2^{-1})$

$\because h_1, h_2^{-1} \in H \Longrightarrow h_1 * h_2^{-1} \in H$

$\therefore f(h_1 * h_2^{-1}) \in f(H)$

$\therefore f(h_1) *' f(h_2)^{-1} \in f(H)$

$\therefore (f(H), *')$ is a sub group of G'

(2) (ii) $f^{-1}(H') = \{h ; f(h) \in H'\}$

Let $h_1, h_2 \in f^{-1}(H')$

$\Rightarrow f(h_1), f(h_2) \in H'$

$f(h_1 * h_2^{-1}) = f(h_1) *' f(h_2^{-1})$

$= f(h_1) *' f(h_2)^{-1}$

$\because f(h_1), f(h_2)^{-1} \in H'$

$\therefore f(h_1) * f(h_2)^{-1} \in H'$

$\therefore f(h_1 * h_2^{-1}) \in H'$

$\therefore h_1 * h_2^{-1} \in f^{-1}(H')$

$\therefore (f^{-1}(H'), *)$ is a sub group of G

Def:

1) A one-one hom. is called a monomorphism.

2) An onto hom. is called epimorphism.

3) A one-one and onto hom. is called (isomorphism)

4) A hom. of a group into it self is called endomorphism

5) An isomorphism of a group onto it self is called outomorphism.

Ex) If $f:(\mathbb{Z},+)\longrightarrow(\mathbb{Z}_e,+)$ defind by $f(n)=2n\ ,\ \forall n\in\mathbb{Z}$ is

① hom. ② epimorphism

③ isomorphism ④ outomorphism

Sol) Let $n, m\in\mathbb{Z}$

① $f(n+m)=2(n+m)=2n+2m$

$=f(n)+f(m)$

$\therefore f$ is hom.

② by ① f is hom.

$\because f(\mathbb{Z})=\{2n : n\in\mathbb{Z}\}=\mathbb{Z}_e$

~~$\therefore f$ is onto $\Rightarrow f$ is ep~~

$\therefore f$ is onto $\Rightarrow f$ is epimorphism

(3) by (1) (2) f is hom. and onto

Let $n, m \in Z$ s.t $f(n) = f(m)$

$\Rightarrow \cancel{2}n = \cancel{2}m \Rightarrow \therefore n = m$

$\therefore f$ is 1-1 $\Rightarrow f$ is isomorphism.

(4) by (3) f is isomorphism but $Z \neq Z_e$

$\therefore f$ is not onto marphism

Ex Let $f : (G, *) \rightarrow (G/H ; \circledast)$ s.t

$f(a) = a * H$ Show that

f is epimorphism.

Sol Let $a, b \in G$

$f(a * b) = a * b * H = a * H \otimes b * H$

$= f(a) \otimes f(b)$

$\therefore f$ is hom.

To show f is onto

$\forall\, a * H \in G/H,\ a \in G$

s.t $f(a) = a * H$

$\therefore G/H$ is the set of all imeges.

$\therefore f$ is onto $\Rightarrow f$ is epimorphism

الموضوع : ——————— التاريخ : / /

Def Let $f:(G,*) \to (\acute{G},\acute{*})$ be hom. and let $\acute{e}$ be the identity of $\acute{G}$, the Kernal of f denoted by $Ker(f)$ is the Set

$$Ker(f) = \{a \in G : f(a) = \acute{e}\}$$

Ex Let $f:(Z,+) \to (Z_e,+)$ s.t $f(n) = 2n$, $\forall n \in Z$ find $ker(f)$

Sol $Ker(f) = \{n \in Z : f(a) = \acute{e}\}$

$= \{n \in Z : 2n = 0\}$

$= \{n \in Z : n = 0\} = \{0\}$

Ex. Let $f:(\mathbb{R},+)\longrightarrow(\mathbb{R}^{+},\cdot)$ s.t $f(a)=e^{a}$ $\forall a\in\mathbb{R}$ find $\mathrm{Ker}(f)$.

Sol. $\mathrm{Ker}(f)=\{n\in\mathbb{R} : f(a)=1\}$

$$=\{a\in\mathbb{R} : e^{a}=1\}=\{0\}$$

Ex. Let $f:(\mathbb{Z},+)\longrightarrow(\mathbb{Z}_n,+_n)$ s.t $f(a)=[a]$ find $\mathrm{Ker}(f)$

Sol. $\mathrm{Ker}(f)=\{a\in\mathbb{Z} : f(a)=[0]\}$

$$=\{a\in\mathbb{Z} : [a]=[0]\}$$

$$=\{a\in\mathbb{Z} : a\equiv 0 \bmod n\}$$

$$=\{a\in\mathbb{Z} : a=kn,\ k\in\mathbb{Z}\}$$

$$=\{0,\mp n,\mp 2n,\mp 3n,\dots\}$$

٢٠١٦/ ٤ / ١٢ :التاريخ ٨ الموضوع :

Theorem 5.3: If $f:(G,*) \to (\acute{G}, \acute{*})$ is hom. then $(Ker(f), *)$ is normal Subgroup.

Proof: $Ker(f) \neq \phi$ Since $f(e) = \acute{e}$

Now let $a, b \in Ker(f) \Rightarrow f(a) = f(b) = \acute{e}$

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

$$= \acute{e} \acute{*} (\acute{e})^{-1} = \acute{e} \acute{*} \acute{e} = \acute{e}$$

$\therefore a * b^{-1} \in Ker(f) \Rightarrow (Ker(f), *)$ is Subgroup

Now To Prove $Ker(f)$ is normal we must Prove that $a * Ker(f) * a^{-1} \subseteq Ker(f)$, $\forall a \in G$

Let $x \in a * Ker(f) * a^{-1} \Rightarrow x = a * k * a^{-1}$
$k \in Ker(f)$

ناخذ (f) للطرفين

$$f(x) = f(a * k * a^{-1}) = f(a) \acute{*} f(k) \acute{*} f(a^{-1})$$

$$= f(a) \acute{*} \acute{e} \acute{*} f(a)^{-1}$$

$$= f(a) \acute{*} f(a)^{-1} = \acute{e}$$

$\therefore a * k * a^{-1} \in Ker(f)$

$\therefore (Ker(f), *)$ is normal Subgroup

2016/4/12 :التاريخ

الموضوع :

Theorem 5.4 if $f:(G,*)\to(G',*')$ is hom. then f is one-one iff $Ker(f)=\{e\}$

Proof: $\Rightarrow$ suppose that f is 1-1,

T.P. $Ker(f)=\{e\}$

Let $a\in Ker(f)\Rightarrow f(a)=e'$

$\because f(e)=e'\Rightarrow f(a)=f(e)$

$\Rightarrow a=e$ since f is 1-1

$\Rightarrow a\in\{e\}\Rightarrow Ker(f)\subseteq\{e\}$ — (1)

$\because e\in\{e\}$ s.t $f(e)=e'\Rightarrow e\in Ker(f)$

$\Rightarrow\{e\}\subseteq Ker(f)$ — (2)

from (1) (2) we get $Ker(f)=\{e\}$

$\Leftarrow$ suppose that $Ker(f)=\{e\}$

T.P f is 1-1

let $a,b\in G$ s.t $f(a)=f(b)$

$$\Rightarrow f(a) \acute{*} f(b)^{-1} = \acute{e}$$

$$\Rightarrow f(a) \acute{*} f(b^{-1}) = \acute{e}$$

$$\therefore a * b^{-1} \in Ker(f)$$

but $Ker(f) = \{e\}$

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

نضرب طرفي ال بـ (b) $\left[\therefore a * b^{-1} = e \Rightarrow a = b \right.$

$$a * \underbrace{b * b^{-1}}_{e} = \underbrace{e * b}_{b}$$

$\therefore f$ is 1-1

2016/4/20 التاريخ:

الموضوع:

Theorem 5.5

Every infinite Cyclic group is isomorphi

to $(Z,+)$.

Proof Let $(G,*)$ be acyclic group

generated by a, $\Rightarrow G=(a)$.

Let $f: G \to Z$ s.t. $f(a^m)=m$.

T.P f is isomorphism.

① T.P f is Well define

Let $a^m = a^n \Rightarrow m=n \Rightarrow f(a^m)=f(a^n)$

② T.P f is hom

$f(a^m * a^n) = f(a^{m+n})$

$= m+n = f(a^m)+f(a^n$

التاريخ : / /   الموضوع :

3) T.P f is 1-1

Let $a^n, a^m \in G$ s.t $f(a^n) = f(a^m)$

$\Rightarrow n = m \Rightarrow a^n = a^m$

4) T.P f is onto

$\forall n \in \mathbb{Z} \Rightarrow \exists a \in G$ s.t $a^n \in G$ where $f(a^n) = n$

$\therefore f$ is isomorphism
تشاكل

Theorem 5.6 (The factor theorem)

Let $f:(G,*) \to (G', *')$ be hom. of a group G onto G', then

$(G/Ker(f), \circledast) \cong (G', *')$.

Proof Let $g: G/Ker(f) \to G'$

defined by $g(a * Ker(f)) = f(a)$

$\forall a * Ker(f) \in G/Ker(f)$

① T.P g is well define

Let $a * Ker(f),\ b * Ker(f) \in G/Ker(f)$

s.t $a * Ker(f) = b * Ker(f)$

$\Rightarrow a * b^{-1} \in Ker(f) \Rightarrow f(a * b^{-1}) = e'$

$\Rightarrow f(a) *' f(b)^{-1} = e' \Rightarrow f(a) = f(b)$

$\Rightarrow g(a * Ker(f)) = g(b * Ker(f))$

الموضوع :   التاريخ :   /   /

② T.P. g is hom.

Let $a * Ker(f),\ b * Ker(f) \in G/Ker(f)$

$g(a * Ker(f) \otimes b * Ker(f)) = g(a * b * Ker(f))$

$= f(a*b) = f(a) \acute{*} f(b)$

$= g(a * Ker(f)) \acute{*} g(b * Ker(f))$

③ T.P. g is onto

$\forall f(a) \in \acute{G} \Rightarrow \exists a \in G$ s.t

$a * Ker(f) \in G/Ker(f)$

Where $g(a * Ker(f)) = f(a)$

$\therefore G/Ker(f) \cong \acute{G}$

نفس المعنى

$G/Ker(f)$ isomorphism

/ / التاريخ : الموضوع :

Ex Show that $(Z_{20}/\{[5],[10],[15],[0]\}, +_{20}) \cong (Z_5, +_5)$

Sol Let $f : Z_{20} \to Z_5$ defined by

$f([0]) = f([5]) = f([10]) = f([15]) = [0]$

$f(1) = f(6) = f(11) = f(16) = [1]$

$f(2) = f(7) = f(12) = f(17) = [2]$

$f(3) = f(8) = f(13) = f(18) = [3]$

$f(4) = f(9) = f(14) = f(19) = [4]$

To show f is hom.

$\forall [a],[b] \in Z_{20} \Rightarrow f([a] +_{20} [b])$
$= f([a]) +_5 f([b])$

$\therefore f$ is hom.

التاريخ: / / الموضوع :

② $f(Z_{20}) = \{[0], [1], [2], [3], [4]\} = Z_5$

$\Rightarrow f$ is onto

③ $Ker(f) = \{[0], [5], [10], [15]\}$

$\therefore$ by Th. 3.6 $(Z_{20}/[5], +_{20}) \cong (Z_5, +_5)$

The Chain

Def: Let $(H_i, *)$ be all subgroups of a group $(G, *)$, The chain of G is any finite sequence of subsets of G.

$$G = H_0 \supset H_1 \supset \cdots \supset H_{n-1} \supset H_n = \{e\}$$

The integer n is called the length of the chain.

Remark: if $n = 1$, then the chain is called trivial chain

Def: if $(H_i, *)$ is normal, $\forall i$ then the chain is called normal chain

Ex The group $(Z_6, +_6)$

$Z_6 \supset \{e\} = [0]$ trivial chain

$Z_6 \supset ([3]) \supset ([0])$ normal chain of length 2.

Ex A symmetric group $(S_3, \circ)$

$S_3 \supset A_3 \supset \{I\}$ is normal chain

Ex In a group $(Z_{16}, +_{16})$

$Z_{16} \supset ([2]) \supset ([4]) \supset ([8]) \supset ([0])$ is a chain of length 4.

التاريخ : / / الموضوع :

(EX) A group $(Z_{12}, +_{12})$

anormal cyclic subgroups is

$([2]) = \{[0], [2], [4], [6], [8], [10]\}$

and

$([3]) = \{[0], [3], [6], [9]\}$

~~are anormal~~

are amaximal normal subgroups

of $\cancel{Z_{12}}$ Z_{12}

The chain is

$Z_{12} \supset ([2]) \supset ([4]) \supset ([0])$

is composition chain since

$([2])$ is amaximal of Z_{12}

$([4])$ 〃 〃 〃 $([2])$

$([0])$ 〃 〃 〃 $([4])$

Theorem 5.7 (Jordan Holder)

In a finite group $(G, *)$ with more than one element, any two composition chain are equivalent.

Def: A group $(G, *)$ is called solvable group iff $\exists$ a finite collection of subgroups of $(G, *)$

$H_0 \supset H_1 \supset \cdots H_n$

1. $G = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\}$
2. H_{i+1} is normal subgroup of H_i
3. H_i / H_{i+1} Comm. group

التاريخ : / /　　　　الموضوع :

(Ex) Every Comm. group is Solvble

Sol: Let $(G, *)$ be a Com. group.

T.P $(G, *)$ is Solvable.

Let $H_0 = G$, $H_1 = \{e\}$

① $G = H_0 \supset H_1 = \{e\}$

② T.P H_{i+1} normal sub group of H_i

H_1 is normal Sub group of H_0

Since $\{e\}$ is normal sub group of G

③ T.P H_i / H_{i+1} is Com group

$G/\{e\} = G$ is Com. group

$\therefore H_i / H_{i+1}$ is Com. group

$\therefore (G, *)$ is Solvable group

الموضوع : ______ التاريخ : / /

(EX) Show that (S_3, o) is Solvable

{Sol} Let $H_0 = S_3$, $H_1 = \{I, (2\,3), (1\,3)\}$

$H_2 = \{I\}$

① $S_3 = H_0 \supset H_1 \supset H_2 = \{I\}$ ∴ تحقق الشرط الاول من التعريف

② T.P H_{i+1} is normal subgroup of H_1

and H_1 is normal subgroup of H_0

∴ تحقق الشرط الثاني من التعريف

∴ H_{i+1} is normal subgroup of H_i

③ T.P H_i / H_{i+1} Com. group

$|H_1/H_2| = \frac{|H_1|}{|H_2|} = \frac{3}{1} = 3 < b \Rightarrow$ com. group

نستفاد من نظرية لاكرانج

$|H_0/H_1| = \frac{|H_0|}{|H_1|} = \frac{6}{3} = 2 < 6 \Rightarrow$ Com. group

∴ (S_3, o) is Solvable group.