Subject Date No.

Abstract Algebra 1

* Contenporary Abstract Algebra by Joseph A. Gallian

* Abstract Algebra by D.S. Malik

Def :- Let A & B be non-empty set (i.e $A, B \neq \phi$) a relation f from A into B is called a function.

or maping from A into B if $D(f) = A$ (Domain)

$f : A \to B$

$\forall (x, y)\ (x', y') \in f$

$x = x' \rightarrow y = y'$

Subject Date No.

Ex Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$
Let f be the subset of $A \times B$ defined by $f = \{(1,a), (2,b), (3,c), (4,b)\}$
is f function?

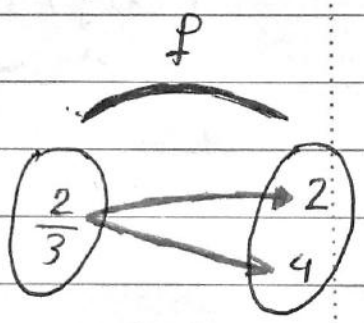
→ $D(f) = \{1, 2, 3, 4\} = A$

f is function.

Ex Let f be the subset of $\mathbb{Q} \times \mathbb{Z}$ defined by :-

$$f = \{(\frac{p}{q}, p) : p, q \in \mathbb{Z} , q \neq 0\}$$

is f function? why?.



→ $(\frac{2}{3}, 2) \in f$

$(\frac{4}{6}, 4) \in f$

∴ f is not function

Subject Date No.

Sets :-

[1] The set of Natural numbers or set of Positive Integer numbers ($\mathbb{Z}^+$)

→ $\mathbb{N} = \{1, 2, 3, \dots\}$

[2] The set of Integer numbers

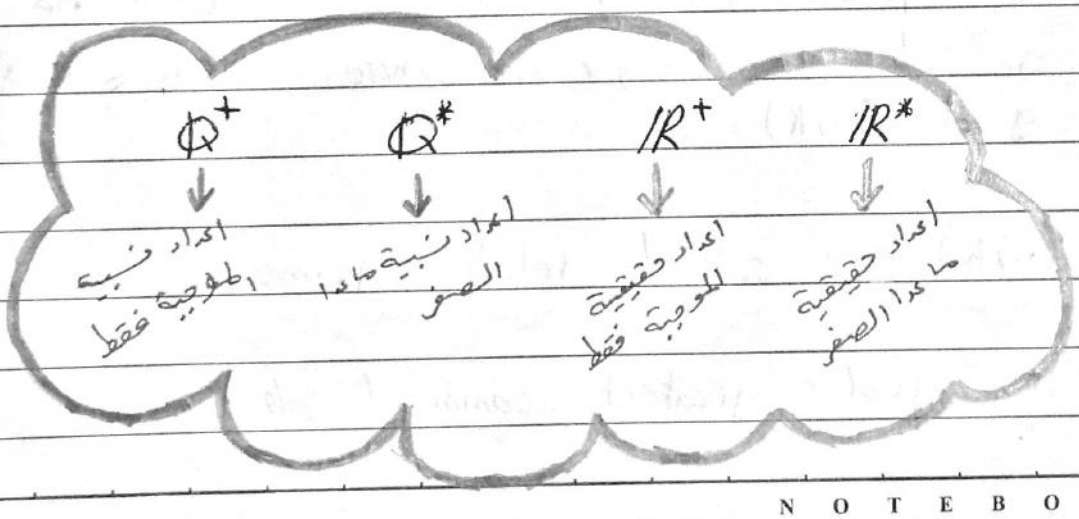
→ $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

[3] The set of Rational numbers

→ $\mathbb{Q} = \{\frac{a}{b} , a, b \in \mathbb{Z} , b \neq 0\}$

[4] The set of Real numbers

→ $\mathbb{R} = (-\infty, \infty)$



Subject Date No.

5 The set of Complex numbers

$$\mathbb{C} = \{ a+bi \ , \ a,b \in \mathbb{R} \ \& \ i = \sqrt{-1} \}$$

→ **Operation on Complex :-**

- Addition

$a+bi \ , \ c+di \in \mathbb{C}$

$(a+c) + (b+d)i$

جزء حقيقي — جزء تخيلي

- Multiplication

$(a+bi) \cdot (c+di)$ ← توزيع الاقواس

$ac - bd + (ad+bc)i$

6 U(n)

Def :- For positive integer «n» let U(n) be a set of integer k where $1 \leq k \leq n$ & $\gcd(n,k) = 1$

(n,k) are called relative prime.

gcd :- greatest commend devisor القاسم المشترك الأكبر

Subject Date No.

Ex $U(10)$

→ 1 2 3 4 5 6 7 8 9 10

1 ✓ 2 X 3 ✓ 4 X 5 X 6 X 7 ✓ 8 X 9 ✓ 10 X

$\therefore U(10) = \{1, 3, 7, 9\}$

$1 \leq n < 10$

gcd (10, 1) → $10 = 2 \cdot 5 \cdot 1$
$1 = 1$

gcd (10, 2) → $10 = 2 \cdot 5 \cdot 1$ $\neq 1$
$2 = 2 \cdot 1$

gcd (10, 3) → $10 = 2 \cdot 5 \cdot 1$
$3 = 3 \cdot 1$

1:500

Ex $U(15)$

→ $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Subject Date No.

7 General linear group $GL(2,R)$

→ is the set of all (invertible) 2x2 with Entries in $\mathbb{R}$, $\det A \neq 0$

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in GL(2,R)$$

← مجموعة كل المصفوفات المربعة (2×2) التي عناصرها من $\mathbb{R}$ ولها معكوس و $\det A \neq 0$

8 Special linear group $SL(2,R)$

→ is the set of all (invertible) 2x2 with Entries in $\mathbb{R}$, with $\det A = 1$

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2,R)$$

← مجموعة المصفوفات المربعة (2×2) عناصرها من $\mathbb{R}$ ولها معكوس و $\det A = 1$

Subject Date No.

Ex $B = \begin{bmatrix} \frac{1}{2} & 0 \\ 5 & 2 \end{bmatrix} \rightarrow B \in SL(2,R)$

إذا تحققت SL ليس بالضرورة أن تحقق GL

$\Rightarrow SL(2,R) \subseteq GL(2,R)$

* Function (1-1)

Def :- Let $f: A \rightarrow B$ is said to be injective (1-1) :-

$\forall a, a' \in A \;,\; a \neq a' \rightarrow f(a) \neq f(a')$

or $\forall a, a' \in A \;,\; a = a' \rightarrow f(a) = f(a')$

Ex $f(x) = e^x$

$\rightarrow f(x_1) = f(x_2)$

$e^{x_1} = e^{x_2}$ ← أخذ ln للطرفين

$\ln e^{x_1} = \ln e^{x_2}$

$x_1 \ln e = x_2 \ln e$ $\rightarrow f(x) = e^x$ is (1-1)

$x_1 = x_2$

Subject Date No.

* (on-to)

Def: A function $f: A \to B$ is said to be syrjective (on-to)

if $f(A) = B$

Def: A function $f: A \to B$ is said to be Bijective if:-

f is (1-1) & (onto)

Def: A relation $x \sim y$ on a set X is:-

[1] reflexive if $x \sim x$, $\forall x \in X$

[2] symmetric if $x \sim y \to y \sim x$, $\forall x, y \in X$

[3] transitive if $x \sim y$, $y \sim z \to x \sim z$

$\forall x, y, z \in X \times X$

→ by [1], [2] & [3]

→ «~» is equivelence relation.

Subject Date No.

Binary Operation :-

Def : A binary operation on set X is a function

$$* : X \times X \to X$$

Ex On the set $\mathbb{Z}$, defined a binary operation $+$, is a binary operation $(+)$?

→ $(\mathbb{Z}, +)$ $\quad 2, -2 \in \mathbb{Z} \rightarrow 2+(-2) = 0 \in \mathbb{Z}$

$a+b = c \in \mathbb{Z}$

∴ is binary operation.

Ex On the set $\mathbb{R}^* = \mathbb{R} - \{0\}$ define binary operation $(+)$.

→ $5, -5 \in \mathbb{R}^* \rightarrow 5+(-5) = 0 \notin \mathbb{R}^*$

∴ not binary operation.

Subject Date No.

Ex $(\mathbb{Z}, \div)$

$\rightarrow 1, 2 \in \mathbb{Z} \rightarrow 1 \div 2 = \frac{1}{2} \notin \mathbb{Z}$

$\therefore$ not binary operation.

Def: A binary operation on the set X is commutative iff

$$b * a = a * b$$

Def: A binary operation on a set X is associative if

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

Subject Date No.

Ex $X = \{a, b, c\}$

*	a	b	c
a	b	c	b
b	a	d	b
c	c	b	a

1) Is * binary operation on X? why?

2) Is * commutative binary operation on X?

3) Is * associative binary operation on X?

→ ① → $b.b = d \notin X$

not binary operation.

② → $a*b \stackrel{?}{=} b*a$

$c \neq a$ → ∴ not commutative binary operation.

③ → $(a*b)*c \stackrel{?}{=} a*(b*c)$

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

$a \neq c$ → * isnot associative on X

Subject Date No.

Ex $(\mathbb{N}, -)$ / → on the set $\mathbb{N}$ defined a binary operation $(-)$, is $(-)$ a binary operation ?

→ $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$

$4, 5 \in \mathbb{N}$ but $4 - 5 = -1 \notin \mathbb{N}$

∴ $(-)$ is not binary operation on $\mathbb{N}$

Ex $X = \mathbb{Z}^+$

$*$ defined by $a * b = a^b$, $a, b \in \mathbb{Z}^+$

is $*$ associative on X ?

القاعدة $\boxed{(a*b)*c = a*(b*c)}$

$2, 3, 2 \in \mathbb{Z}^+$

$(2*3)*2 \stackrel{?}{=} 2*(3*2)$

$(2^3)*2 \stackrel{?}{=} 2*(3^2)$

$(8)*2 \stackrel{?}{=} 2*(9)$ → not associative

$8^2 \stackrel{?}{=} 2^9$

$64 \neq 519$

Subject Date No.

(H.W) on $X = \mathbb{Q}$, $*$ defined by

$a * b = \frac{a}{b}$, is $*$ binary operation?

let $3, 0 \in \mathbb{Q}$

$\rightarrow 3 * 0 = \frac{3}{0} = \infty \notin \mathbb{Q}$

$\rightarrow 0 * 3 = \frac{0}{3} = 0 \in \mathbb{Q}$

$\therefore \rightarrow$ $*$ is not binary operation.

(H.W) on $X = \mathbb{Z}^+$, $*$ defined by

$a * b = \frac{a}{b}$, is $*$ binary operation?

$\mathbb{Z}^+ = \{1, 2, 3, 4, \dots\} = \mathbb{N}$

let $1, 2 \in \mathbb{Z}^+ \rightarrow 1 * 2 = \frac{1}{2} \notin \mathbb{Z}^+$

$\therefore \rightarrow$ $*$ is not binary operation.

Subject Date No.

group «G»

Def: A group is not empty set together with a binary operation defined on G s.t :-

1. $a, b \in G \rightarrow a * b \in G$
2. Associative $\rightarrow (a*b)*c = a*(b*c)$
3. Identity $\rightarrow$ There is an element defined by $e \in G$ s.t
   $$a.e = e.a = a$$
4. Inverse $\rightarrow$ for each $a \in G$
   $$ab = ba = e$$

ملاحظة
Identity «e»

بالضرب ← قيمتها 1
بالجمع والطرح ← قيمتها 0

Subject Date No.

Ex $(\mathbb{Z}, +)$ is a group ? why?

① $a, b \in \mathbb{Z} \rightarrow a+b=c \in \mathbb{Z}$

$\rightarrow 2,3 \in \mathbb{Z} \rightarrow 2+3=5 \in \mathbb{Z}$

$\therefore (+)$ is a binary operation.

② $a+(b+c) = (a+b)+c$

$\rightarrow 2,3,4 \in \mathbb{Z} \rightarrow 2+(3+4) \stackrel{?}{=} (2+3)+4$

$2+7 \stackrel{?}{=} 5+4$

$9 = 9$ ✓

$\therefore (+)$ is associative binary operation

③ $a+0 = 0+a = a$

$\rightarrow 2,0 \in \mathbb{Z} \rightarrow 2+0=0+2=2$ ✓

④ $a+a^{-1} = e$

$\rightarrow 2,-2 \in \mathbb{Z} \rightarrow 2+(-2) = 0$ ✓

$\therefore$ by ①, ②, ③ & ④ $\rightarrow (\mathbb{Z}, +)$ is group

Subject Date No.

(H.W) $(\mathbb{R}, \cdot)$ is a group ? why?

1) closed binary operation

let $2,3 \in \mathbb{R} \rightarrow 2 \cdot 3 = 6 \in \mathbb{R}$ ⌙

2) associative

let $1,2,3 \in \mathbb{R} \rightarrow (1 \cdot 2) \cdot 3 \stackrel{?}{=} 1 \cdot (2 \cdot 3)$

$2 \cdot 3 \stackrel{?}{=} 1 \cdot 6$

$6 = 6$ ⌙

3) identity $e = 1$

$3 \in \mathbb{R} \rightarrow 3 \cdot 1 = 3$ ⌙

4) inverse $a \cdot \bar{a}^{1} = e$

let $3 \in \mathbb{R} \rightarrow 3 \cdot \frac{1}{3} = 1 = e$ ⌙

$\rightarrow (\mathbb{R}, \cdot)$ is group

Ex $(\mathbb{N}, -)$ is a group ? why?

$\rightarrow 2,5 \in \mathbb{N}$ but $2 - 5 = -3 \notin \mathbb{N}$

$\therefore \mathbb{N}$ not group.

Subject Date No.

Ex $(\mathbb{Z}, .)$ is a group? why?

→ inverse $a \cdot a^{-1} = 1$

$2 \in \mathbb{Z}$ but $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$

$\therefore (\mathbb{Z}, .)$ is not group.

Ex $G = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$, $(G, \cdot)$ is a group? why?

→

$\cdot$	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 closed binary operation.

② Associative → $1, i, -i \in G$

$(1 \cdot i) \cdot -i \stackrel{?}{=} 1 \cdot (i \cdot -i)$

$i \cdot -i \stackrel{?}{=} 1 \cdot (1)$

$1 = 1$ ✓

Subject Date No.

③ Identity $= 1$

④ inverse → $1 \cdot 1 = 1$

$-1 \cdot -1 = 1$

$i \cdot -i = 1$

$-i \cdot i = 1$

ماهي القيم التي إذا ضربناها بهذه الأعداد تعطينا $e = 1$ ((الجواب من الجدول)).

∴ G is group.

Ex $(\mathbb{Q}^+, \cdot)$ is group?

① closed binary operation.

$\frac{1}{2}, \frac{1}{3} \in \mathbb{Q}^+ \rightarrow \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6} \in \mathbb{Q}^+$

② Identity $e = 1$ ✓

$\mathbb{Q}^+ = \{\frac{p}{q} , p, q \in \mathbb{Z}^+, q \neq 0\}$

③ Inverse $a \cdot a^{-1} = e$

$\frac{1}{2} \cdot 2 = 1$ ✓

④ Associative $(\frac{1}{2} \cdot \frac{1}{4}) \cdot \frac{1}{3} \stackrel{?}{=} \frac{1}{2} \cdot (\frac{1}{4} \cdot \frac{1}{3})$

$\frac{1}{8} \cdot \frac{1}{3} \stackrel{?}{=} \frac{1}{2} \cdot \frac{1}{12}$

$\frac{1}{24} = \frac{1}{24}$ ✓

∴ $(\mathbb{Q}^+, \cdot)$ is a group.

Subject Date No.

Def:- let G be a group then G is abelian group if $ab = ba$, $\forall a, b \in G$

Ex $(\mathbb{Z}, +)$ is abelian group?

→ $2, 3 \in \mathbb{Z}$ → $2+3 \stackrel{?}{=} 3+2$

$5 = 5$ ✓

→ $\therefore (\mathbb{Z}, +)$ is abelian group

Ex let $M_2(R)$ be a set of all 2×2 matrix with interies from $\mathbb{R}$ then $(M_2(R), +)$ is a group?

ملاحظة: $M_2(R)$ ← 2×2 مصفوفة ، → $\mathbb{R}$ عناصرها

* في هذا السؤال نحتاج على ٣ عناصر للحل
عشرين لجميع الخطوات
ماعدا الخطوة ٣ (asso) نستخدمها لاثبات عناصر.

الحل ←

Subject Date No.

Q31 ① closed binary operation.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} \in M_2(R)$$

② Identity $= e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

③ Associative.

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \in M_2(R)$$

$$\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} =$$

$$\begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} = \begin{bmatrix} a_1+a_2+a_3 & b_1+b_2+b_3 \\ c_1+c_2+c_3 & d_1+d_2+d_3 \end{bmatrix}$$

--- (a)

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right) =$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2+a_3 & b_2+b_3 \\ c_2+c_3 & d_2+d_3 \end{bmatrix} = \begin{bmatrix} a_1+a_2+a_3 & b_1+b_2+b_3 \\ c_1+c_2+c_3 & d_1+d_2+d_3 \end{bmatrix}$$

--- (b)

(a) = (b) ✓

Subject Date No.

④ Inverse $A+A^{-1} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$$\rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$\therefore (M_2(R), +)$ is group

* group
  - binary operation
  - associative
  - inverse
  - identity.

Subject Date No.

(H.W) $(M_2(R), \cdot)$ is a group?

1) closed binary operation

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in M_2(R)$$

$$\rightarrow \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \in M_2(R)$$

2) associative

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \in M_2(R)$$

$$\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \overset{?}{=} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}\right)$$

3) identity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

4) inverse

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow \therefore (M_2(R), \cdot) \text{ is group}$$

Subject Date No.

Ex $(U_{(10)}, \cdot)$ is a group? why?

→ $U_{(10)} = \{1, 3, 7, 9\}$ → mod 10

·	1	3	7	9
1	1	3	7	9
3	3	9	21 | 1	27 | 7
7	7	21 | 1	49 | 9	63 | 3
9	9	27 | 7	63 | 3	81 | 1

→

·	1	3	7	9
1	(1)	3	7	9
3	3	9	(1)	7
7	7	(1)	9	3
9	9	7	3	(1)

(1) Closed binary operation.

(2) $e = 1$

(3) $a \cdot \bar{a}^{-1} = e$, $e = 1$

$1 \cdot 1 = 1$

$3 \cdot 7 = 1$

$7 \cdot 3 = 1$

$9 \cdot 9 = 1$

(4) Asso , $\forall\, 1, 3, 7 \in U_{(10)}$

→ $1 \cdot (3 \cdot 7) \stackrel{?}{=} (1 \cdot 3) \cdot 7$

$1 \cdot 1 \stackrel{?}{=} 3 \cdot 7$

$1 = 1$ ✓

$\therefore (U_{(10)}, \cdot)$ is a group.

Subject Date No.

Ex $(Z_4, \cdot)$ is a group? why?

→ $Z_4 = \{0, 1, 2, 3\}$ → mod 4

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	4 → 0	6 → 2
3	0	3	6 → 2	9 → 1

→

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

① closed binary operation.

② $e = 1$

③ inverse $a \cdot \bar{a}^1 = 1$ but $0 \cdot 0 \neq 1$

∴ $(Z_4, \cdot)$ is not group.

Subject Date No.

Ex $(Z_5, +)$ is a group? why?

→ $Z_5 = \{0, 1, 2, 3, 4\}$ → mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5 | 0
2	2	3	4	5 | 0	6 | 1
3	3	4	5 | 0	6 | 1	7 | 2
4	4	5 | 0	6 | 1	7 | 2	8 | 3

+	0	1	2	3	4
0	(0)	1	2	3	4
1	1	2	3	4	(0)
2	2	3	4	(0)	1
3	3	4	(0)	1	2
4	4	(0)	1	2	3

① closed binary operation.

② $e = 0$

③ inverse $a + a^{-1} = 0$

$0+0=0$

$1+4=0$

$2+3=0$

$3+2=0$

$4+1=0$

④ Asso $1, 2, 3 \in Z_5$

$(1+2)+3 \stackrel{?}{=} 1+(2+3)$

$3+3 \stackrel{?}{=} 1+0$

$1 = 1$ ✓

$\therefore (Z_5, +)$ is a group

Subject Date No.

(H.W) $(\mathbb{C}, +)$ is a group ? why ?

$$\mathbb{C} = \{ a+bi,\ a,b \in \mathbb{R},\ i = \sqrt{-1} \}$$

1) closed binary operation

let $(a_1+b_1i), (a_2+b_2i) \in \mathbb{C}$

$\rightarrow (a_1+b_1i) + (a_2+b_2i) = (a_1+a_2) + (b_1+b_2)i \in \mathbb{C}$ ✓

2) associative

let $(a_1+b_1i), (a_2+b_2i), (a_3+b_3i) \in \mathbb{C}$

$\rightarrow ((a_1+b_1i) + (a_2+b_2i)) + (a_3+b_3i) \stackrel{?}{=} (a_1+b_1i) + ((a_2+b_2i) + (a_3+b_3i))$

$((a_1+a_2) + (b_1+b_2)i) + (a_3+b_3i) \stackrel{?}{=} (a_1+b_1i) + ((a_2+a_3) + (b_2+b_3)i)$

$(a_1+a_2+a_3) + (b_1+b_2+b_3)i = (a_1+a_2+a_3) + (b_1+b_2+b_3)i$ ✓

3) Identity $(e=0)$

let $(a+bi) \in \mathbb{C}$

$\rightarrow (a+bi) + 0 = a+bi$ ✓

4) inverse

let $(a+bi) \in \mathbb{C}$

$a + \bar{a}^{-1} = e = 0$

$(a+bi) + (-a-bi) = 0$ ✓

$\therefore (\mathbb{C}, +)$ is group.

Subject Date No.

(H.W) $(\mathbb{C}, \cdot)$ is a group? why?

1) closed binary operation

let $(a_1+b_1i), (a_2+b_2i) \in \mathbb{C}$

$\rightarrow (a_1+b_1i)\cdot(a_2+b_2i) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1) \in \mathbb{C}$ ✓

2) associative

let $(a_1+b_1i), (a_2+b_2i)$ & $(a_3+b_3i) \in \mathbb{C}$

$\rightarrow ((a_1+b_1i)\cdot(a_2+b_2i))\cdot(a_3+b_3i) \stackrel{?}{=} (a_1+b_1i)\cdot((a_2+b_2i)\cdot(a_3+b_3i))$

الطرف الأيسر $((a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1))\cdot(a_3+b_3i)$

$=((a_1a_2-b_1b_2)a_3 - (a_1b_2+a_2b_1)b_3) + i((a_1a_2-b_1b_2)b_3 + (a_1b_2+a_2b_1)a_3)$

$= (a_1a_2a_3 - b_1b_2a_3 - a_1b_2b_3 - a_2b_1b_3) + i(a_1a_2b_3 - b_1b_2b_3 + a_1b_2a_3 + a_2b_1a_3)$

الطرف الأيمن $(a_1+b_1i)\cdot((a_2+b_2i)\cdot(a_3+b_3i))$

$=(a_1+b_1i)\cdot((a_2a_3-b_2b_3)+i(a_2b_3+b_2a_3))$

$=(a_1(a_2a_3-b_2b_3) - b_1(a_2b_3+b_2a_3)) + i(b_1(a_2a_3+b_2b_3) + a_1(a_2b_3+b_2a_3))$

$=(a_1a_2a_3 - a_1b_2b_3 - a_2b_1b_3 - a_3b_1b_2) + i(a_2a_3b_1 + b_1b_2b_3 + a_1a_2b_2 + a_2a_3b_2)$

الطرف الأيسر = الطرف الأيمن ✓

3) Identity $e=1$

let $(a+bi) \in \mathbb{C}$

$\rightarrow (a+bi)\cdot 1 = (a+bi)$ ✓

Subject Date No.

Uniqness of Identity نظرية الوحدانية للحايد (الحايد وحيد)

Thm 1

Let G be a group then the identity of G is unique.

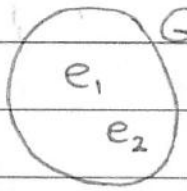
Proof :-

Let e_1, e_2 be two identity of G

Since e_1 is identity & $e_2 \in G \rightarrow e_1 \cdot e_2 = e_2$ --- ①

Since e_2 is identity & $e_1 \in G \rightarrow e_1 \cdot e_2 = e_1$ --- ②

so $e_1 = e_2$ by ① & ②



→ The identity is unique.

عنصر * الحايد = العنصر

Subject Date No.

(H.W) Find the inverse of the element

$$A = \begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}_{2\times 2} \text{ in } GL(2, Z_{11})$$

(mod 11)

$Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$

$$A = \begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix} \longrightarrow A^{-1} = \frac{1}{-8}\begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix}$$

الاعداد السالبة →

$-8 \mod 11 \rightarrow 3$

$-6 \mod 11 \rightarrow 5$

$-3 \mod 11 \rightarrow 8$

$$A^{-1} = \frac{1}{3}\begin{bmatrix} 5 & 5 \\ 8 & 2 \end{bmatrix}$$

Subject Date No.

Thm 2 Concellation الاختزال أو الحذف

Let G be agroup with Identity (e)
let $a, b, c \in G$ such that
$ab = ac \rightarrow b = c$

proof :-

Let $a, b, c \in G$ want to show that $b = c$

Assume that $ab = ac$
multiply both sides by $\bar{a}^1$

$\bar{a}^1 (ab) = \bar{a}^1 (ac)$ → by Associative

$(\bar{a}^1 . a) \cdot b = (\bar{a}^1 . a) \cdot c$ → by inverse $a . \bar{a}^1 = e$

$e \cdot b = e \cdot c$

$b = c$ ∎

Thm 3 «غير مطلوب الاثبات»

Let b be any element then the inverse of b is unique.

← معكوس أي عنصر يكون وحيد

← كل عنصر له معكوس واحد فقط.

Sub group

Def of order :- (تعريف رتبة الـ group)

→ The order of a group G is number of elements in G (infinite or finite) we denoted by $|G|$ → $O(G)$

الـ order هي عدد عناصر المجموعة

Ex $|Z_{10}| = 10$

$|\mathbb{R}| = \infty$

$|U(15)| = 8$ → $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$|U(10)| = 4$ → $U(10) = \{1, 3, 7, 9\}$

$|Z_n| = n$

Subject Date No.

Ex Let $A = \{1, 2, 4\}$

→ $|A| = 3$

Ex Let $G = \{1, -1, i, -i\}$

→ $|G| = 4$

Def of subgroup :-

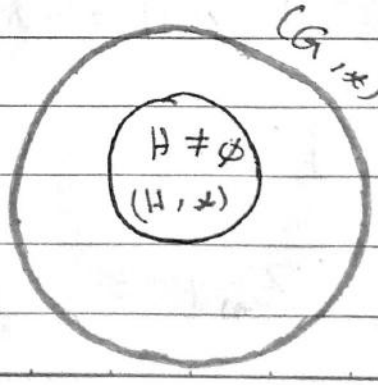
→ Let G be a group with identity (e)
Let H a non-empty subset of G $(H \neq \emptyset)$

then H is a subgroup of G $(H \leq G)$

subgroups (ج) ↓

→ If H itself is group under the same operation on G.

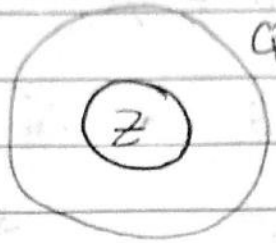
$H \neq \emptyset$ ← يعني يوجد على الأقل عنصر واحد في H



Subject Date No.

Ex $(\mathbb{Q}, +)$ is a group & $(\mathbb{Z}, +)$ is a group.

→ $\mathbb{Z} \leq \mathbb{Q}$, $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$



Subgroup test :-

Thm : Let G be group , $H \neq \emptyset$ of G is a subgroup of G iff

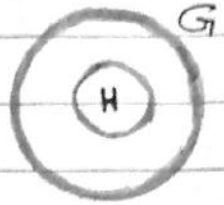
① $\forall a, b \in H \rightarrow a * b \in H$ (closed)

② $\forall a \in H \rightarrow a^{-1} \in H$

③ $\forall a, b \in H \rightarrow a b^{-1} \in H$

Subject Date No.

Thm Let G be a group, let H be a non-empty set of G then $H \leq G$



proof :-

let G be a group

① $H \neq \emptyset$

② $\forall a,b \in H \rightarrow a \cdot b^{-1} \in H$ group $b_{g,-1}$

let $a = b \rightarrow a \cdot a^{-1}$ → identity

let $a = e \rightarrow e \cdot b^{-1} = b^{-1} \in H$ → inverse

G is a group :-

$\forall a,b,c \in G \rightarrow (ab)c = a(bc)$ → associative

$\Rightarrow \forall a,b,c \in H \rightarrow (ab)c = a(bc)$

(H.W) → ③ closed ⇒ let $a,b \in H \rightarrow ab \in H$

→ $b \in H$ by ② → $b^{-1} \in H$

$a \cdot b^{-1} \in H$ by assume → $a \cdot (b^{-1})^{-1} \in H$

→ $ab \in H$

so its closed

→ $H \leq G$

Subject Date No.

Ex let G be abelian group, show that
$H = \{x \in G : x^2 = e\}$
is a subgroup of G.

يكفي هنا كتابة شرطين بدل الاثنين اذا تحقق جميع الشروط

① $H \neq \phi$
since $e \in H \rightarrow e^2 = e \in H$.

② $\forall a, b \in H \rightarrow ab^{-1} \in H$

$(ab^{-1}) \rightarrow (ab^{-1})^2 = ab^{-1} \cdot ab^{-1}$ (G is abelian)
$= a \cdot a \cdot b^{-1} \cdot b^{-1}$
$= a^2 \cdot (b^{-1})^2$
$= e^2 \cdot e^2 = e \cdot e = e$

$\rightarrow ab^{-1} \in H$

③ $\forall a, b \in H \rightarrow ab \in H$

$(ab)^2 = (ab) \cdot (ab)$
$= a \cdot a \cdot b \cdot b = a^2 \cdot b^2$
$= e \cdot e = e$

$\rightarrow a.b \in H$

④ $\forall b \in H \rightarrow b^{-1} \in H$

$(b^{-1})^2 = (b^2)^{-1} = e \rightarrow b^{-1} \in H$

Subject Date No.

(H.W) Let G be abelian group, show that
$H = \{ x \in G : x^3 = e \}$
is a subgroup of G.

① $H \neq \emptyset$ since $e \in G \Rightarrow (e^3 = e)$

② $\forall a, b \in H \Rightarrow ab \in H$

let $a, b \in H$ then $a = x^3$ & $b = y^3$, $x, y \in G$

→ $a, b \in H$
$x, y \in G$

③ $\forall a, b \in H \Rightarrow ab^{-1} \in H$

→ $a = x^3$, $b = y^3$ then $ab^{-1} = x^3 (y^3)^{-1}$
$= x^3 (y^{-1})^3$

Since G is abelian and $xy^{-1} \in G$
so $ab^{-1} = (xy^{-1})^3 \Rightarrow ab^{-1} \in H$.

$\therefore H$ is a subgroup of G $(H \leq G)$

④ let $a, b \in H$ then $a = x^3$, $b = y^3$, $x, y \in G$
then $ab = x^3 y^3$
so $ab = (xy)^3 \Rightarrow ab \in H$ ((G is ablian group $x, y \in G$))

$\therefore H \leq G$

Subject Date No.

Ex prove or disprove :-
Every subset of group is a group ?

→ disprove , for example $(Z_{10}, +)$ is group

→ let $H = \{0, 1, 2, 4\}$

→ $2, 4 \in H$ → $2+4 = 6 \notin H$.
↳ ليست موجودة في Z_{10} وليست في H

Ex let $G = (\mathbb{R}^*, \cdot)$, $K = \{x \in \mathbb{R}^* = R - \{0\} ; x \geq 1\}$
is $K \leq G$? why ?
↳ يوجد شرط
لو لم يكن هذا الشرط
موجوداً لكان ناتج
هذا السؤال $K \leq G$

→ $x = 2$, $2 \geq 1$

$x \cdot x^{-1} = e$

$2 \cdot \frac{1}{2} = e$

↳ $\frac{1}{2} \geq 1$ X ∴ $K \not\leq G$

Subject Date No.

Cyclic group :-

Any element $a \in G$ generated G if $\langle a \rangle = G$.

A group G is cyclic if there is some element "a" in G that generated.

→ for any element $a \in G$ we let $\langle a \rangle$ denoted the $\{ a^n, n \in \mathbb{Z} \}$ المولدة

$\langle a \rangle$ is called the cyclic subgroup generated by a.

$\langle a \rangle = \{ \dots, a^{-1}, a^0, a^1, \dots \}$

$a^0 = e$

Subject Date No.

Ex find $|\langle 1\rangle|$, $|\langle 2\rangle|$, $|\langle 3\rangle|$ in $(Z_4, +)$

→ $Z_4 = \{0, 1, 2, 3\}$, $(Z_4, +)$ → group

$\langle 1\rangle$

العملية تحدد في السؤال هنا العملية هي عملية Z_4

$1^1 = 1$

$1^2 = 1+1 = 2$

$1^3 = 1+1+1 = 3$

$1^4 = 1+1+1+1 = 4 \mod 4 = 0$

$\Rightarrow \langle 1\rangle = \{0, 1, 2, 3\} = Z_4$ → generated

$|\langle 1\rangle| = 4$ ∴ Z_4 is cyclic

$\langle 2\rangle$

$2^1 = 2$

$2^2 = 2+2 = 4 \mod 4 = 0$

$2^3 = 2+2+2 = 6 \mod 4 = 2$

$2^4 = 2+2+2 = 8 \mod 4 = 0$

$\Rightarrow \langle 2\rangle = \{0, 2\}$ → not generated.

$|\langle 2\rangle| = 2$

تكملة

Subject Date No.

تكملة حل السؤال

$\langle 3 \rangle$

$3^1 = 3$

$3^2 = 3+3 = 6 \mod 4 = 2$

$3^3 = 3+3+3 = 9 \mod 4 = 1$

$3^4 = 3+3+3+3 = 12 \mod 4 = 0$

$\langle 3 \rangle = \{0, 1, 2, 3\} = Z_4$ is cyclic generated.

$|\langle 3 \rangle| = 4$

Ex $(Z_6, +)$ is cyclic ? why?

→ $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$\langle 1 \rangle$

$1^1 = 1$

$1^2 = 1+1 = 2$

$1^3 = 1+1+1 = 3$

$1^4 = 1+1+1+1 = 4$

$1^5 = 1+1+1+1+1 = 5$

$1^6 = 1+1+1+1+1+1 = 6 \mod 6 = 0$

$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\} = Z_6$ → Z_6 is cyclic

$|\langle 1 \rangle| = 6$

Subject Date No.

Ex $U_{(10)}$ is cyclic ? and find $|\langle 9\rangle|$.

→ $U_{(10)} = \{1, 3, 7, 9\}$

$\langle 1\rangle$

$1^1 = 1$

$1^2 = 1 \cdot 1 = 1$

$1^3 = 1 \cdot 1 \cdot 1 = 1$

$1^4 = 1 \cdot 1 \cdot 1 \cdot 1 = 1$ → $\langle 1\rangle = \{1\}$ not generated

$\langle 3\rangle$

$3^1 = 3$

$3^2 = 3 \cdot 3 = 9$

$3^3 = 3 \cdot 3 \cdot 3 = 27 \bmod 10 = 7$

$3^4 = 3 \cdot 3 \cdot 3 \cdot 3 = (3^3) \cdot 3 = 7 \cdot 3 = 21 \bmod 10 = 1$

→ $\langle 3\rangle = \{1, 3, 7, 9\} = U_{(10)}$ → is cyclic

↳ generated.

$\langle 7\rangle$

$7^1 = 7$

$7^2 = 7 \cdot 7 = 49 \bmod 10 = 9$

$7^3 = 7^2 \cdot 7 = 9 \cdot 7 = 63 \bmod 10 = 3$

$7^4 = 7^3 \cdot 7 = 3 \cdot 7 = 21 \bmod 10 = 1$

→ $\langle 7\rangle = \{1, 3, 7, 9\} = U_{(10)}$

generated → cyclic

Subject Date No.

<9>

$9^1 = 9$

$9^2 = 9 \cdot 9 = 81 \mod 10 = 1$

$9^3 = 9^2 \cdot 9 = 1 \cdot 9 = 9$

$9^4 = 9^3 \cdot 9 = 9 \cdot 9 = 81 \mod 10 = 1$

$\langle 9 \rangle = \{1, 9\}$ → not generated

Ex $U(8)$ is cyclic ? why ?

$U(8) = \{1, 3, 5, 7\}$ → $U(8)$ is not cyclic

$\langle 1 \rangle = \{1\}$ not generated

$1^1 = 1$

$1^2 = 1 \cdot 1 = 1$

$1^3 = 1 \cdot 1 \cdot 1 = 1$

$1^4 = 1 \cdot 1 \cdot 1 \cdot 1 = 1$

$\langle 3 \rangle = \{1, 3\}$ not generated

$3^1 = 3$

$3^2 = 3 \cdot 3 = 9 = 1$

$3^3 = 3^2 \cdot 3 = 27 = 3$

$3^4 = 3^3 \cdot 3 = 1$

$\langle 5 \rangle = \{1, 5\}$ not generated

$5^1 = 5$

$5^2 = 25 = 1$

$5^3 = 5^2 \cdot 5 = 5$

$5^4 = 5^3 \cdot 5 = 25 = 1$

$\langle 7 \rangle = \{1, 7\}$ not generated

$7^1 = 7$

$7^2 = 7 \cdot 7 = 49 = 1$

$7^3 = 7^2 \cdot 7 = 7$

$7^4 = 7^3 \cdot 7 = 7 \cdot 7 = 49 = 1$ O K

Subject Date No.

Note :-

Z_n is cyclic since $\langle 1 \rangle = Z_n$

$\langle 1 \rangle = Z_n$ ← فقط بالنسبة لـ Z_n

لون الاقلب حج ← تأليف الجمع

$U(n)$ ← تأليف الضرب في حال لم يذكر السؤال العملية

Thm Every cyclic group is abelian.

Proof :-

let $a, b \in G$ & G is cyclic group

(want to show) G is abelian → $(ab = ba)$

$G = \langle c \rangle$ for $c \in G$

$a = c^i$, $\exists i \in Z$

$b = c^j$, $\exists j \in Z$

i, j ← هما أعداد ينتميان إلى Z قوى الـ cyclic

$ab = c^i \cdot c^j$

$= c^{i+j} = c^j \cdot c^i = ba$ ∴ G is abelian

Subject Date No.

(H.W) let $(H,*)$, $(K,*)$ be a subgroup of $(G,*)$ prove or disprove

① $((H \cap K), *)$ is a subgroup.

② $((H \cup K), *)$ is a subgroup.

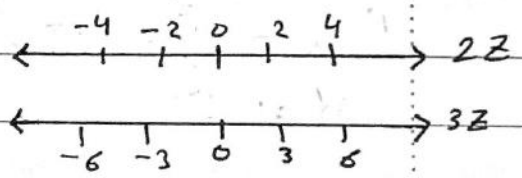
① let $a,b \in H \cap K \rightarrow a,b \in H$ & $a,b \in K$

so, $a * b^{-1} \in H$ and $a * b^{-1} \in K$

$\rightarrow a * b^{-1} \in H \cap K$ so $H \cap K$ is subgroup of G

② disprove, for example :-

- let $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ → الاعداد الزوجية
- let $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$ → الاعداد الفردية



→ let $\underbrace{(2\mathbb{Z}, +)}_{H}$, $\underbrace{(3\mathbb{Z}, +)}_{K}$

→ $((2\mathbb{Z} \cup 3\mathbb{Z}), +)$ is not subgroup of $\mathbb{Z}$

$5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

Subject Date No.

Ex Find all subgroup of Z_{24}.

→ $Z_{24} = \{0, 1, 2, \ldots, 23\}$

→ $\{24\} = \{1, 2, 3, 4, 6, 8, 12, 24\}$ → القواسم لـ 24

$\langle 1 \rangle = \{1, 2, 3, 4, \ldots, 23, \underline{0}\}$ mod 24

$\langle 2 \rangle = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, \underline{0}\}$

$\langle 3 \rangle = \{3, 6, 9, 12, 15, 18, 21, \underline{0}\}$ → mod 24

$\langle 4 \rangle = \{4, 8, 12, 16, 20, \underline{0}\}$

$\langle 6 \rangle = \{6, 12, 18, \underline{0}\}$

$\langle 8 \rangle = \{8, 16, \underline{0}\}$

$\langle 12 \rangle = \{12, \underline{0}\}$

$\langle 24 \rangle = \{\underline{0}\} = \langle 0 \rangle$

↳ mod 24

(H.W) find all subgroup of Z_{30}

$\{30\} = \{1, 2, 3, 5, 6, 10, 15, 30\}$

$\langle 1 \rangle = \{1, 2, 3, \ldots, 29, \underline{0}\}$

$\langle 2 \rangle = \{2, 4, 6, \ldots, 28, \underline{0}\}$ → mod 30

$\langle 3 \rangle = \{3, 6, 9, 12, \ldots, 27, \underline{0}\}$

$\langle 5 \rangle = \{5, 10, 15, 20, 25, \underline{0}\}$

$\langle 6 \rangle = \{6, 12, 18, 24, \underline{0}\}$

$\langle 10 \rangle = \{10, 20, \underline{0}\}$ → mod 30

$\langle 15 \rangle = \{15, \underline{0}\}$

$\langle 30 \rangle = \{\underline{0}\} = \langle 0 \rangle$

Subject Date No.

Permutation group :-

Def :- A permutation of set $A \neq \phi$ is a function $\phi : A \to A$ that is (1-1)
let S_A be the set of permutation on A.

Def :- $*$ binary operation on S_A as follows
$\delta * \tau = \delta \circ \tau$ ← العملية هنا الضرب

Thm if δ, τ are one to one function then $\delta \circ \tau$ is one to one.

proof :- let $x_1, x_2 \in A$

$\delta \circ \tau(x_1) \stackrel{?}{=} \delta \circ \tau(x_2)$
$\delta(\tau(x_1)) = \delta(\tau(x_2))$ → δ, τ are (1-1)
→ $\tau(x_1) = \tau(x_2)$ → since τ is (1-1)

→ $x_1 = x_2$

Subject Date No.

Thm if δ, τ are onto function then $\delta \circ \tau$ is onto.

proof : (H.W)

→ let $a \in A$. want $c \in A$ s.t $(\delta \circ \tau)(c) = a$

→ since δ is onto, $\exists b \in A$ s.t $\delta(b) = a$

→ since τ is onto, $\exists c \in A$ s.t $\tau(c) = b$

→ Now, $(\delta, \tau)(c) = \delta(\tau(c))$

$= \delta(b) = a$

$\therefore \delta \circ \tau$ is onto.

Subject Date No.

Symmetric group on set A :.

Ex $A = \{1, 2, 3, 4, 5\}$

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} = (1435)$$

cycle

نبدأ من هنا

ننظر إلى كل عنصر من مرتبط

1 → 4 (العدد الذي يصل إليه ← نبدأ بهذا)

4 → 3

3 → 5

5 → 1 ← نغلق القوس عندما نصل إلى العدد الذي بدأنا به

نكتب أول رقمين

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = (13425)$$

cycle

1 → 3

3 → 4

4 → 2

2 → 5

5 → 1

* العدد الذي لا يظهر يكون مرتبط بنفسه مثل المثال السابق في δ ← (2) مرتبط بنفسه لذلك لم يظهر في الجواب.

---

* التحويل من ( ) ← ( )

→ $\delta = (1435) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ ← نكتب العدد الأول كامل

ثم ننظر إلى كل عنصر مرتبط بالعنصر الذي بعده

1 → 4

4 → 3

3 → 5

5 → 1

والعنصر المفقود 2 يكون مرتبط بنفسه

Subject Date No.

→ find $\delta \circ \tau$. (من معطيات السؤال السابق)

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

← العملية هنا الضرب

↑ دائماً نبدأ بالضرب من هنا

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

← النتيجة الاول نكتبه كامل مثل ما هو

$1 \to 3 \to 5$

$2 \to 5 \to 1$

$3 \to 4 \to 3$

$4 \to 2 \to 2$

$5 \to 1 \to 4$

↑ نلغي الوسط

→ $\delta \circ \tau = (1\,5\,4\,2)$

$1 \to 5$

$5 \to 4$

$4 \to 2$

$2 \to 1$

الضرب في Symmetric group ليست تبديلي

Subject Date No.

⇒ find $\tau \circ \delta$ (من معطيات السؤال السابق)

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

نبدأ من هنا ↑

نكتب أول رقمين ←

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

$1 \to 4 \to 2$

$2 \to 2 \to 5$

$3 \to 5 \to 1$

$4 \to 3 \to 4$

$5 \to 1 \to 3$

↑ نلغي الوسط

→ $\tau \circ \delta = (1253)$

$1 \to 2$

$2 \to 5$

$5 \to 3$

$3 \to 1$

→ $\tau \circ \delta \neq \delta \circ \tau$ → العملية ليست تبديلية

Subject Date No.

* الطريقة الثانية للضرب :-

* $\delta \circ \tau = (1435)(13425)$

* هنا لا يجوز أن نكتب أول رقمين

نبدأ من هنا

$= (1542)$

1 → 3 → 5
5 → 1 → 4
4 → 2 → 2
2 → 5 → 1

* $\tau \circ \delta = (13425)(1435)$

نبدأ من هنا

$= (1253)$

1 → 4 → 2
2 → 2 → 5
5 → 1 → 3
3 → 5 → 1

Subject Date No.

Def :- let A be a finite set $\{1, 2, \dots, n\}$ the group of all permution of A is the symmetric group on n letters and denoted be S_n

$$|S_n| = n!$$

Ex ① In S_3 find $|S_3|$

$\rightarrow |S_3| = 3! = 6$

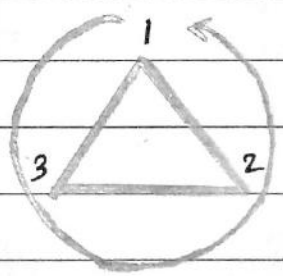
② In S_n find $|S_4|$

$\rightarrow |S_4| = 4! = 24$

Ex $A = \{1, 2, 3\}$, $|S_3| = 6$

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

$(1)(2)(3)$



بالدوران
360°

Subject Date No.

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

العملية ∘	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

الضرب هنا الأفقي بالعمودي
العمودي هو اليمين

* $(12) \cdot (12) = (1)(2)(3) = e$

$(1) \to 2 \to (1)$
$(2) \to 1 \to (2)$
$(3) \to 3 \to (3)$

بس تشكر من الاطراف → تكون e.

السبب: الضرب ليست تبديلي
not abilian group.

Subject Date No.

Def : The subgroup A_n is called the alterating Group of degree n.

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

$\rightarrow A_3 = \{e, (123), (132)\}$

(A_3, o) is a group ? why?

العملية على الضرب

o	e	(123)	(132)
e	e	(123)	(132)
(123)	(123)	(132)	e
(132)	(132)	e	(123)

① closed binary operation.

② Associative $\rightarrow$ $(123) \cdot (e \cdot (132)) \stackrel{?}{=} ((123) \cdot e) \cdot (132)$

$(123) \cdot (132) \stackrel{?}{=} (123) \cdot (132)$

$e = e$ ✓

③ Identity $e \rightarrow e \cdot e = e$

$e \cdot a = a$ $\quad (123) \cdot e = (123)$

$(132) \cdot e = (132)$ ✓

④ Inverse $\rightarrow e \cdot e = e$

$a \cdot \bar{a}^{-1} = e$ $\quad (132) \cdot (123) = e$

$(123) \cdot (132) = e$ ✓

$\Rightarrow (A_3, o)$ is group

Subject Date No.

Ex Find $|(12)|$

عندما يطلب order نبقى نرفع للأس 1+ حتى ينتج e

$\rightarrow (12)^1 = (12)$

$(12)^2 = (12)\cdot(12) = e$ *

$\rightarrow |(12)| = 2$

Ex Find $|(123)|$

$\rightarrow (123)^1 = (123)$

$(123)^2 = (123)(123) = (132)$

$(123)^3 = (123)^2 \cdot (123) = (132)\cdot(123) = e$ *

$\rightarrow |(123)| = 3$

(H.W) Find the order of $Z = (13425)$

$(13425)^1 = (13425)$

$(13425)^2 = (13425)(13425) = (14532)$

$(13425)^3 = (13425)^2(13425) = (14532)(13425) = (12354)$

$(13425)^4 = (13425)^3(13425) = (12354)(13425) = (15243)$

$(13425)^5 = (13425)^4(13425) = (15243)(13425) = (1)(2)(3)(4)(5)$

$\rightarrow |(13425)| = 5$

Subject Date No.

(H.W) let $H = \{a+ib,\ a,b \in \mathbb{R},\ ab \geq 0\}$ prove or disprove that $H \leq \mathbb{C}$ under addition ?

① $H \neq \phi$ $\{0+0i = 0 \in H\}$

$\forall x,y \in H$

② let $x = 3+i$; $3,1 \in \mathbb{R}$, $3 \cdot 1 = 3 \geq 0$

$y = 2i$; $-2,0 \in \mathbb{R}$, $2 \cdot 0 = 0 \geq 0$

$x \cdot \bar{y}^{-1} = (3+i)(-2i) = -6i + 2$

(conjugate)

$\rightarrow -6 \cdot 2 = -12 < 0$

$\Rightarrow x \cdot \bar{y}^{-1} \notin H$

$\Rightarrow$ Disprove $\Rightarrow$ H not subgroup.

Subject Date No.

Thm Every cyclic is a product of transpositions in general :

$$(a_1 a_2 a_3 \cdots a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_2)$$

Def :- if δ can be write as a product of even number of transpositions then δ is an even permutation the some for the odd.

Ex $\delta = (1456) \longrightarrow = \underbrace{(16)}_{1}\underbrace{(15)}_{2}\underbrace{(14)}_{3} \longrightarrow$ odd فردي

$\delta = (145) \longrightarrow = \underbrace{(15)}_{1}\underbrace{(14)}_{2} \longrightarrow$ even زوجي

Subject Date No.

Unique inverse :-

Thm let $(G, *)$ be a group then $\forall a \in G$,
$\exists$ unique $\acute{a} \in G$ s.t $a * \acute{a}^{1} = \acute{a}^{1} * a = e$

proof :- suppose the $a \in G$ has inverse a', a''

$\rightarrow a * a' = a' * a = e$ ---(1)

$\rightarrow a * a'' = a'' * a = e$ ---(2)

$a' * a = a'' * a$ by concellation Thm

$\rightarrow a' = a''$ $\#$

Cosets group

Def :- [1] left cosets

let $H \leq G \rightarrow aH = \{ah : h \in H\}$ of G

[2] right cosets

let $H \leq G \rightarrow Ha = \{ha : h \in H\}$

Subject Date No.

Ex $Z_9 = \{0,1,2,3,4,5,6,7,8\}$, $H = \langle 3 \rangle = \{0,3,6\}$

→ Find left and right cosets.

sol → $(Z_9, +)$ عملية الجمع فقط

left $a+H$

* $0+H = 0+\{0,3,6\} = \{0,3,6\} = H$
* $1+H = 1+\{0,3,6\} = \{1,4,7\}$
* $2+H = 2+\{0,3,6\} = \{2,5,8\}$
* $3+H = 3+\{0,3,6\} = \{3,6,0\} = H$
* $4+H = 4+\{0,3,6\} = \{4,7,1\}$ → mod 9
* $5+H = 5+\{0,3,6\} = \{5,8,2\}$ →
* $6+H = 6+\{0,3,6\} = \{6,0,3\} = H$
* $7+H = 7+\{0,3,6\} = \{7,1,4\}$
* $8+H = 8+\{0,3,6\} = \{8,2,5\}$

→ the left cosets

$\{0+H, 1+H, 2+H\}$

Subject Date No.

right H+a

- $H+0 = \{0,3,6\} + 0 = \{0,3,6\} = H$
- $H+1 = \{0,3,6\} + 1 = \{1,4,7\}$
- $H+2 = \{0,3,6\} + 2 = \{2,5,8\}$
- $H+3 = \{0,3,6\} + 3 = \{3,6,0\} = H$
- $H+4 = \{0,3,6\} + 4 = \{4,7,1\}$ → mod 9
- $H+5 = \{0,3,6\} + 5 = \{5,8,2\}$
- $H+6 = \{0,3,6\} + 6 = \{6,0,3\} = H$
- $H+7 = \{0,3,6\} + 7 = \{7,1,4\}$
- $H+8 = \{0,3,6\} + 8 = \{8,2,5\}$

→ the right cosets
$\{H+0, H+1, H+2\}$

Subject Date No.

Ex in $S_3 = \{ e, (12), (13), (23), (123), (132) \}$,
$H = \langle 13 \rangle$ find left and right cosets.

$\langle 13 \rangle = \{ e, 13 \}$ توضيح $(13)^1 = (13)$

$(13)^2 = (13)(13) = e$

left

$e \circ \{e, (13)\} = \{ e, (13) \}$ *

$(12) \circ \{e, (13)\} = \{ (12), (132) \}$ **

$(13) \circ \{e, (13)\} = \{ (13), e \}$ *

$(23) \circ \{e, (13)\} = \{ (23), (123) \}$ ☆

$(123) \circ \{e, (13)\} = \{ (123), (23) \}$ ☆

$(132) \circ \{e, (13)\} = \{ (132), (12) \}$ **

→ the left cosets

$\{ e \circ H, (12) \circ H, (23) \circ H \}$

الضرب في S_3 ليست تبديلي

right

$\{e, (13)\} \circ e = \{ e, (13) \}$ *

$\{e, (13)\} \circ (12) = \{ (12), (123) \}$ **

$\{e, (13)\} \circ (13) = \{ (13), e \}$ *

$\{e, (13)\} \circ (23) = \{ (23), (132) \}$ ☆

$\{e, (13)\} \circ (123) = \{ (123), (12) \}$ **

$\{e, (13)\} \circ (132) = \{ (132), (23) \}$ ☆

→ the right cosets

$\{ H \circ e, H \circ (12), H \circ (23) \}$

Subject Date No.

Thm let $H \leq G$, let $a, b \in G$

(i) [1] $a \in aH$ ← left [2] $a \in Ha$ ← right

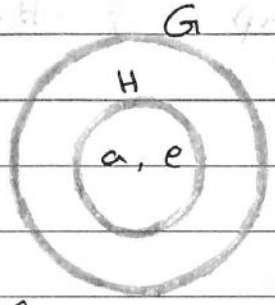
proof proof

$H \leq G \Rightarrow e \in H$ $H \leq G \Rightarrow e \in H$

ضرب الطرفين بـ a من جهة اليسار $\Rightarrow a.e \in a.H$ ضرب الطرفين بـ a من جهة اليمين $\Rightarrow e.a \in H.a$

$\Rightarrow a \in aH$ $\Rightarrow a \in Ha$

left coset right coset

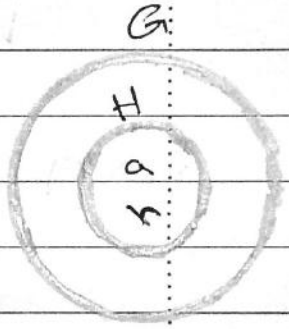


إتيان بالعاكسين ←

(ii) $aH = H$ iff $a \in H$

proof

$(\rightarrow)$ $a \in H$ w.t.s $aH = H$



let $a \in H$ & $H \leq G$ let $a \in H$ & $H \leq G$ w.t.s $H \subseteq aH$

$(H, .)$ let $h \in H$ & $\bar{a}' \in H$

so, $ah \in H$, $\forall h \in H$ $\Rightarrow \bar{a}'h \in H$ & $h.\bar{a}' \in H$

تحول $H \leftarrow h$ $\Rightarrow a.(\bar{a}'h) \in a.H$ (ضرب الطرفين بـ a من اليسار)

وتغير الاشارة من $\subseteq \leftarrow \in$ $aH \subseteq H$ ... (1) $\Rightarrow (a.\bar{a}')h \in a.H$ by asso

$\Rightarrow e.h \in aH \Rightarrow H \subseteq aH$ .. (2)

NOTEBOOK

تكملة ←

Subject Date No.

اثبات • by (1) & (2) $\Rightarrow aH = H$

$(\leftarrow)$ $aH = H$ w.t.s $a \in H$

Since $a \in aH$ $(H = aH)$

$\Rightarrow a \in H$

Lagrange's Thm «غير مطلوب الاثبات»

Let G a finite group & $H \leq G$

then $\frac{|H|}{|G|}$

* Every group of prime order is cyclic.

Subject Date No.

Normal subgroup

Def :- let G be a group, H is normal subgroup of G iff $aH = Ha$

left = right

$\rightarrow H \triangledown G$

↳ normal subgroup

Note :-

Every subgroup of abelian group is normal.

$aHa^{-1} = H \quad \forall a \in H$

$\rightarrow aH = Ha$

---

* Corollary $A_n \triangledown S_n \quad n \geq 2$

$\{S_n : A_n\} = 2$

↳ $\frac{|S_n|}{|A_n|} = 2$

Ex S_3, A_3

$\Rightarrow \frac{|S_3|}{|A_3|} = \frac{6}{3} = 2$

Subject Date No.

Ex $Z_9 = \{0,1,2,3,\dots,8\}$

$H = \langle 3 \rangle = \{0,3,6\}$, is $H \trianglelefteq G$? why?

left coset $a+H$	right coset $H+a$
$0+H = \{0,3,6\}$	$H+0 = \{0,3,6\}$
$1+H = \{1,4,7\}$	$H+1 = \{1,4,7\}$
$2+H = \{2,5,8\}$	$H+2 = \{2,5,8\}$
$3+H = \{3,6,0\}$	$H+3 = \{3,6,0\}$
$4+H = \{4,7,1\}$	$H+4 = \{4,7,1\}$
$5+H = \{5,8,2\}$	$H+5 = \{5,8,2\}$
$6+H = \{6,0,3\}$	$H+6 = \{6,0,3\}$
$7+H = \{7,1,4\}$	$H+7 = \{7,1,4\}$
$8+H = \{8,2,5\}$	$H+8 = \{8,2,5\}$

→ left coset = right coset

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

$\therefore H \trianglelefteq Z_9$

Subject Date No.

Ex is $H \trianglelefteq S_3$ where $H = \langle 23 \rangle$

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

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

left coset $(a+H)$	right coset $(H+a)$
$e \circ \{e, (23)\} = \{e, (23)\}$	$\{e, (23)\} \circ e = \{e, (23)\}$
$(12) \circ \{e, (23)\} = \{(12), (123)\}$	$\{e, (23)\} \circ (12) = \{(12), (132)\}$
$(13) \circ \{e, (23)\} = \{(13), (123)\}$	$\{e, (23)\} \circ (13) = \{(13), (123)\}$
$(23) \circ \{e, (23)\} = \{(23), e\}$	$\{e, (23)\} \circ (23) = \{(23), e\}$
$(123) \circ \{e, (23)\} = \{(123), (12)\}$	$\{e, (23)\} \circ (123) = \{(123), (13)\}$
$(132) \circ \{e, (23)\} = \{(132), (13)\}$	$\{e, (23)\} \circ (132) = \{(132), (12)\}$

$\rightarrow$ left coset $\neq$ right coset $\rightarrow H \not\trianglelefteq S_3$

* عملية الضرب في S_3 ليست تبديلية

Subject Date No.

Thm $H \trianglelefteq G \iff xHx^{-1} \subseteq H \;,\; \forall x \in G$

proof :- [1] + [2]

[1] $H \trianglelefteq G$ w.t.s $xHx^{-1} \subseteq H$

let $H \leq G$ & H is normal subgroup.

$\rightarrow aH = Ha \quad \forall a \in G$

$\rightarrow aHa^{-1} = Ha \cdot a^{-1}$ ← بضرب الطرفين بـ a^{-1} (من معطيات السؤال xHx^{-1})

$\rightarrow aHa^{-1} = H \cdot e$

$\rightarrow aHa^{-1} = H \quad \rightarrow aHa^{-1} = H$

[2] $xHx^{-1} \subseteq H \;\; \forall x \in G$ w.t.s $H \trianglelefteq G$ $(aH = Ha)$

$aH = Ha$

نريد أن نثبت

$aH \subseteq Ha$

let $a \in G$, then $aHa^{-1} \subseteq H$

$\Rightarrow aHa^{-1} \cdot a \subseteq H \cdot a$

$aH \cdot e \subseteq Ha$

$aH \subseteq Ha$ -- ①

$Ha \subseteq aH$

let $a^{-1} \in G$, then

$a^{-1}H(a^{-1})^{-1} \subseteq H$

$\Rightarrow a^{-1}Ha \subseteq H$

$\Rightarrow a \cdot a^{-1}Ha \subseteq a \cdot H$

$\Rightarrow e \cdot Ha \subseteq aH$

$Ha \subseteq aH$ ... ②

$\rightarrow$ by ① & ② $\Rightarrow aH = Ha$

$\rightarrow H \trianglelefteq G$

Subject Date No.

(H.W) in S_3, let $H = \{e, (13)\}$.
is $H \trianglelefteq S_3$?

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

left coset $a \circ H$	right coset $H \circ a$
$e \circ \{e, (13)\} = \{e, (13)\}$	$\{e, (13)\} \circ e = \{e, (13)\}$
$(12) \circ \{e, (13)\} = \{(12), (132)\}$	$\{e, (13)\} \circ (12) = \{(12), (123)\}$
$(13) \circ \{e, (13)\} = \{(13), e\}$	$\{e, (13)\} \circ (13) = \{(13), e\}$
$(23) \circ \{e, (13)\} = \{(23), (123)\}$	$\{e, (13)\} \circ (23) = \{(23), (132)\}$
$(123) \circ \{e, (13)\} = \{(123), (23)\}$	$\{e, (13)\} \circ (123) = \{(123), (12)\}$
$(132) \circ \{e, (13)\} = \{(132), (12)\}$	$\{e, (13)\} \circ (132) = \{(132), (23)\}$

$\therefore$ left coset $\neq$ right coset

$\therefore H \not\trianglelefteq S_3$

Subject Date No.

Factor Group :

Def :- let G be a group & H be a normal of G then group $\frac{G}{H}$

is called (factor group) quotient group of G by H group.

Ex $G = Z_{18}$ & $H = \langle 6 \rangle = \{0, 6, 12\}$ Find $\frac{G}{H}$

$\rightarrow Z_{18} = \{0, 1, 2, 3, \ldots, 17\}$

left coset

$0+H = 0 + \{0, 6, 12\} = \{0, 6, 12\}$

$1+H = 1 + \{0, 6, 12\} = \{1, 7, 13\}$

$2+H = 2 + \{0, 6, 12\} = \{2, 8, 14\}$

$3+H = 3 + \{0, 6, 12\} = \{3, 9, 15\}$

$4+H = 4 + \{0, 6, 12\} = \{4, 10, 16\}$

$5+H = 5 + \{0, 6, 12\} = \{5, 11, 17\}$

$6+H = 6 + \{0, 6, 12\} = \{6, 12, 0\}$

$7+H = 7 + \{0, 6, 12\} = \{7, 13, 1\}$

$8+H = 8 + \{0, 6, 12\} = \{8, 14, 2\}$

$9+H = 9 + \{0, 6, 12\} = \{9, 15, 3\}$

Subject Date No.

left coset

$10 + H = 10 + \{0, 6, 12\} = \{10, 16, 4\}$ △

$11 + H = 11 + \{0, 6, 12\} = \{11, 17, 5\}$ ###

$12 + H = 12 + \{0, 6, 12\} = \{12, 0, 6\}$ ※

$13 + H = 13 + \{0, 6, 12\} = \{13, 1, 7\}$ ☆

$14 + H = 14 + \{0, 6, 12\} = \{14, 2, 8\}$ ✳

$15 + H = 15 + \{0, 6, 12\} = \{15, 3, 9\}$ □

$16 + H = 16 + \{0, 6, 12\} = \{16, 4, 10\}$ △

$17 + H = 17 + \{0, 6, 12\} = \{17, 5, 11\}$ ###

right coset

$H + 0 = \{0, 6, 12\} + 0 = \{0, 6, 12\}$ ※

$H + 1 = \{0, 6, 12\} + 1 = \{1, 7, 13\}$ ☆

$H + 2 = \{0, 6, 12\} + 2 = \{2, 8, 14\}$ ✳

$H + 3 = \{0, 6, 12\} + 3 = \{3, 9, 15\}$ □

$H + 4 = \{0, 6, 12\} + 4 = \{4, 10, 16\}$ △

$H + 5 = \{0, 6, 12\} + 5 = \{5, 11, 17\}$

$H + 6 = \{0, 6, 12\} + 6 = \{6, 12, 0\}$ ※

$H + 7 = \{0, 6, 12\} + 7 = \{7, 13, 1\}$ ☆

$H + 8 = \{0, 6, 12\} + 8 = \{8, 14, 2\}$ ✳

$H + 9 = \{0, 6, 12\} + 9 = \{9, 15, 3\}$ □

$H + 10 = \{0, 6, 12\} + 10 = \{10, 16, 4\}$ △

$H + 11 = \{0, 6, 12\} + 11 = \{11, 17, 5\}$ ###

$H + 12 = \{0, 6, 12\} + 12 = \{12, 0, 6\}$ ※

$H + 13 = \{0, 6, 12\} + 13 = \{13, 1, 7\}$ ☆

$H + 14 = \{0, 6, 12\} + 14 = \{14, 2, 8\}$ ✳

aisi →

Subject Date No.

تكملة ١٥

$H+15 = \{0,6,12\} +15 = \{15,3,9\}$ □

$H+16 = \{0,6,12\} +16 = \{16,4,10\}$ △

$H+17 = \{0,6,12\} +17 = \{17,5,11\}$ ##

left coset = right coset ⇒ Normal

$$\frac{|G|}{|H|} = \frac{18}{3} = 6$$

$$\frac{G}{H} = \{0+H, 1+H, 2+H, 3+H, 4+H, 5+H\}$$

يجب كتابتها بهذا الشكل المجموعة

الترتيب غير مهم، يجوز لو كتبنا

$\{H+0, H+1, H+2, H+3, H+4, H+5\}$

(normal) left = right ∴

Subject Date No.

Ex Let $G = S_3$, $H = A_3$, Find $\frac{G}{H}$

→ $S_3 = \{ e, (12), (13), (23), (123), (132) \} = G$

$A_3 = \{ e, (123), (132) \} = H$

H is Normal subgroup

left coset $a+H$ left coset = right coset

$e \circ \{ e, (123), (132) \} = \{ e, (123), (132) \}$ ※

$(12) \circ \{ e, (123), (132) \} = \{ (12), (23), (13) \}$ ✱

$(13) \circ \{ e, (123), (132) \} = \{ (13), (12), (23) \}$ ✱

$(23) \circ \{ e, (123), (132) \} = \{ (23), (13), (12) \}$ ✱

$(123) \circ \{ e, (123), (132) \} = \{ (123), (132), e \}$ ※

$(132) \circ \{ e, (123), (132) \} = \{ (132), e, (123) \}$ ※

right coset $H+a$

$\{ e, (123), (132) \} \circ e = \{ e, (123), (132) \}$ ※

$\{ e, (123), (132) \} \circ (12) = \{ (12), (13), (23) \}$ ✱

$\{ e, (123), (132) \} \circ (13) = \{ (13), (23), (12) \}$ ✱

$\{ e, (123), (132) \} \circ (23) = \{ (23), (12), (13) \}$ ✱

$\{ e, (123), (132) \} \circ (123) = \{ (123), (132), e \}$ ※

$\{ e, (123), (132) \} \circ (132) = \{ (132), e, (123) \}$ ※

$\frac{S_3}{A_3} = \{ e \circ H, (123) \circ H, (132) \circ H \}$

Subject Date No.

Group Homomorphism :- المجموعة التشاكلية

Def :- A homomorphism from G to G' is a function :-

$$(\phi : G \to G')$$

($f: x \to y$) مثل ←

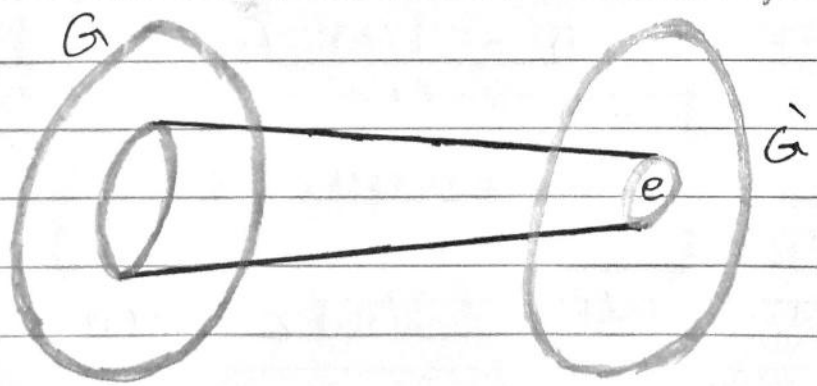
$$\text{s.t} \quad \phi(ab) = \phi(a)\,\phi(b)$$

groups ← G , G'

Def :- Let $\phi : G \to G'$, ϕ is homomorphism then :-

$$\ker \phi = \{ g \in G \ , \ \phi(g) = e \}$$

إذا كان العنصر g ينتمي للمجموعة G و كانت صورة العنصر تعطي e نسميها $\ker \phi$



Subject Date No.

Ex Let $(\mathbb{R}, +) \to (\mathbb{R}, +)$, is ϕ homomorphism? and find $\ker \phi$ in :-

① $f(x) = 2x$ → polynomial function.

← هل هي homomorphism ؟

$\ker \phi$ ← إذا تحقق ← ϕ ← نطبق الشرطين السابقين ←

let $x, y \in (\mathbb{R}, +) \to \phi(x+y) = 2(x+y)$

$= 2x + 2y$

$= \phi(x) + \phi(y)$

$\Rightarrow \phi$ is homomorphism.

← إذا استطعنا فصل ϕ ← x, y

يكون الاقتران homomorphism

$\ker \phi = \{ x \in \mathbb{R} : f(x) = 0 \}$

$= \{ x \in \mathbb{R} : 2x = 0 \}$ ← العنصر المحايد بالجمع هو الصفر

$= \{0\}$ ← ما هو الذي صورته تساوي صفر ؟

② $f(x) = x^3$

let $x, y \in (\mathbb{R}, +) \to \phi(x+y) = (x+y)^3$

$\neq x^3 + y^3$

$\therefore \phi$ is not group homomorphism .

Subject Date No.

Ex Let $(\mathbb{R}^*, .) \to (\mathbb{R}^*, .)$

$f(x) = x^3$, is ϕ homomorphism? and Find $\ker \phi$.

let $x, y \in (\mathbb{R}^*, .)$

$$\phi(xy) = (xy)^3$$
$$= x^3 \cdot y^3$$
$$= \phi(x) \cdot \phi(y)$$

$\therefore \phi$ is group homomorphism.

$$\ker \phi = \{ x \in \mathbb{R}^* , f(x) = 1 \}$$
$$= \{ x \in \mathbb{R}^* , x^3 = 1 \}$$
$$= \{1\}$$

العنصر المحايد بالضرب هو الواحد 1

Subject Date No.

Ex $F : (\mathbb{R}, +) \to (\mathbb{R}^+, .)$

$f(x) = 2^x$ is homomorphism?

Let $x, y \in \mathbb{R}$

$F(x+y) = 2^{x+y} = 2^x \cdot 2^y$

$= F(x) \cdot F(y)$

$\therefore F$ is group homomorphism.

(H.W) $\phi : GL(2,\mathbb{R}) \to (\mathbb{R}^*, .)$

given by $\phi(A) = \det A$

this group homomorphism, find $\ker \phi$.

let $A, B \in GL(2,\mathbb{R})$

$\phi(AB) = \det A \cdot \det B$

$= \phi(A) \cdot \phi(B)$ *

Remark

$\det(AB) = \det A . \det B$

$\det(A \pm B) \neq \det A \pm \det B$

$\ker \phi = \{ A \in GL(2,\mathbb{R}) , \phi(A) = 1 \}$ المعلومة الجديدة

$= \{ A \in GL(2,\mathbb{R}) : \det A = 1 \} = SL(2,\mathbb{R})$

Subject Date No.

Ex $\phi : (\mathbb{R}[x], +) \longrightarrow (\mathbb{R}[x], +)$

given by $\phi(F) = F'$

ϕ is homomorphism & find $\ker \phi$.

let $f, g \in \mathbb{R}[x]$

$\phi(f+g) = (f+g)' = f' + g'$

$= \phi(f) + \phi(g)$

$\therefore \phi$ is homomorphism.

$\ker f = \{ f \in \mathbb{R}[x] : f' = 0 \}$

مشتقة ثابت = صفر

$= \{c\}$

يعني $\in [x]$ أنه Polynomial

ϕ توزع على عملية الجمع

والمشتقة توزع على عملية الجمع

Subject Date No.

(H.W) $\phi : (\mathbb{R}^*, .) \to (\mathbb{R}^*, .)$ where $\phi(x) = |x|$ is ϕ homomorphism, find $\ker \phi$.

let $a, b \in \mathbb{R}^* \rightarrow \phi(ab) = |a \cdot b|$

$= |a| \cdot |b|$

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

$\therefore \phi$ is homomorphism

$\ker \phi = \{ a \in \mathbb{R}^* : \phi(a) = 1 \}$

$= \{ a \in \mathbb{R}^* : |x| = 1 \}$

$= \{ 1, -1 \}$

(H.W) $\phi : (\mathbb{R}^*, .) \to (\mathbb{R}^*, .)$ where $f(x) = x^2$ is ϕ homomorphism and find $\ker \phi$.

let $x, y \in \mathbb{R}^*$

$\phi(x, y) = (xy)^2 = x^2 \cdot y^2 = \phi(x) \cdot \phi(y)$

$\therefore \phi$ is homomorphism.

$\ker \phi = \{ a \in \mathbb{R}^* : f(a) = 1 \}$

$= \{ a \in \mathbb{R}^* : x^2 = 1 \}$

$= \{ 1, -1 \}$

Subject Date No.

Isomorphism :-

Def:- let $(G,*)$ & $(B,*)$ be two group,

$\phi : G \to B$ is called isomorphism iff :-

1. ϕ is one to one.
2. ϕ is on-to
3. ϕ is homomorphism.

$\Rightarrow G \cong B$

يعني ← isomorphism

Note

That any group isomorphism is homomorphism.

* العكس ليس بالضرورة أن يكون صحيح

Subject Date No

Ex $F: \mathbb{R} \to \mathbb{R}^+$ s.t $f(x) = e^x$, show that $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$

① let $x, y \in (\mathbb{R}, +)$

$$F(x+y) = e^{x+y} = e^x \cdot e^y$$
$$= F(x) \cdot F(y)$$

$\therefore F$ is homomorphism.

② let $x, y \in \mathbb{R}$, $F(x) = F(y) \Rightarrow x = y$

$$F(x) = F(y) \Rightarrow e^x = e^y$$
$$\Rightarrow \ln e^x = \ln e^y$$
$$\Rightarrow x = y$$

$\therefore F$ is $(1-1)$

③ F is onto ?

$r \in \mathbb{R}^+ \Rightarrow F(\ln r) = r$

↳ $e^{\ln r} = r$

$\therefore F$ is onto

by ① , ② & ③

$(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$

Subject Date No.

(H.W) let $\mathbb{C}^*$ be the group of non-zero complex number multiplication.

let $\phi : \mathbb{C}^* \to \mathbb{C}^*$ by $\phi(x) = x^4$

① ϕ is homomorphism?

② find Ker ϕ.

let $x, y \in \mathbb{C}^*$

① $\phi(x \cdot y) = (x \cdot y)^4 = x^4 \cdot y^4 = \phi(x) \cdot \phi(y)$

$\therefore \phi$ is homomorphism

② $\text{Ker } \phi = \{ x \in \mathbb{C}^* : \phi(x) = 1 \}$

$= \{ x \in \mathbb{C}^* : x^4 = 1 \}$

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

Subject Date No.

Thm let f be a homomorphism of group G into group G_1, then :

① $f(e) = e_1$

② $f(a^{-1}) = f^{-1}(a)$, $\forall a \in G$

Proof

let $F: G \to G_1$ is homomorphism by $F(e) = e_1$

① $F(e) = F(e \cdot e)$ → بما أن homomorphism لازم نستطيع ان نفعلها

$= F(e) \cdot F(e)$

$F(e) \cdot F(e) = F(e) \cdot e_1 \Rightarrow F(e) = e_1$ ✱

↳ by cancellation thm

② $F(a^{-1}) = F^{-1}(a)$, $\forall a \in G$ (H.W)

let $a \in G$ & F is homomorphism.

$F(a) \cdot F(a^{-1}) = F(a \cdot a^{-1}) = F(e) = e_1$ → Since $F(a)$ has a unique inverse

& $F(a^{-1}) \cdot F(a) = F(a^{-1} \cdot a) = F(e) = e_1$

$\Rightarrow F(a^{-1}) = F^{-1}(a)$

Subject Date No.

Thm $H \leq G$, $K \leq G$ & $HK \in G$ then
$HK = KH$

يعني أن $HK = KH$
وأيضاً يعني أنه abelian
Normal

Proof

$HK = KH$

want to show that

$HK \subseteq KH$ ... ①

$KH \subseteq HK$ ... ②

① given $K \leq G$, $H \leq G$ & $HK \leq G$
want to show that $HK \subseteq KH$

let $hk \in HK$ where $h \in H$ & $k \in K$

$(hk)^{-1} \in HK$ & so $(hk)^{-1} = h_1 k_1$

$\exists h_1 \in H$ & $k_1 \in K$

عالجبر الخطي
$(AB)^{-1} = BA$

thus $hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$

$hk \in KH \Rightarrow HK \subseteq KH$ ※

(2) given $K \leq G$, $H \leq G$ & $HK \leq G$

want to show that $KH \subseteq HK$

let $kh \in KH$ where $k \in K$ & $h \in H$

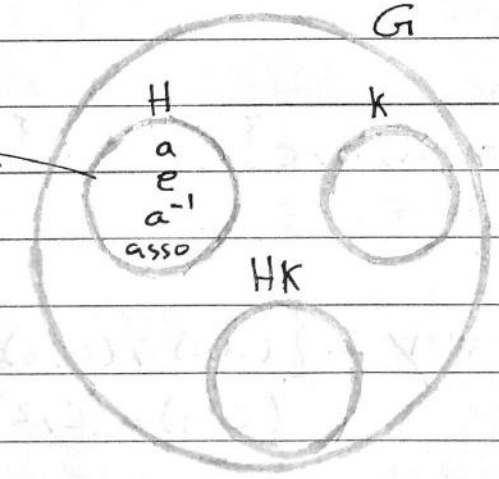
Now, $h = h.e \in HK$

$k = e.k \in HK$

since HK subgroup of G

$kh \in HK \Rightarrow KH \subseteq HK$ ✳

$\therefore$ by (1) & (2) $\Rightarrow HK = KH$



group بعض عناصره

Direct product

Def: The cartesian product of a set $S_1, S_2, \ldots, S_n$ is the set of all ordered n-tuple $(a_1, a_2, \ldots, a_n)$

where $a_i \in S_i$ for $i = 1, 2, \ldots, n$
the cartesian product is denoted by:

$$S_1 \otimes S_2 \otimes \cdots \otimes S_n \quad \text{or} \quad \prod_{i=1}^{n} S_i$$

cartesian product

* let X & Y be two sets

Define $X \otimes Y = \{(x,y) : x \in X \ \& \ y \in Y\}$

Ex let $X = \{a, b, c\}$, $Y = \{1, 2\}$, find $X \otimes Y$

$$\Rightarrow X \otimes Y = \{(a,1), (a,2), (b,1), (b,2), (c,1), (c,2)\}$$

$$|X \otimes Y| = 6$$

Subject Date No.

Ex Consider the group $Z_2 \times Z_3$ is cyclic.

$Z_2 = \{0,1\}$	$\lvert Z_2 \rvert = 2$	$\lvert Z_2 \times Z_3 \rvert = 2 \cdot 3 = 6$
$Z_3 = \{0,1,2\}$	$\lvert Z_3 \rvert = 3$	

$Z_2 \times Z_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

هنا نأخذ mod 2 للعنصر الأول
mod 3 للعنصر الثاني

$\langle (0,0) \rangle$

$(0,0)^1 = (0,0)$

$(0,0)^2 = (0,0)$

$\langle (0,1) \rangle$

$(0,1)^1 = (0,1)$

$(0,1)^2 = (0,2)$

$(0,1)^3 = (0,3) = (0,0)$

$\langle (0,2) \rangle$

$(0,2)^1 = (0,2)$

$(0,2)^2 = (0,4) = (0,1)$

$(0,2)^3 = (0,6) = (0,0)$

$\langle (1,0) \rangle$

$(1,0)^1 = (1,0)$

$(1,0)^2 = (2,0) = (0,0)$

$\langle (1,1) \rangle$

$(1,1)^1 = (1,1)$

$(1,1)^2 = (2,2) = (0,2)$

$(1,1)^3 = (1,3) = (1,0)$

$(1,1)^4 = (2,1) = (0,1)$

$(1,1)^5 = (1,2)$

$(1,1)^6 = (2,3) = (0,0)$

$\therefore (1,1)$ is generated

$\therefore Z_2 \times Z_3$ is cyclic.

Subject Date No.

Ex Find the order of (0,2) ? من معطيات السؤال السابق

$(0,2)^1 = (0,2)$

$(0,2)^2 = (0,4) = (0,1)$

$(0,2)^3 = (0,3) = (0,0)$

↳ عندما ينتج e نتوقف

$|\langle(0,2)\rangle| = 3$

Ex $Z_3 \times Z_5$ is cyclic ?

$Z_3 = \{0,1,2\}$, $|Z_3 \times Z_5| = 15$

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

$Z_3 \times Z_5 = \{(0,0), (0,1), (0,2), (0,3), (0,4), (1,0), (1,1), (1,2), (1,3), (1,4), (2,0), (2,1), (2,2), (2,3), (2,4)\}$

$\langle(0,0)\rangle$	$\langle(0,1)\rangle$	$\langle(0,2)\rangle$
$(0,0)^1 = (0,0)$	$(0,1)^1 = (0,1)$	$(0,2)^1 = (0,2)$
	$(0,1)^2 = (0,2)$	$(0,2)^2 = (0,4)$
	$(0,1)^3 = (0,3)$	$(0,2)^3 = (0,1)$
	$(0,1)^4 = (0,4)$	$(0,2)^4 = (0,3)$
	$(0,1)^5 = (0,0)$	$(0,2)^5 = (0,0)$

$\langle(0,3)\rangle$	$\langle(0,4)\rangle$	$\langle(1,0)\rangle$
$(0,3)^1 = (0,3)$	$(0,4)^1 = (0,4)$	$(1,0)^1 = (1,0)$
$(0,3)^2 = (0,1)$	$(0,4)^2 = (0,3)$	$(1,0)^2 = (2,0)$
$(0,3)^3 = (0,4)$	$(0,4)^3 = (0,2)$	$(1,0)^3 = (0,0)$
$(0,3)^4 = (0,2)$	$(0,4)^4 = (0,1)$	
$(0,3)^5 = (0,0)$	$(0,4)^5 = (0,0)$	

$\langle(1,1)\rangle$ → generated

$(1,1)^1 = (1,1)$

$(1,1)^2 = (2,2)$

$(1,1)^3 = (0,3)$

$(1,1)^4 = (1,4)$

$(1,1)^5 = (2,0)$

$(1,1)^6 = (0,1)$

$(1,1)^7 = (1,2)$

$(1,1)^8 = (2,3)$

$(1,1)^9 = (0,4)$

$(1,1)^{10} = (1,0)$

$(1,1)^{11} = (2,1)$

$(1,1)^{12} = (0,2)$

$(1,1)^{13} = (1,3)$

$(1,1)^{14} = (2,4)$

$(1,1)^{15} = (0,0)$

$\langle(1,1)\rangle = \mathbb{Z}_3 \times \mathbb{Z}_5$

$|\langle(1,1)\rangle| = 15 = |\mathbb{Z}_3 \times \mathbb{Z}_5|$

$\therefore \mathbb{Z}_3 \times \mathbb{Z}_5$ is cyclic

Subject Date No.

Thm The group $Z_m \times Z_n$ is cyclic & isomorphism to Z_m iff m and n are relating prime that $\gcd(m,n)=1$ كل التوالي

Ex $Z_2 \times Z_3$

→ (2, 3) is prime
∴ cyclic.

العلاقة بين العددين الاوليين
يجب أن يكون القاسم الذي بينهم فقط 1

8 , 11

2 . 4 . ① ① . 11

(H.W) $Z_3 \times Z_4$ is cyclic ?

Ex $G = Z_4 \times Z_6$, $H = \langle (0,1) \rangle$

Describe the factor group $\frac{G}{H}$?

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

$Z_6 = \{0,1,2,3,4,5\}$

$|Z_4 \times Z_6| = 24$

$Z_4 \times Z_6 = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5),$
$(1,0), (1,1), (1,2), (1,3), (1,4), (1,5),$
$(2,0), (2,1), (2,2), (2,3), (2,4), (2,5),$
$(3,0), (3,1), (3,2), (3,3), (3,4), (3,5)\}$

$H = \langle (0,1) \rangle$

$(0,1)^1 = (0,1)$

$(0,1)^2 = (0,2)$

$(0,1)^3 = (0,3)$

$(0,1)^4 = (0,4)$

$(0,1)^5 = (0,5)$

$(0,1)^6 = (0,0) = e$ توقف

نريد أن نثبت $H \trianglelefteq G$ إذا كان مع أول

$\frac{|G|}{|H|} = \frac{24}{6} = 4$ لازم تطلع في left & right

1 $H + (0,0) = H$

2 $H + (1,1) = \{(1,2), (1,3), (1,4), (1,5), (1,0), (1,1)\}$

3 $H + (2,2) = \{(2,3), (2,4), (2,5), (2,0), (2,1), (2,2)\}$

4 $H + (3,3) = \{(3,4), (3,5), (3,0), (3,1), (3,2), (3,3)\}$

Subject Date No.

Thm fundamental of identity generated abelian group every finite generated abelian group G is isomorphism to a direct product of cyclic group in the form

$$Z_{(P_1)^{r_1}} \times Z_{(P_2)^{r_2}} \times \cdots \times Z_{(P_n)^{r_n}} \times Z \times Z \times Z \times \cdots \times Z$$

where the p_i are prime not necessarly distance and r_i are positive integers the number of factor Z is unique & the prime power $(p_i)^{r_i}$ are unique.

Ex Find all abelian group up to isomorphism of order 300 ?

2	300
2	150
3	75
5	25
5	5
	1

$\Rightarrow 300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$

$= 2^2 \cdot 3^1 \cdot 5^2$

① $\Rightarrow Z_2 \times Z_2 \times Z_5 \times Z_5 \times Z_3$

② $\Rightarrow Z_4 \times Z_5 \times Z_5 \times Z_3$

③ $\Rightarrow Z_2 \times Z_2 \times Z_{25} \times Z_3$

④ $\Rightarrow Z_4 \times Z_{25} \times Z_3$

Ex Find the order of $(8,4,10)$ in group $Z_{12} \times Z_{60} \times Z_{24}$

نأخذ الأعداد مع بعضها على الترتيب

$10 \to Z_{24}$ ، $4 \to Z_{60}$ ، $8 \to Z_{12}$

$\therefore |Z_{12} \times Z_{60} \times Z_{24}| = 12 \cdot 60 \cdot 24$

$\gcd(8,12) = 4 \longrightarrow$ $12 = \boxed{1 \cdot 3 \cdot 2 \cdot 2}$, $8 = \boxed{1 \cdot 2 \cdot 2 \cdot 2}$

$\gcd(4,60) = 4 \longrightarrow$ $4 = \boxed{1 \cdot 2 \cdot 2}$, $60 = \boxed{1 \cdot 2 \cdot 2} \cdot 3 \cdot 5$

$\gcd(10,24) = 2 \longrightarrow$ $24 = \boxed{1 \cdot 2} \cdot 2 \cdot 2 \cdot 3$, $10 = \boxed{1 \cdot 2} \cdot 5$

ثم نقسم الأعداد على الـ gcd ➡ $\frac{12}{4} = 3$

$\frac{60}{4} = 15$

$\frac{24}{4} = 12$

$3 = 3 \cdot 1$

$15 = 5 \cdot 3 \cdot 1$

$12 = 4 \cdot 3 \cdot 1$

ثم نأخذ المضاعف المشترك الأصغر لهم ⇒ $LCM(3,15,12) = 3 \cdot 4 \cdot 5 = 60$

$\therefore |(8,4,10)| = 60 = 1 \cdot 3 \cdot 4 \cdot 5$

Sylow Theorem

Thm first sylow theorem

let G be a finite group & let $|G| = p^n m$. (p: prime) where $n \geq 1$ & where p does not divide m.

① contains a subgroup of order p^i for each : $1 \leq i \leq n$.

② every subgroup H of G of $\equiv p^i$ is normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$

Thm second sylow theorem

Any two sylow p-subgroup of G are conjugate.

Subject Date No.

Thm thirds sylow theorem.

if G is a finite group with $|G| = p^n m$

$p \nmid m$ then $n_p \equiv 1 \bmod p$ & $n_p \mid |G|$

يعني لا يقسم ← هنا لازم

First isomorphism theorem :-

let F be a homomorphism of a group G into G_1
then $F(G)$ is a subgroup of G_1

and $\frac{G}{\ker F} \cong F(G)$

isomorphism ← 1-1

proof let $\ker F = K$

Define function $F : \frac{G}{K} \to F(G)$

by $F(aK) = F(a)$

$\ker = e$ ← يعني انه اذا ضرب e بعنصر يعطي العنصر نفسه.

تكملة

تكملة الإثبات

① F is homomorphism

$aK, bK \in \frac{G}{K}$ ← تعويض في F

$F(aK \cdot bK) = F(a \cdot bK) = F(ab) = F(a) \cdot F(b)$

↑ الخاصية من المعطيات — $bK = e$

$= F(aK) \cdot F(bK)$

② F is one to one

let $F(aK) = F(bK)$

→ $F(a) = F(b)$ multiplying both sides $(F(b))^{-1}$

$\Rightarrow (F(b))^{-1} \cdot F(a) = (F(b))^{-1} \cdot F(b)$

← من النظريات السابقة

$\Rightarrow F(b^{-1}) \cdot F(a) = e \rightarrow Ker$

$\Rightarrow b^{-1} \cdot a \in Ker\, F$

$\Rightarrow b^{-1} \cdot a = K \Rightarrow b \cdot b^{-1} \cdot a = b \cdot K$

$\Rightarrow e \cdot a = b \cdot K \Rightarrow a = b \cdot e \Rightarrow \boxed{a = b}$

③ F is on-to

let $\grave{a} \in F(G_1)$, then $\exists a \in G_1 \Rightarrow F(a) = \grave{a}$ ← يعني أن

↑ co-domain

Now, $aK \in \frac{G}{K}$ & $F(aK) = F(a) = \grave{a}$ ✗

Second Isomorphism theorem

let H & K subgroup of group G with $K \trianglelefteq G$ then :-

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

Third isomorphism theorem

let H_1, H_2 be normal subgroup of a group G s.t $H_1 \leq H_2$ then

$$\frac{\frac{G}{H_1}}{\frac{H_2}{H_1}} = \frac{G}{H_2}$$

proof :-

$$\phi : G \longrightarrow (G/H_1)/(H_2/H_1)$$

$$\phi(g) = (gH_1)(H_2/H_1)$$

① ϕ is homomorphism

let $g_1, g_2 \in G$ want to show ϕ is homomorphism

$$\phi(g_1 \cdot g_2) = (g_1 g_2 H_1)(H_2/H_1)$$
$$= (g_1 H_1 \cdot g_2 H_2)(H_2/H_1)$$
$$= (g_1 H_1 (H_2/H_1) \cdot g_2 H_2 (H_2/H_1)) = \phi(g_1) \cdot \phi(g_2)$$

Subject Date No.

تكملة الاثبات

(2) ϕ is onto (H.W)

let $(gH_1)(H_2/H_1) \in (g/H_1)/(H_2/H_1)$

then $g \in G \Rightarrow \phi(g) = (gH_1)(H_2/H_1)$

$\ker \phi = \{ g \in G : \phi(g) = H_2/H_1 \}$

$\ker \phi = H_2$

$\subseteq$

let $g \in \ker \phi$

then $\phi(g) = H_2/H_1$

$g(H_1)(H_2/H_1) = H_2/H_1$

$g(H_1) \in H_2/H_1$

so, $g \in H_2$

$\supseteq$

let $g \in H_2$

so, $gH_1 \in H_2/H_1$

then $(gH_1)(H_2/H_1) = H_2/H_1$

$\phi(g) = H_2/H_1$

then $g \in \ker \phi$

$\Rightarrow$ by the first isomorphism thm :-

$G/\ker \phi \cong \phi(G) \rightarrow G/H_1 \cong (G/H_1)(H_2/H_1)$

$\ll$