نـظـريــة الــزمــر

Groups Theory

University of Baghdad – College of Education for Pure Sciences – Ibn Al-Haitham – Department of Mathematic

2th Stage

Year 2023 – 2024

اعـداد و تدريس

أ. د. فـاطــمـــة فـيـصـل كـريــم

م. رنــــــا نـــــوري مـــجــيــد

CONTENTS

المصادر العربية :

[1] مقدمة في الجبر المجرد الحديث. تاليف ديفيد بيرتون وترجمه عبد العالي جاسم.

English References

[1] Introduction to modern abstract algebra. By David M. Burton.

[2] A first course in abstract algebra. By J.B. Fraleigh.

[3] Group theory. By M. Suzuki

Chapter One : Groups Theory
الفصل الاول : نظرية الزمر

Definition 1.1: Binary Operations

Let A be a non empty set. A binary operation on a set A is a function from $A \times A$ into A. (i.e.)

$*: A \times A \to A$ is a binary operation iff

(1) $a * b \in A, \forall a, b \in A$ (Closure)

(2) If $a, b, c, d \in A$ such that $a = c$ and $b = d$, then $a * b = c * d$ (well-define).

Example 1.2:

(1) The operations $\{+, -, \times\}$arebinary operations on R, Z, Q, C.
But " $-$ " is not binary operation on N.

(2) The operations $\{+, -\}$ are not binary operations on O (odd number).

(3) The operation $\div$ is abinary operation on $R\backslash\{0\}, Q\backslash\{0\}, C\backslash\{0\}$.

Example 1.3:

Let $a * b = a + b + 2, \forall a, b \in Z^+$. Is $*$ a binary operation on Z^+?

Solution:

(1) Closure : Let $a, b \in Z^+$, then $a * b = \overbrace{a + b}^{\in Z^+} + 2 \in Z^+$.

(2) well-define : Let $a, b, c, d \in A$ such that $a = c$ and $b = d$,
then $a * b = a + b + 2 = c + d + 2 = c * d$
$\Rightarrow *$ is a binary operation on Z^+.

Example 1.4:

Let $a * b = a^b, a, b \in Z$. Is $*$ is a binary operation on Z.

Solution:

(1) Closure : if $a = 3$ and $b = -1$. Then $a * b = 3^{-1} = \frac{1}{3} \notin \mathrm{Z}$
$\Rightarrow *$ is not a binary operation on Z.

Remark 1.5: Some time we used the symbols $*, \circ, \#, \odot, \ldots$ to denote a binary operation.

Exercises (1): which of the following are binary operations?

[1] $a * b = a + b, \forall a, b \in R\backslash\{0\}$.

[2] $a \odot b = \frac{a}{b}, \forall a, b \in Z$.

[3] $a \# b = a + b - 3, \forall a, b \in N$.

[4] $a \circ b = a + 2b - 5, \forall a, b \in R$.

[5] $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \forall \frac{a}{b}, \frac{c}{d} \in Q\backslash\{0\}$.

Definition 1.6: (Commutative)

A binary operation $*$ on a set A is called a commutative if and only if

$$a * b = b * a \quad \forall \quad a, b \in A.$$

Definition 1.7: (Associative)

A binary operation $*$ on a set A is called an associative if

$$(a * b) * c = a * (b * c) \quad \forall \quad a, b, c \in A.$$

Example 1.8: Let R be a set of real numbers and $*$ be a binary operation on R defined as $a * b = a + b - ab$. Is $*$ commutative and associative.

Solution:

Let $a, b \in R$, then

$a * b = a + b - ab = b + a - ba = b * a$

Which implies that $*$ is commutative.

Let $a, b, c \in R$, then

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

$= (a + b - ab) + c - (a + b - ab)c$

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

$a * (b * c) = a * (b + c - bc)$

$= a + (b + c - bc) - a(b + c - bc)$

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

$\Rightarrow$ (1) = (2) $\Rightarrow$ $*$ is associative.

Exercises (2): Which of the following binary operations is a comm., asso.?

[1] $a * b = a - b, \quad \forall a, b \in Z$.

[2] $a \odot b = 2ab, \quad \forall a, b \in E$.

[3] $a \# b = a^3 + b^3, \quad \forall a, b \in R$.

Definition 1.9: (**Mathematical System**)

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

Example 1.10:

$(R,+), (R,.), (R,-), (R\backslash\{0\},\div), (R,+,.), (N,+), (E,+,\times)$ are Math. System. But $(N,-), (R,\div), (0,+,-)$are not Math. System.

Definition 1.11: (Semi group)

A semi group is a pair $(S,\ *)$ in which S is an empty set and $*$ is a binary operation on S with associative law.

(i.e.) $(S,*)$ is semi group $\Leftrightarrow$ **(1)** $S \neq \emptyset$,

(2) $*$ is a binary operation,

(3) $\forall\ a, b, c \in S$, (a $*$b) $*$c = a $*$(b $*$c).

Example 1.12:

(1) $(Z,+), (Z,\times), (N,+), (N,\times), (E,+), (E,\times)$ are semi groups.

(2) $(0,+), (Z,-)$, (E, $-$), $(R\backslash\{0\},\div)$ are not semi groups.

Definition 1.13: (**The identity element**)

Let $(S,*)$ be a Mathematical System and $e \in S$. Then e is called an identity element if $a * e = e * a = a, \forall\ a \in S$.

Definition 1.14: (**The inverse element**)

Let $(S,*)$ be a Mathematical System and $a, b \in S$. Then b is called an inverse of a if $a * b = b * a = e$ and dented by b = a^{-1}.

Definition 1.15: (**The Group**)

The pair $(G,*)$ is a group iff $(G,*)$ is a semi group with identity in which each element of G has an inverse.

Definition 1.16: (**The Group**)

A group $(G,*)$ is a non-empty set G and a binary operation $*$, such that the following axioms are satisfied:

(1) The binary operation $*$ is associative.

$$\text{(i.e.) } (a * b) * c = a * (b * c), \ \forall \ a, b, c \in G$$

(2) There is an element e in G such that

$$a * e = e * a = a, \forall a \in G.$$

This element e is an identity element for $*$ on G.

(3) For each a in G, there is an element b in G such that

$$a * b = b * a = e.$$

The element b is an inverse of a and denoted by a^{-1}.

Remark 1.17:

Every group is a semi group but the converse is not true as in the following example shows.

$(N, +)$ is a semigroup but not group because $\nexists a^{-1} \in N, \forall a \in N$.

Definition 1.18: (**Commutative group**)

A group $(G,*)$ is called a Commutative group iff $a * b = b * a, \forall a, b \in G$.

Example 1.19:

(1) $(Z, +), (E, +), (Q, +), (C, +)$ are commutative groups .

(2) $(Z^+, +)$ is not a group because there is no identity element for $+$ in Z^+.

(3) $(Z^+, \times)$ is not a group because there is an identity element 1 but no inverse for 5.

(4) $(G = \{1, 0, -1, 2\}, +)$ is not group since $+$ is not a binary operation on G, $1+2 = 3 \notin G$.

(5) $(G = \{1, -1\}, \times)$ is comm. Group.

(6) $(R\backslash\{0\}, \times)$, $(Q\backslash\{0\}, \times)$, $(C\backslash\{0\}, \times)$ are comm. Groups.

Example 1.20: Let $G = \{a, b, c, d\}$ be a set. Define operation $*$ on G by the following table. **(Klein 4-group)**

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

Is $(G,*)$ a commutative group?

Solution:

(1) Closure is true.

(2) Asso. ?

(a ∗ b) ∗ c = a ∗ (b ∗ c) ?

b ∗ c = a ∗ d

d = d

b ∗ (a ∗ c) = b ∗ c = d = (b ∗ a) ∗ c

c ∗ (a ∗ b) = c ∗ b = d = (c ∗ a) ∗ b

d ∗ (a ∗ c) = d ∗ c = b = (d ∗ a) ∗ c ….→

$\Rightarrow *$ is asso.

(3) The identity: To prove $\exists e \in G \;\; s.t. a * e = e * a = a, \forall a \in G.$

$a * a = a, b * a = b, c * a = c, d * a = d.$

$\Rightarrow e = a$ is an identity element of G.

(4) The inverse: $a * a = a \Rightarrow a^{-1} = a$

$b * d = a \Rightarrow b^{-1} = d$

$c * c = a \Rightarrow c^{-1} = c$

$a * a = a \Rightarrow a^{-1} = a$

$d * b = a \Rightarrow d^{-1} = b$

(5) Comm. ?

$a * b = b * a$?

$b = b$

$a * c = c * a = c$

$a * d = d * a = d$

$b * c = c * b = d$

$b * d = d * b = a$

$c * d = d * c = b$

$\Rightarrow *$ is a comm.

Therefore $(G,*)$ is a comm. group and called **Klein 4-group**.

Example 1.21: Let $G = \{1, -1, i, -i\}$ be a set and "." be operation on G.

Is $(G, .)$ a group ? Comm. ?

Solution:

.	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

(1) Closure is true.

(2) Asso. Law is true

(3) 1 is an identity element.

(4) $1^{-1} = 1$, $-1^{-1} = -1, i^{-1} = -i, -i^{-1} = i$

(5) Comm .is true

∴ (G , .) is a comm.group.

Example 1.22: Let G = { $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, a, b ∈ Z }. Is (G,+) group?

Show that (G, +) is a comm. group? (H.W)

Solution:

(1) Closure: ?

Let a,b,c,d ∈Z , then $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix}$ ∈ G since a+c ∈Z and b+d ∈ Z ⟹ Closure is true

(2) Asso. Low: H.W

(3) Identity: ?

$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity element of G since

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

(4) Inverse: ?

Let a , b ∈ Z ∋ A= $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. To prove B = $\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}$ is the inverse element of A

$$A+B = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix} = \begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix} + \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

∴ B = A^{-1} ⟹ ∀A∈G ∃ B∈G such that B= A^{-1}.

∴ (G , +) is a group.

Example 1.23:

Let **G** = R×R = {(a, b) : a , b ∈ R, $a \neq 0$ } and ∗ be defined by

(a , b) ∗ (c , d) = (ac , bc + d)

Prove that (G , ∗) is group. Is (G, ∗) Comm.?

Solution:

(1) Closure : Let (a , b) , (c , d) ∈ G ⟹ a ≠ 0 , c ≠ 0 ⟹ ac ≠ 0

(a , b) ∗ (c , d) = (ac , bc + d) ∈ G ac ≠ 0

(2) Asso. : Let (a , b) , (c , d) , (e , f) ∈ G , we have

(a , b) ∗[(c , d) ∗ (e , f)] = (a , b) ∗ (ce , de + f)

= (ace , bce + de + f) ……(1)

[(a , b) ∗ (c , d)] ∗ (e , f) = (ac , bc + d) ∗ (e , f)

= (ace , (bc + d)e + f))

= (ace , bce + de + f)….. (2)

∴ (1) = (2) , then asso. is true

(3) $Identity : Let\ (a,b),\ (x,y) \in G \ni$

$(a,b) * (x,y) = (x,y) * (a,b) = (a,b)$

$(a,b) * (x,y) = (ax, bx + y) = (a,b)$

∴ ax = a ⇒ $x = 1$

and $bx + y = b \Rightarrow b + y = b \Rightarrow y = 0$

$\therefore (x,y) = (1,0)$

Also, $(x,y) * (a,b) = (xa, ya + b) = (a,b)$

$\therefore xa = a \Rightarrow x = 1$

$ya + b = b \Rightarrow ya = b - b \Rightarrow ya = 0 \Rightarrow y = 0$

$\therefore (x,y) = (1,0)$

$\therefore (1,0)$ *is an identity element of G*

(4) Inverse: $Let\ (a,b),\ (c,d) \in G\ , a \neq 0, c \neq 0$

$(a,b) * (c,d) = (c,d) * (a,b) = (1,0)$

$(c,d) * (a,b) = (1,0)$

$(ac, bc + d) = (1,0) \Rightarrow ac = 1 \Rightarrow c = \frac{1}{a}$

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

$\therefore (c,d) = \left(\frac{1}{a}, \frac{-b}{a}\right)$ *is an inverse of G*

(5) Comm : G is not comm. , since Take (3,5) , (4,6)

$\left.\begin{array}{l}(3, 5) * (4, 6) = (12, 26) \\ (4, 6) * (3, 5) = (12, 23)\end{array}\right\} \Rightarrow$ G is not comm..

Example 1.24: Let (G , *) be an arbitrary group. The set of the function from G in to G : $F_G = \{f_a : a \in G\}$, $f_a: G \to G$ s.t. $f_a(x) = a * x$, $x \in G$,
With the composition (F_G , o) is forms a group, prove that.

Solution:

(1) Closure: Let $f_a, f_b \in F_G$, a, b ∈ G

$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b * x)$

$= a * (b * x)$

$= (a * b) * x$, since G is a group.

$= f_{a*b}(x) \in F_G$, since $a*b \in G$

(2) Asso : Let $f_a, f_b, f_c \in F_G$, a, b, c ∈ G

$(f_a \circ f_b) \circ f_c = f_{a*b} \circ f_c = f_{(a*b)*c}$

since * is asso. on G

$= f_{a*(b*c)} = f_a \circ f_{b*c} = f_a \circ (f_a \circ f_c)$

(3) Identity : f_e is an identity of F_G, since

$f_a \circ f_e = f_{a*e} = f_{e*a} = f_e \circ f_a = f_a$

(4) Inverse : The inverse of f_a in F_G is f_a^{-1}, since

$f_a \circ f_a^{-1} = f_{a*a^{-1}} = f_{a^{-1}*a} = f_a^{-1} \circ f_a = f_e$

Also, if G is comm. group, then (F_G, o) is comm. group .

Exercises (3): Determine the systems (G, ∗) . Is (G,*) group? Is (G,*) comm. group?

[1] G = Z, a ∗ b = a + b + 4

[2] G = R × R = {a, b) : a , b ∈ R} s.t

(a, b) ∗ (c, d) = (a + b, b + d - 3bd).

[3](G = {$f_1, f_2, f_3, f_4, f_5, f_6$}, o) , where

$f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1+x$, $f_4(x) = \frac{x+1}{x}$, $f_5(x) = \frac{x}{x+1}$, $f_6(x) = \frac{1}{1+x}$

[4] G = {(a, b) : a, b ∈ R , a ≠ 0 , b ≠ 0} s.t.

(a, b) ∗ (c, d) = (ac, b+d)

[5] (G = { am : m ∈ Z } , +)

[6] $G = Q^+$, $a * b = \frac{ab}{5}$.

[7] G = Z, a ∗ b = a + b - 2

[8] Let G = { $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, a, b ∈ Z }. Is (G, .) group? zdxr

[9] Let G = { $\begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$, a ∈ Z }. Is (G, +) group?

[10] Let $G = \{f_1, f_2, f_3, f_4\}$, where $f_i \ni i = 1, 2, 3, 4$, are mappings on $R\backslash\{0\} \ni$ $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$. Show that $(G, \circ)$ is a group. Is (G , ∘) Comm. ?

Some Properties of Groups:

Theorem 1.25: If G is a group with a binary operation $*$, then the left and right cancellation laws hold in G, that is:

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

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

For all a, b, c $\in$ G.

Proof: H.W.

Theorem 1.26: In a group $(G, *)$, there is only one element e in G such that $e * a = a * e = a, \quad \forall a \in G$.

Proof: Suppose that G has two identity elements e and e'

that mean $\forall a \in G$.

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

Since each e and e' belong to G , so

$e * e' = e' * e = e$ (e عنصر و e' عنصر محايد)

$e' * e = e * e' = e'$ (e' عنصر و e عنصر محايد)

It follows that $e' = e$.

Theorem 1.27: In a group $(G, *)$, the inverse element of each element in G is unique.

Proof: Let $a \in G$ and a has two inverse x and x' . Such that

$a * x = x * a = e$

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

$$\Rightarrow x = x * e = x * (a * x') = (x * a) * x' = e * x' = x'$$

$\therefore x = x' \Rightarrow$ the inverse is an unique element.

Theorem 1.28: If $(G, *)$ is group , then

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

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

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

Proof:

(1) Let $e^{-1}= x$

e is the identity element of G $\Longrightarrow x * e = e * x = x$ ------- (1)

x is the inverse of e $\Longrightarrow e * x = x * e = e$ ------- (2)

from (1) and(2) $\Longrightarrow x = e \Rightarrow e^{-1} = e$.

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

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

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

$= e * a = a.$

(3) To prove, $(a * b)^{-1} = b^{-1} * a^{-1}, \quad \forall a , b \in G$

Since $(a * b) \in G \Longrightarrow (a * b)^{-1} \in G$

$(a * b) * (a * b)^{-1} = (a * b)^{-1} * (a * b) = e$ (def . of inverse)

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

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

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

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

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

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

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

Theorem 1.29: Let (G , ∗) be a group . Then

(1) $(a * b)^{-1} = a^{-1} * b^{-1} \Longleftrightarrow$ G is comm. group.

(2) If $a = a^{-1}$, then G is a comm . gp . (Is the converse true?)

Proof: **(1)** ($\Longrightarrow$) Let (G , ∗) be a group and $(a * b)^{-1} = a^{-1} * b^{-1}$.

To prove G is comm.

Let $a , b \in G$. To show $a * b = b * a , \forall a , b \in G$

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

$= (b^{-1} * a^{-1})^{-1}$ (by Theorem 1.29 (3))

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

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

$\therefore$ G is comm. gp.

($\Longleftarrow$) Let (G , ∗) is a comm . gp.

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

$(a * b)^{-1} = b^{-1} * a^{-1}$ (by Theorem 1.29 (3))

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

(2) If $a = a^{-1}$, then G is a comm . gp . (Is the converse true?)

Proof: Let $a = a^{-1}$ To prove, $a * b = b * a$, $\forall a , b \in G$

Let $a , b \in G$ and $a * b \in G \Longrightarrow (a * b) = (a * b)^{-1}$

$= b^{-1} * a^{-1}$ (by Theorem 1.29 (3))

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

$\therefore$ G is a comm. Group.

The converse of this part is not true.

(i.e.) if $(G , *)$ is comm . $\nRightarrow$ $a = a^{-1}$

For example:

Let $(G = \{1, -1, i, -i\}, .)$ be comm . group,

Let $a = i \Longrightarrow a^{-1} = -i$

$\therefore a \neq a^{-1}$

Give another example (H. W.)

Theorem 1.30: In a group $(G , *)$, the equations $a * x = b$ and $y * a = b$ have a unique solution.

proof: we take

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

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

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

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

To show the solution is a unique

Let $x' \in G$ s.t. $a * x' = b$

$\Longrightarrow a * x' = a * x$

$\Longrightarrow x' = x$ (by com. law)

By same way, we prove $y * a = b$ has Solution $y = b * a^{-1}$.

Definition 1.31: (The Integral Powers of *a*)

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

(1) $a^n = \underbrace{a * a \ldots * a}_{n-tim}$

(2) $a^0 = e$

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

(4) $a^{n+1} = a^{n} * a \;\; , n \in Z^{+}$.

For example 1.32:

(1) In (R , +),

$3^0 = 0$,

$3^3 = 3 + 3 + 3 = 9$,

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

$= -6$.

(2) In (R , .) ,

$2^0 = 1$,

$2^3 = 2 \times 2 \times 2 = 8$,

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

$= \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16}$

(3) In (G = {1, -1, i, -i}, .) ,

$i^o = 1$, $i^2 = i \times i = -1$, $i^{-2} = (i^{-1})^2 = (-i)^2 = -i \times -i = -1$

Theorem 1.33: Let (G , ∗) be agroup and $a \in G$, $m , n \in Z$, then :

(1) $a^n * a^m = a^{n+m}$ $\forall n , m \in Z$ (H. W.)

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

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

(4) $(a * b)^n = a^n * b^n$ $\forall n \in Z$ ⇔ G is comm . group.

Proof:

(2) To prove, $(a^n)^m = a^{nm}$, $\forall n , m \in Z^+$

Let p(m) : " $(a^n)^m = a^{nm}$ $\forall n \in Z^+$ "

To prove, P(m) is true $\forall m \in Z^+$

If $m = 1 \Longrightarrow p(1) : (a^n)^1 = a^n = a^{n \times 1} \Longrightarrow$ p(1) is true

Suppose that p(k) is true with $k \in Z^+$ and $k \leq m$

$\therefore$ $(a^n)^k = a^{nk}$

We have to prove that p (k + 1) is true P (k+ 1) : $(a^n)^{k+1} = a^{n(k+1)}$??

$(a^n)^{k+1} = (a^n)^k * (a^n)^1$ (by define of $a^{n+1} = a^n * a^1$)

$= a^{nk} * a^n$

$= a^{nk+n}$ by (1) above

$= a^{n(k+1)}$

$\therefore$ p (k + 1) is true

By the principle of mathematical induction

$\Longrightarrow$ p (m) is true $\forall m \in Z^+$

$\therefore (a^n)^m = a^{nm}$, $\forall n , m \in Z^+$

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

If $n = 1 \Rightarrow p(1) : (a^{-1})^1 = a^{-1} = (a^1)^{-1}$

Suppose that if $n = k$ is true $\Rightarrow p(k) = (a^{-1})^k = (a^k)^{-1}$

We must prove p (k+1) is true

$P(k+1) : (a^{-1})^{k+1} = (a^{k+1})^{-1}$?

$(a^{-1})^{k+1} = (a^{-1})^k * (a^{-1})^1 = (a^k)^{-1} * (a^1)^{-1} = (a^{k+1})^{-1}$

$\therefore$ p (k +1) is true

By the principle of math. ind. $\Rightarrow$ p (n)is true , $\forall\, n \in Z^+$.

(4) ($\Rightarrow$) If $n = 2 \Rightarrow (a * b)^2 = a^2 * b^2$, To prove, is comm. Group.

$(a * b) * (a * b) = a * a * b * b$ (by def . of power int.)

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

$(b * a) * b = (a * b) * b$ (by cancellation law)

$b * a = a * b$ (by cancellation law)

$\therefore$ G is comm . group.

($\Leftarrow$) Let G be comm . group .

To prove, $(a * b)^n = (a^n * b^n)$, $\forall\, n \in Z$.

Let $p(n) : (a * b)^n = a^n * b^n$

If $n = 1 \Rightarrow (a * b)^1 = a^1 * b^1$ is true

Suppose that p (k) is true with $k \in Z^+$ and $k \le n$

s.t . $(a * b)^k = a^k * b^k$

We must prove P (k +1) is true

$P(k+1) : (a * b)^{k+1} = (a * b)^k * (a * b)^1$

$= a^k * b^k * a^1 * b^1$

$= (a^k * b^k) * (b * a)$ (G is comm .)

$= a^k * (b^k * b) * a$ (by asso .)

$= a^k * b^{k+1} * a$

$= a^k * a * b^{k+1}$

$= a^{k+1} * b^{k+1}$

$\therefore$ p(k + 1) is true , $\forall\, n \in Z^+$

Definition 1.34: ((**Order of a Group**))

The number of elements of a group G is called the order of G and is denoted by | G | or o (G).

G is called a finite group if $|G| < \infty$ and infinite group otherwise .

Definition 1.35: (**The Order of an Element**)

The order of an element a , $a \in$ G is the least positive integer n such that $a^n = e$, where e is the identity element of G. We denoted to order a by $|a|$ or o(a).

(i.e.) $|a| = n$ if $a^n = e$, $n \in Z^+$

Example 1.36: (Z , +) is an infinite group .

Example 1.37: In a trivial group G = { 0 }

| G | = 1 , G is the only group of order 1.

Example 1.38: find the order of G and the order of each element of (G, .). Such that G = { 1, -1 , i, -i}.

Solution:

| G | = 4 and

$|a| = ??$

If $a = 1$, and $(1)^1 = 1$, $\Rightarrow |a| = |1| = 1$ (since $e = 1$)

If $a = -1$, and $(-1)^2 = 1$ $\Rightarrow |-1| = 2$

If $a = i$, and $i^2 = -1$, $i^4 = 1 \Rightarrow |i| = 4$

If $a = -i$, and $-i^2 = -1$, $-i^3 = i$, $-i^4 = 1 \Rightarrow |-i| = 4$

The Group of Integers Modulo *n* ***(زمرة الاعداد الصحيحة مقياس n)***

Definition 1.39:

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

Example 1.40:

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

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

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

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

Theorem 1.41: The congruence module n is an equivalence relation on the set of integers.

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

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

$\therefore a \equiv a \pmod{n}$ **Reflexive is true**

(2) If $a \equiv b \pmod{n}$, To prove, $b \equiv a \pmod{n}$

Since $a \equiv b \pmod{n} \Rightarrow a - b = nk , k \in Z$

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

$\therefore b \equiv a \pmod{n} \Rightarrow$ **Symmetric is true**

(3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. To prove, $a \equiv c \pmod{n}$

Since $a \equiv b \pmod{n}$, then $a-b = nk$

And $b \equiv c \pmod{n}$, then $b - c = nk^{/}$

By adding these two eqs . $\Rightarrow a - c = n (k + k^{/}) , k + k^{/} \in Z$

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

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

Definition 1.42: Let $a \in Z$, $n > o$. The congruence class of a modulo n, denoted by [a] is the set of all integers that are congruent to a modulo n .

(i.e.)

$[a] = \{z \in Z : z \equiv a \pmod{n} \}$

$= \{z \in Z : z = a + k n , k \in Z \}$

Example 1.43:

If $n = 2$, find [0] , [1]

$[0] = \{ z \in Z : z \equiv 0 \pmod{2} \}$

$= \{ z \in Z : z = 0 + 2k , k \in Z \}$

$= \{ 0 , \mp 2 , \mp 4 , \ldots\ldots\ldots\ldots \}$

$[1] = \{ z \in Z : z \equiv 1 \pmod{2} \}$

$= \{ z \in Z : z = 1 + 2k , k \in Z \}$

$= \{\mp 1 , \mp 3 , \mp 5 , \ldots. \}$.

Example 1.44:

If $n = 3$, find [1] , [7]

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

$= \{ 1 , 1 \mp 3, 1 \mp 6 \ldots. \}$

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

[7] (H. W.)

Definition 1.45:

The set of all congruence classes modulo n is denoted by Z_n (which is read Z mod n). Thus

$Z_n = \{ [\,0\,], [\,1\,], [\,2\,], \ldots\ldots, [\,n-1\,] \}$, or

$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

Z_n has n elements.

Example 1.46:

$Z_1 = \{\bar{0}\}$

$Z_2 = \{ \bar{0}, \bar{1} \}$

$Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

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

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

Similarly, **we define multiplication on Z_n** (write "$._n$" by the following :

$$[a]\, ._n\, [b] = [a\, ._n\, b], \quad \forall\, [a], [b] \in Z_n$$

It is easy to see that $(Z_n, +_n)$ is an abelian group with identity [0] and for every [a] $\in Z_n$, $[a]^{-1} = [\, n - a \,]$. **This group is called the Additive Group of Integers Modulo *n* .**

Also, $(Z_n, ._n)$ is abelian semi group with identity [1] . **It is called the Multiplicative Semi Group of Integers modulo *n*.**

Example 1.47: $(Z_4, +_4)$, $Z_4 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}$

(1) Closure is true

(2) Asso. is true

(3) $\bar{0}$ is an identity element

(4) Inverse:

$\bar{1}^{-1} = \bar{4} - \bar{1} = \bar{3}$

$\bar{2}^{-1} = \bar{4} - \bar{2} = \bar{2}$

$\bar{3}^{-1} = \bar{4} - \bar{3} = \bar{1}$

(5) Comm :

$\bar{1} + \bar{2} = \bar{3} = \bar{2} + \bar{1}$

$\bar{1} + \bar{3} = \bar{0} = \bar{3} + \bar{1}$

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

$\therefore$ $(Z_4, +_4)$ is a Comm.group.

<u>Example 1.48</u>: $(Z_4, \cdot_4)$, $Z_4 = \{\, \overline{0}\,, \overline{1}\,, \overline{2}\,, \overline{3}\,\}$

It is clear that we cannot have a group.
Since the number $\overline{1}$ is identity,
but the numbers $\overline{0}$ and $\overline{2}$ have no inverse.
It follows that $(Z_4,\ \cdot_4)$ is not a group,
but it is semi group.

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

<u>Example 1.49:</u> Find the order of G and the order of each element of (G, *), such that (G, *) = $(Z_8, +_8)$.

<u>Solution:</u>

$Z_8 = \{\, \overline{0}\,, \overline{1}\,, \overline{2}\,, \overline{3}\,, \overline{4}\,, \overline{5}\,, \overline{6}\,, \overline{7}\,\}$, e = $\overline{0}$

$o(Z_8) = 8$ since (The number of elements of a group $Z_8 = 8$)

The order of an element a, a ∈ Z_8 is the least positive integer n such that $a^n = \overline{0}$, where $\overline{0}$ is the identity element of Z_8.

$o(\overline{0}) = 1$ since $(\overline{0})^1 = \overline{0}$ = e

$o(\overline{1}) = 8$ since $(\overline{1})^8 = \overline{1}+\overline{1}+\overline{1}+\overline{1}+\overline{1}+\overline{1}+\overline{1\ +1} = \overline{8} = \overline{0}$ = e

$o(\overline{2}) = 4$ since $(\overline{2})^2 = \overline{2}+\overline{2}+\overline{2}+\overline{2} = \overline{8} = \overline{0}$ = e

$o(\overline{3}) = 8$ since $(\overline{3})^8 = \overline{3}+\overline{3}+\overline{3}+\overline{3}+\overline{3}+\overline{3}+\overline{3}+\overline{3} = \overline{24}$
$= \overline{8}+\overline{8}+\overline{8} = \overline{0}+\overline{0}+\overline{0} = \overline{0}$ = e

$o(\overline{4}) = 2$ since $(\overline{4})^2 = \overline{4}+\overline{4} = \overline{8} = \overline{0}$ = e

$o(\overline{5}) = 8$ since $(\overline{5})^8 = \overline{5}+\overline{5}+\overline{5}+\overline{5}+\overline{5}+\overline{5}+\overline{5}+\overline{5} = \overline{40}$
$= (\overline{8})^5 = \overline{(0)}^5 = \overline{0}$ = e

$o(\overline{6}) = 4$ since $(\overline{6})^8 = \overline{6}+\overline{6}+\overline{6}+\overline{6} = \overline{24} = \overline{0}$ = e

$o(\overline{7}) = 8$ since $(\overline{7})^8 = \overline{56} = \overline{0}$ = e

<u>Exercises (4):</u>

1. Find the order of Z_6 and the order of each element of $(Z_6, +_6)$.
2. Find the order of Z_9 and the order of each element of $(Z_8, +_8)$.
3. Find the order of Z_6 and the order of each element of $(Z_9, +_9)$.

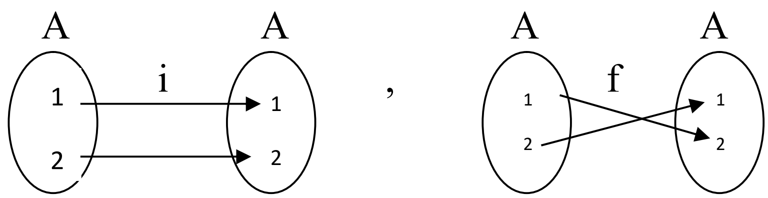
The Permutations : (التباديل)

Definition 1.50: A Permutation or symmetric of a set A is a function from A in to A that is both one to one and on to.

$$f: A \xrightarrow{1-1, onto} A$$

Symm (A) = $\{f \mid f: A \xrightarrow{1-1, onto} A\}$ the set of all permutation on A.
If A is the finite set $\{1, 2, \ldots, n\}$, then the set of all permutation of A is denoted by S_n or P_n and $o(S_n) = n!$, where $n! = n\,(n-1) \ldots (3)(2)\,(1)$

Example 1.51: Let A = {1, 2} . Write all permutation on A.



Symm(A) = {i, f } = $\left\{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}$.

Example 1.52: Let $A = \{1, 2, 3\}$. Write all permutation on A.

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

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

$P_3 = Symm(A) = \{f_1, f_2, f_3, f_4, f_5, f_6\}$
$o(P_3)$= 3 ! = (3) (2) = 6

Theorem 1.53: If $A \neq \varphi$, then the set of all permutation on A Forms agroup with composition of Mapps.
(i.e.) Let $A \neq \varphi$, then (Symm(A) , o) is a group.

Proof:

Symm (A) = $\{f \mid f: A \xrightarrow{1-1, onto} A \ \ is\ a\ mapp.\}$,
To prove, (Symm(A) ,o) is a group.
since $\exists\, i_A: A \xrightarrow{1-1, onto} A$ a perm. on A
$\therefore i_A \in$ Symm(A) $\Longrightarrow$ Symm(A) $\neq \varphi$.
(1) Closure : Let f , $g \in$ symm(A) , it follows that

$$f: A \xrightarrow{1-1,onto} A \ , \ g: A \xrightarrow{1-1,onto} A$$

$$\Rightarrow fog: A \xrightarrow{1-1,onto} A \Rightarrow fog \in \text{Symm}(A)$$

(2) Asso. : True since the composition of maps is an asso.

(3) The identity : since $i_A \in$ symm(A) and $i_A o f = f o i_A = f$ for all f in symm(A) $\Rightarrow i_A$ is an idenetity element

(4) The inverse : $\forall f: A \xrightarrow{1-1,onto} A, \exists f^{-1}: A \xrightarrow{1-1,onto} A$

$\therefore f^{-1} \in$ Symm(A) and $f o f^{-1} = f^{-1} o f = i_A$

$\therefore$ (Symm(A), o) is a group.

Is (Symm(A), o) comm. group ? (H.W.)

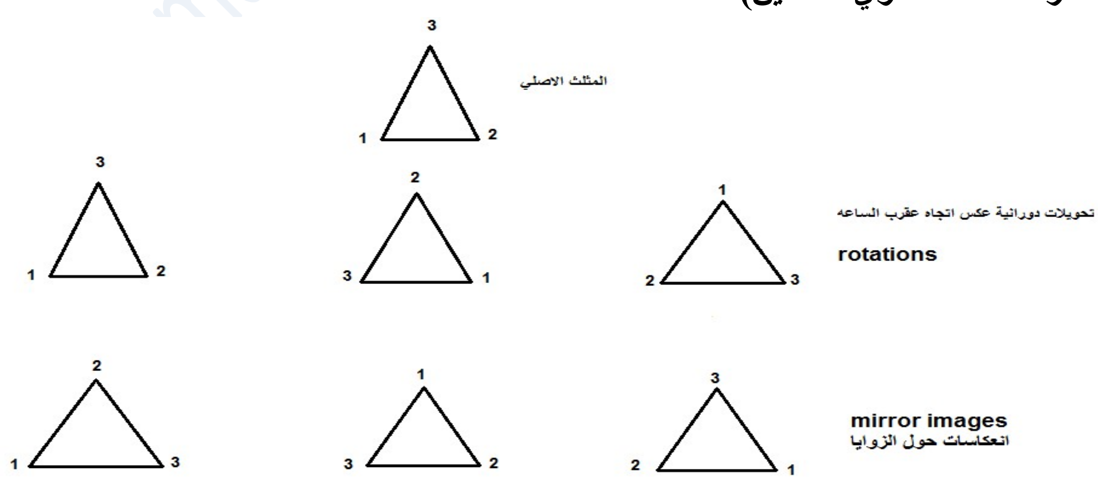
Example 1.54: Let $A = \{1, 2, 3\}$, then $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ and (S_3, o) is a group. This group is called symmetric group.

O	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

(S_3 , o) is not Comm. Group.

Also (S_3,o) is **called the group of symmetries of on equilateral triangle** .

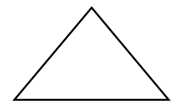
(زمرة تناظر المثلث متساوي الساقين)



<u>Definition 1.55</u> (The Dihedral Group D_n of Order $2n$)

The n^{th} dihedral group is the group of symmetries of the regular n-gon. $o(D_n) = 2n$

D_3 : is the third dihedral group.

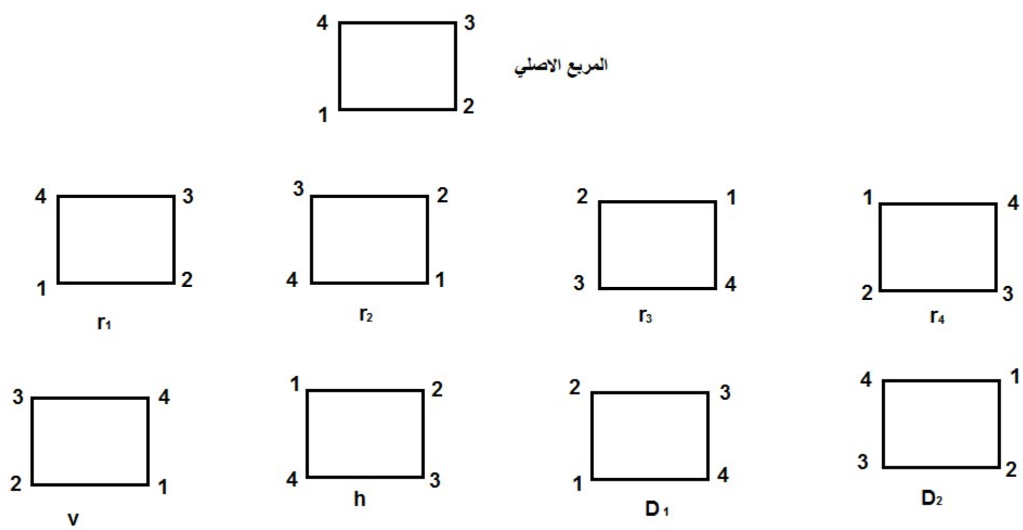


, $O(D_3) = (2)(3) = 6$ elements.

<u>Example 1.56:</u> The group of symmetries of square D_4 or Gs, $o(D_4) = 8$

$G_s = D_4 = \{r_1, r_2, r_3, r_4, h, v, D_1, D_2\}$, where r_i are a clockwise rotation

V, h, D_1, D_2 are mirror images



(1) Write all elements of Gs as a permutation.

(2) Is (Gs , o) comm. group? Use table (H.W.)

<u>Definition 1.57:</u> A permutation f of a set A is called a cycle of length n if there exist $a_1, a_2, \ldots\ldots, a_n \in A$ such that

$f(a_1) = a_2$, $f(a_2) = a_3$, ..., $f(a_{n-1}) = a_n$, $f(a_n) = a_1$ and $f(x) = x$,

for $x \in A$ but $x \notin \{a_1, a_2, \ldots\ldots, a_n\}$. We write $f = (a_1, a_2, \ldots, a_n)$.

<u>Example 1.58:</u> If $A = \{1, 2, 3, 4, 5\}$, then

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1354)(2) = (1354)$$

Observe that

$(1354) = (3541) = (5413) = (4135)$.

Example 1.59: Let $A = \{1, 2, 3, 4, 5, 6\}$ be a set of a group S_6 . Then

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = (142)o(3)o(56) = (142)o(56)$$

And

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} = (16)o(245)o(3) = (16)o(245)$$

These permutations above are not cycles.

Theorem 1.60: Every permutation f of a finite set A is a product of disjoint cycles.

Definition 1.61: A cycle of length 2 is a transposition.

Example 1.62: The permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24) \text{ is a transposition.}$$

Proposition 1.63: Any permutation can be expressed as the product of transpositions.

(i.e.) $(a_1a_2 \ldots a_n) = (a_1a_2)\,(a_1a_3) \;\ldots..(a_1a_n)$

Therefore any cycle is a product of transpositions.

Example 1.64: We see that (16) (2 5 3) = (16) (2 5) (2 3).

Definition 1.65: A permutation is **even or odd** according as it can be written as the product of an even or odd number of transpositions.

Example 1.66: Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in P_3$. Is f even or odd permutation.

Solution: $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) = (13)\,(12)$

f has 2 transpositions $\Rightarrow f$ is an even perm.

Example 1.67: Determine an even and odd permutations of P_4. (H.W)

Definition 1.68: **(Alternating Group)** زمرة التباديل

The Alternating group on n letters, denoted by A_n is the group consisting of all even permutations in the symmetric group S_n.

$$o(A_n) = \frac{n!}{2} \quad , \quad A_n \subset S_n$$

Example 1.69: Let $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, then

$A_3 = \{i , f_2, f_3\}$ is a sub group of S_3

$o(A_3) = \frac{6}{2} = 3$