CHAPTER SIX

Binary Operations العمليات الثنائية

Chapter Three Contents:

1. Binary operation العملية الثنائية

2. Properties of binary operations خواص العمليات الثنائية

3. Group, Ring and Field الزمرة والحلقة والحقل

<u>Definition</u> 3.1: Let A be a nonempty set. Any mapping from $A \times A$ into A is called **a binary operation on A**. The binary operation is denoted by the symbols $*$, #, $, o, ….

Mathematically,

$*: A \times A \to A$ is a binary operation iff
1. $*((a,b)) = a * b \in A$ (**closure condition**)
i.e., $\forall a, b \in A \Rightarrow a * b \in A$
2. if $a, b, c, d \in A$ s.t. $(a,b) = (c,d)$ then $a * b = c * d$ (**well defined condition**).

<u>Example</u> 3.2: Let $A = \{0,1,-1\}$, let * be an operation on A such that

$a * b = b^2 \quad \forall a, b \in A$

Is * binary operation on A?

<u>Solution</u>:

Closure? Let $a, b \in A \Longrightarrow a * b \in A$?

$\forall a, b \in A \Longrightarrow a * b = b^2 \in A \Longrightarrow *$ is closure

Well defined? Let $a, b, c, d \in A$ s.t. $(a,b) = (c,d) \Longrightarrow a * b = c * d$?

Since $(a,b) = (c,d) \Longrightarrow a = c \wedge b = d$

$a * b = b^2$ (def. of *)

$= d^2$ $(b = d)$

$= c * d$ (def. of $*$)

$\therefore *$ is well defined

$\therefore *$ is a binary operation on A

<u>Example</u> 3.3: Let $A = \{0,1,-1\}$, let * be an operation on A such that

$a * b = a - b \qquad \forall a, b \in A$

Is * binary operation on A?

<u>Solution</u>:

Closure? Let $a, b \in A \Longrightarrow a * b \in A$?

If $a, b \in A \Longrightarrow a * b = a - b \notin A$

Take $a = 1, b = -1 \Longrightarrow a * b = a - b = 1 + 1 = 2 \notin A$

$\therefore *$ is not closure

$\therefore$ * is not a binary operation on A

<u>Example</u> 3.4: Let $A = N$, let # be an operation on N such that

$a\#b = a - b \qquad \forall a, b \in N$

Is # binary operation on N?

<u>Solution</u>: Closure? Let $a, b \in N \Longrightarrow a\#b \in N$?

If $a, b \in N \Longrightarrow a\#b = a - b \notin N$

Take $a = 2, b = 5 \Longrightarrow a\#b = a - b = 2 - 5 = -3 \notin N$

$\therefore$ # is not closure

$\therefore$ # is not a binary operation on N

<u>Example</u> 3.5: (H. W.) Let $A = Z$, let * be an operation on Z such that

$a * b = a + b + 1 \qquad \forall a, b \in Z$

Is * binary operation on Z?

<u>Example</u> 3.6: (H. W.) Let $A = E$, let * be an operation on E such that

$a * b = 2ab \quad \forall a, b \in E$

Is * binary operation on E?

<u>Example</u> 3.7: (H. W.) Let $A = O$, let * be an operation on O such that

$a * b = a + b \quad \forall a, b \in O$

Is * binary operation on O?

<u>Example</u> 3.8:

1. Let $A = N$, $a * b = a + b \quad \forall a, b \in N$

   "+" is a binary operation on N الجمع عملية ثنائية على مجموعة الاعداد الطبيعية

2. "+" is a binary operation on Z, R, Q, E

3. "-" is a binary operation on Z, R, Q, E

4. "×" is a binary operation on Z, R, Q, E, O, N

5. "÷" is a binary operation on $R\backslash\{0\}, Q\backslash\{0\}$

6. "÷" is not a binary operation on $N\backslash\{0\}, Z\backslash\{0\}$

<u>Properties of Binary Operations</u> خواص العمليات الثنائية

<u>1. Commutative Binary Operation</u> العملية الثنائية الابدالية

A binary operation * on a set A is called **commutative** iff $a * b = b * a \quad \forall a, b \in A$

<u>Example</u> 3.9:

"+" is a commutative binary operation on $N, Z, \mathbb{R}, Q, E$

"." is a commutative binary operation on $N, Z, \mathbb{R}, Q, E$

"-" is not commutative binary operation on $N, Z, \mathbb{R}, Q, E$

<u>Example</u> 3.10: Let $a * b = a + b + ab \quad \forall a, b \in Z$. Is * commutative binary operation on Z?

<u>Solution</u>: * binary operation?

Closure? Let $a, b \in Z \Longrightarrow a + b \in Z \Longrightarrow \mathrm{a + b + ab \in Z}$

$\therefore$ * is closure

well-defined? Let $a, b, c, d \in Z$ s.t. $(a, b) = (c, d) \Longrightarrow a * b = c * d$?

Since $(a, b) = (c, d) \Longrightarrow a = c \wedge b = d$

$\Longrightarrow a * b = a + b + ab$ (def. of *)

$= c + d + cd \quad (a = c \wedge b = d)$

$= c * d$

$\therefore *$ is well defined

$\therefore$ * is a binary operation

Commutative? $a * b = a + b + ab = b + a + ba = b * a$

$*$ is commutative

<u>Example</u> 3.11: Let $a\$b = a \ \forall a, b \in Q$. Is \$ commutative binary operation on Q?

<u>Solution</u>: \$ binary operation? (**H.W.**)

Comm.? $a\$b = a$ and $b\$a = b$

$\Longrightarrow a \neq b$

Take $a = \frac{1}{3}$ and $b = 5$

$a\$b = \frac{1}{3}$ and $b\$a = 5$

<u>Example</u> 3.12: Let $A * B = A \cup B \quad \forall A, B \in P(X)$. Is $\cup$ commutative binary operation on $P(X)$?

<u>Solution</u>: * binary operation?

Closure? Let $A, B \in P(X) \Longrightarrow A * B = A \cup B \subseteq X \Longrightarrow A * B \in$ P(X)

$\therefore$ $\cup$ is closure

well-defined? Let $A, B, C, D \in P(X)$ s.t. $(A, B) = (C, D) \Longrightarrow A * B = C * D$?

$(A, B) = (C, D) \Longrightarrow A = C \wedge B = D$

$\Longrightarrow A * B = A \cup B$ (def. of *)

$= C \cup D \quad (A = C \wedge B = D)$

$= C * D$

$\therefore$ * is well defined

$\therefore$ * is a binary operation

Commutative? (H.W.)

<u>2. Associative Binary Operation</u> العملية الثنائية التجميعية

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

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

<u>Example</u> 3.13: Let $a.b = a + b - 2 \quad \forall a, b \in Z$. Is "." associative, commutative binary operation on Z?

<u>Solution</u>: "." binary operation? (**H.W.**)

Associative? Let $a, b, c \in Z, (a.b).c = a.(b.c)$?

$(a.b).c = (a + b - 2).c$ (def. of .)

$= (a + b - 2) + c - 2$ (def. of .)

$= a + b + c - 4 \dots .(1)$

$a.(b.c) = a.(b + c - 2)$ (def. of .)

$= a + (b + c - 2) - 2$ (def. of .)

$= a + b + c - 4 \dots .(2)$

From (1) &(2), $(a.b).c = a.(b.c)$

Commutative? (H.W.)

Example 3.14: **(H.W.)** Let $A * B = A \cup B \quad \forall A, B \in P(X)$. Is $\cup$ associative binary operation on $P(X)$?

Example 3.15: **(H.W.)** Let $A * B = A \cap B \quad \forall A, B \in P(X)$. Is $\cap$ associative, commutative binary operation on $P(X)$?

3. Distributive Property خاصية التوزيع

Let * and # are two binary operations on a set A. Then *** is distributive over # from the left** if and only if

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

Also, *** is distributive over # from the right** if and only if

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

Remark 3.16:

1. $a * (b\#c) \neq (b\#c) * a$ (in general)

2. If $a * (b\#c) = (b\#c) * a$ then we say that $*$ **is distributive over** #

Example 3.17: Let $*$ be a binary operation on Z such that

$$a * b = a \quad \forall a, b \in Z$$

Let # be a binary operation on Z such that $a\#b = a + b - 2 \ \ \forall a, b \in Z$

Is * distributive over # from left and from right?

*** distributive over # from left ?**

We must show if $a * (b\#c) = (a * b)\#(a * c) \quad \forall a, b, c \in Z$

$a * (b\#c) = a$ (def. of *)…..(1)

$(a * b)\#(a * c) = a\#a$ (def. of *)

$= a + a - 2$ (def. of #)

$= 2a - 2$ ….(2)

From (1) and (2), $a * (b\#c) \neq (a * b)\#(a * c)$

$\therefore$ * is not distributive over # from left

*** distributive over # from, right ?**

We must show if $(b\#c) * a = (b * a)\#(c * a) \quad \forall a, b, c \in A$

$(b\#c) * a = b\#c$ (def. of *)

$= b + c - 2$ (def. of #) ….(1)

$(b * a)\#(c * a) = b\#c$ (def. of *)

$= b + c - 2$ (def. of #) ….(2)

From (1) and (2), $(b\#c) * a = (b * a)\#(c * a)$

$\therefore$ * is distributive over # from right

Example 3.18: (H.W.) Let $*$ be a binary operation on N such that $a * b = ab \ \forall a, b \in N$

Let # be a binary operation on N such that $a \# b = a + b \ \forall a, b \in N$

Is * distributive over # from left and from right?

Example 3.19: (H.W.) Let $*$ be a binary operation on $P(X)$ such that $A * B = A \cup B \ \forall A, B \in P(X)$

Let # be a binary operation on $P(X)$ such that $A \# B = A \cap B \ \forall A, B \in P(X)$

Is * distributive over # from left and from right?

Definition: The Identity Element العنصر المحايد

Let $*$ be a binary operation on a set A and $e \in A$, then e is called **the identity element of A** if and only if $a * e = e * a = a \quad \forall a \in A$

Example 3.20:

1. "0" is the identity element of the sets $Z, Q, \mathbb{R}$ with respect to (w.r.t.) (+)

الصفر هو العنصر المحايد للمجموعات $Z, Q, \mathbb{R}$ بالنسبة لعملية الجمع

$i.e., a + 0 = 0 + a \quad \forall a \in Z, Q, \mathbb{R}$

2."0" is not the identity element of the sets Z, Q, R with respect to (w.r.t.) (-)

الصفر لايمثل العنصر المحايد للمجموعات $Z, Q, \mathbb{R}$ بالنسبة لعملية الطرح

$i.e., \ \exists a \in Z, Q, \mathbb{R} \ s.t. \ a - 0 \neq 0 - a$

3. "1" is the identity element of the sets $N, Z, Q, \mathbb{R}$ w.r.t. (.)

الواحد هو العنصر المحايد للمجموعات $N, Z, Q, \mathbb{R}$ بالنسبة لعملية الضرب

$i.e., a.1 = 1.a \quad \forall a \in N, Z, Q, \mathbb{R}$

4. "1" is not the identity element of the sets $Q - \{0\}, \mathbb{R} - \{0\}$ with respect to (w.r.t.) (/)

الواحد لايمثل العنصر المحايد للمجموعات $Q - \{0\}, \mathbb{R} - \{0\}$ بالنسبة لعملية القسمة

$i.e., \quad \exists a \in Q - \{0\}, \mathbb{R} - \{0\} \;\; s.t. \;\; \frac{a}{1} \neq \frac{1}{a}$

<u>Example</u> 3.21: Let # be a binary operation on $\mathbb{R}\backslash\{-1\}$ such that

$a\#b = a + b + ab \quad \forall a, b \in \mathbb{R}\backslash\{-1\}$. Find the identity element of $\mathbb{R}\backslash\{-1\}$ with respect to #.

<u>Solution</u>: Let e be the identity element of $\mathbb{R}\backslash\{-1\}$ s.t. $a\#e = e\#a = a \quad \forall a \in \mathbb{R}\backslash\{-1\}$

We must find e?

$a\#e = a \;\Rightarrow a + e + ae = a$ (def. of #)

$\Rightarrow \mathrm{e + ae = 0}$

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

Either $e = 0$

or $1 + a = 0 \Rightarrow \mathrm{a} = -1 \notin R\backslash\{-1\}$ يهمل

$\therefore e = 0 \in R\backslash\{-1\}$ ….(1)

$e\#a = a \;\Rightarrow e + a + ea = a$ (def. of #)

$\Rightarrow \mathrm{e + ea = 0}$

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

Either $e = 0$

or $1 + a = 0 \Rightarrow \mathrm{a} = -1 \notin R\backslash\{-1\}$ يهمل

$\therefore e = 0 \in R\backslash\{-1\}$….(2)

From (1) and (2), $e = 0$

Example 3.22: (H. W.) Let # be a binary operation on $Z\backslash\{-1\}$ such that

$a\#b = a + b + ab \quad \forall a, b \in Z\backslash\{-1\}$. Find the identity element of $Z\backslash\{-1\}$ with respect to #.

Example 3.23: (**H. W.**) Let $*$ be a binary operation on N such that

$a * b = a + b - 1 \quad \forall a, b \in N$. Find the identity element of N with respect to *.

Example 3.24: Let $*$ be a binary operation on $P(X)$ such that

$A * B = A \cup B \quad \forall A, B \in P(X)$. Find the identity element of $P(X)$ with respect to *.

Solution: Let e be the identity element of $P(X)$ s.t. $A * e = e * A = A \quad \forall A \in P(X)$

$e = \emptyset$ because $A \cup \emptyset = \emptyset \cup A = A \quad \forall A \in P(X)$

Example 3.25: (**H. W.**) Let $*$ be a binary operation on $P(X)$ such that

$A * B = A \cap B \quad \forall A, B \in P(X)$. Find the identity element of $P(X)$ with respect to *.

Theorem 3.26: Let e is the identity element of a set A with respect to *, then e is unique.

Proof: Let e is the identity element of a set A with respect to *

Suppose e' is another identity of A w.r.t. *

Since e is the identity $\Longrightarrow e * e' = e' * e = e'$….(1)

Since e' is the identity $\Longrightarrow\Longrightarrow e' * e = e * e' = e$….(2)

From (1) and (2), $e = e'$

$\therefore e$ is unique

<u>Definition</u>: The Inverse Element العنصر النظير

Let $*$ be a binary operation on a set A and e is the identity element of A. Let $a \in A$, then $b \in A$ is called **the inverse element of a** if and only if $a * b = b * a = e$.

The inverse element b is denoted by a^{-1}. So

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

<u>Example</u> 3.27: Find the inverse element of each element in $Z, Q, \mathbb{R}$ w.r.t "+"

<u>Solution</u>: The identity element $e = 0$

$$a * a^{-1} = 0 \Longrightarrow a + a^{-1} \quad = 0 \Longrightarrow \mathrm{a}^{-1} = -\mathrm{a} \quad \forall \mathrm{a} \in \mathrm{Z}, \mathrm{Q}, \mathbb{R}$$

AND,

$$a^{-1} * a = 0 \Longrightarrow a^{-1} \quad + a = 0 \Longrightarrow \mathrm{a}^{-1} = -\mathrm{a} \quad \forall \mathrm{a} \in \mathrm{Z}, \mathrm{Q}, \mathbb{R}$$

$\therefore a^{-1} = -a \quad \forall \mathrm{a} \in \mathrm{Z}, \mathrm{Q}, \mathbb{R}$

<u>Example</u> 3.28: Find the inverse element of each element in $Q\backslash\{0\}, \mathbb{R}\backslash\{0\}$ w.r.t "."

<u>Solution</u>: The identity element $e = 1$

$$a * a^{-1} = e \Longrightarrow a.a^{-1} \quad = 1 \Longrightarrow \mathrm{a}^{-1} = \frac{1}{\mathrm{a}} \quad \forall \mathrm{a} \in Q\backslash\{0\}, \mathbb{R}\backslash\{0\}$$

AND,

$$a^{-1} * a = 1 \Longrightarrow a^{-1} \quad .a = 1 \Longrightarrow \mathrm{a}^{-1} = \frac{1}{\mathrm{a}} \quad \forall \mathrm{a} \in Q\backslash\{0\}, \mathbb{R}\backslash\{0\}$$

$\therefore a^{-1} = \frac{1}{a} \quad \forall \mathrm{a} \in Q\backslash\{0\}, \mathbb{R}\backslash\{0\}$

<u>Example</u> 3.29: Let # be a binary operation on $Z\backslash\{-1\}$ such that

$a\#b = a + b + ab \quad \forall a, b \in Z\backslash\{-1\}$. Find the inverse element of each element in $Z\backslash\{-1\}$ (if exist).

Solution: From **Example 3.22,** $e = 0$

Let $a \in Z\backslash\{-1\}$ and $a^{-1}$is the inverse of a

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

$a * a^{-1} = e \Longrightarrow a + a^{-1} + aa^{-1} = 0$

$$\Longrightarrow \mathrm{a} + \mathrm{a}^{-1}(1 + \mathrm{a}) = 0$$

$$\Longrightarrow \mathrm{a}^{-1} = -\frac{\mathrm{a}}{1+\mathrm{a}}$$

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

$$\Longrightarrow \mathrm{a} + \mathrm{a}^{-1}(1 + \mathrm{a}) = 0$$

$$\Longrightarrow \mathrm{a}^{-1} = -\frac{\mathrm{a}}{1+\mathrm{a}} \in Q$$

بصورة عامة نظير كل عدد في $Z\backslash\{-1\}$ هو عدد نسبي ماعدا $a = 0, -2$ فان نظيرهما عدد صحيح

If $a = 0 \Longrightarrow a^{-1} = 0 \in Z\backslash\{-1\} \Longrightarrow 0^{-1} = 0$

If $a = -2 \Longrightarrow \mathrm{a}^{-1} = \frac{2}{-1} = -2 \Longrightarrow \mathrm{a}^{-1} = -2 \in Z\backslash\{-1\}$

If a =3$\Longrightarrow \mathrm{a}^{-1} = -\frac{3}{4} \notin Z\backslash\{-1\}$

$\therefore a = 3$ has no inverse

$\therefore \forall a \neq 0, -2$, $a^{-1} \notin Z\backslash\{-1\}$

<u>**Example**</u> **3.30:** (**H. W.**) Let $*$ be a binary operation on $Q\backslash\{0\}$ such that

$a * b = 2ab \quad \forall a, b \in Q\backslash\{0\}$. Find the identity element of $Q\backslash\{0\}$ with respect to *.

Find the inverse of each element in $Q\backslash\{0\}$ (if exist).

Example 3.31: (**H. W.**) Let $*$ be a binary operation on Z such that

$a * b = a + b + 5 \quad \forall a, b \in Z$. Find the inverse of each element of Z with respect to *.

Group الزمرة

Let G be a nonempty set and * be a binary operation on G. The pair $(G,*)$ is called **group** if and only if * is associative, there is an identity element and each element have an inverse.

Mathematically,

(G, *) is called **group** iff

1. $G \neq \emptyset$
2. * is a binary operation on G
3. * is associative on G
4. $\exists$ identity element $e \in G$ s.t. $a * e = e * a = a$
5. $\forall a \in G, \exists a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$

Remark 3.32: If $(G,*)$ is a group and * is a commutative then $(G,*)$ is called **commutative group**.

Mathematically,

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

<u>Example</u> 3.33: Show that $(Z,+)$ is a commutative group

1. $Z \neq \emptyset$

2. + is associative binary operation on Z

3. $\exists e = 0 \in Z \; s.t. \, a + 0 = 0 + a = a \quad \forall a \in Z$

4. $\exists a^{-1} = -a \in Z \quad \forall a \in Z \; s.t. \, a + a^{-1} = a^{-1} + a = 0$

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

$\forall a, b \in Z \quad a + b = b + a$

$\therefore$ $(Z,+)$ is a commutative group

<u>Example</u> 3.34:

$(Q,+)$ is a comm. group

$(R,+)$ is a comm. group

$(N,+)$ is not a group

$(Z,.)$ is not a group

$(O,+)$ is not a group

$(\mathbb{R}\backslash\{0\},.)$ is a group

$(\mathbb{R},.)$ is not a group

Example 3.35: Show that $(Z,*)$ is a commutative group such that $a*b = a+b-5$

Solution:

1. **Closure:** let $a,b \in Z \Longrightarrow$ a $*$ b $= a+b-5 \in Z \Longrightarrow$ closure is true

well-defined: let $a,b,c,d \in Z$ s.t. $(a,b)=(c,d) \Longrightarrow a*b=c*d$?

Since $(a,b)=(c,d) \Longrightarrow a=c \wedge b=d$

$\Longrightarrow a*b=a+b-5$ (def. of *)

$= c+d-5 \quad (a=c \wedge b=d)$

$= c*d$

$\therefore *$ is well defined

$\therefore$ * is a binary operation

2. **associative (H.W.)**

3. **Identity:** let $a \in Z$ we find $e \in Z$ such that $a*e=e*a=a$

$a*e=a$

$\Longrightarrow a+e-5=a$

$\Longrightarrow e=5 \in Z$ …(1)

Similarly, $e*a=a$

$\Longrightarrow e+a-5=a$

$\Longrightarrow e=5 \in Z$ …(2)

From (1) &(2) , $e=5$

4. **Inverse:** $\forall a \in Z$, we find $a^{-1} \in Z$ such that $a*a^{-1}=a^{-1}*a=e$

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

$\Longrightarrow a+a^{-1}-5=5$

$\Longrightarrow a^{-1} = 10 - a \in Z$ …(1)

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

$\Longrightarrow a^{-1} + a - 5 = 5$

$\Longrightarrow a^{-1} = 10 - a \in Z$ …(2)

From (1) &(2) , $a^{-1} = 10 - a$

$\therefore$ $(Z,*)$ is a group

Commutative: (H.W.)

<u>Example</u> 3.36: Is $(P(X),\cup)$ group?

<u>Solution</u>:

1. $\cup$ is a binary operation (see Example 3.12)

2. $\cup$ is associative (see Example 3.14)

3. $\exists \emptyset \in P(X)$ s.t. $A \cup \emptyset = \emptyset \cup A = A$

$\therefore e = \emptyset$

4. **Inverse:** $\forall A \in P(X)$, we find $A^{-1} \in P(X)$ such that $A \cup A^{-1} = A^{-1} \cup A = \emptyset$

If $A = \emptyset$ then $A^{-1} = \emptyset$ s.t. $A \cup A^{-1} = \emptyset$

When $A \neq \emptyset$ then there is no inverse to A

المجموعة الوحيدة التي يوجد لها نظير هي ال $\emptyset$

$\therefore$ $(P(X),\cup)$ is not a group

<u>Example</u> 3.37: (H.W.) Is $(P(X),\cap)$ group?

Is $(P(X),\backslash)$ group?

Example 3.38: Let $F(A) = \{f, f: A \to A$ is bijective map.$\}$

let * be an operation on $F(A)$ s.t. $f * g = fog$

Is $(F(A),*)$ commutative group?

Solution:

1. **Closure:** let $f, g \in F(A) \Longrightarrow f * g = fog \in F(A)$?

$f \in F(A) \Longrightarrow f: A \to A$ is bijective

$g \in F(A) \Longrightarrow g: A \to A$ is bijective

$\therefore fog: A \to A$ is bijective

Closure is true

well-defined: let $f_1, f_2, g_1, g_2 \in F(A)$ s.t. $(f_1, f_2) = (g_1, g_2) \Longrightarrow f_1 * f_2 = g_1 * g_2$?

Since $(f_1, f_2) = (g_1, g_2) \Longrightarrow f_1 = g_1 \wedge f_2 = g_2$

$\Longrightarrow f_1 * f_2 = f_1 o f_2$ (def. of *)

$= g_1 o g_2 \quad (f_1 = g_1 \wedge f_2 = g_2)$

$= g_1 * g_2$

$\therefore *$ is well defined

$\therefore$ * is a binary operation

2. **associative:** $\forall f, g, h \in F(A)$

$(fog)oh = fo(goh)$ (by theorem 4.26(4), chapter4)

3. **Identity:** $\exists i_A: A \to A$ is bijective such that $foi_A = i_A of = f \ \forall f \in F(A)$(by thm 4.25, ch4)

$\therefore e = i_A$

4. **Inverse:** $\forall f \in F(A) \Longrightarrow f: A \to A$ is bijective

$\exists f^{-1}: A \to A$ is bijective $\Longrightarrow f^{-1} \in F(A)$

Such that $fof^{-1} = f^{-1}of = i_A$ (by thm 4.26(2), ch4)

$\therefore (F(A), o)$ is a group

Commutative:

Since $f: A \to A$ and $g: A \to A$

$fog = gof$

$\therefore (F(A), o)$ is a commutative group

Semi Group شبه الزمرة

Let A be a nonempty set and * be a binary operation on A. The pair $(A,*)$ is called **semi group** if and only if * is associative.

Mathematically,

(A, *) is called **semi group** iff

1. $A \neq \emptyset$

2. * is a binary operation on A

3. * is associative on A

Example 3.39:

$(\mathrm{N}, +)$ is a semi group but not a group

$(\mathrm{Z}, .)$ is a semi group but not a group

Remark 3.40: Every group is a semi group.

Ring الحلقة

Let R be a nonempty set and * and # be two binary operations on R. The ordered triple $(R,*,\#)$ is called **ring** if and only if

1. $R \neq \emptyset$

2. $(R,*)$ is a commutative group

3. $(R,\#)$ is a semi group

4. # is distributed over * (from left and right)

Example 3.41: $(Z,+,.)$ is a ring

1. $(Z,+)$ is a commutative group

2. $(Z,.)$ is a semi-group

3. $a.(b+c) = a.b + a.c \quad \forall a,b,c \in R$ (distribution from left)

$(b+c).a = b.a + c.a \quad \forall a,b,c \in R$ (distribution from right)

Example 3.42: $(Q,+,.)$ is a ring

$(\mathbb{R},+,.)$ is a ring

Commutative Ring الحلقة الابدالية

A ring $(R,*,\#)$ is called **commutative** iff $a\#b = b\#a \quad \forall a,b \in R$

الابدال يجب ان يتحقق على العملية الثانية

Example 3.43: $(Z,+,.)$ is a commutative ring because $a.b = b.a \quad \forall a, \in Z$

$(Q,+,.)$ is a commutative ring

$(\mathbb{R},+,.)$ is a commutative ring

Ring with Identity Element الحلقة ذات العنصر المحايد

A triple $(R,*,\#)$ has an identity element with respect to (#) if and only if

$$a\#e = e\#a = a \quad \forall a \in R$$

<u>Example</u> 3.44: $(Z,+,.),(Q,+,.),(\mathbb{R},+,.)$ are rings with $e = 1$ because $a.1 = 1.a$

Ordered Ring الحلقة المرتبة

A triple $(R,*,\#)$ is called **totally ordered ring** if and only if there is a totally ordered relation such that

1. $(R,*,\#)$ is a ring

2. The relation $\preccurlyeq$ is totally ordered relation T.O.R

3. $\forall a,b \in R$ if $a \preccurlyeq b$ then $a * c \preccurlyeq b * c, \quad \forall c \in \mathbb{R}$

4. $\forall a,b \in R$ if $a \preccurlyeq b$ then $a\#c \preccurlyeq b\#c, \quad \forall c \geq 0$

The totally ordered relation is denoted by $(R,*,\#, \preccurlyeq)$

<u>Example</u> 3.45: $(Z,+,.,\leq)$ is a totally ordered ring since

1. $(Z,+,.)$ is a ring (from Example 3.38)

2. $(Z,\leq)$ is T.O.R (see Example 3.85 from Mathematical logic and set theory)

3. $\forall a,b \in Z$ and $c \in Z$ if $a \leq b$ **T.P.** $a + c \leq b + c$

Let $a \leq b \Longrightarrow a = b - r,\ r \geq 0$

$$\Longrightarrow \mathrm{a + c = (b + c) - r},\ \ c \in Z \text{ and } r \geq 0$$

$$\Longrightarrow\ a + c \leq b + c$$

4. $\forall a,b \in Z$ and $c \geq 0,$ if $a \leq b$ then $a.c \leq b.c$

Let $a \leq b \Longrightarrow a = b - r,\ r \geq 0$

$$\Longrightarrow \mathrm{a.c} = \mathrm{b.c} - \mathrm{cr} \quad \forall c \geq 0$$

$$\Longrightarrow \mathrm{a.c} = \mathrm{b.c} - \mathrm{cr} \quad cr \geq 0$$

$$\Longrightarrow\ a.c \leq b.c$$

Example 3.46: (H.W.) Show that $(Z, +, ., \geq)$ is a totally ordered ring

Definition: Field الحقل

Let F be a nonempty set and * and # be two binary operations on F. The ordered triple $(F,*,\#)$ is called **field** if and only if

1. $F \neq \emptyset$

2. $(F,*)$ is a commutative group

3. $(F\backslash\{e\}, \#)$ is a commutative group

Where e is the identity w.r.t. *

4. # is distributed over * (from left and right)

Example 3.47: $(\mathbb{R}, +, .)$ is field since

1. $(\mathbb{R}, +)$ is comm. Group

2. $(\mathbb{R}\backslash\{0\}, .)$ is a commutative group

3. (.) dist. over (+)

Example 3.48: (**H.W.**) Show that $(Q, +, .)$ is field

Ordered field الحقل المرتب

A triple $(F,*,\#)$ is called **totally ordered field** if and only if there is a totally ordered relation such that

1. $(F,*,\#)$ is a field

2. The relation is totally ordered relation T.O.R

3. $\forall a, b \in F$ if $a \preccurlyeq b$ then $a * c \preccurlyeq b * c, \quad \forall c \in \mathbb{R}$

4. $\forall a, b \in F$ if $a \preccurlyeq b$ then $a \# c \preccurlyeq b \# c, \quad \forall c \geq 0$

The totally ordered relation is denoted by $(F, *, \#, \preccurlyeq)$

<u>Example</u> 3.49: $(\mathbb{R}, +, ., \leq)$ is a totally ordered field since

1. $(\mathbb{R}, +)$ is a comm. Group

2. $(\mathbb{R} \backslash \{0\}, .)$ is a comm. Group

3. (.) is distributive over (+)

4. $(\mathbb{R}, \leq)$ is T.O.R (see Example 3.86 from Mathematical logic and set theory)

5. $\forall a, b \in \mathbb{R}$ and $c \in \mathbb{R}$ if $a \leq b$ then $a + c \leq b + c$ (see example 3.42)

6. $\forall a, b \in \mathbb{R}$ and $c \geq 0$, if $a \leq b$ then $a. c \leq b. c$ (see example 3.42)

<u>Example</u> 3.50: show that $(\mathbb{R}, +, ., \geq)$ is a totally ordered field

show that $(Q, +, ., \geq)$ is a totally ordered field

show that $(Q, +, ., \leq)$ is a totally ordered field