Department of Mathematics , Jazan University ,Saudi Arabia

Lecture note for Math221 -Foundation of Mathematics,

Instructor :Seid Mohammed (Dr)

Semester I ,2016/17 academic year.

Introduction. The materials covered on Foundation of Mathematics are set to lay the basic concepts of mathematical logic that are essential to acquire the skill in the language and mode of reasoning needed at all levels of undergraduate study in mathematics.

Contents of the course :

Chapter One. Propositional logic.

The word “logic “ is generally understood as a systematic study of the form of argument. We shall confine our study to propositional logic, that is, the study of the logic of declarative sentences

Definition . A Proposition is a sentence (or declarative sentence) that is either true or false but not both.

Example . The following sentences are propositions :

1. Riyadh is the capital city of Saudi Arabia.

2 Egypt is in Europe.

3. $1+5=6$

4. $12-3=8$

Sentences 1 and 3 are true whereas 2 and 4 are false.

Example 2 . considerer the following sentences.

1.What time is it? 2. read carefully. 3. $2+3$. 4. $x+2=3$ 5. $x+y=3$

Sentences 1 , 2. and 3 are not propositions because they are not declarative sentences. Sentences 4 and 5 are not propositions because they are nether true nor false.

We say the truth value of a proposition is true, denoted by T, if the proposition is true and the truth value of a proposition is false , denoted by F, if the proposition is false. We use the letters p, q , r, s , …. to represent propositional variables ,that is ,variables that represent propositions just as we use the letters x ,y ,z to represent numerical variables.

The area of logic that deals with propositions is called Propositional logic or propositional calculus.

Logical operators : We consider how to obtain new proposition from a given one or more proposition s using logical operators . The main logical operators are :negation ,and , or , implication and bi-implication. A proposition formed from existing proposition or propositions using the logical operators is called a compound proposition. Now we discussed the rules of assigning the truth value for compound propositions formed using the logical operators. Logical operators are also called logical connectives.

Definition.(Negation) Let p be a proposition .The negation of p denoted by $\neg p$ is the statement :"It is not the case that p".

The proposition $\neg p$ is read "not p". The truth value of the negation of p , $\neg p$, is the opposite of the truth value of p. That is :

Rule I. If the truth value p is T then its negation $\neg p$ is F . If p is F ,its negation $\neg p$ is T .

We use a table called truth table to show all possible values that a compound proposition takes under all possible assignments for the truth value of its component proposition (s) .

Truth table for the Negation of a proposition

p	$\neg p$
T	F
F	T

Example . Write the negation of the following propositions and find their truth values.

1. 2 +4 = 8.

2. China is in Asia.

3. Riyadh is the capital city of Saudi Arabia.

4. 3 < 4.

Solution.

1. The negation reads : It is not the case that 2 + 4 = 8 . In other words the negation of $2+4=8$ is "2 + 4 $\neq$ 8".

Since the truth value of 2 +4 = 8 is F ,the truth value of its negation

(2 + 4 $\neq$ 8.) is T.

2 The negation reads :It is not the case China is in Asia. In other words , the negation is "China is not in Asia". Since the truth value of "China is in Asia " is T the truth value of its negation ,"China is not in Asia." is F.

3. The negation reads :Riyadh is not the capital city of Saudi ; and its truth value is F .

4.The negation reads : It is not the case 3 < 4 .In other words the negation is the proposition $3 \geq 4$;which is F.

Definition (Conjunction) Let p and q be propositions . The conjunction of p and q denoted by $p \wedge q$ is the proposition "p and q".

Rule II. The conjunction $p \wedge q$ is true when both p and q are true and is false otherwise.

The truth table for $p \wedge q$

p	q	$p \wedge q$
T	T	T
F	T	F
T	F	F
F	F	F

Example Write the conjunction of the proposition p and q and find their truth value.

1 P : 3 is greater than 2 ; q : Egypt is in Europe.

2. p : Riyadh is a city in Saudi ; q : Jizan university is in Jizan .

Solution

1. The conjunction of p and q , $p \wedge q$, is the proposition " 3 is greater than 2 and Egypt is in Europe". Since p is T and q is F , the truth value of the proposition $p \wedge q$ is F.

2..The conjunction $p \wedge q$ is the proposition "Riyadh is a city in Saudi and Jizan university is in Jizan".

Since p is T and q is T by the rule for conjunction ,the truth value of $p \wedge q$ is T.

Definition. Let p and q be propositions . The disjunction of p and q denoted by $p \vee q$ is the proposition "p or q".

Rule III. The disjunction $p \vee q$ is false when both p and q are false and is true otherwise.

The truth table for $p \vee q$ is :

p	q	$p \vee q$
T	T	T
F	T	T
T	F	T
F	F	F

Example Let p : 4 is greater than 6 and q : Egypt is in Africa.

Express the disjunction of p and q , $p \vee q$, as statement in English, and determine its truth value.

Solution. The disjunction of p and q , $p \vee q$ is the proposition "4 is greater than 6 or Egypt is in Africa". ; Since p is F and q is T by the rule for disjunction $p \vee q$ is T.

Definition. Let p and q be propositions . the conditional statement $p \to q$ is the proposition "If p then q"

Rule IV. The conditional statement $p \to q$ is false when p is true and q is false and is true otherwise.

The truth table for the conditional statement $p \to q$

p	q	$p \to q$
T	T	T
F	T	T
T	F	F
F	F	T

Remark : In the conditional statement $p \to q$, p is called the hypothesis and q is called the conclusion. Most theorems in mathematics are of the form $p \to q$.

A conditional statement is also called an implication.

The conditional statement $p \to q$ is also expressed as

"If p then q " " p implies q" ' p only if q "

"p is sufficient for q " " q is necessary condition for p "

Example.

1 . Let p : 3 is greater than 2 . q : 4 is greater than 5.

Write the conditional statement $p \to q$ and determine its truth value.

Solution .The conditional statement $p \to q$ is the proposition " If 3 is greater than 2 then 4 is greater than 5" . Since p is T and q is F by the rule for implication , $p \to q$ is F.

2. Let p : Washington is in Europe . q : Riyadh is the capital city of Saudi Arabia.

Write the conditional statements in words $a)\, p \to q\,, b) \neg p \to q\,, c)\, q \to p\,, d) \neg p \to \neg q$ and determine their truth values.

Solution. a) If Washington is in Europe then Riyadh is the capital city of Saudi Arabia.

b) If Washington is not in Europe i then Riyadh is the capital city of Saudi Arabia.

c) If Riyadh is the capital city of Saudi Arabia then Washington is in Europe.

d)If Washington is not in Europe then Riyadh is not the capital city of Saudi Arabia.

Since p is false and q is true we have (a) is true (b) is True (c) is false and (d) is false.

We consider the Converse , Contrapositive and inverse of a conditional statement $p \to q$.

a) The conditional statement $q \to p$ is called the converse of $p \to q$.

b) The conditional statement $\neg p \to \neg q$ is called the inverse of $p \to q$.

c) The conditional statement $\neg q \to \neg p$ is called the contrapositive of $p \to q$.

Example .

Write the converse , inverse and contrapositive of the conditional statement " If it is raining then it is cold".

Solution . In this conditional statement we have p : It is raining and q : It is cold. Thus

The converse is " If it is cold then it is raining".

The inverse is " If is not raining then it is not cold".

The contrapositive is " if it is not cold the it is not raining"

Example . Suppose p and q are propositions such that q is F and p is T. Find the truth value of the converse, inverse and contrapositive of $p \to q$.

Solution . Since q is F and p is T , $\neg q$ is T and $\neg p$ is F .Thus

The converse , $q \to p$ is T.

The inverse , $\neg p \to \neg q$ is T , and the contrapositive , $\neg q \to \neg p$ is F.

Definition . Let p and q be propositions. The bi- conditional statement of p and q denoted by $p \leftrightarrow q$ is the proposition "p if and only if q".

Rule 5. The bi-conditional statement $p \leftrightarrow q$ is true only when p and q have the same truth valueand is false otherwise.

The truth table for $p \leftrightarrow q$ is ;

p	q	$p \leftrightarrow q$
T	T	T
F	T	F
T	F	F
F	F	T

Bi-conditional statements are also called bi-implications.

Remark . $p \leftrightarrow q$ is usually expressed as :

“p is a sufficient and necessary condition for q”.

“p iff q”.

Example. Let p: It is snowing q : It is cold. Express in English the statement $p \leftrightarrow q$.

Solution . $p \leftrightarrow q$ is the statement “ it is snowing if and only if it is cold “

Example . Let p and q be propositions such that p is T and q is F. Find the truth value of the following compound proposition.

$a)\ (q \to p) \wedge \neg q \quad b)\ (p \vee q) \wedge q \quad c)\ (p \leftrightarrow \neg q) \to q$

Solution . a) since $q \to p$ is T and $\neg q$ is T , by the rule for conjunction $(q \to p) \wedge \neg q$ is T

b) Since $p \vee q$ is T and q is F , by the rule for conjunction $(p \vee q) \wedge q$ is F.

Exercise

1. Which of the following sentences are propositions? What are the truth value of those that are propositions?

a. Tunisia is in Europe.

b. Riyadh is the capital city of Saudi Arabia.

c. x + 2 = 11.

. d. Answer the question.

e. Good morning Ahmed.

f. Long live the King.

2.What is the negation of each of the following proposition?

a. Ahmed has an iphone.

b. 2 + 1 = 3

C. Naser is a student in Jazan university

d. 2 is greater than 5.

e.. There is no rain today in jazan

3.Let p and q be the propositions:

p : It is below freezing. q : It is snowing.

Write the following propositions using p and q; and logical connectives.

a. It is below freezing and it is snowing. c. It is snowing or it is freezing.

b. It is below freezing and not snowing. d. It is not freezing and it not snowing.

e. If it is freezing then it is snowing. f. It is snowing if and only if it is freezing.

4.Let p and q be propositions

p : I bought a book yesterday. q: $2 > 3$.

Express each of the following as English sentence.

$a. \neg p \quad b.\ p \vee q \quad c.\ p \to q \quad d. p \wedge q \quad e..\ \neg q \to \neg p$.

5. Determine the truth value of the following conditional statements,

a. If 1 + 1 = 2 then 2 + 2 = 5 b. If 1 + 1 = 3 then 2 + 2 = 4

6. State the converse , contrapositive and inverse of each of the following conditional statements.

a. If it snows to day then I will ski tomorrow.

b. If it rains then it is cold. C. If it snows tonight then I will stay at home.

7. Let p and q be propositions .The Exclusive or of p and q denoted by $p \oplus q$ is the proposition that is true when exactly one only one of them is true and is false otherwise . Construct a truth table for $p \oplus q$.

Truth table for compound propositions.

We show by examples how to use truth table to determine the truth value of a compound proposition .

Example . Construct the truth table for each of the following compound propositions.

$a)\ \neg(\neg p) \quad b)\ p \vee \neg q) \rightarrow (p \wedge q) \quad c)\ (q \rightarrow \neg p) \vee (\neg p \rightarrow \neg q) \quad d)\ p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$

Solution.a) The compound proposition has only one propositional variable p. Thus the truth table for $\neg(\neg p)$ consists of first column for p ,second column for $\neg p$ and a third column for $\neg(\neg p)$ given by below.

p	$\neg p$	$\neg(\neg p)$
T	F	T
F	T	F

b) The compound proposition involves two propositional variables p and q .and each has two possible values ,T or F. Thus the truth table must have four rows , the first two columns for p and q the third column for $\neg q$, the fourth column for $p \vee \neg q$,the fifth column for $p \wedge q$ and last column for the truth value $(p \vee \neg q) \rightarrow (p \wedge q)$.

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

(c) and (d) are left for exercise.

Propositional equivalence.

Definition. A compound proposition that is always true no matter the truth values of the propositional variables that occurs in it is called a tautology.

A compound proposition that is always false is called a contradiction.

We use truth table to show a given compound proposition is either a tautology or a contradiction .

Example. Show that the following compound proposition s are tautologies.

$a)\ p \vee \neg p \quad b)\ (p \wedge p) \leftrightarrow p \quad c)\ \neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$

Solution. We use truth table to show that the compound propositions are tautology

a)

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

From the third column of the table we see that $p \vee \neg p$ is always true . Thus $p \vee \neg p$ is a tautology.

b) is left for exercise.

c)

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q$
T	T	F	F	T	F	F	T
T	F	F	T	F	T	T	T
F	T	T	F	F	T	T	T
F	F	T	T	F	T	T	T

.

From the last column we see that $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q$ is always true hence it is a tautology.

Example. Show that each of the following compound propositions are contradictions.

$a)\ p \wedge \neg p \quad b)(p \wedge q) \wedge (\neg p \vee \neg q)$,

Solution

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

We see that $p \wedge \neg p$ is always F. hence it is a contradiction.

Definition. We say two compound propositions p and q are equivalent (Logically equivalent) if and only if $p \leftrightarrow q$ is a tautology. In this case we write $p \equiv q$.

Thus $p \equiv q$ if and only if p and q have the same truth value.

Example . Show the following compound propositions are equivalent.

$a)\, p \to q$ and $\neg p \vee q\ b)\neg(p \wedge q)$ b) $\neg p \vee \neg q\ c)\neg(p \to q)$ and $p \wedge \neg q$

$d)\, p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$.

Solution. We use truth table to show that both have the same truth value.

p	q	$\neg p$		$\neg p \vee q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

From columns three and four of the table we see that both $p \to q$ and $\neg p \vee q$ have the same truth values . Hence they are equivalent ,that is, $p \to q \equiv \neg p \vee q$.

b)

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

We see from columns six and seven both have the same truth values. Hence they are equivalent.

(c) and (d) are left for exercise.

List of some logical equivalence

a) $p \vee q \equiv q \vee p \quad p \wedge q \equiv q \wedge p$ (Commutative Law)

$p \vee q) \vee r \equiv p \vee (q \vee r)$
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r$ (Associative Law)

$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (Distributive Law)

$\neg(p \vee q) \equiv \neg p \wedge \neg q$
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ (De Morgan 's Laws)

Exercise. Use truth table to show the equivalence of commutative law distributive law and De Morgan's law

Quantifiers**.**

Consider the following sentences involving variables such as :

i) x is greater than three (x > 3) ii) $x + y = 3$, iii) y is the capital city of Saudi.iv) y is a city in the country z.

Each of the above sentences have the property that once you specify a particular value to the variable(s)it becomes a proposition.

For example in (i) if you replace x by 4 the sentence read s : 4 is greater than 3 which is a proposition with truth value T. If you replace x by 2 the sentence reads : 2 is greater than 3 , which is again a proposition with truth value F.

In (ii) if put x =2 and y=1 , we get 2+1 =3 which is a proposition

Now consider the sentence " x is greater than 3" . This sentence has two parts : The first part Is the variable x , which the subject of the sentence . and the second part ,the predicate "is greater than 3" , which refers to the property the subject can have.

If we let the predicate (or the property) "is greater than 3 " by P and x the variable then we denote the sentence "x is greater by than 3 " by P(x) . We read p(x) a s "x has the property p".

We write p(x) : x is greater than 3.

p(4) : 4 is greater than 3 , which is a proposition.

Let P be a certain property. p(x) is called a propositional function of x .Once a value is assigned to the variable x the sentence p(x) becomes a proposition and has a truth value.If p(x) is a propositional function the value that the variable x assumes is called the domain
Example . 1. Let P(x) : $x < 3$.

What are the truth value of p(4) , P(0) ; p(-1)?

Solution: P(4): $4 < 2$ which is false.

P(0) : $0 < 2$ which is true

P(-1) : $-1 < 2$, which is true.

2.Let P(x , y) : $x > y$.

Find the truth value s of P(1.2) ; P(3 , 2), Solution : P(1,2) :   1 > 2   which is false.

P(3,2)   : 3   >   2   which is true.

3. Q(x,y) : x is the capital city of country y.

Find the truth value of   Q(Riyadh , Egypt)   . Q(Cairo   , Egypt)   .

Solution : Q(Riyadh , Egypt): Riyadh is the capital city of Egypt . which is false.

Q(Cairo , Egypt) : Cairo is the capital city of Egypt . True.

Universal and existential quantifiers

- Universal **quantifier**.

Definition . The universal quantification of p(x) is the statement
"For every x p(x)"   (x in the domain of p(x)).
We denote this statement by   "$\forall x\, p(x)$". We call the symbol $\forall$ the universal quantifier.
Thus $\forall x\, p(x)$ is read as " for every x p(x)" or " for all x   p(x)" .

$\forall x\, p(x)$ **is true if for every x in the domain p(x) is always true.**

$\forall x\, p(x)$ **is false if there an x for which p(x) is false.**

An x for which p(x) is false is called a **counter example** for $\forall x\, p(x)$**.**

Example   Find the truth value $\forall x\, p(x)$ where $p(x)$ is :

$a. x+1 > x \quad b. x^2 > 0 \quad c. x^2 \geq 0 \quad d. 2x+1=3$. (domain consists of all real numbers

Solution . a) Since $x+1 > x$ is true for every real number x   , $\forall x\, p(x)$ is true.

b)Since $0 = 0^2 > 0$ is false   (p(0) is false) $\forall x\, p(x)$ is false. Note   x = 0 is a counter example.

c) Since $x^2 \geq 0$ is true for all real numbers   , $\forall x\, p(x)$ ($\forall x (x^2 \geq 0)$) is true.

d) $2x+1=3 \leftrightarrow 2x=2 \leftrightarrow x=1$.Thus $2x+1 \neq 3$ for all $x \neq 1$. Hence $\forall x\, p(x)$ is false.

For example take $x=0$ we get $2\times 0+1=3$, that is , 1 = 3 , which is false..Hence $\forall x\,(2x+1=3)$ is false. Here 0 is a counter example.

- **Existential quantifier**.

Definition. The existential quantification of $p(x)$ is the statement "There exists x in the domain such that $p(x)$".

We denote the statement by $\exists x\, p(x)$. '$\exists$' is called existential quantifier.

Thus $\exists x\, p(x)$ is read as " There exists x such that $p(x)$) " or "there is at least one x such that $p(x)$".

$\exists x\, p(x)$ **is true if there exist at least one x in the domain such that** $p(x)$ **is true.**

$\exists x\, p(x)$ **is false if** $p(x)$ **is false for every x in the domain.**

Example .Find the truth value of $p(x)$ where $p(x)$ is :

$a. x>3$ $b. x^2<0$ $c. 2x+1=3$; x is a real number.

Solution . a. Since 4 is a real number and 4 > 3 is true , $p(4)$ is true .Hence $\exists x\, p(x)$ is true.

b. Since $x^2<0$ is for all x , $\exists x(x^2<0)$ is false , that is $\exists x\, p(x)$ is false.

c. Solving for x we get $2x+1=3 \leftrightarrow 2x=2 \leftrightarrow x=1$. Thus $2x+1=3$ is true if x = 1. ,that is , $p(1)$ is true . $\therefore \exists x\,(2x+1=3)$ is true , that is ($\exists x\, p(x)$ is true..

Introduction to Proof.

In mathematics a theorem is statement that can be shown to be true.

A proof of a theorem is an argument that establishes the truth of the theorem.

Most theorems in mathematics are of the form $p \to q$, that is ,, "If p then q."

There are three basic methods of proof :

- Direct proof.
- Indirect proof :
  Proof by contrapositive
  Proof bycontradiction

Direct proof : A direct proof is used to show $p \to q$ true whenever p is true. Thus in a direct proof we **assume** p **is true** and use axioms ,definitions and previously proven theorems to show that q must be true.
Note that in $p \to q$, p is the hypothesis and q is the conclusion.
Thus in a direct proof we assume the hypothesis is true and show that the conclusion is true.
Before we give examples we give the following definitions.
Definition . i) An integer n is called even if $n = 2m$ for some integer m.
ii) An integer n is called odd if $n = 2m + 1$ for some integer m.

An integer is either odd or even but not both.
Example. Give a direct proof to the theorem " if n is an odd integer then n^2.is odd."

Solution. We assume the statement n is an odd integer is true .we want to show the statement n^2 is odd is true.
Since n is odd by definition $n = 2m + 1$ for some integer m. Thus

$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1 = 2k + 1$ where $k = 2m^2 + 2m$ is an integer. Hence by definition of odd integer n^2 is an odd integer.

$\therefore$ The theorem is true.

Definition . An integer n is said to be a perfect square if $n = a^2$ for some integer a .

Example1 .The integers $1, 4, 9, 16, \cdots$ are perfect squares since ,

$1 = 1^2$, $4 = 2^2$ $9 = 3^2$ $16 = 4^2$

Example2 . Give a direct proof : If m and n are perfect squares then their product mn is also a perfect square.

Solution . We assume m and n are perfect squares. To show mn is a perfect square.

By definition perfect square $m = a^2$ and $n = b^2$. We have

$mn = a^2.b^2 = (ab)^2 = c^2$ where $c = ab$ is an integer.

$\therefore mn$ is a perfect square.

Indirect proof.

Consider a theorem of the form $p \to q$.sometimes the direct proof may not helpful to prove the theorem. Proofs of theorem that does not start with hypothesis and end with the conclusion is called indirect proof.

A useful type of indirect proof is proof by contraposition. The proof by contraposition make use of the fact that $(p \to q) \equiv (\neg q \to \neg p)$. To show a theorem of the form $p \to q$ is true by proof by contraposition involves showing $\neg q \to \neg p$ is true . Thus in the proof by contraposition we assume $\neg q$ is true and show that $\neg p$.That is , we use direct proof to show $\neg q \to \neg p$.

Example 3 Use proof by contraposition to prove the theorem "If n is an integer and $3n + 2$ is odd then n is odd"

.

Proof. We have to prove the statement : If n is even then $3n + 2$ is even using direct proof.

Assume n is even. To show $3n + 2$ is even.

Since n is even , $n = 2m$. Thus

$3n+2=3(2m)+2=6m+2=2(3m+1)=2k$, for some integer k. By definition of even integer $3n+2$ is even.

$\therefore$ The theorem is proved.

Example . Prove that if n is an integer and n^2 is odd then n is odd.

Proof. We use proof by contraposition. Assume n is even and show n^2 is even. Since n is even , by definition of even $n=2m$ for some integer m. Thus $n^2=(2m)^2=4m^2=2(2m^2)=2k$ where $k=2m^2$, which is an integer.

$\therefore n^2$ is even.

Proof by contradiction.

Suppose we want to prove that a given statement p is true. The proof by contradiction involves assuming that p is false , that is , we assume $\neg p$ is true ,we arrive at a statement which contradicts known facts or proven theorem ,or arrive at a false statement. This we conclude $\neg p$ is false and hence p is true.

Definition A real number x is called rational number if $x=\frac{m}{n}$, for some integers m,n and $n\neq 0$.

A real number which is not a rational number is called an irrational number

A real number is either rational or irrational but not both.

Example .Prove that $\sqrt{2}$ is an ir rational number.

Proof. Suppose $\sqrt{2}$ is not an irrational number ,that is, $\sqrt{2}$ is a rational number. By definition of rational number $\sqrt{2}$ **=** $\frac{m}{n}$ **where m and are integers and n $\neq$0 having no common factor other than 1 . We have**

$$\sqrt{2}=\frac{m}{n}\rightarrow 2=\left(\frac{m}{n}\right)^2=\frac{m^2}{n^2}\rightarrow 2n^2=m^2 \quad \text{.........} \quad (1)$$

Thus m^2 is even and therefore m is even. Let $m=2k$ for some integer k.

Using (1) we have

$2n^2 = m \to 2n^2 = (2k)^2 = 4k^2 \to n^2 = 2k$. Thus n^2 Is even. $\therefore$ n is even. Hence both m and n are even. That is 2 is a common factor of m and n . This is contradiction since the only common factor of m and n is 1 . We conclude $\sqrt{2}$ is not a rational number ,that is , $\sqrt{2}$ is an irrational number,

Remark.1.Sometimes we use the method of proof by contradiction to show $p \to q$ is true . Since $(p \to q) \equiv (\neg p \vee q)$ to proof $p \to q$ is true we show the statement $\neg p \vee q$ is true .Thus we can use proof by contradiction to show $\neg p \vee q$ is true. So we assume $\neg(\neg p \vee q)$ is true ,that is , $p \wedge \neg q)$ is true .Therefore to prove $p \to q$ is true by contradiction we must assume p is true and $\neg q$ is true and arrive at contradiction.

Example . Give proof by contradiction of the theorem "If $3n+2$ is odd then n is odd".

Solution. Let P : $3n+2$ is odd and q : n is odd. We assume $3n+2$ is odd true (p is true) and n is even is true ($\neg q$) is true.

Since n is even , $n = 2k$ for some integer k . Thus

$3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1) = 2m$ where $m = 3k+1$ which is an integer.

Hence $3n+2$ is even , this is a contradiction to the fact that $3n+2$ is odd.

$\therefore$ The theorem is proved .

2. To prove a theorem of the form $p \Leftrightarrow q$ (p if and only if q).

Since $p \Leftrightarrow q \equiv (p \to q) \wedge (q \to p)$, to prove $p \Leftrightarrow q$ is true we need to prove i) $p \to q$ is true and ii) $q \to p$ is true .

Example. Prove the following theorem: An integer n is even if and only if n^2 is even.

Proof. i) we prove : $(\Rightarrow)$ If n is even then n^2 is even. We use direct proof ,that is,we assume n is even and show n^2 is even.

Since n is even , $n = 2m$ for some integer m (by definition of even)

Thus $n^2 = (2m)^2 = 4m^2 = 2(2m^2) = 2k$, where $k = 2m^2$, an integer.

Therefore by definition of even , n^2 is even.

ii) To prove : $(\Leftarrow)$ If n^2 is even then n is even. We use proof by contrapositions that is, we assume n is odd is true and show n^2 is odd.

Since n is odd $n = 2m+1$ for some integer m (by definition of odd). Thus

$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1 = 2k + 1$, where $k = 2m^2 + 2m$, an integer,

Therefore n^2 is odd integer.

It follows from (i) and (ii) the theorem is proved .

Exercise

1. Let $p(x) : x = x^2$ with domain the integers. Find the truth value of the following propositions.

$a.\ p(0) \quad b.\ p(1) \quad c.\ p(2) \quad d.\ p(-1) \quad e.\ \exists x\, p(x) \quad f.\ \forall x\, p(x)$.

2. Determine the truth value of the following propositions if the domain for the variables consists of all real numbers.

$a. \exists x\,(x^3 = -1) \quad b, \exists x\,(x^4 < x^2) \quad c. \forall x((-x)^2 = x^2) \quad d. \forall x\,(2x > x)$

3.Let $Q(x); x + 1 > 2x$, x an integer. Find the truth value

$a. Q(0) \quad b. Q(-1) \quad c. Q(1) \quad d. \forall x Q(x) \quad e. \exists x Q(x) \quad f. \forall x \neg Q(x)$.

4.Use direct proof to show that

a. if m and n are odd integers their sum $m+n$ is even.

b. If n is odd integer then n^2+1 is even.

c. if m and n are odd integers their product mn is odd.

5. Show that if m and n are integers and n^3+5 is odd then n is even using

a) a proof by contraposition b. a proof by contradiction.

6, Use proof by contraposition to show the following statements;

a. If $5n+2$ is odd then n is odd.

b. If $(n+1)^2$ is odd then n is even.

7.Prove the theorem : An integer n is odd if and only if n^2 is odd.

Chapter 2.Basic structure of sets.

We regard a set as a collections of objects. The objects of a set are called elements.

We denote sets by capital letters and elements by small letters .We write $x \in A$ if x is an element of A. Thus "$x \in A$" is read " x is an element of A " or "x belongs to A" or " x is a member of A". If x is not an element of A, we write $x \notin A$.

There are several ways to describe a set .

1.Listing method Roster method. If the elements of a set can be listed , for example the elements of a set A are only a , b , c and d then we write

A = {a , b , c, d} .That is ,we list the elements of the set and enclosed by braces. This way of describing a set is called roster method.

Example. The set A of all natural numbers less than 7 can be written as A = { 1 , 2 , 3 ,4 , 5, 6}.

The set B of all positive odd integers less than 10 can be written as

B = {1 , 3 ,5 ,7 , 9}

The roster method is also used to describe a set without listing all of its elements if the elements have some pattern. In this case we list some members of the set followed by three dots "$\cdots$" and then enclose by braces.

Example. The set of all positive integers less 100 can be written as

A = { 1 , 2 ,3 , $\cdots$, 99}.

If the elements of a set cannot be listed but have certain pattern then we write a few elements followed by three dots and enclosed by braces.

Example The set $\mathbb{N}$ of all natural numbers can be written as

$\mathbb{N}$ = { 1 ,2 , 3 , $\cdots$ }.

The set Z^{-} of all negative integers can be written as Z^{-} = { $\cdots$, -3 ,-2 ,-1}

The set of integers $\mathbb{Z}$ = { $\cdots$, -2 , -1 , 0 ,1 , 2 , $\cdots$}

The set of all odd positive integers $O = \{1, 3, 5, \cdots\}$

Set Builder method : If the elements of set A satisfy certain property p , that is , if the elements of set A are those which have the property p, then we write

A = { x : p(x) } we read as the set of all x such that p(x).

The elements of A are those for which p(x) is true.

This way of describing a set is called set builder method.

Example. The set of O all odd integers can be written

O ={ x : x is an odd integer }. Here the property p is "being an odd integer".

$4 \notin O$ since 4 is not an odd integer , that is, p(4) is false.

Example .List the elements of the following set.

a. A = {x : x is a positive integer less 10}

b. B = { x: x is a perfect square integer less 17 }

c. C = { x : x is an integer and 2x +3 = 5.}

Solution

a) {1 ,2,3 , . . . , 10}   b) {1 ,4 ,9 ,16} c) { 1 }

Equality of sets and subsets.

Definition .Two sets A and B are equal written A = B if and only they the same elements.

Example If A = {2 , 4 . 1 } and B = { 1 , 2, 4 } then A are B. are since they the same elements .

Thus A = B.

Note the order in which the elements are listed does not matter.

Example The sets {1 ,2 3, } and { 1,1,2,2,3,3,3,} are equal since they have the same elements.

A set does not changed If its elements are listed more than once .

Remark. we shall use the following sets

$\mathbb{N} = \{1, 2, 3, \cdots\}$ The set of natural numbers

$\mathbb{Z} = \{\cdots, -3\ , -2, -1, 0, 1, 2, 3, \cdots,\}$, the set of integers

$\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z}, n \neq 0\}$, the set of rational numbers

$\mathbb{R}$ = the set of real numbers.

Two special set : The Empty set and the Universal set.

A set which does not any element is called the Empty set or null set and is denoted by $\varnothing$ or { }.

Example .The set A = {x : x is an integer and x $\neq$ x} has no element .Thus A = $\varnothing$.

The universal set denoted by $\cup$ is the set which contains all elements under consideration for a certain discussion. If $\cup$ is the universal set and A is any set then every element in A must be in $\cup$.

Note. Sets may contain other sets.

Example. Let $A = \{a, \{b\}, c, \{c\}\}$ .Find the truth value of the following statemnets.

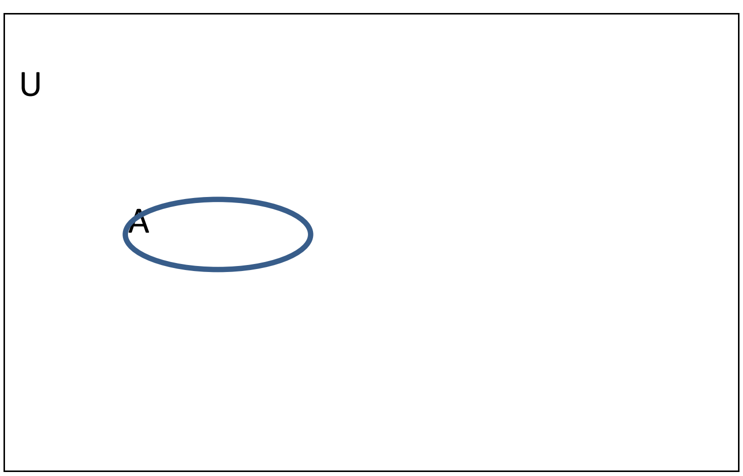
$i) a \in A \quad ii) b \in A \quad iii) \{b\} \in A \quad iv) \{c\} \in A \quad v) c \in A \quad vi) \{a\} \in A$.

Solution. i) T ii) F iii) T iv) T v) T vi) F

Venn diagram :

Sets can be represented graphically using diagrams called Venn diagrams.In Venn diagrams the universal set is represented by rectangles ,inside the rectangle circles or other figures are used to represent sets.

Example. Let U =the set of integers . Draw a Venn diagram that represents the set A = he set of all positive integers less than 5.



Subset

Definition .The set A is a subset of the set B written $A \subseteq B$ if and only if every element of A is also an element of B.

Thus $A \subseteq B \leftrightarrow \forall x\,(x \in A \rightarrow x \in B)$ is true.

Note . To show that A is a subset of B show that if x belongs to A then x also belongs to B

To show that A is not a subset of B find a single $x \in A$ such that $x \notin B$. Such element x is call counter example.

Example 1. If $A = \{a, b, c, 2, 3\}$ and $B = \{1, a, 4, b, 5,\ c, 2, 3\}$ then $A \subseteq B$ since each element of A is also an element of B. But B is not a subset of A since $1 \in B$ and $1 \notin A$ (1 is a counter example)

2. If A is the set of positive integers less than 100 then $A \subseteq \mathbb{Z}$.

Theorem. For every set S $i)\ \varnothing \subseteq S$ $ii)\ S \subseteq S$.

Proof. i) Suppose $\varnothing$ is not a subset S .Then there is a single element $x \in \varnothing$ such that $x \notin S$. But this is a contradiction since $\varnothing$ has no member. $\therefore \varnothing \subseteq S$.

ii) If x belongs to S then x belongs S is true . Thus $S \subseteq S$.

Example. Let $S = \{a, b\}$. List all subsets of the set $S = \{a, b\}$.

Solution. $\varnothing \subseteq S, S \subseteq S, \{a\} \subseteq S, \{b\} \subseteq S$ are the subsets of S.

Proper subset : If an $A \subseteq B$ and $A \neq B$ we say A is a proper subset of B and we write $A \subset B$.

Thus $A \subseteq B$ if and only if $\forall x(x \in A \rightarrow x \in B) \quad \wedge \exists x\,(x \in B \wedge x \notin A)$.

Note. For any set $S, S \subset S$ is false.

Example . Let $A = \{a, b, c\}$ and $B = \{a, b, c, d, e\}$. Then $A \subset B$ since $A \subseteq B$ and $A \neq B$.

Example. Let $S = \{a, b\}$. List all proper subsets of the set $S = \{a, b\}$.

Solution. $\varnothing \subset S, , \{a\} \subset S, \{b\} \subset S$ are the only proper subsets of S.

.

Note. To show two sets A and B are equal we must show $A \subseteq B$ and $B \subseteq A$.

Example Let $A = \{x : x$ is even integer } and

$B = \{x : x$ is the sum of two odd integers}

Show that $A = B$.

Solution. We must show i) $A \subseteq B$ and ii) $B \subseteq A$.

i). To show $A \subseteq B$.

$$\begin{aligned} x \in A &\to x = 2m, \quad m \in \mathbb{Z} \\ &\to x = (2m-1) + 1 \\ &\to x \in B \end{aligned}$$

$$\therefore \quad A \subseteq B$$

ii) To show $B \subseteq A$.

$$\begin{aligned} x \in B &\to x = (2m+1) + (2n+1), \quad n\,, m \in \mathbb{Z} \\ &\to x = 2(m+n+1) \\ &\to x = 2k \quad , k = m+n+1 \in \mathbb{Z} \\ &\to x \in A \end{aligned}$$

$$\therefore \quad B \subseteq A$$

Thus $A = B$.

Example. Let

$A = \{1 , \{1\} , \{\varnothing\} , \{\{1\}\} , \{2 , \{1\}\} , \{\{1\}\}\}$.Determine the truth value of the following statements.

$i) \{1\} \in A$, $ii)\ 2 \in A$, $iii)\ \varnothing \in A$ $\ iv)\ \{\{1\}\} \subseteq A$ $\ v)\ \{2, \{1\}\} \in A$ $\ vi)\ \{\varnothing\} \subseteq A$.

Solution. i) T ii) F iii) F iv) T v) T vi) F.

Power set.

Definition . Given a set S , the power set of S denoted by $\wp(S)$ is the set of all subsets of the set S .

Note that always the $\varnothing$ and S belong to $\wp(S)$.

Example . $S = \{a , \varnothing , \{1\}\}$. Find $\wp(S)$.

Solution. We want all subsets of S .

$\wp(S) = \{\varnothing , S, \{a\}, \{\varnothing\} , \{\{1\}\} , \{a , \varnothing\} , \{a , \{1\}\} , \{\varnothing , \{1\}\}\}$

Size of a set.

Definition. Let S be a set. If there are exactly n distinct elements in S where n is a nonnegative integer, we say S is finite and we call n the cardinality of S .The cardinality of S is denoted by $|S|$.

Example Let $S = \{1 , a , b , c , a\}$. The distinct elements of S are 1 ,a ,b ,c. Thus S is finite and $|S|$ = 4 .

$|\varnothing| = 0$, since the $\varnothing$ has no element.

Definition. A set is said to be infinite if it is not finite.

Example .The set of positive integers is infinite

Note .If a set S has n elements then $|\wp(s)| = 2^n$.

Set Operations.

Definition. Let A and B be sets. The union of the sets A and B denoted by $A \cup B$ is the set that contains those elements that are in A or in B or in both.

Thus $A \cup B. = \{x : x \in A \vee x \in B\}$.

Example. Let $A = \{1, 3, 5\}$ and $B = \{1, 2, 3, 5, 4\}$.The union of A and B is the set

$A \cup B = \{1, 2, 3, 4, 5\}$.

Example Let $A = \{x : x < 5 \vee x > 9\}$ $U = \{1, 2\ 3, \cdots, 11\}$. List the elements of A.

Solution. For $x \in U$, $x < 5 \vee x > 9$ is true if and only if x < 5 is true or x > 9 is true . Thus

$A = \{x : x < 5\} \cup \{x : x > 9\} = \{1, 2, 3, 4\} \cup \{10, 11\} = \{1, 2, 3, 4, 10, 11\}$.

Remark :The union operation "$\cup$" on sets is the counter part of the logical connective "$\vee$".

Definition. Let A and B be sets. The intersection of the sets A and B denoted by $A \cap B$, is the set containing those elements in both A and B. Thus

$A \cap B = \{x : x \in A \wedge x \in B\}$.

Remark: The intersection operation "$\cap$" on sets is the counter part of the logical connective "$\wedge$".

Example . Let $A = \{1, 3, 5\}$ $B = \{1, 2, 3\}$. Then the intersection of A and B ,

$A \cap B = \{1, 3, 5\} \cap \{1, 2, 3\} = \{1, 3\}$.

Definition. Two sets are disjoint if their intersection is the empty set.

Example . Let $A=\{1,3,5,7,9\}$, $B=\{2,4,6,8\}$ .Because $A\cap B=\varnothing$, A and B are disjoint sets.

Note If A and B are finite sets then $|A\cup B|=|A|+|B|-|A\cap B|$.

Definition . Let A and B be sets. The difference of A and B denoted by $A-B$, is the set containing those elements that are in A but not in B.

$$A-B=\{x : x\in A\wedge x\notin B\}$$

We also denote $A-B$ by $A\setminus B$.

The difference of A and B is also called the complement of B with respect to A.

Example. The difference of the sets $\{1,3,5\}$ and $\{1,2,3\}$ is $\{5\}$, that is

$\{1,3,5\}-\{1,2,3\}=\{5\}$ .The difference of the sets $\{1,2,3\}$ and $\{1,3,5\}$, that is. $\{1,2,3\}-\{1,3.5\}=\{2\}$. This shows that in general $A-B\neq B-A$.

Definition. Let U be the universal set .The complement of the set A denoted by $\bar{A}$ is the complement of A with respect to U. Therefore $\bar{A}=U-A$.

$x\in\bar{A}$ if and only if $x\notin A$.

$\bar{A}=U-A=\{x\in U : x\notin A\}$.

Example .Let $U=\{1,2,\cdots,90\}$. Find the complement of the set A if

i) $A=\{1,2,3,\cdots 11\}$. ii) $A=\{2,4,6,\cdots 90\}$

Solution .i) $\bar{A}=U-\{1,2,3,6,\cdots 11\}=\{12,13,14,\cdots,90\}$.

ii) $\bar{A}=U-\{2,4,6,\cdots,90\}=\{1,3.5,\cdots;99\}$.

Example Prove that $A-B=A\cap\bar{B}$.

Solution.

We must show i) $A-B\subseteq A\cap\bar{B}$ $ii)$ $A\cap\bar{B}\subseteq A-B$.

$i)\ x \in A - B \to x \in A \wedge x \notin B$ (by definition of difference of sets)

$\to x \in A \wedge x \in \bar{B}$ (definition of complement)

$\to x \in A \cap \bar{B}$ (Definition of intersection)

$\therefore \quad A - B \subseteq A \cap \bar{B}$.

. $ii)\ x \in A \cap \bar{B} \to x \in A \wedge x \in \bar{B} \to x \in A \wedge x \notin B \to x \in (A - B)$. Thus $A \cap \bar{B} \subseteq A - B$.

Therefore $A - B = A \cap \bar{B}$.

Exercise

1. List the members of the following sets.

a. { x :x is a real number such that $x^2 = 1$}

b. {x/ x is a positive integer less than 12 }.

c. {x / x is the square of an integer and x < 100 }

d. { x : x is an integer such that $x^2 = 2$}

2.Let A = { 0 , 2 ,4 ,6 ,8} B = {0 , 3 ,2 , 1 ,4 ,5 ,6}

C = { 4 ,5 ,6 ,7 ,8 ,9 ,10}

Find

$a\,.\ A \cup B \quad b.\ B \cap C \quad c.\ A - B \quad d.\ A \cap (B \cup C) \quad e.\ (A \cap B) \cup (A \cap C) \quad f.\ (A - B) \cap (C - B)$.

3. Let $\cup = \{1, 2, 3, \cdots, 10\}$ be the universal set. List the elements of the following sets.

$a.\ \{x : x < 6 \wedge x > 3\} \quad b.\ \{x : x^2 < 7 \vee x > 3\} \quad c.\ \{x \,/\, x^2 - 7x + 12 = 0 and\ x < 5\}$

4. Which of the following sets contain 2 as an element of these sets.

a) $\{x \in \mathbb{R}$: is an integer greater than 1 }

b. {$x \in \mathbb{R}$: is the square of an integer}

c. {2 ,{2}} d.{{2} , {{2}}} e. {{2} ,{2 , {2} } f {{2}}

5.Determine which of the of following statement is true or false.

a. $0 \in \varnothing$ **b.** $\varnothing \in$ **{ 0 }** **c. {** $\varnothing$ } $\subseteq$ { $\varnothing$} d. {0 } $\subset$ { 0 }

e. $\varnothing \in$ { $\varnothing$ } f. {$\varnothing$ } $\in$ { $\varnothing$ } g. $\varnothing \in$ { $\varnothing$, { $\varnothing$ } } h. $\varnothing \subset$ { $\varnothing$, { $\varnothing$ } }.

6 Find the power set of the following sets .

a. $\varnothing$ b. { 1 } c. (1 ,a } d . { $\varnothing$, {1} } .

Properties of union and intersection

Theorem The set operations union and intersection have the following properties:

1. $A \cup B = B \cup A \quad ii. A \cap B = B \cap A$ (Commutative property)

2. $A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$ (Associative Property)

3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distributive property)

4. $\overline{A \cup B} = \bar{A} \cap \bar{B}, \quad \overline{A \cap B} = \bar{A} \cup \bar{B}$ De Morgan's law for sets.

Proof. The proofs depend on the properties of logical equivalence and the definitions of union and intersection.

1. $A \cup B = \{x : x \in A \vee x \in B\} = \{x : x \in B \vee x \in A\} = B \cup A$ (since $p \vee q \equiv q \vee p$ and the definition of union offsets.)

2

$$x \in A \cup (B \cup C) \leftrightarrow x \in A \vee x \in (B \cup C) \leftrightarrow x \in A \vee (x \in B \vee x \in C) \leftrightarrow (x \in A \vee x \in B) \vee x \in C \leftrightarrow x \in (A \cup B)$$

(since $p \vee (q \vee r) \equiv (p \vee q) \vee r$ and the definition of union)

Therefore $A \cup (B \cup C) = A \cup B) \cup C$.

3. We show i. $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and ii. $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

i. $x \in A \cup (B \cap C) \to x \in A \vee x \in (B \cap C)$ (Definition of "U"

$\to x \in A \vee (x \in B \wedge x \in C)$ (Definition of " $\cap$"

$\to (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ ($p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

$\to x \in (A \cup B) \wedge x \in (A \cup C)$ (Definition of "U")

$\to x \in (A \cup B) \cap (A \cup C)$ (Definition of intersection)

Therefore $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ (Definition of subset)

ii. left for exercise.

4. $x \in \overline{A \cup B} \leftrightarrow x \notin A \cup B$ (definition of complement)

$\leftrightarrow x \notin A \wedge x \notin B$ (definition of "U"

$\leftrightarrow x \in \bar{A} \wedge x \in \bar{B}$ (definition of complement)

$\leftrightarrow x \in \bar{A} \cap \bar{B}$ (Definition of intersection)

$\therefore$ $\overline{A \cup B} = \bar{A} \cap \bar{B}$ (by equality of sets since $(p \leftrightarrow q \equiv= (p \to q) \wedge (q \to p)$

Exercise.

1. Let $A = \{x : x = 3m\ , m \in \mathbb{Z}\}$ and $B = \{x : x = 6m\ , m \in \mathbb{Z}\}$. Show that $B \subset A$.

2. Show that for sets A and B . U is the universal set.

$i) A \bigcap B \subseteq A$ $ii) \overline{A \cap B} = \bar{A} \cup \bar{B}$ $iii) A \cup \bar{A} = U$.

3. Find sets A and B if $A - B = \{1,5,7\ ,8\}$ $B - A = \{2,10\}$ $A \cap B = \{3\ ,6,9\}$.

4. Use De-Morgan's law for sets to show $\overline{A \cup B \cup C} = \bar{A} \cap \bar{B} \cap \bar{C}$.

5. Show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

6. Let $U = \{1,2,\cdots,10\}$ be the universal set . List the elements of the following sets.

a) $A = \{x : x < 5 \vee x > 6\}$ $b)$ $B = \{x : x > 2 \wedge x < 7\}$

Generalized Union and Intersection.

Since union and intersection of sets satisfy associative property ,the sets $A \cup B \cup C$ and $A \cap B \cap C$ are well defined . Thus $A \cup B \cup C$ contains those elements that are in at least one of the sets $A, B \text{ and } C$ and $A \cap B \cap C$ contains those elements that are in all the sets $A, B \text{ and } C$.

Example. Let $A = \{0,2,4,6,8\}$ $B = \{0,2,3,4\}$ $C = \{0,3,6,9\}$. What are $A \cup B \cup C$ and $A \cap B \cap C$?

Solution $A \cup B \cup C = \{0,1,2,3,4,6,8,9\}$.

$A \cap B \cap C = \{0\}$.

Let $A_1, A_2, A_3, \cdots, A_n$ be n sets .Their union and intersection are written as follows

$$A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i = \{x \,/\, x \in A_i \text{ for some } i,\ i = 1,2,\cdots,n\}$$

$$A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i = \{x \,/\, x \in A_i \text{ for each } i,\ i = 1,2,\cdots,n\}.$$

Example For $i = 1,2,3,\cdots$ let

$A_i = \{i, i+1, i+2, i+3, \cdots,\}$

Find $a)\ A_1, A_2, A_3$ $\quad b)\ \bigcup_{i=1}^{4} A_i$ $\quad c)\ \bigcap_{i=1}^{4} A_i$ $\quad d)\ \bigcup_{i=3}^{n} A_i$ $\quad e)\ \bigcap_{i=1}^{n} A_i$ $\quad f)\ \bigcup_{i=2}^{4} A_i$

Solution. a) $A_1 = \{1,2,3,\cdots\}$ $A_2 = \{2,3,4,\cdots\}$ $A_3 = \{3,4,5,\cdots\}$.

$b) \bigcup_{i=1}^{4} A_i = A_1 \cup A_2 \cup A_3 \cup A_4 = A_1$ $c) \bigcap_{i=1}^{4} A_i = A_1 \cap A_2 \cap A_3 \cap A_4 = A_4$

d) $\bigcup_{i=3}^{n} A_i = A_3 \cup A_4 \cup A_5 \cup \cdots \cup A_n = A_3$ $\bigcap_{i=3}^{n} A_i = A_3 \cap A_4 \cap A_5 \cap \cdots \cap A_n = A_n$.

f) $\bigcup_{i=2}^{4} A_i = A_2 \cap A_3 \cap A_4 = A_2$

Suppose $A_1, A_2, A_3, \cdots, A_n, \cdots$, are sets we define

$$A_1 \cup A_2 \cup A_3 \cup \cdots, \cup A_n \cup \cdots, = \bigcup_{i=1}^{\infty} A_i = \{x \,/\, x \in A_i \text{ for at least one } i, i = 1,2,3,\cdots,\}$$

$$A_1 \cap A_2 \cap A_3 \cap \cdots, \cap A_n \cap \cdots, = \bigcap_{i=1}^{\infty} A_i = \{x \,/\, x \in A_i \text{ for each } i, i = 1,2,3,\cdots,\} .$$

Example . Let $A_i = \{1,2,3,\cdots,i\}, i = 1,2,3,\cdots$

Find a) A_1, A_2, A_8, A_{100} $b) A_1 \cup A_2 \cup A_8 \cup A_{100}$

$c) \bigcup_{i=1}^{100} A_1$ $d) \bigcap_{i=1}^{100} A_i$ $e) \bigcup_{i=1}^{\infty} A_i$ $f) \bigcap_{i=1}^{\infty} A$

Solution. a) $A_1 = \{1\}$ $A_2 = \{1,2\}$ $A_3 = \{1,2,3\}$ $A_{100} = \{1,2,3,\cdots,100\}$.

$b) A_1 \cup A_2 \cup A_3 \cup A_{100} = \{1\} \cup \{1,2\} \cup \{1,2,3\} \cup \{1,2,3,\cdots,100\} = A_{100}$

$c) \bigcup_{i=1}^{100} A_i = A_{100}$ $d) \bigcap_{i=1}^{100} A_i = A_1 = \{1\}$

Chapter Three. Relation and Mappings

Cartesian product

Definition .Let A and B be sets . The Cartesian product of A and B , denoted by $A \times B$, is the set of all ordered pairs (a,b) , where $a \in A$ and $b \in B$. Hence

$A \times B = \{(a,b) : a \in A \wedge b \in B\}$.

Note in the order pair (a,b) , we call a the first element and b the second element.

Example .Let A be the set of all students in the Department of Mathematics at Jazan University and B the set of all courses offered by the Department of mathematics at Jazan University. What is the Cartesian product $A \times B$?

Solution .The Cartesian product $A \times B$ consists of the ordered pairs of the form (a,b) where a is a student in the Department of Mathematics and b a course offered by the Department of Mathematics.

Example. Let $A = \{1,2\}$ $B = \{a,b,c\}$. Find the Cartesian product s $A \times B$ and $B \times A$.

Solution. The Cartesian product $A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$

$B \times A = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$.

We see that $A \times B \neq B \times A$.

The Cartesian product of more two sets can be defined similarly.

Definition. Let $A_1, A_2, \cdots, A_n$ be n sets .The Cartesian product of the sets $A_1, A_2, \cdots, A_n$, denoted by

$A_1 \times A_2 \times \cdots \times A_n$ is the set of ordered n –tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in A_i \quad for\ i = 1,2,\ldots,n$ .That is ,

$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i \ for\ i = 1,2,\ldots,n\}$.

We use the notation A^2 to denote $A \times A$ the Cartesian product of the set A with itself.

Example. What is the Cartesian product $A \times B \times C$ where $A = \{0,1\} \quad B = \{1,2\} \quad and \quad C = \{0,1,2\}$?

Solution. The Cartesian product $A \times B \times C$ consists of all ordered triples (a, b, c) where $a \in A, b \in B \quad and\ c \in C$. Hence

$$A \times B, \times C = \{(0,1,0),(0,1,1),(0\ ,1,2\}),(0,2,0)\ .(0,2,1)\ ,(0,2,2)$$
$$(1,1,0)\ ,(1,1,1)\ ,(1,1\ ,2),(1,2,0)\ ,(1,2,1)\ ,(1,2,2)\}$$

Definition. A subset R of the Cartesian product $A \times B$ is called a relation from $A\ to\ B$.

Thus R is a relation from $A\ to\ B$ if and only if $R \subseteq A \times B$.The elements of the relation R are ordered pairs ,where the first element belongs to A and the second element belongs to B.

Example . The set $R = \{(a,2),(b,3),(a,1),(c,2)\}$ is a relation from the set $\{a,b,c,d\}$ to the set $\{1,2,3,4\}$ since $R \subseteq \{a,b,c,d\} \times \{1,2,3,4\}$.

Definition .A relation from a set A to itself is called a relation on A. That is R is a relation on A if and only if $R \subseteq A \times A$.

Example Let R be a relation on the set A = $\{0,1,2,3\}$ having the property that $(a,b) \in R$ if and only if $a \le b$. That is $R = \{(a,b) : a \le b\ , where\ a \in A \wedge b \in A\}$.

a) Write T or F : $i)(2,1) \in R \quad ii)\ (0,2) \in R \quad iii)(1,4)$.

b) What are the ordered pairs of R?

Solution. i) F ii) T iii) F

$R = \{(0,2),(0,2)\}, \{0,3),(1,1)(1.2),(1,3),(2,2),(2,3),(3,3)\}$.

Example . Let $A = \{0,1,2\}$ $B = \{0,2\}$*.Let* $R = \{(a,b) : a < b\}$ *be the relation from* A *to* B*..What are the ordered pairs of* R*.*

Solution The ordered pair $(a,b) \in R$ *if and only if* $a \in A$ *,* $b \in B$ *and* $a < b$*. Thus*

$R = \{(0,2),(1,2)\}$

Functions.

Definition .Let A and B be nonempty sets. A function from A to B is a rule that assigns exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A.

If f is a function from A to B, we write $f : A \to B$.

Remark : Functions are sometimes also called mappings or transformations.

A function $f : A \to B$ can also be defined in terms of a relation from A to B.

As follows: A relation from A to B that contains one and only one ordered pair (a,b) for every element $a \in A$ defines a function f from A to B. This function is defined by setting $f(a) = b$ where

(a,b) is the unique ordered pair in the relation that has a as its first element.

Example. Let $R = \{(a,1),(b,2),(c,4)\}$ be a relation from the set $A = \{a,b,c\}$ to the set $B = \{1,2,3,4\}$

Does the relation R define a function from A to B?

Solution .We see that each element in A is a first element of one and only one (unique) ordered pair of elements of R.Thus R define a function f from A to B and is defined as follows

$f(a)=1$, $f(b)=2$, $f(c)=4$.

Example Let $A=\{1,a,2,b\}$ and $B=\{3,a,2,b,4\}$. Which of the following relations from A to B define a function from A to B?

$i)\{(1,a),(a,2),(2,a),(b,b)\}$ $ii)\{(a,a),(1,4),(b,2),(2.2),(1,b)\}$.

Solution . i) The relation $i)\{(1,a),(a,2),(2,a),(b,b)\}$ defines a function f from A to B since each element in the set A is a first element of exactly one ordered pair .the function f is defined as follows

$f(1)=a$, $f(a)=2$, $f(2)=a$ and $f(b)=b$

$ii)\{(a,a),(1,4),(b,2),(2.2),(1,b)\}$ does not define a function from A to B since the element 1 in A is a first element of two ordered pairs namely $(1,4)$ and $(1,b)$.

Definition. If $f:A\to B$ is function we call the set A the Domain of f and B the Codomain of f. If $f(a)=b$ we say b is the image of a and a is the pre-image of b.

The range of f or the image of f is the set of all images of elements of A.That is ,

Range of f = $\{f(a):a\in A\}$.

Example .Let $f:\{1,2,3\}\to\{a,b,c,d\}$ be defined by $f(1)=b$, $f(2)=c$, $f(3)=a$. What is the domain and range of f?

Solution .Domain of f = $\{1,2\ 3\}$ Range of f = The set of all images of elements of the set $\{1,2\ 3\}=\{f(1),f(2),f(3)\}$ = $\{a,b,c\}$.

Note in this example b is the image of 1 , c is the image of 2 and a is the image of 3.

The codomain of f is { a ,b ,c, d}.

Example Let $f:\mathbb{Z}\to\mathbb{Z}$ be given by $f(x)=x^2$.

i)Find the images of the elements $-2\ ,-1,0,1\ ,2$.

ii)Find the range of f.

Solution. i) The images of -2 ,-1 ,0 , 1 ,2 are given by

$f(-2)=(-2)^2=4$, $f(-1)=(-1)^2=1$ $f(0)=0^2=0$ $f(1)=(1)^2=1$, $f(2)=2^2=4$.

Ii) Range of $f=\{f(x):x\in\mathbb{Z}\}=\{x^2:x=0,\pm 1,,\pm 2,\cdots\}=\{0,1,4,9,\cdots,\}$

A Function is called a real –valued if its codomain is the set of real numbers and is an integer –valued if its codomain is the set of integers. Two real –valued or integer-valued functions can be added or multiplied.

Definition. Let $f_1\ ,f_2:A\to\mathbb{R}$ be functions and k a real number.Then f_1+f_2 , f_1-f_2 , kf_1 and f_1f_2 are also functions from A to $\mathbb{R}$ defined for all $x\in A$ by

$(kf_1)(x)=kf_1(x)\ (f_1+f_2)(x)=f_1(x)+f_2(x)$

$(f_1-f_2)(x)=f_1(x)-f_2(x)\ (f_1f_2)(x)=f_1(x)f_2(x)$

Example Le t $f_1\ ,f_2:\mathbb{R}\to\mathbb{R}$ be functions defined by $f_1(x)=x^2$, $f_2(x)=x-x^2$.

a) Find $(f_1+f_2)(x)=f_1(x)+f_2(x)=x^2+x-x^2=x$, $(f_1f_2)(x)=f_1(x).f_2(x)=x^2(x-x^2)=x^3-x^4$

b) Find the functions f_1+f_2 and f_1f_2.

Solution a)

$i)\ (f_1+f_2)(-1)=f_1(-1)+f_2(-1)=(-1)^2+(-1)-(-1)^2=1-1-1=-1$ $ii)\ (f_1-f_2)(0)=f_1(0)-f_2(0)=0$ $iii)\ (f_1f_2)(2)=f_1(2)f_2(2)=2^2.(2-2^2)=-8$

$iv)\ (3f_1)(-2)=3f_1(-2)=3(-2)^2=3.4=12$.

b) $(f_1+f_2)(x)=f_1(x)+f_2(x)=x^2+x-x^2=x$, $(f_1f_2)(x)=f_1(x).f_2(x)=x^2(x-x^2)=x^3-x^4$.

Definition. Let $f : A \to B$ and $S \subseteq A$. The image of the of S under the function f denoted by

$f(S)$, is a subset of B consisting of all images of elements of S. That is ,

$f(S) = \{f(x) : x \in S\}$.

Example Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4\}$.Let $f : A \to B$ be defined by

$f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$ and $f(e) = 1$. Find the image of the set $S = \{b, c, d\}$, that is find $f(S) = f(\{b, c, d\})$.

Solution . $f(S) = f(\{b, c, d\}) = \{f(x) : x \in S\} = \{f(b), f(c), f(d)\} = \{1, 4, 1\} = \{1, 4\}$.

One- to -One and Onto functions

Definition . A function $f : A \to B$ is called one –to-one or injective if $f(a) = f(b)$ implies $a = b$ for all a, b in A

The above definition is equivalent to :. f is one-to-one if $a \neq b \text{ implies } f(a) \neq f(b)$. (That is distinct elements have distinct images)

Remark. Suppose $f : A \to B$.

i)To show f is one- to-one Assume $f(a) = f(b)$ (where a and b arbitrary elements in the domain of f) and show $a = b$. Or If $a \neq b$ show that $f(a) \neq f(b)$.

ii)To show f is Not one-to-one find two elements $x, y \in A$, $x \neq y$ such that $f(x) = f(y)$.

Example. Let $f : \{a, b, c, d\} \to \{1, 2, 3, 5\}$ be given by $f(a) = 4, f(b) = 5, f(c) = 1, f(d) = 3$.

Is f one-to-one?

Solution. f is one-to-one since it takes different values at the four elements .That is ,distinct elements in the domain have different images.

Example. Let $f:\mathbb{Z}\to\mathbb{Z}$ be given by $f(x)=x^2$. Is f one-to-one?

Solution . f is not one –to-one since $f(-1)=f(1)$ but $-1\neq 1$.

Example. Determine whether the function $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=x+1$ is one-to-one.

Solution. If $x\neq y$ then $x+1\neq y+1$. Thus f is one-to-one.

Or Assume $f(x)=f(y)$ and show $x=y$.

$f(x)=f(y)\to x+1=y+1\to x=y$. Thus f is one-to-one.

Definition. Let $f:A\to B$. We say f is onto or surjective if for every element $b\in B$ there is an element $a\in A$ with $f(a)=b$.

That is, f is onto if every element in B is an image of some element in A Equivalently , $f(A)=B$ .or range of $f=B$.

Remark .Suppose $f:A\to B$.

i) To show is onto take any element $b\in B$ and find some element $a\in A$ such that $f(a)=b$.

ii) To Show f is not onto find $y\in B$ such that $f(x)\neq y$ for all $x\in A$

Example .Let $f:\{a,b,c,d\}\to\{1,2,3\}$ given by $f(a)=3$, $f(b)=2$, $f(c)=1$, $f(d)=3$.

Is f one-to-one? Onto?

Solution. f is not one-to - one since $f(a)=3=f(d)$ but $a\neq d$.

f is onto since all elements in the codomain are images of elements in the domain (every element in $\{1,2,3\}$ is an image of some element in $\{a,b,c,d\}$) .That is ,

$f(\{a,b,c,d\})=\{1,2,3\}$ or Range of f is $\{1,2,3\}$.

Example . Let $f:\mathbb{Z}\to\mathbb{Z}$ defined by $f(x)=x^2$. Is f on to?

Solution. f is not on to since $-1\in\mathbb{Z}$ and $f(x)\neq -1$ for all $x\in\mathbb{Z}$ as $f(x)=x^2\geq 0$ for all $x\in\mathbb{Z}$

Example Let $f:\mathbb{Z}\to\mathbb{Z}$ given by $f(x)=x+2$. Is f onto?

Solution. Let $y\in\mathbb{Z}$. We need to find $x\in\mathbb{Z}$ such that $f(x)=y$. We have

$f(x)=y\Rightarrow x+2=y\Rightarrow x=y-2\in\mathbb{Z}$. With $x=y-2$ we get $f(x)=f(y-2)=y-2+2=y$

(y is the image of $y-2$).Since y is arbitrary , f is onto.

Example. $g:\mathbb{R}\to\mathbb{R}$ be given by $g(x)=2x+1$. Show that g is one to one and onto.

Definition . Let $f:A\to B$. We say f is one to one correspondence or bijective if it is both one –to –one and onto.

Example Let $f:\{a,b,c,d\}\to\{1,2,3,4\}$ be given by $f(a)=4,f(b)=2,f(c)=3$ $f(d)=1$. Is f bijective?

Solution. It easy to check that f is one –to-one and onto. Hence it is bijective.

Example. Show $f:\mathbb{R}\to\mathbb{R}$ given $f(x)=2x-1$ is bijective.

Solution. a) To show f is one to one. Suppose $f(x_1)=f(x_2)$, $x_1,x_2\in\mathbb{R}$. To show $x_1=x_2$.

$f(x_1)=f(x_2)\Rightarrow 2x_1-1=2x_2-1\Rightarrow 2x_1=2x_2\Rightarrow x_1=x_2$. Thus f is one to one.

b) To show f is on to. Let $y\in\mathbb{R}$. (codomain) .To find $x\in\mathbb{R}$ (domain) such that $f(x)=y$.

Now $f(x)=y\Rightarrow 2x-1=y\Rightarrow 2x=y+1\Rightarrow x=\dfrac{y+1}{2}\in\mathbb{R}$.

Thus $f(x)=f(\frac{y+1}{2})=2(\frac{y+1}{2})-1=y+1-1=y$.

Hence f is on to.

Form (a) and (b) f is bijective.

Example Let A be a set .The identity function on denoted by ι_A is the function $i_A : A \to A$ and defined by $\iota_A(x)=x$ for all $x \in A$. ι_A is bijective.

Example. Let $A=\{a, b\ c\}$ and $B=\{1, 2, 3\}$. The following relations from A to B define a function f from A to B. Determine whether they are one-to-one , onto and bijective.

$i)\ \{(a, 2), (b, 1), (c\ 3)\}$ $ii)\ \{(a, 3), (b, 1), (c, 3)\}$.

Solution i)Here $f(a)=2, f(b)=1$ and $f(c)=3$.Thus f takes different values at the three elements. Hence f is one-to one. Since the Range of f is the set B , f is onto. Thus f is bijective and f^{-1} is given by

$f^{-1}(2)=a, f^{-1}(1)=b, f^{-1}(3)=c$.

ii) Here $f(a)=3, f(b)=1$ and $f(c)=3$. f is not one to-one since $f(a)=f(c)$ but $a \neq c$.

It is not onto since $2 \in B$ but $f(x) \neq 2$ for all $x \in A$.(or since range of f $=\{1, 3\} \neq B$ f is not onto.)

Exercise

1. Why is f not a function from $\mathbb{R}$ to $\mathbb{R}$,if

$i)\ f(x)=\frac{1}{x}$ $,ii)\ f(x)=\sqrt{x}$ $iii)\ f(x)=\pm\sqrt{x^2+1}$

2.Determine whether f is a function from $\mathbb{Z}$ to $\mathbb{R}$ if

$i)\ f(n) = \pm n \quad ii)\ f(n) = \sqrt{n^2+1} \quad ii)\ f(n) = \dfrac{1}{n^2-4}$.

3. Let $A = \{1,2,3,a\}$ and $B = \{a,b,2,3,4\}$ .Which of the following sets are relations from A to B.? from B to A ?.

$i)\ \{(1,2),(3,b),(1,a)\}\ \ ii)\ \{(2,2),(3,3),(a,4),(a,4)\}\ \ iii)\ \{(2,4),((a,a),(b,3)\}$. $iv)\ \{(2.3),(3,4),(a,1)\}$.

4.Let $A = \{2,3,4,a\}$ and $B = \{a,b,d,2,3\}$. Which of the following relations define a function from A to B. $i)\ \{(2,2),(3,3),(a,a),(4,3)\}\ ii)\ \{(2,b),(3.b),(4,b),(a,b)\}$,

$iii)\ \{(a.b),(3,d),(4,3),(2,2),(3,3)\}\ iv)\ \{(2,3),(3,4),(a,b)\}$.

5.Determine whether each of these function from $\{a,b,c,d\}$ to itself is one-to-one ? on to?

$i)\ f(a)=b, f(b)=a, f(c)=c, f(d)=d\ \ ii)\ f(a)=b, f(b)=b, f(c)=d, f(d)=c$

$iii)\ f(a)=d, f(b)=b, f(c)=c, f(d)=d$.

Inverse Function and composition of functions

Definition. Let $f : X \to Y$ be a one to one correspondence (bijective).

The inverse of the function f is the function that assigns to an element $y \in Y$ the unique element $x \in X$ such that $f(x) = y$.The inverse function of f is denoted by f^{-1}.

Thus we have $f^{-1}(y) = x$ whenever $f(x) = y$ and $f^{-1} : Y \to X$.

From the definition, we have $f^{-1}(f(x)) = x$ for all $x \in X$ and $f(f^{-1}(y)) = y$ for all $y \in Y$.

If f is bijective we say it is invertible.

Remark. If f is not one to one correspondence then we cannot define inverse function.

Example. Let $f:\{a,b,c\}\to\{1,2,3\}$ be given by $f(a)=2, f(b)=3, f(c)=1$. Is f invertible? If so find

f^{-1}.

Solution. It is easy to see that f is bijective. Thus f is invertible.
$f^{-1}:\{1,2,3\}\to\{a,b,c\}$ is given by $f^{-1}(1)=c, f^{-1}(2)=a, f^{-1}(3)=b$.

Example Let $f:\mathbb{R}\to\mathbb{R}$ be given by $f(x)=2x-3$. Is f invertible? If so find a formula for f^{-1}.

Solution. We must show f is bijective, that it is one-to one and onto.

I) To show f is one -to-one. Suppose $f(x)=f(y)$. We have to show $x=y$.

$f(x)=f(y)\Rightarrow 2x-3=2y-3\Rightarrow 2x=2y\Rightarrow x=y$. Thus f is one –to-one.

ii) to show f is onto. Let $y\in\mathbb{R}$. We must find $x\in\mathbb{R}$ such that $f(x)=y$.

$$f(x)=y\Rightarrow 2x-3=y\Rightarrow 2x=y+3\Rightarrow x=\frac{y+3}{2}\in\mathbb{R}$$

If we take $x=\frac{y+3}{2}$ then $f(x)=f(\frac{y+3}{2})=2(\frac{y+3}{2})-3=y+3-3=y$. Thus f is onto.

From (i) and (ii) f is bijective. Hence f is invertible.

To find f^{-1}. Let $f(x)=y$ so that $f^{-1}(y)=x$. We have

$f(x)=y.\Rightarrow 2x-3=y\Rightarrow 2x=y+3\Rightarrow x=\frac{y+3}{2}$. Thus

$f^{-1}(y)=\frac{y+3}{2}$.(Hence $f^{-1}(x)=\frac{x+3}{2}$ replacing y by x)

Definition Let. $f:A\to B$ and $g:B\to C$. The composition of g and f denoted by gof is defined by

$(gof)(x)=g(f(x))$ for all $x\in A$.

Note. gof is a function from A to C.

Range of f must be a subset of the Domain of g.

Example Let $f:\{a,b,c\}\to\{a,b,c\}$ be given by $f(a)=b$, $f(b)=c$, $f(c)=a$ and $g:\{a,b,c\}\to\{1,2,3\}$ where $g(a)=3$, $g(b)=2$, $g(c)=1$. Find gof.

Solution . gof is defined by
$(gof)(a)=g(f(a))=g(b)=2$, $(gof)(b)=g(f(b))=g(c)=1$, $(gof)(c)=g(f(c))=g(a)=3$.

Note fog is not defined since the range of g is not a subset of the domain of f.

Example .Let $g, f:\mathbb{Z}\to\mathbb{Z}$ be defined by $f(x)=2x+3$, $g(x)=3x+2$.

i) Find $(gof)(2)$, $(fog)(-1)$.

ii) Find the function s fog and gof.

Solution .i) $(gof)(2)=g(f(2))=g(7)=21+3=24$, $(fog)(-1)=f(g(-1))=f(-1)=1$.

ii) $(gof)(x)=g(f(x))=g(2x+3)=3(2x+3)+2=6x+9+2=6x+11$

Remark . From the above example we see that $fog\neq gof$,that is composition of functions is not commutative.

Note. 1.Suppose $f:A\to B$ is invertible, that is, $f^{-1}:B\to A$ exists. We have

$f(a)=b\Leftrightarrow f^{-1}(b)=a$ .Th.us $fof^{-1}:B\to B$ and $f^{-1}of:A\to A$. Moreover

$(fof^{-1})(b)=f(f^{-1}(b)=f(a)=b$ for every $b\in B$, Hence $fof^{-1}=\iota_B$.

$(f^{-1}of)(a)=f^{-1}(f(a))=f^{-1}(b)=a$ for every $a\in A$,Hence $f^{-1}of=\iota_A$.

2, Suppose $f:A\to B$, $g:B\to C$, $h:C\to D$.Since $gof:A\to C$,we have

$ho(gof):A\to D$, and $(ho(gof))(a)=h((gof)(a))=h(g(f(a))$.

Relation on a set.

Recall that :

Definition. A relation on a set A is a relation from A to A.That is , a relation on a set A is a subset $A \times A$.

Example . Let $A = \{1 ,2 ,3 ,4\}$. Write the elements of the relation $R = \{(a,b) : a \ divide \ b\}$ on the set A.

Solution. $(a,b) \in R$ if and only if $a,b \in A$ and a divides b. Thus

$$R = \{(1,1) ,(2,2) ,(3,3) ,(4,4),(1,2) ,(1,3) ,(1,4) ,(2 ,4)\}.$$

Example . Consider the following relation on the set of integers.

$i)\ R_1 = \{(a,b) : a \le b\}$ $ii)\ R_2 = \{(a,b) : a > b\}$ $iii)\ R_3 = \{(a,b) : a = b \vee a = -b\}$

$iv)\ R_4 = \{(a,b) : a = b\}$, $v)\ R_5 = \{(a,b) : a = b+1\}$ $vi)\ R_6 = \{(a,b) : a+b \le 3\}$

Which of these relations contain each of the ordered pairs

$(1,1)\ ,(1,2)\ ,((2,1)\ ,(1,-1)\ ,(2,2)?$.

Solution . $(1,1)$ belongs to $R_1\ ,R_3\ ,R_4$, and R_6.

$(1,2)$ belongs to R_1 , R_6 ; $(2,1)$ belongs to $R_2\ ,R_5$ and R_6.

$(1,-1)$ belongs to $R_2\ ,R_3\ ,R_6$; $(2,\ 2)$ belongs to $R_1\ ,R_3\ ,R_4$.

How many relations are there on set of n elements?

Solution. Note that a set with m elements has 2^m elements. A relation on a set is A is a subset of $A \times A$. If A has n elements then $A \times A$ has n^2 elements. Thus the number of subsets of $A \times A$ (That is the number of relations on the set A) is 2^{n^2}.

Properties of relations.

Definition . A relation R on set A is called reflexive if $(a,a) \in R$ (aRa) for all $a \in A$

Example Consider the following relation on the set $A = \{1,2,3,4\}$.

$R_1 = \{\{(1,1)\ ,(1,2)\ ,(2,2)\ ,(3,4)\ ,(4,1)\ ,(4,4)\}$
$R_2 = \{(1,1)\ ,(1,2)\ ,(2,1)\}$
$R_3 = \{(1,1)\ ,(1,2)\ ,(1,4)\ ,(2,2)\ ,(3,3)\ ,(4,1)\ ,(4,4)\}$

Which of these relations are reflexive

Solution. R_1 is not reflexive since $3 \in A$ but $(3,3) \notin R_1$.

R_2 is not reflexive since $(3,3) \notin R_2$.

R_3 is reflexive since $(a,a) \in R_3$ for all $a \in A$.

Example .On the set of integers define a relation $R = \{(a,b) : a\ divides\ b\}$.

a) Write true or false : $i)\ (2,3) \in R$,$ii)\ (4,2) \in R$,$iii)\ (8\ ,16)$

b).Is R reflexive?

Solution. a) i) false ii) false iii) true

b) No , since $0 \in \mathbb{Z}$ 0 divides 0 is false $(0,0) \notin R$.

Example .On Z we define a relation $R = \{(a,b) : a$ is a multiple of b}.

a) Write true or false . $i)(6,2)$, $ii)\ (5,3)$, $iii)\ (-8,4)\}$

b) Is R reflexive?

Solution . a) i) True since 6 = 3.2 ii) false iii) True since -8 = (-2).4

b) Since for any $a \in Z$ we have $a = 1.a$, that is a is a multiple of itself, $(a,a) \in R$. Hence

R is reflexive.

Definition. I) A relation R on a set A is called symmetric if $(b,a) \in R$ whenever $(a,b) \in R$.

ii) A relation R on a set A is called anti symmetric if $(a,b) \in R$ and $(b,a) \in R$ then $a = b$.

Example. Let $A = \{a,b.c\}$. Which of the following relations on A are symmetric?

$$R_1 = \{(a,a)\ ,(b,c)\ ,(a,b)\ ,(c,b)\}$$
$$R_2 = \{(b,b)\ ,(c,c)\ ,(a,a)\}$$
$$R_3 = \{(c,a)\ ,(a,b)\ ,(a,c),(b,a)\}$$

Solution. R_1 is not symmetric since $(a,b) \in R_1$ but $(b,a) \notin R_1$.

R_2 and R_3 are symmetric.

Example On the set $\mathbb{Z}^+$ define a relation $R = \{(a,b) : a / b\}$. (a/b means a divides b ,that is, b = k.a for some integer k.)

Is R symmetric ?antisymmetric ? reflexive?

Solution. R is not symmetric since $(1,2) \in R$ but $(2,1) \notin R$ since 2 does not divide 1.

To check for anti-symmetric :Suppose $(a,b) \in R$ and $(b,a) \in R$. To show $a = b$.

Since $(a,b) \in R$ and $(b,a) \in R$ we have $b = ka$ and $a = mb$ for some $k, m \in \mathbb{Z}^+$. Thus we get

$b = kmb \Rightarrow km = 1 \Rightarrow m = k = 1$. Hence $a = b$.

Since for any $a \in \mathbb{Z}^+$ a / a is true we have $(a,a) \in R$. Thus R is reflexive.

Definition. A relation R on a set A is called transitive if whenever $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$.

Example Which of the following relations on the set $A = \{1,2,3,4\}$ are transitive?

$R_1 = \{\{(1,1), (1,2), (2,2), (3,4), (4,1), (4,4)\}$
$R_2 = \{(1,1), (1,2), (2,1)\}$
$R_3 = \{(1,1), (1,2), (1,4), (2,2), (3,3), (4,1), (4,4)\}$

Solution R_1 is not transitive since $(3,4) \in R_1$ and $(4,1) \in R_1$ but $(3,1) \notin R_1$.

R_2 is transitive. R_3 is not transitive since $(4,1) \in R_3 \wedge (1,2 \in R$ but $(4,2) \notin R$.

Example .Let $R = \{(a,b) : a / b , a, \in \mathbb{Z}\}$, Show that R is transitive.

Solution. Suppose $(a,b) \in R$ and $(a,b) \in R$ .To show $(a,c) \in R$. Since

$(a,b) \in R \wedge (b,c) \in R \Rightarrow b = ka \wedge c = mb$ for some $k, m \in \mathbb{Z}$.Thus we get

$c = mb = m(ka) = (mk)a = na$, where $n = mk \in \mathbb{Z}$.Therefore a / c. Hence $(a,c) \in R$.

Equivalence relation.

Definition .A relation on a set A is called an equivalence relation if it is reflexive , symmetric and transitive.

Definition. Two elements a and b that are related by an equivalence relation are called equivalent and we write $a \sim b$.

Example. Let $A = \{1,2,3\}$. which of the following relations on A are equivalence relation?

$$R_1 = \{(1,1),(1,2),\ (2,2),(3,1),(3,3),(3,2)\}$$
$$R_2 = \{(2,2),(2,3),(1,1),(3,3),(3,2)\}$$
$$R_3 = \{(1,1),(2,2),(3,3)\}$$

Solution. R_1 is not an equivalence relation since it is not symmetric we see $(1,2) \in R_1$ but $(2,1) \notin R_1$. R_2 and R_3 are reflexive , symmetric and transitive and hence an equivalence relation

Example. Let $R = \{(a,b) : a = b \vee a = -b ,\ a,b \in \mathbb{Z}\}$. Show that R is an equivalence relation on $\mathbb{Z}$.

Solution. We have to show R is i) reflexive ii) symmetric and iii) transitive.

Note that $(a,b) \in R$ if and only if $a,b \in \mathbb{Z}$ and $a = b$ or $a = -b$, that is , $a = \pm b$.

To show R is reflexive

(i) For every $a \in \mathbb{Z}$, $(a,a) \in R$ since $a = a$ is true. Hence R is reflexive.

ii) To show R is symmetric :suppose $(a,b) \in R$. Then $a = b$ or $a = -b$. This implies $b = a$ or $b = -a$. Thus by definition of R $(b,a) \in R$. Hence R is symmetric.

iii) To show R is transitive : suppose $(a,b) \in R$ and $(b,c) \in R$. To show $(a,c) \in R$.

Since $(a,b) \in R$, and $(b,c) \in R$ we have $a = \pm b \wedge b = \pm c$ .which implies $a = \pm(\pm c) = \pm c$. Thus $(a,c) \in R$. Hence R is transitive,

From (i) , (ii) and (iii) we conclude that R is an equivalence relation.

Example. Let $R = \{(a,b) : a \,/\, b \, , a,b \in \mathbb{Z}^+\}$. Is R an equivalence relation on $\mathbb{Z}^+$.

Solution. No. since it is not symmetric . $(2,4) \in R$ but $(4,2) \notin R$ since $4 \,/\, 2$ is false.

Example Let R be relation on the set of real numbers and $R = \{(a,b) : a - b \in \mathbb{Z}\}$. Show that R is an equivalence relation.

Solution. We have to show R is i) reflexive ii) symmetric and iii) transitive.

i) Reflexive : since for all real number a , $a - a = 0 \in \mathbb{Z}$ is true R is reflexive.

ii) Symmetric): Suppose $(a,b) \in R$. We have

$a - b \in \mathbb{Z} \Rightarrow -(a - b) \in \mathbb{Z} \Rightarrow b - a \in \mathbb{Z}$. Thus $(b,a) \in R$. Therefore R is symmetric.

iii) Transitive : $(a,b) \in R \wedge (b,c) \in R$. To show $(a,c) \in R$. We have

$(a,b) \in R \wedge (b,c) \in R \Rightarrow a - b \in \mathbb{Z} \wedge b - c \in Z \Rightarrow (a - b) + (b - c) \in \mathbb{Z} \Rightarrow a - c \in \mathbb{Z}$. Thus $(a,c) \in R$.

$\therefore R$ is transitive.

From (i) ,(ii) and (iii) R is an equivalence relation.

Example . Congruence Modulo m. Let $m \in \mathbb{Z}$ $, m > 1$.

We write $a \equiv b (\bmod m)$ if and only if $m | a - b$ that is m divides $a - b$.

Example . Let $R = \{(a,b) : a \equiv b(\bmod 5)\}$.

Write true or false.

$i)\ (10,5) \in R \quad ii)\ (12,2) \in R \quad iii)\ (15,6) \in R$.

Solution. i) True . since $5|(10 - 5)$ ii) True, since $5|(12 - 2)$ iii) False ,since $5|(15 - 6)$ is false.

Example. Let $R = \{(a,b) : a \equiv b(\operatorname{mod} m)\}$. Show that R is an equivalence relation for any $m > 1$, $m \in \mathbb{Z}$.

Solution. i) Reflexive :Since $a - a = 0.m$ for any $a \in \mathbb{Z}$ we have $a \equiv a(\operatorname{mod} m)$ Thus , $(a,a) \in R$. So it isreflexive.

ii) Symmetric : If Suppose $(a,b) \in R$. To show $(b,a) \in R$.

$(a,b) \in R \Rightarrow a - b = km$ for some $k \in \mathbb{Z}$

$\Rightarrow b - a = (-k)m$ where $c = -k \in \mathbb{Z}$.

$\Rightarrow b \equiv a(\operatorname{mod} m)$

Thus $(b,a) \in R$. Hence R is symmetric.

iii)Transitivity: Suppose $(a,b) \in R \wedge (b,c) \in R$ ($aRb \wedge bRc)$) .To show $(a,c) \in R$ (bRc)

$aRb \wedge bRc) \Rightarrow a - b = km \wedge b - c = cm$ for some $k, m \in \mathbb{Z}$.

$\Rightarrow (a-b) + (b-c) = km + cm$

$\Rightarrow (a-b) + (b-c) = (k+c)m$

$\Rightarrow b - c = dm$ where $d = k + c \in \mathbb{Z}$.

$\Rightarrow b \equiv c(\operatorname{mod} m)$

Hence bRc. $\therefore R$ is transitive .From (i) ,(ii) and (iii) R is an equivalence relation.

Example Show that the relation $R = \{(a,b) : a \mid b \quad ,a,b \in \mathbb{Z}^{+}\}$ is not an equivalence relation.

Solution .It is not symmetric .since $2 \mid 4$ is true but $4 \mid 2$ is false.

Equivalence Classes.

Definition. Let R be a relation on a set A. The set of all elements in A that are related to an element a of A is called an equivalence class of a with respect to R. It is denoted by [a].

Thus

$[a] = \{b : aRb\} = \{b : (a,b) \in R\}$.

If $b \in [a]$ then b is called a representative of the equivalence class determined by a.

Note. $[a] \neq \varnothing$ since $a \in [a]$.

Example .The relation $R = \{(1,1),(2,2),(3,3) \quad (3,1),(1,3)\}$ on the set $\{1,2,3\}$ is an equivalence relation. Find. $i)\,[1] \quad ii)\,[3] \quad iii)[2]$

Solution

$i)\,[1] = \{b : (1,b) \in R\} = \{1,3\} \qquad ii)\,[3] = \{b : (3,b) \in R = \{1,3\} \quad iii)[2] = \{b : (2,b) \in R\} = \{2\}$

Example .Let $R = \{(a,b) : a = b \vee a = -b\}$ be a relation on the set of real numbers.

We have seen R is an equivalence relation. Find $i)\,[-1] \quad ii)\left[\frac{2}{3}\right] \quad iii)\,[a], a \in \mathbb{R}$

Solution

$i)\,[-1] = \{b \in \mathbb{R} : (-1,b) \in R\} = \{b : -1 = b \vee -1 = -b\} = \{-1,1\} \quad ii)\left[\frac{2}{3}\right] = \{b \in \mathbb{R} : \frac{2}{3} = b \vee \frac{2}{3} = -b\} = \{-\frac{2}{3}, \frac{2}{3}\} \quad iii)\,[a] = \{-a, a\}$

Theorem .Let R be an equivalence relation on a set A. The following statements for elements a,b of A are equivalent.

$i)\ aRb \qquad ii)\,[a] = [b] \qquad iii)\,[a] \cap [b] \neq \varnothing$

Proof. to prove $(i) \Rightarrow (ii)$. We assume (i) is true . If $x \in [a]$ then xRa. Thus we have $xRa \wedge aRb$.Since R is transitive xRb . Hence $x \in [b]$.

$\therefore [a] \subseteq [b]$. In the same way one can show $[b] \subseteq [a]$. Thus $[a] = [b]$.

To show $(ii) \Rightarrow (iii)$. Assume $[a]=[b]$ .Since $a \in [a]$ we have $a \in [a] \cap [b]$. Thus $[a] \cap [b] \neq \varnothing$.

To Show $(iii) \Rightarrow (i)$. Assume $[a] \cap [b] \neq \varnothing$.To show aRb. Let $c \in [a] \cap [b]$. Then $aRc \wedge bRc$

By symmetric cRb. Thus we have $aRc \wedge cRb$ Thus ,since , R is transitive aRb.

Thus we have proved $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$. Thus all the statements are equivalent.

Remark. 1. The Theorem shows two equivalence classes are either equal or disjoint. That is

either $[a] \cap [b] = \varnothing$ or $[a]=[b]$

2. Since $a \in [a]$ for each $a \in A$. It follows that $A = \bigcup_{a \in A} [a]$.

3. The equivalence classes split the set A in to disjoint subsets.

Partition of a set.

Definition. A partition of a set S is a collection of nonempty disjoint subsets of S that have S as their union..

Example . Let $S=\{1,2,3,4,5\}$. Let $A_1=\{1,2\}$ $A_2=\{3.4\}$ $A_3=\{5\}$ .The set $\{A_1, A_2, A_3\}$

Is a disjoint collections of subsets of S Their union $A_1 \cup A_2 \cup A_3 = S$.

Thus $\{A_1, A_2, A_3\}$ is partition of the set S.

Remark. 1. The distinct equivalence classes of an equivalence relation form a partition of A.

2. If S is a a partition of a set A then there is an equivalence relation R on A that the sets in S as its equivalence class The relation R on A is defined as follows : aRb if and only if a and b belong to the same set in S.

Example. Let $A=\{1,2,3,4\}$ and $R=\{(1,1),(1,2),(2,2),(3,3),(4,4)\}$. Find the equivalence classes..

Solution

$[1] = \{x : 1Rx\} = \{1,2\} = [2]$
$[3] = \{3\} \quad [4] = \{4\}$

$S = \{[1], [3] . [4]\}$ is a partition of the set A. $A = [1] \cup [3] \cup [4]$.

Example. The relation $R = \{(a,b) : a \equiv \mathrm{mod}(3)\}$ on $\mathbb{Z}$ is an equivalence relation. Find the equivalence classes of R.

Solution. For $a \in \mathbb{Z}$,

$[a] = \{b : a = b \,\mathrm{mod}(3)\} = \{b : 3 \big| b - a\} = \{b : b - a = 3m$ for some $m \in \mathbb{Z}\}$

$= \{b : b = a + 3m, m \in \mathbb{Z}\}$.

Thus $b \in [a] \Leftrightarrow b = a + 3m \quad m \in \mathbb{Z}$.

For $a = 0$ we get

$[0] = \{b : b = 3m , m \in \mathbb{Z}\} = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$

For $a = 1$ we get

$[1] = \{b : b = 1 + 3m , m \in \mathbb{Z}\} = \{\ldots, -5 , -2 , 1 , 4, 7, \cdots\}$

$[2] = \{b : b = 2 + 3m\} = \{\cdots, -4 , -1, 2, 5, 7, \cdots\}$.

It is not hard to see that these are the only distinct equivalence classes of R.

The set $\{[0], [1], [2]\}$ is a partition of $\mathbb{Z}$.

$\mathbb{Z} = [0] \cup [1] \cup [2$

Example . Let $A_1 = \{1,2,3\} \quad A_2 = \{4,5\} \quad A_3 = \{6\}$. $\{A_1 , A_2 , A_3\}$ be a partition of $\{1,2,3,4,5,6\}$
.

List the ordered pair in the equivalence relation R produced by the partition.

Solution. The subsets in the partition are the equivalence classes of R.

Thus $R=\{(1,1),(2,2),(3,3),(1,2),(1,3),(2,1),(2,3),(3,1),(3,2),(4,4),(5,5),(4,5),(5,4).(6,6)\}$

Exercise

1. List the order pairs in the relation R from $A=\{0\ ,1\ ,2\ ,3\ ,4\}$ to $B=\{0\ ,1\ ,2\ ,3\ \}$ where

$i)\ R=\{(a,b)\ /\ a=b \quad ii)\ R=\{(a,b)\ /\ a+b=4\} \quad iii)\ R=\{(a,b)\ /\ a>b\} \quad iv)\ R=\{(a,b)\ /\ a\ divides\ b\}$

2. List all the order pairs in the relation $R=\{(a,b)\ /\ a\ divides\ b\ \}$ on the set $\{1\ ,2\ ,3\ ,4\ ,5\ ,6\}$.

3.For each of these relation on the set $A=\{0\ ,1\ ,2\ ,3\ ,4\}$ decide whether it is reflexive , symmetric, anti - symmetric and transitive.

i) $\{(2,2)\ ,(2\ ,3)\ ,(2,4)\ ,(3,2)\ ,(3\ ,3)\ ,(3,4)\}$ $\quad ii)\{(1,1)\ ,(1,2)\ ,(2,1)\ ,(2,)\ ,(3,3),(4,4)\}$ $\quad iii)\{(2,4)\ ,(4,2\}$

$iv)\{(1,2)\ ,(2,3)\ ,(3,4)\}\ \ v)\ \{(1,1)\ ,(2,2)\ ,(3,3)\ ,(4,4)\}\ \ v)\{(1,3)\ ,(1,4)\ ,(2,3)\ ,(2,4)\ ,(3,1)\ ,(3,4)\}$.

4.Determine whether the following relation s on the set of real numbers are reflexive , symmetric , anti -symmetric and transitive .

$i)\,R_1=\{(x,y)\ /\ x+y=0\}\ \ ii)\,R_2=\{(x,y)\ /\ x=\pm y\}\ \ iii)\ R_3\{(x,y)=0\ /\ x=2y\}\quad iv)\,R_4=\{(x,y)\ /\ xy=0\}\ \ v)\ R_5=\{(x,y)\ /\ x=1\}$

5 .Determine whether the following relation s on the set of integers are reflexive , symmetric , anti-symmetric and transitive .

$i)\,R_1=\{(x,y)\ /\ x\neq y\}\ \ ii)\,R_2=\{(x,y)\ /\ x=y+1\ or\ x=y-1\}\ \ iii)\ R_3=\{(x,y)\ /\ x=y(\bmod 7)\}\quad iv)\,R_4=\{(x,y)\ /\ x\ is\ a\ multiple\ of\ y\}\ \ v)\ R_5=\{(x,y)\ /\ x=y^2\}$

6. Show that the relation $R=\{(x,y)\ /\ x-y\,is\ an\ \mathrm{int}eger\}$ is an equivalence relation on the set of real numbers. And find $i)\quad [1]\quad ii)\ \left[\frac{1}{2}\right]$.

7, Show that the relation $R=\{(m,n)\ /\ m=n\quad or\quad m=-n\}$ is an equivalence relation on the set of integers and find $[0]\ ,[1]\ .[n]\quad n\in\mathbb{Z}$

8,.Let $A=\{f\ /\ f:\mathbb{Z}\to\mathbb{Z}\}$. Show that the following relations on A is an equivalence relation.

$a)\ \{(f,g)\ /\ f(1)=g(1)\}$ $b)\ \{(f,g)\ /\ f(0)=g(0)\quad or\ f(1)=g(1)\}$

9)Let $A=\{(a,b)\ /\ a,b\in\mathbb{Z}^{+}\}$ .Show that the following relations on A are equivalence relations.

$i)\ R_1=\{((a,b),(c,d))\ /\ ad=bc\}$ $ii)\ R_2=\{((a,b),(c,d))\ /\ a+d=b+c\}$

10. Consider $a=b(\mathrm{mod}\,4)$ .Find $[0],\ [1],\ [2]$.

Chapter Five. Binary Operations.

Definition. Let A be a set . A binary operation on A is a function from $A \times A$ to A. That is , $*$ is a binary operation on A if

$* : A \times A \to A$.

We write $a * b$ for $*((a,b))$.

Example. 1. $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $+((a,b)) = a + b$ is a binary operation on $\mathbb{Z}$ .That is the operation addition on $\mathbb{Z}$ is a binary operation.

2. $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $*((a,b)) = a - b$ is a binary operation on $\mathbb{Z}$. That is , the operation subtraction is a binary operation on $\mathbb{Z}$.

Here $*((a,b)) = a * b = a - b$. So $3 * 5 = 3 - 5 = -2$.

3. Subtraction is not a binary operation on $\mathbb{N}$. For example $3 * 5 = 3 - 5 = -2 \notin \mathbb{N}$. In this case we say $\mathbb{N}$ is not closed under (the operation) subtraction.

4. Let A and $\wp(A)$ be the power set of A .The operation union "$\cup$" and intersection "$\cap$" are binary operations on the power set $\wp(A)$ of A.

5. Let P be the set of all propositions ..The logical connectives "and" ($\wedge$) and "or"($\vee$) are binary operations on P. That is

$\wedge : P \times P \to P$ given by $\wedge((p,q)) = p \wedge q$; $\vee : P \times P \to P$ given by $\vee((p,q)) = p \vee q$

are binary operations on P.

6.Let $A = \{1,0\}$. Define $\otimes$

$$\otimes((0,0)) = 0 \otimes 0 = 0 \quad ,\otimes((0,1)) = 0 \otimes 1 = 1$$
$$\otimes((1,0)) = 1 \otimes 0 = 1 \quad ,\otimes((1,1)) = 1 \otimes 1 = 1$$

is a binary operation on A , that is it is a function from A xA to A.

We illustrate $\otimes$ by a table below :

$\otimes$	0	1
0	0	1
1	1	1

Example . Let $S = \{1,2,3\}$. Define $\triangle$ and $\triangledown$ as follows.

$\triangle$	1	2	3
1	1	1	2
2	2	3	3
3	3	2	1

$\triangledown$	1	2	3
1	1	1	2
2	3	3	1
3	3	1	2

Find $i)\ 1\Delta 1\ , ii)\ \ (1\Delta 1)\Delta 3 \quad iii)\ (1\Delta 1)\nabla 1 \quad iv)\ (3\nabla 2)\Delta 3$

Solution. Note $\triangle$ and $\triangledown$ are binary operations on S .

i) $1\Delta 1 = 1$ ii) $(1\Delta 1)\Delta 3 = 1\Delta 3 = 2$ iii) $(1\Delta 1)\nabla 1 = 1\nabla 1 = 1$ iv) $(3\nabla 2)\Delta 3 = 1\Delta 3 = 2$.

Example Let $\odot$ be a binary operation on $\mathbb{Z}$ defined by $a \odot b = 2b + a$.

Find $i)\ 2 \odot 3 \quad ii)\ 4 \odot 3 \quad iii)\ 3 \odot 4 \quad iv)\ (1 \odot (-3)) \quad v) \quad (2 \odot 1) \odot -3$.

Solution. $i)\ 2 \odot 3 = 2.3 + 2 = 8 \quad ii)\ 4 \odot 3 = 2.3 + 4 = 10$

$iii)\ 3 \odot 4 = 2.4 + 3 = 11 \quad iv)\ 2 \odot (1 \odot (-3)) = 2 \odot (-5) = -10 + 2 = -8$

$v) \quad (2 \odot 1) \odot (-3) = 4 \odot (-3) = -6 + 4 = -2$

Definition. (Identity element) Let $*$ be a binary operation on a set A . An element $e \in A$ is an identity element for $*$ if $e * a = a = a * e$ for all $a \in A$.

Example. 1. 0 is an identity element for addition on $\mathbb{Z}$.

2. 1 is an identity element for multiplication $\mathbb{Z}$.

3.There is no identity element for subtraction on $\mathbb{Z}$. To see this ,assume there is $e \in \mathbb{Z}$ such that

$a - e = a = e - a$ for all $a \in A$. Then with $a = 1$ we get

$1 - e = 1 = e - 1$ .That is

$1 - e = 1$ and also $1 = e - 1 \rightarrow e = 0$ and $e = 2$, which is false.

Hence There is no identity element for subtraction on $\mathbb{Z}$.

3. Consider the power set $P(A)$ of a set A. Since

$B \cup \varnothing = B = \varnothing \cup B$ for all $B \in P(A)$, $\varnothing$ is an identity element for the binary operation $\cup$.

$A \cap B = B = B \cap A$ for $B \in P(A)$, A is an identity element for the binary operation $\cap$.

Theorem (Uniqueness of identity element)

Let $*$ be a binary operation on a set A. If e and f are identity element for $*$. Then $e = f$.

Proof. Since e is an identity element , $f = e * f$. Again since f is an identity element we have $e * f = e$ .Thus e = f.

Definition.(Inverse). Let $*$ be a binary operation on a set A and has an identity element e for $*$. Let $x \in A$. We say an element y of A is an inverse for x if

$x * y = e = y * x$.

In this case we say x is invertible.

Example 1. Addition (+) on $\mathbb{Z}$ .Every element x in $\mathbb{Z}$ has an inverse under addition ,namely $-x$.

2. Multiplication on $\mathbb{N}$: 1 is only element that has an inverse for multiplication and its inverse is 1 since 1.1=1.

3.Multilpication on $\mathbb{Q}$: Every element $x \neq 0$ of $\mathbb{Q}$ has a n inverse for multiplication , namely $\frac{1}{x}$.

Definition. Let $*$ be a binary operation on a set A. We say

1. $*$ is associative if for all elements a,b,c in A, $a*(b*c)=(a*b)*c$.

2. $*$ is commutative if for all elements a,b in A, $a*b=b*a$.

Example. 1. $+$ and . are associative binary operations on $\mathbb{Z}$.

2.Let $A=\{1,2,3\}$ and let Δ be defined by the following table

Δ	1	2	3
1	3	1	2
2	1	2	3
3	2	3	1

a) Is Δ commutative ?

b) What is the identity element for Δ ?

c.) Which element s of A are invertible under Δ

Solution. a) Yes ,(Check that it is symmetric with respect to the diagonal)

$1\Delta 2 = 2\Delta 1$, $1\Delta 3 = 3\Delta 1$,$2\Delta 3 = 3\Delta 2$..

b) 2 is the identity element. (the elements in the row along 2 and the elements in the column under 2 are the same.)

c. all are invertible.

Theorem. Let $*$ be an associative binary operation on a A set with identity element e. If $x \in A$ has an inverse under $*$, then its inverse is unique. That is if y and z are inverses of x then $y = z$.

Proof. by the definition of inverse $x * y = e = y * x$ and $x * z = e = z * x$.

$y = y * e = y * (x * z) = (y * x) * z = e * z = z$ (Since $*$ is associative and e is the identity element)

$\therefore y = z$.

Example. Determine whether Δ is associative ,commutative operation on $\mathbb{Z}$. Check for identity element.

$i) x\Delta y = x + y + x^2 y \quad ,ii)\ x\Delta y = 2x + 2y \quad iii)\ x\Delta y = x + y - 3$

Solution.

$i)\ x\Delta y = 2x + 2y \quad ii)\ x\Delta y = x + y - 3$

Solution .i) $x\Delta y = 2x + 2y$

a)to check Δ is associative. We calculate $x\Delta(y\Delta z)$ and $(x\Delta y)\Delta z$.

$x\Delta(y\Delta z) = x\Delta(2y + 2z) = 2x + 2(2y + 2z) = 2x + 4y + 4z$

and $(x\Delta y)\Delta z = (2x + 2y)\Delta z = 2(2x + 2y) + 2z = 4x + 4y + 2z$.

$x\Delta(y\Delta z) = (x\Delta y)\Delta z \Leftrightarrow 2x + 4y + 4z = 4x + 4y + 2z \Leftrightarrow 2x - 2z = 2z \Leftrightarrow x = z$

Thus if $x \neq z$ then $x\Delta(y\Delta z) \neq (x\Delta y)\Delta z$. Hence Δ is not associative.

As a counter example take $x = 1, y = 1, \quad z = 2$ .we have

$1\Delta(1\Delta 2) = 1\Delta(2 + 4) = 1\Delta 6 = 2 + 2.6 = 14$

$(1\Delta 1)\Delta 2 = (2 + 2)\Delta 2 = 4\Delta 2 = 2.4 + 2.2 = 12$

Thus $1\Delta(1\Delta 2 \neq (1\Delta 1)\Delta 2$.

b)To Check Δ is commutative . $x\Delta y = 2x + 2y = 2y + 2x = y\Delta x$.Thus Δ is commutative.

c. To Check existence of identity element. We know that if there is an identity element e it is unique

Suppose $x\Delta e = x$ for all $x \in \mathbb{Z}$. Then

$x\Delta e = x \to 2x + 2e = x \to 2e = -x$ .Thus e depends on x . that is , e is not unique. Thus Δ has no identity element.

ii) $x\Delta y = x + y - 3$.

a) Associative

$x\Delta(y\Delta z) = x\Delta(y + z - 3) = x + (y + z - 3) - 3 = x + y + z - 6$

$(x\Delta y)\Delta z = (x + y - 3)\Delta z = x + y - 3 + z - 3 = x + y + z - 6 = x\Delta(y\Delta z)$ for all $x, y, z \in \mathbb{Z}$.

Thus Δ is associative.

b)commutative . $x\Delta y = x + y - 3 = y + x - 3 = y\Delta x$ for all $x, y \in \mathbb{Z}$.

Thus Δ is commutative.

c)Existence of identity. Suppose there is $e \in \mathbb{Z}$ such that $x\Delta e = x$ for all $x \in \mathbb{Z}$. We have,

$x\Delta e = x \Rightarrow x + e - 3 = x \Rightarrow e = 3$. Thus 3 is the identity element for Δ.

d) Let $x \in \mathbb{Z}$.To find the inverse of x. Suppose y is the inverse of x .Then we have

$x\Delta y = 3 \Rightarrow x + y - 3 = 3 \Rightarrow y = 6 - x \in \mathbb{Z}$. Thus the inverse of x is $6 - x$.

Thus every element in $\mathbb{Z}$ has an inverse with respect to Δ.

For example the inverse of 7 is 6-7 = 1.

Example .Let $\mathbb{Z}_n = \{0,1,2,\cdots,n-1\}$ $n \geq 1, n \in \mathbb{N}$ .We define $\oplus_n$ and $\odot_n$ on $\mathbb{Z}_n$ as follows

For all $a,b \in \mathbb{Z}_n$

1 . $a \oplus_n b = r$ where r is the remainder obtained when $a+b$ is divided by n. That is, $a+b = kn + r$ for some $k \in \mathbb{Z}$ and $r \in \{0,1,2,\cdots,n-1\} = \mathbb{Z}_n$

2. $a \odot_n b = s$ **where** s **is the remainder obtained when** ab **is divided by** n

That is, $ab = cn + s$ for some $c \in \mathbb{Z}$ and $0 \leq s \leq n-1$ (by Division algorithm)

$\oplus_n$ is called addition modulo n and $\odot_n$ multiplication modulo n .Both are binary operations on $\mathbb{Z}_n$

As an example consider $\mathbb{Z}_4 = \{0,1,2,3\}$, here $n = 4$ .Addition and multiplication modulo 4 are given by the tables:

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$2 \oplus_4 3 = 1$ since $2+3 = 4.1+1$. (r = 1)

$2 \oplus_4 2 = 0$ since $2 = 2 = 4.1+0$ (r = 0)

$2 \oplus_4 1 = 3$ since $2+1 = 4.0+3$ (r =3).

Definition.

1. A semi-group is a set with a binary operation that is associative.

2. A monoid is a set with a binary operation that is associative and has an identity element.

That is, a monoid is a semi-group having an identity element.

3. A group is a monoid in which every element in the set is invertible (has inverse)

Example .

1. $\mathbb{N} = \{1, 2, 3, \cdots,\}$ under addition is a semi-group but not a monoid.

2. $\mathbb{Z}$ under multiplication is monoid but not a group.

3. $\mathbb{Q}$ under multiplication is a monoid but not a group.

4. $\mathbb{Z}$ under addition is a group.

5. $\mathbb{Q}$ under addition is group.

6. $\mathbb{Z}_n$ under addition modulo n is a group .

Exercise

1. Determine which of the following are monoid , groups.

a) The set {-1 ,1} under multiplication.

b)The P(A) under union and $A \neq \varnothing$.

c) The P(A) under intersection and $A = \varnothing$.

d) $\mathbb{Z}$, under Δ where $a\Delta b = a + b - 1$

2.Give an addition and multiplication table for $\mathbb{Z}_5$.

3. Let G be the set of all functions $f:\mathbb{R}\to\mathbb{R}$. Show the G together with the usual addition functions is a group. Show that is not a group under multiplication of function.