2.7

Functions

Function: Let A and B be two sets. A relation f from A to B is called a function if for every $a \in A$ there is a unique element $b \in B$ such that $(a, b) \in f$.

Note: A relation must satisfy the following two additional conditions to qualify to be a function.

(i) The domain of f must be A (not merely a subset of A)

(ii) The second requirement of uniqueness can be expressed as

$$\big((\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{f}\big) \wedge \big((\boldsymbol{x}, \boldsymbol{z}) \in \boldsymbol{f}\big) \Rightarrow \boldsymbol{y} = \boldsymbol{z}$$

Terms such as *map* (or *mapping*), *operation*, *transformation* and *correspondence* are used as synonyms for *function*.

The notations $\boldsymbol{f} : \boldsymbol{A} \longrightarrow \boldsymbol{B}$ or $\boldsymbol{A} \xrightarrow{\boldsymbol{f}} \boldsymbol{B}$ are used to express f as a function from A to B.

For a function $\boldsymbol{f}: \boldsymbol{A} \longrightarrow \boldsymbol{B}$ if $(x, y) \in f$, then x is called the **argument** and the corresponding y is called the **image of $\boldsymbol{x}$ under $\boldsymbol{f}$**.

Instead of writing $(x, y) \in f$, it is customary to write $y = f(x)$ and to call $\boldsymbol{y}$ as the **value of the function $\boldsymbol{f}$ at $\boldsymbol{x}$**. The domain of f is denoted by $\boldsymbol{D_f}$ and $D_f = A$.The range of f is denoted by $\boldsymbol{R_f}$ and

$$\boldsymbol{R_f} = \{\boldsymbol{y} \in \boldsymbol{B} | (\exists \boldsymbol{x} \in \boldsymbol{A}) \wedge \big(\boldsymbol{y} = \boldsymbol{f}(\boldsymbol{x})\big)\}$$

Note that $R_f \subseteq B$ and B is called the **codomain** of f.

Since a function is a relation, we can write a relation matrix or draw a graph to represent it when its domain and co domain are finite sets.

Note: From the definition of a function it follows that every row of its relation matrix have only one entry 1 and all other entries in the rows are 0's.

When the domain and co domain of a function f are infinite, the correspondence can be expressed more easily by a rule.

For example, $f(x) = x^2$, $x \in \boldsymbol{R}$ represents a function $\{(x, x^2) | x \in \boldsymbol{R}\}$ where $\boldsymbol{R}$ is the set of real numbers and $f : \boldsymbol{R} \longrightarrow \boldsymbol{R}$**.**

Note: A program written in a high-level language is transformed (or mapped) into a machine language by a compiler. Similarly, the output from a computer is a function of its input**.**

Restriction of a function: If $\boldsymbol{f : A \longrightarrow B}$ and $X \subseteq A$, then $f \cap (X \times B)$. (i.e., the intersection of the ordered pairs of f and $X \times B$) is a function from X to B called the **restriction of $\boldsymbol{f}$ to $\boldsymbol{X}$** and is written as $\boldsymbol{f/X}$. If g is the restriction of f then f is called the **extension** of g.

Note: Notice that $\boldsymbol{(f/X): X \longrightarrow B}$ is such that for any $x \in X$, $(f/X)(x) = f(x)$. The domain of f/X is X, while that of f is A.

If g is a restriction of f then $D_g \subseteq D_f$ and $g(x) = f(x)$, $\forall x \in D_g$ and as relations $g \subseteq f$.

Example: Let $\boldsymbol{f : R \longrightarrow R}$ be given by $\boldsymbol{f(x) = x^2}$. We have $\boldsymbol{N \subset R}$ and

$$\boldsymbol{f/N = \{(1,1), (2,4), (3,9), (4,16), \ldots\}}$$

Equality of functions: Equality of functions can be defined in terms of the equality of sets, since functions are sets of ordered pairs. Note that this definition also requires that equal functions have the same domain and the same range.

It is known that not all possible subsets of $A \times B$ are functions from A to B.

We know that not all relations from A to B are functions from A to B. The collection of all those relations from A to B which are functions from A to B is denoted by $\boldsymbol{B^A}$.

Example: Let $\boldsymbol{A = \{a, b, c\}}$ and $\boldsymbol{B = \{0, 1\}}$. Write all functions from $\boldsymbol{A}$ to $\boldsymbol{B}$

Solution: We have $A \times B = \{(a, 0), (a, 1), (b, 0), (b, 1), (c, 0), (c, 1)\}$

and there are 2^6 relations from A to B. Of these, only the following 2^3 relations are function from A to B:

$f_0 = \{(a, 0), (b, 0), (c, 0)\}$

$f_1 = \{(a, 0), (b, 0), (c, 1)\}$

$f_2 = \{(a, 0), (b, 1), (c, 0)\}$

$f_3 = \{(a, 0), (b, 1), (c, 1)\}$

$f_4 = \{(a, 1), (b, 0), (c, 0)\}$

$f_5 = \{(a, 1), (b, 0), (c, 1)\}$

$f_6 = \{(a, 1), (b, 1), (c, 0)\}$

$f_7 = \{(a, 1), (b, 1), (c, 1)\}$

The number of function from $\boldsymbol{A}$ to $\boldsymbol{B}$ when $\boldsymbol{A}$, $\boldsymbol{B}$ are finite

Let A and B be finite sets with m and n elements respectively. Since the domain of any function from A to B is A, there are exactly m ordered pairs in each of the functions. Further, any element $x \in A$ can have any one of the n elements of B as its image; therefore, there are $n \times n \times \ldots \times n$ (m times)$= n^m$ possible distinct functions.

Note: The number n^m explains why the notation B^A is used to represent the set of all function from A to B. The same notation is used even when A or B are infinite sets.

A mapping $f : A \longrightarrow B$ is called **onto** (**surjective** or **surjection**) if the range $\boldsymbol{R_f = B}$; otherwise, it is called an **into function**.

A mapping $f : A \longrightarrow B$ is called **one-to-one** (**injective** or **1-1**) if distinct elements of A are mapped into distinct elements of B. In other words, f is one-to-one if

$$\boldsymbol{x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)}$$

or equivalently

$$\boldsymbol{f(x_1) = f(x_2) \Longrightarrow x_1 = x_2}$$

Note: Let A and B be finite sets. A mapping $f : A \longrightarrow B$ is one-to-one only if $|\boldsymbol{A}| \leq |\boldsymbol{B}|$.

A mapping $f : A \longrightarrow B$ is called **bijective** if it is both *injective* and *surjective*. Such a mapping is also called a **one-to-one correspondence** between A and B.

Note: For $f : A \longrightarrow B$ to be bijective, when A, B are finite, requires that $|A| = |B|$.

Composition of functions

The operation of composition of relations can be extended to functions.

Let $\boldsymbol{f : A \longrightarrow B}$ and $\boldsymbol{g : B \longrightarrow C}$ be two functions. The **composite relation** $g \circ f$ such that

$$\boldsymbol{g \circ f = \{(x, z) | (x \in A) \wedge (z \in C) \wedge (\exists y)(y \in B \wedge y = f(x) \wedge z = g(y))\}}$$

is called the **composition** of functions (or **relative product** of functions f and g. More precisely, $g \circ f$ is called the **left composition** of g with f.Note that, **if $\boldsymbol{R_f \subseteq D_g}$ then $\boldsymbol{g \circ f}$ is nonempty, otherwise $\boldsymbol{g \circ f}$ is empty .**

$\boldsymbol{g \circ f}$ is a function from $\boldsymbol{A}$ to $\boldsymbol{C}$: Assume that $g \circ f$ is not a function. Suppose that $g \circ f$ is not empty. That is assume that (x, z_1) and (x, z_2) are both in $g \circ f$. That is there is an element $y \in B$ such that $y = f(x)$ and $z_1 = g(y)$; also $z_2 = g(y)$. This shows that $(y, z_1) \in g$ and $(y, z_2) \in g$. Since g is a function, this is not possible. Thus, $g \circ f$ is a functioin.

Any function g for which $g \circ f$ can be formed is said to be **left-composable** with the function f. In such a case, $\boldsymbol{(g \circ f)(x) = g(f(x))}$, where x is in the domain of $g \circ f$.

Associativity of the composition of functions: Let $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$. Then the composite functions $g \circ f : A \longrightarrow C$ and $h \circ g : B \longrightarrow D$ can be formed. Other composite functions such as $h \circ (g \circ f) : A \longrightarrow D$ and $(h \circ g) \circ f : A \longrightarrow D$ can also be formed. Since each function is a relation and the composition of relations is associative; the composition of functions is also associative.

Therefore $\boldsymbol{h \circ (g \circ f) = (h \circ g) \circ f}$.

Since the composition of functions is associative we may drop parenthesis in writing the associativity, $i.e.$,

$$\boldsymbol{h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f}$$

Example: Let $\boldsymbol{A = \{1, 2, 3\}}$, $\boldsymbol{B = \{p, q\}}$ and $\boldsymbol{C = \{a, b\}}$. Let $\boldsymbol{f : A \longrightarrow B}$ be $\boldsymbol{f = \{(1, p), (2, p), (3, q)\}}$ and $\boldsymbol{g : B \longrightarrow C}$ be $\boldsymbol{g = \{(p, b), (q, b)\}}$. Find $\boldsymbol{g \circ f}$.

Solution: We have $\boldsymbol{A \xrightarrow{f} B \xrightarrow{g}}$, $\boldsymbol{A \xrightarrow{g \circ f} C}$

$$\boldsymbol{g \circ f = \{(1, b), (2, b), (3, b)\}}$$

Example: Let $\boldsymbol{A = \{1, 2, 3\}}$ and $\boldsymbol{f, g, h}$ and $\boldsymbol{s}$ be functions on $\boldsymbol{A}$ given by

$\boldsymbol{f = \{(1, 2), (2, 3), (3, 1)\}}$, $\boldsymbol{g = \{(1, 2), (2, 1), (3, 3)\}}$

$\boldsymbol{h = \{(1, 1), (2, 2), (3, 1)\}}$, $\boldsymbol{s = \{(1, 1), (2, 2), (3, 3)\}}$**. Find $\boldsymbol{f \circ g}$, $\boldsymbol{g \circ f}$, $\boldsymbol{f \circ h \circ g}$, $\boldsymbol{s \circ g}$, $\boldsymbol{g \circ s}$, $\boldsymbol{s \circ s}$ and $\boldsymbol{f \circ s}$.**

Solution:

$f \circ g = \{(1,3), (2,2), (3,1)\}$, $g \circ f = \{(1,1), (2,3), (3,2)\}$

Note that $f \circ g \neq g \circ f$.

$f \circ h \circ g = \{(1,3), (2,2), (3,2)\}$

$s \circ g = \{(1,2), (2,1), (3,3)\} = g = g \circ s$

Note that $s \circ s = s$, $f \circ s = s$.

Example: Let $(x) = x + 2$, $g(x) = x - 2$ and $h(x) = 3x$ for $x \in R$. Find $g \circ f$, $f \circ g$, $g \circ g$, $f \circ h$, $h \circ g$, $h \circ f$ and $f \circ h \circ g$.

Solution:

(i) We have $(g \circ f)(x) = g\big(f(x)\big) = g(x+2) = (x+2) - 2 = x$.
Therefore, $g \circ f = \{(x, x) | x \in \boldsymbol{R}\}$

(ii) $(f \circ g)(x) = f\big(g(x)\big) = f(x-2) = (x-2) + 2 = x$.
Therefore, $f \circ g = \{(x, x) | x \in \boldsymbol{R}\} = g \circ f$.

(iii) $f \circ f = \{(x, x+4) | x \in \boldsymbol{R}\}$

(iv) $g \circ g = \{(x, x-4) | x \in \boldsymbol{R}\}$

(v) $(f \circ h)(x) = f\big(h(x)\big) = f(3x) = 3x + 2$

(vi) $(h \circ g)(x) = h\big(g(x)\big) = h(x-2) = 3(x-2) = 3x - 6$
Therefore, $h \circ g = \{(x, 3x-6) | x \in \boldsymbol{R}\}$.

(vii) $(h \circ f)(x) = h\big(f(x)\big) = h(x+2) = 3(x+2) = 3x + 6$
Therefore, $h \circ f = \{(x, 3x+6) | x \in \boldsymbol{R}\}$.

(viii) $\big((f \circ h) \circ g\big)(x) = (f \circ h)\big(g(x)\big) = f\big(h(x-2)\big) = f(3x-6)$
$= 3x - 6 + 2 = 3x - 4$
Therefore, $(f \circ h) \circ g = \{(x, 3x-4) | x \in \boldsymbol{R}\} = (f \circ h) \circ g = f \circ h \circ g$.

Example: Let $\boldsymbol{f} : \boldsymbol{R} \longrightarrow \boldsymbol{R}$ be given by $\boldsymbol{f}(\boldsymbol{x}) = -\boldsymbol{x}^2$ and $\boldsymbol{g} : \boldsymbol{R}^+ \longrightarrow \boldsymbol{R}^+$ be given by $(\boldsymbol{x}) = \sqrt{\boldsymbol{x}}$, where $\boldsymbol{R}^+$ is the set of non-negative real numbers. Find $\boldsymbol{f} \circ \boldsymbol{g}$. Is $\boldsymbol{g} \circ \boldsymbol{f}$ defined.

Solution:

(i) Note that $R_g = \boldsymbol{R}^+ \subseteq \boldsymbol{R} = D_f$. Therefore, $f \circ g$ is defined and
$(f \circ g)(x) = f\big(g(x)\big) = f\big(\sqrt{x}\big) = -x$, for $x \in \boldsymbol{R}^+$.

(ii) Note that R_f is the set of nonpositive real numbers and it is not included in domain of g. Therefore, $g \circ f$ is not defined.

Inverse function

The converse of a relation R from A to B is defined to be a relation $\bar{R}$ from B to A such that $(y, x) \in \bar{R} \Leftrightarrow (x, y) \in R, i.e.$, the ordered pairs of $\bar{R}$ are obtained from those of R by simply interchanging the components.

Let $\bar{f}$ be the converse of f, where $\boldsymbol{f : A \longrightarrow B}$ is considered as a relation from A to B. Now $\bar{f}$ may not be a function, because the $D_{\bar{f}}$ may not be B but only a subset of B.

$\bar{f}$ may not be a function from R_f to A because it may not satisfy the uniqueness condition. For example, (x_1, y) and (x_2, y) may be in f, so that (y, x_1) and (y, x_2) will be in $\bar{f}$.

For a function $f : A \longrightarrow B$, $\bar{f}$ is a function only if f is one-to-one. But this condition does not guarantee that $\bar{f}$ will be a function from B to A. However, if is bijective then $\bar{f}$ is a function from B to A. In such case $\bar{f}$ is written as $\boldsymbol{f^{-1}}$ so that $\boldsymbol{f^{-1} : B \longrightarrow A}$ and $\boldsymbol{f^{-1}}$ is called the **inverse** of the function f. If f^{-1} exists then f is said to be **invertible**.

Note: If f is a bijective function from A to B then $\boldsymbol{f^{-1} : B \longrightarrow A}$ exists and f^{-1} is also bijective.

A map $\boldsymbol{I_A : A \longrightarrow A}$ is called an **identity map** if $I_A = \{(x, x) | x \in A\}$.

Theorem

(a) For any function $\boldsymbol{g : A \longrightarrow A}$, the function $I_A \circ g = g \circ I_A = g$.
For any $x \in A$, $(I_A \circ g)(x) = I_A\big(g(x)\big) = g(x)$.Therefore $I_A \circ g = g$.
Similarly $g \circ I_A = g$.

(b) If $\boldsymbol{f : A \longrightarrow B}$ and $\boldsymbol{g : B \longrightarrow A}$, then $g = f^{-1}$ only if $g \circ f = I_A$ and $f \circ g = I_B$.

(c) If $\boldsymbol{f : A \longrightarrow B}$ is invertible then $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_B$.

(d) If $\boldsymbol{f : A \longrightarrow B}$ and $g : B \longrightarrow A$ are bijective then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Theorem: Let F_A be the collection of all bijective function on a nonempty set A. Then the following properties hold:

i) For any , $g \in F_A$, $f \circ g$ and $g \circ f$ are also in F_A. This is called ***closure property*** of the operation of composition.

ii) For any $f, g, h \in F_A$,$(\boldsymbol{f} \circ \boldsymbol{g}) \circ \boldsymbol{h} = \boldsymbol{f} \circ (\boldsymbol{g} \circ \boldsymbol{h})$
$i.e.$, the composition is associative.

iii) There exists a function $I_A \in F_A$ called the ***identity map*** such that
$\boldsymbol{I_A} \circ \boldsymbol{f} = \boldsymbol{f} \circ \boldsymbol{I_A} = f$ for all $f \in F_A$.

iv) For every $f \in F_A$ there exists an inverse $f^{-1} \in F_A$ such that
$$\boldsymbol{f} \circ \boldsymbol{f^{-1}} = \boldsymbol{f^{-1}} \circ \boldsymbol{f} = \boldsymbol{I_A}.$$

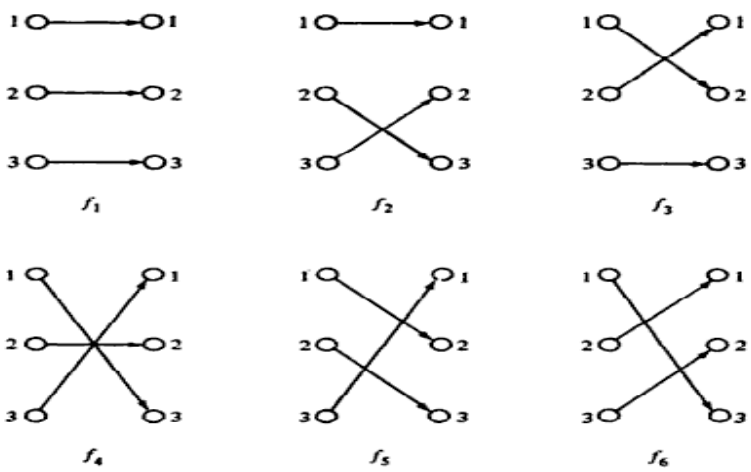
Note:

(1) Closure and associative properties of the composition of maps hold for all the functions of $\boldsymbol{A^A}$ (i.e., for all function on A) and not only for the functions of F_A.

(2) If A is a finite set with n elements $|F_A| = n!$

Example: Let $A = \{1, 2, 3\}$. Find all elements of F_A and find the inverse of each element.

Solution: The following are the $3! = 6$ functions $f_1, f_2, \dots, f_6$ of F_A, where $A = \{1,2,3\}$.



Note that

(a) f_1 is the identity map of F_A. Therefore, $f_1 \circ f_i = f_i \circ f_1 = f_i$, for $i = 1,2, \ldots ,6$.

(b) $f_2 \circ f_2$ maps 1,2 and 3 onto 1,2 and 3 respectively; Therefore, $f_2 \circ f_2 = f_1$. Thus, ${f_2}^{-1} = f_2$, similarly ${f_3}^{-1} = f_3$, ${f_4}^{-1} = f_4$.

(c) $f_5 \circ f_6 = f_1$ and $f_6 \circ f_5 = f_1$. Thus ${f_5}^{-1} = f_6$ and ${f_6}^{-1} = f_5$

For example, $f_4 \circ f_3$ is done in the following way

$$(f_4 \circ f_3)(1) = f_4\big(f_3(1)\big) = f_4(2) = 2$$
$$(f_4 \circ f_3)(2) = f_4\big(f_3(2)\big) = f_4(1) = 3$$
$$(f_4 \circ f_3)(3) = f_4\big(f_3(3)\big) = f_4(3) = 1$$

Thus $f_4 \circ f_3 = f_5$.

Other compositions of elements of F_A are given in the following table, in which $f_i \circ f_j$ is entered at the intersection of the i^{th} row and j^{th} colum:

Table 1

$*$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_4
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_2	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

Binary operations

We now restrict our discussion to functions from a set $A \times A$ to A, or more generally to a function from $A^n = A \times A \times \ldots \times A(n \text{ times})$ to A where n is a given fixed natural number.

Let A be non-empty set and f be a mapping

$$\boldsymbol{f : A \times A \longrightarrow A}$$

Then f is called a **binary operation** on A.

In general, a mapping $\boldsymbol{f : A^n \longrightarrow A}$ is called an $\boldsymbol{n}$**-ary** operation on A and n is called the **order** of the operation.

For $n = 1$, $\boldsymbol{f : A \longrightarrow A}$ is called a **unary** operation.
The operations of addition, subtraction, and multiplication are binary operations on $\boldsymbol{Z}$ and also on $\boldsymbol{R}$. The operation of division is not a binary operation on these sets.
The operations of set union and intersections are binary operations on the set of subsets of a universal set. They are binary operations on the power set of any set. The operation of complementation is a unary operation on these sets.

The composition of bijective functions from a set A to itself (i.e., on F_A) is a binary operation.

The operations of conjunction and disjunction are binary operations on the set of propositions as well as of the set of well-formed formulas in propositional logic. The operation of negation is a unary operation on these sets.

Sometimes a binary operation can be conveniently specified by a table called **composition table**.(for example see Table 1).

Example: Construct the composition tables for the binary operations union and intersection for the power set $\boldsymbol{P(A)}$, where $\boldsymbol{A = \{a, b\}}$.

Solution: We have $A = \{a, b\}$ and $P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

Let $B_0 = \phi$, $B_1 = \{b\}$, $B_2 = \{a\}$, $B_3 = \{a, b\} = A$. Then $P(A) = \{B_0, B_1, B_2, B_3\}$.

The composition tables for ∪ and ∩ are given below:

Table 2

∪	B_0	B_1	B_2	B_3
B_0	B_0	B_1	B_2	B_3
B_1	B_1	B_1	B_3	B_3
B_2	B_2	B_3	B_2	B_3
B_3	B_3	B_3	B_3	B_3

Table 3

∩	B_0	B_1	B_2	B_3
B_0	B_0	B_0	B_0	B_0
B_1	B_0	B_1	B_0	B_1
B_2	B_0	B_0	B_2	B_2
B_3	B_0	B_1	B_2	B_3

It is customary to denote a binary operation by a symbol (such as $+, -, \circ, *, \oplus, \cup, \cap, \vee, \wedge, \sim$, etc.,) **and the value of the operation (or function) by placing the operator between the two operands.**

For example, $\boldsymbol{f(x,y)}$ may be written as $\boldsymbol{xfy}$ or $\boldsymbol{x * y}$ or $\boldsymbol{x + y}$ as the case may be.

Properties of binary operations: Let A be any non-empty set. A binary operation $\boldsymbol{f : A \times A \longrightarrow A}$ is said to be

(i) **Commutative** if $f(x,y) = f(y,x)$, for all $x, y \in A$.

(ii) **Associative** if for every $x, y, z \in A$,

$$f(f(x,y),z) = f\big(x, f(y,z)\big)$$

(iii) **Distributive** if for every $x, y, z \in A$

$$f\big(x, g(y,z)\big) = g\big(f(x,y), f(x,z)\big)$$

If $*$ and $\circ$ denote the operations f and g respectively, the above properties respectively become

$$\boldsymbol{x * y = y * x}\text{, for all } \boldsymbol{x, y \in A}$$

$$\boldsymbol{(x * y) * z = x * (y * z)}\text{, for all } \boldsymbol{x, y, z}$$

$$\boldsymbol{x * (y \circ z) = (x * y) \circ (x * z)}$$

The operations of addition and multiplication over $\boldsymbol{R}$ are commutative and associative.

The operation of union and intersection over the power set of any sets are commutative and associative.

The operation of subtraction over $\boldsymbol{R}$ is not commutative.

The operation of composition of bijective maps on a set is not commutative.

The operation of multiplication is distributive over the addition in $\boldsymbol{R}$.

Both union and intersection of sets distributive over each other on the power set of any set.

Certain distinguished elements: Given a binary operation $*$ on a set A, we now define certain distinguished elements of A associated with the operation $*$. *Such elements may or may not exist*.

Identity element: Let $*$ be a binary operation on a set A. If there exists an element $e \in A$ such that

$$\boldsymbol{e * x = x * e = x}$$

for every $x \in A$, then e is called the **identity** with respect to $*$.

The element 0 is the identity for addition and 1 the identity for multiplication over $\boldsymbol{R}$. The empty set ϕ is the identity for the operation of union and the universal set U is the identity for the operation of intersection over the set of subsets of a universal set U.

The identity map I_A is the identity w.r.t the composition of bijective functions of F_A.

A contradiction (i.e., an identically false proposition) is an identity for disjunction, while a tautology is an identity for conjunction of propositions.

Zero element: Let $*$ be a binary operation on A.If there exists an element $0 \in A$ such that

$$\boldsymbol{0 * x = x * 0 = 0} \text{ for all } x \in A$$

then 0 is called the **zero** w.r.t to $*$,
the element 0 is the zero for multiplication on $\boldsymbol{R}$**.** The empty set $\emptyset$ is the zero for intersection and the universal set U is the zero for the union of subsets of a universal set U.

Idempotent element: Let $*$ be a binary operation on A. An element $a \in A$ is called **idempotent** w.r.t $*$, if $\boldsymbol{a * a = a}$**.**

The *identity* and *zero* elements w.r.t. a binary operation are idempotent. There may be other idempotent elements besides the identity and zero elements. Note that every set is idempotent w.r.t. to the operations of union and intersection.

Invertible elements and inverse elements: Let $*$ be a binary operation on A with the identity e. An element $a \in A$ is said to be invertible, if there is an element $x \in A$ such that

$$\boldsymbol{a * x = x * a = e}$$

Such an element x is called the **inverse** of a, it is denoted by a^{-1} and

$$\boldsymbol{a * a^{-1} = a^{-1} * a = e}.$$

By symmetry it follows that $(\boldsymbol{a^{-1}})^{\boldsymbol{-1}} = \boldsymbol{a}$

In many binary operation the identity element, if it exists, is invertible, since it is idempotent, the **identity element is its own inverse.**

The other invertible elements may or may not exist. For example, every real number $a \in \boldsymbol{R}$ has an inverse $-a \in \boldsymbol{R}$ for the operation of addition. Similarly, for the operation of multiplication, the inverse of every nonzero real number $a \in \boldsymbol{R}$ is $\frac{1}{a} \in \boldsymbol{R}$. In F_A, the set of all bijections on A ,every function is invertible for the operation of composition . Note that a zero element w.r.t. an operation is not invertible.

Cancelable element: Let $*$ be a binary operation on . An element $a \in A$ is called **cancellable** w.r.t $*$ if for every $x, y \in A$,

$$(\boldsymbol{a * x = a * y}) \vee (\boldsymbol{x * a = y * a}) \Longrightarrow (\boldsymbol{x = y})$$

Lemma: If the operation $*$ is associative and the element $\boldsymbol{a} \in \boldsymbol{A}$ is invertible, then $\boldsymbol{a}$ is cancellable.

***Proof*:** Let $x, y \in A$ and $a * x = a * y$ or $x * a = y * a$. Suppose that $a * x = a * y$. Since a is invertible a^{-1} exists and $a * a^{-1} = a^{-1} * a = e$. Now $a^{-1}(a * x) = a^{-1}(a * y) \Longrightarrow (a^{-1} * a) * x = (a^{-1} * a) * y$ (since $*$ is associative)

$$\Longrightarrow e * x = e * y \Longrightarrow x = y$$

Thus, a is cancellable.

Note: There are cases where an element is cancellable but not necessarily invertible. For example in , any nonzero integer is cancellable with respect to multiplication, although the only integer which is invertible is 1

Characteristic function of a set

We shall discuss functions from the universal set U to the set $[0, 1]$.

Let U be a universal set and A be a subset of U. The function $\psi_A: E \longrightarrow [0, 1]$ defined by

$$\psi_A = \begin{cases} 1, & if\ x \in A \\ 0, & if\ x \notin A \end{cases}$$

is called the ***characteristic function*** of the set A.The following properties suggest how we can use the characteristic functions of the sets to determine set relations:

Properties of Characteristic function

Let A and B be any two subsets of a universal set U. Then the following hold for all $x \in U$

i) $\psi_A(x) = 0, \forall x \in U \Leftrightarrow A = \emptyset$
ii) $\psi_A(x) = 1, \forall x \in U \Leftrightarrow A = U$
iii) $\psi_A(x) \leq \psi_B(x), \forall x \in U \Leftrightarrow A \subseteq B$
iv) $\psi_A(x) = \psi_B(x), \forall x \in U \Leftrightarrow A = B$
v) $\psi_{A \cap B}(x) = \psi_A(x) * \psi_B(x), \forall x \in U$
vi) $\psi_{A \cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A \cap B}(x), \forall x \in U$
vii) $\psi_{A'}(x) = 1 - \psi_A(x), \forall x \in U$
viii) $\psi_{A-B}(x) = \psi_{A \cap B'}(x) = \psi_A(x) - \psi_{A \cap B}(x), \forall x \in U$

Note that the operations $\leq, =, +, *$ and $-$ used with the characteristic functions are arithmetic operations (because the values of the characteristic functions are always either 1 or 0). The above properties can easily be proved using the definition of characteristic functions. Following is the proof of (v):

$$\psi_{A \cap B}(x) = \psi_A(x) * \psi_B(x), \forall x \in U$$

We have $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$. For $x \in A \cap B$, we have

$$\psi_{A\cap B}(x) = 1, \psi_A(x) = 1, \psi_B(x) = 1$$

Therefore, for $x \in A \cap B, \psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x)$

For $x \notin A \cap B$, we have $x \in (A \cap B)'$ i.e., $x \in A' \cup B'$ i.e., $x \in A' \vee x \in B'$

For $x \notin A \cap B$, we have $\psi_{A\cap B}(x) = 0, \psi_A(x) = 0 \; or \; \psi_B(x) = 0$

Therefore, for $x \notin A \cap B, \psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x)$

Thus, we have $\psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x), \forall x \in U$

This proves (v).

Many set identities and other relations can be proved using characteristic functions and the usual arithmetic operations and relation.

Example: Show that $\boldsymbol{A \cap (B \cup C) = (A \cap B) \cup (A \cap C)}$

Solution: For all $x \in U$, we have

$$\begin{aligned}
\psi_{A\cap(B\cup C)}(x) &= \psi_A(x) * \psi_{B\cup C}(x) \quad \text{(by } (v)\text{)} \\
&= \psi_A(x) * \left(\psi_B(x) + \psi_C(x) - \psi_{B\cap C}(x)\right) \quad \text{(by } (vi)\text{)} \\
&= \psi_A(x) * \psi_B(x) + \psi_A(x) * \psi_C(x) - \psi_A(x) * \psi_{B\cap C}(x) \\
&= \psi_{A\cap B}(x) + \psi_{A\cap C}(x) - \psi_{A\cap(B\cap C)}(x) \\
&= \psi_{A\cap B}(x) + \psi_{A\cap C}(x) - \psi_{A\cap B\cap C}(x) \\
&= \psi_{A\cap B}(x) + \psi_{A\cap C}(x) - \psi_{(A\cap B)\cap(A\cap C)}(x) \\
&= \psi_{(A\cap B)\cap(A\cap C)}(x)
\end{aligned}$$

Thus, $\psi_{A\cap(B\cup C)}(x) = \psi_{(A\cap B)\cup(A\cap C)}(x)$, $\forall x \in U$

$\Longrightarrow A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ by (iv)

Example: **Show that** $(A')' = A$**.**

Solution: For all $x \in U$, $\psi_{(A')'}(x) = 1 - \psi_{A'}(x)$ (by (vii))

$= 1 - \big(1 - \psi_A(x)\big)$ (by (vii))

$= \psi_A(x)$

$\Longrightarrow (A')' = A$ (by (iv))

We can name the subsets of a finite set by using the characteristic function.

Consider $U = \{a, b, c\}$. The subsets of U are $\phi, \{a\}, \{b\}, \{a, b\}, \{a, c\}, \{b, c\}$ and $\{a, b, c\}$.

The values of the characteristic functions of these subsets are given in the following table

Table 4

x	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	$\{a, b, c\}$
a	0	1	0	0	1	1	0	1
b	0	0	1	0	1	0	1	1
c	0	0	0	1	0	1	1	1

The values of the characteristic function of any of the subsets of U are binary triples.

Let $B = \{000, 001, 010, 011, 100, 101, 110, 111\}$. Now Table 4 can be considered as a function from powerset of U to B. Clearly this function is bijective and therefore describes a one-to-one correspondence between the sets of $P(U)$ and B. The elements of B will be used to denote the corresponding subsets. That is $B_0 = \phi, B_1 = \{c\}, B_2 = \{b\}, B_3 = \{b, c\}, B_4 = \{a\}, B_5 = \{a, c\}, B_6 = \{a, b\}$, $B_7 = \{a, b, c\}$.

Note: The characteristic functions are associated with sets in the same way as the principle of specification (given in earlier module unit 1). We have seen that a one-to-one correspondence can be established between these characteristic functions and the sets. With the use of these characteristic functions, statements about sets and their operations can be represented in terms of *binary numbers* and so their manipulation on a computer becomes easier.

Hashing functions

Any transformation which maps the internal bit representation of a set of keys to a set of addresses is called a **hashing function**.

Various hashing functions are available. One commonly used hashing function is the **division method** (mod function)

Note that every key has a binary representation, which may be treated as a binary number. Let the numerical value of a key be denoted by k. Let n be a fixed positive integer (preferably a prime number), which is suitably chosen. The hashing function h defined by the division method is

$$\boldsymbol{h(k) = k(\mathbf{mod}\, n)}$$

i.e., $h(k)$ is the remainder of dividing k by n. Therefore, $h(k)$ is an element of the set $\{0,1,2,\dots,n-1\}$. Thus the hashing function maps the set of keys to the set of n addresses, $\{0,1,2,\dots,n-1\}$, which is called the **address set**.

Clearly, a hashing function maps different keys to the set of n addresses. Thus the set of records is partitioned into n equivalence classes. Those records which are mapped to the same address are in the same equivalence class.

It is therefore necessary to provide storage space for and also a method of finding the *collision* of or *overflow* records when more than one record has the same address. There are many techniques, called *collision resolution techniques* for this purpose.

Recursively defined functions

Sometimes it is difficult to define an object explicitly. However, it may be easy to define this object in terms of itself. This process is called **recursion**.

We use two steps to define a function f with the set of non-negative integers $W = \{0,1,2,3, \dots\}$ as its domain.

Let $a \in W$ and $A = \{a, a+1, a+2, \dots\}$. The **recursive** definition of a function f with domain A, consists of the following two parts, where $k \geq 1$.

Basis step: A few initial values of the function $f(a), f(a+1), \dots, f(a+k-1)$ are specified. An equation that specifies such initial values is an **initial condition**.

Recursive step: A formula to compute $f(n)$ from k preceding functional values $f(n-1), f(n-2), \dots, f(n-k)$ is made. Such a formula is a **recurrence relation** (or **recursion formula**).

Thus recursive definition of f consists of one or more (a finite number of) initial conditions and a recurrence relation.

Recursively defined functions are **well-defined**. That is, given any positive integer we can use the two parts of the definition to find the value of the function at that integer and that we obtain the same value no matter how we apply the two parts of the definition.

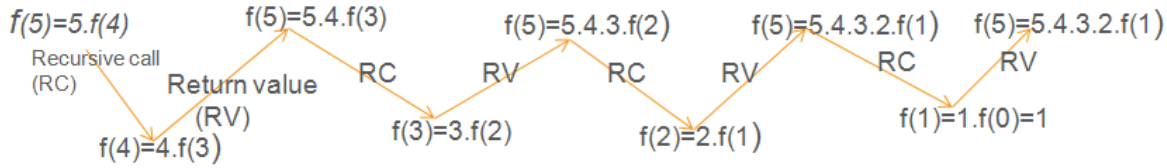
Example: Define recursively the factorial function f.

Solution: Recall that the factorial function f is defined by $(n) = n!$, where $f(0) = 1$. Since $! = n(n-1)!$, f can be defined recursively as follows:

$$\boldsymbol{f(0) = 1} \quad - \textbf{ Initial condition}$$

$$\boldsymbol{f(n) = n \cdot f(n-1)\,, n \geq 0} \quad - \textbf{ Recurrence relation}$$

Suppose we would like to compute $f(5)$ using recursive definition. We then continue to apply the recurrence relation until the initial condition is reached, as shown below:



P1:

List all possible functions from $A = \{a, b, c\}$ and $B = \{0, 1\}$ and indicate in each case whether the function is one-to-one and is onto.

Solution: We have $A = \{a, b, c\}$, $B = \{0,1\}$.

The number of functions from A to B is $|B|^{|A|} = 2^3 = 8$.

Since $|A| \not\leq |B|$, none of these functions is one-to-one. The functions are

$f_0 = \{(a, 0), (b, 0), (c, 0)\}$, into

$f_1 = \{(a, 0), (b, 0), (c, 1)\}$, onto

$f_2 = \{(a, 0), (b, 1), (c, 0)\}$, onto

$f_3 = \{(a, 0), (b, 1), (c, 1)\}$, onto

$f_4 = \{(a, 1), (b, 0), (c, 0)\}$, onto

$f_5 = \{(a, 1), (b, 0), (c, 1)\}$, onto

$f_6 = \{(a, 1), (b, 1), (c, 0)\}$, onto

$f_7 = \{(a, 1), (b, 1), (c, 1)\}$, onto

P2:

Let $f: A \longrightarrow B$, $g : B \longrightarrow C$ and $g \circ f \neq \phi$.

i. **If f, g are one-to-one then so is $g \circ f$.**
ii. **If f, g are onto then so is $g \circ f$.**
iii. **If f, g are bijective then so is $g \circ f$.**

Solution: We have $f: A \longrightarrow B$, $g : B \longrightarrow C$ and $g \circ f \neq \phi$.

(i) Suppose f, g are one-to-one. Now

$$(g \circ f)(x) = (g \circ f)(y) \Longrightarrow g\big(f(x)\big) = g\big(f(y)\big)$$
$$\Longrightarrow f(x) = f(y) \qquad \text{(since } g \text{ is one-to-one)}$$
$$\Longrightarrow x = y \qquad \text{(since } f \text{ is one-to-one)}$$

Thus, $g \circ f$ is one-to-one when f, g are one-to-one.

(ii) Suppose f, g are onto.

Let c be any element C. Since g is onto there exists an element $b \in B$ such that $g(b) = c$. Since f is onto, for the $b \in B$, there exists an element $a \in A$ such that $f(a) = b$. Thus, for any $c \in C$ there exists an element $a \in A$ such that

$$(g \circ f)(a) = g\big(f(a)\big) = g(b) = c$$

This shows that $g \circ f$ is onto.

(iii) Suppose f, g are bijective, $i.e.$, f, g are one-to-one and onto.

$\Longrightarrow g \circ f$ is one-to-one and onto$\Longrightarrow g \circ f$ is bijective.

P3:

Show that there exists a one–to – one mapping from $\boldsymbol{A \times B}$ to $\boldsymbol{B \times A}$. Is it also onto?

Solution:

We have nonempty sets A and B. Define a map $\boldsymbol{f}: \boldsymbol{A \times B} \longrightarrow \boldsymbol{B \times A}$ by $f(x, y) = (y, x)$

(i) *f is one – to – one:*

$$f(x_1, y_1) = f(x_2, y_2) \implies (y_1, x_1) = (y_2, x_2)$$
$$\implies y_1 = y_2 \text{ and } x_1 = x_2$$
$$\implies (x_1, y_1) = (x_2, y_2)$$

Thus, f is one – to – one.

(ii) *f is onto:*

Let (b, a) be any element of $B \times A$, i.e., $b \in B$ and $a \in A$. Clearly, $(a, b) \in A \times B$ and $f(a, b) = (b, a)$. This shows f is onto.

Note: There is a one – to – one correspondence between $A \times B$ and $B \times A$.

P4:

How many distinct binary operations are there on the set $\{0, 1\}$? Can you determine the number of distinct binary operations on any finite set?

Solution:

Let A be a nonempty finite set. A binary operation on A is a mapping $\boldsymbol{A \times A \longrightarrow A}$.

The number of distinct binary operations on A.

$=$ The number of distinct functions from $A \times A$ to A

$= |A|^{|A \times A|}$ (Since number of functions from X to Y is $|Y|^{|X|}$)

$= |A|^{|A|.|A|} = |A|^{|A|^2}$

The number of distinct binary operations on the set $A = \{0,1\}$ is

$|A|^{|A|^2} = 2^{2^2} = 16$

P5:

Let A and B be subsets of a universal set U. Then

$$\boldsymbol{\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A\cap B}(x),\ x \in U}$$

Solution:

Case (*a*)

$x \in A \cup B$. Then $\Psi_{A\cup B}(x) = 1$

$x \in A \cup B \Longrightarrow\ (x \in A,\ x \notin A \cap B)$ or $(x \in B,\ x \notin A \cap B)$ or $(x \in A \cap B)$

If $x \in A,\ x \notin A \cap B$, then $\psi_A(x) = 1\ ,\ \psi_B(x) = 0\ ,\ \psi_{A\cap B}(x) = 0$

and $\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A\cap B}(x)$

Similarly, in the case of $x \in B, x \notin A \cap B$.

If $x \in A \cap B$, then $x \in A,\ x \in B,\ \psi_A(x) = \psi_B(x) = \psi_{A\cap B}(x) = 1$ and $\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A\cap B}(x)$.

Case (b)

$x \notin A \cup B$. Then $\psi_{A\cup B}(x) = 0$

i.e., $\psi_{A\cup B}(x) = 0\ , \psi_A(x) = \psi_B(x) = 0$

$x \notin A \cup B \Longrightarrow x \notin A$ and $x \notin B$ (De Morgan's law)

Further, we have $\psi_{A\cap B}(x) = \psi_A(x).\psi_B(x) = 0$

Therefore$\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) = -\psi_{A\cap B}(x)$, for all $x \in U$.

P6:

Let A and B be subsets of a universal set U. Then

(i) $\psi_A(x) = 1 - \psi_A(x)$ **, for all** $x \in U$

(ii) $\psi_{A \oplus B}(x) = \psi_A(x) + \psi_B(x) - 2\,\psi_{A \cap B}(x)$

Solution:

(i) Let $x \in A'$. Then $\psi_{A'}(x) = 1$

$x \in A' \implies x \notin A \implies \psi_A(x) = 0$

Thus, $\psi_{A'}(x) = 1 - \psi_A(x)$

Let $\notin A'$. Then $\psi_{A'}(x) = 0$

$x \notin A' \implies x \in A \implies \psi_A(x) = 1$

Thus, $\psi_{A'}(x) = 1 - \psi_A(x)$

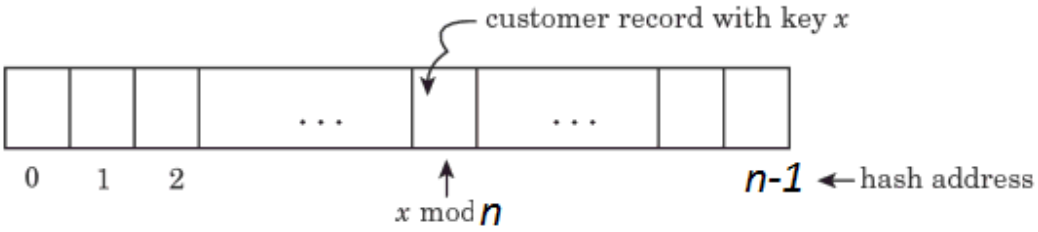
Therefore, $\psi_A(x) = 1 - \psi_A(x)$ for all $x \in U$

(ii) For all $x \in U$

$$\begin{aligned}
\psi_{A \oplus B} &= \psi_{(A-B)\,\cup\,(B-A)}(x) \\
&= \psi_{A-B}(x) + \psi_{B-A}(x) \quad \text{(since } A - B,\ B - A \text{ are disjoint)} \\
&= \psi_{A \cap B'}(x) + \psi_{B \cap A'}(x) \\
&= \psi_A(x)\ \psi_{B'}(x) + \psi_B(x)\,\psi_{A'}(x) \\
&= \psi_A(x)\left(1 - \psi_B(x)\right) + \psi_B(x)\left(1 - \psi_A(x)\right) \\
&= \psi_A(x) - \psi_A(x)\psi_B(x) + \psi_B(x) - \psi_A(x)\,\psi_B(x) \\
&= \psi_A(x) + \psi_B(x) - 2\,\psi_A(x)\,\psi_B(x).
\end{aligned}$$

P7:

Banks use nine – digit account numbers to create and maintain customer accounts. Customer records are stored in an array in a computer and can be accessed easily and quickly using their unique **keys**, which in this case are the account numbers. Access is often accomplished using the hashing function. $h(x) = k\ (mod\ n)$, where x denotes the key $(i.e.$, account number in this case) and n is the number of cells in the array $(n \in \{0, 1, 2, \dots, n-1\})$ and $h(x)$ denotes the **hash address** of the customer record with key x.



Let $n = 1009$ (prime number) and $x = 20763074$ (account number) .The corresponding record is stored in the location.

$$h(207630764) = (207630764)\ (mod\ 1009) = 762$$

Similarly $h(307620765) = 307620765(mod\ \ 1009) = 881$

Since the hashing function is not injective, theoretically different customer records can be assigned to the same location. For example

$$h(207630764) = 762 = h(208801204)$$

This results in a collision.
You will learn how to resolve collisions in a different topic in CSE.