Ganpat University- U. V. Patel College of engineering

Subject: 2BS3102 Discrete Mathematics & Probability

Unit-1 Algebraic Structures and Morphism

1. Set theory:

1.1 Set: Definite collection is set. We denote it by capital letter A, B,…etc.

For example: A= {1, 2, 3}, B= {Ram, Sham, a, 1,*}, M= { } =∅

Some standard sets:

$N = \{1,2,3, \dots\}$= set of natural numbers

$Z = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$=Set of integer

$Q = \left\{\frac{p}{q} : p \in Z, q \in N, q \neq 0\right\}$=Set of all rational numbers

R= set of real numbers

$C = \{a + ib : a, b \in R, i = \sqrt{-1}\}$ =Set of complex numbers

$Z_+ =$ Set of positive integers

1.1.1 Subset:

$A \subset B \; if \; \forall x \in A \Rightarrow x \in B$ (**Read as** A is subset of B if for each x belongs to A implies x belongs to B)

For example: (1) $N \subset Z \subset Q \subset R \subset C$

(2) $A = \{a, b, c\}$ and $B = \{a, b, c, d\}$ then $A \subset B$

(3) Empty set = ∅ is subset of every set.

1.1.2 Union and intersection:

$$A \cup B = \{x : x \in A \; or \; x \in B\}$$

$$A \cap B = \{x : x \in A \; and \; x \in B\}$$

For example: $A = \{1,2,3\}, B = \{2,3,4\}$ then $A \cup B = \{1,2,3,4\}$ and

$$A \cap B = \{2,3\}$$

1.2 Function or mapping:

Let A and B be two given two non-empty sets. Suppose there exists a correspondence denoted by f, which associates to each member of A, a unique member of B. Then f is called a function or a mapping of A to B.

Notation: $f: A \to B$ where A is domain and B is codomain.

1.2.1 Function as sets of ordered pair:

$f: A \to B$ is subset of $A \times B$ satisfying following conditions:

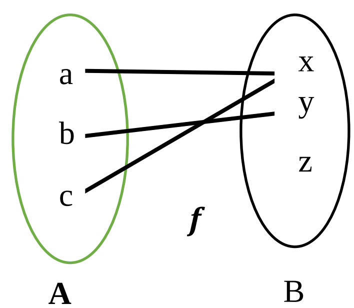
(i) $\forall\, a \in A, (a, b) \in f$ for some $b \in B$

(ii) If $(a, b) \in f$ and $(a, b') \in f \Rightarrow b = b'$

For example: If $A = \{a, b, c\}$ and $B = \{x, y, z\}$

$\Rightarrow A \times B = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z), (c, x), (c, y), (c, z)\}$

Here (1) $f = \{(a, x), (b, y), (c, x)\}$ is function.



Domain: A

Codomain: B

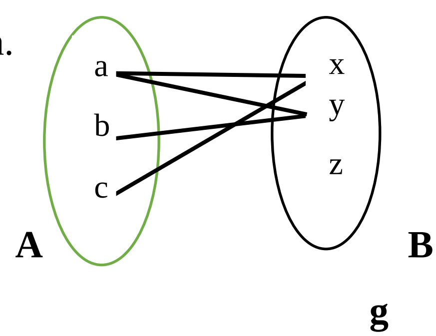
Range={x, y}

Onto: Codomain = Range (Note: f is not onto)

One one: different element have different image (Note: f is not one-one)

(2) g= $\{(a, x), (a, y), (b, y), (c, x)\}$ is NOT a function.

as a has two images(not unique image).



1.3 Relation: Relation R from A to B is subset of A × B.

Symbolically, R is a relation from A to B if and only if (iff)$R \subset A \times B$.

For example: If $A = \{a, b, c\}$ and $B = \{x, y, z\}$

$\Rightarrow A \times B = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, y), (c, x), (c, y), (c, z)\}$ then

(1) $R = \{(a, x), (a, y), (b, y), (c, x)\}$ is relation (Not function) from A to B.

Here we can write $aRx, aRy, \ldots$ (Read as a is related to x)

(2) Let P be set of person living in Mehsana. Then the statement "x is a son of y where x, y ∈ P" determines a relation R in P.

Obviously R ⊂ P × P.

(3) Let Z be a set of integer then the statement "x is less than y, x, y ∈Z" is relation R. R = {(x, y) / x ∈ Z, y∈ Z, x<y}⊂ Z × Z.

Clearly (3, 4) ∈ R or 3 R 4.

Also (2, 1) ∉ R.

(4) L=set of all lines in a plane. "x is parallel to y" is also relation.

(5) **Definition: Congruence modulo n (Residue modulo m)**

a is congruent to b modulo n if and only if $a - b$ is divisible by n.

i.e. $a = b(mod\ n)$ iff $n|\ (a - b)$

For example: R = {(x, y) / x ∈ Z, y∈ Z, x-y is divisible by 5} then R is relation in Z and known as congruence modulo 5 or residue modulo 5 relation.

Here 5| $x - y$ which means, x-y=5k for some k ∈ Z   Therefore x=5k+y.

Here (5, 10) ∈ R as 5| 5-10 i.e. 5| (-5). So we can say $5 = 10\ (mod\ 5)$

Also (6,11) ∈ R as 5 | 6-11 So we can say $6 = 11\ (mod\ 5)$

- If [a] is congruence class (mod m) (here class means equivalence class) then set of congruence classes (mod m) = Z_m (say)

Here $[a] = [b]\ if\ and\ only\ if\ a = b(mod\ m)$ then

$Z_5 = \{[0], [1], [2], [3], [4]\}\ or\ Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Note: (1) $^2/_6 = \frac{1}{3} = 0.333$ is value

(2) 2 | 6 read as "2 divides 6" is relation. (Note here remainder r will be 0)

6=2× k, for some k ∈Z here k=3

1.3 Binary operations:

Let A be a nonempty set. Then $A \times A = \{(a, b) | a, b \in A\}$. A function $*: A \times A \to A$ is said to be binary operation on A if $*(a, b) = a * b \in A$.

For example:

(1)'$+$'is binary operation on N.
(2)'$\times$' 'is binary operation on R.
(3)'$-$' is not binary operation on N.

(4) **"Addition modulo m"**

Let a and b be any two integer and m is a fixed positive integer, then addition modulo m is written as $a +_m b = r, 0 \le r < m$ where r is the least non-negative remainder when $a + b$ is divided by m.

For example:

(1) $17 +_3 4 = 0$ as if we divide 17+4=21 by 3 we have 0 as remainder.
(2) $15 +_2 4 = 1$

(5) **"Multiplication modulo p"**

Let a and b be any two integer and p is a fixed positive integer, then multiplication modulo p is written as $a \times_p b = r, 0 \le r < p$ where r is the least non-negative remainder when $a \times b$ is divided by p.

For example:

(3) $7 \times_3 4 = 1$ as if we divide 7×4=28 by 3 we have 1 as remainder.
(4) $5 \times_4 7 = 3$