

Integers

Well ordering principle :- Let, S be non empty subset of the set of natural numbers N then S has a smallest member.

Let, S be a non empty subset of N then α is smallest/least member of S if i) $\alpha \in S$, ii) $\alpha \leq a \forall a \in S$

If α be smallest member of S then $\alpha - 1 \notin S$

Principle of induction :- Let, S be a subset of N such that i) $1 \in S$
ii) $k \in S \Rightarrow k+1 \in S$

then $S = N$

Let, $t = N - S$, we shall show that t is empty that is $t = \emptyset$.

Let, it possible $t \neq \emptyset$

Clearly, t is a nonempty subset of N . Therefore, by well ordering principle, t has smallest member m (say). Since, $1 \in S$ therefore $m > 1$ and hence $m-1$ is a positive integer.

Since, m is the smallest member of t , $m-1 \notin t$, therefore $m-1 \in S$

\therefore by condition (ii) $m-1+1 \in S \Rightarrow m \in S$

which is a contradiction. Therefore, $t = \emptyset$.

if E_1 is true involving a natural number N if $i) E_1$ is true

ii) If E_k is true $\Rightarrow E_{k+1}$ is true.

and $i) E_k$ is true $\Rightarrow E_{k+1}$ is true for all natural numbers N .

Then the statement E_N is true for all natural numbers N .

Let, S be the set of natural numbers for which the E_n is true.

Therefore, S has the following property

if $k \in S$, $i) k \in S \Rightarrow k+1 \in S$

Therefore, by the principle of induction $S = N$. Therefore the

statement E_N is true for all natural no.

Show by the principle of mathematical induction $1+2+3+\dots+n = \frac{n(n+1)}{2}$

We have, $1 = \frac{1(1+1)}{2} = 1$

\therefore The result is true for $n=1$

Let, the result be true for $n=k$

$$1+2+3+\dots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) \quad (\text{by(i)})$$

$$\frac{(k+1)(k+2)}{2} = \frac{(1+k)(k+1+1)}{2}$$

\therefore The result is true for $m = 1$. Therefore by principle of induction $1+2+3+\dots+m = \frac{m(m+1)}{2} \quad \forall m \in \mathbb{N}$

Q) Prove that $3^{2n} - 8n - 1$ is divisible by 64 $\forall n \in \mathbb{N}$.

$$\Rightarrow \text{Let, } f(n) = 3^{2n} - 8n - 1$$

we have, $f(1) = 9 - 8 - 1 = 0$

$\therefore f(1)$ is divisible by 64.

Let, $f(k)$ be divisible by 64.

$$\text{Now we have, } f(k+1) - f(k) = 3^{2k+2} - 8(k+1) - 1 - (3^{2k} - 8k - 1)$$

$$= 9 \cdot 3^{2k} - 8 + 3^{2k} = 8 \cdot 3^{2k} - 8$$

$$= 8(9^k - 1)$$

$$= 8(9-1)(9+9^1+\dots+9^k)$$

$$= 64p; p = 1+9+9^2+\dots+9^k \text{ is an integer.}$$

$\therefore f(k+1)$ is divisible by 64.

\therefore By the principle of induction $f(n)$ is divisible by 64, $n \in \mathbb{N}$.

Division Algorithm:

For given integers a and b with $b > 0$, there exists unique integers q and r such that $a = qb+r$, where $0 \leq r < b$.

Let, $S = \{a - bn : n \in \mathbb{Z}; a - bn \geq 0\}$

Let us 1st show that S is non empty.

We have, $b \geq 1$

$$b|a| \geq |a|$$

$$\Rightarrow a - b|a| \geq a - |a| \geq 0$$

$$\Rightarrow a - b(-|a|) \geq 0$$

$$\therefore a - b(-|a|) \in S$$

$\therefore S$ is non empty.

Let, r be the smallest member of S . Therefore, we have,

$$a - bq = rb, \quad r \geq 0 \quad \text{and } q \in \mathbb{Z}$$

We shall show that $r < b$, let it

Let, it Possible $n > b$

$$\therefore \text{we have, } a - (q+1)b = a - bq - b = n - b > 0$$

$$\therefore a - (q+1)b \in S$$

$$\text{again we have, } a - (q+1)b \\ = a - bq - b = n - b < 0 \text{ which is contradiction.}$$

$$\therefore b \nmid n < b$$

$$\therefore a = bq + r, \quad 0 \leq r < b \\ \Rightarrow n - b < r, \quad r \neq b$$

Finally we shall show that q and r are unique.

$$\text{Let, } a = bq + r, \quad 0 \leq r < b \quad (i)$$

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b \quad (ii)$$

$$\therefore \text{from (i) and (ii) we get, } 0 = b(q_1 - q) + (r_1 - r)$$

$$b(q - q_1) = r_1 - r$$

$$\Rightarrow |b| |q - q_1| = |r_1 - r|$$

$$\Rightarrow b |q - q_1| = |r_1 - r| \quad (iii)$$

$$\text{from (i) and (iii) we have, } \begin{aligned} 0 &\leq r_1 < b \\ -b &< -r \leq 0 \\ \hline -b &< r_1 - r < b \\ \hline r_1 - r &< b \end{aligned}$$

$$\therefore \text{from (iii), } \frac{|q - q_1|}{|r_1 - r|} < 1 \quad (\text{since, } q \text{ and } q_1 \text{ are both integers satisfying (iv).}} \\ \therefore q = q_1$$

$$\therefore \text{from (iii), } r = r_1$$

Thus the uniqueness is true.

q is called the quotient and r is called the remainder in the division of a by b .

Divisibility: — An integer a is said to be divisible by an integer b ($\neq 0$) if there exists an integer c . such that $a = cb$.

In this case, we say that b divides a and symbolically denoted by $b | a$.

Some properties:-

1) a/b and $b/c \Rightarrow a/c$

2) a/b and $b/a \Rightarrow a = \pm b$

⑩ Theorem: If a/b and a/c then $a/(b+cy)$ for arbitrary integers x and y .

\Rightarrow Since a/b :

$$\therefore b = ma \text{ for some } m \in \mathbb{Z}$$

again since, a/c

$$\therefore c = nc \text{ for some } n \in \mathbb{Z}$$

\therefore for any integers x and y we have,

$$bx+cy = \cancel{m}ax + \cancel{n}ay = a(\cancel{m}x+\cancel{n}y)$$

$$= pa; p = mx+ny \in \mathbb{Z}.$$

$\therefore a/(b+cy)$

7) Prove that the square of an odd integer is of the form $8k+1$, where k is an integer.

\Rightarrow By division algorithm, the remainder will be 0, 1, 2 or 3 upon division by 4,

\therefore any integer can be expressed in any one of the following forms.

$$4q, 4q+1, 4q+2, 4q+3, \text{ where } q \text{ is an integer.}$$

Among these forms $4q+1$ and $4q+3$ are odd.

\therefore we have,

$$(4q+1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k+1, k = 2q^2 + q \in \mathbb{Z}$$

$$(4q+3)^2 = 16q^2 + 24q + 9 = 16q^2 + 24q + 8 + 1 = 8(2q^2 + 3q + 1) + 1 = 8k+1, k = 2q^2 + 3q + 1 \in \mathbb{Z}$$

Common divisors

An integer d is said to be common divisor of the integers a and b if d/a and d/b .

For example :- The divisors of 8 are 1, 2, 4 and 8.

The divisors of 12 are 1, 2, 3, 4, 6 and 12.

∴ Common divisors of 8 and 12 are 1, 2 and 4.

(*) 1 is a common divisor of any integers of a and b .

Greatest common divisors:-

Let a and b be two integers not both zero. An integer d said to be greatest common divisor of a and b denoted by G.C.D. of $a, b = d$ if

$$\text{i)} d/a \text{ and } d/b \Rightarrow c/d$$

$$\text{ii)} c/a \text{ and } c/b \quad \text{gcd of } (8, 12) = 4$$

For example, gcd of $(8, 12) = 4$.

(*) Let, a and b be two integers not both zero and $d = \text{gcd}(a, b)$. Then \exists integers q and r such that, $d = aq + br$.

Prime to each other (relatively prime)

Defn. Two integers a and b not both zero are said to be prime to each other if $\text{gcd}(a, b) = 1$.

For example The integers 8 and 15 are said to be prime to each other if $\text{gcd}(8, 15) = 1$.

Theorem :- Two integers a and b not both zero are prime to each other if and only if there exist some integer q and r such that $aq + br = 1$.

Proof :- Let us first suppose that a and b are prime to each other.

$$\therefore \text{gcd}(a, b) = 1 \quad \text{s.t. } 1 = d = g(a, b) = aq + br$$

∴ there exists an integer q and r s.t.

Conversely, suppose that there exists two integer q and r s.t. $aq + br = 1$.

Let, $\gcd(a, b) = d$
 \therefore There exists integers u and v s.t. $d = au + bv$ for $u \in \mathbb{Z}$
 and $v \in \mathbb{Z}$

$$\therefore d = au + bv$$

$\therefore a$ and b are prime to each other.

① Theorem: Let, $\gcd(a, b) = d$ (a and b are not both zero)
 then $\frac{a}{d}$ and $\frac{b}{d}$ are integers prime to each other.

Proof: Since, $\gcd(a, b) = d$

$$\therefore d/a \text{ and } d/b$$

\therefore there exists integer m and n s.t. $a = md$ and $b = nd$

$\therefore \frac{a}{d}$ and $\frac{b}{d}$ are both integers.

$$\therefore \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = d$$

\therefore There exists integer x and y s.t. $d = ax + by$

$$d = \frac{a}{d}x + \frac{b}{d}y$$

$$= mx + ny$$

$$\therefore \gcd(m, n) = 1$$

$\therefore a$ and b are relatively prime.

$\therefore \frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.
 alternative, we have,

② By division alternative, we have,
 $72 = 30 \cdot 2 + 12$ ↑ $72N + 30U = 12$

$$30 = 12 \cdot 2 + 6$$

$$12 = 6 \cdot 2 + 0$$

$$12 = (30 - 12 \cdot 2) \cdot 2 = 30 \cdot 2 - 12 \cdot 4$$

$$\therefore 12 = 6 \cdot 2 = (30 - 30 \cdot 2) \cdot 4$$

$$= 30 \cdot 2 - 72 \cdot 4 + 30 \cdot 3$$

$$= 30(10) + 72(-4)$$

$$\therefore u = 10 \text{ and } v = -4$$

\therefore two integers u and v satisfying $54u + 24v = 30$

1) Find two integers u and v satisfying $54u + 24v = 30$
 By division alternative, we have,

$$54 = 24 \cdot 2 + 6$$

$$24 = 6 \cdot 4 + 0$$

$$\begin{array}{r} 24) 54 \\ 48) 54 \\ \hline 6 | 54 | 4 \\ \hline 0 \end{array}$$

$$\therefore 24 = 6 \cdot 4 = (54 - 24) \cdot 24 / 4 = 54 \cdot 4 - 24 \cdot 3 \\ = 54 \cdot 4 + 24(-3)$$

$\therefore u = 4$ and $v = -3$

Prime integer

Defn An integer $p > 1$ is said to be prime integer if the only divisors of p are 1 and p .

Fundamental theorem of arithmetic

Statement:- Any tre integer is either 1 or prime or can be expressed as product of primes.

Euklid theorem:-

Statement:- The number of primes is infinite

Note:- Every tre integers which are not prime can be expressed as $P = P_1 d_1, P_2 d_2 \dots P_m d_m$ where $P_1 < P_2 < \dots < P_m$ are primes and d_1, d_2, \dots, d_m are positive integers.

1) Use principle of mathematical induction to prove that

$3^{2^n-1} + 2$ is divisible by 7.

$$\text{Let } f(n) = 3^{2^n-1} + 2^{n+1}$$

$$\therefore \text{we have, } f(1) = 3^1 + 2^2 = 7$$

\therefore the result is true for $n=1$

\therefore the result is true for $n=k$

Let, the result is true for $n=k$.
 $\therefore f(k) = 3^{2^k-1} + 2^{k+1}$ is divisible by 7.

$$\text{Now we have, } f(k+1) - 2f(k) = 3^{2^{k+1}-1} + 2^{k+2} - 2(3^{2^k-1} + 2^{k+1})$$

$$= 3^{2^{k+1}} + 2^{k+2} - 2 \cdot 3^{2^k-1} - 2 \cdot 2^{k+1}$$

$$= 3^{2^{k+1}} + 2^{k+2} - 2 \cdot 3^{2^k-1} - 2 \cdot 2^{k+1}$$

$$\text{then } f(k+1) = 2f(k) + 7P \quad [P = 3^{2^k-1}]$$

$\therefore f(n+1)$ is divisible by 7.

\therefore By the principle of induction $f(n)$ is divisible by 7 for all natural values of n .

1) Show that if a/b and b/c then a/c .

\Rightarrow Since, a/b

\therefore there exists an integer m such that $b = ma$
again since, b/c , there exists an integer n such that $c = nb$

\therefore we have,

$$\begin{aligned} c &= nb \\ &= nma \\ &= pa, \quad p = mn \in \mathbb{Z} \end{aligned}$$

$\therefore a/c \dots$

Show that $\gcd(a, a+2) = 1$ or 2 $\forall a \in \mathbb{Z}$

2) \Rightarrow let, $\gcd(a, a+2) = d$

$\therefore d | a$ and $d | a+2$

$\therefore d | \{ax + (a+2)y\} \quad \forall x, y \in \mathbb{Z}$

~~\therefore choosing $x = -1$ and $y = 1$ we have,~~

$$d | \{ -a + (a+2) \}$$

$$\Rightarrow d | 2$$

$$\Rightarrow d = 1 \text{ or } 2$$

\therefore then show that p/a and if $a, b \in \mathbb{Z}$ s.t.

3) If p is a prime and if p/a or p/b .

\Rightarrow If p/a then the result is proved.

~~let p does not divide a~~

let, $p \nmid a$

$$\therefore \gcd(p, a) = 1$$

\therefore There exists integers x and y such that $px + ay = 1$ — (i)

Now, we have, $p | pb$

and given that $p | ab$

$$\therefore p | (pbx + aby)$$

$$\Rightarrow p | b(px + ay)$$

$$\Rightarrow p | b [by(i)]$$

4) If P is a prime and $1 \leq a < P$ then show that P is prime to a .

\Rightarrow Let, $\gcd(P, a) = d$

$\therefore d | P$ and $d | a$

Now, $d | P \Rightarrow d = 1$ or P

Since, $a < P$

$\therefore d \neq P$

$\therefore d = 1$

$\therefore P$ is prime to a .

5) If a is prime to b then prove that $(\tilde{a} + \tilde{b})$ is prime to $\tilde{a}\tilde{b}$.

6) If a is prime to b then prove that $(\tilde{a} + \tilde{b})$ is prime to ab .

7) If a is prime to b then prove that $(\tilde{a} + \tilde{b})$ is prime to $\tilde{a}\tilde{b}$.

8) If $p \geq q \geq 5$ and p, q are both primes then prove that

$$2^4 | (p^{\tilde{v}} - q^{\tilde{v}})$$

9) If P be let, P be a prime and a be a positive integer then prove that a^n is divisible by P if and only if a is divisible by P .

10) Prove that no prime factors of $(\tilde{n}+1)$ can be of the form $4m-1$, where m is integer.

11) $\therefore a$ is prime to b

~~$\therefore \gcd(a, b) = 1$~~

~~$\therefore \text{There exists two integers } u \text{ and } v \text{ such that } au + bv = 1 \quad (i)$~~

~~Now, let $\gcd(\tilde{a} + \tilde{b}, \tilde{a}\tilde{b}) = d$~~

~~$\therefore d | \tilde{a} + \tilde{b}$ and $d | \tilde{a}\tilde{b} \Rightarrow \tilde{a} + \tilde{b} = dm$ and $\tilde{a}\tilde{b} = mn$ for some integers m, n~~

~~Now, there exists two integers u and v such that $(\tilde{a} + \tilde{b})u + \tilde{a}\tilde{b}v = d$~~

$$\text{or, } d = \frac{\tilde{a} + \tilde{b}}{d}u + \frac{\tilde{a}\tilde{b}}{d}v$$

$$= mu + nv$$

~~$\therefore (\tilde{a} + \tilde{b})$ and $\tilde{a}\tilde{b}$ are prime to each other.~~

$$\therefore \gcd(m, n) = 1$$

Relation

Cartesian product :- The Cartesian products of two sets A and B is denoted by $A \times B$ and defined to be $A \times B = \{(x,y) : x \in A \text{ and } y \in B\}$

For example, consider the sets $A = \{a, b, c\}$ and $B = \{1, 2\}$

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

Note :- $\Omega(A \times B) = \Omega(A) \times \Omega(B)$

Relation set :- Let, A be a set and R be a subset of $A \times A$ such that $(a,b) \in R$ if and only if a and b satisfy a particular relation.

(For example, consider $A = \{1, 2, 3\}$)

$$\text{Here } A \times A = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$$

Let, R be a subset of $A \times A$ if and only if $(a,b) \in R \Rightarrow a < b$.

$$\text{Then, } R = \{(1,2), (1,3), (2,3)\}$$

The set R is called a relation set on A.

Note :- If $(a,b) \in R$ then we write symbolically aRb .

Types of relation :- i) Reflexive relation :- Let, A be a set and R be the relation defined in it. R is said to be reflexive if aRa i.e. $(a,a) \in R, \forall a \in A$

ii) Symmetric relation :- Let, A be a set and R be a relation in it. R is said to be symmetric if $aRb \Rightarrow bRa$.

iii) Antisymmetric relation :- Let, A be a set and R be a relation in it. R is said to be antisymmetric if aRb and $bRa \Rightarrow a=b$

iv) Transitive relation :- Let, A be a set and R be a relation defined in it. R is said to be transitive if aRb and $bRc \Rightarrow aRc$

Equivalence relation :- Let, A be a set and R be a relation defined in it. R is said to be equivalence relation if it is reflexive, symmetric and transitive.

1) Let, $S = \{a, b, c\}$ and $R = \{(a, a), (b, c), (c, b)\}$. Is R an equivalence relation? Justify your answer.

\Rightarrow Since, " aRa " does not hold for $\forall a \in S$.

$\therefore R$ is not reflexive.

$\therefore R$ is not an equivalence relation.

2) A relation R is defined on N by mRn iff " m is a divisor of n ", $\forall m, n \in N$. Prove that R is transitive but not symmetric.

\Rightarrow Let, aRb and bRc hold.

Now, $aRb \Rightarrow a|b \quad (i)$

and $bRc \Rightarrow b|c \quad (ii)$

From (i) and (ii),
 $a|c$

$\Rightarrow aRc$

$\therefore R$ is transitive.

clearly, $5R5$ holds but $5R10$ is \cancel{R} does not hold.

$\therefore R$ is not symmetric.

3) Give an example of a relation which is reflexive but not symmetric.

\Rightarrow Let, R be a relation on the sets of natural number N , defined by aRb iff $a > b$, $a, b \in N$.

Clearly, aRa holds $\forall a \in N$.

$\therefore R$ is reflexive.

clearly $7R7$ holds but $5R7$ does not hold.

$\therefore R$ is not symmetric.

4) On the set of complex number C a relation R is defined by $z_1 R z_2$ iff $z_1 z_2 \geq 0$. Determine whether R is reflexive or symmetric or transitive.

\Rightarrow since, $\cancel{z_1 z_1} = -1 \not\geq 0 \therefore$ if

$\therefore R$ is not reflexive.

$$\begin{aligned} \text{we have, } z_1 P z_2 &\Rightarrow z_1 z_2 > 0 \\ &\Rightarrow z_2 z_1 > 0 \\ &\Rightarrow z_2 P z_1 \end{aligned}$$

$\therefore P$ is symmetric.
 when we have, $z_i P z_j$ and $z_j P z_i$ hold but if
 $\therefore P$ is not transitive.

Home - Work

6) Since, a and b are prime to each other
 \therefore there exists two integers x and y such that $ax+by=1$

NOW,

$$\begin{aligned} a(x+y) - q(a+b) &= 1 \\ \therefore a(x+y) + q(a+b) &= 1 \end{aligned}$$

$\therefore (x+y)$ and $q(a+b)$ are integers
 $\therefore a$ and $(a+b)$ is prime to each other.

again, $b(x+y) + q(a+b) = 1$

$\therefore (y-a)$ and $q(b)$ are integers
 $\therefore b$ and $(a+b)$ is prime to each other.

$\therefore (a+b)$ is prime to ab .

$\therefore (a+b)$ is prime to each other.

5) Since, a and b are prime to each other
 \therefore there exists two integers x and y such that $ax+by=1$

NOW,

$$\begin{aligned} ax+by &= 1 \\ \text{or, } (a(x+y)) &= 1 \\ \text{or, } a^{\cancel{x}} + b^{\cancel{y}} + 2ab^{\cancel{xy}} &= 1 \\ \text{or, } (\cancel{a+b})^{\cancel{x}} + q(b)^{\cancel{y}} - \cancel{2b} - 2ab^{\cancel{xy}} &= 1 \\ \text{or, } (\cancel{a+b})^{\cancel{x}} + b^{\cancel{y}} - q(b)(\cancel{a+b} + \cancel{2qy}) &= 1 \end{aligned}$$

$\therefore (\cancel{a+b})^{\cancel{x}}$ and $b^{\cancel{y}}$ are prime to each other.

If $(\cancel{a+b})^{\cancel{x}}$ and $b^{\cancel{y}}$ are prime to each other.

$\therefore (\cancel{a+b})^{\cancel{x}} m^{\cancel{y}} n^{\cancel{z}} = 1$

or,

$\therefore (a+b)$ is prime to ab

$$\therefore (a+b)u + abv = 1, u, v \in \mathbb{Z}$$

$$\text{or, } (a+b)u = 1 - abv$$

$$\text{or, } (\tilde{a}+\tilde{b})\tilde{u} = 1 + \tilde{a}\tilde{b}\tilde{v} - 2abv$$

$$\text{or, } \cancel{(\tilde{a}+\tilde{b})\tilde{u} + 2ab(u+v)} - \cancel{abv} = 1$$

~~$$\text{or, } \cancel{(\tilde{a}+\tilde{b})\tilde{u} + \tilde{a}\tilde{b}\tilde{v} - 2abv + 2ab(u+v)} = 1$$~~

~~$$\text{or, } \cancel{(\tilde{a}+\tilde{b})\tilde{u} + abv - 2ab(u+v-abv)} = 1$$~~

~~$$\text{or, } \cancel{(\tilde{a}+\tilde{b})\tilde{u} + 2ab\tilde{u} + 2abv - \tilde{a}\tilde{b}\tilde{v}} = 1$$~~

~~$$\text{or, } \cancel{(\tilde{a}+\tilde{b})\tilde{u} + ab} ($$~~

$$\tilde{a}\tilde{b}\tilde{v} = [1 - (a+b)u] = 1 + (a+b)\tilde{u} - 2u(a+b)$$

$$= 1 + (\tilde{a}+\tilde{b} + 2ab)\tilde{u} - 2au - 2bu$$

$$= 1 + \tilde{a}\tilde{u} + \tilde{b}\tilde{u} + 2ab\tilde{u} - 2au - 2bu$$

~~$$\text{or, } \tilde{a}\tilde{b}\tilde{v} + 2au + 2bu - \tilde{a}\tilde{u} - \tilde{b}\tilde{u} - 2abu = 1$$~~

~~$$\tilde{a}\tilde{b}\tilde{v} + 2u(a+b) - \tilde{u}(\tilde{a}+\tilde{b}) - 2abu = 1$$~~

~~$$\tilde{a}\tilde{b}\tilde{v} + \tilde{u}(\tilde{a}+\tilde{b}) - 2\tilde{u}(\tilde{a}+\tilde{b}) + 2u(a+b) - 2abu = 1$$~~

~~$$\text{or, } \tilde{a}\tilde{b}\tilde{v} + \tilde{u}(\tilde{a}+\tilde{b}) - 2u(\tilde{a}\tilde{u} + \tilde{b}\tilde{u} - a - b + abu) = 1$$~~

~~$$\text{or, } \tilde{a}\tilde{b}\tilde{v} + \tilde{u}(\tilde{a}+\tilde{b}) - 2u[u(a+b) - (a+b)] = 1$$~~

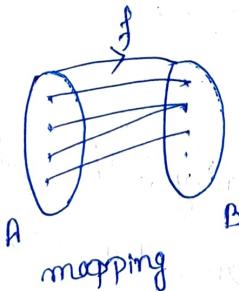
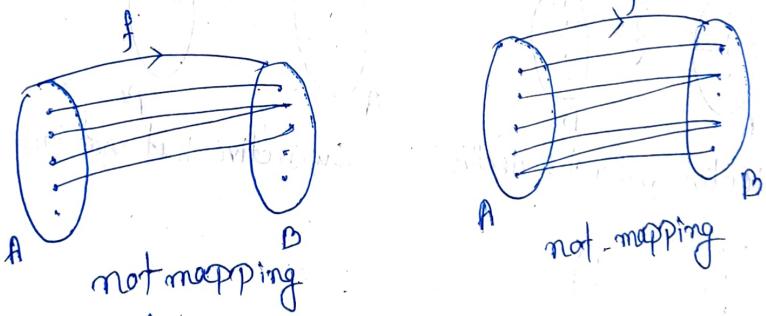
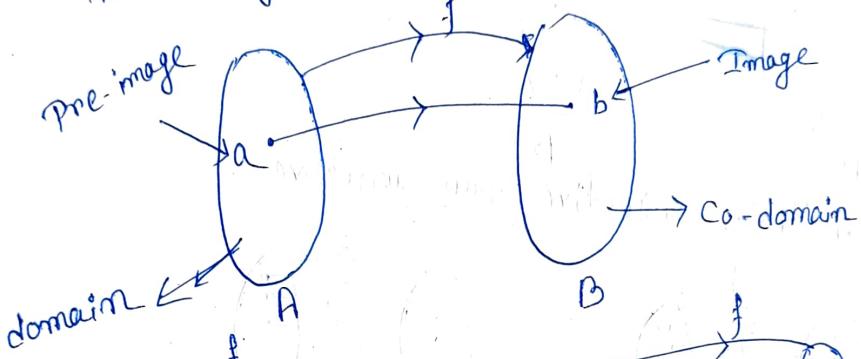
~~$$\text{or, } \tilde{a}\tilde{b}\tilde{v} + \tilde{u}(\tilde{a}+\tilde{b}) - 2u[(a+b)(au + bu^{-1})] = 1$$~~

Functions

Definition :- Let, A and B be two non empty sets (not necessarily different). A map or mapping or function f from A into B is defined to be a subset of $A \times B$ [i.e. f is a relation from A to B] so that the following properties are satisfied —

- To each $a \in A$, there corresponds some $b \in B$ such that $(a, b) \in f$
- $(a, b) \in f$ and $(a, c) \in f \Rightarrow b = c$.

and ii) The mapping f is symbolically denoted by $f: A \rightarrow B$

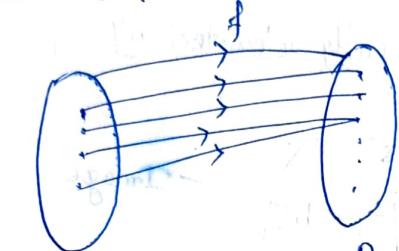
Types of mapping :-

i) Injective map / one-to-one mapping :- A mapping $f: A \rightarrow B$ is said to be injective if for $x_1, x_2 \in A$; $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

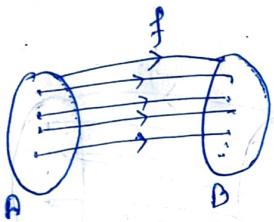
i.e. $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

2) Surjective or onto mapping :- A mapping $f: A \rightarrow B$ is said to be surjective or onto if for every element $b \in B$, there exists some elements $a \in A$ such that $f(a) = b$.

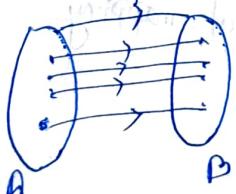
3) Bijective / one-one mapping :- A mapping $f: A \rightarrow B$ is said to be bijective if it is injective and ~~not~~ surjective.



f
A B
neither injective nor surjective

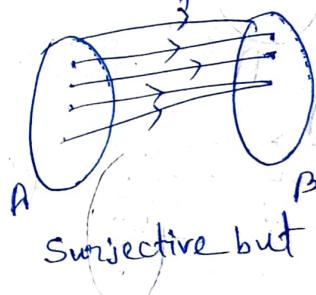


f
A B
Injective but not surjective



f
A B
Bijective mapping

f
A B
surjective



f
A B
Surjective but not injective

Range set :- Let, $f: A \rightarrow B$ be a mapping. The set of elements of the image of the elements of A is called range set and it's denoted by $f(A)$. Clearly, $f(A) \subseteq B$.

[Note :- If $f: A \rightarrow B$ be an onto mapping then $f(A) = B$.]

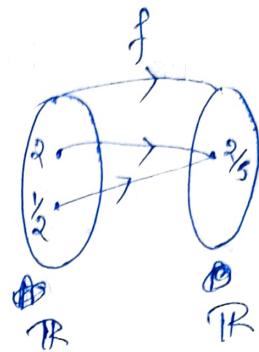
Theorem :- If $f: A \rightarrow B$ be a bijective mapping then the cardinalities of A and B are same. H.W.

3) Show that the mapping $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = \frac{x}{x^2 + 1}$, $\forall x \in \mathbb{R}$ is neither injective nor surjective.

\Rightarrow we have,

$$f(2) = \frac{2}{5}$$

$$\text{and } f\left(\frac{1}{2}\right) = \frac{\frac{1}{2}}{1 + \frac{1}{4}} = \frac{2}{5}$$



\therefore we have, $2 \neq \frac{1}{2}$
but, $f(2) = f\left(\frac{1}{2}\right)$

\therefore The mapping is not injective.
The element 1 $\in \mathbb{R}$ has no pre-image for if a be the pre-image of 1 then

$$\frac{a}{a^2 + 1} = 1$$

$$\text{or, } a^2 - a + 1 = 0$$

$$\text{or, } a = \frac{1 \pm \sqrt{61-4}}{2}$$

$$= \frac{1 \pm i\sqrt{3}}{2} \notin \mathbb{R}$$

$\therefore f$ is not surjective.

2) Show that the mapping $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = \frac{x}{1+|x|}$, $\forall x \in \mathbb{R}$ is one to one.

\Rightarrow we have,

$$f(x) = \frac{x}{1+|x|}$$

$$= \begin{cases} \frac{x}{1+x}, & x \geq 0 \\ \frac{x}{1-x}, & x < 0 \end{cases}$$

case I: Let, $x_1 \geq 0$

In this case we have,

$$f(x_1) = f(x_2)$$

$$\Rightarrow \frac{x_1}{1+x_1} = \frac{x_2}{1+x_2}$$

$$\Rightarrow x_1 + x_1 x_2 = x_2 + x_1 x_2$$

$$\Rightarrow x_1 = x_2$$

2) In this case $f(x)$ is one-to-one.

Case II: Let $x < 0$

If in this case,

$$f(x_1) = f(x_2)$$

$$\Rightarrow \frac{x_1}{1-x_1} = \frac{x_2}{1-x_2}$$

$$\Rightarrow x_1 - x_1 x_2 = x_2 - x_1 x_2$$

$$\Rightarrow x_1 = x_2$$

In this case $f(x)$ is one-to-one.

Combining Cases I and II $f(x)$ is one-to-one.

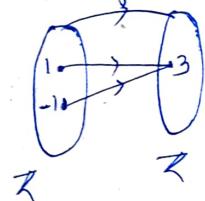
3) Let \mathbb{Z} be the set of all integers. Is the mapping $f: \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $f(x) = x+2$, $\forall x \in \mathbb{Z}$ a one-to-one mapping? Justify your answer.

\Rightarrow We have, $f(1) = 3 = f(-1)$

$$\therefore 1 \neq -1$$

but $f(1) = f(-1)$

$\therefore f$ is not one-to-one.



4) Show whether the mapping $f: \mathbb{Z} \rightarrow \mathbb{Z}^+$ defined by $f(x) = |x|$, $\forall x \in \mathbb{Z}$ and \mathbb{Z} is the set of all integers. Is onto or not?

\Rightarrow Let, b be any element of the codomain set.

Let, a be the pre-image of b under f .

$$\therefore f(a) = b$$

$$\Rightarrow |a| = b$$

$$\Rightarrow a = \pm b$$

$$\Rightarrow a = b, -b$$

$\therefore b$ and $-b$ are the pre-images of B .

$\therefore f$ is onto.

5) Give an example with justification, of a mapping which is surjective but not injective.
 $\Rightarrow f(a) = \{x\}, \forall x \in \mathbb{Z}$

6) Show that the mapping $f: C \rightarrow C - \{0\}$, where C is the set of complex numbers defined by $f(z) = e^z, \forall z \in C$ is onto but not one-to-one.

\Rightarrow Let, z be any element of the co-domain set.

Let, a be the pre-image of z under f .

$$\therefore f(a) = z$$

$$\text{or, } e^a = z$$

or, $a = \log z \in C$

$\therefore \log z$ is the preimage of z under f

$\therefore f$ is onto.

Let, $z_1 = \pi i$ and $z_2 = 3\pi i$

$$\text{we have, } f(z_1) = e^{\pi i} = \cos \pi + i \sin \pi = -1$$

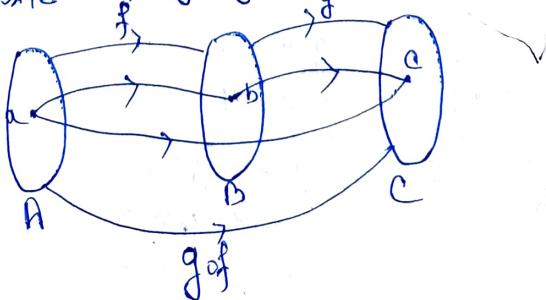
$$\text{and } f(z_2) = e^{3\pi i} = \cos 3\pi + i \sin 3\pi = -1$$

Thus, $z_1 \neq z_2$
 $\text{But } f(z_1) = f(z_2)$

$\therefore f$ is not one-to-one.

Composite mapping:— Let, $f: A \rightarrow B$ and $g: B \rightarrow C$ be two mappings

The composite mapping $gof: A \rightarrow C$ is defined by $(gof)(a) = g(f(a))$



1) Two mappings $f: \mathbb{R} \rightarrow \mathbb{R}$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ are defined as
 $f(x) = x+1$, $\forall x \in \mathbb{R}$ and $g(x) = x$, $\forall x \in \mathbb{R}$.
Find the composite mapping gof and gof .

\Rightarrow We have,

$$gof = f(g(x)) = f(x) = x+1$$

$$\text{and } gof = g(f(x)) = g(x+1) = x+1$$

[Note:— In general $gof \neq gof$]

2) Let, $f: S \rightarrow T$ and $g: T \rightarrow U$, show that gof is one-to-one if each of g and f is one to one.

\Rightarrow Let, $h = gof$

We have, $h(x_1) = h(x_2)$, $x_1, x_2 \in S$ Let, $y_1 = f(x_1)$ and $y_2 = f(x_2)$.

$$\Rightarrow (gof)(x_1) = (gof)(x_2)$$

$$\Rightarrow g(f(x_1)) = g(f(x_2))$$

$$\Rightarrow g(y_1) = g(y_2)$$

$\Rightarrow y_1 = y_2$ [since, g is one-to-one]

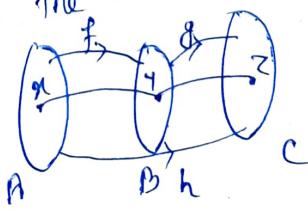
$$\Rightarrow f(x_1) = f(x_2)$$

$$\Rightarrow x_1 = x_2$$
 [since, f is one-to-one]

$\therefore gof$ is one-to-one.

$\therefore gof$ is one-to-one.

3) Let, $f: A \rightarrow B$ and $g: B \rightarrow C$ be both bijective mappings,
show that the composite mapping $gof: A \rightarrow C$ is bijective.



$$g(y) = z$$

$$f(x) = y$$

$$\therefore g(f(x)) = z$$

$$(gof)(x) = z$$

$$h(x) = z$$

4) Let, $f: A \rightarrow B$ and $g: B \rightarrow A$ be two mappings such that $g \circ f = I_A$, the identity mapping on A . Show that f is one-to-one and g is onto.

\Rightarrow Let, $h = g \circ f$

Since, h is identity mapping on A .

$$\therefore h(x) = x, \forall x \in A$$

Now let, from $x_1, x_2 \in A$ we have,

$$f(x_1) = f(x_2)$$

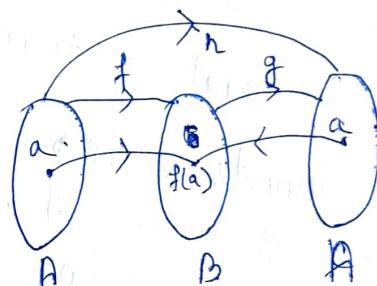
$$\Rightarrow g(f(x_1)) = g(f(x_2))$$

$$\Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2)$$

$$\Rightarrow h(x_1) = h(x_2)$$

$$\Rightarrow x_1 = x_2$$

$\therefore f$ is one-to-one



Let, a be any element of A .

$$\therefore f(a) \in B$$

Now we have, $g(f(a))$

$$= (g \circ f)(a)$$

$$= h(a)$$

$$= a$$

This shows that $f(a)$ is the preimage of a under g .

$\therefore g$ is onto.

Inverse of a mapping:-

If $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ be defined by $f(x) = x + 3$, where \mathbb{R}^+ is the set of all positive real numbers, then find $f^{-1}(7)$

\Rightarrow Let, $f^{-1}(7) = x$

$$\therefore 7 = f(x) = x + 3$$

$$\text{or, } x = \pm 2$$

$$\therefore x=2 \quad [\because f: \mathbb{R} \rightarrow \mathbb{R}^+]$$

2) A mapping $f: \mathbb{R} \rightarrow \mathbb{R}$ defined as follows $f(x) = \begin{cases} 1, & x \text{ is rational} \\ -1, & x \text{ is irrational} \end{cases}$
Find $f(\sqrt{7})$. Is the mapping one-to-one or onto?
Find the range set of f .

\Rightarrow Since, $\sqrt{7}$ is irrational

$$\therefore f(\sqrt{7}) = -1$$

We have, $f\left(\frac{1}{2}\right) = 1$

$$f\left(\frac{1}{4}\right) = 1$$

$$\therefore \frac{1}{2} \neq \frac{1}{4}$$

 $\text{but } f\left(\frac{1}{2}\right) = f\left(\frac{1}{4}\right)$

$\therefore f$ is not one-to-one
The elements except -1 and 1 of \mathbb{R}' has no pre-image under f .

$\therefore f$ is not onto.

\therefore The range set of f $\{-1, 1\}$

