STUDY MATERIAL

VIVEKANANDA COLLEGE

THAKURPUKUR

NAAC ACCREDITED GRADE—'A'

Mathematics
(Honours)
Algebra

Dr. Debasis Mukherjee*

*Associate Professor

Department of Mathematics

Vivekananda College, Thakurpukur

Core Course- II

Algebra

Unit-2

Relation

Let S and T be two non-empty sets. Intuitively a relation ρ between S and T is a rule that associates some or all of the elements of S and with the elements of T.

Definition. Let S and T be two non-empty sets. A binary relation ρ between S and T is a subset of S×T.

If the ordered pair (s,t) ϵ ρ, then the element s of the set S is said to be related to the element t of the set by the relation ρ.

If (s,t) ϵ (S×T)-ρ, then s is said to be not related to t by the relation ρ.

Examples.

1. Let S ={2,3,4,5}, T={11,12,13,14}. A relation ρ between S and T is defined by specifying that an element s in S is related to an element t in T if s is a divisor of t. Then ρ= {(2,12),(2,14),(3,12),(4,12)}.

(2,11) ϵ (S×T) but (2,11) does not belong to ρ.

Definition. Let ρ be a relation between the sets A and B. The inverse of the relation ρ, denoted by ρ^{-1}, is a relation between the sets B and A and is defined by $\rho^{-1} = \{(b,a): (a,b) \epsilon\, \rho\}$.

Equivalence relation.

Let S be a nonempty set and ρ be a binary relation on S.

The relation ρ is said to be reflexive if (a,a) ϵ ρ for all a in S, i.e, aρa holds for all in S.

The relation ρ is said to be symmetric if for any two elements a, b in S, (a,b) ϵ ρ ⇒ (b,a) ϵ ρ, i.e, aρb ⇒ bρa . The relation ρ is said to be transitive if for any three elements a, b, c in S , (a,b) ϵ ρ and (b,c) ϵ ρ ⇒ (a,c) ϵ ρ, i.e, aρb and bρc ⇒ aρc.

The relation ρ on S is said to be an equivalence relation on S if ρ is reflexive, symmetric and transitive.

Example1.

A relation ρ is defined on the set Z by " aρb if and only if a-b is divisible by 5" for a, b ϵ Z. Examine if ρ is an equivalence on Z.

(i) Let a ϵ Z. Then a-a is divisible by 5. Therefore aρa holds for all a in Z. and ρ is reflexive.

(ii) Let a, b ϵ Z and aρb hold. Then a-b is divisible by 5 and therefore b-a is divisible by 5. Thus aρb ⇒ bρa and therefore ρ is symmetric.

(iii) Let a, b, c ϵ Z and aρb, bρc both hold. Then a-b and b-c are both divisible by 5. Therefore a-c=(a-b)+(b-c) is divisible by 5. Thus aρb and bρc ⇒ aρc and therefore ρ is transitive. Since ρ is reflexive, symmetric and transitive, ρ is an equivalence relation.

Remark. This relation ρ is said to be the relation of congruence (mod 5), and is expressed as ' a≡ $b(mod\ 5)$'.

Definition

Let ρ be an equivalence relation on a set S. Let a ϵ S. Let cl(a) be a subset of S defined by cl(a)={x ϵ S : xρa}.

cl(a) is a non-empty subset of S since a ϵ cl(a). cl(a) is said to be the ρ-equivalence class of a and each element of cl(a) is said to be ρ-equivalent to a.

Theorem 1. Let ρ be an equivalence relation on a set S and a, b ϵ S. Then cl(a)=cl(b) if and only if aρb.

Proof. Let cl(a)=cl(b) and let x ϵ cl(a). Then x ϵ cl(b) also.

xρa and xρb ⇒ aρx and xρb, since ρ is symmetric.

⇒ aρb, since ρ is transitive.

Therefore cl(a)=cl(b) ⇒ aρb.

Conversely, let aρb. Let x ϵ cl(a). Then xρa holds.

x ϵ cl(a) and aρb ⇒ xρa and aρb

⇒ xρb, since ρ is transitive.

⇒ x ϵ cl(b). This proves that cl(a) ⊂ cl(b). Similarly cl(b) ⊂ cl(a). It follows that cl(a)=cl(b). Thus aρb ⇒ cl(a)=cl(b) and this proves the theorem.

Theorem 2. Let ρ be an equivalence relation on a set S and a, b ϵ S. If a$\bar{\rho}$b then cl(a) and cl(b) are disjoint.

Proof. If possible, let cl(a)∩ cl(b)≠ ∅ and x ϵ cl(a)∩cl(b). x ϵ cl(a) ⇒ xρa, x ϵ cl(b) ⇒ xρb.

xρa and xρb ⇒ aρx and xρb, since ρ is symmetric.

$\Rightarrow$ aρb, since ρ is transitive. This is a contradiction. Therefore cl(a)∩cl(b)=∅.

Theorem 3. Let ρ be an equivalence relation on a set S and a, b ϵ S. Then the classes cl(a) and cl(b) are either equal or disjoint.

Proof. Since a, b ϵ S, (a,b) ϵ S×S. Since ρ is a binary relation on S, either (a,b) ϵ ρ or (a,b) $\notin$ ρ.

Let (a,b) ϵ ρ. Then aρb holds. We have cl(a)=cl(b), by Theorem 1.

Let (a,b) $\notin$ ρ. Then cl(a) and cl(b) are disjoint, by Theorem 2. Consequently, either cl(a)=cl(b) or cl(a)∩cl(b)=∅.

Partition of a set.

Let S be a non-empty set. A family of non-empty subsets $\{S_\alpha : \alpha \in I\}$, I being the index set, is said to form a partition of S if (i) $\cup S_\alpha$=S, $\alpha \in$ I and (ii)$S_\alpha \cap S_\beta = \emptyset$ for $\alpha, \beta \in$ I and $\alpha \neq \beta$.

If ρ be an equivalence relation on a set S then the family of distinct ρ-equivalence classes is such that

(i) each class in the family is non-empty,
(ii) the union of the family of classes is the set S and
(iii) the classes are pairwise disjoint.

Therefore the distinct ρ- equivalence classe form a partition of the set S.

Example.

Find the equivalence classes determined by the equivalence relation ρ on Z defined by " aρb if and only if a-b is divisible by 5" for a, b ϵ Z.

There are five distinct equivalence classes. They are

Cl(0)={5n : n is an integer},

Cl(1)={5n+1 : n is an integer},

Cl(2)={5n+2 : n is an integer},

Cl(3)={5n+3 : n is an integer},

Cl(4)={5n+4 : n is an integer}.

The classes cl(0), cl(1), cl(2), cl(3), cl(4) are called the classes of residues of Z(mod 5).

Theorem 4. An equivalence relation ρ on a set S determines a partition of S. Conversely, each partition of S yields an equivalence relation on S.

Proof. Each element of S belongs to a ρ-equivalence class, because if p ϵ S then p ϵ cl(p). If a, b be elements of S then the ρ-equivalence classes cl(a) and cl(b) are either disjoint or equal.

If we consider the family of distinct ρ-equivalence classes we observe that (i) each class in the family is non-empty, (ii) the union of the family of classes is the set S and (iii) the classes are pairwise disjoint.

Therefore the family of distinct ρ-equivalence classes form a partition of the set S.

Conversely, let there be a partition P of the set S into subsets.

Let us define a relation ρ on the set S to mean that aρb holds if a and b belong to one and the same subset of the partition P.

Let a ϵ S. Then aρa holds since a and a belong to one and the same subset of the partition P. Therefore ρ is reflexive.

Let a, b ϵ S and aρb. Then a and b belong to one and the same subset of the partition P and therefore b and a belong to the same subset of P. That is, aρb $\Rightarrow$ bρa. Therefore ρ is symmetric.

Let a, b, c ϵ S and aρb, bρc both hold. Then and b belong to one and the same subset, say S_1 of P; band c belong to one and the same subset, say S_2 of P.

Now S_1 and S_2 being subsets of a partition, must be either identical or disjoint. Since b ϵ $S_1 \cap S_2$, it follows that $S_1 = S_2$ and consequently, a and c belong to one and the same subset of P. That is, aρb and bρc $\Rightarrow$ aρc. Therefore ρ is transitive.

Thus ρ is a equivalence relation on S. This completes the proof.

Example 1. A relation R is defined on the set A = {1,2,3,4} by R ={(1,1),(1,3),(2,2),((2,4),((3,1),((4,2),(4,4). Show that R is an equivalence relation. Describe the R-equivalence classes.

(i) A={(1,1),(2,2),(3,3),(4,4)}. A is a subset of R. So R is reflexive.
(ii) R^{-1}={(1,1),(3,1),(2,2),(4,2),(1,3),(2,4),(4,4)}. $R^{-1} = R$. So R is symmetric.
(iii) R◦R= {(1,1),(1,3),(2,2)(2,4),(3,1),(3,3),(4,2),(4,4)}. R◦R is a subset of R. So R is transitive.
(iv) Consequently, R is an equivalence relation.

cl(1) = {x ϵ S : (1,x) ϵ R} = {1,3}.

cl(1) = {x ϵ S : (2,x) ϵ R} = {2,4}.

cl(1) = {x ϵ S : (3,x) ϵ R} = {3,1}.

cl(1) = {x ϵ S : (4,x) ϵ R} = {4,2}. The R-equivalence classes are cl(1)=cl(3)={1,3}, cl(2)=cl(4)={2,4}.

Partial order relation

Definition. Let S be a non-empty set. A relation ρ on the set S is said to be antisymmetric if aρb and bρa $\Rightarrow$ a=b for a, b ϵ S.

Example 1. The relation ρ defined on R by "xρy if and only if x≤y" for x, y ϵ R is antisymmetric.

Example 2. Let X be a non-empty set. The relation ρ defined on P(X) by "AρB if and only if A is a subset of B " for A, B ϵ P(X) is antisymmetric.

Definition. Let S be a non-empty set. A relation ρ on S is said to be a partial order relation if ρ is reflexive, antisymmetric and transitive.

A relation of partial order is often denoted by '≤', even if it is not "less than".

Poset. A nonempty set S together with a relation of partial order ≤ on S is called a Post (Partialy Ordered set) and is denoted by (S,≤).

Examples.

(R,≤) is a poset where x≤ y means " x is less than or equal to y" for x, y ϵ R.

Let X be a non-empty set and P(X) be the power set of X. (P(X),≤) is a poset where A ≤ B means " A is a subset of B".

Linear order relation.

If R is a partial ordering of non-empty set A, then we usually write a ≤ b in place (a,b) ϵ R.

Elements a, b ϵ A are said to be comparable, provided a ≤ b or b ≤ a. However, two given elements of a partially ordered set need not be comparable. A partial ordering of a set A such that any two elements are comparable is called linear ordering.

Example. Let A be the power set of {1,2,3,4,5}. Define C ≤ D if and only if C ⊂ D. Then A is partially ordered, but not linearly ordered (for example, {1,2} and {3,4} are not comparable).

Exercise 1

1. Determine the nature of the following relations ρ on the set Z.

(i) aρb if and only if a, b ϵ Z and $a^2 + b^2$ is a multiple of 2.
(ii) aρb if and only if a, b ϵ Z and 2a+3b is divisible by 5.
(iii) aρb if and only if a, b ϵ Z and a-b < 3.

Mapping

Definition. Let A and B be two non-empty sets. A mapping f from A to B is a rule that assigns to each element x of A a definite element y in B.

A is said to be the domain of f and B is said to be the co-domain B is displayed symbolically by f : A $\rightarrow$ B.

A mapping f is also called a function, or a transformation, or a map or an operator.

Let f : A $\rightarrow$ B be a mapping and x $\in$ A. Then the unique element y of B that corresponds to x by the mapping f is called the f-image of x and is denoted by f(x). If f(x)=y, we often say that 'f maps x to y'.

The set of all f-images, i.e, {f(x) : x $\in$ A } is denoted by f(A) and is said to be the image set of f (denoted by im f) or the range set of f.

Example 1. Let f={(x,y) $\in$ R×R : y=1/x}. Let us examine if f is a mapping from R to R. The element 0 in the domain set R is not related to an element of the co-domain set. Therefore f is not mapping from R to R.

Let S=R-{0}. Then f= {(x,y) $\in$ S×R : y=1/x} is a mapping from S to R. It is written in the form " f : S $\rightarrow$ R is defined by f(x)= 1/x, x $\in$ S".

Definitions.

1. A mapping f : A $\rightarrow$ B is said to be into mapping if f(A) is a proper subset of B.
2. A mapping f : A $\rightarrow$ B is said to be an onto mapping if f(A) = B.

Examples.

3. Let f : Z $\rightarrow$ Z be defined by f(x) = 2x, x $\in$ Z. Then f is an into mapping because f(Z) is a proper subset of the co-domain set Z.
4. Let f : Z $\rightarrow$ Z be defined by f(x) = |x|, x $\in$ Z. Then f is an into mapping because f(Z) is a proper subset of the co-domain set Z.
5. Let f : Z $\rightarrow$ Z be defined by f(x) = x+1, x $\in$ Z. Then every element y in the co-domain set Z has pre-image y-1 in the domain set Z. Therefore f(Z)=Z and f is onto mapping.

Definitions.

6. A mapping f : A $\rightarrow$ B is said to be injective (or one-to-one) if for each pair of distinct elements of A, their f-images are distinct.
7. A mapping f : A $\rightarrow$ B is said to be surjective (or onto) if f(A) = B.
8. A mapping f : A $\rightarrow$ B is said to be bijective if f is both injective and surjective.

Thus f : A $\rightarrow$ B is injective if $x_1 \neq x_2$ in A implies f(x_1) $\neq$ f(x_2) in B. In this case , each element of B has at most one pre-image.

If f is surjective, each element of B has at least one pre-image.

If f is bijective, each element of B has exactly one pre-image.

9. A mapping f : A $\rightarrow$ B is said to be a constant mapping if f maps each element of A to one and the same element of B, i.e, f(A) is a singleton set.

For example, the mapping f : R $\rightarrow$ R defined by f(x) = 2, x $\in$ R is a constant mapping.

10. A mapping f : A $\rightarrow$ A is said to be the identity mapping on A if f(x) = x, x $\in$ A. The identity mapping on A is denoted by i_A.
11. Let f : R $\rightarrow$ R be defined by f(x) = sin x, x $\in$ R. This mapping is neither surjective nor injective. If we reduce the co-domain to T = {x $\in$ R : -1 $\leq$ x $\leq$ 1 }, then the mapping f : R $\rightarrow$ T defined by f(x) = sin x, x $\in$ R is surjective, but not injective.
12. Let f : R $\rightarrow$ R be defined by f(x) = 3x+1, x $\in$ R. Examine if f is (i) injective, (ii) surjective.

(i) Let us take two distinct elements x_1, x_2 in R, the domain of f. f(x_1) = 3x_1+1, . f(x_2) = 3x_2+1.

f (x_1) - f(x_2) = 3($x_1 - x_2$) $\neq$ 0, since $x_1 \neq x_2$. Since $x_1 \neq x_2 \Rightarrow$ f(x_1) $\neq$ f(x_2), f is injective.

(ii) Let us take an arbitrary element y in in the set R, the co-domain of f ; and let us examine if y has a pre-image x in the domain of f. Then f(x) = y and therefore 3x+1 = y or, x = $\frac{y-1}{3}$. Since y $\in$ R , $\frac{y-1}{3}$ $\in$ R. Therefore y has a pre-image $\frac{y-1}{3}$ in the domain of f. Since y is arbitrary, each element in the co-domain of f has a pre-image under f. Therefore f is surjective.

13. Let f : R $\rightarrow$ R be defined by f(x) = x^2, x $\in$ R. Examine if f is (i) injective, (ii) surjective.

(i) f(2) =4, f(-2) = 4. f is not injective, since two distinct elements 2 and -2 in the domain of have the same image.

(ii) f is not surjective, since -1 in the co-domain of f has no pre-image in the domain of f.

Composition of mappings.

Let f : A $\rightarrow$ B and g : C $\rightarrow$ D be two mappings such that f(A) is a subset of C.

Let x $\in$ A. The f maps x to an element y in f(A) $\subset$ B and since y $\in$ f(A) $\subset$ C, g maps y to an element z in D. We conceive of a mapping h : A $\rightarrow$ D defined by h(x) = g(f(x)), x $\in$ A. The mapping h : A $\rightarrow$ D is said to be the composite of f and g and is denoted by g$\circ$f.

Example 14. Let f : Z $\rightarrow$ Q and g : Q $\rightarrow$ Q be defined by f(x) = $\frac{1}{2}x$, x $\in$ Z and g(x) = x^2, x $\in$ Q .

g$\circ$f : Z $\rightarrow$ Q is defined by (g$\circ$f)(x) = g($\frac{1}{2}x$)= $\frac{1}{4}x^2$, x $\in$ z.

Theorem 5. Let f : A $\rightarrow$ B, g : B $\rightarrow$ C, h : C $\rightarrow$ D be three mappings. Then h$\circ$(g$\circ$f) = (h$\circ$g)$\circ$f.

Proof. Here the composite mappings g$\circ$f, h$\circ$g are defined because the range f $\subset$ dom g and the range g $\subset$ dom h. The composite mappings h$\circ$(g$\circ$f), (h$\circ$g)$\circ$f are defined because the range g$\circ$f $\subset$ dom h and the rage f $\subset$ dom h$\circ$g.

We shall now prove the equality of the mappings h$\circ$(g$\circ$f) : A $\rightarrow$ D and (h$\circ$g)$\circ$f : A $\rightarrow$ D.

Let x be an element of A and let f(x) = y, g(y) = z, h(z) = w. Then (g◦f)(x) = g(y)= z, (h◦g)(y) = h(z) = w.

h◦(g◦f) : A $\rightarrow$ D is defined by h◦(g◦f)(x) = h(z) = w, x ∈ A,

(h◦g)◦f : A $\rightarrow$ D is defined by (h◦g)f(x) = (h◦g) (y) = w, x ∈ A.

Since h◦(g◦f)(x) = (h◦g)◦f(x) for all x ∈ A, we have h◦(g◦f) = (h◦g)◦f.

Theorem 6. If f : A $\rightarrow$ B and g : B $\rightarrow$ C be both injective mappings then the composite mappings g◦f : A $\rightarrow$ C is injective.

Proof. Let x_1, x_2 be two distinct elements of A.

Let f(x_1) = y_1, f(x_2) = y_2.

Since f is injective, y_1 andy_2 are distinct elements of B.

Let g(x_1) = z_1, g(x_2) = z_2.

Since g is injective, z_1 and z are distinct elements of C.

Now (g◦f) (x_1) = g(y_1) = z_1, (g◦f)(x_2) = g(y_2) = z_2 and $x_1 \neq x_2$ in A $\Rightarrow z_1 \neq z_2$ in C. Therefore g◦f is injective.

Remark. The converse of the theorem is not true. However if g◦f is injective then f is injective (while g need not be).

For example, let f : R $\rightarrow$ R be defined by f(x) = e^x, x ∈ R and g : R $\rightarrow$ R be defined by g(x) = $x^2, x \in$ R.

Here g◦f : R $\rightarrow$ R is defined by g◦f(x) = e^{2x}, x ∈ R. g◦f is injective but g is not injective.

Theorem 7. If f : A $\rightarrow$ B and g : B $\rightarrow$ C be two mappings such that g◦f : A $\rightarrow$ C is injective then f is injective.

Proof. Let f(x_1) = f(x_2) for some x_1, x_2 in A. Then g(f(x_1)) = g(f(x_2)), since g is a mapping. So (g◦f)(x_1) =(g◦f)(x_2). Because g◦f is injective, (g◦f)(x_1) = (g◦f)(x_2) implies $x_1 = x_2$ and therefore f is injective.

Theorem 8. If f : A $\rightarrow$ B and g : B $\rightarrow$ C be both surjective mappings then the composite mappings g◦f : A $\rightarrow$ C is surjective.

Proof. Let z be an element of C.

Since g is surjective, there is at least one pre-image of z in B. Let one such be y. Then y ∈ B and g(y) = z. Since f is surjective and y ∈ B, there is at least on pre-image of y in A. Let one such be x. Then x ∈ A and f(x) = y.

(g◦f) (x) = g(y) = z. This implies that z has a pre-image x in A under the mapping g◦f. Since z is arbitrary, g◦f is surjective.

Remark. The converse of the theorem is not true. However if g◦f is surjective then g is surjective (while f need not be).

For example, let f : Z $\rightarrow$ Z be defined by f(x) = 2x, x $\in$ Z and g : Z $\rightarrow$ Z be defined by g(x) = $[\frac{x}{2}]$, x $\in$ Z. [x] denotes the greatest integer $\leq$ x. Then g◦f : Z $\rightarrow$ Z is defined by (g◦f)(x) = x, x $\in$ Z.

g◦f = i_z and is, therefore, surjective; but f is not surjective.

Theorem 9. If f : A $\rightarrow$ B and g : B $\rightarrow$ C be two mappings such that g◦f : A $\rightarrow$ C is surjective then g is surjective.

Proof. Let z be an element of C.

Since g◦f is surjective there is an element x in A such that (g◦f)(x) = z. Therefore g(f(x)) = z.

This shows that z has a pre-image f(x) in B under the mapping g. Since z is arbitrary, g is surjective.

Theorem 10. . If f : A $\rightarrow$ B and g : B $\rightarrow$ C be both bijective mappings then the composite mappings g◦f : A $\rightarrow$ C is bijective.

This is combination of the Theorems 6 and 8.

Inverse mapping.

Definition. Let f : A $\rightarrow$ B be a mapping. If there exists a mapping g : B $\rightarrow$ A such that g◦f = i_A then g is said to be a left inverse (invertible) of f. If there exists a mapping h : B $\rightarrow$ A such that f◦h = i_B then h is said to be a right inverse (invertible) of f.

Definition. Let f : A $\rightarrow$ B be a mapping. f is said to be invertible if there exists a mapping g : B $\rightarrow$ A such that g◦f = i_A and f◦g = i_B. In this case g is said to be an inverse of f.

Theorem 10. If f : A $\rightarrow$ B is invertible then its inverse is unique.

Proof. Since f : A $\rightarrow$ B is invertible, there exists a mapping g : B $\rightarrow$ A such that g◦f = i_A and f◦g = i_B.

If possible, let there exists another mapping h : B $\rightarrow$ A such that h◦f = i_A and f◦h = i_B.

h◦(f◦g) = (h◦f)◦g, since composition of mappings is associative. Therefore h◦i_B = i_A◦g, i.e, h = g. This proves that g is unique.

Examples.

1. Let f : R$\rightarrow$ Z be defined by f(x) = |x|, x $\in$ R and g : Z $\rightarrow$ R be denoted by g(x) = x+$\frac{1}{2}$, x $\in$ Z.

f◦g : Z $\rightarrow$ Z is defined by (f◦g)(x) = f(x+$\frac{1}{2}$) = [x+$\frac{1}{2}$] $= x$, x ∈ Z.

g◦f : R $\rightarrow$R is defined by (g◦f)(x) = g[x]) = [x]+$\frac{1}{2} = x$, x ∈ R.

Here f◦g = i_Z, g◦f ≠ i_R.

Therefore g is a right inverse of f, but not a left inverse of f.

Let h : Z $\rightarrow$ R be defined by h(x) = x+$\frac{1}{3}$, x ∈ Z. Then f◦h = i_Z and therefore h is a right inverse of f.

2. Let f : R$\rightarrow$ R be defined by f(x) = 3x, x ∈ R and g : R $\rightarrow$ R be denoted by g(x) = $\frac{x}{3}$, x ∈ Z.

g◦f : R $\rightarrow$R is defined by (g◦f)(x) = g(3x) = x, x ∈ R.

f◦g : R $\rightarrow$ R is defined by (f◦g)(x) = f($\frac{x}{3}$) = x, x ∈ R.

Here f◦g = i_R = g◦f. Therefore g is the inverse of f.

Theorem 11. Let f : A $\rightarrow$ B be a mapping. Then the following assertions hold.

(i) f is injective if and only if f is left invertible.
(ii) f is surjective if and only if f is right invertible.
(iii) f is bijective if and only if f is invertible.

Proof. (i) Suppose f is left invertible. Then there exists g : B $\rightarrow$ A such that g◦f = i_A. Let x, y ∈ A be such that f(x) = f(y). Then g(f(x)) = g(f(y)) or (g◦f)(x) = (g◦f)(y). Hence, i_A(x) = i_A(y), i.e, x = y. Thus f is injective.

Conversely, suppose f is injective. Then for y ∈ B, either y has no pre-image or there exists a unique x_y ∈ A such that f(x_y) = y. Fix x ∈ A. Define g : B $\rightarrow$ A by

g(y) = $\begin{cases} x & if\ y\ has\ no\ preimage\ under\ f \\ x_y & if\ y\ has\ a\ preimage\ under\ f\ and\ f(x_y) = y \end{cases}$

for all y ∈ B. By the definition of D(g) = B. To show that g is well defined, suppose y,$\acute{y}$ ∈ B and y = $\acute{y}$. Then either both y and $\acute{y}$ have no pre-images or there exists $x_y, x_{\acute{y}}$ ∈ A such that f(x_y) = y and f($x_{\acute{y}}$) = $\acute{y}$. Suppose both y and $\acute{y}$ have no pre-images. Then g(y) = x =g($\acute{y}$). Now suppose there exists unique $x_y, x_{\acute{y}}$ ∈ A such that that f(x_y) = y and f($x_{\acute{y}}$) = $\acute{y}$. Thus, g(y) = x_y and g($\acute{y}$) = $\acute{x_y}$. Since y = $\acute{y}$, we have f(x_y) = f($x_{\acute{y}}$). Since f is injective $x_y = \acute{x_y}$ and so g(y) = g($\acute{y}$). We have thus shown that g is well defined and so g is a mapping. We now show that g◦f = i_A. Let u ∈ A and suppose f(u) = v for some v ∈ B. Then by the definition of g(v) = u. Thus,

(g◦f)(u) = g(f(u)) = g(v) = $i_A(u)$. Hence, g◦f = i_A.

(iii) Suppose f is right invertible. Then there exists g : B $\to$ A such f$\circ$g = i_B. Let y ∈ B. Let x = g(y) ∈ A. Now y = $i_B(y)$ = (f$\circ$g)(y) = f(g(y)) = f(x). Hence f is surjective.

Conversely, suppose f is surjective. Let y ∈ B. Since f is surjective, there exists x ∈ A such that f(x) = y. Let A_y = {x ∈ A : f(x) = y }. Then $A_y \neq \emptyset$. Choose $x_y \in A_y$ for all y ∈ B. Define h : B $\to$ A such that h(y) = x_y for all y ∈ B. Then h is a mapping. Let y ∈ B. Then (f$\circ$h)(y) = f(h(y)) = f(x_y) = y = $i_B(y)$. Hence, f$\circ$h = i_B and so f is right invertible.

(iv) The result here follows from (i) and (ii).

Theorem 12. Let A be a set and f : A $\to$ A be injective. Then f^n : A $\to$ A is injective for all integers n $\geq$ 1.

Proof. Suppose there exists n > 1 such that f^n is not injective. Then there exists x, y ∈ A such that x ≠ y and $f^m(x) = f^m(y)$. But then $f\left(f^{m-1}(x)\right) = f(f^{m-1}(y))$ and hence $f^{m-1}(x) = f^{m-1}(y)$ since f is injective. Now since m is the smallest positive integer such that f^m is not injective, f^{m-1} is injective. Hence, x = y, which is a contradiction. Thus, f^n is injective for all n $\geq$ 1.

Theorem 13. Let A be a finite set. If f : A $\to$ A be injective, then f is surjective.

Proof. Let y ∈ A. Now $f^n(y)$ ∈ A for all n $\geq$ 1. Hence, $\{y, f(y), f^2(y), \dots\} \subset A$. Since A is finite, all elements of the set $\{y, f(y), f^2(y), \dots\}$ cannot be distinct. Thus, there exist positive integers s and t such that s > t and $f^s(y) = f^t(y)$. Then $f^t\left(f^{s-t}(y)\right) = f^t(y)$. Hence, $f^{s-t}(y) = y$ since by Theorem 12, f^t is injective. Let x = $f^{s-t-1}(y)$ ∈ A. Then f(x) = y. Hence, f is surjective.

Exercise.

1. Given f : X $\to$ Y and A, B $\subset$ X, prove that

(i) f(A∪B) = f(A)∪f(B),

(ii) f(A∩B) $\subset$ f(A)∩f(B),

(iii)f(A \ B) $\subset$ f(A) \ f(B) if f is injective.

2. Given f : X $\to$ Y. Let S $\subset$ Y. Define f^{-1}(S) = { x ∈ X : f(x) ∈ S}. Let A, B $\subset$ Y. Prove that

(i) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$,

(ii) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$,

(iii) $f^{-1}(A \backslash B) = f^{-1}(A) \backslash f^{-1}(B)$.

Let f : Z $\to$ Z be a mapping defined by $f(x) = \begin{cases} x & if\ x\ is\ even \\ 2x+1 & if\ x\ is\ odd \end{cases}$

3. for all x ∈ Z. Find a left inverse of f if one exists.
4. Let f : Z $\to$ Z be a mapping defined by $f(x) = x + |x|$ for all x ∈ Z. Find a right inverse of f if one exists.

Let X and Y be nonempty sets and $f : X \to Y$. If $T \subset X$, then f(T) denotes the set $\{ f(x) : x \in T \}$. f(T) is called the image set of T under f. Prove that f is injective if and only if) $f(A \cap B) = f(A) \cap f(B)$ for all nonempty sets A and B of X.

References.

1.S. K. Mapa. Higher Algebra, Abstract and Linear, Sarat Impressions Pvt.Ltd.1984

2.D. S . Malik, J N. Mordeson, M. K. Sen. Fundmentals of Abstract Algebra. McGraw-Hill International Editions, 1997.

.