(9) Group: A monoid in which every element has inverse

A Group $(G, *)$ is a algebraic system in which a binary operation $*$ satisfies the following

(i) Associative : $(x * y) * z = x * (y * z)$ for $x, y, z \in G$

(ii) Identity : $x * e = e * x = x$ (e is identity element)

(iii) Inverse : $x^{-1} * x = x * x^{-1} = e$

→ let $(G, *)$ is cyclic group

a is generator

let $x, y \in G$ as G is cyclic $x = a^m$ $y = a^n$ for m, n in $\mathbb{Z}$

so, $x * y = a^m * a^n = a^{m+n}$

$y * x = a^n * a^m = a^{m+n}$

$x * y = y * x$ (commutative)

(4) Reflexive : aRa

Symmetric : $aRb \quad bRa$

Transitive : $aRb \quad bRc \quad aRc$

} Equivalence

anti symmetric : $aRb \quad bRa$ then $a=b$

asymmetric : $aRb \quad b \not R a$

irreflexive : $a \not R a$

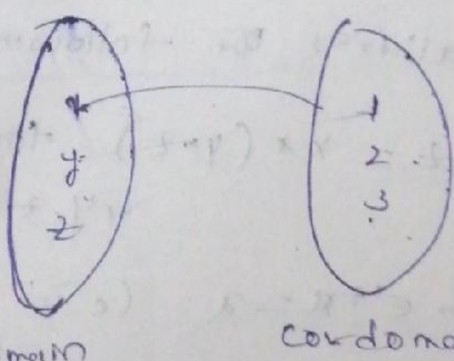
Reflexive, antisymmetric, transitive — partial ordering relation

Spl relations

Reflexive, transitive, antisymmetric } partial order

Reflexive, transitive, symmetric } Equivalence relation

A   B $f: A \to B$



Domain   Codomain

One-one (injective)

onto (surjective)

Bijective

one-one every element in domain has different images in co-domain

on-to: every element in co-domain has pre-image in domain.

Range = Co-domain

PO set (partially ordered set)

If we take any set with partial ordering relation.

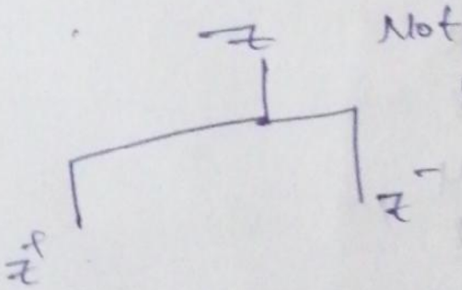
→ when partial ordering relation exists b/w sets there are comparable otherwise incomparable

Totally ordered set: when every element in the set is comparable

ex: $(Z, \leq)$

Well-orderd set: If we take any set with any relation. every ~~elem~~ subset of the set has minimal elements.

ex.



Not well ordered

Z^+ - well ordered set

poset - example:

The set of N natural numbers with relation $\leq$ is a poset because

$x \leq x$ (reflexive)

$x \leq y,\ y \leq x$ $\quad x = y$ (anti symmetric)

$x \leq y,\ y \leq z$ $\quad x \leq z$ (transitive)

$x, y, z \in N$

$(P(S), \subseteq)$ is a poset.

(8) order of a element: let $(G, *)$ be a group and a be an element of G, then the order of the element a is the smallest positive integer n for which $a^n = e$ if such an integer exists and is denoted by $O(a)$

$$\begin{array}{ccc} & \text{order} & \\ \swarrow & & \searrow \\ \text{finite} & & \text{infinite} \\ a^n = e & & a^n \neq e \end{array}$$

$(Z_8, +_8)$

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$\frac{a+b}{8}$ ~~8~~ 8

$1 \to 8$
$2 \to 4$
$3 \to 8$
$4 \to 2$
$5 \to 8$
$6 \to 4$
$7 \to 8$

(3) $R = \{(a, b) \mid \underbrace{a \equiv b \pmod m}_{\text{congruence relation}}\}$ is equivalence relation

reflexive, transitive, symmetric $\}$ $aRb \quad bRa$

<u>congruence.</u> $a \equiv b \pmod m$

$a - b$ is divisible by m

<u>reflexive</u> :- $a - a = 0$ is divisible by m
$a \equiv a \pmod m$

<u>~~transitive~~</u>: $(a - b)$ is divisible by m

<u>symmetric</u>: $-(a - b)$ is divisible by m
$(b - a)$ is divisible by m

$a \equiv b \pmod{m}$

$b \equiv a \pmod{m}$

transitive: $a \equiv b \pmod{m}$ $b \equiv c \pmod{m}$

$(a-b)$ is divisbly by m

$(b-c)$ is divisible by m

~~$(a-c)$~~ is

$a-b+b-c = a-c$ is divisible by m

$(a-c)$ ~~is~~ divisible by m

$a \equiv c \pmod{m}$

$\therefore$ congurance relation is a equivalence relation.