



## Set Theory

→ A set is a collection of objects called its members

→ A set is an object.

$$a \in A \quad a \notin A.$$

Principle of Extensionality :- For any 2 sets  $A \& B$  if for every object  $x$ ,  $x \in A$  iff  $x \in B$   
then  $A = B$ .

Empty set :- A set with no members exists  
— empty set  $\emptyset$

$$\boxed{\emptyset \neq \{\emptyset\}}$$

\* If every member of  $A$  is also a member of  $B$  then  
 $A \subseteq B$  subset.  
and  $B \supseteq A$  superset.

If  $A \neq B$  and  $A \subseteq B$  then  $A \subset B$ ,  $A \subsetneq B$   
( $A$  is a proper subset of  $B$ ).

$A \cup B$  : the set of all of objects in  $A$  or in  $B$

$A \cap B$  : \_\_\_\_\_ and in  $B$

$U - A$  : \_\_\_\_\_ not in  $A$ , but in  $U$

\*  $A$  stands for a predicate  $\alpha(x)$

$$x \in A$$

↳ First order predicate with one variable.

$$A \equiv \{x \mid \alpha(x)\}$$

$$A \cup B \equiv \{x \mid \alpha_A(x) \vee \alpha_B(x)\}$$

#  $U \equiv V$  (union corresponds to OR)

$\cap \equiv \wedge$  (intersection corresponds to AND)

$U^- \equiv \neg$  (complement corresponds to NOT)

$U, \cap, U^-$  ] Define Boolean algebra

## Properties:

- ①  $A \cap U = A$        $A \cup \emptyset = A$       (Identity)  
 $x \wedge 1 = x$        $x \vee 0 = x$
- ②  $A \cup U = U$        $A \cap \emptyset = \emptyset$       (Domination)
- ③  $A \cup A = A$        $A \cap A = A$       (Idempotent)
- ④  $U - (U - A) = A$       (Double negation law)
- ⑤  $A \cup B = B \cup A$       (commutative)  
 $A \cap B = B \cap A$
- ⑥  $A \cup (B \cup C) = (A \cup B) \cup C$       (associative)  
 $A \cap (B \cap C) = (A \cap B) \cap C$
- ⑦  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$       (Distributive)
- ⑧  ~~$U - (A \cap B) = (U - A) \cup (U - B)$~~       (DeMorgan's law)  
 $U - (A \cup B) = (U - A) \cap (U - B)$
- ⑨  $A \cup (A \cap B) = A$       (Absorption)  
 $A \cap (A \cup B) = A$
- ⑩  $A \cup (U - A) = U$       (Negation)  
 $A \cap (U - A) = \emptyset$

The Power set:  
 The set of all subset of  $A$        $|A| = n$   
 $2^A$        $P(A)$       then  $|2^A| = 2^n$   
 is the power set of  $A$ .

$$\cup_A = \{x \mid \exists b (\text{ } b \in A \wedge x \in b)\}$$

↳ union of all members of members of  $A$

e.g.  $\cup \{\underbrace{\{2, 3\}}_{\text{set}}, \underbrace{4}_{\text{not a set}}, \{5\}\} = \{2, 3, 5\}$

$$\cap_A = \{x \mid \forall b \in A (x \in b)\}$$

↳ every member of  $A$  has to be set.  $x$  should belong to every set of  $A$ .

Embedding of Natural no.s in set Theory

→ successor operator  
for set  $a$   $a^+ = a \cup \{a\}$ .

$$a = \{2, 3, 4\}$$

$$a^+ = \{\{2, 3, 4\}, \{2, 3, 4\}\}$$

→ inductive:

A set  $A$  is inductive

if  $\emptyset \in A$

and  $\forall a (a \in A \rightarrow a^+ \in A)$

$A$  is closed under  
the successor  
operator

$$\omega = \bigcap \{A | A \text{ is inductive}\}$$

$x \in \omega$  iff  $x$  belongs to every inductive set.

∴  $\omega$  is a subset of every inductive set.

\*  $\omega$  is inductive

$$\emptyset \in \omega$$

$$a \in \omega \rightarrow a \text{ belongs to all IS,}$$

$$a^+ \in \omega \leftarrow a^+ \text{ belongs to all IS,}$$

\*  $x \subseteq \omega \wedge x$  is inductive  $\rightarrow x = \omega$

OR No proper subset of  $\omega$  is inductive.

\*  $\omega$  is the smallest inductive set.

How  $\omega$  looks like?

$$0 = \emptyset \in \omega$$

$$1 = 0^+ = \emptyset^+ \in \omega \quad \emptyset^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\}$$

$$2 = 1^+ = 0^{++} \in \omega \quad \emptyset^{++} = \emptyset^+ \cup \{\emptyset^+\} = \{\emptyset\} \cup \{\{\emptyset\}\}$$

$$= \{\emptyset, \{\emptyset\}\}$$

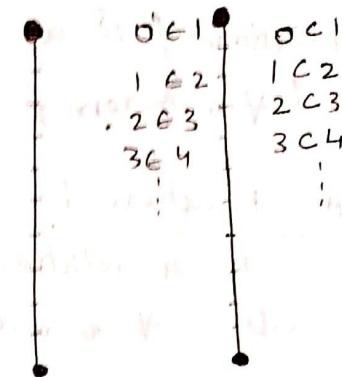
$\emptyset = \phi$

$$1 = \{\emptyset\} = \{0\}$$

$$2 = \{\emptyset, \{\emptyset\}\} = \{\emptyset, 1\}$$

$$3 = \{\emptyset, 1, \{\emptyset, 1\}\} = \{0, 1, 2\}$$

$$n = \{0, 1, 2, \dots, n-1\}$$



For any two distinct objects  $x, y$

$\{x, y\}$  — unordered pair

ordered pair:

$$(x, y) := \{x, \{x, y\}\}$$

A relation is a set of ops  
 $\text{dom } R = \{x \mid \exists y. (x, y) \in R\}$   
 $\text{ran } R = \{y \mid \exists x. (x, y) \in R\}$

field of  $R$

$$\text{fld } R = (\text{dom } R) \cup (\text{ran } R)$$

$A \times B$ : The set of all ops. set.  $\rightarrow$   $\text{set.}$   
the first is from  $A$ , the 2nd is from  $B$ .

$\star R$  from  $A$  to  $B$  is a subset of  $A \times B$

$\star$  A binary relation  $R$  on  $A$  is a subset of  $A \times A$ .

Extending to  $n$  elements:

$$(a, b, c) = ((a, b), c)$$

$$(a_1, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$$

$$(a_1, \dots, a_n) = (a_1, (a_2, (a_3, \dots, (a_{n-1}, a_n))))$$

$n$ -ary relation:

$$(A_1 \times \dots \times A_n) = (A_1 \times \dots \times A_{n-1}) \times A_n$$

If  $A_1, A_2, \dots, A_n \subseteq A$  then the  $n$ -ary relations can be written as:  $A^2, A^3, \dots$

A function  $f$  is a relation s.t.  
 $(\forall x \in \text{dom } f) (\exists! y (x, y) \in f)$

# A Function  $F$   
is a relation  
s.t.  $\forall x \in \text{dom } F (\exists! y x F y)$

$F(x)$ : the unique  $y$  s.t.  $x F y$ .

$F$  maps  $A$  into  $B$ , if  $\text{dom } F = A$  and  $\text{ran } F \subseteq B$   
 $F$  maps  $A$  onto  $B$ , if  $\text{dom } F = A$  and  $\text{ran } F = B$

\* A set  $R$  is single rooted  
if for each  $y \in \text{ran } R$ .

$\exists! x$  s.t.  $(x, y) \in R$ .

$\{(2, 0), (2, 1), e\}$  is single rooted.

\* A function that is 1-rooted is 1-1.

Bijection = one-one, onto

Injection = one-one, into

Surjection = onto

bijection iff injection and surjection

#  $F^{-1} = \{(u, v) \mid (v, u) \in F\}$

#  $F \circ G = \{(u, v) \mid (u, t) \in G \text{ and } (t, v) \in F \text{ for some } t\}$

# the restriction of set  $F$  to set  $A$

$F \upharpoonright A = \{(u, v) \mid (u, v) \in F \wedge v \in A\}$

#  $F[A]$  image of  $A$  under  $F$

=  $\text{ran } F \upharpoonright A = \{v \mid \exists u \in A (u, v) \in F\}$

1) For a set  $F$ :

$$\text{dom } F^{-1} = \text{ran } F$$

$$\text{ran } F^{-1} = \text{dom } F$$

2) For a relation  $F$ ,

$$(F^{-1})^{-1} = F$$

3) For a set  $F$ ,  $F^{-1}$  is a function iff  $F$  is 1-rooted.

4) if  $F$  is a 1-1 function,

$$\text{if } x \in \text{dom } F, \text{ then } F^{-1}(F(x)) = x$$

$$\text{if } y \in \text{ran } F, \text{ then } F(F^{-1}(y)) = y$$

5) if  $F$  and  $G$  are functions,  
then  $F \circ G$  is a function

There  $\circ$  - composition  
is an operator on set of  
functions. (it is closed)

its domain :-

$$\{x \in \text{dom } G \mid G(x) \in \text{dom } F\}$$

for  $x \in \text{dom } F \circ G$

$$(F \circ G)(x) = F(G(x))$$

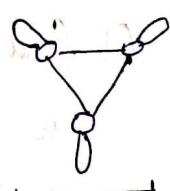
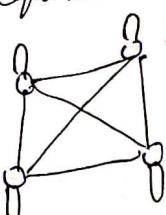
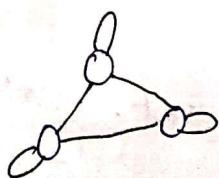
6) For any two sets  $F$  and  $G$

$$(F \circ G)^{-1} = G^{-1} \circ F^{-1}$$

- A binary rel<sup>n</sup> ~~on~~ R on A is reflexive if  $\forall x \in A (x R x)$
- A binary rel<sup>n</sup> ~~on~~ R on A is symmetric if  $\forall x, y \in A (x R y \rightarrow y R x)$
- A binary rel<sup>n</sup> ~~on~~ R on A is transitive if  $\forall x, y, z \in A (x R y \wedge y R z \rightarrow x R z)$

R is an equivalence relation if R satisfies all the above three properties.

Graphical interpretation of equivalence relation



equivalence class

# clique are being formed.

# If there is a path b/w  $x$  and  $y$  then there is  
a direct edge b/w them also.

# equivalence classes are being formed.

e.g.  $x R y \equiv x \equiv y \pmod{5}$

0	1	2	3	4	$\{0, 1, 2, 3, 4\}$
5	6	7	8	9	
10	11	12	13	14	$[0] \equiv \pmod{5}$
15	16	17	18	19	

$x \equiv x \pmod{5}$  (symmetric) (reflexive)

if  $x \equiv y$  then  $y \equiv x \pmod{5}$  (symmetric)

if  $x \equiv y$ ,  $y \equiv z \rightarrow x \equiv z \pmod{5}$  (transitive)

Trichotomy is a binary relation  $R$

Set.  $x R y$ ,  $x = y$ ,  $y R x$

exactly one holds  $\forall x, y \in A$

e.g.  $\subset \leq$

# If a relation is transitive and trichotomy : strict linear order

# Antisymmetry property

$\forall x, y (x R y \wedge y R x \rightarrow x = y) \rightarrow$  e.g.  $\leq$

# reflexive, antisymmetric, transitive  $\Rightarrow$  linear order

total order

successor

$$a^+ = a \cup \{a\}$$

inductive set : contains  $\emptyset$ , closed under

$$w = \cap \{\text{all inductive sets}\}$$

-  $w$  is inductive

-  $w$  is a subset of every inductive set.

$\omega$  is the "smallest" inductive set.  
 $\omega = \mathbb{N}$

$$\phi^0 = \emptyset \quad n = \{0, 1, 2, \dots, n-1\}$$

$$\phi^+ = \phi^{\phi^0} = 1 \quad \Rightarrow \quad 0 \in 1 \in 2 \in 3 \dots$$

$$\vdash = \phi^{+\phi^+} = \varphi_2 \quad 0 \in 1 \in 2 \in 3 \dots$$

successor  $\vdash = +1$

$$m+n = m^{+(n)}$$

$m \times n = +$  operators applied on  $m$  itself  $(n-1)$  times.

$$m \times 1 = m \quad m \times 2 = m^{+(m)}$$

## Integers in Set Theory

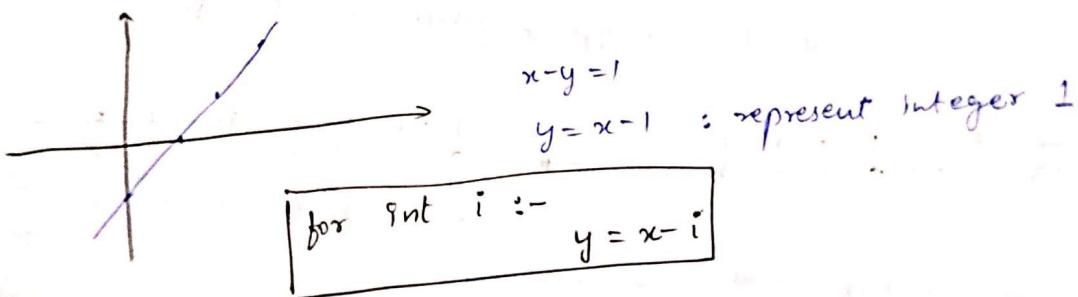
$\sim$  on  $\mathbb{N} \times \mathbb{N}$

$$(m, n) \sim (p, q) \text{ iff } m+p = n+q$$

equivalence rel<sup>n</sup>

$$(2, 3) \sim (3, 2) \quad (2, 1) \sim (-1, 0)$$

$$(1, 2) \sim (-1, -1)$$



## Integer addition:-

$$+_z : \frac{[(m, n)]}{m-n} \times_z \frac{[(p, q)]}{p-q} \rightarrow \frac{[(m+p, n+q)]}{m+p - n-q}$$

$$\times_z : \frac{[(m, n)]}{m-n} \times_z \frac{[(p, q)]}{p-q} \rightarrow \frac{[(mp + nq, pn + mq)]}{m-p - n-q}$$

$$*_z = \mathbb{N} \times \mathbb{N} / \sim$$

$$+_z : \frac{[(m, n)]}{m-n} +_z \frac{[(p, q)]}{p-q} = \frac{[(m+p, n+q)]}{m+p - n-q}$$

$$[(m, n)] \times_z [(p, q)] = \frac{[(mp + nq, pn + mq)]}{m-p - n-q}$$

natural Number multiplication

$x_z$  is commutative, associative  
 $x_z$  distributive over  $+_z$

$$[(2, 1)]_z = -1_z \text{ is id of } x_z$$

$$[(1, 1)]_z = 0_z \neq 1_z$$

$(\mathbb{Z}, +_z, x_z, 0_z, 1_z)$  form an integral domain.

\*  $[(m, n)]_z <_z [(p, q)]_z \rightarrow$  Trichotomy and Transitivity  
 $\Rightarrow$  strict linear order

when  $m+nq \in n+nq'$

$$m-n < p-q$$

$$m+nq <_n p+nq'$$

$\Rightarrow m+nq \in p+nq$  (w.r.t natural numbers)

\*  $\mathbb{Z}$  is countable

( $S$  is countable iff  
 $\exists$  a 1-1 mapping from  $S$  onto  $\mathbb{N}$ )



# One-One and onto mapping

### Rational Number

$$q = \frac{p}{q} \text{ where } p, q \in \mathbb{Z} \quad q \neq 0$$

$$\mathbb{Z}' = \mathbb{Z} - \{0_z\}$$

$$(a, b) \bowtie (c, d)$$

↓  
bow tie!

$$a, c \in \mathbb{Z}$$

$$a, b, c, d \in \mathbb{Z}'$$

stands for stands for

$$\frac{a}{b} = \frac{c}{d}$$

iff  $a x_z d = b x_z c$

$(a, b) \bowtie (a, b)$   
 $(a, b) \bowtie (c, d) \rightarrow (c, d) \bowtie (a, b)$   
 If  $(a, b) \bowtie (c, d)$  and  $(c, d) \bowtie (e, f)$  then  $(a, b) \bowtie (e, f)$

$$(\mathbb{Z} \times \mathbb{Z}')/\bowtie = \emptyset$$

$$\frac{1}{3} \equiv \{(1, 3), (2, 6), (3, 9), \dots\}$$

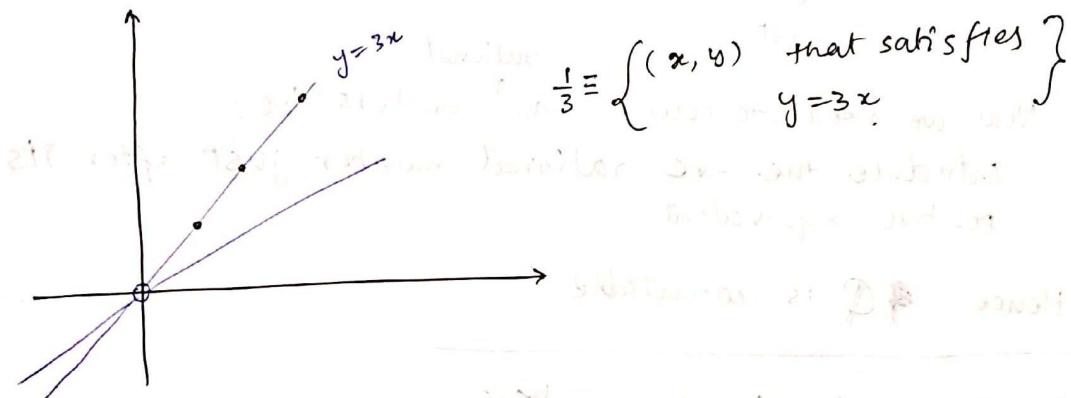
$$\quad \quad \quad (-1, -3), (-2, -6), \dots$$

$$3 \equiv \{(3, 1), (6, 2), (9, 3), \dots\}$$

$$\quad \quad \quad (-3, -1), (-6, -2), (-9, -3), \dots$$

In general  $p/q \equiv \{(p, q), (2p, 2q), (3p, 3q), \dots\}$

$$\quad \quad \quad \{(-p, -q), (-2p, -2q), \dots\}$$



---

$+_\bowtie : [(a, b)]_\bowtie +_\bowtie [(c, d)]_\bowtie = [(\underline{ad+bc}, \underline{bd})]_\bowtie$

$$\frac{a}{b} + \frac{c}{d} = \frac{\underline{ad+bc}}{\underline{bd}}$$

Integer addition and multiplication

$\times_\bowtie : [(a, b)]_\bowtie \times_\bowtie [(c, d)]_\bowtie = [(ac, bd)]_\bowtie$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

$(\emptyset, +_\bowtie, \times_\bowtie, 0_\bowtie, 1_\bowtie)$  field

---

$[(a, b)]_\bowtie <_\bowtie [(c, d)]_\bowtie \text{ iff } ad <_z cb$

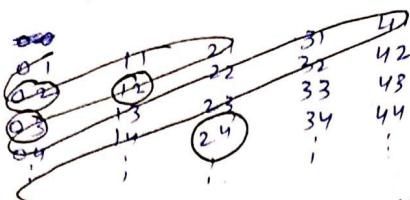
$(a < c \Rightarrow ad < bc)$  Trichotomy and Transitive

Linear Order

$\mathbb{Q}$  is countable

Consider

$$\mathbb{N} \times \mathbb{N}^+$$



When we count in this manner, we are going through every rational number in 1st quadrant.

but we need a 1-1 mapping, i.e., a number should be counted only once.

→ First assign numbers in the pattern as above, then remove the numbers/mapping for equal numbers except when encountered first.

Now we need to count -ve numbers too;

introduce the -ve rational number just after its positive equivalent.

Hence  $\mathbb{Q}$  is countable

There are irrational numbers.

$\sqrt{2}$  is irrational

$$\sqrt{2} = \frac{p}{q} \quad \gcd(p, q) = 1$$

$$p = \sqrt{2}q$$

$$p^2 = 2q^2 \Rightarrow p^2 \text{ is an even square}$$

$$\Rightarrow p^2 = (2k)^2 = 4k^2$$

$$\text{thus } 4k^2 = 2q^2$$

$$2k^2 = q^2 \Rightarrow q^2 \text{ is an even number}$$

( $q$  is also even)

thus  $p$  and  $q$  both are even

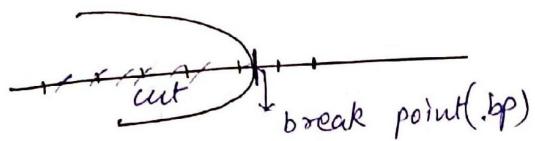
→ they have 2 as a common factor

Contradiction to the fact

Real Numbers      Done using Dedekind cuts

Dedekind Cut :- is a subset of  $\mathbb{Q}$  such that

- ①  $\emptyset \neq x \neq \mathbb{Q}$
- ②  $x$  is closed downwards  
 $\forall q_1, q_2 \in \mathbb{Q} ((q_1 \in x) \wedge (q_2 < q_1) \rightarrow (q_2 \in x))$ .
- ③  $x$  has no largest member belonging to  $\mathbb{Q}$



$\mathbb{Z} =$  the set of all rational number less than 3

Every dedekind cut is a real number.  
Set of all dedekind cut is equal to set of all ~~rational~~ real numbers

$\mathbb{R}$  is uncountable.  
(0,1)

$$\begin{array}{ccccccc} 1 & 0, & a_1 & a_2 & a_3 & a_4 & \dots \\ 3 & 0, & b_1 & b_2 & b_3 & b_4 & \dots \\ 4 & 0, & c_1 & c_2 & c_3 & c_4 & \dots \end{array}$$

construct a. number as:-  
1st digit is not equal to the 1st rational  
2nd digit is not equal to the 2nd rational  
3rd digit is not equal to the 3rd rational

In this way, we can find that the number that we constructed has never been counted.  
thus  $(0,1)$  is uncountable  
 $\Rightarrow \mathbb{R}$  is uncountable

## Dedekind cut (continued)

if the break point (bp) is rational;  
then the complement of the cut includes the b,

- \* the set of all Dedekind cuts  $\equiv R$

#  $r <_R s$  iff.  $r \in S$   
 $\Rightarrow$  strict linear order

#  $x +_R y = \{ q+r \mid q \in x \text{ and } r \in y \}$

#  $x \times_R y = \{ qr \mid \begin{array}{l} 0 \leq q \in x \\ 0 \leq r \in y \end{array} \} \cup 0_R$

$\rightarrow$  if  $x$  and  $y$  are non negative real

# If both  $x$  and  $y$  are negative real, then

$$x \times_R y = |x| \times_R |y|$$

$$\# x \times_R y = -|x| \times_R |y|$$

- \*  $(R, +_R, \times_R, 0_R, 1_R)$  is a field.

## Naive Set Theory

- By Georg Cantor

$\{x \mid a(x)\} \rightarrow$  this is the base for defining sets.

$\rightarrow$  this has many problems and paradoxes:-

One of them is — Berry's Paradox

$A = \{x \mid x \in N \text{ and } x \text{ can be defined in at most } 10^3$   
characters\}

$n =$  the smallest member/natural no. defined  $< 10^3$   
 $\downarrow$  not

## Russell's Paradox

$$S = \{x \mid x \notin x\}$$

Abnormal: Self membership. (Paradox)  
 $s \in S \text{ iff } s \notin s$

## \* Russells Type theory

## \* Zermelo Fraenkel Axioms of set Theory

### ① Extensionality Axiom

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

### ② Empty Set Axiom

$$\exists x \forall y (y \notin x)$$

### ③ Pairing Axiom

$$\forall x \forall y \exists z \forall u (u \in z \leftrightarrow u = x \vee u = y)$$

given any two elements, we can pair them  
into a set (an unordered pair)

### ④ Power Set Axiom

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$$

### ⑤ Subset Axiom Schema

for any formula  $\alpha$  with free variable  $x$ ,  
the following is an axiom

$$\forall t_1 \dots \forall t_k \forall u \forall x (\forall y (y \in x \leftrightarrow y \in u \wedge \alpha(t_1, \dots, t_k, y, x)))$$

= for every set  $u$ , there is a subset  $x$  s.t.  
 $y \in x$  iff  $y \in u \wedge \alpha(t_1, \dots, t_k, y, x)$

\* e.g.  $\{x \mid x \notin x\}$  → the above axiom says that you  
cannot talk about self membership in the complement  
in unrestricted manner.

$$\neg \exists y \forall x (x \in y \leftrightarrow x \notin x)$$

and hence  $\neg \exists y$

$\forall t \forall u \exists x \exists y (y \in x \leftrightarrow y \in t \wedge y \in u)$   
there exist intersection  $t$  and  $u$

⑥ Union Axiom :- there exist  $y$  ~~such~~ that is made of members of members of  $x$

⑦ Infinity Axiom :- there exist an inductive set

⑧ Regularity Axiom :- Every non-empty set  $x$  has a member  $y$  s.t.  $x \cap y = \emptyset$

# For any formula  $\psi(x, y)$  in which  $\exists$  is not free

if every member of  $x$  has a nomine then there is a set made up of these nominees.

⑨ Axiom of choice : For any relation  $R$ , there is a function  $F \subseteq R$  s.t.  $\text{dom } F = \text{dom } R$

Relation  $R$  on  $A$  :-

is reflexive if  $\forall x \in A (x R x)$

antisymmetric if  $\forall x, y \in A (x R y \wedge y R x \rightarrow x = y)$

transitive if  $\forall x, y, z \in A (x R y \wedge y R z \rightarrow x R z)$

then  $R$  is partial order on  $A$

$A$  is a partially ordered set (poset) w.r.t.  $R$

e.g.  $(N, \leq)$

For any

$x, y \in A$

$\forall t \forall u \exists x \exists y (y \in x \rightarrow y \in t \wedge y \in u)$   
there exist intersection  $t$  and  $u$

⑥ Union Axiom :- there exist  $y$  ~~set~~. that is made up  
members of members of  $x$

⑦ Infinity Axiom :- there exist an inductive set

⑧ Regularity Axiom :- Every non-empty set  $x$  has a  
member  $y$  s.t.  $x \cap y = \emptyset$

# For any formula  $\psi(x, y)$  in which  $z$  is not free

If every member of  $x$  has a nominee then  
there is a set made up of these nominees.

⑨ Axiom of choice : For any relation  $R$ , there is a  
function  $F \subseteq R$  s.t.  $\text{dom } F = \text{dom } R$

Relation  $R$  on  $A$  :-

is reflexive if  $\forall x \in A (x R x)$

antisymmetric if  $\forall x, y \in A (x R y \wedge y R x \rightarrow x = y)$

transitive if  $\forall x, y, z \in A (x R y \wedge y R z \rightarrow x R z)$

then  $R$  is partial order on  $A$

$A$  is a partially ordered set (poset) w.r.t.  $R$

e.g.  $(\mathbb{N}, \leq)$

For any  $x, y \in A$   
 $x R y \vee y R x$   
Not necessarily

\*  $a \rightsquigarrow b$       a precedes b  
or b succeeds a.

$b \geq a$        $\succeq = \rightsquigarrow^{-1}$  ] → dual

Trichotomy :  $a R b$  xor  $b R a$  xor  $a = b$

\*  $\star$  reflexive, transitive :- quasi order

\* quasi order with trichotomy :- strict partial order

$a < b \equiv a \leq b \text{ and } a \neq b$

e.g.  $\subseteq$  on  $2^A$        $\rightarrow$  partial order  
 $A = \{a, b\}$

$$2^A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$\{a\} \neq \{b\}$

e.g. Divides on  $\mathbb{N}^+$        $\rightarrow$  partial order

$$x | n$$

$$x | y \wedge y | x \rightarrow x = y$$

$$x | y \wedge y | z \rightarrow x | z$$

Hasse diagram

S is a poset

$$a, b \in S$$

$a$  is an immediate predecessor of  $b$  ( $a << b$ )

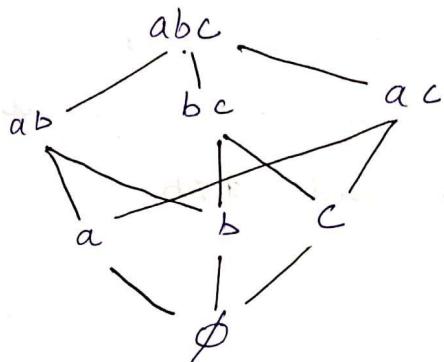
$a$  is an immediate successor of  $b$  ( $a >> b$ )

if  $a < b$  and  $\nexists c (a < c < b)$

$b$  is an immediate successor of  $a$  ( $b >> a$ )

## Directed Graph

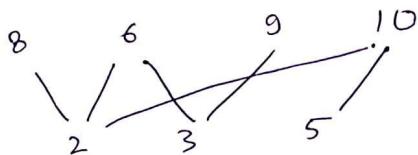
Take a vertex for each  $a \in S$   
 If  $a \ll b$  then construct  $(a, b) \in E$   
 $(a \rightarrow b)$



we can draw  
all order pairs  
using transitivity.

# we do not draw  
a direct edge from  
a to abc ; but  
there is an intermediate  
path via ab or ac .

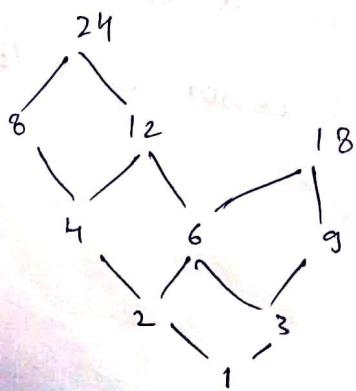
e.g. divide Relation :-



# since  $\mathbb{N}$  has infinite elements, Hasse diagram seems useless.

But when there are finite elements, Hasse diagram seems good to implement.

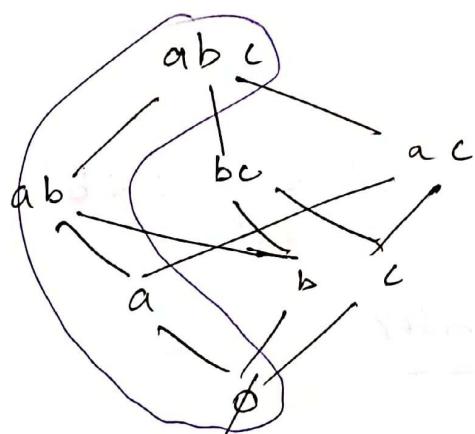
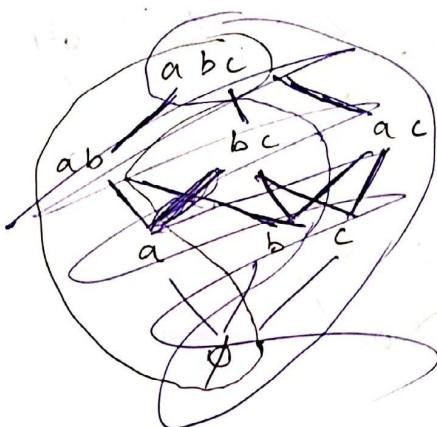
e.g. restriction of  $|$  onto  $\{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$



# a and b are comparable in R if  
 $aRb$  or  $bRa$ . (and can have a path)  
 12 and 18 are incomparable  $12 \parallel_R 18$

- \* Total order // linear order has every pair comparable while this need not be a case in proper partial order.
- \* every subset of linear order is a linear order.

But — A linear order taken from a partial order through restriction is a chain of the POSET.



Anti-chain: of a poset is a subset - no two elements of which are comparable

## Ordering of ordered tuples

### 1. Product order

$s, t$  are both linearly ordered sets.

$$s \times t \quad (a, b) \leq (a', b') \text{ iff } a \leq a' \text{ and } b \leq b'$$

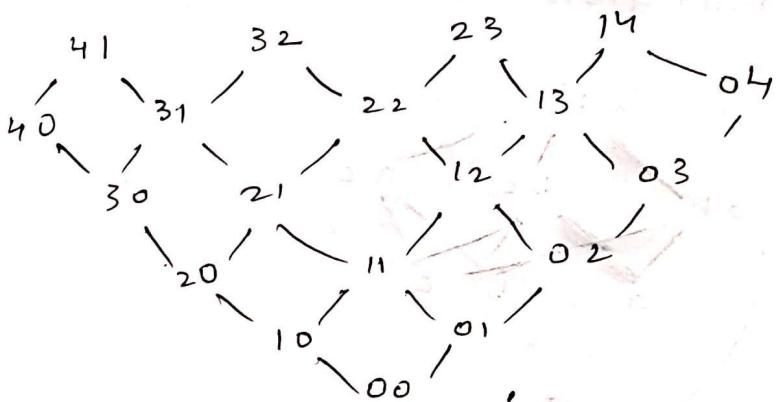
$$a \leq a'$$

$$\text{and } b \leq b'$$

$41 \quad 32 \quad 23 \quad 14 \rightarrow \text{Not comparable}$

$$\begin{array}{c} 4 \\ \downarrow \\ 4 \geq 3 \\ \text{but } 1 \leq 2 \end{array}$$

But



### 2. Lexicographic order

$$(a, b) \leq (a', b')$$

If  $a < a'$  or  $a = a'$  and  $b < b'$

$\begin{matrix} 20 \\ 1n \\ 12 \\ 11 \\ 10 \\ 0n \\ 02 \\ 01 \\ 00 \end{matrix}$

Linear order

String: finite sequence of symbols

alphabet  $A = \{a, b, c\}$

$A^*$  = {

- $\epsilon \rightarrow$  string of zero length
- $a, b, c \rightarrow$  unit length.  $(3 \times 1)$
- $aa, ab, ac$
- $ba, bb, bc$   $\rightarrow$  2 unit length  $(3 \times 3)$
- $ca, cb, cc$
- $- 3$  unit length  $(3 \times 3 \times 3)$

}

$A^*$   $\rightarrow$  kleene closure of  $A$

Lexicographic order:

$$\# \quad u = a^u, \quad a, b \in A$$

$$v = b^v$$

$$u, v, u', v' \in A^*$$

$u < v$  iff  $a < b$  or  $a = b$  and  $u' < v'$

$\epsilon < w$  for any non empty  $w$

e.g. cat  $<$  catch

at  $<$  atch

t  $<$  tch

$\epsilon < ch$



Short lexi. order

=

$u < v$  if  $|u| < |v|$

or  $|u| = |v|$

and  $u$  precedes  $v$   
lexicographically

finite poset  $S$

Draw the Hasse diagram.

it is a Directed Acyclic Graph.

Topographically sorted

when  $f(a) < f(b)$

Strings :- A finite sequence of symbols

alphabet  $A = \{a, b, c\}$

$A^* = \left\{ \begin{array}{l} \epsilon \rightarrow \text{string of zero length} \\ a, b, c \rightarrow \text{unit length. } (3 \times 1) \\ aa, ab, ac \\ ba, bb, bc \\ ca, cb, cc \end{array} \right. \begin{array}{l} \rightarrow 2 \text{ unit length } (3 \times 3) \\ \rightarrow 3 \text{ unit length } (3 \times 3 \times 3) \end{array} \right\}$

$A^*$  → kleene closure of  $A$

Lexicographic order:

#  $u = a u'$ ,  $a, b \in A$

$v = b v'$

$u, v, u', v' \in A^*$

$u < v$  iff  $a < b$  or  $a = b$  and  $u' < v'$

$\epsilon < w$  for any non empty  $w$

e.g. cat < catch

at < atch

t < tch

ε < ch

Short lex. order

$u < v$  if  $|u| < |v|$

or  $|u| = |v|$

and  $u$  precedes  $v$   
lexicographically

finite poset  $S$

Draw the Hasse diagram.

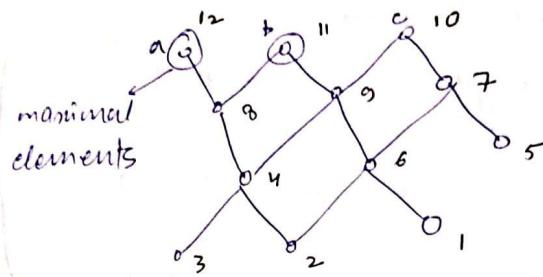
It is a Directed Acyclic Graph.

Topographically sorted

$a < b$  then  $f(a) < f(b)$

### Maximal Element

a es is maximal if ~~forall  $x \in A$~~   $\nexists x (x \geq a)$



$\begin{cases} a & b & c \\ \downarrow & & \\ \text{all 3 are} & \text{maximal, we} & \text{can pick any of} \\ \text{these three} & & \end{cases}$

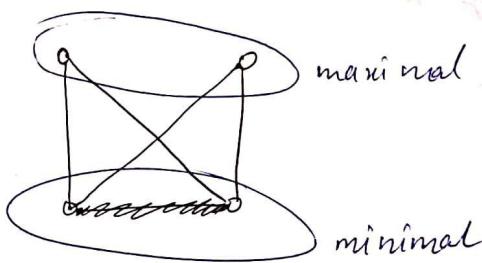
Pick a maximal  $\rightarrow$  name is  $n$   
then rest can be numbered.

Basis :-  $\underline{n = 1}$

$\rightarrow$  Consistent enumeration of partially ordered set.

### Minimal element :-

if  $\nexists x \in A (x \leq a)$



Chain :- A subset of the poset that is in Linear Order

Antichain :- A subset of the poset s.t. no 2 members of it are comparable.

if a poset has a chain of length  $n$

then it has  $n$  disjoint anti-chain

$\rightarrow$  Remove all the maximal length (then they will form an antichain)

now the path with  $n$  nodes will loose 1 node

$\Rightarrow$  By induction they will have  $n-1$  anti-chains

$\Rightarrow$  we have a total of  $n-1+1$  anti-chains

If a finite poset has  $nm+1$  elements at least,

then either it has a chain of length  $n$  or it has an antichain of size  $n$ .

Proof  $\Rightarrow$

Assume that it is wrong  $\rightarrow$

suppose that it has the maximum

chain length =  $n$

then we can have a total of  $n-1$  antichains.

If each antichain has elements  $\leq m$

then total elements  $\leq m(n)$

$\leq nm$

But total number of elements =  $nm+1$

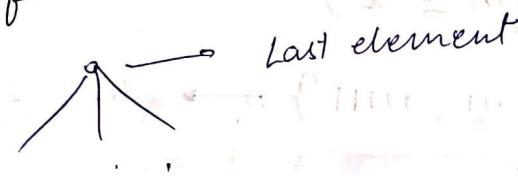
thus we have a contradiction.

# The first element of a poset is an element  $a$

set.  $\forall x \in S (a \leq x)$

If the number of minimal elements = 1, then that element is the first element,

similarly of last element.



First element

e.g. integer  $\rightarrow m \in \mathbb{N}^+$

suppose  $m = m_1 + m_2 + \dots + m_k$

assume  $m_1 \geq m_2 \geq \dots \geq m_k$

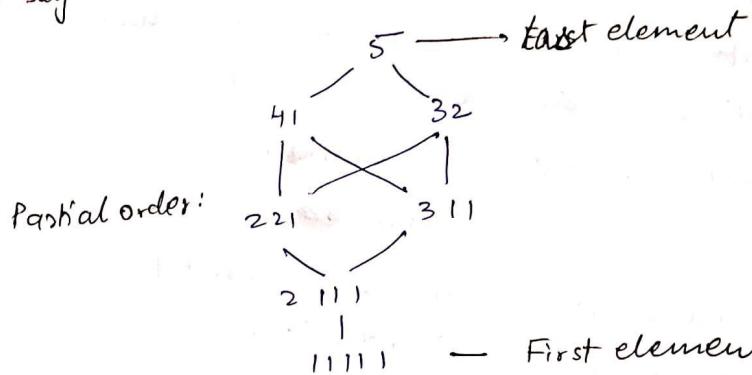
then we say the sequence  $m_1, m_2, \dots, m_k$  is a partition of  $m$

$P_1 \leq P_2 \rightarrow$  if  $P_1$  is a refinement of  $P_2$   
 (Take  $P_2$ , split some of integers)

e.g.  $m = 5$   
 $\Rightarrow 5 = 4 + 1$

$$5 = 2 + 2 + 1$$

Then say :-  $221 \leq 41$



$M$  is an upper bound of  $A \subseteq S$ ,  
 if  $\forall x \in A (M \geq x)$

$$\{41, 32\} \rightarrow 5$$

↓  
upper bound

$m$  is a lower bound of  $A \subseteq S$   
 if  $\forall x \in A (m \leq x)$

$$\underbrace{\{221, 311, 2111, 11111\}}_{LB} \rightarrow \{41, 32\} \xrightarrow{UB} 5$$

$$\underbrace{\{221, 311\}}_{LB} \xrightarrow{UB} 41, 32, 5$$

$$\xrightarrow{LB} 2111, 11111$$

Supremum ( $A$ ) :-

LUB / Least Upper Bound ( $A$ )

is an UB of  $A$  that precedes every UB of  $A$

$$\{41, 32\} \xrightarrow{\text{LUB}} 41, 32, 5$$

LUB Doesn't exist. ( $41$  and  $32$  are not comparable.)

Infimum (A) :-

GLB / Greatest Lower Bound (A)

is a LB of A that succeeds every LB of A

$$\{221, 311\} \xrightarrow{\text{LB}} 2111, 1111$$

GLB 2111

$$\{41, 32\} \xrightarrow{\text{LB}} 221, 311, 2111, 1111$$

GLB Doesn't exist ( $221$  and  $311$  are not comparable)

e.g.  $(\mathbb{N}^+, 1)$   
the set of VB(a, b) = the set of all common multiples

$$\text{LUB}(a, b) = \text{LCM}(a, b)$$

$$\text{GLB}(a, b) = \text{GCD}(a, b)$$

the set of LB(a, b) = the set of all common divisors of a and b.

Isomorphic Posets

$$f: X \rightarrow Y \quad 1 - 1$$

$$a \leq a' \rightarrow f(a) \leq f(a')$$

If  $a \parallel a'$  then  $f(a) \parallel f(a')$

An ordered set is well ordered if every subset has a first element.

# A well ordered set is a LO

Every subset of a WOS is a WOS.

If  $X$  is WO then  $Y \cong X$  (isomorphic)

If  $X$  is WO then  $Y$  is also WO.

- \* All WOs, of size  $n$  are isomorphic to  $\{1, 2, \dots, n\}$ .
  - \* If  $S$  is WO, then every  $a \in S$  other than the last of  $S$  has an imm. successor
- Proof :- take any element; say  $a$ , then take the set of all elements which succeeds  $a$ ; then this will be a subset of  $S$ , and since  $S$  is WO, this is also WO hence it will have a minimal that will be the immediate successor of  $a$ .

### Lattices

A lattice is poset in which every pair  $a, b$  has a GLB and a LUB.

→ Set of natural numbers under division.

$L$  is a non-empty set, closed under meet ( $\wedge$ ) and join ( $\vee$ )

$L$  is a ~~set~~ lattice if

$$(L1) \quad \begin{aligned} a \wedge b &= b \wedge a \\ a \vee b &= b \vee a \end{aligned} \quad \left. \begin{array}{l} \text{commutative} \\ \text{ } \end{array} \right\}$$

$$(L2) \quad \begin{aligned} a \wedge (b \wedge c) &= (a \wedge b) \wedge c \\ a \vee (b \vee c) &= (a \vee b) \vee c \end{aligned} \quad \left. \begin{array}{l} \text{associative} \\ \text{ } \end{array} \right\}$$

$$(L3) \quad \begin{aligned} a \wedge (a \vee b) &= a \\ a \vee (a \wedge b) &= a \end{aligned} \quad \left. \begin{array}{l} \text{absorptive} \\ \text{ } \end{array} \right\}$$

Swapping of  $\wedge$  with  $\vee$  in any theorem will also give us a theorem.

### Dual Theorems.

$$\left\{ \begin{array}{l} a \wedge a = \underline{a} \wedge (\underline{a} \vee (a \wedge b)) \underset{L3(b)}{=} \\ \quad = a \quad L3(a) \\ a \vee a = a \quad (\text{Idempotent Law}) \end{array} \right.$$

$(L, \wedge, \vee)$

$a \leq b \text{ iff } a \wedge b = a$

Theorem :-

If  $L$  is a lattice,  $a \wedge b = a$  iff  $a \vee b = b$   
and  $\leq$  is a partial order (PO)  
(reflexive, antisymmetric and transitive)

Proof :-

$$\begin{aligned} b &= b \vee (b \wedge a) \quad L3b \\ \Rightarrow a &= b \vee (\underline{a \wedge b}) \\ &= b \vee a \\ &= a \vee b \\ &= \boxed{a \vee b} \quad \text{H.P.} \end{aligned}$$

$\Leftarrow$  If  $a \vee b = b$   
to show -  $a \wedge b = a$

$$\begin{aligned} a &= a \wedge (a \vee b) \quad L3a \\ &= \underline{a \wedge b} \quad \text{n.p.} \end{aligned}$$

thus  $a \leq b$  iff  $\frac{a \wedge b = a}{a \vee b = b}$

To prove now :-  $(L, \leq)$  is a partial order

Acknowledgments

①  $\forall a \in L (a \wedge a = a) \Rightarrow \forall a \in L (a \leq a)$   
 thus  $\leq$  is reflexive on  $L$

②  $a \leq b$  and  $b \leq a$   
 $\Rightarrow a \wedge b = a$  and  $b \wedge a = b = a \wedge b$   
 $\Rightarrow a \wedge b = a$  as well as  $a \wedge b = b$   
 $\Rightarrow a = b$   
 thus  $\leq$  is antisymmetric on  $L$

③  $a \leq b$  and  $b \leq c$   
 $\Rightarrow a \wedge b = a$  and  $b \wedge c = b$   
 Now:  $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$   
 $\Rightarrow a \leq c$   
 thus  $\leq$  is transitive on  $L$

Hence  $(L, \leq)$  is a partial order

Claim: LUB and GLB exist for any  $a, b \in L$

Consider: -  $(a, b)$

if  $a \leq b$  then  $GLB(a, b) = a$   
 and  $LUB(a, b) = b$

if  $a \geq b$  then  $GLB(a, b) = b$   
 and  $LUB(a, b) = a$

If  $a \parallel b$  then let  $c = a \wedge b \neq a, b$

$$\begin{aligned} a \wedge c &= a \wedge (a \wedge b) \\ &= (a \wedge a) \wedge b \\ &= a \wedge b \\ &= c \end{aligned}$$



the defn: -  $a \leq b$  iff  $a \wedge b = a$  provides the required ordering such that meet comes down in Hasse diagram

By similar argument: -

$$b \wedge c = c \Rightarrow c \leq b$$

Now  $c$  is a common lower bound of both  $a$  and  $b$ .  
Now we want to show that  $c$  is in fact the greatest  
lower bound.

→ say some  $y$  is also a LB of  $a$  &  $b$   
 $y \leq a$  and  $y \leq b$

$$c \wedge y = (a \wedge b) \wedge y = a \wedge (b \wedge y) = a \wedge y = y.$$
$$\Rightarrow y \leq c$$

thus every other LB should precede  $c$ ;

Hence  $\underline{c \rightarrow GLB}$ .

Hence :- if  $a \parallel b$  then  $GLB = a \wedge b$

Hence we can say that for any  $(a, b)$  in  $L$

$$GLB : a \wedge b$$

$$LUB : a \vee b$$

Let  $P$  be a poset with  $GLB$  and  $LUB$  defined for

all  $a, b \in P$  set is closed under

$$a \wedge b = GLB(a, b)$$

$\wedge$  and  $\vee$ .

$$a \vee b = LUB(a, b)$$

Now we need to show that the 3 properties of lattice

are defined.

Commutativity :-

$$a \wedge b = b \wedge a$$

$$GLB(a, b) = GLB(b, a)$$

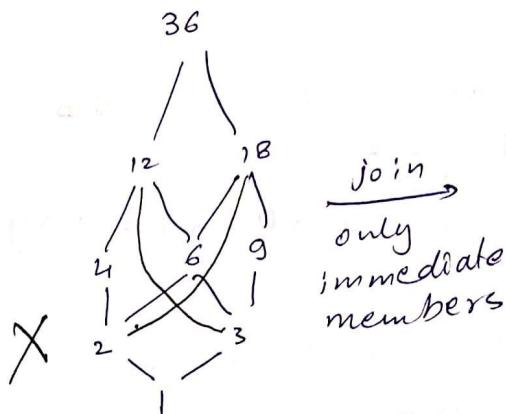


associativity :-

Try This !!

absorptive :-

$$D_{36} := 1, 2, 3, 4, 6, 9, 12, 18, 36$$



$\star (D_{36}, \leq)$  is a sublattice of  $(N^+, \leq)$

Isomorphic :  $f(a \wedge b) = f(a) \wedge f(b)$

Bounded lattice :-

$L$  has a LB 0,  $\forall x \in L (0 \leq x)$

$L$  has an UB 1,  $\forall x \in L (x \leq 1)$

If  $L$  has a LB and an UB, it is bounded.

What if  $L$  has finite elements?

Can we say that it has a LB and UB.

Consider :-

$$a_i \wedge (\underbrace{a_1 \wedge a_2 \dots \wedge a_n}_b) = b$$

$$\Rightarrow b \leq a_i \text{ for every } i$$

thus  $b$  is a LB

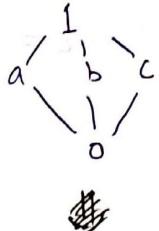
similar argument for UB.

Distributive Lattice

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Non distributive lattice :-



If a Lattice has a part isomorphic to any of these two, then the lattice is Non-distributive lattice

$$\begin{aligned} a \vee (b \wedge c) &= a \vee 0 \\ &= a \end{aligned}$$

$$(a \vee b) \wedge (a \vee c) = 1 \wedge c = c$$

both are not equal

Similarly for the 2<sup>nd</sup> :-

$$a \vee (b \wedge c) = a \vee 0 = a$$

$$(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1$$

But

### Complements

$L$  is bounded LB - 0

UB - 1

for  $a \in L$ , the complement  $\bar{a}$  of  $a$   
 $x = \bar{a}$  iff  $a \vee x = 1$  and  $x \wedge a = 0$

Theorem:- If  $L$  is a bounded distributive lattice, then complements are unique (if they exist)

and  $L$  is a complemented lattice, if  $L$  is bounded and every element has a complement

\*  $(L, \wedge, \vee)$  is distributive.

$$\text{if } a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

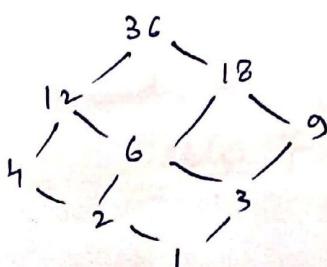
$$\text{and } a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

$$D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

$\wedge$  GCD

$\vee$  LCM

(Divides)



$$\begin{array}{l}
 \text{Q2} \\
 \begin{array}{l}
 (a, b, c) \rightarrow \text{GCD}(a, b, c) = g \\
 a = Ag \\
 b = \hat{B}g \\
 = BG_1g
 \end{array}
 \quad \left. \begin{array}{l}
 \text{GCD}(\hat{B}, \hat{C}) = G_1 \\
 c = \hat{C}g \\
 = CG_1g
 \end{array} \right\} \quad \begin{array}{l}
 \text{GCD}(B, C) = 1 \\
 \text{GCD}(A, B, C) = 1
 \end{array}
 \end{array}$$

$$\begin{aligned}
 \cdot a \underline{\text{LCM}} (b \underline{\text{GCD}} c) &= Ag \underline{\text{LCM}} (BG_1g \underline{\text{GCD}} CG_1g) \\
 &= Ag \cdot \underline{\text{LCM}} G_1g \\
 &= g \times \text{LCM}(A, G_1) = gAG_1
 \end{aligned}$$

$$\cdot a \underline{\text{LCM}} b = Ag \underline{\text{LCM}} BG_1g = ABG_1g$$

$$\cdot a \underline{\text{LCM}} c = ACG_1g = AG_1g$$

$$\begin{aligned}
 \cdot a \underline{\text{GCD}} (b \underline{\text{LCM}} c) &= a \underline{\text{GCD}} (BG_1g \underline{\text{LCM}} CG_1g) \\
 &= Ag \underline{\text{GCD}} (BCG_1g) \\
 &= g \times \text{GCD}(A, BC)
 \end{aligned}$$

$$\begin{aligned}
 (a \underline{\text{GCD}} b) &= Ag \underline{\text{GCD}} BG_1g \\
 &= g \times \text{GCD}(A, BG_1) \\
 &= g \times \text{GCD}(A, B) \\
 &= g \times \text{GCD}(A, C)
 \end{aligned}$$

$$\begin{aligned}
 &\text{Multiplication} \quad \text{of } (\text{GCD}, \text{L}) \\
 &(ab) \times (cd) = (a \times c)(b \times d) \text{ L.R.P} \\
 &(a \times b) \times (c \times d) = (a \times c) \times (b \times d) \text{ L.R.P} \\
 &\{ \text{Multiplication, Division, Addition, Subtraction} \} \text{ L.R.P}
 \end{aligned}$$



For any lattice  $L$ ,  $0$  is LB,  $1$  is UB  
 for  $a \in L$   $\bar{a} = x$  iff  $a \vee x = 1$  and  $a \wedge x = 0$   
complement of  $x$

complements may not exist.

e.g.

$$v = 1$$

$$u$$

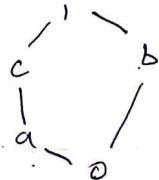
$$z$$

$$y$$

$$x = 0$$

} without complements.

complements may not be unique.



Theorem:- Let  $L$  be a distributive lattice.

complements are unique if they exist.

Proof:- Same  $x$  and  $y$  are two complements of a

$$a \vee x = a \vee y = 1$$

$$a \wedge x = a \wedge y = 0$$

$$x = x \vee 0 = x \vee (a \wedge y)$$

$$\begin{aligned} \text{Now } x &= (x \vee a) \wedge (x \vee y) \\ &= (x \vee a) \wedge (x \vee y) \end{aligned}$$

$$\text{If } x = x \vee y \text{ and } x \neq y \text{ then } x \vee y \neq x$$

similarly  $y = y \vee x$ ; we have  $x \vee y = y \vee x$

By commutativity of  $\vee$

$$\Rightarrow \boxed{x = y} \quad \text{H.P.}$$

lattice  $L$  has Lower Bound  $0$

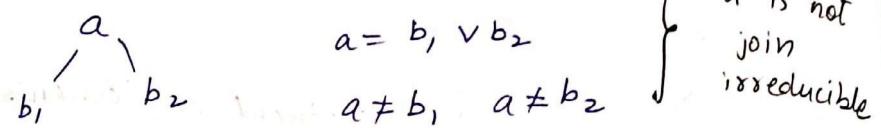
at  $L$  is join irreducible, if  $a = x \vee y \rightarrow a = x \vee a = y$

(if  $p$  is a prime  
if  $p = x \vee y \rightarrow p = x \vee p = y$ )

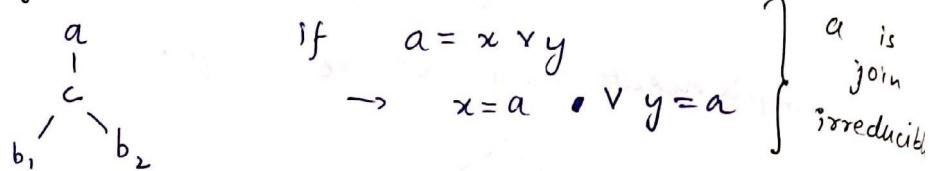
$0$  is join irreducible

$$\Rightarrow 0 = x \vee y \rightarrow x = 0 \vee y = 0$$

if  $a$  has 2 immediate predecessors -



if  $a$  has only 1 immediate predecessor



- ★  $a$  has  $\geq 2$  immediate predecessors  $\Rightarrow$  Not join irreducible
  - ★  $a$  has  $< 2$  immediate predecessors  $\Rightarrow$  join irreducible
- 

★ Immediate successors of  $0$  are called atoms

(In any divisibility lattice, the atoms are prime numbers)

→ ★ All prime powers are also join irreducible.

---

Finite lattice  $L$

$a \in L$  is <sup>not</sup> J.I.

$a = b_1 \vee b_2$  where  $b_1 \neq a$  and  $b_2 \neq a$

Further if both  $b_1$  and  $b_2$  are not J.I.

then

$$a = c_1 \vee c_2 \vee c_3 \vee c_4$$

we can continue like this until we find an exp. of the form →

$$a = d_1 \vee d_2 \vee \dots \vee d_n$$

where  $d_i$  is J.I.

→ every non J.I. element can be expressed as a join of J.I. elements.

$$\left. \begin{array}{l} d_i \leq d_j \\ d_i \vee d_j = d_j \end{array} \right\} d_i \text{ is redundant.}$$

Let us get rid of all such  $d_i$ 's  
then we will have

$a = \text{join of irredundant J.I. elements}$   
(in fact there is a unique such factorisation)

Let  $L$  be a distributive lattice, Then every  $a \in L$   
can be written uniquely (except for order) as  
the join of irredundant J.I. elements.

Proof:-

$$a = b_1 \vee \dots \vee b_s = c_1 \vee \dots \vee c_s$$

$b_i$ 's and  $c_i$ 's are irredundant and J.I.

$$b_i \leq (b_1 \vee \dots \vee b_s) = a = c_1 \vee \dots \vee c_s$$

$$b_i = b_i \wedge a = b_i \wedge (c_1 \vee \dots \vee c_s)$$

$$= \underbrace{(b_i \wedge c_1)}_{b_i \text{ is J.I. and it is}} \vee \underbrace{(b_i \wedge c_2)}_{\text{written as join of different}} \dots \underbrace{(b_i \wedge c_s)}_{\text{elements.}}$$

$$b_i = b_i \wedge c_j$$

$\Rightarrow b_i \leq c_j$

Similarly we can argue that  $c_j \leq b_k$

Then by transitivity we have  $b_i \leq c_j \leq b_k$

$$\Rightarrow b_i \leq b_k$$

but we removed all redundancies

$$\Rightarrow i = k$$

thus

$$\begin{aligned} b_i &\leq c_j \\ c_j &\leq b_i \end{aligned}$$

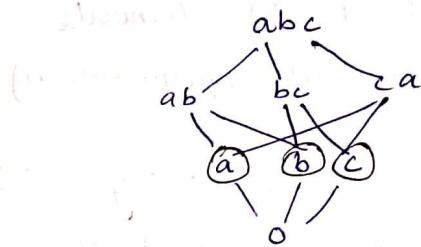
$$\Rightarrow b_i = c_j$$

Hence  $b_i$  is identical to some  $c_j$

Hence for every  $b_i$  there is a unique  $c_j$  (which is equal to  $b_i$  itself).

Theorem:- Let  $L$  be a complemented lattice with unique complements.

Then the J.I. elements of  $L$  other than  $0$  are its atoms.



Proof:- Say  $a$  is JI  $a \neq 0$  and  $a$  is not an atom. Then  $a$  has a unique predecessor  $b$   $b \neq 0$ . Then  $\bar{b}$  exists. (unique property of  $L$ )

$$b \neq 0 \rightarrow \bar{b} \neq 1$$

$$\textcircled{1} \quad \text{If } a \leq \bar{b} \text{ then } b \leq a \leq \bar{b}$$

$$\rightarrow b \leq \bar{b}$$

$$\rightarrow b \vee \bar{b} = \bar{b} = 1 \text{ (contradiction)}$$

thus  $a \not\leq \bar{b}$

$\Rightarrow$  Now  $a \wedge \bar{b}$  must strictly precede  $a$ .

If  $b$  is the imm. pred. of  $a \rightarrow a \wedge \bar{b}$  precedes  $b$

$$a \wedge \bar{b} \leq \inf(b, \bar{b}) = b \wedge \bar{b} = 0$$

$$\Rightarrow a \wedge \bar{b} = 0 \quad * a \vee b = a$$

$$a \vee \bar{b} = (a \vee b) \vee \bar{b} = a \vee (b \vee \bar{b}) = a \vee 1 = 1$$

$$\Rightarrow \bar{a} = \bar{b}$$

$$\Rightarrow a = b$$

(but  $b$  is immediate predecessor of  $a$  thus contradiction)

# Discrete Numeric Functions

$$f: N \rightarrow \mathbb{Z}$$

$$\langle a_0, a_1, \dots \rangle$$

e.g.  $1, 1, 1, 1, \dots$

$$1, 2, 3, 4, \dots$$

$$1, -2, 3, -4, 5, -6, \dots$$

e.g.  $a_r = 7r^3 + 1, r \geq 0$

$$b_r = \begin{cases} 2r & 0 \leq r \leq 11 \\ 3^r - 1 & r > 11 \end{cases}$$

$$\bar{a} = \langle a_0, a_1, \dots \rangle$$

$$\bar{b} = \langle b_0, b_1, \dots \rangle$$

①  $c = a + b = \langle a_0 + b_0, a_1 + b_1, \dots \rangle$

②  $a \times b = \langle a_0 b_0, a_1 b_1, \dots \rangle$

③  $|a| = \langle |a_0|, |a_1|, \dots \rangle$

④  $s' a = \langle \underbrace{0, 0, \dots 0}_{i}, a_0, a_1, \dots \rangle \rightarrow$  i shifted (Right)

⑤  $s^{-i} a = \langle a_i, a_{i+1}, \dots a_{i+2}, \dots \rangle \rightarrow$  (left shifted)

⑥ forward difference

$$\Delta a = \langle a_1 - a_0, a_2 - a_1, a_3 - a_2, \dots \rangle$$

backward diff.

$$\nabla a = \langle 0, a_1 - a_0, a_2 - a_1, \dots \rangle$$

$$\boxed{\nabla a = s'(\Delta a)}$$

⑦  $c = a * b$  convolution

$$c_r = a_0 b_r + a_1 b_{r-1} + a_2 b_{r-2} + \dots + a_{r-2} b_2 + a_{r-1} b_1 + a_r b_0$$

$$= \sum_{i=0}^r a_i b_{r-i}$$

\* DNF  $a = \langle a_0, a_1, a_2, \dots \rangle$

$$A(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \dots$$

$A(z) \rightarrow$  the generating fn of  $a$

$$a = \langle 1, 1, 1, 1, \dots \rangle$$

$$\text{then } A(z) = 1 + z + z^2 + \dots z^j + \dots$$

$$= \frac{1}{1-z}$$

$$a = \langle 1, 3, 3^2, 3^3, \dots \rangle \quad 1 + 3z + 3^2 z^2 + \dots = \frac{1}{1-3z}$$

$$a = \langle 7, 7, 7, 7, \dots \rangle \quad \frac{7}{1-3z}$$

$$a_r = 3^{r+2}, r \geq 0 \Rightarrow \frac{9}{1-3z}$$

If  $c = a + b$

$$C(z) = A(z) + B(z)$$

$$\text{e.g. } a_r = 3^r + 2^r; r \geq 0$$

$$A(z) = \frac{1}{1-3z} + \frac{1}{1-2z}$$

$$A(z) = \frac{2 + 3z - 6z^2}{1-2z}$$

$$= 3z + \frac{2}{1-2z}$$

$$\downarrow \\ + 3z^2 (1 + 2z + 2^2 z^2 + \dots + 2^r z^r + \dots)$$

$$= 2 + 7z + 2^2 z^2 + 2^4 z^3 + \dots$$

$$a_r = \begin{cases} 2 & r=0 \\ 7 & r=1 \\ 2^{r+1} & r>1 \end{cases}$$