Discrete Mathematics

Algebraic Structures

H. Turgut Uyar   Ayşegül Gençata Yayımlı   Emre Harmancı

2001-2011

License

Topics

Algebraic Structure

Definition

algebraic structure:
- carrier
- operations
- constants

- *signature*: <carrier, operations, constants>

Operation

- binary operation:
  $\circ : S \times S \to T$
- unary operation:
  $\Delta : S \to T$
- every operation is a function
- closed: $T \subseteq S$

Closed Operation Examples

Example

- subtraction is closed on $\mathbb{Z}$
- subtraction is not closed on $\mathbb{Z}^+$

Binary Operation Properties

Definition
commutativity:
$\forall a, b \in S \;\; a \circ b = b \circ a$

Definition
associativity:
$\forall a, b, c \in S \;\; (a \circ b) \circ c = a \circ (b \circ c)$

Binary Operation Example

Example
$\circ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$a \circ b = a + b - 3ab$

- commutative:
  $a \circ b = a + b - 3ab = b + a - 3ba = b \circ a$
- associative:

$$\begin{aligned} (a \circ b) \circ c &= (a + b - 3ab) + c - 3(a + b - 3ab)c \\ &= a + b - 3ab + c - 3ac - 3bc + 9abc \\ &= a + b + c - 3ab - 3ac - 3bc + 9abc \\ &= a + (b + c - 3bc) - 3a(b + c - 3bc) \\ &= a \circ (b \circ c) \end{aligned}$$

Constants

Definition

identity:

$x \circ 1 = 1 \circ x = x$

- left identity: $1_l \circ x = x$
- right identity: $x \circ 1_r = x$

Definition

zero:

$x \circ 0 = 0 \circ x = 0$

- left zero: $0_l \circ x = 0$
- right zero: $x \circ 0_r = 0$

Examples of Constants

Example

- identity for $< \mathbb{N}, max >$ is 0
- zero for $< \mathbb{N}, min >$ is 0

Example

∘	a	b	c
a	a	b	b
b	a	b	c
c	a	b	a

- b is a left identity
- a and b are right zeros

Constants

Theorem

$\exists 1_l \wedge \exists 1_r \Rightarrow 1_l = 1_r$

Proof.

$1_l \circ 1_r = 1_l = 1_r$ □

Theorem

$\exists 0_l \wedge \exists 0_r \Rightarrow 0_l = 0_r$

Proof.

$0_l \circ 0_r = 0_l = 0_r$ □

Inverse

Definition

if $x \circ y = 1$:

- x is a *left inverse* of y
- y is a *right inverse* of x

- if $x \circ y = y \circ x = 1$ x and y are inverse

Inverse

Theorem

if the operation $\circ$ is associative:
$w \circ x = x \circ y = 1 \Rightarrow w = y$

Proof.

$$\begin{aligned} w &= w \circ 1 \\ &= w \circ (x \circ y) \\ &= (w \circ x) \circ y \\ &= 1 \circ y \\ &= y \end{aligned}$$

□

Algebraic Families

- *algebraic family*: signature + axioms

Algebraic Family Examples

Example

- axioms:
  - $x \circ y = y \circ x$
  - $(x \circ y) \circ z = x \circ (y \circ z)$
  - $x \circ 1 = x$
- structures obeying these axioms:
  - $< \mathbb{Z}, +, 0 >$
  - $< \mathbb{Z}, \cdot, 1 >$
  - $< \mathcal{P}(S), \cup, \emptyset >$

Subalgebra

Definition

subalgebra:
let $A =< S, \circ, \Delta, k > \quad \wedge \quad A' =< S', \circ', \Delta', k' >$

- A' is a subalgebra of A if:
  - $S' \subseteq S$
  - $\forall a, b \in S' \;\; a \circ' b = a \circ b \in S'$
  - $\forall a \in S' \;\; \Delta' a = \Delta a \in S'$
  - $k' = k$

Subalgebra Example

Example

$<\mathbb{Z}, +, 0>$ is a subalgebra of $<\mathbb{R}, +, 0>$

Semigroups

Definition

semigroup: $< S, \circ >$

- $\forall a, b, c \in S \ (a \circ b) \circ c = a \circ (b \circ c)$

Semigroup Examples

Example

$< \Sigma^+, \& >$

- Σ: alphabet, Σ^+: strings of length at least 1
- &: string concatenation

Monoids

Definition

monoid: $< S, \circ, 1 >$

- $\forall a, b, c \in S \ (a \circ b) \circ c = a \circ (b \circ c)$
- $\forall a \in S \ a \circ 1 = 1 \circ a = a$

Monoid Examples

Example

$< \Sigma^*, \&, \epsilon >$

- Σ: alphabet, Σ^*: strings of any length
- $\&$: string concatenation
- ϵ: empty string

Groups

Definition

group: $< S, \circ, 1 >$

- $\forall a, b, c \in S \ (a \circ b) \circ c = a \circ (b \circ c)$
- $\forall a \in S \ a \circ 1 = 1 \circ a = a$
- $\forall a \in S \ \exists a^{-1} \in S \ \ a \circ a^{-1} = a^{-1} \circ a = 1$
- *Abelian group*: $\forall a, b \in S \ a \circ b = b \circ a$

Group Examples

Example

$< \mathbb{Z}, +, 0 >$

- $x^{-1} = -x$

Example

$< \mathbb{Q} - \{0\}, \cdot, 1 >$

- $x^{-1} = \frac{1}{x}$

Group Examples

Example (composition of permutations)

A	1_A	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}
1	1	1	1	1	1	1	2	2	2	2	2	2
2	2	2	3	3	4	4	1	1	3	3	4	4
3	3	4	2	4	2	3	3	4	1	4	1	3
4	4	3	4	2	3	2	4	3	4	1	3	1

A	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}	p_{17}	p_{18}	p_{19}	p_{20}	p_{21}	p_{22}	p_{23}
1	3	3	3	3	3	3	4	4	4	4	4	4
2	1	1	2	2	4	4	1	1	2	2	3	3
3	2	4	1	4	1	2	2	3	1	3	1	2
4	4	2	4	1	2	1	3	2	3	1	2	1

$p_8 \diamond p_{12} = 1_A \Rightarrow p_{12} = p_8^{-1}$
$p_{14} \diamond p_{14} = 1_A \Rightarrow p_{14} = p_{14}^{-1}$

$< \{1_A, p_1, \ldots, p_{23}\}, \diamond, \Delta^{-1}, 1_A >$

Subgroup Example

Example (composition of permutations)

$\diamond$	1_A	p_2	p_6	p_8	p_{12}	p_{14}
1_A	1_A	p_2	p_6	p_8	p_{12}	p_{14}
p_2	p_2	1_A	p_8	p_6	p_{14}	p_{12}
p_6	p_6	p_{12}	1_A	p_{14}	p_2	p_8
p_8	p_8	p_{14}	p_2	p_{12}	1_A	p_6
p_{12}	p_{12}	p_6	p_{14}	1_A	p_8	p_2
p_{14}	p_{14}	p_8	p_{12}	p_2	p_6	1_A

Left and Right Cancellation

Theorem

$a \circ c = b \circ c \Rightarrow a = b$
$c \circ a = c \circ b \Rightarrow a = b$

Proof.

$$
\begin{array}{rrcl}
 & a \circ c & = & b \circ c \\
\Rightarrow & (a \circ c) \circ c^{-1} & = & (b \circ c) \circ c^{-1} \\
\Rightarrow & a \circ (c \circ c^{-1}) & = & b \circ (c \circ c^{-1}) \\
\Rightarrow & a \circ 1 & = & b \circ 1 \\
\Rightarrow & a & = & b
\end{array}
$$

□

Basic Theorem of Groups

Theorem

The unique solution of the equation $a \circ x = b$ *is:* $x = a^{-1} \circ b$.

Proof.

$$
\begin{array}{rrcl}
 & a \circ c & = & b \\
\Rightarrow & a^{-1} \circ (a \circ c) & = & a^{-1} \circ b \\
\Rightarrow & 1 \circ c & = & a^{-1} \circ b \\
\Rightarrow & c & = & a^{-1} \circ b
\end{array}
$$

□

Ring

Definition

ring: $< S, +, \cdot, 0 >$

- $\forall a, b, c \in S \ (a + b) + c = a + (b + c)$
- $\forall a \in S \ a + 0 = 0 + a = a$
- $\forall a \in S \ \exists (-a) \in S \ a + (-a) = (-a) + a = 0$
- $\forall a, b \in S \ a + b = b + a$
- $\forall a, b, c \in S \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\forall a, b, c \in S$
  - $a \cdot (b + c) = a \cdot b + a \cdot c$
  - $(b + c) \cdot a = b \cdot a + c \cdot a$

Field

Definition

field: $< S, +, \cdot, 0, 1 >$

- all properties of a ring
- $\forall a, b \in S \; a \cdot b = b \cdot a$
- $\forall a \in S \; a \cdot 1 = 1 \cdot a = a$
- $\forall a \in S \; \exists a^{-1} \in S \; a \cdot a^{-1} = a^{-1} \cdot a = 1$

References

Grimaldi

- Chapter 5: Relations and Functions
  - 5.4. Special Functions
- Chapter 16: Groups, Coding Theory, and Polya's Method of Enumeration
  - 16.1. Definitions, Examples, and Elementary Properties
- Chapter 14: Rings and Modular Arithmetic
  - 14.1. The Ring Structure: Definition and Examples

Partially Ordered Set

Definition

partial order relation:

- reflexive
- anti-symmetric
- transitive

- *partially ordered set (poset)*:
  a set with a partial order relation defined on its elements

Poset Examples

Example (set of sets, $\subseteq$)

- $A \subseteq A$
- $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$
- $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

Poset Examples

Example $(\mathbb{Z}, \leq)$

- $x \leq x$
- $x \leq y \land y \leq x \Rightarrow x = y$
- $x \leq y \land y \leq z \Rightarrow x \leq z$

Poset Examples

Example $(\mathbb{Z}^+, |)$

- $x|x$
- $x|y \land y|x \Rightarrow x = y$
- $x|y \land y|z \Rightarrow x|z$

Comparability

- $a \preceq b$: *a precedes b*
- $a \preceq b \lor b \preceq a$: *a and b are comparable*
- total order (linear order, chain):
  all elements are comparable with each other

Comparability Examples

Example

- $\mathbb{Z}^+, |$: 3 and 5 are not comparable
- $\mathbb{Z}, \leq$: total order

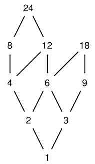
Hasse Diagrams

- $a \ll b$: *a immediately precedes b*
  $\neg \exists x \; a \preceq x \preceq b$
- Hasse diagram:
  - draw a line between a and b if $a \ll b$
  - preceding element is below

Hasse Diagram Examples

Example

$\{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$
$|$ relation



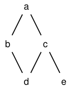
Consistent Enumeration

Definition
consistent enumeration:
$f : S \to \mathbb{N}$
$a \preceq b \Rightarrow f(a) \leq f(b)$

- there can be more than one consistent enumeration

Consistent Enumeration

Example



- $f(d) = 1, f(e) = 2, f(b) = 3, f(c) = 4, f(a) = 5$
- $f(e) = 1, f(d) = 2, f(c) = 3, f(b) = 4, f(a) = 5$

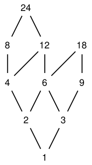
Upper Bound - Lower Bound

Definition
upper bound: max
$\forall x \in S \;\; max \preceq x \Rightarrow x = max$

Definition
lower bound: min
$\forall x \in S \;\; x \preceq min \Rightarrow x = min$

Upper Bound - Lower Bound Examples

Example



$max: \;\; 18, 24$
$min: \;\; 1$

Supremum

Definition
$A \subseteq S$

M is an upper bound of A:
$\forall x \in A \;\; x \preceq M$

Definition
$M(A)$: set of upper bounds of A

$sup(A)$ is the supremum of A:
$\forall M \in M(A) \;\; sup(A) \preceq M$

Infimum

Definition
$A \subseteq S$

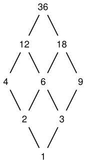
m is a lower bound of A:
$\forall x \in S \;\; m \preceq x$

Definition
$m(A)$: set of lower bound of A

$inf(A)$ is the infimum of A:
$\forall m \in m(A) \;\; m \preceq inf(A)$

Bound Example

Example (factors of 36)



inf = gcd
sup = lcm

Lattice

Definition
lattice: $< L, \wedge, \vee >$
$\wedge$: meet, $\vee$: join

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

Poset - Lattice Relationship

- If P is a poset, then $< P, inf, sup >$ is a lattice.
  - $a \wedge b = inf(a, b)$
  - $a \vee b = sup(a, b)$
- Every lattice is a poset where these definitions hold.

Duality

Definition
dual:
$\wedge$ instead of $\vee$, $\vee$ instead of $\wedge$

Theorem (Duality Theorem)
Every theorem has a dual theorem in lattices.

Lattice Theorems

Theorem
$a \wedge a = a$

Proof.
$a \wedge a = a \wedge (a \vee (a \wedge b))$ $\square$

Lattice Theorems

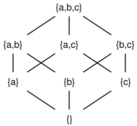
Theorem
$a \preceq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$

Lattice Examples

Example

$< \mathcal{P}\{a, b, c\}, \cap, \cup >$

$\subseteq$ relation



Bounded Lattice

Definition
lower bound of lattice L: 0
$\forall x \in L \; 0 \preceq x$

Definition
upper bound of lattice L: I
$\forall x \in L \; x \preceq I$

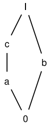
Theorem
Every finite lattice is bounded.

Distributive Lattice

- *distributive lattice*:
  - $\forall a, b, c \in L \; a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
  - $\forall a, b, c \in L \; a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Counterexamples

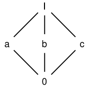
Example



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

Counterexamples

Example



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

Distributive Lattice

Theorem
A lattice is nondistributive if and only if it has a sublattice isomorphic to any of these two structures.

Join Irreducible

Definition

join irreducible element:
$a = x \vee y \Rightarrow a = x \vee a = y$

- *atom*: a join irreducible element which immediately succeeds the minimum

Join Irreducible Example

Example (Divisibility Relation)

- prime numbers and 1 are join irreducible
- 1 is the minimum, the prime numbers are the atoms

Join Irreducible

Theorem

Every element in a lattice can be written as the join of join irreducible elements.

Complement

Definition

a and x are complements:
$a \wedge x = 0$ and $a \vee x = I$

Complemented Lattice

Theorem
In a bounded, distributive lattice the complement is unique, if it exists.

Proof.
$a \wedge x = 0, a \vee x = I$, $a \wedge y = 0, a \vee y = I$

$$\begin{aligned} x &= x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = I \wedge (x \vee y) \\ &= x \vee y = y \vee x = I \wedge (y \vee x) \\ &= (y \vee a) \wedge (y \vee x) = y \vee (a \wedge x) = y \vee 0 = y \end{aligned}$$

□

Boolean Algebra

Definition
Boolean algebra:
$< B, +, \cdot, \overline{x}, 1, 0 >$

$a + b = b + a$	$a \cdot b = b \cdot a$
$(a + b) + c = a + (b + c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
$a + 0 = a$	$a \cdot 1 = a$
$a + \overline{a} = 1$	$a \cdot \overline{a} = 0$

Boolean Algebra - Lattice Relationship

Definition
A Boolean algebra is a finite, distributive, complemented lattice.

Duality

Definition
dual:
$+$ instead of $\cdot$, $\cdot$ instead of $+$
0 instead of 1, 1 instead of 0

Example
$(1 + a) \cdot (b + 0) = b$
dual of the theorem:
$(0 \cdot a) + (b \cdot 1) = b$

Boolean Algebra Examples

Example

$B = \{0, 1\}, + = \vee, \cdot = \wedge$

Example

$B = \{$ factors of 70 $\}, + = lcm, \cdot = gcd$

Boolean Algebra Theorems

$$
\begin{array}{ll}
a + a = a & a \cdot a = a \\
a + 1 = 1 & a \cdot 0 = 0 \\
a + (a \cdot b) = a & a \cdot (a + b) = a \\
(a + b) + c = a + (b + c) & (a \cdot b) \cdot c = a \cdot (b \cdot c) \\
 & \\
\overline{\overline{a}} = a & \\
\overline{a + b} = \overline{a} \cdot \overline{b} & \overline{a \cdot b} = \overline{a} + \overline{b}
\end{array}
$$

References

To read: Grimaldi

- Chapter 7: Relations: The Second Time Around
  - 7.3. Partial Orders: Hasse Diagrams
- Chapter 15: Boolean Algebra and Switching Functions
  - 15.4. The Structure of a Boolean Algebra