Structured Sets

CS1200, CSE IIT Madras

Meghana Nasre

April 23, 2020

Structured Sets

- Relational Structures
  - Properties and closures ✓
  - Equivalence Relations ✓
  - Partially Ordered Sets (Posets) and Lattices ✓
- Algebraic Structures
  - Groups and Rings

Binary Operator: Example 1

Consider a toy vending machine which takes two input $\mathcal{I}_1$ and $\mathcal{I}_2$ and can output 3 different things.

We have two different tokens which can be used: blueT and redT tokens.

The behaviour of the vending machine is as follows.

$\mathcal{I}_2$ \ $\mathcal{I}_1$	*redT*	*blueT*
redT	*ball*	*car*
blueT	*car*	*pencil*

- The above is a function from $A \times A$ to B where
  $A = \{redT, blueT\}$ $\quad B = \{$ car, ball, pencil$\}$
- A function from $A \times A$ to B is called a binary operator.
- A binary operator tells how two elements are "combined" to get output!
- A binary operator from $A \times A$ to A is called closed.

Binary Operator: Example 2

Consider the hair color of a child being determined by the hair color of the parents.

Say, we have two possibilities of hair color for the parents light and dark.

Following is the way in which the hair color of the child is determined.

Mother \ Father	*light*	*dark*
light	*light*	*dark*
dark	*dark*	*dark*

- The above is a function from $A \times A$ to A where $A = \{light, dark\}$
- Note that in this case the binary operator is closed.
- Typical to represent $f(a, b)$ as "a **f** b" or use one of the symbols like $\cdot$ or $*$ and write $a \cdot b$ or $a * b$

Algebraic System

A set A with operations on the set is called an algebraic system.

We will deal with binary operations, but one can have ternary operations and so on. Our examples above are systems with one (binary) operator, but we can have multiple operators as well.

Ex 1: $A = \{redT, blueT\}$, operator $\cdot$

$\cdot$	$redT$	$blueT$
$redT$	$ball$	car
$blueT$	car	$pencil$

Ex 2: $A = \{light, dark\}$, operator $*$

$*$	$light$	$dark$
$light$	$light$	$dark$
$dark$	$dark$	$dark$

Some more examples:

- Z^+ along with the addition $+$ and multiplication $\cdot$ form an algebraic system $(Z^+, +, \cdot)$.
- Let $\diamond$ be a binary operator which is 1 if the $a + b$ is even and 0 otherwise. Let $\triangle$ denote the ternary operator which gives maximum of three integers a, b, c. Then $(Z^+, \diamond, \triangle)$ form an algebraic system.

Semi-group

Let $*$ be a binary operator on a set A.

The operator $*$ is associative if for all p, q, r in A, we have:

$$(p * q) * r = p * (q * r)$$

An algebraic system $(A, *)$ is called a semi-group if both the following hold:

- $*$ is a closed operation.
- $*$ is an associative operation.

Examples:

- Let $A = \{2, 4, 6, 8, \ldots\}$. The operator is addition "$+$". Then, $(A, +)$ is a semi-group.
- Let $B = \{2, 4, 6, 8\}$ (finite set). The operator is addition "$+$". Then $(B, +)$ is not a semi-group since $+$ is not closed.
- Let $A = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. The operator is subtraction "-". Then $(A, -)$ is not a semi-group since $-$ is not associative.

Identity Elements

$(A, *)$ is an algebraic system where $*$ is a binary operator.

Qn: Does there exist a "neutral" element e such that when it is combined with any element, it leaves the element "unchanged"?

- Let $A = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and operator is addition "+". Then clearly "0" is the neutral element. That is, $0 + b = b$, for all $b \in A$.
- $(\{2, 4, 6, 8, \ldots, \}, +)$ does not have such a neutral element (although it is a semi-group).

Lets call such a neutral element (if it exists) as identity element e.

Some more questions:

- What if $e * a$ and $a * e$ are not the same? Note that "$*$" may not be commutative.
- Can there be multiple identity elements?

Identity Elements

$(A, *)$ is an algebraic system where $*$ is a binary operator.

Left Identity: An element $e \in A$ is called left identity if for all $b \in A$, we have $e * b = b$.

Right Identity defined similarly.

Claim 1: If e_1 is a left identity for $(A, *)$, then e_1 is also a right identity.

Proof: Suppose e_1 is left identity and e_2 is right identity for $(A, *)$. Since e_1 is left identity, $e_1 * e_2 = e_2$. Since e_2 is right identity, $e_1 * e_2 = e_1$. Thus $e_1 = e_2$.

Claim 2: For an algebraic system $(A, *)$, there is a unique identity element.

Ex: Complete the proof.

Monoid

An algebraic system $(A, *)$ is called a monoid if all of the following hold:

- $*$ is a closed operation.
- $*$ is an associative operation.
- There is an identity element.

Thus a monoid is a semi-group that has an identity element.

Examples:

- Let X be some set and $A = \mathcal{P}(X)$ be the power set of X. Let the operator be $\cup$. Then, $(\mathcal{P}(X), \cup)$ is a monoid. $\emptyset$ is the identity element.
- The set $(Z, \times)$ is a monoid with 1 as the identity element.
- $(\{2, 4, 6, 8, \ldots, \}, +)$ is a sub-group but not a monoid.

Inverse Element

$(A, *)$ is an algebraic system where $*$ is a binary operator with an identity element e.

Qn: For an element $b \in A$ does there exist an element $c \in A$ such that when it is combined with b, it "cancels" the effect?

That is $c * b = e$.

- c is called left inverse if $c * b = e$. right inverse defined similarly.
- An element c is called inverse of b if it is both a left inverse and right inverse of b.

Examples:

- $(Z, +)$. For each $b \in Z$, we have $-b$ is inverse of b.
- $(Z^+, \times)$. Here 2 does not have an inverse.
- The set of non-zero reals with the $\times$ operator. Here element b has an inverse which is $\frac{1}{b}$.

Qn: Can left inverse and right inverse be different?

Inverse Element

$(A, *)$ is an algebraic system where $*$ is a closed binary operator with an identity element e.

In addition, assume $*$ is associative and every element has a left inverse.

Claim: For any element $b \in A$, the left inverse and right inverse coincide.

Proof: Let c be left inverse of b. We will show that c is also the right inverse of b. Consider

$$(c * b) * c = e * c = c$$

Since left inverse exists for every element, let d be left inverse of c. Consider,

$$d * ((c * b) * c) = d * c = e$$

Now we use associativity of $*$ to rewrite the LHS of the above.

$$\begin{aligned} e = d * ((c * b) * c) &= ((d * c) * b) * c = (e * b) * c \\ &= b * c \end{aligned}$$

This shows that c is the right inverse of b. Hence proved.

Group

An algebraic system $(A, *)$ is called a group if all of the following hold:

- $*$ is a closed binary operation.
- $*$ is an associative operation.
- There is an identity element e.
- Every element $b \in A$ has an inverse element.

Thus group is a monoid where every element has an inverse.

Examples:

- $(Z, +)$. For each $b \in Z$, we have $-b$ is inverse of b. ✓
- $(Z^+, \times)$. Here 2 does not have an inverse. $\times$
- The set of non-zero reals with the $\times$ operator. Here every element has an inverse which is $\frac{1}{b}$. ✓

Summary

- Binary Operation with properties.
- Algebraic system using a set and operations.
- Semi-groups, Monoids and Groups.
- Upcoming: Properties of groups and some applications.
- Ref: Elements of Discrete Mathematics, C. L. Liu, Section 11.1, 11.2.