Structured Sets

CS1200, CSE IIT Madras

Meghana Nasre

April 27, 2020

Structured Sets

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

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, and an identity element e exists, and every element $b \in A$ has an inverse then $(A, *)$ is a group.
- If $B \subseteq A$ and $(B, *)$ forms a group, then B is a sub-group of $(A, *)$.

- Generator of a group and cyclic groups.
  Example group that is not cyclic.

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

- Lagrange's Theorem: The order of any subgroup of a finite group divides the order of the group.

Cosets of a subset

Let $(A, *)$ be a group and H be any subset of A. For any element $c \in A$, the left coset of H w.r.t. c is defined as:

$$H_c = \{c * b \mid b \in H\}$$

Example:

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the subset $H = \{0, 1, 5\}$.

$$H_1 = \{1, 2, 0\} \qquad H_2 = \{2, 3, 1\} \qquad H_3 = \{3, 4, 2\}$$

Now let us consider a set $B = \{0, 2, 4\}$.

$$B_1 = \{1, 3, 5\} \qquad B_2 = \{2, 4, 0\} \qquad B_3 = \{3, 5, 1\}$$

Observe the difference between the cosets obtained when the subset forms a subgroup (recall $B, \oplus_6$) is a group, whereas $(H, \oplus_6)$ is not a group.

Cosets of a subset

Let $(A, *)$ be a group and H be any subset of A. For any element $c \in A$, the left coset of H w.r.t. c is defined as:

$$H_c = \{c * b \mid b \in H\}$$

Claim: If $(H, *)$ is a subgroup of $(A, *)$ then for any $c \in A$ and $d \in A$, either $H_c = H_d$ or $H_c \cap H_d = \emptyset$.

Proof: Let $H_c \cap H_d \neq \emptyset$. Let $f \in H_c \cap H_d$.

Thus there exists h_1 and h_2 in H such that $f = c * h_1 = d * h_2$.

Since $(H, *)$ is a group, inverse exists for every element, in particular h_1. Therefore $c = d * h_2 * h_1^{-1}$.

For any element $y \in H_c$, we can write it as $y = c * h_3$ for some $h_3 \in H$. Thus, $y = d * h_2 * h_1^{-1} * h_3$ (substituting value of c from above.)

Since h_2, h_1^{-1}, h_3 all belong to H, we know that $h_2 * h_1^{-1} * h_3$ belongs to H. Thus, $y \in H_d$. This shows that $H_c \subseteq H_d$.

Similarly argue that $H_d \subseteq H_c$. This completes the argument that if there is even one common element then the sets are equal.

Proof of Lagrange's Theorem

Lagrange's Theorem (restated): If $(H, *)$ is a subgroup of $(A, *)$ then $|A| = k|H|$ for some positive integer k.

Proof: Let h_1 and h_2 be distinct elements in H. Now for any $b \in A$, we have $b * h_1 \neq b * h_2$.
Thus, $|H_b| = |H|$.

Now if $H_b = A$ we are done, else pick some $c \in A \setminus H_b$.

We know by previous claim that either $H_c = H_b$ or $H_c \cap H_b = \emptyset$. We claim that $H_c \neq H_b$ (by the way c has been selected). Thus $|H_c \cup H_b| = 2|H|$.

We repeat till we exhaust the set A. This way, we have partitioned the set A into some k-many blocks of $|H|$. Thus $|A| = k|H|$.

In other words, the order of any subgroup of a finite group divides the order of the group.

Algebraic Structures with two operations

Lets say we have two algebraic systems $(A, *)$ and $(A, \bullet)$.

Can we combine them into another system $(A, *, \bullet)$? Yes! Meaningful if the operations are related in some way.

Say, they are related by distributivity.

Example: $(\{a, b\}, *, \bullet)$

$*$	a	b
a	a	b
b	b	a

$\bullet$	a	b
a	a	a
b	a	b

We say that $\bullet$ distributes over $*$ if for $a, b, c \in A$

$$a \bullet (b * c) = (a \bullet b) * (a \bullet c)$$

and

$$(b * c) \bullet a = (b \bullet a) * (c \bullet a)$$

Verify that in the above example, $\bullet$ is distributive over $*$. However, $*$ is not distributive over $\bullet$ example: $b * (a \bullet b) = b$ and $(b * a) \bullet (b * b) = a$.

Algebraic Structures with two operations

Let $(A, +, \cdot)$ be an algebraic structure. It is called a ring if

- $(A, +)$ is an Abelian group. recall Abelian says $+$ is commutative.
- $(A, \cdot)$ is a semigroup.
- The operation $\cdot$ is distributive over the operation $+$.

Additionally, if $(A, \cdot)$ is a monoid, then $(A, +, \cdot)$ is a called a ring with identity.

Examples:

- $(Z, +, \cdot)$ is a ring with identity.
- Recall the set Z_n for any positive integer n. We have seen the operation $\oplus_n$ and verified that $(Z_n, \oplus_n)$ is a group. Now define $\odot$ as

$$a \odot_n b = ab \mod n$$

  - Verify that $(Z_n, \odot_n)$ is a semigroup
  - Verify that $\odot_n$ distributes over $\oplus_n$

  Thus, $(Z_n, \oplus_n, \odot_n)$ is a ring.

Summary

- Semigroups, Monoids and Groups.
- Subgroups and interesting properties.
- Lagranges Theorem and proof.
- Algebraic Structures with multiple operations.
- Reference: Section 11.3, Elements of Discrete Mathematics by C. L. Liu.