Discrete Mathematics (ITPC-309)

Algebraic Structures - Part II

Dr. Sanga Chaki

Department of Information Technology

Dr. B. R. Ambedkar National Institute of Technology, Jalandhar

Recap

1. Algebraic Structures
2. Binary Operation on a Set
3. Important properties of an algebraic system are:
   - Closure
   - Associativity
   - Commutativity
   - Existence of identity
   - Existence of inverse
   - Cancellation Laws
4. Semigroup
5. Monoid
6. Group
7. Abelian group or commutative group
8. Finite group and infinite group
9. The order of a group

Algebraic Structures - Definition

1. In mathematics, an algebraic structure consists of
   a) a nonempty set A,
   b) a collection of binary operations on A
   c) and a finite set of identities, known as axioms, that these operations must satisfy.
2. The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.
3. The properties are as follows:

Closure

1. Consider a non empty set G and a binary operation (•)
2. Closure:
   - If a and b are elements of G, then c = a • b is also an element of G.
3. All algebraic structures must follow closure property.

Associativity

1. Consider a non empty set G and a binary operation (•)
2. Associativity:
   - If a, b, and c are elements of G, then (a • b) • c = a • (b • c)
3. (G, •) is called a **semigroup** if it follows both closure and associativity.
4. A semi-group is always an algebraic structure.

Existence of identity element

1. Consider a non empty set G and a binary operation (•)
2. Identity element:
   - For all a in G, there exists an element e, called the identity element, such that e • a = a • e = a.
3. (G, •) is called a **monoid** if it follows closure, associativity, and identity element.
4. A monoid is always a semi-group and algebraic structure. .

Existence of Inverse element

1. Consider a non empty set G and a binary operation (•)
2. Identity element:
   - For each a in G, there exists an element a′, called the inverse of a, such that a • a′ = a′ • a = e.
3. (G, •) is called a **group** if it follows closure, associativity, identity element and inverse element.
4. A group is always a monoid, semigroup, and algebraic structure.

Commutativity

1. Consider a non empty set G and a binary operation (•)
2. Commutativity:
   - For all a and b in G, we have a • b = b • a.
3. (G, •) is called an **abelian** group (after the mathematical Abel) or **commutative** group if it follows closure, associativity, identity element, inverse element and commutativity.
4. Every abelian group is a group, monoid, semigroup, and algebraic structure.

Contents

- Groups
- Modulo operator
- Integers Modulo n
- Subgroups

Group: Theorem 1

1. For every group G,
   a) The identity of G is unique
   b) The inverse of each element in G is unique
   c) If a, b, c $\in$ G, and ab = ac, then b = c (left cancellation property)
   d) If a, b, c $\in$ G, and ba = ca, then b = c (right cancellation property)
2. Proof of a: if e_1 and e_2 are both identities in G, then $e_1 = e_1e_2 = e_2$.
3. Proof of b: let a $\in$ G and suppose b and c are both inverses of a. Then b = be = b(ac) = (ba)c [This step uses associativity] = ec = c
4. Exercise: Can you prove c and d?

The Modulo (%) Operator

1. Modulus or remainder operator
2. 5 mod 2 = 1
3. 2 mod 5 = 2
4. 1 mod 1 = 0
5. 9 mod 3 = 0

The Integers Modulo n

1. Let n be a positive integer.
2. For a, b $\in$ Z,
   1. we say that **a is congruent to b modulo n**,
   2. if n|(a-b) or n divides (a-b)
   3. or a = b + kn where k $\in$ Z.
3. This is written as: **a $\equiv$ b (mod n)**
4. Example: is 17 $\equiv$ 2 (mod 5)? – yes, as 17 – 2 = 15, which is divisible by 5. k=3.
5. Is -7 $\equiv$ -49 (mod 6)?
6. Is 11 $\equiv$ -5 (mod 6)?
7. Is 11 $\equiv$ -5 (mod 8)?

The Integers Modulo n – Some Observations

Let $a, b, n \in Z$, and $n > 1$

1. If $a \equiv b \pmod{n}$ then, a and b have same remainder when divided by n.
2. $a = b \Rightarrow a \equiv b \pmod{n}$ but $a \equiv b \pmod{n}$ does not $\Rightarrow a = b$
3. If $a \equiv b \pmod{n}$ and $a, b \in \{0, 1, 2, \ldots, n-1\}$ then $a = b$.

The Integers Modulo n – Examples

1. What do we mean by the following notations? Z_5 or Z_6 or Z_n?
2. This denotes integers modulo n
3. Z_5 means the set of integers {0, 1, 2, 3, 4}
4. When we define binary operations in Z_5 they are defined wrt modulo 5
5. Eg: the operation of addition/multiplication defined modulo 5. This means that, for any two integers in $Z_{5,}$ their sum/product will also be in Z_5

Z_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Subgroup

1. A special subset of a group
2. If (G, •) is a group and H is a non-null proper subset of G, then H is said to be a subgroup of (G, •) if H is a group under the binary operation •
3. Example: let (G, •) = (Z_6, +) : what is Z_6 ? = {0, 1, 2, 3, 4 ,5} with + defined in modulo 6. Can you create the table for this?
4. If H = {0, 2, 4}, then H is a nonempty subset of Z_6
5. Can we show that (H, +) is a subgroup of (Z_6, +) ? Given, the table for (H, +), check for closure, associativity, identity and inverse.

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2