DISCRETE STRUCTURE

LECTURE-17

MONOID

Topics covered

- Introduction to Monoid
- Groups
- Subgroups

Introduction & Definition of Monoid

$\langle A, \bullet \rangle$ is a monoid if the following conditions are satisfied:

1. $\bullet$ is a closed operation i.e. if $a \in A$ and $b \in G$ then $a \bullet b \in A$
2. $\bullet$ is associative
3. There is an identity element

Examples: Let A be a finite set of heights. Let $\bullet$ be a binary operation such that $a \bullet b$ is equal to the taller of a and b. Then $\langle A, \bullet \rangle$ is a monoid where the identity is the shortest person in A

$\langle \{\text{true, false}\}, \wedge \rangle$ is a monoid: $\wedge$ is associative, true is the identity, but false has no inverse

$\langle \{\text{true, false}\}, \vee \rangle$ is a monoid: $\vee$ is associative

false is the identity, but true has no inverse

PROPERTIES OF ALGEBRAIC STRUCTURES

properties

Semigroup $\subseteq$ monoid $\subseteq$ group $\subseteq$ Abelian Group

Theorem: (unique identity) Suppose that $\langle A, \bullet \rangle$ is a monoid then the identity element is unique

Proof: Suppose there exist two identity elements e and f. [We shall prove that e=f]

$$e = e \bullet f \; (\text{since f is an identity})$$

$$= f \; (\text{since e is an identity})$$

Theorem: (unique inverse) Suppose that $\langle A, \bullet \rangle$ is a monoid and the element x in A has an inverse. Then this inverse is unique.

Proof: ??

Properties of Groups

Theorem (The cancellation laws): Let $\langle G, \bullet \rangle$ be a group then $\forall a, x, y \in G$

(i) $a \bullet x = a \bullet y \Rightarrow x = y$

(ii) $x \bullet a = y \bullet a \Rightarrow x = y$

Proof: (i) Suppose that $a \bullet x = a \bullet y$ then by axiom 3 a has an identity a^{-1} and we have that

$$a^{-1} \bullet (a \bullet x) = a^{-1} \bullet (a \bullet y)$$

$$\Rightarrow (a^{-1} \bullet a) \bullet x = (a^{-1} \bullet a) \bullet y \text{ (associativity)}$$

$$\Rightarrow e \bullet x = e \bullet y \; (a^{-1} \text{ is the inverse})$$

$$\Rightarrow x = y \text{ (identity)}$$

(ii) is proved similarly

Theorem (The division laws): Let $\langle G, \bullet \rangle$ be a group then $\forall a, x, y \in G$

(i) $a \bullet x = b \Leftrightarrow x = a^{-1} \bullet b$

(ii) $x \bullet a = b \Leftrightarrow x = b^{-1} \bullet a$

Proof ??

Theorem (double inverse) :If x is an element of the group $\langle G, \bullet \rangle$ then

$$\left(x^{-1}\right)^{-1} = x$$

Proof:

$$\left(x^{-1}\right)^{-1} \bullet x^{-1} = e \left(\left(x^{-1}\right)^{-1} \text{ is inverse of } x^{-1} \right)$$

$$\Rightarrow \left(\left(x^{-1}\right)^{-1} \bullet x^{-1} \right) \bullet x = e \bullet x = x$$

$$\Rightarrow \left(x^{-1}\right)^{-1} \bullet \left(x^{-1} \bullet x\right) = x \; (\text{associativity})$$

$$\Rightarrow \left(x^{-1}\right)^{-1} \bullet e = x \; \left(x^{-1} \text{ is inverse of } x\right)$$

$$\Rightarrow \left(x^{-1}\right)^{-1} = x \; (\text{identity})$$

Theorem (reversal rule)

If x and y are elements of the group $\langle G, \bullet \rangle$ then

$$(x \bullet y)^{-1} = y^{-1} \bullet x^{-1}$$

Proof ??

For a an arbitrary element of a group $\langle G, \bullet \rangle$ we can define functions $\sigma_a : G \to G$ and $\rho_a : G \to G$ such that

$$\forall x \in G \ \sigma_a(x) = a \bullet x \text{ and } \rho_a(x) = x \bullet a$$

Theorem: $\sigma_a : G \to G$ and $\rho_a : G \to G$ are permutations of G

Proof: Consider σ_a

[prove 1-1] suppose for x,y in G

$\sigma_a(x) = \sigma_a(y)$

$\Rightarrow a \bullet x = a \bullet y \Rightarrow x = y$ (cancellation laws)

[Prove onto] For any y in G

$\sigma_a(a^{-1} \bullet y) = a \bullet (a^{-1} \bullet y)$

$= (a \bullet a^{-1}) \bullet y$ (associativity)

$= e \bullet y$ (a^{-1} is inverse of a)

$= y$ (identity)

Corollary: In every row or column of the multiplication table of G each element of G appears exactly once.

SUBGROUPS

$\langle H, \bullet \rangle$ is a subgroup of the group $\langle G, \bullet \rangle$ if $H \subseteq G$ and $\langle H, \bullet \rangle$ is also a group

Examples: $\langle Q - \{0\}, \times \rangle$ is a subgroup of $\langle R - \{0\}, \times \rangle$
$\langle \{1, -1, i, -i\}, \times \rangle$ is a subgroup of $\langle C - \{0\}, \times \rangle$

Test for a subgroup
Let H be a subset of G. Then $\langle H, \bullet \rangle$ is a subgroup of $\langle G, \bullet \rangle$ iff the following conditions all hold:

(1) $H \neq \varnothing$

(2) H is closed under multiplication

(3) $x \in H \Rightarrow x^{-1} \in H$

For every group $\langle G, \bullet \rangle$, $\langle G, \bullet \rangle$ and $\langle \{e\}, \bullet \rangle$ are subgroups
$\langle \{e\}, \bullet \rangle$ is called the trivial subgroup of $\langle G, \bullet \rangle$

a proper subgroup of $\langle G, \bullet \rangle$ is a subgroup different from G

A non-trivial proper subgroup is a subgroup equal neither to $\langle G, \bullet \rangle$ or to $\langle \{e\}, \bullet \rangle$

Algebraic Structures with two Operations

- So far we have studied algebraic systems with one binary operation. We now consider systems with two binary operations.
- In such a system a natural way in which two operations can be related is through the property of distributivity;

Let $\langle A, \bullet, * \rangle$ be an algebraic system with two binary operations $\bullet$ and $*$. Then the operation $*$ is said to distribute over the operation $\bullet$ if

$\forall x, y, z \in A \; x * (y \bullet z) = (x * y) \bullet (x * z)$

and

$(y \bullet z) * x = (y * x) \bullet (z * x)$

Example: $\times$ distributes over +

$\wedge$ distributes over $\vee$

$\vee$ distributes over $\wedge$

Application & Scope of resech

- Coding theory
- Cryptography
- Automata Theory