BLG501E – Discrete Mathematics

2021 – 2022 Fall Term

Asst. Prof. Gökhan SEÇİNTİ

Outline

- Algebraic Structures
- Cyclic Permutations
- Homomorphism

Algebraic Structures

Definitions:

- Underlying (carrier) set S
- Set of operations
  - An ***n-ary operation*** on a set S is a function : $S \times S \times \cdots \times S \rightarrow S$, where the domain is the product of n factors.
  - A ***binary operation*** on a set S is a function : $S \times S \rightarrow S$.
  - A ***monadic operation*** (or ***unary operation***) on a set S is a function : $S \rightarrow S$.
- Special elements
  - Identity, inverse, absorbing/zero

Algebraic Structures

A binary operation can have some of the following properties:

- ***associative property***: $a\ (b\ c) = (a\ b)\ c$ for all $a, b, c \in S$;

- ***existence of an identity element***:
there is an element $e \in S$ such that
$e\ a = a\ e = a$ for all $a \in S$ (*e* is an *identity* for *S*);

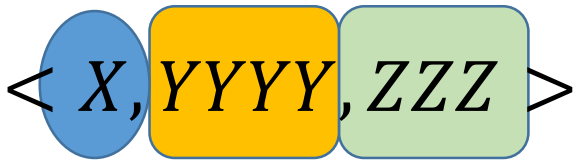
- ***existence of inverses***: for each element $a \in S$
there is an element $a' \in S$ such
that $a'\ a = a\ a' = e$ (*a'* is an *inverse* of *a*);

- ***commutative property***: $a\ b = b\ a$ for all $a, b \in S$

Algebraic Structures

Algebraic signature

The signature of an algebraic system is the collection of relations and operations on the basic set of the given algebraic system together with an indication of their arity.



Underlying set, Operations, Elements

https://encyclopediaofmath.org/

Algebraic Structures

Algebraic Family: Set of algebraic structures employing same axioms

Example:

- $< I, \cdot, 1 >, < R, +, 0 >, < \wp(S), \cap, \emptyset >$
- $< \ Propositions, \ \wedge, \ \vee, \neg, TRUE, FALSE >$
  $< \wp(S), \cap, \cup, \ \overline{\ }, \emptyset, S >$

Algebraic Structures

Closure property: a set *S* is closed under an operation if the range of is a subset of *S*.

Example:

$A = < S, \circ, \triangle, k >$ S carrier; $\circ$ binary, $\triangle$ unary operations; k element

Closure of $T' \subseteq T$ under $\circ, \triangle$ operations

- $\forall a, b \in T' \Rightarrow a \circ b \in T'$
- $\forall a \in T' \Rightarrow \triangle a \in T'$

Example:

$T = N$ and $T' = \{x | 0 \leq x \leq 10\}$

Operation $\max(x, y)$ has closure over T'

Algebraic Structures

Subalgebra: is a subset of an algebra, closed under all its operations, and carrying the special elements.

$A = < S, \circ, \triangle, k >$ $A' = < S', \circ', \triangle', k' >$

Example: $I, \mathbb{O}, \mathbb{E}$ integer, odd and even numbers

- $< I, +, 0 > < \mathbb{E}, +, 0 >$
- $< I, \cdot, 1 > < \mathbb{O}, \cdot, 1 >$

Algebraic Structures

Identity: an element e in an algebraic structure S such that

$$e\ a = a\ e = a \text{ for all } a \in S.$$

Absorbing/zero: an element 0 in an algebraic structure S such that

$$0\ a = a\ 0 = 0 \text{ for all } a \in S.$$

Algebraic Structures

For a binary operation $*$ on a set S:

Left/Right Identity:

An element e is (left) absorbing if for all $a \in A$ we have $e*a=a$.

An element e is (right) absorbing if for all $a \in A$ we have $a*e=a$.

Left/Right Absorbing/zero:

An element z is (left) absorbing if for all $a \in A$ we have $z*a=z$.

An element z is (right) absorbing if for all $a \in A$ we have $a*z=z$.

A two-sided absorbing element is both left and right absorbing: $z*a=a*z=z$ for all a. A two-sided absorbing element is unique.

Algebraic Structures

Definition of Inverse elements:

For a binary operation $*$ on a set S:

if $w * x = 1$ then w is a left inverse of x

if $x * y = 1$ then y is a right inverse of x

if $x * y = y * x = 1$ then y is an inverse of x.

Algebraic Structures

Definition of Inverse elements:

*For a binary **associative** operation $*$ on a set S:*

Lets say w and y are left and right inverses of x respectively.

$$w * x = x * y = 1$$

$$w = w * 1 = w * (x * y) = (w * x) * y = 1 * y = y$$

Algebraic Structures

Theorem: *if an inverse of an element exists, it is unique.*

Let's say $b \neq a$ *and both a and b are inverse of x*

$$ax = xa = 1 \text{ and } bx = xb = 1$$

$$a = a1 = a(xb) = (ax)b = b \quad (\textbf{associative property})$$

Algebraic Structures

	closed	*associative*	*commutative*	*existence of identity*	*existence of inverses*
semigroup	√	√			
monoid	√	√		√	
group	√	√		√	√
abelian group	√	√	√	√	√

Algebraic Structures

Example:

$\sum alphabet;$

- $< \sum^{+}, \& >$: semigroup
- $< \sum^{*}, \&, \Omega >$: monoid

Example: (Semigroup)

$$R_\alpha \subseteq A \times A \; ; |A| = n; |\wp(A \times A)| = 2^{n^2}$$

$R_\alpha \circ R_\rho \rightarrow R_\gamma$ composition operation

Algebraic Structures

Theorem: Elimination on groups

$$ac = bc \Rightarrow a = b$$

$$(ac)c' = (bc)c' \Rightarrow a = b$$

Theorem:

for ax =b only solution of x = a'b

Theorem:

(cd)' = d'c'

Operations on subgroup

Show that every group operation is

injective / one-to-one

and

surjective / onto.

Permutation Groups

Permutation is a one-to-one and onto function σ: $S \rightarrow S$, where S is any nonempty set.

If $S = \{a_1, a_2, \ldots, a_n\}$, a permutation σ is sometimes written as the $2 \times n$ matrix.

$$\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & a_n \\ a_1\sigma & a_2\sigma & a_3\sigma \cdots & a_n\sigma \end{pmatrix}$$

where $a_i\sigma$ means $\sigma(a_i)$.

Permutation Groups

Example: $A = \{1,2,3\}$

$$p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Permutation Groups

$$A = B \cup C, B \cap C = \emptyset ; |B| = r \ ; |C| = n - r$$

$B = \{b_0, b_2 \dots b_{r-1}\} = \{b_i | p(b_i) = b_{i+1} \, mod \, r\}$ elements in cycle

$C = \{c_0, c_1 \dots c_{n-r-1}\} = \{c_i | p(c_i) = c_i \, mod \, n - r\}$ elements that are not in cycle

$$\mathrm{p} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

B= {1,2,5} (1,2,5) or (2,5,1) or (5,1,2)

C= {3,4}

Permutation Groups

Composition over permutation groups is **not *commutative***.

$$(4,1,3,5) \circ (5,6,3) \neq (5,6,3) \circ (4,1,3,5)$$

If cycles do not share a common element commutative property still holds.

Additional Reads

Reads:

- Chapter 14 and 16, Discrete and Combinatorial Math. 5ed, Grimaldi.
- Handbook of Discrete and Combinatorial Math., Grimaldi.