Algebraic Systems

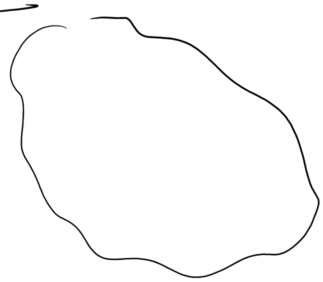
28 October 2020 09:03

n-ary operation

→ Various examples

→ properties

→ Special elements.



$\langle S, * \rangle$ w.r.t $*$

- Closure
- Associative
- Identity
- Inverse
- Commutative.

Closure + Associative: Semigroup

Semigroup + Identity: monoid

monoid + Inverse: Group (most important)

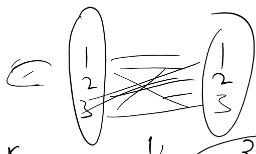
Group + Commutative: abelian group.

Unit-4
Unit-5
2
1-Lecture

quiz-2
version 1
version 2
7 quiz →
best five

Evaluation
3
4
2
1
1
whole Syllabus
final Evaluation
(20)

$n \quad n \quad n^n \rightarrow \quad \langle X^X, \circ \rangle$



3^3 i.e. 9

$X \rightarrow$ set

$X^X \rightarrow$ set of all mappings from X to X.

$\circ \rightarrow$ Composition of these mapping. $f \circ g(x) = f(g(x))$ for all $x \in X$ in X^X.

$x \circ e = e \circ x = x$

$\langle X^X, \circ \rangle$ is a monoid ?

1. Associativity $\rightarrow$ identity mapping
2. Identity $\rightarrow$ $f(x) = x$ for all $x \in X$.

identity wrt $\circ$

$S \rightarrow$ non-empty set

$P(S) \rightarrow$ Powerset

$\langle P(S), \cup \rangle \qquad \langle P(S), \cap \rangle$

monoid $\rightarrow$? $\qquad$?

$e = \phi \qquad e = S.$

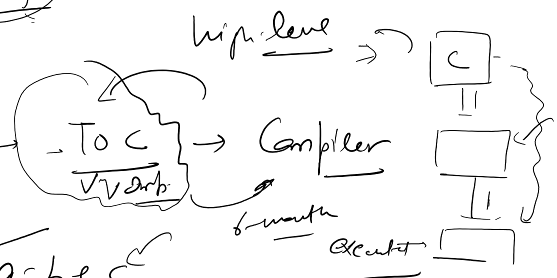
not a monoid $\rightarrow \langle I, \angle \rangle$

28 October 2020 09:20

{He is a boy.}

Semigroup but not monoid. ⇒ $(< E, + >)$ 0 →

App^n of Monoid :- Grammars and formal language.



a = b + c

V → non-empty finite set of Symbols.

alphabet

$V_1 = \{0, 1\}$, $V_2 = \{a, b, c\}$,

C lang.

vocabulary

V = character, Symbol, numbers

$V = \{ -, -, - \}$

letter

Symbol Symbols.

Character

While

$\{a, b, \ldots z\}$

While

A string is an ordered set of

→ Sequence

→ Word

→ Sentence

lexicographic ordering.

$V = \{a, b\}$

|aa, ab, ba, bb, aab

2 3

Empty String → Λ → String of length 0.

$\langle V^*, \circ \rangle$ Monoid

$V = \{a, b\}$

$V^* = \{\Lambda, a, b, aa, ab, bb, aab, \ldots$

→ V^* → set of Strings over the alphabet V

→ V^+ → set of non-empty Strings $\quad V^+ = V^* - \{\Lambda\}$

$\langle V^*, \circ \rangle$ → Monoid

$\circ$ → Associative

identity → Λ

$\langle V^+, \circ \rangle$

Monoid

→ Identity ✗

not a monoid

Assumption: String in V^*, V^+ are of finite length.

Let $\alpha, \beta \in V^*$ then operation $\circ$ → Concatenation.

$\alpha \circ \beta = \alpha\beta$

Let $V = \{a, b\}$ $\quad V^+ = \{ab, \quad baa\}$

$\alpha . \Lambda = \Lambda . \alpha = \alpha$

$(ab) \circ (baa) = abbaa$

Concatenation

28 October 2020 09:36

Sequential machines

S : any non-empty set

$\pi(S)$:- set of all partitions of S

$S_1 = \{a, b\}$, $\pi(S_1) = \{\{\overline{a}, \overline{b}\}, \{\overline{a, b}\}\}$

$S_2 = \{a, b, c\} = \pi(S_2) = \{\{\overline{a}, \overline{b}, \overline{c}\}, \{a, \overline{b, c}\}, \{\overline{a, b}, c\}, \{\overline{a, b, c}\}\}$

$S_3 = \{a, b, c, d\} \Rightarrow$ 12 - 7

$\rightarrow |S| = n$, $\rightarrow$

$2^{n-1} - 1 = {}^{n}C_2 + 1$ {Home exercise}

$P = \{ P_1, P_2 \ldots \}$ $Q = \{ Q_1, Q_2 \ldots \}$ two partitions of set $\underline{S}$.

$P, Q \in \pi(S)$

Binary operation $*$ on $\pi(S)$ s.t.

$P * Q$ = set of intersections of every element of P with every elem of Q, leaving out empty sets.

$x * e = e * x = x$ $e \in S$.

$\pi(S) \to$

$\overline{x_1, x_2} \cap \overline{x_3, x_4, x_5} = \phi$

$\overline{x_1, x_2}$

$S = \{ x_1, x_2 \ldots x_6 \}$

$P = \{ \overline{x_1, x_2}, \overline{x_3, x_4, x_5}, \overline{x_6} \}$ $Q = \{ \overline{x_1, x_2, x_3}, \overline{x_4}, \overline{x_5, x_6} \}$

$P * Q = \{ \overline{x_1, x_2}, \overline{x_3}, \overline{x_4}, \overline{x_5}, \overline{x_6} \}$

$\langle \pi(S), * \rangle$ is monoid or not

$* \to$ Associative

identity $\to \{ \overline{x_1, x_2, x_3, x_4, x_5, x_6} \}$

$(\overline{x_1, x_2, x_3}) * (\overline{x_1, x_2, \ldots x_6})$
$= \overline{x_1, x_2, x_3}$

Power of element :- $\langle M, * \rangle$ $a \in M$.

$a^0 = e$, $a^1 = a$, $a^2 = a^1 * a$ ...

$a^{j+k} = a^j * a^k = a^k * a^j = a^{k+j}$ for all $j, k \in N$

Cyclic Monoid :- $a \in M$.

If every element can be written as some power of a. i.e. a^n for $n \in N$

$\langle 3^n, * \rangle$ $3^0 = 1$

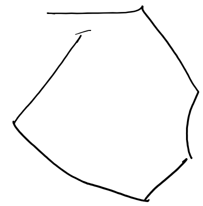
$\langle I, + \rangle$

M

a a^n

$\langle 0, 1, 2 \rangle$

$\langle N, + \rangle$



28 October 2020 09:55

$f: X \to X$

$\circ \to$

$\langle S, \circ \rangle$

$\langle Z_m, +_m \rangle \quad m = 4$

$Z_m \to$

$+_4 \to$

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_2	f_3	f_0
f_2	f_2	f_3	f_0	f_1
f_3	f_3	f_0	f_1	f_2

(I)

$+_4$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

(II)

$I \to II$

Re-lable the entries

$f^0 \quad f^1 \quad f^2 \quad f^3$

$[0] \quad [1] \quad [2] \quad [3]$

$\circ$

$\downarrow$

$+_4 \to$

$i, j \to 0, 1, 2, 3$

$\psi: F \to Z_4$ s.t.

$\psi(f_j) = [j]$ for $j = 0, 1, 2, 3$

$\psi(f_i \circ f_j) = \psi(f_i) +_4 \psi(f_j)$

$\psi(f_2 \circ f_3) = \psi(f_2) +_4 \psi(f_3)$

$\psi(f_1) = [2] +_4 [3]$

$\| \; [1] = [1]$

$[1] = [1] \Rightarrow$ equation holds

$X \to Y$

Let $\langle X, \circ \rangle$ and $\langle Y, * \rangle$

mapping $g: X \to Y$ is called Homomorphism from $\langle X, \circ \rangle$ to $\langle Y, * \rangle$

if for any $x_1, x_2 \in X$

$$g(x_1 \circ x_2) = g(x_1) * g(x_2)$$] Question

then $\langle Y, * \rangle$ is a homomorphic image of $\langle X, \circ \rangle$

$g: X \to Y$ is onto $\to$ epimorphism

one to one $\to$ monomorphism

one to one onto $\to$ isomorphism

28 October 2020 10:06

$\langle Z_4, +_4 \rangle$ $\langle B, + \rangle$

$B = \{0, 1\}$

$Z_4 = \{[0], [1], [2], [3]\}$

$+_4 \Rightarrow [i] +_4 [j] = [(i+j) \bmod 4]$

+	0	1
0	0	1
1	1	0

Show that $\langle B, + \rangle$ is a homomorphic image of $\langle Z_4, +_4 \rangle$

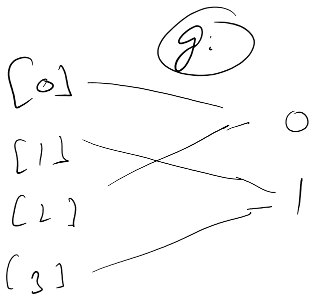
→ find a mapping $g : Z_4 \to B$

→ 5-minute Break

10:15 AM

$g(x +_4 y) = g(x) + g(y)$

homomorphism



$g([i] +_4 [j]) = g([i]) + g([j])$

Verify it

28 October 2020 10:20

Homomorphism for Semigroups and Monoids.

$\langle S, * \rangle \qquad \langle T, \Delta \rangle$

$g : S \to T$ s.t for any $a, b \in S$

$g(a * b) = g(a) \, \Delta \, g(b)$ — (1) → Semigroup homomorphism

Implication of Equation (1).

$g : S \to T$.

$\langle S, * \rangle \to$ Semigroup.

$\langle T, \Delta \rangle \to$ may or may not be a Semigroup

and eq. (1) holds.

then Δ must be associative, and hence $\langle T, \Delta \rangle$ ~~is~~ must be a Semigroup.

$\langle S, * \rangle$

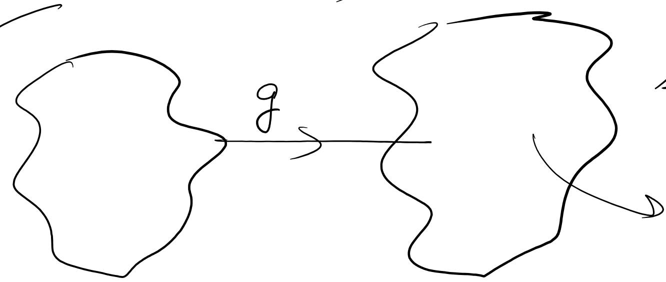
Let $a, b, c \in S$

$$g((a*b)*c) = g(a*b) \, \Delta \, g(c) = (g(a) \, \Delta \, g(b)) \, \Delta \, g(c)$$

$$g(a*(b*c)) = g(a) \, \Delta \, ((g(b) \, \Delta \, g(c)))$$

!! Δ is also associative

Sem



has the semigroup.

Conclusion :⇒ Eq. (1) preserves the semigroup character because it preserves the associativity.

Associativity.

→ idempotent element is preserved or not?. $g(a*a) = g(a) = g(a) \Delta g(a)$

→ identity is preserved or not ??. —

Let $\langle S, *, e \rangle$!! Monoid

$\langle S, * \rangle$ e_S $\langle T, \Delta \rangle$ e_T $g(e_S) = e_T$ $\neq e_T$.

$g : S \to T$ → Semigroup homomorphism

$x*e = e*x = x$

q. (1) → not sufficient to prove that identity preserved ∃

For any $a \in S$

✓ $g(a*e) = g(e*a) = g(a) \Delta g(e) = g(e) \Delta g(a) = g(a)$

Δ ↑

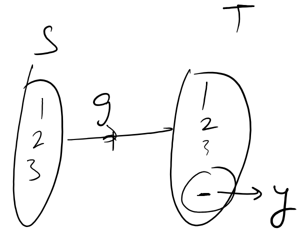
✗ ✓ $g(a) \Delta g(e) = g(a)$ → Can g write !!??

↑ identity

$x*e = x$

$g(e)$ is identity w.r.t Δ.

e →



onto.

$g(e) \Delta y \neq y$

→ onto ✓

(1) g.1(1) $g(x * y) = g(x) \Delta g(y)$ (1) → g: → onto ✓

$g(e_S) = e_T$ (2)

identity element
would be preserving

Conclusion..

If $\langle M, *, e_M \rangle$ and $g: M \to T$ (onto) exist then

$\langle T, \Delta \rangle$ must be monoid with $g(e_M)$ as

identity element

Group theory :- → Complete book

→ basic properties → fast-adders } → Digital logic

→ Wellknown examples → Error Correcting Codes - { Group Codes }

Computer N/ws.

→ Subgroups -

→ group homomorphism

→ Imp. Theorems of group theory }

A ~~sss~~ssociative whole system
identity →
Inverse → for $x \in G$, $x * x^{-1} = x^{-1} * x = e$

Properties –
→ Unique

A group cannot have zero element

$0 * x = x * 0 = 0$ ✗

$a * a = a$

→ identity → idempotent

Let $a \in G$ → $a * a = a$ → no other element except e is idempotent in G. $\{a = e\}$

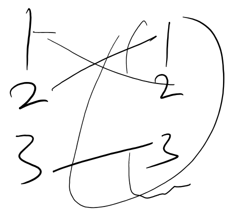
$$e = a^{-1} * a = a^{-1} * (a * a) = (a^{-1} * a) * a = e * a = a$$

28 October 2020 10:45

Composition table :-

permutation :- $S \xrightarrow{1\text{-}1} S$. $\to n!$

one-to-one mapping



3!

1
2
3

$(3)(2)(1) \to 3!$

$n!$

1. Every element is covered
2. no element is repeated

Theorem!

$\langle G, \circ \rangle$

Each row | Column → is a permutation

1	2	3	4	5
3	4	1	2	5

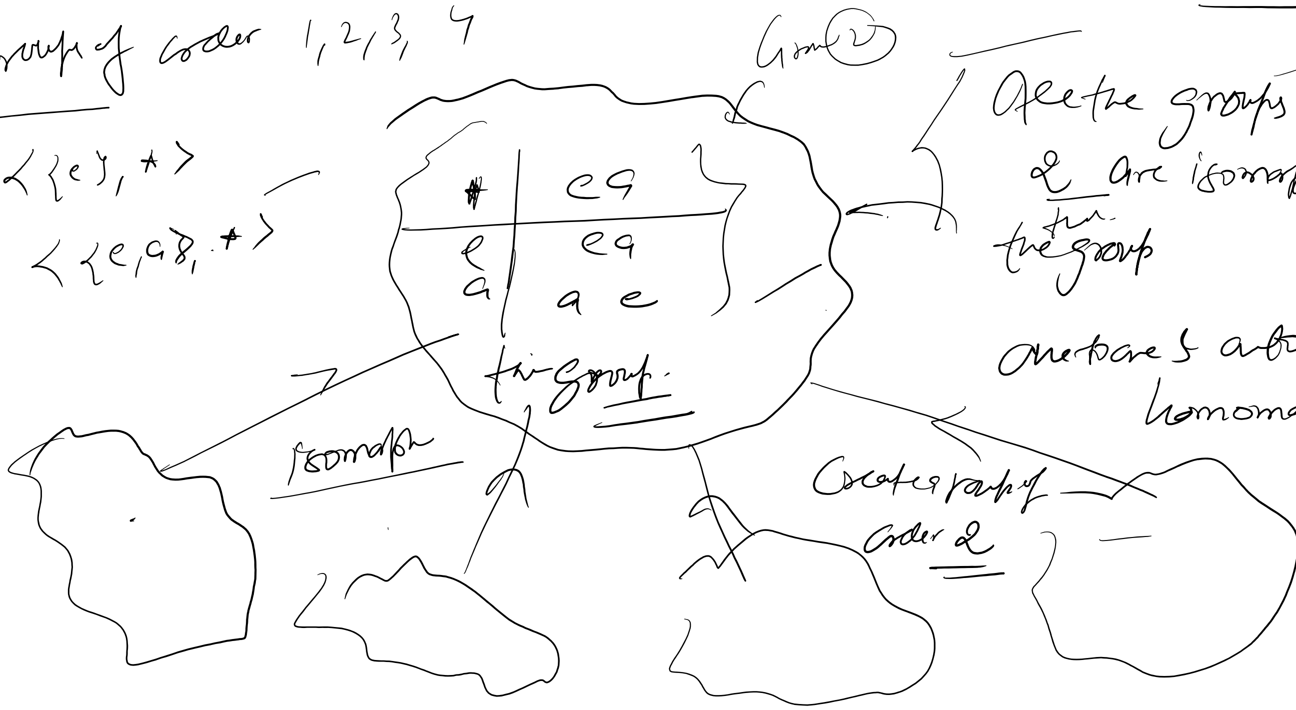
28 October 2020 10:50

order of a group → no. of elem — $\langle G, * \rangle$ → $*$ → Commutative

↳ abelian groups.

Groups of order 1, 2, 3, 4

1. $\langle \{e\}, * \rangle$
2. $\langle \{e, a\}, * \rangle$



All the groups of order 2 are isomorphic to the group.

one to one & onto homomorphism

28 October 2020 10:55

order 3. $G = \{e, a, b\}, *$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

no other composition table is possible.

$|G| = 3$

14/24.

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

not isomorphic to each other

home exercise

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_2	f_3	f_0
f_2	f_2	f_3	f_0	f_1
f_3	f_3	f_0	f_1	f_2

fact:- all the groups of order 4 are isomorphic to these two groups.