MATRIX ANALYSIS - SUPLEMENTARY MATERIAL

Groups, Rings and Fields

OCT/17/2021 LEC04

Algebraic structures : $(S, \circ)$

- A nonempty set S
- A binary operation $a \circ b$ to be constructed a and b are selected from S : $\underbrace{\circ : S \times S \rightarrow S}$
- the operation $\circ$ is closed in S

  if $a, b \in S$ then $a \circ b \in S$ this can also be represented by

Nothing else here yet (No Associativeness, No commutativeness, etc) this comes in more sophisticated structures

Examples

AS1) $(\mathbb{Z}, +)$: $S = \mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$, $a \circ b \triangleq a + b$

$5; 7 \in \mathbb{Z}$, $5 \circ 7 = 5 + 7 = 12 \in \mathbb{Z}$

the sum + $(\circ = +)$ of any two integers is always an integer. then this is an algebraic structure (A.S.)

AS2) $(\mathbb{R}, \cdot)$: $S = \mathbb{R}$, $a \circ b \triangleq a \cdot b$ (regular multiplication

$\sqrt{2}, \pi \in \mathbb{R}$, $\sqrt{2} \circ \pi = \sqrt{2} \cdot \pi = \sqrt{2}\pi \in \mathbb{R}$

the multiplication of any two real numbers returns always another real number. this is an AS counter examples

AS3) $(\mathbb{N}, -)$: $S = \mathbb{N}$, $a \circ b \triangleq a - b$

$\mathbb{N} = \{0, 1, 2, \dots\}$ $\quad 7, 2 \in \mathbb{N}$, $7 - 2 = 5 \in \mathbb{N}$

$3, 1 \in \mathbb{N}$, $3 - 1 = 2 \in \mathbb{N}$

$2, 6 \in \mathbb{N}$, $2 - 6 = -4 \notin \mathbb{N}$ Not an A.S.

$a < b$
whenever we pick ~~$a<b$~~
$a \circ b \notin S$: closedness fails!

When testing, it is enough to find just one case (with two members a and b) ~~in~~ which fails to show it is not an AS. To show it is an AS we need proof in terms of $a, b \in S$, then explore the construction of $\circ$ (i.e., how it is defined) to show $a \circ b \in S$ for any $a, b \in S$

AS4) $(\mathbb{Z}, \div)$: $S = \mathbb{Z}$, $a \circ b = a \div b$ (regular division)

$4, 2 \in \mathbb{Z}$, $4 \div 2 = \frac{4}{2} = 2 \in \mathbb{Z}$

$121, 11 \in \mathbb{Z}$, $121 \div 11 = 11 \in \mathbb{Z}$

$-9, 3 \in \mathbb{Z}$, $-9 \div 3 = -3 \in \mathbb{Z}$

$5, 3 \in \mathbb{Z}$, $5 \div 3 = \frac{5}{3} \notin \mathbb{Z}$ (it is not an integer
it is a rational number
which is not in $\mathbb{Z}$)

it is not an AS

it is common to use previously defined AS, add more properties to it and then form a new AS that is more sophisticatted. By doind so, the new AS inherits all properties of the existing AS.

recall that $a,b \in S \Rightarrow a \circ b \in S$ (closedness)

GROUPS: $\underbrace{(S,\circ)}$ + 3 extra properties

- $a \circ b$ is associative: $(a\circ b)\circ c = a\circ(b\circ c)$

  this property means that we can start combining any two elements, generate an intermediary result, ~~then~~ which is then combined again to form the final result

  $\underbrace{(a\circ b)}_{e}\circ c\circ d = e\circ c\circ d = e\circ\underbrace{(c\circ d)}_{f} = e\circ f$ // or

  $a\circ(\underbrace{b\circ c}_{g})\circ d = a\circ g\circ d = a\circ\underbrace{(g\circ d)}_{h} = a\circ h$, etc

  any order will provide the same result whenever the op $\circ$ is associative, If the results are diff, then the op $\circ$ is not associative

- there is a neutral element $0_S \in S$ such that for any $a \in S$

  $$0_S\circ a = a\circ 0_S = a$$

  0_s is unique!

~~th~~A group can be represented by the notation $(S, \circ, 0_S)$, which shows that this new structure is closed in S via $\circ$ and has a neutral element 0_S. However, associativeness and the existence of inverse elements $\bar{a}' \in S$ for all a is not captured is this notation. Then we can use a better notation:

$(G, \circ, 0_G)$: the set can still be S, the op is the same $\circ$ and we also have the neutral elem. ~~0_G~~ $0_G = 0_S$. However we can now define that whenever we use this notation we are saying that we talk about an AS $(S, \circ)$ that has a neutral 0_S, an associative op $\circ$, ~~and a neutral~~ and that has inverse elements $\bar{a}'$ for all $a \in S$. that is, $(G, \circ, 0_G)$ assures that this is a group and has all the required properties for a group.

Examples

G1) $(\mathbb{Z},+,0)$ is a group over the integers $\mathbb{Z}$ with $a \circ b \hat{=} a+b$, with neutral el 0?

It is! because the ordinary sum $(\circ = +)$ of any two integers returns another integer (closedness) the neutral element $0_G = 0$ works via $\circ = +$ over all $a \in G = \mathbb{Z}$, since any integer summed with zero is again the same ~~[illegible]~~ integer

$$a+0 = 0+a = a$$

What is the inverse a^{-1} for any given a? We can use the defined op $\circ \hat{=} +$ and the set $G = \mathbb{Z}$ to check/calculated if a^{-1} exists, and/or what it is. We ~~know~~ $a \circ b = a+b = b+a = b \circ a$, that is, this op. is <u>commutative</u> but we don't ~~[illegible]~~ need that ~~for~~ ~~a~~ to define a group. If it is comm., it's just better to work with this group. let's use the definition of Neutrality

$$a^{-1} \circ a = 0_G \Rightarrow a^{-1} + a = 0 \Rightarrow \boxed{a^{-1} = -a} \;\; \forall a \in \mathbb{Z}.$$

that is, in this case the inverse a^{-1} is just minus the original element a.

G2) $(M_2(\mathbb{R}), +, O_{2\times 2})$, $M_2(\mathbb{R})$ = set of 2×2 matrices with real entries

$+$ = ordinary matrix addition (entrywise sum)

$O_{2\times 2} \triangleq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the neutral element.

take two els from $M_2(\cdot)$: $A, B \in M_2(\cdot)$

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ \delta & h \end{bmatrix}$.

$$A \circ B = A + B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \in M_2$$

Matrix sum is associative: $(A+B)+C = A+(B+C)$.

the neutral element $O_{2\times 2}$ works for any matrix:

$$A + O_{2\times 2} = O_{2\times 2} + A = A.$$

Where is the inverse element for A? We have $A \circ A^{-1} = O_G$ ~~and $A^{-1} \circ A$~~

$$A \circ A^{-1} = A + A^{-1} = O_{2\times 2} \Leftrightarrow A^{-1} = O_{2\times 2} - A = -A$$

the inverse for A is minus A, i.e., $-A$.

We also have that the sum of any $A, B \in M_2$ is again a new matrix $A+B$ that is in M_2.

this is a group!

G3) $\left(M_2(\mathbb{R}), \overset{\text{Matrix}}{\text{product}}, I_2\right)$; $A \circ B \triangleq AB$

$I_2 \triangleq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \triangleq 0_G$

is it a closed structure?

$\forall$ A, B are 2×2 matrices of real numbers the product AB is always defined (matrices have compatible dimensions) and return a new matrix $C = AB$ that is again a 2x2 matrix with real entries, i.e., $C = AB \in M_2$

Is it associative? Yes, because the matrix product is associative

$$ABC = (AB)C = A(BC) \quad \text{or} \quad (A \circ B) \circ C = A \circ (B \circ C).$$

Neutral I_2 works? Yes! $AI_2 = I_2 A = A \; \forall A \in M_2$

And the inverse A^{-1}? Note that we talk here about the inverse element $A^{-1} \in M_2$ that is not necessarily the matrix inverse. In example G2 we had $A^{-1} = -A$. Here, by coincidence, the inverse element is related to a matrix inverse because we selected the matrix product for an operation. We want to find an element B such that $A \circ B = 0_G$ or $AB = I_2$. Or we want $A^{-1}AB = A^{-1}I_2$

$$B = A^{-1}$$

In this case the inverse of any element $A \in M_2$ is the matrix inverse itself, i.e., $\underset{\substack{\uparrow \\ \text{inverse} \\ \text{elem.}}}{A^{-1}} = \underset{\substack{\uparrow \\ \text{Matrix} \\ \text{inverse}}}{A^{-1}}$

However, take $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

$\nexists\, A^{-1}$ for matrix A above. there are infinite elements $A \in M_2(\mathbb{R})$ that do not have an inverse element under $\circ = \text{matrix product}$ in $M_2(\mathbb{R})$.

Then it is not a group!

G4) $(\bar{M}_2(\mathbb{R}), \text{matrix product}, I_2)$, where $\bar{M}_2(\mathbb{R})$ = set of 2x2 invertible matrices with real entries.

By restricting the set $M_2(\mathbb{R})$ to contain only invertible matrices, we fix the problem of inverse elements in example G3! Now $\bar{M}_2(\mathbb{R})$ with $A \circ B = AB$ with $O_G = I_2$ is a group!

Commutative Groups (CG) are those in which

$$\boxed{a \circ b = b \circ a}$$

and are of special interest for us. they are also known as Abelian groups.

Examples

CG1) Examples G1, G2 [illegible] are comm.

CG2) Example G_4 is Not commutative because matrix product is not commutative.

CG3) $\left(\bar{M}_2^D(\mathbb{R}), \text{matrix product}, I_2\right)$, where $\bar{M}_2^D$ is the set of invertible diagonal matrices.

the matrix product of diagonal matrices does commute (check it with an example!):

$$D_1 D_2 = D_2 D_1 \in \bar{M}_2^D(\mathbb{R})$$ and the product of diag. matrices is again diagonal!

then CG3 is a commutative group!

RING is an Abelian group with a seconda operation $\star$ having the following properties $(R, \circ, \star, 0_R, 1_R)$

- $\star$ is associative: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$
- $\star$ is distributive over $\circ$

$$a \star (b \circ c) = (a \star b) \circ (a \star c)$$

and

$$(b \circ c) \star a = (b \star a) \circ (c \star a)$$

because op $\star$ does not need to be commut. i.e. $a \star b \neq b \star a$

(- $\star$ has a unique neutral element 1_G.) ~~this is not~~

this is not required for a ring. When it holds, we call it a unit ring

Examples

R1) $(\mathbb{Z}, +, \cdot, 0, 1)$ is a ring, since ordinary addition and multiplication over the integers have neutral elements 0 and 1 and produce numbers that are again integers.

this is a ring with unity, or a unit ring

$a, b \in \mathbb{Z}$: $a \circ b \triangleq a + b$ (Group op)

$a, b \in \mathbb{Z}$: $a \star b \triangleq a \cdot b$ (ring op)

$0_R \triangleq 0$: $a + 0 = 0 + a = a$ (neutral for group op)

$1_R \triangleq 1$: $a \cdot 1 = 1 \cdot a = a$ (neutral for ring op) (unit)

a^{-1}: $a^{-1} \circ a = a \circ a^{-1} = 0_R$: $a^{-1} \circ a = a^{-1} + a = 0 \Rightarrow a^{-1} = -a$ (Group inverse)

a^{-1}: $a^{-1} \star a = a \star a^{-1} = 1_R$: $a^{-1} \star a = a^{-1} \cdot a = 1 \Rightarrow a^{-1} = \frac{1}{a}$ (ring inverse)

Note that the notation a^{-1} coincides with the natural arithmetic inverse notation!

R_2) $(M_2(\mathbb{R}), +, \underset{\text{prod}}{\text{Matrix}}, O_{2\times2}, I_2)$

~~we have seen in example G3~~

Recall from example G2 that the triple $M_2(\mathbb{R}), +, O_{2\times2}$ forms a group. Let's test for the ring operation now: $A \star B \triangleq AB$

- Matrix product is associative: $(AB)C = A(BC)$

- Is the matrix product distributive over matrix addition? $$\left.\begin{array}{l} A(B+C) = AB + AC \\ (B+C)A = BA + CA \end{array}\right\}$$ Yes, it is! from the left and from the right.

- Is I_2 a neutrol element for $\star$ = matrix product? $$AI_2 = I_2A = A \quad \forall\, A \in M_2(\mathbb{R})$$ Yes! It is a Unit ring

then R_2 **is** a ring!

Remark: If we select M_2, matrix product, I_2 from whithin ring R_2, does it form another group?

No! Because there is no inverse for $\star$ = Matrix product!

In fact, in the ring construction $(R, \circ, \star, 0_R, 1_R)$ $(R, \circ, 0_R)$ forms a group from the ring definition. $(R, \star, 1_R)$ DOES NOT form a group because there is no inverse defined for the ring operation $\star$.

R3) $(\mathbb{Z}, \circ, \star, 0_R, 1_R)$, with $a \circ b \triangleq a+b-1$

$a \star b \triangleq ab+a+b$

What are the neutral elements for $\circ$ and $\star$?

$a \circ 0_R = 0_R \circ a = a$: $\underbrace{a}_{a} \circ \underbrace{0_R}_{b} = a + 0_R - 1 = a$

It is a unit ring

$0_R = \cancel{a} - \cancel{a} + 1 \quad \therefore \quad \boxed{0_R = 1}$

$a \star 1_R = 1_R \star a = a$: $\underbrace{a}_{a} \star \underbrace{1_R}_{b} = a 1_R + \cancel{a} + 1_R = \cancel{a}$

$a 1_R + 1_R = 0 \iff (a+1) 1_R = 0 \Rightarrow \boxed{1_R = 0}$

if $a+1 \neq 0$ then $1_R = \frac{0}{a+1} = 0$

if $a+1 = 0$ then $0 \, 1_R = 0 \Rightarrow 0 = 0$. $a+1=0$ $a=-1$

$-1 \star 1_R = -1 \star 0 = -1 \cdot 0 + (-1) + 0 = -1$ ok!

Are $\circ$ and $\star$ associative?

$\underbrace{(a \circ b)}_{\triangleq d} \circ c = d \circ c = ~~dc~~ \; d + c - 1 = (a+b-1) + c - 1$

$= a+b+c-2$ //

$d = a \circ b = a + b - 1$

$a \circ \underbrace{(b \circ c)}_{\triangleq e} = a \circ e = a + e - 1 = a + (b+c-1) - 1 = a+b+c-2$ //

$e = b \circ c = b + c - 1$

therefore $(a \circ b) \circ c = a \circ (b \circ c)$ ✓ $\circ$ is associat.

$\underbrace{(a \star b)}_{} \star c = d \star c = dc + d + c = (ab+a+b)c + d + c$

$d = a \star b = ab + a + b$

$= abc + ac + bc + (ab+a+b) + c$

$= abc + ab + bc + ac + a + b + c$ //

$a \star \underbrace{(b \star c)}_{} = a \star e = ae + a + e = a(bc+b+c) + a + (bc+b+c)$

$e = b \star c = bc + b + c$

$= abc + ab + ac + a + bc + b + c$

$= abc + ab + ab + ac + a + b + c$ //

thus, $\star$ is associate too!

$\therefore$ R3 is a ring!

<u>Field</u> is a unit commutative ring with an inverse for the ring operation for $F \setminus \{0_F\}$

We may change notation to reflect this fact: $(F, \circ, \star, 0_F, 1_F) \triangleq \mathbb{F}$ (in this course)

<u>Examples</u> inverse exists for all $a \in F \setminus \{0_F\}$.
It can be shown that $0_F \star 1_F = 0_F$

F1) $F = \mathbb{Q}$, $\circ = +$, $\star = \cdot$, $0_F = 0$, $1_F = 1$ is a field

F2) $(\mathbb{R}, +, \cdot, 0, 1)$ is a field

F3) $(\mathbb{C}, +, \cdot, 0, 1)$ is a field

<u>Remark</u>: whithin a field, $(F, \circ, 0_F)$ forms an abelian group and $(F, \star, 1_F)$ also forms an abelian group.