Lecture 6 – Linear Algebra (MA4020)

September 07, 2021.

PART II. VECTOR SPACES.

M. Artin – Chapter 3
S. Lang – Chapter 1
S. Axler – Chapter 1
Hoffman & Kunze – Chapter 2

Recall from lecture 1:

Binary operation. A binary operation $*$ (or $f, \circ, +, -,$ etc.) on a non-empty set G is a map

$$* : G \times G \longrightarrow G \quad \text{such that}$$
$$(a, b) \longmapsto *(a,b) := a * b \in G.$$

$$* : G \times G \longrightarrow \operatorname{im}(*) = *(G \times G)$$

map

$$\operatorname{im}(*) = \{ *(a,b) \text{ where } (a,b) \in G \times G \}$$

If $\operatorname{im}(*) \subseteq G$, then $*$ is a binary operation.

If $G \subsetneq \operatorname{im}(*)$ (in larger universal set), then $*$ is not a binary operation.

Examples.

1. $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$(m, n) \longmapsto f(m,n) := m+n$

$\cancel{\frac{m}{n}, n \neq 0.}$

2. $GL_n(\mathbb{R})$: Set of all $n \times n$ matrices A s.t. $\det(A) \neq 0$.
(over $\mathbb{R}$)

$f : GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$

or $*$

map

$(A, B) \longmapsto f(A,B) := AB$

$\det(AB) = \det(A) \cdot \det(B)$

3. $M_n(\mathbb{R})$: Set of all $n \times n$ matrices over $\mathbb{R}$.

$f : M_n(\mathbb{R}) \times M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$

$(A, B) \longmapsto A + B$

$A - B$

4. $M_{m,n}(\mathbb{R})$: Set of all $m \times n$ matrices over $\mathbb{R}$

$f : M_{m,n}(\mathbb{R}) \times M_{m,n}(\mathbb{R}) \longrightarrow M_{m,n}(\mathbb{R})$

$(A, B) \longmapsto A + B$

5. $\mathbb{R}^2 = \{ (a,b) \mid a,b \in \mathbb{R} \}$

Set of row vectors

$[a, b]$

Set of column vectors

$\begin{bmatrix} a \\ b \end{bmatrix}$

$$f : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$
$$(v, w) \longmapsto f(v,w) := v + w$$

Definition. [Associative Binory operation].

$* : G \times G \longrightarrow G$ is associative

Notation.

if $a * (b * c) = (a * b) * c$ for all $a,b,c \in G$.

$\downarrow$

$f : G \times G \longrightarrow G$ is associative

if $f(a, f(b,c)) = f(f(a,b), c)$

Examples.

associative binary operation

1. ~~M~~ $M_n(\mathbb{R})$ with $+$.

$$(A + B) + C = A + (B + C)$$

2. $GL_n(\mathbb{R})$ with $\cdot$

$$(AB) \cdot C = A \cdot (BC)$$

3. $M_{m,n}(\mathbb{R})$ with $+$

4. $\mathbb{R}^2, +$:

Abelian Binary operation.

(or Commutative)

$* : G \times G \longrightarrow G$ is abelian

if $a * b = b * a$ for all a, b in G.

Examples.

1. $M_2(\mathbb{R}), +$

$\downarrow$

$A + B = B + A$

$M_2(\mathbb{R}), \cdot$

$A \cdot B = B \cdot A$

2. ~~$\mathbb{R}^2$~~ $\mathbb{R}^2$ with $+$

$\mathbb{R}^n, +$

$+ : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$(v, w) \longmapsto v + w$

$v + w = w + v \quad \forall\, v, w \in \mathbb{R}^2$

3. $GL_n(\mathbb{R})$ with $\cdot$

$GL_n(\mathbb{R})$ with $+$

NO

$\cdot : GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$

YES

$(A, B) \longmapsto A \cdot B$

$A + (-A)$

Is it true? $A \cdot B = B \cdot A$ $\times$

$GL_n(\mathbb{R}) = \{ A \mid \det A \neq 0 \}$

Group. A group is a pair $(G, *)$, where $G \neq \phi$, and $*$ is a binary operation on G satisfying the following axioms.

(i) $*$ is associative

(ii) For every $g \in G$, there exist $e \in G$ such that

$$g * e = e * g = g.$$

[Existence of identity element]

(iii) For every $g \in G$, there exist $h \in G$ such that

$$g * h = h * g = e$$

[Existence of inverse element].

Examples.

$$+ : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$$
$$(v, w) \longmapsto v + w$$
$$(v, 0) \longmapsto v$$
$$(0, v) \longmapsto v$$

1. $G = (\mathbb{R}^n, +)$

$e = 0$ vector

identity

$g^{-1} =$

$v + (-v) = 0$

identity

"Identity is always unique"

$$\overset{G}{\overset{\shortparallel}{}}$$

2. $(M_n(\mathbb{R}), +)$ is a group.

$n=1$, $(\mathbb{R}, +)$

$e = [0]$ $\qquad A^{-1} = -A$

$A + (\quad) = A = (\quad) + A$ $\qquad A + (-A) = 0$

3. $(GL_n(\mathbb{R}), +)$

$+$ is not a binary operation $\qquad A + B = [0]$

$e = \times$ $\qquad A^{-1} = \times$

4. $(GL_n(\mathbb{R}), \cdot)$ is a group.

$A \cdot (\quad) = A = (\quad) \cdot A$

$(\mathbb{R}^{\times}, \cdot) = (\mathbb{R} - \{0\}, \cdot)$

$\det A \neq 0$

$e = I_n$ $\qquad A^{-1} =$ exist.

5. $(\mathbb{C} - \{0\}, \cdot) = G$

$\cdot : G \times G \longrightarrow G$

$(z, w) \longmapsto z \cdot w$

$e = 1$

$z \cdot (\quad) = 1 = (\quad) \cdot z$ $\qquad z \cdot \bar{z} = 1$

$z^{-1} =$

Abelian group. A group $(G, *)$ is abelian if $*$ is abelian, i.e. $a * b = b * a$ for all $a, b \in G$.

Examples.

1. $(\mathbb{R}^n, +)$ is a group, $v + w = w + v \quad \forall\, v, w \in \mathbb{R}^n$
   Abelian

2. $(M_n(\mathbb{R}), +)$ Abelian group.

3. $(GL_n(\mathbb{R}), \cdot)$ ~~Abelian group~~ $\underline{\underline{NO}}$
   Group. $A \cdot B \neq B \cdot A$

4. $(M_{m,n}(\mathbb{R}), +)$ Abelian group.
   $M_{m,n}(\mathbb{R}) = \{A : m \times n \text{ matrices over } \mathbb{R}\}$

Let $AX = 0$ be a homogeneous system.

(i) $X = 0$ is always a solution of $AX = 0$, known as trivial solution.

(ii) If $X \neq 0$ (i.e., some $x_i \neq 0$), and $AX = 0$, then X is a non-trivial solution.

Remark.

(a). If $AX = 0$ and $AY = 0 \Rightarrow A(X+Y) = 0$.

In other words, if X and Y are solutions, then so is $X+Y$.

(b) $AX = 0 \Rightarrow A(cX) = 0$, where $c \in \mathbb{R}$.

If X is a solution, then so is cX.

$\neq \phi$

G = set of solutions of system $AX = 0$.

Define

$$+ : G \times G \longrightarrow G$$
$$(X, Y) \longmapsto X+Y$$

$+$ is a binary operation on G.

$$A(X+Y) = 0$$
$$\Downarrow$$
$$A(Y+X) = 0$$

$+$ is abelian ✓

$+$ is associative ✓

identity element 0_G ✓

inverse exist for each X ✓

$+ : G \times G \longrightarrow G$ is a binary operation,

infact $(G, +)$ is an abelian group.

Now,

$$\cdot : G \longrightarrow G \quad \text{or} \quad \left(\begin{array}{rl} \cdot : \mathbb{R} \times G & \longrightarrow G \\ (c, X) & \longmapsto cX \end{array} \right)$$

$$X \longmapsto \cdot(X) := cX \qquad \text{for fixed } c \in \mathbb{R}$$

Terminology.

G is <u>closed under addition.</u>

G is <u>closed under scalar multiplication.</u>

<u>Quick recap.</u>

Let V be a non-empty set.

$(V, +)$ is an "Abelian Group" if

- $+$ is abelian ✓
- $+$ is associative ✓
- Existence of identity element in V ✓
- Existence of inverse element in V ✓

Definition. A non-empty set V is said to be a **real vector space** if there exist two maps

$$+ : V \times V \longrightarrow V \qquad [\text{Addition}]$$
$$(v, w) \longmapsto v + w$$

$$\cdot : \mathbb{R} \times V \longrightarrow V \qquad [\text{Scalar multiplication}]$$
$$(c, v) \longmapsto cv$$

satisfying the following axioms:

(i) $(V, +)$ is an abelian group

(ii) $\cdot$ is associative with multiplication of real numbers:

$$(ab) \cdot v = a \cdot (b \cdot v) \qquad \text{for all } a, b \in \mathbb{R} \text{ and } v \in V$$

(iii) $1 \cdot v = v$, here $1 \in \mathbb{R}$.

(iv) Two distributive laws holds:

$$(a+b) \cdot v = a \cdot v + b \cdot v \qquad \text{for all } a, b \in \mathbb{R}$$
$$a \cdot (v + w) = a \cdot v + a \cdot w \qquad \text{and } v, w \in V.$$

Definition. A non-empty set V is said to be a **real vector space** if there exist maps

$$+ : V \times V \longrightarrow V$$
$$(v, w) \longmapsto v+w \qquad \text{called addition,}$$

$$\cdot : \mathbb{R} \times V \longrightarrow V$$
$$(c, v) \longmapsto c \cdot v \qquad \text{called scalar multiplication}$$

satisfying the following axioms:

(i) (a) $v + w = w + v$ [commutativity of addition]

(i) (b) $v + (w+z) = (v+w)+z$ [associativity of addition

(i) (c) There exists $0_V \in V$ such that

$$v + 0_V = v = 0_V + v$$ [existence of additive identity]

(i) (d) For every $v \in V$ there exists $w \in V$ such that

$v + w = 0_V = w + v$. This w is denoted by $-v$.

[Existence of additive inverse]

(ii) $\cdot$ is associative.

$$(ab) \cdot v = a \cdot (b \cdot v)$$

(iii) $1 \cdot v = v$

8 conditions

(iv) ~~(a)~~. Distributive law holds.

(iv) (a). $(a+b) \cdot v = a \cdot v + b \cdot v$

(b) $a \cdot (v+w) = a \cdot v + a \cdot w$

Examples.

1. Let $V = \mathbb{R}^n$ is a vector space over $\mathbb{R}$.

$$+ : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$(\mathbb{R}^n, +)$ is an abelian group.

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \longmapsto \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}$$

$$v, w \longmapsto v + w$$

$$\cdot : \mathbb{R} \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$$(c, w) \longmapsto c \cdot w$$

$$c, \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \longrightarrow c \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} c a_1 \\ \vdots \\ c a_n \end{bmatrix}$$

$V, +, \cdot$ is a Vector space.

2. Let $V = \mathbb{C}$ set of complex numbers.

$$+ : V \times V \longrightarrow V$$
$$(z_1, z_2) \longmapsto z_1 + z_2$$

$$\cdot : \mathbb{R} \times \mathbb{C} \longrightarrow \mathbb{C}$$
$$(\alpha, z) \longmapsto \alpha z$$

(i) $(\mathbb{C}, +)$ Abelian gr.

(ii) $(\alpha\beta) \cdot z = \alpha(\beta z)$

(iii) $1 \cdot z = z$

(iv) $\leftrightarrows$

3. $V = \mathcal{F}(\mathbb{R}, \mathbb{R})$: set of real valued functions on $\mathbb{R}$.

$$\mathcal{F}(\mathbb{R}, \mathbb{R}) = \{ f : \mathbb{R} \longrightarrow \mathbb{R} \}$$

Define $+$ on V,

$$+ : V \times V \longrightarrow V$$
$$(f, g) \longmapsto \underline{\underline{f+g}} \in V$$

(How to define $\underline{\underline{f+g}}$)

$$f+g : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto (f+g)(x) = f(x) + g(x).$$

$$\cdot : \mathbb{R} \times V \longrightarrow V$$
$$(\alpha, f) \longmapsto \alpha f \in V$$

$$\alpha f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto (\alpha f)(x) = \alpha \cdot f(x)$$

$$(f+g)(x) := f(x) + g(x)$$
$$(\alpha f)(x) := \alpha f(x)$$

4. $V = M_{m,n}(\mathbb{R})$

$(M_{m,n}(\mathbb{R}), +)$ is Abelian group.

$$+ : M_{m,n}(\mathbb{R}) \times M_{m,n}(\mathbb{R}) \longrightarrow M_{m,n}(\mathbb{R})$$

$$(A, B) \longmapsto A + B$$

$$(A+B)_{(ij)} = A_{ij} + B_{ij}$$

$$\cdot : \mathbb{R} \times M_{m,n}(\mathbb{R}) \longrightarrow M_{m,n}(\mathbb{R})$$

$$(\alpha, A) \longmapsto \alpha A$$

$$(\alpha A)_{(ij)} = \alpha A_{ij}$$

5. Let S be any non-empty set.

$V = \mathcal{F}(S, \mathbb{R})$: set of all functions from the set to $\mathbb{R}$.

$$+ : V \times V \longrightarrow V$$

$$(f, g) \longmapsto \underbrace{f+g}_{h}$$

$$\underset{h}{\underset{\shortparallel}{(f+g)}} : S \longrightarrow \mathbb{R}$$

$$s \longmapsto \underset{f(s)+g(s)}{\underset{\shortparallel}{(f+g)(s)}}$$

$$\cdot : \mathbb{R} \times V \longrightarrow V$$

$$(\alpha, f) \longmapsto \alpha f$$

6. $V = \{ p(x) \}$, where $p(x) = a_n x^n + \cdots + a_0$;

$\uparrow$ real polynomials

$a_0, \ldots, a_n$ are fixed real numbers.

$$+ : V \times V \longrightarrow V$$
$$(p, q) \longmapsto p + q$$

$$\cdot : \mathbb{R} \times V \longrightarrow V$$
$$(\alpha, p) \longmapsto \alpha p$$

$f+g$

f is continous

f continuous $\forall$

$-f$ continuous

7. $V = \mathcal{C}([0,1]) = \{ f : [0,1] \longrightarrow \mathbb{R}$ s.t. f is continuous$\}$

$\parallel$

set of continuous real-valued functions on the interval $[0,1]$.

Is this vector space over $\mathbb{R}$?

YES

$$+ : \mathcal{C}([0,1]) \times \mathcal{C}([0,1]) \longrightarrow \mathcal{C}([0,1])$$
$$(f, g) \longmapsto f + g$$

$$\cdot : \mathbb{R} \times \mathcal{C}([0,1]) \longrightarrow \mathcal{C}([0,1])$$
$$(\alpha, f) \longmapsto \alpha f$$

$S = \{1, 2, \dots, n\}$

$V = \mathcal{F}(S, \mathbb{R})$ (Set of all functions from S into $\mathbb{R}$)

$\quad\quad \shortparallel$

$\{ f : S \longrightarrow \mathbb{R} \}$

define $f : S \longrightarrow \mathbb{R}$

$\quad\quad\quad i \longmapsto f(i) \quad$ for $1 \leq i \leq n$

Note that $\mathbb{R}^n$ may be regarded as a function from the set of integers $\{1, \dots, n\}$ into $\mathbb{R}$.

$\eta : \quad f \longrightarrow (f(1), \dots, f(n))$

$\eta : \quad V = \mathcal{F}(S, \mathbb{R}) \longrightarrow \mathbb{R}^n$

$f + g$

αf

Definition. A *field* F is a set together with binary operations

$(\mathbb{R}, +, \cdot)$

$$+ : F \times F \longrightarrow F \quad \text{[Addition]}$$
$$(a, b) \longmapsto a + b$$

$(\mathbb{C}, +, \cdot)$

$$\cdot : F \times F \longrightarrow F$$
$$(a, b) \longmapsto a \cdot b \quad \text{[Multiplication]}$$

satisfying the following axioms:

(identity and inverse w.r.t. $+$) $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

(i) $(F, +)$ is an abelian group

$ab = ba$
$a(bc) = (ab)c$

(ii) • Multiplication is associative and commutative,

and $(F - \{0\}, \cdot)$ is a group $(\mathbb{R} - \{0\}, \cdot)$

(iii) Distributive law: $(a + b) \cdot c = a \cdot c + b \cdot c$,

holds for all $a, b, c \in F$.

(identity and inverse w.r.t. $\cdot$)

$(F, +) \rightsquigarrow$ additive identity is denoted by 0.

$(F - \{0\}, \cdot) \rightsquigarrow$ Multiplicative identity is denoted by 1.

Examples.

1. $\mathbb{R}$ with $+$ and $\cdot$

$(\mathbb{R}, +)$ is an abelian group

$(\mathbb{R} - \{0\}, \cdot)$ is a group

2. $\mathbb{C}$ with $+$ and $\cdot$:

$(\mathbb{C}, +)$ is an abelian group.

$(\mathbb{C} - \{0\}, \cdot)$ is a group

3. $\mathbb{Q}$ with $+$ and $\cdot$

$(\mathbb{Q}, +)$ Abelian group

$(\mathbb{Q} - \{0\}, \cdot)$ Group

4. $\mathbb{Q}[\sqrt{3}] = \{ a + b\sqrt{3} \mid a, b \in \mathbb{Q} \}$

$\frac{p}{q} \cdot \frac{q}{p} = 1$

$\vartheta \cdot (\cdot) = 1$

Fields $\mathbb{N}$, $\mathbb{Z}$,

Discussion. (Example of fields).

$m \cdot n = 1$

$\mathbb{N}$ ✗

$\mathbb{Z}$ ✗

$[\quad]$ square matrix. (need not be)

$\mathbb{Q}$ ✓

$(\mathbb{Q}, +)$, $(\mathbb{Q} - \{0\}, \cdot)$

$(-) \cdot (-) = 1$

$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{ [0], [1], \ldots, [p-1] \}$

(— mod p)

if p is prime

$\mathbb{Z}/p\mathbb{Z}$ is a field.

V : vector space over F.

Definition. A vector space V over a field F is a set if there exist two maps

(a) (addition) $+ : V \times V \longrightarrow V$

$$(v, w) \longmapsto v + w$$

(b) (scalar multiplication) $\cdot : F \times V \longrightarrow V$

$$(c, v) \longmapsto cv$$

satisfying the following axioms:

(i) $(V, +)$ is an abelian group

(ii) Scalar multiplication is associative, with multiplication in F:

$$(ab) \cdot v = a \cdot (b \cdot v)$$

for all $a, b \in F$ and $v \in V$

(iii) The element $1^{\in F}$ acts as identity

$$1 \cdot v = v, \text{ for all } v \in V$$

(iv) Two distributive law hold:

$$(a+b) \cdot v = a \cdot v + b \cdot v$$

$$a \cdot (v+w) = a \cdot v + a \cdot w$$

for all $a, b \in F$ and $v, w \in V$.

Examples.

1. $V = F^n$

$$+ : F^n \times F^n \longrightarrow F^n$$
$$(v, w) \longmapsto v+w$$

$$\cdot : F \times F^n \longrightarrow F^n$$
$$(c, v) \longmapsto cv$$

2. $F = \mathbb{C}$.

$$+ : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$$
$$(z_1, z_2) \longmapsto z_1 + z_2$$

$$\cdot : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$$
$$(\alpha, z) \longmapsto \alpha z$$

3. $V = \mathcal{F}(F, F)$ set of F-valued functions

$$\begin{gathered} \mathcal{F}(F,F) \\ \| \\ f : F \longrightarrow F \end{gathered}$$