

④ Group: A group is a set ( $G$ ) equipped with a binary operation (+) such that the following properties hold true —

- For all  $x, y \in G$ ,  $x + y \in G$  (Closure)
- For all  $x, y, z \in G$ ,  $(x+y)+z = x+(y+z)$  (Associativity)
- There exists an element  $e \in G$  such that  $x+e = e+x = x$  for all  $x \in G$ . (Identity element)
- For all  $x \in G$ , there exists an element  $\tilde{x} \in G$  such that  $x+\tilde{x} = \tilde{x}+x = e$ . This element  $\tilde{x}$  is called the Inverse of  $x$ . (Inverse)  $\blacksquare$

$\hookrightarrow$  Additionally, if  $x+y = y+x$  for all  $x, y \in G$ , then  $G$  is called an abelian group.

$\hookrightarrow$  Claim: For any  $x \in G$ , its inverse is unique.

Proof: Suppose  $x \in G$  has two inverses  $\tilde{x}$  and  $\hat{x}$ .

$$\begin{aligned} \text{Then, } \tilde{x} &= \tilde{x} + e = \hat{x} + (x + \hat{x}) = (\tilde{x} + x) + \hat{x} \\ &= e + \hat{x} = \hat{x} \end{aligned} \quad \blacksquare$$

### ④ Examples:

- Integers with addition.
- Matrices of size  $m \times n$  with addition.
- $m \times n$  non-singular matrices with multiplication.
- permutation group (has a connection with controllability for certain type of systems)
- roots of unity with multiplication.

④ Ring: A ring is a group with some additional structures imposed on it. A ring is a set ( $R$ ) equipped with two binary operations  $(+, \circ)$  such that the following properties hold true —

09/19/17

BD | Q-2

- i)  $R$  is an abelian group under " $+$ " with  $e$  as identity.
- ii) For all  $x, y, z \in R$ ,  $x \circ (y \circ z) = (x \circ y) \circ z$ . (Associativity)
- iii) There exists an element  $1 \in R$  such that  $x \circ 1 = 1 \circ x = x$  for all  $x \in R$ . (Multiplicative identity)
- iv)  $a \circ (b + c) = (a \circ b) + (a \circ c)$  and  $(a + b) \circ c = (a \circ c) + (b \circ c)$  for all  $a, b, c \in R$ . (Distributivity)

↳ Claim: For any  ~~$\in R$~~ , its multiplicative ~~identity~~ is unique.

Proof: EXERCISE!

↳ Claim: For any  $x \in R$ ,  $x \circ e = e = e \circ x$  and  $1 \circ x = x$  where  $1 + 1 = 1 + 1 = e$  and  $oc + xc = xc + oc = e$ .

Proof: EXERCISE!

⑤ Examples:

- Integers with addition and multiplications.
- Polynomials with addition and multiplications.
- Power sets.  
(has application in controllability results)

⑥ Field: A field is a ring with additional structure imposed on it. A set ( $F$ ) equipped with two binary operations  $(+, \circ)$  will be called a field if the following holds true —

i)  $F$  is a ring with "+" and " $\circ$ ", with  $e$  and  $1$ .

09/19/17

BD/2-3

ii) For any  $x, y \in F$ , the multiplication ( $\circ$ )

is commutative, i.e.  $x \circ y = y \circ x$ . (commutativity)

iii) For every  $x \in F$ ,  $x \neq e$ , there exists another element  $y \in F$  s.t.  $x \circ y = y \circ x = 1$ . This element is called the multiplicative inverse of  $x$ .

(Inverse) We typically use  $x^{-1}$  to denote multiplicative inverse of  $x$ .

↳ This is the structure that has more relevance in the initial part of this course.

↳ We also need a field in order to define a vector space.

### ● Examples:

→ Rational numbers/Real numbers/Complex numbers.

→  $\mathbb{Z}_p$  i.e. the set of integers modulo "p" when  $p$  is prime.

→ Rational fractions, i.e. ratio of polynomials.

→ ~~Smooth/continuously differentiable functions, analytic functions, positive numbers, ratios~~

↳ Claim: If for  $x, y \in F$ ,  $x \circ y = 0$  then either of  $x$  or  $y$ , or both must be zero.

Proof: Suppose  $x \neq 0$ .

Then, its multiplicative inverse  $x^{-1}$  exists.

$$0 = x^{-1} \cdot 0 = x^{-1} \cdot (x \circ y) = (x^{-1} \circ x)y = 1 \circ y = y.$$

## Vector Space:

A vector space ( $V$ ) over a field  $F$  is a set equipped with two operations " $+$ " (vector addition) and " $\cdot$ " (scalar multiplication) such that the following axioms hold true for any  $x, y, z \in V$  and  $\alpha, \beta \in F$  —

- i)  $x+y \in V$  { Closure (As we will see later this plays a critical role in showing whether a space is subspace.)
- ii)  $\alpha x \in V$
- iii).  $\alpha + (\gamma + z) = (\alpha + \gamma) + z$  (Associativity)
- iv)  $\alpha + \gamma = \gamma + \alpha$  (Commutativity)
- v) There exists  $0 \in V$  (called the zero vector)  
s.t.  $\alpha + 0 = 0 + \alpha = \alpha$
- vi) For every  $\alpha$ , there exists a unique element  $(-\alpha)$  such that  $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$ .  
 $(-\alpha)$  is called the additive inverse of  $\alpha$ .
- vii)  $\alpha(\beta\alpha) = (\alpha\beta)\alpha$
- viii)  $1\alpha = \alpha$  where  $1$  is the multiplicative identity of  $F$ .
- ix)  $(\alpha + \beta)\alpha = \alpha\alpha + \beta\alpha$
- x)  $\alpha(\alpha + \gamma) = \alpha\alpha + \alpha\gamma$

From axioms (iii)-(xi) we can conclude that a vector space is an abelian group.

Vector subtraction and division by non-zero scalar can be defined.

## Examples:

- ↳  $n$ -tuple of real numbers, i.e. an ordered list of  $n$ -real numbers. We denote this space as  $\mathbb{R}^n$ .
- ↳ Similarly,  $\mathbb{C}^n$  over  $\mathbb{R}$  or  $\mathbb{C}$ ,  $\mathbb{Q}^n$  over  $\mathbb{Q}$ .
- ↳  $\mathbb{Z}_p^n$  over  $\mathbb{Z}_p$  where  $p$  is a prime number.
- ↳ Real matrices of size  $m \times n$ , i.e.  $\mathbb{R}^{m \times n}$ , over  $\mathbb{R}$ .
- ↳ Continuous functions over  $\mathbb{R}$ .
- ↳ Solutions of  $Ax=0$  where  $A \in \mathbb{R}^{m \times n}$  is given.

## Linear Independence and Basis:

- ↳ For a given vector space  $V$ , a set of vectors  $v_1, v_2, \dots, v_m \in V$  are linearly independent if  $\sum_{i=1}^m \alpha_i v_i = 0$  ( $\alpha_i \in F$ , the underlying field) implies that  $\alpha_i = 0$  for every  $i \in \{1, \dots, m\}$ .

- ↳ Given a set of vectors  $v_1, \dots, v_m \in V$ , its span is defined as the set of linear combinations, i.e.

$$\text{span}(\{v_1, \dots, v_m\}) = \left\{ \sum_{i=1}^m \alpha_i v_i \mid \alpha_i \in F, i=1, \dots, m \right\}$$

- ↳ A set of vectors  $S = \{v_1, \dots, v_m\}$  will be called a basis for the vector space  $V$  if  $v_1, \dots, v_m$  are linearly independent and  $\text{span}(S) = V$ .

- ↳ Claim: Any vector  $v \in V$  can be uniquely represented as a linear combination of its basis vectors.

↳ An example:

Consider the set of continuous functions defined over  $[0, 2\pi]$ .

$$V = \{ f : [0, 2\pi] \rightarrow \mathbb{R} \mid f : \text{continuous} \}$$

Clearly,  $\cos x, \sin x \in V$  for  $x \in [0, 2\pi]$ .

\* Are they linearly independent?

$$\alpha \cos x + \beta \sin x = 0$$

$$\Rightarrow \sqrt{\alpha^2 + \beta^2} \cos(x - \phi) = 0 \quad \text{where } \phi = \arctan(\beta/\alpha)$$

$$\Rightarrow \sqrt{\alpha^2 + \beta^2} = 0$$

$$\Rightarrow \alpha = \beta = 0$$

↳ Hence,  $\cos x$  and  $\sin x$  are linearly independent.

↳ A vector space  $V$  is finite dimensional if its basis set  $S$  has finite number of elements. Then, the cardinality of  $S$  will be called the dimension of  $V$ .

↳ Given a vector space  $V$  over a field  $F$ , we can show that  $V$  is isomorphic to  $F^n$  where  $n$  is the dimension of  $V$ . (Hint: Think about the elements of  $V$  as linear combinations of its basis vectors) [Isomorphic means that there is an one-to-one and onto mapping between them.]

↳ Subspace: A subset  $W \subseteq V$  will be called a subspace of  $V$  (a vector space over  $F$ ) if  $W$  itself is a vector space over  $F$ .

Let  $V = \{M \in \mathbb{R}^{n \times n}\}$

Clearly  $V$  is a vector space over  $\mathbb{R}$ .

Define,  $W = \{A \in V \mid A^T = -A\}$  ← the set of  $n \times n$  skew-symmetric matrices.

Then,  $W$  is a subspace of  $V$ .

We call this space " $so(n)$ ". It plays an important role in rigid body dynamics.

### Inner products and Norms:

Let  $V$  be a vector space over  $\mathbb{F}$ . An inner product is a map  $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{F}$ ,  $\langle v_1, v_2 \rangle \mapsto u_1$ , such that —

- $\langle \alpha v, w \rangle = \overline{\langle v, w \rangle}$   $(v, w \in V; \alpha, \beta \in \mathbb{F})$

- $\langle \alpha v + \beta w, u \rangle = \alpha \langle v, u \rangle + \beta \langle w, u \rangle$

- $\langle v, v \rangle \geq 0$  and  $\langle v, v \rangle = 0$  if and only if  $v=0$ .

The last property is called positive definiteness.

Can be perceived as a generalization of dot products.

Let  $V = \{f : [0, 2\pi] \rightarrow \mathbb{R} \mid f: \text{continuous}\}$

For  $h, g \in V$  define —

$$\langle h, g \rangle = \int_0^{2\pi} h(x)g(x)dx$$

$$\rightarrow \text{Clearly, } \langle h, g \rangle = \langle g, h \rangle$$

$$\rightarrow \langle \alpha h_1 + \beta h_2, g \rangle = \alpha \langle h_1, g \rangle + \beta \langle h_2, g \rangle$$

$$\rightarrow \langle h, h \rangle = \int_0^{2\pi} h^2(x)dx \geq 0$$

$$\text{and, } \langle h, h \rangle = \int_0^{2\pi} h^2(x)dx = 0 \Rightarrow h(x) \equiv 0, \text{i.e. } h = 0$$

i.e. the space of continuous functions over  $[0, 2\pi]$

Let,  $V$  be a vector space equipped with  $\langle \cdot, \cdot \rangle: V \times V \rightarrow F$ . Then, a pair of vectors  $v, w \in V$  are orthogonal (with respect to this inner product) if  $\langle v, w \rangle = 0$ .

Claim:  $v, w$  are orthogonal  $\Rightarrow$  they are linearly independent. The converse need not be true.

Let,  $V$  be a vector space over  $F$ . A norm on  $V$  is a mapping  $\|\cdot\|: V \rightarrow \mathbb{R}_+$  such that —

- i)  $\|\alpha x\| \geq 0$  for any  $\alpha \in F$  and  $\|\alpha x\| = 0$  if and only if  $\alpha x = 0$ .
- ii)  $\|\alpha x\| = |\alpha| \|x\|$  for any  $\alpha \in F$  and  $x \in V$ .
- iii)  $\|x + y\| \leq \|x\| + \|y\|$

Given a vector space  $V$  with an inner product  $\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{R}$ , we can define a norm —

$$\|x\| = \sqrt{\langle x, x \rangle} \quad (\text{induced from inner product})$$

Cauchy - Schwarz Inequality:

$$|\langle x, y \rangle| \leq \|x\| \cdot \|y\| \quad \forall x, y \in V$$

$\rightarrow$  It can be interpreted as a generalization of

$$x^T y = \|x\| \|y\| \cos \theta$$

Suppose,  $v_1, v_2 \in V$  are linearly independent.

$$\text{Define } z = v_2 - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1$$

$$\begin{aligned}
 \text{Then, } \langle v_1, v_2 \rangle &= \left\langle v_1, v_2 - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 \right\rangle \\
 &= \left\langle v_2 - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1, v_1 \right\rangle \\
 &= \overline{\langle v_2, v_1 \rangle} - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} \langle v_1, v_1 \rangle \\
 &= 0
 \end{aligned}$$

Also,

$$\begin{aligned}
 \alpha v_1 + \beta v_2 &= \alpha v_1 + \beta \left[ z + \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 \right] \\
 &= \left( \alpha + \frac{\beta \langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} \right) v_1 + \beta z
 \end{aligned}$$

Therefore,  $\text{span}(\{v_1, v_2\}) = \text{span}(\{v_1, z\})$ . Thus we can get a set of orthogonal vectors from a set of linearly independent vectors such that they have same span, i.e. they span the same subspace.

↪  $\{(1), (1)\} \mapsto \{(0), (1)\}$  ← An example.

### Sequence and Convergence:

↪ A sequence maps the set of natural numbers  $\mathbb{N}$  to some suitable space  $X$ . (e.g.:  $a_n = \frac{n+1}{n}$ )

↪ Suppose  $X$  is a vector space equipped with a norm. Then a sequence  $(a_n, n=1, 2, 3, \dots)$  converges to  $a_0 \in X$  if for any  $\epsilon > 0$ , there exist  $N(\epsilon)$  such that  $\|a_n - a_0\| < \epsilon$  when  $n \geq N(\epsilon)$ .

↳ A sequence  $(a_m, m \in \mathbb{N})$ , if  $a_m \in X$  is called a Cauchy sequence if for any  $\epsilon > 0$ , there exists  $N(\epsilon)$  such that  $\|a_m - a_n\| < \epsilon$  whenever  $m, n \geq N$ .

→ Convergence implies Cauchy.

→ The converse is not true.

→ Counter example:

$X = \mathbb{Q}$  — the set of rational numbers.

$a_m = \frac{F_{m+1}}{F_m}$  —  $F_m$  is the  $m$ -th. number in the Fibonacci seq.

As  $F_m \in \mathbb{N}$ ,  $a_m \in \mathbb{Q}$  for any  $m \in \mathbb{N}$ .

But  $a_m \rightarrow a_0 = \frac{1+\sqrt{5}}{2} \notin \mathbb{Q}$

↳ A normed vector space  $X$  is complete if every Cauchy sequence in  $X$  converges to an element in  $X$ .

↳ A vector space  $V$  with an inner-product  $\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{R}$  will be called an Hilbert Space if this space is complete with respect to the norm induced by the inner-product.

→ Example:  $\mathbb{R}^m$

↳ A vector space  $X$  with a norm will be called a Banach Space if this space is complete with respect to this norm.