

① Group: A group is a set (G) equipped with a binary operation ($+$) such that the following properties hold true —

i) For all $x, y \in G$, $x + y \in G$ (Closure)

ii) For all $x, y, z \in G$, $(x + y) + z = x + (y + z)$ (Associativity)

iii) There exists an element $e \in G$ such that $x + e = e + x = x$ for all $x \in G$. (Identity element)

iv) 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) \square

\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} .

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

② Examples:

\rightarrow Integers with addition.

\rightarrow Matrices of size $m \times n$ with addition.

\rightarrow $n \times n$ non-singular matrices with multiplication.

\rightarrow permutation group (has a connection with controllability for certain type of systems)

\rightarrow roots of unity with multiplication.

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

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

↳ Claim: For any ~~R~~ R , its multiplicative ~~identity~~ ^{identity} is unique.

Proof: EXERCISE!

↳ Claim: For any $x \in R$, $x \cdot e = e = e \cdot x$ and $\hat{1} \cdot x = \tilde{x}$ where $\hat{1} + \hat{1} = \hat{1} + \hat{1} = e$ and $x + \tilde{x} = \tilde{x} + x = e$.

Proof: EXERCISE!

Examples:

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

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

i) F is a ring with "+" and "•", with e and 1 ,

09/19/17
BD | (2-3)

ii) For any $x, y \in F$, the multiplication (•) is commutative, i.e. $x \cdot y = y \cdot x$. (Commutativity)

iii) For every $x \in F, x \neq e$, there exists another element $y \in F$ s.t. $x \cdot y = y \cdot x = 1$. 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/infinitely differentiable functions with positive range.~~

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

Proof: Suppose $x \neq 0$.

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

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

□

Vector Space:

09/19/17
BDO (2-4)

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

i) $x + y \in V$
ii) $\alpha x \in V$ } Closure (As we will see later this plays a critical role in showing whether a space is subspace)

iii) $\alpha + (y + z) = (\alpha + y) + z$ (Associativity)

iv) $\alpha + y = y + \alpha$ (Commutativity)

v) There exists $0 \in V$ (called the zero vector)

$$\text{s.t. } x + 0 = 0 + x = x$$

vi) For every x , there exists a unique element $(-x)$ such that $x + (-x) = (-x) + x = 0$.

$(-x)$ is called the additive inverse of x .

vii) $\alpha(\beta x) = (\alpha\beta)x$

viii) $1x = x$ where 1 is the multiplicative identity of F .

ix) $(\alpha + \beta)x = \alpha x + \beta x$

x) $\alpha(x + y) = \alpha x + \alpha y$

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

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

Examples:

09/19/17
100 | 2-5

- ↳ 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:

03/19/17
BD/2-6

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?

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

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

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

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

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

09/19/17
BD | (2-7)

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 F . An inner product is a map $\langle \cdot, \cdot \rangle : V \times V \rightarrow F$, $(v_1, v_2) \mapsto \langle v_1, v_2 \rangle$ such that —

i) $\langle v, w \rangle = \overline{\langle w, v \rangle}$ $[u, v, w \in V ; \alpha, \beta \in F]$

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

iii) $\langle v, v \rangle \geq 0$ 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 —

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

→ clearly, $\langle h, g \rangle = \langle g, h \rangle$

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

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

and, $\langle h, h \rangle = \int_0^{2\pi} h^2(x) dx = 0 \Rightarrow h(x) \equiv 0$, 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) $\|x\| \geq 0$ for any $x \in V$ and $\|x\| = 0$ if and only if $x = 0$.

ii) $\|\alpha x\| = |\alpha| \|x\|$ for any $x \in V$ and $\alpha \in F$.

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 —

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

↳ 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

$$\text{of } |x^T y| = \|x\| \|y\| \cos \theta$$

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

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

$$\text{Then, } \langle v_1, v_2 \rangle = \left\langle v_1, v_2 - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 \right\rangle$$

$$= \left\langle v_2 - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1, v_1 \right\rangle$$

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

$$= 0$$

Also,

$$\alpha v_1 + \beta v_2 = \alpha v_1 + \beta \left[z + \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 \right]$$

$$= \left(\alpha + \frac{\beta \langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} \right) v_1 + \beta z$$

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.

$$\hookrightarrow \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \longmapsto \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \leftarrow \text{An example.}$$

Sequence and Convergence:

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

\hookrightarrow 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 $(a_n, n \in \mathbb{N})$, is $a_n \in X$ 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.

$a_n = \frac{F_{n+1}}{F_n}$ — F_n is the n -th number in the Fibonacci seq.

As $F_n \in \mathbb{N}$, $a_n \in \mathbb{Q}$ for any $n \in \mathbb{N}$.

But $a_n \rightarrow x_0 = \frac{1+\sqrt{5}}{2} \notin \mathbb{Q}$

↳ 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 a Hilbert Space if this space is complete with respect to the norm induced by the inner-product.

→ Example: \mathbb{R}^n

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