Vector Spaces

First, Group & then Field.

Def: A set G of elements with an operation $+ : G \times G \to G$ is called a group if the following properties hold:

(P1) Associativity: $\forall a, b, c \in G : (a+b)+c = a+(b+c)$

(P2) Identity element: $\exists\, e \in G, \forall g \in G$
$$e+g = g+e = g$$

(P3) Inverse element: $\forall a \in G \;\exists\, b \in G :$
$$a+b = b+a = e$$

The group is called a commutative group (Abelian group) if we have an additional property:

(P4) $\forall a, b \in G : \; a+b = b+a$

Examples:

- $(\mathbb{R}^n, +)$ is a group
- $(\mathbb{R}^+, \cdot)$ is a group
- $(\mathbb{R}^-, \cdot)$ is not a group
- $S_n := \{ \pi : \{1,2,..n\} \to \{1,2,..n\} \mid \pi \text{ is bijective} \}$

  $\circ : S_n \times S_n \to S_n$,

  $\pi_1 \circ \pi_2 (i) = \pi_1(\pi_2(i))$

  $(S_n, \circ)$ is a group

Def: A set F with two operations $+, \cdot : F \times F \to F$ is called a field if the following properties hold:

(P1) $(F, +)$ is a commutative group with identity element 0.

(P2) $(F \setminus \{0\}, \cdot)$ is a commutative group with identity element of 1.

(P3) Distributivity: $\forall a, b, c \in F$:

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

Examples:
- $(\mathbb{R}, +, \cdot)$
- $(\mathbb{C}, +, \cdot)$
- $n \in \mathbb{Z}$, consider $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

$$a +_n b := (a+b) \bmod n$$

$$a \cdot_n b := (a \cdot b) \bmod n$$

Then $(\mathbb{Z}_n, +_n, \cdot_n)$ is a field if & only if (iff) $\boxed{n \text{ is a prime}}$.

Def: Let F be a field with identity elements 0 & 1. A vector space defined over the field F is a set V with a mapping $+ : V \times V \to V$ ("vector addition")

$\cdot : F \times V \to V$ ("scalar multiplication")

such that:

(P1) $(V, +)$ is a commutative group

(P2) Multiplicative identity: $\forall v \in V : 1 \cdot v = v$

(P3) Distributive property: $\forall a, b \in F,\ u, v \in V$

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

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

Remark: Elements of V are called vectors, elements of field F are scalars

Examples: • $\mathbb{R}^n$ with the standard operation $(+, \cdot)$

• Function spaces:

$\mathcal{F}(\mathcal{X}, \mathbb{R}) := \{f : \mathcal{X} \to \mathbb{R}\}$ the space of all real-valued functions on a set $\mathcal{X}$.

Define: $\boxed{+:}\ \mathcal{F}(\mathcal{X}, \mathbb{R}) \times \mathcal{F}(\mathcal{X}, \mathbb{R}) \to \mathcal{F}(\mathcal{X}, \mathbb{R})$

$$(f+g)(x) \boxed{:=} f(x) + g(x)$$

↳ definition

$\boxed{\cdot}\ \mathbb{R} \times \mathcal{F}(\mathcal{X}, \mathbb{R}) \to \mathcal{F}(\mathcal{X}, \mathbb{R})$,

$$(\lambda \cdot f)(x) := \lambda f(x)$$

then $(\mathcal{F}(\mathcal{X}, \mathbb{R}), +, \cdot)$ is a real-vector space.

• $\mathbb{C}(\mathcal{X}) := \{f : \mathcal{X} \to \mathbb{R} \mid f \text{ is continuous}\}$

• $\mathbb{C}^r([a,b]) := \{f : [a,b] \to \mathbb{R} \mid f \text{ is } r \text{ times continuosly differentiable}\}$

Def: Let V be a vector space, $U \subset V$ non-empty set. We call U a <u>subspace</u> of V if it is <u>closed</u> under linear combinations.

↳ still in th same set.

$$\forall \lambda, \mu \in F, \ \forall u, v \in U: \lambda u + \mu v \in U$$

Examples:

- $C(x)$ is a subspace $F(x, \mathbb{R})$
- The set S of symmetric matrices of size $n \times n$ is a subspace of $\mathbb{R}^{n \times n}$
- Consider set $\{u, v\}$ → not a subspace. $\lambda u + \mu v \notin \{u, v\}$

  $\lambda, \mu \in \mathbb{R}$

Def: V is a vector space over F, $u_1, u_2 \dots u_n \in V$, $\lambda_1, \lambda_2 \dots \lambda_n \in F$ then $\sum_{i=1}^{n} \lambda_i u_i$ is called a linear combination.

The set of all linear combinations of $(u_1, \dots u_n)$ is called the span (linear hull) of $(u_1 \dots u_n)$. Notation:

$$\text{span}(u_1, u_2 \dots u_n) := \left\{ \sum_{i=1}^{n} \lambda_i u_i \;\middle|\; \lambda_i \in F \right\}$$

The set $U := \{u_1, u_2 \dots u_n\}$ is the generator of $\text{span}(U)$.

Def: A set of vectors $v_1 \dots v_n$ is called linearly independent if the following holds.

$$\sum_{i=1}^{n} \lambda_i v_i = 0 \Rightarrow \lambda_1 = \lambda_2 = \dots \lambda_n = 0$$

Examples: • Vectors $\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \in \mathbb{R}^3$ are linearly independent

• Functions $\sin(x)$ and $\cos(x)$ are lin. ind.

• Any set of $\underline{d+1}$ vectors in $\mathbb{R}^d$ is linearly dependent.

Basis and Dimension

Def: A subset B of a vector space V is called a (Hamel) basis if

↳ finite linear combinations even for infinite dimensional spaces.

(P1) $\text{span}(B) = V$

(P2) B is linearly independent

Examples: • The canonical basis of $\mathbb{R}^3$:

$\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}$

Basis is not unique

• Another basis of $\mathbb{R}^3$

$\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}$ or $\begin{pmatrix}0.5\\0.8\\0.4\end{pmatrix}, \begin{pmatrix}1.8\\0.3\\0.3\end{pmatrix}, \begin{pmatrix}-2.2\\-1.3\\3.5\end{pmatrix}$

Proposition: If $U = \{u_1, \dots u_n\}$ spans a vector space V, then the set U can be reduced to a basis of V.

Informal Proof:

- If U is already linearly independent, done
- If U is dependent: $\exists\, a \in U$ that is a linear combination of the other vectors in U.

  We will remove it.

  Keep removing vectors until remaining vectors are linearly independent.

Formal Proof:

- Why does this procedure terminate?
- Why resulting set is a non-empty set.
- . . . .

Def: A vector space is called finite-dimensional if it has at least one finite basis.

Proposition: Let $U = \{u_1, \dots u_n\} \subset V$ be a set of linearly independent vectors, and let V be a finite-dimensional vector space, then U can be extended to a basis of V.

Proof (sketch): Let $w_1, w_2 \dots w_m$ be a basis of V. Consider the set $\{u_1, u_2 \dots u_n, w_1, w_2 \dots w_m\}$

Remove vectors "from the end" until the remaining vectors are linearly independent.

- remaining set span V
- remaining set is linearly independent by construction.
- remaining set contains U. ∎

Extend every independent set to a basis

For infinte-dimensional spaces need Zorn's Lemma to prove proposition.

Corollary: Let V be a finite-dimensional vector space, then any two bases of V have the same length

Def: The length of a basis of a finite dimensional vector space is called the dimension of V.

We have seen what a basis is and what a subspace is. The notion which connects the two is sum and direct sum.

Def: Assume that U_1, U_2 are subspaces of V. The sum of the two spaces is defined as,

for non-overlapping subspaces

$$U_1 + U_2 := \{ u_1 + u_2 \mid u_1 \in U_1 ,\ u_2 \in U_2 \}$$

helps define notion of space & its complement

The sum is called a direct sum, if each element in the sum can be written in exactly one way. Notation: $U_1 \oplus U_2$

Proposition: Suppose V is a finite-dimensional vector space, and $U \subset V$ is a subspace. Then there exists a subspace $W \subset V$, such that

$$U \oplus W = V.$$

Proof (sketch): Let the set $\{u_1, u_2 \dots u_n\}$ be a basis of U. Extend it to a basis of V, say the resulting set is

$$\{\underbrace{u_1, \dots u_n}_{\to U}, \underbrace{v_1, v_2 \dots v_m}_{\to W}\}.$$

Define

$$W = \text{span}\{v_1, v_2 \dots v_m\}$$

$\blacksquare$