

Fields

Definition

A *field* \mathbb{F} is a number system where addition and multiplication satisfy:

< ⊡ >

∢ 臣 ♪

June 13, 2018

2

2 / 1

•
$$a+b=b+a$$

•
$$(a+b) + c = a + (b+c)$$

•
$$\exists 0 \in \mathbb{F}$$
 such that $\forall a \in \mathbb{F}(0 + a = a)$

- $\forall a \in \mathbb{F}(\exists a \in \mathbb{F} \text{ such that } a + (-a) = 0)$
- ab = ba

•
$$(ab)c = a(bc)$$

- $\exists 1 \in \mathbb{F}$ such that $orall a \in \mathbb{F}(1a = a)$
- $\forall a \in \mathbb{F} \setminus \{0\} (\exists a^{-1} \in \mathbb{F} \text{ such that } aa^{-1} = 1)$
- a(b+c) = ab + ac

•
$$0 \neq 1$$

Fields

Examples

- \mathbb{Q} (the rationals)
- \mathbb{R} (the reals ... our favorite field!!!)
- \mathbb{C} (the complex numbers)
- \mathbb{Z}_p (integers mod p, where p is prime)

Close... but no cigar

- $\mathbb Z$ (the integers) \exists nonzero integers w/o multiplicative inverses in $\mathbb Z$
- \mathbb{H} (the quaternions) multiplication fails to be commutative
- \mathbb{Z}_n (integers mod *n*, where *n* is composite)

Vector Spaces

Definition

A vector space V over field \mathbb{F} is a set of "vectors" that can be added to each other, and scaled by elements of \mathbb{F} so that:

• $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$

•
$$(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$$

- $\exists \mathbf{0} \in V$ such that $\forall \mathbf{u} \in V(\mathbf{u} + \mathbf{0} = \mathbf{u})$
- $\forall \mathbf{u} \in V(\exists \mathbf{u} \in V \text{ such that } \mathbf{u} + (-\mathbf{u}) = \mathbf{0})$
- $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$
- $(a+b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$
- $(ab)\mathbf{u} = a(b\mathbf{u})$

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

5 9 Q (P

June 13, 2018 3 / 1

▲□▶ ▲圖▶ ▲厘▶ ▲厘▶ -

Quintessential finite dimensional example

 \mathbb{R}^n is a vector space over \mathbb{R} with addition and scaling defined componentwise

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$a(x_1, x_2, \ldots, x_n) = (ax_1, ax_2, \ldots, ax_n)$$

An infinite dimensional example

 $C^n((0,1);\mathbb{R})$, the space of *n* times continuously differentiable real-valued functions on the interval (0,1), is a vector space over \mathbb{R} with addition of functions (in this context a.k.a. "vectors") and scaling performed pointwise.

Vector Spaces A relevant example $T_{(1,0,0)}S^2 = \{((1,0,0), (0, y, z)) : y, z \in \mathbb{R}\}$ is a vector space over \mathbb{R} with addition and scaling defined by $((1,0,0), (0, y_1, z_1)) + ((1,0,0), (0, y_2, z_2)) = ((1,0,0), (0, y_1 + y_2, z_1 + z_2))$ a((1,0,0), (0, y, z)) = ((1,0,0), (0, ay, az))

∢ ≣ ≯

June 13, 2018

・日・ ・日・

æ

590

5 / 1



Definition

The span of $S \subset V$ is the set of all linear combinations of vectors in S.

$$span(S) = \{a_1u_1 + \cdots + a_ku_k : a_1, \ldots, a_k \in \mathbb{F}, u_1, \ldots, u_k \in S\}$$



Definition

The span of $S \subset V$ is the set of all linear combinations of vectors in S.

$$span(S) = \{a_1u_1 + \cdots + a_ku_k : a_1, \ldots, a_k \in \mathbb{F}, u_1, \ldots, u_k \in S\}$$

Definition

A set of vectors S in V is *linearly independent* if no vector in S is contained in the span of the other vectors in S.

Definition

A basis for V is a linearly independent set of vectors that spans V.

Example

 $\{\boldsymbol{\hat{i}}, \boldsymbol{\hat{j}}, \boldsymbol{\hat{k}}\}$ is a basis for $\mathbb{R}^3.$

June 13, 2018 10 / 1

Definition

A basis for V is a linearly independent set of vectors that spans V.

Example

Recall $T_{(1,0,0)}S^2 = \{((1,0,0), (0, y, z)) : y, z \in \mathbb{R}\}$ is a vector space over \mathbb{R} with addition and scaling defined by

 $((1,0,0),(0,y_1,z_1)) + ((1,0,0),(0,y_2,z_2)) = ((1,0,0),(0,y_1+y_2,z_1+z_2))$ a((1,0,0),(0,y,z)) = ((1,0,0),(0,ay,az)).

 $\{((1,0,0),(0,1,0)), ((1,0,0),(0,0,1))\}$ is a basis for $T_{(1,0,0)}S^2$.

Vector Spaces

Definition

A basis for V is a linearly independent set of vectors that spans V.

Theorem

Any two bases for a given vector space V have the same cardinality.

This justifies the following definition.

Definition

The *dimension* of a vector space V is the number of vectors in any basis for V.

Examples

The dimension of \mathbb{R}^n is *n*. The dimension of $T_{(1,0,0)}S^2$ is 2.

June 13, 2018 12 / 1

▲□ → ▲ 三 → ▲ 三 →

590

11 / 1

3

June 13, 2018

Linear Transformations

Definition

Suppose V and W are vector spaces over a common field \mathbb{F} . Then $T: V \to W$ is *linear* if $\forall a, b \in \mathbb{F}, \forall \mathbf{u}, \mathbf{v} \in V$

$$T(a\mathbf{u} + b\mathbf{v}) = aT(\mathbf{u}) + bT(\mathbf{v})$$

Example

$$rac{d}{dx}: \mathit{C^n}((0,1);\mathbb{R}) o \mathit{C^{n-1}}((0,1);\mathbb{R})$$
 is linear (for $n=1,2,\ldots)$

Example

Given an $m \times n$ matrix M (with real entries), the map $L_M : \mathbb{R}^n \to \mathbb{R}^m$ defined by

$$L_M(\mathbf{u}) = M\mathbf{u}$$

Linear Transformations

Definition

Suppose V and W are vector spaces over a common field \mathbb{F} . Then $T: V \to W$ is *linear* if $\forall a, b \in \mathbb{F}$, $\forall \mathbf{u}, \mathbf{v} \in V$

$$T(a\mathbf{u} + b\mathbf{v}) = aT(\mathbf{u}) + bT(\mathbf{v})$$

Example

Any rotation about any axis through the origin of space is a linear transformation from \mathbb{R}^3 to \mathbb{R}^3 . Consider for example rotation by $\frac{\pi}{4}$ radians about the *z*-axis counterclockwise (as viewed from above). (Incidentally, this transformation is equal to L_R where $R = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0\\ 0 & 0 & 1 \end{bmatrix}$.)

June 13, 2018 14 / 1



Linear Transformations

Definition

Suppose V and W are vector spaces over a common field \mathbb{F} . Then $T: V \to W$ is *linear* if $\forall a, b \in \mathbb{F}$, $\forall \mathbf{u}, \mathbf{v} \in V$

$$T(a\mathbf{u} + b\mathbf{v}) = aT(\mathbf{u}) + bT(\mathbf{v})$$

Surprise

 $f: \mathbb{R}^1
ightarrow \mathbb{R}^1$ given by f(x) = 3x + 5 is *not* linear

Inner Products

Definition

An *inner product* on vector space V over \mathbb{R} is a map $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ such that:

- $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$
- $\langle a\mathbf{u} + b\mathbf{v}, \mathbf{w} \rangle = a \langle \mathbf{u}, \mathbf{w} \rangle + b \langle \mathbf{v}, \mathbf{w} \rangle$
- $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$ (with $\langle \mathbf{u}, \mathbf{u} \rangle = 0$ iff $\mathbf{u} = \mathbf{0}$)

Prototypical Example

Ordinary dot product on \mathbb{R}^n

For
$$\mathbf{u} = (u_1, \ldots, u_n)$$
, $\mathbf{v} = (v_1, \ldots, v_n)$, the dot product $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^n u_i$

is an inner product.

Note that, if **u** and **v** are written as $n \times 1$ matrices (a.k.a. column vectors), then $\mathbf{u} \cdot \mathbf{v}$ may be written as $\mathbf{u}^{\mathsf{T}} \mathbf{v}$ or $\mathbf{u}^{\mathsf{T}} I \mathbf{v}$.

June 13, 2018 17 / 1

Vi

п

3

June 13, 2018

SQA

18 / 1

Inner Products

A Useful Observation

If M is a positive definite matrix (i.e. symmetric with all positive eigenvalues), then

$$\langle \mathbf{u},\mathbf{v}
angle = \mathbf{u}^{\intercal}M\mathbf{v}$$

is an inner product.

For example
$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}^{\mathsf{T}} \begin{bmatrix} 3 & -2 \\ -2 & 5 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$
 is an inner product on \mathbb{R}^2 .

Another example

 $\langle f,g\rangle = \int_0^1 f(x)g(x)dx$ is an inner product on $C^0([0,1];\mathbb{R})$.

Inner Products

Euclidean norm

The ordinary Euclidean length (a.k.a norm) of vector $\mathbf{u} \in \mathbb{R}^n$ may computed using the ordinary dot product:

$$||\mathbf{u}|| = \sqrt{\mathbf{u} \cdot \mathbf{u}}$$

A generalization

Any inner product on a vector space V may be used to define a notion of length for the vectors in V:

$$||\mathbf{u}|| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$$

Arclength

A key ingredient in the computation of arclength is the computation of length of velocity vectors:

$$L = \int_{t_0}^{t_1} ||\mathbf{v}(\tau)|| d\tau$$

June 13, 2018 19 / 1

Dual Spaces

Definition

Given a vector space V over \mathbb{R} , a linear transformation from V to \mathbb{R} is called a *linear functional* (or *dual vector* or *covector*). The set of all dual vectors (endowed with its natural vector space structure) is called the *dual space*. The dual space is denoted V^* .

Example

If $V = \mathbb{R}^3$ and $\mathbf{w} \in \mathbb{R}^3$, then $dot_{\mathbf{w}} : V \to \mathbb{R}$ defined by $dot_{\mathbf{w}}(\mathbf{v}) = \mathbf{v} \cdot \mathbf{w}$ is a dual vector. Of course $dot_{\mathbf{w}}(a\mathbf{u} + b\mathbf{v}) = (a\mathbf{u} + b\mathbf{v}) \cdot \mathbf{w} = a\mathbf{u} \cdot \mathbf{w} + b\mathbf{v} \cdot \mathbf{w} = a dot_{\mathbf{w}}(\mathbf{u}) + b dot_{\mathbf{w}}(\mathbf{v})$. So $dot_{\mathbf{w}}$ is, as advertised, linear from V to \mathbb{R} .

Dual Spaces

Theorem

Suppose $\lambda \in (\mathbb{R}^3)^*$. Then there exists $\mathbf{w} \in \mathbb{R}^3$ such that $\lambda = dot_{\mathbf{w}}$.

Proof

Suppose λ is a dual vector on \mathbb{R}^3 . Let $\mathbf{w} = (\lambda(\hat{\mathbf{i}}), \lambda(\hat{\mathbf{j}}), \lambda(\hat{\mathbf{k}}))$. Now suppose $\mathbf{u} = (u_1, u_2, u_3)$ is an arbitrary element of \mathbb{R}^3 . Then $\lambda(\mathbf{u}) = \lambda(u_1\hat{\mathbf{i}} + u_2\hat{\mathbf{j}} + u_3\hat{\mathbf{k}})$ (obviously) $= u_1\lambda(\hat{\mathbf{i}}) + u_2\lambda(\hat{\mathbf{j}}) + u_3\lambda(\hat{\mathbf{k}})$ (since λ is linear) $= u_1W_1 + u_2W_2 + u_3W_3$ (by definition of \mathbf{w})

(by definition of dot_{w})

June 13, 2018

21 / 1

Since λ and dot_{w} agree on all inputs, they're equal.

 $= \mathbf{u} \cdot \mathbf{w}$ $= dot_{\mathbf{w}}(\mathbf{u})$

