Reminder: Group

Definition

A group is a pair $(X, \circ)$, where

- X is a set and $\circ : X \times X \to X$ is a total function,

satisfying the following axioms:

associativity	$(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in X$.
neutral element	There exists $e \in X$ s.t. $a \circ e = e \circ a = a$ for every $a \in X$.
inverse	for every $a \in X$ there exists $a^{-1} \in X$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

The group is abelian if additionally

commutativity	$a \circ b = b \circ a$ for all $a, b \in X$.

Reminder: Field

Definition

A field is a triple $(F, +, \cdot)$, where

- $(F, +)$ is an abelian group,
  - let 0 denote its neutral element and $-x$ the inverse to x,
- $(F \setminus \{0\}, \cdot)$ is an abelian group,
  - let 1 denote its neutral element and x^{-1} the inverse to x,
- $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$ (distributivity)

Examples:

- rational numbers $\mathbf{Q}$
- real numbers $\mathbf{R}$
- complex numbers $\mathbf{C}$
- finite fields.

Vector space

Let **F** be a field.

Definition

A vector space over **F** is a triple $(V, +, \cdot)$, where

- $(V, +)$ is an abelian group (neutral element o, inverse $-v$) and
- $\cdot : \mathbf{F} \times V \to V$ is a total function (multiplication by a scalar),

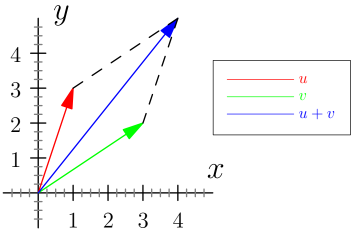
satisfying the following axioms for all $\alpha, \beta \in \mathbf{F}$ and $u, v \in V$:

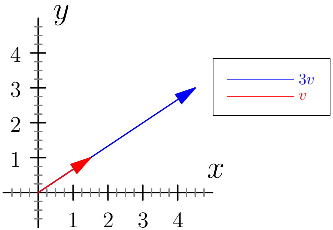
associativity	$(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$
neutral element	$1 \cdot v = v$
distributivity (1)	$(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$
distributivity (2)	$\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$

Elements of a vector space are called vectors.

Examples of vector spaces

Euclidean plane:





$(\mathbf{R}^2, +, \cdot)$, where

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$\alpha \cdot (x, y) = (\alpha x, \alpha y)$$

Similarly: for any integer $n \geq 1$, $(\mathbf{R}^n, +, \cdot)$, where

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$$
$$\alpha \cdot (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n)$$

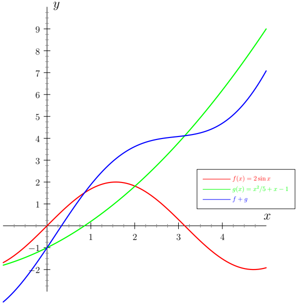
Examples of vector spaces

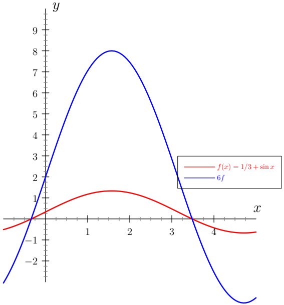
For any field **F** and integers $n, m \geq 1$, the set $\mathbf{F}^{n \times m}$ of all $n \times m$ matrices with coefficients in **F**.

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} + 2\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} + \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 6 & 7 \end{pmatrix}$$

Examples of vector spaces

The set of all functions $\mathbf{R} \to \mathbf{R}$





- $f + g$ is the function whose value at β is $f(\beta) + g(\beta)$
- αf is the function whose value at β is $\alpha f(\beta)$

Related vector spaces:

- functions from $[0, 1]$ to $\mathbf{R}$
- continuous functions from $\mathbf{R}$ to $\mathbf{R}$
- functions from $\mathbf{Q}$ to $\mathbf{Q}$

Examples of vector spaces

$\mathcal{P}$: polynomials with real coefficients

$$\begin{aligned}(1 + x + x^3) + 3(2 - x + x^2) &= (1 + x + x^3) + (6 - 3x + 3x^2) \\ &= 7 - 2x + 3x^2 + x^3\end{aligned}$$

Related vector spaces:

- For any $n \geq 0$, $\mathcal{P}_n$: polynomials of degree at most n.
- Formal infinite series

$$\begin{aligned}\left(\sum_{i=0}^{\infty} \alpha_i x^i\right) + \left(\sum_{i=0}^{\infty} \beta_i x^i\right) &= \sum_{i=0}^{\infty} (\alpha_i + \beta_i) x^i \\ \alpha \left(\sum_{i=0}^{\infty} \beta_i x^i\right) &= \sum_{i=0}^{\infty} (\alpha \beta_i) x^i\end{aligned}$$

- Infinite sequences

$$\begin{aligned}(\alpha_0, \alpha_1, \ldots) + (\beta_0, \beta_1, \ldots) &= (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \ldots) \\ \alpha(\beta_0, \beta_1, \ldots) &= (\alpha\beta_0, \alpha\beta_1, \ldots)\end{aligned}$$

More confusing examples

- Trivial space $(\{o\}, +, \cdot)$
- Every field forms a vector space over itself.
- Complex numbers are a vector space over real numbers.
- Real numbers are a vector space over rational numbers.

Basic properties

Lemma

If $\mathbf{V}$ *is a vector space, then*

$$\alpha v = o \text{ if and only if } \alpha = 0 \text{ or } v = o$$

and

$$(-1)v = -v \text{ for every } v \in \mathbf{V}.$$

Proof.

$$0v = 0v + o = 0v + 0v + (-(0v)) = (0+0)v + (-(0v))$$
$$= 0v + (-(0v)) = o$$
$$\alpha o = \alpha o + o = \alpha o + \alpha o + (-(\alpha o)) = \alpha(o+o) + (-(\alpha o))$$
$$= \alpha o + (-(\alpha o)) = o$$
$$\alpha \neq 0 \wedge \alpha v = o \Rightarrow v = 1v = (\alpha^{-1}\alpha)v = \alpha^{-1}(\alpha v) = \alpha^{-1} o = o$$
$$v + (-1)v = 1v + (-1)v = (1 + (-1))v = 0v = o$$

Basic properties

Lemma

If $\mathbf{V}$ *is a vector space, then*

$$\alpha v = o \text{ if and only if } \alpha = 0 \text{ or } v = o$$

and

$$(-1)v = -v \text{ for every } v \in \mathbf{V}.$$

Proof.

$$0v = 0v + o = 0v + 0v + (-(0v)) = (0+0)v + (-(0v))$$
$$= 0v + (-(0v)) = o$$
$$\alpha o = \alpha o + o = \alpha o + \alpha o + (-(\alpha o)) = \alpha(o + o) + (-(\alpha o))$$
$$= \alpha o + (-(\alpha o)) = o$$
$$\alpha \neq 0 \wedge \alpha v = o \Rightarrow v = 1v = (\alpha^{-1}\alpha)v = \alpha^{-1}(\alpha v) = \alpha^{-1} o = o$$
$$v + (-1)v = 1v + (-1)v = (1 + (-1))v = 0v = o$$

Basic properties

Lemma

If $\mathbf{V}$ *is a vector space, then*

$$\alpha v = o \text{ if and only if } \alpha = 0 \text{ or } v = o$$

and

$$(-1)v = -v \text{ for every } v \in \mathbf{V}.$$

Proof.

$$\begin{aligned} 0v = 0v + o = 0v + 0v + (-(0v)) &= (0+0)v + (-(0v)) \\ &= 0v + (-(0v)) = o \end{aligned}$$

$$\begin{aligned} \alpha o = \alpha o + o = \alpha o + \alpha o + (-(\alpha o)) &= \alpha(o+o) + (-(\alpha o)) \\ &= \alpha o + (-(\alpha o)) = o \end{aligned}$$

$$\alpha \neq 0 \wedge \alpha v = o \Rightarrow v = 1v = (\alpha^{-1}\alpha)v = \alpha^{-1}(\alpha v) = \alpha^{-1}o = o$$

$$v + (-1)v = 1v + (-1)v = (1+(-1))v = 0v = o$$

Basic properties

Lemma

If **V** *is a vector space, then*

$$\alpha v = o \text{ if and only if } \alpha = 0 \text{ or } v = o$$

and

$$(-1)v = -v \text{ for every } v \in \mathbf{V}.$$

Proof.

$$0v = 0v + o = 0v + 0v + (-(0v)) = (0+0)v + (-(0v))$$
$$= 0v + (-(0v)) = o$$
$$\alpha o = \alpha o + o = \alpha o + \alpha o + (-(\alpha o)) = \alpha(o+o) + (-(\alpha o))$$
$$= \alpha o + (-(\alpha o)) = o$$
$$\alpha \neq 0 \wedge \alpha v = o \Rightarrow v = 1v = (\alpha^{-1}\alpha)v = \alpha^{-1}(\alpha v) = \alpha^{-1}o = o$$
$$v + (-1)v = 1v + (-1)v = (1 + (-1))v = 0v = o$$

Linear combinations

Let $\mathbf{V}$ be a vector space over $\mathbf{F}$, let $v_1, \ldots, v_n \in \mathbf{V}$ be vectors.

Definition

For any $\alpha_1, \ldots, \alpha_n \in \mathbf{F}$, the vector

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$$

is a linear combination of $v_1, \ldots, v_n$.

Remark: the number of terms in a linear combination must be finite.

Example

$(1, 2, 3)$ is a linear combination of

$$(-1, 2, -3), (3, -2, 0), \text{ and } (0, 0, 1/2),$$

since

$$(1, 2, 3) = 2(-1, 2, -3) + (3, -2, 0) + 18(0, 0, 1/2).$$

Example

Problem

Is $3x^2+1$ a linear combination of x^2+x and x^2+2x+1?

Suppose that

$$3x^2+1=\alpha(x^2+x)+\beta(x^2+2x+1).$$

Then

$$\begin{aligned} \alpha + \beta &= 3 && \ldots\text{coefficient at } x^2 \\ \alpha + 2\beta &= 0 && \ldots\text{coefficient at } x \\ \beta &= 1 && \ldots\text{constant term} \end{aligned}$$

The system has no solution, so $3x^2+1$ is not a linear combination of x^2+x and x^2+2x+1.

Span

Let $\mathbf{V}$ be a vector space, let $S \subseteq \mathbf{V}$ be a set of vectors.

Definition

The linear span of S (denoted by $\mathrm{span}(S)$) is the set of all linear combinations of elements of S.

- For S finite, instead of $\mathrm{span}(\{v_1, \ldots, v_n\})$, we sometimes write $\mathrm{span}(v_1, \ldots, v_n)$.
- $S \subseteq \mathrm{span}(S)$, since $1v$ is a linear combination belonging to $\mathrm{span}(S)$ for $v \in S$.
- $o \in \mathrm{span}(S)$, since empty linear combination is equal to o.

Examples

$\mathrm{span}(1, x, x^2, x^3) = \{\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 : \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}\}$
is the space $\mathcal{P}_3$ of polynomials of degree at most 3.

$$\mathrm{span}((1, 1, 0), (1, 2, 3)) = \{(x, y, z) : 3x - 3y + z = 0\}$$

is a plane in 3-dimensional Euclidean space.

Spans and matrices

Let $a_1, \ldots, a_m \in R^n$, let $A = (a_1|a_2|\ldots|a_m)$. Then

$$\text{span}(a_1, \ldots, a_m) = \{Ax : x \in R^m\}.$$

Hence,

$$b \in \text{span}(a_1, \ldots, a_m)$$

if and only if the system

$$Ax = b$$

has a solution. Equivalently,

- the last column of $\text{RREF}(A|b) = (A'|b')$ is not a basis column, and
- the coefficients of the linear combination can be chosen as
  - 0 for non-basis columns
  - the entries of b' for the corresponding basis columns

Example

Problem

Does $(1,1)$ *belong to span*$((1,2),(2,4),(1,3),(2,1))$*?*

Equivalently, does

$$\left(\begin{array}{c|c|c|c} 1 & 2 & 1 & 2 \\ 2 & 4 & 3 & 1 \end{array}\right) x = \left(\begin{array}{c} 1 \\ 1 \end{array}\right)$$

have a solution?

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 2 & 1 \\ 2 & 4 & 3 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 1 & 2 & 1 \\ 0 & 0 & 1 & -3 & -1 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} \color{red}{1} & 2 & 0 & 5 & \color{red}{2} \\ 0 & 0 & \color{green}{1} & -3 & \color{green}{-1} \end{array}\right)$$

Example

Problem

Does $(1,1)$ *belong to span*$((1,2),(2,4),(1,3),(2,1))$*?*

Equivalently, does

$$\left(\begin{array}{c|c|c|c} 1 & 2 & 1 & 2 \\ 2 & 4 & 3 & 1 \end{array}\right) x = \left(\begin{array}{c} 1 \\ 1 \end{array}\right)$$

have a solution?

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 2 & 1 \\ 2 & 4 & 3 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 1 & 2 & 1 \\ 0 & 0 & 1 & -3 & -1 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & 5 & 2 \\ 0 & 0 & 1 & -3 & -1 \end{array}\right)$$

Example

Problem

Does $(1,1)$ *belong to span*$((1,2),(2,4),(1,3),(2,1))$*?*

Equivalently, does

$$\left(\begin{array}{c|c|c|c} 1 & 2 & 1 & 2 \\ 2 & 4 & 3 & 1 \end{array}\right) x = \left(\begin{array}{c} 1 \\ 1 \end{array}\right)$$

have a solution?

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 2 & 1 \\ 2 & 4 & 3 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 1 & 2 & 1 \\ 0 & 0 & 1 & -3 & -1 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & 5 & 2 \\ 0 & 0 & 1 & -3 & -1 \end{array}\right)$$

Hence,

$$(1,1) = 2(1,2) - 1 \cdot (1,3).$$

Span is a vector space

Theorem

Let $\mathbf{V} = (V, +, \cdot)$ *be a vector space over* $\mathbf{F}$*, let* $S \subseteq V$ *be any set of vectors. Then*

$$(span(S), +, \cdot)$$

is a vector space, satisfying $span(S) \subseteq V$*.*

Span is a vector space

Proof.

It suffices to prove that $+$ and $\cdot$ are total on span(S), and $o \in$ span(S).

- inverses $-v = (-1)v$ are in span(S) by the totality of $\cdot$

If $u, v \in$ span(S), then there exist $v_1, \ldots, v_n \in S$ and $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbf{F}$ such that

$$u = \alpha_1 v_1 + \ldots + \alpha_n v_n$$
$$v = \beta_1 v_1 + \ldots + \beta_n v_n$$

Then,

$$u + v = (\alpha_1 + \beta_1)v_1 + \ldots + (\alpha_n + \beta_n)v_n$$
$$\alpha v = (\alpha\beta_1)v_1 + \ldots + (\alpha\beta_n)v_n$$

and thus $u + v, \alpha v \in$ span(S). □

Subspaces

Definition

Let $\mathbf{V} = (V, +, \cdot)$ be a vector space. If $U \subseteq V$ and $\mathbf{U} = (U, +, \cdot)$ is a vector space, we say that $\mathbf{U}$ is a subspace of $\mathbf{V}$.
We write $\mathbf{U} \Subset \mathbf{V}$.

Examples:

- the plane $\{(x, y, z) : 3x - 3y + z = 0\} \Subset \mathbf{R}^3$
  - More generally, any line or plane in $\mathbf{R}^3$ containing the origin $(0, 0, 0)$ is a subspace of $\mathbf{R}^3$.
- $\mathcal{P}_n$ (polynomials of degree at most n) form a subspace of the space $\mathcal{P}$ of all polynomials
- $\mathcal{P}$, and the space of continuous functions $\mathbf{R} \to \mathbf{R}$, form subspaces of the space of all functions $\mathbf{R} \to \mathbf{R}$
- trivial subspaces: $(\{o\}, +, \cdot)$ and $\mathbf{V}$ itself.

All subspaces are spans

Lemma

Let $\mathbf{V} = (V, +, \cdot)$ be a vector space, and let U be a subset of V. Then $(U, +, \cdot)$ is a vector space if and only if span$(U) = U$.

Proof.

If span$(U) = U$: As we observed before, span(U) is a vector space; hence, U is a vector space.

If span$(U) \neq U$: Then $+$ or $\cdot$ is not total on U, and thus U is not a vector space.

□

We say that S generates $\mathbf{U}$ if $\mathbf{U} = \text{span}(S)$.

Intersection of subspaces

Lemma

Let $\mathbf{V} = (V, +, \cdot)$ *be a vector space over* $\mathbf{F}$*, let* I *be an arbitrary set, and for* $i \in I$*, let* $\mathbf{U}_i$ *be a subspace of* $\mathbf{V}$*. Then*

$$\mathbf{U}_I = \bigcap_{i \in I} \mathbf{U}_i$$

is a subspace of $\mathbf{V}$*.*

Proof.

Note that $o \in \mathbf{U}_I$. It suffices to show that $+$ and $\cdot$ are total on $\mathbf{U}_I$. If $u, v \in \mathbf{U}_I$ and $\alpha \in \mathbf{F}$, then

- $u, v \in \mathbf{U}_i$ for every $i \in I$, hence
- $u + v, \alpha \cdot v \in \mathbf{U}_i$ for every $i \in I$, hence
- $u + v, \alpha \cdot v \in \mathbf{U}_I$

□

Example

Problem

Describe the intersection of spaces

$$\mathbf{U}_1 = span((1,1,0),(1,2,3)) \quad \textit{and}$$
$$\mathbf{U}_2 = span((1,0,-1),(1,-1,0)).$$

If $(x,y,z) \in \mathbf{U_1} \cap \mathbf{U_2}$, then there exist $\alpha, \beta, \gamma, \delta \in \mathbf{R}$ such that

$$(x,y,z) = \alpha(1,1,0) + \beta(1,2,3) \qquad \ldots v \text{ is in } \mathbf{U_1}$$
$$(x,y,z) = \gamma(1,0,-1) + \delta(1,-1,0) \qquad \ldots v \text{ is in } \mathbf{U_2}$$

Comparing the coefficients, we get

$$\begin{aligned} \alpha + \beta - \gamma - \delta &= 0 \quad \text{at } x \\ \alpha + 2\beta + \delta &= 0 \quad \text{at } y \\ 3\beta + \gamma &= 0 \quad \text{at } z \end{aligned}$$

Example

Problem

Describe the intersection of spaces

$$\mathbf{U}_1 = \mathit{span}((1,1,0),(1,2,3)) \qquad \mathit{and}$$
$$\mathbf{U}_2 = \mathit{span}((1,0,-1),(1,-1,0)).$$

If $(x,y,z) \in \mathbf{U_1} \cap \mathbf{U_2}$, then there exist $\alpha, \beta, \gamma, \delta \in \mathbf{R}$ such that

$$(x,y,z) = \alpha(1,1,0) + \beta(1,2,3) \qquad \ldots v \text{ is in } \mathbf{U_1}$$
$$(x,y,z) = \gamma(1,0,-1) + \delta(1,-1,0) \qquad \ldots v \text{ is in } \mathbf{U_2}$$

The set of solutions is $(\alpha, \beta, \gamma, \delta) \in \{(-3t, t, -3t, t) : t \in \mathbf{R}\}$.

$$\begin{aligned}
\mathbf{U}_1 \cap \mathbf{U}_2 &= \{\alpha(1,1,0) + \beta(1,2,3)\} \\
&= \{-3t(1,1,0) + t(1,2,3) : t \in \mathbf{R}\} \\
&= \{t(-2,-1,3) : t \in \mathbf{R}\} = \text{span}((-2,-1,3)).
\end{aligned}$$

Example

Problem

Describe the intersection of spaces

$$\mathbf{U}_1 = \mathit{span}((1,1,0),(1,2,3)) \qquad \mathit{and}$$
$$\mathbf{U}_2 = \mathit{span}((1,0,-1),(1,-1,0)).$$

$$\mathbf{U}_1 \cap \mathbf{U}_2 = \mathrm{span}((-2,-1,3))$$

Span as an intersection

Lemma

Let $\mathbf{V} = (V, +, \cdot)$ *be a vector space and let* S *be a subset of* V*. Then span*(S) *is the smallest subspace of* $\mathbf{V}$ *containing* S*, that is,*

$$\mathit{span}(S) = \bigcap_{\mathbf{U} \in \mathbf{V}, S \subseteq \mathbf{U}} \mathbf{U}.$$

Proof.

Let

$$\mathbf{W} = \bigcap_{\mathbf{U} \in \mathbf{V}, S \subseteq \mathbf{U}} \mathbf{U}.$$

- Since $S \subseteq \mathbf{W}$, we have $\text{span}(S) \in \text{span}(\mathbf{W}) = \mathbf{W}$.
- Since $S \subseteq \text{span}(S)$, the subspace $\text{span}(S)$ is one of the spaces in the intersection, hence $\mathbf{W} \in \text{span}(S)$.

□