Vector space

Definition: A *vector space* $(V, +, \cdot)$ over a field $(\mathbb{K}, +, \cdot)$ is a set V with a binary operation $+$ on V and a binary operation $\cdot : \mathbb{K} \times V \to V$ called *scalar multiplication* s.t.:

- $(V, +)$ is an Abelian group
- $\forall a, b \in \mathbb{K}, \forall \boldsymbol{v} \in V : (a \cdot b) \cdot \boldsymbol{v} = a \cdot (b \cdot \boldsymbol{v})$
- $\forall \boldsymbol{v} \in V : 1 \cdot \boldsymbol{v} = \boldsymbol{v}$
- $\forall a, b \in \mathbb{K}, \forall \boldsymbol{v} \in V : (a + b) \cdot \boldsymbol{v} = (a \cdot \boldsymbol{v}) + (b \cdot \boldsymbol{v})$
- $\forall a \in \mathbb{K}, \forall \boldsymbol{u}, \boldsymbol{v} \in V : a \cdot (\boldsymbol{u} + \boldsymbol{v}) = (a \cdot \boldsymbol{u}) + (a \cdot \boldsymbol{v})$

Elements of $\mathbb{K}$ are called *scalars*, elements of V are called *vectors*.

Distinguish the zero scalar $0 \in \mathbb{K}$ and the zero vector $\mathbf{0} \in V$.
We have opposite scalars $-a \in \mathbb{K}$ and opposite vectors $-\boldsymbol{v} \in V$.

There are inverse scalars $a^{-1} \in \mathbb{K}$ but *no inverse vectors* $\boldsymbol{v}^{-1}$*!*
Products $\boldsymbol{v} \cdot a$ and $\boldsymbol{v} \cdot \boldsymbol{u}$ are not defined and are *formally wrong!*

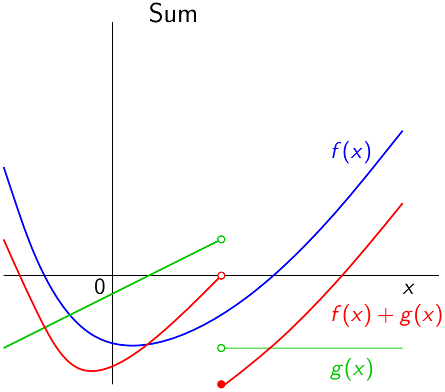
The product symbol $\cdot$ is often omitted and has priority to $+$.

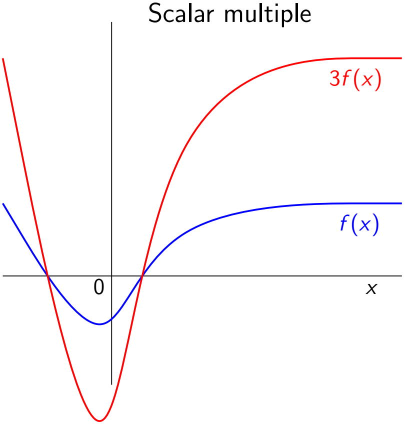
Examples

- The *arithmetic* vector space $\mathbb{K}^n$ of dimension n over $\mathbb{K}$.
  Vectors are ordered n-tuples of elements of $\mathbb{K}$.
  Additions and scalar multiplications are done componentwise.
  Any field $\mathbb{K}$ yields the vector space $\mathbb{K}^1$ of the same cardinality.
- $\mathbb{K}^{m \times n}$ ... matrices of order $m \times n$ over $\mathbb{K}$.
- $V = \{\mathbf{0}\}$ the *trivial* vector space over any field $\mathbb{K}$.
- Polynomials with coefficients in $\mathbb{K}$.
- Polynomials of bounded degree.

The vector space of real functions over the field $\mathbb{R}$

Vectors f, g are the real functions of real variable





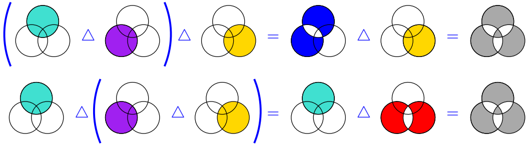
Set systems as vector spaces

Let $\mathcal{X}$ be a system of subsets of a set X that is closed under taking symmetric difference $\triangle$.

Then $(\mathcal{X}, \triangle, \cdot)$ is a vector space over $\mathbb{Z}_2$, where $\cdot$ is defined as: $0 \cdot A = \emptyset$, the neutral element of $\triangle$, and $1 \cdot A = A$ for all $A \in \mathcal{X}$.

Observe that $\forall A, B, C \in \mathcal{X} : (A \triangle B) \triangle C = A \triangle (B \triangle C)$,

since the result contains those elements of X that belong to an odd number of sets A, B and C.

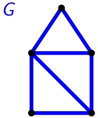


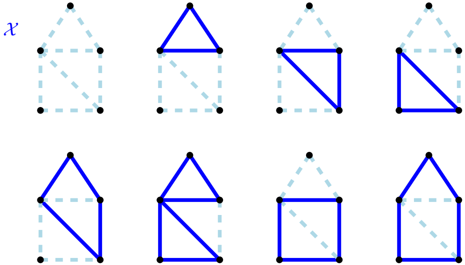
We may represent any $A \in \mathcal{X}$ by its *characteristic function* $\chi_A : X \to \mathbb{Z}_2$ defined as $\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$

Observation: The set $A \triangle B$ has the characteristic function $\chi_{A \triangle B} = \chi_A + \chi_B$, since $1 + 1 = 0$ in $\mathbb{Z}_2$.

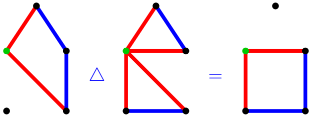
A vector space on graphs

Let $X = E_G$ and $\mathcal{X}$ contain those edge sets A such that every vertex of G is incident with an even number of edges in A. Such sets A induce the so called *even subgraphs* of G.





Observe that $\triangle$ preserves the even degree, since the symmetric difference of two sets of even cardinality, namely the edges incident to a vertex, has also an even cardinality.



Properties of vector spaces

Since $(V, +)$ is a group, we have already proved:

- uniqueness of the vector $\mathbf{0}$,
- uniqueness of $-\boldsymbol{u}$,
- correctness of equiv. transforms: $\boldsymbol{u} = \boldsymbol{v} \Leftrightarrow \boldsymbol{u} + \boldsymbol{w} = \boldsymbol{v} + \boldsymbol{w}$,
- solubility of equations: $\boldsymbol{x} + \boldsymbol{u} = \boldsymbol{v} \Leftrightarrow \boldsymbol{x} = \boldsymbol{v} - \boldsymbol{u}$.

Observation: For any $\boldsymbol{v} \in V$ and $a \in \mathbb{K}$ holds: $0\boldsymbol{v} = a\mathbf{0} = \mathbf{0}$.

Proof:

$0\boldsymbol{v} = 0\boldsymbol{v} + \mathbf{0} = 0\boldsymbol{v} + 0\boldsymbol{v} - 0\boldsymbol{v} = (0+0)\boldsymbol{v} - 0\boldsymbol{v} = 0\boldsymbol{v} - 0\boldsymbol{v} = \mathbf{0}$

$a\mathbf{0} = a\mathbf{0} + \mathbf{0} = a\mathbf{0} + a\mathbf{0} - a\mathbf{0} = a(\mathbf{0} + \mathbf{0}) - a\mathbf{0} = a\mathbf{0} - a\mathbf{0} = \mathbf{0}$

Observation: For any $\boldsymbol{v} \in V$ holds $(-1)\boldsymbol{v} = -\boldsymbol{v}$.

Proof: $(-1)\boldsymbol{v} + \boldsymbol{v} = (-1)\boldsymbol{v} + 1\boldsymbol{v} = (-1+1)\boldsymbol{v} = 0\boldsymbol{v} = \mathbf{0}$

Observation: If $a\boldsymbol{v} = \mathbf{0}$ then $a = 0$ or $\boldsymbol{v} = \mathbf{0}$.

Proof: If $a \neq 0$ then $\boldsymbol{v} = 1\boldsymbol{v} = a^{-1}a\boldsymbol{v} = a^{-1}\mathbf{0} = \mathbf{0}$.

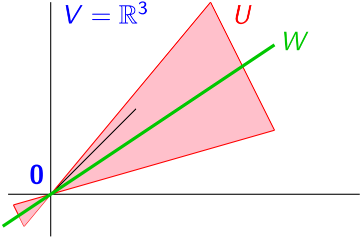
Subspace

Definition: Let V be a vector space over $\mathbb{K}$ then a *subspace* U is a nonempty subset of V satisfying:

- $\forall \boldsymbol{u}, \boldsymbol{v} \in U : \boldsymbol{u} + \boldsymbol{v} \in U$
- $\forall \boldsymbol{v} \in U, \forall a \in \mathbb{K} : a\boldsymbol{v} \in U$

Example: A plane U through the origin $\mathbf{0}$ is a subspace of $V = \mathbb{R}^3$.

A line $W \subset U$ through the origin is a subspace of U and of V as well.



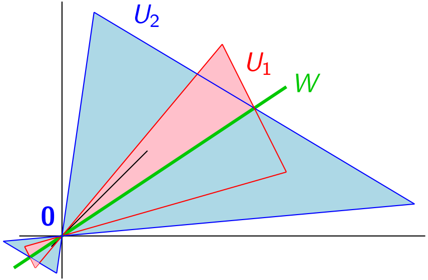
Polynomials of degree ≤ 5 form a subspace of the function space.

Observation: Any subspace is also a vector space, because the existential axioms follow the closure: $\mathbf{0} = 0\boldsymbol{v} \in U$ and $-\boldsymbol{v} = (-1)\boldsymbol{v} \in U$. Other axioms hold already on V.

Intersection of subspaces

Theorem: Let $(U_i, i \in I)$ be any system of subspaces of a space V. The intersection of this system $\bigcap_{i \in I} U_i$ is also a subspace of V.

Example: Planes U_1 and U_2 are subspaces of the vector space $\mathbb{R}^3$. Their intersection is the line W. It is also a subspace of $\mathbb{R}^3$.



Intersection of subspaces

Theorem: Let $(U_i, i \in I)$ be any system of subspaces of a space V. The intersection of this system $\bigcap_{i \in I} U_i$ is also a subspace of V.

Proof: Let $W = \bigcap_{i \in I} U_i$. We show that W is closed on $+$ and $\cdot$.

$\forall \boldsymbol{u}, \boldsymbol{v} \in W$:
$\boldsymbol{u}, \boldsymbol{v} \in W \Rightarrow \forall i \in I : \boldsymbol{u}, \boldsymbol{v} \in U_i \Rightarrow \forall i \in I : \boldsymbol{u} + \boldsymbol{v} \in U_i \Rightarrow \boldsymbol{u} + \boldsymbol{v} \in W$

$\forall a \in \mathbb{K}, \boldsymbol{v} \in W$:
$\boldsymbol{v} \in W \Rightarrow \forall i \in I : \boldsymbol{v} \in U_i \Rightarrow \forall i \in I : a\boldsymbol{v} \in U_i \Rightarrow a\boldsymbol{v} \in W$

Note that when $I = \emptyset$, then the empty intersection $W = \bigcap_{i \in \emptyset} U_i = V$ is a subspace of V itself.

Linear combination, linear hull

Definition: The *linear hull* $\mathcal{L}(X)$ of a subset X of a vector space V is the intersection of all subspaces U of V that contain X.

Formally $\mathcal{L}(X) = \bigcap\{U : X \subseteq U, U \text{ is a subspace of } V\}$

It is also called *the subspace generated by* X
or the *linear span* and may be denoted by $\text{span}(X)$.

Examples: For $V = \mathbb{R}^3$, $\mathcal{L}(\{(2,2,2)^T\}) = \{(a,a,a)^T, a \in \mathbb{R}\}$
... the line containing points having all three coordinates identical

$\mathcal{L}(\{(1,0,0)^T,(0,1,0)^T\}) = \{(a,b,0)^T, a,b \in \mathbb{R}\}$
... the plane determined by the first two axes

Definition: A *linear combination* of vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k \in V$ over $\mathbb{K}$ is any vector $\boldsymbol{u} = a_1\boldsymbol{v}_1 + \ldots + a_k\boldsymbol{v}_k$ where $a_1, \ldots, a_k \in \mathbb{K}$.

Theorem: Let V be a vector space over $\mathbb{K}$ and X be a subset of V. Then $\mathcal{L}(X)$ is the set of all linear combinations of vectors from X.

Example for $W = \{\boldsymbol{x} : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}\}$

For $\boldsymbol{A} = \begin{pmatrix} 1 & -2 & 4 & 0 & 3 \\ -2 & 4 & -6 & 6 & 0 \\ 4 & -8 & 13 & -9 & -4 \\ 3 & -6 & 9 & -9 & 1 \end{pmatrix} \sim\sim \begin{pmatrix} 1 & -2 & 4 & 0 & 3 \\ 0 & 0 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

we solve $W = \{p_1(2,1,0,0,0)^T + p_2(12,0,-3,1,0)^T : p_1, p_2 \in \mathbb{R}\}$

1. W could be viewed the *intersection* of the following subspaces:

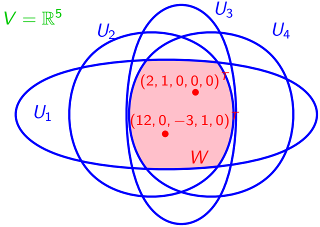
$U_1 = \{\boldsymbol{x} : (1,-2,4,0,3) \cdot \boldsymbol{x} = 0\}$
$U_2 = \{\boldsymbol{x} : (-2,4,-6,6,0) \cdot \boldsymbol{x} = 0\}$
$U_3 = \{\boldsymbol{x} : (4,-8,13,-9,-4) \cdot \boldsymbol{x} = 0\}$
$U_4 = \{\boldsymbol{x} : (3,-6,9,-9,1) \cdot \boldsymbol{x} = 0\}$

Each U_i corresponds to one equation of the system.

(Each is a *hyperplane* in $\mathbb{R}^5$.)

2. The same subspace W was already described as a *set of linear combinations* $W = \mathcal{L}((2,1,0,0,0)^T, (12,0,-3,1,0)^T)$

Correctness of Gaussian elimination and backward substitution yields that both ways describe the same space.



Proof of the theorem

Theorem: Let V be a vector space over $\mathbb{K}$ and X be a subset of V. Then $\mathcal{L}(X)$ is the set of all linear combinations of vectors from X.

For $W_1 = \bigcap_{X \subseteq U_i \subseteq V} U_i$, $W_2 = \left\{ \sum_{i=1}^{k} a_i \boldsymbol{v}_i : k \in \mathbb{N}, a_i \in \mathbb{K}, \boldsymbol{v}_i \in X \right\}$.
we want to show $W_1 = \mathcal{L}(X) = W_2$.

W_2 is a subspace, because it is closed on scalar multiples

$$\boldsymbol{u} \in W_2 \Rightarrow \boldsymbol{u} = \sum_{i=1}^{k} a_i \boldsymbol{v}_i \Rightarrow \alpha \boldsymbol{u} = \alpha \sum_{i=1}^{k} a_i \boldsymbol{v}_i = \sum_{i=1}^{k} (\alpha a_i) \boldsymbol{v}_i \Rightarrow \alpha \boldsymbol{u} \in W_2$$

and analogously also on addition

$$\boldsymbol{u}, \boldsymbol{u}' \in W_2 \Rightarrow \ldots \Rightarrow \boldsymbol{u} + \boldsymbol{u}' \in W_2$$

Since $X \subseteq W_2$, we have W_2 among the intersecting subspaces U_i. Hence $W_1 \subseteq W_2$.

Every U_i contains X and is closed on addition and scalar multiples. Thus every U_i contains all linear combinations of vectors of X. Hence $\forall U_i : W_2 \subseteq U_i \Rightarrow W_2 \subseteq W_1$.

Spaces determined by a matrix

Definition: The *kernel* of $\boldsymbol{A} \in \mathbb{K}^{m \times n}$ is $\ker(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{K}^n : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}\}$, the *row space* $\mathcal{R}(\boldsymbol{A}) \subseteq \mathbb{K}^n$ is the linear hull of the rows of $\boldsymbol{A}$, the *column space* $\mathcal{C}(\boldsymbol{A}) \subseteq \mathbb{K}^m$ is the linear hull of the columns of $\boldsymbol{A}$.

Example: For the matrix $\boldsymbol{A} = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 2 & 1 \\ 1 & 1 & 2 & 0 \end{pmatrix} \in \mathbb{Z}_3^{3\times 4}$ we get

The row space:

$$\mathcal{R}(\boldsymbol{A}) = \left\{ \begin{matrix} (0,0,0,0)^T, & (1,2,0,1)^T, & (2,1,0,2)^T, \\ (2,0,2,1)^T, & (0,2,2,2)^T, & (1,1,2,0)^T, \\ (1,0,1,2)^T, & (2,2,1,0)^T, & (0,1,1,1)^T \end{matrix} \right\} \subseteq \mathbb{Z}_3^4$$

The column space:

$$\mathcal{C}(\boldsymbol{A}) = \left\{ \begin{matrix} (0,0,0)^T, & (1,2,1)^T, & (2,1,2)^T, \\ (2,0,1)^T, & (0,2,2)^T, & (1,1,0)^T, \\ (1,0,2)^T, & (2,2,0)^T, & (0,1,1)^T \end{matrix} \right\} \subseteq \mathbb{Z}_3^3$$

Spaces determined by a matrix

Definition: The *kernel* of $\boldsymbol{A} \in \mathbb{K}^{m \times n}$ is $\ker(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{K}^n : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}\}$,
the *row space* $\mathcal{R}(\boldsymbol{A}) \subseteq \mathbb{K}^n$ is the linear hull of the rows of $\boldsymbol{A}$,
the *column space* $\mathcal{C}(\boldsymbol{A}) \subseteq \mathbb{K}^m$ is the linear hull of the columns of $\boldsymbol{A}$.

Formally:

$$\mathcal{C}(\boldsymbol{A}) = \{\boldsymbol{u} \in \mathbb{K}^m : \boldsymbol{u} = \boldsymbol{A}\boldsymbol{x}, \boldsymbol{x} \in \mathbb{K}^n\}$$
$$\mathcal{R}(\boldsymbol{A}) = \{\boldsymbol{v} \in \mathbb{K}^n : \boldsymbol{v} = \boldsymbol{A}^T\boldsymbol{y}, \boldsymbol{y} \in \mathbb{K}^m\}$$

Observation: The kernel $\ker(\boldsymbol{A})$ is a subspace of $\mathbb{K}^n$.

Observation: Elementary transforms do not alter $\mathcal{R}(\boldsymbol{A})$ nor $\ker(\boldsymbol{A})$.

Observation: $\forall \boldsymbol{v} \in \mathcal{R}(\boldsymbol{A}), \forall \boldsymbol{x} \in \ker(\boldsymbol{A}) : \boldsymbol{v}^T\boldsymbol{x} = 0$.
Proof: $\boldsymbol{v}^T\boldsymbol{x} = (\boldsymbol{A}^T\boldsymbol{y})^T\boldsymbol{x} = \boldsymbol{y}^T\boldsymbol{A}\boldsymbol{x} = \boldsymbol{y}^T\boldsymbol{0} = 0$ for some $\boldsymbol{y} \in \mathbb{K}^m$.

Corollary: Each subspace of an arithmetic vector space is a set of solutions of some homogeneous system of linear equations.

Proof: Take a basis of V as rows of $\boldsymbol{B}$, then take a basis of $\ker(\boldsymbol{B})$ as rows of $\boldsymbol{A}$. Now: $\ker(\boldsymbol{A}) = \ker(\ker(\boldsymbol{B})) = \mathcal{R}(\boldsymbol{B}) = V$.