Groups and Vector Spaces

In the following, we will have a closer look at vector spaces, i.e., the space in which vectors live.

We can informally characterize vectors as objects that can be added together and multiplied by a scalar, and they remain objects of the same type. In the following, we will formalize this intuition and we will start by introducing the concept of a group, which is a set of elements and an operation defined on these elements that keeps some structure of the set intact.

Groups

Groups play an important role in computer science. Besides providing a fundamental framework for operations on sets, they are heavily used in cryptography, coding theory and graphics.

Definition 1 (Group)**.** Consider a set $\mathcal{G}$ and an operation $\otimes : \mathcal{G} \to \mathcal{G}$ defined on $\mathcal{G}$.

Then $G := (\mathcal{G}, \otimes)$ is called a *group* if the following hold: group

1. *Closure* of $\mathcal{G}$ under $\otimes$: $\forall x, y \in \mathcal{G} : x \otimes y \in \mathcal{G}$ Closure
2. *Associativity:* $\forall x, y, z \in \mathcal{G} : (x \otimes y) \otimes z = x \otimes (y \otimes z)$ Associativity:
3. *Neutral element:* $\exists e \in \mathcal{G}\, \forall x \in \mathcal{G} : x \otimes e = x$ and $e \otimes x = x$ Neutral element:
4. *Inverse element:* $\forall x \in \mathcal{G}\, \exists y \in \mathcal{G} : x \otimes y = e$ and $y \otimes x = e$. We often write x^{-1} to denote the inverse element of x. Inverse element:

If additionally $\forall x, y \in \mathcal{G} : x \otimes y = y \otimes x$ then $G = (\mathcal{G}, \otimes)$ is an *Abelian group* (commutative). Abelian group

For example, $\otimes$ could be $+, \cdot$ defined on $\mathbb{R}, \mathbb{N}, \mathbb{Z}$ or $\cup, \cap, \setminus$ defined on $\mathcal{P}(B)$, the power set of B.

Remark. The inverse element is defined with respect to the operation $\otimes$ and does not necessarily mean $\frac{1}{x}$.

Example: (Groups)

- $(\mathbb{Z}, +)$ is a group
- $(\mathbb{N}_0, +)$[1] is not a group: Although $(\mathbb{N}_0, +)$ possesses a neutral element (0), the inverse elements are missing.
- $(\mathbb{Z}, \cdot)$ is not a group: Although $(\mathbb{Z}, \cdot)$ contains a neutral element (1), the inverse elements for any $z \in \mathbb{Z}, z \neq \pm 1$, are missing.

[1] $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$

- $(\mathbb{R}, \cdot)$ is not a group since 0 does not possess an inverse element.
- $(\mathbb{R}\backslash\{0\})$ is Abelian.
- $(\mathbb{R}^n, +), (\mathbb{Z}^n, +), n \in \mathbb{N}$ are Abelian if $+$ is defined componentwise, i.e.,

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n). \tag{1}$$

  Then, $(x_1, \cdots, x_n)^{-1} := (-x_1, \cdots, -x_n)$ is the inverse element and $e = (0, \cdots, 0)$ is the neutral element.
- $(\mathbb{R}^{m \times n}, +)$, the set of $m \times n$-matrices is Abelian (with componentwise addition).

Vector Spaces

When we discussed groups, we looked at sets $\mathcal{G}$ and inner operations on $\mathcal{G}$, i.e., mappings $\mathcal{G} \times \mathcal{G} \to \mathcal{G}$. In the following, we will consider sets that in addition to an inner operation $+$ also contain an outer operation $\cdot$, the multiplication by a scalar $\lambda \in \mathbb{R}$.

Definition 2 (Vector space)**.** A real-valued *vector space* (also called an $\mathbb{R}$-*vector space*) is a set $\mathcal{V}$ with two operations

vector space
$\mathbb{R}$-vector space

$$+ : \mathcal{V} \times \mathcal{V} \to \mathcal{V} \tag{2}$$
$$\cdot : \mathbb{R} \times \mathcal{V} \to \mathcal{V} \tag{3}$$

where

1. $(\mathcal{V}, +)$ is an Abelian group
2. Distributivity:
   (a) $\lambda \cdot (\boldsymbol{x} + \boldsymbol{y}) = \lambda \cdot \boldsymbol{x} + \lambda \cdot \boldsymbol{y} \quad \forall \lambda \in \mathbb{R}, \boldsymbol{x}, \boldsymbol{y} \in \mathcal{V}$
   (b) $(\lambda + \psi) \cdot \boldsymbol{x} = \lambda \cdot \boldsymbol{x} + \psi \cdot \boldsymbol{x} \quad \forall \lambda, \psi \in \mathbb{R}, \boldsymbol{x} \in \mathcal{V}$
3. Associativity (outer operation): $\lambda \cdot (\psi \cdot \boldsymbol{x}) = (\lambda\psi) \cdot \boldsymbol{x} \quad \forall \lambda, \psi \in \mathbb{R}, \boldsymbol{x} \in \mathcal{V}$
4. Neutral element with respect to the outer operation: $1 \cdot \boldsymbol{x} = \boldsymbol{x}, \quad \forall \boldsymbol{x} \in \mathcal{V}$

The elements $\boldsymbol{x} \in V$ are called *vectors*. The neutral element of $(\mathcal{V}, +)$ is the zero vector $\mathbf{0} = [0, \ldots, 0]^\top$, and the inner operation $+$ is called *vector addition*. The elements $\lambda \in \mathbb{R}$ are called *scalars* and the outer operation $\cdot$ is a *multiplication by scalars*. Note that a scalar product is an inner product and, therefore, something different.

vectors
vector addition
scalars
multiplication by scalars

Remark. A "vector multiplication" $\boldsymbol{ab}$, $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^n$, is not defined. Theoretically, we could define an element-wise multiplication, such that $\boldsymbol{c} = \boldsymbol{ab}$ with $c_j = a_j b_j$. This "array multiplication" is common to many programming languages but makes mathematically limited sense using the standard rules for matrix multiplication: By treating vectors as $n \times 1$ matrices (which we usually do), we can use the matrix multiplication. However, then the dimensions of the vectors do not match. Only the following multiplications for vectors are defined: $\boldsymbol{ab}^\top \in \mathbb{R}^{n \times n}$ (outer product), $\boldsymbol{a}^\top \boldsymbol{b} \in \mathbb{R}$ (inner/scalar/dot product).

Vector Subspaces

In the following, we will introduce vector subspaces. Intuitively, they are sets contained in the original vector space with the property that when we perform vector space operations on elements within this subspace, we will never leave it. In this sense, they are "closed".

Definition 3 (Vector Subspace)**.** Let $(\mathcal{V}, +, \cdot)$ be an $\mathbb{R}$-vector space and $\mathcal{U} \subseteq \mathcal{V}$, $\mathcal{U} \neq \emptyset$. Then $U = (\mathcal{U}, +, \cdot)$ is called *vector subspace* of V (or *linear subspace*) if U is a vector space with the vector space operations $+$ and $\cdot$ restricted to $\mathcal{U} \times \mathcal{U}$ and $\mathbb{R} \times \mathcal{U}$. We write $U \subseteq V$ to denote a subspace U of V.

vector subspace

linear subspace

Remark. If $\mathcal{U} \subseteq \mathcal{V}$ and V is a vector space, then U naturally inherits many properties directly from V because they are true for all $\boldsymbol{x} \in \mathcal{V}$, and in particular for all $\boldsymbol{x} \in \mathcal{U} \subseteq \mathcal{V}$. This includes the Abelian group properties, the distributivity, the associativity and the neutral element. To determine whether $(\mathcal{U}, +, \cdot)$ is a subspace of V we still do need to show

1. $\mathcal{U} \neq \emptyset$, in particular: $\mathbf{0} \in \mathcal{U}$
2. Closure of U:
   (a) With respect to the outer operation: $\forall \lambda \in \mathbb{R} \, \forall \boldsymbol{x} \in \mathcal{U} : \lambda \boldsymbol{x} \in \mathcal{U}$
   (b) With respect to the inner operation: $\forall \boldsymbol{x}, \boldsymbol{y} \in \mathcal{U} : \boldsymbol{x} + \boldsymbol{y} \in \mathcal{U}$.

Example: (Vector Subspaces)

- For every vector space V the trivial subspaces are V itself and $\{\mathbf{0}\}$.
- Only example D in Figure 1 is a subspace of $\mathbb{R}^2$ (with the usual inner/ outer operations). In A and C, the closure property is violated; B does not contain $\mathbf{0}$.
- The solution set of a homogeneous linear equation system $\boldsymbol{Ax} = \mathbf{0}$ with n unknowns $\boldsymbol{x} = [x_1, \ldots, x_n]^\top$ is a subspace of $\mathbb{R}^n$.
- The solution of an inhomogeneous equation system $\boldsymbol{Ax} = \boldsymbol{b}$, $\boldsymbol{b} \neq \mathbf{0}$ is not a subspace of $\mathbb{R}^n$.

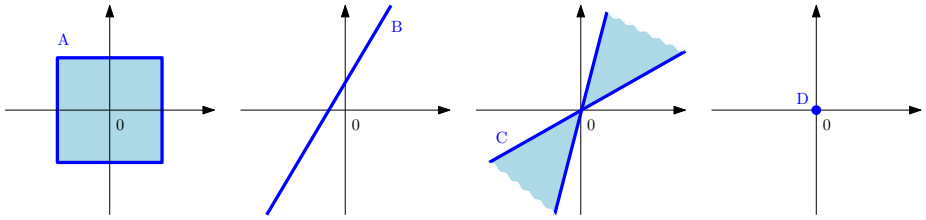

Figure 1: Not all subsets of $\mathbb{R}^2$ are subspaces. In A and C, the closure property is violated; B does not contain $\mathbf{0}$. Only D is a subspace.
