Mathematical Reference

Leonardo Cerasi[1]

GitHub repository: LeonardoCerasi/notes

[1] leo.cerasi@pm.me

Contents

Part I

Multilinear Algebra

Chapter 1

Vector Spaces and Applications

§1.1 Matrices

Definition 1.1.1 (Matrix)
Given a field $\mathbb{K}$ and $n, m \in \mathbb{N}$, an $n \times m$ **matrix** on $\mathbb{K}$ is the object:

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix} \equiv [a_{ij}]^{i=1,\dots,n}_{j=1,\dots,m} \quad : \quad a_{ij} \in \mathbb{K}\ \forall i = 1, \dots, n,\ j = 1, \dots, m$$

The set of all $n \times m$ matrices on $\mathbb{K}$ is denoted by $\mathbb{K}^{n\times m}$.

When the dimensions of the matrix A are unambiguous, we simply write $\mathrm{A} = [a_{ij}]$. We say that an $n \times n$ matrix is a **square matrix**, an $n \times 1$ matrix is a **column vector** and a $1 \times n$ matrix is a **row vector**.
It is possible to define three operations between matrices:

- sum $+ : \mathbb{K}^{n\times m} \times \mathbb{K}^{n\times m} \to \mathbb{K}^{n\times m} : [a_{ij}]^{i=1,\dots,n}_{j=1,\dots,m} + [b_{ij}]^{i=1,\dots,n}_{j=1,\dots,m} \mapsto [a_{ij} + b_{ij}]^{i=1,\dots,n}_{j=1,\dots,m}$
- product by a scalar $\cdot : \mathbb{K} \times \mathbb{K}^{n\times m} \to \mathbb{K}^{n\times m} : \alpha \cdot [a_{ij}]^{i=1,\dots,n}_{j=1,\dots,m} = [\alpha a_{ij}]^{i=1,\dots,n}_{j=1,\dots,m}$
- product $\cdot : \mathbb{K}^{n\times p} \times \mathbb{K}^{p\times m} \to \mathbb{K}^{n\times m} : [a_{ij}]^{i=1,\dots,n}_{j=1,\dots,p} \cdot [b_{ij}]^{i=1,\dots,p}_{j=1,\dots,m} = [c_{ij}]^{i=1,\dots,n}_{j=1,\dots,m}$, $c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj}$

Note that αa_{ij} is the $\mathbb{K}$-product.

Proposition 1.1.1
$(\mathbb{K}^{n\times m}, +)$ is an abelian group.

Proof. The matrix sum is equivalent to the $\mathbb{K}$-sum of corresponding elements, which is associative and commutative. The neutral element is the zero matrix $0_{n\times m} = [0]^{i=1,\dots,n}_{j=1,\dots,m}$, while the inverse element is $-\mathrm{A} = [-a_{ij}]^{i=1,\dots,n}_{j=1,\dots,m}$. □

Theorem 1.1.1

$(\mathbb{K}^{n\times n}, +, \cdot)$ is a non-commutative ring.

Proof. By Prop. 1.1.1, $(\mathbb{K}^{n\times n}, +)$ is an abelian group. It is trivial to show the associativity and distributivity of the matrix product, i.e.:

1. $\mathrm{A}\cdot(\mathrm{B}\cdot\mathrm{C}) = (\mathrm{A}\cdot\mathrm{B})\cdot\mathrm{C}$, $\lambda(\mathrm{A}\cdot\mathrm{B}) = (\lambda\mathrm{A})\cdot\mathrm{B} = \mathrm{A}\cdot(\lambda\mathrm{B})$ $\forall\mathrm{A},\mathrm{B},\mathrm{C}\in\mathbb{K}^{n\times n}, \lambda\in\mathbb{K}$
2. $\mathrm{A}\cdot(\mathrm{B}+\mathrm{C}) = \mathrm{A}\cdot\mathrm{B}+\mathrm{A}\cdot\mathrm{C}$, $(\mathrm{A}+\mathrm{B})\cdot\mathrm{C} = \mathrm{A}\cdot\mathrm{C}+\mathrm{B}\cdot\mathrm{C}$ $\forall\mathrm{A},\mathrm{B},\mathrm{C}\in\mathbb{K}^{n\times n}$

Finally, the neutral element of the matrix product is the identity matrix $\mathrm{I}_n = [\delta_{ij}]_{i,j=1,\dots,n}$. □

Definition 1.1.2 (Transposed matrix)

Given a matrix $\mathrm{A}\in\mathbb{K}^{n\times m}$, its **transpose** is defined as $\mathrm{A}^\intercal\in\mathbb{K}^{m\times n} : [a^\intercal_{ij}]^{i=1,\dots,m}_{j=1,\dots,n} = [a_{ji}]^{j=1,\dots,n}_{i=1,\dots,m}$.

A square matrix $\mathrm{A}\in\mathbb{K}^{n\times n}$ is said **symmetric** if $\mathrm{A}^\intercal = \mathrm{A}$ or **antisymmetric** if $\mathrm{A}^\intercal = -\mathrm{A}$, and it is **diagonal** if $a_{ij} = 0\ \forall i\neq j\in\{1,\dots,n\}$.

Definition 1.1.3 (Inverse matrix)

A square matrix $\mathrm{A}\in\mathbb{K}^{n\times n}$ is **invertible** if $\exists\mathrm{A}^{-1}\in\mathbb{K}^{n\times n} : \mathrm{A}^{-1}\cdot\mathrm{A} = \mathrm{A}\cdot\mathrm{A}^{-1} = \mathrm{I}_n$.

Example 1.1.1 (Non-invertible matrix)

The matrix $\begin{bmatrix}2 & 0\\ 0 & 0\end{bmatrix}$ is non-invertible, as $\begin{bmatrix}2 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix} = \begin{bmatrix}2\alpha & 2\beta\\ 0 & 0\end{bmatrix} \neq \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ $\forall\alpha,\beta,\gamma,\delta\in\mathbb{R}$.

Definition 1.1.4 (General linear group)

The **general linear group** $\mathrm{GL}(n,\mathbb{K})$ is defined as the subset of $\mathbb{K}^{n\times n}$ of all invertible matrices.

Note that $\mathrm{GL}(1,\mathbb{K}) = \mathbb{K}-\{0\}$.

Theorem 1.1.2

$(\mathrm{GL}(n,\mathbb{K}),\cdot)$ is a non-abelian group.

Proof. The neutral element is I_n, as $\mathrm{I}_n^{-1} = \mathrm{I}_n \implies \mathrm{I}_n\in\mathrm{GL}(n,\mathbb{K})$, while the existence of the inverse is granted by definition. We only have to show closure under matrix multiplication:

$$(\mathrm{AB})^{-1} = \mathrm{B}^{-1}\mathrm{A}^{-1} \impliedby \mathrm{I}_n = \mathrm{A}\cdot\mathrm{A}^{-1} = \mathrm{AI}_n\mathrm{A}^{-1} = \mathrm{ABB}^{-1}\mathrm{A}^{-1} = (\mathrm{AB})(\mathrm{AB})^{-1}$$

Hence, $\mathrm{A},\mathrm{B}\in\mathrm{GL}(n,\mathbb{K}) \implies \mathrm{AB}\in\mathrm{GL}(n,\mathbb{K})$. □

§1.1.1 Linear systems of equations

A **linear equation** with $n \in \mathbb{N}$ variables and $\mathbb{K}$-coefficients is an expression of the form:

$$a_1x_1 + \cdots + a_nx_n = b \qquad a_i, b \in \mathbb{K}\ \forall i = 1, \ldots, n$$

A **solution** of the equation is an n-tuple $(\bar{x}_1, \ldots, \bar{x}_n) \in \mathbb{K}^n$ which satisfies this expression.

Definition 1.1.5 (Linear system of equations)

A linear system of equations (or simply **linear system**) is a collection of m linear equations with n variables:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \qquad \Longleftrightarrow \qquad \mathrm{A}\mathbf{x} = \mathbf{b}$$

where we defined:

$$\mathrm{A} = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{bmatrix} \in \mathbb{K}^{m\times n} \qquad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{K}^{m\times 1} \qquad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^{n\times 1}$$

Two linear systems with the same set of solutions are called **equivalent systems**: note that two equivalent systems must have the same number of variables, but not necessarily the same number of equations.
Based on the cardinality of its solution set, a linear system is said to be **impossible** if it has no solutions, **determined** if it has one solution and **undetermined** if it has infinitely-many solutions. Moreover, if the solution set can be parametrized by $k \in \mathbb{N}_0$ variables, the system is of kind ∞^k: a determined system is of kind ∞^0.
Linear systems can be systematically solved applying a reduction algorithm to their corresponding matrices: **Gauss algorithm**. Starting with a general composed matrix $[\mathrm{A}|\mathbf{b}] \in \mathbb{K}^{m\times(n+1)}$, first we multiply the first row by a_{11}^{-1}, so that:

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array}\right] \longrightarrow \left[\begin{array}{cccc|c} 1 & a'_{12} & \ldots & a'_{1n} & b'_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array}\right]$$

Then, at each row $\mathrm{R}_2, \ldots, \mathrm{R}_m$ we apply the transformation $\mathrm{R}_k \mapsto \mathrm{R}_k - a_{k1}\mathrm{R}_1$, so that:

$$\left[\begin{array}{cccc|c} 1 & a'_{12} & \ldots & a'_{1n} & b'_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array}\right] \longrightarrow \left[\begin{array}{cccc|c} 1 & a'_{12} & \ldots & a'_{1n} & b'_1 \\ 0 & a'_{22} & \ldots & a'_{2n} & b'_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & a'_{m2} & \ldots & a'_{mn} & b'_m \end{array}\right]$$

Reiterating this process to progressively smalles submatrices, the algorithm yields the general transformation:

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right] \longrightarrow \left[\begin{array}{cccc|c} 1 & a'_{12} & \dots & a'_{1n} & b'_1 \\ 0 & 1 & \dots & a'_{2n} & b'_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & b'_m \end{array}\right]$$

As these are linear transformations, the two matrices represent equivalent linear systems: the transformed linear system is substantially easier to solve, and its solution set is a solution set of the starting linear system too.

Definition 1.1.6 (Character)

Given a matrix $\mathrm{M} \in \mathbb{K}^{n\times m}$, its **character** $\mathrm{car}(\mathrm{M})$ is the number of non-zero rows remaining after Gauss reduction.

It can be proven that the character is independent of the operations performed during the reduction algorithm.

Theorem 1.1.3 (Rouché–Capelli theorem)

A linear system $\mathrm{A}\mathbf{x} = \mathbf{b}$ has solutions only if $\mathrm{car}(\mathrm{A}) = \mathrm{car}([\mathrm{A}|\mathbf{b}])$. Moreover, if the system has solutions, then it is of kind ∞^{n-r}, with n number of variables and $r = \mathrm{car}(\mathrm{A})$.

§1.2 Vector spaces

Definition 1.2.1 (Vector space)

Given a set $V \neq \varnothing$ and a field $\mathbb{K}$, then V is a **$\mathbb{K}$-vector space** if there exist two operations:

$$+ : V \times V \to V \,:\, (\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v} + \mathbf{w} \qquad\qquad \cdot : \mathbb{K} \times V \to V \,:\, (\lambda, \mathbf{v}) \mapsto \lambda \cdot \mathbf{v}$$

such that $(V, +)$ is an abelian group and the following properties hold $\forall \lambda, \mu \in \mathbb{K}, \mathbf{v}, \mathbf{w} \in V$:

1. $(\lambda + \mu) \cdot (\mathbf{v} + \mathbf{w}) = \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{v} + \lambda \cdot \mathbf{w} + \mu \cdot \mathbf{w}$
2. $(\lambda \cdot \mu) \cdot \mathbf{v} = \lambda \cdot (\mu \cdot \mathbf{v}) = \mu \cdot (\lambda \cdot \mathbf{v})$
3. $1_{\mathbb{K}} \cdot \mathbf{v} = \mathbf{v}$

Note that there are three unique neutral elements: $0_{\mathbb{K}} \equiv 0$, $1_{\mathbb{K}} \equiv 1$ and $0_V \equiv \mathbf{0}$. In the following, the multiplication symbol $\cdot$ is suppressed, as the factors clarify which multiplication is occurring ($\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ or $\cdot : \mathbb{K} \times V \to V$, which have the same neutral element $1_{\mathbb{K}}$).

Example 1.2.1 (Complex numbers)

$V = \mathbb{C}$ is a vector space both for $\mathbb{K} = \mathbb{R}$ and $\mathbb{K} = \mathbb{C}$, although they are different objects.

Example 1.2.2 (Field as vector space)

$V = \mathbb{K}$ is a $\mathbb{K}$-vector space. Note that, in this case, $0_\mathbb{K} \equiv 0_V$.

Note that, by the uniqueness of 0_V, then $\forall \mathbf{v} \in V\ \exists! -\mathbf{v} \in V : \mathbf{v} + (-\mathbf{v}) = 0_V$, so the following cancellation rule holds $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V$:

$$\mathbf{u} + \mathbf{v} = \mathbf{w} + \mathbf{v} \quad \Longrightarrow \quad \mathbf{u} = \mathbf{w} \tag{1.1}$$

We can now state some basic properties of vector spaces.

Lemma 1.2.1 (Basic properties of vector spaces)

Given a $\mathbb{K}$-vector space V, then $\forall \lambda \in \mathbb{K}, \mathbf{v} \in V$:

a. $0_\mathbb{K} \cdot \mathbf{v} = 0_V$

b. $(-\lambda) \cdot \mathbf{v} = -(\lambda \cdot \mathbf{v})$

c. $\lambda \cdot 0_V = 0_V$

d. $\lambda \cdot \mathbf{v} = 0_V \iff \lambda = 0_\mathbb{K} \lor \mathbf{v} = 0_V$

Proof. Respectively:

a. Consider $c \in \mathbb{K} - \{0_\mathbb{K}\}$; then $c\mathbf{v} + 0_V = c\mathbf{v} = (c + 0_\mathbb{K})\mathbf{v} = c\mathbf{v} + 0_\mathbb{K} \cdot \mathbf{v}$, which by Eq. 1.1 proves $0_\mathbb{K} \cdot \mathbf{v} = 0_V$.

b. $\lambda\mathbf{v} + (-\lambda)\mathbf{v} = (\lambda - \lambda)\mathbf{v} = 0_\mathbb{K} \cdot \mathbf{v} = 0_V$, which by the uniqueness of the negative element proves $(-\lambda)\mathbf{v} = -(\lambda\mathbf{v})$.

c. $\lambda \cdot 0_V = \lambda(\mathbf{v} - \mathbf{v}) = \lambda\mathbf{v} + \lambda \cdot (-1_\mathbb{K}) \cdot \mathbf{v} = \lambda\mathbf{v} + (-\lambda)\mathbf{v} = \lambda\mathbf{v} - (\lambda\mathbf{v}) = 0_V$

d. $\lambda = 0_\mathbb{K}$ is trivial, so consider $\lambda \neq 0_\mathbb{K}$; then $\exists! \lambda^{-1} \in \mathbb{K} : \lambda^{-1} \cdot \lambda = 1_\mathbb{K}$, so $0_V = \lambda^{-1} \cdot 0_V = \lambda^{-1} \cdot (\lambda\mathbf{v}) = (\lambda^{-1} \cdot \lambda)\mathbf{v} = 1_\mathbb{K} \cdot \mathbf{v} = \mathbf{v}$, i.e. $\mathbf{v} = 0_V$.

□

§1.2.1 Subspaces

Definition 1.2.2 (Subspace)

Given a $\mathbb{K}$-vector space V and a subset $U \subseteq V : U \neq \varnothing$, then U is a **subspace** of V if it is closed under $+ : U \times U \to U$ and $\cdot : \mathbb{K} \times U \to U$.

Lemma 1.2.2

If U is a subspace of $V(\mathbb{K})$, then $0_V \in U$.

Proof. By definition $U \neq \varnothing \implies \exists \mathbf{v} \in U$. By the closure condition $\lambda\mathbf{v} \in U\ \forall \lambda \in \mathbb{K}$, hence taking $\lambda = 0_\mathbb{K}$ proves the thesis. □

A typical strategy to prove that U is a subspace of $V(\mathbb{K})$ is showing the closure properties, while to prove that it is *not* a subspace we usually show that $0_V \notin U$.

Example 1.2.3 (Polynomial subspaces)
Given $V = \mathbb{K}[x]$, then $U = \mathbb{K}_n[x]$ is a subspace $\forall n \in \mathbb{N}_0$.

An important concept to analyze vector spaces is that of linear combination. Given two sets $\{\lambda_k\}_{k=1,\ldots,n} \subset \mathbb{K}$ and $\{\mathbf{v}_k\}_{k=1,\ldots,n} \subset V$, their **linear combination** is:

$$\sum_{k=1}^{n} \lambda_k \mathbf{v}_k = \lambda_1 \mathbf{v}_1 + \ldots \lambda_n \mathbf{v}_n \in V \tag{1.2}$$

Proposition 1.2.1 (Subspaces and linear combinations)
Given a $\mathbb{K}$-vector space V and $U \subset V : U \neq \varnothing$, then U is a subspace of V if and only if it is closed under linear combinations, that is:

$$\{\lambda_k\}_{k=1,\ldots,n} \subset \mathbb{K}, \{\mathbf{v}_k\}_{k=1,\ldots,n} \subset U \quad \implies \quad \sum_{k=1}^{n} \lambda_k \mathbf{v}_k \in U$$

Proof. First, note that the general case of linear combinations of n vectors can be reduced to the case of 2 vectors.
($\Rightarrow$) Being U a subspace, it is closed under $+ : U \times U \to U$ and $\cdot : \mathbb{K} \times U \to U$; then, by definition $\lambda, \mu \in \mathbb{K}, \mathbf{v}, \mathbf{w} \in U \implies \lambda\mathbf{v} + \mu\mathbf{w} \in U$.
($\Leftarrow$) Given $\lambda \in \mathbb{K}$ and $\mathbf{v}, \mathbf{w} \in V$, then $\mathbf{v}+\mathbf{w} = 1_{\mathbb{K}}\mathbf{v}+1_{\mathbb{K}}\mathbf{w}$ and $\lambda\mathbf{v} = \lambda\mathbf{v}+0_{\mathbb{K}}\mathbf{w}$, hence closure under linear combinations implies closure under $+ : U \times U \to U$ and $\cdot : \mathbb{K} \times U \to U$. □

Generally, it is easier to show closure under linear combinations rather than under addition and scalar multiplication.

Lemma 1.2.3 (Intersection of subspaces)
Given two subspaces of V_1, V_2 of $V(\mathbb{K})$, then $V_1 \cap V_2$ is still a subset of $V(\mathbb{K})$.

Proof. Being V_1, V_2 subspaces, both V_1 and V_2 are closed under linear combinations, so $V_1 \cap V_2$ is too, as $\mathbf{v} \in V_1 \cap V_2 \implies \mathbf{v} \in V_1 \wedge \mathbf{v} \in V_2$. □

On the other hand, in general $V_1 \cup V_2$ is not a subspace. As a counterexample, consider e.g. $V = \mathrm{Vect}_0(\mathbb{E}^3)$, the plane $\pi : z = 0$ and the line $r : (x, y, z) = (0, 0, t), t \in \mathbb{R}$; then, consider the subspaces $V_1 = \mathrm{Vect}_0(\pi), V_2 = \mathrm{Vect}_0(r)$: their union is clearly not closed under addition, as:

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \in V_1, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \in V_2 \qquad \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \notin V_1 \cup V_2$$

Definition 1.2.3 (Sum of subspaces)
Given a $\mathbb{K}$-vector space V and two subspaces V_1, V_2, their **sum** is defined as:

$$V_1 + V_2 := \{\mathbf{w} \in V : \mathbf{w} = \mathbf{u} + \mathbf{v}, \mathbf{u} \in V_1, \mathbf{v} \in V_2\}$$

This is a **direct sum**, denoted by $V_1 \oplus V_2$, if every $\mathbf{w} \in V_1 + V_2$ has a unique representation as $\mathbf{w} = \mathbf{u} + \mathbf{v}, \mathbf{u} \in V_1, \mathbf{v} \in V_2$.

Trivially $V_1, V_2 \subseteq V_1 + V_2$.

Lemma 1.2.4 (Direct sum as disjoint sum)

Given two subspaces V_1, V_2 of $V(\mathbb{K})$, then $V_1 + V_2 = V_1 \oplus V_2 \iff V_1 \cap V_2 = \{\mathbf{0}\}$.

Proof. ($\Rightarrow$) Suppose $\exists \mathbf{v} \in V_1 \cap V_2 : \mathbf{v} \neq \mathbf{0}$; then $\mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v}$, i.e. the expression of $\mathbf{v} \in V_1 + V_2$, but the expression of $\mathbf{v} \in V_1 \oplus V_2$ must be unique, hence $\mathbf{v} = \mathbf{0}$ $\rightarrow\!\leftarrow$
($\Leftarrow$) Suppose $\exists \mathbf{w} \in V_1 + V_2 : \mathbf{w} = \mathbf{u}_1 + \mathbf{v}_1 = \mathbf{u}_2 + \mathbf{v}_2, \mathbf{u}_1 \neq \mathbf{u}_2 \in V_1, \mathbf{v}_1 \neq \mathbf{v}_2 \in V_2$; then $V_1 \ni \mathbf{u}_1 - \mathbf{u}_2 = \mathbf{v}_2 - \mathbf{v}_1 \in V_2 \implies \mathbf{v}_2 - \mathbf{v}_1 \in V_1$, so $\mathbf{v}_2 - \mathbf{v}_1 \in V_1 \cap V_2$, but $V_1 \cap V_2 = \{\mathbf{0}\}$, hence $\mathbf{v}_2 = \mathbf{v}_1$ and idem for $\mathbf{u}_1 = \mathbf{u}_2$ $\rightarrow\!\leftarrow$ ☐

The sum of subspaces preserves the subspace structure, contrary to the simple union.

Proposition 1.2.2 (Sum as subspace)

Given a $\mathbb{K}$-vector space and two subspaces V_1, V_2, their sum $V_1 + V_2$ is still a subspace of V.

Proof. Consider $\mathbf{a}, \mathbf{b} \in V_1 + V_2$ and define $\mathbf{u}_{a,b} \in V_1, \mathbf{v}_{a,b} \in V_2 : \mathbf{a} = \mathbf{u}_a + \mathbf{v}_a \wedge \mathbf{b} = \mathbf{u}_b + \mathbf{v}_b$: as V_1, V_2 are subspaces, they are closed under linear combinations, so, given $\lambda, \mu \in \mathbb{K}$, then $\lambda\mathbf{a} + \mu\mathbf{b} = (\lambda\mathbf{u}_a + \mu\mathbf{u}_b) + (\lambda\mathbf{v}_a + \mu\mathbf{v}_b) \equiv \mathbf{u} + \mathbf{v} \in V_1 + V_2$, where $\mathbf{u} \in V_1$ and $\mathbf{v} \in V_2$, which shows that $V_1 + V_2$ too is closed under linear combinations and a subspace by Prop. 1.2.1. ☐

§1.2.2 Bases

To give a more explicit description of vector spaces, we have to define the concept of basis and its properties.

§1.2.2.1 Generators

Definition 1.2.4 (Linear dependence)

Given a $\mathbb{K}$-vector space V and a set $\{\mathbf{v}_j\}_{j=1,\ldots,k} \equiv S \subseteq V$, then the vectors of S are:

- **linearly dependent** (LD) if $\exists \{\lambda_j\}_{j=1,\ldots,k} \subset \mathbb{K} - \{0\} : \lambda_1\mathbf{v}_1 + \ldots \lambda_k\mathbf{v}_k = \mathbf{0}$
- **linearly independent** (LI) if $\lambda_1\mathbf{v}_1 + \ldots \lambda_k\mathbf{v}_k = \mathbf{0} \iff \lambda_j = 0 \; \forall j = 1, \ldots, k$

The generalization to infinite sets is trivial: $\{\mathbf{v}_\alpha\}_{\alpha\in\mathcal{I}} \equiv S \subset V(\mathbb{K})$ is LI if every finite subset of S is LI, while it is LD if there exists at least one non-empty subset which is LD.

Example 1.2.4 (Complex numbers)

$\{1, \mathrm{i}\}$ are LD in $\mathbb{C}(\mathbb{C})$, as $1 \cdot 1 + \mathrm{i} \cdot \mathrm{i} = 0$, while they are LI in $\mathbb{C}(\mathbb{R})$.

Example 1.2.5 (Polynomials)
$\{1, x, \dots, x^n, \dots\}$ are LI in $\mathbb{K}[x]$.

We can prove some basic properties of linear dependence.

Lemma 1.2.5 (Basic properties of linear dependence)
Given a $\mathbb{K}$-vector space V and $S \subseteq V : S \neq \varnothing$, then:

a. given $S \subseteq T \subseteq V$, then S LD $\implies T$ LD
b. $S = \{\mathbf{v}\}$ LD $\implies \mathbf{v} = \mathbf{0}$
c. $S = \{\mathbf{v}_1, \mathbf{v}_2\}$ LD $\implies \exists \lambda \in \mathbb{K} : \mathbf{v}_1 = \lambda \mathbf{v}_2$
d. if $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ LD, then at least one $\mathbf{v}_i$ is a linear combination of the other vectors
e. if S LI and $S \cup \{\mathbf{w}\}$ LD, then $\mathbf{w}$ is a linear combination of the vectors of S
f. if $\lambda_1 \mathbf{v}_1 + \dots + \lambda_n \mathbf{v}_n = \mathbf{0}$ and $\lambda_n \neq 0$, then $\mathbf{v}_n$ is a linear combination of $\{\mathbf{v}_1, \dots, \mathbf{v}_{n-1}\}$

Proof. Respectively:

a. $S \subseteq T \implies \mathbf{v} \in T \; \forall \mathbf{v} \in S$, hence $\{\mathbf{v}_i\}_{i=1,\dots,n} \subset S$ LD $\implies \{\mathbf{v}_i\}_{i=1,\dots,n} \subset T$ LD
b. $\lambda \mathbf{v} = \mathbf{0} \iff \lambda = 0 \vee \mathbf{v} = \mathbf{0}$, so $\mathbf{v} = \mathbf{0} \implies S$ LD, while S LD $\implies \lambda \neq 0 \implies \mathbf{v} = 0$
c. $\{\mathbf{v}_1, \mathbf{v}_2\}$ LD $\implies \exists \lambda, \mu \in \mathbb{K} - \{0\} : \lambda \mathbf{v}_1 + \mu \mathbf{v}_2 = \mathbf{0} \iff \mathbf{v}_1 = \lambda^{-1} \mu \mathbf{v}_2$
d. If $\{\mathbf{v}_j\}_{j=1,\dots,n}$ LD, then by definition $\exists \{\lambda_j\}_{j=1,\dots,n} \subset \mathbb{K} - \{0\} : \sum_{j=1}^n \lambda_j \mathbf{v}_j = \mathbf{0}$, hence WLOG $\mathbf{v}_1$ can be isolated as $\mathbf{v}_1 = -\lambda_1^{-1} \sum_{j=2}^n \lambda_j \mathbf{v}_j$
e. $\{\mathbf{v}_1, \dots, \mathbf{v}_n, \mathbf{w}\}$ LD $\implies \exists \lambda_1, \dots, \lambda_n, \alpha \in \mathbb{K} - \{0\} : \sum_{j=1}^n \lambda_j \mathbf{v}_j + \alpha \mathbf{w} = \mathbf{0}$, so $\mathbf{w}$ can be isolated as $\mathbf{w} = -\alpha^{-1} \sum_{j=1}^n \lambda_j \mathbf{v}_j$
f. $\sum_{j=1}^n \lambda_j \mathbf{v}_j = \mathbf{0} \wedge \lambda_n \neq 0 \implies \mathbf{v}_n = -\lambda_n^{-1} \sum_{j=1}^{n-1} \lambda_j \mathbf{v}_j$

□

We can now introduce the notion of generators.

Definition 1.2.5 (Generated subset)
Given a $\mathbb{K}$-vector space V and $\{\mathbf{v}_\alpha\}_{\alpha \in \mathcal{I}} \equiv S \subseteq V$, the **subset generated by** S is the set:

$$\operatorname{span} S := \{\mathbf{v} \in V : \exists \lambda_1, \dots, \lambda_n \in \mathbb{K}, \mathbf{v}_{\alpha_1}, \dots, \mathbf{v}_{\alpha_n} \in S : \mathbf{v} = \lambda_1 \mathbf{v}_{\alpha_1} + \dots + \lambda_n \alpha_{\mathbf{n}}\}$$

The elements of S are called **generators** of $\operatorname{span} S$.

We often denote $\operatorname{span} S \equiv \langle S \rangle$: this subset contains all vectors of V which can be expressed as linear combinations of vectors of S.

Proposition 1.2.3 (Generated subspace)

Given a $\mathbb{K}$-vector space and $S \subseteq V : S \neq \varnothing$, then $\langle S \rangle$ is a subspace of V.

Proof. Let $S = \{\mathbf{s}_\alpha\}_{\alpha \in \mathcal{I}}$ and $\mathbf{v}, \mathbf{w} \in S : \mathbf{v} = \sum_{j=1}^{k} \lambda_j \mathbf{s}_{\alpha_j}, \mathbf{w} = \sum_{j=1}^{n} \mu_j \mathbf{s}_{\beta_j}$, with coefficients $\{\lambda_j\}_{j=1,\dots,k}, \{\mu_j\}_{j=1,\dots,n} \subset \mathbb{K} - \{0\}$. Adding vectors with vanishing coefficients, we can rewrite $\mathbf{v}$ and $\mathbf{w}$ in terms of the same vectors:

$$\mathbf{v} = \sum_{j=1}^{m} a_j \mathbf{s}_{\gamma_j} \qquad \mathbf{w} = \sum_{j=1}^{m} b_j \mathbf{s}_{\gamma_j} \qquad \Longrightarrow \qquad \zeta\mathbf{v} + \xi\mathbf{w} = \sum_{j=1}^{m} (\zeta a_j + \xi b_j)\, \mathbf{s}_{\gamma_j} \in \langle S \rangle$$

This shows that $\langle S \rangle$ is closed under linear combination, hence the thesis. $\square$

Note that, give a subspace $U \subseteq V(\mathbb{K})$, then at most $U = \langle U \rangle$, hence every subspace admits a family of generators. If U has a finite number of generators, then it is a **finitely-generated subspace**: for example, $\mathbb{K}_n[x] = \langle 1, \dots, x^n \rangle$, $\mathbb{C}(\mathbb{C}) = \langle 1 \rangle$ and $\mathbb{C}(\mathbb{R}) = \langle 1, \mathrm{i} \rangle$ are finitely-generated. We can state two trivial properties of generated subsets.

Lemma 1.2.6

Given $S \subseteq V(\mathbb{K})$ and $U = \langle S \rangle$, then:

a. given $S \subseteq T \subseteq V$, then $U = \langle T \rangle$

b. if $U = \langle \mathbf{s}_1, \dots, \mathbf{s}_n \rangle$ and $\mathbf{s}_n \in \langle \mathbf{s}_1, \mathbf{s}_{n-1} \rangle$, then $U = \langle \mathbf{s}_1, \dots, \mathbf{s}_{n-1} \rangle$

Proof. Respectively:

a. If $S \subseteq T$, then each linear combination in S is a linear combination in T too, hence $\langle S \rangle = \langle T \rangle$

b. Given $\mathbf{v} = \lambda_1 \mathbf{s}_1 + \dots + \lambda_n \mathbf{s}_n \in U$ and $\mathbf{s}_n = \mu_1 \mathbf{s}_1 + \dots + \mu_{n-1} \mathbf{s}_{n-1}$, then $\mathbf{v} = (\lambda_1 + \mu_1)\, \mathbf{s}_1 + \dots + (\lambda_{n-1} + \mu_{n-1})\, \mathbf{s}_{n-1}$, hence the thesis

$\square$

§1.2.2.2 Bases of generic vector spaces

Definition 1.2.6 (Basis of a vector space)

Given a $\mathbb{K}$-vector space V, a **basis** of V is a LI subset $\mathcal{B} \subseteq V : V = \langle \mathcal{B} \rangle$.

Every non-trivial vector space (i.e. $V \neq \{\mathbf{0}\}$) admits the existence of a basis, but the proof is non-trivial as it relies on Zorn's Lemma (or equivalently to the Axiom of Choice).

Theorem 1.2.1 (Basis theorem)

Every non-trivial vector space admits a basis.

Proof. First, we prove that every LI subset of V can be extended to a basis of V. Let $A \subseteq V$ be a non-empty LI subset of V, and define $\mathscr{S}$ the collection of all LI supersets of A.

Lemma 1.2.7

Given a chain $\{A_\alpha\}_{\alpha\in\mathcal{I}} \subseteq \mathscr{S} : A_1 \subseteq A_2 \subseteq \dots$, then $\bigcup_{\alpha\in\mathcal{I}} A_\alpha \in \mathscr{S}$.

Proof. Set $\mathcal{A} \equiv \bigcup_{\alpha\in\mathcal{I}} A_\alpha$. If $A \subseteq A_\alpha\ \forall\alpha \in \mathcal{I}$, then trivially $A \subseteq \mathcal{A}$. To prove the linear independence, consider a linear combination $\lambda_1\mathbf{v}_1 + \cdots + \lambda_n\mathbf{v}_n$ in $\mathcal{A}$, with $n \in \mathbb{N}$, and choose an A_{α_n} large enough so that $v_1, \dots, v_n \in A_{\alpha_n}$. Then, $\lambda_1\mathbf{v}_1 + \cdots + \lambda_n\mathbf{v}_n = \mathbf{0} \implies \lambda_1, \dots, \lambda_n = 0$, as A_{α_n} is LI by definition. Since $n \in \mathbb{N}$ is generic, $\mathcal{A}$ is LI. □

It is then clear that $\mathscr{S}$ satisfies the hypotheses of Zorn's Lemma (Lemma A.2.1), therefore it has a maximal element $\mathcal{B}$. Now, suppose $\langle\mathcal{B}\rangle \neq V$, i.e. $\exists\mathbf{b} \in V - \langle\mathcal{B}\rangle$, and consider the linear combination $\mu\mathbf{b} + \lambda_1\mathbf{v}_1 + \cdots + \lambda_n\mathbf{b}_n = \mathbf{0}$, with $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathcal{B}$ and $n \in \mathbb{N}$: then $-\mu\mathbf{b} \in \langle\mathcal{B}\rangle$, but $\mathbf{b} \notin \langle\mathcal{B}\rangle$, so $\mu = 0$ (as $\mathbf{b} \neq \mathbf{0} \in \langle\mathcal{B}\rangle$). Consequently, $\lambda_1 = \cdots = \lambda_n = 0$ as $\mathcal{B}$ is LI, thus $\mathcal{B} \cup \{\mathbf{b}\}$ is LI and a superset of $\mathcal{B} \in \mathscr{S}$, which contradicts $\mathcal{B}$ being a maximal element of $\mathscr{S}$ $\rightarrow\!\leftarrow$

Having showed that every LI subset $A \subseteq V$ can be extended to a basis $\mathcal{B}$ of V, the thesis is trivially found taking $A = \varnothing$, which is a subset of every non-trivial vector space. □

This, though trivial for finite-dimensional spaces, is quite impressive for infinite-dimensional ones (for dimensionality, see SECTION).

Proposition 1.2.4

Given a $\mathbb{K}$-vector space V, then $S \subseteq V$ is a basis of V if and only if every element of V has a unique representation as a linear combination of elements of S.

Proof. Note that two representations are equal if they differ only by vanishing coefficients.
($\Rightarrow$) As $V = \langle S\rangle$, then every $\mathbf{v} \in V$ can be written as a linear combination of elements of S. Suppose that $\mathbf{v}$ has two representations:

$$\mathbf{v} = \lambda_1\mathbf{s}_1 + \dots \lambda_n\mathbf{s}_n \qquad\qquad \mathbf{v} = \mu_1\mathbf{t}_1 + \cdots + \mu_m\mathbf{t}_m$$

with $\{\mathbf{s}_j\}_{j=1,\dots,n}, \{\mathbf{t}_k\}_{k=1,\dots,m} \subseteq S$ and $\{\lambda_j\}_{j=1,\dots,n}, \{\mu_k\}_{k=1,\dots,m} \subseteq \mathbb{K}$. Now, we can extend both representations by adding vanishing coefficients, so that both include the same vectors of S:

$$\mathbf{v} = \zeta_1\mathbf{v}_1 + \cdots + \zeta_r\mathbf{v}_r \qquad\qquad \mathbf{v} = \xi_1\mathbf{v}_1 + \cdots + \xi_r\mathbf{v}_r$$

with $\{\mathbf{v}_j\}_{j=1,\dots,r} \subseteq S$ and $\{\zeta_j\}_{j=1,\dots,r}, \{\xi_j\}_{j=1,\dots,r} \subseteq \mathbb{K}$. Subtracting these two expressions:

$$\mathbf{0} = (\zeta_1 - \xi_1)\,\mathbf{v}_1 + \cdots + (\zeta_r - \xi_r)\,\mathbf{v}_r$$

But S is LI, hence $\zeta_j = \xi_j\ \forall j = 1, \dots, r$, i.e. the two representations are equal.
($\Leftarrow$) As every $\mathbf{v} \in V$ can be written as a linear combination of elements of S, then $V = \langle S\rangle$. We only have to prove that S is LI. Consider $\mathbf{0} \in V$: by hypothesis, it has a unique representation as a linear combination of vectors in S, and a possible representation is

$\mathbf{0} = 0 \cdot \mathbf{s}$ for some $\mathbf{s} \in S$, i.e. the trivial representation with all vanishing coefficients. Now, consider a linear combination in S:

$$\lambda_1 \mathbf{s}_1 + \cdots + \lambda_n \mathbf{s}_n = \mathbf{0}$$

with $n \in \mathbb{N}$. This too is a representation of $\mathbf{0}$, hence $\lambda_j = 0 \; \forall j = 1, \ldots, n$ by the uniqueness of the representation. As $n \in \mathbb{N}$ is generic, this is the definition of S being LI. □

§1.2.2.3 Bases of finitely-generated vector spaces

We now turn our attention to finitely-generated vector spaces, i.e. $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$ with $n \in \mathbb{N}$.

Proposition 1.2.5

Given a $\mathbb{K}$-vector space $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, then $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ contains a basis of V.

Proof. If $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is LI, then it is a basis of V, so consider $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ LD, i.e. $\exists \mathbf{v} \in \langle \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} - \{\mathbf{v}\} \rangle$. WLOG, consider $\mathbf{v} = \mathbf{v}_n$, so that $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_{n-1} \rangle$: reiterating this procedure, all LD vectors are eliminated, leaving a basis of V, as at most only a single vector $\mathbf{v}_1$ remains ($\mathbf{v}_1 \neq \mathbf{0}$ as it is LI). □

A direct corollary is that every finitely-generated vector space admits a finite basis, found by the elimination algorithm highlighted in the previous proof.

Definition 1.2.7 (MSLIV)

Given a $\mathbb{K}$-vector space V, then a LI subset $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq V$ is a **maximal set of linearly-independent vectors** (MSLIV) if $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \cup \{\mathbf{v}\}$ is LD $\forall \mathbf{v} \in V$.

We extend this notion considering $V = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$: then, a LI subset $\{\mathbf{v}_{j_1}, \ldots, \mathbf{v}_{j_r}\} \subseteq \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, with $r \leq n$, is a **maximal subset of linearly-independent vectors** (MSLIV) if $\{\mathbf{v}_{j_1}, \ldots, \mathbf{v}_{j_r}\} \cup \{\mathbf{v}_j\}$ is LD $\forall j \in \{1, \ldots, n\} - \{j_1, \ldots, j_r\}$. Trivially, a maximal subset of LI vectors is also a maximal set of LI vectors in V, so the redundant acronym MSLIV is justified. We can now prove that bases and MSLIVs are equivalent notions.

Theorem 1.2.2 (Bases as MSLIVs)

Given a non-trivial $\mathbb{K}$-vector space $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, then $\mathcal{B} \subseteq V$ is a basis if and only if it is a MSLIV.

Proof. ($\Leftarrow$) WLOG let $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$, with $r \leq n$, be a MSLIV of $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$: then WTS $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_r \rangle$. If $r = n$ the proof is complete, so consider $r < n$ and $\mathbf{v}_j : r < j \leq n$: by definition $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\} \cup \{\mathbf{v}_j\}$ is LD, i.e. $\exists \{\lambda_{j_k}\}_{k=1,\ldots,r} \subseteq \mathbb{K} : \mathbf{v}_i = \lambda_{j_1} \mathbf{v}_1 + \cdots + \lambda_{j_r} \mathbf{v}_r$, which means that $\mathbf{v}_i \in \langle \mathbf{v}_1, \ldots, \mathbf{v}_r \rangle \implies V = \langle \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} - \{\mathbf{v}_i\} \rangle$. This holds $\forall i \in [r{+}1, n] \subseteq \mathbb{N}$, hence $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_r \rangle$.
($\Rightarrow$) Let $\mathcal{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis of $V$and $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\} \subseteq V : m > n$, and suppose this is LI. By definition $\exists \lambda_1, \ldots, \lambda_n \in \mathbb{K} : \mathbf{w}_1 = \lambda_1 \mathbf{v}_1 + \cdots + \lambda_n \mathbf{v}_n$, but $\mathbf{w}_1$ is LI, therefore

$\exists j \in [1, \dots, n] \subseteq \mathbb{N} : \lambda_j \neq 0$. WLOG $j = 1$, hence $\mathbf{v}_1 \in \langle \mathbf{w}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \rangle$. Iterating, we can substitute $\mathbf{v}_1, \dots, \mathbf{v}_n$ with $\mathbf{w}_1, \dots, \mathbf{w}_n$: indeed, supposing that $\{v_1, \dots, \mathbf{v}_r\}$ have been substituted with $\mathbf{w}_1, \dots, \mathbf{w}_r$, with $1 \leq r < n$, then $\mathbf{v}_{r+1}$ can be substituted with $\mathbf{w}_{r+1}$ as $V = \langle \mathbf{w}_1, \dots, \mathbf{w}_r, \mathbf{v}_{r+1}, \dots, \mathbf{v}_n \rangle \implies \exists \alpha_1, \dots, \alpha_r, \beta_{r+1}, \dots, \beta_n \in \mathbb{K} : \mathbf{w}_{r+1} = \alpha_1 \mathbf{w}_1 + \dots + \alpha_r \mathbf{w}_r + \beta_{r+1} \mathbf{v}_{r+1} + \dots + \beta_n \mathbf{v}_n$, but $\{\mathbf{w}_1, \dots, \mathbf{w}_{r+1}\}$ are LI, thus $\exists j \in [r+1, n] \subseteq \mathbb{N} : \beta_j \neq 0$, and WLOG $j = r+1$ by reordering indices. Performing the reiteration $V = \langle \mathbf{w}_1, \dots, \mathbf{w}_n \rangle$, so $\mathbf{w}_{n+1}$ is a linear combination of $\{\mathbf{w}_1, \dots, \mathbf{w}_n\}$ $\rightarrow\!\leftarrow$ $\square$

There is still another equivalent concept to introduce.

Definition 1.2.8 (MSG)

Given a $\mathbb{K}$-vector space V, then $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} \subseteq V$ is a **minimal set of generators** (MSG) if $V = \langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle$ and $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} - \{\mathbf{v}_j\}$ does not generate V $\forall j = 1, \dots, n$.

Theorem 1.2.3 (Bases ad MSGs)

Given a non-trivial $\mathbb{K}$-vector space V, then $\mathcal{B} \subseteq V$ is a basis of V if and only if it is a MSG.

Proof. ($\Leftarrow$) Let $\{\mathbf{v}_1, \dots, \mathbf{v}_n\} \subseteq V$ be a MSG: then WTS $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is LI. Consider a linear combination $\lambda_1 \mathbf{v}_1 + \dots + \lambda_n \mathbf{v}_n = \mathbf{0}$ and suppose $\lambda_1 \neq 0$: this allows to express $\mathbf{v}_1$ as a linear combination of $\{\mathbf{v}_2, \dots, \mathbf{v}_n\}$, but then $V = \langle \mathbf{v}_2, \dots, \mathbf{v}_n \rangle$ $\rightarrow\!\leftarrow$
($\Rightarrow$) Suppose $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is not a MSG, and WLOG $V = \langle \mathbf{v}_2, \dots, \mathbf{v}_n \rangle$: then $\mathbf{v}_1$ can be expressed as linear combination of $\{\mathbf{v}_2, \dots, \mathbf{v}_n\}$, i.e. $\mathcal{B}$ is LD $\rightarrow\!\leftarrow$ $\square$

This shows that bases, MSLIVs and MSGs are all equivalent notions.

§1.2.2.4 Dimensionality

To properly define the concept of dimensionality of a vector space, we first have to prove that all bases are equivalent.

Theorem 1.2.4 (Equicardinality of bases)

Given a non-trivial $\mathbb{K}$-vector space V and two bases $\mathcal{B}_1 = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}, \mathcal{B}_2 = \{\mathbf{w}_1, \dots, \mathbf{w}_m\}$, then $n = m$.

Proof. As $\mathcal{B}_1$ is a MSLIV by Th. 1.2.2, then every subset of $n+1$ vectors in V is LD, hence $m \leq n$ as $\mathcal{B}_2$ must be LI. The vice versa applies too, hence $n = m$. $\square$

By this theorem, all bases of finitely-generated spaces are equivalent, since the equicardinality ensures that we can define a bijection $f : \mathcal{B}_1 \leftrightarrow \mathcal{B}_2$ $\forall \mathcal{B}_1, \mathcal{B}_2$ bases of V.
Moreover, this result hints to the fact that the cardinality of the bases of V is a fundamental property of the vector space, linked to hits dimensionality, so we give a proper definition of this quantity.

Definition 1.2.9 (Dimension)

Given a $\mathbb{K}$-vector space V, then we define its **dimension** as:

$$\dim_{\mathbb{K}} V := \begin{cases} 0 & V = \{\mathbf{0}\} \\ n & |\mathcal{B}| = n \ \forall \mathcal{B} \text{ basis of } V \\ \infty & V \text{ not finitely-generated} \end{cases}$$

The dimension of a vector space is a well-defined quantity by Th. 1.2.1 and Th. 1.2.4.

Example 1.2.6 (Various spaces)

Trivially, $\dim_{\mathbb{K}} \mathbb{K}^n = n$, so $\dim_{\mathbb{C}} \mathbb{C}^n = n$ and $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$, while $\dim_{\mathbb{R}} \mathbb{R}^{\mathbb{R}} = \infty$.

We can now give some trivial properties of dimensionality.

Lemma 1.2.8 (Basic property of dimension)

Given an n-dimensional $\mathbb{K}$-vector space V, then:

a. $\{\mathbf{v}_1, \dots, \mathbf{v}_m\} \subseteq V$ is LD $\forall m > n$

b. $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ LI is a basis of V

c. $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ set of generators of V is a basis of V

Proof. These results are corollaries of Th. 1.2.2 and Th. 1.2.3. □

Proposition 1.2.6 (Dimension of subspaces)

Given $\dim_{\mathbb{K}} V = n$ and a subspace $U \subseteq V$, then $\dim_{\mathbb{K}} U \equiv k \leq n$ and $k = n \iff U = V$.

Proof. The case $U = \{\mathbf{0}\}$ is trivial, so consider $U \neq \{\mathbf{0}\}$. Let $\mathbf{u}_1 \in U$ LI and add $\mathbf{u}_2, \mathbf{u}_3, \dots \in U$ to get $\{\mathbf{u}_1, \mathbf{u}_2\}, \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}, \dots$: a LD subset is reached in at most n steps. Let WLOG $\{\mathbf{u}_1, \dots, \mathbf{u}_k\}$ the MSLIV of $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$, with $k \leq n$: by Th. 1.2.2, this is a basis of U, hence $k = \dim_{\mathbb{K}} U \leq n$.
$U = V \implies k = n$ is trivial, while $k = n \implies \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ is a MSLIV of V, hence a basis of V, so $V = \langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle = V$. □

A consequence of this theorem is the fact that LI subset $\{\mathbf{v}_1, \dots, \mathbf{v}_r\} \subseteq V$, with $r < n$, can always be completed to a basis, i.e. $\exists \mathbf{w}_{r+1}, \dots, \mathbf{w}_n \in V : \{\mathbf{v}_1, \dots, \mathbf{v}_r, \mathbf{w}_{r+1}, \mathbf{w}_n\}$ is a basis of V.

Theorem 1.2.5 (Grassmann's Theorem)

Given a $\mathbb{K}$-vector space V and finitely-generated subspaces $X, Y \subseteq V$, then:

$$\dim_{\mathbb{K}} X + \dim_{\mathbb{K}} Y = \dim_{\mathbb{K}} (X + Y) + \dim_{\mathbb{K}} (X \cap Y) \tag{1.3}$$

Proof. Let $\mathcal{B}_X = \{\mathbf{x}_1, \dots, \mathbf{x}_r\}, \mathcal{B}_Y = \{\mathbf{y}_1, \dots, \mathbf{y}_s\}$ be bases of X, Y and $m \equiv \dim_{\mathbb{K}}(X \cap Y)$. If $m = 0$, then $X \cap Y = \{\mathbf{0}\}$, while if $m \geq 1$ let $\mathcal{B}_{XY} = \{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ be a basis of $X \cap Y$, which is a finitely-generated subspace by Lemma 1.2.3. Then, completing the bases, $\exists \mathbf{x}_{m+1}, \dots, \mathbf{x}_r \in X : \{\mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_{m+1}, \dots, \mathbf{x}_r\}$ is a basis of X and $\exists \mathbf{y}_{m+1}, \dots, \mathbf{y}_s \in Y$: $\{\mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{y}_{m+1}, \dots, \mathbf{y}_s\}$ is a basis of Y (WLOG same vectors as in $\mathcal{B}_X$ and $\mathcal{B}_Y$). Now, WTS $\dim_{\mathbb{K}}(X+Y) = r + s - m$, so consider $\mathcal{B} = \{\mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_{m+1}, \dots, \mathbf{x}_r, \mathbf{y}_{m+1}, \dots, \mathbf{y}_s\}$:

- $X + Y \coloneqq \{\mathbf{v} = \mathbf{x} + \mathbf{y} : \mathbf{x} \in X, \mathbf{y} \in Y\}$, but $\mathbf{x} \in \langle \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_{m+1}, \dots, \mathbf{x}_r \rangle$ and $\mathbf{y} \in \langle \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{y}_{m+1}, \dots, \mathbf{y}_s \rangle$, so $\mathbf{x} + \mathbf{y} \in \langle \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{x}_{m+1}, \dots, \mathbf{x}_r, \mathbf{y}_{m+1}, \dots, \mathbf{y}_s \rangle$, i.e. $X + Y = \langle \mathcal{B} \rangle$;
- consider the following linear combination:

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_m \mathbf{v}_m + \beta_{m+1} \mathbf{x}_{m+1} + \dots + \beta_r \mathbf{x}_r + \gamma_{m+1} \mathbf{y}_{m+1} + \dots + \gamma_s \mathbf{y}_s = \mathbf{0}$$

  and rearrange it as:

$$\underbrace{\alpha_1 \mathbf{v}_1 + \dots + \alpha_m \mathbf{v}_m + \beta_{m+1} \mathbf{x}_{m+1} + \dots + \beta_r \mathbf{x}_r}_{\in X} = \underbrace{-\gamma_{m+1} \mathbf{y}_{m+1} - \dots - \gamma_s \mathbf{y}_s}_{\in Y}$$

  Therefore, both expressions are in $X \cap Y = \langle \mathbf{v}_1, \dots, \mathbf{v}_m \rangle$, hence $\exists \delta_1, \dots, \delta_m \in \mathbb{K}$ such that:

$$\delta_1 \mathbf{v}_1 + \dots + \delta_m \mathbf{v}_m + \gamma_{m+1} \mathbf{y}_{m+1} + \dots + \gamma_s \mathbf{y}_s = \mathbf{0}$$

  But $\mathcal{B}_Y$ is a basis of Y, i.e. LI, so $\delta_1 = \dots = \delta_m = \gamma_{m+1} = \dots = \gamma_s = 0$, thus:

$$\alpha_1 \mathbf{v}_1 + \dots + \alpha_m \mathbf{v}_m + \beta_{m+1} \mathbf{x}_{m+1} + \dots + \beta_r \mathbf{x}_r = \mathbf{0}$$

  But $\mathcal{B}_X$ is a basis of X, i.e. LI, so $\alpha_1 = \dots = \alpha_m = \beta_{m+1} = \dots = \beta_r = 0$. This shows that $\mathcal{B}$ is LI.

By Def. 1.2.6, $\mathcal{B}$ is a basis of $X + Y$, i.e. $\dim_{\mathbb{K}}(X+Y) = r + s - m$. □

This is a fundamental theorem of Linear Algebra.

Example 1.2.7 (Eucldean geometry)

Consider $V = \mathrm{Vect}_0(\mathbb{E}^3)$ and α, β planes such that $\mathbf{0} \in \alpha, \beta$: they then determine a line $r \equiv \alpha \cap \beta \ni \{\mathbf{0}\}$. Setting $X = \mathrm{Vect}_0(\alpha)$, $Y = \mathrm{Vect}_0(\beta)$ and $X \cap Y = \mathrm{Vect}_0(r)$, we correctly have $2 + 2 = 3 + 1$.

§1.3 Linear applications

§1.4 Inner-product spaces

Appendices

Appendix A

Logic

§A.1 Binary relations

Definition A.1.1 (Binary relation)

Given two sets $\mathcal{A}$, $\mathcal{B}$ and their cartesian product $\mathcal{A} \times \mathcal{B} := \{(a, b) : a \in \mathcal{A} \wedge b \in \mathcal{B}\}$, a **binary relation** $\mathfrak{R}$ is a subset of $\mathcal{A} \times \mathcal{B}$. Two elements $a \in \mathcal{A}$, $b \in \mathcal{B}$ are related, and we write $a\mathfrak{R}b$, if $(a, b) \in \mathfrak{R} \subseteq \mathcal{A} \times \mathcal{B}$.

If $\mathcal{B} = \mathcal{A}$, we say that $\mathfrak{R}$ is a relation "on" $\mathcal{A}$.

Definition A.1.2 (Function)

A **function** between two sets $\mathcal{A}$, $\mathcal{B}$ is a relation $\mathfrak{R}_f$ such that, given an element $a \in \mathcal{A}$, then there exists at most one element $b \in \mathcal{B} : a\mathfrak{R}_f b$.

We usually write $b = f(a)$ in place of $a\mathfrak{R}_f b$.

Definition A.1.3 (Equivalence relation)

Given a set $\mathcal{A}$, a relation $\mathfrak{R}$ on $\mathcal{A}$ is an **equivalence relation** if it has the following properties:

1. reflexivity: $a\mathfrak{R}a \ \forall a \in \mathcal{A}$
2. symmetry: $a\mathfrak{R}b \iff b\mathfrak{R}a \ \forall a, b \in \mathcal{A}$
3. transitivity: $a\mathfrak{R}b \wedge b\mathfrak{R}c \implies a\mathfrak{R}c \ \forall a, b, c \in \mathcal{A}$

Example A.1.1

Take $\mathcal{A} = \mathbb{Z}$. Then, the relation $a\mathfrak{R}b \iff \exists k \in \mathbb{Z} : a - b = 2k$ is an equivalence relation: $a - a = 2k$ with $k = 0$ (reflexivity), $a - b = 2k \iff b - a = 2h$ with $h = -k$ (symmetry) and $a - b = 2k, b - c = 2h \implies a - c = 2l$ with $l = k + h$ (transitivity.

Definition A.1.4 (Equivalence class)

Given a set $\mathcal{A}$ and an equivalence relation $\mathfrak{R}$ on $\mathcal{A}$, then the **equivalence relation** of $a \in \mathcal{A}$ is defined as $[a]_{\mathfrak{R}} := \{b \in \mathcal{A} : a\mathfrak{R}b\}$.

In absence of ambiguity, the subscript $\mathfrak{R}$ is dropped, and the equivalence class $a \in \mathcal{A}$ is simply denoted by $[a]$.

Theorem A.1.1

Given a set $\mathcal{A}$, an **equivalence** relation $\mathfrak{R}$ on $\mathcal{A}$ and two elements $a, b \in \mathcal{A}$, then:

1. $a \in [a]_{\mathfrak{R}}$
2. $a\mathfrak{R}b \implies [a]_{\mathfrak{R}} = [b]_{\mathfrak{R}}$
3. $a\not{\mathfrak{R}}b \implies [a]_{\mathfrak{R}} \cap [b]_{\mathfrak{R}} = \varnothing$

Proof. The first proposition is true by reflexivity. To prove the second proposition, let $x \in [a]_{\mathfrak{R}}$: then, $x\mathfrak{R}a$, but also $x\mathfrak{R}b$ by transitivity, hence $x \in [b]_{\mathfrak{R}}$. This proves $[b]_{\mathfrak{R}} \subseteq [a]_{\mathfrak{R}}$, and the vice versa is equivalently proven, hence $[a]_{\mathfrak{R}} = [b]_{\mathfrak{R}}$. To prove the third proposition, suppose $\exists x \in [b]_{\mathfrak{R}} \cap [a]_{\mathfrak{R}}$: then, $x\mathfrak{R}a \wedge x\mathfrak{R}b \implies a\mathfrak{R}b$ by transitivity, which is absurd. □

This theorem shows that an equivalence relation splits the set in separated equivalence classes.

Definition A.1.5 (Partition)

Given a set $\mathcal{X} \neq \varnothing$ and its power set $\mathcal{P}(\mathcal{X}) \coloneqq \{\mathcal{A} : \mathcal{A} \subseteq \mathcal{X}\}$, a **partition** of $\mathcal{X}$ is a collection of subsets $\{\mathcal{A}_i\}_{i\in\mathcal{I}} \subseteq \mathcal{P}(\mathcal{X})$ which satisfies the following propeties:

1. $\mathcal{A}_i \neq \varnothing \ \forall i \in \mathcal{I}$
2. $\mathcal{A}_i \cap \mathcal{A}_j = \varnothing \ \forall i \neq j \in \mathcal{I}$
3. $\mathcal{X} = \bigcup_{i\in\mathcal{I}} \mathcal{A}_i$

The equivalence classes determined by an equivalence relation form a partition of the set it is defined on.

Definition A.1.6 (Quotient set)

Given a set $\mathcal{A}$ and an equivalence relation $\mathfrak{R}$ on $\mathcal{A}$, the **quotient set** $\mathcal{A}/\mathfrak{R}$ is defined as the set of all equivalence classes of $\mathcal{A}$ determined by $\mathfrak{R}$.

Example A.1.2 ($\mathbb{Z}$ as a quotient set)

The set $\mathbb{Z}$ can be seen as a quotient set $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\mathfrak{R}$ with $(n, m)\mathfrak{R}(n', m') \iff n - m = n' - m'$. Indeed, there are three kinds of equivalence classes: $[(n, 0)] \equiv n$, $[(0, n)] \equiv -n$ and $[(0, 0)] \equiv 0$.

Example A.1.3 (Modular equivalence)

Given $n \in \mathbb{N}$, the **congruence modulo** n relation is an equivalence relation on $\mathbb{Z}$ defined as $a \equiv_n b \iff \exists k \in \mathbb{Z} : a - b = kn$. This relation defines the quotient set $\mathbb{Z}_n \equiv \mathbb{Z}/(\operatorname{mod} n)$, which in general is $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$.

§A.2 Zorn's Lemma

Zorn's Lemma is an equivalent expression of the Axiom of Choice.

Definition A.2.1 (Order relation)

Given a set $\mathcal{X}$, an **order relation** is a relation $\leq$ with the following properties:

1. reflexivity: $x \leq x \ \forall x \in \mathcal{X}$
2. antisymmetry: $x \leq y \land y \leq x \iff x = y$
3. transitivity: $x \leq y \land y \leq z \implies x \leq z$

Then, $(\mathcal{X}, \leq)$ is an **ordered set**.

Note that we define $x < y$ as $x \leq y \land x \neq y$. Moreover, trivially, every subset of an ordered set is an ordered set too, with the induced order relation.

Example A.2.1 (Inclusion)

Let $\mathcal{X}$ be a set. Then the **inclusion** $\subseteq$ is an order relation on $\mathcal{P}(\mathcal{X})$.

An order relation on $\mathcal{X}$ is a **total ordering** is $x \leq y \lor y \leq x \ \forall x, y \in \mathcal{X}$, and $\mathcal{X}$ is a **totally-ordered set**[1].

Definition A.2.2 (Chains)

Given an ordered set $(\mathcal{X}, \leq)$, then:

1. a subset $\mathcal{C} \subseteq \mathcal{X}$ is a **chain** if $(\mathcal{C}, \leq)$ is a totally-ordered set
2. given $\mathcal{C} \subseteq \mathcal{X}$ and $x \in \mathcal{X}$, then x is an **upper bound** of $\mathcal{C}$ if $y \leq x \ \forall y \in \mathcal{C}$
3. an element $m \in \mathcal{X}$ is a **maximal element** of $\mathcal{X}$ if $\{x \in \mathcal{X} : m \leq x\} \equiv \{m\}$

Lemma A.2.1 (Zorn's Lemma)

Let $(\mathcal{X}, \leq)$ be a non-empty ordered set. If every chain in $\mathcal{X}$ has at least one upper bound, then $\mathcal{X}$ has at least one maximal element.

[1] Not a universal convention: some refer to ordered set as "partially-ordered sets" and to totally-ordered sets as "ordered sets". We use the convention of e.g. [1]

Index

Bibliography

[1] M. Manetti. *Topologia*. Springer Milano, 2014. DOI: 10.1007/978-88-470-5662-6.