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 $-\mathrm{A} = [-a_{ij}]^{i=1,\dots,n}_{j=1,\dots,m}$. $\square$

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:

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

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

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 $\{\lambda_k\}_{k=1,\dots,n} \subset \mathbb{K}$ and $\{\mathbf{v}_k\}_{k=1,\dots,n} \subset V$, their **linear combination** is:

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

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:

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

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 $\cdot : \mathbb{K} \times U \to U$. $\square$

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 $\mathbf{v} \in V_1 \cap V_2 \implies \mathbf{v} \in V_1 \wedge \mathbf{v} \in V_2$. $\square$

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 expression 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)
$\{1, x, \ldots, x^n, \ldots\}$ 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 $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ 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 $\lambda_1 \mathbf{v}_1 + \cdots + \lambda_n \mathbf{v}_n = \mathbf{0}$ and $\lambda_n \neq 0$, then $\mathbf{v}_n$ is a linear combination of $\{\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}\}$

Proof. Respectively:

a. $S \subseteq T \implies \mathbf{v} \in T \; \forall \mathbf{v} \in S$, hence $\{\mathbf{v}_i\}_{i=1,\ldots,n} \subset S$ LD $\implies \{\mathbf{v}_i\}_{i=1,\ldots,n} \subset T$ 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 $\{\mathbf{v}_j\}_{j=1,\ldots,n}$ LD, then by definition $\exists \{\lambda_j\}_{j=1,\ldots,n} \subset \mathbb{K} - \{0\} : \sum_{j=1}^n \lambda_j \mathbf{v}_j = \mathbf{0}$, 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. $\{\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{w}\}$ LD $\implies \exists \lambda_1, \ldots, \lambda_n, \alpha \in \mathbb{K} - \{0\} : \sum_{j=1}^n \lambda_j \mathbf{v}_j + \alpha \mathbf{w} = \mathbf{0}$, so $\mathbf{w}$ can be isolated as $\mathbf{w} = -\alpha^{-1} \sum_{j=1}^n \lambda_j \mathbf{v}_j$

f. $\sum_{j=1}^n \lambda_j \mathbf{v}_j = \mathbf{0} \wedge \lambda_n \neq 0 \implies \mathbf{v}_n = -\lambda_n^{-1} \sum_{j=1}^{n-1} \lambda_j \mathbf{v}_j$

$\square$

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:

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

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. □

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 the thesis.

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

□

§1.3 Linear applications

§1.4 Inner products

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. $\square$

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 $\mathbb{Z}_n \equiv \mathbb{Z}/(\mathrm{mod}\, n)$, which in general is $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

Index