Linear algebra

1. | Matrices

Linear systems

Definition 1. A *linear equation* is an equation of the form

$$a_1x_1 + \cdots + a_nx_n = b$$

where $x_1, \ldots, x_n$ are the *variables* or *unknowns* and $a_i, b \in \mathbb{R}$, $i = 1, \ldots, n$, are the coefficients of the equation. The term b is usually called *constant term*.

Definition 2. A *system of linear equations* is a collection of one or more linear equations involving the same set of variables.

Definition 3. Let

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

be a system of linear equations. A *solution of a system of equations* is a set of numbers $c_1, \ldots, c_n$ such that

$$a_{i1}c_1 + \cdots + a_{in}c_n = b_i$$

for $i = 1, \ldots, m$. A linear system may behave in three possible ways:

1. The system has a unique solution.
2. The system has infinitely many solutions.
3. The system has no solution.

Definition 4. Two systems of equations are *equivalent* if they have the same solutions.

Matrices

Definition 5 (Matrix). A *matrix* $\mathbf{A}$ with coefficients in $\mathbb{R}$ is a table of real numbers arranged in rows and columns. That is, $\mathbf{A}$ is of the form:

$$\mathbf{A} = (a_{ij}) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

for some values $a_{ij} \in \mathbb{R}$, $i = 1, \ldots, m$ and $j = 1, \ldots, n$. The set of $m \times n$ matrices with real coefficients is denoted by $\mathcal{M}_{m\times n}(\mathbb{R})$[1].

Definition 6. Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and $\alpha \in \mathbb{R}$. If $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{ij})$, we define the *sum* $\mathbf{A} + \mathbf{B}$ as:

$$\mathbf{A} + \mathbf{B} = (a_{ij} + b_{ij})$$

We define the *product* $\alpha\mathbf{A}$ as:

$$\alpha\mathbf{A} = (\alpha a_{ij})$$

[1] In the case when $m = n$ we will denote $\mathcal{M}_{n\times n}(\mathbb{R})$ by $\mathcal{M}_n(\mathbb{R})$.

Proposition 7 (Properties of addition and scalar multiplication of matrices). The following properties are satisfied:

1. Commutativity:
$$\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$$
for all $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{R})$.
2. Associativity:
$$(\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$$
for all $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathcal{M}_{m\times n}(\mathbb{R})$.
3. Additive identity element: $\exists \mathbf{0} \in \mathcal{M}_{m\times n}(\mathbb{R})$ such that
$$\mathbf{A} + \mathbf{0} = \mathbf{A}$$
for all $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$.
4. Additive inverse element: $\forall \mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})\ \exists (-\mathbf{A}) \in \mathcal{M}_{m\times n}(\mathbb{R})$ such that
$$\mathbf{A} + (-\mathbf{A}) = \mathbf{0}$$
5. Distributivity:
$$(\alpha + \beta)\mathbf{A} = \alpha\mathbf{A} + \beta\mathbf{A}$$
for all $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and all $\alpha, \beta \in \mathbb{R}$.

Definition 8. Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and $\mathbf{B} \in \mathcal{M}_{n\times p}(\mathbb{R})$. We define the *product* $\mathbf{AB}$ as

$$\mathbf{AB} = (c_{ij}) \quad \text{where } c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

Proposition 9 (Properties of matrix product). The following properties are satisfied:

1. Associativity:
$$(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$$
for all $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$, $\mathbf{B} \in \mathcal{M}_{n\times p}(\mathbb{R})$ and $\mathbf{C} \in \mathcal{M}_{p\times q}(\mathbb{R})$.
2. Multiplicative identity element: $\exists \mathbf{I}_n \in \mathcal{M}_n(\mathbb{R})$ such that
$$\begin{aligned} \mathbf{A}\mathbf{I}_n &= \mathbf{A} \quad \forall \mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R}) \text{ and} \\ \mathbf{I}_n\mathbf{A} &= \mathbf{A} \quad \forall \mathbf{A} \in \mathcal{M}_{n\times p}(\mathbb{R}) \end{aligned}$$
3. Distributivity:
$$(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$$
for all $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{R})$ and $\mathbf{C} \in \mathcal{M}_{n\times p}(\mathbb{R})$.

Definition 10. We say that a matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ is *invertible* if there is a matrix $\mathbf{B} \in \mathcal{M}_n(\mathbb{R})$ satisfying

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n$$

The set of invertible matrices of size n over $\mathbb{R}$ is denoted by $\mathrm{GL}_n(\mathbb{R})$[2].

Lemma 11. The product of invertible matrices is invertible.

Definition 12. We say that a matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ is *idempotent* if $\mathbf{A}^2 = \mathbf{A}$.

Definition 13. We say that a matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ is *nilpotent* if $\mathbf{A}^k = \mathbf{0}_n$ for some $k \in \mathbb{N}$. The value k is usually called *index* of $\mathbf{A}$.

Lemma 14. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$ such that $\mathbf{A}$ is idempotent. Then, $\mathbf{A} = \mathbf{I}_n$.

Lemma 15. Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{R})$ such that $\mathbf{A}$ is nilpotent of index $k \in \mathbb{N}$. Then, $\mathbf{A} = \mathbf{0}_n$.

Echelon form of a matrix

Definition 16. Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. The *i-th pivot* of $\mathbf{A}$ is the first nonzero element in the i-th row of $\mathbf{A}$.

Definition 17 (Row echelon form). A matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ is in *row echelon form* if:

- All rows consisting of only zeros are at the bottom.
- The pivot of a nonzero row is always strictly to the right of the pivot of the row above it.

Definition 18 (Reduced row echelon form). A matrix $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ is in *reduced row echelon form* if:

- It is in row echelon form.
- Pivots are equal to 1.
- Each column containing a pivot has zeros in all its other entries.

Theorem 19 (Gauß' theorem). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. Then, there is a matrix $\mathbf{P} \in \mathrm{GL}_m(\mathbb{R})$ such that $\mathbf{PA} = \mathbf{A}'$ is in reduced row echelon form. Moreover, $\mathbf{A}'$ is uniquely determined by $\mathbf{A}$.

Theorem 20 (PAQ reduction theorem). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. Then, there exist matrices $\mathbf{P} \in \mathrm{GL}_m(\mathbb{R})$ and $\mathbf{Q} \in \mathrm{GL}_n(\mathbb{R})$ such that:

$$\mathbf{PAQ} = \left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right)$$

The number r is uniquely determined by $\mathbf{A}$.

Rank of a matrix

Definition 21 (Rank). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix and suppose

$$\mathbf{PAQ} = \left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right)$$

for some matrices $\mathbf{P} \in \mathcal{M}_m(\mathbb{R})$ and $\mathbf{Q} \in \mathcal{M}_n(\mathbb{R})$. We define the *rank* of $\mathbf{A}$, denoted by $\operatorname{rank}\mathbf{A}$, as the number ones in the matrix $\mathbf{PAQ}$, that is, $\operatorname{rank}\mathbf{A} := r$.

Proposition 22. Let $\mathbf{A}, \mathbf{A}' \in \mathcal{M}_{m\times n}(\mathbb{R})$, $\mathbf{B}, \mathbf{B}' \in \mathcal{M}_{1\times n}(\mathbb{R})$ and $\mathbf{P} \in \mathrm{GL}_m(\mathbb{R})$ be matrices. Suppose we have a system of linear equations $\mathbf{Ax} = \mathbf{B}$. If $\mathbf{P}(\mathbf{A} \mid \mathbf{B}) = (\mathbf{A}' \mid \mathbf{B}')$[3], then the systems $\mathbf{Ax} = \mathbf{B}$ and $\mathbf{A}'\mathbf{x} = \mathbf{B}'$ are equivalent.

Corollary 23. The reduced row echelon form of an invertible matrix is the identity matrix.

Definition 24 (Transposition). Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. If $\mathbf{A} = (a_{ij})$, we define the *transpose* $\mathbf{A}^{\mathrm{T}}$ of $\mathbf{A}$ as the matrix $\mathbf{A}^{\mathrm{T}} = (b_{ij})$, where $b_{ij} = a_{ji}$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$.

Proposition 25. Let $\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{R})$ be a matrix. Then, $\operatorname{rank}\mathbf{A} = \operatorname{rank}\mathbf{A}^{\mathrm{T}}$.

Theorem 26 (Rouché-Frobenius theorem). Let $\mathbf{Ax} = \mathbf{B}$ be a system of equations with n variables. The system is:

- *determined and consistent* if and only if
$$\operatorname{rank}\mathbf{A} = \operatorname{rank}(\mathbf{A} \mid \mathbf{B}) = n$$
- *indeterminate* with *s free variables* if and only if
$$\operatorname{rank}\mathbf{A} = \operatorname{rank}(\mathbf{A} \mid \mathbf{B}) = n - s$$
- *inconsistent* if and only if
$$\operatorname{rank}\mathbf{A} \neq \operatorname{rank}(\mathbf{A} \mid \mathbf{B})$$

Determinant of a matrix

Definition 27 (Determinant). A determinant is a function $\det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ satisfying the following properties:

1. If $\mathbf{A} = (\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_n)$, where $\mathbf{a}_i$ are column vectors in $\mathbb{R}^n$ for $i = 1, \ldots, n$ and $\mathbf{a}_j = \lambda\mathbf{u} + \mu\mathbf{v}$ for some other column vectors $\mathbf{u}$ and $\mathbf{v}$, then:
$$\begin{aligned} \det\mathbf{A} = \det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_j \mid \cdots \mid \mathbf{a}_n) &= \\ = \det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_{j-1} \mid \lambda\mathbf{u} + \mu\mathbf{v} \mid \mathbf{a}_{j+1} \mid \cdots \mid \mathbf{a}_n) &= \\ = \lambda\det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_{j-1} \mid \mathbf{u} \mid \mathbf{a}_{j+1} \mid \cdots \mid \mathbf{a}_n) &+ \\ + \mu\det(\mathbf{a}_1 \mid \cdots \mid \mathbf{a}_{j-1} \mid \mathbf{v} \mid \mathbf{a}_{j+1} \mid \cdots \mid \mathbf{a}_n) \end{aligned}$$
2. The determinant changes its sign whenever two columns are swapped.
3. $\det\mathbf{I}_n = 1$ for all $n \in \mathbb{N}$.

Lemma 28. Whenever two columns of a matrix are identical, the determinant is 0.

[2] Or more generally, the set of invertible matrices of size n over a field (see ??) K is denoted by $\mathrm{GL}_n(K)$.
[3] Here $(\mathbf{A} \mid \mathbf{B})$ denotes the augmented matrix obtained by appending the columns of $\mathbf{B}$ to the columns of $\mathbf{A}$.

Proposition 29. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a matrix in its row echelon form. If $\mathbf{A} = (a_{ij})$, then:

$$\det \mathbf{A} = \prod_{i=1}^{n} a_{ii}$$

Proposition 30. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a matrix. The following are equivalent:

1. $\mathbf{A}$ is not invertible.
2. $\operatorname{rank} \mathbf{A} < n$.
3. $\det \mathbf{A} = 0$.

Theorem 31. Let $\det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ be a determinant. Then, for all matrices $\mathbf{A}, \mathbf{B} \in \mathcal{M}_n(\mathbb{R})$:

$$\det(\mathbf{AB}) = \det \mathbf{A} \det \mathbf{B}$$

Corollary 32. Let $\det, \det' : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ be two determinants. Then, for all matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$:

$$\det \mathbf{A} = \det{}' \mathbf{A}$$

Proposition 33. Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$. Then:

$$\det \mathbf{A} = \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

Proposition 34. For all matrix $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$:

$$\det \mathbf{A} = \det \mathbf{A}^{\mathrm{T}}$$

Proposition 35. Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$. We denote by $\mathbf{A}_{ij}$ the square matrix obtained from $\mathbf{A}$ by removing the i-th row and j-th column. Then, for every $i \in \{1, \ldots, n\}$:

$$\det \mathbf{A} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det \mathbf{A}_{ij}$$

Definition 36. Let $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$. We define the *cofactor matrix* $\mathbf{C}$ of $\mathbf{A}$ as:

$$\mathbf{C} = (b_{ij}), \quad \text{where } b_{ij} = (-1)^{i+j} \det \mathbf{A}_{ij}{}^{4}$$

We define the *adjugate matrix* $\operatorname{adj} \mathbf{A}$ of $\mathbf{A}$ as:

$$\operatorname{adj} \mathbf{A} = \mathbf{C}^{\mathrm{T}}$$

Theorem 37. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. Then:

$$\mathbf{A} \operatorname{adj} \mathbf{A} = (\det \mathbf{A}) \mathbf{I}_n$$

Moreover if $\det \mathbf{A} \neq 0$, then:

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \operatorname{adj} \mathbf{A}$$

Block matrices

Definition 38. Let $\mathbf{A} \in \mathcal{M}_{m \times n}(\mathbb{R})$ and $r, s \in \mathbb{N}$ such that $r \leq m$ and $s \leq n$. We define a *block matrix* as a matrix of the form

$$\begin{pmatrix} \mathbf{A}_{11} & \cdots & \mathbf{A}_{1s} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{r1} & \cdots & \mathbf{A}_{rs} \end{pmatrix}$$

where $\mathbf{A}_{ij}$, $i = 1, \ldots, r$ and $j = 1, \ldots, s$ are submatrices of $\mathbf{A}$ created from partitioning the $\mathbf{A}$ with $s-1$ vertical lines and $r-1$ horizontal lines.

Proposition 39. Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m \cdot n}(\mathbb{R})$ be a block matrix of the form:

$$\mathbf{A} = \begin{pmatrix} \mathbf{X} & \mathbf{0} \\ \mathbf{Z} & \mathbf{Y} \end{pmatrix} \quad \mathbf{B} = \begin{pmatrix} \mathbf{X} & \mathbf{W} \\ \mathbf{0} & \mathbf{Y} \end{pmatrix}$$

where $\mathbf{X} \in \mathcal{M}_m(\mathbb{R})$, $\mathbf{Y} \in \mathcal{M}_n(\mathbb{R})$, $\mathbf{Z} \in \mathcal{M}_{n \times m}(\mathbb{R})$ and $\mathbf{W} \in \mathcal{M}_{m \times n}(\mathbb{R})$. Then,

$$\det \mathbf{A} = \det(\mathbf{X}) \det(\mathbf{Y}) = \det \mathbf{B}$$

2. | Vector spaces

Introduction and basic definitions

Definition 40. A *vector space* over a field[5] K is a set V together with two operations

$$\begin{aligned} + : V \times V &\longrightarrow V \\ (\mathbf{v}_1, \mathbf{v}_2) &\longmapsto \mathbf{v}_1 + \mathbf{v}_2 \end{aligned} \qquad \begin{aligned} \cdot : K \times V &\longrightarrow V \\ (\lambda, \mathbf{v}_2) &\longmapsto \lambda \cdot \mathbf{v}_2 \end{aligned}$$

that satisfy the following properties:

1. $\mathbf{v}_1 + (\mathbf{v}_2 + \mathbf{v}_3) = (\mathbf{v}_1 + \mathbf{v}_2) + \mathbf{v}_3 \quad \forall \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in V$.
2. $\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_2 + \mathbf{v}_1 \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$.
3. $\exists \mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v} \quad \forall \mathbf{v} \in V$.
4. $\forall \mathbf{v} \in V$ there exists $-\mathbf{v} \in V$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.
5. $\lambda \cdot (\mu \cdot \mathbf{v}) = (\lambda\mu) \cdot \mathbf{v} \quad \forall \mathbf{v} \in V$ and $\forall \lambda, \mu \in K$.
6. $1 \cdot \mathbf{v} = \mathbf{v} \quad \forall \mathbf{v} \in V$, where 1 denotes the multiplicative identity element in K.
7. $\lambda \cdot (\mathbf{v}_1 + \mathbf{v}_2) = \lambda \cdot \mathbf{v}_1 + \lambda \cdot \mathbf{v}_2 \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$ and $\forall \lambda \in K$.
8. $(\lambda + \mu) \cdot \mathbf{v} = \lambda \cdot \mathbf{v} + \mu \cdot \mathbf{v} \quad \forall \mathbf{v} \in V$ and $\forall \lambda, \mu \in K$.

In these conditions, we say that $(V, +, \cdot)$ is a vector space[6]. The elements of V are called *vectors* and the elements of K, *scalars*.

Definition 41. Let V be a vector space over a field K and $U \subseteq V$ be a subset of V. Then, U is a vector space over K if the following property is satisfied:

$$\lambda \mathbf{u}_1 + \mu \mathbf{u}_2 \in U \quad \forall \mathbf{u}_1, \mathbf{u}_2 \in U \text{ and } \forall \lambda, \mu \in K$$

Definition 42. Let V be a vector space and $U \subseteq V$. U is a *vector subspace* of V if it's itself a vector space with the operations defined in V.

[4] $\mathbf{C}$ is usually denoted as cof $\mathbf{A}$.
[5] See **??**.
[6] For simplicity we will denote the vector space only by V and if the context is clear we won't refer to its associated field. Moreover sometimes we will also omit the product $\cdot$ between a scalar and a vector.

Definition 43. Let V be a vector space over a field K. A *linear combination* of the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ is a vector of the form

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$$

where $a_i \in K$, $i = 1, \dots, n$.

Definition 44. Let V be a vector space over a field K and $U \subseteq V$. The set

$$\langle U \rangle = \{a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n : a_i \in K, \mathbf{u}_i \in U, i = 1, \dots, n\}$$

is called *linear span* by U.

Lemma 45. Let V be a vector space and $U \subseteq V$. Then, $\langle U \rangle$ is a vector subspace of V. Moreover, $\langle U \rangle$ is the smallest subspace containing U.

Definition 46. Let V be a vector space and $U \subseteq V$. We say that U is a *generating set* of V if $\langle U \rangle = V$.

Linear independence

Definition 47. Let V be a vector space over a field K. The vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ are *linearly independent* if the unique solution of the equation

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = 0$$

for $a_i \in K$, $i = 1, \dots, n$, is $a_1 = \cdots = a_n = 0$. Otherwise we say that the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are *linearly dependent*.

Lemma 48. Let V be a vector space. The vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly dependent if and only if one of them is a linear combination of the others.

Definition 49. Let V be a vector space. A *basis* of V is an ordered set $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ of vectors of V such that:

1. $\langle \mathbf{v}_1, \dots, \mathbf{v}_n \rangle = V$.
2. $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linearly independent.

Lemma 50 (Steinitz exchange lemma). Let V be a vector space, $\mathcal{B}$ be bases of V be and $\mathbf{v}_1, \dots, \mathbf{v}_k \in V$ be linearly independent vectors of V. Then, we can exchange k appropriate vectors of $\mathcal{B}$ by $\mathbf{v}_1, \dots, \mathbf{v}_k$ to define a new basis.

Corollary 51. Let V be a vector space that has a finite basis $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$. Then, all basis of V be are finite and they have the same number (n) of vectors.

Lemma 52. Let V be a vector space. Suppose we have a generating set $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ of V. Then, V be admits a basis formed with a subset of S.

Definition 53. Let V be a finite vector space over a field K. The *dimension* of V, denoted by $\dim_K V$ (or $\dim V$ if K can be inferred from context), is the number of vectors in any basis of V.

Definition 54. Let V be a finite vector space over a field K, $\mathcal{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ be a basis of V be and $\mathbf{v} \in V$. Suppose

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$$

for some $a_i \in K$, $i = 1, \dots, n$. We call $(a_1, \dots, a_n) \in K^n$ *coordinates* of $\mathbf{v}$ on the basis $\mathcal{B}$ and we denote it by $[\mathbf{v}]_{\mathcal{B}}$.

Proposition 55. Let V be a vector space. If $\dim V < \infty$, the maximum number of linearly independent vectors is equal to $\dim V$. If $\dim V = \infty$, there is no such maximum.

Proposition 56. Let V be a vector space of dimension n. Then, n is the minimum size of a generating set of V.

Proposition 57. Let V be a finite vector space and U be a vector subspace of V. Then, $\dim U \leq \dim V$ and

$$\dim U = \dim V \iff U = V$$

Sum of subspaces

Lemma 58. Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. Then, the intersection $U \cap W$ is a vector subspace of V.

Definition 59. Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. The *sum* of U and W is:

$$U + W = \langle U \cup W \rangle = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U, \mathbf{w} \in W\}$$

Proposition 60 (Graßmann formula). Let V be a finite vector space and $U, W \subseteq V$ be two vector subspace of V. Then:

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W$$

Lemma 61. Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. Then, $U \cap W = \{0\}$ if and only if all vectors $\mathbf{v} \in U + W$ can be written uniquely as $\mathbf{v} = \mathbf{u} + \mathbf{w}$, with $\mathbf{u} \in U$ and $\mathbf{w} \in W$.

Definition 62 (Direct sum). Let V be a vector space and $U, W \subseteq V$ be two vector subspaces of V. Then, the sum $U + W$ is *direct* if $U \cap W = \{0\}$. In this case we denote the sum as $U \oplus W$. More generally, if $U_1, \dots, U_n \subseteq V$ are vector subspaces of V, the sum $U = U_1 + \cdots + U_n$ is direct if all vector $\mathbf{u} \in U$ can be written uniquely as $\mathbf{u} = \mathbf{u}_1 + \cdots + \mathbf{u}_n$, where $\mathbf{u}_i \in U_i$ for $i = 1, \dots, n$. In this case we denote the sum by $U_1 \oplus \cdots \oplus U_n$.

Rank of a matrix

Definition 63. Let $\mathbf{A} \in \mathcal{M}_{n \times m}(\mathbb{R})$. The *row rank* of $\mathbf{A}$ is the dimension of the linear span of the rows of $\mathbf{A}$ in $\mathbb{R}^m$. Analogously, the *column rank* of $\mathbf{A}$ is the dimension of the linear span of the columns of $\mathbf{A}$ in $\mathbb{R}^n$.

Proposition 64. Let $\mathbf{A} \in \mathcal{M}_{n \times m}(\mathbb{R})$. Then, the row rank of $\mathbf{A}$ is equal to the column rank of $\mathbf{A}$. Therefore, we refer to it simply as *rank* of $\mathbf{A}$ or rank $\mathbf{A}$.

Definition 65. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$. A *minor* of order k of $\mathbf{A}$ is a submatrix $\mathbf{A}' \in \mathcal{M}_k(\mathbb{R})$ obtained from $\mathbf{A}$ selecting k rows and k columns of $\mathbf{A}$.

Proposition 66. Let $\mathbf{A} \in \mathcal{M}_{n \times m}(\mathbb{R})$. Then:

$$\operatorname{rank} \mathbf{A} = \max\{k : \mathbf{A} \text{ has an invertible minor of order } k\}$$

Quotient vector space

Definition 67. Let V be a vector space and $U \subseteq V$ be a vector subspace. We say that $W \subseteq V$ is a *complementary subspace* of U if $U \oplus W = V$.

Definition 68. Let V be a finite vector space of dimension n and $U \subseteq V$ be a vector subspace of dimension m. Then, there exists a complementary subspace of U and its dimension is $n - m$.

Definition 69. Let V be a vector space and $U \subseteq V$ be a vector subspace. We say the vectors $\mathbf{v}_1, \mathbf{v}_2 \in V$ are *equivalent* modulo U, $\mathbf{v}_1 \sim_U \mathbf{v}_2$, if $\mathbf{v}_1 - \mathbf{v}_2 \in U$.

Lemma 70. Let V be a vector space and $U \subseteq V$ be a vector subspace. Then, $\sim_U$ is an equivalence relation and, moreover, if $\mathbf{v} \in V$ the *equivalence class* $[\mathbf{v}]$ of $\mathbf{v}$ is:

$$[\mathbf{v}] = \mathbf{v} + U := \{\mathbf{v} + \mathbf{u} : \mathbf{u} \in U\}$$

Definition 71. Let V be a vector space over a field K and $U \subseteq V$ be a vector subspace. We define the *quotient space* V/U under $\sim_U$ as the set of equivalence classes with the operations defined as:

$$[\mathbf{v}_1] + [\mathbf{v}_2] = [\mathbf{v}_1 + \mathbf{v}_2] \qquad \lambda[\mathbf{v}_1] = [\lambda \mathbf{v}_1]$$

for all $\mathbf{v}_1, \mathbf{v}_2 \in V$ and all $\lambda \in K$.

Proposition 72. Let V be a vector space over a field K and $U \subseteq V$ be a vector subspace. The set V/U together with the two operations defined above is a vector space over K.

Proposition 73. Let V be a finite vector space of dimension n and $U \subseteq V$ be a vector subspace. Then:

$$\dim \left({}^{V}\!/\!_{U}\right) = \dim V - \dim U$$

3. | Linear maps

Definition 74. Let U, V be two vector spaces over a field K. A function $f : U \to V$ is a *linear map* if $\forall \mathbf{u}_1, \mathbf{u}_2 \in U$ and $\forall \lambda \in K$ the following two conditions are satisfied:

1. $f(\mathbf{u}_1 + \mathbf{u}_2) = f(\mathbf{u}_1) + f(\mathbf{u}_2)$.
2. $f(\lambda \mathbf{u}_1) = \lambda f(\mathbf{u}_1)$.

Proposition 75. Let U, V be two vector spaces over a field K. Then, if $f : U \to V$ is a linear map, $\forall \mathbf{u}_1, \mathbf{u}_2 \in U$ and $\forall \lambda, \mu \in K$ we have:

1. $f(\mathbf{0}) = \mathbf{0}$.
2. $f(-\mathbf{u}_1) = -f(\mathbf{u}_1)$.
3. $f(\lambda \mathbf{u}_1 + \mu \mathbf{u}_2) = \lambda f(\mathbf{u}_1) + \mu f(\mathbf{u}_2)$.

Proposition 76. Let U, V, W be three vector spaces. If $f : U \to V$ and $g : V \to W$ are linear maps, then $g \circ f : U \to W$ is a linear map.

Proposition 77. Let U, V be two vector spaces. If $f : U \to V$ is a bijective linear map, then $f^{-1} : U \to V$ is a linear map.

Proposition 78. Let U, V be two vector spaces, $f : U \to V$ be a linear map and $W \subseteq U$ and $Z \subseteq V$ be vector subspaces. Then:

1. $f(W) = \{f(\mathbf{w}) : \mathbf{w} \in W\} \subseteq V$ is a vector subspace.
2. $f^{-1}(Z) = \{\mathbf{u} \in U : f(\mathbf{u}) \in Z\} \subseteq U$ is a vector subspace.

In particular, $f(V)$ is denoted by $\operatorname{im} f$ and $f^{-1}(\{0\})$ is denoted by $\ker f$ and these subspaces are called *image* of f and *kernel* of f, respectively. More precisely, their definitions are:

$$\operatorname{im} f = \{f(\mathbf{u}) : \mathbf{u} \in U\} \qquad \ker f = \{\mathbf{u} \in U : f(\mathbf{u}) = 0\}$$

Proposition 79. Let U, V be two vector spaces and $f : U \to V$ be a linear map. Then:

1. f is injective $\iff \ker f = \{0\}$
2. f is surjective $\iff \operatorname{im} f = V$.

Corollary 80. Let U, V be two finite vector spaces and $f : U \to V$ be a linear map. Then:

1. f is injective $\iff \dim(\ker f) = 0$
2. f is surjective $\iff \dim(\operatorname{im} f) = \dim V$.

Definition 81.

- A monomorphism is an injective linear map.
- An epimorphism is a surjective linear map.
- An isomorphism is a bijective linear map.
- An endomorphism is a linear map from a vector space to itself.
- An automorphism is a bijective endomorphism.

Definition 82. We say that two vector spaces U and V are *isomorphic*, $V \cong U$, if there exists an isomorphism between them.

Proposition 83. Let U, V be two vector spaces and $f : U \to V$ be a monomorphism. If $\mathbf{u}_1, \ldots, \mathbf{u}_n \in U$ are linearly independent vectors, then $f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n)$ are linearly independent.

Lemma 84. Let U, V be two vector spaces and $f : U \to V$ be a linear map. If $\mathbf{u}_1, \ldots, \mathbf{u}_n \in U$, then:

$$\langle f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n) \rangle = f(\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle)$$

Corollary 85. Let U, V be two vector spaces and $f : U \to V$ be an epimorphism. If $\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle = U$, then $\langle f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n) \rangle = V$.

Corollary 86. Let U, V be two vector spaces and $f : U \to V$ be an isomorphism. If $(\mathbf{u}_1, \ldots, \mathbf{u}_n)$ is a basis of U, then $(f(\mathbf{u}_1), \ldots, f(\mathbf{u}_n))$ is a basis of V.

Theorem 87 (Coordination theorem). Let V be a finite vector space over a field K of dimension n and $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V. Then, the function $f : K^n \to V$ defined by

$$f(a_1, \ldots, a_n) = a_1 \mathbf{v}_1 + \cdots a_n \mathbf{v}_n$$

is an isomorphism.

Corollary 88. Two finite vector spaces are isomorphic if and only if they have the same dimension.

Isomorphism theorems

Theorem 89 **(First isomorphism theorem).** Let U, V be two vector spaces and $f : U \to V$ be a linear map. Then, there exists an isomorphism $\tilde{f} : U/\ker f \to \operatorname{im} f$ satisfying $f = \tilde{f} \circ \pi$, where $\pi : U \to U/\ker f$, $\pi(\mathbf{u}) = [\mathbf{u}]$.

$$\begin{tikzcd} U \arrow[r, "f"] \arrow[d, "\pi"'] & \operatorname{im} f \\ U\big/\ker f \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

Figure 1

Corollary 90. Let U, V be two vector spaces such that $\dim U = n$ and let $f : U \to V$ be a linear map. Then:

$$\dim(\ker f) + \dim(\operatorname{im} f) = n$$

Corollary 91. Let U, V be two finite vector spaces of dimensions n and $f : U \to V$ be a linear map. Then:

$$f \text{ is injective} \iff f \text{ is surjective} \iff f \text{ is bijective}$$

Theorem 92 **(Second isomorphism theorem).** Let V be a vector space and $U, W \subseteq V$ be two vector subspaces. Then, there exists an isomorphism

$$U\big/U \cap W \cong U + W\big/W$$

Theorem 93 **(Third isomorphism theorem).** Let U, V, W be three vector spaces such that $W \subseteq U \subseteq V$. Then, there exists an isomorphism

$$(V/W)\big/(U/W) \cong V\big/U$$

Theorem 94. Let U, V be two vector spaces over a field K, $\mathcal{B} = (\mathbf{u}_1, \ldots, \mathbf{u}_n)$ be a basis of U and $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ be any vectors of V. Then, there exists a unique linear map $f : U \to V$ such that $f(\mathbf{u}_i) = \mathbf{v}_i$, $i = 1, \ldots, n$.

Matrix of a linear map

Proposition 95. Let U, V be two finite vector spaces over a field K with $\dim U = n$ and $\dim V = m$, $\mathcal{B}$ and $\mathcal{B}'$ be bases of U be and V respectively and $f : U \to V$ be a linear map. Then, there exists a matrix $\mathbf{A} \in \mathcal{M}_{m \times n}(K)$ such that $\forall \mathbf{u} \in U$:

$$[f(\mathbf{u})]_{\mathcal{B}'} = \mathbf{A}[\mathbf{u}]_{\mathcal{B}}$$

The matrix $\mathbf{A}$ is called *matrix* of f in the basis $\mathcal{B}$ and $\mathcal{B}'$ and it is denoted by $[f]_{\mathcal{B},\mathcal{B}'}$[7].

Corollary 96. Let V be a finite vector space, $\mathcal{B}$ and $\mathcal{B}'$ be two basis of V respectively and $\mathrm{id} : V \to V$ be the identity linear map. Then, $\forall \mathbf{u} \in V$ we have:

$$[\mathbf{u}]_{\mathcal{B}'} = [\mathrm{id}]_{\mathcal{B},\mathcal{B}'}[\mathbf{u}]_{\mathcal{B}}$$

The matrix $[\mathrm{id}]_{\mathcal{B},\mathcal{B}'}$ is called *change-of-basis matrix.*

Proposition 97. Let U, V, W be three vector spaces, $\mathcal{B}$, $\mathcal{B}'$, $\mathcal{B}''$ be bases of U, V and W respectively and $f : U \to V$ and $g : V \to W$ be linear maps. Then, $g \circ f : U \to W$ has the following matrix in the basis $\mathcal{B}$ and $\mathcal{B}''$:

$$[g \circ f]_{\mathcal{B},\mathcal{B}''} = [g]_{\mathcal{B}',\mathcal{B}''}[f]_{\mathcal{B},\mathcal{B}'}$$

Corollary 98. Let V be a finite vector space, $\mathcal{B}$ and $\mathcal{B}'$ be two basis of V. Then, the matrix $[id]_{\mathcal{B},\mathcal{B}'}$ is invertible and

$$([\mathrm{id}]_{\mathcal{B},\mathcal{B}'})^{-1} = [\mathrm{id}]_{\mathcal{B}',\mathcal{B}}$$

Corollary 99. Let U, V be two finite vector spaces, $\mathcal{B}$ and $\mathcal{B}'$ be bases of U and V respectively and $f : U \to V$ be a linear map. Then:

1. f is injective $\iff \operatorname{rank}[f]_{\mathcal{B},\mathcal{B}'} = \dim U$.
2. f is surjective $\iff \operatorname{rank}[f]_{\mathcal{B},\mathcal{B}'} = \dim V$.

Corollary 100. Let U, V be two finite vector spaces. A linear map $f : U \to V$ is an isomorphism if and only if there exist basis $\mathcal{B}$ and $\mathcal{B}'$ of U and V respectively such that $[f]_{\mathcal{B},\mathcal{B}'}$ is invertible.

Proposition 101 **(Change of basis formula).** Let U, V be two finite vector spaces, $\mathcal{B}_1$ and $\mathcal{B}_2$ be bases of U, $\mathcal{B}_1'$ and $\mathcal{B}_2'$ be bases of V and $f : U \to V$ be a linear map. Then:

$$[f]_{\mathcal{B}_2,\mathcal{B}_2'} = [\mathrm{id}]_{\mathcal{B}_1',\mathcal{B}_2'}[f]_{\mathcal{B}_1,\mathcal{B}_1'}[\mathrm{id}]_{\mathcal{B}_2,\mathcal{B}_1}$$

Lemma 102. Let U, V be two finite vector spaces over a field K with $\dim U = n$ and $\dim V = m$ and $\mathcal{B}$ and $\mathcal{B}'$ be bases of U be and V respectively. Then, any matrix $\mathbf{A} \in \mathcal{M}_{m \times n}(K)$ determines a linear map $f : U \to V$ with $[f]_{\mathcal{B},\mathcal{B}'} = \mathbf{A}$.

Theorem 103. Let U, V be two finite vector spaces and $f : U \to V$ be a linear map. Then, there exist basis $\mathcal{B}$ of U and $\mathcal{B}'$ of V such that:

$$[f]_{\mathcal{B},\mathcal{B}'} = \left(\begin{array}{c|c} \mathbf{I}_r & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right)$$

where $r = \dim(\operatorname{im} f)$.

Dual space

Lemma 104. Let U, V be two finite vector spaces over a field K. Then, the set

$$\mathcal{L}(U, V) := \{f : f \text{ is a linear map from } U \text{ to } V\}^{8}$$

is a vector space over K with the operations defined as:

1. $(f + g)(\mathbf{u}) = f(\mathbf{u}) + f(\mathbf{u}) \quad \forall f, g \in \mathcal{L}(U, V)$ and $\forall \mathbf{u} \in U$.
2. $(f\lambda)(\mathbf{u}) = \lambda f(\mathbf{u}) \quad \forall f, g \in \mathcal{L}(U, V)$, $\forall \mathbf{u} \in U$ and $\forall \lambda \in K$.

[7] If $U = V$ and $\mathcal{B} = \mathcal{B}'$, we denote $[f]_{\mathcal{B},\mathcal{B}}$ simply by $[f]_{\mathcal{B}}$.
[8] If $U = V$, we denote $\mathcal{L}(V, V)$ simply as $\mathcal{L}(V)$.

Proposition 105. Let U, V be two finite vector spaces over a field K with $\dim U = n$ and $\dim V = m$. Then, for all basis $\mathcal{B}$ of U be and $\mathcal{B}'$ of V, the function

$$\begin{aligned} \mathcal{L}(U,V) &\longrightarrow \mathcal{M}_{m\times n}(K) \\ f &\longmapsto [f]_{\mathcal{B},\mathcal{B}'} \end{aligned}$$

is an isomorphism.

Corollary 106. Let U, V be two finite vector spaces with $\dim U = n$, $\dim V = m$. Then, $\dim \mathcal{L}(U,V) = nm$.

Definition 107. Let V be a vector space over a field K. We define the *dual space* V^* of V as:

$$V^* := \mathcal{L}(V,K)$$

Proposition 108. Let V be a finite vector space over a field K with $\dim V = n$ and $\mathcal{B}$ be a basis of V. Then, the function

$$\begin{aligned} V^* &\longrightarrow \mathcal{M}_{1\times n}(K) \\ \omega &\longmapsto [\omega]_{\mathcal{B},1} \end{aligned}$$

is an isomorphism. Therefore, $\dim V^* = \dim V$.

Definition 109. We define the *Kronecker delta* δ_{ij} as the function:

$$\delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

Definition 110. Let V be a finite vector space and $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V. We define the *dual basis* $\mathcal{B}^*$ of $\mathcal{B}$ as the basis of V^* formed by $(\eta_1, \ldots, \eta_n)$ where

$$\eta_i(\mathbf{v}_j) = \delta_{ij}$$

Lemma 111. Let V be a vector space over a field K, $\mathcal{B}$ be a basis of V and $(\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*)$ be the dual basis of $\mathcal{B}$. Then, $\forall \mathbf{v} \in V$:

$$[\mathbf{v}]_{\mathcal{B}} = (\mathbf{v}_1^*(\mathbf{v}), \ldots, \mathbf{v}_n^*(\mathbf{v})) \in K^n$$

Lemma 112. Let V be a vector space over a field K, $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\mathcal{B}^*$ be the dual basis of $\mathcal{B}$. Then, $\forall \omega \in V^*$:

$$[\omega]_{\mathcal{B}^*} = (\omega(\mathbf{v}_1), \ldots, \omega(\mathbf{v}_n)) \in K^n$$

Definition 113 (Dual map). Let U, V be two vector spaces over a field K and $f \in \mathcal{L}(U,V)$. The function f^* defined by

$$\begin{aligned} f^* : U^* &\longrightarrow V^* \\ \omega &\longmapsto \omega \circ f \end{aligned}$$

is a linear map and it's called *dual map* of f.

Theorem 114. Let U, V be two finite vector spaces, $\mathcal{B}$ and $\mathcal{B}'$ be bases of U and V respectively and $f \in \mathcal{L}(U,V)$. Then:

$$[f^*]_{\mathcal{B}'^*,\mathcal{B}^*} = \left([f]_{\mathcal{B},\mathcal{B}'}\right)^{\mathrm{T}}$$

Double dual space

Definition 115 (Double dual space). Let V be a vector space over a field K. The *double dual space* V^{**} of V is defined as:

$$V^{**} := (V^*)^* = \mathcal{L}(V^*, K)$$

Proposition 116. Let V be a vector space over a field K and $\mathbf{v} \in V$. We define the function:

$$\begin{aligned} \phi_{\mathbf{v}} : V^* &\longrightarrow K \\ \omega &\longmapsto \omega(\mathbf{v}) \end{aligned}$$

which is linear. This map induces an injective linear map Φ defined by:

$$\begin{aligned} \Phi : V &\longrightarrow V^{**} \\ \mathbf{v} &\longmapsto \phi_{\mathbf{v}} \end{aligned}$$

Moreover, if $\dim V < \infty$, Φ is a natural isomorphism[9].

Annihilator space

Definition 117. Let V be a vector space and $U \subseteq V^*$ be a vector subspace of V^*. We define the *annihilator* of U as:

$$U^0 = \{\mathbf{v} \in V : \omega(\mathbf{v}) = 0 \ \forall \omega \in U\}$$

Lemma 118. Let V be a vector space and $U \subseteq V^*$ be a vector subspace of V^*. If $U = \langle \omega_1, \ldots, \omega_n \rangle$, then U^0 is the set of solutions of the system:

$$\begin{cases} \omega_1(\mathbf{v}) = 0 \\ \quad\vdots \\ \omega_n(\mathbf{v}) = 0 \end{cases}$$

Lemma 119. Let V be a vector space and $U \subseteq V^*$ be a vector subspace of V^*. Then, U^0 is a vector subspace of V^*.

Theorem 120. Let V be a finite vector space and $U \subseteq V^*$ be a vector subspace of V^*. Then:

$$\dim U^0 + \dim U = \dim V$$

Definition 121. Let V be a vector space and $U \subseteq V$ be a vector subspace of V. We define the *annihilator* of U as:

$$U^0 = \{\omega \in V^* : \omega(\mathbf{v}) = 0 \ \forall \mathbf{v} \in U\}$$

Lemma 122. Let V be a vector space and $U \subseteq V$ be a vector subspace of V. If $U = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$, then:

$$U^0 = \{\omega \in V^* : \omega(\mathbf{v}_1) = \cdots = \omega(\mathbf{v}_n) = 0\}$$

Proposition 123. Let V be a vector space. Then, whether $U \subseteq V$ or $U \subseteq V^*$, we have:

$$\left(U^0\right)^0 = U$$

4. | Classification of endomorphisms

Definition 124. Let V be a vector space over a field K and $\lambda \in K$. A *homothety* of ratio λ is a linear map $f : V \to V$ such that $f(\mathbf{v}) = \lambda \mathbf{v} \ \forall \mathbf{v} \in V$.

[9] This means that the definition of Φ does not depend on a choice of basis.

Similarity

Definition 125. Let V be a vector space and $f, g \in \mathcal{L}(V)$. We say that f and g are *similar* if there are basis $\mathcal{B}$ and $\mathcal{B}'$ of V such that $[f]_{\mathcal{B}} = [g]_{\mathcal{B}'}$.

Lemma 126. Let V be a vector space, $\mathcal{B}$ and $\mathcal{B}'$ basis of V and $f \in \mathcal{L}(V)$. If $\mathbf{M} = [f]_{\mathcal{B}}$, $\mathbf{N} = [f]_{\mathcal{B}'}$ and $\mathbf{P} = [\mathrm{id}]_{\mathcal{B},\mathcal{B}'}$, then:

$$\mathbf{M} = \mathbf{P}^{-1}\mathbf{N}\mathbf{P}$$

Definition 127. Let K be a field. Two matrices $\mathbf{M}, \mathbf{N} \in \mathcal{M}_n(K)$ are *similar* if there exists a matrix $\mathbf{P} \in \mathrm{GL}_n(K)$ such that $\mathbf{M} = \mathbf{P}^{-1}\mathbf{N}\mathbf{P}$.

Proposition 128. Let V be a finite vector space and $f, g \in \mathcal{L}(V)$.

1. f and g are similar if and only if for all basis $\mathcal{B}$ of V the matrices $[f]_{\mathcal{B}}$ and $[g]_{\mathcal{B}}$ are similar.
2. f and g are similar if and only if there is an automorphism $h \in \mathcal{L}(V)$ such that $g = h^{-1}fh$.

Diagonalization

Definition 129. Let K be a field. A matrix $\mathbf{A} = (a_{ij}) \in \mathcal{M}_n(K)$ is *diagonal* if $a_{ij} = 0$ whenever $i \neq j$. That is, $\mathbf{A}$ is of the form:

$$\mathbf{A} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

In this case, we denote $\mathbf{A} := \mathrm{diag}(a_{11}, \ldots, a_{nn})$.

Definition 130. Let K be a field. A matrix $\mathbf{A} \in \mathcal{M}_n(K)$ is *diagonalizable* if it is similar to diagonal matrix.

Definition 131. An endomorphism is *diagonalizable* if its associated matrix in some basis is diagonalizable.

Definition 132. Let V be a vector space over a field K and $f \in \mathcal{L}(V)$. We say that a nonzero vector $\mathbf{v} \in V$ is an *eigenvector* of f with eigenvalue $\lambda \in K$ if $f(\mathbf{v}) = \lambda\mathbf{v}$.

Lemma 133. Let V be a vector space over a field K, $f \in \mathcal{L}(V)$ and $\lambda \in K$. The eigenvectors of f of eigenvalue λ are the nonzero vectors of the subspace $\ker(f - \lambda\mathrm{id})$, called *eigenspace* corresponding to λ.

Lemma 134. Let V be a vector space over a field K with $\dim V = n$, $\mathcal{B}$ be a basis of V and $f \in \mathcal{L}(V)$. Then, $\det([f - x\mathrm{id}]_{\mathcal{B}})$ is a polynomial on the variable x of degree n and with coefficients in K. Moreover, the dominant coefficient is $(-1)^n$ and the constant term is $\det([f]_{\mathcal{B}})$.

Corollary 135. Let V be a vector space of dimension n and $f \in \mathcal{L}(V)$. Then, f has at most n distinct eigenvalues.

Corollary 136. Let V be a vector space over $\mathbb{C}$ and $f \in \mathcal{L}(V)$. Then, f has at least one eigenvalue.

Definition 137. Let K be a field and $\mathbf{A} \in \mathcal{M}_n(K)$. The polynomial $p_{\mathbf{A}}(\lambda) = \det(\mathbf{A} - \lambda\mathbf{I}_n)$ is called *characteristic polynomial* of $\mathbf{A}$.

Proposition 138. Let V be a vector space and $f \in \mathcal{L}(V)$. For all basis $\mathcal{B}$ of V, the characteristic polynomial of $[f]_{\mathcal{B}}$ is the same. Therefore, we denote it $p_f(\lambda)$ and we refer to it as *characteristic polynomial* of f.

Proposition 139. Let V be a vector space and $f \in \mathcal{L}(V)$. Then, eigenvectors of f of distinct eigenvalues are linearly independent.

Corollary 140. Let V be a vector space and $f \in \mathcal{L}(V)$. Suppose $\lambda_1, \ldots, \lambda_n$ are the distinct eigenvalues of f and $V_{\lambda_1}, \ldots, V_{\lambda_n}$ are their corresponded eigenspaces. Then,

$$V_{\lambda_1} + \cdots + V_{\lambda_n}$$

is a direct sum.

Proposition 141. Let V be a finite vector space of dimension n, $f \in \mathcal{L}(V)$ and λ be a root of multiplicity m of the characteristic polynomial $p_f(x)$. Then:

$$1 \leq \dim(\ker(f - \lambda\mathrm{id})) \leq m$$

The number m is called *algebraic multiplicity* of λ, whereas the value $\dim(\ker(f - \lambda\mathrm{id}))$ is called *geometric multiplicity* of λ.

Theorem 142 (Diagonalization theorem). Let V be a finite vector space and $f \in \mathcal{L}(V)$. f is diagonalizable if and only if:

1. $p_f(x) = (-1)^n(x - \lambda_1)^{m_1} \cdots (x - \lambda_k)^{m_k}$ with distinct $\lambda_1, \ldots, \lambda_k \in K$.
2. $\dim(\ker(f - \lambda_i\mathrm{id})) = m_i$, $i = 1, \ldots, k$.

Corollary 143. Let V be a finite vector space with $\dim V = n$ and $f \in \mathcal{L}(V)$. If f has n distinct eigenvalues, f is diagonalizable.

Proposition 144. Let V be a finite vector space and $f, g \in \mathcal{L}(V)$ such that f and g are similar. Then:

$$f \text{ is diagonalizable} \iff g \text{ is diagonalizable}$$

Lemma 145. Let K be a field and $\mathbf{A}, \mathbf{B} \in \mathcal{M}_n(K)$ be similar matrices. Then, $\forall k \in \mathbb{N}$, $\mathbf{A}^k$ and $\mathbf{B}^k$ are similar.

Lemma 146. Let V be a finite vector space over a field K with $\dim V = n$ and $f \in \mathcal{L}(V)$. Then, the function $\phi_f : K[x] \to \mathcal{L}(V)$ defined by

$$\phi_f(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1f + \cdots + a_nf^n$$

is linear and satisfies:

$$\phi_f((pq)(x)) = \phi_f(p(x))\phi_f(q(x)) \quad \forall p(x), q(x) \in K[x]$$

Definition 147. Let V be a finite vector space with $\dim V = n$ and $f \in \mathcal{L}(V)$. The *minimal polynomial* $m_f(x) \in K[x]$ of f is the unique a polynomial satisfying:

- $m_f(f) = 0$.
- m_f is monic.
- m_f is of minimum degree.

Proposition 148. Let V be a vector space over a field K and $f \in \mathcal{L}(V)$. If $p(x) \in K[x]$ is such that $p(f) = 0$, then $m_f(x) \mid p(x)$.

Cayley-Hamilton theorem

Theorem 149 (Cayley-Hamilton theorem). Let K be a field, $n \geq 1$ and $\mathbf{A} \in \mathcal{M}_n(K)$. Then:

$$m_{\mathbf{A}}(x) \mid p_{\mathbf{A}}(x) \mid m_{\mathbf{A}}(x)^n$$

Therefore $p_{\mathbf{A}}(\mathbf{A}) = 0$ and $m_{\mathbf{A}}(x)$ and $p_{\mathbf{A}}(x)$ have the same irreducible factors.

Corollary 150. Let K be a field and $\mathbf{A} \in \mathrm{GL}_n(K)$ be a matrix with $p_{\mathbf{A}}(x) = a_0 + a_1 x + \cdots + (-1)^n x^n$. Then:

$$\mathbf{A}^{-1} = -\frac{1}{a_0}\left(\mathbf{A}^{n-1} + a_{n-1}\mathbf{A}^{n-2} + \cdots + a_2\mathbf{A} + a_1\mathbf{I}_n\right)$$

Lemma 151. Let V be a finite vector space over a field K, $\mathcal{B}$ be a basis of V and $f \in \mathcal{L}(V)$. Then $\forall \lambda, \mu \in K$ and $\forall r, s \in \mathbb{N}$:

1. $[f^r]_{\mathcal{B}} = ([f]_{\mathcal{B}})^r$.
2. $[\lambda f]_{\mathcal{B}} = \lambda [f]_{\mathcal{B}}$.
3. $[\lambda f^r + \mu f^s]_{\mathcal{B}} = [\lambda f^r]_{\mathcal{B}} + [\mu f^s]_{\mathcal{B}}$.

Lemma 152. Let V be a finite vector space over a field K, $f \in \mathcal{L}(V)$ and $\mathbf{v}$ be an eigenvector of f of eigenvalue λ. Then, $\forall p(x) \in K[x]$ we have:

$$p(f)(\mathbf{v}) = p(\lambda)\mathbf{v}$$

Theorem 153 (Cayley-Hamilton theorem). Let V be a finite vector space over a field K such that $\dim V = n$ and $f \in \mathcal{L}(V)$. Then:

$$m_f(x) \mid p_f(x) \mid m_f(x)^n$$

Definition 154. A field K satisfying that all polynomial with coefficient in K of degree greater o equal to 1 factorizes as a product of linear factors is called an *algebraically closed field*.

Definition 155. Let V be a vector space and $f \in \mathcal{L}(V)$. We say that $U \subseteq V$ is an *invariant subspace* of V under f if $f(U) \subseteq U$.

Lemma 156. Let V be a vector space and $f \in \mathcal{L}(V)$.

1. If $U \subseteq V$ is an invariant subspace of V under f, then:
$$p_{f|_U}(x) \mid p_f(x)$$ [10]
2. If U_1 and U_2 are invariant subspaces of V under f such that $V = U_1 \oplus U_2$, then:
   - $p_f(x) = p_{f|_{U_1}}(x) \cdot p_{f|_{U_2}}(x)$.
   - $m_f(x) = \mathrm{lcm}(m_{f|_{U_1}}(x), m_{f|_{U_2}}(x))$.

Lemma 157. Let V be a vector space, $f \in \mathcal{L}(V)$ and $a(x), b(x) \in K[x]$. Suppose $m(x) = \mathrm{lcm}(a(x), b(x))$ and $d(x) = \gcd(a(x), b(x))$. Then:

1. $\ker(a(f)) + \ker(b(f)) = \ker(m(f))$.
2. $\ker(a(f)) \cap \ker(b(f)) = \ker(d(f))$.

[10]Here $f|_U$ is the function f restricted to the subspace U.

In particular, if $a(x)$ and $b(x)$ are coprime and $a(f)b(f) = 0$, then:

$$V = \ker(a(x)) \oplus \ker(b(x))$$

Theorem 158. Let V be a finite vector space such that $\dim V = n$ and $f \in \mathcal{L}(V)$. If $p_f(x) = q_1(x)^{n_1} \cdots q_r(x)^{n_r}$ and $m_f(x) = q_1(x)^{m_1} \cdots q_r(x)^{m_r}$ with $q_i(x)$ distinct irreducible factors, then:

$$V = \ker(q_1(f)^{m_1}) \oplus \cdots \oplus \ker(q_r(f)^{m_r})$$

Moreover, $\dim\left(\ker(q_i(f)^{m_i})\right) = n_i \deg(q_i(x))$.

Jordan form

Definition 159. Let K be a field and $\mathbf{A} \in \mathcal{M}_n(K)$. A *Jordan block* of $\mathbf{A}$ is a square submatrix composed by a value $\lambda \in K$ on the principal diagonal, ones on the diagonal just below the principal diagonal and zeros elsewhere. That is, a Jordan block is a matrix of the form:

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \ddots & \vdots \\ 0 & 1 & \lambda & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \lambda \end{pmatrix}$$

A *Jordan matrix* is a block diagonal matrix whose blocks are Jordan blocks.

Proposition 160. Let V be a finite vector space over a field K with $\dim V = n$ and $f \in \mathcal{L}(V)$. If $p_f(x) = \pm(x-\lambda_1)^{n_1} \cdots (x-\lambda_k)^{n_k}$, there exists a basis $\mathcal{B}$ of V such that

$$[f]_{\mathcal{B}} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{J}_r \end{pmatrix}$$

where $\mathbf{J}_1, \ldots, \mathbf{J}_r$ are Jordan blocks associated with eigenvalues $\lambda_1, \ldots, \lambda_k$ satisfying:

1. For $i = 1, \ldots, k$, the sum of the sizes of Jordan blocks associated with the eigenvalue λ_i is n_i.
2. The sizes of Jordan blocks are determined by $\dim(\ker((f - \lambda_i \mathrm{id})^r))$, $r = 1, \ldots, n_i - 1$.

Proposition 161. Let V be a finite vector space over a field K with $\dim V = n$ and $\mathbf{A} \in \mathcal{M}_n(K)$. If $p_{\mathbf{A}}(x) = \pm(x-\lambda_1)^{n_1} \cdots (x-\lambda_k)^{n_k}$, there exist a matrix $\mathbf{P} \in \mathrm{GL}_n(K)$ such that:

$$\mathbf{J} := \mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \begin{pmatrix} \mathbf{J}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{J}_r \end{pmatrix}$$

where $\mathbf{J}_1, \ldots, \mathbf{J}_r$ are Jordan blocks associated with eigenvalues $\lambda_1, \ldots, \lambda_k$ satisfying Items 160-1 and 160-2 of Theorem 160. In that case, we say that $\mathbf{J}$ is the *Jordan form* of $\mathbf{A}$.

Theorem 162. Let V be a vector space and $f, g \in \mathcal{L}(V)$ be such that $p_f(x) = (x-\lambda_1)^{n_1} \cdots (x-\lambda_k)^{n_k}$. If g satisfies:

1. $p_f(x) = p_g(x)$
2. $m_f(x) = m_g(x)$
3. $\dim(\ker((f-\lambda \mathrm{id})^r)) = \dim(\ker((g-\lambda \mathrm{id})^r))$ $\forall \lambda \in K$ $\forall r \geq 1$

then f is similar to g.

5. | Symmetric bilinear forms

Basic definitions

Definition 163. Let U, V, W be three vector spaces over a field K. We say that a function $\varphi : U \times V \to W$ is *bilinear* if $\forall \mathbf{u}_1, \mathbf{u}_2, \mathbf{u} \in U$, $\forall \mathbf{v}_1, \mathbf{v}_2, \mathbf{v} \in V$ and $\forall \lambda \in K$ we have:

1. $\varphi(\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v}) = \varphi(\mathbf{u}_1, \mathbf{v}) + \varphi(\mathbf{u}_2, \mathbf{v})$.
2. $\varphi(\lambda \mathbf{u}, \mathbf{v}) = \lambda \varphi(\mathbf{u}, \mathbf{v})$.
3. $\varphi(\mathbf{u}, \mathbf{v}_1 + \mathbf{v}_2) = \varphi(\mathbf{u}, \mathbf{v}_1) + \varphi(\mathbf{u}, \mathbf{v}_2)$.
4. $\varphi(\mathbf{u}, \lambda \mathbf{v}) = \lambda \varphi(\mathbf{u}, \mathbf{v})$.

Definition 164. Let V be a vector space over a field K. A *bilinear form* from V onto K is a bilinear map $\varphi : V \times V \to K$.

Definition 165. Let V be a vector space over a field K. A bilinear form $\varphi : V \times V \to K$ is *symmetric* if

$$\varphi(\mathbf{v}_1, \mathbf{v}_2) = \varphi(\mathbf{v}_2, \mathbf{v}_1) \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$$

Matrix associated with a bilinear form

Definition 166. Let V be a finite vector space over a field K, $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. We define the *matrix of the bilinear form* φ with respect to the basis $\mathcal{B}$ as the matrix $[\varphi]_\mathcal{B} \in \mathcal{M}_n(K)$ defined as:

$$[\varphi]_\mathcal{B} = \begin{pmatrix} \varphi(\mathbf{v}_1, \mathbf{v}_1) & \varphi(\mathbf{v}_1, \mathbf{v}_2) & \cdots & \varphi(\mathbf{v}_1, \mathbf{v}_n) \\ \varphi(\mathbf{v}_2, \mathbf{v}_1) & \varphi(\mathbf{v}_2, \mathbf{v}_2) & \cdots & \varphi(\mathbf{v}_2, \mathbf{v}_n) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi(\mathbf{v}_n, \mathbf{v}_1) & \varphi(\mathbf{v}_n, \mathbf{v}_2) & \cdots & \varphi(\mathbf{v}_n, \mathbf{v}_n) \end{pmatrix}$$

Lemma 167. Let V be a finite vector space over a field K, $\mathcal{B}$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then:

$$\varphi(\mathbf{v}_1, \mathbf{v}_2) = ([\mathbf{v}_1]_\mathcal{B})^{\mathrm{T}} [\varphi]_\mathcal{B} [\mathbf{v}_2]_\mathcal{B} \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$$

Proposition 168. Let V be a finite vector space over a field K, $\mathcal{B}$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then:

$$\varphi \text{ is symmetric} \iff [\varphi]_\mathcal{B} \text{ is symmetric}$$

Proposition 169. Let V be a finite vector space over a field K, $\mathcal{B}$ and $\mathcal{B}'$ be bases of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then:

$$[\varphi]_{\mathcal{B}'} = ([\mathrm{id}]_{\mathcal{B}',\mathcal{B}})^{\mathrm{T}} [\varphi]_\mathcal{B} [\mathrm{id}]_{\mathcal{B}',\mathcal{B}}$$

Orthogonal basis

Definition 170. Let V be a finite vector space over a field K, $\varphi : V \times V \to K$ be a symmetric bilinear form and $\mathbf{v}_1, \mathbf{v}_2 \in V$.

- We say that $\mathbf{v}_1$ and $\mathbf{v}_2$ are *orthogonal* if $\varphi(\mathbf{v}_1, \mathbf{v}_2) = 0$.
- If $\mathbf{v}_1 \neq 0$, we say that $\mathbf{v}_1$ is *isotropic* if $\varphi(\mathbf{v}_1, \mathbf{v}_1) = 0$.

Definition 171. Let V be a finite vector space over a field K, $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form.

- We say that $\mathcal{B}$ is *orthogonal* with respect to φ if $\varphi(\mathbf{v}_i, \mathbf{v}_j) = 0$ $\forall i \neq j$.
- We say that $\mathcal{B}$ is *orthonormal* with respect to φ if $\varphi(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij}$.

Theorem 172. Let V be a finite vector space over a field K, $\mathcal{B}$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then, V has an orthogonal basis with respect to φ and an orthonormal basis with respect to φ.

Corollary 173. Let K be a field with $\operatorname{char} K \neq 2$ and $\mathbf{A} \in \mathcal{M}_n(K)$ be a symmetric matrix. Then, there exists a matrix $\mathbf{P} \in \mathrm{GL}_n(K)$ such that $\mathbf{P}^{\mathrm{T}} \mathbf{A} \mathbf{P}$ is diagonal.

Orthogonal decompositions

Definition 174. Let V be a finite vector space over a field K, $U \subseteq V$ be a vector subspace of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. We define the *orthogonal complement* of U as:

$$U^\perp = \{\mathbf{v} \in V : \varphi(\mathbf{v}, \mathbf{u}) = 0 \ \forall \mathbf{u} \in U\}$$

Definition 175. Let V be a finite vector space over a field K and $\varphi : V \times V \to K$ be a symmetric bilinear form. We define the *radical* of φ as:

$$\operatorname{rad} \varphi = V^\perp$$

We say that φ is *nonsingular* if $\operatorname{rad} \varphi = \{0\}$.

Definition 176. Let V be a finite vector space over a field K, $\varphi : V \times V \to K$ be a nonsingular symmetric bilinear form and $\mathbf{v}_0 \in V$. We define $\varphi_{\mathbf{v}_0} : V \to K$, $\varphi_{\mathbf{v}_0}(\mathbf{v}) = \varphi(\mathbf{v}_0, \mathbf{v})$. Then, the function

$$\begin{aligned} V &\longrightarrow V^* \\ \mathbf{v}_0 &\longmapsto \varphi_{\mathbf{v}_0} \end{aligned}$$

is an isomorphism.

Definition 177. Let V be a finite vector space over a field K, $U \subseteq V$ be a vector subspace of V and $\varphi : V \times V \to K$ be a nonsingular symmetric bilinear form. Then:

1. $\dim V = \dim U + \dim U^\perp$.
2. $(U^\perp)^\perp = U$.
3. If $\varphi|_U$ is nonsingular, then $V = U \oplus U^\perp$.

Definition 178. Let V be a finite vector space over a field K, $U_1, U_2 \subseteq V$ be vector subspaces of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. We say that the sum $U_1 + U_2$ is *orthogonal* if it is direct and $\varphi(\mathbf{u}_1, \mathbf{u}_2) = 0$ $\forall \mathbf{u}_1 \in U_1$ and $\mathbf{u}_2 \in U_2$. In this case, we denote $U_1 + U_2$ by $U_1 \perp U_2$.

Proposition 179. Let V be a finite vector space over a field K, $U_1, U_2 \subseteq V$ be vector subspaces of V such that $V = U_1 \perp U_2$ and $\varphi : V \times V \to K$ be a symmetric bilinear form. Then, $\forall \mathbf{v} \in V$ there exist unique $\mathbf{u}_1 \in U_1$ and $\mathbf{u}_2 \in U_2$ such that $\mathbf{v} = \mathbf{u}_1 + \mathbf{u}_2$.

Definition 180. Let V be a finite vector space over a field K, $U_1, U_2 \subseteq V$ be vector subspaces of V such that $V = U_1 \perp U_2$ and $\varphi : V \times V \to K$ be a symmetric bilinear form. The function

$$\begin{aligned} \pi : U_1 \perp U_2 &\longrightarrow U_i \\ \mathbf{u}_1 + \mathbf{u}_2 &\longmapsto \mathbf{u}_i \end{aligned}$$

for $i = 1, 2$ is called *orthogonal projection* of V onto U_i according to the decomposition $V = U_1 \perp U_2$.

Proposition 181 (Gram-Schmidt process). Let V be a finite vector space over a field K, $\mathcal{B} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ be a basis of V and $\varphi : V \times V \to K$ be a symmetric bilinear form. $\forall \mathbf{u}, \mathbf{v} \in V$, we define

$$\operatorname{proj}_{\mathbf{u}}(\mathbf{v}) = \frac{\varphi(\mathbf{u}, \mathbf{v})}{\varphi(\mathbf{u}, \mathbf{u})}\mathbf{u}$$

We will create an orthogonal basis $(\mathbf{u}_1, \ldots, \mathbf{u}_n)$ of V from $\mathcal{B}$. We define $\mathbf{u}_i$, $i = 1, \ldots, n$, to be:

$$\begin{aligned} \mathbf{u}_1 &= \mathbf{v}_1 \\ \mathbf{u}_2 &= \mathbf{v}_2 - \operatorname{proj}_{\mathbf{u}_1}(\mathbf{v}_2) \\ \mathbf{u}_3 &= \mathbf{v}_3 - \operatorname{proj}_{\mathbf{u}_1}(\mathbf{v}_3) - \operatorname{proj}_{\mathbf{u}_2}(\mathbf{v}_3) \\ &\vdots \\ \mathbf{u}_n &= \mathbf{v}_n - \sum_{i=1}^{n-1} \operatorname{proj}_{\mathbf{u}_i}(\mathbf{v}_n) \end{aligned}$$

To obtain an orthogonal basis $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ of V from $\mathcal{B}$, define $\mathbf{e}_i$, $i = 1, \ldots, n$, to be:

$$\mathbf{e}_i = \frac{\mathbf{u}_i}{\sqrt{\varphi(\mathbf{u}_i, \mathbf{u}_i)}}$$

Sylvester's law of inertia

Definition 182. An *orthogonal geometry* over a field K is a pair (V, φ), where V is a vector space over K and φ is a symmetric bilinear form over V.

Definition 183. Let (V_1, φ_1), (V_2, φ_2) be two orthogonal geometries over a field K. An *isometry* from (V_1, φ_1) to (V_2, φ_2) is an isomorphism $f : V_1 \to V_2$ such that

$$\varphi_2(f(\mathbf{u}), f(\mathbf{v})) = \varphi_1(\mathbf{u}, \mathbf{v}) \quad \forall \mathbf{u}, \mathbf{v} \in V_1$$

We say that (V_1, φ_1) and (V_2, φ_2) are *isometric* if there exists an isometry between them.

Definition 184. Let V be a vector space over a field K and φ_1, φ_2 be symmetric bilinear forms. We say that φ_1 and φ_2 are *equivalent* if (V, φ_1) and (V, φ_2) are isometric.

Definition 185. Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_n(\mathbb{R})$. We say that $\mathbf{A}$ and $\mathcal{B}$ are congruent if there exists a matrix $\mathbf{P} \in \mathrm{GL}_n(\mathbb{R})$ such that

$$\mathbf{A} = \mathbf{P}^{\mathrm{T}}\mathbf{B}\mathbf{P}$$

Proposition 186. Let V be a finite vector space over a field K, $\mathcal{B}_1$ be a basis of V and φ_1, φ_2 be symmetric bilinear forms. Then the following statements are equivalent:

1. The orthogonal geometries (V, φ_1) and (V, φ_2) are isometric.
2. There exists a basis $\mathcal{B}_2$ of V such that $[\varphi_1]_{\mathcal{B}_1} = [\varphi_2]_{\mathcal{B}_2}$.
3. The matrices $[\varphi_1]_{\mathcal{B}_1}$ and $[\varphi_2]_{\mathcal{B}_2}$ are congruent.

Theorem 187 (Sylvester's law of inertia). Let V be a finite vector space over $\mathbb{R}$ and φ be a symmetric bilinear form over V. Then, there exists a basis $\mathcal{B}$ of V such that:

$$[\varphi]_{\mathcal{B}} = \operatorname{diag}\left(0, \overset{(r_0)}{\ldots}, 0, 1, \overset{(r_+)}{\ldots}, 1, -1, \overset{(r_-)}{\ldots}, -1\right)$$

where in the diagonal there are r_0 zeros, r_+ ones and r_- minus ones and the triplet (r_0, r_+, r_-) doesn't depend on the basis $\mathcal{B}$.

Definition 188. Let V be a finite vector space over $\mathbb{R}$ and φ be a symmetric bilinear form over V. Let $\mathcal{B}$ be an orthogonal basis of V with respect to φ. We define the *rank* of φ as:

$$\operatorname{rank}\varphi = \operatorname{rank}([\varphi]_{\mathcal{B}})$$

We define the *signature* of φ as:

$$\operatorname{sig}\varphi = (r_+, r_-)$$

where r_+ is el number of positive real numbers on the diagonal of $[\varphi]_{\mathcal{B}}$ and r_- is el number of negative real numbers on the diagonal of $[\varphi]_{\mathcal{B}}$.

Theorem 189. Let (V_1, φ_1), (V_2, φ_2) be two orthogonal geometries over $\mathbb{R}$ of finite dimension. Then, (V_1, φ_1) and (V_2, φ_2) are isometric if and only if $\dim V_1 = \dim V_2$ and $\operatorname{sig}\varphi_1 = \operatorname{sig}\varphi_2$.

Inner products

Definition 190. Let V be a finite vector space over $\mathbb{R}$ and φ be a symmetric bilinear form over V. We say that φ is *positive-definite* if

$$\varphi(\mathbf{v}, \mathbf{v}) > 0 \quad \forall \mathbf{v} \in V \setminus \{0\}$$

We say that φ is *negative-definite* if

$$\varphi(\mathbf{v}, \mathbf{v}) < 0 \quad \forall \mathbf{v} \in V \setminus \{0\}$$[11]

Definition 191. Let V be a vector space over $\mathbb{R}$. An *inner product* over V is a positive-definite symmetric bilinear form over V.

[11] The terms *positive-semidefinite* and *negative-semidefinite* are used when $\forall \mathbf{v} \in V \setminus \{0\}$, $\varphi(\mathbf{v}, \mathbf{v}) \geq 0$ or $\varphi(\mathbf{v}, \mathbf{v}) \leq 0$, respectively.

Definition 192. An *Euclidean vector space* is a pair (V, φ), where V is a vector space over $\mathbb{R}$ and φ is an inner product over V.

Theorem 193 (Cauchy-Schwarz inequality). Let (V, φ) be an Euclidean vector space. Then:

$$\varphi(\mathbf{v}_1, \mathbf{v}_2)^2 \leq \varphi(\mathbf{v}_1, \mathbf{v}_1)\varphi(\mathbf{v}_2, \mathbf{v}_2) \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$$

Definition 194. Let V be a vector space over $\mathbb{R}$. A *norm* on V is a function

$$\begin{aligned} \|\cdot\| : V &\longrightarrow \mathbb{R} \\ \mathbf{v} &\longmapsto \|\mathbf{v}\| \end{aligned}$$

such that:

1. $\|\mathbf{v}\| = 0 \iff \mathbf{v} = \mathbf{0}\ \forall \mathbf{v} \in V$.
2. $\|\lambda \mathbf{v}\| = |\lambda|\|\mathbf{v}\|$, $\forall \mathbf{v} \in V$, $\lambda \in \mathbb{R}$.
3. $\|\mathbf{v}_1 + \mathbf{v}_2\| \leq \|\mathbf{v}_1\| + \|\mathbf{v}_2\|$, $\forall \mathbf{v}_1, \mathbf{v}_2 \in V$[12].

Proposition 195. Let (V, φ) be an Euclidean vector space. Then, the function

$$\begin{aligned} \|\cdot\|_\varphi : V &\longrightarrow \mathbb{R} \\ \mathbf{v} &\longmapsto \sqrt{\varphi(\mathbf{v}, \mathbf{v})} \end{aligned}$$

is a norm called *norm associated with the inner product* φ.

Definition 196. Let (V, φ) be an Euclidean vector space and $\mathbf{v}_1, \mathbf{v}_2 \in V \setminus \{0\}$. We define the *angle* with respect to φ between $\mathbf{v}_1$ and $\mathbf{v}_2$ as the unique $\theta \in [0, \pi]$ such that:

$$\cos\theta = \frac{\varphi(\mathbf{v}_1, \mathbf{v}_2)}{\|\mathbf{v}_1\|_\varphi \|\mathbf{v}_2\|_\varphi}$$

Spectral theorem

Definition 197. Let (V, φ) be a finite Euclidean vector space and $f \in \mathcal{L}(V)$. Then, there exists a unique $f' \in \mathcal{L}(V)$ such that

$$\varphi(f(\mathbf{v}_1), \mathbf{v}_2) = \varphi(\mathbf{v}_1, f'(\mathbf{v}_2)) \quad \forall \mathbf{v}_1, \mathbf{v}_2 \in V$$

This f' is called *adjoint* of f.

Definition 198. Let (V, φ) be a finite Euclidean vector space and $f \in \mathcal{L}(V)$. f is called *auto-adjoint* if $f = f'$.

Lemma 199. Let (V, φ) be a finite Euclidean vector space of dimension n and $f \in \mathcal{L}(V)$ be auto-adjoint. Then, there exist $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ such that

$$p_f(x) = (x - \lambda_1) \cdots (x - \lambda_n)$$

Definition 200. Let K be a field and $A \in \mathrm{GL}_n(K)$ be a matrix. We say that A is *orthogonal* if

$$\mathbf{P}\mathbf{P}^{\mathrm{T}} = \mathbf{P}^{\mathrm{T}}\mathbf{P} = \mathbf{I}_n$$

The set of orthogonal matrices of size n over K is denoted by $\mathcal{O}_n(K)$.

Theorem 201 (Spectral theorem). Let (V, φ) be a finite Euclidean vector space and $f \in \mathcal{L}(V)$ be auto-adjoint. Then, V has an orthonormal basis of eigenvectors of f. In particular, f diagonalizes.

Corollary 202. Let K be a field. All symmetric matrices $A \in \mathcal{M}_n(K)$ are diagonalizable. More precisely, there exists $\mathbf{P} \in \mathcal{O}_n(K)$ such that $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P}$ is diagonal.

Definition 203. Let $A = (a_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{C})$. We define the *complex conjugate* $\overline{\mathbf{A}}$ of $\mathbf{A}$ as $\overline{\mathbf{A}} = (\overline{a_{ij}})$.

Proposition 204. Let $\mathbf{A}, \mathbf{B} \in \mathcal{M}_{m\times n}(\mathbb{C})$, $\mathbf{C} \in \mathcal{M}_{n\times p}(\mathbb{C})$ and $\lambda \in \mathbb{C}$. Then:

1. $\overline{\mathbf{A} + \mathbf{B}} = \overline{\mathbf{A}} + \overline{\mathbf{B}}$.
2. $\overline{\mathbf{A}\mathbf{C}} = \overline{\mathbf{A}} \cdot \overline{\mathbf{C}}$.
3. $\overline{\lambda \cdot \mathbf{A}} = \overline{\lambda} \cdot \overline{\mathbf{A}}$.

Corollary 205. Let $\mathbf{A} \in \mathcal{M}_n(\mathbb{R})$ be a symmetric matrix. Then, there exist $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ such that

$$p_{\mathbf{A}}(x) = (x - \lambda_1) \cdots (x - \lambda_n)$$

Theorem 206 (Descartes' rule of signs). Let $P(x) = a_0 + \cdots + a_n x^n \in \mathbb{R}[x]$:

1. The number of positive roots of $P(x)$ is at most equal to the number of sign variations in the sequence $[a_d, a_{d-1}, \ldots, a_1, a_0]$.
2. If $P(x) = a_n(x - \alpha_1)^{n_1} \cdots (x - \alpha_r)^{n_r}$, then the number of positive roots of $P(x)$ is equal to the number of sign variations in the sequence (having in account multiplicity).

[12] Note that $\forall \mathbf{v} \in V$ we have: $0 = \|\mathbf{v} + (-\mathbf{v})\| \leq \|\mathbf{v}\| + \|-\mathbf{v}\| = 2\|\mathbf{v}\| \implies \|\mathbf{v}\| \geq 0$.