- Given a set A, an **n-tuple** over A is a function $f: [n] \longrightarrow A$

- A **vector space** is a quadruple $(V, F, +, \cdot)$, such that
  1. V is a non-empty set, called vectors;
  2. F is a numeric field;
  3. $+$ is a binary operation that satisfies
     - **Commutativity**: $\forall u, v \in V,\ u+v = v+u$
     - **Associativity**: $\forall u, v, w \in V,\ (u+v)+w = u+(v+w)$
     - **Neutral element**: $\forall u \in V,\ u+0 = u$, sendo 0 o elemento neutro
     - **Inverse**: $\forall u, \exists w,\ u+w = 0$
  4. $\cdot$ is an operator that associates $v \in V$ with a escalar $a \in F$, such that it satisfies
     - **Associativity**: $\forall \alpha, \beta \in F$ and $u \in V,\ (\alpha\beta)u = \alpha(\beta u)$
     - **Neutral element**: $\forall u \in V,\ u \cdot 1 = u$
     - **Distributes over addition**: $\forall \alpha \in F$ and $\forall u, v \in V,\ \alpha(u+v) = \alpha u + \alpha v$
     - **Distributes over escalar addition**: $\forall \alpha, \beta \in F,\ \forall u \in V,\ u(\alpha+\beta) = u\alpha + u\beta$

Proposition: A vector space has a unique additive identity

Proposition: Every element in a vector space has unique additive inverse.

Proposition: $0v = 0$ for every $v \in V$.

Proposition: $\alpha 0 = 0$ for every $\alpha \in F$

Proposition: $(-1)v = -v$ for every $v \in V$

- A **subspace** U is a vector space, such that U is a subset of V, with V being another vector space that contains U and satisfies:
  1. additive identity $0 \in U$
  2. closed under addition $u, v \in U,\ u+v \in U$
  3. closed under scalar multiplication $\alpha \in F$ and $v \in U,\ \alpha \cdot v \in U$

- The **sum** of $U_1, \dots, U_m$, with U_i being a subspace of V, is the set all possible sums of elements of $U_1, \dots, U_m$:

$$U_1 + \dots + U_m = \{u_1 + \dots + u_m : u_1 \in U_1, \dots, u_m \in U_m\}$$

• A **direct sum** of subspaces $U_1, \dots, U_m$, written $U = U_1 \oplus \dots \oplus U_m$, is a sum $U = U_1 + \dots + U_m$, such that each element in U can be written uniquely as a sum $u_1 + \dots + u_m$, with $u_j \in U_j$.

Proposition: Let $U_1, \dots, U_n$ be subspaces of V. Then, $V = U_1 \oplus \dots \oplus U_n$ if and only if:

1. $V = U_1 + \dots + U_n$
2. $u_1 + \dots + u_n = 0$, if $\forall u_j \in U_j$, $u_j = 0$

Proposition Suppose that U and W are subspaces of V. Then, $V = U + W$ and $U \cap W = \{0\}$

• **Linear inpendent:** Consider a linear combination $a_1 v_1 + a_2 v_2 + \dots + a_m v_m$, with $a_1, \dots, a_m \in F$ and $v_1, \dots, v_m \in V$. We say it is **linear independent** if the only way that $a_1 v_1 + \dots + a_m v_m = 0$ is that $a_1 = a_2 = \dots = a_m = 0$.

• **span** is the set of all combinations of a list $(v_1, \dots, v_m)$ of V, such that $\text{span}(v_1, \dots, v_m) = \{a_1 v_1 + \dots + a_m v_m : a_1, \dots, a_m \in F\}$

Linear Dependence Lemma: If $(v_1, \dots, v_m)$ is linearly dependent in V and $v_1 \neq 0$, then there exists $j \in \{2, \dots, m\}$ such that the following hold:

1. $v_j \in \text{span}(v_1, \dots, v_{j-1})$;
2. If the j^{th} term is removed from $(v_1, \dots, v_m)$, the span of the remaining list equals $\text{span}(v_1, \dots, v_m)$.

Theorem: In a finite-dimensional vector space, the length of every linearly independent list of vectors is less than or equal to the length of every spanning list of vectors.

Proposition: Every subspace of a finite-dimension vector space is finite dimensional

• A **basis** of V, with V being a vector space, is a list of vectors in V that is **linearly independent** and **spans** V.

Proposition: A list $(v_1, \dots, v_n)$ of vectors in V is a basis of V if and only if every $v \in V$ can be written uniquely in the form

$$v = \alpha_1 v_1 + \cdots + \alpha_n v_n,$$

in which $\alpha_1, \ldots, \alpha_n \in F$.

Theorem: Every spanning list in a vector space can be reduced to a basis of the vector space.

Corollary: Every finite-dimensional vector space has a basis.

Theorem: Every linearly independent list of vectors in a finite-dimensional vector space can be extended to a basis of the vector space.

Proposition: Suppose V is finite dimensional and U is a subspace of V. Then there is a subspace W of V such that $V = U \oplus W$.

Theorem: Any two bases of a finite-dimensional vector space have the same length

Proposition: If V is finite dimensional and U is a subspace of V, then $\dim U \leq \dim V$.

Proposition: If V is finite dimensional, then every spanning list of vectors in V with length $\dim V$ is a basis of V.

Proposition: If V is finite dimensional, then every linearly independent list of vectors in V with length $\dim V$ is a basis of V.

Theorem: If U_1 and U_2 are subspaces of a finite-dimensional vector space, then

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$$

Proposition: Suppose V is finite dimensional and $U_1, \ldots, U_m$ are subspaces of V such that

$$V = U_1 + \cdots + U_m \quad \text{and} \quad \dim V = \dim U_1 + \cdots + \dim U_m$$

Then, $V = U_1 \oplus \cdots \oplus U_m$

- A **linear map** is a function $T: V \longrightarrow W$, such that
  1. $T(u+v) = Tu + Tv$, $\forall u, v \in V$;
  2. $T(\alpha v) = \alpha(Tv)$, $\forall \alpha \in F$ e $\forall v \in V$.

The set of all linear maps from V to W is $\mathcal{L}(V, W)$.

• The **null space** of T, for $T \in \mathcal{L}(V, W)$, is the subset of V consisting of those vectors that T maps to 0.

$$\text{null } T = \{v \in V : Tv = 0\}.$$

Proposition: If $T \in \mathcal{L}(V,W)$, then null T is a subspace of V

Proposition: Let $T \in \mathcal{L}(V,W)$. Then T is injective if and only if null $T = \{0\}$

Proposition: If $T \in \mathcal{L}(V,W)$, then range T is a subspace of W.

Theorem: If V is finite dimensional and $T \in \mathcal{L}(V,W)$, then range T is finite-dimensional subspace of W and

$$\dim V = \dim \text{null } T + \dim \text{range } T.$$

Corollary: If V and W are finite-dimensional vector spaces such that $\dim V > \dim W$, then no linear map from V to W is injective.

Corollary: If V and W are finite-dimensional vector spaces such that $\dim V < \dim W$, then no linear map from V to W is surjective

Theorem: The set of all linear transformations on a vector space is itself a vector space.

• An **m-by-n matrix** is a rectangular array with m rows and n columns, such like

$$\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}$$

• A **matrix of T** is represented by

$$\mathcal{M}(T, (v_1, \ldots, v_n), (w_1, \ldots, w_m))$$

in which $T \in \mathcal{L}(V,W)$, $(v_1, \ldots, v_n)$ is a basis of V and $(w_1, \ldots, w_m)$ is a basis of W. We have that, for each $k = 1, \ldots, n$,

$$Tv_k = a_{1,k} w_1 + \cdots + a_{m,k} w_m,$$

such that $a_{j,k} \in F$ for $j = 1, \dots, m$. However, we prefer to use the compact notation, such that $M(T)$ is Matriz of Linear Map.

- A linear map $T \in \mathcal{L}(V,W)$ is called **invertible** if there exists a linear map $S \in \mathcal{L}(W,V)$ such that $ST = I$ and $TS = I$. Then, S is the **inverse** of T.

Proposition: A linear map is invertible if and only if it is injective and surjective.

- Two vector spaces are called **isomorphic** if there is an invertible linear map from one vector space onto the other one.

Theorem: If A, B, C are linear transformations such that $AB = CA = I$, A is invertible and $A^{-1} = B = C$.

Theorem: A linear transformation A on a finite-dimensional vector space V is invertible if and only if $Ax = 0$ implis that $x = 0$, or, alternatively, if and only if V can be written in the form $y = Ax$.

Theorem: If A and B are invertible, then AB is invertible and $(AB)^{-1} = B^{-1}A^{-1}$. If A is invertible and $\alpha \neq 0$, then αA is invertible and $(\alpha A)^{-1} = \frac{1}{\alpha} A^{-1}$. If A is invertible, then A^{-1} is invertible and $(A^{-1})^{-1} = A$.

- A **matriz of a linear map** is an array n by n, such that each column represents the linear combination of Tv_k, in which $k = 1, \dots, n$. Therefore, let $T \in \mathcal{L}(V,W)$, $(v_1, \dots, v_n)$ is a basis of V and $(w_1, \dots, w_m)$, a basis of W. We have $\alpha_{j,k} \in F$, for $j = 1, \dots, m$ in

$$Tv_k = \alpha_{1,k} w_1 + \cdots + \alpha_{m,k} w_m,$$

which determines a **matriz of T** with respect to the bases $(v_1, \dots, v_n)$ and $(w_1, \dots, w_m)$ denoted by

$$M(T, (v_1, \dots, v_n), (w_1, \dots, w_m)) \quad \text{or (for short)} \quad M(T)$$

It means that each column represents a linear combination for Tv_k vector in W. Notice tha Tv_k spans W

Theorem: Among the set of all matrices (α_{ij}), (β_{ij}), etc, $i,j=1,\dots,n$, we define sum, scalar multiplication, product, o_{ij}, and e_{ij}, by

1. $(\alpha_{ij})+(\beta_{ij})=(\alpha_{ij}+\beta_{ij})$
2. $c(\alpha_{ij})=(c\,\alpha_{ij})$
3. $(\alpha_{ij})(\beta_{ij})=(\Sigma_k \alpha_{ik}\beta_{kj})$
4. $o_{ij}=0$
5. $e_{ij}=\delta_{ij}$ (Kronecker delta)

Proposition: Suppose $T\in\mathcal{L}(V,W)$ and $(v_1,\dots,v_n)$ is a basis of V and $(w_1,\dots,w_m)$ is a basis of W. Then

$$\mathcal{M}(Tv)=\mathcal{M}(T)\,\mathcal{M}(v)$$

- $\mathcal{M}(T+S)=\mathcal{M}(T)+\mathcal{M}(S)$
- $\mathcal{M}(cT)=c\,\mathcal{M}(T)$
- $\mathrm{Mat}(m,n,F)$ is a vector space and defined as the set of all m-by-n matrices with entries in F.
- $\mathcal{M}(TS)=\mathcal{M}(T)\,\mathcal{M}(S)$, in which $S:U\longrightarrow V$ and $T:V\longrightarrow W$. Notice that TS is a composition of linear maps and $\mathcal{M}(T)\,\mathcal{M}(S)$ is a multiplication of matrices.
- A matrix multiplication is an operation defined as

$$\begin{aligned} TSu_k &= T\Big(\sum_{r=1}^{n} b_{r,k}v_r\Big)\\ &=\sum_{r=1}^{n} b_{r,k}\,Tv_r\\ &=\sum_{r=1}^{n} b_{r,k}\sum_{j=1}^{m} a_{j,r}w_j\\ &=\sum_{j=1}^{m}\Big(\sum_{r=1}^{n} a_{j,r}b_{r,k}\Big)w_j, \text{ with } S:U\to V \text{ and } T:V\to W \end{aligned}$$

Therefore, $\mathcal{M}(TS)$ is the m-by-p matrix where entry in row j, column k equals $\sum_{r=1}^{n} a_{j,r}b_{r,k}$

! This operation is defined only when the number of columns of the first matrix equals the number of rows of the second matrix.

. The **matrix of** v is a matrix of the uniques scalars $b_1, \dots, b_n$ that spans v. Then, let $(v_1, \dots, v_n)$ a basis of V,

$$v = b_1 v_1 + \dots + b_n v_n,$$

such that $\mathcal{M}(v)$ or

$$\mathcal{M}(v, (v_1, \dots, v_n)) = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

- A **norm** of $x = (x_1, \dots, x_n)$ is defined as $\|x\| = \sqrt{\langle x, x \rangle}$
- A **dot product** of x and y is defined as $x \cdot y = x_1 y_1 + \dots + x_n y_n$

An inner product is a generalization of the dot product.

- An **inner product** on V is a function that takes each ordered pair (u, v) of elements of V to a number $\langle u, v \rangle \in F$ and follow the properties

1. **Positivity** $\langle v, v \rangle \geq 0, \quad \forall v \in V$
2. **Definiteness** $\langle v, v \rangle = 0 \iff v = 0$
3. **Additivity in first slot** $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
4. **Homogeneity in first slot** $\langle \alpha v, w \rangle = \alpha \langle v, w \rangle, \quad \forall \alpha \in F, \quad \forall v, w \in V$
5. **Conjugate symetry** $\langle v, w \rangle = \overline{\langle w, v \rangle}, \quad \forall v, w \in V$

- An **Euclidian inner product** is defined as an inner-product space is F^n, such that

$$\langle (w_1, \dots, w_n), (z_1, \dots, z_n) \rangle = w_1 \bar{z}_1 + \dots + w_n \bar{z}_n$$

- **Cauchy-Schwarz Inequality**: If $u, v \in V$, then

$$|\langle u, v \rangle| \leq \|u\| \, \|v\|$$

This inequality is an equality if and only if one of u, v is a scalar multiple of the other.

- **Triangle Inequality**: If $u, v \in V$, then

$$\|u, v\| \leq \|u\| + \|v\|$$

This inequality is an equality if and only if one of u, v is a scalar multiple of the other.

- **Parallelogram Equality**: If $u, v \in V$, then

$$\|u+v\|^2 + \|u-v\|^2 = 2(\|u\|^2 + \|v\|^2)$$

- An **Orthonormal bases** is a list of vectors, in which they are pair-wise orthogonal and each vector has norm 1. This means that for a list $(e_1, \dots, e_m)$ is orthonormal if $\langle e_j, e_k \rangle$ equals 0 when $j \neq k$ and equals 1 when $j = k$, for $j, k \in [1, \dots m]$.

Proposition: If $(e_1, \dots, e_m)$ is orthonormal list of vectors in V, then

$$\|a_1 e_1 + \dots + a_m e_m\|^2 = |a_1|^2 + \dots + |a_m|^2$$

for all $a_1, \dots, a_m \in F$.

Polynomials

- A function $p: F \longrightarrow F$ is called a polynomial if there exists $a_0, \dots, a_m \in F$ such that

$$p(z) = a_0 + a_1 z + a_2 z^2 + \dots + a_m z^m$$

- A polynomial p has **degree** m if

$$p(z) = a_0 + a_1 z + \dots + a_m z^m$$

and $a_m \neq 0$.

* If $a_0 = 0, \dots, a_m = 0$, then p has degree $-\infty$.

- $\mathcal{P}(F)$ is the vector space of all polynomials with coefficients in F.

- $\mathcal{P}_m(F)$ is the subspace of $\mathcal{P}(F)$ consisting of the polynomials with coefficients in F and degree at most m.

- $\lambda \in F$ is called a **root** of a polynomial $p \in \mathcal{P}(F)$ if $p(\lambda) = 0$.

Proposition: Suppose $p \in \mathcal{P}(F)$ is a polynomial with degree $m \geq 1$. Let $\lambda \in F$. Then λ is a root of p if and only if there is a polynomial $q \in \mathcal{P}(F)$ with degree $m-1$ such that

$$p(z) = (z - \lambda) q(z)$$

for all $z \in F$.

Corollary: Suppose $p \in \mathcal{P}(F)$ is a polynomial with degree $m \geq 0$. Then p has at most m distinct roots in F.

Corollary: Suppose $a_0, \dots, a_m \in F$. If

$$a_0 + a_1 z + a_2 z^2 + \dots + a_m z^m = 0$$

for all $z \in F$, then $a_0 = \dots = a_m = 0$.

Division Algorithm: Suppose $p, q \in \mathcal{P}(F)$, with $p \neq 0$. Then, there exist polynomials $s, r \in \mathcal{P}(F)$ such that

$$q = sp + r$$

and $\deg r < \deg p$

Fundamental Theorem of Algebra: Every nonconstant polynomial with complex coefficients has a root.

Corollary: If $p \in \mathcal{P}(\mathbb{C})$ is a nonconstant polynomial, then p has a unique factorization (except for the order of factors) of the form

$$p(z) = c(z-\lambda_1)\cdots(z-\lambda_m)$$

where $c, \lambda_1, \ldots, \lambda_m \in \mathbb{C}$.

Proposition: Suppose p is a polynomial with real coefficients. If $\lambda \in \mathbb{C}$ is a root of p, then so is $\bar{\lambda}$.

Proposition: Let $\alpha, \beta \in \mathbb{R}$. Then there is a polynomial factorization of the form

$$x^2 + \alpha x + \beta = (x-\lambda_1)(x-\lambda_2)$$

with $\lambda_1, \lambda_2 \in \mathbb{R}$, if and only if $\alpha^2 \geq 4\beta$.

Theorem: If $p \in \mathcal{P}(\mathbb{R})$ is a nonconstant polynomial, then p has a unique factorization (except for the order of factors) of the form

$$p(x) = c(x-\lambda_1)\ldots(x-\lambda_m)(x^2+\alpha_1 x+\beta_1)\ldots(x^2+\alpha_m x+\beta_m)$$