CS724: Topics in Algorithms
Linear Spaces
Slide Set 2

Prof. Dan A. Simovici

The Definition of Linear Spaces - I

Let $\mathbb{F}$ be the field of real numbers $\mathbb{R}$ or the field of complex numbers $\mathbb{C}$. An *$\mathbb{F}$-linear space* is a set L on which two operations are defined: the addition $\mathbf{x} + \mathbf{y}$ of elements $\mathbf{x}$ and $\mathbf{y}$ of L and the multiplication of an element $\mathbf{x}$ of L with a member a of $\mathbb{F}$, denoted by $a\mathbf{x}$, such that the following conditions are satisfied:

I. Additive Conditions:

- addition is associative, that is, $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$;
- addition is commutative, that is, $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$;
- for every $\mathbf{x} \in L$ there is an element $(-\mathbf{x})$ in L such that $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}_L$.

The Definition of Linear Spaces - II

II. Multiplicative Conditions:

- L contains an element $\mathbf{0}_L$ such that $0\mathbf{x} = \mathbf{0}_L$;
- $(a + b)\mathbf{x} = a\mathbf{x} + b\mathbf{x}$;
- $a(\mathbf{x} + \mathbf{y}) = a\mathbf{x} + a\mathbf{y}$;
- $(ab)\mathbf{x}) = a(b\mathbf{x})$;
- $1\mathbf{x} = \mathbf{x}$

for every $a, b \in F$ and $\mathbf{x}, \mathbf{y} \in L$.

The elements of the field $\mathbb{F}$ are referred to as *scalars* while the elements of L are referred to as *vectors*.

If the field $\mathbb{F}$ is irrelevant, or it is clearly designated from the context we refer to an $\mathbb{F}$-linear space just as a linear space. On another hand if $\mathbb{F}$ is the real field $\mathbb{R}$ or the complex field $\mathbb{C}$ we designate an $\mathbb{R}$-linear space as a *real linear space* and a $\mathbb{C}$-linear space as a *complex linear space*.

Example

If $\mathbb{F}$ is a field, then the one-element linear space $L = \{\mathbf{0}_L\}$, where $a\mathbf{0}_L = \mathbf{0}_L$ for every $a \in \mathbb{F}$ is the *zero $\mathbb{F}$-linear space*, or, for short, the *zero linear space*.
The field $\mathbb{F}$ itself is an $\mathbb{F}$-linear space, where the Abelian group is $(\mathbb{F}, \{0, +, -\})$ and scalar multiplication coincides with the scalar multiplication of $\mathbb{F}$.

Note that the zero $\mathbb{F}$-linear space is the smallest linear space.

Example

The set of all sequences of real numbers, $\mathbf{Seq}(\mathbb{R})$ is a real linear space, where the sum of two sequences $\boldsymbol{x} = (x_0, x_1, \ldots)$ and $\boldsymbol{y} = (y_0, y_1, \ldots)$ is the sequence $\boldsymbol{x} + \boldsymbol{y}$ defined by $\boldsymbol{x} + \boldsymbol{y} = (x_0 + y_0, x_1 + y_1, \ldots)$ and the multiplication of $\boldsymbol{x}$ by a scalar a is $a\boldsymbol{x} = (ax_0, ax_1, \ldots)$.
A related real linear space is the set $\mathbf{Seq}_n(\mathbb{R})$ of all sequences of real numbers having length n, where the sum and the scalar multiplications are defined in a similar manner. Namely, if $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$ and $\boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1})$, the sequence $\boldsymbol{x} + \boldsymbol{y}$ is defined by $\boldsymbol{x} + \boldsymbol{y} = (x_0 + y_0, x_1 + y_1, \ldots, x_{n-1} + y_{n-1})$ and the multiplication of $\boldsymbol{x}$ by a scalar a is $a\boldsymbol{x} = (ax_0, ax_1, \ldots, ax_{n-1})$. This linear space is denoted by $\mathbb{R}^n$ and its zero element is denoted by $\mathbf{0}_n$.

Example

If the real field $\mathbb{R}$ is replaced by the complex field $\mathbb{C}$, we obtain the linear space $\mathbf{Seq}(\mathbb{C})$ of all sequences of complex numbers. Similarly, we have the complex linear space $\mathbb{C}^n$ which consists of all sequences of length n of complex numbers.

Example

Let L be an $\mathbb{F}$-linear space and let S be a non-empty set. The set L^S that consists of all functions of the form $f : S \longrightarrow L$ is an $\mathbb{F}$-linear space. The addition of functions is defined by

$$(f + g)(s) = f(s) + g(s),$$

while the multiplication by a scalar is given by $(af)(s) = af(s)$, for $s \in S$ and $a \in \mathbb{F}$.

Example

Let $\mathbb{R}[x]$ be the set of polynomials of variable x with coefficients in $\mathbb{R}$. For example, $p \in \mathbb{R}[x]$, where

$$p(x) = 3x^7 - 5x^3 + x - 6.$$

The sum of two polynomials $p, q \in \mathbb{R}[x]$ belongs to $\mathbb{R}[x]$. Also, for every $a \in \mathbb{R}$, ap is again a polynomial with coefficients in $\mathbb{R}$.

Definition

Let L be an $\mathbb{F}$-linear space. A subset U of L is a *linear subspace* of L (or just a subspace of L) if it satisfies the following conditions:

- if $\mathbf{x}, \mathbf{y} \in U$, then $\mathbf{x} + \mathbf{y} \in U$;
- if $a \in \mathbb{F}$ and $\mathbf{x} \in U$, then $a\mathbf{x} \in U$.

If U is a subspace of a linear space L and $\mathbf{x} \in L$, we denote the set $\{\mathbf{x} + \mathbf{u} \mid \mathbf{u} \in U\}$ by $\mathbf{x} + U$.

Example

The set of polynomials $P_{\leqslant k}$ of degree less or equal to k is a subspace of the linear space of polynomials. Indeed, $p, q \in P_{\leqslant k}$ their sum has degree less or equal to k; also, if $a \in \mathbb{R}$ and $p \in P_{\leqslant k}$, then $ap \in P_{\leqslant k}$.

The following statements are immediate for an $\mathbb{F}$-linear space L:

- the sets L and $\{\mathbf{0}_L\}$ are subspaces of L;
- each subspace U of L contains $\mathbf{0}_L$.

Example

The subset $\{\mathbf{0}_L\}$ of any $\mathbb{F}$-linear space L is a subspace of L named the *zero subspace*. This is the smallest subspace of L.

Theorem

If $\mathcal{L} = \{L_i \mid i \in I\}$ is a collection of subspaces of an $\mathbb{F}$-linear space L, then $\bigcap \mathcal{L}$ is a subspace of L.

Proof.

Suppose that $\boldsymbol{x}, \boldsymbol{y} \in \bigcap \mathcal{L}$. Then, $\boldsymbol{x}, \boldsymbol{y} \in L_i$, so $\boldsymbol{x} + \boldsymbol{y} \in L_i$ and $a\boldsymbol{x} \in L_i$ for every $i \in I$. Thus, $\boldsymbol{x} + \boldsymbol{y} \in \bigcap \mathcal{L}$ and $a\boldsymbol{x} \in \bigcap \mathcal{L}$, which allows us to conclude that $\bigcap \mathcal{L}$ is a subspace of L. □

Since L itself is a subspace of L it follows that the collection of subspaces of a linear space is a closure system $\mathcal{C}$. If $\boldsymbol{K}_{\text{sub}}$ is the closure operator induced by $\mathcal{C}$, then for every subset X of L, $\boldsymbol{K}_{\text{sub}}(X)$ is the smallest subspace of L that contains X.

Let SUBSP(M) be the collection of subspaces of a linear space M. If this set is equipped with the inclusion relation $\subseteq$ (which is a partial order), then for any two subspaces K, L both $\sup\{K, L\}$ and $\inf\{K, L\}$ exist and are given by:

$$\sup\{K, L\} = \{\boldsymbol{x} + \boldsymbol{y} \mid \boldsymbol{x} \in K \text{ and } \boldsymbol{y} \in L\} \quad (1)$$

$$\inf\{K, L\} = K \cap L. \quad (2)$$

Let $H = \{\boldsymbol{x} + \boldsymbol{y} \mid \boldsymbol{x} \in K \text{ and } \boldsymbol{y} \in L\}$. Observe that we have both $K \subseteq H$ and $L \subseteq H$ because $\mathbf{0}$ belongs to both K and L.

If $\boldsymbol{u}$ and $\boldsymbol{v}$ belong to H, then $\boldsymbol{u} = \boldsymbol{x}_1 + \boldsymbol{y}_1$ and $\boldsymbol{v} = \boldsymbol{x}_2 + \boldsymbol{y}_2$, where $\boldsymbol{x}_1, \boldsymbol{x}_2 \in K$ and $\boldsymbol{y}_1, \boldsymbol{y}_2 \in L$. Since $\boldsymbol{x}_1 + \boldsymbol{x}_2 \in K$ and $\boldsymbol{y}_1 + \boldsymbol{y}_2 \in L$ (because K and L are subspaces), it follows that

$\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{x}_1 + \boldsymbol{y}_1 + (\boldsymbol{x}_2 + \boldsymbol{y}_2) = (\boldsymbol{x}_1 + \boldsymbol{x}_2) + (\boldsymbol{y}_1 + \boldsymbol{y}_2) \in H$.

We have $a\boldsymbol{u} = a\boldsymbol{x}_1 + a\boldsymbol{x}_2 \in H$ because $a\boldsymbol{x}_1 \in K$ and $a\boldsymbol{x}_2 \in L$. Thus, H is a subspace of M and is an upper bound of $\{K, L\}$ in the partially ordered set $(\text{SUBSP}(M), \subseteq)$.

If G is a subspace of M that contains both K and L, then $\boldsymbol{x} + \boldsymbol{y} \in G$ for $\boldsymbol{x} \in K$ and $\boldsymbol{y} \in L$, so $H \subseteq G$. Thus, $H = \sup\{K, L\}$.

We denote $H = \sup\{K, L\}$ by $K + L$.

Next, we prove the *modularity* of SUBSP(M).

Theorem

Let M be an $\mathbb{F}$-linear space. For any $P, Q, R \in SUBSP(M)$ such that $Q \subseteq P$ we have $P \cap (Q + R) = Q + (P \cap R)$.

Proof.

Note that $Q \subseteq P \cap (Q + R)$, $P \cap R \subseteq P \cap (Q + R)$. Therefore, we have the inclusion $Q + (P \cap R) \subseteq P \cap (Q + R) =$, which leaves us with the reverse inclusion to prove.

Let $\boldsymbol{z} \in P \cap (Q + R)$. This implies $\boldsymbol{z} \in P$ and $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}$, where $\boldsymbol{x} \in Q \subseteq P$ and $\boldsymbol{y} \in R$. Therefore, $\boldsymbol{y} = \boldsymbol{z} - \boldsymbol{x} \in P$, so $\boldsymbol{y} \in P \cap R$.
Consequently, $\boldsymbol{z} \in Q + (P \cap R)$, so $P \cap (Q + R) \subseteq Q + (P \cap R)$. □

Definition

If L is an $\mathbb{F}$-linear space, and X is a subset of L, an X-*linear combination* is an element $\boldsymbol{w}$ of L that can be written as

$$\boldsymbol{w} = \sum_{i=1}^{n} c_i \boldsymbol{x}_i,$$

where $\boldsymbol{x}_i \in X$.
A *linear combination of* L is an X-linear combination, where X is a subset of L.

The set of all X-linear combinations is denoted by $\langle X \rangle$ and is referred to as the *set spanned by* X.

Theorem

Let L be an $\mathbb{F}$-linear space. If $X \subseteq L$, then $\langle X \rangle$ is the smallest subspace of L that contains the set X. In other words, we have:

- $\langle X \rangle$ *is a subspace of* L;
- $X \subseteq \langle X \rangle$;
- *if* $X \subseteq M$, *where* M *is a subspace of* L, *then* $\langle X \rangle \subseteq M$.

Proof

It is clear that if $\boldsymbol{u}$ and $\boldsymbol{v}$ are two X-linear combinations, then $\boldsymbol{u}+\boldsymbol{v}$ and $a\boldsymbol{u}$ are also X-linear combinations, so $\langle X \rangle$ is a subspace of L.
For $\boldsymbol{x} \in X$ we can write $1\boldsymbol{x} = \boldsymbol{x}$, so $X \subseteq \langle X \rangle$.
Finally, suppose that $X \subseteq M$, where M is a subspace of L and $a_1\boldsymbol{x}_1 + \cdots + a_n\boldsymbol{x}_n \in \langle X \rangle$, where $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in X$. Since $X \subseteq M$, we have $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in M$, hence $a_1\boldsymbol{x}_1 + \cdots + a_n\boldsymbol{x}_n \in M$ because M is a subspace.
Thus, $\langle X \rangle \subseteq M$.

Definition

Let L be an $\mathbb{F}$-linear space. A finite subset $U = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ of L is *linearly dependent* if $a_1\mathbf{x}_1 + \cdots + a_n\mathbf{x}_n = \mathbf{0}_L$, where at least one element a_i of $\mathbb{F}$ is not equal to 0.
If this condition is not satisfied then U is said to be *linearly independent*.

A set U that consists of one vector $\mathbf{x} \neq \mathbf{0}_L$ is linearly independent.

$U = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ of L is linearly independent if $a_1\boldsymbol{x}_1 + \cdots + a_n\boldsymbol{x}_n = \mathbf{0}_L$ implies $a_1 = \cdots = a_n = 0$. Also, note that a set U that is linearly independent does not contain $\mathbf{0}_L$.

Example

Let L be an $\mathbb{F}$-linear space. If $\boldsymbol{u} \in L$, then the set $L_{\boldsymbol{u}} = \{a\boldsymbol{u} \mid a \in F\}$ is a linear subspace of L. Moreover, if $\boldsymbol{u} \neq \mathbf{0}_L$, then the set $\{\boldsymbol{u}\}$ is linearly independent. Indeed, if $a\boldsymbol{u} = \mathbf{0}_L$ and $a \neq 0$, then multiplying both sides of the above equality by a^{-1} we obtain $(a^{-1}a)\boldsymbol{u} = \boldsymbol{a}^{-1}\mathbf{0}$, or equivalently, $\boldsymbol{u} = \mathbf{0}_L$, which contradicts the initial assumption. Thus, $\{\boldsymbol{u}\}$ is a linearly independent set.

Definition

Let L be an $\mathbb{F}$-linear space. A subset W of L is *linearly dependent* if it contains a finite subset U that is linearly dependent.
A subset W is *linearly independent* if it is not linearly dependent.

Thus, W is linearly independent if every finite subset of W is linearly independent. Further, any subset of a linearly independent subset is linearly independent and any superset of a linearly dependent set is linearly dependent.

Example

For every $\mathbb{F}$-linear space L the set $\{\mathbf{0}_L\}$ is linearly dependent because we have $1\mathbf{0}_L = \mathbf{0}_L$.

Theorem

Let L be an $\mathbb{F}$-linear space and let W be a linearly independent subset of L. If $\boldsymbol{y}$ is a linear combination

$$\boldsymbol{y} = a_1\boldsymbol{x}_1 + \cdots + a_n\boldsymbol{x}_n,$$

for some finite subset $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ of W, then the coefficients $a_1, \ldots, a_n$ are uniquely determined.

Proof

Suppose that $\boldsymbol{y}$ can be alternatively written as

$$\boldsymbol{y} = b_1\boldsymbol{x}_1 + \cdots + b_n\boldsymbol{x}_n,$$

for some $b_1, \ldots, b_n \in \mathbb{F}$. Since W is linearly independent this implies

$$(a_1 - b_1)\boldsymbol{x}_1 + \cdots + (a_n - b_n)\boldsymbol{x}_n = \boldsymbol{0}_L,$$

which, in turn, yields $a_1 - b_1 = \cdots = a_n - b_n = 0$. This, we have $a_i = b_i$ for $1 \leqslant i \leqslant n$.

Definition

Let $\mathbb{F}$ be a field and let L and M be two $\mathbb{F}$-linear spaces. A *linear mapping* is a function $\boldsymbol{h} : L \longrightarrow M$ such that

$$\boldsymbol{h}(a\boldsymbol{x} + b\boldsymbol{y}) = a\boldsymbol{h}(\boldsymbol{x}) + b\boldsymbol{h}(\boldsymbol{y})$$

for every scalars $a, b \in \mathbb{F}$ and $\boldsymbol{x}, \boldsymbol{y} \in L$.
An *affine mapping* is a function $\boldsymbol{f} : L \longrightarrow M$ such that there exists a linear mapping $\boldsymbol{h} : L \longrightarrow M$ and $\boldsymbol{b} \in M$ such that $\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{b}$ for $\boldsymbol{x} \in L$.

Linear mappings are also referred to as *linear spaces homomorphisms*, as *linear morphisms*, or as *linear operators*.
The set of morphisms between two $\mathbb{F}$-linear spaces L and M is denoted by $\text{Hom}(L, M)$. The set of affine mappings between two $\mathbb{F}$-linear spaces L and M is denoted by $\text{Aff}(L, M)$.

Example

Let $h : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be the transformation defined by

$$h\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$$

This is a linear mapping $h : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$.

Define the mapping $h : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$ as

$$h(p)(x) = \int_0^x p(t)\, dt.$$

For example, for $p(x) = x^2 + \frac{1}{3}x$ we have

$$h(p)(x) = \int_0^x (t^2 + \frac{1}{3}t)\, dt = \frac{1}{3}x^3 + \frac{1}{6}x^2.$$

It is easy to see that $h(p_1 + p_2) = h(p_1) + h(p_2)$ and $h(ap) = ah(p)$, which means that h is indeed a linear mapping

The notion of subspace is closely linked to the notion of linear mapping as we show next.

Theorem

Let L, M be two $\mathbb{F}$-linear spaces. If $h : L \longrightarrow M$ is a linear mapping than the sets

$$Im(h) = \{h(\mathbf{x}) \mid \mathbf{x} \in L\},$$

and

$$Ker(h) = \{\mathbf{x} \in L \mid h(\mathbf{x}) = \mathbf{0}_M\}$$

are subspaces of the linear spaces M and L, respectively.

Proof

Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be two elements of $\text{Im}(h)$. There exist $\boldsymbol{x}, \boldsymbol{y} \in L$ such that $\boldsymbol{u} = h(\boldsymbol{x})$ and $\boldsymbol{v} = h(\boldsymbol{y})$. Since h is a linear mapping we have

$$\boldsymbol{u} + \boldsymbol{v} = h(\boldsymbol{x}) + h(\boldsymbol{y}) = h(\boldsymbol{x} + \boldsymbol{y}).$$

Thus, $\boldsymbol{u} + \boldsymbol{v} \in \text{Im}(h)$. Further, if $a \in \mathbb{F}$, then $a\boldsymbol{u} = ah(\boldsymbol{x}) = h(a\boldsymbol{x})$, so $a\boldsymbol{u} \in \text{Im}(h)$. Thus, $\text{Im}(h)$ is indeed a subspace of M.
Suppose now that $\boldsymbol{s}$ and $\boldsymbol{t}$ belong to $\text{Ker}(h)$, that is $h(\boldsymbol{s}) = h(\boldsymbol{t}) = \mathbf{0}_M$. Then, $h(\boldsymbol{s} + \boldsymbol{t}) = h(\boldsymbol{s}) + h(\boldsymbol{t}) = \mathbf{0}_M$, so $\boldsymbol{s} + \boldsymbol{t} \in \text{Ker}(h)$. Also, $h(a\boldsymbol{s}) = ah(\boldsymbol{s}) = a\mathbf{0}_M = \mathbf{0}_M$, which allows us to conclude that $\text{Ker}(h)$ is a subspace of L.

We refer to $\text{Im}(h)$ as the *image* of h, and to $\text{Ker}(h)$ as the *kernel* of h.

Definition

Let $\boldsymbol{h}, \boldsymbol{g} \in \text{Hom}(L, M)$ be two linear mappings between the $\mathbb{F}$-linear spaces L and M. The *sum* of $\boldsymbol{h}$ and $\boldsymbol{g}$ is the mapping $\boldsymbol{h} + \boldsymbol{g}$ defined by

$$(\boldsymbol{h} + \boldsymbol{g})(\boldsymbol{x}) = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{g}(\boldsymbol{x})$$

for $\boldsymbol{x} \in L$.
If $a \in \mathbb{F}$, the product $a\boldsymbol{f}$ is defined as $(a\boldsymbol{f})(\boldsymbol{x}) = a\boldsymbol{f}(\boldsymbol{x})$ for $\boldsymbol{x} \in L$.

If L, M are two $\mathbb{F}$-linear spaces, then the set $\text{Hom}(L, M)$ is never empty because the zero morphism $\mathbf{0}_{L,M} : L \longrightarrow M$ defined as $\mathbf{0}_{L,M}(\boldsymbol{x}) = \mathbf{0}_M$ for $\boldsymbol{x} \in L$ is always an element of $\text{Hom}(L, M)$.

Note that

$$\begin{aligned}(\boldsymbol{f}+\boldsymbol{g})(a\mathbf{x}+b\mathbf{y}) &= \boldsymbol{f}(a\mathbf{x}+b\mathbf{y})+\boldsymbol{g}(a\mathbf{x}+b\mathbf{y})\\ &= a\boldsymbol{f}(\mathbf{x})+b\boldsymbol{f}(\mathbf{y})+a\boldsymbol{g}(\mathbf{x})+b\boldsymbol{g}(\mathbf{y})\\ &= \boldsymbol{f}(a\mathbf{x}+b\mathbf{y})+\boldsymbol{g}(a\mathbf{x}+b\mathbf{y}),\end{aligned}$$

for all $a, b \in F$ and $\mathbf{x}, \mathbf{y} \in L$. This shows that the sum of two linear mappings is also a linear mapping.

Theorem

$Hom(L, M)$ equipped with the sum and product defined above is an $\mathbb{F}$-linear space.

Proof: The zero element of $\mathrm{Hom}(L, M)$ is the mapping $\mathbf{0}_{L,M}$.

Definition

Let L be an $\mathbb{F}$-linear space. A *linear form* on L is a morphism in $\mathrm{Hom}(L, \mathbb{F})$, where the field $\mathbb{F}$ is regarded as a linear space.

Definition

A *basis* of an $\mathbb{F}$-linear space L is a linearly independent subset W such that $\langle W \rangle = L$.
If an $\mathbb{F}$-linear space L has a finite basis, then we say that L is a *linear space of finite type*.

Theorem

Every non-zero $\mathbb{F}$*-linear space* L *has a basis.*

UMASS BOSTON

Corollary

(Independent Set Extension Corollary) *Let L be an $\mathbb{F}$-linear space. If W is a linearly independent set, then there exists a basis T of L such that $W \subseteq T$.*

Proof: Since W is a linearly independent set, if $\langle T \rangle = L$, then $W \cup T$ is also generating L.

If an $\mathbb{F}$-linear space L has a finite basis, then we say that L is a linear space of *finite type*.

Lemma

Let L be a finite type $\mathbb{F}$-linear space and let T be a finite subset of L that is not linearly independent. If $k = |T| \geqslant 2$ and $(\boldsymbol{t}_1, \ldots, \boldsymbol{t}_k)$ is a list of the vectors in T, then there exists a number j such that $2 \leqslant j \leqslant k$ and $\boldsymbol{t}_j$ is a linear combination of its predecessors in the sequence. Furthermore, we have $\langle T - \{\boldsymbol{t}_j\} \rangle = \langle T \rangle$.

Proof

Since T is not linearly in dependent, there exists a linear combination $\sum_{i=1}^{k} a^i \boldsymbol{t}_i = \mathbf{0}_L$ such that some of the scalars $a^1, \ldots, a^k$ are different from 0.
Let j the largest number such that $1 \leqslant j \leqslant k$ and $a_j \neq 0$. The definition of j implies

$$a^1 \boldsymbol{t}_1 + \cdots + a^j \boldsymbol{t}_j = \mathbf{0}_L,$$

so $\boldsymbol{t}_j = -\sum_{i=1}^{j-1} \frac{a^i}{a^j} \boldsymbol{t}_i$, which shows that $\boldsymbol{t}_j$ is a linear combination of its predecessors in the list. Consequently, the set of linear combinations of the vectors in $T - \{\boldsymbol{t}_j\}$ equals $\langle T \rangle$.

Theorem

(The Replacement Theorem) *Let L be a finite type $\mathbb{F}$-linear space such that the set W spans the linear space L and $|W| = n$.*
If U is a linearly independent set in V such that $|U| = m$, then $m \leqslant n$ and there exists a subset W' of W such that W' contains $n - m$ vectors and $U \cup W'$ spans the space L.

UMASS BOSTON

Proof

Suppose that $W = \{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ and $U = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ is linearly independent, where $m \leqslant n$. The argument is by induction on m.
The basis case, $m = 0$, is immediate.
Suppose the statement holds for m and let $U = \{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{u}_{m+1}\}$ be a linearly independent set that contains $m + 1$ vectors.
The set $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ is linearly independent, so by the inductive hypothesis there exists a subset W' of W that contains $n - m$ vectors such that $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\} \cup W'$ spans the space L.
Without loss of generality we may assume that $W' = \{\mathbf{w}_1, \ldots, \mathbf{w}_{n-m}\}$.
Thus, $\mathbf{u}_{m+1}$ is a linear combination of the vectors of $\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{w}_1, \ldots, \mathbf{w}_{n-m}\}$, so we have

$$\mathbf{u}_{m+1} = a^1\mathbf{u}_1 + \cdots + a^m\mathbf{u}_m + b^1\mathbf{w}_1 + \cdots + b^{n-m}\mathbf{w}_{n-m}.$$

Proof (cont'd)

We have $m+1 \leqslant n$ because, otherwise, $m+1=n$ and $\boldsymbol{u}_{m+1}$ would be a linear combination of $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m$, thereby contradicting the linear independence of the set U.
The set $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m, \boldsymbol{u}_{m+1}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-m}\}$ is not linearly independent. Let $\boldsymbol{v}$ be the first member of the sequence $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m, \boldsymbol{u}_{m+1}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-m})$ that is a linear combination of its predecessors. Then, $\boldsymbol{v}$ cannot be one of the $\boldsymbol{u}_i$ (with $1 \leqslant i \leqslant m$) because this would contradict the linear independence of the set U. Therefore, there exists k such that $\boldsymbol{w}_k$ is a linear combination of its predecessors and $1 \leqslant k \leqslant n-m$. By a previous lemma we can remove this element from the set $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m, \boldsymbol{u}_{m+1}, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-m}\}$ without affecting the set spanned.

Corollary

Let L be a finite type $\mathbb{F}$-linear space and let U, W be two bases of L. Then $|U| = |W|$.

Proof.

Since U is a linearly independent set and $\langle W \rangle = L$ we have $|U| \leqslant |W|$. The reverse inequality, $|W| \leqslant |U|$, is obtained by asserting that W is linearly independent and $\langle U \rangle = L$. Thus, $|U| = |W|$. □

This allows the introduction of the notion of dimension for a linear space.

Definition

The *dimension* of a finite type linear space L is the number of elements of any basis of L.
The dimension of L is denoted by $\dim(L)$.

If a linear space L is not of finite type than we say that $\dim(L)$ is infinite.

Theorem

Let L be an $\mathbb{F}$-linear space of finite type having the basis $B = \{\mathbf{x}_1, \ldots, x_n\}$ and let $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ be a subset of an $\mathbb{F}$-linear space M. There exists a unique linear mapping $f : L \longrightarrow M$ such that $f(\mathbf{x}_i) = \mathbf{y}_i$ for $1 \leqslant i \leqslant n$.

Proof: If $\mathbf{x} \in L$ we have $\mathbf{x} = a_1\mathbf{x}_1 + \cdots + a_n\mathbf{x}_n$ because $\{\mathbf{x}_1, \ldots, x_n\}$ is a basis of L. Define $f(\mathbf{x})$ as $f(\mathbf{x}) = \sum_{i=1}^{n} a_i\mathbf{y}_i$. The uniqueness of the expression of $\mathbf{x}$ as a linear combination of the elements of B makes f well-defined. The linearity of f is immediate. For uniqueness, note that the value of f is determined by the values of $f(\mathbf{x}_i)$.

Theorem

Let L, M be two linear spaces of finite type with $\dim(L) = p$ *and* $\dim(M) = q$. *Then,* $\dim(Hom(L, M)) = pq$.

Proof

Suppose that $\{\mathbf{x}_1, \ldots, \mathbf{x}_p\}$ is a basis in L and $\{\mathbf{y}_1, \ldots, \mathbf{y}_q\}$ is a basis in M. For every i such that $1 \leqslant i \leqslant p$ and j such that $1 \leqslant j \leqslant q$ there exists a unique linear mapping $f_{ij} : \{\mathbf{x}_1, \ldots, \mathbf{x}_p\} \longrightarrow M$ such that:

$$f_{ij}(\mathbf{x}_k) = \begin{cases} \mathbf{y}_j & \text{if } i = k, \\ \mathbf{0}_M & \text{otherwise,} \end{cases}$$

for $1 \leqslant k \leqslant p$.
Note that if $\mathbf{x} = \sum_{k=1}^{p} a_k \mathbf{x}_k$, the linearity of f_{ij} implies:

$$f_{ij}(\mathbf{x}) = f_{ij}\left(\sum_{k=1}^{p} a_k \mathbf{x}_k\right) = \sum_{k=1}^{p} a_k f_{ij}(\mathbf{x}_k) = a_i f_{ij}(\mathbf{x}_i).$$

We claim that the set $\{f_{ij} \mid 1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q\}$ is a basis for $\mathrm{Hom}(L, M)$.

Proof cont'd

Let $f : L \longrightarrow M$ be a linear mapping. If $\boldsymbol{x} \in L$ we can write $\boldsymbol{x} = \sum_{i=1}^{p} a_i \boldsymbol{x}_i$, so $f(\boldsymbol{x}) = \sum_{i=1}^{p} a_i f(\boldsymbol{x}_i)$. In turn, since $\{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_q\}$ is a basis in M, $f(\boldsymbol{x}_i) = \sum_{j=1}^{q} b_{ij} \boldsymbol{y}_j$, for some $b_{ij} \in F$. This allows us to write:

$$f(\boldsymbol{x}) = \sum_{i=1}^{p} a_i \sum_{j=1}^{q} b_{ij} \boldsymbol{y}_j = \sum_{i=1}^{p} \sum_{j=1}^{q} a_i b_{ij} \boldsymbol{y}_j = \sum_{i=1}^{p} \sum_{j=1}^{q} a_i b_{ij} f_{ij}(\boldsymbol{x}),$$

which shows that each linear mapping in $\mathrm{Hom}(L, M)$ is a linear combination of functions f_{ij}.

Proof cont'd

Furthermore, the set $\{f_{ij} \mid 1 \leqslant i \leqslant p, 1 \leqslant j \leqslant p\}$ is linearly independent in $\mathrm{Hom}(L, M)$. Indeed, suppose that $\sum_{i=1}^{p} \sum_{j=1}^{q} c_{ij} f_{ij}(\boldsymbol{x}) = \mathbf{0}_M$. Then, for $\boldsymbol{x} = \boldsymbol{x}_i$ we have $\sum_{j=1}^{q} c_{ij} \boldsymbol{y}_j = \mathbf{0}_M$, which implies $c_{ij} = 0$. We may conclude that $\dim(\mathrm{Hom}(L, M)) = \dim(L) \dim(M)$.

Theorem

If W is a subspace of a finite type linear space L, then $\dim(W) \leqslant \dim(L)$.

Proof.

If U is a linearly independent set in the subspace W, then it is clear that U is linearly independent in L. There exists a basis V of L such that $U \subseteq V$ and $|V| = \dim(L)$. Therefore, $\dim(W) \leqslant \dim(L)$. □

UMASS BOSTON

The notion of subspace is closely linked to the notion of linear mapping as we show next.

Theorem

Let L, M be two $\mathbb{F}$-linear spaces. If $h : L \longrightarrow M$ is a linear mapping than $Im(h)$ is a subspace of M and $Ker(h)$ is a subspace of L.

Proof

Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be two elements of $\text{Im}(h)$. There exist $\boldsymbol{x}, \boldsymbol{y} \in L$ such that $\boldsymbol{u} = h(\boldsymbol{x})$ and $\boldsymbol{v} = h(\boldsymbol{y})$. Since h is a linear mapping we have

$$\boldsymbol{u} - \boldsymbol{v} = h(\boldsymbol{x}) - h(\boldsymbol{y}) = h(\boldsymbol{x} - \boldsymbol{y}).$$

Thus, $\boldsymbol{u} - \boldsymbol{v} \in \text{Im}(h)$. Further, if $a \in S$, then $a\boldsymbol{u} = ah(\boldsymbol{x}) = h(a\boldsymbol{x})$, so $a\boldsymbol{u} \in \text{Im}(h)$. Thus, $\text{Im}(h)$ is indeed a subspace of P.
Suppose now that $\boldsymbol{s}$ and $\boldsymbol{t}$ belong to $\text{Ker}(h)$, that is $h(\boldsymbol{s}) = h(\boldsymbol{t}) = \mathbf{0}_M$. Then, $h(\boldsymbol{s} - \boldsymbol{t}) = h(\boldsymbol{s}) - h(\boldsymbol{t}) = \mathbf{0}_M$, so $\boldsymbol{s} - \boldsymbol{t} \in \text{Ker}(h)$. Also, $h(a\boldsymbol{s}) = ah(\boldsymbol{s}) = a\mathbf{0}_M = \mathbf{0}_M$, which allows us to conclude that $\text{Ker}(h)$ is a subspace of h.

Theorem

Let L and M be two linear spaces, where $\dim(L) = n$, and let $h : L \longrightarrow M$ be a linear mapping. Then, we have

$$\dim(Ker(h)) + \dim(Im(h)) = n.$$

Proof

Suppose that $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m\}$ is a basis for the subspace $\text{Ker}(h)$ of L. Each such basis can be extended to a basis

$$\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m, \boldsymbol{e}_{m+1}, \ldots, \boldsymbol{e}_n\}$$

of the space L. Any $\boldsymbol{v} \in L$ can be written as

$$\boldsymbol{v} = \sum_{i=1}^{n} a^i \boldsymbol{e}_i.$$

Since $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m\} \subseteq \text{Ker}(h)$ we have $h(\boldsymbol{e}_i) = \mathbf{0}_M$ for $1 \leqslant i \leqslant m$, so

$$h(\boldsymbol{v}) = \sum_{i=m+1}^{n} a^i h(\boldsymbol{e}_i).$$

This means that the set $\{h(\boldsymbol{e}_{m+1}), \ldots, h(\boldsymbol{e}_n)\}$ spans the subspace $\text{Im}(h)$ of M.

Proof cont'd

We show now that this set is linearly independent.
Indeed, suppose that $\sum_{i=m+1}^{n} b^i h(\mathbf{e}_i) = \mathbf{0}_M$. This implies $h(\sum_{i=m+1}^{n} b^i \mathbf{e}_i) = \mathbf{0}_M$, that is, $\sum_{i=m+1}^{n} b^i \mathbf{e}_i \in \text{Ker}(h)$. Since $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ is a basis for $\text{Ker}(h)$ there exist m scalars $c^1, \ldots, c^m$ such that

$$\sum_{i=m+1}^{n} b^i \mathbf{e}_i = c^1 \mathbf{e}_1 + \cdots + c^m \mathbf{e}_m.$$

The fact that $\{\mathbf{e}_1, \ldots, \mathbf{e}_m, \mathbf{e}_{m+1}, \ldots, \mathbf{e}_n\}$ is a basis for L implies that $c^1 = \cdots = c^m = b^{m+1} = \cdots = b^n = 0$, so the set $\{h(\mathbf{e}_{m+1}), \ldots, h(\mathbf{e}_n)\}$ is linearly independent and, therefore, a basis for $\text{Im}(h)$. Thus, $\dim(\text{Im}(h)) = n - m$, which concludes the argument.

Definition

Let L and M be two $\mathbb{F}$-linear spaces and let $h \in \text{Hom}(L, M)$. The *rank* of h is $\text{rank}(h) = \dim(\text{Im}(h))$; the *nullity* of h is $\text{nullity}(h) = \dim(\text{Ker}(h))$.

If $h : L \longrightarrow M$ is a linear mapping and L is a linear space of finite type, then

$$\dim(L) = \text{rank}(h) + \text{nullity}(h).$$

Theorem

Let $h : L \longrightarrow M$ be a linear mapping between two linear spaces. Then, $rank(h) \leqslant \min\{\dim(L), \dim(M)\}$.

Proof.

It is clear that $\mathrm{rank}(h) \leqslant \dim(L)$. On the other hand, $\mathrm{rank}(h) = \dim(\mathrm{Im}(h)) \leqslant \dim(M)$ because $\mathrm{Im}(h)$ is a subspace of M, so the inequality of the theorem follows. □

Example

Let L, M be two $\mathbb{F}$-linear spaces. For $h \in L^*$ and $\boldsymbol{y} \in M$ define the mapping $\ell_{h,\boldsymbol{y}}$ as $\ell_{h,\boldsymbol{y}}(\boldsymbol{x}) = h(\boldsymbol{x})\boldsymbol{y}$ for $\boldsymbol{x} \in L$. It is easy to verify that $\ell_{h,\boldsymbol{y}}$ is a linear mapping, that is, $\ell_{h,\boldsymbol{y}} \in \mathrm{Hom}(L, M)$. Furthermore, we have $\mathrm{rank}(\ell_{h,\boldsymbol{y}}) = 1$ because $\mathrm{Im}(\ell_{h,\boldsymbol{y}})$ consists of the multiples of the vector $\boldsymbol{y}$.

UMASS BOSTON

Definition

Let L and M two $\mathbb{F}$-linear spaces. An *isomorphism* between these linear spaces is a linear mapping $h : L \longrightarrow M$ that is a bijection.
If an isomorphism exists between two $\mathbb{F}$-linear spaces L and M we say that these linear spaces are *isomorphic* and we write $L \cong M$.

Two $\mathbb{F}$-linear spaces that are isomorphic are indiscernible from an algebraic point of view.

If L_1, L_2 are subspaces of an $\mathbb{F}$-linear space L, then their intersection is non-empty because $\mathbf{0}_L \in L_1 \cap L_2$. Moreover, it is easy to see that $L_1 \cap L_2$ is also a subspace of L.

Let L_1, L_2 be two subspaces of a linear space L. Their *sum* is the subset $L_1 + L_2$ of L defined by

$$L_1 + L_2 = \{\mathbf{x} + \mathbf{y} \mid \mathbf{x} \in L_1 \text{ and } \mathbf{y} \in L_2\}.$$

It is immediate to verify that $L_1 + L_2$ is a subspace of L and that $\mathbf{0}_L \in L_1 \cap L_2$.

Theorem

Let L_1, L_2 be two subspaces of the $\mathbb{F}$-linear space L. If $L_1 \cap L_2 = \{\mathbf{0}_L\}$, then any vector $\mathbf{x} \in L_1 + L_2$ can be uniquely written as $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$, where $\mathbf{x}_1 \in L_1$ and $\mathbf{x}_2 \in L_2$.

Proof.

By the definition of the sum $L_1 + L_2$ it is clear that any vector $\mathbf{x} \in L_1 + L_2$ can be written as $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$. We need to prove only the uniqueness of $\mathbf{x}_1$ and $\mathbf{x}_2$.

Suppose that $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2 = \mathbf{y}_1 + \mathbf{y}_2$, where $\mathbf{x}_1, \mathbf{y}_1 \in L_1$ and $\mathbf{x}_2, \mathbf{y}_2 \in L_2$. This implies $\mathbf{x}_1 - \mathbf{y}_1 = \mathbf{y}_2 - \mathbf{x}_2$ and, since $\mathbf{x}_1 - \mathbf{y}_1 \in L_1$ and $\mathbf{y}_2 - \mathbf{x}_2 \in L_2$ it follows that $\mathbf{x}_1 - \mathbf{y}_1 = \mathbf{y}_2 - \mathbf{x}_2 = \mathbf{0}_L$ by hypothesis. Therefore, $\mathbf{x}_1 = \mathbf{y}_1$ and $\mathbf{x}_2 = \mathbf{y}_2$. □

Theorem

Let L_1, L_2 be two subspaces of the $\mathbb{F}$-linear space L. If every vector $\mathbf{x} \in L_1 + L_2$ can be uniquely written as $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$, then $L_1 \cap L_2 = \mathbf{0}_L$.

Proof.

Suppose that the uniqueness of the expression of $\mathbf{x}$ holds but $\mathbf{z} \in L_1 \cap L_2$ and $\mathbf{z} \neq \mathbf{0}_L$. If $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$, then we can also write $\mathbf{x} = (\mathbf{x}_1 + \mathbf{z}) + (\mathbf{x}_2 - \mathbf{z})$, where $\mathbf{x}_1 + \mathbf{z} \in L_1$ and $\mathbf{x}_2 - \mathbf{z} \in L_2$, $\mathbf{x}_1 + \mathbf{z} \neq \mathbf{x}_1$ and $\mathbf{x}_2 - \mathbf{z} \neq \mathbf{x}_2$, and this contradicts the uniqueness property. □

Let L be an $\mathbb{F}$-linear space. The set of linear forms defined on L is denoted by L^*. This set has the natural structure of an $\mathbb{F}$-linear space known as the *dual of the space L*.

The elements of L^* are also referred to as *covariant vectors* or *covectors*.

Frequently, we will refer to the vectors of the original linear space as *contravariant vectors*.

Theorem

Let $B = \{\boldsymbol{u}_i \in L \mid 1 \leqslant i \leqslant n\}$ be a basis in an n-dimensional $\mathbb{F}$-linear space L. If $\{a_i \in \mathbb{F} \mid 1 \leqslant i \leqslant n\}$ is a set of scalars, then there is a unique covector $\boldsymbol{f} \in L^*$ such that $\boldsymbol{f}(\boldsymbol{u}_i) = a_i$ for $1 \leqslant i \leqslant n$.

Proof.

Since B is a basis in L we can write $\boldsymbol{v} = \sum_{i=1}^n c_i \boldsymbol{u}_i$ for every $\boldsymbol{v} \in L$. Thus,

$$\boldsymbol{f}(\boldsymbol{v}) = \boldsymbol{f}\left(\sum_{i=1}^n c_i \boldsymbol{u}_i\right) = \sum_{i=1}^n c_i a_i,$$

which shows that the covector $\boldsymbol{f}$ is uniquely determined by the n-tuple of scalars $\boldsymbol{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. □

Corollary

Let L be an n-dimensional $\mathbb{F}$-linear space. Then, its dual L^* is isomorphic to $\mathbb{F}^n$, and, thus, $\dim(L^*) = \dim(L) = n$.

Proof.

The function $h : \mathbb{F}^n \longrightarrow \mathrm{Hom}(L, \mathbb{F})$ that maps the vector

$$\boldsymbol{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

to the function $\boldsymbol{f}$ defined as

$$\boldsymbol{f}(\boldsymbol{v}) = \boldsymbol{f}\left(\sum_{i=1}^{n} c_i \boldsymbol{u}_i\right) = \sum_{i=1}^{n} c_i a_i,$$

where $B = \{\boldsymbol{u}_i \in L \mid 1 \leqslant i \leqslant n\}$ is a basis in L and $\boldsymbol{v} = \sum_{i=1}^{n} c_i \boldsymbol{u}_i$ is an isomorphism. □

A linear form $\boldsymbol{f} \in L^*$ is uniquely determined by its values on a basis of the space L. This allows us to prove the following extension theorem.

Theorem

Let U be a subspace of a finite-dimensional $\mathbb{F}$-linear space L. A linear function $g : U \longrightarrow \mathbb{F}$ belongs to U^* if and only if there exists a linear form $\boldsymbol{f} \in L^*$ such that g is the restriction of $\boldsymbol{f}$ to U.

Proof

If g is the restriction of $\boldsymbol{f}$ to U, then it is immediate that $g \in U^*$. Conversely, let $g \in U^*$ and let $B = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_p\}$ be a basis of U, where $\dim(U) = p$. Consider an extension of B to a basis of the entire space $B_1 = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_p, \boldsymbol{u}_{p+1}, \ldots, \boldsymbol{u}_n\}$, where $n = \dim(L)$ and define the linear form $\boldsymbol{f} : L \longrightarrow \mathbb{F}$ by

$$\boldsymbol{f}(\boldsymbol{u}_i) = \begin{cases} g(\boldsymbol{u}_i) & \text{if } i \leqslant p, \\ 0 & \text{if } p+1 \leqslant i \leqslant n. \end{cases}$$

Since $\boldsymbol{f}$ and g coincide for all members of the basis of U if follows that g is the restriction of $\boldsymbol{f}$ to U.
We refer to $\boldsymbol{f}$ as the *zero-extension* of the linear form g defined on the subspace U.

Theorem

If $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ *is a basis of the* $\mathbb{F}$*-linear space* L*, then the set of linear forms* $\{\mathbf{f}^j \mid 1 \leqslant j \leqslant n\}$ *defined by*

$$\mathbf{f}^j(\mathbf{u}_i) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise} \end{cases}$$

is a basis of the dual linear space L^**.*

Proof

The set $F = \{\boldsymbol{f}^1, \ldots, \boldsymbol{f}^n\}$ spans the entire dual space L^*. Indeed, let $\boldsymbol{f} \in L^*$ be defined by $\boldsymbol{f}(\boldsymbol{u}_i) = a_i$ for $1 \leqslant i \leqslant n$. Then, we have:

$$\boldsymbol{f}(\boldsymbol{x}) = a_1\boldsymbol{f}^1(\boldsymbol{x}) + \cdots + a_n\boldsymbol{f}^n(\boldsymbol{x})$$

for $\boldsymbol{x} \in L$. Indeed, if $\boldsymbol{x} = c^i\boldsymbol{u}_i$, then

$$\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{f}\left(c^i\boldsymbol{u}_i\right) = c^i\boldsymbol{f}(\boldsymbol{u}_i) = c^i a_i.$$

On another hand,

$$a_i\boldsymbol{f}^i(\boldsymbol{x}) = a_i\boldsymbol{f}^i(u_j) = a_i c^j\boldsymbol{f}^i(\boldsymbol{u}_j) = a_i c^i,$$

due to the definition of the linear forms $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$. Therefore, $\boldsymbol{f} = a_1\boldsymbol{f}^1 + \cdots + a_n\boldsymbol{f}^n$, which shows that $\langle F\rangle = L^*$.

Proof cont'd

To prove that the set F is linearly independent in L^* suppose that $a_1\boldsymbol{f}^1 + \cdots + a_n\boldsymbol{f}_n = \mathbf{0}_{L^*}$. This implies $a_1\boldsymbol{f}^1(\boldsymbol{x}) + \cdots + a_n\boldsymbol{f}^n(\boldsymbol{x}) = \mathbf{0}_L$ for every $\boldsymbol{x} \in L$. Choosing $\boldsymbol{x} = \boldsymbol{u}_j$ we obtain $a_j\boldsymbol{f}^j(\boldsymbol{u}_j) = 0$, hence $a_j = 0$, and this can be shown for $1 \leqslant j \leqslant n$, which implies the linear independence.

The basis $F = \{\boldsymbol{f}^1, \ldots, \boldsymbol{f}^n\}$ of L^* constructed before is the *dual basis* of the basis $U = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ of L. We refer to the pair (U, F) as a pair of *dual bases*.

Corollary

The dual of an n-dimensional $\mathbb{F}$-linear space is an n-dimensional linear space.

Example

Let $P_2[x]$ the linear space of polynomials of degree 2 in x, that consists of polynomials of the form $p(x) = ax^2 + bx + c$. The set $\{p_0, p_1, p_2\}$ given by $p_0(x) = 1$, $p_1(x) = x$, and $p_2(x) = x^2$ is a basis in $P_2[x]$. Note that we have

$$\begin{aligned} c &= p(0), \\ b &= \frac{1}{2}(p(1) - p(-1)), \\ a &= \frac{1}{2}(p(1) + p(-1) - 2p(0)). \end{aligned}$$

If $f : P_2[x] \longrightarrow \mathbb{R}$ is a linear form we have

$$\begin{aligned} f(p) &= af(x^2) + bf(x) + cf(0) \\ &= \frac{1}{2}(p(1) + p(-1) - 2p(0))f(x^2) + \frac{1}{2}(p(1) - p(-1))f(x) + p(0)f(1). \end{aligned}$$

UMASS BOSTON

Example cont'd

Example

Therefore, a basis in $P_2[x]^*$ consists of the functions

$$\begin{aligned} f^0(p) &= p(0), \\ f^1(p) &= \frac{1}{2}(p(1) - p(-1)), \\ f^2(p) &= \frac{1}{2}(p(1) + p(-1) - 2p(0)). \end{aligned}$$

We saw that the dual L^* of a $\mathbb{F}$-linear space L is an $\mathbb{F}$-linear space. The construction of the dual may be repeated, and L^{**}, the dual of the dual $\mathbb{F}$-linear space is an $\mathbb{F}$-linear space. In the case of finite dimensional linear spaces we have $\dim(L^{**}) = \dim(L^*) = \dim(L)$, and all these spaces are isomorphic.

Theorem

Let L be a finite-dimensional $\mathbb{F}$-linear space. Then, the dual L^{**} of the dual L^* of L is an $\mathbb{F}$-linear space isomorphic to L.

The notion of linear mapping can be extended as follows.

Definition

Let $L_1, \ldots, L_n, L$ be real linear spaces and let $L_1 \times \cdots \times L_n$ be the Cartesian product of the sets $L_1, \ldots, L_n$.
An *real multilinear function* is a mapping $f : L_1 \times \cdots \times L_n \longrightarrow L$ that is linear in *each of its components when the other components are held fixed*. In other words, f satisfies the conditions:

$$\begin{aligned} & f\left(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{i-1}, \sum_{j=1}^{k} a_j \boldsymbol{x}_i^j, \boldsymbol{x}_{i+1}, \ldots, \boldsymbol{x}_n\right) \\ = & \sum_{j=1}^{k} a_j f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{i-1}, \boldsymbol{x}_i^j, \boldsymbol{x}_{i+1}, \ldots, \boldsymbol{x}_n), \end{aligned}$$

for every $\boldsymbol{x}_i, \boldsymbol{x}_i^j \in L_i$ and $a_1, \ldots, a_k \in \mathbb{R}$.

Definition

Let L, M be two complex linear spaces. A function $f : L \times M \longrightarrow \mathbb{C}$ is said to be *Hermitian bilinear* if it is linear in the first variable and skew-linear in the second, that is, it satisfies the equalities:

$$\begin{aligned} f(a_1\mathbf{x}_1 + a_2\mathbf{x}_2, \mathbf{y}) &= a_1 f(\mathbf{x}_1, \mathbf{y}) + a_2 f(\mathbf{x}_2, \mathbf{y}), \\ f(\mathbf{x}, b_1\mathbf{y}_1 + b_2\mathbf{y}_2) &= \overline{b}_1 f(\mathbf{x}, \mathbf{y}_1) + \overline{b}_2 f(\mathbf{x}, \mathbf{y}_2) \end{aligned}$$

for $a_1, a_2, b_1, b_2 \in \mathbb{C}$.

The set of real multilinear functions defined on the linear spaces $L_1, \ldots, L_n$ and ranging in the real linear space L is denoted by $\mathfrak{M}(L_1, \ldots, L_n; L)$. The set of real multilinear forms is $\mathfrak{M}(L_1, \ldots, L_n; \mathbb{R})$.

Example

Multilinearity is distinct from the notion of linearity on a product of linear spaces. For instance, the mapping $h : \mathbb{R}^2 \longrightarrow \mathbb{R}$ defined by $h(x, y) = x + y$ is linear but not bilinear. On the other hand, the mapping $g : \mathbb{R}^2 \longrightarrow \mathbb{R}$ given by $h(x, y) = xy$ is bilinear but not linear.

Definition

Let $L_1, \ldots, L_n, L$ be real linear spaces.
If $f, g \in \mathfrak{M}(L_1, \ldots, L_n; L)$ are two multilinear functions, their *sum* is the function $f + g$ defined by

$$(f+g)(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) + g(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n),$$

and the product af, where $a \in \mathbb{F}$ is the function af given by

$$(af)(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = af(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$$

for $\boldsymbol{x}_i \in L_i$ and $1 \leqslant i \leqslant n$.

It is immediate to verify that $\mathfrak{M}(L_1, \ldots, L_n; L)$ is an $\mathbb{R}$-linear space relative to these operations.

Let $f : L_1 \times L_2 \longrightarrow L$ be a real bilinear function. Observe that for $\boldsymbol{x} \in L_1$ and $\boldsymbol{y} \in L_2$ we have:

$$\begin{aligned} f(\boldsymbol{x}, \mathbf{0}_{L_2}) &= f(\boldsymbol{x}, 0\boldsymbol{y}) = 0f(\boldsymbol{x}, \boldsymbol{y}) = \mathbf{0}_L \text{ and} \\ f(\mathbf{0}_{L_1}, \boldsymbol{y}) &= f(0\boldsymbol{x}, \boldsymbol{y}) = 0f(\boldsymbol{x}, \boldsymbol{y}) = \mathbf{0}_L. \end{aligned}$$

Example

Let L be an $\mathbb{R}$-linear space and let $\langle \cdot, \cdot \rangle : L^* \times L \longrightarrow \mathbb{R}$ be the function given by $\langle h, \mathbf{y} \rangle = h(\mathbf{y})$ for $h \in L^*$ and $\mathbf{y} \in L$. It is immediate that $\langle \cdot, \cdot \rangle$ is a bilinear function because

$$\begin{aligned} \langle ah + bg, \mathbf{y} \rangle &= a\langle h, \mathbf{y} \rangle + b\langle g, \mathbf{y} \rangle, \\ \langle h, a\mathbf{y} + b\mathbf{z} \rangle &= a\langle h, \mathbf{y} \rangle + b\langle h, \mathbf{z} \rangle, \end{aligned}$$

for $a, b \in \mathbb{R}$, $h, g \in L^*$, and $\mathbf{y}, \mathbf{z} \in L$.
Moreover, we have $\langle h, \mathbf{y} \rangle = 0$ for every $\mathbf{y} \in L$ if and only if $h = \mathbf{0}_{L^*}$ and $\langle h, \mathbf{y} \rangle = 0$ for every $h \in L^*$ if and only if $\mathbf{y} = \mathbf{0}_L$.

Example

Let $L_1, \ldots, L_n, L$ be $\mathbb{R}$-linear spaces, $\boldsymbol{a}_i \in L_i$ for $1 \leqslant i \leqslant n$, and let $g_i \in L_i^*$. Define the function $G : L_1 \times L_n \longrightarrow \mathbb{R}$ as:

$$G(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = g_1(\boldsymbol{a}_1) \cdots g_n(\boldsymbol{a}_n)$$

for $\boldsymbol{a}_i \in L_i$ and $1 \leqslant i \leqslant n$.
The function G is multilinear. Indeed, if $\boldsymbol{a}_i, \boldsymbol{b}_i \in L_i$ and $a \in \mathbb{R}$ it is immediate to verify that

$$\begin{aligned} & G(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i + \boldsymbol{b}_i, \ldots, \boldsymbol{a}_n) \\ & \quad = \quad G(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) + G(\boldsymbol{a}_1, \ldots, \boldsymbol{b}_i, \ldots, \boldsymbol{a}_n), \end{aligned}$$

and

$$G(\boldsymbol{a}_1, \ldots, a\boldsymbol{a}_i, \ldots, \boldsymbol{a}_n) = aG(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i, \ldots, \boldsymbol{a}_n).$$

Note, however, that G is not a linear function because

$$G(a\boldsymbol{a}_1, \ldots, a\boldsymbol{a}_n) = a^n G(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$$

Example

The function $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ defined by $f(x_1, x_2) = x_1 x_2$ is bilinear because it is linear in each of its variables, separately, but is not linear in the ensemble of its arguments. Indeed, we have

$$\begin{aligned} f(x_1 + y_1, x_2) &= f(x_1, x_2) + f(y_1, x_2), \\ f(x_1, x_2 + y_2) &= f(x_1, x_2) + f(x_1, y_2) \end{aligned}$$

for every $x_1, x_2, y_1, y_2 \in \mathbb{R}$, which shows the bilinearity of f. However, we have:

$$\begin{aligned} f(x_1 + x_2, y_1 + y_2) &= x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2 \\ &\neq f(x_1, y_1) + f(x_2, y_2), \end{aligned}$$

which means that f is not a linear function.

Theorem

Let U, V be two real linear spaces and let $\mathfrak{M}(U, V; \mathbb{R})$ be the linear space of bilinear forms defined on $U \times V$. The linear spaces $\mathfrak{M}(U, V; \mathbb{R})$, $Hom(U, V^*)$ and $Hom(V, U^*)$ are isomorphic.

Proof

It is immediate that Φ is a linear mapping because for $c, d \in \mathbb{R}$ and $h_1, h_2 \in \mathfrak{M}(U, V; \mathbb{R})$ we have:

$$\begin{aligned}
\Phi(ch_1 + dh_2)(\boldsymbol{a})(\boldsymbol{v}) &= ((ch_1 + dh_2)^{\boldsymbol{a}})(\boldsymbol{v}) \\
&= (ch_1 + dh_2)(\boldsymbol{a}, \boldsymbol{v}) = ch_1(\boldsymbol{a}, \boldsymbol{v}) + dh_2(\boldsymbol{a}, \boldsymbol{v}) \\
&= ch_1^{\boldsymbol{a}}(\boldsymbol{v}) + dh_2^{\boldsymbol{a}}(\boldsymbol{v}) \\
&= c\Phi(h_1)(\boldsymbol{a})(\boldsymbol{v}) + d\Phi(h_2)(\boldsymbol{a})(\boldsymbol{v}),
\end{aligned}$$

or

$$\Phi(ch_1 + dh_2) = c\Phi(h_1) + d\Phi(h_2).$$

Note that Φ maps $h : U \longrightarrow V$ into the linear form that transforms $\boldsymbol{a}$ into $h^{\boldsymbol{a}}$ for $\boldsymbol{a} \in U$. Thus, if $\Phi(h_1) = \Phi(h_2)$ we have both h_1 and h_2 yield equal values for $\boldsymbol{a} \in U$, so $h_1 = h_2$, which proves the injectivity of Φ.

Proof cont'd

Let $f \in \text{Hom}(U, V^*)$. For every $\boldsymbol{a} \in U$ there exists a linear form $g : V \longrightarrow \mathbb{R}$ such that $f(\boldsymbol{a}) = g$, or $f(\boldsymbol{a})(\boldsymbol{v}) = g(\boldsymbol{v})$ for every $\boldsymbol{v} \in V$. The mapping $h : U \times V \longrightarrow \mathbb{R}$ defined by $h(\boldsymbol{u}, bfv) = f(\boldsymbol{u})(\boldsymbol{v})$ is bilinear and $\Phi(h)(\boldsymbol{u})(\boldsymbol{v}) = h^{\boldsymbol{u}}(\boldsymbol{v}) = h(\boldsymbol{u}, \boldsymbol{v}) = f(\boldsymbol{u})(\boldsymbol{v})$, which means that $\Phi(h) = f$. Thus, Φ is also surjective and, therefore, it is an isomorphism between the linear spaces $\mathfrak{M}(U, V; \mathbb{R})$, and $\text{Hom}(U, V^*)$.

The existence of an isomorphism between and $\text{Hom}(V, U^*)$ has a similar argument.

The linear space $\mathfrak{M}(U, V; \mathbb{R})$ will also be denoted by $U^* \bigotimes V^*$. We will refer to this space as the *tensor product* of the spaces U and V.

Corollary

Let U, V be two $\mathbb{R}$-linear spaces. Then, $\dim(U \bigotimes V) = \dim(U) \cdot \dim(V)$.

Proof.

Since $\dim(V^*) = \dim(V) = n$, we have $\dim(\text{Hom}(U, V^*)) = mn$. The result follows immediately. □

Let U, V, W be three $\mathbb{R}$-linear spaces of finite dimensions having the bases $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$, $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ and $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_p\}$, respectively, and let $f : U \times V \longrightarrow W$ be a bilinear function. If $\boldsymbol{u} = \sum_{i=1}^{m} a_i \boldsymbol{u}_i \in U$, $\boldsymbol{v} = \sum_{j=1}^{n} b_j \boldsymbol{v}_j$, then

$$f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j f(\boldsymbol{u}_i, \boldsymbol{v}_j).$$

Since $f(\boldsymbol{u}_i, \boldsymbol{v}_j) \in W$ there exist c_{ij}^k such that $f(\boldsymbol{u}_i, \boldsymbol{v}_j) = \sum_{k=1}^{p} c_{ij}^k \boldsymbol{w}_k$, hence

$$f(\boldsymbol{u}, \boldsymbol{v}) = \sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{p} a_i b_j c_{ij}^k w_k.$$

Thus, the set $\{c_{ij}^k \in \mathbb{R} \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n, 1 \leqslant k \leqslant p\}$ (which contains mnp elements) determines a bilinear function relative to the chosen bases in U, V and W.

Unlike the case $n = 1$, the set of values of a multilinear function $f : M_1 \times \cdots \times M_n \longrightarrow M$ is not a subspace of M in general. Indeed, consider a two-dimensional $\mathbb{R}$-linear space U having a basis $\{\boldsymbol{u}_1, \boldsymbol{u}_2\}$, a four-dimensional $\mathbb{R}$-linear space W having the basis $\{\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}_3, \boldsymbol{w}_4\}$, and the bilinear function $f : U \times U \longrightarrow W$ defined as:

$$f(\boldsymbol{u}, \boldsymbol{v}) = u_1 v_1 \boldsymbol{w}_1 + u_1 v_2 \boldsymbol{w}_2 + u_2 v_1 \boldsymbol{w}_3 + u_2 v_2 \boldsymbol{w}_4,$$

where $\boldsymbol{u} = u_1 \boldsymbol{u}_1 + u_2 \boldsymbol{u}_2$ and $\boldsymbol{v} = v_1 \boldsymbol{u}_1 + v_2 \boldsymbol{u}_2$.

Let S be the set of all vectors of the form $\boldsymbol{s} = f(\boldsymbol{u}, \boldsymbol{v})$. By the definition of S there exist $\boldsymbol{u}, \boldsymbol{v} \in U$ such that

$$s_1 = u_1 v_1, s_2 = u_1 v_2, s_3 = u_2 v_1, s_4 = u_2 v_2,$$

hence $s_1 s_4 = s_2 s_3$ for any $\boldsymbol{s} \in S$.
Define the vectors $\boldsymbol{z}, \boldsymbol{t}$ in W as

$$\begin{aligned} \boldsymbol{z} &= 2\boldsymbol{w}_1 + 2\boldsymbol{w}_2 + \boldsymbol{w}_3 + \boldsymbol{w}_4, \\ \boldsymbol{t} &= \boldsymbol{w}_1 + \boldsymbol{w}_3. \end{aligned}$$

Note that we have both $\boldsymbol{z} \in S$ and $\boldsymbol{t} \in S$. However,

$$\boldsymbol{x} = \boldsymbol{z} - \boldsymbol{t} = \boldsymbol{w}_1 + 2\boldsymbol{w}_2 + \boldsymbol{w}_4$$

does not belong to S because $x_1 x_4 = 1$ and $x_2 x_3 = 0$.

Let $f : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}$ be a bilinear form. Since the vectors

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \boldsymbol{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

form a basis in $\mathbb{R}^2$, f can be written as

$$\begin{aligned} & f(a\boldsymbol{e}_1 + b\boldsymbol{e}_2, c\boldsymbol{e}_1 + d\boldsymbol{e}_2) \\ = \; & af(\boldsymbol{e}_1, c\boldsymbol{e}_1 + d\boldsymbol{e}_2) + bf(\boldsymbol{e}_2, c\boldsymbol{e}_1 + d\boldsymbol{e}_2) \\ = \; & acf(\boldsymbol{e}_1, \boldsymbol{e}_1) + adf(\boldsymbol{e}_1, \boldsymbol{e}_2) + bcf(\boldsymbol{e}_2, \boldsymbol{e}_1) + bdf(\boldsymbol{e}_2, \boldsymbol{e}_2) \\ = \; & \alpha f(\boldsymbol{e}_1, \boldsymbol{e}_1) + \beta f(\boldsymbol{e}_1, \boldsymbol{e}_2) + \gamma f(\boldsymbol{e}_2, \boldsymbol{e}_1) + \delta f(\boldsymbol{e}_2, \boldsymbol{e}_2), \end{aligned}$$

where

$$\alpha = ac, \beta = ad, \gamma = bc, \delta = bd.$$

Thus, the multilinearity of f implies $\alpha\delta = \beta\gamma$.