Linear Algebra

Berkant Ustaoğlu

CRYPTOLOUNGE.NET

Linear Transformations

Linear map

Definition (linear map, homomorphism)

Let $\mathbf{V}$ and $\mathbf{W}$ be two vector spaces. A function $L : \mathbf{V} \to \mathbf{W}$ is a *linear map* if

1. $\forall \vec{u}, \vec{v} \in \mathbf{V}, L(\vec{u} + \vec{v}) = L(\vec{u}) + L(\vec{v})$
2. $\forall c \in \mathbb{C}, \forall \vec{u} \in \mathbf{V}, L(c\vec{u}) = cL(\vec{u})$

Isomorphism

Definition (isomorphism)

Let $\mathbf{V}$ and $\mathbf{W}$ be two vector spaces. A linear map $\phi : \mathbf{V} \to \mathbf{W}$ is an *isomorphism* between $\mathbf{U}$ and $\mathbf{V}$ if

1. ϕ is one-to-one and onto (correspondence)
   1.1 onto $\forall \vec{w} \in \mathbf{W}, \exists \vec{v} \in \mathbf{V} : \phi(\vec{v}) = \vec{w}$
   1.2 1-1 $\forall \vec{u}, \vec{v} \in \mathbf{V}, \phi(\vec{u}) = \phi(\vec{v}) \Rightarrow \vec{u} = \vec{v}$

we write $\mathbf{V} \cong \mathbf{W}$ is there is an isomorphism between $\mathbf{V}$ and $\mathbf{W}$. In this case $\mathbf{V}$ is called the *domain* and $\mathbf{W}$ is called the *codomain* of ϕ.

Examples and counterexamples

- identity
- column vectors to row vectors
- polynomials of degree 3 to $\mathbb{C}^3$
- 2×2 upper triangular matrices to $\mathbb{C}^3$
- projection from $\mathbb{C}^2$ to $\mathbb{C}^3$.
- $\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x^3 & y^3 \end{pmatrix}$
- $p(x) \to p(x-1)$

Representation map

Theorem

The representation map from a vector space $\mathbf{V}$ *with basis* $\mathbf{B} = \left\{\vec{b}_1, \ldots, \vec{b}_d\right\}$ *to the vector space of standard column vectors with* d *components* $\mathbb{C}^d$ *is an isomorphism.*

$$\mathcal{R}_B : \mathbf{V} \to \mathbb{C}^d \qquad \mathcal{R}_B(\vec{u}) = \mathcal{R}_B(\alpha_1 \vec{b}_1 + \cdots + \alpha_d \vec{b}_d) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix}_B$$

Linear transformation

Definition (linear transormation)

A linear map from $\mathbf{V}$ to itself is called a *linear transformation*.

Examples

- $\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x & y \end{pmatrix}$
- identity transformation
- $\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} y \\ x \end{pmatrix}$
- representation map
    1. representing $\mathbb{C}^3$
    2. representing CVS
    3. representing polynomials

Linear transformation

Theorem

A homomorphism is determined by its action on a basis: if $\mathbf{V}$ *is a vector space with basis* $\vec{b}_1, \ldots, \vec{b}_n$ *and* $\mathbf{W}$ *is a vector space with elements* $\vec{w}_1, \ldots, \vec{w}_n$ *(perhaps not distinct elements) then there exists a homomorphism from* $\phi : V \to W$ *such that* $\phi(\vec{b}_i) = \vec{w}_i$*, and that homomorphism is unique.*

Examples

$$\phi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \to \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} \qquad \phi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \to \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\phi\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) \to a\begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Linear extentions

Definition

Let $\mathbf{V}$ and $\mathbf{W}$ be two vector spaces and let $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_d\}$ be a basis for $\mathbf{V}$. A function f defined on the basis $\mathcal{B}$ with $f : \mathcal{B} \to \mathbf{W}$ is *extended linearly* to a function $\hat{f} : \mathbf{V} \to \mathbf{W}$ if $\forall \vec{v} \in \mathbf{V}$ with $\vec{v} = \alpha_1 \vec{b}_1 + \cdots + \alpha_d \vec{b}_d$, the action of $\hat{f}$ is defined as

$$\hat{f}(\vec{v}) = \hat{f}(\alpha_1 \vec{b}_1 + \cdots + \alpha_d \vec{b}_d) = \alpha_1 \hat{f}(\vec{b}_1) + \cdots + \alpha_d \hat{f}(\vec{b}_d)$$

Matrix representation

Definition

Let $\mathbf{V}$ and $\mathbf{W}$ are vector spaces of dimensions n and m with bases $B = \left(\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\right)$ and $E = (\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_m)$, and that $\phi : \mathbf{V} \to \mathbf{W}$ is a linear map. If

$$\mathcal{R}_E(\phi(\vec{b}_1)) = \begin{pmatrix} h_{1,1} \\ h_{2,1} \\ \vdots \\ h_{m,1} \end{pmatrix}_E \quad \ldots \quad \mathcal{R}_E(\phi(\vec{b}_n)) = \begin{pmatrix} h_{1,n} \\ h_{2,n} \\ \vdots \\ h_{m,n} \end{pmatrix}_E$$

then

$$\mathcal{R}_{B\to E}(\phi) = \begin{pmatrix} | & | & & | \\ \mathcal{R}_E\left(\phi(\vec{b}_1)\right) & \mathcal{R}_E\left(\phi(\vec{b}_2)\right) & \ldots & \mathcal{R}_E\left(\phi(\vec{b}_n)\right) \\ | & | & & | \end{pmatrix} = \Bigg($$

Example: derivative

derivative $d : \mathbf{P}_3 \to \mathbf{P}_2$

$$\begin{aligned}
\mathbf{P}_3 = \langle B \rangle &= \left\langle \vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4 \right\rangle = \left\langle x^3, x^2, x, 1 \right\rangle \\
= \langle A \rangle &= \langle \vec{a}_1, \vec{a}_2, \vec{a}_3, \vec{a}_4 \rangle = \big\langle x^3 - 2x^2 + 2x + 1, 2x^3 + 3x + 1, \\
&\qquad 2x^3 + x^2 + 3x + 1, -x^3 + x^2 + x + 1 \big\rangle
\end{aligned}$$

$$\begin{aligned}
\mathbf{P}_2 = \langle E \rangle &= \langle \vec{e}_1, \vec{e}_2, \vec{e}_3 \rangle = \left\langle x^2, x, 1 \right\rangle \\
= \langle R \rangle &= \langle \vec{r}_1, \vec{r}_2, \vec{r}_3 \rangle = \left\langle x^2, x^2 + x, x^2 + x + 1 \right\rangle \\
= \langle C \rangle &= \langle \vec{c}_1, \vec{c}_2, \vec{c}_3 \rangle = \left\langle 4x^2 + 3x + 1, 2x^2 + 2x + 1, 3x^2 + x \right\rangle
\end{aligned}$$

Example: derivative

$$\mathcal{R}_{B\to E}(d) = \begin{pmatrix} | & | & | & | \\ \mathcal{R}_E(\vec{b}_1) & \mathcal{R}_E(\vec{b}_2) & \mathcal{R}_E(\vec{b}_3) & \mathcal{R}_E(\vec{b}_3) \\ | & | & | & | \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}_{B\to E}$$

Example:

$\vec{p} = p(x) = -x^3 + 2x^2$ then $d(\vec{p}) = -3x^2 + 4x$ and

$$\vec{p} = -1\vec{b}_1 + 2\vec{b}_2 + 0\vec{b}_3 + 0\vec{b}_4 = -2\vec{a}_1 + 4\vec{a}_2 - 3\vec{a}_3 + 1\vec{a}_4$$

$$\vec{p} = \begin{pmatrix} -1 \\ 2 \\ 0 \\ 0 \end{pmatrix}_B = \begin{pmatrix} -2 \\ 4 \\ -3 \\ 1 \end{pmatrix}_A$$

Example:

$$
\begin{aligned}
\mathcal{R}_E\left(d(\vec{p})\right) &= \mathcal{R}_{B\rightarrow E}(\phi)\mathcal{R}_E(\vec{p}) \\
&= \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}_{B\rightarrow E} \begin{pmatrix} -1 \\ 2 \\ 0 \\ 0 \end{pmatrix}_B \\
&= \begin{pmatrix} -3 \\ 4 \\ 0 \end{pmatrix}_E
\end{aligned}
$$

Example:

$$\mathcal{R}_{A\to E}(d) = \begin{pmatrix} | & | & | & | \\ \mathcal{R}_E(\vec{a}_1) & \mathcal{R}_E(\vec{a}_2) & \mathcal{R}_E(\vec{a}_3) & \mathcal{R}_E(\vec{a}_3) \\ | & | & | & | \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 6 & 6 & -3 \\ -4 & 0 & 2 & 2 \\ 2 & 3 & 3 & 1 \end{pmatrix}_{A\to E}$$

Example:

$$
\begin{aligned}
\mathcal{R}_E\left(d(\vec{p})\right) &= \mathcal{R}_{A\to E}(\phi)\mathcal{R}_A(\vec{p}) \\
&= \begin{pmatrix} 3 & 6 & 6 & -3 \\ -4 & 0 & 2 & 2 \\ 2 & 3 & 3 & 1 \end{pmatrix}_{A\to E} \begin{pmatrix} -2 \\ 4 \\ -3 \\ 1 \end{pmatrix}_A \\
&= \begin{pmatrix} -3 \\ 4 \\ 0 \end{pmatrix}_E
\end{aligned}
$$

Linear transformation

Definition

A linear map (homomorphism) from a vector space $\mathbf{V}$ to itself is called a *linear transformation*

Example

$id : \mathbf{P}_3 \to \mathbf{P}_3$ with bases

$$\begin{aligned}\mathbf{P}_3 = \langle B\rangle \quad &= \left\langle \vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4 \right\rangle = \left\langle x^3, x^2, x, 1 \right\rangle \\ = \langle A\rangle \quad &= \langle \vec{a}_1, \vec{a}_2, \vec{a}_3, \vec{a}_4 \rangle = \left\langle x^3 - 2x^2 + 2x + 1, 2x^3 + 3x + 1, \right. \\ &\qquad \left. 2x^3 + x^2 + 3x + 1, -x^3 + x^2 + x + 1 \right\rangle\end{aligned}$$

Example

$$\mathcal{R}_{B\to A}(id) = \begin{pmatrix} 2 & 0 & -3 & 5 \\ -6 & -1 & 9 & -14 \\ 5 & 1 & -7 & 11 \\ -1 & 0 & 1 & -1 \end{pmatrix}_{B\to A}$$

$$\mathcal{R}_{A\to B}(id) = \begin{pmatrix} 1 & 2 & 2 & -1 \\ -2 & 0 & 1 & 1 \\ 2 & 3 & 3 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}_{A\to B}$$