Lecture 4: Linear Transformations

Today we start Chapter 3.

Basics on Linear Transformations

Definition (Text, Definition 11.2)

Let V and W be vector spaces over $\mathbb{R}$. A linear transformation T from V to W is a function $T : V \longrightarrow W$ such that for all $v_1, v_2 \in V$, $c \in \mathbb{R}$,

(i) $T(v_1 + v_2) = T(v_1) + T(v_2)$

(ii) $T(cv_1) = cT(v_1)$.

We let $\mathrm{Hom}(V, W)$ (text: $L(V, W)$) be the set of linear transformations from V to W.

Proposition

$\mathrm{Hom}(V, W)$ *is a vector space under the operations:*

$$\begin{array}{rcl} (S+T)(v) & := & S(v) + T(v) \\ (c \cdot S)(v) & : & = c(S(v).) \end{array}$$

Proof. Show that $(S + T)$ and $c \cdot T$ are both linear transformations.

Algebra

If $V = W$ then $\mathrm{Hom}(V, W) = \mathrm{End}(V)$ has more structure. It is an associative algebra over $\mathbb{R}$ (i.e., a ring and a vector space).

Definition

An $\mathbb{R}$-vector space $(A, +, \bullet)$ is an **algebra** if it has a binary operation $\bullet : A \times A \longrightarrow A$ (multiplication) that satisfies: for all $a_1, a_2, a_3 \in A$ and $c \in \mathbb{R}$:

(i) $\bullet$ is associative

$$(a_1 \bullet a_2)a_3 = a_1 \bullet (a_2 \bullet a_3)$$

(ii) $\bullet$ is bilinear

$$\begin{aligned} (a_1 + a_2) \bullet a_3 &= a_1 \bullet a_3 + a_2 \bullet a_3 \\ a_1 \bullet (a_2 + a_3) &= a_1 \bullet a_2 + a_1 \bullet a_3 \\ c \cdot (a_1 \bullet a_2) &= (ca_1) \bullet a_2 = a_1 \bullet (ca_2) \end{aligned}$$

(So, $b(a_1, a_2) = a_1 \bullet a_2$ is linear with respect to each of a_1 and a_2).

(iii) There is a unit element 1 for A: $1 \bullet a = a = a \bullet 1$.

Warning: We do not require $\bullet$ to be commutative.

Identity, Center

Proposition

Define $\bullet$ *on* $\mathrm{End}(V)$ *by*

$$S \bullet T = S \circ T.$$

Then $(\mathrm{End}(V), \circ, +, \cdot)$ *is an algebra.*

Note: The unit element is $I =$ identity.

Definition

Given an algebra $(A, \bullet, +, \cdot)$, the **center** of A, denoted $Z(A) := \{a \in A : ab = ba \quad \forall b \in A\}$. That is, the elements of A which commute with all elements of A.

Inverse

Theorem

$Z\left(\text{End}(V)\right) = \{c\mathbb{I}\} : c \in \mathbb{R}.$

Definition

A linear tranformation $T \in \text{End}(V)$ is said to be invertible is there exists an element $S \in \text{End}(V)$ such that $S \circ T = I$ and $T \circ S = I$. We write $S = T^{-1}$. (We will also refer to such elements as units.)

Note: We will often omit the symbol "$\circ$" and simply write ST for $S \circ T$.

Invertibility

Proposition

Let $T \in \mathrm{Hom}(V, W)$. *Then* T *is invertible*
$\iff$ *it is an invertible element of* $\mathrm{Maps}(V, W)$ *(the set of all maps from* V *to* W*)*
$\iff$ T *is 1:1 and onto.*

Proof. ($\Longrightarrow$) Obvious.
($\Longleftarrow$) Suppose there is an inverse mapping F. We claim F is in fact a linear transformation. First, we show that, give $u, v \in V$

$$F(u + v) = F(u) + F(v).$$

But $T(F(u + v)) = u + v$ and
$T(F(u) + F(v)) = T(F(u)) + T(F(v)) = u + v$.

Thus $T(F(u+v)) = T(F(u)) + T(F(v))$ and since T is 1:1 we have $F(u+v) = F(u) + F(v)$.
Similary, $T(F(cu)) = c(u) = cT(F(u)) = T(cF(u))$ and thus $F(cu) = cF(u)$ for all $u \in V$, $c \in \mathbb{R}$. □

We will later see that if V is finite dimensional and $S \in \mathrm{End}(V)$, then

$$\begin{aligned} S \text{ is invertible} \quad &\iff \quad S \text{ is } 1:1 \\ &\iff \quad S \text{ is onto.} \end{aligned}$$

$\mathrm{Aut}(V)$

We write $\mathrm{Aut}(V)$ for the set of all invertible linear transformations of V, so $\mathrm{Aut}(V) \subset \mathrm{End}(V)$.
Warning: $\mathrm{Aut}(V)$ is not a subspace.

$$T \text{ invertible } \implies -T \text{ invertible, but}$$

$$T + (-T) = 0 \text{ is not invertible.}$$

Proposition

$\mathrm{Aut}(V)$ *is a group.*
(What does it mean?)

Definition

A group $(G, \bullet)$ is a set G equipped with a binary operation $\bullet : G \times G \longrightarrow G$ satisfying:

(i) $\bullet$ is associative

(ii) There is an identity element $e \in G$ such that

$$e \bullet g = g \bullet e = g \text{ for all } g \in G$$

(iii) Every element g has an inverse. This means there is an element $g^{-1} \in G$ such that $g \bullet g^{-1} = g^{-1} \bullet g = e$.