MATH 31AH - Homework 4

Merrick Qiu

October 22, 2021

1 Projections

Proof. P_v is linear.

P_v preserves vector addition since

$$\begin{aligned} P_v((v,w)+(v',w')) &= P_v(v+v',w+w') \\ &= v+v' \\ &= P_v(v,w)+P_v(v',w'). \end{aligned}$$

P_v also preserves scalar multiplication since

$$\begin{aligned} P_v(c(v,w)) &= P_v(cv,cw) \\ &= cv \\ &= cP_v(v,w). \end{aligned}$$

Therefore, P_V is a linear map. □

P_v is always surjective since every element $v \in V$ is mapped onto by $(v, 0)$. P_v is only injective when the size of W is 1. If the size of W is greater than 1, then multiple tuples can be projected into V.

2 Linear maps and spanning

Proof. $T(S) := \{T(v) : v \in S\}$ spans $Image(T)$.

Since $Image(T) := \{T(w) : w \in V\}$, we must show that every $T(w)$ can be written as a linear combination of $T(v)$.

Let $v_1, v_2, ..., v_n$ be vectors in $T(S)$ and $c_1, c_2, ..., c_n$ be scalars. We have that

$$\begin{aligned} T(w) &= T(c_1v_1 + c_2v_2 + ... + c_nv_n) \\ &= c_1T(v_1) + c_2T(v_2) + ... + c_nT(v_n) \end{aligned}$$

Therefore, $T(S)$ spans $Image(T)$ since any arbitrary $T(w)$ can be written as a linear combination of vectors in $T(S)$. □

3 Linear maps and independence

Proof. $T(I) := \{T(v) : v \in I\}$ is linearly independent.

Since T is injective and linear, we have that

$$\begin{aligned} c_1T(v_1) + c_2T(v_2) + ... + c_nT(v_n) = 0 &\xrightarrow{Linear} \\ T(c_1v_1 + c_2v_2 + ... + c_nv_n) = 0 &\xrightarrow[T^{-1}(0)=0]{Injective} \\ c_1v_1 + c_2v_2 + ... + c_nv_n = 0 & \end{aligned}$$

Therefore, if a nontrivial linear combination of the vectors in $T(I)$ exists, it would imply that a nontrivial linear combination of vectors in I exists, which contradicts the fact that I is linearly independent. Therefore $T(I)$ is linearly independent.

If T was not injective, then it would be possible for two vectors in V to map to the same vector, which would make $T(I)$ not linearly independent. Therefore, it doesn't hold if the assumption of injectivity is removed. $\square$

4 Representing matrices

$$\begin{aligned} \frac{d}{dx}(c_1x^3 + c_2x^2 + c_3x + c_4) &= 3c_1x^2 + 2c_2x + c_3 \\ &= (3c_1)(x+1)^2 + (-6c_1 + 2c_2)(x+1) + (3c_1 - 2c_2 + c_3)(1) \end{aligned}$$

Therefore,

$$[T]_{\mathcal{C}}^{\mathcal{B}} = \begin{bmatrix} 3 & 0 & 0 & 0 \\ -6 & 2 & 0 & 0 \\ 3 & -2 & 1 & 0 \end{bmatrix}$$

.

5 A matrix map

The Kernel of T is the set of all solutions to the equation $Ax = 0$. This can be found by finding the RREF of A

$$
\begin{aligned}
&\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \quad \begin{array}{l} -4 \\ + \\ \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 7 & 8 & 9 \end{pmatrix} \quad \begin{array}{l} -7 \\ \\ + \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \quad \begin{array}{l} \\ -2 \\ + \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{array}{l} \\ \Big| \cdot -\frac{1}{3} \\ \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{array}{l} + \\ -2 \\ \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}
\end{aligned}
$$

Solutions are in the form $\begin{bmatrix} x_3 \\ -2x_3 \\ x_3 \end{bmatrix}$ so $\{ \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \}$ is a basis for $Ker(T)$.

The image of T is the column space of A. This can be found by finding the RREF of A^T.

$$
\begin{aligned}
&\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} \begin{array}{l} -2 \\ + \\ \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 4 & 7 \\ 0 & -3 & -6 \\ 3 & 6 & 9 \end{pmatrix} \begin{array}{l} -3 \\ \\ + \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 4 & 7 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \begin{array}{l} \\ -2 \\ + \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 4 & 7 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \begin{array}{l} \\ \mid \cdot -\frac{1}{3} \\ \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 4 & 7 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{array}{l} + \\ -4 \\ \end{array} \\
\Rightarrow &\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}
\end{aligned}
$$

The top two rows are a linear combination of the columns of A. Since the third row is all-zeros, $\{ \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \}$ is a basis for $Image(T)$.

6 Inverses of linear maps

Proof. The inverse of a linear transformation T is also linear.

Since T is linear and additivity is preserved, we have that

$$
\begin{aligned}
T(v_1 + v_2) &= T(v_1) + T(v_2) \\
&= w_1 + w_2
\end{aligned}
$$

From this, we have that $T^{-1}(w_1) = v_1$, $T^{-1}(w_2) = v_2$, and $T^{-1}(w_1 + w_2) = v_1 + v_2$. Therefore, we have that

$$
\begin{aligned}
T^{-1}(w_1 + w_2) &= v_1 + v_2 \\
&= T^{-1}(w_1) + T^{-1}(w_2)
\end{aligned}
$$

Since T is linear and scalar multiplication is preserved, we have that

$$
\begin{aligned}
T(cv) &= cT(v) \\
&= cw
\end{aligned}
$$

. From this, we have that $T^{-1}(cw) = cv$ and $T^{-1}(w) = v$. Therefore, $T^{-1}(cw) = cv = cT^{-1}(w)$. Since addition and scalar multiplication are preserved, T^{-1} is a linear transformation. $\square$

7 Polynomial change of basis

These are the transformations of the basis vectors from $\mathcal{B}$ to $\mathcal{C}$:
$1 = 1$
$x + 1 = 2(1) + 1(x - 1)$
$x^2 + x + 1 = 2(1) + 2(x - 1) + (x^2 - x + 1)$
$x^3 + x^2 + x + 1 = 2(1) + 2(x - 1) + 2(x^2 - x + 1) + (x^3 - x^2 + x - 1)$

Therefore, the transition matrix can be written as $[T]_{\mathcal{C}}^{\mathcal{B}} = \begin{bmatrix} 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

These are the transformations of the basis vectors from $\mathcal{C}$ to $\mathcal{B}$:
$1 = 1$
$x - 1 = -2(1) + 1(x + 1)$
$x^2 - x + 1 = 2(1) - 2(x + 1) + 1(x^2 + x + 1)$
$x^3 - x^2 + x - 1 = -2(1) + 2(x + 1) - 2(x^2 + x + 1) + 1(x^3 + x^2 + x + 1)$

Therefore, the transition matrix can be written as $[T]_{\mathcal{B}}^{\mathcal{C}} = \begin{bmatrix} 1 & -2 & 2 & -2 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

8 Invariant subspaces and block matrices

Proof. There exists an ordered basis of V, $\mathcal{B} = (v_1, v_2, ..., v_m, v_{m+1}, v_{m+2}, ..., vn)$, such that $(v_1, v_2, ..., v_m)$ is an ordered basis of W.

Let $(v_1, v_2, ..., v_m)$ be an ordered basis for W. Since W is a finite linearly independent subset of V ,and using problem 7 from problem set 3, $(v_1, v_2, ..., v_m)$ can be completed to formed an ordered basis of V. $\square$

Proof. T is invariant iff the lower-left block of the representing matrix is zeros.

Since $\mathcal{B}$ is linearly independent, none of the vectors $(v_{m+1}, v_{m+2}, ..., v_n)$ can be formed as a linear combination of the vectors from $(v_1, v_2, ..., v_m)$. Since $(v_1, v_2, ..., v_m)$ is a basis for W, the vectors $(v_{m+1}, v_{m+2}, ..., v_n)$ are not in W. Therefore, the corresponding vector in $\mathbb{F}^n$ for a vector $w \in W$ must have zeros in indexes $m + 1$ to n.

If a vector, w, has zeros in indexes $m + 1$ to n, then it will be a linear combination of the vectors in $(v_1, v_2, ..., v_m)$. Since $(v_1, v_2, ..., v_m)$ is a basis for W, then $w \in W$. Therefore a vector is in W if and only if it has zeros in indexes $m + 1$ to n.

W is invariant under T if and only if the any vector with zeros in indexes $m + 1$ to n maintains zeros in indexes $m + 1$ to n after the transformation T. If the bottom left $(n - m) \times (m)$ block of $[T]_{\mathcal{B}}^{\mathcal{B}}$ is not all zeros, then it is possible for $T(w)$ to have a nonzero value in indexes $m + 1$ to n

when w has zero values for these indexes. Therefore W is only invariant under T if and only if the bottom left $(n-m)\times(m)$ block of $[T]_{\mathcal{B}}^{\mathcal{B}}$ is all zeros. $\square$

9 Optional Question

Proof. $\mathbb{F} := 0, 1, 2, ..., p-1 \subseteq \mathbb{K}$

Let $a, b \in \mathbb{F}$. Since the characteristic of $\mathbb{F}$ is p, we have that

$$\begin{aligned}
a+b &= \overbrace{1+1+...+1}^{a}+\overbrace{1+1+...+1}^{b} \\
&= \overbrace{1+1+...+1}^{a+b} \\
&= \overbrace{1+1+...+1}^{np}+\overbrace{1+1+...+1}^{(a+b) \mod p} \\
&= \overbrace{1+1+...+1}^{(a+b) \mod p} \\
&= (a+b) \mod p
\end{aligned}$$

Since $(a+b) \mod p \in \mathbb{F}$, $\mathbb{F}$ is closed under addition.

We also have that

$$\begin{aligned}
ab &= \overbrace{\overbrace{1+1+...+1}^{a}+...+\overbrace{1+1+...+1}^{a}}^{b} \\
&= \overbrace{1+1+...+1}^{ab} \\
&= \overbrace{1+1+...+1}^{np}+\overbrace{1+1+...+1}^{(ab) \mod p} \\
&= \overbrace{1+1+...+1}^{(ab) \mod p} \\
&= (ab) \mod p
\end{aligned}$$

Since $(ab) \mod p \in \mathbb{F}$, $\mathbb{F}$ is closed under multiplication. Since $\mathbb{F}$ is closed under addition and multiplication, $\mathbb{F}$ is a subfield of $\mathbb{K}$. $\square$

Proof. Any finite field has size equal to some power p^r of a prime number p, where $r > 0$ is an integer.

It has already been proven that all fields either have a characteristic that is prime, or a characteristic that is zero. If a field has a size that is not a power of a prime number, then [Proof goes here] $\square$