Algebra II 189-251B **Instructor: Dr. E. Goren.**

Assignment 3

To be submitted by February 2, 12:00

In this assignment V and W are vector spaces over a field $\mathbb{F}$.

1. Let $\mathcal{B} = \{s_1, \dots, s_n\}$ be a basis for V and let $\mathcal{C} = \{t_1, \dots, t_n\}$ be any subset of W. Show that there is a unique linear map $T : V \longrightarrow W$ such that

$$T(s_i) = t_i, \quad i = 1, \dots, n.$$

2. Let $T : V \longrightarrow W$ be a surjective linear map. Prove that if $\dim(V) = \dim(W)$ then T is an isomorphism.

3. **Nilpotent operators**. Let $T : V \longrightarrow V$ be a nilpotent linear operator.[1] Prove that if $n = \dim(V)$ then $T^n \equiv 0$. Show that for every $n \geq 2$ there exists a vector space V of dimension n and a nilpotent linear operator $T : V \longrightarrow V$ such that $T^{n-1} \not\equiv 0$.

4. **Direct sum**. (a) Let U and W be subspaces of a vector space V. Show that $V = U \oplus W$ (internal direct sum) iff every vector $v \in V$ may be written uniquely in the form

$$v = u + w, \quad u \in U,\ w \in W.$$

(b) Take $V = \mathbb{R}^3$. Let

$$U_1 = \text{Span}\left\{ \begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \\ 0 \end{pmatrix} \right\}, \quad U_2 = \text{Span}\left\{ \begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix} \right\}, \quad U_3 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} : x_1 - x_4 + x_3 = 0 \right\}.$$

For each pair of subspaces among U_1, U_2, U_3 determine whether $\mathbb{R}^3$ is their direct sum or not.

(c) Find a 3×3 real matrix A such that the transformation $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$, defined by

$$Tv = Av,$$

is a projection on U_1 along the z-axis (i.e., the kernel is the z-axis).

5. (a) Find a linear map $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ whose image is generated by $(1, 2, 3)$ and $(3, 2, 1)$. Here 'find' means represent by a matrix with respect to the standard basis.

(b) Find a linear map $T : \mathbb{R}^4 \longrightarrow \mathbb{R}^3$ whose kernel is generated by $(1, 2, 3, 4), (0, 1, 0, 1)$.

6. **Rudiments of coding theory II**. How do we construct codes?

Fix a pair of positive integers (n, k). Let $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$ be the field of two elements. Consider the vector space $\mathbb{F}^n$ as column vectors of length n. Consider an $n \times k$ matrix A with entries in $\mathbb{F}$. Then A defines a linear transformation

$$T : \mathbb{F}^k \longrightarrow \mathbb{F}^n, \quad T\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = A\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}.$$

[1] One often calls a linear transformation from a vector space to itself a 'linear operator'.

Assume now that the first k rows of A just consist of the k standard basis vectors of $\mathbb{F}^k$. For example for $n = 4$ and $k = 3$, the matrix A could be taken to be

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ * & * & * \end{pmatrix}$$

(where the $*$ are any elements of $\mathbb{F}$). We call such matrix a *standard* $k \times n$ *generator matrix.*

(i) Show that the image of T is a linear (n, k) code (called a systematic (n, k) code*) and explain how to decode a message.*

(ii) Consider a particular case where $n = k+1$. Let A be a standard $(k+1, k)$ generator matrix whose last row consists of 1's. For example, for $(4, 3)$ we get the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The code we obtain is called a parity check code*. Indeed, prove that the code word assigned to a vector $\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ is of the form $\begin{pmatrix} a_1 \\ \vdots \\ a_k \\ \alpha \end{pmatrix}$ where $\alpha = 0$ if the vector $\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ has an even number of 1's and $\alpha = 1$ if the vector $\begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ has an odd number of ones. Prove that the linear code we obtain is precisely the set of vectors in $\mathbb{F}^{k+1}$ with even number of 1's. Hence, we may check if a word is a code word or not by checking whether it has an even number of 1's or not. Find how many errors this code detects and how many errors it corrects.*

(iii) The most naive way to try and transmit a message clearly is by repeating everything twice. The most naive way to try and transmit a message clearly is by repeating everything twice. Namely, we are using the standard $(2k, k)$ generator matrix $\left(\begin{smallmatrix} I_k \\ I_k \end{smallmatrix}\right)$. How many errors does this detect? correct? Is there a $(2k, k)$ standard code that does better?