1. **Linear functions over $\mathbb{F}^n$.**
   (a) Show that the function $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ defined by $f(x) = Ax$, where $A \in \mathbb{F}^{m \times n}$, is linear.
   (b) Show that any linear function $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ has a representation $f(x) = Ax$ for some $A \in \mathbb{F}^{m \times n}$.
   (c) Show that the representation in part (b) is unique by proving that $Ax = Bx$ for every $x$ implies that $A = B$.

2. **A linear function from convolution.** Suppose that real-valued sequences $\{u(n)\}_{n=-\infty}^{\infty}$ and $\{v(n)\}_{n=-\infty}^{\infty}$ represent the input and output signals of a discrete-time linear time-invariant system with impulse response $h(n) \in \mathbb{R}$, $n \in \mathbb{Z}$. Then, $\{u(n)\}$ and $\{v(n)\}$ are related via convolution as
   $$v(n) = \sum_{k=-\infty}^{\infty} h(k)u(n-k), \quad n \in \mathbb{Z}.$$ 
   Suppose that $u(n) = 0$ for $n < 0$ or $n > N$, and define
   $$x = \begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(N) \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} v(0) \\ v(1) \\ \vdots \\ v(N) \end{bmatrix}.$$ 
   Thus $x$ and $y$ are vectors that capture $N + 1$ values of the input and output signals, respectively.
   (a) Find the matrix $T$ such that 
   $$y = Tx$$ 
   in terms of $h(n)$.
   (b) Describe the structure of $T$. Matrices of this structure are said to be **Toeplitz**.

3. **Adjacency graph.** Consider a simple graph (an undirected graph with no self loops or multiple edges) with $n$ vertices. Let $A \in \mathbb{R}^{n \times n}$ be the adjacency graph, defined by
   $$A_{ij} = \begin{cases} 1 & \text{if there is an edge between vertex } i \text{ and vertex } j, \\ 0 & \text{otherwise.} \end{cases}$$ 
   Note that $A = A^T$ and $A_{ii} = 0$, $i = 1, 2, \ldots, n$, since there are no self loops. Let $B = A^k$, where $k \in \mathbb{Z}$. Given a simple interpretation of $B_{ij}$ in terms of the original graph and $k$. (Hint: Use the concept of a path between two nodes.)
4. **Matrix multiplication.** Let $A, B \in \mathbb{R}^{n \times n}$. Prove or provide a counterexample to each of the following statements.

(a) If $AB = 0$, then $A = 0$ or $B = 0$.
(b) If $A^2 = 0$, then $A = 0$.
(c) If $A^T A = 0$, then $A = 0$.

5. **Affine functions.** A function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ is said to be **affine** if for any $x, y \in \mathbb{R}^n$ and any $\alpha, \beta \in \mathbb{R}$ with $\alpha + \beta = 1$, we have

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y).$$

Note that without the restriction $\alpha + \beta = 1$, this would be the definition of linearity.

(a) Suppose that $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$. Show that the function $f(x) = Ax + b$ is affine.
(b) Prove the converse, namely, show that any affine function $f$ can be represented uniquely as $f(x) = Ax + b$ for some $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$.

(Hint: Consider the linearity of the function $g(x) = f(x) - f(0)$.)

6. **Zero vector.** Using the vector space axioms, show that the zero vector (additive identity) $0$ in any vector space $\mathcal{V}$ over $\mathbb{F}$ must satisfy $\alpha \cdot 0 = 0$ for every $\alpha \in \mathbb{F}$.

7. **Symmetric and Hermitian matrices.** A square matrix $A$ is said to be **symmetric** if its transpose $A^T$ satisfies $A^T = A$, and a complex-valued square matrix $A$ is said to be **Hermitian** if its conjugate transpose $A^H = (\overline{A})^T = \overline{A}^T$ satisfies $A^H = A$. Thus, a real-valued square matrix $A$ is symmetric if and only if it is Hermitian. Which of the following is a vector space?

(a) The set of all $n \times n$ real-valued symmetric matrices over $\mathbb{R}$.
(b) The set of all $n \times n$ complex-valued symmetric matrices over $\mathbb{C}$.
(c) The set of all $n \times n$ complex-valued Hermitian matrices over $\mathbb{R}$.
(d) The set of all $n \times n$ complex-valued Hermitian matrices over $\mathbb{C}$.

For each case, either verify that it is a vector space or prove otherwise.

8. **Differentiation of polynomials.** Let $\mathcal{P}_n$ be the vector space consisting of all polynomials of degree $\leq n$ with real coefficient.

(a) Show that the monomials $x^i$, $i = 0, 1, \ldots, n$, form a basis for $\mathcal{P}_n$.
(b) Consider the transformation $T : \mathcal{P}_n \rightarrow \mathcal{P}_n$ defined by

$$T(p(x)) = \frac{dp(x)}{dx}.$$ 

For example, $T(1 + 3x + x^2) = 3 + 2x$. Show that $T$ is linear.
(c) Using $\{1, x, \ldots, x^n\}$ as a basis, represent the transformation in part (b) by a matrix $A \in \mathbb{R}^{(n+1) \times (n+1)}$. Find the rank of $A$. 


9. **Subspaces.** Let \( V \) and \( W \) be subspaces of a vector space. Which of the following is also a subspace?

(a) *Minkowski sum* \( V + W = \{v + w : v \in V, w \in W\} \).
(b) \( V \cap W \).
(c) \( V \cup W \).

For each case, either verify that it is a subspace or prove otherwise.

10. **Bases.** Find a basis for each of the following subspaces of \( \mathbb{R}^4 \).

(a) All vectors whose components are equal.
(b) All vectors whose components sum to zero.
(c) All vectors orthogonal to both \( \begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix}^T \) and \( \begin{bmatrix} 0 & 0 & 1 & 1 \end{bmatrix}^T \).
(d) All vectors spanned by \( \begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix}^T, \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}^T, \begin{bmatrix} 0 & 0 & 1 & 1 \end{bmatrix}^T \), and \( \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}^T \).

Repeat parts (a)–(d) for \( \mathbb{F}^4_2 \) instead of \( \mathbb{R}^4 \).

11. **Orthogonal complement of a subspace.** Suppose that \( V \) is a subspace of \( \mathbb{F}^n \). Let

\[ V^\perp = \{x \in \mathbb{F}^n : x^T y = 0, \forall y \in V\} \]

be the set of vectors orthogonal to every element in \( V \).

(a) Verify that \( V^\perp \) is a subspace of \( \mathbb{F}^n \).
(b) Suppose that \( V = \text{span}(v_1, v_2, \ldots, v_k) \) for some \( v_1, v_2, \ldots, v_k \in \mathbb{F}^n \). Express \( V \) and \( V^\perp \) as subspaces induced by the matrix \( A = [v_1 \ v_2 \ \cdots \ v_k] \in \mathbb{F}^{n\times k} \) and its transpose \( A^T \).
(c) Show that \( (V^\perp)^\perp = V \).
(d) Show that \( \dim(V) + \dim(V^\perp) = n \).
(e) Show that \( V \subseteq W \) for another subspace \( W \) implies \( W^\perp \subseteq V^\perp \).
(f) Suppose that \( \mathbb{F} = \mathbb{R} \) or \( \mathbb{C} \). Show that every \( x \in \mathbb{F}^n \) can be expressed uniquely as \( x = v + v^\perp \), where \( v \in V \) and \( v^\perp \in V^\perp \). (Hint: Let \( v \) be the projection of \( x \) on \( V \).)

12. **Halfspace.** Suppose that \( a, b \in \mathbb{R}^n \) are two given points. Show that the set of points in \( \mathbb{R}^n \) that are closer to \( a \) than \( b \) is a halfspace, i.e.,

\[ \{x : |x - a| \leq |x - b|\} = \{x : c^T x \leq d\} \]

for appropriate \( c \in \mathbb{R}^n \) and \( d \in \mathbb{R} \).

(a) Find \( c \) and \( d \) explicitly in terms of \( a \) and \( b \).
(b) Draw a picture showing \( a, b, c, \) and the halfspace.
13. **Parity check codes.** Let

\[ G = \begin{bmatrix} I \\ A \end{bmatrix} \in \mathbb{F}_2^{n \times k}, \]

where \( A \in \mathbb{F}_2^{(n-k) \times k} \) and \( n \geq k \). Suppose that a \( k \)-bit message \( x \in \mathbb{F}_2^k \) is encoded into an \( n \)-bit codeword \( y = Gx \in \mathbb{F}_2^n \). This is an example of an \( (n, k) \) binary linear parity check code. In this context, \( G \) is referred to as a **generator** matrix of the code and its range \( \mathcal{R}(G) \) is referred to as the set of codewords or the **codebook**. The additional \( n - k \) bits, or **parity bits**, provide redundant information that can be used for correction (or detection) of errors that occur to the codewords.

(a) Find \( |\mathcal{R}(G)| \) and interpret this value in terms of the codewords of the \( (n, k) \) code.

(b) Let \( H = [A \quad I] \in \mathbb{F}_2^{(n-k) \times n} \). Show that \( HG = 0 \).

(c) Show that \( \mathcal{N}(H) = \mathcal{R}(G) \), namely, \( y \) is a codeword if and only if \( Hy = 0 \). For this reason, \( H \) is referred to as a **parity check matrix** of the code.

(d) Show that \( \mathcal{R}(G) \) and \( \mathcal{R}(H^T) \) are orthogonal complements of each other.

(e) Consider the code with generator matrix \( H^T \) that encodes \( (n-k) \)-bit messages into \( n \)-bit codewords. This \( (n, n-k) \) code is said to be **dual** to the original \( (n, k) \) code with generator matrix \( G \). Find a parity check matrix \( P \) of the dual code, that is, a matrix \( P \) that satisfies \( Py = 0 \) if and only if \( y \) is a codeword of the dual code.

(f) Consider the \( (7, 4) \) **Hamming code**, specified by the generator matrix

\[
G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.
\]

How many codewords are there? List all of them.

(g) Consider the dual code of the \( (7, 4) \) Hamming code in part (f). How many codewords are in the dual code? List all of them.