Applied Linear Algebra: Problem set-2

Instructor: Dwaipayan Mukherjee*
Indian Institute of Technology Bombay, Mumbai- 400076, India

Definitions: (1) For a non-empty set S and a field $\mathbb{F}$, we define $\mathcal{F}[S;\mathbb{F}]$ as $\mathcal{F}[S;\mathbb{F}] := \{f : S \to \mathbb{F}\}$, which is a vector space over $\mathbb{F}$.
(2) The vector space of all polynomials of degree less than or equal to n, with coefficients in the field $\mathbb{F}$, is denoted by $\mathbb{F}[x]_n$.

1. Consider the subspace of all quadratic polynomials over $\mathbb{R}$, given by $\mathbb{R}[x]$. Is the set $G := \{x^2+1, x^2-1, 2x+3, x+3, 5\}$ a generating set for $\mathbb{R}[x]$? Is G linearly independent? Justify your answers.
2. If a vector space $\mathbb{V}$ over $\mathbb{Z}_2$ contains linearly independent vectors x, y, z, then are $x+y, y+z, z+x$ also linearly independent? Justify your answer mathematically.
3. If a vector space $\mathbb{V}$ over a subfield of $\mathbb{C}$ contains linearly independent vectors x, y, z, then show that $x+y, y+z, z+x$ are also linearly independent.
4. Considering $\mathbb{C}$, the set of complex numbers, to be a vector space over $\mathbb{R}$, show that '1 and x are linearly independent' $\iff$ 'x is not a real number'.
5. Are the vectors $v_1 = [1\ 1\ 2\ 4]^T$, $v_2 = [2\ -1\ -5\ 2]^T$, $v_3 = [1\ -1\ -4\ 3]^T$, $v_4 = [2\ 1\ 1\ 6]^T$ linearly independent in $\mathbb{R}^4$? Find a basis for the subspace $\langle\{v_1, v_2, v_3, v_4\}\rangle$.
6. Find a basis for symmetric 3×3 matrices, having real entries, as a vector space over $\mathbb{R}$.
7. Consider the vector space $\mathbb{F}^{2\times 2}$ ($\mathbb{F}$ is any field). Obtain a basis for this vector space, say $\mathcal{B} = \{A_1, A_2, A_3, A_4\}$, such that $A_i^2 = A_i,\ i = 1, 2, 3, 4$. Establish that your answer is indeed a valid basis.
8. Suppose $\{v_1, v_2, v_3\}$ is a basis for the vector space $\mathbb{V}$ over the the field $\mathbb{F}$. Is the set $\{v_1+v_2+v_3, v_2+v_3, v_3\}$ also a basis for $\mathbb{V}$? Justify your answer mathematically.
9. Prove that if $\{v_1, v_2, \ldots, v_{n-1}, v_n\}$ is a basis for the finite dimensional vector space $\mathbb{V}$, then so is the set $\{v_1 - v_2, v_2 - v_3, \ldots, v_{n-1} - v_n, v_n\}$.
10. Delineate a constructive method for obtaining the basis of $\mathbb{W}_1 \cap \mathbb{W}_2$ when the bases for the finite dimensional vector spaces $\mathbb{W}_1$ and $\mathbb{W}_2$ are given.
11. In the vector space $\mathbb{F}^{2\times 2}$ over $\mathbb{F}$, consider the following subspaces: $\mathbb{W}_1 \subseteq \mathbb{F}^{2\times 2}$ such that it contains matrices of the form $\begin{bmatrix}\alpha & -\alpha \\ \beta & \gamma\end{bmatrix}$ with $\alpha, \beta, \gamma \in \mathbb{F}$ and $\mathbb{W}_2 \subseteq \mathbb{F}^{2\times 2}$ such that it contains matrices of the form $\begin{bmatrix}p & q \\ -p & r\end{bmatrix}$ with $p, q, r \in \mathbb{F}$. What are the dimensions of $\mathbb{W}_1$, $\mathbb{W}_2$, $\mathbb{W}_1 \cap \mathbb{W}_2$, and $\mathbb{W}_1 + \mathbb{W}_2$?
12. For $A \in \mathbb{F}^{m\times n}$, $B \in \mathbb{F}^{n\times p}$, and $C = AB$, prove that $\text{rank}(C) \leq \min(\text{rank}(A), \text{rank}(B))$.
13. For the vectors $v_1 = [1\ 1\ 2\ 4]^T$, $v_2 = [2\ -1\ -5\ 2]^T$, $v_3 = [1\ -1\ -4\ 0]^T$, consider the subspaces $\mathbb{W}_1 := \text{span}(v_1, v_2)$ and $\mathbb{W}_2 := \text{span}(v_2, v_3)$.
    (a) Obtain a basis for $\mathbb{W}_1 \cap \mathbb{W}_2$.
    (b) Compute $\dim(\mathbb{W}_1 + \mathbb{W}_2)$.
14. Consider $\mathbb{W} := \{p \in \mathbb{F}[x]_3 : p(x) = a_0 + a_1 x + a_2 x^2 + (a_0 + a_1 - a_2)x^3, a_0, a_1, a_2 \in \mathbb{F}\}$. Show that $\mathbb{W}$ is a subspace of $\mathbb{F}[x]_3$. Obtain a basis for $\mathbb{W}$ and hence evaluate $\dim(\mathbb{W})$. Suppose $p_1(x) = 1 + x + x^2 + x^3$ and $p_2(x) = 1 + x^2$. Show that $S = \{p_1, p_2\}$ is a linearly independent set in $\mathbb{W}$. Extend S to a basis for $\mathbb{W}$.
15. For any finite dimensional vector space, $\mathbb{V}$, show that there exist subspaces $\mathbb{W}_1$ and $\mathbb{W}_2$ of $\mathbb{V}$ such that $\mathbb{V} = \mathbb{W}_1 \oplus \mathbb{W}_2$.
16. For $A, B \in \mathbb{R}^{n\times n}$, we have $\text{rank}(A+B) \leq \text{rank}(A) + \text{rank}(B)$. Prove or disprove the assertion.
17. For a finite dimensional vector space, $\mathbb{V}$, suppose there exist subspaces $\mathbb{W}_i$, $i \in \{1, 2, \ldots, m\}$ such that $\mathbb{V} = \oplus_{i=1}^m \mathbb{W}_i$. Show that $\dim(\mathbb{V}) = \sum_{i=1}^m \dim(\mathbb{W}_i)$.
18. Show that $\langle\{1, \cos x, \sin x\}\rangle$ and $\langle\{1, e^{ix}, e^{-ix}\}\rangle$ over $\mathbb{C}$ are the same vector space, say $\mathbb{V}$. Also show that $\{1, \cos x, \sin x\}$ and $\{1, e^{ix}, e^{-ix}\}$ are both bases for $\mathbb{V}$. Obtain the basis transformation matrix between them.

*Asst. Professor, Electrical Engineering, Office: EE 214D, e-mail: dm@ee.iitb.ac.in.

19. Provide an example of each of the following: (a) an injective map from $\mathbb{R}^2$ to $\mathbb{R}^2$, and (b) a surjective map from $\mathbb{R}^2$ to $\mathbb{R}^2$. Can you cook up similar examples from $\mathbb{R}^2$ to $\mathbb{R}^3$? Is it possible to do so from $\mathbb{R}^3$ to $\mathbb{R}^2$? Justify if these are not possible, or provide examples if they are possible.

20. Suppose $\phi : \mathbb{V} \to \mathbb{W}$ is a linear map between two finite dimensional vector spaces. Prove that "ϕ is injective" $\implies$ $\dim(\mathbb{V}) \leq \dim(\mathbb{W})$ and "ϕ is surjective" $\implies$ $\dim(\mathbb{V}) \geq \dim(\mathbb{W})$.

21. Consider a 3×3 matrix of real entries, say $A \in \mathbb{R}^{3\times 3}$ which is used to define a linear transformation $\phi : \mathbb{R}^{3\times 3} \to \mathbb{R}^{3\times 3}$ such that $\phi(X) := AX$. Describe clearly, with suitable mathematical justifications, how you will determine the rank of ϕ.

22. For a linear map $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ that sends the vector (x_1, x_2) to $(-x_2, x_1)$, show that $\varphi^2 = -\text{identity}$. Obtain $[\varphi]_{\mathcal{B}}$, where $\mathcal{B} = \{(1, 2), (-1, 1)\}$. Further, show that for any $\lambda \in \mathbb{R}$, $(\varphi - \lambda \cdot \text{identity})$ is invertible. Can you obtain a unique basis, $\mathcal{B}'$ for $\mathbb{R}^2$, such that $[\varphi]_{\mathcal{B}'} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$? Justify with proper calculations.

23. Suppose $T : \mathbb{R}^3 \to \mathbb{R}^2$ be a linear map such that $T(p_1, p_2, p_3) = (p_1 - p_2, 5p_3 - 2p_2)$. If $\mathcal{B}$ and $\mathcal{B}'$ are the standard bases in $\mathbb{R}^3$ and $\mathbb{R}^2$, respectively, obtain the matrix representation of T relative to $\mathcal{B}$ and $\mathcal{B}'$. Suppose instead someone chooses $\mathcal{B} = \{(-1, 0, 1), (1, -1, 1), (1, 0, 0)\}$ and $\mathcal{B}' = \{(1, 1), (0, 1)\}$, how would (s)he rewrite the same matrix representation?

24. Suppose $\mathbb{V}$ is the vector space of all polynomials having real coefficients with degree less than or equal to $n < \infty$. Let $\mathcal{B} = \{f_0, f_1, \ldots, f_n\}$ and $\mathcal{B}' = \{g_0, g_1, \ldots, g_n\}$ be two ordered bases for $\mathbb{V}$ such that $f_i = x^i$ and $g_i = (x + \alpha)^i$ for some scalar α. Represent the differentiation operator, $\mathcal{D} : \mathbb{V} \to \mathbb{V}$ in both these ordered bases, using basis transformation. What do you observe?

25. Consider the same vector space as in Qn. 24 with the ordered basis $\mathcal{B}$, and $n = 3$. Consider the linear operator $\hat{\mathcal{D}} : \mathbb{V} \to \mathbb{V}$ given by $\hat{\mathcal{D}}(f(x)) = 3f(x) + (3 - x)\frac{d}{dx}(f(x))$. Obtain bases for $\text{Ker}(\hat{\mathcal{D}})$ and $\text{Im}(\hat{\mathcal{D}})$. Suppose $g(x) = 7 + 8x$. What are all possible solutions of $\hat{\mathcal{D}}(f(x)) = g(x)$?

26. For vector spaces $\mathbb{U}$, $\mathbb{V}$, and $\mathbb{W}$, of which $\mathbb{U}$, and $\mathbb{V}$ are finite dimensional, consider two linear transformations $\tau : \mathbb{U} \to \mathbb{V}$ and $\psi : \mathbb{V} \to \mathbb{W}$. Suppose the composition of the two transformations is given by $\psi \circ \tau$. Establish that $\dim(\text{Ker}(\psi \circ \tau)) \leq \dim(\text{Ker}(\tau)) + \dim(\text{Ker}(\psi))$. When does equality hold? What can you say about the inequality when τ is surjective?

27. (*Cryptography: Hill cipher*) A common way of encoding messages is to associate distinct positive integers with each letter of the alphabet. For instance, a very basic encoding would be to choose $A \to 1, B \to 2, C \to 3, \ldots, Z \to 26$. However, this can be easily cracked if it falls into the hands of an adversary. To add a level of security, the messenger and receiver both agree upon a predetermined invertible matrix, say $A \in \mathbb{R}^{n\times n}$. Thereafter, the sender splits up the message (without spaces!) into chunks of n consecutive letters in the message leading to vectors in $\mathbb{R}^n$. If the total number of letters is not a multiple of n, the remaining spaces are filled by a place-holder number such as 27. Thereafter, the matrix acts on each of the vectors and yields transformed vectors as the output, which are then sequentially transmitted to the receiver. The receiver then decodes this message by passing each of these transformed vectors it received through A^{-1}. Then the message is read by mapping the numbers to their corresponding letters.

    Example: Suppose the message is 'I SEE' and the matrix is $A = \begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix} \in \mathbb{R}^{2\times 2}$ (with $n = 2$). Then the sender, using an encoder machine, first converts the message into $\{9, 19, 5, 5\}$, splits it up into two vectors $v_1 = [9\ 19]^T$, $v_2 = [5\ 5]^T$, operates on v_1 and v_2 using A to get $y_1 = Av_1 = [-10\ 37]^T$ and $y_2 = Av_2 = [0\ 15]^T$, and then transmits y_1 and y_2 sequentially to the receiver. The receiver then recovers $v_1 = A^{-1}y_1$ and $v_2 = A^{-1}y_2$ using a decoder, which then reads the message by replacing the numbers with suitable letters.

    Suppose it is known that an adversary uses this form of coding with $n = 3$ but the matrix is unknown to you. However, your spies have managed to steal a model of this encoder machine, used by the sender, and you can now experiment with this machine (without ripping it open!) to find out what this matrix is. You decide to send the message 'LET ME TRY' (without spaces, of course, and using 27 as the place-holder), and obtain a series of numbers at the output.

    (a) Determine the matrix $A \in \mathbb{R}^{3\times 3}$ if the encoder gives an output sequence $\{17, -8, 37, 18, -7, 38, 43, -9, 70\}$ for the chosen message. Give an example of a message (not necessarily meaningful words), using which you will certainly not be able to determine the matrix A.

    (b) Suppose your friend playfully decides to send you a message using this encoder, which you read as the sequence of numbers given by $\{21, -6, 36, 27, 10, 39, 23, 4, 28, 19, 0, 20, 19, 7, 24, 20, 1, 21\}$ at the output of the encoder. What is your friend trying to tell you?

We [he and Halmos] share a philosophy about linear algebra: we think basis-free, we write basis-free, but when the chips are down we close the office door and compute with matrices like fury.

–'Paul Halmos: Celebrating 50 Years of Mathematics', Irving Kaplansky