Linear Algebra Done Right

Notes – Linear Algebra

Zhijie Chen

December 22, 2024

Contents

Prerequisites

We declare several notations below for convenience and clarity.

Notations 1 (Basic notations)**.**

- $\mathbb{F}$ denotes a number field (often $\mathbb{R}$ or $\mathbb{C}$).
- $\boldsymbol{U}$, $\boldsymbol{V}$, $\boldsymbol{W}$ denotes vector spaces (usually over scalar field $\mathbb{F}$).
- $\boldsymbol{V}^S$ denotes the set of functions from a nonempty set S to $\boldsymbol{V}$.

Vector Spaces

Definition 2. The complexification of $\boldsymbol{V}$, denoted by $\boldsymbol{V}_\mathbb{C}$, equals $\boldsymbol{V} \times \boldsymbol{V}$ with normal addition and real scalar multiplication for product space. But we write an element (u, v) of $\boldsymbol{V}_\mathbb{C}$ as $u + iv$. Complex scalar multiplication is defined by

$$(a + bi)(\boldsymbol{u} + i\boldsymbol{v}) = (a\boldsymbol{u} - b\boldsymbol{v}) + i(a\boldsymbol{v} + b\boldsymbol{u})$$

for all $a, b \in \mathbb{R}$ and all $\boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{V}$.[1]

[1] Think of $\boldsymbol{V}$ as a subset of $\boldsymbol{V}_\mathbb{C}$ by identifying $\boldsymbol{u} \in \boldsymbol{V}$ with $\boldsymbol{u} + i0$. The construction of $\boldsymbol{V}_\mathbb{C}$ from $\boldsymbol{V}$ can then be thought of as generalizing the construction of $\mathbb{C}^n$ from $\mathbb{R}^n$.

Lemma 3 (Linear dependence lemma)**.** *Suppose $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ is a linearly dependent set in $\boldsymbol{V}$. Then there exists $k \in \{1, 2, \ldots, m\}$ s.t.*

$$\boldsymbol{v}_k \in \operatorname{span}\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}\,.$$

Further more, removing the k^{th} term from the list does not change the span.[2]

[2] The lemma lays the foundation for a series of basic results for vector spaces.

Theorem 4. *Any two bases of a finite-dimensional vector space have the same length.*[3]

[3] This proposition ensures that *dimension* is well-defined.

Proof. Suppose $\boldsymbol{V}$ is finite-dimensional. Let B_1 and B_2 be two bases of $\boldsymbol{V}$. Considering B_1 as an independent set and B_2 as a spanning set leads to $\#B_1 \le \#B_2$. Interchanging the roles of B_1 and B_2 and we have $\#B_2 \le \#B_1$. Thus $\#B_1 = \#B_2$. □

Linear Maps

Kernal and Image of Linear Maps

Exercise 5. Suppose $\boldsymbol{U}$ and $\boldsymbol{V}$ are finite-dimensional and $S \in \mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$ and $T \in \mathcal{L}(\boldsymbol{U}, \boldsymbol{V})$. Prove that

$$\dim\ker ST \le \dim\ker S + \dim\ker T.$$

Proof. Restrict to $Z = \ker ST$. By the fundamental theorem of linear maps,

$$\begin{aligned}
\dim Z &= \dim T(Z) + \dim\ker T|_Z \\
&\le \dim T(Z) + \dim\ker T \\
&= \dim ST(Z) + \dim\ker S|_{T(Z)} + \dim\ker T \\
&\le \dim\ker S + \dim\ker T.
\end{aligned}$$

□

Corollary 6 (Sylvester's rank inequality)**.** *Suppose $A \in \mathbb{F}^{m,n}$ and $B \in \mathbb{F}^{n,p}$ are two matrices. Then*[4]

$$\operatorname{rank} A + \operatorname{rank} B - n \leq \operatorname{rank}(AB)\,.$$

[4] There is a slicker proof for this inequality using block matrices. But the proof here using linear maps is more informative.

Products and Quotients of Vector Spaces

Lemma 7. *Suppose $\boldsymbol{V}_1, \ldots, \boldsymbol{V}_m$ are subspaces of $\boldsymbol{V}$.*[5] *Define a linear map $\Gamma : \boldsymbol{V}_1 \times \cdots \times \boldsymbol{V}_m \to \boldsymbol{V}_1 + \cdots + \boldsymbol{V}_m$ by*

$$\Gamma(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) = \boldsymbol{v}_1 + \cdots + \boldsymbol{v}_m.$$

Then $\boldsymbol{V}_1 + \cdots + \boldsymbol{V}_m$ is a direct sum if and only if Γ is injective.

[5] Note that $\boldsymbol{V}$ does not have to be finite-dimensional. Recall that $\boldsymbol{V}_1 + \cdots + \boldsymbol{V}_m$ is a direct sum if and only if the only way to write $\boldsymbol{0}$ as a sum of $\boldsymbol{v}_1 + \cdots + \boldsymbol{v}_m$, where each $\boldsymbol{v}_k \in \boldsymbol{V}_k$, is by taking each $\boldsymbol{v}_k$ equal to $\boldsymbol{0}$.

Theorem 8. *Suppose $\boldsymbol{V}$ is finite-dimensional and $\boldsymbol{V}_1, \ldots, \boldsymbol{V}_m$ are subspaces of $\boldsymbol{V}$. Then $\boldsymbol{V}_1 + \cdots + \boldsymbol{V}_m$ is a direct sum if and only* $\dim(\boldsymbol{V}_1 + \cdots + \boldsymbol{V}_m) = \dim \boldsymbol{V}_1 + \cdots + \dim \boldsymbol{V}_m$.

Proof. Recall Lemma 7. Because Γ is surjective, by the fundamental theorem of linear maps, $\boldsymbol{V}_1 + \cdots + \boldsymbol{V}_m$ is a direct sum if and only if $\dim(\boldsymbol{V}_1 + \cdots + \boldsymbol{V}_m) = \dim(\boldsymbol{V}_1 \times \cdots \times \boldsymbol{V}_m) = \dim \boldsymbol{V}_1 + \cdots + \dim \boldsymbol{V}_m$. $\square$

Notation 9. Suppose $T \in \mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$. Define $\tilde{T} : \boldsymbol{V} + \ker \boldsymbol{V} \to \boldsymbol{V}$ by

$$\tilde{T}(\boldsymbol{v} + \ker T) = T\boldsymbol{v}.$$

Exercise 10. Suppose $\boldsymbol{V}_1, \ldots, \boldsymbol{V}_m$ are vector spaces. Prove that $\mathcal{L}(\boldsymbol{V}_1 \times \cdots \times \boldsymbol{V}_m, \boldsymbol{W})$ and $\mathcal{L}(\boldsymbol{V}_1, \boldsymbol{W}) \times \cdots \times \mathcal{L}(\boldsymbol{V}_m, \boldsymbol{W})$ are isomorphic vector spaces.

Proof. We construct an isomorphism T between the two vector spaces.

For every $\Gamma \in \mathcal{L}(\boldsymbol{V}_1 \times \cdots \times \boldsymbol{V}_m, \boldsymbol{W})$, define $\varphi_i : \boldsymbol{V}_i \to \boldsymbol{W}$ for each $i \in \{1, \ldots, m\}$ by

$$\varphi_i(\boldsymbol{v}_i) = \Gamma(\boldsymbol{0}, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{0})$$

with $\boldsymbol{v}_i$ in the i^{th} slot and $\boldsymbol{0}$ in all other slots. It can be verified that $\varphi_i \in \mathcal{L}(\boldsymbol{V}_i, \boldsymbol{W})$.

Let $T(\Gamma) = (\varphi_1, \ldots, \varphi_m)$. It can be verified that T is a linear map. We prove T is an isomorphism by constructing its inverse linear map S.

For every $(\varphi_1, \ldots, \varphi_m) \in \mathcal{L}(\boldsymbol{V}_1, \boldsymbol{W}) \times \cdots \times \mathcal{L}(\boldsymbol{V}_m, \boldsymbol{W})$, let

$$S(\varphi_1, \ldots, \varphi_m)\,(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) = \varphi_1(\boldsymbol{v}_1) + \cdots + \varphi_m(\boldsymbol{v}_m)\,.$$

It can be shown that S is a linear map, and that $S \circ T = I$ and $T \circ S = I$, where I is the identity operator on the proper vector space. That proves T is indeed an isomorphism between the two vector spaces, as desired. $\square$

Theorem 11. *A nonempty subset A of $\boldsymbol{V}$ is a translate of some subspace of $\boldsymbol{V}$ if and only if $\lambda\boldsymbol{v} + (1 - \lambda)\,\boldsymbol{w} \in A$ for all $\boldsymbol{v}, \boldsymbol{w} \in A$ and all $\lambda \in \mathbb{F}$.*

Exercise 12. Suppose $A_1 = \boldsymbol{v} + \boldsymbol{U}_1$ and $A_2 = \boldsymbol{w} + \boldsymbol{U}_2$ for some $\boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{V}$ and some subspaces $\boldsymbol{U}_1$, $\boldsymbol{U}_2$ of $\boldsymbol{V}$. Prove that $A_1 \cap A_2$ is either the empty set or a translate of some subspace of $\boldsymbol{V}$.[6]

[6] Recall Theorem 11.

Proposition 13. *Suppose $\boldsymbol{U}$ is a subspace of $\boldsymbol{V}$ and $v_1 + \boldsymbol{U}, \ldots, v_m + \boldsymbol{U}$ is a basis of $\boldsymbol{V}/\boldsymbol{U}$ and $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ is a basis of $\boldsymbol{U}$. Then $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ is a basis of $\boldsymbol{V}$. In other words, $\boldsymbol{V} = \operatorname{span}\{v_1, \ldots, v_m\} \oplus \boldsymbol{U}$.*[7]

[7] $\boldsymbol{V} = \operatorname{span}\{v_1, \ldots, v_m\} \oplus \boldsymbol{U}$ still holds without the hypothesis that $\boldsymbol{U}$ is finite-dimensional.

Exercise 14. Suppose $\boldsymbol{U}$ is a subspace of $\boldsymbol{V}$ s.t. $\boldsymbol{V}/\boldsymbol{U}$ is finite-dimensional.

(a) Show that if $\boldsymbol{W}$ is a finite-dimensional subspace of $\boldsymbol{V}$ and $\boldsymbol{V} = \boldsymbol{U} + \boldsymbol{W}$, then $\dim \boldsymbol{W} \geq \dim \boldsymbol{V}/\boldsymbol{U}$.

(b) Prove that there exists a finite-dimensional subspace $\boldsymbol{W}$ of $\boldsymbol{V}$ s.t. $\dim \boldsymbol{W} = \dim \boldsymbol{V}/\boldsymbol{U}$ and $\boldsymbol{V} = \boldsymbol{U} \oplus \boldsymbol{W}$.

Proof. Let $\overline{\boldsymbol{w}}_1 + \boldsymbol{U}, \ldots, \overline{\boldsymbol{w}}_m + \boldsymbol{U}$ be a basis of $\boldsymbol{V}/\boldsymbol{U}$. Then by Proposition 13, we have $\boldsymbol{V} = \operatorname{span}\{\overline{\boldsymbol{w}}_1, \ldots, \overline{\boldsymbol{w}}_m\} \oplus \boldsymbol{U}$. Let $W_0 = \operatorname{span}\{\overline{\boldsymbol{w}}_1, \ldots, \overline{\boldsymbol{w}}_m\}$, then $\boldsymbol{V} = \boldsymbol{U} \oplus W_0$, as desired.

Now we prove that for each subspace $\boldsymbol{W}$ of $\boldsymbol{V}$ s.t. $\boldsymbol{V} = \boldsymbol{U} + \boldsymbol{W}$, we have $\dim \boldsymbol{W} \geq m = \dim \boldsymbol{V}/\boldsymbol{U}$.

For each $\overline{\boldsymbol{w}}_i \in \boldsymbol{V}$ above, by definition we have $\overline{\boldsymbol{w}}_i = \boldsymbol{u}_i + \boldsymbol{w}_i$ for some $\boldsymbol{u}_i \in \boldsymbol{U}$ and $\boldsymbol{w}_i \in \boldsymbol{W}$. It can be shown from the linear independence of $\overline{\boldsymbol{w}}_1 + \boldsymbol{U}, \ldots, \overline{\boldsymbol{w}}_m + \boldsymbol{U}$ that $\overline{\boldsymbol{w}}_1 - \boldsymbol{u}_1, \ldots, \overline{\boldsymbol{w}}_m - \boldsymbol{u}_m$ are independent vectors in $\boldsymbol{W}$. Hence $\dim \boldsymbol{W} \geq m$. $\square$

Duality

Theorem 15. *Suppose $\boldsymbol{V}$ and $\boldsymbol{W}$ are finite-dimensional and $T \in \mathcal{L}(\boldsymbol{V}, \boldsymbol{W})$. Then*

$$T \text{ is surjective} \iff T' \text{ is injective} \quad \text{and} \quad T \text{ is injective} \iff T' \text{ is surjective.}$$[8]

[8] This result can be useful because sometimes it is easier to verify that T' is injective (surjective) than to show directly that T is surjective (injective).

Proposition 16. *Suppose $\boldsymbol{V}$ is finite-dimensional and $\boldsymbol{U}$ is a subspace of $\boldsymbol{V}$. Then*[9]

$$\boldsymbol{U} = \left\{ v \in \boldsymbol{V} : \varphi(v) = \boldsymbol{0} \text{ for every } \varphi \in \boldsymbol{U}^0 \right\}.$$

[9] The proposition can be easily verified from definition. But it can be useful.

Exercise 17. Suppose $\boldsymbol{V}$ is finite-dimensional and $\boldsymbol{U}$ and $\boldsymbol{W}$ are subspaces of $\boldsymbol{V}$.

(a) Prove that $\boldsymbol{W}^0 \subseteq \boldsymbol{U}^0$ if and only if $\boldsymbol{U} \subseteq \boldsymbol{W}$.

(b) Prove that $\boldsymbol{W}^0 = \boldsymbol{U}^0$ if and only if $\boldsymbol{U} = \boldsymbol{W}$.[10]

[10] Recall Proposition 16.

Exercise 18. Suppose $\boldsymbol{V}$ is finite-dimensional and $\boldsymbol{U}$ and $\boldsymbol{W}$ are subspaces of $\boldsymbol{V}$.

(a) Prove that $(\boldsymbol{U} + \boldsymbol{W})^0 = \boldsymbol{U}^0 \cap \boldsymbol{W}^0$.

(b) Prove that $(\boldsymbol{U} \cap \boldsymbol{W})^0 = \boldsymbol{U}^0 + \boldsymbol{W}^0$.

Lemma 19. *Suppose $\boldsymbol{V}$ is finite-dimensional. $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is a basis of $\boldsymbol{V}$. Then $\varphi_1, \ldots, \varphi_n \in \boldsymbol{V}'$ is the dual basis of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ if and only if*

$$\begin{bmatrix} \mathcal{M}(\varphi_1) \\ \vdots \\ \mathcal{M}(\varphi_n) \end{bmatrix} = I$$

where $\mathcal{M}(\varphi_i)$ is the $1 \times n$ matrix of φ_i with respect to basis $\boldsymbol{v}_1, \ldots \boldsymbol{v}_n$ of $\boldsymbol{V}$ for each $i \in \{1, \ldots, n\}$.

Exercise 20. Suppose $\boldsymbol{V}$ is finite-dimensional and $\varphi_1, \dots, \varphi_n$ is a basis of $\boldsymbol{V}'$. Prove that there exists a basis of $\boldsymbol{V}$ whose dual basis is $\varphi_1, \dots, \varphi_n$.

Proof. We start from an arbitrary basis $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ of $\boldsymbol{V}$. Let $\psi_1, \dots, \psi_n$ be its dual basis. In this proof, we take standard basis $e_1, \dots, e_n$ as the basis of $\mathbb{F}^n$.

Define $S, T \in \mathcal{L}(\boldsymbol{V}, \mathbb{F}^n)$ by

$$T(\boldsymbol{v}) = (\varphi_1(\boldsymbol{v}), \dots, \varphi_n(\boldsymbol{v}))\,, S(\boldsymbol{v}) = (\psi_1(\boldsymbol{v}), \dots, \psi_n(\boldsymbol{v}))\,.$$

Then by Lemma 19, $\mathcal{M}(S, (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) = I$.

Let A be the change of basis matrix from ψ's to φ's, i.e.,

$$A = \mathcal{M}(I, (\psi_1, \dots, \psi_n), (\varphi_1, \dots, \varphi_n))\,.$$

Then by the definition of change of basis matrix, we have

$$\mathcal{M}(T, (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) = \begin{bmatrix} \mathcal{M}(\varphi_1, (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) \\ \vdots \\ \mathcal{M}(\varphi_n, (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) \end{bmatrix}$$

$$= A^\intercal \begin{bmatrix} \mathcal{M}(\psi_1, (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) \\ \vdots \\ \mathcal{M}(\psi_n, (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) \end{bmatrix} = A^\intercal \mathcal{M}(S, (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)) = A^\intercal.$$

Consider basis $\overline{\boldsymbol{v}}_1, \dots, \overline{\boldsymbol{v}}_n$ of $\boldsymbol{V}$ s.t. the change of basis matrix from $\boldsymbol{v}$'s to $\overline{\boldsymbol{v}}$'s is $A^\intercal$. Thus

$$\mathcal{M}(T, (\overline{\boldsymbol{v}}_1, \dots, \overline{\boldsymbol{v}}_n)) = \mathcal{M}(T, (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n))\, \mathcal{M}(I, (\overline{\boldsymbol{v}}_1, \dots, \overline{\boldsymbol{v}}_n), (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)) = I.$$

Then by Lemma 19, the dual basis of $\overline{\boldsymbol{v}}_1, \dots, \overline{\boldsymbol{v}}_n$ is precisely $\varphi_1, \dots, \varphi_n$, as desired. □

Polynomials

Theorem 21 (Division algorithm for polynomials)**.** *Suppose that $p, s \in \mathcal{P}(\mathbb{F})$, with $s \neq 0$. Then there exist unique polynomials $q, r \in \mathcal{P}(\mathbb{F})$ s.t. $p = sq + r$.*[11]

Proof. Let $n = \deg p$ and $m = \deg s$. The case where $n < m$ is trivial. Thus we now assume that $n \geq m$.

The list

$$1, z, \dots, z^{m-1}, s, zs, \dots, z^{n-m}s$$

is linearly independent in $\mathcal{P}_n(\mathbb{F})$. And it also has length $n+1$. Hence the list is a basis of $\mathcal{P}_n(\mathbb{F})$.

Because $p \in \mathcal{P}_n(\mathbb{F})$, there exist unique constants $a_0, \dots, a_{m-1}, b_0, \dots, b_{n-m} \in \mathbb{F}$ s.t.

$$p = a_0 + a_1 z + \cdots + a_{m-1}z^{m-1} + b_0 s + b_1 zs + \cdots + b_{n-m}z^{n-m}s$$

[11] The division algorithm for polynomials can be proved without using any linear algebra. This proof makes a nice use of a basis of $\mathcal{P}_n(\mathbb{F})$.

$$= \underbrace{\left(a_0 + a_1 z + \cdots + a_{m-1} z^{m-1}\right)}_{q} + s \underbrace{\left(b_0 + b_1 z + \cdots + b_{n-m} z^{n-m}\right)}_{r}$$

□