# Notes – Linear Algebra

*Zhijie Chen*
*January 16, 2025*

## Contents

## Vector Spaces

**Definition 1.** The complexification of $V$, denoted by $V_{\mathbb{C}}$, equals $V \times V$ with normal addition and real scalar multiplication for product space. But we write an element $(u, v)$ of $V_{\mathbb{C}}$ as $u + iv$. Complex scalar multiplication is defined by

$$(a + bi)(u + iv) = (au - bv) + i(av + bu)$$

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

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

**Lemma 2** (Linear dependence lemma)**.** *Suppose $v_1, \ldots, v_m$ is a linearly dependent set in $V$. Then there exists $k \in \{1, 2, \ldots, m\}$ such that*

$$v_k \in \operatorname{span}\{v_1, \ldots, v_m\}\,.$$

*Furthermore, removing the $k^{th}$ term from the list does not change the span.*[2]

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

**Theorem 3.** *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 $V$ is finite-dimensional. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two bases of $V$. Considering $\mathcal{B}_1$ as an independent set and $\mathcal{B}_2$ as a spanning set leads to $\#\mathcal{B}_1 \leq \#\mathcal{B}_2$. Interchanging the roles of $\mathcal{B}_1$ and $\mathcal{B}_2$ and we have $\#\mathcal{B}_2 \leq \#\mathcal{B}_1$. Thus $\#\mathcal{B}_1 = \#\mathcal{B}_2$. □

## Linear Maps

### Kernal and Image of Linear Maps

**Exercise 4.** Suppose $U$ and $V$ are finite-dimensional and $S \in \mathcal{L}(V, W)$ and $T \in \mathcal{L}(U, V)$. Prove that

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

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

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

□

**Corollary 5** (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 6.** *Suppose $V_1, \ldots, V_m$ are subspaces of $V$.*[5] *Define a linear map $\Gamma : V_1 \times \cdots \times V_m \to V_1 + \cdots + V_m$ by*

$$\Gamma(v_1, \ldots, v_m) = v_1 + \cdots + v_m.$$

*Then $V_1 + \cdots + V_m$ is a direct sum if and only if $\Gamma$ is injective.*

[5] Note that $V$ does not have to be finite-dimensional. Recall that $V_1 + \cdots + V_m$ is a direct sum if and only if the only way to write 0 as a sum of $v_1 + \cdots + v_m$, where each $v_k \in V_k$, is by taking each $v_k$ equal to 0.

**Theorem 7.** *Suppose $V$ is finite-dimensional and $V_1, \dots, V_m$ are subspaces of $V$. Then $V_1 + \cdots + V_m$ is a direct sum if and only* $\dim(V_1 + \cdots + V_m) = \dim V_1 + \cdots + \dim V_m$.[6]

[6] Recall Lemma 6.

**Notation 8.** Suppose $T \in \mathcal{L}(V, W)$. Define $\widetilde{T} : V + \ker V \to V$ by

$$\widetilde{T}(v + \ker T) = Tv.$$

**Exercise 9.** Suppose $V_1, \dots, V_m$ are vector spaces. Prove that $\mathcal{L}(V_1 \times \cdots \times V_m, W)$ and $\mathcal{L}(V_1, W) \times \cdots \times \mathcal{L}(V_m, W)$ are isomorphic vector spaces.

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

For every $\Gamma \in \mathcal{L}(V_1 \times \cdots \times V_m, W)$, define $\varphi_i : V_i \to W$ for each $i \in \{1, \dots, m\}$ by

$$\varphi_i(v_i) = \Gamma(0, \dots, v_i, \dots, 0)$$

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

Let $T(\Gamma) = (\varphi_1, \dots, \varphi_m)$. 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 $(\varphi_1, \dots, \varphi_m) \in \mathcal{L}(V_1, W) \times \cdots \times \mathcal{L}(V_m, W)$, let

$$S(\varphi_1, \dots, \varphi_m)(v_1, \dots, v_m) = \varphi_1(v_1) + \cdots + \varphi_m(v_m).$$

It can be shown that $S$ is a linear map, and that $S \circ T = I$ and $T \circ S = I$. That proves $T$ is indeed an isomorphism between the two vector spaces. $\square$

**Proposition 10.** *A nonempty subset $A$ of $V$ is a translate of some subspace of $V$ if and only if $\lambda v + (1 - \lambda) w \in A$ for all $v, w \in A$ and all $\lambda \in \mathbb{F}$.*

**Exercise 11.** Suppose $A_1 = v + U_1$ and $A_2 = w + U_2$ for some $v, w \in V$ and some subspaces $U_1$, $U_2$ of $V$. Prove that $A_1 \cap A_2$ is either the empty set or a translate of some subspace of $V$.[7]

[7] Recall Proposition 10.

**Proposition 12.** *Suppose $U$ is a subspace of $V$ and $v_1 + U, \dots, v_m + U$ is a basis of $V/U$ and $u_1, \dots, u_n$ is a basis of $U$. Then $v_1, \dots, v_m, u_1, \dots, u_n$ is a basis of $V$. In other words,* $V = \operatorname{span}\{v_1, \dots, v_m\} \oplus U$.[8]

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

**Exercise 13.** Suppose $U$ is a subspace of $V$ such that $V/U$ is finite-dimensional.

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

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

*Proof.* Let $\overline{w}_1 + U, \dots, \overline{w}_m + U$ be a basis of $V/U$. Then by Proposition 12, we have $V = \operatorname{span}\{\overline{w}_1, \dots, \overline{w}_m\} \oplus U$. Let $W_0 = \operatorname{span}\{\overline{w}_1, \dots, \overline{w}_m\}$, then $V = U \oplus W_0$, as desired.

Now we prove that for each subspace $W$ of $V$ such that $V = U + W$, we have $\dim W \geq m = \dim V/U$.

For each $\overline{w}_i \in V$ above, by definition we have $\overline{w}_i = u_i + w_i$ for some $u_i \in U$ and $w_i \in W$. It can be shown from the linear independence of $\overline{w}_1 + U, \dots, \overline{w}_m + U$ that $\overline{w}_1 - u_1, \dots, \overline{w}_m - u_m$ are independent vectors in $W$. Hence $\dim W \geq m$. $\square$

## Duality

**Theorem 14.** *Suppose $V$ and $W$ are finite-dimensional and $T \in \mathcal{L}(V, W)$. Then*

$$T \text{ is surjective} \iff T' \text{ is injective} \quad \text{and} \quad T \text{ is injective} \iff T' \text{ is surjective.}^{9}$$

[9] 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 15.** *Suppose $V$ is finite-dimensional and $U$ is a subspace of $V$. Then*

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

**Exercise 16.** Suppose $V$ is finite-dimensional and $U$ and $W$ are subspaces of $V$.

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

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

[10] Recall Proposition 15.

**Exercise 17.** Suppose $V$ is finite-dimensional and $U$ and $W$ are subspaces of $V$.

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

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

**Proposition 18.** *Suppose $V$ is finite-dimensional and $v_1, \ldots, v_n$ is a basis of $V$. Then $\varphi_1, \ldots, \varphi_n \in V'$ is the dual basis of $v_1, \ldots, v_n$ if and only if*

$$\begin{bmatrix} \mathcal{M}(\varphi_1, (v_1, \ldots, v_n)) \\ \vdots \\ \mathcal{M}(\varphi_n, (v_1, \ldots, v_n)) \end{bmatrix} = I.$$

**Exercise 19.** Suppose $V$ is finite-dimensional and $\varphi_1, \ldots, \varphi_n$ is a basis of $V'$. Prove that there exists a basis of $V$ whose dual basis is $\varphi_1, \ldots, \varphi_n$.

*Proof.* We start from an arbitrary basis $u_1, \ldots, u_n$ of $V$. Let $\psi_1, \ldots, \psi_n$ be its dual basis. In this proof, we take standard basis $e_1, \ldots, e_n$ as the basis of $\mathbb{F}^n$.

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

$$T(v) = (\varphi_1(v), \ldots, \varphi_n(v)), \quad S(v) = (\psi_1(v), \ldots, \psi_n(v)).$$

Then by Lemma 18, $\mathcal{M}(S, (u_1, \ldots, u_n)) = I$.

Let $A$ be the change of basis matrix from $\psi$'s to $\varphi$'s, i.e.,

$$\begin{bmatrix} \varphi_1 & \cdots & \varphi_n \end{bmatrix} = \begin{bmatrix} \psi_1 & \cdots & \psi_n \end{bmatrix} A.$$

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

$$\mathcal{M}(T, (u_1, \ldots, u_n)) = \begin{bmatrix} \mathcal{M}(\varphi_1, (u_1, \ldots, u_n)) \\ \vdots \\ \mathcal{M}(\varphi_n, (u_1, \ldots, u_n)) \end{bmatrix} = A^t \begin{bmatrix} \mathcal{M}(\psi_1, (u_1, \ldots, u_n)) \\ \vdots \\ \mathcal{M}(\psi_n, (u_1, \ldots, u_n)) \end{bmatrix}$$

$$= A^t \cdot \mathcal{M}(S, (u_1, \ldots, u_n)) = A^t.$$

Consider basis $v_1, \ldots, v_n$ of $V$ such that the change of basis matrix from $u$'s to $v$'s is $\left(A^t\right)^{-1}$.[11] Thus

$$\mathcal{M}(T, (v_1, \ldots, v_n)) = \mathcal{M}(T, (u_1, \ldots, u_n)) \cdot \mathcal{M}(I, (v_1, \ldots, v_n), (u_1, \ldots, u_n)) = I.$$

Then by Proposition 18, the dual basis of $v_1, \ldots, v_n$ is precisely $\varphi_1, \ldots, \varphi_n$, as desired. □

[11] The change of basis for $V' \to V'$ corresponds to the transpose of $V \leftarrow V$, where transpose and inverse both come from duality. That gives the idea of considering $\left(A^t\right)^{-1}$.

## Polynomials

**Theorem 20.** *Suppose $p \in \mathcal{P}(\mathbb{F})$ is a nonconstant polynomial of degree $m$. Then $\lambda \in \mathbb{F}$ is a zero of $p$ if and only if there exists a polynomial $q \in \mathcal{P}(\mathbb{F})$ of degree $m-1$ such that $p(z) = (z - \lambda)q(z)$ for every $z \in \mathbb{F}$.*

**Theorem 21.** *Suppose $p \in \mathcal{P}(\mathbb{F})$ is a nonconstant polynomial of degree $m$. Then $p$ has at most $m$ zeros in $\mathbb{F}$.*[12,13]

[12] This theorem indicates that when a polynomial $p$ has too many zeros, $p = 0$.

[13] This theorem implies that the coefficients of a polynomial are uniquely determined. In particular, the *degree* of a polynomial is well-defined.

**Theorem 22** (Division algorithm for polynomials)**.** *Suppose that $p, s \in \mathcal{P}(\mathbb{F})$, with $s \neq 0$. Then there exist unique polynomials $q, r \in \mathcal{P}(\mathbb{F})$ such that $p = sq + r$.*

*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

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

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 $a_0, \ldots, a_{m-1}, b_0, \ldots, b_{n-m} \in \mathbb{F}$ such that

$$\begin{aligned} p &= a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} + b_0 s + b_1 zs + \cdots + b_{n-m} z^{n-m} s \\ &= \left(a_0 + a_1 z + \cdots + a_{m-1} z^{m-1}\right) + s\left(b_0 + b_1 z + \cdots + b_{n-m} z^{n-m}\right). \end{aligned}$$

□

**Theorem 23** (Fundamental theorem of algebra, first version)**.** *Every nonconstant polynomial with complex coefficients has a zero in $\mathbb{C}$.*

*Proof.* Suppose $p \in \mathcal{P}(\mathbb{C})$ is a nonconstant polynomial with highest-order nonzero term $c_m z^m$. Then $|p(z)| \to \infty$ as $|z| \to \infty$. Thus the continuous function $z \mapsto |p(z)|$ has a global minimum at some $\zeta \in \mathbb{C}$. Assume that $p(\zeta) \neq 0$.

Consider polynomial $q = p(z + \zeta)/p(\zeta)$. The function $z \mapsto |q(z)|$ has a global minimum at $z = 0$. Write

$$q(z) = 1 + a_k z_k + \cdots + a_m z^m$$

where $k$ is the smallest positive integer such that the coefficient of $z_k$ is nonzero.

Let $\beta$ be the $k^{\text{th}}$ root of $-1/a_k$. There is a constant $c > 1$ such that if $t \in (0,1)$, then

$$|q(t\beta)| \leq \left|1 + a_k t^k \beta^k\right| + ct^{k+1} = 1 - t^k(1 - tc).$$

Thus taking $t$ to be $1/(2c)$ leads to $|q(t\beta)| < 1$. The contradiction implies that $p(\zeta) = 0$, as desired. □

**Theorem 24** (Fundamental theorem of algebra, second version)**.** *If $p \in \mathcal{P}(\mathbb{C})$ is a nonconstant polynomial, then $p$ has a unique factorization of the form*

$$p(z) = c(z - \lambda_1) \cdots (z - \lambda_m),$$

*where $c, \lambda_1, \ldots, \lambda_m \in \mathbb{C}$.*

**Theorem 25** (Factorization of a polynomial over $\mathbb{R}$)**.** *If $p \in \mathcal{P}(\mathbb{R})$ is a nonconstant polynomial, then $p$ has a unique factorization of the form*

$$p(x) = c(x - \lambda_1) \cdots (x - \lambda_m)(x^2 + b_1 x + c_1) \cdots (x^2 + b_M x + c_M),$$

*where $m, M \in \mathbb{N}$ and $c, \lambda_1, \ldots, \lambda_m, b_1, \ldots, b_M, c_1, \ldots, c_M \in \mathbb{R}$, with $b_k^2 < 4c_k$ for each $k$.*

**Exercise 26.** Suppose $p, q \in \mathcal{P}(\mathbb{C})$ are nonconstant polynomials with no zeros in common. Let $m = \deg p$ and $n = \deg q$. Prove that there exist $r \in \mathcal{P}_{n-1}(\mathbb{C})$ and $s \in \mathcal{P}_{m-1}(\mathbb{C})$ such that $rp + sq = 1$.

*Proof.* $\square$