Linear Algebra Note

Zhen Yao, Department of Mathematics
University of Pittsburgh

Contents

Chapter 1

Fundamentals of Linear Spaces

1.1 Linear Spaces, Isomrphism

A *field* K is a nonempty set in which two operations are defined, usually called addition and multiplication, denoted by $+$ and $\cdot$ respectively such that it satisfies the following axioms:

(1) K is closed under addition and multiplication, i.e., if $a, b \in K$, then $a+b, a \cdot b \in K$.

(2) Associativity of addition and multiplication, i.e., for any $a, b, c \in K$, $a + (b + c) = (a + b) + c, a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(3) Existence of additive and multiplicative identity elements, i.e., there exists an element of K called additive identity, denoted by 0, such that for any $a \in K, a + 0 = a$. Similarly, there exists an element of K called multiplicative identity, denoted by 1, such that for any $a \in K, a \cdot 1 = a$.

(4) Existence of additive inverse and multiplicative inverse, i.e., for any $a \in K$, there exists an element $-a \in K$, such that $a + (-a) = 0$. Similarly, for any $a \in K \setminus \{0\}$, there exists an element $a^{-1} \in K$, such that $a \cdot a^{-1} = 1$.

(5) Distributivity of mulitiplication over addition, i.e., for any $a, b, c \in K, a \cdot (b + c) = a \cdot b + a \cdot c$.

Example 1.1.1. Examples of field: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$. When K is $\mathbb{R}$ or $\mathbb{C}$, the elements of K are called scalars.

Example 1.1.2. Some important structures are "very nearly"fields. For example, let $\mathbb{R}_\infty = \mathbb{R} \cup \{\infty\}$, and define operations $\boxplus$ and $\boxdot$ on $\mathbb{R}_\infty$ as

$$a \boxplus b = \begin{cases} \min\{a, b\} & \text{if } a, b \in \mathbb{R}, \\ b & \text{if } a = \infty, \\ a & \text{if } b = \infty. \end{cases} \quad \text{and} \quad a \boxdot b = \begin{cases} a + b & \text{if } a, b \in \mathbb{R}, \\ \infty & \text{otherwise.} \end{cases}$$

This structure, called the *optimization algebra*, satisfies all of the conditions of a field *except* for the existence of additive inverse (such structures are known as *semields*[3]).

Example 1.1.3. Fields do not have to be infinite. Let p be a positive integer and $\mathbb{Z}/(p) = \{1, 2, \cdots, p-1\}$. For each nonnegative integer n, denote the remainder after dividing n by p as $[n]_p$. Then it is easy to see that $[n]_p \in \mathbb{Z}/(p)$ for each nonnegative integer n and $[i]_p = i$ for all $i \in \mathbb{Z}/(p)$.

We now define operations on $\mathbb{Z}/(p)$ by setting $[n]_p + [k]_p = [n+k]_p$ and $[n]_p \cdot [k]_p = [n \cdot k]_p$. It is easy to check that if the integer p is prime, then $\mathbb{Z}/(p)$ with two operations is a field, known as the *Galois field* of order p, usually denoted by $GF(p)$.

Proposition 1.1.1. *Let a be an nonzero element of a finite field K which contains q elements. Then $a^{-1} = a^{q-2}$.*

Proof. If $q = 2$, then $K = \mathrm{GF}(2)$ and $a = 1$. Then the result is obvious.

If $q > 2$, let $B = \{a_1, \cdots, a_{q-1}\}$ be nonzero elements of K. Then $aa_i \neq aa_k$ for $i \neq k$. If not, we would have $a_i = a^{-1}(aa_k) = a_k$. Therefore, $B = \{aa_1, \cdots, aa_{q-1}\}$ and we have

$$\prod_{i=1}^{q-1} a_i = \prod_{i=1}^{q-1} aa_i = a^{q-1} \prod_{i=1}^{q-1} a_i$$

Then we have $a^{q-1} = 1 = aa^{-1}$, which implies $a^{-1} = a^{q-2}$. □

Definition 1.1.1. *Now we define the characteristic of a field K to be equal to the smallest positive integer p such that $1 + \cdots + 1$(p summands) equals 0—if such an integer p exists—and to be equal to 0 otherwise.*

Proposition 1.1.2. *If K is a field having characteristic $p > 0$, then p is prime.*

Proof. Suppose by contrary that $p = xy, 0 < x, y < p$. Therefore $a = x$ nd $b = y$ are nonzero elements of K and we have $ab = xy = 0$, which implies $a = b = 0$. Then there is a contradiction. □

Theorem 1.1.1 (Loo-Keng Hua's Identity)**.** *If a and b are nonzero elements of a field K satisfying $a \neq b^{-1}$, then*

$$a - aba = \left(a^{-} + (b^{-1} - a)^{-1}\right)^{-1}$$

Proof. We have

$$\begin{aligned} a^{-} + (b^{-1} - a)^{-1} &= a^{-1}\left((b^{-1} - a) + a\right)(b^{-1} - a)^{-1} \\ &= a^{-1}b^{-1}(b^{-1} - a)^{-1} \\ \Rightarrow \left(a^{-} + (b^{-1} - a)^{-1}\right)^{-} &= (b^{-1} - a)ba = a - aba \end{aligned}$$

□

Now we introduce the term of linear space.

Definition 1.1.2. *A linear space X over a field K is a set in which two operations are defined:*

(1) Addition, denoted by $+$, such that for any $x, y \in X, x + y \in X$.

(2) Scalar multiplication, denoted by $\cdot$, such that for $a \in K$ and $x \in X$, $aX \in X$.

And these two operations satisfy the following axioms:

(1) Associativity of addition, i.e., for $x, y, z \in X, x + (y + z) = (x + y) + z$.

(2) Commutativity of addition, i.e., for $x, y \in X, x + y = y + x$.

(3) Identity element of addiiton, i.e., for all $x \in X$, there exists an element $0 \in X$, called the zero vector, such that $x + 0 = x$.

(4) Inverse element of addition, i.e., for all $x \in X$, there exists an element $-x \in X$, called the additive inverse of x, such that $x + (-x) = 0$.

(5) Compatibility(Associativity) of scalar multiplication with field multiplication, i.e., for any $a, b \in K$ and $x \in X$, $a \cdot (b \cdot x) = (a \cdot b) \cdot x$.

(6) Identity element of scalar multiplication, i.e., for all $x \in X$, there exists an element $1 \in X$, such that $1 \cdot x = x$.

(7) Distributivity of scalar multiplicaytion with respect to vector addition, i.e., for $a \in K, x, y \in X, a \cdot (x + y) = a \cdot x + a \cdot y$.

(8) Distributivity of scalar multiplicaytion with respect to field addition, i.e., for $a, b \in K, x \in X, (a + b) \cdot x = a \cdot x + b \cdot y$.

Remark 1.1.1. *Zero vector is unique.*

Proof. If there exist two zeros 0_1 and 0_2 in X, then for all $x \in X$, we have $x + (-x) = 0_1$, $x + (-x) = 0_2$. Then $0_1 = 0_2$. □

Remark 1.1.2. $0x = x, (-1) \cdot x = -x$.

Example 1.1.4 (Examples of Linear Spaces)**.**

(i) $\mathbb{R}^n, \mathbb{C}^n$.

(ii) Set of all row vectors: $(a_1, \cdots, a_n)$ in K, this space is denoted as K^n.

(iii) Set of all real-valued functions $f(x)$ defined on the real line, $K = \mathbb{R}$.

(iv) Set of all functions with values in K, defined on an arbitrary set S.

(v) Set of all polynomials with real coefficients of order at most n.

Definition 1.1.3. *A one-to-one corresponding between two linear spaces over the same field that maps sum into sum and scalar multiples into scalar multiples is called isomorphism.*

Example 1.1.5. The linear space of real valued functions on $\{1, 2, \cdots, n\}$ is isomorphic to $\mathbb{R}^n$.

Example 1.1.6. The set (ii) and (v) in example (1.1.4) are isomorphic.

Proof. Polynomials can be written as $a_1 + a_2 x + a_3 x^2 + \cdots + a_n x^{n-1}$, where we can represent this as $p(x) = (a_1, a_2, \cdots, a_n)x$. Then we can define a map $p(a_1, a_2, \cdots, a_n) = a_1 + a_2 x + a_3 x^2 + \cdots + a_n x^{n-1}$, which is an isomorphism. $\square$

Example 1.1.7. If S in (iv) has n elements, then (ii) and (iv) in example (1.1.4) are isomorphic.

Proof. Assume $S = \{x_1, x_2, \cdots, x_n\}$, then we can define $T(f) = (f(x_1), f(x_2), \cdots, f(x_n)) \in K^S$, which is indeed an isomorphism. $\square$

Example 1.1.8. If $K = \mathbb{R}$ in (v), then (v) and (iv) in example (1.1.4) are isomorphic when S consists of n distinct points of $\mathbb{R}$.

1.2 Subspace

Definition 1.2.1. *A subset Y of a linear space X is said to be subspace if sums and scalar multiples of elements of Y belong to Y. The set $\{0\}$ consisting of the zero element of a linear space X is a subspace of X, called the trivial subspace.*

Definition 1.2.2. *The sum of two subsets Y and Z of a linear space X, is the set defined by*

$$Y + Z = \{y + z \in X : y \in Y, z \in Z\}$$

The intersection of two subsets Y and Z of a linear space X, is the set defined by

$$Y \cap Z = \{x \in X : x \in Y, x \in Z\}$$

Proposition 1.2.1. *If Y and Z are two linear subspaces of X, then both $Y + Z$ and $Y \cap Z$ are linear subspaces of X.*

Remark 1.2.1. *The union of two subspaces many not be a subspace. For exapmle, two lines that intersect into one point in $\mathbb{R}^2$, then the union of these two lines is not a subspace.*

1.3 Algebra Over a Field

A vector space X over a field K is an *K-algebra* if and only if there exists a function $X \times X \ni (x, y) \mapsto x \cdot y \in X$ such that

(1) $x \cdot (y + z) = x \cdot y + x \cdot z$,

(2) $(x + y) \cdot z = x \cdot z + y \cdot z$,

(3) $a(x \cdot y) = (ax) \cdot y = x \cdot (ay)$.

for all $x, y, z \in X$ and $a \in K$. And these conditions suffice to show that $0 \cdot x = x \cdot 0 = 0$ for all $x \in X$. Indeed, $0 \cdot x = (-x + x) \cdot x = (-x) \cdot x + x \cdot x = -(x \cdot x) + (x \cdot x) = 0$.

Remark 1.3.1. *The operation $\cdot$ need not be associative, nor need there exist an identify element for this operation.*

If this operation is associative, i.e., it satisfies $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in X$, then the algebra is called an *associative K-algebra.* If an identify element for operation $\cdot$ exists, i.e., there exists an element $e \neq 0 \in X$ satisfying $e \cdot x = x \cdot e = x$ for all $x \in X$, then we call this K-algebra $(X, \cdot)$ is *unital.*

If x is an element of an associative K-algebra $(K, \cdot)$ and if n is a positive integer, we write x^n instead of $x \cdot x \cdots x \cdot x$ (n factors). If X is also unital and has a multiplicative identity e, we set $x^0 = e$ for all $x \in X, x \neq 0$. The element 0^0 is not defined.

If $x \cdot y = y \cdot x$ for all $x, y \in X$ in some K-algebra $(X, \cdot)$, then the algebra is *commutative.* An F-algebra $(X, \cdot)$ satisfying $x \cdot y = -y \cdot x$ is called *anticommutative.* If the characteristic of K is other than 2, then this condition is equivalent to the condition that $x \cdot x = 0$ for all $x \in X$.

If $(X, \cdot)$ is an associative and K-algebra having a multiplicaiton identity e, and if $x \in X$ satisfies the condition that there exists an element $y \in X$ such that $x \cdot y = y \cdot x = e$, then we say that x is a *unit* of X. If such element y exists, then it is unique and denoted by x^{-1}. Also, if x, y are units of X, then so is $x \cdot y$. Indeed,

$$\begin{aligned}(x \cdot y) \cdot \left(y^{-1} \cdot x^{-1}\right) &= \left(x \cdot \left(y \cdot y^{-1}\right)\right) \cdot x^{-1} \\ &= (x \cdot e) \cdot x^{-1} = e\end{aligned}$$

similarly, $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = e$.

Remark 1.3.2. *Loo-Keng Hua's identity holds in any associative unital F-algebra in which the inverses exist, since the proof relies only on associativity of addition and multiplication and distributivity of multiplication over addition[3].*

Example 1.3.1 (Examples of X-algebra)**.**

(1) Any vector space V over a field K can be turned into an associative and commutative K-algebra which is not unital by setting $x \cdot y = 0$ for all $x, y \in V$.

(2) If F is a subfield of K, then K has the structure of an associative F-algebra, with multiplication being the multiplication in K. Thus, $\mathbb{C}$ is an $\mathbb{R}$-algebra and $\mathbb{Q}(\sqrt{p})$ is a $\mathbb{Q}$-algebra for prime number p.

Definition 1.3.1. *Let K be a field. An anticommutative K-algebra $(X, \cdot)$ is a Lie algebra over K if and only if it satisfies Jacobi identity:*

$$x \cdot (y \cdot z) + y \cdot (z \cdot x) + z \cdot (x \cdot y) = 0$$

for all $x, y, z \in X$. This algebra is not associative unless $x \cdot y = 0$ for all $x, y \in X$.

One particular Lie algebra on $\mathbb{R}^3$ is defined with multiplication $\times$, called *cross product*, as below

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} \times \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} a_2b_3 - a_3b_2 \\ a_3b_1 - a_1b_3 \\ a_1b_2 - a_2b_1 \end{bmatrix}.$$

and $(\mathbb{R}^3, \times)$ is a Lie algebra over $\mathbb{R}$. Moreover, the cross product is the only possible anticommutative product which can be defined on $\mathbb{R}^3$. Indeed, if $\cdot$ is any such product defined on $\mathbb{R}^3$, then

$$\begin{aligned} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} &= \left(\sum_{i=1}^{3} a_i x_i \right) \cdot \left(\sum_{i=1}^{3} b_i x_i \right) = \sum_{i=1}^{3} \sum_{j=1}^{3} a_i b_j (x_i \cdot x_j) \\ &= \begin{bmatrix} a_2b_3 - a_3b_2 \\ a_3b_1 - a_1b_3 \\ a_1b_2 - a_2b_1 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} \times \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}. \end{aligned}$$

1.4 Linear Dependence

Definition 1.4.1. *A linear combination of m vectors $x_1, \cdots, x_m$ of a linear space is a vector of the form*

$$\sum_{j=1}^{m} c_j x_j, \text{where}\, c_j \in K$$

Given m vectors $x_1, \cdots, x_m$ of a linear space X, the set of all linear combinations of $x_1, \cdots, x_m$ is a subspace of X, and it is the smallest subspace of X containing $x_1, \cdots, x_m$. This is called the subspace spanned by $x_1, \cdots, x_m$.

Definition 1.4.2. *A set of vectors $x_1, \cdots, x_m$ in X spans the whole space X if every x in X can be expressed as a linear combination of $x_1, \cdots, x_m$.*

Definition 1.4.3. *The vectors $x_1, \cdots, x_m$ are called linearly dependent if there exist scalars $c_1, \cdots, c_m$, not all of them are zero, such that*

$$\sum_{j=1}^{m} c_j x_j = 0$$

The vectors $x_1, \cdots, x_m$ are called linearly independent if they are not dependent.

Definition 1.4.4. *A finite set of vectors which span X and are linearly independent is called a basis for X.*

Proposition 1.4.1. *A linear space which is spanned by a finite set of vectors has a basis.*

Proof. Let m be the smallest number such that there exist $x_1, \cdots, x_m \in X$, and $X = \text{span}\{x_1, \cdots, x_m\}$. If $x_1, \cdots, x_m$ are linearly dependent, then there exist $c_1, \cdots, c_m \in K$, not all of them are zero, such that

$$\sum_{j=1}^{m} c_j x_j = 0$$

Suppose without losing generality that $c_1 \neq 0$, then

$$\begin{aligned} & c_1 x_1 + c_2 x_2 + \cdots + c_m x_m = 0 \\ \Rightarrow\ & x_1 = -\frac{c_2}{c_1} x_2 - \cdots - \frac{c_m}{c_1} x_m \end{aligned}$$

then $\{x_2, \cdots, x_m\}$ is also a span of X, which is a contradiction. $\square$

Theorem 1.4.1. *All bases for a finite-dimensional linear space X contain the same number of vectors. This number is called the dimension of X and is denoted as* $\dim X$.

Proof. The theorem follows from the lemma below. $\square$

Lemma 1.4.2. *Suppose that the vectors $\{x_1, \cdots, x_n\}$ span a linear space X and that the vectors $\{y_1, \cdots, y_m\}$ in X are linear independent. Then $m \leq n$.*

Proof. Since $\text{span}\{x_1, \cdots, x_m\} = X$, then for y_1, we have $y_1 = \sum_{j=1}^{n} c_j x_j \neq 0$. Then, for some k such that $c_k \neq 0$, we have

$$\begin{aligned} c_k x_k &= y_1 - \sum_{j=1, j\neq k}^{n} c_j x_j \\ x_k &= \frac{y_1}{c_k} - \sum_{j=1, j\neq k}^{n} \frac{c_j}{c_k} x_j \end{aligned}$$

Then we have $\{y_1\} \cup \{x_1, \cdots, x_{j-1}, x_{j+1}, \cdots, x_n\}$ can span X. Then, y_2 can be written as a linear combination of y_1 and $\{x_j\}_{j\neq k}$. Some coefficients for $x_j, j \neq k$ must be nonzero, since y_1 and y_2 are linearly independent. Then we can replace x_j by y_2, and continue this process until it spans X. If $m \geq n$, then n steps total yields that $y_1, \cdots, y_m$ span X. If $m > n$, this contradicts the linear independence of the vectors $y_1, \cdots, y_m$. $\square$

Remark 1.4.1. *The dimension of the trivial space consisting of the single element* 0 *is zero.*

Theorem 1.4.3. *Every linearly independent set of vectors $y_1, \cdots, y_n$ in a finite dimensional linear space X can be completed to a basis of X.*

Proof. If $\text{span}\{y_1, \cdots, y_n\} \neq X$, then there exists $y_{n+1} \in X \setminus \{y_1, \cdots, y_n\}$. We can continue this process if $\text{span}\{y_1, \cdots, y_n, y_{n+1}\} \neq X$. Since $\dim X \subset \infty$, then the process will stop after finitely many step, which constructs a basis of X. $\square$

Theorem 1.4.4. *Let X be a finite dimensional space over K with $\dim X = n$, then X is isomorphic to K^n.*

Proof. Let $x_1, \cdots, x_n$ be a basis of X. For any $x \in X$, we have $x = \sum_{k=1}^n c_k x_k$. We can define $\varphi : X \to K^n$ as $\varphi(x) = (c_1, \cdots, c_n) \in K^n$. Then φ is an isomorphism. $\square$

Theorem 1.4.5.

(a) *Every subspace Y of a finite dimensional linear space X is of finite dimensional.*

(b) *Every subspace Y has a complement in X, that is, another subspace Z such that every vector x in X can be decomposed uniquely as*

$$x = y + z, y \in Y, z \in Z.$$

Furthermore $\dim X = \dim Y + \dim Z$.

Proof.

(a) Construct a finite basis for X and pick $y_1 \in Y, y_1 \neq 0$. If $\text{span}\{y_1\} = Y$, then we are done. Otherwise, we can pick $y_2 \in Y \setminus \{y_1\}$ and y_1, y_2 are linearly independent. And we can continue this process and this process will stop in finite steps, since we cannot find more than $\dim X$ linearly independent vectors.

(b) Let $\{y_1, \cdots, y_m\}$ be a basis of Y and $\dim Y = m$. Then we can complete it into a basis of X, saying $\text{span}\{y_1, \cdots, y_m, y_{m+1}, \cdots, y_n\} = X$.

We define $Z = \text{span}\{y_{m+1}, \cdots, y_n\}$, and then $\dim Z = n - m$. For any $x \in X$, we have

$$x = \sum_{k=1}^{n} c_k x_k, y = \sum_{k=1}^{m} c_k x_k, z = \sum_{k=m+1}^{m} c_k x_k$$

then we have $x = y + z$. If $x = \tilde{y} + \tilde{z}, \tilde{y} \in Y, \tilde{z} \in Z$, then we have $\tilde{y} + \tilde{z} = y + z$, which implies $\tilde{y} - y = z - \tilde{z}$. Since Y, Z are subspaces of X, then we can have

$$\tilde{y} - y = \sum_{k=1}^{m} a_k y_k = \sum_{k=m+1}^{m} b_k y_k = z - \tilde{z}$$
$$\Rightarrow \sum_{k=1}^{m} a_k y_k - \sum_{k=m+1}^{m} b_k y_k = 0$$

Since $y_1, \cdots, y_n$ are linearly independent, then $a_k = b_k = 0$, which implies that $\tilde{y} = y, \tilde{z} = z$.

□

Remark 1.4.2.

(a) $Y \cap Z = \{0\}$.

(b) *X is said to be direct sum of* Y *and* Z*, if* $X = Y + Z$ *and* $Y \cap Z = \{0\}$*. Then we write* $X = Y \oplus Z$*.*

Definition 1.4.5. *X is said to be a direct sum of its subspaces* $Y_1, \cdots, Y_m$ *if every* $x \in X$ *can be uniquely expressed as*

$$x = \sum_{j=1}^{m} y_j, y_j \in Y_j$$

We write $X = Y_1 \oplus \cdots \oplus Y_m$*. Furthermore,* $\dim X = \dim Y_1 + \cdots + \dim Y_m$*.*

Exercise 1.4.1. *Prove that if* $X = Y_1 \oplus \cdots \oplus Y_m$*, then* $\dim X = \dim Y_1 + \cdots + \dim Y_m$*.*

Proof. Suppose $y_{i1}, \cdots, y_{in_i}$ form a basis for $Y_i, 1 \le i \le m$. Then for any $x \in X$, we have $x = x_1 + \cdots + x_m$, where $x_i \in Y_i$. Also, we can express x_i as $x_i = \sum_{k=1}^{n_i} c_{ik} y_{ik}$. Then we have

$$x = \sum_{i=1}^{m} \sum_{k=1}^{n_i} c_{ik} y_{ik}$$

If $\sum_{i=1}^{m} \sum_{k=1}^{n_i} c_{ik} y_{ik} = 0$ for some $c_{ik} \neq 0$, then it contradicts with the definition of then direct sum. □

Exercise 1.4.2. *Prove that every finite dimensional space* X *over field* K *is isomorphic to* K^n*, where* $n = \dim X$*. And this isomorphism is not unique if* $n > 1$*.*

Proof. Suppose $x_1, \cdots, x_n$ form a basis for X. Then for any $x \in X$, it can be expressed as $x = \sum_{k=1}^{n} c_k x_k$. We define $T(x) = (c_1, \cdots, c_n) \in K$, then this is an isomorphism. However, different choice of basis will give different isomorphism. □

1.5 Quotient Space

Definition 1.5.1. *For* X *being a linear space, and* Y *being a subspace of* X*, we say that two vectors* $x_1, x_2 \in X$ *are congruent modulo* Y*, denoted by*

$$x_1 \equiv x_2 \bmod Y$$

if $x_1 - x_2 \in Y$*.*

Congruent mod$Y$ is an equivalence relation, i.e., it satisfies

(1) Symmetric, i.e., if $x_1 \equiv x_2$, then $x_2 \equiv x_1$.

(2) Reflexive, i.e., $x \equiv x$ for all $x \in X$.

(3) Transitive, i.e., if $x_1 \equiv x_2$ and $x_2 \equiv x_3$, then $x_1 \equiv x_3$.

Thus, we can divide elements of X into congruence classes mod$Y$. The congruence class containing the vector x is the set of all vectors congruent with X, denoted by $\{x\}$.

The set of congruence classes can be made into a linear space by dening addition and multiplication by scalars in K, as follows:

$$\{x\} + \{y\} = \{x + y\}$$
$$a\{x\} = \{ax\}$$

That is, the sum of the congruence class containing x and the congruence class containing y is the class containing $x + y$. Similarly for multiplication by scalars.

The linear space of congruence classes dened above is called the quotient space of X mod Y and is denoted as X/Y.

Example 1.5.1. Taking X to be the linear space of all row vectors $(x_1, \cdots, x_n)$ with n components, and take Y to be all vectors $y = (0, 0, x_3, \cdots, x_n)$ whose first two components are zero. Then two vectors are congruent mod$Y$ if and only if their first two components are equal. Each equivalence class can be represented by a vector with two components, the common components of all vectors in the equivalence class.

Exercise 1.5.1. *Prove that two congruence classes are either identical or disjoint.*

Proof. For $\{x\}$ and $\{y\}$ are congruence classes mod$Y$, if there exists $z \in \{x\} \cap \{y\}$, then $x - z \in Y$ and $y - z \in Y$. Then we have $x - y = x - z - (y - z) \in Y$. So if $\{x\} \cap \{y\} \neq \varnothing$, then $x \equiv y$ mod Y, which means $\{x\} = \{y\}$. Otherwise, $\{x\}$ and $\{y\}$ are disjoint. □

Theorem 1.5.1. *If Y is a subspace of a finite-dimensional linear space X, then*

$$\dim X = \dim Y + \dim X/Y.$$

Proof. Let $\{x_1, \cdots, x_m\}$ be a basis of Y, where $m = \dim Y$. This set can be completed into a basis for X by adding $x_{m+1}, \cdots, x_n, n = \dim X$. We claim that $\{x_{m+1}\}, \cdots, \{x_n\}$ form a basis for X/Y by verifying that they span the whole space X/Y and they are linearly independent as below

(1) For any $x \in X$, we can write it as

$$x = \sum_{k=1}^{m} a_k x_k + \sum_{k=m+1}^{n} a_k x_k$$

Then we have

$$\{x\} = \sum_{k=m+1}^{n} a_k \{x_k\}.$$

(2) Suppose that $\sum_{k=m+1}^{n} a_k\{x_k\} = 0$, then we have

$$\sum_{k=m+1}^{n} a_k x_k = y, y \in Y$$

And y can be expressed as $\sum_{k=1}^{m} a_k x_k$, then we have

$$\sum_{k=m+1}^{n} a_k x_k - \sum_{k=1}^{m} a_k x_k = 0$$

which implies $a_k = 0$ for all k, since $x_1, \cdots, x_n$ form a basis for X.

□

Corollary 1.5.1. *A subspace Y of a finite-dimensional linear space X whose dimension is the same as the dimension of X is all of X.*

Proof. Suppose $\dim X = n$, and a subspace Y of X with dimension n. Suppose $y_1, \cdots, y_n$ form a basis for Y, then we can complete it into a basis of X. If we can find another $x \in X$ that is linearly independent with $y_1, \cdots, y_n$, then we have $\{y_1, \cdots, y_n, x\}$ is the basis of X, which is a contradiction.

Also, we can prove it with $\dim X/Y = 0$, which implies $X/Y = \{\{0\}\}$. □

Theorem 1.5.2. *Suppose X is a finite-dimensional linear space, U and V two subspaces of X. Then we have*

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V).$$

Proof. If $U \cap V = \{0\}$, then $U + V$ is a direct sum and hence

$$\dim(U + V) = \dim U + \dim V$$

In general, let $W = U \cap V$, we claim that $U/W + V/W = (U + V)/W$, which is a direct sum. It suffices to prove that $U/W \cap V/W = \{0\}$. Let $\{x\} \subset U/W \cap V/W$, then $x = u + w_1$ for some $u \in U$ and $w_1 \in W$, also, $x = v + w_2$ for some $v \in V$ and $w_2 \in W$. Then we have $u + w_1 = v + w_2$, and hence $u + w_1 = v + w_2 \in U \cap V = W$. Thus, we have $x \in W$, which gives $\{x\} = \{0\}$.

Now we proved $U/W + V/W = (U + V)/W$, then we have

$$\begin{aligned} \dim U/W + \dim V/W &= \dim(U + V)/W \\ \Rightarrow \dim U - \dim W + \dim V - \dim W &= \dim(U + V) - \dim W \\ \Rightarrow \dim U + \dim V - \dim(U \cap V) &= \dim(U + V) \end{aligned}$$

The proof is complete. □

Definition 1.5.2. *The Cartesian sum $X_1 \oplus X_2$ of two linear spaces X_1, X_2 over the same field is the set of pair (x_1, x_2) where $x_i \in X_i, i = 1, 2$. $X_1 \oplus X_2$ is a linear space with addition and multiplication by scalars defined componentwisely.*

Theorem 1.5.3.

$$\dim X_1 \oplus X_2 = \dim X_1 + \dim X_2$$

Proof. Let $x_1, \cdots, x_n$ be a basis of X_1 and $y_1, \cdots, y_m$ be a basis of X_2. We claim that $(x_1, 0), \cdots, (x_n, 0), (0, y_1), \cdots, (0, y_n)$ form a basis for $X_1 \oplus X_2$ by verifying this is indeed a basis.

Also, we can prove it in another way by defining

$$Y_1 = \{(x, 0) : x \in X_1, 0 \in X_2\}$$
$$Y_2 = \{(0, x) : 0 \in X_1, x \in X_2\}$$

and it is easy to see that Y_1 is isomorphic to X_1 and Y_2 isomorphic to X_2. Also, we have $Y_1 \cap Y_2 = \{0\}$, then we have

$$\dim X_1 \oplus X_2 = \dim Y_1 + \dim Y_2 - \dim X_1(Y_1 \cap Y_2) = \dim X_1 + \dim X_2$$

□

Moreover, we can define the Cartesian sum $\oplus_{k=1}^m X_k$ of m linear spaces and we have

$$\dim \oplus_{k=1}^m X_k = \sum_{k=1}^m \dim X_k.$$

Next we present an important theorem.

Theorem 1.5.4. *Let K be a field such that it has infinite number of elements and let X be a finite dimensional linear space over K. Prove that X cannot be written as a finite union of its proper subspaces.*

Proof. Suppose by contrary that there exist $W_1, W_2, \cdots, W_n$, which are proper subspaces of X such that $X = \bigcup_{i=1}^n W_i$.

If for any $1 \le j \le n$, $W_j \subset \bigcup_{i \ne j}^n W_i$, then we can remove such W_j. Thus, without losing generality, we can assume that no W_j is contained in the union of other W_i's. Note that since W_i's are proper subspaces of X, then X must have $\dim X = n \ge 2$. Since $W_1 \not\subset \bigcup_{i \ne 1}^n W_i$, then there exists $u \in W_1$ such that $u \notin W_i, i \ge 2$. Also, W_1 is a proper subspace, then there exists $v \notin W_1$.

Now consider $v + \lambda u$ for $\lambda \in K$. We claim that $v + \lambda u \in W_j$ for at most one $\lambda \in K$. Now we prove this:

(1) Consider the case $j = 1$. If $v + \lambda u \in W_1$ for some $\lambda \in K$, then $(v + \lambda u) - \lambda u \in W_1$, since $u \in W_1$ and W_1 is a subspace. Thus, we have $v \in W_1$, which is a contradiction.

(2) Now consider the case $j \geq 2$. If there exist $\lambda_1, \lambda_2 \in K, \lambda_1 \neq \lambda_2$ such that $v+\lambda_1 u \in W_j$ and $v+\lambda_2 u \in W_j$, then $(v+\lambda_1 u)-(v+\lambda_2 u) = (\lambda_1 - \lambda_2)u \in W_j$. Then, since $\lambda_1 \neq \lambda_2$, we have $u \in W_j$, which is a contradiction.

This claim implies that there are only finitely many $\lambda \in K$, saying $\lambda_1, \cdots, \lambda_s$ such that

$$v + \lambda_i u \in \bigcup_{i=1}^{n} W_i = X$$

Since K has infinitely many elements, then we can choose $\lambda_0 \in K$ such that $\lambda_0 \notin \{\lambda_1, \cdots, \lambda_s\}$, then $v + \lambda_0 u \notin \bigcup_{i=1}^{n} W_i = X$, which is a contradiction. □

1.6 Exercises

Exercise 1.6.1. *Consider a polynomial $X(t) : \mathbb{C} \to \mathbb{C}$. Let V be vector space for all complex valued polynomials and let $M = \{X(t) : X \text{ is even}\}$ and $N = \{X(t) : X \text{ is odd}\}$. Prove that*

(a) M, N are subspaces of X.

(b) M, N are each other's complement in V, i.e., $V = M \oplus N$.

Proof.

(a) Let $f(t), g(t) \in M$ and $\lambda \in \mathbb{C}$, then we have $f(-t) = f(t)$ and $g(t) = -g(-t)$. Thus, we have $(f + \lambda g)(-t) = f(-t) + \lambda g(-t) = f(t) + \lambda g(t) = (f + \lambda g)(t)$, which implies that $f + \lambda g \in M$. Same argument is similar for N.

(b) Let $f(t) \in V$, then we have

$$\begin{aligned} f(t) &= \frac{f(t) + f(-t)}{2} + \frac{f(t) - f(-t)}{2} \\ &= f_1(t) + f_2(t) \end{aligned}$$

and it is easy to see that $f_1 \in M$ and $f_2 \in N$. Also, if $f(t) \in M \cap N$, then we have $f(t) = f(-t)$ and $f(t) = -f(-t)$. Thus, $f(t) = 0$, which implies $M \cap N = \{0\}$. Thus, $V = M \oplus N$.

□

Exercise 1.6.2. *Let U, V and W be subspaces of a finite-dimensional vector space X. Is the statement*

$$\begin{aligned} \dim(U + V + W) =& \dim U + \dim V + \dim W - \dim(U \cap V) - \dim(U \cap W) \\ & - \dim(V \cap W) + \dim(U \cap V \cap W) \end{aligned}$$

true or false? If true, prove it. If false, provide a counterexample

Proof. The statement is not true. Consider three lines U, V, W in $\mathbb{R}^2$ such that they intersect in one point. So we have

$$\dim(U + V + W) = 2$$

and

$$\dim(U) + \dim(V) + \dim(W) - \dim(U \cap V) - \dim(U \cap W) - \\ \dim(V \cap W) + \dim(U \cap V \cap W) = 3$$

the left and right sides are not the same. □

Exercise 1.6.3. *Let U, V, and W be subspaces of a finite dimensional linear space X. Show that if $W \subset U$, then*

$$U \cup (V + W) = U \cup V + W$$

Proof.

(1) We set $u_1 \in U \cap (V + W)$, then there exist some $v_1 \in V$ and $w_1 \in W$ such that $u_1 = v_1 + w_1$ since $u_1 \in U$ and also $u_1 \in (V + W)$. Also, $u_1 \in U$ and $W \subset U$ which means $w_1 \in U$, then we have $v_1 \in U$ since U is a subspace which is closed under addition. Then from $v_1 \in U$, we have $v_1 \in (U \cap V)$. Based on the fact that $u_1 = v_1 + w_1$ and $w_1 \in W$, we have $u_1 \in (U \cap V + W)$. This implies that $U \cap (V + W) \subset (U \cap V + W)$.

(2) Now we set $u_2 \in (U \cap V + W)$, then there exist some $\lambda \in U \cap V$ and $w_2 \in W$ such that $u_2 = \lambda + w_2$. And we have $\lambda + w_2 \in V + W$, since $\lambda \in U \cap V$ and $w_2 \in W$. Also, we know that $W \subset U$, then we have $\lambda + w_2 \in U$. Thus we can have $\lambda + w_2 \in U \cap (V + W)$. Hence, $u_2 \in U \cap (V + W)$, which implies $(U \cap V + W) \subset U \cap (V + W)$.

□

Exercise 1.6.4. *Denote by X the linear space of all polynomials $p(t)$ of degree less than n, and denote by Y the subset of X containing polynomials that are zero at distinct $t_1, t_2, \cdots, t_m \in K$, where $m < n$.*

(i) Show that Y is a subspace of X.

(ii) Determine $\dim Y$ *and find a basis of Y.*

(iii) Determine $\dim X = Y$ *and find a basis of X/Y.*

Proof.

(i) Set $P_1, P_2 \in Y$ of form $P_i = (t-t_1)(t-t_2)\cdots(t-t_m)q_i(t)$ that are zero at distinct $t_1, t_2, \cdots, t_m \in K$. Then we have

$$P_1 + P_2 = \sum_{i=1}^{2}(t-t_1)(t-t_2)\cdots(t-t_m)q_i(t)$$
$$aP_1 = a(t-t_1)(t-t_2)\cdots(t-t_m)q_1(t)$$

where $a \in K$. It is easy to see that both $P_1 + P_2$ and aP_1 are zero at points $t_1, t_2, \cdots, t_m \in K$. So Y is closed under addition and multiplication. Hence, Y is a subspace of X.

(ii) In order to being zero at distinct $t_1, t_2, \cdots, t_m \in K$ where $m < n$, the polynomial $P_Y(t) \in Y$ has the form $P_Y(t) = (t-t_1)(t-t_2)\cdots(t-t_m)q(t)$, where $q(t)$ is not determined. Also, we know that the space of all polynomials is degree less than n, which means that $q(t)$ is degree less than $n-m$.

Since the polynomials $P(t)$ in the space X are degree less that n, it can be presented by the form

$$P(t) = \sum_{k=0}^{n-1} c_k t^k$$

So the basis of X can be written as $1, t, t^2, \cdots, t^{n-1}$, and we have dim $X = n$. Now we can present $q(t)$ by utilizing this basis as

$$q(t) = \sum_{k=0}^{n-m-1} c_k t^k$$

then the basis for subspace Y can be presented as

$$\left\{\prod_{i=1}^{m}(t-t_i), t\prod_{i=1}^{m}(t-t_i), \cdots, t^{n-m-1}\prod_{i=1}^{m}(t-t_i)\right\}$$

and we can check that the linear combination of this basis is equal to zero if and only if all coefficients are all zero. So we have dim $Y = n-m$.

(iii) We have dim $X/Y =$ dim $X-$ dim $Y = m$. Now we set a basis that spans the subspace X/Y.

We firstly set $P_1(t) = (t-t_2)\cdots(t-t_m)q(t)$ and the class $\{P_1\}$ of P_1 is the space $\{P(t) \in X : P(t) - P_1(t) \in Y\}$, and then set $P_2(t) = (t-t_1)(t-t_3)\cdots(t-t_m)q(t)$ and the class $\{P_2\}$ in the same way. And we continue this process where we get rid of $(t-t_i)$ in class P_i until we finally have $P_m(t) = (t-t_1)\cdots(t-t_{m-1})q(t)$ and the class $\{P_m\}$. Then we can check that $(\{P_1\}, \{P_2\}, \cdots, \{P_m\})$ is the span of X/Y.

Better solution for (iii): From (ii) we know the basis of Y, and we can know that every $p(t)$ in X can be replaced by a polynomial of degree less than m in x/Y, so $1, t, \cdots, t^{m-1}$ form a basis of X/Y.

$\square$

Exercise 1.6.5. *Let $U_1, U_2, \cdots, U_k$ be subspaces of a finite-dimensional linear space X such that*

$$\dim U_1 = \dim U_2 = \cdots = \dim U_k$$

Then there is a subspace V of X for which

$$X = U_1 \oplus V = U_2 \oplus V = \cdots = U_k \oplus V$$

Proof. If $\dim U_1 = \cdots = \dim U_k = n$, then we can simply take $V = \varnothing$.

If $\dim U_1 = \cdots = \dim U_k = n-1$, based on the fact that space X cannot be a finite union of its proper subspace, there exists a $v \notin U_k$ for every k, and we can define the complement of $U_1, U_2, \cdots, U_k$ as $U^c = \text{span}(v)$.

Then we consider the case when $\dim U_1 = \cdots = \dim U_k = n-2$, also there exists a $v \notin U_k$ for every k. Then we can define a new subspace $= \text{span}(u_i, v)$ for $1 \leq i \leq k$, and we can immediately know that $\dim \tilde{U}_i = n-1$. Then we can get a complement of $\tilde{U}_i$, denoted by U_i^c and we have $\dim U_i^c = 1$. In particular, $v \notin U_i^c$, so we can take $\text{span}(U_i^c, v)$, which is dimension 2 and a complement of $U_1, U_2, \cdots, U_k$.

Now we can continue this induction and consider $\dim U_1 = \cdots = \dim U_k = m, m < n$, and we can find $v \notin U_k$ for every k. Then we can define $= \text{span}(u_i, v)$ for $1 \leq i \leq k$, and we can immediately know that $\dim \tilde{U}_i = m+1$. Then we can get a complement of $\tilde{U}_i$, denoted by U_i^c and we have $\dim U_i^c = n-m-1$. In particular, $v \notin U_i^c$, so we can take $\text{span}(U_i^c, v)$, which is dimension $n-m$ and a complement of $U_1, U_2, \cdots, U_k$. $\square$

Exercises (1.6.1) to (1.6.5) are Homework 1 for MATH2370. Next we present some exercises from the book Challenging Problems for Students by Fuzhen Zhang[8] and other books.

Exercise 1.6.6. *Let $\mathbb{C}, \mathbb{R}$, and $\mathbb{Q}$ be the fields of complex, real, and rational numbers, respectively. Determine whether each of the following is a vector space. Find the dimension and a basis for each that is a vector space.*

(a) $\mathbb{C}$ *over* $\mathbb{C}$. *Yes, the dimension is* 1, *with a basis* $\{1\}$.

(b) $\mathbb{C}$ *over* $\mathbb{R}$. *Yes, the dimension is* 2, *with a basis* $\{1, i\}$.

(c) $\mathbb{R}$ *over* $\mathbb{C}$. *No, since* $i \in \mathbb{C}$, *and* $1 \cdot i = i \notin \mathbb{R}$.

(d) $\mathbb{R}$ *over* $\mathbb{Q}$. *Yes, the dimension is infinite, since* $1, \pi, \pi^2, \cdots$ *are linearly independent over* $\mathbb{Q}$.

(e) $\mathbb{Q}$ *over* $\mathbb{R}$. *No, since* $\pi \in \mathbb{R}$, *and* $\pi \cdot 1 = \pi \notin \mathbb{Q}$.

(f) $\mathbb{Q}$ *over* $\mathbb{Z}$. *No, since* $\mathbb{Z}$ *is not a field.*

(g) $\mathbb{S} = \{a + \sqrt{2}b + \sqrt{5}c |\, a, b, c \in \mathbb{Q}\}$ *over* $\mathbb{Q}, \mathbb{R}$ *or* $\mathbb{C}$.

Yes over $\mathbb{Q}$*, and the dimension is* 3*, with a basis* $\{1, \sqrt{2}, \sqrt{5}\}$.

No over $\mathbb{R}$*, since* $1 + \sqrt{2} + \sqrt{5} \in \mathbb{S}, \sqrt{10} \in \mathbb{R}$*, and* $(1 + \sqrt{2} + \sqrt{5}) \cdot \sqrt{10} \notin \mathbb{S}$.

No over $\mathbb{C}$*, with the similar argument.*

Chapter 2

Duality

2.1 Linear Functions and Dual Space

Let X be a linear space over a field K. A scalar valued function $l : X \to K$ is called *linear* if

$$\begin{aligned} l(x+y) &= l(x) + l(y) \\ l(kx) &= kl(x) \end{aligned}$$

for all $x, y \in X$, and for all $k \in K$.

The set of linear functions on a linear space X forms a linear space X', the *dual space* of X, if we define

$$\begin{aligned} (l+m)(x) &= l(x) + m(x) \\ (kl)(x) &= k(l(x)) \end{aligned}$$

Theorem 2.1.1. *Let X be a linear space of dimension n. Under a chosen basis $x_1, \cdots, x_n$, the elements of X can be represented as arrays of n scalars:*

$$x = (c_1, \cdots, c_n) = \sum_{k=1}^{n} c_k x_k$$

Let $a_1, \cdots, a_n$ be any array of n scalars, the function l defined by

$$l(x) = \sum_{k=1}^{n} a_k c_k$$

is a linear function of X. Conversely, every linear function l of X can be so represented.

Proof. For any $l \in X'$, define $a_k = l(x_k)$, then we have

$$l(x) = l\left(\sum_{k=1}^{n} c_k x_k\right) = \sum_{k=1}^{n} c_k l(x_k) = \sum_{k=1}^{n} c_k a_k.$$

$\square$

Theorem 2.1.2. $\dim X = \dim X'$.

Proof. Suppose $\dim X = n$. Define $l_j(x) = c_j$, for $x \in X$. We claim $l_j, 1 \leq j \leq n$ form a basis of X'. Indeed, we have

(1) For any $l \in X'$, we have $l(x) = \sum_{k=1}^{n} c_k a_k = \sum_{k=1}^{n} a_k l_k(x)$. Thus, $l = \sum_{k=1}^{n} a_k l_k$, which implies that $\{l_j, 1 \leq j \leq n\}$ span the space X'.

(2) We claim $l_j, 1 \leq j \leq n$ are linearly independent. If $\sum_{k=1}^{n} b_k l_k = 0$, then we have

$$\sum_{k=1}^{n} b_k l_k(x_k) = \sum_{k=1}^{n} b_k c_k = 0$$

for all $x_k \in X$. Then we have $b_k = 0, 1 \leq k \leq n$.

$\square$

We defined $l(x) = \sum_{k=1}^{n} a_k c_k$ in theorem (2.1.1), the right-hand side depends symmetrically on l and x, then we can write left-hand side also symmetrically, we introduce the *scalar product* notation

$$(l, x) \equiv l(x)$$

which is a bilinear function of l and x.

The dual of X' is X'', consisting of all linear functions on X'. Also, (l, x) defines an element in X''.

Theorem 2.1.3. (l, x) *is a bilinear form, which gives a natural identification of* X *with* X''*. The map* $\varphi : X \ni x \to x^{**} \in X''$ *is an isomorphism, where* $(x^{**}, l) = (l, x)$ *or any* $l \in X'$*.*

Proof. $\varphi(x)$ is a subspace of X''.

(1) If $\varphi(x_1) = \varphi(x_2)$, then $(l, x_1) = (l, x_2)$ for any $l \in X'$. Then we have $(l, x_1 - x_2) = 0$. Now we can set $x_1 - x_2 = (c_1, \cdots, c_n)$, and pick $l = (\overline{c_1}, \cdots, \overline{c_n})$, then we have $\sum_{k=1}^{n} |c_k|^2 = 0$. Then, $c_k = 0$, which implies $x_1 = x_2$. Thus, φ is noe-to-one.

(2) We claim that $\varphi(x) = X''$. It suffices to prove that $\dim \varphi(x) = \dim X''$.

Let $x_1, \cdots, x_n$ be a basis of X, then $x_1^{**}, \cdots, x_n^{**}$ is a basis of X''. Thus, φ is onto.

$\square$

2.2 Annihilator and Codimension

Definition 2.2.1. *Let Y be a subspace of X. The set of linear functions that vanish on Y, that is, satisfying $l(y) = 0$ for all $y \in Y$ is called the annihilator of the subspace Y, denoted by $Y^{\perp}$.*

Remark 2.2.1. *$Y^{\perp}$ is a subspace of X'.*

Theorem 2.2.1. $\dim Y^{\perp} + \dim Y = \dim X$.

Proof. We can establish a natural isomorphism $T : Y^{\perp} \to (X/Y)'$ as follows

$$T(l)(\{x\}) = l(x)$$

for any $l \in Y^{\perp}$ and $\{x\} \in X/Y$. It suffices to prove that T is well-defined.

(1) If $\{x_1\} = \{x_2\}$, then $x_1 = x_2 + y$ for some $y \in Y$. Then $l(x_1) = l(x_2) + l(y) = l(x_2)$. Then $T(l)$ is well defined.

(2) Also, $T(l)$ is linear. Indeed, for $l_1, l_2 \in Y^{\perp}$ and $a, b \in K$, we have $T(al_1 + bl_2)(\{x\}) = (al_1 + bl_2)(x) = al_1(x) + bl_2(x) = aT(l_1)(\{x\}) + bT(l_2)(\{x\})$.

(3) $T(l)$ is an isomorphism.

   (a) T is one-to-one. Indeed, if $T(l) = 0$, then $T(l)(\{x\}) = l(x) = 0$, for all $x \in X$. Then we have $l = 0$.

   (b) T is onto. For $\forall \tilde{l} \in (X/Y)'$, define $l \in X'$ such that $l(x) = \tilde{l}(\{x\})$. If $x \in Y$, then $l(x) = \tilde{l}(\{0\}) = 0$, it follows $l \in Y^{\perp}$. Thus, $T(l) = \tilde{l}$ is onto.

Thus, we have $\dim Y^{\perp} = \dim(X/Y)' = \dim(X/Y)$ and hence

$$\dim Y^{\perp} = \dim(X/Y) = \dim X - \dim Y.$$

□

The dimension of $Y^{\perp}$ is called the *codimension* of Y as subspace of X. And since $Y^{\perp}$ is a subspace of X', its annihilator denoted by $Y^{\perp\perp}$ is a subspace of X''.

Theorem 2.2.2. *Under the natural identification of X'' and X, for every subspace Y of a finite-dimensional space X, $Y^{\perp\perp} = Y$.*

Proof. For any $y \in Y$ and $l \in Y^{\perp}$, $y^{**}(l) = l(y) = 0$, where $y^{**} \in Y^{\perp\perp}$. Thus we have $Y \subset Y^{\perp\perp}$. Also, $\dim Y^{\perp\perp} = \dim X' - \dim Y^{\perp} = \dim X - \dim Y^{\perp} = \dim Y$. Thus, $Y = Y^{\perp\perp}$. □

Definition 2.2.2. *Let X be a finite-dimensional linear space, and let S be a subset of X. The annihilator $S^{\perp}$ of S is the set of linear functions l that are zero at all vectors $s \in S$, that is, $l(s) = 0$.*

Theorem 2.2.3. *Denote by Y the smallest subspace containing S, then $S^\perp = Y^\perp$.*

Proof.

(1) Since $S \subset Y$, then $Y^\perp \subset S^\perp$. Indeed, if $l \in Y^\perp$, then $l(y) = 0$ for all $y \in Y$. Since $S \subset Y$, then for $\forall s \in S$, we have $l(s) = 0$. Thus, $Y^\perp \subset S^\perp$.

(2) Now we prove $S^\perp \subset Y^\perp$. Suppose $x_1, \cdots, x_j$ be the basis of S, then $\text{span}\{x_1, \cdots, x_j\} = Y$. Then for any $y \in Y$, it can be written as $y = \sum_{k=1}^{j} c_k x_k$. For $l \in S^\perp$, we have $l(x_k) = 0, 1 \le k \le j$, then $l(y) = \sum_{k=1}^{j} c_k l(x_k) = 0$. Thus, $l \in Y^\perp$, which implies $S^\perp \subset Y^\perp$.

In another words, $S^\perp = (\text{span}S)^\perp$. □

2.3 Quadrature Formula

Theorem 2.3.1. *Let I be an interval on the real axis, $t_1, \cdots, t_n$ are n distinct points. Then there exist n numbers $m_1, \cdots, m_n$ such that the quadrature formula*

$$\int_I p(t)\mathrm{d}t = m_1 p(t) + \cdots + m_n p(t_n)$$

holds for all polynomials p of degree less than n.

Proof. Denote by X the space of all polynomials $P(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1}$ of degree less than n. Since X is isomorphic to the space $\mathbb{R}^n = (a_0, a_1, \cdots, a_{n-1})$, then $\dim X = n$. We define $l_j \in X'$ as the linear function

$$l_j(p) = p(t_j)$$

We claim that $l_j, 1 \le j \le n$ are linearly independent. Indeed, assume $\sum_{k=1}^{n} c_k l_k = 0$, then we have

$$\sum_{k=1}^{n} c_k l_k(p) = \sum_{k=1}^{n} c_k p(t_k) = 0$$

and for k, pick $p(t) = \prod_{j \neq k}(t - t_j)$, then we have $c_k = 0, 1 \le k \le n$. Then $\{l_j\}_{j=1}^{n}$ form a basis of X', since $\dim X' = \dim X = n$. Then any linear function l on X can be represented as below

$$l = m_1 l_1 + \cdots + m_n l_n.$$

The integral of p over I is a linear function, therefore it can be represented as above. □

2.4 Exercises

Exercise 2.4.1. *Suppose $\{x_1, x_2, \cdots, x_n\}$ is a basis for the vector space X. Show that there exists linear functions $\{e_1, e_2, \cdots, e_n\}$ in the dual space X' satisfying*

$$e_i(x_j) = \delta_{ij}$$

Show that $\{e_1, e_2, \cdots, e_n\}$ is a basis of X', called the dual basis.

Proof.

(1) First, we check that $\{e_1, e_2, \cdots, e_n\}$ are linearly independent. Suppose that there exist $a_1, a_2, \cdots, a_n \in K$ such that

$$a_1e_1 + a_2e_2 + \cdots + a_ne_n = 0$$

then for $\forall x_i \in X$, we have

$$(a_1e_1 + a_2e_2 + \cdots + a_ne_n)(x_i) = a_1e_1(x_i) + \cdots + a_ne_n(x_i) = a_i = 0$$

Thus, $a_i = 0$, for $\forall a_i$, which means $\{e_1, e_2, \cdots, e_n\}$ are linearly independent.

(2) Then, we need to show that $\text{span}(e_1, e_2, \cdots, e_n) = X'$. For any $f \in X'$, let $b_i = f(x_i)$, and $f = b_1e_1 + b_2e_2 + \cdots + b_ne_n$. Then, for $\forall x_i$, we have

$$f(x_i) = (b_1e_1 + b_2e_2 + \cdots + b_ne_n)(x_i) = b_i$$

Thus, f can be presented by $\{e_1, e_2, \cdots, e_n\}$. The proof is complete.

□

Exercise 2.4.2. *Let X be a finite dimensional linear space. Show that two nonzero linear functionals $T, S \in X'$ have the same null space if and only if there is a nonzero scalar λ such that $S = \lambda T$.*

Proof.

(1) Since $T : X \to R$, then there $x_1 \in X$ such that $Tx \neq 0$. And we let $x_2 = \frac{x_1}{T(x_1)}$, then we have $T(x_2) = 1$. And for $\forall x \in X$we can know

$$T(x - T(x) \cdot x_2) = T(x) - T(x) = 0$$

Since T and S have the same null space, then we have $S(x - T(x) \cdot x_2) = 0$, then

$$\begin{aligned} S(x) &= S(x - T(x) \cdot x_2 + T(x) \cdot x_2) \\ &= S(x - T(x) \cdot x_2) + S(T(x) \cdot x_2) \\ &= 0 + S(x_2)T(x) \end{aligned}$$

(2) Let $\lambda = S(x_2)$, then we proved that $S = \lambda T$. If $S = \lambda T$, then for $\forall x \in N_P$, we have $T(x) = \frac{1}{\lambda}S(x) = 0$, which means $N_P \subset N_T$. And for $\forall x \in N_T$, $S(x) = 0$, which means $N_T \subset N_P$. So $N_T = N_P$. The proof is complete.

□

Chapter 3

Linear Mappings

3.1 Null-space and Range

Let X, U be linear spaces over the same field K. A mapping $T : X \to Y$ is called linear if it is additive and homogeneous, i.e.,

$$\begin{aligned} T(x+y) &= T(x) + T(y), \forall x, y \in X \\ T(kx) &= kT(x), \forall x \in X, \forall k \in K \end{aligned}$$

For simplicity, we write $T(x) = Tx$.

Example 3.1.1 (Examples of Linear Mappings)**.**

(1) Any isomorphism.

(2) Differentiation from polynomial $P_n(t)$ to $P_{n-1}(t)$.

(3) Linear functionals.

(4) $X = \mathbb{R}^n, U = \mathbb{R}^m, u = TX$ defined by

$$u_i = \sum_{j=1}^{n} t_{ij} x_j, i = 1, 2, \cdots, m$$

Hence, $u = (u_1, \cdots, u_m), x = (x_1, \cdots, x_n)$.

Theorem 3.1.1.

(1) The image of a subspace of X under a linear map T is a subspace of U.

(2) The inverse image of a subspace of U, that is the set of all vectors in X mapped by T into the subspace, is the subspace of X.

Proof. It follows from the definition of subspace. □

Definition 3.1.1. *The range of T is the image of X under T, denoted by R_T. The null-space of T is the inverse image of $\{0\}$, denoted by N_T.*

Remark 3.1.1. *If $T : X \to U$, then $R_T \subset U, N_T \subset U$ are subspaces of U.*

Definition 3.1.2. $\dim R_T$ *is called the rank of the mapping T and* $\dim N_T$ *is called the nullity of the mapping T.*

3.2 Rank-Nullity Theorem

Theorem 3.2.1 (Rank-Nullity Theorem)**.** *Let $T : X \to U$ be a linear map. Then*

$$\dim R_T + \dim N_T = \dim X.$$

Proof. We can define $\tilde{T} : X/N_T \to R_T$ as $\tilde{T}(\{x\}) = Tx \in R_T$, for $\forall x \in X$. We claim that $\tilde{T}$ is an isomorphism. Indeed, if $\{x\} = \{y\}$, then $x - y \in N_T$, then we have $T(x - y) = 0$, which implies $Tx = Ty$. Thus, $\tilde{T}(\{x\}) = \tilde{T}(\{y\})$. Also, $\tilde{T}$ is linear, since $\tilde{T}(a\{x\}+b\{y\}) = a\tilde{T}(\{x\}) + b\tilde{T}(\{y\})$.

Thus, we have $\dim X/N_T = \dim R_T$. With theorem (1.5.1), we have $\dim X - \dim N_T = \dim R_T$. □

Theorem 3.2.2. *Let $T : X \to U$ be a linear map, then*

(a) Suppose $\dim U < \dim X$*, then there exists $x \neq 0$, such that $Tx = 0$.*

(b) Suppose $\dim U = \dim X$*, the only vector satisfying $Tx = 0$ is $x = 0$. Then $R_T = U$ and T is an isomorphism.*

Proof.

(a) Since $\dim R_T \leq \dim U < \dim X$, then we have $\dim N_T = \dim X - \dim R_T > 0$. Then there exists $x \neq 0, x \in N_T$ such that $Tx = 0$.

(b) Since $\dim U = \dim X$, we have $\dim N_T = 0$. Then we have $\dim R_T = \dim U$. Thus $R_T = U$ and T is an isomorphism.

□

3.3 Injectivity and Surjectivity

Definition 3.3.1. *A linear mapping $T : X \to U$ is called injective (or one-to-one) if $Tu = Tv$ implies $u = v$.*

Theorem 3.3.1. *Injectivity is equivalent to null space equals $\{0\}$, i.e., if $T : X \to U$, then T is injective if and only if $N_T = \{0\}$.*

Proof.

(1) ($\Rightarrow$) Suppose T is injective, and we need to prove that $N_T = \{0\}$. We already know that $\{0\} \subset N_T$.

 Let $v \in N_T$, then we have $Tv = 0 = T(0)$. Since T is injective, then we have $v = 0$. Thus, $N_T = \{0\}$.

(2) ($\Leftarrow$) Suppose $N_T = \{0\}$. Let $u, v \in X$ such that $Tu = Tv$. Then we have $Tu - Tv = T(u - v) = 0$, which implies $u = v$. Thus, T is injective.

□

Definition 3.3.2. *A linear mapping $T : X \to U$ is called surjective (or onto) if its range equals U, i.e., $R_T = U$.*

Theorem 3.3.2. *Suppose X and U are finite-dimensional vector spaces such that $\dim X > \dim U$, then no linear map from X to U is injective.*

Proof. Let $T : \mathcal{L}(X, U)$, then with Rank-Nullity theorem, we have

$$\begin{aligned} \dim N_T &= \dim X - \dim R_T \\ &\geq \dim X - \dim U \\ &> 0 \end{aligned}$$

Thus, T is not injective. □

Theorem 3.3.3. *Suppose X and U are finite-dimensional vector spaces such that $\dim X < \dim U$, then no linear map from X to U is surjective.*

Proof. Let $T : \mathcal{L}(X, U)$, then with Rank-Nullity theorem, we have

$$\begin{aligned} \dim R_T &= \dim X - \dim R_T \\ &\leq \dim X \\ &< \dim U \end{aligned}$$

Thus, T is not surjective. □

3.4 Underdetermined Linear Systems

Theorem 3.4.1. *Suppose $m < n$, then for any real numbers $t_{ij}, 1 \leq i \leq m, 1 \leq i \leq n$, the system of linear equations*

$$\sum_{j=1}^{n} t_{ij} x_j = 0, 1 \leq i \leq m$$

has a nontrivial solution.

Proof. Define $T : \mathbb{R}^n \to \mathbb{R}^m$ as

$$T(x_1, \cdots, x_n) = \left(\sum_{j=1}^{n} t_{1j} x_j, \cdots, \sum_{j=1}^{n} t_{nj} x_j \right)$$

Then T is linear, and with previous theorem, there exists $x \in \mathbb{R}^n, x \neq 0$ such that $Tx = 0$. Thus, $x = (x_1, \cdots, x_n)$ is an nontrivial solution. □

Theorem 3.4.2. *Given n^2 real numbers $t_{ij}, 1 \leq i, j \leq n$, the inhomogeneous system of linear equations*

$$\sum_{j=1}^{n} t_{ij} x_j = u_i, 1 \leq i \leq n$$

has a unique solution for any $u_i, 1 \leq i \leq n$ if and only if the homogeneous system

$$\sum_{j=1}^{n} t_{ij} x_j = 0, 1 \leq i \leq n$$

has only the trivial solution.

Proof.

(1) ($\Rightarrow$) Set $u_i = 0$ and it is trivial.

(2) ($\Leftarrow$) Define $T : \mathbb{R}^n \to \mathbb{R}^n$ as

$$T(x_1, \cdots, x_n) = \left(\sum_{j=1}^{n} t_{1j} x_j, \cdots, \sum_{j=1}^{n} t_{nj} x_j \right)$$

If homogeneous system has only trivial solution, then $N_T = \{0\}$, which implies $R_T = \mathbb{R}^n$. Thus, T is an isomoorphism.

□

3.5 Algebra of Linear Mappings

Let X, U be linear spaces and let $\mathscr{L}(X, U)$ be the collection of all linear maps from X to U. $\mathscr{L}(X, U)$ is a linear space if we define

$$(T + S)(x) = Tx + Sx$$
$$(kT)(x) = kTx$$

for $\forall x \in X, \forall k \in K, \forall T, S \in \mathscr{L}(X, U)$.

Definition 3.5.1. *Let $T \in \mathscr{L}(X, U)$ and $S \in \mathscr{L}(U, V)$, where X, U and V are linear spaces. The composition of S and T is defined by*

$$S \circ T(x) = S\left(T(x)\right)$$

denoted by ST, called the multipilication of S and T. In general, $ST \neq TS$.

Remark 3.5.1.

(1) $S \circ T \in \mathscr{L}(X, V)$.

(2) The composition is associative, i.e., if $R \in \mathscr{L}(V, Z)$, then $R \circ (S \circ T) = (R \circ S) \circ T$.

(3) The composition is distributive, i.e., if $T \in \mathscr{L}(X, U)$ and $R, S \in \mathscr{L}(U, V)$, then $(R + S) \circ T = R \circ T + S \circ T$.

Definition 3.5.2. *A linear map is called invertible if it is one-to-one and onto, that is, if it is isomorphism, denoted by T^{-1}.*

Theorem 3.5.1.

(1) The inverse of invertible map is linear.

(2) If S and T are both invertible, then ST is also invertible and $(ST)^{-1} = T^{-1}S^{-1}$.

Proof.

(1) Let $T \in \mathscr{L}(X, U)$ be invertible, it suffices to prove that

$$T^{-1}(k_1u_1 + k_2u_2) = k_1T^{-1}(u_1) + k_2T^{-1}(u_2)$$

for all $k_1, k_2 \in K$ and $u_1, u_2 \in U$. We have

$$\begin{aligned} T\left(T^{-1}(k_1u_1 + k_2u_2)\right) &= k_1TT^{-1}(u_1) + k_2TT^{-1}(u_2) \\ &= k_1u_1 + k_2u_2 \end{aligned}$$

which implies the above indication.

(2) Let $T : U \to V, S : V \to W$ and then $ST : U \to W$, then ST is also an isomorphism, which implies it is invertible. For any $w \in W$, there exists a $u \in U$ such that $(ST)^{-1}(w) = u$. It suffices to prove that $T^{-1}S^{-1}(w) = u$.

If $T^{-1}S^{-1}(w) \neq u$, then there is another $u' \in U$ such that $T^{-1}S^{-1}(w) = u'$. Since S is isomorphism, then there exists only one element in V, saying v such that $S^{-1}(w) = v$ and we have $T^{-1}(v) = u$ and also $T^{-1}(v) = u'$, which is a contradiction.

□

3.6 Transposition

Definition 3.6.1. *Let $T \in L(X, U)$ the transpose $T' \in \mathscr{L}(U', X')$ of T is defined by*

$$(T'(l))(x) = l(T(x))$$

for any $l \in U'$ and $x \in X$. We could use the dual notation to represent the identity as $(T'l, x) = (l, Tx)$.

Theorem 3.6.1.

(1) $(ST)' = T'S'$.

(2) $(T + R)' = T' + R'$.

(3) $(T^{-1})' = (T')^{-1}$.

Proof.

(1) Let $T : X \to U, S : U \to V$. Then we have

$$((ST)'l, x) = (l, STx) = (S'l, Tx) = (T'S'l, x).$$

(2) It is obvious.

(3) Let $T \in \mathscr{L}(X, U)$ be invertible. And we assume $I_U = T \circ T^{-1} : U \to U$. We claim $(T \circ T^{-1})' = (I_U)'$ is an identity of U'. Indeed, $(T^{-1})' \circ T' = I_{U'}$, then we have $(T')^{-1} = (T^{-1})'$. We need to prove that $(I_U)' = I_{U'}$. Indeed, we have $((I_U)'l, u) = (l, I_U u) = (l, u)$, which implies $(I_U)'l = l$. Thus, we have $(I_U)' = I_{U'}$.

□

Example 3.6.1. Let $X = \mathbb{R}^n, U = \mathbb{R}^m$ and $T : X \to U$ is defined by $y = Tx$, where

$$y_i = \sum_{j=1}^{n} t_{ij} x_j, 1 \le i \le m.$$

Identifying $(\mathbb{R}^n)' = \mathbb{R}^n, \mathbb{R}^m = \mathbb{R}^m$, then $T' : \mathbb{R}^m \to \mathbb{R}^n$ is defined by $v = T'u$, where

$$v_j = \sum_{i=1}^{m} t_{ij} u_i, 1 \le j \le m.$$

Theorem 3.6.2. *Let $T \in L(X, U)$. Identifying $X'' = X, U'' = U$, then $T'' = T$.*

Proof. We have $T' \in \mathscr{L}(U', X'), T'' \in \mathscr{L}(X'', U'') = L(X, U)$. Now we pick $X'' \ni x^{**} = x \in X$, then we have

$$(T''x^{**}, l) = (x^{**}, T'l) = (T'l, x) = (l, Tx) = ((Tx)^{**}, l)$$

Thus, $T'' = T$. □

3.7 Dimension of Null-space and Range

Theorem 3.7.1. *Let $T \in \mathscr{L}(X, U)$, then we have $R_T^{\perp} = N_{T'}$ and $R_T = N_{T'}^{\perp}$.*

Proof.

(1) For $l \in R_T^{\perp}$, then for any $u \in R_T$, $(l, u) = 0$. Since $u \in R_T$, then $u = Tx$ for some $x \in X$. Thus, we have

$$(l, Tx) = 0 \Rightarrow (T'l, x) = 0$$

for $\forall x \in X$. Then $T'l = 0$, which implies $l \in N_{T'}$.

(2) Since $R_T^{\perp} = N_{T'}$, then we have $R_T^{\perp\perp} = N_{T'}^{\perp} = R_T$.

□

Theorem 3.7.2. *Let $T \in \mathscr{L}(X, U)$, then* $\dim R_T = \dim R_{T'}$.

Proof. First, we have $\dim R_T + \dim R_T^{\perp} = \dim U$, then we have

$$\dim R_T + \dim N_{T'} = \dim U$$

With Rank-Nullity theorem, we have

$$\dim R_{T'} + \dim N_{T'} = \dim U' = \dim U$$

Thus, $\dim R_{T'} = \dim R_T$. □

Corollary 3.7.1. *Suppose $T \in \mathscr{L}(X, U)$ and* $\dim X = \dim U$*. Then,* $\dim N_T = \dim N_{T'}$.

Proof. From Rank-Nullity theorem, we have

$$\dim R_T + \dim N_T = \dim U$$
$$\dim R_{T'} + \dim N_{T'} = \dim U' = \dim U = \dim X$$

Then it is easy to see that $\dim N_T = \dim N_{T'}$. □

3.8 Similarity

Definition 3.8.1. *Given an invertible element $S \in \mathscr{L}(X,X)$, we assign to each $M \in \mathscr{L}(X,X)$ the element*

$$M_S = SMS^{-1}$$

The assignment $M \mapsto M_S$ is called similarity transformation, M is said to be similar to M_S.

Theorem 3.8.1.

(a) Every similarity transformation is an automorphism of $\mathscr{L}(X,X)$:

$$\begin{aligned}(kM)_S &= kM_S\\ (M+K)_S &= M_S + K_S\\ (MK)_S &= M_S K_S\end{aligned}$$

(b) The similarity transformations form a group with

$$(M_S)_T = M_{TS}.$$

Proof.

(a) We only prove $(MK)_S = M_S K_S$. Indeed, we have

$$(MK)_S = SMKS^{-1} = SMSS^{-1}KS^{-1} = M_S K_S.$$

(b) We have

$$\begin{aligned}M_{TS} = TSM(TS)^{-1} = TSMS^{-1}T^{-1} &= T(SMS^{-1})T^{-1}\\ &= (M_S)_T.\end{aligned}$$

□

Theorem 3.8.2. *Similarity is an equivalence relation, i.e., it is:*

(i) Reflexive. M is similar to itself.

(ii) Symmetric. If M is similar to K, then K is similar to M.

(iii) Transitive. If M is similar to K, K is similar to L, then M is similar to L.

Proof.

(i) It is true if we choose $S = I$ in definition (3.8.1).

(ii) We have $K = SMS^{-1}$, then we have $S^{-1}KS = S^{-1}SMS^{-1}S = M$. Then K is similar to M.

(iii) We have $K = SMS^{-1}$ and $L = TKT^{-1}$, then we have

$$L = TSMS^{-1}T^{-1} = (TS)M(TS)^{-1}$$

which is similar to M.

□

Theorem 3.8.3. *If either A or B in $\mathscr{L}(X, X)$ is invertible, then AB and BA are similar.*

Proof. Assume A is invertible, then we have

$$AB = ABAA^{-1} = (BA)_A.$$

□

3.9 Projection

Definition 3.9.1. *A linear mapping $P \in \mathscr{L}(X, X)$ is called a projection if $P^2 = P$.*

Theorem 3.9.1. *If $P \in \mathscr{L}(X, X)$ is a projection, then $X = N_P \oplus R_P$, and $P|_{R_P} = I$ is identity.*

Proof. Assume $x \in N_P \cap R_P$, then we have $P(x) = 0$. And $x = Py$ for some $y \in X$. Then we have $Px = P^2y = Py = x = 0$, which implies $N_P \cap R_P = \{0\}$. Moreover, with $\dim N_P + \dim R_P = \dim X$, we have $X = N_P \oplus R_P$.

For any $x \in R_P$, we have $x = Py$ for some $y \in X$. Then we have $Px = P^2y = Py = x$, which implies $P|_{R_P}$ is an identity. □

Remark 3.9.1. *The opposite direction of the theorem above is also true. Indeed, for any $x \in X$, we can write $x = y + z$, where $y \in N_P, z \in R_P$. Then we have*

$$\begin{aligned} Px &= Py + Pz = Pz \\ P^2x &= P^2y + P^2z = Pz = Px \end{aligned}$$

Then we have $P^2 = P$.

Definition 3.9.2. *The commutator of two linear mappings A and B of X into X is $AB - BA$. Two mappings of X into X commute if their commutator is zero.*

3.10 Exercises

Exercise 3.10.1. *Let X, U be two linear spaces such that $\dim X = \dim U < \infty$. Prove that a linear mapping $T \in \mathscr{L}(X, U)$ is one-to-one if and only if it is onto.*

Proof.

(1) ($\Rightarrow$) Assume $(x_1, x_2, \cdots, x_n)$ is a basis of X, then we have $\dim R_T = \dim X - \dim N_T$. If $T \in \mathscr{L}(X, U)$ is one-to-one, then $\dim N_T = 0$. We can have $\dim R_T = \dim X = \dim U$. Then $R_T = U$, which implies that T is an isomorphism. Then T is onto.

(2) ($\Leftarrow$) If T is onto, and $\dim X = \dim N$, then the only element $x \in X$ satisfying $Tx = 0$ is $x = 0$. So $\dim N_T = 0$. Then $\dim R_T = \dim U$, which means $R_T = U$. Then T is an isomorphism and T is of course one-to-one.

□

Exercise 3.10.2. *Let X be a finite dimensional linear space and $T \in \mathscr{L}(X, X)$. Suppose*

$$\dim R_{T^2} = \dim R_T.$$

Prove that $R_T \cap N_T = \{0\}$, where $T^2 = T \circ T$.

Proof. We knew that $R_{T^2} \subset R_T$, and since $\dim R_{T^2} = \dim R_T$, we have $R_{T^2} = R_T$, which also implies $N_{T^2} \subset N_T$ by Rank-Nullity theorem.

Assume $y \in N_T \cap R_T$,then there must exists a $x \in X$ such that $y = Tx$. Then we have $T(Tx) = Ty = 0$, since $y \in N_T$. Then, $x \in N_{T^2} = N_T$, then $Tx = 0 = y$. Now we concluded that $R_T \cap N_T = \{0\}$. □

Exercise 3.10.3. *If Y and Z are subspaces of a finite dimensional linear space, prove that*

$$(Y + Z)^\perp = Y^\perp \cap Z^\perp \text{ and } (Y \cap Z)^\perp = Y^\perp + Z^\perp.$$

Proof.

(1) Assume $l \in (Y + Z)^\perp$. Then we have $l(m) = 0$, for all $m \in Y + Z$. Also, we know $Y \subset Y + Z$, so $l(y) = 0, \forall y \in Y$. Similarly, we have $l(z) = 0, \forall z \in Z$. Then we have $l \in Y^\perp \cap Z^\perp$, which implies $(Y + Z)^\perp \subset Y^\perp \cap Z^\perp$.

Now assume $l \in Y^\perp \cap Z^\perp$, then we have $l(y) = 0$ and $l(z) = 0$, for $\forall y \in Y, \forall z \in Z$. Then, for $\forall m \in Y + Z$ we have $l(m) = 0$, since $m = y + z$ for some $y \in Y$ and $z \in Z$. Thus, we have $l \in (Y + Z)^\perp$, which implies $Y^\perp \cap Z^\perp \subset (Y + Z)^\perp$. Now we proved that $(Y + Z)^\perp = Y^\perp \cap Z^\perp$.

(2) It is equivalent to prove that $(Y \cap Z)^{\perp\perp} = Y \cap Z = (Y^\perp + Z^\perp)^\perp$.

If $l \in (Y^\perp + Z^\perp)^\perp$, we have $l(l_1 + l_2) = 0$, for $l_1 \in Y^\perp$ and $l_2 \in Z^\perp$. Also, we have $Y^\perp \subset Y^\perp + Z^\perp$, we have $l(l_1) = 0$ for $\forall l_1 \in Y^\perp$. Similarly, we have $l(l_2) = 0$ for $\forall l_2 \in Z^\perp$. Then $l \in Y^{\perp\perp} = Y$ and $l \in Z^{\perp\perp} = Z$. Thus, $l \in Y \cap Z$, which implies $(Y^\perp + Z^\perp)^\perp \subset Y \cap Z$.

If $l \in Y \cap Z = (Y \cap Z)^{\perp\perp}$, we have $l \in Y \cap Z$, then $l \in Y = Y^{\perp\perp}$ and $l \in Z = Z^{\perp\perp}$. Then we have $l(l_1) = 0, l_1 \in Y^\perp$ and $l(l_2) = 0, l_2 \in Z^\perp$. Thus, we have $l(l_1 + l_2) = 0, l_1 + l_2 \in Y^\perp + Z^\perp$, which implies $l \in (Y^\perp + Z^\perp)^\perp$. Then we have $Y \cap Z \subset (Y^\perp + Z^\perp)^\perp$.

□

Exercise 3.10.4. *Let X, Y be finite dimensional linear space and $T \in \mathscr{L}(X, Y)$ be invertible. Prove that T' is also invertible and $(T^{-1})' = (T')^{-1}$.*

Proof.

(1) Assume $l_1, l_2 \in Y'$, and $(T'l_1)(x) = (T'l_2, x)$ for all $x \in X$. Then we have $(l_1 - l_2, Tx) = 0$ for all $x \in X$, then we have $l_1 = l_2$, which imlpies T is one-to-one.

Also, if $(T'l)(x) = 0$ for all $x \in X$, then it implies $l(T(x)) = 0$. Then l can only be zero. Thus, T' is invertible.

(2) Since T is invertible, then $T \circ T^{-1} = I$. For T', we denote

$$\begin{aligned} &(T \circ T^{-1})' = I' \\ \Rightarrow &(T^{-1})' \circ T' = I' \end{aligned}$$

We need to show $I = I'$. For $y \in Y$, we have

$$(I'l, y) = (l, I(y)) = (l, y)$$

Then $I' = I$, thus we have $(T^{-1})' = (T')^{-1}$.

□

Exercise 3.10.5. *Let X be an n-dimensional linear space and $T \in \mathscr{L}(X, X)$. Prove that there is a non-zero polynomial $p(t)$ of degree no more than n^2 such that $p(T) = 0$.*

Proof. Since X is n-dimensional linear space, and $T \in \mathscr{L}(X, X)$, then T can be presented as an $n \times n$ matrix. Polynomials $p(T)$ can be viewed as an operator acting on the space of matrix T, which is n^2-dimensional, denoted by P. Since $\dim P = n^2$, then for any $T \in P$, $1, T, T^2, \cdots, T^{n^2}$ must be linear dependent, since there are $n^2 + 1$ elements. So there exist $a_0, a_1, a_2, \cdots, a_{n^2}$ such that

$$p(T) = a_0 \cdot 1 + a_1 T + a_2 T^2 + \cdots + a_{n^2} T^{n^2} = 0$$

which is at most degree n^2. □

Exercise 3.10.6. *Prove that if U, V, W are finite dimensional vector spaces, and $T \in \mathscr{L}(U, V), S \in \mathscr{L}(V, W)$, then*

$$\dim N_{ST} \leq \dim N_S + \dim N_T.$$

Proof. Assume $u \in U$, such that $ST(u) = 0$. Then we have two possibilities, that is $u \in N_T$ or $T(u) \in N_S$.

With Rank-Nullity theorem, we have

$$\begin{aligned} \dim N_{ST} &\leq \dim U = \dim N_T + \dim R_T \\ \dim R_T &\leq \dim V = \dim N_S + \dim R_S \\ \Rightarrow \dim N_{ST} &\leq \dim N_T + \dim N_S + \dim R_S \end{aligned}$$

Now we assume $Z = N_{ST} \subset U$, then we have $ST(z) = 0$ for $z \in Z$, and

$$\begin{aligned} \dim N_{ST} &= \dim Z = \dim N_T + \dim T|_Z \\ \dim T|_Z &\leq \dim N_S + \dim ST(Z) \end{aligned}$$

combining these, we have $\dim N_{ST} \leq \dim N_S + \dim N_T$. $\square$

Chapter 4

Matrices

Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be defined by $y = Tx$, where

$$y_i = \sum_{j=1}^{n} t_{ij} x_j, 1 \le i \le m.$$

Then T is a linear map. On the other hand, every map $T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$ can be represented in this form. Actually, t_{ij} is the ith component of Te_j, where $e_j \in \mathbb{R}^n$ has jth component 1, others be 0. We write

$$T = (t_{ij})_{m\times n} = \begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \cdots & t_{mn} \end{pmatrix}$$

which is called an m by n ($m \times n$) matrix, where t_{ij} is called the *entries* of the matrix T. A matrix is called a *square matrix* if $m = n$.

A matrix T can be thought of as a row of column vectors, or a column of row vectors:

$$T = (c_1, \cdots, c_n) = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{pmatrix}.$$

where $c_j = Te_j$, $e_j \in \mathbb{R}^n$ is defined as above.

4.1 Matrix Multiplication and Transposition

Since matrices represent linear mappings, the algebra of linear mappings induces a corresponding algebra of matrices, i.e., if $T, S \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$, then

$$T + S = (t_{ij} + s_{ij})_{m\times n}$$
$$kT = (kt_{ij})_{m\times n}$$

If $T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$ and $S \in \mathscr{L}(\mathbb{R}^m, \mathbb{R}^l)$, then the product $St = S \circ T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^l)$. For $e_j \in \mathbb{R}^n$,

$$\begin{aligned}(ST)(e_j^n) = S(Te_j^n) = S\left(\sum_{i=1}^m t_{ij} e_i^m\right) &= \sum_{i=1}^m t_{ij} S(e_i^m) \\ &= \sum_{i=1}^m t_{ij}\left(\sum_{k=1}^l s_{ki} e_k^l\right) = \sum_{k=1}^l \left(\sum_{i=1}^m t_{ij} s_{ki}\right) e_k^l \\ &= \sum_{k=1}^l (ST)_{kj} e_k^l\end{aligned}$$

where $e_j^m \in \mathbb{R}^m, e_j^l \in \mathbb{R}^l$. Hence, we have

$$(ST)_{kj} = \sum_{i=1}^m t_{ij} s_{ki}$$

which is the product of kth row of S and jth column of T.

We can write any $n \times n$ matrix A in 2×2 block form

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

where A_{11} is $k \times k$ matrix, and A_{22} is $(n-k) \times (n-k)$ matrix.

We shall identify the dual of the space $\mathbb{R}^n$ of all column vectors with n components as the space $(\mathbb{R}^n)'$ of all row vectors with n components. For $l \in (\mathbb{R}^n)'$ and $x \in \mathbb{R}^n$,

$$lx = \sum_{i=1}^n l_i x_i$$

Let $x \in \mathscr{L}(\mathbb{R}, \mathbb{R}^n), T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$, and $l \in \mathscr{L}(\mathbb{R}^m, \mathbb{R})$ be linear mappings, according to associative law, we have

$$(lT)x = l(Tx)$$

We identity l as an element of $(\mathbb{R}^m)'$, and lT as an element of $(\mathbb{R}^n)'$, and we can rewrite is into form

$$(lT, x) = (l, Tx)$$

and we recall the definition of transpose T' of T, defined by $(T'l, x) = (l, Tx)$. Now we can define the transpose T^T of the matrix T as

$$\left(T^T\right)_{ij} = T_{ji}.$$

4.2 Rank

Theorem 4.2.1. *Let $T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$, the range of T consists of all linear combinations of the columns of the matrix T.*

Definition 4.2.1. *The* $\dim R_T$ *is called the column rank of T, and* $\dim R_{T^T}$ *is called the row rank of T.*

Theorem 4.2.2. $\dim R_T = \dim R_{T^T}$.

Proof. We can apply elementary row operations and elementary column operations to make A into a matrix that is in both row and column reduced form, i.e., there exist invertible matrices P and Q (which are products of elementary matrices) such that

$$PAQ = E = \begin{pmatrix} I_k & \\ & 0_{(m-k)\times(n-k)} \end{pmatrix}$$

Since P and Q are invertible, then the maximum number of linearly independent rows in A is equal to the maximum number of linearly independent rows in E. Also, it is similar for the column rank. Then it is obvious that $\dim R_T = \dim R_{T^T}$. □

Now we present another different approach to prove this theorem.

Proof. Let T be $m \times n$ matrix and it has row rank k. Therefore, the dimension of the row space of T is k. Let $x_1, \cdots, x_k$ be a basis of row space of T and we claim that $Tx_1, \cdots, Tx_k$ are linearly independent. Indeed, we choose coefficients $c_1, \cdots, c_k$ and then

$$c_1Tx_1 + \cdots + c_kTx_k = T(c_1x_1 + \cdots + c_kx_k) = Tx = 0$$

Then x is a linear combination of basis of row space of T, which implies that x belongs to row space of T. Also, $TX = 0$ implies that x is orthogonal to every vector of row space of T, then x is orthogonal to itself, giving us $x^2 = c_1^2x_1^2 + \cdots + c_k^2x_k^2 = 0$. Then it is obvious that $c_1 = \cdots = c_k = 0$.

Now, each Tx_i is obviously in the column space of T, and then $Tx_1, \cdots, Tx_k$ are k linearly independent vectors in the column space of T, implying that $\dim R_{T_T} \leq \dim R_T$.

Now we can consider T^T in the similar argument, and it will give us $\dim R_{T_T} \geq \dim R_T$. Thus, we have $\dim R_{T_T} = \dim R_T$. □

Next, we discuss some properties of rank of a matrix.

Proposition 4.2.1. *Let $T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$, and define the linear map f by $f(x) = Tx$, then*

(1) $\operatorname{rank}(T) \leq \min(m, n)$*. A matrix that has rank equal to* $\min(m, n)$ *is called full rank; otherwise, the matrix is rank deficient.*

(2) Only a zero matrix has rank zero.

(3) f is injective(or one-to-one) if and only if T has rank n, i.e. full column rank.

(4) f is surjective(or onto) if and only if T has rank m, i.e. full row rank.

(5) If T is a square matrix, i.e., $m = n$, then T is invertible if and only if T has rank n(that is, T has full rank).

(6) If T is a square matrix, then T is invertible if and only if its determinant is non-zero.

(7) If $S \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^k)$, then

$$\operatorname{rank}(TS) \leq \min(\operatorname{rank}(T), \operatorname{rank}(S)).$$

(8) If S is an $n \times k$ matrix of rank n, then

$$\operatorname{rank}(TS) = \operatorname{rank}(T).$$

(9) If K is a $l \times m$ matrix of rank m, then

$$\operatorname{rank}(KT) = \operatorname{rank}(T).$$

(10) The rank of T is equal to k if and only if there exists an invertible $m \times m$ matrix P and an invertible $n \times n$ matrix Q such that

$$PTQ = \begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}$$

where $I_{k \times k}$ is $k \times k$ identity matrix.

(11) Sylvester's rank inequality: if A is an $m \times n$ matrix and B is $n \times k$, then

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

(12) Frobenius inequality: if AB, ABC and BC are defined, then

$$\operatorname{rank}(AB) + \operatorname{rank}(BC) \leq \operatorname{rank}(B) + \operatorname{rank}(ABC).$$

(13) Subadditivity:

$$\operatorname{rank}(A + B) \leq \operatorname{rank}(A) + \operatorname{rank}(B).$$

when A and B are of the same dimension. As a consequence, a rank-k matrix can be written as the sum of k rank-1 matrices, but not fewer.

(14) Rank–Nullity theorem: The rank of a matrix plus the nullity of the matrix equals the number of columns of the matrix, i.e., for T being a $m \times n$ matrix, then

$$\operatorname{Rank} T + \operatorname{Nullity} T = n.$$

Proof.

(1) Since $T : \mathbb{R}^n \to \mathbb{R}^m$, then the image of T is a subspace of $\mathbb{R}^m$, and it is easy to see that $\operatorname{rank}(T) \leq m$. Also, with Rank-Nullity theorem, we have $\operatorname{rank}(T) \leq n$. Thus, $\operatorname{rank}(T) \leq \min(m, n)$.

(2) T is $m \times n$ matrix and has rank 0, then the nullity of T is n, which implies that all columns of T are zero vectors.

(3) ($\Rightarrow$) If f is injective, then there exists only one element x' in $\mathbb{R}^n$ such that $Tx' = 0 \in \mathbb{R}^m$. Also, we claim $x' = 0 \in \mathbb{R}^n$. Indeed, we have $T0 = T(0 - 0) = T(0) - T(0) = 0$. Thus, we have $N_T = \{0\}$, implying that T is full column rank.

($\Leftarrow$) Since T is full column rank, and then we have $N_T = \{0\}$. For $x_1, x_2 \in \mathbb{R}^n$ such that $Tx_1 = Tx_2$, we have $T(x_1 - x_2) = 0$. Thus, $x_1 = x_2$, implying that f is one-to-one.

(4) ($\Rightarrow$) If f is surjective, then the columns of T span the space $\mathbb{R}^m$, which implies $\operatorname{rank} T = m$.

($\Leftarrow$) This direction is bovious.

(5) ($\Rightarrow$) If T is invertible, then there exists T^{-1} such that $TT^{-1} = I$. Then we have $\det(T)\det(T^{-1}) = 1$, which implies $\det(T) \neq 0$. Thus, T has full rank.

($\Leftarrow$) If T is full rank, the its row reduced echelon form is identity matrix. Then there exists a $n \times n$ matrix H such that $TH = I$. Thus, T is invertible.

(6) It is shown in last statement.

(7) We have TS is a $m \times k$ matrix, and then we have $R_{TS} \subset R_T$, which implies $\operatorname{rank}(TS) \leq \operatorname{rank}(T)$. Similarly, we have $R_{(TS)'} \subset R_{S'}$, which implies $\operatorname{rank}(TS) = \operatorname{rank}(TS)' \leq \operatorname{rank}(S') = \operatorname{rank} S$. Then the result follows.

(8) The rank is the dimension of the column space. The column space of TS is the same as the column space of T. Indeed, for any $y \in \mathbb{R}^n$, there is a $x \in \mathbb{R}^k$ such that $y = Sx$, since S is of rank n, implying that S is onto. Then we have $Ty = TSx$. Thus, $\operatorname{rank}(TS) = \operatorname{rank}(T)$.

(9) For any $x \in \mathbb{R}^n$, we denote Tx by $y \in \mathbb{R}^m$. And since K is full column rank, then the rank of Ky is equal to the rank of y, which implies that $\operatorname{rank}(KT) = \operatorname{rank}(T)$.

(10) With Rank-Nullity theorem and $T : \mathbb{R}^n \to \mathbb{R}^m$, we have $\dim R_T + \dim N_T = n$. Then we can find a basis $(x_1, \cdots, x_k, x_{k+1}, \cdots, x_n)$ for $\mathbb{R}^n$, where $(x_{k+1}, \cdots, x_n)$ is a basis for null space N_T of T.

Now we define $f_j = T(e_j), 1 \leq j \leq k$, then it is easy to see that $(f_1, \cdots, f_k)$ is linearly independent. Then we can complete this basis into a basis $(f_1, \cdots, f_k, f_{k+1}, \cdots, f_m)$ of $\mathbb{R}^m$. Relative to this basis, we can choose

$$f_1 = (1, 0, \cdots, 0)^T, \cdots, f_j = (0, \cdots, \underbrace{1}_{j\text{th}}, \cdots, 0)^T, \cdots, f_k = (0, \cdots, \underbrace{1}_{k\text{th}}, \cdots, 0)^T$$

which gives us I_K, along with all zeros below for the first k columns of T, which is [1]

$$\begin{pmatrix} I_k \\ 0 \end{pmatrix}.$$

(11) Suppose A is an $m \times n$ matrix and B is an $n \times k$ matrix, then we have AB is an $m \times k$ matrix. With Rank-Nullity theorem, we have

$$\begin{aligned} \dim R_A + \dim N_A &= n \\ \dim R_B + \dim N_B &= k \\ \dim R_{AB} + \dim N_{AB} &= k \end{aligned}$$

Then, we have

$$\begin{aligned} \dim N_A + \dim R_B + \dim N_A + \dim N_B &= n + \dim R_{AB} + \dim N_{AB} \\ \Rightarrow \dim R_{AB} - \dim R_A - \dim R_B + n &= \dim N_A + \dim N_B - \dim N_{AB} \geq \dim N_A \geq 0 \end{aligned}$$

since $\dim N_B - \dim N_{AB} \leq 0$. Indeed, for any $v \in N_B$, we have $BV = 0$, also, we have $ABv = 0$, which implies $N_B \subset N_{AB}$ [7].

(12) Consider $A_{m\times n}$ and $B_{n\times k}$ and B is of rank r. Using full-rank factorization of B, we have $B = U_{n\times r}V_{r\times k}$, where both U and V are of rank r[6][4]. With Sylvester's rank inequality, we have

$$\begin{aligned} \operatorname{rank}(ABC) &\geq \operatorname{rank}(AU) + \operatorname{rank}(VC) - r \\ &= \operatorname{rank}(AB) + \operatorname{rank}(BC) - \operatorname{rank}(B) \end{aligned}$$

Then the inequality follows[5].

(13) It is easy to see that $C(A+B) \subset C(A) + C(B)$, where $C(A)$ denote the column space of A. Indeed, for any $y \in C(A+B)$, we can find x such that $y = (A+B)x = Ax + Bx \in C(A) + C(B)$. Thus, $\operatorname{rank}(A+B) \leq \operatorname{rank}(A) + \operatorname{rank}(B)$.

(14) Rank–Nullity theorem is proved before.

□

A linear mapping $T \in \mathscr{L}(X, U)$ can be represented by a matrix if the bases for X and U are chosen. A choice of basis for X defineds an isomorphism $B : X \to \mathbb{R}^n$, and similarly, we have isomorphism $C : U \to \mathbb{R}^m$. Clearly, there are as many isomorphisms as there are bases. We can use any of these isomorphisms to represent T as a matrix from $\mathbb{R}^n$ to $\mathbb{R}^m$, and we have a matrix representation M:

$$CTB^{-1} = M.$$

If $T \in \mathscr{L}(X, X)$, and $B : X \to \mathbb{R}^n$ is an isomorphism, then we have $M = BTB^{-1} \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^n)$ is a square matrix. Let $C : X \to \mathbb{R}^n$ be another isomorphism, then $N = CTC^{-1}$ is another square matrix. Also, we have

$$N = CB^{-1}MBC^{-1}$$

then M and N are similar. Thus, similar matrices represent the same linear mapping under different choices of bases.

Definition 4.2.2. *Two $n \times n$ matrices A and B are similar if there exists isomorphism $M \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^n)$ such that $A = MBM^{-1}$.*

Definition 4.2.3. *An $n \times n$ matrix A is said to be invertible if and only if A is an isomorphism. And we say A is singular if it is not invertible.*

Remark 4.2.1. *Invertible, non-singular and full rank are equivalent.*

Definition 4.2.4. *Let I be the identity matrix, if A is invertible, then there exists a matrix, called inverse of A, denoted by A^{-1} such that $AA^{-1} = A^{-1}A = I$.*

4.3 Exercises

Chapter 5

Determinant and Trace

5.1 Ordered Simplices, Signed Volume and Determinant

A *simplex* in $\mathbb{R}^n$ with $n+1$ vertices. We take one of the vertices to be the origin and denote others by $a_1, \cdots, a_n$. The orders in which the vertices are taken matters, and we say $0, a_1, \cdots, a_n$the vertices of an *ordered simplex*.

An ordered simplex S is called *degenerate* if it lies on an $(n-1)$-dimensional subspace. An ordered nondegenerate simplex $S = (0, a_1, \cdots, a_n)$ is called *positively oriented* if it can be deformed continuously and nondegenerately into the standard simplex $(0, e_1, \cdots, e_n)$, where e_j is the jth unit vector in the standard basis of $\mathbb{R}^n$. By such deformation we mean n vector-valued continuous functions $a_j(t)$ of $t, 0 < t < 1$, such that (i) $S(t) = (0, a_1(t), \cdots, a_n(t))$ is nondegenerate for all t and (ii) $a_j(0) = 0, a_j(i) = e_j$. Otherwise, we say it *negatively oriented*.

For a nondegenerate simplex S, we define $\mathcal{O}(S) = +1(-1)$ if it is positivelt (negatively) oriented. For a degenerate simplex S, we set $\mathcal{O}(S) = 0$. The *volume* of a simplex S is given by elementary formula

$$\text{Vol}(S) = \frac{1}{n}\text{Vol}_{n-1}(\text{base}) \times \text{Altitude}$$

by base we mean any of the $(n-1)$-dimensional surfaces of S, and by altitude we mean the distance from the opposite vertices to the hyperplane that contains the base.

And the *signed volume* of an ordered simplex S is defined as

$$\sum(S) = \mathcal{O}(S)\text{Vol}(S).$$

Since S is described by its vertices, $\sum(S)$ is a function of $a_1, \cdots, a_n$. Obviously, when two vertices are equal, S is degenerate. Thus, we have following properties:

(i) $\sum(S) = 0$ if $a_j = a_k, i \neq k$.

(ii) $\sum(S)$ is a linear function of a_j when $a_k, k \neq j$ are fixed.

(iii) $\sum(0, e_1, \cdots, e_n) = \frac{1}{n!}$.

Now we consider the signed volume as

$$\sum(S) = \frac{1}{n}\mathrm{Vol}_{n-1}(\text{base})$$

where $k = \mathcal{O}(S)$Altitude. The altitude is the *distance* of the vertex a_j, also k is called *signed distance* of the vertex from the hyperplane containing the base.

Determinant are related to the signed volume of ordered simplices by formula

$$\sum(S) = \frac{1}{n!}D(a_1, \cdots, a_n).$$

Definition 5.1.1. *Let $A = (a_1, \cdots, a_n)$ be a square matrix, where $a_j \in \mathbb{R}^n, 1 \leq j \leq n$ are column vectors. Its determinant is defined by*

$$\det A = D(a_1, \cdots, a_n) = n! \sum(S)$$

where $S = (0, a_1, \cdots, a_n)$.

Theorem 5.1.1.

(i) $D(a_1, \cdots, a_n) = 0$ if $a_j = a_k$ for some $j \neq k$.

(ii) $D(a_1, \cdots, a_n)$ is a multilinear function of its arguments.

(iii) Normalization: $D(e_1, \cdots, e_n) = 1$.

(iv) D is an alternating function of its arguments, i.e., if a_j and a_k are interchanged, $j \neq k$, the value of D changes by -1.

(v) If $a_1, \cdots, a_n$ are linearly dependent, then $D(a_1, \cdots, a_n) = 0$.

Proof. The first three statements are obvious. We only prove (iv) and (v).

(iv) Let $D(a, b) = (\cdots, a_i, \cdots, a_j, \cdots)$ and $D(b, a) = (\cdots, a_j, \cdots, a_i, \cdots)$. Then we have

$$\begin{aligned}
D(a, b) &= D(a, a) + D(a, b) \\
&= D(a, a+b) - D(a+b, a+b) \\
&= -D(b, a+b) \\
&= -D(b, a+b) + D(b, b) \\
&= -D(b, a).
\end{aligned}$$

(v) Suppose $a_1, \cdots, a_n$ are linearly dependent, then there exist $c_1, \cdots, c_n$ not all zero, such that $\sum_{j=1}^n c_j a_k = 0$. Without losing generality, assume $c_1 \neq 0$, then we have

$$\begin{aligned}
a_1 &= -\sum_{j=2}^n \frac{c_k}{c_1} a_k \\
\Rightarrow D(a_1, \cdots, a_n) &= D\left(-\sum_{j=2}^n \frac{c_k}{c_1} a_k, a_2, \cdots, a_n\right) \\
&= -\frac{c_k}{c_1}\sum_{j=2}^n D(a_k, a_2, \cdots, a_n) = 0.
\end{aligned}$$

$\square$

5.2 Permutation

Definition 5.2.1. *A permutation is a mapping p of n objects, saying the numbers $1, 2, \cdots, n$, onto themselves. Permutations are invertible and they form a group with compositions. These groups, except for $n = 2$, are noncommutative.*

Example 5.2.1. Let $p = \frac{1234}{2413}$. Then

$$p^2 = \frac{1234}{4321}, \quad p^{-1} = \frac{1234}{3142}$$
$$p^3 = \frac{1234}{3142}, \quad p^4 = \frac{1234}{1234}.$$

Next we introduce *signature* of a permutation, denoted by $\sigma(p)$. Let $x_1, \cdots, x_n$ be n variables, their *discriminant* is defined by

$$P(x_1, \cdots, x_n) = \prod_{i<j} (x_i - x_j).$$

Let p be any permutation, then we have

$$\prod_{i<j} \left(x_{p(i)} - x_{p(j)} \right)$$

is either $P(x_1, \cdots, x_n)$ or $-P(x_1, \cdots, x_n)$.

Definition 5.2.2. *The signature $\sigma(p)$ of a permutation p is defined by*

$$P\left(x_{p(1)}, \cdots, x_{p(n)}\right) = \sigma(p) P(x_1, \cdots, x_n).$$

Hence, $\sigma(p) = \pm 1$.

Theorem 5.2.1. *$\sigma(p_1 \circ p_2) = \sigma(p_1)\sigma(p_2)$.*

Proof.

$$\begin{aligned}
\sigma(p_1 \circ p_2) &= \frac{P\left(x_{p_1 p_2(1)}, \cdots, x_{p_1 p_2(n)}\right)}{P(x_1, \cdots, x_n)} \\
&= \frac{P\left(x_{p_1 p_2(1)}, \cdots, x_{p_1 p_2(n)}\right)}{P(x_{p_2(1)}, \cdots, x_{p_2(n)})} \cdot \frac{P\left(x_{p_2(1)}, \cdots, x_{p_2(n)}\right)}{P(x_1, \cdots, x_n)} \\
&= \sigma(p_1)\sigma(p_2).
\end{aligned}$$

$\square$

Given any pair of indices, $j \neq k$, we can define a permutation p such that

$$p(i) = \begin{cases} i, i \neq j \text{ or } k \\ k, i = j \\ j, i = k \end{cases}$$

Such a permutation is called *transposition*. And we claim that transposition has following properties:

(1) The signature of a transposition t is -1, i.e., $\sigma(t) = -1$.

(2) Every permutation p can be written as a composition of transpositions, i.e.,

$$p = t_k \circ \cdots \circ t_1 \tag{5.2.0.1}$$

Proof.

(1) Assume t interchanges i_0 and j_0, with $i_0 < j_0$, then we have

$$\begin{aligned} P\left(t(x_1, \cdots, x_n)\right) &= P(x_1, \cdots, x_{j_0}, \cdots, x_{i_0}, \cdots, x_n) \\ &= (x_{j_0} - x_{i_0}) \prod_{i<j,(i,j)\neq(i_0,j_0)} (x_i - x_j) \\ &= -\prod_{i<j}(x_i - x_j) \\ &= -P(x_1, \cdots, x_n) \end{aligned}$$

Hence, $\sigma(t) = -1$.

(2) It is easy to see that $p = t_k \circ \cdots \circ t_1$ is equivalent to $I = p = t_k \circ \cdots \circ t_1 \circ p^{-1}$. Consider $(1, \cdots, n) = t_k \circ \cdots \circ t_1 \circ p^{-1}(1, \cdots, n)$. Then we claim a sequence of transposition can sort an array of numbers into ascending order.

□

With the results above, we have

$$\sigma(p) = (-1)^k$$

where k is the number of transpositions in the decomposition (5.2.0.1) of p.

5.3 Formula for Determinant

Theorem 5.3.1. *Assume that for* $1 \leq k \leq n$,

$$a_k = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{nk} \end{pmatrix} \in \mathbb{R}^n.$$

This is the same as

$$a_k = a_{1k}e_1 + \cdots + a_{nk}e_n.$$

with multilinearity, we can write

$$\begin{aligned} D(a_1, \cdots, a_n) &= D(a_{11}e_1 + \cdots + a_{n1}e_n, a_2, \cdots, a_n) \\ &= a_{11}D(e_1, a_2, \cdots, a_n) + \cdots + a_{n1}D(e_n, a_2, \cdots, a_n) \end{aligned}$$

Next we can express a_2 *as a linear combination of* $e_1, \cdots, e_n$*, and obtain a equation like above, with* n^2 *terms. Repeating this process, we have*

$$D(a_1, \cdots, a_n) = \sum_f a_{f_1 1}a_{f_2 2} \cdots a_{f_n n} D(e_{f_1}, e_{f_2}, \cdots, e_{f_n})$$

where the summation is over all functions f *mapping* $\{1, \cdots, n\}$ *into* $\{1, \cdots, n\}$*. If* f *is not a permutation, then* $f_i = f_j$ *for some* $i \neq j$*. Then we have* $D(e_{f_1}, e_{f_2}, \cdots, e_{f_n}) = 0$*. This shows that we only need to sum over permutations.*

Since each permutation can be decomposed into k *transpositions, thus we have*

$$D(e_{f_1}, e_{f_2}, \cdots, e_{f_n}) = \sigma(p)D(e_1, e_2, \cdots, e_n)$$

for any permutation. Then the determinant can be represented as

$$D(a_1, \cdots, a_n) = \sum_p \sigma(p)a_{p(1)1}a_{p(2)2} \cdots a_{p(n)n}$$

where the summation is over all permutations.

Proof. The proof is within the explanation of the theorem, i.e.,

$$\begin{aligned} D(a_1, \cdots, a_n) &= D\left(\sum_{j=1}^n a_{j1}e_j, \cdots, \sum_{j=1}^n a_{jn}e_j\right) \\ &= \sum_{1 \leq j_k \leq n, 1 \leq k \leq n} a_{f_1 1}a_{f_2 2} \cdots a_{f_n n} D(e_{f_1}, e_{f_2}, \cdots, e_{f_n}) \\ &= \sum_p \sigma(p)a_{p(1)1}a_{p(2)2} \cdots a_{p(n)n}. \end{aligned}$$

□

Remark 5.3.1. *Determinant is defined by properties (i),(ii) and (iii) in Theorem 5.1.1.*

Theorem 5.3.2. $\det A^T = \det A$.

Proof. Assume $A = (a_{ij})_{n\times n}$, then $A^T = (b_{ij})_{n\times n}, b_{ij} = a_{ji}$. Then we have

$$\begin{aligned} \det A^T &= \sum_p \sigma(p)b_{p(1)1}b_{p(2)2} \cdots b_{p(n)n} \\ &= \sum_p \sigma(p)a_{1p(1)}a_{2p(2)} \cdots a_{np(n)} \\ &= \sum_p \sigma(p)a_{p^{-1}(1)}a_{p^{-1}(2)2} \cdots a_{p^{-1}(n)n} \end{aligned}$$

we denote p^{-1} by $\tilde{p}$, then we have

$$\det A^T = \sum_{\tilde{p}} \sigma(\tilde{p}) a_{\tilde{p}(1)} a_{\tilde{p}(2)2} \cdots a_{\tilde{p}(n)n} = \det A.$$

□

Theorem 5.3.3. *Let A, B be two $n \times n$ matrices, then* $\det(BA) = \det A \cdot \det B$.

Proof. Assume $A = D(a_1, \cdots, a_n)$, then $BA = (Ba_1, \cdots, Ba_n)$, which implies $\det BA = D(Ba_1, \cdots, Ba_n)$.

(1) Define for $\det B \neq 0$, that $C(a_1, \cdots, a_n) = \frac{\det BA}{\det B}$. It suffices to show that C satisfies:

   (i) If $a_i = a_j$ for some $i \neq j$, then $C = 0$. Indeed, if $a_i = a_j$ for some $i \neq j$, then $Ba_i = Ba_j$. Thus, $D(Ba_1, \cdots, Ba_n) = 0$.

   (ii) C is linear in $a_k, 1 \leq k \leq n$. This is obvious.

   (iii) $C(e_1, \cdots, c_n) = 1$. Indeed, setting $a_i = e_i, 1 \leq i \leq n$. And we get

$$\begin{aligned} C(e_1, \cdots, e_n) &= \frac{D(Be_1, \cdots, Be_n)}{\det B} \\ &= \frac{D(b_1, \cdots, b_n)}{\det B} \\ &= \frac{\det B}{\det B} = 1. \end{aligned}$$

   Then we claim $C(a_1, \cdots, a_n) = \det A$.

(2) If $\det B = 0$, then there exists $\varepsilon_n \to 0$ as $n \to \infty$ such that $\det(B + \varepsilon_n I) \neq 0$. Then we have

$$\begin{aligned} \det\left((B + \varepsilon_n I)A\right) &= \det(B + \varepsilon_n I) \det A \\ &\overset{n \to \infty}{=} \det A \det B. \end{aligned}$$

□

Corollary 5.3.1. *Let A be an $n \times n$ matrix, then A is invertible if and only if* $\det A \neq 0$.

Proof.

(1) ($\Rightarrow$) If A is invertible, then there exists A^{-1} such that $A^{-1}A = I$. Then we have $\det A = 1/\det A^{-1} \neq 0$.

(2) If $\det A \neq 0$, then A is both full row rank and full column rank. Then, A is bijective from $\mathbb{R}^n$ to $\mathbb{R}^n$. Thus, A is invertible.

□

5.4 Laplace Expansion

Now we discuss another property of determinant, starting with a lemma.

Lemma 5.4.1. *Let A be an $n \times n$ matrix, whose first column is e_1:*

$$A = \begin{pmatrix} 1 & \times \\ 0 & A_{11} \end{pmatrix},$$

here A_{11} denote the $(n-1) \times (n-1)$ submatrix formed by entries $a_{ij}, i > 1, j > 1$. We claim that

$$\det A = \det A_{11}.$$

Proof. First, we show that $\det A = \det \begin{pmatrix} 1 & 0 \\ 0 & A_{11} \end{pmatrix}$. And from properties (i) and (ii) that if we add suitable multiples of the first column of A to the others, we can obtain $\begin{pmatrix} 1 & 0 \\ 0 & A_{11} \end{pmatrix}$, and the determinant will not change.

Define

$$C(A_{11}) = \det \begin{pmatrix} 1 & 0 \\ 0 & A_{11} \end{pmatrix}$$

then it suffices to verify C satisfies all three properties:

(1) If $a_i, a_j \in A_{11}$ such that $a_i = a_j, i \neq j$, then we have $\begin{pmatrix} 0 \\ a_1 \end{pmatrix} = \begin{pmatrix} 0 \\ a_2 \end{pmatrix}$ Thus, $C(A_{11}) = 0$.

(2) Any linear operations of A_{11} can be extended to $\begin{pmatrix} 0 \\ a_i \end{pmatrix}$, then C is multilinear.

(3) When $A_{11} = I_{(n-1)\times(n-1)}$, then we have $\begin{pmatrix} 1 & 0 \\ 0 & A_{11} \end{pmatrix} = I_{n \times n}$, then $C(A_{11}) = 1$.

□

Now we present another approach to prove this lemma.

Proof.

$$\begin{aligned}
\det \begin{pmatrix} 1 & \times \\ 0 & A_{11} \end{pmatrix} = \det \begin{pmatrix} 1 & 0 \\ \times & A_{11}^T \end{pmatrix} &= \det \begin{pmatrix} 1 & 0 & \cdots & 0 \\ a_{12} & & & \\ \vdots & & A_{11} & \\ a_{1n} & & & \end{pmatrix} \\
&= D\left(e_1 + \sum_{k=2}^{n} a_{1k} e_k, \widetilde{A_{11}}\right) \\
&= D(e_1, \widetilde{A_{11}}) + \sum_{k=2}^{n} a_{1k} D(e_k, \widetilde{A_{11}}) \\
&= \det A_{11}.
\end{aligned}$$

□

Theorem 5.4.2 (Laplace expansion)**.** *For any $j = 1, \cdots, n$,*

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} c \det A_{ij}$$

where A_{ij} is the (ij)th minor of A.

Proof. The jth column $a_j = \sum a_{ij} e_i$. Hence,

$$\begin{aligned}
\det A &= \sum_{i=1}^{N} a_{ij} D(a_1, \cdots, a_{j-1}, e_i, a_{j+1}, \cdots, a_n) \\
&= \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}
\end{aligned}$$

where we need the lemma below. □

Lemma 5.4.3. *Let A be a matrix with jth column being e_i. Then*

$$\det A = (-1)^{i+j} \det A_{ij}.$$

Proof.

$$\begin{aligned}
\det A &= D(a_1, \cdots, a_{j-1}, e_i, a_{j+1}, \cdots, a_n) \\
&= (-1)^{j-1} D(e_i, a_1, \cdots, a_{j-1}, a_{j+1}, \cdots, a_n) \\
&= (-1)^{i+j-2} \det \begin{pmatrix} 1 & \times \\ 0 & A_{11} \end{pmatrix} \\
&= (-1)^{i+j} \det A_{11}.
\end{aligned}$$

where the last step comes from lemma above. □

5.5 Cramer's Rule

If $A_{n\times n}$ is invertible, then for all $u \in \mathbb{R}^n$, $Ax = u$ has a unique solution $x = A^{-1}u$. Assume $A = (a_1, \cdots, a_n)$ and $x = \sum x_j e_j$, then we have

$$u = \sum x_j a_j.$$

Now consider $A_k = (a_1, \cdots, a_{k-1}, \underbrace{u}_{k\,\text{th}}, a_{k+1}, \cdots, a_n)$. Then we have

$$\det A_k = \sum x_j \det(a_1, \cdots, a_{k-1}, a_j, a_{k+1}, \cdots, a_n) = x_k \det A$$

hence, we have

$$x_k = \frac{\det A_k}{\det A}.$$

And since

$$\det A_k = \sum_{j=1}^{n} (-1)^{j+k} u_j \det A_{jk}$$

we have

$$x_k = \sum_{j=1}^{n} (-1)^{j+k} u_j \frac{\det A_{jk}}{\det A}.$$

Comparing it with $x = A^{-1}u$, we have the following result.

Theorem 5.5.1. *The inverse matrix A^{-1} of an invertible matrix A has the form*

$$\left(A^{-1}\right)_{kj} = (-1)^{j+k} \frac{\det A_{jk}}{\det A}.$$

5.6 Trace of A Matrix

Definition 5.6.1. *The trace of a square matrix A, denoted by $\operatorname{tr} A$, is the sum of all diagonal entries:*

$$\operatorname{tr} A = \sum_{i=1}^{n} a_{ii}.$$

Theorem 5.6.1.

(i) Trace is a linear functional on matrices.

(ii) Trace is commutative: $\operatorname{tr} AB = \operatorname{tr} BA$.

Proof. The proof is obvious. □

Definition 5.6.2. *Let A be an $n \times n$ matrix, then we have*

$$\operatorname{tr} AA^T = \sum_{i=1}^{n} (a_{ii})^2$$

and the Euclidean norm (or Hilbert-Schmidt norm) of matrix A is defined by

$$\|A\| = \sqrt{\operatorname{tr} AA^T} = \sqrt{\sum_{i=1}^{n} (a_{ii})^2}.$$

Theorem 5.6.2. *Similar matrices have the same trace and determinant.*

Proof. Assume A and B are similar, then there exists an invertible matrix S such that $A = SBS^{-1}$.

(1) $\operatorname{tr} A = \operatorname{tr} SBS^{-1} = \operatorname{tr} SS^{-1}B = \operatorname{tr} B$.

(2) $\det A = \det SBS^{-1} = \det S \cdot \det B \cdot \det S^{-1} = \det I \cdot \det B = \det B$.

$\square$

Remark 5.6.1. *Let A, B, C, D be $n \times n$ matrices, in general, the following equations do not hold*

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det A \det D - \det C \det B$$
$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB).$$

Theorem 5.6.3. *Let A, B, C, D be $n \times n$ matrices and $AC = CA$, then*

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB).$$

Proof.

(1) If $\det A \neq 0$, then we have

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & -A^{-1}B \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & D - CA^{-1}B \end{pmatrix}.$$

Thus, we can have

$$\begin{aligned} \det \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \det A \det\big(D - CA^{-1}B\big) \\ &= \det\big(AD - ACA^{-1}B\big) \\ &= \det\big(AD - CAA^{-1}B\big) \\ &= \det(AD - CB). \end{aligned}$$

(2) If A is singular, then there exists $\varepsilon \to 0$, such that, $\det A_k = \det(A + \varepsilon I) \neq 0$. Thus, we have $A_k C = CA_k$ and then

$$\det \begin{pmatrix} A_k & B \\ C & D \end{pmatrix} = \det(A_k D - CB) \overset{k \to \infty}{=} \det(AD - CB).$$

$\square$

Remark 5.6.2. *Similar to the theorem above, we can have following results, that:*

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{cases} \det(AD - BC), \text{ if } CD = DC; \\ \det(DA - CB), \text{ if } AB = BA; \\ \det(DA - BC), \text{ if } BD = DB; \\ \det(AD - CB), \text{ if } AC = CA. \end{cases}$$

Theorem 5.6.4. *Let A, B be $n \times n$ matrices, then* $\det(I - AB) = \det(I - BA)$.

Proof.

(1) If $\det A \neq 0$, then we have

$$\begin{aligned} \det(I - AB) &= \det A \left(A^{-1} - B\right) \\ &= \det A \det \left(A^{-1} - B\right) \\ &= \det \left(A^{-1} - B\right) \det A \\ &= \det \left(A^{-1} - B\right) A \\ &= (I - BA)\,. \end{aligned}$$

(2) If $\det A = 0$, then we can approximate $A_k = A + \varepsilon I$ such that $\det A_k \neq 0$ and let $\varepsilon \to 0$.

□

Remark 5.6.3. *In general,* $\det(A - BC) \neq \det(A - CB)$.

5.7 Complex Matrix

Let $T \in \mathscr{L}(X, X)$, where X is a complex linear space and $\dim X = n$. With chosen basis of X, T can be represented by a matrix A. For a complex $n \times n$ matrix $A = (a_1, \cdots, a_n)$, we have $\det A = D(a_1, \cdots, a_n)$.

Remark 5.7.1. *In general,* $\det(A + iB) \neq \det A + i \det B$, *for A, B being real matrices.*

Theorem 5.7.1. *Let A, B be real matrices. Then A, B are similar as real matrices is equivalent to that they are similar as complex matrices, i.e., $A \overset{R}{\sim} B \iff A \overset{C}{\sim} B$.*

Proof.

(1) ($\Rightarrow$) This is trivial.

(2) ($\Leftarrow$) If $A \overset{C}{\sim} B$, then there exists a matrix $M = P + iQ$, where P, Q are real matrices, such that $B = MAM^{-1}$. Then we have

$$
\begin{aligned}
& BM = MA \\
\Rightarrow\ & B(P + iQ) = (P + iQ)A \\
\Rightarrow\ & BP + iBQ = PA + iQA
\end{aligned}
$$

which implies $BP = PA$ and $BQ = QA$. If either P, Q are nonsingular, then we have $A \overset{R}{\sim} B$.

Consider $M_t = P + tQ$, where t can be real or complex. Then $\det(P + tQ)$ is a polynomial in t. And $\det M_i \neq 0$, then there exists $t \in \mathbb{R}$ such that $\det(P + tQ) \neq 0$. Since $BM_t = M_t A$, then $B = M_t A M_t^{-1}$. Thus, $A \overset{R}{\sim} B$.

$\square$

Next we discuss the determinant of some special matrices.

Example 5.7.1 (Vandermonde matrix)**.** Let $n \geq 2$, and $a_1, \cdots, a_n$ are scalars, $n \times n$ Vandermonde matrix is defined as following

$$
V(a_1, \cdots, a_n) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 \cdots & a_n & \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}
$$

Then, $\det V(a_1, \cdots, a_n) = \prod_{i<j}(a_j - a_i)$.

Example 5.7.2 (Cauchy matrix)**.** Given $2n$ numbers, $a_k, b_k, 1 \leq k \leq n$, such that $a_i + b_i \neq 0$ for all i, j. The Cauchy matrix is defined as following

$$
C(a_1, \cdots, a_n, b_1, \cdots, b_n) = \left(\frac{1}{a_i + b_j}\right)_{n \times n}
$$

where $c_{ij} = \frac{1}{a_i + b_j}$. Then, the determinant of C is

$$
\det C = \frac{\prod_{j>i}(a_j - a_i) \prod_{j>i}(b_j - b_i)}{\prod_{i,j}(a_i + b_j)}.
$$

5.8 Exercises

Exercise 5.8.1. *Let A, B, C be $n \times n$ matrices satisfying $AB = BA$. Show that*

$$\det(A + BC) = \det(A + CB).$$

Proof.

(1) If B is invertible, since $AB = BA$, then we have $A = B^{-1}AB$. Then we have

$$\begin{aligned}\det(A + BC) &= \det\Big(B^{-1}(A + BC)B\Big)\\ &= \det\Big(B^{-1}AB + CB\Big)\\ &= \det(A + CB).\end{aligned}$$

(2) If B is not invertible. We can set a new matrix $M = \begin{pmatrix} C & -I \\ A & B \end{pmatrix}$, and we can solve for the determinant of this matrix. Since $AB = BA$, then $\det(M) = \det(CB - (-I)A) = \det(CB + A)$. Also, we have $-IB = B(-I)$, then the determinant can be presented as $\det(M) = \det(BC - (-I)A) = \det(BC + A)$. Then we have $\det(A + BC) = \det(A + CB)$.

□

Remark 5.8.1. *In (2), we used if $AB = BC$, then $\det(M) = \det(CB - (-I)A)$. We should give proper proof to this. Suppose matrix $M = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$ and we have $RS = SR$. Then, if S is invertible, we have*

$$\begin{aligned}\det\begin{pmatrix} P & Q \\ R & S \end{pmatrix} &= \det\begin{pmatrix} P - RS^{-1}Q & 0 \\ R & S \end{pmatrix}\\ &= \det\Big(PS - RS^{-1}QS\Big)\\ &= \det\Big(PS - RSS^{-1}Q\Big)\\ &= \det(PS - RQ)\end{aligned}$$

If S is not invertibe, then there exists $\varepsilon_k \to 0$ such that $\det S_k = \det(B + \varepsilon_k I) \neq 0$ and $S_kR = RS_k$. Then $\det\begin{pmatrix} P & Q \\ R & S_k \end{pmatrix} = \det(PS_k - QR)$. Taking $k \to \infty$ will prove this case. The proof is complete. Similarly, we can prove that if $QS = SQ$, then $\det M = \det(SP - QR)$.

Exercise 5.8.2. *Let A, B, C be $n \times n$ matrices. Is it always true that*

$$\det(A + BC) = \det(A + CB)?$$

Prove or find a counter example.

Proof. In general, it is not true. Take $A = \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$ and $C = \begin{pmatrix} 0 & 1 \\ 1 & 6 \end{pmatrix}$. Then we have $\det(A + BC) = 76$ and $\det(A + CB) = 85$. $\square$

Exercise 5.8.3. *Let $n \geq 2$. Given $(2n-1)$ scalars $x_1, \cdots, x_{n-1}$ and $y_1, \cdots, y_n$, we can define an $n \times n$ matrix $A = (a_{ij})$ such that*

$$a_{ij} = x_j \text{ if } i > j,$$
$$a_{ij} = y_j \text{ if } i \leq j.$$

Show that

$$\det A = y_n \prod_{k=1}^{n-1} (y_k - x_k).$$

Proof. We can know that A has the form

$$A = \begin{pmatrix} y_1 & y_2 & y_3 & \cdots & y_n \\ x_1 & y_2 & y_3 & \cdots & y_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & x_3 & \cdots & y_n \end{pmatrix}$$

We can do elementary row operations that starting from the first row, and then apply $\text{row}_i = \text{row}_i + (-1)\text{row}_{i+1}$. Then we get new matrix

$$A = \begin{pmatrix} y_1 - x_1 & 0 & 0 & \cdots & 0 \\ 0 & y_2 - x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & x_3 & \cdots & y_n \end{pmatrix}$$

Then it is obvious that $\det(A) = y_n \prod_{k=1}^{n-1}(y_k - x_k)$. $\square$

Chapter 6

Spectral Theory

6.1 Eigenvalues and Eigenvectors

Definition 6.1.1. *Let A be an $n \times n$ matrix. Suppose that for a nonzero vector v and a scalar number λ, such that*

$$Av = \lambda v$$

then λ is called an eigenvalue of A and v an eigenvector of A corresponding to λ.

Let v be an eigenvector of A corresponding to λ, we have, for any positive integer k,

$$A^k v = \lambda^k v.$$

and more generally, for any polynomial p, we have

$$p(A)v = p(\lambda)v.$$

Theorem 6.1.1. *λ is an eigenvalue of A if and only if $\det(\lambda I - A) = 0$. The polynomial*

$$p_A(\lambda) = \det(\lambda I - A)$$

is called the characteristic polynomial of A.

Theorem 6.1.2. *Eigenvectors of a matrix A corresponding to distinct eigenvalues are linearly independent.*

Proof. Let $\lambda_k, 1 \leq k \leq n$ be n distinct eigenvalues and $v_k, 1 \leq k \leq n$ be corresponding eigenvectors. Now we prove it by induction.

(1) When $k = 1$, the theorem holds.

(2) Suppose it holds for $k = N$. When $k = N + 1$, suppose

$$\sum_{k=1}^{N+1} c_k v_k = 0,$$

then we have

$$\sum_{k=1}^{N+1} c_k \lambda_{N+1} v_k = 0.$$

Applying A to both sides of the first equation above, then we have

$$\begin{aligned}
&\sum_{k=1}^{N+1} c_k \lambda_k v_k = 0 = \sum_{k=1}^{N+1} c_k \lambda_{N+1} v_k \\
\Rightarrow &\sum_{k=1}^{N+1} c_k (\lambda_k - \lambda_{N+1}) v_k = 0 \\
\Rightarrow &c_k (\lambda_k - \lambda_{N+1}) = 0
\end{aligned}$$

and since $c_k = 0, 1 \leq k \leq n$, we have $c_{N+1} = 0$. Thus, the theorem holds for $N + 1$.

□

Corollary 6.1.1. *If the characteristic polynomial p_A of an $n \times n$ matrix A has n distinct roots, then A has a basis formed by n linearly independent eigenvectors.*

Corollary 6.1.2. *If A has n distinct eigenvalues, then A is diagonalizable in the sense that A is similar to a diagonal matrix.*

Proof. Let $\lambda_k, 1 \leq k \leq n$ be n distinct eigenvalues of A, with corresponding eigenvectors $v_k, 1 \leq k \leq n$ such that $Av_k = \lambda_k v_k, 1 \leq k \leq n$. Let $S = (v_1, v_2, \cdots, v_n)$, then we have

$$AS = S \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}$$

which implies $A = S\Lambda S^{-1}$. □

Theorem 6.1.3. *Let $\lambda_k, 1 \leq k \leq n$ be eigenvalues of A, with the same multiplicity they have as roots of the characteristic equation of A. Then*

$$\det A = \sum_{k=1}^{n} \lambda_k \text{ and } \operatorname{tr} A = \sum_{k=1}^{n} \lambda_k.$$

Proof. We claim that $\lambda_1, \lambda_n, \cdots, \lambda_n$ are n roots of polynomial, which has the following form

$$\begin{aligned} p_A(\lambda) &= \det(\lambda I - A) \\ &= \sum_p \sigma(p) \prod_{k=1}^{n} (\lambda \delta_{p_k k} - a_{p_k k}) \\ &= \lambda^n - (\operatorname{tr} A)\, \lambda^{n-1} + \cdots + (-1)^n \prod_{k=1}^{n} \lambda_k. \end{aligned}$$

Then we have

(1) Let $\lambda = 0$, then we have $\det(-A) = (-1)^n \prod_{k=1}^{n} \lambda_k$, which implies $\det A = \prod_{k=1}^{n} \lambda_k$.

(2) According to elementary algebra, the polynomial p_A can be written as

$$p_A = \prod_{k=1}^{n} (\lambda - \lambda_k)$$

which implies the coefficient of λ^{n-1} is $-\sum_{k=1}^{n} \lambda_k$. Thus, we have $\operatorname{tr} A = \sum_{k=1}^{n} \lambda_k$.

□

6.2 Spectral Mapping Theorem

Theorem 6.2.1 (Spectral Mapping Theorem)**.**

(a) Let q be any polynomial, A a square matrix, λ an eigenvalue of A. Then $q(\lambda)$ is an eigenvalue of $q(A)$.

(b) Every eigenvalue of $q(A)$ is of the form $q(\lambda)$, where λ is an eigenvalue of A.

Proof.

(a) We have $Av = \lambda v$, which implies $q(A)v = q(\lambda)v$. Indeed, we have

$$q(A) = \sum_{k=0}^{m} c_k A^k \Rightarrow q(A)v = \sum_{k=0}^{m} c_k \lambda^k v = q(\lambda)v.$$

(b) Let μ be an eigenvalue of $q(A)$, then we have $\det(\mu I - q(A)) = 0$. Suppose

$$q(\lambda) - \mu = c \prod_{i=1}^{m} (\lambda - \lambda_i),$$

then substituting by A, we have

$$\prod_{i=1}^{m} \det(\lambda_i I - A) = 0.$$

Thus, for some λ_i, $\det(\lambda_i I - A) = 0$, which implies $\mu = q(\lambda_i)$, where λ_i is an eigenvalue of A.

$\square$

Remark 6.2.1. *Let $p_A = \det(\lambda I - A)$, then every eigenvalue of $p_A(A)$ is zero.*

Theorem 6.2.2 (Cayley-Hamilton)**.** *Every matrix A satisfies its own characteristic equation, i.e.,*

$$p_A(A) = 0.$$

Proof. Let $Q(s) = sI - A$ and $P(s)$ defined as the matrix of cofactors of $Q(s)$, i.e.,

$$P_{ij}(s) = (-1)^{i+j} D_{ji}(s)$$

where $D_{ij}(s)$ is the determinant of (j,i)th minor of $Q(s)$. Then we have

$$P(s)Q(s) = \det(Q(s))I = p_A(s)I.$$

Since the coefficients of Q commutes with A, we have

$$P(A)Q(A) = p_A(A)I = 0$$

hence, $p_A(A) = 0$. $\square$

Lemma 6.2.3. *Let $P(s), Q(s)$ and $R(s)$ be polynomials in s with $n \times n$ matrices P_k, Q_k, R_s as coefficients. Suppose*

$$P(s) = \sum P_k s^k, Q(s) = \sum Q_k s^k, R(s) = \sum R_k s^k$$

and

$$P(s)Q(s) = R(s).$$

Also, A commutes wit each Q_k, then we have

$$P(A)Q(A) = R(A).$$

Proof. Since $P(s)Q(s) = R(s)$, we have

$$\sum P_k s^k \sum Q_k s^k = \sum R_k s^k$$

which implies

$$R_k = \sum_{i+j=k} P_i Q_j.$$

Then, substituting by A, we have

$$\begin{aligned} P(A)Q(A) &= \sum P_k A^k \sum Q_k A^k \\ &= \sum_{i,j} P_i A^i Q_j A^j \\ &= \sum_{i,j} P_i Q_j A^{i+j} \\ &= \sum_{i+j=k} P_i Q_j A^{i+j} = \sum R_k A^k = R(A). \end{aligned}$$

$\square$

6.3 Generalized Eigenvectors and Spectral Theorem

Definition 6.3.1. *A nonzero vector u is said to be a generalized eigenvector of A corresponding to eigenvalue λ if*

$$(A - \lambda I)^m u = 0$$

for some $m \in \mathbb{N}$.

Theorem 6.3.1 (Spectral Theorem)**.** *Every vector in $\mathbb{C}^n$ can be written as a sum of eigenvectors of A, genuine or generalized.*

Proof. Let x be any vector, then $p_A(A)x = 0$. We factor polynomial as

$$p_A(\lambda) = \prod_{j=1}^{J} (\lambda - \lambda_j)^{m_j}$$

where λ_j are distinct eigenvalues of A. Then we have

$$\begin{aligned} p_A(A) = \prod_{j=1}^{J} (A - \lambda_j)^{m_j} = 0 \\ \Rightarrow \prod_{j=1}^{J} (A - \lambda_j)^{m_j} x = 0. \end{aligned}$$

Let $p_j = (\lambda - \lambda_j)^{m_j}$, then $x \in N_{p_1(A)p_2(A)\cdots p_J(A)}$, i.e., x belongs to the null space of $p_1 p_2 \cdots p_J(A)$. We claim:

$$N_{p_1 p_2 \cdots p_J(A)} = \oplus_{i=1}^{J} N_{p_i(A)}.$$

If this is true, then $x = \sum_{i=1}^{J} x_i, x_i \in N_{p_j(A)}$. Then we need a lemma.

Lemma 6.3.2. *Let p, q be a pair of polynomials, with complex coefficients, and p, q have no common zeros. Then, we have*

(1) There exist two polynomials a, b, such that $ap + bq = 1$.

(2) Let A be a square matrix, then

$$N_{p(A)q(A)} = N_{p(A)} \oplus N_{q(A)}.$$

(3) Let $P_k k = 1, \cdots, m$ be polynomials and they have no common zeros, then

$$N_{p_1(A)\cdots p_m(A)} = N_{p_1(A)} \oplus \cdots \oplus N_{p_m(A)}.$$

Proof.

(1) Let $\mathcal{P} = \{ap+bq\}$, where a, b are two polynomials, and let d be a nonzero polynomial in P with lowest degree.

First, we claim that d divides both p and q.Indeed, if not, then the division algorithm yields a remainder, i.e.,

$$r = p - md.$$

where the degree of r is less than that of d. Since p and d belong to $\mathcal{P}$, then $r \in \mathcal{P}$, which is a contradiction.

Second, we claim that d has degree zero. Suppose not, then by the fundamental theorem of algebra, d would have a root. Since d divides p and q, and p and q have no common zeros, d is a nonzero constant. Thus, $1 \in \mathcal{P}$.

(2) From (1), there are two polynomials a and b such that

$$a(A)p(A) + b(A)q(A) = I.$$

For any x, we have

$$x = a(A)p(A)x + b(A)q(A)x \triangleq x_1 + x_2$$

and it is easy to see that if $x \in N_{p(A)q(A)}$, then $x \in N_{p(A)}$ and $x \in N_{q(A)}$. Also, suppose $x \in N_{p(A)} \cap N_{q(A)}$, the above equation implies

$$x = a(A)p(A)x + b(A)q(A)x = 0,$$

Hence, $N_{p(A)q(A)} = N_{p(A)} \oplus N_{q(A)}$.

(3) The third argument follows naturally.

$\square$

Now the proof of the theorem is completed. $\square$

6.4 Minimal Polynomial

We denote by $\mathcal{P}_A$ the set of all polynomials such that $p(A) = 0$. It is obvious $\mathcal{P}_A$ forms a linear space. Denote by $m = m_A$ a polynomial of smallest degree in $\mathcal{P}_A$, and we normalized m to have coefficient 1 at its highest degree.

Now we claim that any $p \in \mathcal{P}_A$ is a multiple of m. Indeed, we can write $p = qm + r$, where the degree of r is less that that of m. Then we have

$$r(A) = p(A) - q(A)m(A) = 0$$

then $r \in \mathcal{P}_A$, hence, $r = 0$, which proved the argument. And this polynomial m is called the *minimal polynomial* of A.

Now we consider generalized eigenvector. We denote by $N_m = N_m(\lambda)$ the null space of $(A - \lambda I)^m$. The subspaces N_m, consist of generalized eigenvectors; they are indexed increasingly, i.e.,

$$N_1 \subset N_2 \subset N_3 \subset \cdots \subset \mathbb{C}^n.$$

We denote by $d = d(\lambda)$ the smallest index such that

$$\begin{aligned} &N_d = N_{d+k}, k \geq 1 \\ &N_d \neq N_{d-1} \end{aligned}$$

and d is called the *index* of the eigenvalue λ.

Remark 6.4.1. *A maps N_d into itself, i.e., N_d is an invariant subspace under the matrix A.*

Proof. If $v \in N_d$, then $(A - \lambda I)^d v = 0$. Then, we have $(A - \lambda I)^d Av = A(A - \lambda I)^d v = 0$. Thus, $Av \in N_d$. □

Theorem 6.4.1. *Let $\lambda_1, \cdots, \lambda_k$ be distinct eigenvalues of A, whose index is $d(\lambda_j) = d_j, 1 \leq j \leq k$. Then,*

(1) $\mathbb{C}^n = \oplus_{j=1}^k N_{d_j}(\lambda_j)$.

(2) The minimal polynomial is $m_A = \prod_{j=1}^k (\lambda - \lambda_j)^{d_j}$.

Proof.

(1) $\mathbb{C}^n$ is the span of generalized eigenvectors and others follows from spectral theorem.

(2) For any $x \in \mathbb{C}^n$, we have $x = \sum_{j=1}^k x_j, x_j \in N_{d_j}(\lambda_j)$. Then, we have

$$\prod_{j=1}^k (A - \lambda_j I)^{d_j} x = \sum_{j=1}^k \left(\prod_{j=1}^k (A - \lambda_j I)^{d_j} \right) x_j = 0$$

Hence, we have

$$\prod_{j=1}^k (A - \lambda_j I)^{d_j} = 0.$$

Thus, we have $m(\lambda) = \prod_{j=1}^k (\lambda - \lambda_j I)^{d_j} = 0$. Since $m(A) = 0$, then $m \in \mathcal{P}_A$. Then we can have that m is a multiple of m_A. Suppose $m_A = \prod_{j=1}^k (\lambda - \lambda_j I)^{e_j}, e_j \leq d_j$. Then, we have

$$\mathbb{C}^n = N_{m_A(A)} = \oplus_{j=1}^k N_{(A-\lambda_j I)^{e_j}} = \oplus_{j=1}^k N_{(A-\lambda_j I)^{d_j}}$$

which implies $e_j = d_j, 1 \leq j \leq k$.

$\square$

Theorem 6.4.2. *Suppose A and B similar, then A, B has the same distinct eigenvalues $\lambda_1, \cdots, \lambda_k$. Furthermore, the null space $N_{(A-\lambda_j I)^m}$ and $N_{(B-\lambda_j I)^m}$ has the same dimension for $1 \le j \le k, m \ge 1$.*

Proof. Since A and B similar, then there exists nonsingular S such that $A = SBS^{-1}$. Then we have

$$(A - \lambda I)^m = S(A - \lambda I)^m S^{-1}.$$

If $v \in N_{(A-\lambda_j I)^m}$, then we have $S^{-1}v \in N_{(B-\lambda_j I)^m}$. Thus, $\dim N_{(A-\lambda_j I)^m} = \dim N_{(B-\lambda_j I)^m}$. $\square$

Remark 6.4.2.

(1) $A - \lambda I$ maps $N_{i+1}(\lambda)$ into $N_i(\lambda)$, where $N_j(\lambda) = N_{(A-\lambda I)^j}$.

(2) $A - \lambda I$ defines a map from N_{i+1}/N_i to N_i/N_{i-1}, for $i \ge 1$, and $N_0 = \{0\}$.

Proof. For all $x, y \in N_{i+1}$ and $x - y \in N_i$, we have $(A - \lambda I)x, (A - \lambda I)y \in N_i$ and $(A - \lambda I)x - (A - \lambda I)y \in N_{i-1}$. $\square$

Lemma 6.4.3. *The map*

$$A - \lambda I : N_{i+1}/N_i \to N_i/N_{i-1}$$

is one-to-one. Hence,

$$\dim N_{i+1}/N_i \le \dim N_i/N_{i-1}.$$

Proof. Let $B = A - \lambda I$, if $\left\{B\{x\}_{N_{i+1}/N_i}\right\}_{N_i/N_{i-1}} = \{0\}$, then $Bx \in N_{i-1}$, which implies $\{x\} \in N_i$ and $\{x\}_{N_{i+1}/N_i} = \{0\}_{N_{i+1}/N_i}$. Thus, $A - \lambda I$ is one-to-one. $\square$

6.5 Jordan Canonical Form

6.5.1 Proof of Jordan Canonical Form

We want to construct a basis for $N_{d_j}(\lambda_j)$. For simplicity, assume $\lambda_j = 0$ and $d_j = 0$. Also, we have $N_1 \subset N_2 \subset \cdots \subset N_d$, $A : N_{i+1} \to N_i, i \ge 1$ and $A : N_{i+1}/N_i \to N_i/N_{i-1}$. Now we preset how to construct Jordan Canonical form.

Step I: Let $l_0 = \dim(N_d/N_{d-1}) \ge 1$. Let $x_1, \cdots, x_{l_0}$ be vectors such that $\{x_1\}, \cdots \{x_{l_0}\} \in N_d$ form a basis of N_d/N_{d-1}.

Step II: Let $l_1 = \dim(N_{d-1}/N_{d-2}) \geq l_0$, then $\{Ax_1\}, \cdots, \{Ax_{l_0}\} \in N_{d-1}$ are linearly independent. If $l_1 > l_0$, we can pick $x_{l_0+1}, \cdots, x_{l_1}$ such that $\{Ax_1\}, \cdots, \{Ax_{l_0}\}, x_{l_0+1}, \cdots, x_{l_1}$ form a basis of N_{d-1}/N_{d-2}.

Step III: Continue this process until N_1. Let $l_{d-1} = \dim N_1$ and $A : N_2 \to N_1$ and add vectors $x_{l_{d-2}+1}, \cdots, x_{l_{d-1}}$, and the rest is the similar. We thus constructed a basis of N_d.

Step IV: We present the vectors in a list as below:

$$\begin{array}{ccccc}
x_1 & Ax_1 & \cdots & & A^{d-1}x_1 \\
\vdots & & & & \vdots \\
x_{l_0} & Ax_{l_0} & \cdots & & A^{d-1}x_{l_0} \\
x_{l_0+1} & Ax_{l_0+1} & \cdots & A^{d-2}x_{l_0+1} & \\
\vdots & & & & \\
x_{l_1} & Ax_{l_1} & \cdots & A^{d-2}x_{l_1} & \\
\vdots & & & & \\
x_{l_{d-2}+1} & & & & \\
\vdots & & & & \\
x_{l_{d-1}} & & & &
\end{array}$$

Also, we have

$$\begin{aligned}
\dim N_d &= \dim N_1 + \dim N_2/N_1 + \cdots + \dim N_d/N_{d-1} \\
&= l_{d-1} + l_{d-2} + \cdots + l_0.
\end{aligned}$$

and we claim that these vectors are linearly independent. Under this basis, we have

$$N_d = \oplus_{k=1}^{l_{d-1}} M_K$$

where M_k is the span of vectors in the kth row. Under the basis of M_k, A has the representation

$$J_m = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$$

which is called a *Jordan block* where $J_m(i,j) = 1$ for $j = i+1$ and $J_m(i,j) = 0$ otherwise.

Theorem 6.5.1. *Any matrix A is similar to its Jordan canonical form which consists diagonal blocks of the form*

$$J_m = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

where λ is the eigenvalue of A.

6.5.2 Another Proof

Now we present more details about Jordan canonical form from other materials[2]. We start from the beginning and consider nilpotent operator.

Example 6.5.1. Let $N \in \mathcal{L}(\mathbb{R}^4, \mathbb{R}^4)$ be the nilpotent operator defined by

$$N(x_1, x_2, x_3, x_4) = (0, x_1, x_2, x_3).$$

If $x = (1, 0, 0, 0)$, then $\{N^3x, N^2x, Nx, x\}$ is a basis for $\mathbb{R}^4$. We denote by M the matrix spanned by $\{N^3x, N^2x, Nx, x\}$. The matrix of N with respect to this basis is

$$J = M^{-1}NM = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Example 6.5.2. Let $N \in \mathcal{L}(\mathbb{R}^6, \mathbb{R}^6)$ be the nilpotent operator defined by

$$N(x_1, x_2, x_3, x_4, x_5, x_6) = (0, x_1, x_2, 0, x_4, 0).$$

and there does not exist a vector $x \in \mathbb{R}^6$ such that $\{N^5x, N^4x, N^3x, N^2x, Nx, x\}$ form a basis of $\mathbb{R}^6$. If we take $v_1 = (1, 0, 0, 0, 0, 0), v_2 = (0, 0, 0, 1, 0, 0)$ and $v_3 = (0, 0, 0, 0, 0, 1)$, then $\{N^2v_1, Nv_1, v_1, Nv_2, v_2, v_3\}$ form a basis of $\mathbb{R}^6$. The matrix of N with respect to this basis is

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

Next, we show that every nilpotent operator $N \in \mathcal{L}(X, X)$ behaves similarly to the examples above. Specifically, there is a finite collection of vectors $v_1, \cdots, v_n \in X$ such that there is a basis of X consisting of the vectors of the form $N^kv_j \in X$ where $1 \le j \le n$ and k varies from 0 to the largest nonnegative integer m_j such that $N^{m_j}v_j \neq 0$.

Theorem 6.5.2. *Suppose $N \in \mathcal{L}(X, X)$ is nilpotent. Then there exist vectors $v_1, \cdots, v_n \in X$ and nonnegative integers $m_1, \cdots, m_n$ such that*

(1) $N^{m_1}v_1, \cdots, Nv_1, v_1, \cdots, N^{m_n}v_n, \cdots, Nv_n, v_n$ is a basis of X.

(2) $N^{m_1+1}v_1 = N^{m_2+1}v_2 = \cdots = N^{m_n+1}v_n = 0$.

Proof. We prove by induction and the theorem obviously holds for $\dim X = 1$, since the only nilpotent operator is 0 and we can pick any nonzero vector as v_1 and $m_1 = 0$.

Because N is nilpotent, then N is not injective. Thus N is not surjective and hence R_N is a subspace of X, i.e., $\dim R_N \leq \dim X$. Thus we can apply the induction to the restriction operator $N|_{R_N} \in \mathcal{L}(R_N)$. We can ignore the case where $R_N = \{0\}$, since we can pick $v_1, \cdots, v_n$ be any basis and $m_1 = \cdots = m_n = 0$.

By induction applied to $N|_{R_N} \in \mathcal{L}(R_N)$, there exist $v_1, \cdots, v_n \in R_N$ and $m_1, \cdots, m_n$ such that

$$N^{m_1}v_1, \cdots, Nv_1, v_1, \cdots, N^{m_n}v_n, \cdots, Nv_n, v_n \tag{6.5.2.1}$$

is a basis of R_N and

$$N^{m_1+1}v_1 = N^{m_2+1}v_2 = \cdots = N^{m_n+1}v_n = 0.$$

Since $v_j \in R_N, 1 \leq j \leq n$, then for any j, there exists a $u_j \in X$ such that $v_j = Nu_j$. Then $N^{k+1}u_j = N^k v_j$ for each j and each nonnegative integer k.

We claim

$$N^{m_1+1}u_1, \cdots, Nu_1, u_1, \cdots, N^{m_n+1}u_n, \cdots, Nu_n, u_n \tag{6.5.2.2}$$

is linearly independent in X. Indeed, suppose

$$\sum_{j=1}^{n} \sum_{i=0}^{m_j+1} N^i u_j = 0$$

then we apply N to both sides and we have

$$\sum_{j=1}^{n} \sum_{i=0}^{m_j+1} c_{ij} N^{i+1} u_j = \sum_{j=1}^{n} \sum_{i=0}^{m_j+1} c_{ij} N^i v_j = 0$$

which implies $c_{ij} = 0$ for all i, j.

Now we extend (6.5.2.2) into a basis

$$N^{m_1+1}u_1, \cdots, Nu_1, u_1, \cdots, N^{m_n+1}u_n, \cdots, Nu_n, u_n, w_1, \cdots, w_p \tag{6.5.2.3}$$

of X. Also, each Nw_j is in the range of N and hence Nw_j is in the span of (6.5.2.1), and for each $1 \leq j \leq p$, there exists x_j in the span of (6.5.2.2) such that $Nx_j = Nw_j$. And we define

$$u_{n+j} = w_j - x_j$$

then we have $Nu_{n+j} = 0$. Furthermore,

$$N^{m_1+1}u_1, \cdots, Nu_1, u_1, \cdots, N^{m_n+1}u_n, \cdots, Nu_n, u_n, u_{n+1}, \cdots, u_{n+p} \tag{6.5.2.4}$$

form a basis of X since its span contains $w_j, 1 \leq j \leq p$. This basis has the required form, completing the proof. $\square$

Definition 6.5.1. *Suppose $T \in \mathcal{L}(X,X)$. A basis of X is called a Jordan basis for T if, with respect to this basis, T has a block diagonal representation*

$$T = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_p \end{pmatrix},$$

where each A_j is an upper-triangular matrix of the form

$$A_j = \begin{pmatrix} \lambda_j & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_j \end{pmatrix}.$$

and λ_j is an eigenvalue of T.

Theorem 6.5.3. *Suppose X is a complex vector space. If $T \in \mathcal{L}(X,X)$, then there exists a basis of X which is a Jordan basis for T.*

Proof. First consider a nilpotent operator $N\mathcal{L}(X,X)$ and the vector $v_1, \cdots, v_n \in X$ given by previous theorem. For each j, N maps the first vector in the list $\{N^{m_j}v_j, \cdots, Nv_j, v_j\}$ to 0 and each vector other than $N^{m_j}v_j$ to the previous one. Then, the previous theorem gives a basis of X with respect to which, N has a block diagonal matrix, where each one has the form

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

Thus, the theorem holds for nilpotent operators.

Now suppose $T \in \mathcal{L}(X,X)$, and let $\lambda_1, \cdots, \lambda_m$ be distinct eigenvalues of T. Then we have the generalized eigenspace decompisition

$$X = G(\lambda_1, T) \oplus \cdots \oplus G(\lambda_m, T)$$

where each $(T - \lambda_j I)|_{G(\lambda_j,T)}$ is nilpotent. Thus, some basis of each $G(\lambda_j, T)$ is a Jordan basis for $(T - \lambda_j I)|_{G(\lambda_j,T)}$. Putting these bases together gives a basis of X that is a Jordan basis for T. $\square$

Example 6.5.3. Consider

$$A = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 4 & -1 \\ -4 & 13 & -3 \end{pmatrix}.$$

The characteristic polynomial of A is

$$\lambda(\lambda-1)^2$$

and the generalized eigenspace corresponding to 0 is just the ordinary eigenspace, so there will be only one single Jordan block corresponding to 0 in the Jordan form of A. Moreover, this block has size 1 since 1 is the exponent of λ in the characteristic (and hence in the minimal polynomial as well) polynomial of A.

Now we determine the dimension of the eigenspace corresponding to $\lambda = 1$, which is the dimension of the null space of

$$A - I = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 3 & -1 \\ -4 & 13 & -4 \end{pmatrix}.$$

and row-reducing gives

$$\begin{pmatrix} 0 & -1 & 0 \\ -1 & 3 & -1 \\ -4 & 13 & -4 \end{pmatrix} \to \begin{pmatrix} -1 & 3 & -1 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Thus, the dimension of the eigenspace corresponding to $\lambda = 1$ is 1, since the null space is of dimension 1, implying that there is only one Jordan block corresponding to 1 in the Jordan form of A. Thus, the Jordan form of A is

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

Example 6.5.4. Consider

$$A = \begin{pmatrix} 5 & -1 & 0 & 0 \\ 9 & -1 & 0 & 0 \\ 0 & 0 & 7 & -2 \\ 0 & 0 & 12 & -3 \end{pmatrix}.$$

The characteristic polynomial of A is

$$(\lambda-2)^2(\lambda-3)(\lambda-1)$$

From the multiplicities, the generalized eigenspaces corresponding to $\lambda = 3$ and $\lambda = 1$ are the ordinary eigenspaces, so each of these give blocks of size 1 in the Jordan form.

The eigenspace corresponding to $\lambda = 2$ is the null space of

$$A - 2I = \begin{pmatrix} 3 & -1 & 0 & 0 \\ 9 & -3 & 0 & 0 \\ 0 & 0 & 5 & -2 \\ 0 & 0 & 12 & -5 \end{pmatrix}$$

and row-reducing gives

$$\begin{pmatrix} 3 & -1 & 0 & 0 \\ 9 & -3 & 0 & 0 \\ 0 & 0 & 5 & -2 \\ 0 & 0 & 12 & -5 \end{pmatrix} \to \begin{pmatrix} 3 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & -2 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Thus, the eigenspace is of dimension 1, which implies there is only one Jordan block in the Jordan form of A, with size 2×2. Hence, the Jordan form of A is

$$J = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Next, we find the *Jordan basis* which puts A into its Jordan form. Recall that this should be a basis consisting of *Jordan chains*. For the block of size 1, the chain will be of length 1 and consists of exactly one eigenvector for the corresponding eigenvalue. For $\lambda = 3$ and $\lambda = 1$, the corresponding eigenvectors are

$$\begin{pmatrix} 0 \\ 0 \\ -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 3 \end{pmatrix}.$$

Then we can find a eigenvector for $\lambda = 2$, which is

$$v_1 = \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix}$$

and we need to find the final vector in the Jordan chain for $\lambda = 2$. And the Jordan chain has the form of $(v, (A - 2I)v)$. Then we can pick

$$\begin{pmatrix} 3 & -1 & 0 & 0 \\ 9 & -3 & 0 & 0 \\ 0 & 0 & 5 & -2 \\ 0 & 0 & 12 & -5 \end{pmatrix} v = \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix}$$

which implies

$$v = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}.$$

Thus, the Jordan basis corresponding to A is

$$\begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 3 \end{pmatrix}.$$

Example 6.5.5. Consider

$$A = \begin{pmatrix} 1 & -1 & -2 & 3 \\ 0 & 0 & -2 & 3 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

The characteristic polynomial of A is

$$(\lambda - 1)^4$$

and we need to determine the dimension of the eigenspace corresponding to 1. And, $A - I$ can reduce as following

$$\begin{pmatrix} 0 & -1 & -2 & 3 \\ 0 & -1 & -2 & 3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & -2 & 3 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which implies there are two Jordan blocks corresponding to 1 in the Jordan form of A. Then, there are two possibilities:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

with corresponding minimal polynomial $(\lambda - 1)^2$ or $(\lambda - 1)^3$.

To determine which it is, we need to determine the length of the Jordan chains. We start with ordinary eigenvectors

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

and each will give a Jordan chain. Consider v such that

$$(A - I)v = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

and we cannot find a solution for v, which implies this eigenvector is its own Jordan chain. Now we consider w such that

$$(A - I)w = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

and it gives us

$$w = \begin{pmatrix} 1 \\ 1 \\ -1 \\ 0 \end{pmatrix}.$$

Then we try to find u such that

$$(A - I)u = \begin{pmatrix} 1 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

and it gives us

$$u = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}.$$

Thus, we can find a Jordan chain of length 3:

$$(u, (A-I)u, (A-I)^2 u) = \left(\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right).$$

Thus, the Jordan form of A is

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

6.6 Commuting Maps

Lemma 6.6.1. *If A, B have same eigenvalues $\{\lambda_j\}$ and if for each λ_j, we have*

$$\dim N_m(\lambda_j) = \dim M_m(\lambda_j),$$

where $N_m(\lambda_j) = N_{(A-\lambda_j I)^m}$ and $M_m(\lambda_j) = N_{(B-\lambda_j I)^m}$, then A, B are similar.

Proof. By the construction of Jordan canonical form. □

Remark 6.6.1. *The inverse of this lemma is also true.*

Theorem 6.6.2. *Suppose A, B are $n \times n$ matrices, such that $AB = BA$, then there is a basis of $\mathbb{C}^n$ which consists of eigenvectors and generalized eigenvectors of both A and B.*

Proof. Let $\{\lambda_j\}_{j=1}^K$ be K distinct eigenvalues of A, then

$$\mathbb{C}^n = \oplus_{j=1}^K N_j$$

where $N_j = N_{(A-\lambda_j I)^{d(\lambda_j)}}$. For any $x \in \mathbb{C}^n$, since $AB = BA$, then we have

$$(A - \lambda_j I)^{d(\lambda_j)} Bx = B(A - \lambda_j I)^{d(\lambda_j)} x.$$

If $x \in N_j$, then $(A - \lambda_j I)^{d(\lambda_j)} x = 0$, which implies $Bx \in N_j$. Then, B is a map from N_j into N_j. Applying Spectral theorem (6.3.1) to $B|_{N_j}$, then we obtain a spectral decomposition of each N_j, i.e., N_j has a basis consisting of eigenvectors and generalized eigenvectors of B. Thus, we obtain a basis of $\mathbb{C}^n$. □

Remark 6.6.2. *If A, B are both diagonalizable and $AB = BA$, then A, B can be diagonalized at the same time, i.e., there exists nonsingular matrix S such that $S^{-1}AS$ and $S^{-1}BS$ are both diagonal.*

Theorem 6.6.3. *Every square matrix A is similar to its transpose A^T.*

Proof. Since $\dim N_A = \dim N_{A^T}$, then $\dim N_{(A-\lambda I)^m} = \dim N_{(A^T-\lambda I)^m}$. Then, A and A^T have the same Jordan canonical form. Thus, A and A^T are similar. □

Theorem 6.6.4. *Let λ, μ be distinct eigenvalues of A. Suppose u is an eigenvector with respect to λ and v is an eigenvector with respect to μ, i.e., $Au = \lambda u, Av = \mu v$. Then $u^T v = 0$.*

Proof. We have

$$\begin{aligned} v^T A u &= u^T A^T v \\ \Rightarrow \lambda v^T u &= \mu u^T v. \end{aligned}$$

Since $\lambda \neq \mu$, we have $u^T v = 0$. □

6.7 Exercises

Exercise 6.7.1. *Let A be an invertible $n \times n$ matrix, show that there exists a polynomial g such that*

$$A^{-1} = g(A).$$

Proof. Since A is invertible, then A has no zero engenvalues. Thus, the characteristic polynomial $P(x)$ for A has constant terms, which can be written as $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Also, we know that $P(A) = 0$, thus we have

$$\begin{aligned} &A^n + a_{n-1}A^{n-1} + \cdots + a_0 = 0 \\ \Rightarrow &A^{-1} = -\frac{1}{a_0}(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1) = g(A) \end{aligned}$$

Then $A^{-1} = g(A)$, the proof is complete. □

Exercise 6.7.2. *Let*

$$A = \begin{pmatrix} A_1 & \\ & A_2 \end{pmatrix}.$$

Show that the minimal polynomial m_A is the least common multiple of m_{A_1} and m_{A_2}.

Proof. From the form of A, we can know that $\det(\lambda - IA) = \det(\lambda - IA_1)\det(\lambda - IA_1)$. Then, for any polynomial $T(x)$ such that $T(A) = 0$, then we have $T(A_1) = 0$ and $T(A_2) = 0$. And since m_A, m_{A_1} and m_{A_2} are minimal polynomials corresponding to A, A_1 and A_2, then we have $T(x) = m_1 m_{A_1}(x)$ and $T(x) = m_2 m_{A_1}(x)$ for some m_1, m_2. Also, we have $m_A(x)|T(x)$, then we have $m_{A_1}(x)|m_A(x)$ and $m_{A_1}(x)|m_A(x)$, then m_A is the least common multiple of m_{A_1} and m_{A_2}. □

Exercise 6.7.3. *Find the minimal polynomial m_A for*

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Proof. The characteristic polynomial for A is that $P(\lambda) = (\lambda - 1)(\lambda - 2)^2$. Then the minimal polynomial is $m_A = (\lambda - 1)(\lambda - 2)$. □

Exercise 6.7.4. *Let A be an $n \times n$ matrix where $n \geq 2$ satisfying* $\operatorname{rank} A = 1$.

(1) Show that there exists two column vectors a, b such that $A = ab^T$.

(2) Show that the minimal polynomial

$$m_A = \lambda^2 - \left(a^T b\right)\lambda.$$

Proof.

(1) Since rank$A = 1$, then the image of A is one-dimensional. Thus, there exist $u, v \in \mathbb{R}^n$ such that $Au = kv$ for a fixed v. It also holds for a basis for $\mathbb{R}^n$, then every column of A is a multiple of v. Then there exists $(w_1, w_2, \cdots, w_n) \in \mathbb{R}^n$, such that

$$A = v(w_1, w_2, \cdots, w_n)$$

then we denote $v = a$, and $(w_1, w_2, \cdots, w_n) = b^T$, where $a, b \in \mathbb{R}^n$.Then $A = ab^T$.

(2) We have $A^2 = ab^T ab^T = a(b^T a)b^T = (b^T a)ab^T = (b^T a)A$, which implies $q(A) = A^2 - (b^T a)A = 0$. This polynomial satisfies that $q(A) = 0$, then $m_a | q(\lambda) = \lambda^2 - (b^T a)\lambda$. Also, m_A cannot be λ or $\lambda - (b^T a)$, since this means A is a scalar. Thus, $m_A = \lambda^2 - (b^T a)\lambda$. The proof is complete.

□

Exercise 6.7.5. *Let A_k, $1 \leq k \leq K$ be $n \times n$ matrices satisfying*

$$A_i A_j = A_j A_i \textit{ for any } 1 \leq i, j \leq k.$$

Show the existence of a basis of $\mathbb{C}^n$ which consists of eigenvector and generalized eigenvectors of A_k for each $1 \leq k \leq K$.

Proof. Let $\{\lambda_j\}_{j=1}^J$ be J distinct eigenvalues of A_1, and then we have

$$\mathbb{C}^n = \bigoplus_{j=1}^J N_j$$

where $N_j = N_{(A_1 - \lambda_j I)^{d_j}}$, d_j is index of jth eigenvalue λ_j. For $\forall x \in \mathbb{C}^n$, since $A_1 A_i = A_i A_1, 2 \leq i \leq K$, then we have $(A_1 - \lambda_j I)^{d_j} A_i = A_i (A_1 - \lambda_j I)^{d_j}$. Thus, if $x \in N_k$

$$(A_1 - \lambda_j I)^{d_j} A_i x = A_i (A_1 - \lambda_j I)^{d_j} x = 0$$

which means $A_i x \in N_j$. Thus, A_i is a mapping from N_j to N_j. Now we apply Spectral Theorem to the linear mapping A_i and we know that N_j has a basis consisting of eigenvevtors and generalized eigenvevtors of A_i. And it is true for all $A_i, 2 \leq i \leq K$. Thus, a basis of $\mathbb{C}^n$ consists of eigenvectors and generalized eigenvectors of A_j for each $1 \leq j \leq K$. The proof is complete. □

Method II of proof

Proof. We will prove it by induction on $\dim V$ and $1 \leq k \leq K$. And assume we have pairwise commuting operators $A_1, A_2, \cdots, A_K$ on V.

When $\dim V = 1$, and in this case, all A_i are scalars. Take $B = \{1\}$, and k be arbitrary. Assume the result is true whenever $\dim V < l$, and $A_1, A_2, \cdots, A_k$ are pairwise commuting operators on V if $\dim V < l$. And we want to show that if $\dim V = l$, and $A_1, \cdots, A_{k+1}$ are pairwise commuting operators on V, then there exists a basis of generalized eigenvectors.

For A_1, we have

$$\mathbb{C}^l = \bigoplus_{j=1}^{m} N_{\lambda_j}(A_1)$$

since $A_1 A_i = A_i A_1, 2 \leq i \leq k+1$, we have $A_i : N_{\lambda_j}(A_1) \to N_{\lambda_j}(A_1), \forall j = 1, \cdots, m$ and $\forall i = 1, 2, \cdots, k+1$.

(1) If $m = 1$, then there exists a basis B of $\mathbb{C}^1$ consisting of generalized eigenvectors for $A_2, \cdots, A_k, A_{k+1}$. Any vectors in $\mathbb{C}^l$ is a generalized eigenvectors for A_1 because $\mathbb{C}^l = N_{\lambda_1}(A_1)$, then any vectors in B is a a generalized eigenvectors for $A_1, A_2, \cdots, A_{k+1}$.

(2) If $m > 1$, then $N_{\lambda_j}(A_1) \neq \mathbb{C}^l, \forall j = 1, \cdots, k+1$. On $N_{\lambda_j}(A_1)$, we have $A_1|_{N_{\lambda_j}(A_1)}, A_2|_{N\lambda_j}(A_1), \cdots, A_{k+1}|$ By induction, there exists a basis $\beta_j, j = 1, 2, \cdots, m$ of $N_{\lambda_j}(A_1)$, which are generalized eigenvectors for $A_1|_{N_{\lambda_j}(A_1)}, \cdots, A_{k+1}|_{N\lambda_j}(A_1)$. Take

$$\beta = \bigcup_{j=1}^{m} \beta_j$$

then β is a basis for $\mathbb{C}^l$ consisting of generalized eigenvectors for $A_1, A_2, \cdots, A_{k+1}$.

□

Exercise 6.7.6. *Let λ be an eigenvalue of an $n \times n$ matrix A. Suppose that*

$$\begin{aligned} &\dim N_1(\lambda) = 2, \dim N_2(\lambda) = 4 \\ \textit{and } &\dim N_3(\lambda) = \dim N_4(\lambda) = 5, \end{aligned}$$

Find the Jordan blocks of A corresponding to λ.

Proof. Since $\dim N_3(\lambda) = \dim N_4(\lambda) = 5$, then we can know that the index $d(\lambda) = 3$, then we can know the Jordan blocks of A corresponding to λ is

$$J = \begin{pmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix}.$$

We can verify that this is the Jordan blocks we want. We can compute $N_{(J-\lambda I)}$, $N_{(J-\lambda I)^2}$, $N_{(J-\lambda I)^3}$ and $N_{(J-\lambda I)^4}$. We have

$$J - \lambda I = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and it is obvious that $\dim N_{(J-\lambda I)} = 2$, since there are two 0 column vectors. Similarly, we have

$$(J-\lambda I)^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, (J-\lambda I)^3 = (J-\lambda I)^4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and we can know that $\dim N_{(J-\lambda I)^2} = 4$ and $\dim N_{(J-\lambda I)^3} = \dim N_{(J-\lambda I)^3} = 5$. The proof is complete. $\square$

Exercise 6.7.7. *Let A be a 5×5 rank one matrix, find all possible Jordan canonical forms of A. The order of Jordan blocks should be ignored.*

Proof. Since A is rank one matrix, then there exists two column vectors a, b such that $A = ab^T$, also we know that the minimal polynomial for A is $m_A(\lambda) = \lambda^2 - \alpha\lambda$. So A has eigenvalue 0 with multiplicity 4 and α with multiplicity 1. There are several possible Jordan forms for eigenvalue 0, which are

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha \end{pmatrix}$$

and

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

Since the null space of $A - 0I$ has dimension 4 and one of them is generated by eigenvalue α. Thus, $\dim N_{A-0I} = 3$, which means that there are 3 blocks corresponding to eigenvalue 0. Thus, we can know that all possible Jordan canonical forms of A are

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \text{and} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha \end{pmatrix}.$$

$\square$

Exercise 6.7.8. *Let*

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

Find its eigenvectors and generalized eigenvectors. Find its Jordan canonical form J and the corresponding matrix S so that

$$A = SJS^{-1}.$$

Proof. Taking $A - \lambda I = 0$, we can have characteristic polynomial $p_A(\lambda) = (1-\lambda)^3$, which gives us eigenvalues 1. Now we determine the null space of $A - 1 \dots I$

$$A - I = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

So this eigenspace is dimensional-2. Hence there are two Jordan blocks corresponding to the eigenvalue 1 in the Jordan form. So we have its Jordan canonical form

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

Then we can know the eigenvectors corresponding to 1 are

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \text{ and } v_2 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}.$$

Each of these will give Jordan chain and we compute $(A - I)w_1 = v_1$ and $(A - I)w_2 = v_2$. The second equation does not have solution, so we can know that

$$w_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Then we have the engenvectors and generalized engenvectors, which are

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \text{and } \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}.$$

Thus, we can find S, such that $AS = JS$, and we have

$$S = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

□

Exercise 6.7.9. *Let P be the linear space of polynomials with real coefficients equipped with the scalar product*

$$(f,g) = \int_0^1 f(x)\, g(x)\, dx.$$

(1) Using Gram-Schmidt process to generate an orthonormal basis of the span of vectors $\{1, x^2\}$.

(2) Find the projection of polynomial x on the span of vectors $\{1, x^2\}$.

Proof.

(1) Set $y_1 = 1$ and $y_2 = x^2$, using Gram-Schmidt process, we can have

$$x_1 = \frac{y_1}{\|y_1\|} = \frac{1}{\sqrt{\int_0^1 1 dx}} = 1$$
$$x_2 = \frac{y_2 - (y_2, x_1)x_1}{\|y_2 - (y_2, x_1)x_1\|} = \frac{x^2 - \frac{1}{3}}{\sqrt{\int_0^1 (x^2 - 1/3)^2 dx}} = \frac{3\sqrt{5}x^2 - \sqrt{5}}{2}.$$

(2) Finding the projection of polynomial x on the span of vectors $\{1, x^2\}$ is equivalent to findind the solution for a, b in the equations

$$(1, x - (a + bx^2)) = 0$$
$$(x^2, x - (a + bx^2)) = 0$$

which gives us $b = \frac{15}{16}, a = \frac{3}{16}$. Thus, the projection is $\left(\frac{3}{16}, \frac{15}{16}\right)$.

□

Exercise 6.7.10. *Find the least squares solution to the over-determined system*

$$3x - y = 1,$$
$$x + y = 1,$$
$$2x + 3y = 2.$$

Proof. Writting these equations into $AX = b$, where $A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \\ 2 & 3 \end{pmatrix}, X = \begin{pmatrix} x \\ y \end{pmatrix}$, and $b = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$, then the least square least solution can be determined by $z = (A^T A)^{-1} A^T b = \begin{pmatrix} 0.4638 \\ 0.3768 \end{pmatrix}$. □

Chapter 7

Euclidean Structure

7.1 Scalar Product and Distance

Definition 7.1.1. *An Euclidean structure in a linear space X over $\mathbb{R}$ is furnished by a real-valued function of two vector arguments called a scalar product and denoted by (x, y), which has the following properties:*

(i) (x, y) *is a bilinear function.*

(ii) Symmetricity: $(x, y) = (y, x)$*.*

(iii) Positivity: $(x, x) > 0$ *except for* $x = 0$*.*

Remark 7.1.1. *Scalar product is also called inner product or dot product.*

Definition 7.1.2. *The Euclidean length (or the norm) of x is defined by*

$$\|x\| = \sqrt{(x, x)}.$$

For any $x, y \in X$, $\|x - y\|$ is called the distance of these two vectors.

Theorem 7.1.1 (Schwarz Inequality)**.** *For any $x, y \in X$, $|(x, y)| \leq \|x\|\|y\|$.*

Proof. Consider, for all t, we have

$$\begin{aligned} q(t) &= \|x + ty\|^2 \\ &= (x + ty, x + ty) \\ &= (x, x) + (x, ty) + (ty, x) + (ty, ty) \\ &= \|x\|^2 + 2t(x, y) + t^2\|y\|^2 \geq 0 \end{aligned}$$

Thus, we have

$$\begin{aligned} &4\,|(x, y)|^2 - 4\|x\|^2\|y\|^2 \leq 0 \\ &\Rightarrow |(x, y)| \leq \|x\|\|y\|. \end{aligned}$$

$\square$

Definition 7.1.3. *Suppose $x, y \neq 0$, we define the angle θ between x and y by*

$$\cos\theta = \frac{(x,y)}{\|x\|\|y\|}.$$

Corollary 7.1.1.

$$\|x\| = \max_{\|y\|=1}(x,y).$$

Proof. Let $y = \frac{x}{\|x\|}$, then $\|x\| = \left(x, \frac{x}{\|x\|}\right) \leq \max_{\|y\|=1}(x,y)$. With Schwarz inequality, we have $\max_{\|y\|=1}(x,y) \leq \|x\|$. Thus, we have the desired result. $\square$

Theorem 7.1.2 (Triangle Inequality)**.**

$$\|x+y\| \leq \|x\| + \|y\|.$$

Proof.

$$\|x+y\|^2 = (x+y, x+y) = \|x\|^2 + 2(x,y) + \|y\|^2 \leq (\|x\| + \|y\|)^2.$$

$\square$

Definition 7.1.4. *Two vectors x and y are called orthogonal (perpendicular) if $(x,y) = 0$, denoted by $x \perp y$.*

Theorem 7.1.3 (Pythagorean Theorem)**.** $\|x-y\|^2 = \|x\|^2 + \|y\|^2$ *holds if $x \perp y$.*

Definition 7.1.5. *Let X be a finite-dimensional linear space with an Euclidean structure. A basis $x_1, \cdots, x_n$ is called orthonormal if*

$$(x_i, x_j) = \delta_{ij}, \forall 1 \leq i, j \leq n.$$

Theorem 7.1.4 (Gram-Schmidt)**.** *Given a basis $y_1, \cdots, y_n$ of a finite-dimensional linear space X, then there is an orthonormal basis $x_1, \cdots, x_n$ such that x_k is a linear combination of $y_1, \cdots, y_n, 1 \leq k \leq n$.*

Proof. Define

$$\begin{aligned}
x_1 &= \frac{y_1}{\|y_1\|} \\
x_2 &= \frac{y_2 - (y_2, x_1)x_1}{\|y_2 - (y_2, x_1)x_1\|} \\
&\vdots \\
x_k &= \frac{y_{k+1} - \sum_{j=1}^{k}(y_{k+1}, x_j)x_j}{\|y_{k+1} - \sum_{j=1}^{k}(y_{k+1}, x_j)x_j\|}.
\end{aligned}$$

We claim that $x_1, \cdots, x_n$ form an orthonormal basis of X. $\square$

Let $x_1, \cdots, x_n$ be an orthonormal basis of X and assume

$$x = \sum_{j=1}^{n} a_j x_j, y = \sum_{j=1}^{n} b_j y_j,$$

then $(x, y) = \sum_{j=1}^{n} a_j b_j$ and $\|x\|^2 = \sum_{j=1}^{n} a_j^2$. The mapping $x \mapsto (x_1, \cdots, x_n)$ carries Euclidean structure of X into $\mathbb{R}^n$, and we could identify x with $\mathbb{R}^n$.

Consider inner product (x, y), for $\forall x \in X$, we fix y, then (x, y) is a linear functional on X. We can write it as

$$y \mapsto l_y \in X'$$

then y is in dual space of X.

Theorem 7.1.5. *Every linear functional $l \in X'$ can be written in the form $l(x) = (x, y)$ for some $y \in X$. The mapping $l \mapsto y$ is an isomorphism of X and X'.*

Proof. Let $x_1, \cdots, x_n$ be an orthonormal basis of X'. Let $y = \sum_{j=1}^{n} l(x_j) x_j$, then for any $x = \sum_{j=1}^{n} a_j x_j$, we have

$$l(x) = \sum_{j=1}^{n} l(a_j) x_j = \sum_{j=1}^{n} \sum_{i=1}^{n} l(x_j) a_i (x_j, x_i) = (x, y).$$

$\square$

7.2 Orthogonal Complement and Projection

Definition 7.2.1. *Let Y be a subspace of X. The orthogonal complement of Y is*

$$Y^{\perp} = \{x \in X | (x, y) = 0, \forall y \in Y\}.$$

Recall that we defined before $Y^{\perp} = \{l \in X' | l(y) = 0, \forall y \in Y\}$, these two definitions match if we identify X' with X.

Theorem 7.2.1. *For any subspace $Y \subset X$, we have*

$$X = Y \oplus Y^{\perp}.$$

Proof. Let $y_1, \cdots, y_k$ be an orthogonal basis of Y. We can expend it to a basis of X: $y_1, \cdots, y_k, \widetilde{y_{k+1}}, \cdots, \widetilde{y_n}$. With Gram-Schmidt theorem, we obtain an orthonormal basis $y_1, \cdots, y_k, y_{k+1}, \cdots, y_n$ of X.

We claim that $Y^{\perp} = \operatorname{span}\{y_{k+1}, \cdots, y_n\}$. Indeed, $\operatorname{span}\{y_{k+1}, \cdots, y_n\} \subset Y^{\perp}$ and $\dim Y^{\perp} = n - k$, and then they are equal. $\square$

Definition 7.2.2. *Given a subspace Y of X, $X = Y \oplus Y^{\perp}$, and for any $x \in X$, $x = y + y^{\perp}$, where $y \in Y, y^{\perp}$. The component y is called the orthogonal projection of x into Y, denoted by*

$$y = P_Y x.$$

Theorem 7.2.2. *P_Y is linear and $P_Y^2 = P_Y$, i.e., P_Y is a projection.*

Proof. Let $y_1, \cdots, y_n$ be an orthonormal basis of X, $Y = \operatorname{span}\{y_1, \cdots, y_k\}$ and $Y^{\perp} = \operatorname{span}\{y_{k+1}, \cdots, y_n\}$. Then for any $x \in X$, $x = \sum_{j=1}^{n} a_j y_j$, and we have

$$P_Y(x) = \sum_{j=1}^{k} a_j y_j.$$

Thus, $P_Y^2 = P_Y$ follows naturally. □

Theorem 7.2.3. *Let Y be a linear subspace of Euclidean space X, and $x \in X$, then*

$$\|x - P_Y x\| = \min_{z \in Y} \|x - z\|.$$

Proof. For any $x \in X$, we can write $x = x_1 + x_2$, where $x_1 \in P_Y x, x_2 \in Y^{\perp}$. Then, for any $z \in Y$, we have

$$\|z - x\| = \|z - x_1\|^2 + \|x_2\| \geq \|x_2\|^2$$

and the equation obtain equal sign only when $z = x_1 = P_Y x$. □

7.3 Adjoint

Let X, U be two Euclidean spaces and $A : X \to U$ is a linear map, then we can define its transpose $A' : U' \to X'$ defined as follows, for any $l \in U'$:

$$(A'l, x) = (l, Ax).$$

We can identify U' with U, X' with X.

Definition 7.3.1. *The transpose of a map A of Euclidean space X into U is called the adjoint of A, denoted by $A^* : U \to X$, which is defined as follows:*

$$(A^* y, x) = (y, Ax).$$

Theorem 7.3.1.

(i) If A, B are two linear maps of X into U, then $(A + B)^* = A^* + B^*$.

(ii) If $A : X \to U, C : U \to V$, then $(CA)^* = A^* C^*$.

(iii) If A is a bijection from X onto U, then $(A^{-1})^* = (A^*)^{-1}$.

(iv) $(A^*)^* = A$.

Proof.

(i) For $\forall x \in X, \forall y \in U$, we have

$$\begin{aligned}((A+B)^* y, x) &= (y, (A+B)x) \\ &= (y, Ax + Bx) \\ &= (y, Ax) + (y, Bx) \\ &= (A^* y, x) + (B^* y, x) \\ &= ((A^* + B^*) y, x).\end{aligned}$$

(ii) We have $CA : X \to V, (CA)^* : V \to X$, and then for $\forall z \in V, \forall x \in X$,

$$\begin{aligned}((CA)^* z, x) &= (z, (CA)x) \\ &= (z, C(Ax)) \\ &= (C^* z, Ax) \\ &= (A^* C^* z, x).\end{aligned}$$

(iii) Claim $I^* = I$, and $I = A^{-1}A : X \to X$. Indeed, for $\forall x_1, x_2 \in X$,

$$(I^* x_1, x_2) = (x_1, I x_2) = (x_1, x_2) = (I x_1, x_2).$$

Then we have

$$\begin{aligned}&\left(A^{-1}A\right)^* = A^* \left(A^{-1}\right)^* = I \\ \Rightarrow\ &(A^*)^{-1} = \left(A^{-1}\right)^*.\end{aligned}$$

(iv) For $\forall x \in X$, we have

$$\begin{aligned}(A^{**} x, y) &= (x, A^* y) \\ &= (A^* y, x) \\ &= (y, Ax) \\ &= (Ax, y).\end{aligned}$$

□

Remark 7.3.1. *If we choose an orthogonal basis of X and U, then X and U can be identified as $\mathbb{R}^m$ and $\mathbb{R}^n$. And $A : X \to U$ can be represented by a matrix $A : \mathbb{R}^m \to \mathbb{R}^n$, also $A^* : U \to A$ is represented by the transpose of A, denoted by A'.*

7.4 Overdetermined Systems

Consider a matrix equation

$$Ax = p,$$

where $p_1, \cdots .p_m$ are the measured values, and A is an $m \times n$ matrix. We shall consider the case where the number m of measurements exceeds the number n of quantities.

Theorem 7.4.1. *Let A be $m \times n$ matrix, $m > n$, and suppose that A has only the trivial nullvector 0. Then the vector x that mninimizes $\|Ax - p\|$ is the unique solution z to the equation*

$$A^*Az = A^*p.$$

Proof. The equation $A^*Az = A^*p$ has a unique solution if and only if A^*A is invertible. Indeed, suppose $A^*Ay = 0$ for some $y \in \mathbb{R}^n$, then

$$\begin{aligned} (A^*Ay, y) &= 0 \\ \Rightarrow (Ay, Ay) &= 0 \\ \Rightarrow Ay &= 0. \end{aligned}$$

Since A has only trivial nullvector, then $y = 0$, then the solution is unique.

Let z be the minimizer, then we have

$$Az - p \perp R_A,$$

and for $\forall x \in \mathbb{R}^n$, $(Az - p, Ax) = 0$, which implies $(A^*Az - A^*p, x) = 0$. Thus, since it holds for all x, then we have $A^*Az = A^*p$. □

Remark 7.4.1. *If A has a nontrivial nullvector, then the minimizer cannot be unique.*

Theorem 7.4.2. *For any subspace Y of X, $P_Y^* = P_Y$.*

Proof. For $\forall x_1, x_2 \in X$, we have

$$(x_1, P_Y x_2) = (P_Y x_1, P_Y x_2) = (P_Y x_1, x_2).$$

which implies $P_Y^* = P_Y$. □

7.5 Isometry and Orthogonal Group

Definition 7.5.1. *A mapping of a Euclidean space into itself is called an isometry if it preserves the distance of any paired points, i.e., for any $x, y \in X$, then*

$$\|M(x) - M(y)\| = \|x - y\|.$$

Theorem 7.5.1. *Let M be an isometry from X into itself and $M(0) = 0$. Then:*

(i) M is linear.

(ii) $M^*M = I$ and $\det M = \pm 1$.

(iii) M is invertible and its inverse is an isometry.

Proof.

(i) For all $x \in X$, write $Mx = x'$, and then $\|x\| = \|x'\|$. And for any $x, y \in X$, we have $\|x' - y'\|^2 = \|x - y\|^2$. Then we have

$$\begin{aligned} \|x'\|^2 - 2(x', y') + \|y'\|^2 &= \|x\|^2 - 2(x, y) + \|y\|^2 \\ &\Rightarrow (x', y') = (x, y). \end{aligned}$$

Let $z = x + y$, then we have $\|z' - (x' + y')\| - \|z - (x + y)\| = 0$, which implies $z' = x' + y'$. Also, let $z = cy$, then we have

$$\begin{aligned} \|z' - cy'\|^2 &= (z' - cy', z' - cy') \\ &= \|z'\|^2 - 2c(z', y') + c^2\|y'\|^2 \\ &= \|z\|^2 - 2c(z, y) + c^2\|y\|^2 \\ &= \|z - cy\| = 0 \end{aligned}$$

then $z' = cy$. Combined, we have M is linear.

(ii) For all $x, y \in X$, $(x, y) = (Mx, My) = (M^*Mx, y)$, which implies $M^*M = I$.

(iii) M is an isometry, implying M is invertible. And since it one-to-one, also it is onto. Then M^{-1} is also isometry. Indeed,

$$\|M^{-1}x - M^{-1}y\| = \|MM^{-1}x - MM^{-1}y\| = \|x - y\|.$$

□

Remark 7.5.1. *Conversely, if $M : X \to X$ is a linear map such that $M^*M = I$, then M preserves the distance.*

Proof. $\|Mx\|^2 = (Mx, Mx) = (M^*Mx, x) = (x, x) = \|x\|^2$. □

Definition 7.5.2. *A matrix that maps $\mathbb{R}^n$ onto itself isometrically is called orthogonal.*

Proposition 7.5.1 (Properties of orthogonal)**.** *A matrix M is orthogonal if and only if its columns are pairwise orthogonal unit vectors.*

Proof.

(1) ($\Rightarrow$) If M is orthogonal, then M preserves the product

$$(Me_i, Me_j) = (c_i, c_j) = (e_i, e_j) = \delta_{ij}$$

where $M = (c_1, \cdots, c_n)$. Then $(c_i, c_j) = \delta_{ij}$ implies its columns are pairwise orthogonal unit vectors.

(2) ($\Leftarrow$) If $(c_i, c_j) = \delta_{ij}$ for all $1 \le i, j \le n$, then we have $M^*M = I$ naturally. Thus, M is isometry.

$\square$

Proposition 7.5.2. *A matrix M is orthogonal if and only if its rows are pairwise orthogonal unit vectors.*

Proof. It is obvious since $M^* = M^{-1}$. $\square$

Remark 7.5.2. *If M is orthogonal, then M maps any orthogonal basis into another orthogonal basis. The inverse is also true.*

Proof. Suppose $u_1, \cdots, u_n$ is orthogonal basis and $v_1, \cdots, v_n$ is also orthogonal basis, and $v_k = Mu_k, 1 \le k \le n$. Then we have $V = (v_1, \cdots, v_n) = M(u_1, \cdots, u_n) = MU$. Thus we have $M = VU^{-1}$. Hence, M is orthogonal. $\square$

7.6 Norm of a Linear Map

Definition 7.6.1. *The norm of a linear map $A : X \to U$ is defined by*

$$\|A\| = \sup_{\|x\|=1} \|Ax\| = \sup_{\|x\|\le 1} \|Ax\|.$$

Theorem 7.6.1. *Let A be a linear mapping from the Euclidean space X into the Euclidean space U, where $\|A\|$ is its norm. Then,*

(i) For any $z \in X$, $\|Az\| \le \|A\| \cdot \|z\|$.

(ii) $\|A\| = \sup_{\|x\|=\|z\|=1} (x, Az)$.

Proof.

(i) If $z = 0$, then it holds. If $z \neq 0$, then we have

$$\|Az\| = \left\| A \frac{z}{\|z\|} \|z\| \right\| = \|z\| \cdot \left\| A \frac{z}{\|z\|} \right\| \le \|A\| \cdot \|z\|.$$

(ii) For any $x, z \in X$, and $\|x\| = \|z\| = 1$, then

$$\begin{aligned}(x, Az) &\leq \|x\| \cdot \|Az\| \leq \|Az\| \\ \Rightarrow \sup_{\|x\|=\|z\|=1} (x, Az) &\leq \|Az\|.\end{aligned}$$

If $\|A\| = 0$, then $\sup(x, Az) = 0$, which implies $\|A\| \leq \sup(x, Az)$. If $\|A\| \neq 0$, then for all $\varepsilon > 0$, there exists $z \in X$ and $\|z\| = 1$ such that

$$\|Az\| \geq \|A\| - \varepsilon.$$

Take $x = \frac{Az}{\|Az\|}$, then we have

$$\begin{aligned}(x, Az) = \frac{\|Az\|^2}{\|Az\|} &= \|Az\| \geq \|A\| - \varepsilon \\ \Rightarrow \|A\| - \varepsilon &\leq \sup_{\|x\|=\|z\|=1} (x, Az) \\ \xrightarrow{\varepsilon \to 0} \|A\| &\leq \sup_{\|x\|=\|z\|=1} (x, Az).\end{aligned}$$

Thus, we have $\|A\| = \sup_{\|x\|=\|z\|=1} (x, Az)$.

□

Remark 7.6.1. *For any* $1 \leq i, j \leq n$, $|a_{ij}| \leq \|A\|$.

Proof. With the second argument in the previous theorem, $a_{ij} = (e_i, Ae_j) \leq \|A\|$. □

Theorem 7.6.2.

(i) *For all* $k \in \mathbb{R}$, $\|kA\| = |k| \cdot \|A\|$.

(ii) $A, B : X \to U$, *then* $\|A + B\| \leq \|A\| + \|B\|$.

(iii) $A : X \to U, B : U \to V$, *then* $\|BA\| \leq \|B\| \cdot \|A\|$.

(iv) $\|A^*\| = \|A\|$.

Proof.

(i) If $k = 0$, then it holds. If $k \neq 0$, then $\|kAx\| = |k| \cdot \|Ax\|$, which implies

$$\|kA\| = \sup_{\|x\|=1} \|kAx\| = \sup_{\|x\|=1} |k| \cdot \|Ax\| = |k| \cdot \|A\|.$$

(ii) For any $x \in X$, and $\|x\| = 1$, we have

$$\|A + B\| \leq \sup \|(A + b)x\| = \sup \|Ax + Bx\| \leq \sup \|Ax\| + \sup \|Bx\| = \|A\| + \|B\|.$$

(iii) For any $x \in X$, and $\|x\|= 1$, we have

$$\|BA\|\leq \sup\|BAx\|\leq \|B\|\cdot\|Ax\|\leq \|B\|\cdot\|A\|.$$

(iv) $A^* : U \to X$, for all $x \in X$ and all $u \in U$, we have $(A^*u, x) = (u, Ax) = (Ax, u)$. Thus,

$$\|A^*\| = \sup_{\|x\|=\|u\|=1}(A^*u, x) = \sup_{\|x\|=\|u\|=1}(Ax, u) = \|A\|.$$

$\square$

Theorem 7.6.3. *Let X be a finite-dimensional Euclidean space and $A : X \to X$ is an invertible linear map. Let $B : X \to X$ be linear map such that*

$$\|B - A\|\leq \frac{1}{\|A^{-1}\|}$$

then B is invertible.

Proof. Let $C = A - B$, then $B = A - C = A\,(I - A^{-1}C)$.

It suffices to show that $I - A^{-1}C$ is invertible. Suppose by contradiction that for some $x \neq 0$, $(I - A^{-1}C)\,x = 0$. Then we have

$$\begin{aligned}\|x\| &= \|A^{-1}Cx\|\\ &\leq \|A^{-1}C\|\|x\|\\ &\leq \|A^{-1}\|\|C\|\|x\|.\end{aligned}$$

Since $\|C\|\leq \frac{1}{\|A^{-1}\|}$, then we have $\|x\|< \|x\|$, which is a contradiction.

Then, $I - A^{-1}C$ is invertible, so is B. $\square$

Remark 7.6.2. *Invertible matrices form an open and dense set.*

7.7 Completeness and Local Compactness

Definition 7.7.1. *A sequence of vectors $\{x_n\}$ in Euclidean space X converges to $x \in X$ if $\|x_k - x\|\to 0$ if $k \to \infty$. We write $\lim_{k\to\infty} x_k = x$.*

Theorem 7.7.1. *A sequence $\{x_n\} \subset X$ is called a Cauchy sequence if $\forall\varepsilon > 0$, there exists $N > 0$, such that for all $k, j \geq N$, $\|x_k - x_j\|< \varepsilon$.*

(i) Completeness: every Cauchy sequence in a finite-dimensional Euclidean space is convergent.

(ii) Locally compactness: any bounded sequence in a finite-dimensional Euclidean space contains a convergent subsequence.

Proof.

(i) Let x, y be two vectors in X, and a_j, b_j are their jth component respectively, then

$$|a_j - b_j| \leq \|x - y\|.$$

Denote by $a_{k,j}$ the jth component of x_k. Since $\{x_k\}$ is Cauchy sequence, then the sequence $\{a_{k,j}\}$ is also a Cauchy sequence. Then $\{a_{k,j}\}$ converges to a real number a_j. Denote $x = (a_1, \cdots, a_n)$, then we have

$$\|x_k - x\| = \sum_{j=1}^{n} |a_{k,j} - a_j|^2$$

it foolows that $\lim_{k\to\infty} x_k = x$.

(ii) Since $|a_{k,j}| \leq \|x_k\|$, then $|a_{k,j}| \leq M \in \mathbb{R}$ for all k. Since real numbers are locally compactness, then the theorem follows.

□

Corollary 7.7.1.

$$\|A\| = \max_{\|x\|=1} \|Ax\|.$$

Proof. We know that $\|A\| = \sup_{\|x\|=1} \|Ax\|$, then there exists a sequence $\{x_k\}$ such that $\|x_k\| = 1$ and $\lim_{k\to\infty} \|Ax_k\| = \|A\|$. Also there exists convergent subsequence $\|x_{n_k}\|$ of $\{x_k\}$, and denote by $\lim_{k\to\infty} x_{n_k} = x$. Then, we have $\|x\| = \lim_{k\to\infty} \|x_{n_k}\| = 1$.

Since $\lim_{k\to\infty} Ax_{n_k} = Ax$, indeed, we have

$$\|Ax_{n_k} - Ax\| \leq \|A\| \cdot \|x_{n_k} - x\| \to 0,$$

then we have

$$\|A\| = \lim_{k\to\infty} \|Ax_{n_k}\| = \|Ax\|.$$

□

Theorem 7.7.2. *Let X be an Euclidean space and suppose X is locally compact in the sense that any bounded sequence has a convergent subsequence. Then X is of finite dimension.*

Proof. Assume $\dim X = \infty$, then there exists a sequence $\{x_k\}_{k=1}^{\infty}$ and any finite set of vectors are linearly independent (otherwise X will be finite-dimensional). Then there exists $\{e_k\}_{k=1}^{\infty}$ such that $(e_i, e_j) = \delta_{ij}$. And for any $i \neq j$, we have $\|e_i - e_j\|^2 = 2$.

Thus, $\{e_k\}_{k=1}^{\infty}$ has no convergent subsequence, which is a contradiction. □

Definition 7.7.2. *A sequence of linear mappings $\{A_n\}$ from X to Y converges to $A: X \to Y$ if* $\lim_{n\to\infty}\|A_n - A\|= 0$.

Theorem 7.7.3. *In finite-dimensional spaces, then* $\lim_{n\to\infty} A_n = A$ *if and only if, for all $x \in X$,* $\lim_{n\to\infty} A_n x = Ax$*, which is called weak convergence.*

Proof.

(1) ($\Rightarrow$) If $\lim_{n\to\infty} A_n = A$, then

$$\|A_n x - Ax\|\leq \|A_n - A\|\cdot\|x\|\xrightarrow{n\to 0} 0.$$

(2) ($\Leftarrow$)

(a) First, we show that $\{A_n\}$ is bounded. Let $\{e_i\}$ be an orthogonal basis of X. For each $e_i, 1 \leq i \leq \dim X = N$, we have

$$\lim_{n\to\infty} A_n e_i = Ae_i,$$

then $\|A_n e_i\|\leq a_i$ for all n and some $a_i \geq 0$. For any $x \in X$, $x = \sum_{i=1}^N x_i e_i$, then

$$\begin{aligned}\|A_n x\| &= \left\|\sum_{i=1}^N x_i A_n e_i\right\| \\ &\leq \sum_{i=1}^N a_i\|x_i\| \\ &\leq \left(\sum_{i=1}^N a_i^2\right)^{\frac{1}{2}} \cdot \left(\sum_{i=1}^N\|x_i\|^2\right)^{\frac{1}{2}} \\ &= \left(\sum_{i=1}^N a_i^2\right)^{\frac{1}{2}} \|x\|.\end{aligned}$$

Thus, $\|A_n\|\leq \left(\sum_{i=1}^N a_i^2\right)^{\frac{1}{2}}$, which implies $\{A_n\}$ is bounded.

(b) Second, we prove the convergence.
Let $A: X \to Y$ be defined as $Ax = \lim_{n\to\infty} A_n x$. We claim A is linear. For any $x \in X, \|x\|= 1$ and $\forall\varepsilon > 0$, there exists a sequence $\{x_k\}_{k=1}^{N_\varepsilon}$ such that $\|x_k\|= 1$ and for $1 \leq k \leq N_\varepsilon$, $\|x_k - x\|\leq \varepsilon$. Thus, we have

$$\begin{aligned}\|A_n x_k - Ax_k\| &\leq \|A_n x - A_n x_k\|+\|A_n x - Ax\|+\|Ax_k - Ax\| \\ &\leq a\|x - x_k\|+\|A_n x - Ax\|+\|A\|\cdot\|x_k - x\| \\ &\leq (a + \|A\|)\|x_k - x\|+\|A_n x - Ax\|\xrightarrow{n\to\infty} 0.\end{aligned}$$

Hence, $\lim_{n\to\infty} A_n = A$.

$\square$

7.8 Complex Euclidean Structure

Definition 7.8.1. *A complex Euclidean structure over a linear space X over $\mathbb{C}$ is furnished by a complex valued function, called a scalar product or inner product, denoted by (x, y), such that*

(1) (x, y) is linear in x when y is fixed.

(2) Conjuate: $(x, y) = \overline{(y, x)}$ for all $x, y \in X$.

(3) Positivity: $(x, x) > 0$ for all $x \neq 0$.

Remark 7.8.1. *For x fixed, (x, y) is a skew linear function of y, i.e.,*

$$\begin{aligned}(x, \alpha y_1 + \beta y_2) &= \overline{(\alpha y_1 + \beta y_2, x)} \\ &= \overline{(\alpha y_1, x) + (\beta y_2, x)} \\ &= \overline{\alpha}\overline{(y_1, x)} + \overline{\beta}\overline{(y_2, x)} \\ &= \overline{\alpha}(x, y_1) + \overline{\beta}(x, y_2).\end{aligned}$$

Definition 7.8.2. *The norm of $x \in X$ is defined as: $\|x\| = \sqrt{(x, x)}$.*

Theorem 7.8.1 (Schwarz Inequality)**.**

$$|(x, y)| \leq \|x\| \cdot \|y\|.$$

Proof. We have

$$\begin{aligned}\|x + y\|^2 &= \|x\| + (x, y) + (y, x) + \|y\|^2 \\ &= \|x\| + 2\operatorname{Re}(x, y) + \|y\|^2.\end{aligned}$$

For any λ, $\|\lambda x + y\|^2 = \lambda^2\|x\|^2 + 2\lambda\operatorname{Re}(x, y) + \|y\|^2 \geq 0$, then we have

$$\begin{aligned}&4\left|\operatorname{Re}(x, y)\right|^2 - a\|x\|^2\|y\|^2 \leq 0 \\ &\Rightarrow |\operatorname{Re}(x, y)| \leq \|x\| \cdot \|y\|.\end{aligned}$$

Since $\left(e^{i\theta}x, y\right) = e^{i\theta}(x, y)$, then we pick θ such that $e^{i\theta}(x, y) > 0$. Thus, we have

$$|(x, y)| = \left|\operatorname{Re}(e^{i\theta}x, y)\right| \leq \|x\| \cdot \|y\|.$$

□

Theorem 7.8.2 (Triangle Inequality)**.**

$$\|x + y\| \leq \|x\| + \|y\|.$$

Proof. We have

$$\begin{aligned}\|x+y\|^2 &= \|x\|+2\operatorname{Re}(x,y)+\|y\|^2\\ &\le \|x\|+2\,|(x,y)|+\|y\|^2\\ &\le \|x\|+2\|x\|\cdot\|y\|+\|y\|^2\\ &= (\|x\|+\|y\|)^2.\end{aligned}$$

□

Let X, Y be two complex Euclidean spaces and $AX \to Y$. The adjoint A^* of A is defined as follows

$$(x, A^*y) = (Ax, y)$$

then $A^* = \overline{A^T}$ as matrix. Fix y, (Ax, y) is linear in X. We claim that there exists $z \in X$ such that $(x, z) = (Ax, y)$, then $A^*y = z$. Indeed, we define in $\mathbb{C}^n$:

$$(x, y) = ((x_1, \cdots, x_n), (y_1, \cdots, y_n)) = \sum_{i=1}^{n} x_i \overline{y_i}.$$

Then, for $A = (a_{ij})_{n\times n} : \mathbb{C}^n \to \mathbb{C}^n$, we have

$$\begin{aligned}(Ax, y) &= \sum_{1\le i,j\le n} a_{ij} x_j \overline{y_j}\\ &= \sum_{1\le i,j\le n} a_{ij} \overline{\overline{a_{ij}} y_i}\\ &= (x, A^*y).\end{aligned}$$

Definition 7.8.3. *A linear mapping of a complex Euclidean space into itself is called unitary if it is isometry.*

Theorem 7.8.3. *M is unitary if and only if $M^*M = 1$. Hence, for a unitary map M,* $|\det M| = 1$.

Proof.

(1) ($\Rightarrow$) Since M is isometric, then we have $(x, y) = (Mx, My) = (M^*Mx, y)$, which implies $M^*M = I$.

   Also, $\det M \det M^* = 1$ and $\det M = \det \overline{M}^T = \overline{\dim M}$. Thus, we have $|\det M| = 1$.

(2) ($\Leftarrow$) If $M^*M = 1$, then we have

$$(x, y) = (M^*Mx, y) = (Mx, My)$$

   which implies M is isometric.

□

Theorem 7.8.4. *Let $A : \mathbb{R}^n \to \mathbb{R}^n$ or $A : \mathbb{C}^n \to \mathbb{C}^n$, then*

$$\|A\| = \left(\sum_{1 \le i,j \le n} |a_{ij}|^2 \right)^{\frac{1}{2}}.$$

Proof. For any $x \in \mathbb{C}^n$, we have

$$\begin{aligned} \|Ax\|^2 &= \sum_{i=1}^n \left| \sum_{j=1}^n a_{ij} x_j \right|^2 \\ &\le \sum_{i=1}^n \left(\sum_{j=1}^n |a_{ij}|^2 \right) \left(\sum_{j=1}^n x_j^2 \right) \\ &= \|x\| \left(\sum_{i=1}^n \sum_{j=1}^n |a_{ij}|^2 \right), \end{aligned}$$

then we have $\|A\| \le \left(\sum_{i=1}^n \sum_{j=1}^n |a_{ij}|^2 \right)$. □

Definition 7.8.4. *The quantity $\left(\sum_{i,j=1}^n |a_{ij}|^2 \right)^{\frac{1}{2}}$ is called the Hilbert-Schmidt norm of the matrix A, denoted by $\|A\|_{HS}$.*

Remark 7.8.2. $\sum_{i,j=1}^n |a_{ij}|^2 = \operatorname{tr} A^* A = \operatorname{tr} AA^*$.

7.9 Spectral Radius

Definition 7.9.1. *The spectral radius $r(A)$ of a linear mapping $A : X \to X$ is defined as*

$$r(A) = \max_j |\lambda_j|$$

where λ_j are all possible eigenvalues.

Remark 7.9.1. *$r(A), \|A\|, \|A\|_{HS}$ are measures of the sign of A.*

Proposition 7.9.1. *$\|A\| \ge r(A)$.*

Proof. Let λ be an eigenvalue of A such that $r(a) = |\lambda|$. Assume $x \neq 0$, $Ax = \lambda x$, then we have $\|A\| \cdot \|x\| \ge \|Ax\| = |\lambda| \cdot \|x\|$. Thus, $\|A\| \ge r(A)$. □

Remark 7.9.2.

(1) Take $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, then $r(A) = 0$ and $\|A\| \neq 0$. Then we can have strictly inequality.

(2) If there exists orthogonal basis formed by eigenvectors, then $\|A\| = r(A)$.

Proof. Suppose $\{x_k\}$ is the orthogonal basis and $Ax_k = \lambda_k x_k$. And for any $x \in X$, $x = \sum_{k=1}^n x_k e_k$, then

$$Ax = \sum_{k=1}^n x_k \lambda_k e_k$$

where $\|x\|^2 = \sum_{i=1}^n |x_k|^2$. Then we have

$$\|Ax\|^2 = \sum_{k=1}^n |x_k \lambda_k|^2 \le r(A)^2 \|x\|^2.$$

which implies

$$\frac{\|Ax\|}{\|x\|} = \left\| A \frac{x}{\|x\|} \right\| \le r(A).$$

Since this is true for any x, and $\|A\| = \max_{\|x\|=1} \|Ax\|$, therefore $\|A\| \le r(A)$. With previous proposition, we have $\|A\| = r(A)$. □

Theorem 7.9.1 (Gelfand's Formula)**.**

$$r(A) = \lim_{k\to\infty} \left(\left\| A^k \right\| \right)^{1/k}.$$

Proof. First, we need a lemma.

Lemma 7.9.2. *If $r(A) < 1$, then $\lim_{k\to\infty} A^k = 0$.*

Proof. Let J be the Jordan canonical form of A, then $r(A) = r(J) < 1$. And we have

$$J = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_l \end{pmatrix}$$

where

$$J_s = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}_{n_s \times n_s}, 1 \le s \le l.$$

Then we have

$$J_s^k = \begin{pmatrix} \lambda^k & \binom{k}{1}\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \cdots & \binom{k}{n_s-1}\lambda^{k-n_s+1} \\ & \ddots & \ddots & & \vdots \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & \binom{k}{1}\lambda^{k-1} \\ & & & & \lambda^k \end{pmatrix}.$$

We claim $\lim_{k\to\infty} \binom{k}{j}\lambda^{k-j} = 0, 0 \le j \le n_s - 1$ for $|\lambda| < 1$. Then we have $\lim_{k\to\infty} J_s^k = 0$, which implies $\lim_{k\to\infty} J^k = 0$. Since $A = MJM^{-1}$, then $\lim_{k\to\infty} A^k = 0$. □

Now we complete the proof of the theorem.

(1) Since $\|A\| \geq r(A)$, then we have $\left\|A^k\right\| \geq \left(r\left(A^k\right)\right)^{\frac{1}{k}} = \left(r(A)^k\right)^{\frac{1}{k}} = r(A)$. Then,

$$\liminf_{k\to\infty} \left(\left\|A^k\right\|\right)^{1/k} \geq r(A).$$

(2) Consider for any $\varepsilon > 0$ and let $A_\varepsilon = \frac{A}{\varepsilon + r(A)}$. Since $r(A_\varepsilon) < 1$, the above lemma implies that $\lim_{k\to\infty} A_\varepsilon^k = 0$ and hence $\lim_{k\to\infty} \left\|A_\varepsilon^k\right\| = 0$. In particular, there exists $K > 0$ such that for all $k \geq K$, $\left\|A_\varepsilon^k\right\| < 1$. Then,

$$\begin{aligned} \left(\left\|A_\varepsilon^k\right\|\right)^{\frac{1}{k}} &< 1 \\ \Rightarrow \left\|A_\varepsilon^k\right\|^{\frac{1}{k}} &< \varepsilon + r(A) \\ \Rightarrow \limsup_{k\to\infty} \left\|A_\varepsilon^k\right\|^{\frac{1}{k}} &\leq \varepsilon + r(A) \end{aligned}$$

Thus, as $\varepsilon \to 0$, we have $\limsup_{k\to\infty} \left\|A_\varepsilon^k\right\|^{\frac{1}{k}} \leq r(A)$.

Combined results above gives us $r(A) = \lim_{k\to\infty} \left(\left\|A^k\right\|\right)^{1/k}$. □

Corollary 7.9.1. *Suppose $A_1A_2 = A_2A_1$, then $r(A_1A_2) \leq r(A_1)r(A_2)$.*

Proof. We can have $r(A_1A_2) = \lim_{k\to\infty} \left\|(A_1A_2)^k\right\|^{1/k}$, and $(A_1A_2)^k = A_1^kA_2^k$ since they commute. Thus,

$$\left\|(A_1A_2)^k\right\|^{1/k} \leq \left(\left\|A_1^k\right\|^{1/k}\right)\left(\left\|A_2^k\right\|^{1/k}\right)$$

which implies $r(A_1A_2) \leq r(A_1)r(A_2)$. □

7.10 Exercises

Exercise 7.10.1. *Suppose $1 \leq k \leq n$ and $x_1, x_2, \cdots x_k$ are k vectors in $\mathbb{R}^n$ satisfying for any $1 \leq i, j \leq k$,*

$$(x_i, x_j) = \delta_{ij}.$$

For each $1 \leq j \leq k$, let a_j be the first component of x_j. Show that

$$\sum_{j=1}^{k} a_j^2 \leq 1.$$

Proof. Since $(x_i, x_j) = \delta_{ij}, 1 \leq i, j \leq n$, then we can arrange $x_1, x_2, \cdots, x_n$ into a matrix and denote it by $A = (x_1, x_2, \cdots, x_n)$, then we have A is an orthogonal matrix with determinant 1. Then $\det A^* = 1$.

Now we pick a vector $z = (1, 0, \cdots, 0)^T \in \mathbb{R}^n$. Then we have $A^* z = (a_1, a_2, \cdots, a_n)^T$, and therefore the first component of the vector AA^*z is $\sum_{j=1}^k a_j^2$, which means $AA^*z = \left(\sum_{j=1}^k a_j^2, \cdots\right)^T$. Also, we have $\|AA^*z\| \leq \|Iz\| = 1$. We denote other components of AA^*z as $w_2, w_3, \cdots, w_n$, then we have

$$\sum_{j=1}^k a_j^2 \leq \|AA^*z\|^{1/2} = \sqrt{\sum_{j=1}^k a_j^2 + w_2^2 + \cdots + w_n^2} = 1$$

$$\Rightarrow \sum_{j=1}^k a_j^2 \leq 1.$$

□

Exercise 7.10.2. *Let A be an $m \times n$ matrix, c_j $1 \leq j \leq n$ be column vectors of A and r_i, $1 \leq i \leq m$ be row vectors of A, show that*

$$\|A\| \geq \max_{1 \leq j \leq n} \|c_j\| \quad and \quad \|A\| \geq \max_{1 \leq i \leq m} \|r_i\|.$$

Here we view A as a linear map from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Proof. For jth column c_j of A, we pick a unit vector $e_j = (0, \cdots, 0, 1, 0, \cdots, 0)^T \in \mathbb{R}^n$, where jth entry is 1, others are all zero. Then we can have $Ae_j = c_j$. Thus, we have

$$\|c_j\| \leq \|A\| \|e_j\| = \|A\|$$

since this is true for all $1 \leq j \leq n$, then we have $\max_{1 \leq j \leq n} \|c_j\| \leq \|A\|$.

For ith row r_i of A, we can consider $A^* = (r_1, r_2, \cdots, r_m)$. And still, we pick a vector $e_i' = (0, \cdots, 0, 1, 0, \cdots, 0)^T \in \mathbb{R}^m$, where ith entry is 1, others are all zero. And then we take $A^* e_i' = r_i$, which gives us

$$\|r_i\| \leq \|A^*\| \|e_i'\| = \|A^*\| = \|A\|$$

in the last step we used the fact that $\|A^*\| = \|A\|$. This is true for all $1 \leq i \leq m$, then we have $\max_{1 \leq i \leq m} \|r_i\| \leq \|A\|$. The proof is complete. □

Exercise 7.10.3. *Let*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}.$$

Find the spectral radius, operator norm and Hilbert-Schmidt norm of $A : \mathbb{R}^n \to \mathbb{R}^n$.

Proof. The eigenvalues of A are 1 and 3, and then we can know that the spectral radius is $r(a) = \max|\lambda| = 3$. The operator norm of A is the largest eigenvalues of AA^T, which is

$$AA^T = \begin{pmatrix} 5 & 6 \\ 6 & 9 \end{pmatrix}.$$

And the charasteristic polynomial is $\lambda^2 - 14\lambda + 9 = 0$, which gives us norm of A is $\max_{j=1,2} \lambda_j = 7 + 2\sqrt{10}$. The Hilbert-Schmidt norm of A is $\|A\| = \left(\sum_{i,j} |a_{ij}^2|\right)^{1/2} = \sqrt{14}$. □

Chapter 8

Spectral Theory of Self-Adjoint Mappings

8.1 Self-Adjoint Mapping

Definition 8.1.1. *A linear mapping A of a linear or complex Euclidean space into itself is said to be self-adjoint if $A^* = A$.*

Remark 8.1.1. *If we pick an orthogonal basis of Euclidean space, we can view A as a matrix $A = (a_{ij})_{n\times n}$, then*

(i) In real case, $A^* = A \iff A^T = A \iff A$ is real symmetric, i.e., $a_{ij} = a_{ji}$.

(ii) In complex case, $A^* = A \iff \overline{A^T} = A$, i.e., $a_{ij} = \overline{a_{ji}}$. We say A is Hermitian matrix.

Theorem 8.1.1. *A self-adjoint map H of complex Euclidean space X into itself has real eigenvalues and the set of eigenvectors which is formed by orthogonal basis of X.*

Proof. We can view H as a matrix. Then,

(i) All eigenvalues are real. Assume λ is eigenvalue, such that $Hx = \lambda x$. Then we have

$$\begin{aligned}(Hx, x) &= (x, Hx)\\ \Rightarrow (\lambda x, x) &= (x, \lambda x)\\ \Rightarrow \lambda(x, x) &= \overline{\lambda}(x, x)\end{aligned}$$

and since $\|x\| \neq 0$, we have $\lambda = \overline{\lambda}$. Thus, $\operatorname{Im}\lambda = 0$, which implies λ is real.

(ii) There are no generalized eigenvectors. Suppose $x \in N_{(N-\lambda_i I)^2}$ and $\lambda = 0$ for simplicity, then $H^2x = 0$, which implies

$$\begin{aligned}(H^2x, x) &= 0\\ \Rightarrow (Hx, Hx) &= 0\\ \Rightarrow \|Hx\|^2 &= 0\\ \Rightarrow Hx &= 0.\end{aligned}$$

Hence, $x \in N_{(N-\lambda_i I)}$, and the index of λ_i is 1. Thus, there are no generalized eigenvectors.

(iii) Eigenvectors of H are orthogonal. Suppose $\lambda \neq \mu$ are two eigenvalues such that $Hx = \lambda x, Hy = \mu y$. Then we have

$$\begin{aligned} &(Hx, y) = (x, Hy) \\ \Rightarrow\ &(\lambda x, y) = (x, \mu y) \\ \Rightarrow\ &\lambda(x, y) = \overline{\mu}(x, y) = \mu(x, y), \end{aligned}$$

which implies $(x, y) = 0$.

$\square$

Remark 8.1.2. *With the theorem abovem, $X = \oplus_{\lambda_i} N_{(H-\lambda_i I)}$. We can pick orthogonal basis for $N_{(H-\lambda_i I)}$ for each λ_i, then we get orthogonal basis.*

Corollary 8.1.1. *Any Hermitian matrix can be diagonalized by a unitary matrix.*

Proof. Let $\{x_k\}_{k=1}^n$ be the orthogonal basis consisting of eigenvectors of A, such that $Ax_k = \lambda_k x_k$, and λ_k is real. Let $U = (x_1, x_2, \cdots, x_n)$, which is unitary, then we have

$$AU = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix},$$

which implies $A = U\Lambda U^{-1}$. $\square$

Theorem 8.1.2. *A self-adjoint map H of real Euclidean space X into itself has real eigenvalues and a set of eigenvectors which is formed by orthogonal basis of X.*

Proof. We pick an orthogonal basis of X and H can be represented by a matrix A if we identify X as $\mathbb{R}^n$, then we have $A^T = A$. We can extend A to a map from $\mathbb{C}^n$ to $\mathbb{C}^n$, denoted by $\widetilde{A}$, then $\widetilde{A}^* = \widetilde{A}$. Then $\widetilde{A}$ is Hermitian matrix and we can apply the theorem (8.1.1).

We claim $\sigma(A) = \sigma\left(\widetilde{A}\right)$ and

$$N_{(A-\lambda I)} = \operatorname{Re} N_{\left(\widetilde{A}-\lambda I\right)}.$$

Indeed, $\widetilde{A}$ can be diagonalized by a unitary matrix U such that $A = U\Lambda U^{-1}$, where Λ is a real diagonal matrix. Then, A can be diagonalized by a real matrix M such that $A = M\Lambda M^{-1}$. Thus, the eigenvalues of A are all real. Ans since

$$\dim_{\mathbb{R}} N_{(A-\lambda I)} = \dim_{\mathbb{C}} N_{\left(\widetilde{A}-\lambda I\right)},$$

we have

$$\mathbb{R}^n = \oplus_{\lambda \in \sigma(A)} N_{(A-\lambda I)}.$$

Thus, we can find a set of eigenvectors that form an orthogonal basis of $\mathbb{R}^n$. $\square$

Corollary 8.1.2. *Any symmetric matrix can be diagonalized by an orthogonal matrix.*

8.2 Quadratic Forms

Consider a quadratic form

$$q(y) = \sum_{i,j=1}^{n} h_{ij} y_i y_j = (y, Hy),$$

where $y = (y_1, \cdots, y_n)^T \in \mathbb{R}^n$, and $H = (h_{ij})_{n \times n}$ is symmetric. Let $x = Ly$, then $y = L^{-1}x$ and

$$\begin{aligned} q(y) &= \left(L^{-1}x, HL^{-1}x\right) \\ &= \left(x, \left(L^{-1}\right)^T HL^{-1}x\right) \\ &= (x, Mx). \end{aligned}$$

Definition 8.2.1. *Two symmetric matrices A and B are called congruent if there exists an invertible matrix S such that $A = S^T BS$.*

Theorem 8.2.1. *Given $q(x) = (x, Ax)$, there exists an invertible matrix L, such that*

$$q\left(L^{-1}x\right) = \sum_{i=1}^{n} d_i x_i^2$$

for some constants d_i, and we can make $d_i = 0$ or $d_i = \pm 1$.

Proof. Since A is self-adjoint, then there exists a unitary matrix Q such that $A = Q\Lambda Q^*$, where

$$\Lambda = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix},$$

where $\lambda_k, 1 \leq k \leq n$ are real eigenvalues of A. Then, we have

$$\begin{aligned} q(x) &= (x, Ax) \\ &= (x, Q\Lambda Q^* x) \\ &= (Q^* x, \Lambda Q^* x) \\ \Rightarrow q(Qx) &= (Q^* Qx, \Lambda Q^* Qx) \\ &= (Ix, \Lambda Ix) \\ &= (x, \Lambda x) = \sum_{i=1}^{n} \lambda_i x_i^2 \end{aligned}$$

and we can pick $L = Q^{-1} = Q^*$. Thus the proof is complete. ∎

8.3 Law of Inertia

Theorem 8.3.1 (Sylvester's Law of Inertia)**.** *Let H be symmetric, $q(x) = (x, Hx)$ and L be an invertible matrix such that*

$$q\left(L^{-1}x\right) = \sum_{i=1}^{n} d_i x_i^2$$

for some constants d_i. Then the numbers of positive, negative and zero terms of d_i equal to the numbers of positive, negative and zero eigenvalues of H.

Proof. Let p_+, p_- and p_0 be the numbers of positive, negative and zero terms of d_i. Let S be a subspace of $\mathbb{R}^n$, we say $q > 0$ on S if for all $u \in S, u \neq 0$, $q(u) > 0$.

We claim that

$$p_+ = \max_{q>0 \text{ on } S} \dim S.$$

Let $S = L^{-1}\left(\text{span}\{e_i, d_i > 0\}\right)$, then $\dim S = p_+, q > 0$ on S.

(1) For $y \in S$, $y = L^{-1}x$, where $x = \sum_{d_i>0} d_i c_i^2$, then

$$q(y) = q\left(L^{-1}x\right) = \sum_{i=1}^{n} d_i x_i^2 = \sum_{d_i>0} d_i c_i^2 \geq 0.$$

Thus, we have $p_+ \leq \max \dim S$.

(2) Let S be any subspace with $\dim S > p_+$, we claim that q cannot be positive on S. For all $u \in S$, we have $Lu = \sum_{i=1}^{n} u_i e_i$.

Define $pu = L^{-1}\left(\sum_{d_i>0} u_i e_i\right)$, which is a projection. Then we have

$$\dim ps \leq p_+ < \dim S.$$

Then there exists $y \in S, y \neq 0$, such that $Lpy = 0$. Assume $L = I$, then $py = 0$, which implies $q(y) = 0$.

□

Remark 8.3.1. *Two symmetric square matrices of the same size have the same numbers of positive, negative and zero eigenvalues if and only if they are congruent.*

8.4 Spectral Resolution

Definition 8.4.1. *The set of eigenvalues of H is called the spectral of H.*

Let H be a self-adjoint map from X into X, then we have

$$X = \oplus_{\lambda_j \in \sigma(H)} N_{H - \lambda_j I}.$$

Hence, $N(\lambda_j) = N_{H-\lambda_j I}$ are orthogonal subspaces. Let $\lambda_j, 1 \leq j \leq k$ be distinct eigenvalues. For any $x \in X$, then x can be represented as $x = \sum_{j=1}^{k} x_j$, where $x_j \in N(\lambda_j)$. We say x_j is orthogonal projection of X to $N(\lambda_j)$, i.e.,

$$x_j = P_{N(\lambda_j)}(x).$$

Applying H, we have

$$Hx = \sum_{j=1}^{k} \lambda_j x_j.$$

Let P_j be the orthogonal projection of X onto $N(\lambda_j)$, we have

$$I = \sum_{j=1}^{k} P_j,$$

which follows $x = \sum_{j=1}^{k} x_j$ and hence

$$H = \sum_{j=1}^{k} \lambda_j P_j.$$

Theorem 8.4.1. *The operators P_j have the following properties:*

(i) $P_j P_k = 0$ *for* $j \neq k, P_j^2 = P_j$.

(ii) Each P_j *is self-adjoint, i.e.,* $P_j^* = P_j$.

Proof.

(i) For any $x \in X$, $x = \sum_{j=1}^{k} x_j$, where $x_j \in N(\lambda_j)$, we have $P_j P_k x = P_j x_k = 0$. Thus, $P_j P_k = 0$ for $j \neq k$.

(ii) For any $x = \sum_{j=1}^{k} x_j \in X$ and $y = \sum_{j=1}^{k} y_j \in X$, where $x_j, y_j \in N(\lambda_j)$, we have

$$(P_j x, y) = (x_j, y) = \left(x_j, \sum_{j=1}^{k} y_j \right) = (x_j, y_j)$$

where in the last step we used the fact that N_i is orthogonal to x_j for $i \neq j$. Similarly, we have

$$(x, P_j y) = (x_j, y_j).$$

Thus, we have $P_j^* = P_j$.

$\square$

Definition 8.4.2. *A decomposition of the form:*

$$I = \sum_{j=1}^{k} P_j$$

where P_j is a projection, i.e., satisfies $P_j P_k = 0$ for $j \neq k, P_j^2 = P_j$ and $P_j^* = P_j$, is called a resolution of the identity. Any self-adjoint map H defineds a resolution of identity.

Definition 8.4.3. *Let H be a self-adjoint map, then*

$$H = \sum_{j=1}^{k} \lambda_j P_j$$

is called the spectral resolution of H.

Given any polynomial p, we have

$$p(H) = \sum_{j=1}^{k} p\left(\lambda_j\right) P_j,$$

since $H^m = \left(\sum_{j=1}^{k} \lambda_j P_j\right)^m = \sum_{j=1}^{k} \lambda_j^m P_j^m = \sum_{j=1}^{k} \lambda_j^m P_j$. Move generally, given a convergent series $f(t) = \sum_{k=0}^{\infty} a_k t^k$, we have

$$f(H) = \sum_{j=1}^{k} f\left(\lambda_j\right) P_j.$$

In particular,

$$e^H = \sum_{m=0}^{\infty} \frac{H^m}{m!} = \sum_{j=1}^{\infty} e^{\lambda_j} P_j.$$

Theorem 8.4.2. *Let H, K be two self-adjoint matrices that commute. Then they have a common resolution of identity $I = \sum_{j=1}^{k} P_j$, such that*

$$H = \sum_{j=1}^{k} \lambda_j P_j, K = \sum_{j=1}^{k} \mu_j P_j$$

where $\lambda_j \in \sigma(H), \mu_j \in \sigma(K)$.

Proof. Since $X = \oplus_{j=1}^{l} N\left(\lambda_j\right)$, where $\lambda_j, 1 \leq j \leq l$ are distinct eigenvalue of H. We claim $N\left(\lambda_j\right)$ is invariant under K, i.e., $K : N\left(\lambda_j\right) \to N\left(\lambda_j\right)$.

Indeed, for any $x \in N\left(\lambda_j\right)$, $HKx = KHx = \lambda_j Kx$, which implies Kx is also an eigenvector of H. So k maps $N\left(\lambda_j\right)$ into $N\left(\lambda_j\right)$, we now apply spectral resolution of K over $N\left(\lambda_j\right)$, which gives us the theorem. $\square$

8.5 Anti-Self Adjoint Mappings

Definition 8.5.1. *A linear mapping A of Euclidean space into itself is called anti-self-adjoint if $A^* = -A$.*

Remark 8.5.1. *If A is anti-self adjoint, then $(iA)^* = iA$. Thus A can be unitary diagonalized. Also, if A is anti-self adjoint, then $AA^* = A^*A$.*

Definition 8.5.2. *A mapping A from a compact Euclidean space into itself is normal if it commutes with its adjoint operator, i.e., $AA^* = A^*A$.*

Theorem 8.5.1. *A normal map N has an orthonormal basis consists of eigenvectors.*

Proof. Define $H = \frac{N+N^*}{2}$ and $A = \frac{N-N^*}{2}$, then both H and A are self-adjoint. Then we have

$$\begin{aligned} HA &= \frac{1}{4}\left(N^2 + N^*N - NN^* - (N^*)^2\right) \\ &= \frac{1}{4}\left(N^2 - (N^*)^2\right) \\ &= AH. \end{aligned}$$

Then there exists a basis consisting of eigenvectors for both A and H. Then we claim that the eigenvectors of $A + H$ are equal to that of N, since if we have $Av = \lambda v$ and $Hv = \mu v$, then $(A + H)v = Nv = (\lambda + \mu)v$. □

Corollary 8.5.1. *If N is a normal matrix, then N can be unitary diagonalized.*

Theorem 8.5.2. *Let U be a unitary map of a complex Euclidean space into itself, that is an isometry linear map. Then,*

(i) There is an orthogonal basis consisting of genuine eigenvectors of U.

(ii) The eigenvalues of U are complex numbers with absolute value 1.

Proof.

(i) Since U is unitray, i.e., $UU^* = U^*U = I$, then U is self-adjoint, which implies U is normal. Thus, the previous theorem indicates the argument.

(ii) Isometry preserves the distance, then

$$\|Ux\| = |\lambda| \|x\| = \|x\|.$$

Thus, $|\lambda| = 1$.

□

8.6 Rayleigh Quotient

Definition 8.6.1. *Let H be self-adjoint, then the quotient*

$$R_H(x) = \frac{(x, Hx)}{(x, x)}$$

is called the Rayleigh quotient of H.

Remark 8.6.1.

(1) $R_H(kx) = R_H(x)$.

(2) $R_H(x)$ is continuous and real valued, thus it has maximum and minimum.

Theorem 8.6.1. *Maximum and minimum of $R_H(x)$ are eigenvalues of H.*

Proof. We can view R_H as a real continuous map on the unit sphere. Hence, R_H has a maximum and a minimum. Let $\|x\|= 1$, then for any y, we have

$$R_H(x) = \max_{\|y\|=1} \frac{(y, Hy)}{(y, y)}.$$

then we have $\frac{\mathrm{d}R_H(x+ty)}{\mathrm{d}t}\Big|_{t=0} = 0$. Also, we have

$$\begin{aligned}
\frac{\mathrm{d}R_H(x+ty)}{\mathrm{d}t}\bigg|_{t=0} &= \frac{\mathrm{d}}{\mathrm{d}t}\bigg|_{t=0} \frac{(x, Hx) + 2t\,\mathrm{Re}(x, Hy) + t^2(y, Hy)}{\|x\|^2+2t\,\mathrm{Re}(x, y) + t^2\|y\|^2} \\
&= \frac{2\,\mathrm{Re}(x, Hy)}{\|x\|^2} - \frac{(x, Hx)2\,\mathrm{Re}(x, y)}{\|x\|^4} \\
&= 2\,\mathrm{Re}(x, Hy) - (x, Hx)2\,\mathrm{Re}(x, y) \\
\Rightarrow \mathrm{Re}(Hx, y) &= \mathrm{Re}((x, Hx)x, y)
\end{aligned}$$

which implies $Hx = (x, Hx)x$. Thus, x is an eigenvector, and $(x, Hx) = R_H(x), \|x\|= 1$ is an eigenvalue. □

Corollary 8.6.1.

$$\max_{x\neq 0} R_H(x) = \max_{\lambda\in\sigma(H)} \lambda$$
$$\min_{x\neq 0} R_H(x) = \min_{\lambda\in\sigma(H)} \lambda.$$

Remark 8.6.2. *Every eigenvector x of H is a critical point of R_H, that is, the first derivative of R_H are zero when x is an eigenvector of H. Conversely, the eigenvectors are the only critical points of $R_H(x)$. The value of the Rayleigh quotient at an eigenvector is the corresponding eigenvalue of H.*

8.7 Minimax Principle

Theorem 8.7.1. *Let H be a self-adjoint map of a Euclidean space X of finite dimension. Denote the eigenvalues of H, arranged in increasing order by $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Then,*

$$\lambda_j = \min_{\dim S = j} \max_{x \in S, x \neq 0} R_H(x),$$

where S is a linear subspace of X.

Proof. Let $\{x_j\}_{j=1}^n$ be the orthogonal basis of X such that $Hx_j = \lambda_j x_j$. For any $x \in X$ and $x = \sum_{j=1}^n c_j x_j$, then

$$R_H(x) = \frac{\sum_{j=1}^n \lambda_j |c_j|^2}{\sum_{j=1}^n |c_j|^2}.$$

Let $S_j = \text{span}\{x_1, \cdots, x_j\}$, then

$$\max_{x \in S_j, x \neq 0} R_H(x) = \max \frac{\sum_{k=1}^j \lambda_k |c_k|^2}{\sum_{k=1}^j |c_k|^2} = \lambda_j,$$

which implies

$$\min_{\dim S = j} \max_{x \in S, x \neq 0} R_H(x) \leq \lambda_j.$$

Next, given any S with $\dim S = j$, we need to show $\max_{x \in S, x \neq 0} R_H(x) \geq \lambda_j$. It suffices to show that there exists $x \in S$, such that the projection of x on S_{j-1} is zero. Denote the projection by $P : S_j \to S_{j-1}$, with Rank-Nullity theorem, there exists $x^* = \sum_{k \geq j} c_k x_k \in S, x^* \neq 0$ such that $Px^* = 0$. Hence, we have

$$\max_{x \in S, x \neq 0} \frac{(x, Hx)}{(x, x)} \geq \frac{(x^*, Hx^*)}{(x^*, x^*)} = \frac{\sum_{k \geq j} \lambda_k |c_k|^2}{\sum_{k \geq j} |c_k|^2} \geq \lambda_j.$$

since S is arbitrary subspace of dimension j, then we have

$$\min_{\dim S = j} \max_{x \in S, x \neq 0} R_H(x) \geq \lambda_j.$$

Thus we complete the theorem. □

8.8 Generalized Rayleigh Quotient

Definition 8.8.1. *A self-adjoint map M is called positive if for all nonzero $x \in X$, $(x, Mx) > 0$.*

Remark 8.8.1. *With Minimax principle, we can know that M being positive is equivalent to that all eigenvalues of M are positive.*

Now we consider a generalization of the Rayleigh quotient: for $H^* = H, M^* = M$ and $M > 0$,

$$R_{H,M}(x) = \frac{(x, Hx)}{(x, Mx)}.$$

Let $M = \left(\sqrt{M}\right)^2$, $\sqrt{M} > 0$ and $y = \sqrt{M}x$, then we have

$$\begin{aligned} R_{H,M}(x) = \frac{(x, Hx)}{(x, Mx)} &= \frac{\left(\sqrt{M}^{-1}y, H\sqrt{M}^{-1}y\right)}{\left(\sqrt{M}^{-1}y, M\sqrt{M}^{-1}y\right)} \\ &= \frac{\left(y, \left(\sqrt{M}^*\right)^{-1} H\sqrt{M}^{-1}y\right)}{(y, y)} = R_{\widetilde{H}}(y). \end{aligned}$$

Now we consider

$$\left.\frac{\mathrm{d}}{\mathrm{d}t}\right|_{t=0} \frac{(x + ty, H(x + ty))}{(x + ty, M(x + ty))} = \frac{2\operatorname{Re}(x, Hy)}{(x, Mx)} - \frac{2(x, Hx)\operatorname{Re}(x, My)}{(x, Mx)^2} = 0,$$

which implies

$$\begin{aligned} &\operatorname{Re}(x, Mx)(x, Hy) = \operatorname{Re}(x, Hx)(x, My) \\ &\quad\Rightarrow \operatorname{Re}(x, Hy) = \operatorname{Re} R_{H,M}(x)(Mx, y). \end{aligned}$$

If x is a critical point of $R_{H,M}(x)$, then $\operatorname{Re}(x, Hy) = \operatorname{Re} R_{H,M}(x)(Mx, y)$ for all $y \in X$. Thus, we have

$$(Hx, y) = R_{H,M}(x)(Mx, y) \iff Hx = R_{H,M}(x)Mx.$$

Theorem 8.8.1. *There exists a basis $\{x_1, \cdots, x_n\}$ of X such that*

$$Hx_j = \lambda_j Mx_j,$$

where λ_j is real and $\lambda_j = R_{H,M}(x_j)$. Moreover, $(x_i, Mx_j) = 0$ for $i \neq j$.

Corollary 8.8.1. *If M, H are self-adjoint, all the eigenvalues of $M^{-1}H$ are real and $M^{-1}H$ is diagonalizable. If $H > 0$, then all the eigenvalues of $M^{-1}H$ are positive.*

8.9 Norm and eigenvalues

We recall that $\|A\|= \max\|Ax\|, \|x\|= 1$ or $\|A\|= \sup \frac{\|Ax\|}{\|x\|}$. Then we have the following theorem.

Theorem 8.9.1. *Suppose N is a normal mapping of an Euclidean space X into itself, then $\|N\|\leq r(A)$.*

Proof.

(1) $r(N) \leq \|N\|$. Indeed, for any eigenvalue λ_j and its corresponding eigenvector x_j, we have

$$\|Nx_j\|= |\lambda_j|\cdot\|x_j\|\leq \|N\|\cdot\|x_j\|$$

which implies $\max \lambda_j = r(N) \leq \|N\|$.

(2) Now we prove the other direction. If N is normal, then there exists orthogonal basis $\{x_1, \cdots, x_n\}$ of X consisting of eigenvectors of N, such that $Nx_j = \lambda_j x_j, 1 \leq j \leq n$. For any $x \in X$, $x = \sum_{j=1}^n c_j x_j$, then we have

$$Nx = \sum_{j=1}^n c_j \lambda_j x_j.$$

Thus, we have

$$\frac{\|Nx\|}{\|x\|} = \left(\frac{\sum_{j=1}^n |c_j|^2 |\lambda_j|^2}{\sum_{j=1}^n |c_j|^2}\right)^{\frac{1}{2}} \leq \max \lambda_j = r(N).$$

□

Theorem 8.9.2. *Let $A : X \to Y$, then $\|A\|= \sqrt{r(A^*A)}$.*

Proof.

(1) A^*A is normal and we have

$$\begin{aligned}\|Ax\|^2 &= (Ax, Ax)\\ &= (x, A^*Ax)\\ &\leq \|A^*A\|\cdot\|x\|^2= r(A^*A)\|x\|^2\end{aligned}$$

which implies $\|A\|\leq \sqrt{r(A^*A)}$.

(2) Let λ be an eigenvalue of A^*A such that $\lambda = r(A^*A) \geq 0$ and $A^*Ax = \lambda x, x \neq 0$. Then, for eigenvector x, we have

$$\begin{aligned}
\|Ax\|^2 &= (Ax, Ax) \\
&= (x, A^*Ax) \\
&= \lambda\|x\|^2 \\
&= r(A^*A)\|x\|^2
\end{aligned}$$

which implies $\|A\| \geq r(A^*A)$. Indeed,

$$\sqrt{r(A^*A)} = \frac{\|Ax\|}{\|x\|} \leq \|A\| = \max \frac{\|Ay\|}{\|y\|}.$$

□

8.10 Schur Decomposition

Theorem 8.10.1. *Let A be an $n \times n$ matrix. There exists unitary matrix U such that*

$$A = UTU^*$$

for some upper triangular matrix T.

Proof. First we pick $\lambda_1 \in \sigma(A)$ and let $N_1 = N_{(A-\lambda_1 I)}$. Assume $k_1 = \dim N_1 \geq 1$, then there exists orthogonal basis $\{x_1, \cdots, x_{k_1}\}$ for N_1. We can complete this basis to an orthogonal basis $\{x_1, \cdots, x_{k_1}, x_{k_1+1}, \cdots, x_n\}$ of $\mathbb{C}^n$. Let $U_1 = (x_1, \cdots, x_n)$, where x_j is jth column of the matrix U_1, and

$$\begin{aligned}
&Ax_j = \lambda_1 x_j, 1 \leq j \leq k_1 \\
&Ax_j = \sum_{k=1}^{n} b_{kj}\lambda_k, k_1 + 1 \leq j \leq n.
\end{aligned}$$

Then we have

$$A(x_1, \cdots, x_n) = (x_1, \cdots, x_n) \begin{pmatrix} \lambda_1 I_{k_1} & B_{12} \\ & B_{22} \end{pmatrix},$$

where

$$\begin{pmatrix} B_{12} \\ B_{22} \end{pmatrix} = \begin{pmatrix} b_{1,k_1+1} & \cdots & b_{1,n} \\ \vdots & \ddots & \vdots \\ b_{n,k_1+1} & \cdots & b_{n,n} \end{pmatrix}.$$

Then we have

$$A = U_1 \begin{pmatrix} \lambda_1 I_{k_1} & B_{12} \\ & B_{22} \end{pmatrix} U_1^*.$$

Second, let $\lambda_2 \in \sigma(B_{22})$, and $k_2 = \dim N_2$, where $N_2 = N_{(B_{22}-\lambda_2 I)}$. Then there exists unitary matrix U_2 such that

$$B_{22} = U_2 \begin{pmatrix} \lambda_2 I_{k_2} & C_{12} \\ & C_{22} \end{pmatrix} U_2^*.$$

Continue this process and we can obtain an upper triangular matrix. $\square$

Theorem 8.10.2. *Let $Ab = BA$, then A and B can be simultaneously upper diagonalized by a unitary matrix.*

Proof. Let $\lambda_1 \in \sigma(A), N_1 = N_{(A-\lambda_1 I)}$, then we can know B is invariant under N_1, i.e., $B : N_1 \to N_1$. Then we have

$$A = U_1 \begin{pmatrix} \lambda_1 I_{k_1} & A_{12} \\ & A_{22} \end{pmatrix} U_1^*$$
$$B = U_1 \begin{pmatrix} \mu_1 I_{k_1} & B_{12} \\ & B_{22} \end{pmatrix} U_1^*,$$

and we claim $A_{22}B_{22} = B_{22}A_{22}$. Then this process can continue. $\square$

Theorem 8.10.3. *If $AB = BA$, then $r(A+B) \leq r(A) + r(B)$.*

Proof. With previous theorem, A, B can be simultaneously upper diagonalized by a unitary matrix, then $A = UT_1U^*, B = UT_2U^*$, where U_1, U_2 are upper triangular matrix where the diagonal components are eigenvalues of A and B. Then we have $A + b = U(T_1 + T_2)U^*$, and

$$T_1 + T_2 = \begin{pmatrix} \lambda_1 + \mu_1 & & \\ & \ddots & \\ & & \lambda_n + \mu_n \end{pmatrix}$$

where $\lambda_j \in \sigma(A), \mu_j \in \sigma(B)$. Thus we have

$$r(A+B) = \max(\lambda_j + \mu_j) \leq \max \lambda_j + \max \mu_j = r(A) + r(B).$$

$\square$

8.11 Exercises

Exercise 8.11.1. *Let*

$$q(x) = 2x_1x_2 - 6x_2x_3 + 2x_1x_3.$$

Find an invertible matrix L, such that

$$q\left(L^{-1}y\right) = d_1y_1^2 + d_2y_2^2 + d_3y_3^2$$

where $d_i = 0$ or ± 1.

Proof. We have $q(x) = (x, Hx)$, where

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & -3 \\ 1 & -3 & 0 \end{pmatrix}$$

and we need to normalize the matrix H, then we can compute for its eigenvalues, which are $\lambda = 3, \frac{3-\sqrt{17}}{2}, \frac{3+\sqrt{17}}{2}$, with eigenvectors

$$\begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} \frac{3-\sqrt{17}}{2} \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} \frac{3+\sqrt{17}}{2} \\ 1 \\ 1 \end{pmatrix},$$

Now we can normalize these vectors and we get

$$\begin{pmatrix} 0 \\ -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} -\sqrt{\frac{17-3\sqrt{17}}{34}} \\ \frac{2}{\sqrt{17-3\sqrt{17}}} \\ \frac{2}{\sqrt{17-3\sqrt{17}}} \end{pmatrix}, \begin{pmatrix} \sqrt{\frac{17+3\sqrt{17}}{34}} \\ \frac{2}{\sqrt{17+3\sqrt{17}}} \\ \frac{2}{\sqrt{17+3\sqrt{17}}} \end{pmatrix},$$

And we arrange eigenvectors into a matrix, denoting it by

$$C = \begin{pmatrix} 0 & -\sqrt{\frac{17-3\sqrt{17}}{34}} & \sqrt{\frac{17+3\sqrt{17}}{34}} \\ -\frac{1}{\sqrt{2}} & \frac{2}{\sqrt{17-3\sqrt{17}}} & \frac{2}{\sqrt{17+3\sqrt{17}}} \\ \frac{1}{\sqrt{2}} & \frac{2}{\sqrt{17-3\sqrt{17}}} & \frac{2}{\sqrt{17+3\sqrt{17}}} \end{pmatrix}.$$

We can verify that $C^*HC = \begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{3-\sqrt{17}}{2} & 0 \\ 0 & 0 & \frac{3+\sqrt{17}}{2} \end{pmatrix}$. Now we denote $z = Cx = (z_1, z_2, z_3)$, where

$$z_1 = -\sqrt{\frac{17-3\sqrt{17}}{34}} x_2 + \sqrt{\frac{17+3\sqrt{17}}{34}} x_3$$
$$z_2 = -\frac{1}{\sqrt{2}} x_1 + \frac{2}{\sqrt{17-3\sqrt{17}}} x_2 + \frac{2}{\sqrt{17+3\sqrt{17}}} x_3$$
$$z_3 = \frac{1}{\sqrt{2}} x_1 + \frac{2}{\sqrt{17-3\sqrt{17}}} x_2 + \frac{2}{\sqrt{17+3\sqrt{17}}} x_3$$

and we need to change variable to get the quadratic form $q\left(L^{-1}y\right) = d_1 y_1^2 + d_2 y_2^2 + d_3 y_3^2$. We make the change of variable

$$y_1 = \frac{1}{\sqrt{3}} z_1$$
$$y_2 = \sqrt{\frac{2}{3-\sqrt{17}}} z_2$$
$$y_3 = \sqrt{\frac{2}{3+\sqrt{17}}} z_3$$

and we can denote this transform by matrix E, where

$$E = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & \sqrt{\frac{2}{3-\sqrt{17}}} & 0 \\ 0 & 0 & \sqrt{\frac{2}{3+\sqrt{17}}} \end{pmatrix}$$

then we can know that $L^{-1} = CE$, which are defined above. And finally, $L = (CE)^{-1}$. $\square$

Exercise 8.11.2. *Show that the congruence is an equivalence relation for symmetric matrices. Find the total number of equivalence classes for $n \times n$ symmetric matrices.*

Proof. We denote the relation of congruence by $\sim$.

(1) a. For A is a symmetric matrix, then we have $A \sim A$, since $A = I^T AI$, where I is identity matrix.

b. For A, B are symmetric matrices, we have if $A \sim B$, then $B \sim A$. Since if $A = S^T BS$, where S is invertible, then we have $B = (S^T)^{-1} AS^{-1}$, which means $B \sim A$.

c. For A, B and C are symmetric matrices, we have if $A \sim B, B \sim C$, then $A \sim C$. Since if we have $A = S^T BS$ and $B = P^T CP$, then we have $A = S^T P^T CPS = (PS)^T CPS$, which implies $A \sim C$. Then we proved the congruence is an equivalence relation.

(2) Suppose $A = S^T BS$, and S is invetible. Also, we have $R_{BS} \subseteq R_B$ with equality when S is invertible, since S is full rank. Then we have, in this case, $\dim B = \dim BS$. Then we have S^T is also full rank and $\dim A = \dim S^T BS = \dim B$. So we can know that for symmetric matrices A and B, if they are congruent then they have the same rank, which means there are $n + 1$ equivalebce classes, since there are matrix with rank $0, 1, 2, \cdots, n$, which are $n + 1$ possibilities.

$\square$

Exercise 8.11.3. *Let A, B be two $n \times n$ real orthogonal matrices satisfying*

$$\det A + \det B = 0.$$

Show there exists a unit vector x such that

$$Ax = -Bx.$$

Proof. Since A and B are orthogonal matrices, then we have $\det A = \det B = \pm 1$ and $A^T A = B^T B = I$. Also, with $\det A + \det B = 0$, we have $\det A \det B = -1$. Now consider

$$\begin{aligned} \det(A + B) &= \det\Big(A(A^T + B^T)B\Big) \\ &= \det A \det\Big(A^T + B^T\Big) \det B \\ &= -\det\Big(A^T + B^T\Big) \\ &= -\det(A + B)^T \\ &= -\det(A + B). \end{aligned}$$

Then we have $\det(A+B)=0$, which means $A+B$ is not full rank. Then we can find a vector $y \in N_{A+B}$ such that $(A+B)y=0$. Now we pick $x=\frac{y}{\|y\|}$, this is the unit vector we need. $\square$

Exercise 8.11.4. *Suppose A and B are normal complex $n \times n$ matrices. Prove that*

$$r(AB) \leq r(A)r(B).$$

Here $r(\cdot)$ is the spectral radius of a matrix. Find a counter example if A or B is not normal.

Proof.

(1) We have $r(AB) \leq \|AB\|$, since if λ be an eigenvalue of AB, then for $x \in \mathbb{C}^n, x \neq 0$ being corresponding eigenvector, we have

$$\begin{aligned} ABx &= \lambda x \\ \Rightarrow \|AB\|\|x\| &\geq \|ABx\| = |\lambda|\|x\| \\ \Rightarrow \|AB\| &\geq |\lambda|. \end{aligned}$$

Also, we have $\|AB\| \leq \|A\|\|B\|$. And with A, B being normal matrices, we know $\|A\| = r(A)$ and $\|B\| = r(B)$. Thus, with all the results above, we have

$$r(AB) \leq \|AB\| \leq \|A\|\|B\| = r(A)r(B).$$

The proof is complete.

(2) Take $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$ and A, B are not normal. We can compute that $r(AB) = \sqrt{3}$ and $r(A)r(B) = 1 \cdot 1 = 1 < r(AB)$. This is a counter example if A and B are not normal.

$\square$

Exercise 8.11.5. *What is the operator norm of the matrix*

$$\begin{pmatrix} 1 & 0 & 1 \\ 2 & 3 & 0 \end{pmatrix}$$

in the standard Euclidean structures of $\mathbb{R}^2$ and $\mathbb{R}^3$.

Proof. Denote the matrix above by A, then the operator norm of A is $\sqrt{r(A^*A)} = \sqrt{\frac{15+\sqrt{137}}{2}}$. $\square$

Exercise 8.11.6. *Let $\{\lambda_i\}_{i=1}^n$ be eigenvalues of matrix $A = (a_{ij})_{n\times n}$. Show that*

$$\sum_{j=1}^{n} |\lambda_j|^2 \leq \sum_{i,j=1}^{n} |a_{ij}|^2 .$$

Proof. With Schur decomposition, we cnould know that $A = QUQ^*$, where Q is unitary and U is upper triangular and its diagonal entries are engenvalues of A, since A and U are similar. And we can show that Hilbert-Schwarz norm norm $\|A\|_{HS}= \sqrt{\sum_{i,j=1}^{n} |a_{ij}|^2}$ is invariant under unitary matrix multiplication:

$$\|QA\|_{HS}^2= \mathrm{tr}\left((QA)^*(QA)\right) = \mathrm{tr}\left(A^*Q^*QA\right) = \mathrm{tr}\left(A^*A\right) = \|A\|_{HS}^2$$

then we can have

$$\|A\|_{HS}^2= \|QAQ^*\|_{HS}^2= \|U\|_{HS}^2.$$

Also we can know that

$$\sum_{j=1}^{n} |\lambda_j|^2 \leq \sum_{i,j=1}^{n} |u_{ij}|^2 = \|A\|_{HS}^2,$$

since the square sum of all diagonal entries of U is smaller than that of all entries of U. □

Exercise 8.11.7. *Let $A = (a_{ij})_{n\times n}$ be normal. Show that*

$$r(A) \geq \max_{1\leq i\leq n} |a_{ii}| .$$

Proof. Since A is normal matrix, then we have $\|A\|= r(A)$. Also, we have known that for all a_{ij}, $|a_{ij}| \leq \|A\|$. Thus, we have $r(A) \geq \max_{1\leq i\leq n} |a_{ii}|$. □

Chapter 9

Calculus of Vector and Matrix valued Functions

9.1 Convergence in Norm

Let $A(t)$ be a matrix valued function, $t \in \mathbb{R}$ and $A(t)$ is an $m \times n$ matrix.

Definition 9.1.1. *We say $A(t)$ is continuous at $t_0 \in I$, where I is an open interval, if*

$$\lim_{t \to t_0} \|A(t) - A(t_0)\| = 0.$$

We say $A(t)$ is differentiable at $t_0 \in I$, with derivative $\dot{A}(t_0) = \frac{\mathrm{d}A(t)}{\mathrm{d}t}\Big|_{t=t_0}$, if

$$\lim_{h \to 0} \left\| \frac{A(t_0 + h) - A(t_0)}{h} - \dot{A}(t_0) \right\| = 0.$$

Remark 9.1.1. *Different norms for finite-dimensional spaces are equivalent. So the above definition will not depend on the norm we use.*

Remark 9.1.2. *Continuity and differentiability is equivalent to those of every element of $A(t)$. If $A(t) = (a_{ij}(t))$, then $\dot{A}(t) = \left(\frac{\mathrm{d}}{\mathrm{d}t} a_{ij}(t)\right)$.*

Theorem 9.1.1 (Basic Rules of Differentiation)**.**

(i) $\frac{\mathrm{d}}{\mathrm{d}t} = \frac{\mathrm{d}}{\mathrm{d}t} A(t) + \frac{\mathrm{d}}{\mathrm{d}t} B(t)$.

(ii) $\frac{\mathrm{d}}{\mathrm{d}t} A(t)B(t) = \left(\frac{\mathrm{d}}{\mathrm{d}t} A(t)\right) B(t) + A(t) \frac{\mathrm{d}}{\mathrm{d}t} B(t)$.

(iii) For $x(t), y(t) \in \mathbb{C}^n$, $\frac{\mathrm{d}}{\mathrm{d}t} = \left(\frac{\mathrm{d}}{\mathrm{d}t} x(t), y(t)\right) + \left(x(t), \frac{\mathrm{d}}{\mathrm{d}t} y(t)\right)$.

Theorem 9.1.2. *Suppose $A(t)$ is differentiable square matrix valued function and $A(t)$ is invertible, then*

$$\frac{\mathrm{d}}{\mathrm{d}t} A^{-1}(t) = -A^{-1} \dot{A} A^{-1}.$$

Proof. $A(t)$ is differentiable, and $AA^{-1} = I$. Then we have

$$
\begin{aligned}
A\frac{\mathrm{d}}{\mathrm{d}t}A^{-1} + \dot{A}A^{-1} &= 0 \\
\Rightarrow \frac{\mathrm{d}}{\mathrm{d}t}A^{-1} &= -A^{-1}\dot{A}A^{-1}.
\end{aligned}
$$

□

Let A be a square matrix valued function, then in general, the chain rule does not hold, i.e., $\frac{\mathrm{d}}{\mathrm{d}t}A^2(t) = \dot{A}A + A\dot{A} \neq 2A\dot{A}$. For $k \in \mathbb{N}$,

$$\frac{\mathrm{d}}{\mathrm{d}t}A^k(t) = \sum_{j=1}^{k} A^{j-1}\dot{A}A^{k-j}.$$

If $A\dot{A} = \dot{A}A$, then

$$\frac{\mathrm{d}}{\mathrm{d}t}A^k(t) = kA^{k-1}(t)\dot{A}.$$

Theorem 9.1.3. *Let p be any polynomial, and A be a square matrix valued function that is differentiable.*

(i) If for a particular value of t, $A(t)\dot{A}(t) = \dot{A}(t)A(t)$, then

$$\frac{\mathrm{d}}{\mathrm{d}t}p(A) = p'(A)\dot{A}.$$

(ii) Even if $A(t)$ and $\dot{A}(t)$ do not commute, chain rule of the trace remains,

$$\frac{\mathrm{d}}{\mathrm{d}t}\operatorname{tr} p(A) = \operatorname{tr}\left(p'(A)\dot{A}\right).$$

Proof.

(i) Suppose $A(t)\dot{A}(t) = \dot{A}(t)A(t)$, then we have

$$\frac{\mathrm{d}}{\mathrm{d}t}A^k(t) = kA^{k-1}(t)\dot{A}.$$

then the argument is proved since all polynomials are combinations of powers.

(ii) For nomcommuting A and $\dot{A}$, we take the trace of

$$\frac{\mathrm{d}}{\mathrm{d}t}A^k(t) = \sum_{j=1}^{k} A^{j-1}\dot{A}A^{k-j},$$

and the trace is commutative, then we have

$$\operatorname{tr}\left(A^{j-1}\dot{A}A^{k-j}\right) = \operatorname{tr}\left(A^{k-1}\dot{A}\right).$$

Thus, we have

$$\frac{\mathrm{d}}{\mathrm{d}t}\operatorname{tr} p(A) = \operatorname{tr}\left(p'(A)\dot{A}\right).$$

$\square$

Now we extend the product rule to multilinear function $M(x_1, \cdots, x_k) : (\mathbb{C}^n)^k \to \mathbb{C}$. Suppose $x_j(t), 1 \leq j \leq k$ are differentiable, then

$$\frac{\mathrm{d}}{\mathrm{d}t} M(x_1, \cdots, x_k) = M(\dot{x}_1, \cdots, x_k) + \cdots + M(x_1, \cdots, \dot{x}_k).$$

Proof. For $k = 2$, we have

$$\begin{aligned}
&\frac{M(x_1(t+h), x_2(t+h)) - M(x_1(t), x_2(t))}{h} \\
=&M\left(\frac{x_1(t+h) - x_1(t+h)}{h}, x_2(t)\right) + M\left(x_1(t), \frac{x_2(t+h) - x_2(t+h)}{h}\right) \\
\overset{n \to 0}{=}&M(\dot{x}_1(t), x_2(t)) + M(x_1(t), \dot{x}_2(t)).
\end{aligned}$$

$\square$

We can apply the above result to the determinant function $D(x_1, \cdots, x_n)$ defined before and we have

$$\frac{\mathrm{d}}{\mathrm{d}t} D(x_1, \cdots, x_n) = D(\dot{x}_1, \cdots, x_k) + \cdots + D(x_1, \cdots, \dot{x}_k).$$

Theorem 9.1.4. *Let $Y(t)$ be a differentiable matrix valued function, then for those t such that Y is invertible, then*

$$\frac{\mathrm{d}}{\mathrm{d}t} \ln|\det Y(t)| = \operatorname{tr}\left(Y^{-1}\dot{Y}\right),$$

which is equivalent to

$$\frac{\frac{\mathrm{d}}{\mathrm{d}t}\det Y(t)}{\det Y(t)} = \operatorname{tr}\left(Y^{-1}\dot{Y}\right).$$

Proof. Fix t_0, and we have $Y(t) = Y(t_0)Y^{-1}(t_0)Y(t)$, which implies

$$\det Y(t) = \det Y(t_0) \det\left(Y^{-1}(t_0)Y(t)\right).$$

Thus, we have

$$\frac{\mathrm{d}}{\mathrm{d}t} \det Y(t)\bigg|_{t=t_0} = \det Y(t_0) \operatorname{tr}\left(Y^{-1}(t_0)\dot{Y}(t)\right)\bigg|_{t=t_0}$$

which proved the theorem. $\square$

9.2 Matrix Exponential

We claim that the Taylor series also holds to define e^A for any square matrix A:

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!}.$$

Theorem 9.2.1.

(i) If A, B are square matrices and $AB = BA$, then

$$e^{A+B} = e^A e^B.$$

(ii) If A and B do not commute, then in general

$$e^{A+B} \neq e^A e^B.$$

(iii) If $A(t)$ depends differentiable on t, then $e^{A(t)}$ is also differentiable.

(iv) If at some t, $A(t)$ and $\dot{A}(t)$ commute, then

$$\frac{\mathrm{d}}{\mathrm{d}t} e^{A(t)} = e^{A(t)} \dot{A}(t).$$

(v) If A is anti-self adjoint, i.e., $A^* = -A$, then e^A is unitary.

Proof.

(i) Since $AB = BA$, we have

$$\begin{aligned} e^{A+B} &= \sum_{k=0}^{\infty} \frac{(A+B)^k}{k!} \\ &= \sum_{k=0}^{\infty} \sum_{j=0}^{k} \frac{\binom{k}{j} A^k B^{k-j}}{k!} \\ &= \sum_{k=0}^{\infty} \sum_{j=0}^{k} \frac{A^k B^{k-j}}{j!\,(k-j)!} \\ &= \sum_{k=0}^{\infty} \frac{A^k}{k!} \sum_{j=0}^{\infty} \frac{B^j}{j!} = e^A e^B. \end{aligned}$$

(v) Since $A^* = -A$, we have $AA^* = A^*A = -A^2$. Then we have $I = e^0 = e^{A^*+A} = e^A e^{A^*} = e^A \left(e^A\right)^*$. Thus, e^A is unitary.

□

To calculate e^A, we could use Jordan canonical form $A = SJS^{-1}$, then we have

$$e^A = Se^J S^{-1},$$

where

$$J = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_K \end{pmatrix}, \text{ and } J_k = \begin{pmatrix} \lambda_k & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_k \end{pmatrix}_{l\times l} = \lambda_k I + N_l.$$

And we can calculate e^J as

$$e^J = \begin{pmatrix} e^{J_1} & & \\ & \ddots & \\ & & e^{J_K} \end{pmatrix},$$

where, with I and N_l commute,

$$e^{J_k} = e^{\lambda_k I + N_l} = e^{\lambda_k I} e^{N_l} = e^{\lambda_k} e^{N_l} = e^{\lambda_k} \sum_{j=0}^{l-1} \frac{N^j}{j!},$$

where the summation only goes to $l-1$ since we can calculate

$$N_l = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}, N_l^2 = \begin{pmatrix} 0 & 0 & 1 & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & \ddots & 0 \\ & & & & 0 \end{pmatrix}, \cdots, N_l^{l-1} = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ & \ddots & \ddots & \vdots \\ & & \ddots & 0 \\ & & & 0 \end{pmatrix}.$$

Corollary 9.2.1. $\det e^A = e^{\operatorname{tr} A}$.

Proof. With Jordan canonical form, $A = SJS^{-1}$ and $e^A = Se^J S^{-1}$. Thus, we have

$$\det e^A = \det e^J = \prod_{j=1}^n e^{\lambda_j} = e^{\sum_{j=1}^n \lambda_j} = e^{\operatorname{tr} A}.$$

□

Theorem 9.2.2. *The eigenvalues depend continuously on the matrix in the sense: If* $\lim_{n\to\infty} A_n = A$, *then* $\sigma(A_n) \to \sigma(A)$, *i.e., for every* $\varepsilon > 0$, *there exists* $N > 0$ *such that for* $\forall n \geq N$, *all eigenvalues of* A_n *are contained in the neighborhood of eigenvalues of* A *with radius* ε.

Proof. $p_\lambda(A) = \det(\lambda I - A) = 0$ and roots of polynomials depend continuous on the coefficients. □

Theorem 9.2.3. *Let $A(t)$ be differentiable. Suppose $A(0)$ has an eigenvalue λ_0 of multiplicity one. Then for t small enough, $A(t)$ has an eigenvalue $\lambda(t)$ that depends differentiably on t and $\lambda(0) = \lambda_0$.*

Proof. Let $p(\lambda, t) = \det(\lambda I - A(t))$. The assumption that λ_0 is a simple root of $p(s, 0)$ implies

$$\begin{aligned} p(\lambda_0, 0) &= 0 \\ \frac{\partial}{\partial \lambda} p(\lambda_0, 0) &\neq 0 \end{aligned}$$

and from the implicit function theorem, the equation $p(\lambda, t) = 0$ has a solution $\lambda = \lambda(t)$ in a neighborhood of $t = 0$ that depends differentiably on t. □

9.3 Simple Eigenvalues

Theorem 9.3.1. *Let $A(t)$ be differentiable and $\lambda(t)$ is a continuous function such that $\lambda(t)$ is an eigenvalue of $A(t)$ with multiplicity 1. Then there exists eigenvector function $v(t)$ which depends differentiably on t.*

Proof. We need a lemma to prove the theorem.

Lemma 9.3.2. *Let A be an $n \times n$ matrix, $p = p_A$ be its characteristic polynomial and λ be some simple root of p. Then at least one of the $(n-1) \times (n-1)$ principle minors of $A - \lambda I$ has nonzero determinant. Moreover, suppose the i-th principal minor of $A - \lambda I$ has nonzero determinant, then the i-th component of an eigenvector v of A corresponding to the eigenvalue λ is nonzero.*

Proof. Without losing generality, and assume $\lambda = 0$. Hence $p(0) = 0, p'(0) \neq 0$. We write $A = (c_1, \cdots, c_n)$ and denote $e_1, \cdots, e_n$ the standard unit vectors. Then we have

$$sI - A = (se_1 - c_1, \cdots, se_n - c_n).$$

Hence, we have

$$\begin{aligned} p'(0) &= \sum_{j=1}^{n} \det(-c_1, \cdots, -c_{j-1}, e_j, -c_{j+1}, \cdots, -c_n) \\ &= (-1)^{n-1} \sum_{j=1}^{n} \det A_j \end{aligned}$$

where A_j is j-th principle minor of A. Since $p'(0) \neq 0$, then at least one of $\det A_j$ is nonzero.

Now suppose the i-th principal minors of A has nonzero determinant. Denote by v_i the eigenvector obtained by omitting i-th component, and by A_i the i-th principle minor of A. Then v_i satisfies $A_i v_i = 0$. Since $\det A_i \neq 0$, we have $v_i = 0$, and hence $v = 0$, which is the eigenvector without omitting i-th component. This is a contradiction. □

Now we prove the theorem. Suppose $\lambda(0) = 0$, and $\det A_i(0) \neq 0$. Then for any t small enough, we have $\det(A_i(t) - \lambda(t)I) \neq 0$ and hence the i-th component of $v(t)$ is not equal to 0. We set it to 1 in order to normalize $v(t)$. For the remaining components, we have an inhomogeneous system of equations

$$(A_i(t) - \lambda(t)I)\, v_i(t) = -c_i^{(i)}(t),$$

where $c_i^{(i)}(t)$ is the vector obtained from i-th column of $A_i(t) - \lambda(t)I$, c_i by omitting the i-th component. So we have

$$v_i(t) = -\left(A_i(t) - \lambda(t)I\right)^{-1} c_i^{(i)}(t).$$

Since all terms on the right hand side depend differentiably on t, so does $v_i(t)$ and $v(t)$. $\square$

Now we consider the derivative of the eigenvalue $\lambda(t)$ and the eigenvector $v(t)$ of a matrix function $A(t)$ when $\lambda(t)$ is a simple root of the characteristic polynomial of $A(t)$. We consider $Av = \lambda v$, then we differentiate with respect to t:

$$\dot{A}v + A\dot{v} = \dot{\lambda}v + \lambda\dot{v}.$$

Let u be an eigenvector of A^T such that $A^T u = \lambda u$. If $(u, v) \neq 0$, then we have

$$(u, \dot{A}v) = \dot{\lambda}(u, v) \;\Rightarrow\; \dot{\lambda} = \frac{(u, \dot{A}v)}{(u, v)}.$$

Lemma 9.3.3. *Let λ be an eigenvalue of A with multiplicity 1, such that $Av = \lambda v, A^T u = \lambda u, uv \neq 0$, then $(u, v) \neq 0$.*

Proof. If $(u, v) = 0$, and $u \in N_{(A^T - \lambda I)}$, then we have

$$v \in N_{(A^T - \lambda I)}^{\perp} = R_{(A - \lambda I)},$$

which implies there exists $w \neq 0$, such that $(A - \lambda I)w = v$. Then w is an genaralized eigenvector, which is contradicted to the fact that λ is multiplicity 1. $\square$

Chapter 10

Matrix Inequalities

10.1 Positive Self-adjoint Matrix

Definition 10.1.1. *A self-adjoint linear mapping H is called positive if*

$$(x, Hx) > 0, \text{ for all } x \neq 0.$$

We write $H > 0$. Similarly, we can define $H < 0, H \geq 0$ and $H \leq 0$.

Now we discuss some basic properties of positive mapping.

Theorem 10.1.1.

(i) *The identity $I > 0$.*

(ii) *If $A, B > 0$, then $A + B > 0$.*

(iii) *If $A > 0, k > 0$, then $kA > 0$.*

(iv) *If $H > 0$ and Q is invertible, then $Q^*HQ > 0$.*

(v) *$H > 0$ if and only if all its eigenvalues are positive.*

(vi) *$H > 0$, then H is invertible.*

(vii) *$H > 0$, then there exists a unique $S > 0$ such that $S^2 = H$.*

Proof.

(iv) $(x, Q^*HQx) = (Qx, HQx) > 0$.

(vii) $H > 0$, then H can be diagonalized by a unitary matrix U such that $U\Lambda U^*$, where

$$\Lambda = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Define $S = U \begin{pmatrix} \sqrt{\lambda_1} & & \\ & \ddots & \\ & & \sqrt{\lambda_n} \end{pmatrix} U^*$, then $S^2 = H$.

Now we need to prove that S is unique. Suppose there exists T such that $T^2 = H, T > 0$, then we have

$$\begin{aligned} (x, (S+T)(S-T)x) &= (x, (TS - ST)x) \\ &= (x, TSx) - (x, STx) \\ &= (Tx, Sx) - (Sx, Tx). \end{aligned}$$

Then $\operatorname{Re}(x, (S+T)(S-T)x) = 0$. Pick x to be eigenvector of $S - T$ such that $(S-T)x = \mu x$, then we have

$$\operatorname{Re} \mu(x, (S+T)x) = 0,$$

which implies $\mu = 0$. Thus, all eigenvalues of $S - T$ are zero, hence $S = T$.

□

Proposition 10.1.1.

(i) $M_1 < N_1, M_2 < N_2$, *then* $M_1 + M_2 < N_1 + N_2$.

(ii) $L < M, M < N$, *then* $L < M$.

Theorem 10.1.2. *If* $M > N > 0$, *then* $0 < M^{-1} < N^{-1}$.

Proof.
Method I. If $N = I, M > I$, then $M^{-1} < I$. Now turn to any matrix N. Let $R = \sqrt{N} > 0$, then we have $M > R^2$. Then

$$\begin{aligned} R^{-1}MR &> I \\ \Rightarrow \left(R^{-1}MR\right)^{-1} &< I \\ \Rightarrow RM^{-1}R^{-1} &< I \\ \Rightarrow M^{-1} &< \left(R^2\right)^{-1} = N^{-1}. \end{aligned}$$

Method II. Define $A(t) = tM + (1-t)M$, and for any $t \in [0,1]$, $A(t) > 0$. And we have

$$\frac{\mathrm{d}}{\mathrm{d}t} A^{-1}(t) = -A^{-1}\dot{A}A^{-1} = -A^{-1}(M-N)A^{-1} < 0.$$

Also, $A^{-1}(0) = N^{-1}$ and $A^{-1}(1) = M^{-1}$. For any $x \in \mathbb{C}^n, x \neq 0$, we have

$$\begin{aligned} \left(x, \frac{\mathrm{d}}{\mathrm{d}t} A^{-1}(t)x\right) &= \frac{\mathrm{d}}{\mathrm{d}t}\left(x, A^{-1}(t)x\right) < 0 \\ \left(x, A^{-1}(0)x\right) &= \left(x, N^{-1}x\right) \\ \left(x, A^{-1}(1)x\right) &= \left(x, M^{-1}x\right) \end{aligned}$$

then we have $(x, N^{-1}x) > (x, M^{-1}x)$. Thus, $(x, (N^{-1} - M^{-1})x) > 0$, which implies $M^{-1} < N^{-1}$. □

Theorem 10.1.3. *Let $A^* = A, B^* = B$, and $A > 0, AB + BA > 0$. Then, $B > 0$.*

Proof. Define $B(t) = B + tA$, and $S(t) = AB(t) + B(t)A = AB + BA + 2tA^2 > 0$. If $B = B(0)$ is not positive, then there exists $t_0 \geq 0$ such that $B(t_0)$ is not positive while $B(t) > 0$ for all $t > t_0$. Then, $0 \in \sigma(B(t_0))$.

Let $x \neq 0$, $B(t_0)x = 0$, then $(x, S(t_0)x) = (x, AB(t_0)x) + (x, B(t_0)Ax) = 0$. This is a contradiction. $\square$

Theorem 10.1.4. *$M > N > 0$, then $\sqrt{M} > \sqrt{N} > 0$.*

Proof. Let $A(t) = tM + (1-t)N > 0$, and $R(t) = \sqrt{A(t)} > 0$. Then we have

$$\dot{A} = \dot{R}R + R\dot{R} = N - M > 0.$$

Hence, $\dot{R} > 0$, which implies $R(0) < R(1)$, i.e., $\sqrt{N} < \sqrt{M}$. $\square$

For any $A > 0$, we can write $A = U\Lambda U^*, \Lambda > 0$. We can define

$$\log A = U \log(\Lambda) U^*.$$

If $\Lambda = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$, then $\log(\Lambda) = \begin{pmatrix} \log \lambda_1 & & \\ & \ddots & \\ & & \log \lambda_n \end{pmatrix}$.

Lemma 10.1.5. *For any $A > 0$,*

$$\log A = \lim_{m\to\infty} m\left(A^{\frac{1}{m}} - 1\right).$$

Proof. We need to check $\log \lambda = \lim_{m\to\infty} m\left(\lambda^{1/m} - 1\right)$ for any $\lambda > 0$. Indeed,

$$\lim_{m\to\infty} m\left(\lambda^{\frac{1}{m}} - 1\right) = \lim_{x\to 0^+} \frac{\lambda^x - 1}{x} = \lim_{x\to 0^+} \frac{\log \lambda \lambda^x}{1} = \log \lambda.$$

Then we have

$$m\left(A^{\frac{1}{m}} - 1\right) =$$

$\square$

Bibliography

[1] amd (`https://math.stackexchange.com/users/265466/amd`). Proof of rank property: $XAY = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$. Mathematics Stack Exchange. `https://math.stackexchange.com/q/3352606(version:2019-09-11)`.

[2] Sheldon Axler. *Linear Algebra Done Right.* Springer International Publishing, Cham, 3rd 2015. edition, 2015.

[3] Jonathan S. Golan. The Linear Algebra a Beginning Graduate Student Ought to Know. *Dordrecht: Kluwer Academic*, 2004.

[4] R. Piziak and P. L. Odell. Full rank factorization of matrices. *Mathematics Magazine*, 72(3):193–201, 1999.

[5] David (`https://math.stackexchange.com/users/117084/david`). Frobenius inequality. Mathematics Stack Exchange. `https://math.stackexchange.com/q/2668713` (version: 2019-12-18).

[6] Wolfy (`https://math.stackexchange.com/users/217910/wolfy`). Full rank factorization. Mathematics Stack Exchange. `https://math.stackexchange.com/q/1784831` (version: 2016-05-14).

[7] Sugata Adhya (`https://math.stackexchange.com/users/36242/sugata-adhya`). Prove that $\operatorname{rank}(ab) \geq \operatorname{rank}(a) + \operatorname{rank}(b) - n$. Mathematics Stack Exchange. `https://math.stackexchange.com/q/269548` (version: 2013-01-03).

[8] Fuzhen Zhang. Linear Algebra : Challenging Problems for Students. *Mathematics Faculty Books and Book Chapters*, (4), January 2009.