Notes on Linear Algebra

Ching-Cheong Lee

Contents

Chapter 1

Linear Systems, Matrices and Determinants

Linear algebra is, roughly speaking, the study of linear transformations between finite dimensional vector spaces. A solid understanding of the subject arguably lead to the success in learning more advanced subject for which "linear spaces" is the object of interest. The central concept of linear algebra can be visualized and easily understood through examples in $\mathbb{R}^n$, in particular, let's start system of linear equations.

1.1 Linear Systems

Given $b_i, a_{ij} \in \mathbb{R}$, $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$ (possibly $m \neq n$), the following

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{1.1.1}$$

is called a system of linear equations with n unknowns. We interpret the brace "{" as "and".

Example 1.1.2.

$$\begin{cases} x + y = 1 \\ x - y = 2 \end{cases}$$

is a system of linear equations with 2 unknowns. This system has exactly 1 solution $(x, y) = (\frac{3}{2}, -\frac{1}{2})$.

Example 1.1.3. Consider the system:

$$(*) \quad \begin{cases} 2x + 2y = 4 \\ x + y = 2 \end{cases}$$

Of course we know that two equations are the same, hence we have just 1 equation with 2 unknowns. It should seem natural to us that this system has infinitely many solutions.

Indeed, fix $y = t \in \mathbb{R}$, then $x + y = 2$ implies $x = 2 - t$, hence $(x, y) = (2 - t, t)$ is the only solution (for each t). Note that t can be arbitrarily fixed, we conclude

$$\{(2 - t, t) : t \in \mathbb{R}\}$$

is the collection of all solutions of the system $(*)$.

Example 1.1.4. Consider the system:

$$\begin{cases} x + y = 1 \\ -x - y = 1 \end{cases}$$

Suppose it does have a solution, then we add two equations to get $0 = 2$, this is impossible, hence the system cannot have any solution.

The above is a few examples to illustrate the general phenomenon that we will study for linear systems. We will study whether or not a system **(i) has exactly one solution; (ii) has infinitely many solutions; (iii) has no solution.**

Definition 1.1.5. A linear system is said to be **consistent** if it has at least one solution; otherwise it is said to be **inconsistent**.

Only coefficients are important in computing the solution(s) of a system, we introduce the matrix notation in order to simplify our work.

Definition 1.1.6. The rectangularly arranged array

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

is called a **matrix**. Bringing the system (2.2.2) into consideration, the above matrix is called the **coefficient matrix** of the system. While the matrix

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_n \end{array}\right]$$

is called the **augmented matrix** of the system.

Example 1.1.7. We try to determine value of h such that the following system is consistent

$$\begin{cases} x + y = 1 \\ 2x + 2y = h \end{cases}$$

We adopt the following notations. By

$$R_i \to aR_i + bR_j$$

we mean the ith row of the matrix is replaced by $a \times$ (ith row) $+ b \times$ (jth row). Also by

$$R_i \leftrightarrow R_j$$

we mean we interchange the ith row and the jth row of the matrix.

We perform row operations on the augmented matrix.

$$\left[\begin{array}{cc|c} 1 & 1 & 1 \\ 2 & 2 & h \end{array}\right] \xrightarrow{R_2 \to R_2 - 2\times R_1} \left[\begin{array}{cc|c} 1 & 1 & 1 \\ 0 & 0 & h-2 \end{array}\right],$$

this is consistent only when $h = 2$ (otherwise we get an absurd that $0 \neq 0$).

Example 1.1.8. We solve the system

$$\begin{cases} x + y + 2z + w = 5 \\ x + y + 2z + 6w = 10 \\ x + 2y + 5z + 2w = 7 \end{cases}$$

by doing row operations on the augmented matrix.

$$\left[\begin{array}{cccc|c} 1 & 1 & 2 & 1 & 5 \\ 1 & 1 & 2 & 6 & 10 \\ 1 & 2 & 5 & 2 & 7 \end{array}\right] \xrightarrow[R_3 \to R_3 - R_1]{R_2 \to R_2 - R_1} \left[\begin{array}{cccc|c} 1 & 1 & 2 & 1 & 5 \\ 0 & 0 & 0 & 5 & 5 \\ 0 & 1 & 3 & 1 & 2 \end{array}\right]$$

$$\xrightarrow[R_3 \to \frac{1}{5}R_3]{R_2 \leftrightarrow R_3} \left[\begin{array}{cccc|c} 1 & 1 & 2 & 1 & 5 \\ 0 & 1 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow[R_2 \to R_2 - R_3]{R_1 \to R_1 - R_2} \left[\begin{array}{cccc|c} 1 & 0 & -1 & 0 & 3 \\ 0 & 1 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

The original system is reduced to:

$$\begin{cases} x \quad - z = 3 \\ y + 3z = 1 \\ w = 1 \end{cases}$$

Solving backward, we have $w = 1$, $y = 1 - 3z$ and $x = 3 + z$. Here we may fix $z = t$ (conventionally), then

$$\{(3 + t, 1 - 3t, t, 1) : t \in \mathbb{R}\}$$

forms a collection of solutions of the system in this example.

Definition 1.1.9. If two systems have the same set of solutions, we say two systems are **equivalent**.

In the previous examples we have seen that a system can be solved by:

(i) Interchange 2 equations.

(ii) Multiply an equation by a nonzero constant.

(iii) Add one equation by another equation.

Clearly each of the above operations is reversible, which means that the solution(s) of a system will not be altered under these operations. Put in other way, (i), (ii) and (iii) produces equivalent systems.

Definition 1.1.10. A matrix is in **row echelon form** if

(i) All nonzero rows are above any zero rows (that is to say, all zero rows, if any, belong at the bottom of the matrix).

(ii) The **leading coefficient**$^{(*)}$ of a nonzero row is always strictly to the right of the leading coefficient of the row above it.

(iii) All entries in a column below a leading entry are zeroes (implied by the first two criteria).

Definition 1.1.11. A matrix is in **reduced row echelon form** if it satisfies:

(i) All nonzero rows are above any rows of all zeroes.

(ii) The leading coefficient of a nonzero row is always strictly to the right of the leading coefficient of the row above it.

(iii) Every leading coefficient is 1 and is the only nonzero entry in its column.

Example 1.1.12. Consider two matrices:

$$A = \begin{bmatrix} 2 & 2 & 3 & 4 \\ 0 & 3 & 4 & 6 \\ 0 & 0 & 0 & 5 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & \mathbf{0} & 3 & \mathbf{0} \\ 0 & 1 & 4 & \mathbf{0} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

A is in row echelon form and B is in reduced row echelon form.

Definition 1.1.13.

(i) For an echelon form, a column containing a pivot (there is at most one) is called a **pivot column**.

(ii) If the ith column of an echelon form *of the coefficient matrix of a system* is a pivot column, then the corresponding ith variable is called a **basic variable**.

(iii) If the ith column of an echelon form *of the coefficient matrix of a system* is not a pivot column, then the corresponding ith variable it is called a **free variable**.

Example 1.1.14. Reconsider coefficient matrix of Example 1.1.8, $A = \left[\begin{smallmatrix} 1 & 1 & 2 & 1 \\ 1 & 1 & 2 & 6 \\ 1 & 2 & 5 & 2 \end{smallmatrix}\right]$. By the solution of Example 1.1.8, we have row reduced A to:

$$\begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Thus the 1st, 2nd and 4th columns of the reduced row echelon form of A are pivot columns.

Consider the system $Ax = b$, for some $b \in \mathbb{R}^3$, since

$$\left[\begin{array}{cccc|c} 1 & 1 & 2 & 1 & b_1 \\ 1 & 1 & 2 & 6 & b_2 \\ 1 & 2 & 5 & 2 & b_3 \end{array}\right] \to \cdots \to \left[\begin{array}{cccc|c} \boxed{1} & 0 & -1 & 0 & * \\ 0 & \boxed{1} & 3 & 0 & * \\ 0 & 0 & 0 & \boxed{1} & * \end{array}\right],$$

here $*$ means some numbers. Since the first, second and forth columns of the row reduced coefficient matrix are pivot columns, therefore x_1, x_2, x_4 are basic variables. The rest, x_3, is a free variable.

$^{(*)}$ The first nonzero number from the left, also called the **pivot**.

The computational experience shows us

$$\# \text{ of columns of coefficient matrix} = \# \text{ of basic variables} + \# \text{ of free variables},$$

also,

$$\begin{aligned}
\# \text{ of basic variables} &= \# \text{ of nonzero rows in echelon form of cofficient matrix} \\
&= \# \text{ of pivots in echelon form of coefficient matrix} \\
&\le \min \left\{ \begin{array}{c} \# \text{ of rows of coefficient matrix,} \\ \# \text{ of columns of coefficient matrix} \end{array} \right\}.
\end{aligned}$$

Theorem 1.1.15. *A homogeneous system of linear equations has a unique solution if and only if there is no free variable.*

Proof. Let's for the moment take it for granted. This statement will be trivial after we have some familiarity with section 2.8. □

Remark. Reconsider Example 1.1.8, since z is a free variable, the solution set can be expressed in terms of z, with $z \in \mathbb{R}$ being arbitrary. This demonstrates if a free variable exists, there will be infinitely many solutions.

On the other hand, if there is no free variable, then every variable will be basic variable, namely, the linear system has at most one solution.

Given a set of linear equations

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m, \end{cases}$$

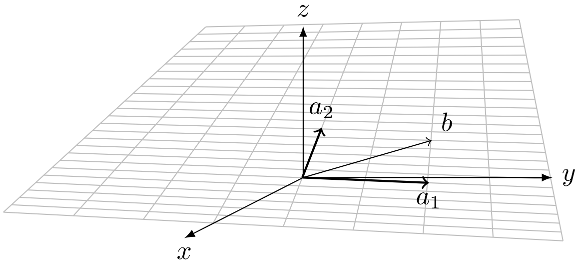
if we define

$$a_1 = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix}, \quad a_2 = \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix}, \quad \ldots, \quad \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix},$$

then the above system of linear equations can be neatly written as

$$x_1a_1 + x_2a_2 + \cdots + x_na_n = b.$$

This equation has a nice geometric interpretation. When $m = 3$ and $n = 2$, the solvability of the above equation is the same as whether or not b is in the plane in $\mathbb{R}^3$ "created" by a_1 and a_2:



$$\boxed{b = a_1 + \frac{5}{6}a_2}$$

This observation enables us to have **three equivalent ways to view a linear system**:

(i) A system of linear equations;

(ii) As a vector equation $x_1a_1 + x_2a_2 + \cdots + x_na_n = b$;

(iii) As a matrix equation $Ax = b$.

1.2 Matrix Operations

1.2.1 Basic Definitions

Convention. Every element $v \in \mathbb{R}^n$ will always be a **column vector**. Moreover, the ith coordinate is usually denoted by v_i.

Definition 1.2.1. We write $A \in M_{m\times n}(\mathbb{R})$ if A is an $m \times n$ matrix. Moreover, if A is expressed as

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},$$

we denote $A = [a_{ij}]_{m\times n}$, which means that i runs through $\{1, 2, \ldots, m\}$ and j runs through $\{1, 2, \ldots, n\}$. By convention a 1×1 matrix is regarded as a real number, namely, $M_{1\times 1}(\mathbb{R}) = \mathbb{R}$.

Definition 1.2.2. The multiplication of matrices is defined as follows:

$$\underbrace{\begin{bmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mp} \end{bmatrix}}_{m\times p} \underbrace{\begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{p1} & \cdots & b_{pn} \end{bmatrix}}_{p\times n} = [c_{ij}]_{m\times n},$$

where $c_{ij} = \sum_{k=1}^{p} a_{ik}b_{kj}$.

Before giving examples, we mention a few computational facts. Let matrices $A \in M_{m\times p}(\mathbb{R})$ and $B \in M_{p\times n}(\mathbb{R})$, B can be written as

$$B = [b_1 \quad \cdots \quad b_n],$$

where $b_i \in \mathbb{R}^p$, hence by definition of matrix multiplication, we have the following computational formula

$$AB = A[b_1 \quad \cdots \quad b_n] = [Ab_1 \quad \cdots \quad Ab_n]. \tag{1.2.3}$$

So to compute two big matrices, we need to know how to compute Ax, where $x \in \mathbb{R}^p$. Again by definition of matrix multiplication, if we write

$$A = [a_1 \quad \cdots \quad a_p],$$

where $a_i \in \mathbb{R}^m$, then

$$Ax = [a_1 \quad \cdots \quad a_p] \begin{bmatrix} x_1 \\ \vdots \\ x_p \end{bmatrix} = x_1a_1 + x_2a_2 + \cdots + x_pa_p. \tag{1.2.4}$$

The formula (1.2.3) and (1.2.4) will suffice to do all computation we need for matrices.

Example 1.2.5. Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}, \quad B = \begin{bmatrix} 7 & 8 \\ 9 & 10 \end{bmatrix}, \quad u = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \quad \text{and} \quad v = \begin{bmatrix} 1 & 1 \end{bmatrix}.$$

We repeatedly use (1.2.3) and (1.2.4) to compute Bu, vA, BA and vBu as follows:

$$\begin{aligned}
Bu &= \begin{bmatrix} 7 & 8 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 7 \\ 9 \end{bmatrix} - \begin{bmatrix} 8 \\ 10 \end{bmatrix} = \begin{bmatrix} -1 \\ -1 \end{bmatrix} \\
vA &= \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} = \left[\begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 6 \end{bmatrix} \right] = \begin{bmatrix} 5 & 7 & 9 \end{bmatrix} \\
BA &= \left[\begin{bmatrix} 7 & 8 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \end{bmatrix} \quad \begin{bmatrix} 7 & 8 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \end{bmatrix} \quad \begin{bmatrix} 7 & 8 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 3 \\ 6 \end{bmatrix} \right] \\
&= \left[\begin{bmatrix} 7 \\ 9 \end{bmatrix} + 4 \begin{bmatrix} 8 \\ 10 \end{bmatrix} \quad 2 \begin{bmatrix} 7 \\ 9 \end{bmatrix} + 5 \begin{bmatrix} 8 \\ 10 \end{bmatrix} \quad 3 \begin{bmatrix} 7 \\ 9 \end{bmatrix} + 6 \begin{bmatrix} 8 \\ 10 \end{bmatrix} \right] \\
&= \begin{bmatrix} 39 & 54 & 69 \\ 49 & 68 & 87 \end{bmatrix}
\end{aligned}$$

and finally

$$vBu = v(Bu) = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} -1 \\ -1 \end{bmatrix} = -1 - 1 = -2.$$

Recall that a 1×1 matrix is considered as a number. This will be found convenient in application.

The computation of vBu might be ambiguous, why does $vBu = v(Bu)$? Can't it be $(vB)u$? Are they necessarily the same? This can be explained by the properties (specifically, the associativity) of matrix multiplication which we summarize below:

Proposition 1.2.6 (Algebraic Properties of Matrix Operations).

(i) $A + B = B + A$ ***(Commutativity of Addition)***

(ii) $(A + B) + C = A + (B + C)$ ***(Associativity of Addition)***

(iii) $(AB)C = A(BC)$ ***(Associativity of Multiplication)***

(iv) $A(B + C) = AB + AC$ *and* $(B + C)A = BA + CA$ ***(Distributive Law)***

(v) $A(aB) = (aA)B = aAB$ *for any* $a \in \mathbb{R}$

Proof. In the following we let $A = [a_{ij}]_{n\times n} = [a_1 \quad a_2 \quad \cdots \quad a_n]$ and define B and C similarly. We shall omit the subscript $n \times n$ to A, B and C for convenience.

(i) $A + B = [a_{ij}] + [b_{ij}] := [a_{ij} + b_{ij}] = [b_{ij} + a_{ij}] = [b_{ij}] + [a_{ij}] = B + A$.

(ii) Similar to (i)

(iii) We use the computational fact (1.2.3). The ith column of the the matrix $(AB)C$ is $(AB)c_i$. While that of $A(BC) = A\,[Bc_1 \quad \cdots \quad Bc_n]$ is also ABc_i.

(iv) $A(B + C) = [a_{ij}][b_{ij} + c_{ij}] = [\sum_{k=1}^n a_{ik}(b_{kj} + c_{kj})] = [\sum_{k=1}^n a_{ik}b_{kj}] + [\sum_{k=1}^n a_{ik}c_{kj}] = AB + BA$. The fact that $(B + C)A = BA + CA$ can be proved similarly.

(v) If also follows from the computational fact (1.2.3). $\square$

Corollary 1.2.7 (Linearity). *Let $A \in M_{m\times n}(\mathbb{R})$, the function $T : \mathbb{R}^n \to \mathbb{R}^m$ defined by $T(x) = Ax$ is **linear** in the sense that*

$$A(x+y) = Ax + Ay \quad \text{and} \quad A(\alpha x) = \alpha Ax, \text{ for any } \alpha \in \mathbb{R}.$$

Next we introduce usual notations and terminologies for some important matrices. The **zero matrix** is

$$\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix},$$

denoted by $\mathbf{0}$ or $\mathcal{O}$. The **identity matrix** in $M_{n\times n}(\mathbb{R})$ is

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

where only the diagonal elements are nonzero, denoted by I_n or simply I.

Definition 1.2.8. Given a matrix $A = [a_{ij}]_{m\times n}$ (possibly $m \neq n$), we define

$$A^T = [b_{ij}]_{n\times m},$$

where $b_{ij} = a_{ji}$.

Example 1.2.9. Given matrices

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

We $A = [a_{ij}]_{2\times 3}$ and $b_{ij} = a_{ji}$, then

$$A^T := [b_{ij}]_{3\times 2} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}.$$

With the experience in computing A^T, we observe that if

$$C = \begin{bmatrix} \text{———} c_1^T \text{———} \\ \vdots \\ \text{———} c_m^T \text{———} \end{bmatrix},$$

where $c_i \in \mathbb{R}^n$, then C is an $m \times n$ matrix, whose transpose C^T is given by

$$C^T = \begin{bmatrix} | & | & & | \\ c_1 & c_2 & \cdots & c_m \\ | & | & & | \end{bmatrix},$$

hence

$$B^T = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}.$$

Another way to compute the transpose of a square matrix is to reflect all its entry along the diagonal.

Definition 1.2.10. Let a square matrix $A = [a_{ij}]_{n\times n}$ be given.

(i) A is said to be **diagonal** if $i \neq j \implies a_{ij} = 0$.

(ii) A is said to be **upper triangular** if $j < i \implies a_{ij} = 0$.

(iii) A is said to be **lower triangular** if $j > i \implies a_{ij} = 0$.

(iv) A is said to be **symmetric** if $a_{ij} = a_{ji}$ for every i, j, i.e., $A^T = A$.

(v) A is said to be **skew-symmetric** if $a_{ij} = -a_{ji}$ for every i, j, i.e., $A^T = -A$.

Example 1.2.11. Consider the matrices:

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 2 & 0 & -1 \end{bmatrix} \quad \text{and} \quad D = \begin{bmatrix} 0 & 2 & -1 \\ -2 & 0 & -3 \\ 1 & 3 & 0 \end{bmatrix}$$

(i) Which is diagonal?

(ii) Which is upper triangular?

(iii) Which is lower triangular?

(iv) Which is symmetric?

(v) Which is skew-symmetric?

(i) Only B is diagonal; (ii) Only A and B are upper triangular; (iii) Only B and C are lower triangular; (iv) Only B is symmetric; (v) Only D is skew-symmetric.

Proposition 1.2.12 (Properties of Transpose). *Given $A, B \in M_{n\times n}(\mathbb{R})$ and $c \in \mathbb{R}$, we have*

$$(AB)^T = B^T A^T, \quad (A+B)^T = A^T + B^T, \quad (cA)^T = cA^T \quad \text{and} \quad (A^T)^{-1} = (A^{-1})^T.$$

Proof. Write $A = [a_{ij}], B = [a_{ij}], A^T = [a'_{ij}]$ and $B^T = [b'_{ij}]$, then $[AB] = [\sum_{k=1}^n a_{ik}b_{kj}]$, it follows that

$$(AB)^T = \left(\left[\sum_{k=1}^n a_{ik}b_{kj}\right]_{n\times n}\right)^T = \left[\sum_{k=1}^n a_{jk}b_{ki}\right]_{n\times n} = \left[\sum_{k=1}^n b'_{ik}a'_{kj}\right] = B^T A^T,$$

we leave the rest as exercises. □

Theorem 1.2.13. *Let A be a real square matrix, then*

(i) $(A + A^T)/2$ is symmetric.

(ii) $(A + A^T)/2 = A$ iff A is symmetric.

(iii) $(A - A^T)/2$ is skew symmetric.

(iv) $(A - A^T)/2 = A$ iff A is skew symmetric.

Proof. This follows directly from Proposition 1.2.12. □

Started from chapter 2 we will consider real and complex vector spaces at the same time, therefore we will also need terminology for complex matrices.

Definition 1.2.14. For a matrix $A \in M_{n\times n}(\mathbb{C})$, write $[a_{ij}]$, we define $\overline{A} = [\overline{a_{ij}}]$. The **conjugate transpose** of A is defined by

$$A^* = \overline{A}^T$$

A matrix A is said to be **Hermitian** if $A^* = A$.

We will see that the matrix A^* on $\mathbb{C}^n$ play the same role as a matrix A^T on $\mathbb{R}^n$. This will be made apparent when "dot product" on $\mathbb{R}^n$ and $\mathbb{C}^n$ are defined respectively. Now Proposition 1.2.12 can be translated to conjugate transpose.

Proposition 1.2.15 (Properties of Conjugate Transpose). *Given $A, B \in M_{n\times n}(\mathbb{R})$ and $c \in \mathbb{C}$, we have*

$$(AB)^* = B^*A^*, \quad (A+B)^* = A^* + B^*, \quad (cA)^* = \bar{c}A^* \quad \textit{and} \quad (A^*)^{-1} = (A^{-1})^*.$$

Proof. By taking $\overline{\cdot}$ on both sides of the first three equalities in Proposition 1.2.12 we get respectively the first three equalities in Proposition 1.2.15. For the last one, we take conjugate transpose on both sides of $AA^{-1} = I$. ☐

1.2.2 Elementary Matrices

We notice that:

multiply the 3rd row by constant k

$$\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & k\end{bmatrix}\begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix} = \begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ ka_{31} & ka_{32} & ka_{33}\end{bmatrix}$$

add the 2nd row to 1st row

$$\begin{bmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix} = \begin{bmatrix}a_{11}+a_{21} & a_{12}+a_{22} & a_{13}+a_{23}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix}$$

$$\begin{bmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{bmatrix}\begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix} = \begin{bmatrix}a_{21} & a_{22} & a_{23}\\ a_{11} & a_{12} & a_{13}\\ a_{31} & a_{32} & a_{33}\end{bmatrix}$$

switch the 1st and 2nd row

Multiplying those kinds of matrices on the left results in elementary operations. Because of that these matrices bear a special name.

Definition 1.2.16. Let R_i denote the ith row of an identity matrix I. Every matrix obtained from I by one of the following operations:

(i) Multiplying the row R_i by a constant.

(ii) Replacing R_i by $R_i + R_j$.

(iii) Switching R_i and R_j.

is called an **elementary matrix**.

As what we observe, multiplying a matrix A (not necessarily square!) on the left by an elementary matrix obtained by doing (i), (ii) or (iii) on I will result in a matrix A' obtained by doing (i), (ii) and (iii) respectively on A.

These observations enable us to observe the following:

Theorem 1.2.17. *For every matrix A, there are elementary matrices $E_1, E_2, \ldots, E_k$ such that*

$$E_k \cdots E_2 E_1 A$$

is in reduced echelon form.

Proof. This follows from the algorithm that always enables us to reduce a matrix into reduced row echelon form by row operations. □

1.2.3 Compute Inverse by Row Operations

Definition 1.2.18. $A \in M_{n\times n}(\mathbb{R})$ is said to be **invertible** if there is a matrix $B \in M_{n\times n}(\mathbb{R})$ such that $BA = AB = I_n$. In this case B is called the **inverse of A**, denoted by A^{-1}.

Remark. It is easy to prove that for $A, B \in M_{n\times n}(\mathbb{R})$,

$$AB = I \iff BA = I,$$

hence to show a matrix B is an inverse of A, it is enough to check one of equalities: $BA = I$ or $AB = I$.

Theorem 1.2.19. *If A is invertible and*

$$\begin{bmatrix} A \mid I \end{bmatrix} \to \cdots \to \begin{bmatrix} I \mid B \end{bmatrix}$$

under finitely many row operations, then $B = A^{-1}$.

Proof. Since A is invertible, after finitely many row operations we can reduce it into I. Namely, there are elementary matrices $E_1, E_2, \ldots, E_k$ such that

$$E_k \cdots E_2 E_1 A = I.$$

From that we conclude $E_k \cdots E_2 E_1 = A^{-1}$. Consider

$$\begin{bmatrix} A \mid I \end{bmatrix},$$

after finitely many same row operations we have

$$\begin{bmatrix} A \mid I \end{bmatrix} \to \cdots \to E_k \cdots E_2 E_1 \begin{bmatrix} A \mid I \end{bmatrix} = \begin{bmatrix} I \mid E_k \cdots E_2 E_1 \end{bmatrix} = \begin{bmatrix} I \mid A^{-1} \end{bmatrix}.$$ □

Example 1.2.20. Consider
$$A = \begin{bmatrix} 3 & 2 & 6 \\ 1 & 1 & 2 \\ 2 & 2 & 5 \end{bmatrix},$$
let's compute A^{-1} by row operations. Construct the augmented matrix $\left[A \mid I\right]$ and reduce the left half of this into I.
$$\left[\begin{array}{ccc|ccc} 3 & 2 & 6 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 & 1 & 0 \\ 2 & 2 & 5 & 0 & 0 & 1 \end{array}\right] \xrightarrow{R_1 \leftrightarrow R_2} \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 3 & 2 & 6 & 1 & 0 & 0 \\ 2 & 2 & 5 & 0 & 0 & 1 \end{array}\right]$$
$$\xrightarrow{R_2 \to R_2 - 3R_1} \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & -3 & 0 \\ 2 & 2 & 5 & 0 & 0 & 1 \end{array}\right]$$
$$\xrightarrow{R_3 \to R_3 - 2R_1} \left[\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & -3 & 0 \\ 0 & 0 & 1 & 0 & -2 & 1 \end{array}\right]$$
$$\xrightarrow{R_1 \to R_1 + R_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & -2 & 0 \\ 0 & -1 & 0 & 1 & -3 & 0 \\ 0 & 0 & 1 & 0 & -2 & 1 \end{array}\right]$$
$$\xrightarrow{R_1 \to R_1 - 2R_3} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 2 & -2 \\ 0 & -1 & 0 & 1 & -3 & 0 \\ 0 & 0 & 1 & 0 & -2 & 1 \end{array}\right]$$
$$\xrightarrow{R_2 \to -R_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 2 & -2 \\ 0 & 1 & 0 & -1 & 3 & 0 \\ 0 & 0 & 1 & 0 & -2 & 1 \end{array}\right].$$
So
$$A^{-1} = \begin{bmatrix} 1 & 2 & -2 \\ -1 & 3 & 0 \\ 0 & -2 & 1 \end{bmatrix}.$$

1.2.4 Uniqueness of Reduced Row Echelon Form

Theorem 1.2.21. *The reduced row echelon form of an $m \times n$ matrix is unique.*

Proof. We will prove by induction on n. The case that $n = 1$ is trivial, let's suppose now every $m \times (n-1)$ matrix has unique reduced row echelon form.

Consider an $m \times n$ matrix $A = [A' \quad a]$, $a \in \mathbb{R}^m$. Let $B = [B' \quad b]$ and $C = [C' \quad c]$, $b, c \in \mathbb{R}^m$, be reduced row echelon form of A. Since B', C' are reduced row echelon form of A', by induction hypothesis $B' = C'$. Therefore B and C only differ from the last column.

For the sake of contradiction let's suppose $b \neq c$. Let $Bx = 0$, then due to row equivalence we have $Cx = 0$, therefore
$$(B - C)x = 0 = [O \quad b - c]\, x,$$
where O denotes a zero matrix and $b - c \neq 0$. If we write $x = (x_1, x_2, \ldots, x_n)^T$, then $x_n = 0$. Similarly, $Cx = 0$ implies $x_n = 0$. Which means that b and c must contain a pivot of A, otherwise the system $Ax = 0$ will have x_n as a free variable, meaning that x_n can be arbitrary, not necessarily zero. Since B and C are reduced row echelon form, the pivot 1 must appear in the row of b, c which is the first zero row of $B' = C'$, meaning that $b = c$, a contradiction. □

1.3 Determinants

1.3.1 As The Unique Multilinear Functional

Let $\mathbb{F}$ denote $\mathbb{R}$ or $\mathbb{C}$. Throughout this section all scalars will be over $\mathbb{F}$. We introduce a "multilinear" function on $M_{n\times n}(\mathbb{F})$ which provides us a useful, systematic and mechanical way to determine the invertability of a square matrix (matrices with complex entries will be found important later). This function is denoted by

$$\delta : M_{n\times n}(\mathbb{F}) \to \mathbb{F}.$$

We will require δ satisfy the following properties:

$$\boxed{\begin{array}{rl} \text{(i)} & \delta(I) = 1. \\ \text{(ii)} & \delta(A) \text{ is linear in the rows of } A. \\ \text{(iii)} & \text{If two adjacent rows are equal, } \delta(A) = 0. \end{array}} \tag{1.3.1}$$

We describe δ as "multilinear" due to property (ii).

For example, if δ satisfies (1.3.1), then

$$\delta \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 0 & 1 \end{bmatrix} = 2\delta \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 3\delta \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = 2 \times 1 + 3 \times 0 = 2.$$

We can already compute $\delta(A)$ for some A, it will be seen later that the rules given in (1.3.1) fix the way we compute $\delta(A)$ for any $n \times n$ matrix A, and thereby showing Theorem 1.3.5.

Before arriving to this uniqueness result, we investigate the properties of such "multilinear" functions.

Proposition 1.3.2. *Let $\delta : M_{n\times n}(\mathbb{F}) \to \mathbb{F}$ satisfy properties in (1.3.1), then:*

(i) If A' is obtained from A by adding a multiple of ith row to jth row $(i \neq j)$, then $\delta(A') = \delta(A)$.

(ii) If A' is obtained from A by interchanging ith row and jth row $(i \neq j)$, then $\delta(A') = -\delta(A)$.

(iii) If A' is obtained from A by multiplying the ith row by a constant c, then $\delta(A') = c\delta(A)$.

(iv) If the ith row of A is a multiple of the jth row of A, then $\delta(A) = 0$.

Proof. (iii) This is just linearity of $\delta(A)$ on rows of A. In the sequel we first assume $j = i + 1$, $i < n$ for simplicity.

$$\text{(i) } \delta \begin{bmatrix} \vdots \\ \text{---}R_i\text{---} \\ \text{---}R_j + \alpha R_i\text{---} \\ \vdots \end{bmatrix} = \delta \begin{bmatrix} \vdots \\ \text{---}R_i\text{---} \\ \text{---}R_j\text{---} \\ \vdots \end{bmatrix} + \alpha\delta \begin{bmatrix} \vdots \\ \text{---}R_i\text{---} \\ \text{---}R_i\text{---} \\ \vdots \end{bmatrix}.$$

(ii)

$$\delta \begin{bmatrix} \vdots \\ \text{——}R_j\text{——} \\ \text{——}R_i\text{——} \\ \vdots \end{bmatrix} = \delta \begin{bmatrix} \vdots \\ \text{——}R_j - R_i\text{——} \\ \text{——}R_i\text{——} \\ \vdots \end{bmatrix} = \delta \begin{bmatrix} \vdots \\ \text{——}R_j - R_i\text{——} \\ \text{——}R_j\text{——} \\ \vdots \end{bmatrix}$$

$$= \delta \begin{bmatrix} \vdots \\ \text{——}-R_i\text{——} \\ \text{——}R_j\text{——} \\ \vdots \end{bmatrix} = -\delta \begin{bmatrix} \vdots \\ \text{——}R_i\text{——} \\ \text{——}R_j\text{——} \\ \vdots \end{bmatrix}.$$

(iv) This follows from linearity of $\delta(A)$ on rows of A and property (iii) of (1.3.1).

Now for the general case, (iv) holds immediately by switching rows finitely many times. From that point, the proof in the special case of (i) carries over to the general case, so (i) holds, and hence the proof of the special case of (ii) also carries over to the general case, (ii) also holds. □

Proposition 1.3.3. *$\delta(E)$ takes the following value when E is an elementary matrix that:*

(i) Adds a multiple of a row to another, $\delta(E) = 1$

(ii) Interchanges two rows, $\delta(E) = -1$.

(iii) Multiplies a row by a nonzero constant c, $\delta(E) = c$.

Proof. This follows directly form Proposition 1.3.2. □

Proposition 1.3.4. *If $A \in M_{n\times n}(\mathbb{F})$ and $E \in M_{n\times n}(\mathbb{F})$ is an elementary matrix, then*

$$\delta(EA) = \delta(E)\delta(A).$$

Proof. This follows directly from Proposition 1.3.2 and Proposition 1.3.3. □

Theorem 1.3.5. *There can be at most one function $\delta : M_{n\times n}(\mathbb{F}) \to \mathbb{F}$ satisfying properties in (1.3.1).*

Proof. For every $n\times n$ matrix A, there are elementary matrices such that $E_k \cdots E_2 E_1 A = R$, where R is the reduced row echelon form of A, and hence

$$\delta(E_1)\delta(E_2)\cdots\delta(E_n)\delta(A) = \delta(R)$$

by applying Proposition 1.3.4 finitely many times. Consider the following dichotomy:

- If A is not invertible, R has a zero row at the bottom.
- If A is invertible, $R = I$, the identity matrix.

It follows that when A is not invertible, $\delta(A) = 0$. When A is invertible,

$$\delta(A) = \frac{1}{\delta(E_1)\delta(E_2)\cdots\delta(E_n)},$$

here δ must be computed by formulas in Proposition 1.3.3 whenever δ satisfies properties in (1.3.1). $\square$

To complete the proof that there is a unique function satisfying properties in (1.3.1), we need to show existence. It turns out that properties (1.3.1) itself provide us the formula:

Theorem 1.3.6. *Let $\delta : M_{n\times n}(\mathbb{F}) \to \mathbb{F}$ satisfy properties in (1.3.1), then for $A = [a_{ij}]_{n\times n}$, we have*

$$\delta(A) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Before going into the proof, we need to explain the notations here. By S_n we mean the collection of all bijective maps $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$, i.e., all permutations of the first n positive integers. Also the quantity $\operatorname{sgn}(\sigma)$ will be explained in the proof.

Proof. Let $e_1 = (1, 0, \dots, 0), e_2 = (0, 1, \dots, 0)$ and $e_n = (0, 0, \dots, 1)$, the standard basis of $M_{1\times n}(\mathbb{F})$. We note that by linearity on the first row, second row, ..., and then nth rows, we have

$$\begin{aligned}
\delta\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} &= \delta\begin{bmatrix} & \sum_{j_1=1}^n a_{1j_1} e_{j_1} & \\ a_{21} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = \sum_{j_1=1}^n a_{1j_1} \delta\begin{bmatrix} & e_{j_1} & \\ a_{21} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \\
&= \sum_{j_1=1}^n \sum_{j_2=1}^n a_{1j_1} a_{2j_2} \delta\begin{bmatrix} & e_{j_1} & \\ & e_{j_2} & \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \\
&\vdots \\
&= \sum_{j_1=1}^n \sum_{j_2=1}^n \cdots \sum_{j_n=1}^n a_{1j_1} a_{2j_2} \cdots a_{nj_n} \delta\begin{bmatrix} e_{j_1} \\ e_{j_2} \\ \vdots \\ e_{j_n} \end{bmatrix} \\
&= \sum_{\substack{1\le j_1,\dots,j_n\le n \\ j_i\ne j_k, \forall i\ne k}} a_{1j_1} a_{2j_2} \cdots a_{nj_n} \delta\begin{bmatrix} e_{j_1} \\ e_{j_2} \\ \vdots \\ e_{j_n} \end{bmatrix} \\
&= \sum_{\sigma\in S_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \delta\begin{bmatrix} e_{\sigma(1)} \\ e_{\sigma(2)} \\ \vdots \\ e_{\sigma(n)} \end{bmatrix} \\
&= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)},
\end{aligned}$$

where $\operatorname{sgn}(\sigma) = \delta \begin{bmatrix} e_{\sigma(1)} \\ e_{\sigma(2)} \\ \vdots \\ e_{\sigma(n)} \end{bmatrix}$ is 1 if σ is an even$^{(\dagger)}$ permutation end -1 if σ is an odd permutation. $\square$

Therefore the unique function stated in Theorem 1.3.5 exists. Henceforth we denote $\delta = \det = |\cdot|$ which we call:

Definition 1.3.7. When A is an $n \times n$ matrix, the **determinant** of A is denoted and defined by

$$\det A = |A| = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

From the last paragraph in the proof of Theorem 1.3.5 we have shown that:

Theorem 1.3.8. *A square matrix A is invertible* $\iff \det A \neq 0$.

1.3.2 Computational Facts and Cofactor Expansions

Finally to develop an effective way to check invertability, we need to develop computational tools in order to make good use of Theorem 1.3.8.

Theorem 1.3.9. *If A, B are $n \times n$ matrices, then*

$$\det(AB) = \det A \det B.$$

Proof. Let P be the product of elementary matrices such that $PA = R$, where R is the reduced row echelon form of A.

If A is not invertible, then the last row of R is a zero row, so is $PAB = RB$, thus PAB is not invertible, i.e, AB is not invertible, hence

$$\det(AB) = 0 \quad \text{and} \quad \det A \det B = 0 \cdot \det B = 0.$$

If A is invertible, then $R = I$, hence A is the product of elementary matrices, $A = E_1 E_2 \cdots E_k$. Then by Proposition 1.3.4 many and many times,

$$\begin{aligned} \det(AB) &= \det(E_1 E_2 \cdots E_k B) \\ &= \det(E_1)\det(E_2)\cdots\det(E_k)\det B \\ &= \det(E_1 E_2 \cdots E_k)\det B = \det A \det B. \end{aligned}$$ $\square$

Theorem 1.3.10. *If A is an $n \times n$ matrix, then*

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

$^{(\dagger)}$ The pairity of the number of steps we switch two rows to turn the matrix $\begin{bmatrix} e_{\sigma(1)} \\ e_{\sigma(2)} \\ \vdots \\ e_{\sigma(n)} \end{bmatrix}$ into I

Proof. If A is not invertible, so is A^T, thus $\det A = \det A^T = 0$.

If A is invertible, then A is the product of elementary matrices, $A = E_1 E_2 \cdots E_k$, by Theorem 1.3.9 it is enough to show Theorem 1.3.10 is true for elementary matrix E, i.e., $\det E = \det E^T$.

If E (times A) adds ith row to jth row, then $E = \begin{bmatrix} & \vdots & \\ \text{——} & e_j + e_i & \text{——} \\ & \vdots & \end{bmatrix}$, a direct verification shows us $E^T = \begin{bmatrix} & \vdots & \\ \text{——} & e_i + e_j & \text{——} \\ & \vdots & \end{bmatrix}$ which (times A) adds jth to ith row, hence $\det E = \det E^T = 1$.

If E (times) A interchange rows, so does E^T (since $E^T = E^{-1}$), thus $\det E = \det E^T = -1$.

Finally, if E (times A) scales one of the rows, then E is diagonal, so $E = E^T$.□

Definition 1.3.11. Given $A \in M_{n\times n}(\mathbb{F})$.

(i) Let $A_{ij} \in M_{(n-1)\times(n-1)}(\mathbb{F})$ denote the matrix obtained by deleting the ith row and the jth column of A.

(ii) We define the (i,j)-**cofactor**, $c_{ij}(A)$, by

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

Example 1.3.12.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix},$$

then

$$c_{11}(A) = (-1)^{1+1} \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix}$$

and

$$c_{21}(A) = (-1)^{2+1} \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = -\begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix}$$

Now we can compute the determinant of a large square matrix by its submatrices.

Theorem 1.3.13 (Cofactor Expansion). *Let $A = [a_{ij}]_{n\times n}$, then the expansion along ith row is*

$$\det A = a_{i1}c_{i1}(A) + a_{i2}c_{i2}(A) + \cdots + a_{in}c_{in}(A).$$

The expansion along the jth column is given by

$$\det A = a_{1j}c_{1j}(A) + a_{2j}c_{2j}(A) + \cdots + a_{nj}c_{nj}(A).$$

We just prove the cofactor expansion along ith row, the one along jth column is essentially the same.

Proof. First of all we prove the following: Suppose B is an $(n-1)\times(n-1)$ matrix, then

$$\det\left[\begin{array}{c|c} 1 & \vec{0}^T \\ \hline \vec{0} & B \end{array}\right] = \det B. \tag{1.3.14}$$

To see this, let $\left[\begin{array}{c|c} 1 & \vec{0}^T \\ \hline \vec{0} & B \end{array}\right] = [b_{ij}]_{n\times n}$, then by Theorem 1.3.6 we have

$$\det[b_{ij}] = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{n\sigma(n)} = \sum_{\substack{\sigma\in S_n \\ \sigma(1)=1}} \operatorname{sgn}(\sigma) b_{1\sigma(1)} b_{2\sigma(2)} \cdots b_{n\sigma(n)}.$$

For simplicity, let $S = \operatorname{Perm}(\{2,3,\ldots,n\})$, the set of bijections from $\{2,\ldots,n\}$ to itself, then

$$\det[b_{ij}] = \sum_{\rho\in S} \operatorname{sgn}(\rho) b_{11} b_{2\rho(2)} \cdots b_{n\rho(n)} = 1\cdot\det B,$$

as desired. We will see that (1.3.14) is the key ingredient to finish the proof very soon.

Let $A=[a_{ij}]$, then by linearity of determinant in the ith row, we have

$$\det A = \sum_{k=1}^{n} a_{ik} \det \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ & e_k^T & \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix},$$

or more precisely,

$$\det A = \sum_{k=1}^{n} a_{ik} \det \begin{bmatrix} a_{11} & \cdots & a_{1(k-1)} & 0 & a_{1(k+1)} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{(i-1)1} & \cdots & a_{(i-1)(k-1)} & 0 & a_{(i-1)(k+1)} & \cdots & a_{(i-1)n} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ a_{(i+1)1} & \cdots & a_{(i+1)(k-1)} & 0 & a_{(i+1)(k+1)} & \cdots & a_{(i+1)n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 & a_{n(k+1)} & \cdots & a_{nn} \end{bmatrix},$$

here we have performed row operations on the kth column, $k=1,2,\ldots,n$. We can move our 1 to the upper left corner by switching 1 to the left $k-1$ times and then switching it upwards $i-1$ times, it follows that by (1.3.14),

$$\det A = \sum_{k=1}^{n} a_{ik}(-1)^{i+k}\det A_{ik} = \sum_{k=1}^{n} a_{ik} c_{ik}(A). \qquad \square$$

Remark. Cofactor expansion is very helpful if the size of the matrix is small and almost all of entries are numerical value. This is why we invent the formula in Theorem 1.3.13 although we already have one in Theorem 1.3.6. In Problem 1.13 you are asked to prove a formula that is not easily explainable by cofactor expansion but still manageable if we use the definition of determinant that we start with.

Example 1.3.15. By cofactor expansion along the first row,

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = a \cdot (-1)^{1+1}(d) + b \cdot (-1)^{1+2}(c) = ad - bc.$$

Remark. We should beware of minus signs in using cofactor expansion. We may memorize the diagram instead of computing $(-1)^{i+j}$ each time:

$$\begin{vmatrix} + & - & + & \cdots \\ - & + & - & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{vmatrix} \tag{1.3.16}$$

Example 1.3.17. We bear (1.3.16) in mind and use cofactor expansion along the first row.

$$\begin{vmatrix} 1 & -1 & 3 \\ 1 & 0 & -1 \\ 2 & 1 & 6 \end{vmatrix} = \begin{vmatrix} 0 & -1 \\ 1 & 6 \end{vmatrix} - (-1) \begin{vmatrix} 1 & -1 \\ 2 & 6 \end{vmatrix} + 3 \begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} = 1 + 8 + 3 = 12.$$

For the second one, since there are many 0's on the last column, we use cofactor expansion along this column with the diagram (1.3.16) in mind.

$$\begin{vmatrix} 3 & 2 & 0 & 0 \\ 5 & 1 & 2 & 0 \\ 2 & 6 & 0 & -1 \\ -6 & 3 & 1 & 0 \end{vmatrix} = -(-1) \begin{vmatrix} 3 & 2 & 0 \\ 5 & 1 & 2 \\ -6 & 3 & 1 \end{vmatrix} = 3 \begin{vmatrix} 1 & 2 \\ 3 & 1 \end{vmatrix} - 2 \begin{vmatrix} 5 & 2 \\ -6 & 1 \end{vmatrix} = -15 - 34 = -49.$$

Example 1.3.18. In the following we use R_i to mean the ith row and C_i to mean the ith column. Our strategy is to produce as many 0's as possible.

$$\begin{aligned}
&\begin{vmatrix} a+b+2c & a & b \\ c & b+c+2a & b \\ c & a & c+a+2b \end{vmatrix} \\
\xlongequal{R_1 \to R_1 - R_3} &\begin{vmatrix} a+b+c & 0 & -(a+b+c) \\ c & b+c+2a & b \\ c & a & a+2b+c \end{vmatrix} \\
= &(a+b+c) \begin{vmatrix} 1 & 0 & -1 \\ c & 2a+b+c & b \\ c & a & a+2b+c \end{vmatrix} \\
\xlongequal{C_1 \to C_1 + C_2 + C_3} &(a+b+c) \begin{vmatrix} 0 & 0 & -1 \\ 2(a+b+c) & 2a+b+c & b \\ 2(a+b+c) & a & a+2b+c \end{vmatrix} \\
= &2(a+b+c)^2 \begin{vmatrix} 0 & 0 & -1 \\ 1 & 2a+b+c & b \\ 1 & a & a+2b+c \end{vmatrix} \\
= &2(a+b+c)^2(-1) \begin{vmatrix} 1 & 2a+b+c \\ 1 & a \end{vmatrix} \\
= &2(a+b+c)^3.
\end{aligned}$$

Example 1.3.19. Let R_i and C_i be defined as in the previous example.

$$\begin{vmatrix} a^2 & bc & c^2+ca \\ a^2+ab & b^2 & ca \\ ab & b^2+bc & c^2 \end{vmatrix}$$

$$
\begin{aligned}
&= abc \begin{vmatrix} a & c & c+a \\ a+b & b & a \\ b & b+c & c \end{vmatrix} \\
&\xlongequal{C_1 \to C_1 - C_2 - C_3} abc \begin{vmatrix} -2c & c & c+a \\ 0 & b & a \\ -2c & b+c & c \end{vmatrix} \\
&\xlongequal{R_3 \to R_3 - R_1} abc \begin{vmatrix} -2c & c & c+a \\ 0 & b & a \\ 0 & b & -a \end{vmatrix} \\
&= abc(-2c) \begin{vmatrix} b & a \\ b & -a \end{vmatrix} \\
&= abc(-2c)(-2ab) \\
&= 4a^2b^2c^2.
\end{aligned}
$$

We summarize what we have in this section:

Facts for Determinants

(i) For square matrix A, $\det A = \det A^T$.

(ii) For square matrix A, A is invertible $\iff$ $\det A \neq 0$.

(iii) For $A, B \in M_{n\times n}(\mathbb{F})$, $\det(AB) = \det A \det B$.

(iv) Let R and S denote rows of a matrix, for any $c \in \mathbb{F}$:

(a) $$\begin{vmatrix} \vdots \\ \text{---}cR\text{---} \\ \vdots \end{vmatrix} = c \begin{vmatrix} \vdots \\ \text{---}R\text{---} \\ \vdots \end{vmatrix}$$

(b) $$\begin{vmatrix} \vdots \\ \text{---}R\text{---} \\ \vdots \\ \text{---}S\text{---} \\ \vdots \end{vmatrix} = \begin{vmatrix} \vdots \\ \text{---}R\text{---} \\ \vdots \\ \text{---}S+cR\text{---} \\ \vdots \end{vmatrix}$$

(c) $$\begin{vmatrix} \vdots \\ \text{---}R\text{---} \\ \vdots \\ \text{---}S\text{---} \\ \vdots \end{vmatrix} = - \begin{vmatrix} \vdots \\ \text{---}S\text{---} \\ \vdots \\ \text{---}R\text{---} \\ \vdots \end{vmatrix}$$

The above are also true for columns due to (i).

(v) **Definition:**

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

(vi) **Cofactor Expansion:** Let $A = [a_{ij}]_{n\times n}$, then the expansion along ith row is

$$\det A = a_{i1}c_{i1}(A) + a_{i2}c_{i2}(A) + \cdots + a_{in}c_{in}(A).$$

The expansion along the jth column is given by

$$\det A = a_{1j}c_{1j}(A) + a_{2j}c_{2j}(A) + \cdots + a_{nj}c_{nj}(A).$$

1.3.3 Compute Inverse by Cofactor Matrix

Apart from performing row operations, we can invent a new formula to compute inverse in terms of cofactors and determinant. For this we define two terms:

Definition 1.3.20. Let A be an $n \times n$ matrix. The **cofactor matrix** of A is defined by

$$\operatorname{cof} A = [c_{ij}(A)]_{n\times n}.$$

The matrix $(\operatorname{cof} A)^T$ is usually called **adjoint matrix** of A. Since later we will adopt this term for "linear maps", to not mess things up we will not adopt the use of this term adjoint for matrices. We are ready for the last theorem in this chapter:

Theorem 1.3.21. *Let A be a square matrix, then*

$$A(\operatorname{cof} A)^T = (\det A)I.$$

Furthermore, if A is invertible, namely, $\det A \neq 0$, we have

$$A^{-1} = \frac{1}{\det A}(\operatorname{cof} A)^T.$$

Proof. To prove $A(\operatorname{cof} A)^T = (\det A)I$, since

$$A(\operatorname{cof} A)^T = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} c_{11}(A) & c_{21}(A) & \cdots & c_{n1}(A) \\ c_{12}(A) & c_{22}(A) & \cdots & c_{n2}(A) \\ \vdots & \vdots & \ddots & \vdots \\ c_{1n}(A) & c_{2n}(A) & \cdots & c_{nn}(A) \end{bmatrix}.$$

We observe that the ith diagonal elements of the product is just the cofactor expansion of A along the ith row, hence it is $\det A$. On the other hand, the nondiagonal ijth elements $(i \neq j)$ of the product is

$$\sum_{k=1}^{n} a_{ik}c_{jk}(A).$$

Which is the determinant of the matrix A', obtained from A by replacing the jth row by the ith row. Therefore A' has two identical rows, $\det A' = 0$, hence we get desired equality.

The second equality follows from taking A^{-1} on both sides of $A(\operatorname{cof} A)^T = (\det A)I$. $\square$

Example 1.3.22. We compute the inverse of the matrix $A := \begin{bmatrix} 3 & 2 & 6 \\ 1 & 1 & 2 \\ 2 & 2 & 5 \end{bmatrix}$ again whose inverse has been computed using row operations in Example 1.2.20. This time we do so by computing $\det A$ and $\operatorname{cof} A$.

By cofactor expansion along the first row,

$$\det A = 3\begin{vmatrix}1 & 2\\2 & 5\end{vmatrix} - 2\begin{vmatrix}1 & 2\\2 & 5\end{vmatrix} + 6\begin{vmatrix}1 & 1\\2 & 2\end{vmatrix} = \begin{vmatrix}1 & 2\\2 & 5\end{vmatrix} = 5 - 4 = 1.$$

Also, we have

$$\operatorname{cof} A = \begin{bmatrix} \begin{vmatrix}1 & 2\\2 & 5\end{vmatrix} & -\begin{vmatrix}1 & 2\\2 & 5\end{vmatrix} & \begin{vmatrix}1 & 1\\2 & 2\end{vmatrix} \\ -\begin{vmatrix}2 & 6\\2 & 5\end{vmatrix} & \begin{vmatrix}3 & 6\\2 & 5\end{vmatrix} & -\begin{vmatrix}3 & 2\\2 & 2\end{vmatrix} \\ \begin{vmatrix}2 & 6\\1 & 2\end{vmatrix} & -\begin{vmatrix}3 & 6\\1 & 2\end{vmatrix} & \begin{vmatrix}3 & 2\\1 & 1\end{vmatrix} \end{bmatrix} = \begin{bmatrix} 1 & -1 & 0\\ 2 & 3 & -2\\ -2 & 0 & 1\end{bmatrix},$$

hence

$$A^{-1} = \frac{1}{\det A}(\operatorname{cof} A)^T = \begin{bmatrix} 1 & 2 & -2\\ -1 & 3 & 0\\ 0 & -2 & 1\end{bmatrix}.$$

1.4 Exercises

Linear Systems

Problem 1.1. Let A be a matrix with the following reduced row echelon form

$$U = \begin{bmatrix} 1 & 0 & 2 & 1\\ 0 & 1 & 1 & 4\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}.$$

Also, let $a_1, a_2, a_3, a_4 \in \mathbb{R}^4$ be the columns of A such that $A = [a_1 \quad a_2 \quad a_3 \quad a_4]$. Find a_3 and a_4 if

$$a_1 = \begin{bmatrix} -3\\ 5\\ 2\\ 1\end{bmatrix} \quad \text{and} \quad a_2 = \begin{bmatrix} 4\\ -3\\ 7\\ -1\end{bmatrix}.$$

Matrix Operations

Problem 1.2. Prove (i) and (iii) of Theorem 1.2.13. Moreover, show that every matrix $A \in M_{n\times n}(\mathbb{R})$ can be written as

$$A = B + C,$$

for some symmetric matrix B and skew symmetric matrix C.

Problem 1.3. Let $P \in M_{2\times 2}(\mathbb{R})$ be such that $PA = AP$, for all $A \in M_{2\times 2}(\mathbb{R})$, show that

$$P = kI_2,$$

for some $k \in \mathbb{R}$.

Problem 1.4. Let $A \in M_{n\times n}(\mathbb{R})$. If $A = [a_{ij}]_{n\times n}$, we define the **trace** of A by

$$\operatorname{Tr} A = a_{11} + a_{22} + \cdots + a_{nn},$$

i.e., $\operatorname{Tr} A$ is the sum of all diagonal elements. Prove that given $A \in M_{n\times k}(\mathbb{R})$ and $B \in M_{k\times n}(\mathbb{R})$, we have

$$\operatorname{Tr}(AB) = \operatorname{Tr}(BA).$$

Hint. You need to use Definition 1.2.2.

Problem 1.5. Prove that if $A = [a_{ij}]_{n\times n}$ is symmetric (i.e., $A^T = A$), then for $B = [b_{ij}]_{n\times n}$, one has

$$\operatorname{Tr}(AB) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ij}.$$

Remark. This formula enables us to write linear 2nd order PDEs in a neat and compact way.

Problem 1.6. Let $a_1, a_2, \ldots, a_n \in \mathbb{R}$. Denote

$$A = [\delta_{ij} + a_i a_j]_{n\times n}, \quad B = \left[\delta_{ij} - \frac{a_i a_j}{1 + a_1^2 + a_2^2 + \cdots + a_n^2}\right]_{n\times n}.$$

Here $\delta_{ij} = 1$ if $i = j$ and $= 0$ otherwise. Find AB.

Hint. You need to use Definition 1.2.2.

Problem 1.7. Let $A, B \in M_{n\times n}(\mathbb{F})$. If $A^3 = B^3$ and $A^2B = B^2A$, can $A^2 + B^2$ be invertible?

Problem 1.8. Show the following properties for square matrices:

(i) Sum and product of **upper triangular** matrices is **upper triangular**.

(ii) Sum and product of **lower triangular** matrices is **lower triangular**.

(iii) Sum and product of **diagonal** matrices is **diagonal**.

Determinants

Problem 1.9. Let $\alpha \in \mathbb{R}$ and $A \in M_{n\times n}(\mathbb{R})$, show that $\det(\alpha A) = \alpha^n \det A$.

Problem 1.10. Consider the following statement and its "proof":

> **Statement.** *Let* $A \in M_{m\times n}(\mathbb{R})$ *and* $B \in M_{n\times m}(\mathbb{R})$, *then* $\det(AB) = \det(BA)$.
> **Proof.** $\det(AB) = \det A \det B = \det B \det A = \det(BA)$.

(i) Is the proof correct?

(ii) Is the statement true? Prove or disprove.

Problem 1.11. Show that

$$\begin{vmatrix} a & b & c \\ a^2 & b^2 & c^2 \\ bc & ac & ab \end{vmatrix} = (a-b)(b-c)(c-a)(ab+bc+ca).$$

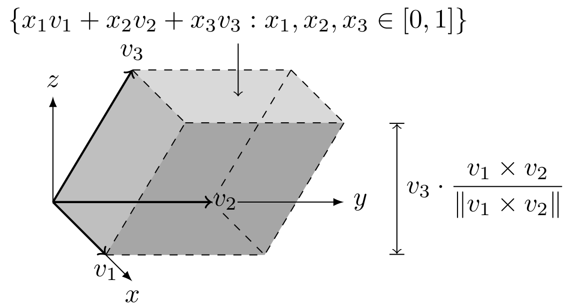
Problem 1.12. Given $v_1, v_2, v_3 \in \mathbb{R}^3$, verify the **scalar triple product**:

$$v_1 \cdot (v_2 \times v_3) = \det[v_1 \quad v_2 \quad v_3].$$

Remark. Let m_n denote the n-dimensional "volume" on $\mathbb{R}^n$, we can show that

$$|\det[v_1 \quad \cdots \quad v_n]| = m_n(\{x_1v_1 + \cdots + x_nv_n : x_1, , \ldots, x_n \in [0,1]\}).$$

So both sides of "scalar triple product" represent "oriented" volume of the parallelepiped spanned by v_1, v_2, v_3, thus it is legitimate to guess such an equality.



Problem 1.13. Let $W(x)$ denote the **Wronskian** of functions $f_1, \ldots, f_n$ evaluated at x

$$W(x) = \begin{vmatrix} f_1(x) & f_2(x) & \cdots & f_n(x) \\ f_1'(x) & f_2'(x) & \cdots & f_n'(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)}(x) & f_2^{(n-1)}(x) & \cdots & f_n^{(n-1)}(x) \end{vmatrix},$$

where $f_1, \ldots, f_n$ are $n-1$ times differentiable at x. Prove that

$$W'(x) = \begin{vmatrix} f_1(x) & f_2(x) & \cdots & f_n(x) \\ f_1'(x) & f_2'(x) & \cdots & f_n'(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-2)}(x) & f_2^{(n-2)}(x) & \cdots & f_n^{(n-2)}(x) \\ f_1^{(n)}(x) & f_2^{(n)}(x) & \cdots & f_n^{(n)}(x) \end{vmatrix},$$

hence, show that if $f_1, f_2, \ldots, f_n$ satisfy the following nth order ODE,

$$y^{(n)} + p_{n-1}(x)y^{(n-1)} + \cdots + p_1(x)y' + p_0(x)y = 0,$$

then $W'(x) = -p_{n-1}(x)\,W(x)$.

Chapter 2

Vector Spaces

In this chapter $\mathbb{F}$ denotes $\mathbb{R}$ or $\mathbb{C}$. We will develop the parallel story of real and complex vector spaces at the same time. Every definition and statement involving the scalar field $\mathbb{F}$ is supposed to be two separate almost identical statements. For example, the statement

$$\text{For every } x \in \mathbb{F}, \text{ there is } y \in \mathbb{F} \text{ such that } x + y = 0.$$

means simultaneously:

$$\text{For every } x \in \mathbb{R}, \text{ there is } y \in \mathbb{R} \text{ such that } x + y = 0; \quad \text{and}$$
$$\text{For every } x \in \mathbb{C}, \text{ there is } y \in \mathbb{C} \text{ such that } x + y = 0.$$

2.1 Definitions

Definition 2.1.1. A **vector space** is a set V along with an **addition** on V and also a **scalar multiplication** on V satisfying the following axioms:

Closedness Under Addition
$u, v \in V \implies u + v \in V$

Closedness Under Scalar Multiplication
$\alpha \in \mathbb{F}, v \in V \implies \alpha v \in V$

Commutativity
For all $u, v \in V$, $\quad u + v = v + u$

Associativity
For all $u, v, w \in V$ and $a, b \in \mathbb{F}$,
$(u + v) + w = u + (v + w), \quad (ab)v = a(bv)$

Additive Identity
There is an $\mathbf{0} \in V$, $v + \mathbf{0} = v \quad$ for all $v \in V$

Additive Inverse
For every $v \in V$, there is $w \in V$, $v + w = \mathbf{0}$

Multiplicative Identity
$1v = v, \quad$ for all $v \in V$

Distributive Properties
For all $a, b \in \mathbb{F}$ and $u, v \in V$
$a(u + v) = au + av, \quad (a + b)u = au + bu$

To avoid our statements being cumbersome, let's adopt the following convention.

Convention. When we just mention V is a vector space, then it is assumed to be over $\mathbb{F}$.

A vector space over $\mathbb{R}$ is called a **real vector space** and that over $\mathbb{C}$ is called a **complex vector space**. They share many similarities that we don't try to distinguish them in this and next chapter, and their main distinction will be seen in Chapter 4.

General Rule. *When we mention a vector space that is not closed under nonreal scalar, then our discussion will be over $\mathbb{R}$, so when we quote any definitions and results, we first replace $\mathbb{F}$ by $\mathbb{R}$.*

Theorem 2.1.2. *Let V be a vector space. They all share the following properties:*

*(i) V has a **unique** additive identity (denoted by $\mathbf{0}$).*

*(ii) Each element $v \in V$ has a **unique** additive inverse $-v$.*

(iii) $0v = \mathbf{0}$ for all $v \in V$.

(iv) $\alpha \cdot \mathbf{0} = \mathbf{0}$ for all $\alpha \in \mathbb{F}$.

(v) $(-1)v = -v$ for all $v \in V$.

Proof. (i) Suppose we have two additive identities $\mathbf{0}$ and $\mathbf{0}'$. Then by definition for every $u, v \in V$, $u + \mathbf{0} = u$ and $v + \mathbf{0}' = v$. In particular, if we take $u = \mathbf{0}'$ and $v = \mathbf{0}$, then

$$\mathbf{0}' = \mathbf{0}' + \mathbf{0} \xlongequal{\text{commutativity}} \mathbf{0} + \mathbf{0}' = \mathbf{0}.$$

(ii) Let $x, y \in V$ be additive inverse of $v \in V$, then

$$x = x + (y + v) = (x + v) + y = y.$$

(iii) $0v = (0+0)v = 0v + 0v$, we add the additive inverse of $0v$ on both sides to get $0v = \mathbf{0}$.

(iv) Let $\alpha \in \mathbb{F}$, by (iii) $0 \cdot \mathbf{0} = \mathbf{0}$, so $\alpha\mathbf{0} = \alpha(0 \cdot \mathbf{0}) = (\alpha \cdot 0)\mathbf{0} = 0 \cdot \mathbf{0} = \mathbf{0}$.

(v) Here $-v$ means the additive inverse of v, not $(-1)v$ by definition, although indeed they are the same:

$$-v = -v + \mathbf{0} = -v + 0v = -v + (1-1)v = -v + v + (-1)v = \mathbf{0} + (-1)v = (-1)v. \quad \square$$

Due to (i) of Theorem 2.1.2, we always denote a zero vector by $\mathbf{0}$, or more often simply by 0. Also due to (ii) every additive inverse of $v \in V$ is denoted by $-v$

Example 2.1.3 (List of Some Vector Spaces). Each of the following is a vector space with naturally defined addition and scalar multiplication.

(i) $\mathbb{F}^n$

(ii) The collection of polynomials with degree at most n

$$\mathbb{P}_n(\mathbb{F}) := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 : a_0, a_1, \ldots, a_n \in \mathbb{F}\}$$

(iii) $C([0,1],\mathbb{F}) := \{\mathbb{F}\text{-valued continuous function on } [0,1]\}$

(iv) $\mathcal{R}[0,1] := \{\mathbb{R}\text{-valued Riemann integrable function on } [0,1]\}$.

(v) $\mathbb{F}^\infty := \{(x_1, x_2, x_3, \dots) : x_1, x_2, x_3, \dots \in \mathbb{F}\}$

(vi) $M_{m\times n}(\mathbb{F}) := \{[a_{ij}]_{m\times n} : a_{ij} \in \mathbb{F}\}$

(vii) Trivial vector space: $\{0\}$

We will see that (iii), (iv) and (v) in Example 2.1.3 are much larger than the rest in the sense of *vector space dimension* (or simply *dimension*) that we will shortly study.

> **Caution.** *The example above serves as a* ***warning*** *that when we speak of vector space, it is not necessarily $\mathbb{F}^n$. By a* ***vector*** *we merely mean an element in a vector space, not a column.*

2.2 Linear Span

Definition 2.2.1. Let V be a vector space and $v_1, v_2, \dots, v_n \in V$, then for every $x_1, x_2, \dots, x_n \in \mathbb{F}$,

$$x_1v_1 + x_2v_2 + \cdots + x_nv_n$$

is called a **linear combination** of $v_1, v_2, \dots, v_n$. The **linear span** (or simply **span**) of $v_1, v_2, \dots, v_n$ is denoted and defined by

$$\operatorname{span}_{\mathbb{F}}\{v_1, v_2, \dots, v_n\} = \{x_1v_1 + x_2v_2 + \cdots + x_nv_n : x_1, x_2, \dots, x_n \in \mathbb{F}\},$$

i.e., linear span is the collection of all possible linear combinations.

Remark. Hereafter in each example **we will mention the vector space that is under consideration at least once**, therefore it will be clear in each discussion that which scalar we are using. Thus instead of using the symbol $\operatorname{span}_{\mathbb{F}}$, we simply write span.

Consider again

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}, \tag{2.2.2}$$

if we define $a_1 = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix}, a_2 = \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix}, \dots, a_n = \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix}$ and $b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$, then the above system of linear equations can be neatly written as $x_1a_1 + x_2a_2 + \cdots + x_na_n = b$. The solvability of the above equation is the same as whether or not b is in the span of $a_1, a_2, \dots, a_n$

Example 2.2.3. Given $\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix} \in \mathbb{R}^3$,

$$\operatorname{span}\left\{\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix}\right\} = \left\{x\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + y\begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix} : x, y \in \mathbb{R}\right\} = \left\{\begin{bmatrix} x \\ x-y \\ 0 \end{bmatrix} : x, y \in \mathbb{R}\right\}.$$

Example 2.2.4. We know that $M_{2\times 2}(\mathbb{R})$ is a real vector space, let

$$v_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 1 & 2 \\ -1 & 1 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad v_4 = \begin{bmatrix} 0 & 0 \\ 1 & -2 \end{bmatrix}.$$

Is the vector $b = \left[\begin{smallmatrix} 3 & 1 \\ 0 & 3 \end{smallmatrix}\right]$ in the span of v_1, v_2, v_3, v_4? If so, do v_1, v_2, v_3, v_4 span b in a unique way?

Let $x_1, x_2, x_3, x_4 \in \mathbb{R}$, the question is the same as asking if

$$x_1 v_1 + x_2 v_2 + x_3 v_3 + x_4 v_4 = b$$

is solvable and if the solution is unique. By expanding everything, the above equation is the same as

$$\begin{cases} x_1 + x_2 + x_3 = 3 \\ 2x_2 - x_3 = 1 \\ x_1 - x_2 + x_3 + x_4 = 0 \\ x_1 + x_2 - x_3 - 2x_4 = 3 \end{cases}.$$

Now we reduce it by doing row operations to the augmented matrix.

$$\left[\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 3 \\ 0 & 2 & -1 & 0 & 1 \\ 1 & -1 & 1 & 1 & 0 \\ 1 & 1 & -1 & -2 & 3 \end{array}\right] \xrightarrow[R_4 \to R_4 - R_1]{R_3 \to R_3 - R_1} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 3 \\ 0 & 2 & -1 & 0 & 1 \\ 0 & -2 & 0 & 1 & -3 \\ 0 & 0 & -2 & -2 & 0 \end{array}\right]$$

$$\xrightarrow[R_4 \to -\frac{1}{2} R_4]{R_3 \to R_3 + R_2} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 3 \\ 0 & 2 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 & -2 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right] \xrightarrow{R_4 \to R_4 + R_3} \left[\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 3 \\ 0 & 2 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 & -2 \\ 0 & 0 & 0 & 2 & -2 \end{array}\right].$$

We get $(x_1, x_2, x_3, x_4) = (1, 1, 1, -1)$. Thus b is in the spanned of v_i's in a unique way.

2.3 Linear Independence

Definition 2.3.1. Let V be a vector space, a set of vectors $\{v_1, v_2, \dots, v_n\}$ in V is said to be **linearly independent** if

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0, a_i \in \mathbb{F} \implies a_1 = a_2 = \cdots = a_n = 0.$$

Otherwise it is said to be **linearly dependent**, i.e., there are $a_1, a_2, \dots, a_n \in \mathbb{F}$, not all zero, such that $a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0$.

Remark. We can also say $v_1, v_2, \dots, v_n$ are linearly independent. Linear independence is needed when we want to make sure no v_i can be dropped in order to span the vector space $\operatorname{span}\{v_1, v_2, \dots, v_n\}$ by using these v_i's

Theorem 2.3.2. *Let V be a vector space and $\{v_1, \dots, v_k\}$ a linearly independent subset of V, then:*

(i) Every subset of $\{v_1, \dots, v_k\}$ is linearly independent.

(ii) If $v \in V \setminus \operatorname{span}\{v_1, \dots, v_k\}$, then $\{v, v_1, \dots, v_k\}$ is linearly independent.

Proof. (i) Suppose $\{v_i : i \in I\}$ is a subset of $\{v_1, \ldots, v_k\}$, then

$$\sum_{i \in I} a_i v_i = 0 \implies \sum_{i \in I} a_i v_i + \sum_{i \notin I} 0 \cdot v_i = 0,$$

as $v_1, v_2, \ldots, v_k$ are linearly independent, necessarily $a_i = 0$, for all $i \in I$.

(ii) Let $a_1, a_2, \ldots, a_k, \alpha \in \mathbb{F}$ be such that

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k + \alpha v = 0.$$

If $\alpha \neq 0$, then $v \in \operatorname{span}\{v_1, \ldots, v_k\}$, a contradiction, hence $\alpha = 0$. But then

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$$

and $\{v_1, \ldots, v_k\}$ is linearly independent, thus $a_1 = a_2 = \cdots = a_k = 0$. $\square$

Example 2.3.3. Let V be a vector space, if $v_1, v_2 \in V$ are linearly dependent, then one of them must be a constant multiple of the other. This is because there are $a_1, a_2 \in \mathbb{F}$, not all zero, such that

$$a_1 v_1 + a_2 v_2 = 0.$$

Since at least one of a_i's is nonzero, say $a_1 \neq 0$, then $v_1 = -\frac{a_2}{a_1} v_2$; otherwise if $a_2 \neq 0$, then $v_2 = -\frac{a_1}{a_2} v_1$.

Example 2.3.4. The vectors

$$(1,0,0)^T, \quad (0,1,0)^T \quad \text{and} \quad (0,0,1)^T$$

are linearly independent in $\mathbb{R}^3$. To prove this, let

$$a_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + a_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + a_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = 0,$$

hence by entrywise comparison, $a_1 = a_2 = a_3 = 0$, so they are linearly independent.

Example 2.3.5. In $\mathbb{F}^n$ every set of $n+1$ vectors, say $v_1, v_2, \ldots, v_{n+1}$, must be linearly dependent. It is because the homogeneous system

$$x_1 v_1 + x_2 v_2 + \cdots + x_{n+1} v_{n+1} = 0$$

satisfies

$$\begin{aligned} n+1 &= \# \text{ of basic variables} + \# \text{ of free variables} \\ &\leq \min\{n, n+1\} + \# \text{ of free variables} = n + \# \text{ of free variables}, \end{aligned}$$

therefore $\#$ of free variables ≥ 1, so $(x_1, x_2, \ldots, x_{n+1}) = (0, 0, \ldots, 0)$ is not the only solution, i.e., $v_1, \ldots, v_{n+1}$ are linearly dependent.

Example 2.3.6. Are the vectors $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$, $\begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix}$ and $\begin{bmatrix} 7 \\ 8 \\ 9 \end{bmatrix}$ linearly independent in $\mathbb{R}^3$? To answer this, suppose

$$x \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} + y \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} + z \begin{bmatrix} 7 \\ 8 \\ 9 \end{bmatrix} = 0,$$

then they are linearly independent iff $(x, y, z) = (0, 0, 0)$ is the only solution. To check this, let's do row operations on the coefficient matrix.

$$\begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \xrightarrow[R_3 \to R_3 - 3R_1]{R_2 \to R_2 - 2R_1} \begin{bmatrix} 1 & 4 & 7 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{bmatrix} \xrightarrow{R_3 \to R_3 - 2R_2} \begin{bmatrix} 1 & 4 & 7 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{bmatrix}$$

Hence there will be at least one free variable, meaning that there are infinitely many solutions to the homogeneous system, so $(0, 0, 0)$ is not the only solution, and thus these vectors are linearly dependent.

By finding the solution, we see that

$$\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} - 2 \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} + \begin{bmatrix} 7 \\ 8 \\ 9 \end{bmatrix} = 0.$$

Example 2.3.7. Let $C(\mathbb{R})$ denote the vector space of continuous functions on $\mathbb{R}$. We try to show that $\{x, xe^x, x^2e^x\}$ is linearly independent in $C(\mathbb{R})$.

Suppose there are $a, b, c \in \mathbb{R}$ such that

$$ax + bxe^x + cx^2e^x = 0, \tag{2.3.8}$$

for all $x \in \mathbb{R}$. We will prove that necessarily $a = b = c = 0$. Dividing x^2e^x on both sides, we have for every $x \neq 0$,

$$\frac{a}{xe^x} + \frac{b}{x} + c = 0,$$

if we let $x \to \infty$, then $c = 0$. Hence (2.3.8) be comes

$$ax + bxe^x = 0.$$

Again dividing both sides by xe^x we have $a/e^x + b = 0$, if we taking $x \to \infty$, then $b = 0$. Finally $a = 0$ from (2.3.8).

Alternatively we can use Wronskian that we usually learn in ODE course, see Problem 2.8 for detail.

2.4 Vector Subspaces

Definition 2.4.1 (Vector Subspace). Let V be a vector space and $W \subseteq V$. W is said to be a **vector subspace**, or simply **subspace**, of V if it satisfies the following:

(i) $0 \in W$.

(ii) $u, v \in W \implies u + v \in W$. **(Closed Under Addition)**

(iii) $\alpha \in \mathbb{R}, v \in W \implies \alpha v \in W$. **(Closed Under Scalar Multiplication)**

Remark. Since W as a subset of V inherits addition and scalar multiplication from that of V, hence loosely speaking:

$$W \textit{ is a subspace of } V \iff W \textit{ is a vector space contained in } V.$$

2.4.1 Examples

As easily seen from definition, linear span has very good algebraic structure:

Theorem 2.4.2. *Let V be a vector space, $v_1, v_2, \dots, v_n \in V$, then*

$$\operatorname{span}\{v_1, v_2, \dots, v_n\}$$

is a subspace of V.

Proof. We just need to check (i), (ii) and (iii) of Definition 2.4.1.

(i) $0v_1 + 0v_2 + \cdots + 0v_n = 0 + 0 + \cdots + 0 = 0 \in \operatorname{span}\{v_1, v_2, \dots, v_n\}$.

(ii) Let $u, v \in \operatorname{span}\{v_1, v_2, \dots, v_n\}$, then there are $a_1, \dots, a_n$ and $b_1, \dots, b_n$ such that $u = \sum_{i=1}^n a_i v_i$ and $v = \sum_{i=1}^n b_i v_i$, thus

$$u + v = \sum_{i=1}^n (a_i + b_i) v_i \in \operatorname{span}\{v_1, v_2, \dots, v_n\}.$$

(iii) Define $v = \sum_{i=1}^n b_i v_i$, for every $\alpha \in \mathbb{F}$ we have

$$\alpha v = \sum_{i=1}^n \alpha b_i v_i \in \operatorname{span}\{v_1, v_2, \dots, v_n\}.$$ □

Example 2.4.3. It is known that $\mathbb{R}^n$ is a vector space. Let $1 \le k \le n$, then

$$\mathbb{R}^k \times \{\underbrace{(0, 0, \dots, 0)}_{n-k \text{ entries}}\} := \{(x_1, \dots, x_k, 0, \dots, 0)^T : x_1, x_2, \dots, x_k \in \mathbb{R}\}$$

is a subspace of $\mathbb{R}^n$.

Example 2.4.4. The collection of symmetric matrices of $M_{n\times n}(\mathbb{R})$

$$W := \{A \in M_{n\times n}(\mathbb{R}) : A^T = A\}$$

is a subspace of the real vector space $M_{n\times n}(\mathbb{R})$. To prove this, we need to verify (i), (ii) and (iii) of Definition 2.4.1 when $\mathbb{F} = \mathbb{R}$.

Since $0^T = 0$, $0 \in W$, (i) is satisfied.

Next, let $A, B \in W$, then $A^T = A$ and $B^T = B$, it follows that

$$(A + B)^T = A^T + B^T = A + B,$$

thus W is closed under addition, (ii) is satisfied.

Finally, let $\alpha \in \mathbb{R}$ and $A \in W$, then

$$(\alpha A)^T = \alpha A^T = \alpha A,$$

so W is closed under scalar multiplication, (iii) is satisfied.

Example 2.4.5. Let X and Y be two vector spaces. The Cartesian product

$$X \times Y := \{(x, y) : x \in X, y \in Y\}$$

becomes a vector space with the following addition and scalar multiplication:

- **Addition:** For $(x_1, y_1), (x_2, y_2) \in X \times Y$,
$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2).$$
- **Scalar Multiplication:** For $(x, y) \in X \times Y$ and $\alpha \in \mathbb{F}$,
$$\alpha(x, y) = (\alpha x, \alpha y).$$

Hereafter the Cartesian product of any two vector spaces is assumed to have the natural operations defined in Example 2.4.5 that make it into a vector space.

2.4.2 Sums and Direct Sums

Let V be a vector space, a subspace U of V is said to be **proper** if $U \neq V$. It can be shown that every vector space cannot be a union of two proper subspaces. So instead of studying union, we focus on *sum*.

Theorem 2.4.6 (Sum and Intersection). *Let V be a vector space and U, W vector subspaces of V, then both*

$$U + W := \{u + w : u \in U, w \in W\} \quad \textit{and} \quad U \cap W$$

are subspaces of V.

Proof. $U + W$ is a subset of V. To argue this, let $x \in U + W$, then $x = u + w$ for some $u \in U$ and $w \in W$. But $u, w \in V$, hence $x = u + w \in V$ by definition of vector space's addition. We have proved the following implication

$$x \in U + W \implies x \in V,$$

this implication is equivalent to saying $U + W \subseteq V$. Also $U \cap W \subseteq V$ because both $U, W \subseteq V$.

To show $U + W$ and $U \cap W$ are subspaces of V, it remains to check (i), (ii) and (iii) of Definition 2.4.1 are satisfied.

(i) Since U, W are vector spaces, the additive identity $0 \in U, W$, so $0 = 0 + 0 \in U + W$ and $0 \in U \cap W$.

(ii) Let $x, y \in U + W$, then $x = u_1 + w_1, y = u_2 + w_2$ for some $u_1, u_2 \in U$ and $w_1, w_2 \in W$, it follows that

$$x + y = u_1 + w_1 + u_2 + w_2 = (u_1 + u_2) + (w_1 + w_2),$$

since U and W are closed under addition, $u_1 + u_2 \in U$ and $w_1 + w_2 \in W$, thus $x + y \in U + W$, i.e., $\boldsymbol{U + W}$ **is closed under addition**.

Likewise, let $x, y \in U \cap W$, then there are $u_1, u_2 \in U$ and $w_1, w_2 \in W$ such that

$$x = u_1 = w_1 \quad \text{and} \quad y = u_2 = w_2,$$

so $x + y = u_1 + u_2 = w_1 + w_2$. Again since U and W are closed under addition, $x + y \in U \cap W$, meaning that $\boldsymbol{U \cap W}$ **is closed under addition**.

(iii) We leave the proof that **$U + W$ and $U \cap W$ are closed under scalar multiplication** as an exercise. This is as easy as (ii). $\square$

Example 2.4.7. Let V be a vector space and $W_1, W_2, \ldots, W_k \subseteq V$ subspaces of V, then

$$W_1 + W_2 + \cdots + W_k := \{w_1 + w_2 + \cdots + w_k : w_i \in W_i,\ i = 1, 2, \ldots k\}$$

is a subspace of V. This is because by Theorem 2.4.6 $W_1 + W_2$ is a subspace of V, so is $(W_1 + W_2) + W_3$, so is $(W_1 + W_2 + W_3) + W_4$, ..., so is $(W_1 + \cdots + W_{k-1}) + W_k$.

Example 2.4.8. We reconsider the set $\mathbb{R}^k \times \{(0, \ldots, 0)^T\} \subseteq \mathbb{R}^n$ in Example 2.4.3. Denote

$$e_i = (a_1, a_2, \ldots, a_n)^T,$$

where $a_i = 1$ and $j \neq i \implies a_j = 0$. For example, $e_1 = (1, 0, 0, \ldots, 0)^T$ and $e_2 = (0, 1, 0, \ldots, 0)^T$.

$\mathbb{R}^k \times \{(0, \ldots, 0)^T\}$ is a subset of $\mathbb{R}^n$. Since

$$\mathbb{R}^k \times \{(0, \ldots, 0)^T\} = \mathrm{span}(e_1) + \mathrm{span}(e_2) + \cdots + \mathrm{span}(e_k),$$

by Example 2.4.7, $\mathbb{R}^k \times \{(0, \ldots, 0)^T\}$ is a subspace of $\mathbb{R}^n$. This also illustrates linear span of a set of vectors is a subspace simply because they are *sum* of vector subspaces.

Given two subspaces U, W of a vector space V, $U + W$ is a subspace of V by Theorem 2.4.6. Now every element in $U + V$ can be written as a sum of $u \in U$ and $w \in W$, the next question is: can every element in $U + W$ be written as such a sum ***uniquely***?

Definition 2.4.9. A vector space V is said to be the **direct sum** of subspaces U and W if

$$V = U + W \quad \text{and} \quad U \cap W = \{0\}.$$

In this case we write $V = U \oplus W$.

Proposition 2.4.10. *Let U and W be subspaces of a vector space V. Then the following are equivalent:*

(i) $V = U \oplus W$

(ii) Each vector in V is a sum of a $u \in U$ and a $w \in W$ ***uniquely***.

Proof. **($\Rightarrow$).** Assume $V = U \oplus W$. Let $v \in V$, then $v = u + w$ for some $u \in U$ and $w \in W$.

Suppose $v = u' + w'$ for some (possibly other) $u' \in U$ and $w' \in W$, we need to show $u = u'$ and $w = w'$.

Since $u + w = v = u' + w'$,

$$u - u' = w' - w \in U \cap W = \{0\},$$

hence $u = u'$ and $w = w'$, showing that the way of writing as a sum is unique.

($\Leftarrow$). Conversely, assume every element in V can be written uniquely as a sum of an element in U and an element in W, then this implies $V \subseteq U + W \subseteq V$, so $V = U + W$.

It remains to show $U \cap W = \{0\}$, to do this, let $v \in U \cap W$, then there are $u \in U$, $w \in W$ such that

$$v = u = w,$$

but then $u - w = v - v = 0$. Since U and W are vector spaces, $0 \in U$ and $0 \in W$, so

$$u - w = 0 = 0 - 0,$$

but by hypothesis each vector in V is summed in a unique way, so $u = 0 = w$, thus $v = 0$. In summary, the logic $(v \in U \cap W \implies v \in \{0\})$ says that $U \cap W \subseteq \{0\}$, but $U \cap W$ as a vector space contains 0, so $U \cap W = \{0\}$. □

Example 2.4.11. In the vector space $\mathbb{R}^5$,

$$U = \{(a, b, c, 0, 0)^T : a, b, c \in \mathbb{R} \quad \text{and} \quad W = \{(0, 0, 0, d, e)^T : d, e \in \mathbb{R}\}$$

sum up to give $\mathbb{R}^5$. It is obvious $U \cap W = \{0\}$, so $\mathbb{R}^5 = U \oplus W$.

2.5 Finite Dimensional Vector Spaces

Definition 2.5.1. A vector space V is said to be **finite dimensional** if there are finitely many vectors $v_1, v_2, \ldots, v_n \in V$ such that

$$V = \operatorname{span}\{v_1, v_2, \ldots, v_n\}.$$

A vector space that is not finite dimensional is said to be **infinite dimensional**.

Remark. For convenience we say a **set** V is finite dimensional if it is a vector space that is finite dimensional.

Example 2.5.2 (Examples and Nonexamples).

(i) $\mathbb{F}^n$ is **finite dimensional** because

$$\mathbb{F}^n = \operatorname{span}\{e_1, e_2, \ldots, e_n\},$$

where e_i's are defined in Example 2.4.8.

(ii) From above, it is also clear $M_{m\times n}(\mathbb{F})$ is **finite dimensional**.

(iii) For $n \geq 1$,

$$\mathbb{P}_n(\mathbb{F}) = \{\textstyle\sum_{i=0}^n a_i x^i : a_1, \ldots, a_n \in \mathbb{F}\} = \operatorname{span}\{1, x, x^2, \ldots, x^n\}$$

is **finite dimensional**.

(iv) The vector space of polynomials

$$\mathbb{P}(\mathbb{F}) := \{\text{polynomial over } \mathbb{F}\} = \bigcup_{n=0}^{\infty} \mathbb{P}_n(\mathbb{F})$$

is **infinite dimensional**. To see this, suppose $\mathbb{P}(\mathbb{F})$ is finite dimensional, then we can find $p_1, p_2, \ldots, p_n \in \mathbb{P}(\mathbb{F})$ such that

$$\mathbb{P}(\mathbb{F}) = \operatorname{span}\{p_1, p_2, \ldots, p_n\}.$$

Let $N = \max\{\deg p_i : i = 1, 2, \ldots, n\}$, then $p \in \mathbb{P}(\mathbb{F}) \implies \deg p \leq N$, i.e., the maximal possible degree of polynomials $\mathbb{P}(\mathbb{F})$ is bounded, this is impossible since $x^{N+1} \in \mathbb{P}(\mathbb{F})$ but $x \notin \operatorname{span}\{p_1, \ldots, p_n\}$.

The same proof as in (iv) of Example 2.5.2 shows that for any interval $I \subseteq \mathbb{R}$, $\mathbb{P}(\mathbb{R})|_I := \{p|_I : p \in \mathbb{P}(\mathbb{R})\}$ is also infinite dimensional. It is also natural to tell whether or not $C([0,1],\mathbb{R})$ is infinite dimensional. Since

$$C([0,1],\mathbb{R}) \supseteq \mathbb{P}(\mathbb{R})|_{[0,1]},$$

we can imagine $C([0,1],\mathbb{R})$ contains a very "big" vector space, so $C([0,1],\mathbb{R})$ must also be very "big". Indeed $C([0,1],\mathbb{R})$ is **infinite dimensional**, which follows quite trivially after we make the "bigness" precise in Section 2.7. Still we will give a proof in Example 2.6.12 before we try to define the "size" of a vector space.

2.6 Bases

Definition 2.6.1. Let V be finite dimensional, a finite set $\{v_1,\dots,v_n\}$ in V is said to be a **basis** of V if:

(i) $V = \operatorname{span}\{v_1, v_2, \dots, v_n\}$.

(ii) $v_1, v_2, \dots, v_n$ are linearly independent.

In this text by basis we always mean a **finite set**, i.e., a collection of *finitely many* vectors. Before giving examples, we give another useful characterization of bases which help us to make sense of the concept *coordinates* in section 3.2.1.

Theorem 2.6.2. *Let V be a vector space, then the following are equivalent:*

(i) $\{v_1, v_2, \dots, v_n\}$ in V is a basis of V.

(ii) For every $v \in V$ there are unique $a_1, a_2, \dots, a_n \in \mathbb{F}$ such that

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n.$$

Proof. (i) $\Rightarrow$ (ii) Let $\{v_1, v_2, \dots, v_n\}$ be a basis of V, if there are $a_1,\dots,a_n \in \mathbb{F}$ and $b_1,\dots,b_n \in \mathbb{F}$ such that

$$v = \sum_{i=1}^n a_iv_i = \sum_{i=1}^n b_iv_i,$$

then $\sum_{i=1}^n (a_i - b_i)v_i = 0$, but $v_1,\dots,v_n$ are linearly independent, we have necessarily $a_i - b_i = 0$, for all i, i.e., $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$.

(ii) $\Rightarrow$ (i) Let $a_1, a_2, \dots, a_n \in \mathbb{F}$ be such that $a_1v_1 + \cdots + a_nv_n = 0$, then

$$a_1v_1 + \cdots + a_nv_n = 0v_1 + \cdots + 0v_n,$$

but then by (ii), we have $a_1 = 0, a_2 = 0, \dots, a_n = 0$. ☐

Example 2.6.3 (Some Bases).

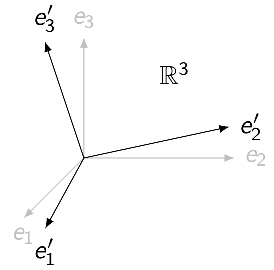
(i) $\{1, x, x^2, \dots, x^n\}$ is a basis of $\mathbb{P}_n(\mathbb{F})$.

(ii) The collection

$$\{e_1, e_2, \dots, e_n\}, \tag{2.6.4}$$

as defined in Example 2.4.8 of, spans $\mathbb{F}^n$ and is linearly independent, thus it forms a basis in $\mathbb{F}^n$. Since this is the most natural choice of bases, (2.6.4) is called a **standard basis** of $\mathbb{F}^n$.

(iii) In $\mathbb{R}^3$, if e_1, e_2, e_3 are rotated by the same angles, they still form a basis in $\mathbb{R}^3$.



Example 2.6.5. We find the dimension of the vector space

$$\mathcal{F} := \{\text{real-valued function defined on } \{1, 2, \ldots, n\}\}.$$

In what follows we will construct a basis of $\mathcal{F}$ which has length n, thus $\dim \mathcal{F} = n$.

We define functions $e_1, e_2, \ldots, e_n : \{1, 2, \ldots, n\} \to \{0, 1\}$ by: for each $i = 1, 2, \ldots, n$, let $j \in \{1, 2, \ldots, n\}$, we define

$$e_i(j) = \delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Then given $f \in \mathcal{F}$, we have for each $k = 1, 2, \ldots, n$

$$f(k) = \sum_{i=1}^{n} f(i) e_i(k),$$

i.e., as a function on $\{1, 2, \ldots, n\}$ we conclude that $f = \sum_{i=1}^{n} f(i) e_i \in \operatorname{span}\{e_1, e_2, \ldots, e_n\}$, hence $\mathcal{F} \subseteq \operatorname{span}\{e_1, e_2, \ldots, e_n\}$. The reverse inclusion is obvious, so

$$\mathcal{F} = \operatorname{span}\{e_1, e_2, \ldots, e_n\},$$

showing that $\mathcal{F}$ is finite dimensional.

Not only that, $\{e_1, e_2, \ldots, e_n\}$ is linearly independent. To see this , let $a_i \in \mathbb{R}$ be such that

$$a_1 e_1 + a_2 e_2 + \cdots + a_n e_n = 0.$$

Recall that the above equality means a equality of two functions on $\{1, 2, \ldots, n\}$. In particular, if we evaluate at $i \in \{1, 2, \ldots, n\}$, then

$$a_1 e_1(i) + a_2 e_2(i) + \cdots + a_n e_n(i) = 0.$$

LHS of the above equation is a_i, and this is true for each $i = 1, 2, \ldots, n$, hence

$$a_1 = a_2 = \cdots = a_n = 0.$$

So $\{e_1, \ldots, e_n\}$ is a basis of $\mathcal{F}$.

Example 2.6.6. Let V, W be vector spaces, if V has a basis $\{v_1, \ldots, v_n\}$ and W has a basis $\{w_1, \ldots, w_k\}$, what is the basis of $V \times W$?

Here $V \times W$ is a vector space with the naturally defined addition and scalar multiplication given in Example 2.4.5.

Firstly we find a spanning set of $V \times W$. For every $(v, w) \in V \times W$, there are $a_i, b_i \in \mathbb{F}$ such that

$$v = \sum_{i=1}^{n} a_i v_i \quad \text{and} \quad w = \sum_{j=1}^{k} b_j w_j,$$

it follows that

$$\begin{aligned}(v, w) &= \left(\sum_{i=1}^{n} a_i v_i, \sum_{j=1}^{k} b_j w_j\right) = \left(\sum_{i=1}^{n} a_i v_i, 0\right) + \left(0, \sum_{j=1}^{k} b_j w_j\right) \\ &= \sum_{i=1}^{n} a_i(v_i, 0) + \sum_{j=1}^{k} b_j(0, w_j) \\ &\in \operatorname{span}\{(v_i, 0), (0, w_i) : i = 1, 2, \dots, n, j = 1, 2, \dots, k\}.\end{aligned}$$

The linearly independnce of $\{(v_i, 0), (0, w_i) : i = 1, 2, \dots, n, j = 1, 2, \dots, k\}$ is easily verified, hence it is a basis of $V \times W$.

Next we present three fundamental results regarding to bases of finite dimensional vector spaces in Theorem 2.6.7, Theorem 2.6.8 and Theorem 2.6.9. They will provide us a base to build the concept of dimensional in the next section.

Theorem 2.6.7. *Let V be finite dimensional. Every (finite) set of vectors that spans V can be reduced into a basis of V*(*).

Proof. Let $\{v_1, \dots, v_n\}$ be a spanning set of V. We may assume $v_i \neq 0$ for all i, otherwise delete it in the list. Let $\alpha = \{v_1, v_2, \dots, v_n\}$.

Step 1
If $v_2 \in \operatorname{span}\{v_1\}$, delete this in α.
Else if $v_2 \notin \operatorname{span}\{v_1\}$, then leave α unchanged.

Step 2
If $v_3 \in \operatorname{span}\{v_1, v_2\}$, delete this in α.
Else if $v_3 \notin \operatorname{span}\{v_1, v_2\}$, leave α unchanged.

Step j
If $v_{j+1} \in \operatorname{span}\{v_1, v_2, \dots, v_j\}$, delete this in α.
Else if $v_{j+1} \notin \operatorname{span}\{v_1, v_2, \dots, v_j\}$, leave α unchanged.

After the step $j = n - 1$, the process terminates. The resulting list α' spans V because we have only discarded vectors that is in the span of the previous ones. Also since each later vector (in terms of index) in α' is not in the span of vectors preceding it, so α' is linearly independent. □

Theorem 2.6.8. *Every finite dimensional vector space has a basis.*

Proof. V being finite dimensional can be spanned by finitely many vectors in V. Then by Theorem 2.6.7 we can reduce this spanning set of V into a basis. □

Theorem 2.6.9. *Let V be finite dimensional. Every linearly independent set in V can be extended to a basis in V.*

(*) It is a finite set by our definition.

Proof. Let $\{v_1, \ldots, v_k\}$ be linearly independent in V and let $\beta = \{b_1, \ldots, b_n\}$ be a basis of V (exists by Theorem 2.6.8). If $\{v_1, \ldots, v_k\}$ is already a basis of V, then we are done.

Suppose now $\{v_1, \ldots, v_k\}$ is not a basis of V.

Step 1
Since $b_1, \ldots, b_n, v_1$ are linearly dependent, there is $b_i \in \operatorname{span}(\{b_1, \ldots, b_n, v_1\} \setminus \{b_i\})$. Discard this b_i from β to get β_1, then $\beta_1 \cup \{v_1\}$ is a basis of V since $v_1 \notin \operatorname{span} \beta_1$.

Step 2
$\beta_1 \cup \{v_1, v_2\}$ is linearly dependent, there is $b_i \in \beta_1$ such that $b_i \in \operatorname{span}(\beta_1 \cup \{v_1, v_2\} \setminus \{b_i\})$, we can discard this b_i from β_1 to get β_2, then $\beta_2 \cup \{v_1, v_2\}$ is a basis of V since $v_2 \notin \operatorname{span}(\beta_2 \cup \{v_1\})$.

Step j
Since $\beta_{j-1} \cup \{v_1, v_2, \ldots, v_j\}$ is linearly dependent, we can discard one of b_i's from β_{j-1} to get β_j such that $\beta_j \cup \{v_1, v_2, \ldots, v_j\}$ is a basis of V.

If in one of the steps $j = 1, 2, \ldots, k-1$, b_i's all disappear in the resulting basis, then $\{v_1, \ldots, v_j\}$ will be a basis of V, a contradiction. Hence the process can continue and stop when $j = k$, and

$$\beta_k \cup \{v_1, v_2, \ldots, v_k\}$$

is a basis of V, where $\emptyset \neq \beta_k \subseteq \beta$.

In fact we have proved a more refined statement:

Let $\{b_1, \ldots, b_n\}$ be a basis of V. Every linearly independent set in V ***that is not a basis*** *can be extended to a basis in V that has cardinality n.*

We will directly use this result in the next proof. □

Remark. Extending a given set of linearly independent vectors to a basis of a vector space is a very basic technique in linear algebra. Later this will be our fundamental technique to prove various results concerning "dimension".

Corollary 2.6.10. *Let V be finite dimensional and $\{b_1, b_2, \ldots, b_n\}$ its basis. Any linearly independent set $\{v_1, v_2, \ldots, v_k\}$ in V must satisfy $k \leq n$.*

Proof. If $\alpha = \{v_1, \ldots, v_k\}$ is not a basis, by the last paragraph in the proof of Theorem 2.6.9, we can extend α to a basis of V with length n. Thus $k < n$.

On the other hand, if $\{v_1, \ldots, v_k\}$ is a basis of V, then $\{v_1, \ldots, v_{k-1}\}$ cannot be a basis, and the previous paragraph shows us $k - 1 < n$, i.e.,

$$(k-1) + 1 \leq n \iff k \leq n.$$ □

Proposition 2.6.11. *Let V be a finite dimensional vector space, then every vector subspace W of V must be finite dimensional.*

Proof. By Theorem 2.6.8, V has a basis $\{v_1, v_2, \ldots, v_n\}$.

If $W = \{0\}$, then we are done. If $W \neq \{0\}$, then we can take $w_1 \in W \setminus \{0\}$. If $W = \operatorname{span}\{w_1\}$, then we are done, otherwise we can take $w_2 \notin \setminus \operatorname{span}\{w_1\}$. This process can be continued to obtain a linearly independent set $\{w_1, w_2, \ldots, w_j\}$.

By Corollary 2.6.10, $j \le n$, hence the process must terminate at some step $j \le n$, and
$$W = \operatorname{span}\{w_1, w_2, \ldots, w_j\},$$
i.e., W is finite dimensional. □

We can now explain why $C([0,1],\mathbb{R})$ is infinite dimensional.

Example 2.6.12. Since $\mathbb{P}(\mathbb{R})|_{[0,1]}$ is a subspace of $C([0,1],\mathbb{R})$, if $C([0,1],\mathbb{R})$ is finite dimensional, so is $\mathbb{P}(\mathbb{R})|_{[0,1]}$ by Proposition 2.6.11, a contradiction. Hence $C([0,1],\mathbb{R})$ must be infinite dimensional.

2.7 Dimension

The dimension of a finite dimensional vector space can be defined due to the following result:

Theorem 2.7.1. *Any two bases of a finite dimensional vector space have the same* ***length*** *(i.e., cardinality).*

Proof. Let α and β be two bases, then by Corollary 2.6.10, since α is a basis, β is linearly independent, $|\beta| \le |\alpha|$. Similarly, β is a basis and α is linearly independent, thus $|\alpha| \le |\beta|$, it follows that $|\alpha| = |\beta|$. □

Definition 2.7.2. Let V be finite dimensional. If $V \neq \{0\}$, we defined the **dimension** of V, denoted by $\dim V$, to be the length of any basis in V. If $V = \{0\}$, we define $\dim V = 0$.

Several remarks are in order:

- Given a finite dimensional vector space V, we have $\dim V = 0 \iff V = \{0\}$.
- A vector space V is finite dimensional if and only if $\dim V < \infty$.
- If $\{v_1, v_2, \ldots, v_n\}$ is linearly independent, then
$$\dim\big(\operatorname{span}\{v_1, v_2, \ldots, v_n\}\big) = n.$$

Example 2.7.3.

(i) $\dim\{0\} = 0$, this is by definition.

(ii) $\dim \mathbb{F}^n = n$ since it has the standard basis $\{e_1, e_2, \ldots, e_n\}$ which has length n.

(iii) $\dim M_{m\times n}(\mathbb{F}) = mn$ since it has the standard basis E_{ij}, where for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$,
$$E_{11} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, E_{12} \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, \ldots, E_{mn} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$
Namely, $E_{hk} = [a_{ij}]_{m\times n}$, where $a_{hk} = 1$ and $a_{ij} = 0$ when $(i,j) \neq (h,k)$.

(iv) $\dim \mathbb{P}_n(\mathbb{F}) = n+1$ since the basis $\{1, x, x^2, \dots, x^n\}$ has length $n+1$.

(v) $\dim \mathcal{F} = n$, where $\mathcal{F}$ is defined in Example 2.6.5 with basis $e_1, e_2, \dots, e_n$.

Theorem 2.7.4. *Let V be a vector space.*

(i) Every subspace U of V satisfies $\dim U \le \dim V$.

If further V is finite dimensional, then:

(ii) Every set of vectors that spans V with length $\dim V$ is a basis of V.

(iii) Every linearly independent set of vectors in V with length $\dim V$ is a basis of V.

Proof. (i) If $\dim V = \infty$, then the inequality is trivial. Let's assume $\dim V < \infty$. By Proposition 2.6.11, U is also finite dimensional, by Theorem 2.6.8, U has a basis $\alpha = \{u_1, u_2, \dots, u_k\}$, by Theorem 2.6.9 we can extend α to α' a basis of V, then

$$\dim U = |\alpha| \le |\alpha'| = \dim V.$$

(ii) Let $n = \dim V$ and $\{v_1, v_2, \dots, v_n\}$ spans V. If $\{v_1, v_2, \dots, v_n\}$ is linearly dependent, then there is v_i such that

$$V = \operatorname{span}\{v_1, v_2, \dots, v_n\} = \operatorname{span}(\{v_1, v_2, \dots, v_n\} \setminus \{v_i\}),$$

but then by (i),

$$n = \dim V = \dim\big(\operatorname{span}(\{v_1, v_2, \dots, v_n\} \setminus \{v_i\})\big) \le n-1,$$

where the last inequality follows from Theorem 2.6.7, a contradiction.

(iii) Let $n = \dim V$ and $\{v_1, v_2, \dots, v_n\}$ a linearly independent set. If

$$\operatorname{span}\{v_1, v_2, \dots, v_n\} \ne V,$$

then we can find a $v \notin \operatorname{span}\{v_1, v_2, \dots, v_n\}$, so $\{v, v_1, v_2, \dots, v_n\}$ is linearly independent by (ii) of Theorem 2.3.2.

However, since $\{v, v_1, v_2, \dots, v_n\}$ is a basis of $\operatorname{span}\{v, v_1, v_2, \dots, v_n\} \subseteq V$, (i) implies

$$n+1 = \dim\big(\operatorname{span}\{v, v_1, v_2, \dots, v_n\}\big) \le V = n,$$

a contradiction. □

Example 2.7.5. Reconsider (iv) of Example 2.5.2: We can show that $\mathbb{P}(\mathbb{F})$ is infinite dimensional by using (i) of Theorem 2.7.4.

Indeed, since $\mathbb{P}(\mathbb{F}) = \bigcup_{n=1}^{\infty} \mathbb{P}_n(\mathbb{F})$, it follows that for each $n \in \mathbb{N}$,

$$\mathbb{P}(\mathbb{F}) \supseteq \mathbb{P}_n(\mathbb{F}) \implies \dim \mathbb{P}(\mathbb{F}) \ge \dim \mathbb{P}_n(\mathbb{F}) = n+1.$$

Let $n \to \infty$, $\dim \mathbb{P}(\mathbb{F}) = \infty$.

Example 2.7.6. The vector space $\mathbb{F}^\infty := \{(x_1, x_2, \dots) : x_1, x_2, \dots \in \mathbb{F}\}$ is not finite dimensional. To see this, for each $n \in \mathbb{N}$ we let

$$V_n = \{(x_1, x_2, \dots, x_n, 0, 0, \dots) : x_1, x_2, \dots, x_n \in \mathbb{F}\},$$

V_n is a subspace of $\mathbb{F}^\infty$. By (i) of Theorem 2.7.4,

$$\dim \mathbb{F}^\infty \geq \dim V_n \xlongequal{\text{(why?)}} n,$$

by letting $n \to \infty$, we have $\dim \mathbb{F}^\infty = \infty$.

Example 2.7.7. Suppose that V is finite dimensional and U is a subspace of V. If $\dim U = \dim V$, then necessarily $U = V$.

To prove this, let $\{u_1, u_2, \ldots, u_n\}$ be a basis of U, then $n = \dim U = \dim V$. By hypothesis $U \subseteq V$, we try to show that $V \subseteq U = \text{span}\{u_1, u_2, \ldots, u_n\}$, therefore $V = U$.

Suppose not, i.e., there is $v \in V$ such that $v \neq 0$ and $v \notin \text{span}\{u_1, u_2, \ldots, u_n\}$, then

$$\text{span}\{u_1, u_2, \ldots, u_n, v\} \subseteq V.$$

Since $\{u_1, u_2, \ldots, u_n, v\}$ is linearly independent in V (by Theorem 2.3.2), it is a basis of $\text{span}\{u_1, \ldots, u_n, v\}$, it follows that by (i) of Theorem 2.7.4,

$$n + 1 = \dim \big(\text{span}\{u_1, u_2, \ldots, u_n, v\}\big) \leq \dim V = n,$$

a contradiction! We conclude $V \subseteq U$, as desired.

Example 2.7.8. Let V and W be finite dimensional, we show that

$$\dim V \times W = \dim V + \dim W.$$

Indeed, let $\{v_1, \ldots, v_n\}$ be a basis of V and $\{w_1, \ldots, w_k\}$ a basis of W, then by Example 2.6.6,

$$\{(v_1, 0), \ldots, (v_n, 0), (0, w_1), \ldots (0, w_k)\}$$

is a basis of $V \times W$, hence

$$\dim(V + W) = n + k = \dim V + \dim W.$$

The structure of a vector V space can be simplified by writing it as a direct sum $V = U \oplus W$. One can see that the Cartesian product $U \times W$ looks very similar to the decomposition $U \oplus W$, one similarity is that every element in $U \times W$ can be written uniquely as (u, w), while every element in $U \oplus W$ can be written uniquely as $u + w$. Another similarity (compared to Example 2.7.8) is the following:

Proposition 2.7.9. *Let V be finite dimensional and U, W be subspaces such that $V = U \oplus W$, then*

$$\dim(U \oplus W) = \dim U + \dim W.$$

Therefore $U \oplus W$ is usually called the **internal direct sum** and $U \times W$ is usually called the **external direct sum** as they are indeed the same algebraically.

Proof. Let $\{u_1, \ldots, u_m\}$ be a basis of U and $\{w_1, \ldots, w_n\}$ a basis of W, then

$$\alpha = \{u_1, \ldots, u_m, w_1, \ldots, w_n\}$$

spans $U \oplus W$. Since $U \cap W = \{0\}$, the set α is linearly independent because

$$\begin{aligned}\sum_{i=1}^{m} a_i u_i + \sum_{i=1}^{n} b_i w_i = 0 &\implies \sum_{i=1}^{m} a_i u_i = \sum_{i=1}^{n} (-b_i) w_i \in U \cap W = \{0\} \\ &\implies a_1 = a_2 = \cdots = a_m = b_1 = b_2 = \cdots = b_n = 0.\end{aligned}$$

Hence α is a basis of $U \oplus W$, thus

$$\dim(U \oplus W) = m + n = \dim U + \dim W.$$

□

Example 2.7.10. Let V be finite dimensional and U, W subspaces of V. If $\dim U + \dim W > \dim V$, then the intersection $U \cap W$ is nontrivial[†], i.e., $U \cap W \neq \{0\}$.

To prove this, let's for the sake of contradiction suppose that $U \cap W = \{0\}$. Then the sum $U + W$ is actually a direct sum $U \oplus W$, which is a subspace of V. Hence from hypothesis, (i) of Theorem 2.7.4 and Proposition 2.7.9, we have

$$\dim V < \dim U + \dim W = \dim(U \oplus W) \leq \dim V,$$

a contradiction.

We have several results above which involve the dimension of the vector space $U + V$, in fact we can relate $\dim(U + V)$ with $\dim U, \dim V$ and $\dim U \cap V$:

Theorem 2.7.11. *Let U and W be subspaces of a finite dimensional vector space V, then*

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

As a general rule, whenever we are asked to prove the relation between various dimensions, the most natural attempt is to count the basis.

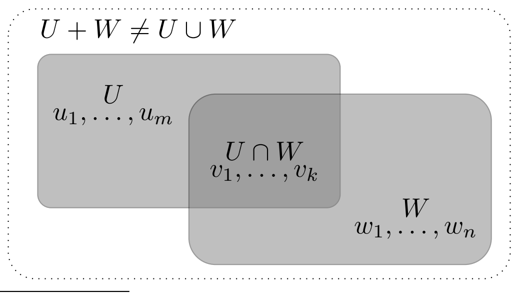
Proof. If one of U and W is zero vector space, then we are done. From now on we exclude this trivial case.

Case 1. If $U \cap W = \{0\}$, namely, $U + W = U \oplus W$, we are done by Proposition 2.7.9.

Case 2. Assume $U \cap W \neq \{0\}$.

Case 2.1. If $U \subseteq W$ or $W \subseteq U$, then we are also done.

Case 2.2. Assume $U \not\subseteq W$ and $W \not\subseteq U$. We let $\{v_1, v_2, \ldots, v_k\}$ be a basis of of $U \cap W$; by Theorem 2.6.9 we can extend the set to a basis of U, $\{v_1, \ldots, v_k, u_1, \ldots, u_m\}$; On the other hand, we can also extend the set to a basis of W, $\{v_1, \ldots, v_k, w_1, \ldots, w_n\}$.



(†) A subspace of V is said to be **trivial** if it is $\{0\}$, as it is too simple.

Obviously $U + W = \operatorname{span}\{v_1, \ldots, v_k, u_1, \ldots, u_m, w_1, \ldots, w_n\}$, we wish

$$\{v_1, \ldots, v_k, u_1, \ldots, u_m, w_1, \ldots, w_n\}$$

could be linearly independent. To prove this, let $a_i, b_i, c_i \in \mathbb{F}$ be such that

$$\sum_{i=1}^{k} a_i v_i + \sum_{i=1}^{m} b_i u_i + \sum_{i=1}^{n} c_i w_i = 0, \tag{2.7.12}$$

then

$$\sum_{i=1}^{n} c_i w_i = -\Big(\sum_{i=1}^{k} a_i v_i + \sum_{i=1}^{m} b_i u_i\Big) \in U \cap W = \operatorname{span}\{v_1, \ldots, v_k\}.$$

Since $v_1, \ldots, v_k, w_1, \ldots, w_n$ are linearly independent, $c_i = 0$, for all i. (2.7.12) becomes

$$\sum_{i=1}^{k} a_i v_i + \sum_{i=1}^{m} b_i u_i = 0,$$

again, $u_1, \ldots u_m, v_1, \ldots, v_k$ are linearly independent, hence all $a_i = 0$ and all $b_i = 0$.

Conclusion: $\{v_1, \ldots, v_k, u_1, \ldots, u_m, w_1, \ldots, w_n\}$ is a basis of $U + W$. Finally,

$$\begin{aligned}\dim(U + W) &= k + m + n \\ &= (k + m) + (k + n) - k \\ &= \dim U + \dim W - \dim(U \cap W).\end{aligned}$$

□

2.8 Subspaces of $\mathbb{F}^n$

2.8.1 Null Spaces, Column Spaces and Row Spaces

Now we return to subspaces of $\mathbb{F}^n$.

Definition 2.8.1. Given a matrix $A \in M_{m\times n}(\mathbb{F})$, we define

$$\operatorname{Nul} A = \{x \in \mathbb{F}^n : Ax = 0\}, \quad \operatorname{Col} A = \{Ax : x \in \mathbb{F}^n\},$$

called **null space** of A and **column space** of A respectively. Also, we define the **row space** of A by

$$\operatorname{Row} A = \operatorname{Col} A^T.$$

Remark. Due to linearity of $A \in M_{m\times n}(\mathbb{F})$ (Corollary 1.2.7), $\operatorname{Nul} A$, $\operatorname{Col} A$ and $\operatorname{Row} A$ are subspaces of $\mathbb{F}^n$, $\mathbb{F}^m$ and $\mathbb{F}^n$ respectively. Note that

$$\operatorname{Col} A = \text{image of } A.$$

Hence A is surjective if and only if $\operatorname{Col} A = \mathbb{F}^m$.

Example 2.8.2. Let $A \in M_{m\times n}(\mathbb{F})$, it can be shown that

$$A \text{ is injective} \iff \operatorname{Nul} A = \{0\} \iff \big(Ax = 0 \implies x = 0\big).$$

We just prove the first two are equivalent since the last two are somewhat a restatement of definition.

($\Rightarrow$). Assume A is injective. Let $x \in \operatorname{Nul} A$, then $Ax = 0$, but $A0 = 0$, hence $Ax = A0$, injectivity of A forces $x = 0$, so $x \in \{0\}$. The implication says that $\operatorname{Nul} A \subseteq \{0\}$, thus $\operatorname{Nul} A = \{0\}$.

($\Leftarrow$). Assume $\operatorname{Nul} A = \{0\}$, let $x, y \in \mathbb{F}^n$ such that $Ax = Ay$, then $A(x - y) = 0$, so $x - y \in \operatorname{Nul} A = \{0\}$, i.e., $x = y$. We conclude A is injective.

Example 2.8.3. Let

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 4 & 5 & 6 \end{bmatrix} \in M_{3\times 3}(\mathbb{R}).$$

Loosely speaking, $\operatorname{Col} A$ is the space spanned by columns and $\operatorname{Row} A$ is the space spanned by rows. Thus by definition,

$$\operatorname{Col} A = \left\{ A \begin{bmatrix} x \\ y \\ z \end{bmatrix} : x, y, z \in \mathbb{R} \right\} = \operatorname{span} \left\{ \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 5 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 6 \end{bmatrix} \right\}.$$

Also,

$$\operatorname{Row} A = \operatorname{Col} A^T = \left\{ A^T \begin{bmatrix} x \\ y \\ z \end{bmatrix} : x, y, z \in \mathbb{R} \right\} = \operatorname{span} \left\{ \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} \right\}.$$

Example 2.8.4 (Dimension of $\operatorname{Nul} A$). We try to compute $\dim \operatorname{Nul} A$, where

$$A = \begin{bmatrix} 1 & 2 & -2 & 3 \\ 2 & 4 & -3 & 4 \\ 5 & 10 & -8 & 11 \end{bmatrix} \in M_{3\times 4}(\mathbb{R}).$$

To count dimension, we first find a basis of $\operatorname{Nul} A$. Let $x \in \operatorname{Nul} A$, since

$$\begin{bmatrix} 1 & 2 & -2 & 3 \\ 2 & 4 & -3 & 4 \\ 5 & 10 & -8 & 11 \end{bmatrix} \to \cdots \to \begin{bmatrix} 1 & 2 & 0 & -1 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

the system $Ax = 0$ is equivalent to

$$\begin{cases} x_1 + 2x_2 - x_4 = 0 \\ x_3 - 2x_4 = 0 \end{cases}.$$

Here x_2 and x_4 are free variables, we let $x_2 = s$ and $x_4 = t$, then $x_1 = t - 2s$ and $x_3 = 2t$, hence

$$\operatorname{Nul} A = \left\{ \begin{bmatrix} t - 2s \\ s \\ 2t \\ t \end{bmatrix} = s \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t \begin{bmatrix} 1 \\ 0 \\ 2 \\ 1 \end{bmatrix} : s, t \in \mathbb{R} \right\} = \operatorname{span} \left\{ \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \\ 1 \end{bmatrix} \right\}.$$

Since $\left[\begin{smallmatrix} -2 \\ 1 \\ 0 \\ 0 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 \\ 0 \\ 2 \\ 1 \end{smallmatrix}\right]$ are linearly independent, we conclude $\dim \operatorname{Nul} A = \boxed{2}$.

To find a basis of $\operatorname{Col} A$, we use the row operation technique:

Theorem 2.8.5. *Let $A \in M_{m\times n}(\mathbb{F})$ be reduced to row echelon form R and $A = [a_1 \quad \cdots \quad a_n]$, $a_i \in \mathbb{F}^m$. If $i_1, i_2, \ldots, i_k$th columns of R are pivot columns, then*

$$\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$$

is a basis of $\operatorname{Col} A$.

Proof. We let E be the product of elementary matrices such that $EA = R$. Since $i_1, i_2, \ldots, i_k$th columns (with $i_1 < i_2 < \cdots < i_k$) of EA are pivotal, then

$$Ea_{i_1} = e_1, Ea_{i_2} = e_2, \ldots, Ea_{i_k} = e_k.$$

It is easy to see that $a_{i_1}, \ldots, a_{i_k}$ are linearly independent. Now we show that every column in A is in the span of $\{a_{i_j} : j = 1, 2, \ldots, k\}$. Indeed, for $p = 1, 2, \ldots, n$,

$$Ea_p = \sum_{j=1}^{k} b_j e_j = \sum_{j=1}^{k} b_j E a_{i_j} \implies a_p = \sum_{j=1}^{k} b_j a_{i_j}.$$

Since each columns of A is in the span of $\{a_{i_j} : j = 1, 2, \ldots, k\}$, thus

$$\operatorname{Col} A = \operatorname{span}\{a_{i_j} : j = 1, 2, \ldots, k\}.$$

□

Example 2.8.6 (Dimension of $\operatorname{Col} A$). We try to compute $\dim \operatorname{Col} A$, where

$$A = \begin{bmatrix} 1 & 2 & -2 & 3 \\ 2 & 4 & -3 & 4 \\ 5 & 10 & -8 & 11 \end{bmatrix} \in M_{3\times 4}(\mathbb{R}).$$

From Example 2.8.4

$$\begin{bmatrix} 1 & 2 & -2 & 3 \\ 2 & 4 & -3 & 4 \\ 5 & 10 & -8 & 11 \end{bmatrix} \to \cdots \to \begin{bmatrix} 1 & 2 & 0 & -1 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

since the first and the third columns of the reduced echelon form are pivotal, $\left[\begin{smallmatrix} 1 \\ 2 \\ 5 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 2 \\ 3 \\ 8 \end{smallmatrix}\right]$ form a basis of $\operatorname{Col} A$, we have $\dim \operatorname{Col} A = \boxed{2}$.

Finally, what is $\dim \operatorname{Row} A = \dim \operatorname{Col} A^T$?

Theorem 2.8.7. *Let $A \in M_{m\times n}(\mathbb{F})$, then*

$$\underbrace{\dim \operatorname{Col} A}_{\text{column rank}} = \underbrace{\dim \operatorname{Col} A^T}_{\text{row rank}}.$$

Proof. Let E be an elementary matrix such that EA is in reduced row echelon form and assume that $i_1, i_2, \ldots, i_k$th columns ($i_1 < i_2 < \cdots < i_k$) of EA are pivotal, then by Theorem 2.8.5, $\dim \operatorname{Col} A = k$. On the other hand, $(EA)^T = A^T E^T$ and $\operatorname{Col}(A^T E^T) = \operatorname{Col}(A^T)$, so

$$\dim \operatorname{Col} A^T = \dim \operatorname{Col}(A^T E^T) = \dim \operatorname{Col}(EA)^T.$$

Since EA is the reduced row echelon form of A, only the first k rows are nonzero, hence $\operatorname{Col}(EA)^T$ is spanned by first k columns of $(EA)^T$ which are linearly independent, thus $\dim \operatorname{Col} A^T = k$. □

Definition 2.8.8. For any matrix A, we define the **rank** of A to be

$$\operatorname{rank} A = \dim \operatorname{Col} A.$$

Now Theorem 2.8.7 can be rephrased as $\operatorname{rank} A = \operatorname{rank} A^T$.

Definition 2.8.9. A matrix $A \in M_{m\times n}(\mathbb{F})$ is said to be of **full rank** if

$$\operatorname{rank} A = \min\{m, n\}.$$

In other words, it has the maximum possible rank among matrices in $M_{m\times n}(\mathbb{F})$.

2.8.2 Rank-Nullity Theorem

The computational Example 2.8.4 and Example 2.8.6 provide us the evidence that

$$\boxed{\text{\# of free variables}} = \dim \operatorname{Nul} A \quad \text{and} \quad \boxed{\text{\# of pivot columns}} = \dim \operatorname{Col} A,$$

in fact we have:

Theorem 2.8.10 (Rank-Nullity). *If $A \in M_{m\times n}(\mathbb{F})$, then*

$$n = \dim \operatorname{Nul} A + \dim \operatorname{Col} A. \tag{$*$}$$

Proof. Note that $\operatorname{Nul} A \subseteq \mathbb{F}^n$ and $\operatorname{Col} A \subseteq \mathbb{F}^m$. If $\dim \operatorname{Nul} A = n$, then we are done since in this case by Example 2.7.7, $\operatorname{Nul} A = \mathbb{F}^n$, then $Ax = 0$ for each $x \in \mathbb{F}^n$ and thus $\operatorname{Col} A = \{0\}$, hence $(*)$ is true.

Suppose $\dim \operatorname{Nul} A = k < n$. Let $\{u_1, u_2, \dots, u_k\}$ be a basis of $\operatorname{Nul} A$, we extend it to

$$\{u_1, \dots, u_k, u_{k+1}, \dots, u_n\}$$

a basis of $\mathbb{F}^n$, we show that $\operatorname{Col} A = \operatorname{span}\{Au_{k+1}, \dots, Au_n\}$. Indeed, for every $x \in \mathbb{F}^n$, there are $a_i \in \mathbb{F}$ such that $x = \sum_{i=1}^n a_i u_i$, it follows that

$$Ax = A\left(\sum_{i=1}^n a_i u_i\right) = \sum_{i=1}^n a_i A u_i = \sum_{i=k+1}^n a_i A u_i \in \operatorname{span}\{Au_{k+1}, \dots, Au_m\},$$

thus $\operatorname{Col} A \subseteq \operatorname{span}\{Au_{k+1}, \dots, Au_m\}$, as the reverse inclusion is obvious, thus the set equality is proved.

Finally we check that $\{Au_{k+1}, \dots, Au_n\}$ is linearly independent. Suppose there are $b_{k+1}, \dots, b_n \in \mathbb{F}$ such that $\sum_{i=k+1}^n b_i A u_i = 0$, then $\sum_{i=k+1}^n b_i u_i \in \operatorname{Nul} A = \operatorname{span}\{u_1, u_2, \dots, u_k\}$. But $u_1, u_2, \dots, u_n$ are linearly independent, hence necessarily $b_{k+1}, \dots, b_n = 0$, as desired. Thus $\dim \operatorname{Col} A = n - k$, and therefore

$$\dim \operatorname{Nul} A + \dim \operatorname{Col} A = k + (n - k) = n. \qquad \square$$

Corollary 2.8.11. *Let A be a square matrix, then the following are equivalent:*

(i) A is injective. *(ii) A is surjective.* *(iii) A is invertible.*

Now we are going to prove the chain

$$\text{(iii)} \implies \text{(i)} \implies \text{(ii)} \implies \text{(iii)}.$$

Proof. (iii) $\Rightarrow$ (i) Since A is invertible $\iff$ A is $1-1$ and onto, hence (i) follows.

(i) $\Rightarrow$ (ii) Assume A is injective, then equivalently, $\operatorname{Nul} A = \{0\}$, hence by rank-nullity theorem,

$$n = 0 + \dim \operatorname{Col} A,$$

hence $\dim \operatorname{Col} A = n$ and $\operatorname{Col} A \subseteq \mathbb{F}^n$, by Example 2.7.7, $\operatorname{Col} A = \mathbb{F}^n$, showing that A is surjective.

(ii) $\Rightarrow$ (iii) Assume A is surjective, then $\operatorname{Col} A = \mathbb{F}^n$, by rank-nullity theorem again,

$$n = \dim \operatorname{Nul} A + \dim \operatorname{Col} A = \dim \operatorname{Nul} A + n,$$

and thus $\dim \operatorname{Nul} A = 0$, i.e., $\operatorname{Nul} A = \{0\}$, so A is injective. Together with assumption (ii), A is invertible, thus (iii) follows. $\square$

Example 2.8.12. Let $A \in M_{2\times 4}(\mathbb{R})$ be such that

$$\mathrm{Nul}\, A = \{(x_1, x_2, x_3, x_4)^T \in \mathbb{R}^4 : x_1 = 5x_2 \text{ and } x_3 = 7x_4\},$$

we try to show that A is surjective as a map from $\mathbb{R}^4$ to $\mathbb{R}^2$. Recall that A is sujective iff $\mathrm{Col}\, A = \mathbb{R}^2$.

Firstly we count the dimension of $\mathrm{Nul}\, A$, for this, note that

$$x \in \mathrm{Nul}\, A \iff x = \begin{bmatrix} 5x_2 \\ x_2 \\ 7x_4 \\ x_4 \end{bmatrix}, \exists x_2, x_4 \in \mathbb{R} \iff x \in \mathrm{span}\left\{ \begin{bmatrix} 5 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 7 \\ 1 \end{bmatrix} \right\}$$

hence $\dim \mathrm{Nul}\, A = 2$. Applying rank-nullity theorem to A, we have

$$4 = \dim \mathrm{Nul}\, A + \dim \mathrm{Col}\, A = 2 + \dim \mathrm{Col}\, A,$$

hence $\dim \mathrm{Col}\, A = 2$. As $\mathrm{Col}\, A$ is a subspace of $\mathbb{R}^2$, $\mathrm{Col}\, A = \mathbb{R}^2$ by Example 2.7.7.

Example 2.8.13. Let $S \in M_{n\times n}(\mathbb{R})$ be skew-symmetric (i.e., $S^T = -S$), we try to show that $I + S$ is invertible.

Since $I + S$ is square, by Corollary 2.8.11 we have

$$I + S \text{ is invertible} \iff I + S \text{ is injective} \iff ((I + S)x = 0 \implies x = 0).$$

Now we try to show the last statement.

Let $(I + S)x = 0$, then $Sx = -x$. Define $\langle a, b\rangle = a \cdot b$, where $a, b \in \mathbb{R}^n$ and $a \cdot b$ means the dot product between a and b. For $x \in \mathbb{R}^n$, recall that $\|x\|^2 = \langle x, x\rangle$, and also for any $n \times n$ matrix A,

$$\langle Ax, y\rangle = (Ax)^T y = x^T (A^T y) = \langle x, A^T y\rangle, \quad x, y \in \mathbb{R}^n$$

hence

$$\|x\|^2 = \langle x, x\rangle = \langle -Sx, x\rangle = -\langle Sx, x\rangle \tag{2.8.14}$$

and

$$\langle Sx, x\rangle = \langle x, S^T x\rangle = \langle x, (-S)x\rangle = -\langle x, Sx\rangle = -\langle Sx, x\rangle,$$

hence $2\langle Sx, x\rangle = 0$, i.e., $\langle Sx, x\rangle = 0$. Continuing from (2.8.14), $\|x\| = 0$, so $x = 0$, as desired. We conclude that $I + S$ is injective, hence invertible.

2.8.3 Some Remarks on "Full Rank"

Let A be an $m \times n$ matrix.

- When A is thin (i.e., $m \geq n$), by rank-nullity theorem, $\dim \operatorname{Col} A = n - \dim \operatorname{Nul} A \leq n$, hence maximum possible rank is attained when $\dim \operatorname{Nul} A = 0$, i.e., A is injective. Hence

$$\boxed{\text{A thin matrix } A \text{ is of full rank} \iff A \text{ is 1-1.}}$$

- When A is strictly fat (i.e., $m < n$), then A (as a map $\mathbb{F}^n \to \mathbb{F}^m$) can never be injective, the argument above fails. Note that $\operatorname{Col} A$ is a subspace of $\mathbb{F}^m$, so the maximum possible rank is m, namely, this happens when A is surjective. Thus

$$\boxed{\text{A strictly fat matrix } A \text{ is of full rank} \iff A \text{ is onto.}}$$

2.9 Quotient Vector Spaces

2.9.1 Equivalence Relation

Definition 2.9.1. An **equivalence relation**, $\sim$, on a set S is a binary relation that satisfies the following three conditions:

Reflexive
For all $x \in S$, $x \sim x$.

Symmetric
For $x, y \in S$, if $x \sim y$, then $y \sim x$.

Transitive
For $x, y, z \in S$, if $x \sim y$, $y \sim z$, then $x \sim z$.

Example 2.9.2. It is easy to find equivalence relation. For example, for the set of straight lines in $\mathbb{R}^2$ "being parallel" is an equivalence relation. In a high school, "being in the same class" is an equivalence relation on pupil. "Being of the same sex" is an equivalence relation on human, normally.

For $x \in S$, we introduce the equivalence class

$$[x] := \{s \in S : s \sim x\}.$$

Also we denote $S/\!\sim$ the collection of all equivalence classes, namely,

$$S/\!\sim\, = \{[s] : s \in S\},$$

which is read as the "set S modulo $\sim$". It is easy to establish the following basic fact:

Proposition 2.9.3. *Let $\sim$ be an equivalence relation on a set S, then:*

$$a \sim b \iff [a] = [b] \iff [a] \cap [b] \neq \emptyset.$$

Therefore every element in a class $[s]$ is called a **representative** of $[s]$, this is because for every $u \in [s]$, we have $u \sim s$, hence $[u] = [s]$, all of them will represent the same class.

Proof. If $a \sim b$, we let $x \in [a]$, then $x \sim a$. But $a \sim b$, so by transitivity, $x \sim b$, hence $x \in [b]$. The argument says that $[a] \subseteq [b]$. By interchanging a, b, $[b] \subseteq [a]$, so $[a] = [b]$.

If $[a] = [b]$, then of course $[a] \cap [b] \neq \emptyset$.

If $[a] \cap [b] \neq \emptyset$, then we can pick $x \in [a] \cap [b]$, which means that $x \sim a$ (by "symmetricity", $a \sim x$) and $x \sim b$. By transitivity, $a \sim b$. ☐

Hence an equivalence relation $\sim$ can be used to partition S because distinct classes have empty intersection (Proposition 2.9.3), moreover,

$$S = \bigcup_{s \in S} [s] = \bigsqcup_{\alpha \in A} [s_\alpha],$$

where we choose s_α's $\in S$ the representative of the distinct classes $[s_\alpha]$'s. Note that the feasibility of choosing those representatives follows from **Axiom of Choice**$^{(\ddagger)}$. The representative of a class may not be unique as we can choose (if exists) a $u_\alpha \in [s_\alpha] \setminus \{s_\alpha\}$ such that $u_\alpha \sim s_\alpha$ and thus $[u_\alpha] = [s_\alpha]$. Note that it is natural to fix the representatives to avoid listing the same equivalence class.

For those who have had acquaintance with group or number theory the following example can be skipped.

Example 2.9.4. Let $a, b \in \mathbb{Z}$, we can declare a relation $\sim$ on $\mathbb{Z}$ by

$$a \sim b \text{ if } a - b \in 2\mathbb{Z} := \{2n : n \in \mathbb{Z}\}.$$

For reflexivity, if $a \in \mathbb{Z}$, then $a - a = 0 \in 2\mathbb{Z}$.

For symmetricity, if $a - b \in 2\mathbb{Z}$, then $b - a \in -2\mathbb{Z} = 2\mathbb{Z}$.

For transitivity, if $a - b \in 2\mathbb{Z}$, $b - c \in 2\mathbb{Z}$, then $a - c = (a - b) + (b - c) \in 2\mathbb{Z}$.

Let's compute $[a]$ when $a \in \mathbb{Z}$. By definition $[a] = \{n \in \mathbb{Z} : n \sim a\}$, so

$$[a] = \{n \in \mathbb{Z} : n - a = 2i, \exists i \in \mathbb{Z}\} = \bigcup_{i \in \mathbb{Z}} \{n \in \mathbb{Z} : n - a = 2i\} = \bigcup_{i \in \mathbb{Z}} \{a + 2i\} = a + 2\mathbb{Z}.$$

Moreover by noting that $[a] = a + 2\mathbb{Z} = a - 2 + 2\mathbb{Z} = [a - 2]$, it can be easily checked that

$$\mathbb{Z}/\!\sim \; = \{[n] : n \in \mathbb{Z}\} = \{[0], [1]\} = \big\{\{\text{even integers}\}, \{\text{odd integers}\}\big\}.$$

$^{(\ddagger)}$ Axiom of Choice is proved equivalent to Zorn's lemma in set theory.

2.9.2 Vector Spaces by Quotienting

Construction of Quotient Vector Spaces

With the concept of quotient spaces one can give another proof of

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

(Theorem 2.7.11) without the messy checking on the number of basis. Let's start with the construction.

Let V be a vector space and U a vector subspace of V, it can be checked that for $x, y \in V$, the relation $x \sim y$ defined by

$$x - y \in U$$

is indeed an equivalence relation on the set V. For $x \in V$,

$$[x] = \{v \in V : v \sim x\} = \{v \in V : v - x \in U\} = \{v \in V : v \in x + U\} = x + U.$$

Conventionally we denote

$$V/U := V/\sim = \{[v] : v \in V\} = \{v + U : v \in V\},$$

read as "V mod U". It is worth noting that V/U is still a vector space (hence called a **quotient vector space**) with the naturally defined **addition**

$$(x+U) + (y+U) = (x+y) + U$$

and **scalar multiplication**

$$\alpha(x+U) = \alpha x + U.$$

It is easy to check that these definitions are **well-defined**. Namely, the definition of these operations are independent of the choices of representatives. Moreover, the **zero element** in V/U is the class $0_{V/U} = [0]$. We shall denote this zero element in V/U also by 0. For $x + U \in V/U$, we observe that

$$x + U = 0 \iff [x] = [0] \iff x \sim 0 \iff x - 0 \in U \iff x \in U. \tag{2.9.5}$$

Hence the representatives of zero element in V/U are precisely every element in U.

Properties of Quotient Vector Spaces

Let's look at the first result:

Theorem 2.9.6. *Let X be a finite dimensional vector space and Y its subspace, then*

$$\dim(X/Y) = \dim X - \dim Y.$$

Proof. Let's consider two extreme cases. If $\dim Y = 0$, i.e., $Y = \{0\}$, and hence $X = X/\{0\}$, so we are done. If $\dim Y = \dim X$, then $Y = X$, and thus $X/Y = \{0\}$, therefore

$$\dim(X/Y) = 0 = \dim X - \dim Y,$$

we are also done.

Suppose now $0 < \dim Y = m < \dim X$. Let $\{v_1, v_2, \ldots, v_m\}$ be a basis of Y, extend it to $\{v_1, \ldots, v_m, u_1, \ldots, u_n\}$ a basis of X, then it is not hard to check

$$X/Y = \operatorname{span} \underbrace{\{u_1 + Y, \ldots, u_n + Y\}}_{:=\alpha}$$

due to (2.9.5). We show that α is linearly independent, thus is a basis of X/Y. Let $a_i \in \mathbb{F}$ be such that

$$\sum_{i=1}^{n} a_i(u_i + Y) = \left(\sum_{i=1}^{n} a_i u_i\right) + Y = 0,$$

then by (2.9.5), $\sum_{i=1}^{n} a_i u_i \in Y = \operatorname{span}\{v_1, \ldots, v_m\}$, but $v_1, \ldots, v_m, u_1, \ldots, u_n$ are linearly independent, hence necessarily $a_1, a_2, \ldots, a_n = 0$, as desired. Now α is a basis of X/Y, therefore

$$\dim(X/Y) = n = (n + m) - m = \dim X - \dim Y. \qquad \square$$

Recall that given two vector subspaces X, Y, the set $X + Y$ and $X \cap Y$ are still vector spaces. Now we have the following:

Theorem 2.9.7. *Let X and Y be vector subspaces of some vector space, then*

$$\frac{X + Y}{X \cap Y} = \frac{X}{X \cap Y} \oplus \frac{Y}{X \cap Y}.$$

Here $\frac{U}{V}$ is another notation for U/V.

Proof. Obviously

$$\frac{X + Y}{X \cap Y} = \frac{X}{X \cap Y} + \frac{Y}{X \cap Y}.$$

To show the sum is actually a direct sum, we let $u \in \frac{X}{X \cap Y} \cap \frac{Y}{X \cap Y}$, and prove $u = 0$. Indeed,

$$u = x + X \cap Y = y + X \cap Y,$$

for some $x \in X, y \in Y$. It follows that $x - y \in X \cap Y$, thus there is $v \in X \cap Y$ such that

$$x - y = v \implies x = v + y \in Y.$$

But $x \in X$, so $x \in X \cap Y$, and hence $u = x + X \cap Y = 0$ by (2.9.5). $\square$

We are ready to give a simpler proof to Theorem 2.7.11. It is good to have two different proofs to an interesting result.

Corollary 2.9.8. *Let U and V be two finite dimensional subspaces of some vector space, then*

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V). \tag{2.9.9}$$

Proof. By Theorem 2.9.7 and Proposition 2.7.9,

$$\dim \frac{U + V}{U \cap V} = \dim \frac{U}{U \cap V} + \dim \frac{V}{U \cap V}.$$

By Theorem 2.9.6,

$$\dim(U + V) - \cancel{\dim(U \cap V)} = \dim U - \cancel{\dim(U \cap V)} + \dim V - \dim(U \cap V). \qquad \square$$

Quotient is an important concept in almost everywhere. You will learn a much general concept in MATH3121 (Algebra I) or 3131 (Honors in Linear and Abstract Algebra II). For analytical aspect, one will learn this in MATH4063 (Functional Analysis) which is a good course for those who already have good background on real analysis (MATH3043) and general point-set topology (MATH4061 Modern Analysis & MATH4225 Topology). Some of them (a set modulo some equivalence relation) even have smooth structure as a smooth manifold which we will learn in MATH4033 (Calculus on Manifold).

2.10 Exercises

Linear Span

Problem 2.1. Let H, K be subsets of a vector space V, prove that

$$\operatorname{span}(H \cup K) = \operatorname{span} H + \operatorname{span} K \quad \text{and} \quad \operatorname{span}(H \cap K) \subseteq \operatorname{span} H \cap \operatorname{span} K.$$

Problem 2.2. Let $A, B \in M_{n\times n}(\mathbb{R})$ such that A is nonzero symmetric matrix and B is a nonzero skew-symmetric matrix, show that $\{A, B\}$ is linearly independent in $M_{n\times n}(\mathbb{R})$.

Problem 2.3. Let $A \in M_{n\times n}(\mathbb{R})$, if $A = B + C = B' + C'$, where B, B' are symmetric and C, C' are skew symmetric, then $B = B'$ and $C = C'$. Recall Example 2.4.4.

Linear Independence

Problem 2.4. Prove that if $\{v_1, v_2, \ldots, v_n\}$ is linearly independent in V, then so is

$$\{v_1 - v_2, v_2 - v_3, \ldots, v_{n-1} - v_n, v_n\}.$$

Problem 2.5. Let V be a vector space. Suppose $\{v_1, v_2, \ldots, v_n\}$ is linearly independent in V and $w \in V$. Prove that

$$\{v_1 + w, v_2 + w, \ldots, v_n + w\} \text{ is linearly dependent } \implies w \in \operatorname{span}\{v_1, v_2, \ldots, v_n\}.$$

Problem 2.6. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct real numbers, show that $\{e^{\alpha_1 t}, e^{\alpha_2 t}, \ldots, e^{\alpha_n t}\}$ is linearly independent in $C(\mathbb{R}, \mathbb{R})$.

Problem 2.7. Let $A \in M_{n\times n}(\mathbb{R})$. Suppose there is a positive integer m such that $A^{m-1}v \neq 0$ but $A^m v = 0$. Prove that

$$\{v, Av, A^2v, \ldots, A^{m-1}v\}$$

is linearly independent.

Problem 2.8 (Wronskian). Let $f_1, f_2, \ldots, f_n : \mathbb{R} \to \mathbb{R}$ be $n-1$ differentiable, define $W(f_1, \ldots, f_n)(x)$ as in Problem 1.13. Show that if $W(x_0) \neq 0$, for some x_0, then $\{f_1, f_2, \ldots, f_n\}$ is linearly independent.

Problem 2.9. Let $f_1, f_2, \dots, f_n \in C([a,b],\mathbb{R})$. Show that the set $\{f_1, f_2, \dots, f_n\}$ is linearly dependent in $C([a,b],\mathbb{R})$ if and only if

$$\det[\langle f_i, f_j\rangle]_{n\times n} = 0.$$

Where $\langle\cdot,\cdot\rangle$ is defined by $\langle f, g\rangle = \displaystyle\int_a^b f(x)g(x)\,dx$.

Sums and Direct Sums

Problem 2.10. We have defined the **trace** of a square matrix in Problem 1.4. Show that $W := \{A \in M_{n\times n}(\mathbb{R}) : \operatorname{Tr} A = 0\}$ is a subspace of $M_{n\times n}(\mathbb{R})$. Moreover, find a subspace V of $M_{n\times n}(\mathbb{R})$ such that

$$M_{n\times n}(\mathbb{R}) = W \oplus V.$$

Vector Spaces and Bases

Problem 2.11. Prove that (vi), (vii) and (viii) of Example 2.5.2 are **(a)** vector spaces with suitably defined addition and scalar multiplication; and **(b)** infinite dimensional.

Hint. The idea used in Example 2.7.6 may be helpful.

Problem 2.12. Let $v_1, v_2, v_3 \in \mathbb{R}^3$, suppose the vector equation

$$x_1v_2 + x_2v_2 + x_3v_3 = b$$

has no solution for some $b \in \mathbb{R}^3$, show that $\{v_1, v_2, v_3\}$ is linearly dependent.

Hint. Use Theorem 2.7.4.

Dimensions

Problem 2.13. Let A be any real matrix, prove that $I + A^TA$ is invertible.

Problem 2.14. Let

$$W = \operatorname{span}\left\{\begin{bmatrix}1 & -5\\ -4 & 2\end{bmatrix}, \begin{bmatrix}1 & 1\\ -1 & 5\end{bmatrix}, \begin{bmatrix}2 & -4\\ -5 & 7\end{bmatrix}, \begin{bmatrix}1 & -7\\ -5 & 1\end{bmatrix}\right\},$$

find a basis of W and $\dim W$.

Problem 2.15. Fix a vector $v \in \mathbb{R}^n \setminus \{0\}$ and let $U = \{A \in M_{n\times n}(\mathbb{R}) : Av = 0\}$. Show that $\dim U = n(n-1)$.

Remark. U is the vector space of matrices that "kill" the vector v ☺.

Problem 2.16 (Generalize Problem 2.15). Let $P \in M_{n\times n}(\mathbb{R})$ be such that $\operatorname{rank} P = r$. Show that

$$\dim\Big(\{A \in M_{n\times n}(\mathbb{R}) : AP = 0\}\Big) = n(n-r).$$

Remark. The vector space (whose dimension is to be computed) is the set of all matrices that "kill" the matrix P ☺.

Problem 2.17. Let V be the vector space of all 2×2 matrices $A \in M_{2\times 2}(\mathbb{R})$ such that

$$A \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} A.$$

(a) Find a basis of V and determine $\dim V$.

(b) Find the dimension of the image of $T : M_{2\times 2}(\mathbb{R}) \to M_{2\times 2}(\mathbb{R})$ defined by

$$T(A) = A \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} - \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} A, \quad \text{for each } A \in M_{2\times 2}(\mathbb{R}).$$

Problem 2.18. Let $S = \{AB - BA : A, B \in M_{n\times n}(\mathbb{R})\}$. This is an infinite subset of the vector space of $n \times n$ matrices. We define

$$\operatorname{span} S := \{a_1 s_1 + \cdots + a_n s_n : a_i \in \mathbb{R}, s_i \in S, n \geq 1\}.$$

Namely, $\operatorname{span} S$ is the collection of all *finite* linear combinations of S.

(a) Show that $\operatorname{span} S$ defined above is indeed a real vector space.

(b) Because $\operatorname{span} S$ is a subspace of $M_{n\times n}(\mathbb{R})$, it is finite dimensional. Show that precisely,

$$\dim(\operatorname{span} S) = n^2 - 1.$$

Hint. The trace map $\mathrm{Tr} : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$ is linear, and $\operatorname{span} S \subseteq \ker \mathrm{Tr}$. Moreover, we know that $\dim \ker \mathrm{Tr} = n^2 - 1$, where $\ker \mathrm{Tr} = \{A \in M_{n\times n}(\mathbb{R}) : \mathrm{Tr}\, A = 0\}$.

Problem 2.19. Let $A, B \in M_{m\times n}(\mathbb{F})$, show that

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

Problem 2.20. Let $A \in M_{m\times k}(\mathbb{F})$ and $B \in M_{k\times n}(\mathbb{F})$, then $AB \in M_{m\times n}(\mathbb{F})$, prove that

$$\dim \operatorname{Nul} AB \leq \dim \operatorname{Nul} A + \dim \operatorname{Nul} B.$$

Problem 2.21. Let $A \in M_{m\times n}(\mathbb{R})$, prove that $\operatorname{rank} A^T A = \operatorname{rank} A$.

Problem 2.22. Raise a counter example to show that

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

can be false for some subspace U, V, W of a real vector space.

Chapter 3

Linear Transformations Between Vector Spaces

Throughout this chapter we use $\mathbb{F}$ to denote $\mathbb{R}$ or $\mathbb{C}$. As a reminder, some of the examples cannot have a direct analogue to complex vector spaces since, as you will see, some of the operations will not make sense in complex field.

3.1 Linear Transformations

3.1.1 Definitions and Basic Results

Definition 3.1.1. A **linear map** or **linear transformation** is a function $T : V \to W$ between vector spaces such that

Additivity
$$T(u + v) = Tu + Tv \quad \forall u, v \in V$$

Homogeneity
$$T(\alpha v) = \alpha T v \quad \forall \alpha \in \mathbb{F}, \forall v \in V$$

Convention.

- For *linear maps* we write Tv instead of $T(v)$.
- We denote $\mathcal{L}(V, W)$ the collection of all linear maps from V to W.
- A linear map $T : V \to V$ is said to be a **linear operator** in linear algebra.

Example 3.1.2 (Linear Transformations $T \in \mathcal{L}(V, W)$).

(i) Any matrix $A \in M_{m\times n}(\mathbb{F})$ gives a linear transformation $L_A \in \mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$ defined by

$$L_A(x) = Ax.$$

We say A is the **standard matrix** of L_A.

(ii) If $V = W$, we have **identity map** $I_V \in \mathcal{L}(V, V)$ defined by

$$I_V(v) = v, \quad \text{for all } v \in V.$$

(iii) Let $T \in \mathcal{L}(\mathbb{F}^7, \mathbb{F}^7)$ be **backward shift** defined by

$$T(x_1, x_2, \ldots, x_7) = (x_2, x_3, \ldots, x_7, 0).$$

(iv) For $n \geq 1$, we can define $S \in \mathcal{L}(\mathbb{P}_n(\mathbb{R}), \mathbb{P}_{n+2}(\mathbb{R}))$ and $T \in \mathcal{L}(\mathbb{P}_n(\mathbb{R}), \mathbb{P}_{n-1}(\mathbb{R}))$ by

$$(Sp)(x) = x^2 p(x) \quad \text{and} \quad (Tp)(x) = \frac{dp}{dx}(x).$$

Note that Sp and Tp are functions, we use the notation $(Sp)(x), (Tp)(x)$ to make explicit what the function is *pointwise*.

(v) We can define $T \in \mathcal{L}(C([0,1], \mathbb{R}), C([0,1], \mathbb{R}))$ by

$$(Tf)(x) = \int_0^x f(t)\, dt.$$

Definition 3.1.3. Let $S \in \mathcal{L}(U, V)$ and $T \in \mathcal{L}(V, W)$, we define $TS \in \mathcal{L}(V, W)$ by

$$(TS)(v) = T \circ S(v) = T(S(v)).$$

Theorem 3.1.4. *Let $\{v_1, v_2, \ldots, v_n\}$ be linearly independent in V, given $w_1, w_2, \ldots, w_n \in W$, there is a unique $T \in \mathcal{L}(\operatorname{span}\{v_1, \ldots, v_n\}, W)$ such that*

$$Tv_i = w_i, \quad i = 1, 2, \ldots, n.$$

That is to say, whenever we have a basis on V, then we can define a linear map on V by assigning each v_i an vector w_i. Those w_i's can possibly repeat.

Proof. We define $T : \operatorname{span}\{v_1, \ldots, v_n\} \to W$ as follows: For every $a_i \in \mathbb{F}$,

$$T\left(a_1 v_1 + a_2 v_2 + \cdots + a_n v_n\right) = a_1 w_1 + a_2 w_2 + \cdots + a_n w_n. \tag{3.1.5}$$

It is easy to check T is indeed linear, hence it a linear map that satisfies desired properties.

On the other hand, if $S : \operatorname{span}\{v_1, \ldots, v_n\} \to W$ is any map such that $Sv_i = w_i$, then T and S agree on a basis, hence $T = S$. ☐

Example 3.1.6. We try to prove that there is a linear map $T : \mathbb{R}^4 \to \mathbb{R}^3$ such that

$$T \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad T \begin{bmatrix} 3 \\ 0 \\ 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}.$$

Obviously $(2, 1, 2, 1)^T$ and $(3, 0, 3, 3)^T$ are linearly independent in $\mathbb{R}^4$, by Theorem 3.1.4 we can already define a unique linear map $T : \operatorname{span}\{(2, 1, 2, 1)^T, (3, 0, 3, 3)^T\} \to \mathbb{R}^3$ given by

$$T \left(a \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \end{bmatrix} + b \begin{bmatrix} 3 \\ 0 \\ 3 \\ 3 \end{bmatrix} \right) = a \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + b \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}.$$

However it is not enough as we seek for a map with domain on $\mathbb{R}^4$. That means we should try to *expand* the domain of our T.

By Theorem 2.6.9 we can extend $\{(2,1,2,1)^T, (3,0,3,3)^T\}$ to a basis

$$\left\{ \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \\ 3 \\ 3 \end{bmatrix}, u_1, u_2 \right\}$$

of $\mathbb{R}^4$. Now we further define $Tu_1 = Tu_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ (i.e., we assign u_1, u_2 the zero vector, and then by Theorem 3.1.4[(*)] we can extend T to $\mathbb{R}^4$ *linearly* by formula (3.1.5), thus we are done.

Indeed one of possible choices is to choose $u_1 = (0,0,1,0)^T$ and $u_2 = (0,0,0,1)^T$, the standard matrix of T become

$$A = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1/3 & 1/3 & 0 & 0 \end{bmatrix},$$

and the direct computation shows us $A \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ and $A \begin{bmatrix} 3 \\ 0 \\ 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}$.

In the next example we use the following terminology. We need to define the **kernel** (the solution to "homogeneous system") of a linear map, which is done in Definition 3.1.9.

Definition 3.1.7. A subset W of $\mathbb{F}^n$ is said to be a **hyperplane** if it takes one of the following equivalent from:

- There are $a_1, a_2, \cdots \in \mathbb{F}$, *not all zero*, and $b \in \mathbb{F}$ such that

$$W = \{(x_1, \dots, x_n)^T \in \mathbb{F}^n : a_1x_1 + a_2x_2 + \cdots + a_nx_n = b\} \neq \emptyset.$$

- There is a *nonzero* $\Lambda \in \mathcal{L}(\mathbb{F}^n, \mathbb{F})$ such that

$$W = \{x \in \mathbb{F}^n : \Lambda x = \Lambda x_0\} = x_0 + \ker \Lambda.$$

Two formulations are equivalent. Indeed, the set $W := \{(x_1, x_2, \dots, x_n)^T \in \mathbb{F}^n : a_1x_1 + a_2x_2 + \cdots + a_nx_n = b\}$ can be written as

$$\{x \in \mathbb{F}^n : \langle x, (a_1, \dots, a_n)^T \rangle = \langle x_0, (a_1, \dots, a_n)^T \rangle\},$$

for some $x_0 \in \mathbb{R}^n$. Of course $x \mapsto \langle x, (a_1, \dots, a_n)^T \rangle$ defines a linear map from $\mathbb{F}^n$ to $\mathbb{F}$, therefore W is reduced to the second formulation.

Conversely, given a nonzero $\Lambda : \mathbb{F}^n \to \mathbb{F}$, then $\Lambda x = \Lambda x_0$ if and only if

$$\Lambda(x_1e_1 + x_2e_2 + \cdots + x_ne_n) = \Lambda x_0 \iff \Lambda(e_1)x_1 + \Lambda(e_2) + \cdots + \Lambda(e_n)x_n = \Lambda x_0,$$

which is again the first formulation. Therefore two formulations are the same and define a hyperplane in $\mathbb{R}^n$.

When $\mathbb{F}^n = \mathbb{R}^3$, $\ker \Lambda$ is just a plane passing through 0, so a hyperplane is just a plane in $\mathbb{R}^3$ with possibly a "shifting" by x_0.

(*) In this theorem, choose $v_1 = \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \end{bmatrix}$, $v_2 = \begin{bmatrix} 3 \\ 0 \\ 3 \\ 3 \end{bmatrix}$, $v_3 = u_1$, $v_4 = u_2$ and $w_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, $w_2 = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}$, $w_3 = w_4 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$.

Example 3.1.8. Given a proper subspace W of $\mathbb{F}^n$ and a point $v \in \mathbb{F}^n \setminus W$, there is a hyperplane

$$P := \{(x_1, \dots, x_n)^T \in \mathbb{F}^n : a_1 x_1 + \cdots + a_n x_n = 0\}$$

such that $W \subseteq P$ and $v \notin P$.

To prove this, let $w_1, \dots, w_k$ be a basis of W, as $v \notin \operatorname{span}\{w_1, \dots, w_n\}$, $v, w_1, \dots, w_k$ are linear independent, extend it to a basis of $\mathbb{F}^n$ by appending $u_1, \dots, u_m$. Now we define a linear map $\Lambda \in \mathcal{L}(\mathbb{F}^n, \mathbb{F})$ by defining

$$\Lambda w_1 = \Lambda w_2 = \cdots = \Lambda w_k = 0, \quad \Lambda v = \Lambda u_1 = \cdots = \Lambda u_m = 1.$$

and then extending Λ linearly by Theorem 3.1.4. Now $W \subseteq \ker \Lambda$ and $v \notin \ker \Lambda$, thus $\ker \Lambda$ is the desired hyperplane.

3.1.2 Kernel and Range

Definition 3.1.9. Let V and W be vector spaces and let $T \in \mathcal{L}(V, W)$. The **kernel** of T and the **range** of T are defined by

$$\ker T = \{v \in V : Tv = 0\} \quad \text{and} \quad \operatorname{range} T = \{Tv : v \in V\}$$

respectively.

The following directly extend the results of matrices with identical proof:

Theorem 3.1.10. *Let V, W be vector spaces and $T \in \mathcal{L}(V, W)$. Then:*

(i) T *is injective* $\iff \ker T = \{0\} \iff \big(Tx = 0 \implies x = 0\big)$.

(ii) $\ker T$ *is a subspace of* V.

(iii) $\operatorname{range} T$ *is a subspace of* W.

Example 3.1.11 (Compute $\ker T$).

(i) Consider $T \in \mathcal{L}(\mathbb{P}_n(\mathbb{R}), \mathbb{P}_{n-1}(\mathbb{R}))$ defined by $Tp = p'$. If $p \in \ker T$, then $Tp = p' = 0$, hence p is a constant function, $p \in \{f \equiv a : a \in \mathbb{R}\}$. That means

$$\ker T \subseteq \{f \equiv a : a \in \mathbb{R}\}.$$

The reverse inclusion is obvious, thus $\ker T = \{f \equiv a : a \in \mathbb{R}\}$.

(ii) Consider $T \in \mathcal{L}(C([0,1], \mathbb{R}), C([0,1], \mathbb{R}))$ defined by

$$(Tf)(x) = \int_0^x f(t)\, dt.$$

If $f \in \ker T$, then $Tf = 0$, i.e., $(Tf)(x) = 0$ for all $x \in [0,1]$. Since f is continuous on $[0,1]$, Tf is differentiable on $(0,1)$. Thus for every $x \in (0,1)$,

$$0 = \frac{d}{dx} Tf(x) = \frac{d}{dx} \int_0^x f(t)\, dt = f(x).$$

Also, $f(0) = \lim_{x \to 0^+} f(x) = 0 = \lim_{x \to 1^-} f(x) = f(1)$, so $f \equiv 0$.

In summary, the logic says that $\ker T \subseteq \{0\}$. The reverse inclusion is obvious, so $\ker T = \{0\}$.

(iii) Consider the **backward shift** $T \in \mathcal{L}(\mathbb{F}^\infty, \mathbb{F}^\infty)$ defined by $T(x_1, x_2, \dots) = (x_2, x_3, \dots)$. It is easy to check $\ker T = \{(a, 0, 0, \dots) : a \in \mathbb{F}\}$.

3.1.3 Generalized Rank-Nullity Theorem

Theorem 3.1.12 (Generalized Rank-Nullity). *Let V be finite dimensional and $T \in \mathcal{L}(V, W)$, then*

$$\dim V = \dim \ker T + \dim \operatorname{range} T.$$

Proof. This is the same as Theorem 2.8.10. □

Next we define invertability of a linear transformation. Note that I_V, as we denote in (ii) of Example 3.1.2, is called the **identity map** on V, i.e., $I_V(v) = v$ for each $v \in V$.

Definition 3.1.13. Let V, W be vector spaces. A linear transformation $T \in \mathcal{L}(V, W)$ is said to be **invertible** if there is $S \in \mathcal{L}(W, V)$ such that,

$$TS = I_W \quad \text{and} \quad ST = I_V.$$

Or equivalently, T is **invertible** if T is injective and surjective.

Remark. Usually we denote such S by T^{-1}.

Corollary 3.1.14. *Let V and W be finite dimensional,* $\dim V = \dim W$ *and $T \in \mathcal{L}(V, W)$, then the following are equivalent.*

(i) T is invertible. *(ii) T is injective.* *(iii) T is surjective.*

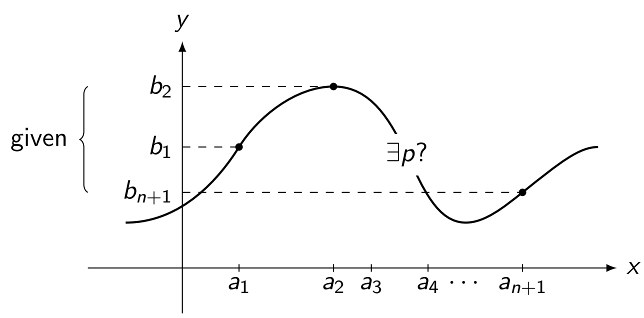
Proof. This is the same as Corollary 2.8.11. □

Remark. In Corollary 3.1.14 given a linear map $T : V \to W$, $\dim V = \dim W$, the result that T is 1-1 $\iff$ T is onto is only true when V is finite dimensional. Consider $V = \mathbb{R}^\infty$, the map $T : V \to V$ defined by $T(a_1, a_2, \dots) = (0, a_1, a_2, \dots)$ is injective but not surjective.

Example 3.1.15 (Interpolation Problem). Let $a_1, a_2, \dots, a_{n+1}$ be $n+1$ distinct real numbers on the x-axis. Given $b_1, b_2, \dots, b_{n+1} \in \mathbb{R}$, there is a polynomial $p \in \mathbb{P}_n$ such that

$$p(a_1) = b_1, \quad p(a_2) = b_2, \quad \dots, \quad p(a_{n+1}) = b_{n+1}.$$

More precisely, given $n+1$ distinct points on the x-y plane, we have a real polynomial that connects all these $n+1$ points!



To prove this, note that the existence problem is the same as showing the linear map

$$T : \mathbb{P}_n \to \mathbb{R}^{n+1}; \quad p \mapsto \begin{bmatrix} p(a_1) \\ p(a_2) \\ \vdots \\ p(a_{n+1}) \end{bmatrix}$$

is onto. For this, since $\dim \mathbb{P}_n(\mathbb{R}) = n+1 = \dim \mathbb{R}^{n+1}$, so by Corollary 3.1.14 showing T is onto is the same as showing T is one-one.

To this end, let $p \in \mathbb{P}_n(\mathbb{R})$ be such that $Tp = 0$, then $p(a_1), p(a_2), \dots, p(a_{n+1}) = 0$, hence a degree n polynomial has $n+1$ distinct roots, from basic algebra, p must be the zero polynomial 0.

The argument shows us $\ker T = \{0\}$, i.e., T is one-one, hence we are done.

Example 3.1.16 (Partial Fractions Decomposition). It was taught in a short course on partial fractions that we can always assume

$$\frac{p(x)}{(x-a)^h(x-b)^k} = \sum_{i=1}^{h} \frac{a_i}{(x-a)^i} + \sum_{j=1}^{k} \frac{b_j}{(x-b)^j}$$

and then solve for a_i's and b_j's, where $a \neq b$ are real, $h, k \geq 1$ and $p \in \mathbb{P}_{h+k-1}(\mathbb{R})$. Why must it work? Note that the feasibility of making such assumption is the same as saying

$$p \in \operatorname{span} \left\{ \begin{array}{c} (x-a)^h(x-b)^i, \\ (x-b)^k(x-a)^j \end{array} : \begin{array}{c} i = 0, 1, \dots, k-1, \\ j = 0, 1, \dots, h-1 \end{array} \right\}.$$

We hope this is always true, namely, we hope that the linear map

$$\begin{aligned} T : \qquad & \mathbb{R}^{h+k} \to \mathbb{P}_{h+k-1}(\mathbb{R}) \\ (a_0, \dots, a_{k-1}, b_0, \dots, b_{h-1}) \mapsto & \sum_{i=0}^{k-1} a_i (x-a)^h (x-b)^i + \sum_{j=0}^{h-1} b_j (x-b)^k (x-a)^j \end{aligned}$$

is surjective. Note that $\dim \mathbb{R}^{h+k} = h+k = \dim \mathbb{P}_{h+k-1}(\mathbb{R})$, by Corollary 3.1.14 it is enough to show T is injective. For this, suppose

$$\sum_{i=0}^{k-1} a_i (x-a)^h (x-b)^i + \sum_{j=0}^{h-1} (x-b)^k (x-a)^j = 0,$$

we try to show a_i's and b_j's are all zero.

Now for every $x \neq a$, we divide $(x-a)^h$ on both sides to get

$$\begin{aligned} -\sum_{i=0}^{k-1} a_i (x-b)^i = \sum_{j=0}^{h-1} \frac{b_j (x-b)^k}{(x-a)^{h-j}} & \\ = (x-b)^k \left(\frac{b_0}{(x-a)^h} + \frac{b_1}{(x-a)^{h-1}} + \cdots + \frac{b_{h-1}}{x-a} \right) & \\ = (x-b)^k \frac{1}{(x-a)^h} (b_0 + b_1(x-a) + \cdots + b_{h-1}(x-a)^{h-1}). & \quad (3.1.17) \end{aligned}$$

We then take absolute value on both sides to get

$$\sum_{i=0}^{k-1} |a_i||x-b|^i \geq |x-b|^k \frac{1}{|x-a|^h} (|b_0| - |b_1||x-a| - \cdots - |b_{h-1}||x-a|^{h-1}).$$

Step 1. For the sake of contradiction, suppose $b_0 \neq 0$. Let's take $x \to a$ on the above inequality, then LHS goes to a finite number while RHS goes to ∞, a contradiction.

Step 2. Now $b_0 = 0$, suppose $b_1 \neq 0$, then we continue from (3.1.17) to get

$$\sum_{i=0}^{k-1} |a_i||x-b|^i \geq |x-b|^k \frac{1}{|x-a|^{h-1}}(|b_1| - |b_2||x-a| - \cdots - |b_{h-1}||x-a|^{h-2}),$$

and we get the same contradiction when $x \to a$, so $b_1 = 0$.

Step j. $b_{j-1} = 0$ due to the same contradiction.

Now from step j, $j = 1, 2, \ldots, h$, we have $b_0 = b_1 = \cdots = b_{h-1} = 0$, hence we have shown that all b_j's are zero. Continuing from (3.1.17) we have

$$\sum_{i=0}^{k-1} a_i(x-b)^i = 0,$$

but then since $\{1, x-b, (x-b)^2, \ldots, (x-b)^{k-1}\}$ is linearly independent, a_i's are necessarily all zero, and we are done.

Remark. In Example 3.1.16 the same proof still work if we replace $\mathbb{R}$ by $\mathbb{C}$. Also with a slight modification of the proof, Example 3.1.16 can be generalized to Problem 3.11.

We end this section by introducing a standard terminology in *abstract algebra* in the context of linear algebra (this is still a very standard term in linear algebra!).

Definition 3.1.18. Let V and W be vector spaces, we say that V and W are **isomorphic** if there is an invertible linear transformation $T : V \to W$. A invertible linear map is said to be an **isomorphism**.

Note that it is also common to write $V \cong W$ to mean V and W are isomorphic. The following result says that for finite dimensional vector spaces being isomorphic is nothing but having the same "size":

Theorem 3.1.19. *Let V and W be finite dimensional, then the following are equivalent.*

(i) $\dim V = \dim W$. *(ii) V and W are isomorphic.*

Proof. (i) $\Rightarrow$ (ii) Suppose $\dim V = \dim W = n$, let $\{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_n\}$ be a basis of V and W respectively. Define a map $T : \{v_1, v_2, \ldots, v_n\} \to \{w_1, w_2, \ldots, w_n\}$ by

$$Tv_i = w_i,$$

then by Theorem 3.1.4 we can extend T linearly on V.

T is one-one (hence invertible by Corollary 3.1.14) since

$$T\left(\sum_{i=1}^{n} a_i v_i\right) = 0 \implies \sum_{i=1}^{n} a_i w_i = 0 \implies a_1, a_2, \ldots, a_n = 0.$$

Thus T is an isomorphism. Hence V and W are isomorphic.

(ii) $\Rightarrow$ (i) Assume V and W are isomorphic, i.e., there is an invertible linear map $T : V \to W$, then by rank-nullity theorem,

$$\dim V = \dim \ker T + \dim \operatorname{range} T = 0 + \dim W = \dim W. \qquad \square$$

Example 3.1.20. Let V be finite dimensional. The **dual space** of V is defined by $V^* = \mathcal{L}(V, \mathbb{F})$(†). We prove that V and V^* are isomorphic.

By Theorem 3.1.19 it is enough to show $\dim V = \dim V^*$. To do this, let's find a basis of V^*. Let $\{v_1, v_2, \ldots, v_k\}$ be a basis of V, we define the linear maps $v_1^*, v_2^*, \ldots, v_k^* \in V^*$ as follows: let

$$v_i^*(v_i) = 1 \quad \text{and} \quad v_i^*(v_j) = 0, \quad \forall j \neq i,$$

then by Theorem 3.1.4, v_i^* can be extended linearly to a map on V. We claim that v_i^*'s form a basis of V^*, it then follows that $\dim V^* = k = \dim V$.

Firstly we show that $V^* = \operatorname{span}\{v_1^*, v_2^*, \ldots, v_k^*\}$. Let $f \in V^*$, we have for $i = 1, 2, \ldots, k$,

$$f(v_i) = \left(\sum_{j=1}^{k} f(v_j) v_j^* \right) (v_i).$$

Since f and $\sum_{j=1}^{k} f(v_j) v_j^*$ agree on a basis of V, it follows that they agree on V, hence

$$f = \sum_{j=1}^{k} f(v_j) v_j^* \in \operatorname{span}\{v_1^*, v_2^*, \ldots, v_k^*\},$$

which means that $V^* \subseteq \operatorname{span}\{v_1^*, v_2^*, \ldots, v_k^*\}$. Since the reverse inclusion is obvious, we have $V^* = \operatorname{span}\{v_1^*, v_2^*, \ldots, v_k^*\}$.

It remains to verify $\{v_1^*, v_2^*, \ldots, v_k^*\}$ is linearly independent, to do this, let $a_i \in \mathbb{F}$ be such that

$$a_1 v_1^* + a_2 v_2^* + \cdots + a_k v_k^* = 0.$$

For each $i = 1, 2, \ldots, k$, the functional on the LHS evaluated at v_i gives

$$a_i = (a_1 v_1^* + a_2 v_2^* + \cdots + a_k v_k^*)(v_i) = 0.$$

Since i is arbitrary, $a_1 = a_2 = \cdots = a_k = 0$, as desired.

3.2 Matrix Representations and Change of Coordinates

In this section V and W are always finite dimensional vector spaces over $\mathbb{F}$.

3.2.1 Coordinates

Definition 3.2.1. Given a basis $\alpha = \{v_1, v_2, \ldots, v_n\}$ of V, for each $v \in V$, there are unique $a_1, a_2, \ldots, a_n \in \mathbb{F}$ such that $v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$. We define

$$[v]_\alpha = (a_1, a_2, \ldots, a_n)^T,$$

called the **coordinate vector** of v w.r.t. α.

(†) Each element in V^* is called a linear functional on V.

Example 3.2.2. Since $A = \begin{bmatrix} 3 & 2 & 6 \\ 1 & 1 & 2 \\ 2 & 2 & 5 \end{bmatrix} \in M_{3\times 3}(\mathbb{R})$ is invertible,

$$\alpha = \left\{ \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 6 \\ 2 \\ 5 \end{bmatrix} \right\}$$

is a basis of $\mathbb{R}^{3}$(‡). What is the coordinate vector of $b = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ w.r.t. α?

Note that $b = A(A^{-1}b)$, let $(x, y, z)^T = A^{-1}b$, then

$$b = A(x, y, z)^T = x \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix} + y \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} + z \begin{bmatrix} 6 \\ 2 \\ 5 \end{bmatrix},$$

hence $[b]_\alpha = (x, y, z)^T = A^{-1}b$. In Example 1.2.20 we have found A^{-1}, so

$$[b]_\alpha = A^{-1}b = \begin{bmatrix} 1 & 2 & -2 \\ -1 & 3 & 0 \\ 0 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} -1 \\ 5 \\ -1 \end{bmatrix}.$$

In summary given a basis $\alpha = \{a_1, \ldots, a_n\}$, if we construct a matrix $A = [a_1 \quad \cdots \quad a_n]$, then $A^{-1}b$ gives the coordinate of b w.r.t. α. This is simply because $b = A(A^{-1}b)$. Thus the meaning of "acting an inverse matrix on a vector" is exactly "extracting coordinate of this vector".

Theorem 3.2.3. *Let α be a basis of V, then the linear "coordinate map"*

$$C_\alpha(v) : V \to \mathbb{F}^{\dim V}; \quad v \mapsto [v]_\alpha$$

is an isomorphism.

Proof. Let $\alpha = \{v_1, v_2, \ldots, v_n\}$, by Corollary 3.1.14 it is enough to show C_α is injective. Indeed, let $v \in V$ be such that $C_\alpha(v) = 0 := (0, 0, \ldots, 0)^T$, then by definition

$$v = 0v_1 + 0v_2 + \cdots + 0v_n = 0. \qquad \square$$

One can apply Theorem 3.2.3 to prove Theorem 3.2.6, which basically says that the properties of any linear map $T : V \to W$, with $\dim V, \dim W < \infty$, remains unchanged under matrix representations in the next section.

3.2.2 Matrix Representations

The concept of bases not only provides us the concept of dimension, it also provides us a method to translate the language of linear transformations to language of matrices.

Definition 3.2.4. Let $\alpha = \{v_1, v_2, \ldots, v_n\}$ be a basis of V, β a basis of W and $T \in \mathcal{L}(V, W)$. The **matrix representation** of T w.r.t to bases α and β is

$$[T]_\alpha^\beta = \big[[Tv_1]_\beta \quad [Tv_2]_\beta \quad \cdots \quad [Tv_n]_\beta\big].$$

When $V = W$ and $\alpha = \beta$, it is customary to write $[T]_\alpha = [T]_\alpha^\alpha$.

(‡) Since $Ax = 0 \implies x = 0$, $\left\{ \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 6 \\ 2 \\ 5 \end{bmatrix} \right\}$ is linearly independent, and hence $\operatorname{span}\left\{ \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 6 \\ 2 \\ 5 \end{bmatrix} \right\}$ is a 3 dimensional subspace of $\mathbb{R}^3$, thus $\operatorname{span}\left\{ \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 6 \\ 2 \\ 5 \end{bmatrix} \right\} = \mathbb{R}^3$, $\left\{ \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 6 \\ 2 \\ 5 \end{bmatrix} \right\}$ is a basis of $\mathbb{R}^3$.

We can memorize it easily by the following diagram. Let $\beta = \{w_1, w_2, \dots, w_m\}$ and let $Tv_k = \sum_{i=1}^m a_{ik} w_i$. Then

$$[T]_\alpha^\beta = \begin{array}{c} \\ w_1 \\ w_2 \\ \vdots \\ w_m \end{array} \begin{array}{c} \begin{array}{cccc} Tv_1 & Tv_2 & \cdots & Tv_n \end{array} \\ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \end{array} \tag{3.2.5}$$

You are asked to prove the following nice result in Problem 3.19.

Theorem 3.2.6. *Let V and B be finite dimensional, $T \in \mathcal{L}(V, W)$ and α, β the basis of V, W respectively. Then*

$$\dim \operatorname{Nul}[T]_\alpha^\beta = \dim \ker T \quad \textit{and} \quad \dim \operatorname{Col}[T]_\alpha^\beta = \dim \operatorname{range} T.$$

To prove this, we keep in mind by definition of matrix representation the following diagram commutes (prove it!):

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "C_\alpha"'] & W \\ \mathbb{F}^{\dim V} \arrow[r, "{[T]_\alpha^\beta}"] & \mathbb{F}^{\dim W} \arrow[u, "C_\beta^{-1}"'] \end{tikzcd}$$

In other words, $T = C_\beta^{-1}[T]_\alpha^\beta C_\alpha$. Theorem 3.2.6 provides us a unified way to tell if a linear map between finite dimensional vector spaces is injective or surjective.

Example 3.2.7. Let $T \in \mathcal{L}(\mathbb{P}_2(\mathbb{R}), \mathbb{P}_4(\mathbb{R}))$ be defined by

$$(Tp)(x) = \frac{dp}{dx}(x) + x^2 p(x).$$

Let $\alpha = \{1, x, x^2\}$ be a basis of $\mathbb{P}_2$ and $\beta = \{1, x, x^2, x^3, x^4\}$ a basis of $\mathbb{P}_4$, we try to find $[T]_\alpha^\beta$ and determine if T is injective.

Since $T(1) = x^2$, $T(x) = 1 + x^3$, $T(x^2) = 2x + x^4$, we have

$$[T]_\alpha^\beta = \begin{array}{c} \\ 1 \\ x \\ x^2 \\ x^3 \\ x^4 \end{array} \begin{array}{c} \begin{array}{ccc} T(1) & T(x) & T(x^2) \end{array} \\ \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}.$$

Now it is easy to tell if T is injective by studying $[T]_\alpha^\beta$. Since $[T]_\alpha^\beta$ is of full rank, by rank-nullity theorem,

$$3 = \dim \operatorname{Nul}[T]_\alpha^\beta + \dim \operatorname{Col}[T]_\alpha^\beta = \dim \operatorname{Nul}[T]_\alpha^\beta + 3 \implies \dim \operatorname{Nul}[T]_\alpha^\beta = 0.$$

By Theorem 3.2.6,

$$\dim \ker T = \dim \operatorname{Nul}[T]_\alpha^\beta = 0,$$

meaning that $\ker T = 0$, so T is injective.

Example 3.2.8. Let $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in M_{2\times 2}(\mathbb{R})$. Define $T \in \mathcal{L}(M_{2\times 2}(\mathbb{R}), M_{2\times 2}(\mathbb{R}))$ by

$$T(A) = MA.$$

Define

$$\alpha = \left\{ E_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, E_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, E_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, E_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\},$$

we try to find the matrix representation $[T]_\alpha$ and also determine the values of a, b, c, d such that the map T is invertible.

Indeed, a direct computation gives

$$\begin{aligned} TE_1 &= aE_1 + cE_3 \\ TE_2 &= aE_2 + cE_4 \\ TE_3 &= bE_1 + dE_3 \\ TE_4 &= bE_2 + dE_4 \end{aligned} \quad \Longrightarrow \quad [T]_\alpha = \begin{array}{c} \\ E_1 \\ E_2 \\ E_3 \\ E_4 \end{array} \begin{array}{c} \begin{array}{cccc} T(E_1) & T(E_2) & T(E_3) & T(E_4) \end{array} \\ \begin{bmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{bmatrix} \end{array}.$$

T is invertible iff $[T]_\alpha$ is invertible iff $\det[T]_\alpha = (ad - bc)^2 \neq 0$, so T is invertible if and only if $ad \neq bc$.

3.2.3 Change of Coordinates

We combine the computational results of matrix representation in the following:

Theorem 3.2.9.

(i) Let α be a basis of V and β a basis of W, then

$$[T]_\alpha^\beta [v]_\alpha = [Tv]_\beta.$$

(ii) Let $S \in \mathcal{L}(V, U)$ and $T \in \mathcal{L}(U, W)$. If we give V, U, W a basis α, γ, β respectively, then

$$[TS]_\alpha^\beta = [T]_\gamma^\beta [S]_\alpha^\gamma.$$

(iii) If α and β are bases of V, then

$$[I_V]_\beta^\alpha = ([I_V]_\alpha^\beta)^{-1},$$

where I_V is the identity map on V, i.e., $I_V(v) = v$ for each $v \in V$.

Proof. (i) Let $\alpha = \{v_1, v_2, \dots, v_n\}$, it is easy to check the equality holds when $v = v_i, i = 1, 2, \dots, n$, hence we are done.

(ii) Let $\alpha = \{v_1, v_2, \dots, v_n\}, \beta = \{w_1, w_2, \dots, w_n\}$ and $\gamma = \{u_1, u_2, \dots, u_n\}$, then the result follows from direct calculation:

$$\begin{aligned} [TS]_\alpha^\beta &= \begin{bmatrix} [T(Sv_1)]_\beta & [T(Sv_2)]_\beta & \cdots & [T(Sv_n)]_\beta \end{bmatrix} \\ &= \begin{bmatrix} [T]_\gamma^\beta [(Sv_1)]_\gamma & [T]_\gamma^\beta [(Sv_2)]_\gamma & \cdots & [T]_\gamma^\beta [(Sv_n)]_\gamma \end{bmatrix} \\ &= [T]_\gamma^\beta \begin{bmatrix} [(Sv_1)]_\gamma & [(Sv_2)]_\gamma & \cdots & [(Sv_n)]_\gamma \end{bmatrix} \\ &= [T]_\gamma^\beta [S]_\alpha^\gamma. \end{aligned}$$

(iii) By (ii) we have

$$I = [I_V]_\alpha^\alpha = [I_V]_\beta^\alpha [I_V]_\alpha^\beta,$$

where I is an identity matrix. Hence $[I_V]_\beta^\alpha$ and $[I_V]_\alpha^\beta$ are inverse to each other. $\square$

Example 3.2.10 (Change of Coordinates). Let α and β be bases of $\mathbb{R}^2$ defined by

$$\alpha = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix} \right\} \quad \text{and} \quad \beta = \left\{ \begin{bmatrix} 7 \\ 8 \end{bmatrix}, \begin{bmatrix} 9 \\ 10 \end{bmatrix} \right\}.$$

We try to find the change of coordinate matrix from α to β: $[I_{\mathbb{R}^2}]_\alpha^\beta$ (§).

Let $A = \left[\begin{smallmatrix} 1 & 3 \\ 2 & 4 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 7 & 9 \\ 8 & 10 \end{smallmatrix}\right]$ and let ϵ be the standard basis of $\mathbb{R}^2$. It is not hard to check $[I_{\mathbb{R}^2}]_\alpha^\epsilon = A$ and $[I_{\mathbb{R}^2}]_\alpha^\epsilon = B$, hence

$$[I_{\mathbb{R}^2}]_\alpha^\beta = [I_{\mathbb{R}^2}]_\epsilon^\beta [I_{\mathbb{R}^2}]_\alpha^\epsilon = ([I_{\mathbb{R}^2}]_\beta^\epsilon)^{-1} [I_{\mathbb{R}^2}]_\alpha^\epsilon = B^{-1}A = \begin{bmatrix} 4 & 3 \\ -3 & -2 \end{bmatrix}.$$

Example 3.2.11. Let $T \in \mathcal{L}(V, W)$. Also let α, α' be two bases of V and β, β' two bases of W, then $[T]_\alpha^\beta$ and $[T]_{\alpha'}^{\beta'}$ are related by

$$[T]_{\alpha'}^{\beta'} = [I_W]_\beta^{\beta'} [T]_\alpha^\beta [I_V]_{\alpha'}^\alpha.$$

This can be shown by repeatedly using (ii) of Theorem 3.2.9. Indeed from the RHS,

$$[I_W]_\beta^{\beta'} \left([T]_\alpha^\beta [I_V]_{\alpha'}^\alpha \right) = [I_W]_\beta^{\beta'} [T I_V]_{\alpha'}^\beta = [I_W T I_V]_{\alpha'}^{\beta'} = [T]_{\alpha'}^{\beta'}.$$

In particular, if $W = V$, we have

$$[T]_{\alpha'}^{\alpha'} = [I_V]_\alpha^{\alpha'} [T]_\alpha^\alpha [I_V]_{\alpha'}^\alpha = ([I_V]_{\alpha'}^\alpha)^{-1} [T]_\alpha^\alpha [I_V]_{\alpha'}^\alpha.$$

In the above, if we denote $P = [I_V]_{\alpha'}^\alpha$, then we have $[T]_{\alpha'}^{\alpha'} = P^{-1}[T]_\alpha^\alpha P$, in this case we say that $[T]_{\alpha'}^{\alpha'}$ and $[T]_\alpha^\alpha$ are *similar*:

Definition 3.2.12. Let $A, B \in M_{n\times n}(\mathbb{R})$, A and B are said to be **similar** if there is an invertible matrix $P \in M_{n\times n}(\mathbb{R})$,

$$A = P^{-1}BP.$$

Example 3.2.13 (Change of Bases From $\mathbb{R}^n$ to $\mathbb{R}^m$). Let $P \in M_{m\times n}(\mathbb{R})$, then there corresponds a linear transformation $T_P \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^m)$ defined by

$$T_P(x) = Px.$$

Let ϵ be the usual basis of $\mathbb{R}^n$ and ϵ' that of $\mathbb{R}^m$, then $[T_P]_\epsilon^{\epsilon'} = P$. Now in general we are interested in how will P change (more precisely, $[T_P]_\epsilon^{\epsilon'}$) if we give $\mathbb{R}^n, \mathbb{R}^m$ a pair of nonstandard bases. Let α and β be such a pair, then

$$[T_P]_\alpha^\beta = [I_{\mathbb{R}^m}]_{\epsilon'}^\beta [T_P]_\epsilon^{\epsilon'} [I_{\mathbb{R}^n}]_\alpha^\epsilon = B^{-1}PA,$$

where the ith columns of A and B are the ith vectors of the bases α and β respectively. This is **natural** because B^{-1}, as we see in Example 3.2.2, can extract the coordinate of Pa_k w.r.t. β (look at the matrix in (3.2.5) to *feel* what I am talking about).

(§) This matrix is also called a **transition matrix** from α to β because $[I_{\mathbb{R}^2}]_\alpha^\beta [x]_\alpha = [x]_\beta$.

3.3 Exercises

Linear Transformations

Problem 3.1. Determine which of the following maps are linear transformations.

(a) The transformation T defined by $T(x_1, x_2)^T = (2x_1 - 3x_2, x_1 + 4, 5x_2)^T$.

(b) The transformation T defined by $T(x_1, x_2)^T = (4x_1 - 2x_2, 3|x_2|)^T$.

(c) The transformation T defined by $T(x_1, x_2, x_3)^T = (1, x_2, x_3)^T$.

(d) The transformation T defined by $T(x_1, x_2, x_3)^T = (x_1, 0, x_3)^T$.

(e) The transformation T defined by $T(x_1, x_2, x_3)^T = (x_1, x_2, -x_3)^T$.

Answers: (a) No (b) No (c) No (d) Yes (e) Yes

Problem 3.2. Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Determine whether or not T is one-to-one in each of the following situations:

(a) When $n > m$: ______

(b) When $n = m$: ______

(c) When $n < m$: ______

Fill the symbols A, B and C in ______ defined below:

$\boxed{\text{A}}$ T is a one-to-one transformation.	$\boxed{\text{B}}$ T is not a one-to-one transformation.	$\boxed{\text{C}}$ There is not enough information to tell.

Answers: (a) B (b) C (c) C

Problem 3.3. Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Let A be the standard matrix of T.

Fill the correct symbols A, B and C in ______ for each of the following situations.

(a) If every row in the row echelon form of A has a pivot, then ______

(b) If the row echelon form of A has a row of zeros, then ______

(c) If two rows in the row echelon form of A do not have pivots, then ______

(d) If the row echelon form of A has a pivot in every column, then ______

Where:

$\boxed{\text{A}}$ T is not onto.	$\boxed{\text{B}}$ T is onto.	$\boxed{\text{C}}$ there is not enough information to tell.

Answers: (a) B (b) A (c) A (d) C

Problem 3.4. Let V be a vector space and $\Lambda, \Lambda_1, \Lambda_2, \ldots, \Lambda_n \in \mathcal{L}(V, \mathbb{F})$. If $\bigcap_{j=1}^n \ker \Lambda_j \subseteq \ker \Lambda$, prove that Λ is a linear combination of Λ_j's.

Hint. Show that

$$W := \{(\Lambda x, \Lambda_1 x, \Lambda_2 x, \ldots, \Lambda_n x)^T : x \in V\}$$

is a proper subspace of $\mathbb{F}^{n+1}$. Extract the "extra point" $v \in \mathbb{F}^{n+1} \setminus W$ and then separate W and v by using a hyperplane constructed in Example 3.1.8.

Problem 3.5. Prove that there does not exist a $T \in \mathcal{L}(\mathbb{R}^5, \mathbb{R}^2)$ whose null space equals

$$\{(x_1, x_2, x_3, x_4, x_5)^T \in \mathbb{R}^5 : x_1 = 3x_2 \text{ and } x_3 = x_4 = x_5\}.$$

Problem 3.6. Let $T \in \mathcal{L}(V, \mathbb{F})$ and $T \neq 0$ (i.e., there is $v \in V$, $Tv \neq 0$). Show that for every $u \notin \ker T$,

$$V = \operatorname{span}\{u\} \oplus \ker T.$$

Problem 3.7. Assume $B \in M_{n\times n}(\mathbb{F})$ satisfies $B^k = 0$ for some $k \geq 1$, show that every matrix in $M_{n\times n}(\mathbb{F})$ has the form $BA - A$, for some $A \in M_{n\times n}(\mathbb{F})$.

Problem 3.8. Let $T \in \mathcal{L}(\mathbb{P}_n(\mathbb{R}), \mathbb{R})$ be defined by

$$Tp = \text{sum of all coefficients of } p.$$

Show that **(i)** $\dim(\ker T) = n$; and **(ii)** conclude that $\{x - 1, x^2 - 1, \ldots, x^n - 1\}$ is a basis of $\ker T$.

Problem 3.9. Let $A, B \in M_{n\times n}(\mathbb{F})$ be idempotent matrices (i.e., $A^2 = A$ and $B^2 = B$) and $I - (A + B)$ be invertible. Show that A and B have equal ranks.

Problem 3.10. In this problem we will establish the proof of rank-nullity theorem.

(a) Let V and W be vector spaces and let $\dim V < \infty$. Show that any linear $T : V \to W$ satisfies the following

$$\dim V = \dim \ker T + \dim \operatorname{range} T \qquad (\clubsuit)$$

in the following steps.

<u>**Step 1.**</u> Explain why $(\clubsuit)$ is trivial if $\dim \ker T = 0$ or $\dim \ker T = \dim V$.

Suppose now $\dim \ker T < \dim V$, let $\alpha = \{u_1, u_2, \ldots, u_k\}$ be a basis of $\ker T$. Since $\ker T$ is a subspace of V, we extend α to a basis of V: $\{u_1, \ldots, u_k, w_1, \ldots, w_n\}$.

<u>**Step 2.**</u> Show that

$$\operatorname{range} T = \operatorname{span}\{Tw_1, \ldots, Tw_n\}.$$

Also show that $\{Tw_1, \ldots, Tw_n\}$ is linearly independent.

<u>**Step 3.**</u> Conclude $(\clubsuit)$.

(b) Let V and W be vector spaces, show that for any linear $T : V \to W$ we still have $(\clubsuit)$ **even when V is infinite dimensional**.

Problem 3.11. Let $a_1, a_2, \dots, a_k \in \mathbb{F}$ be distinct and $p_1, p_2, \dots, p_k \in \mathbb{N}$. Show that

$$\mathbb{P}_{p_1+\cdots+p_k-1}(\mathbb{F}) = \operatorname{span}\left\{ \begin{array}{ll} \prod_{j=1, j\neq 1}^{k} (x-a_j)^{p_j}(x-a_1)^{i_1} & \\ \prod_{j=1, j\neq 1}^{k} (x-a_j)^{p_j}(x-a_1)^{i_2} & i_1 = 0, 1, \dots, p_1 - 1 \\ \vdots & : \; i_2 = 0, 1, \dots, p_2 - 1 \\ & \vdots \\ \prod_{j=1, j\neq 1}^{k} (x-a_j)^{p_j}(x-a_1)^{i_k} & i_k = 0, 1, \dots, p_k - 1 \end{array} \right\}.$$

Therefore we always have the partial fraction decomposition: For every $p \in \mathbb{P}_{p_1+\cdots+p_k-1}(\mathbb{F})$, there are $A'_{ij}s$, $A_{ij} \in \mathbb{F}$, such that

$$\frac{p(x)}{(x-a_1)^{p_1}(x-a_2)^{p_2}\cdots(x-a_k)^{p_k}} = \sum_{i=1}^{k}\sum_{j=1}^{p_i} \frac{A_{ij}}{(x-a_i)^j}.$$

Problem 3.12. Let $M_{n\times n}(\mathbb{R})$ denote the vector space of all $n \times n$ matrices. For every $C \in M_{n\times n}(\mathbb{R})$, define the linear map $T_C : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$ in the following way

$$T_C(A) = \operatorname{Tr}(CA), \quad \text{for each } A \in M_{n\times n}(\mathbb{R}).$$

It is clear that $T_C \in (M_{n\times n}(\mathbb{R}))^*$, show that actually,

$$\{T_C : C \in M_{n\times n}(\mathbb{R})\} = \big(M_{n\times n}(\mathbb{R})\big)^*.$$

Problem 3.13. Let $\mathcal{A} = M_{n\times n}(\mathbb{C})$, we denote $M_{\mathcal{A}}$ the set of **<u>nonzero</u> multiplicative linear functionals** on A. By *multiplicative* we mean for every $\varphi \in M_{\mathcal{A}}$ and for every $A, B \in \mathcal{A}$, we have $\varphi(AB) = \varphi(A)\varphi(B)$.

(i) Show that for every $n \geq 1$, any nonzero $\varphi \in M_{\mathcal{A}}$ satisfies $\varphi(I_n) = 1$.

(ii) By using Problem 3.12, show that when $n \geq 2$, $M_{\mathcal{A}} = \emptyset$.

In other words, $M_{\mathcal{A}}$ has nonzero multiplicative linear functional only when $n = 1$.

Remark. The interest of $M_{\mathcal{A}}$ comes from analysis. When $\mathcal{A}$ is a *commutative* Banach algebra we often call $M_{\mathcal{A}}$ the **spectrum/maximal ideal space** of $\mathcal{A}$ since it is in 1-1 correspondence with maximal ideals in A. For example, let $\mathcal{A} = C[a, b]$ the set of continuous functions on $[a, b]$, one can show that $M_{\mathcal{A}}$ is the set of all pointwise evaluations.

Problem 3.14. Let V be a vector space. We define $V^* = \mathcal{L}(V, \mathbb{F})$ (called the **dual space** of V) and $V^{**} = (V^*)^*$ (called the **bidual** of V), let $i : V \to V^{**}$, with $i(v) \in V^{**}$ *pointwise* defined by

$$i(v)(T) = T(v) \quad \text{for all } T \in V^*.$$

We have shown in Example 3.1.20 that when V is finite dimensional, V and V^* are isomorphic. Show that i is an isomorphism between V and V^{**}.

Remark. The function i is important in functional analysis, called **canonical embedding**.

Matrix Representations

Problem 3.15. Let $T : \mathbb{P}_2(\mathbb{R}) \to \mathbb{P}_2(\mathbb{R})$ be defined by

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

Let $\alpha = \{1 + x, x + x^2, 1 + x + x^2\}$ and $\beta = \{1, x, x^2\}$, show that $[T]_\alpha^\beta = \left[\begin{smallmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 2 & 2 \end{smallmatrix}\right]$.

Problem 3.16. Let $T \in \mathcal{L}(\mathbb{P}_2(\mathbb{R}), \mathbb{R}^2)$ be defined by

$$T(a + bx + cx^2) = (a + b, c).$$

If we let $\alpha = \{1, x, x^2\}$ and $\beta = \{(1, -1)^T, (1, 1)^T\}$, show that $[T]_\alpha^\beta = \frac{1}{2}\left[\begin{smallmatrix} 1 & 1 & -1 \\ 1 & 1 & 1 \end{smallmatrix}\right]$.

Problem 3.17. Let $T \in \mathcal{L}(\mathbb{P}_2(\mathbb{R}), \mathbb{P}_2(\mathbb{R}))$ be defined by

$$(Tp)(x) = p(x) + \frac{dp}{dx}(x) + \frac{d^2p}{dx^2}(x).$$

Prove that T is an isomorphism, also, prove that

$$T^{-1}(a + bx + cx^2) = (a - b) + (b - 2c)x + cx^2.$$

Hint. We are very used to matrices, choose a suitable basis and represent our transformation T as matrix.

Problem 3.18. Show that all the matrices similar to an invertible matrix are invertible. Moreover, show that similar matrices have the same rank.

Problem 3.19. Provide a proof of Theorem 3.2.6 with the help of Theorem 3.2.3.

Problem 3.20. A nilpotent linear map $T : V \to V$ satisfies $T^q = 0$ for some $q \geq 1$.

(a) Prove that any square upper triangular matrix with diagonal elements zero is nilpotent.

(b) Conversely, if a nilpotent linear map $T : V \to V$ is defined on a finite dimensional vector space V, then there is a basis of V such that the matrix representation of T is triangular with diagonal element zero.

Problem 3.21. Let $T : V \to W$ be linear and $\dim V = \dim W < \infty$, show that there are bases α of V and β of W such that $[T]_\alpha^\beta$ is a diagonal matrix.

Problem 3.22. Prove that any 3×3 matrix A over $\mathbb{R}$ for which $A^2 \neq 0$ but $A^3 = 0$ is similar to the matrix

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Chapter 4

Simplification of Matrices

In this chapter we introduce three basic methods to decompose a given matrix. There are different advantages when using different methods. Sometimes simplification of a matrix simplifies a given problem. For example, given a specific matrix B, we try to find all matrices A such that $AB = BA$, equivalently for invertible P,

$$(P^{-1}AP)(P^{-1}BP) = (P^{-1}BP)(P^{-1}AP) \iff A'(P^{-1}BP) = (P^{-1}BP)A',$$

thus once we can decompose a matrix through a change of basis (diagonalization and Jordan form), then the problem is reduced to finding all matrices A' such that A' commutes with a simplified matrix $P^{-1}BP$. This is not a rare occasion that a simplification simplifies a mathematical problem. Sometimes we will find that SVD is more appropriate, it depends on the situation we have. You may work on exercises in this chapter to get exposed to them.

4.1 Diagonalization of Matrices

Throughout this section all scalar field will be denoted by $\mathbb{F}$ which is either $\mathbb{R}$ or $\mathbb{C}$. This is to develop the parallel story of diagonalizability of real and complex matrices at the same time. Some of the result in complex scalar field in this section will be used in this chapter.

4.1.1 Eigenvalues and Eigenvectors

Definition 4.1.1. Let $A \in M_{n\times n}(\mathbb{F})$, an **eigenvalue** of A is a $\lambda \in \mathbb{F}$ such that there is **nonzero** vector $v \in \mathbb{F}^n$, $Av = \lambda v$. Also, we call

$$\mathrm{Nul}(A - \lambda I)$$

the **eigenspace** of λ. Every **nonzero** $v \in \mathrm{Nul}(A - \lambda I)$ is called an **eigenvector** corresponding to the eigenvalue λ.

Theorem 4.1.2. *Let $A \in M_{n\times n}(\mathbb{F})$, then the following are equivalent:*

(i) *λ is an eigenvalue.*

(ii) $\mathrm{Nul}(A - \lambda I) \neq \{0\}$.

(iii) $\mathrm{rank}(A - \lambda I) < n$.

(iv) $\det(A - \lambda I) = 0$.

Proof. (i) $\Rightarrow$ (ii) Trivial.

(ii) $\Rightarrow$ (iii) By rank-nullity theorem (over $\mathbb{F}$),

$$\operatorname{rank}(A - \lambda I) < \dim(A - \lambda I) + \operatorname{rank}(A - \lambda I) = n.$$

(iii) $\Rightarrow$ (iv) Suppose $A - \lambda I$ is not surjective, it is not invertible, hence $\det(A - \lambda I) = 0$.

(iv) $\Rightarrow$ (i) $\det(A - \lambda I) = 0$ implies $A - \lambda I$ is not invertible, which is the same as $A - \lambda I$ is not injective, hence $\operatorname{Nul}(A - \lambda I) \neq \{0\}$, thus there is $v \neq 0$, $(A - \lambda I)v = 0$. □

It is easy to construct a matrix in $M_{2\times 2}(\mathbb{R})$ that has no eigenvalue (as $M_{2\times 2}(\mathbb{R})$ is a real vector space, by eigenvalue we mean real eigenvalue, according to Definition 4.1.1). For example, consider $R_{\pi/2}$ the rotation matrix from $\mathbb{R}^2$ to $\mathbb{R}^2$ by an angle $\pi/2$ counter-clockwise, no nonzero vector can be parallel to itself after a rotation, thus there is no $\lambda \in \mathbb{R}$ and nonzero $v \in \mathbb{R}^2$ such that $R_{\pi/2}v = \lambda v$.

This unpleasant feature can be eliminated if we enlarge the scalar field that we live in:

Corollary 4.1.3. *Let $A \in M_{n\times n}(\mathbb{C})$, then A has at least one eigenvalue.*

This is the first significant distinction between real and complex vector spaces that we see in this text. Later on we will see that the proofs of the existence of several decompositions of matrices depend heavily on the existence of at least one eigenvalue.

Proof. Since $p(z) = \det(A - zI)$ is a polynomial over $\mathbb{C}$, by fundamental theorem of algebra $p(z)$ has n roots (counting multiplicity) in $\mathbb{C}$, therefore there is at least one $z_0 \in \mathbb{C}$ such that $p(z_0) = 0$, and thus z_0 is an eigenvalue. □

Because of (iv) of Theorem 4.1.2 we define:

Definition 4.1.4. For $A \in M_{n\times n}(\mathbb{F})$, the degree n polynomial

$$p_A(t) = \det(A - tI)$$

is called the **characteristic polynomial** of A.

Remark. Now λ is an eigenvalue of A if and only if $p_A(\lambda) = 0$. The definition $\det(tI - A)$ is also commonly used to define characteristic polynomial, which is to obtain a polynomial with positive leading coefficient. This differs from our definition just by $(-1)^n$, and we persist in using $\det(A - tI)$ since it is slightly more convenient in computation.

Example 4.1.5. The characteristic polynomial of $A = \left[\begin{smallmatrix}1 & 2\\ 3 & 4\end{smallmatrix}\right]$ is

$$p_A(t) = \begin{vmatrix} 1-t & 2 \\ 3 & 4-t \end{vmatrix} = t^2 - 5t - 2$$

Example 4.1.6. If
$$A = \begin{bmatrix} a_{11} & & & * \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{bmatrix},$$
then $a_{11}, a_{22}, \dots, a_{nn}$ are eigenvalues of A. This can be seen by cofactor expansion of $p_A(t) = \det(A - tI)$ along the first column**S**.

Example 4.1.7. Let
$$A = \begin{bmatrix} 3 & 2 \\ 0 & 4 \end{bmatrix} \in M_{2\times 2}(\mathbb{R}),$$
we try to find all eigenvalues and eigenvectors of A. Note that by finding all eigenvectors we usually mean finding the basis of each eigenspace.

Since
$$p_A(t) = \det(A - tI) = \begin{vmatrix} 3-t & 2 \\ 0 & 4-t \end{vmatrix} = (3-t)(4-t),$$
3 and 4 are eigenvalues. Namely, both $\mathrm{Nul}(A-3I)$ and $\mathrm{Nul}(A-4I)$ are nonzero.

Next we find all eigenvectors.

When $t = 3$. We find $x \in \mathrm{Nul}(A-3I)$, i.e., we solve $(A-3I)x = 0$, then since
$$A - 3I = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix} \to \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix},$$
so $x_2 = 0$ and $x = (x_1, 0)^T = x_1(1,0)^T$, $(1,0)^T$ is an eigenvector.

When $t = 4$. We solve $(A-4I)x = 0$, since
$$A - 4I = \begin{bmatrix} -1 & 2 \\ 0 & 0 \end{bmatrix},$$
we have $x_1 = 2x_2$, so $x = (2x_2, x_2)^T = x_2(2,1)^T$, $(2,1)^T$ is an eigenvector.

Definition 4.1.8. Let $A \in M_{n\times n}(\mathbb{F})$ and let $p_A(\lambda) = 0$.

(i) The multiplicity of λ as a root of the polynomial $p_A(t)$ is called the **algebraic multiplicity** of λ.

(ii) $\dim \mathrm{Nul}(A - \lambda I)$ is called the **geometric multiplicity** of λ.

Geometric multiplicity essentially counts how many “distinct” vectors are in an eigenspace. If we have enough “distinct” vectors, i.e., if the geometric multiplicities are sufficiently large, then we shall see that a matrix will be diagonalizable. We elaborate this in the next section.

Example 4.1.9. Let $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M_{2\times 2}(\mathbb{R})$, then
$$p_A(t) = \det(A - tI) = t^2.$$

(i) Algebraic multiplicity of the eigenvalue 0 is 2.

(ii) The geometric multiplicity of 0 is $\dim \mathsf{Nul}\, A = 2$.

Example 4.1.10. Let
$$A = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} \in M_{4\times 4}(\mathbb{R}),$$
by Example 4.1.6 we know 1 and 2 are the only eigenvalues. We try to find the algebraic multiplicity and geometric multiplicity of 1 and 2 respectively.

Algebraic multiplicity. Since
$$p_A(t) = \det(A - tI) = (1-t)^2(2-t)^2,$$
the algebraic multiplicity of 1 and 2 are two.

Geometric multiplicity. We don't need to find the bases of $\mathsf{Nul}(A - I)$ and $\mathsf{Nul}(A-2I)$. We just need to row reduce $A - I$ and $A - 2I$ and count the number nonpivot columns.

Since
$$A - I = \begin{bmatrix} 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \to \cdots \to \begin{bmatrix} 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$
there is 1 nonpivot column, $\dim \mathsf{Nul}(A - I) = 1$.

Since
$$A - 2I = \begin{bmatrix} -1 & 2 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$
there are two nonpivot columns, so $\dim \mathsf{Nul}(A - 2I) = 2$.

We conclude that the geometric multiplicity of 1 is one and that of 2 is two.

In general the number of "distinct" eigenvectors of an eigenvalue λ cannot exceed the algebraic multiplicity of λ:

Theorem 4.1.11. *Let $A \in M_{n\times n}(\mathbb{F})$ and $p_A(\lambda) = 0$, then*
$$1 \leq \underline{\text{Geometric Multiplicity of } \lambda} \leq \underline{\text{Algebraic Multiplicity of } \lambda}.$$

Proof. Since $p_A(\lambda) = 0$, $A - \lambda I$ is not invertible, i.e., it is not injective, thus
$$\mathrm{Nul}(A - \lambda I) \neq 0 \implies \dim \mathrm{Nul}(A - \lambda I) \geq 1.$$

Let $\alpha = \{v_1, v_2, \ldots, v_k\}$ be a basis of $\mathrm{Nul}(A - \lambda I)$ and let $L_A : \mathbb{F}^n \to \mathbb{F}^n$ be defined by $L_A(x) = Ax$, for notational rigour.

If $k = n$, then $[L_A]_\alpha = \lambda I$, and thus
$$\det(A - xI) = \det([L_A]_\alpha - xI) = (\lambda - x)^n,$$
so the algebraic multiplicity of λ is also n, we are done.

Suppose that $k < n$, then we can extend α to $\beta = \{v_1, v_2, \ldots, v_k, v_{k+1}, \ldots, v_n\}$, a basis of $\mathbb{F}^n$, and the matrix representation of T w.r.t. β will be

$$[L_A]_\beta = \left[\begin{array}{c|c} \lambda I_k & * \\ \hline O & * \end{array}\right],$$

where I_k denotes a $k \times k$ identity matrix and O denotes a $(n-k) \times k$ zero matrix, now

$$[L_A]_\beta - xI = \left[\begin{array}{c|c} (\lambda - x) I_k & * \\ \hline O & * \end{array}\right],$$

it follows that

$$\det(A - xI) = \det([L_A]_\beta - xI) = (\lambda - x)^k p(x),$$

for some degree $n-k$ polynomial p. Thus λ is a root of $\det(A - xI)$ with algebraic multiplicity at least k, so we are done. $\square$

4.1.2 Diagonalizability and Diagonalization

Let's motivate the definition of diagonalizability. Given $A \in M_{n\times n}(\mathbb{F})$, suppose that there is a basis $\alpha = \{v_1, v_2, \ldots, v_n\}$ of $\mathbb{F}^n$ and each of v_i's is an eigenvector, then there are $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that

$$Av_k = \lambda_k v_k$$

for $k = 1, 2, \ldots, n$. Now the linear transformation $L_A : \mathbb{F}^n \to \mathbb{F}^n$ can be represented as a matrix w.r.t. α that has the form

$$[L_A]_\alpha = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}.$$

Let $P = [v_1 \quad \cdots \quad v_n]$, then $P^{-1}AP = [L_A]_\alpha$ is a diagonal matrix. Therefore we define:

Definition 4.1.12. $A \in M_{n\times n}(\mathbb{F})$ is said to be **diagonalizable** if one of the following equivalent statements hold:

(i) There is a basis consisting of eigenvectors.

(ii) There are n linearly independent eigenvectors.

(iii) The sum of all geometric multiplicities is n.

There are some particular results from which we can tell diagonalizability immediately.

Theorem 4.1.13. *Let $A \in M_{n\times n}(\mathbb{F})$. Eigenvectors associated to different eigenvalues are linearly independent.*

Proof. Let $\lambda_1, \lambda_2, \ldots, \lambda_p \in \mathbb{F}$ be distinct such that there are $v_1, v_2, \ldots, v_p \in \mathbb{F}^n$ satisfying $Av_i = \lambda_i v_i$ for each $i = 1, 2, \ldots, p$.

We prove by contradiction, suppose $\{v_1, \ldots, v_p\}$ is linearly dependent, then there is $k > 1$ such that $v_k \in \operatorname{span}\{v_1, v_2, \ldots, v_{k-1}\}$. Choose $k = N$, where

$$N = \min\{k > 1 : v_k \in \operatorname{span}\{v_1, v_2, \ldots, v_{k-1}\}\}.$$

then there are $a_1, a_2, \ldots, a_{N-1}$, not all zero, such that

$$a_1v_1 + a_2v_2 + \cdots + a_{N-1}v_{N-1} + v_N = 0. \tag{4.1.14}$$

We take A on both sides to get

$$a_1\lambda_1v_1 + a_2\lambda_2v_2 + \cdots + a_{N-1}\lambda_{N-1}v_{N-1} + \lambda_Nv_N = 0. \tag{4.1.15}$$

We perform $\lambda_N \times$ (4.1.14) $-$ (4.1.15) to get

$$(\lambda_N - \lambda_1)a_1v_1 + (\lambda_N - \lambda_2)a_2v_2 + \cdots + (\lambda_N - \lambda_{N-1})a_{N-1}v_{N-1} = 0,$$

a contradiction to the construction of N since we can further choose a number $N' = \max\{1 < i \leq N-1 : a_i \neq 0\}$, then $v_{N'} \in \operatorname{span}\{v_1, v_2, \ldots, v_{N'-1}\}$, with $N' \leq N - 1 < N$. □

Corollary 4.1.16. *Let $A \in M_{n\times n}(\mathbb{F})$. If $p_A(t)$ have n distinct roots, then A is diagonalizable.*

Proof. Since each of eigenvalues has at least one geometric multiplicity, hence n distinct roots of $p_A(t)$ corresponds to n eigenvectors which are linearly independent by Theorem 4.1.13. □

Example 4.1.17. Consider the matrix

$$\begin{bmatrix} 1 & 6 & 5 \\ 0 & 2 & 4 \\ 0 & 0 & 3 \end{bmatrix} \in M_{3\times 3}(\mathbb{R}).$$

Since there are three distinct eigenvalues $1, 2, 3$. By Corollary 4.1.16 the matrix is diagonalizable.

Example 4.1.18. We try to show

$$A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix} \in M_{3\times 3}(\mathbb{R})$$

is diagonalizable and find its diagonalization.

Consider

$$p_A(t) = \det(A - tI) = \begin{vmatrix} 2-t & 1 & 1 \\ 1 & 2-t & 1 \\ 1 & 1 & 2-t \end{vmatrix} = (t-1)^2(4-t),$$

as there are just two eigenvalues 1 and 4, Corollary 4.1.16 is not readily applicable. We need to count the geometric multiplicities carefully.

Geometric multiplicity of 1.

$$A - I = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

thus $\dim \operatorname{Nul}(A - I) = 2$.

Geometric Multiplicity of 4. Since algebraic multiplicity of 4 is one, by Theorem 4.1.11,

$$1 \le \dim \mathrm{Nul}(A - 4I) \le 1,$$

so $\dim \mathrm{Nul}(A - 4I) = 1$.

Conclusion: A is diagonalizable because the sum of all possible geometric multiplicities is 3. Next we try to find the diagonalization of A:

Basis of $\mathbf{Nul}(A - I)$. We make good use of the previous step, let $(A - I)x = 0$, then $x_1 = -x_2 - x_3$, so

$$x = (x_1, x_2, x_3)^T = x_2(-1, 1, 0)^T + x_3(-1, 0, 1)^T,$$

$(-1, 1, 0)^T$ and $(-1, 0, 1)^T$ are linearly independent, they form a basis of $\mathrm{Nul}(A - I)$.

Basis of $\mathbf{Nul}(A - 4I)$. We solve $(A - 4I)x = 0$, then

$$A - 4I = \begin{bmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{bmatrix} \to \cdots \to \begin{bmatrix} 1 & 1 & -2 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix},$$

so $x_2 = x_3$ and $x_1 = -x_2 + 2x_3 = x_3$, we have

$$x = (x_3, x_3, x_3)^T = x_3(1, 1, 1)^T,$$

$(1, 1, 1)^T$ is a basis of $\mathrm{Nul}(A - 4I)$.

Diagonalization. Let $P = \left[\begin{smallmatrix} -1 & -1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right]$, then

$$P^{-1}AP = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix}.$$

Example 4.1.19 (Nonexample). Not every matrix is diagonalizable. For example,

$$A := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_{2\times 2}(\mathbb{R})$$

is not diagonalizable. To see this, since $p_A(t) = \det(A - tI) = t^2$, 0 is the only eigenvalue, but $\operatorname{rank} A = 1$, so the geometric multiplicity of 0 is one. There are not enough eigenvectors to diagonalize A.

Alternatively, if A is diagonalizable, then there is an invertible matrix P such that $P^{-1}AP = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ (0 is the only eigenvalue), so $A = 0$, a contradiction.

Example 4.1.20 (Application of Diagonalization). Let $a_1, a_2, a_3 \ldots$ be a sequence of real numbers recursively defined by

$$a_{n+2} - 42a_{n+1} + 420a_n = 0.$$

We try to find a_n in terms of a_1 and a_2.

Define $x_n = (a_n, a_{n-1})^T$, we note that

$$x_{n+2} = \begin{bmatrix} a_{n+2} \\ a_{n+1} \end{bmatrix} = \begin{bmatrix} 42a_{n+1} - 420a_n \\ a_{n+1} \end{bmatrix} = \underbrace{\begin{bmatrix} 42 & -420 \\ 1 & 0 \end{bmatrix}}_{:=A} \begin{bmatrix} a_{n+1} \\ a_n \end{bmatrix} = Ax_{n+1}.$$

Hence the recursive relation can be repeated to get

$$x_{n+2} = Ax_{n+1} = A^2 x_{n+2} = \cdots = A^n x_2.$$

Now we try to diagonalize A. Since

$$p_A(t) = \det(A - tI) = \begin{vmatrix} 42-t & -420 \\ 1 & -t \end{vmatrix} = t^2 - 42t + 420,$$

by solving it, we have two roots $\alpha = 21 + \sqrt{21}$ and $\beta = 21 - \sqrt{21}$. Corollary 4.1.16 tells us A is diagonalizable. Let P be invertible such that $P^{-1}AP = \left[\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right]$, then

$$x_{n+2} = \left(P \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix} P^{-1} \right)^n x_2 = P \begin{bmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{bmatrix} P^{-1} x_2.$$

To find P it is enough to find all eigenvectors and put them together column by column. The eigenvector corresponding to α is $(\alpha, 1)^T$ and that corresponding to β is $(\beta, 1)^{T\,(*)}$, hence

$$P = \begin{bmatrix} \alpha & \beta \\ 1 & 1 \end{bmatrix}$$

and thus the tedious computation yields

$$x_{n+2} = \frac{1}{2\sqrt{21}} \begin{bmatrix} \alpha^{n+1} - \beta^{n+1} & \alpha\beta^{n+1} - \alpha^{n+1}\beta \\ \alpha^n - \beta^n & \alpha\beta^n - \alpha^n\beta \end{bmatrix} x_2,$$

so

$$a_n = \frac{1}{2\sqrt{21}} \left((\alpha\beta^{n-1} - \alpha^{n-1}\beta)a_1 + (\alpha^{n-1} - \beta^{n-1})a_2 \right).$$

The concept of determinant can be generalized to arbitrary linear map $T : V \to V$ whenever V is finite dimensional:

Definition 4.1.21. Let V be finite dimensional, $T \in \mathcal{L}(V, V)$ and α a basis of V.

(i) We define $\det T = \det\big([T]_\alpha\big)$.

(ii) We define the characteristic polynomial of T, $p_T(t)$, by

$$p_T(t) = \det\big([T]_\alpha - tI\big).$$

It is left as an exercise to check these definitions are independent of the choice of bases of V (see Problem 4.13). The definition of eigenvalues, eigenvectors and eigenspaces can be extended to general vector space in an obvious way. The question of eigenvalues, eigenvectors and "diagonalization" (existence of basis consisting of eigenvectors) can be discussed through matrix representation by fixing a choice of bases$^{(\dagger)}$.

(*) I get these by solving the systems as before. We note that it is easy to check $(a, 1)^T$ and $(b, 1)^T$ are always the eigenvectors of $\left[\begin{smallmatrix} a+b & -ab \\ 1 & 0 \end{smallmatrix}\right]$. By these observations, it is easy to generalize the problem, i.e., find the closed form of a_n defined by $a_{n+2} + Aa_{n+1} + Ba_n = 0$.

(†) This is simple just for linear maps between finite dimensional vector spaces! The similar problems in infinite dimensional spaces are studied in functional analysis, specifically in spectral theory.

4.2 Singular Value Decomposition (SVD)

4.2.1 Matrix p-Norms and Frobenius Norm

We will adopt the following convention: For a matrix $A : \mathbb{F}^n \to \mathbb{F}^m$ the p-norm ($1 \leq p \leq \infty$) of A is denoted by

$$\|A\|_p = \sup\{\|Ax\|_p : x \in \mathbb{F}^n, \|x\|_p = 1\}.$$

$\|\cdot\|_p$ on $M_{m\times n}(\mathbb{F})$ is called *matrix norm* or more generally *operator norm*. This "norm" really defines a norm on the vector space $M_{m\times n}(\mathbb{F})$. Another norm that is commonly used is *Frobenius norm*: For $A = [a_{ij}] \in M_{m\times n}(\mathbb{F})$,

$$\|A\|_F := \sqrt{\operatorname{Tr}(A^*A)} = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} |a_{ij}|^2}.$$

p-norm and Frobenious norm satisfy the following similar properties:

(i) $\|AB\|_p \leq \|A\|_p\|B\|_p$

(ii) $\|AB\|_F \leq \|A\|_F\|B\|_F$

(iii) $\|Ax\|_p \leq \|A\|_p\|x\|_p$

(iv) $\|Ax\|_2 \leq \|A\|_F\|x\|_2$

Special choices of p do have specific geometrical meanings, say $p = 2$ in this section. We are able to compute matrix norms explicitly in some cases. For example, let a_i's be column vectors of $\mathbb{R}^m$, from definition it is easy to show that

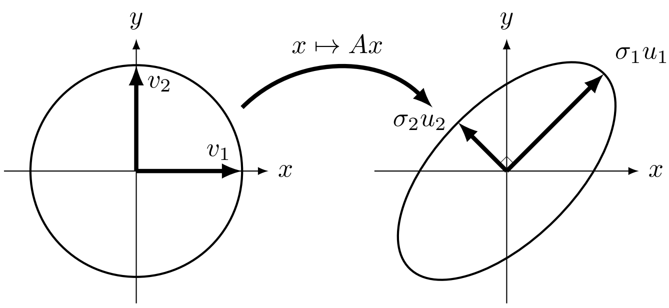
$$A = \begin{bmatrix} | & & | \\ a_1 & \cdots & a_n \\ | & & | \end{bmatrix} \implies \|A\|_1 = \max_{1\leq j\leq n} \|a_j\|_1 \tag{4.2.1}$$

$$A = \begin{bmatrix} \text{———} \; a_1 \; \text{———} \\ \vdots \\ \text{———} \; a_n \; \text{———} \end{bmatrix} \implies \|A\|_\infty = \max_{1\leq i\leq m} \|a_i^t\|_1 \tag{4.2.2}$$

In words, $\|A\|_1$ is the maximum (absolute) column sum, while $\|A\|_\infty$ is the maximum (absolute) row sum.

4.2.2 Heuristic Derivation of SVD

Let A be an $m\times n$ real matrix. We assume, and what we are trying to prove, that $A(S^{n-1}) = \{Ax : x \in S^{n-1}\}$ is a "hyperellipse" (or just an ellipse when $n \leq 3$). Suppose also that $m \geq n$ and A is of full rank, then there are unit vectors $u_1, \ldots, u_n$ in $\mathbb{R}^m$ which point in the direction of semi-axises of the hyperellipse.



We can describe a general construction for u_i's.

Step 1.

Find a vector $u_1' \in \mathbb{R}^m \in AS^{n-1}$ that has largest length, call it $a \in \mathbb{R}^m$, i.e.,

$$\|u_1'\|_2 = \|A\|_2 := \max\{\|Ax\|_2 : x \in \mathbb{R}^n, \|x\|_2 = 1\}.$$

Write $u_1' = \sigma_1 u_1$ with $\|u_1\| = 1$.

Step 2.

Find another vector u_2' in $AS^{n-1} \cap (\mathbb{R}u_1')^\perp$ that has largest length, i.e.,

$$\|u_2'\|_2 = \max\{\|x\|_2 : x \in AS^{n-1} \cap (\mathbb{R}u_1')^\perp\}.$$

Write $u_2' = \sigma_2 u_2$ with $\|u_2\| = 1$.

Step j.

Find $u_j' \in AS^{n-1} \cap (\mathbb{R}u_1')^\perp \cap \cdots \cap (\mathbb{R}u_{j-1}')^\perp$ that has largest length, namely,

$$\|u_j'\|_2 = \max\{\|x\|_2 : x \in AS^{n-1} \cap (\mathbb{R}u_1')^\perp \cap \cdots \cap (\mathbb{R}u_{j-1}')^\perp\}.$$

Write $u_j' = \sigma_j u_j$ with $\|u_j\| = 1$.

We can continue the process for $j = 2, 3, \ldots, n$. This is indeed how we find semi-axises of an ellipse in $\mathbb{R}^3$ and $\mathbb{R}^2$.

Now in the described procedure, the length of semi-axis in the direction of $\sigma_i := \|u_i'\|_2$ is in nonincreasing order, i.e., $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n > 0$ (since we assume A has full rank). Take a unit vector $v_i \in A^{-1}(\sigma_i u_i)$ (recall that $u_i' = \sigma_i u_i \in AS^{n-1}$), one has

$$A \underbrace{\begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}}_{:=V} = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix} \begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_n \end{bmatrix}.$$

Let $u_{n+1}, \ldots, u_m$ be orthonormal basis in $(\operatorname{span}_{\mathbb{R}}\{u_1, \ldots, u_n\})^\perp$, then RHS of the above equation becomes

$$\underbrace{\begin{bmatrix} u_1 & \cdots & u_n & u_{n+1} & \cdots & u_m \end{bmatrix}}_{:=U} \underbrace{\begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_n \\ \hline & \mathcal{O} & \end{bmatrix}}_{:=\Sigma}$$

where $\mathcal{O}$ denotes a matrix with only 0 entries. One can rewrite the above as: $AV = U\Sigma$. It will be proved that indeed $\{v_i\}$ is orthonormal, hence we can conclude both V, U are unitary, and we arrive to the expression

$$A = U\Sigma V^*.$$

Owing to this decomposition u_i's are called **left-singular vectors**, v_i's are called **right-singular vectors** and "diagonal" elements (i.e., if $\Sigma = [d_{ij}]_{m\times n}$, diagonal elements are d_{ii}'s) are called **singular values**. These basically are all the motivation of the general result.

4.2.3 Proof to Existence of "Unique" SVD

In the following, $\mathcal{O}$ denotes a zero matrix of appropriate size.

Theorem 4.2.3.

(i) Every matrix $A \in M_{m\times n}(\mathbb{C})$ has a SVD:

$$A = U\Sigma V^* \qquad \boxed{\begin{array}{ll} U \in M_{m\times m}(\mathbb{C}) & \text{is unitary} \\ V \in M_{n\times n}(\mathbb{C}) & \text{is unitary} \\ \Sigma \in M_{m\times n}(\mathbb{R}) & \text{is “diagonal”} \end{array}}$$

Furthermore, the singular values σ_j's, $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_{\min\{m,n\}}$, are uniquely determined.

(ii) If A is square and σ_j's are distinct, then the left and right singular vectors $\{u_j\}, \{v_j\}$ are unique up to a multiplicative constant with modulus 1.

By examining each step in the following proof, it is no point to require the scalar field be nonreal, therefore after the proof we record Corollary 4.2.7 here as a direct consequence. We start with $\mathbb{C}$ merely because the statement will be more comprehensive.

Proof. (i) The case that $m = 1$ or $n = 1$ is simple, let's assume $m, n \geq 2$. Let $\sigma_1 = \|A\|_2$, then due to compactness of $\{x \in \mathbb{C}^n : \|x\|_2 = 1\}$ in $\mathbb{C}^n$ and the continuity of the map $x \mapsto \|Ax\|_2$, there must be $v_1 \in \mathbb{C}^n$ with $\|v_1\|_2 = 1$ s.t. $\|Av_1\|_2 = \sigma_1$, so there is $u_1 \in \mathbb{C}^m$, $\|u_1\|_2 = 1$, $Av_1 = \sigma_1 u_1$. Hence $\|A\|_2$ is our first singular value.

Extend u_1 to an o.n. basis $\{u_1, \ldots, u_m\}$ of $\mathbb{C}^m$ and v_1 to an o.n. basis $\{v_1, \ldots, v_n\}$ of $\mathbb{C}^n$. Let U_1 be the matrix with columns u_i and V_1 be that with columns v_i, then

$$U_1^* A V_1 = [A]^{\{u_1,\ldots,u_m\}}_{\{v_1,\ldots,v_n\}} = \left[\begin{array}{c|c} \sigma_1 & w^* \\ \hline \mathcal{O} & B \end{array}\right] =: S. \tag{4.2.4}$$

Now

$$\left\| S \begin{bmatrix} \sigma_1 \\ w \end{bmatrix} \right\|_2 \geq \sigma_1^2 + w^* w = \sqrt{\sigma_1^2 + w^* w} \left\| \begin{bmatrix} \sigma_1 \\ w \end{bmatrix} \right\|_2,$$

this implies $w = \mathcal{O}$. Therefore $Av_2, Av_3, \ldots, Av_n \in \operatorname{span}\{u_2, u_3, \ldots, u_m\}$,

$$B = [A]^{\{u_2,\ldots,u_m\}}_{\{v_2,\ldots,v_n\}}.$$

Note that we have $x \perp v_1 \implies Ax \perp Av_1$, and the only assumption to derive this result is $\|Av_1\|_2 = \|A\|_2$, with $\|v_1\|_2 = 1$. We extract this as a technical corollary.

Corollary 4.2.5. *Let $A \in M_{m\times n}(\mathbb{C})$, $v \in \mathbb{C}^n$ with $\|v\|_2 = 1$. Then if $\|Av\|_2 = \|A\|_2$,*

$$w \perp v \implies Aw \perp Av.$$

The same is true when $\mathbb{C}$ is replaced by $\mathbb{R}$.

Proof. Repeat what we have done so far, i.e., replace v by v_1 and $\frac{Av_1}{\|Av_1\|_2}$ by u_1 in the argument preceding the corollary. Then once $w \perp v$, one has $Aw \perp Av_1 = Av$.$\square$

To finish the proof let's induct on $k \geq 4$, where $m + n = k$. Suppose any $m \times n$ matrix with $m + n = 4, 5, \ldots, k-1$ has SVD with uniquely determined singular values in descending order. Then for $m+n=k$, by induction hypothesis, $B = U_2\Sigma V_2^*$ with unique Σ, and the existence of SVD follows from the formula:

$$U_1^*AV_1 = \left[\begin{array}{c|c}\sigma_1 & \mathcal{O} \\ \hline \mathcal{O} & U_2\Sigma V_2^*\end{array}\right] = \left[\begin{array}{c|c}1 & \mathcal{O} \\ \hline \mathcal{O} & U_2\end{array}\right]\left[\begin{array}{c|c}\sigma_1 & \mathcal{O} \\ \hline \mathcal{O} & \Sigma\end{array}\right]\left[\begin{array}{c|c}1 & \mathcal{O} \\ \hline \mathcal{O} & V_2^*\end{array}\right]. \tag{4.2.6}$$

Although Σ is unique for smaller matrices, "Σ" for the matrix A depends on B, while B is dependent on the choice of basis. Fortunately under any changes of $(u_2,\dots,u_m)$ and $(v_2,\dots,v_n)$ to other o.n. bases, U_2 and V_2 will be replaced by other unitary matrices and Σ remains unchanged, hence singular values of A are unique. The proof is almost completed by induction, except for the base case $m+n=4$, which is obvious by (4.2.4).

(ii) Let's assume $A \in M_{n\times n}(\mathbb{C})$ is square. It is clear that $\sigma_1 = \|A\|_2$ since $\|A\|_2$ is the largest possible singular value of A. We first prove that if the right singular vector of σ_1 is not "unique", then σ_1 is not simple, i.e., σ_1 is repeated in Σ.

Let $Av_1 = \sigma_1 u_1$, $\|v_1\|_2 = \|u_1\|_2 = 1$. Suppose there are other vectors $w, w' \in \mathbb{C}^n$, with $\|w\|_2 = \|w'\|_2 = 1$ s.t. $Aw = \sigma_1 w'$. For the sake of contradiction, let's assume $w \notin \mathbb{C}v_1$, then the unit vector $v_2 := \frac{w-\langle v_1,w\rangle v_1}{\|w-\langle v_1,w\rangle v_1\|_2}$ is orthogonal to v_1. Now $\|Av_2\|_2 \le \|A\|_2 = \sigma_1$, the inequality cannot be strict, otherwise since $w = cv_1 + sv_2$ with $|c|^2+|s|^2 = 1$, we have

$$\sigma_1^2 = \|Aw\|_2^2 = \|c\sigma_1 u_1 + sAv_2\|_2^2 = |c|^2|\sigma_1|^2 + |s|^2\|Av_2\|_2^2 < \sigma_1^2,$$

absurd. We conclude $Av_2 = \sigma_1 u_2$, for some unit vector $u_2 \in (\mathbb{C}u_1)^\perp$. Now by the corollary one observes that

$$A|_{(\mathrm{span}_{\mathbb{C}}\{v_1,v_2\})^\perp} : (\mathrm{span}_{\mathbb{C}}\{v_1,v_2\})^\perp \to (\mathrm{span}_{\mathbb{C}}\{u_1,u_2\})^\perp,$$

and thus we can get a complete list of singular values with σ_1 appears twice, a contradiction. Hence if σ_j's are distinct, $w \in \mathbb{C}v_1$, i.e., w and v_1 differ by a multiplicative constant with modulus 1. It follows that u_1 is unique up to a complex sign. Finally since $A|_{(\mathbb{C}v_1)^\perp} : (\mathbb{C}v_1)^\perp \to (\mathbb{C}u_1)^\perp$, by choosing the bases of these two spaces, the uniqueness follows from induction on dimension of the square matrix. □

Corollary 4.2.7. *Theorem 5.8.4 is also true if all symbols $\mathbb{C}$ are replaced by $\mathbb{R}$.*

4.3 Jordan Canonical Form

4.3.1 Upper-Triangularization and a Brief Introduction to Jordan Form

Suppose we are concerned with complex matrices, then every complex matrix has at least one complex eigenvalue by Corollary 4.1.3. Not only that, if we consider the matrix A as a map $\mathbb{C}^n \to \mathbb{C}^n$, then we have the following:

Theorem 4.3.1. *Every square complex matrix can be made upper-trianglar under a change of basis.*

More precisely, we can find a basis $\{u_1, u_2, \dots, u_n\}$ of $\mathbb{C}^n$ such that, with $P = [u_1 \ \cdots \ u_n]$, $P^{-1}AP$ is upper-triangular. i.e., A is similar to an upper-triangular matrix.

Proof. We prove by induction on the size of matrices. The proposition is obviously true for 1×1 matrix. Suppose every $(n-1) \times (n-1)$ matrix is similar to an upper-triangular matrix. Let A be $n \times n$, then there is $u \in \mathbb{C}^n \setminus \{0\}$ and $\lambda \in \mathbb{C}$ such that

$$Au = \lambda u.$$

Extend $\{u\}$ to a basis of $\mathbb{C}^n$: $\{u, v_1, \ldots, v_{n-1}\}$ and let $P = [u \quad v_1 \quad \cdots \quad v_{n-1}]$, then

$$P^{-1}AP = \begin{bmatrix} \lambda & * \\ 0 & A' \end{bmatrix},$$

where A' is $(n-1) \times (n-1)$, hence by induction hypothesis, there is an invertible $Q \in M_{(n-1)\times(n-1)}(\mathbb{C})$ such that $Q^{-1}A'Q$ is upper-triangular. Let $D = \left[\begin{smallmatrix} 1 & 0 \\ 0 & Q \end{smallmatrix}\right]$, then $D^{-1} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & Q^{-1} \end{smallmatrix}\right]$, hence

$$\underbrace{D^{-1}P^{-1}}_{=(PD)^{-1}}APD = \begin{bmatrix} 1 & 0 \\ 0 & Q^{-1} \end{bmatrix} \begin{bmatrix} \lambda & * \\ 0 & A' \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix} = \begin{bmatrix} \lambda & * \\ 0 & Q^{-1}A'Q \end{bmatrix},$$

since PD is invertible, we are done. $\square$

The key to the proof is the existence of eigenvalue, which is a major distinction between (finite dimensional) real vector spaces and complex vector spaces.

Theorem 4.3.1 can be directly translated to every linear $T : V \to V$, with V a finite dimensional complex vector space:

Theorem 4.3.2. *Let V be a finite dimensional complex vector space and $T : V \to V$ linear, then there is a basis $\{v_1, v_2, \ldots, v_n\}$ of V such that*

$$Tv_k \in \operatorname{span}\{v_1, v_2, \ldots, v_k\}$$

for each $k = 1, 2, \ldots, n$

Proof. We fix a choice of bases α of V and apply Theorem 4.3.1 to $[T]_\alpha$. $\square$

Now we are going to show that under a change of basis, a matrix can be made not only upper-triangular, but also in the following much simpler form:

Theorem 4.3.3 (Jordan Canonical Form). *Let V be a finite dimensional complex vector space and $T : V \to V$ a linear map, then there is a basis $\mathcal{B}$ of V such that*

$$[T]_{\mathcal{B}} = \begin{bmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_k \end{bmatrix},$$

where J_i, called ***Jordan block****, is a matrix of the form*

$$[\lambda] \quad \textit{or} \quad \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{bmatrix}.$$

The basis in Jordan canonical form theorem is called a **Jordan basis**, the adjective "canonical" can be omitted for simplicity. Precisely, a **Jordan form** is a diagonal block matrix whose blocks are Jordan blocks. We defer the proof of the existence of Jordan basis to Section 4.3.4. Before this section, we will build several preliminary results and also the concept of generalized eigenspace which we are going to study.

4.3.2 Cayley-Hamilton Theorem

Definition 4.3.4. Let V be a finite dimensional complex vector space and T linear. We denote p_T the characteristic polynomial of T, namely,

$$p_T = \det(T - zI).$$

Here $\det T$ is define to be $\det[T]_{\mathcal{B}}$, for any basis $\mathcal{B}$ of V. It can be shown that $\det T$ is independent of the choices of bases of V.

Theorem 4.3.5 (Cayley-Hamilton). *Suppose that V is a finite dimensional complex vector space and $T : V \to V$ is linear, then $p_T(T) = 0$.*

Given a polynomial $q(z) = a_0 + a_1 z + \cdots + a_n z^n$, the symbol $q(T)$ means

$$q(T) = a_0 I + a_1 T + \cdots + a_n T^n,$$

whereas in Theorem 4.3.5 the statement $p_T(T) = 0$ means $p_T(T)$ is a zero linear map from V to V.

Proof. By Theorem 4.3.2, there is a basis $\{v_1, v_2, \ldots, v_n\}$ of V such that

$$Tv_k \in \operatorname{span}\{v_1, v_2, \ldots, v_k\}$$

for $k = 1, 2, \ldots, n$. Moreover, let $\mathcal{B} = \{v_1, \ldots, v_n\}$,

$$[T]_{\mathcal{B}} = \begin{bmatrix} \lambda_1 & & & * \\ 0 & \lambda_2 & & \\ 0 & 0 & \ddots & \\ 0 & 0 & 0 & \lambda_n \end{bmatrix}. \tag{4.3.6}$$

Hence $p_T(z) = \det(T - zI) = (-1)^{\dim V}(z - \lambda_1)(z - \lambda_2)\cdots(z - \lambda_n)$. Now to show $p_T(T) = 0$, we try to show for each $k = 1, 2, \ldots, n$, $(T - \lambda_1 I)\cdots(T - \lambda_k I)v_k = 0$. By (4.3.6) we have $Tv_1 = \lambda_1 v_1$, so the case that $k = 1$ is done. Suppose that

$$\begin{aligned} 0 &= (T - \lambda_1 I) \\ 0 &= (T - \lambda_1 I)(T - \lambda_2 I)v_2 \\ &\vdots \\ 0 &= (T - \lambda_1 I)\cdots(T - \lambda_{k-1} I)v_{k-1}. \end{aligned}$$

Since $(T - \lambda_k I)v_k = Tv_k - \lambda_k v_k \in \operatorname{span}\{v_1, v_2, \ldots, v_{k-1}\}$, by induction we are done. □

4.3.3 Generalized Eigenspaces

Definition 4.3.7. Let V be a finite dimensional complex vector space and $T : V \to V$ linear. Let λ be an eigenvalue of T, we define

$$\mathcal{E}_\lambda = \{v \in V : (T - \lambda I)^k v = 0, \exists k \geq 1\},$$

called a **generalized eigenspace** with eigenvalue λ. Every $v \in \mathcal{E}_\lambda \setminus \{0\}$ is called a **generalized eigenvector** with eigenvalue λ.

Of couse if we denote E_λ the eigenspace of T, then

$$\{0\} \subsetneq E_\lambda \subseteq \mathcal{E}_\lambda.$$

Generally $E_\lambda \neq \mathcal{E}_\lambda$. For example, consider $A = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, the characteristic polynomial of A is $\det(zI - A) = (z-1)^2$, so the only eigenvalue is 1. But $A - I \to \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$, hence

$$\dim E_\lambda = \dim \operatorname{Nul}(A - I) = 1.$$

However, $(A - I)^2 = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, so $\dim \operatorname{Nul}(A-I)^2 = 2$, it follows that $\mathcal{E}_\lambda \supseteq \operatorname{Nul}(A - I)^2 = \mathbb{R}^2$, so

$$\dim \mathcal{E}_\lambda = 2,$$

of course $E_\lambda \neq \mathcal{E}_\lambda$. We also note that the following are equivalent:

(i) $v \in \mathcal{E}_\lambda \setminus \{0\}$

(ii) $v \neq 0$ and there is $n \geq 1$, $(T - \lambda I)^n v = 0$.

(iii) There is $k \geq 0$ such that $(T - \lambda I)^k v$ is an λ-eigenvector.

Theorem 4.3.8. *Let V be a finite dimensional complex vector space and $T : V \to V$ linear. Let λ, μ be eigenvalues of T.*

(i) $\mathcal{E}_\lambda = \ker(T - \lambda I)^{\dim V}$.

(ii) If $\mu \neq \lambda$, $\mathcal{E}_\lambda \cap \mathcal{E}_\mu = \{0\}$.

(iii) If $\mu \neq \lambda$, then $(T - \mu I)|_{\mathcal{E}_\lambda} : \mathcal{E}_\lambda \to \mathcal{E}_\lambda$ is invertible.

Proof. (i) Consider the following:

$$\{0\} \subsetneq \ker(T - \lambda I) \subseteq \ker(T - \lambda I)^2 \subseteq \cdots \subseteq \ker(T - \lambda I)^{\dim V} \subseteq \mathcal{E}_\lambda.$$

If there is $k < \dim V$ such that $\ker(T - \lambda I)^k = \ker(T - \lambda I)^{k+1}$, then

$$\ker(T - \lambda I)^k = \ker(T - \lambda I)^{k+1} = \ker(T - \lambda I)^{k+2} = \cdots .$$

(check!) Thus we are done because $\mathcal{E}_\lambda = \bigcup_{k \geq 1} \ker(T - \lambda I)^k = \ker(T - \lambda I)^{\dim V}$. If there no such k, then for $k = 1, 2, \ldots, \dim V$,

$$k \leq \dim \ker(T - \lambda I)^k = \dim \mathcal{E}_\lambda \leq \dim V,$$

so we are also done by taking $k = \dim V$.

(ii) Let $v \in \mathcal{E}_\lambda \setminus \{0\}$. For the sake of contradiction, suppose $v \in \mathcal{E}_\mu$. Since $v \in \mathcal{E}_\lambda$, there is $k \geq 0$ such that $v_k := (T - \lambda I)^k v$ is a λ-eigenvector. On the other hand, there is also $n \geq 0$ such that $(T - \mu I)^n v_k$ is a μ-eigenvector. Then

$$T(T - \mu I)^n v_k = (T - \mu I)^n v_k T v_k = \lambda (T - \mu I)^n v_k,$$

thus $(T-\mu I)^n v_k$ is λ-eigenvector and μ-eigenvector at the same time, a contradiction.

(iii) Let $v \in \mathcal{E}_\lambda$, then of course $(T-\mu I)v \in \mathcal{E}_\lambda$. Hence $\mathcal{E}_\lambda$ is $(T-\mu I)$-invariant. To prove invertibility, it is enough to check injectivity. Let $v \in \mathcal{E}_\lambda$ and $(T-\mu I)v = 0$, then $v \in \mathcal{E}_\mu \implies v \in \mathcal{E}_\lambda \cap \mathcal{E}_\mu = \{0\}$. That means

$$(T-\mu I)|_{\mathcal{E}_\lambda} : \mathcal{E}_\lambda \to \mathcal{E}_\lambda$$

is injective, hence invertible. $\square$

Theorem 4.3.9. *Let V be a finite dimensional complex vector space and $T : V \to V$ linear. The sum of all generalized eigenspaces is a direct sum.*

Proof. Let $\lambda_1, \dots, \lambda_k$ be the eigenvalues of T, let $v_i \in \mathcal{E}_{\lambda_i}$, $i = 1, 2, \dots, k$ be such that

$$v_1 + v_2 + \cdots + v_k = 0, \tag{4.3.10}$$

we need to show $v_1 = v_2 = \cdots = v_k = 0$. To do this, for each $i = 1, 2, \dots, k-1$, choose d_i large such that $(T-\lambda_i I)^{d_i} v_i = 0$, if we apply these operators to (4.3.10),

$$(T-\lambda_1 I)^{d_1}(T-\lambda_2 I)^{d_2} \cdots (T-\lambda_{k-1} I)^{d_{k-1}} v_k = 0.$$

By (iii) of Theorem 4.3.8, $(T-\lambda_i)|_{\mathcal{E}_{\lambda_k}}$ are injective, $i = 1, 2, \dots, k-1$, hence $v_k = 0$. We repeat the process to show $v_{k-1} = v_{k-2} = \cdots = v_1 = 0$. $\square$

Theorem 4.3.11. *Let V be a finite dimensional complex vector space and $T : V \to V$ linear, then V is a direct sum of all generalized eigenspaces of T.*

Proof. Let $\lambda_1, \dots, \lambda_k$ be the distinct eigenvalues of T, we just need to show $V \subseteq \mathcal{E}_{\lambda_1} + \cdots + \mathcal{E}_{\lambda_k}$.

Let $x \in V$, then $p_T(z) = (-1)^{\dim V}(z-\lambda_1)^{d_1} \cdots (z-\lambda_k)^{d_k}$, by Cayley-Hamilton Theorem $p_T(T) = 0$, i.e.,

$$(T-\lambda_1 I)^{d_1}(T-\lambda_2 I)^{d_2} \cdots (T-\lambda_k I)^{d_k} x = 0.$$

This shows that $(T-\lambda_2 I)^{d_2} \cdots (T-\lambda_k I)^{d_k} x \in \mathcal{E}_{\lambda_1}$. By (iii) of Theorem 4.3.8 since each $(T-\lambda_i I)|_{\mathcal{E}_{\lambda_1}} : \mathcal{E}_{\lambda_1} \to \mathcal{E}_{\lambda_1}$ $(i = 2, 3, \dots, k)$ is invertible, there is $w_1 \in E_{\lambda_1}$ such that

$$(T-\lambda_2 I)^{d_2} \cdots (T-\lambda_k I)^{d_k}(x - w_1) = 0.$$

Above means that $(T-\lambda_3 I)^{d_3} \cdots (T-\lambda_k I)^{d_k}(x-w_1) \in \mathcal{E}_{\lambda_2}$, by (iii) of Theorem 4.3.8 again and the same reasoning, there is $w_2 \in \mathcal{E}_{\lambda_2}$ such that

$$(T-\lambda_3 I)^{d_3} \cdots (T-\lambda_k I)^{d_k}(x - w_1 - w_2) = 0.$$

The process can be repeated to obtain $x = w_1 + w_2 + \cdots + w_k$, where $w_i \in \mathcal{E}_{\lambda_i}$. $\square$

4.3.4 Proof of Jordan Canonical Form Theorem

We need the following lemma for the construction of Jordan basis.

Lemma 4.3.12. *Let $V \neq \{0\}$ be a finite dimensional complex vector space and $T : V \to V$ linear. Suppose that $T^m = 0$ for some $m \geq 1$ (i.e., T is nilpotent), then there is a basis of V of the form*

$$u_1, Tu_1, \dots T^{a_1-1}u_1, \dots, u_k, Tu_k, \dots, T^{a_k-1}u_k,$$

where $T^{a_i}u_i = 0$ for $1 \leq i \leq k$.

Here we don't exclude the possibility that that $T = 0$, but then necessarily $a_1 = a_2 = \cdots = a_k = 1$.

Proof. We prove by induction on the dimension. Suppose $\dim V = 1$, then we are done. Suppose $\dim V = k$ and every vector spaces of dimension less than k with a nilpotent operator on it has a basis of the form described in the theorem. Note that $T(V) \subsetneq V$, otherwise

$$V = T(V) = T^2(V) = \cdots = T^m(V) = \{0\},$$

a contradiction. As $T(V)$ is T-invariant, i.e., $T|_{T(V)} \in \mathcal{L}(T(V))$, and T is nilpotent, by induction hypothesis $T(V)$ has a basis

$$v_1, Tv_1, \dots, T^{b_1-1}v_1, \dots, v_k, Tv_k, \dots, T^{b_k-1}v_k,$$

where $T^{b_i}v_i = 0$. Since $v_i \in T(V)$, we choose $u_i \in V$ such that $Tu_i = v_i$. Now $\{T^{b_i-1}v_i : i = 1, 2, \dots, k\} \subseteq \ker T$ is linearly independent, we extend this to a basis of $\ker T$:

$$\{T^{b_1-1}v_1, \dots, T^{b_k-1}v_k, w_1, w_2, \dots, w_l\}.$$

We claim that

$$u_1, Tu_1, \dots, T^{b_1}u_1, \dots, u_k, Tu_k, \dots, T^{b_k}u_k, w_1, w_2, \dots, w_l$$

form a basis of V.

The linear independence is left as a routine checking. To prove it does span V, we try to compare the dimension of V and the number of the vectors. We note that $\dim\ker T = k + l$. Also, $\dim T(V) = b_1 + b_2 + \cdots + b_k$. Hence

$$\begin{aligned}
\dim V &= \dim\ker T + \dim T(V)\\
&= (k + l) + (b_1 + \cdots + b_k)\\
&= (b_1 + 1) + \cdots + (b_k + 1) + l
\end{aligned}$$

□

Proof of Jordan Canonical Form Theorem 4.3.3. In the hypothesis V is a finite dimensional complex vector space and $T : V \to V$ is linear, Theorem 4.3.11 asserts that

$$V = \mathcal{E}_{\lambda_1} \oplus \mathcal{E}_{\lambda_2} \oplus \cdots \oplus \mathcal{E}_{\lambda_k},$$

where λ_i are eigenvalues of T. Hence $N_i := (T - \lambda_i I)|_{\mathcal{E}_{\lambda_i}}$ is nilpotent(‡), and the result follows by applying Lemma 4.3.12 to $N_1, N_2, \dots, N_k$ and noting that

$$T = (N_1 + \lambda_1 I) \oplus \cdots \oplus (N_k + \lambda_k I) : \mathcal{E}_{\lambda_1} \oplus \cdots \oplus \mathcal{E}_{\lambda_k} \to \mathcal{E}_{\lambda_1} \oplus \cdots \oplus \mathcal{E}_{\lambda_k}.$$

(‡) It is because $\mathcal{E}_{\lambda_i} = \ker(T - \lambda_i I)^{\dim V} = \ker((T - \lambda_i I)|_{\mathcal{E}_{\lambda_i}})^{\dim V}$, thus $(T - \lambda_i I)|_{\mathcal{E}_{\lambda_i}} : \mathcal{E}_{\lambda_i} \to \mathcal{E}_{\lambda_i}$ is nilpotent.

Specifically, $\{u_1, \ldots, N_1^{a_1-1}u_1, \ldots, u_l, \ldots, N_1^{a_l-1}u_l\}$ be a basis of $\mathcal{E}_{\lambda_1}$, where $N_1^{a_i}u_i = 0$. Let's order the basis in the reverse way:

$$\mathcal{B}_1 := \{N_1^{a_1-1}u_1, N_1^{a_1-2}u_1, \ldots, u_1, \quad \ldots \quad , N_1^{a_l-1}u_l, N_1^{a_l-2}u_l, \ldots, u_l\}. \tag{4.3.13}$$

If $a_1 = 1$, then u_1 is in fact an eigenvector. Let's suppose $a_1 \geq 2$, then

$$\begin{aligned}
T(N_1^{a_1-1}u_1) &= \lambda_1 N_1^{a_1-1}u_1 \\
T(N_1^{a_1-2}u_1) &= N_1^{a_1-1}u_1 + \lambda_1 N_1^{a_1-2}u_1 \\
T(N_1^{a_1-3}u_1) &= N_1^{a_1-2}u_1 + \lambda_1 N_1^{a_1-3}u_1 \\
&\vdots \\
T(u_1) &= N_1 u_1 + \lambda_1 u_1,
\end{aligned}$$

the matrix of T w.r.t. first a_1 vectors of $\mathcal{B}_1$ is of the form

$$\begin{bmatrix} \lambda_1 & 1 & & & \\ & \lambda_1 & 1 & & \\ & & \lambda_1 & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda_1 \end{bmatrix}.$$

Where the entries are all zero elsewhere. Continuing this process to the rest of vectors in $\mathcal{B}_1$, we see that $[T]_{\mathcal{B}_1}$ is a Jordan form. Now for $i = 2, 3, \ldots, k$, let $\mathcal{B}_i$ be the corresponding basis of $\mathcal{E}_i$ ordered reversely as above, then let

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_k,$$

then $[T]_{\mathcal{B}} = \bigoplus_{i=1}^{k}[T]_{\mathcal{B}_i}$ is a Jordan form. □

The proof also reveals that Jordan basis exists in the following specific form:

Definition 4.3.14. Let V be a vector space, $T : V \to V$ linear and let $v \in V$ be a generalized eigenvector of T with eigenvalue λ. Suppose p is a positive integer such that $T^p v = 0$ but $T^{p-1}v \neq 0$, then the ordered set

$$\{(T - \lambda I)^{p-1}v, (T - \lambda I)^{p-2}v, \ldots, v\}$$

is called a **cycle of generalized eigenvectors** of T with eigenvalue λ. We say that the **length** of the cycle is p.

In the proof of Jordan canonical form theorem, $\mathcal{B}_1$ written in (4.3.13) is a union of l disjoint cycles. In general, if a linear maps $T : V \to V$ with $\dim V < \infty$ has k eigenvalues, say $\lambda_1, \lambda_2, \ldots, \lambda_k$, then the basis $\mathcal{B}_i$ of $\mathcal{E}_{\lambda_i}$, due to Lemma 4.3.12 applied to $(T - \lambda_i)|_{\mathcal{E}_{\lambda_i}}$, will consist of $l_i \geq 1$ disjoint cycles of generalized eigenvectors of T with eigenvalue λ_i. The collection of all such cycles forms a Jordan basis of T.

Lastly we also mention the dimension of each generalized eigenspace.

Theorem 4.3.15 (Dimension of $\mathcal{E}_\lambda$). *Let V be finite dimensional and $T : V \to V$ linear. If $\lambda_1, \ldots, \lambda_k$ are eigenvalues of V and $p_T(z) = (-1)^{\dim V}(z - \lambda_1)^{d_1}(z - \lambda_2)^{d_2} \cdots (z - \lambda_k)^{d_k}$, then*

$$\dim \mathcal{E}_{\lambda_i} = d_i.$$

Proof. Let $U_i = T|_{\mathcal{E}_{\lambda_i}}$, by (iii) of Theorem 4.3.8, λ_i is the only eigenvalue of U_i, it follows that $p_{U_i}(z) = (-1)^{\dim U_i}(z - \lambda_i)^{\dim \mathcal{E}_{\lambda_i}}$. Let $\mathcal{B}$ be a basis of $\mathcal{E}_{\lambda_i}$, extend it to a basis $\mathcal{B} \cup \mathcal{B}'$ for V, then

$$[T]_{\mathcal{B}\cup\mathcal{B}'} = \begin{bmatrix} [T]_{\mathcal{B}} & * \\ 0 & * \end{bmatrix},$$

hence $p_T(z) = p_{U_i}(z)g(z)$, for some polynomial g, i.e., p_{U_i} divides p_T, hence

$$\dim \mathcal{E}_{\lambda_i} \le d_i. \tag{4.3.16}$$

On the other hand,

$$\dim V = \dim\left(\bigoplus_{i=1}^{n} \mathcal{E}_{\lambda_i}\right) = \sum_{i=1}^{k} \dim \mathcal{E}_{\lambda_i} \le \sum_{i=1}^{k} d_i = \dim V,$$

hence none of the inequality in (4.3.16) can be strict, thus $\dim \mathcal{E}_{\lambda_i} = d_i$. $\square$

4.3.5 Dot Diagram

Throughout section 4.3.5 we **fix** a linear map $T : V \to V$, where V is a finite dimensional complex vector space. Also, we **fix** a choice of eigenvalue λ of T and consider a **fixed** eigenspace $\mathcal{E}_\lambda$. Since $(T - \lambda I)|_{\mathcal{E}_\lambda}$ is nilpotent, by theorem Lemma 4.3.12, $\mathcal{E}_\lambda$ has a (Jordan) basis consisting of $l \ge 1$ disjoint cycles. We align each cycle as a column and arrange them as in the way of the following dot diagram.

Dot Diagram of $\mathcal{E}_\lambda$

$$\begin{array}{llll}
\bullet\ (T-\lambda I)^{p_1-1}v_1 & \bullet\ (T-\lambda I)^{p_2-1}v_2 & & \bullet\ (T-\lambda I)^{p_l-1}v_l \\
\bullet\ (T-\lambda I)^{p_1-2}v_1 & \bullet\ (T-\lambda I)^{p_2-2}v_2 & \cdots & \qquad\vdots \\
\qquad\vdots & \qquad\vdots & & \bullet\ v_l \\
\bullet\ (T-\lambda I)v_1 & \bullet\ v_2 & & \\
\bullet\ v_1 & & &
\end{array}$$

As before, each $p_i \ge 1$ and $(T - \lambda I)^{p_i} v_i = 0$. Each dot above denotes an element in the Jordan basis of $\mathcal{E}_\lambda$. Moreover, as indicated in the diagram, from now on we will also require

$$p_1 \ge p_2 \ge \cdots \ge p_l,$$

thus the size of Jordan blocks will be in descending order and in this way the Jordan form representation can be **unique**. We denote by $\mathcal{B}_\lambda$ the set of dots (Jordan basis in $\mathcal{E}_\lambda$) above. Later, as in Example 4.3.19, it will be found more convenient to write the dots alone when determing the Jordan form of A without find the Jordan basis.

In Theorem 4.3.17 and Theorem 4.3.18 we will learn how to *compute* the number of dots in each row in the dot diagram, thereby identifying the Jordan form that a matrix has!

Theorem 4.3.17. *For each integer $r \ge 1$, $\dim\ker(T - \lambda I)^r$ is the number of dots in the first r rows indicated in the dot diagram.*

Proof. We observe that $\ker(T - \lambda I)^r \subseteq \mathcal{E}_\lambda$ and we let $N = (T - \lambda I)^r|_{\mathcal{E}_\lambda}$. It is obvious that range $N \subseteq \mathcal{E}_\lambda$ and hence $\ker N = \ker(T - \lambda I)^r$. Let

$$S_1 = \{x \in \mathcal{B}_\lambda : Nx = 0\} \quad \text{and} \quad S_2 = \{x \in \mathcal{B}_\lambda : Nx \ne 0\}.$$

Now S_1 **consists of precisely first r rows of vectors in the diagram**. Let $a = |S_1|$ and $b = |S_2|$, then $a + b = \dim \mathcal{E}_\lambda$, moreover,

$$\operatorname{range} N = \operatorname{span}\{Nx : x \in S_2\}.$$

Since the effect of apply N to $x \in S_2$ is precisely shifting the dot x up by r dots, hence $|\{Nx : x \in S_2\}| = |S_2|$ and thus $\dim \operatorname{range} N = b$. By rank-nullity theorem,

$$\dim \ker N = \dim \mathcal{E}_\lambda - b = a,$$

hence S_1 is a basis of $\ker N = \ker(T - \lambda I)^r$, thus

$$\dim \ker(T - \lambda I)^r = |S_1|. \qquad \square$$

In the next theorem, let's for simplicity write $\operatorname{rank} T$ to mean $\dim \operatorname{range} T$. A direct application of Theorem 4.3.17 yields the calculation of dots in each row:

Theorem 4.3.18. *Denote r_i the number of dots in the ith rows of the dot diagram, then*

$$r_1 = \dim V - \operatorname{rank}(T - \lambda I)$$

and for $i > 1$,

$$r_i = \operatorname{rank}(T - \lambda I)^{i-1} - \operatorname{rank}(T - \lambda I)^i.$$

Proof. Applying $r = 1$ in Theorem 4.3.17, we have

$$r_1 = \dim \ker(T - \lambda I) = \dim V - \operatorname{rank}(T - \lambda I).$$

Next by Theorem 4.3.17 the number r_i is nothing but the number of dots in the first i rows subtract the number of dots in first $i - 1$ rows, thus we have

$$\begin{aligned} r_i &= \dim \ker(T - \lambda I)^i - \dim \ker(T - \lambda I)^{i-1} \\ &= \cancel{\dim V} - \operatorname{rank}(T - \lambda I)^i - (\cancel{\dim V} - \operatorname{rank}(T - \lambda I)^{i-1}) \\ &= \operatorname{rank}(T - \lambda I)^{i-1} - \operatorname{rank}(T - \lambda I)^i. \end{aligned} \qquad \square$$

4.3.6 Examples

In this section we provide one example on the computation of Jordan form and Jordan basis. Also we provide an example which is a well-known result in numerical analysis, in the solution two proofs will be presented (one is due to me). It gives you a taste how a problem can be simplified by studying its simplification.

Computational Example

Example 4.3.19. We try to find the Jordan form and also the Jordan basis of the matrix

$$A = \begin{bmatrix} 2 & -1 & 0 & 1 \\ 0 & 3 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 3 \end{bmatrix}.$$

In general the easiest step is to find the Jordan form, thus it is usually first step. The situation is similar to diagonalizable.

Since

$$\det(A - tI) = (t-2)^3(t-3),$$

The algebraic multiplicity of 2 is three, and that of 3 is one. Therefore by Theorem 4.3.15,

$$\dim \mathcal{E}_2 = 3 \quad \text{and} \quad \dim \mathcal{E}_3 = 1.$$

The generalized eigenspace $\mathcal{E}_3$ is well understood. Next we focus on $\mathcal{E}_2$ and consider its dot diagram in order to determine the Jordan form.

By Theorem 4.3.18, $r_1 = \dim \mathbb{R}^4 - \text{rank}(A - 2I)$, but

$$A - 2I = \begin{bmatrix} 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

hence we have $r_1 = 4 - 2 = 2$. As the dot diagram of $\mathcal{E}_2$ can only have 3 dots, we know that $r_2 = 1$. So we get

$$\begin{matrix} \bullet & \bullet \\ \bullet & \end{matrix}$$

Recall that each column represents a cycle (defined in Definition 4.3.14), therefore the Jordan form of A, with eigenvalues listed in ascending order, is

$$J = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}.$$

Next finding a Jordan basis is little more tedious, we need to be patient.

The Jordan basis in $\mathcal{E}_3$. It is easy to find, let $x \in \text{Nul}(A - 3I)$, then

$$A - 3I = \begin{bmatrix} -1 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Therefore we have $x_2 = x_3 = 0$ and $x_1 = -x_2 + x_4 = x_4$, hence $x = x_4(1,0,0,1)^T$, thus $\boxed{(1,0,0,1)^T}$ is what we want.

The Jordan basis in $\mathcal{E}_2$. The first row of the dot diagram consists of vectors in $\text{Nul}(A - 2I)$, while the second row consists of vectors in $\text{Nul}(A - 2I)^2$. So our strategy is, firstly, we try to find $v \in \text{Nul}(A - 2I)^2$ such that $(A - 2I)v \neq 0$, then the first column of the dot diagram of $\mathcal{E}_2$ is determined by v and $(A - 2I)v$. Next we find $u \in \text{Nul}(A - 2I) \setminus \text{span}\{(A - 2I)v\}$, then the second column is also determined.

Since

$$(A - 2I)^2 = \begin{bmatrix} 0 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 1 \end{bmatrix} \to \begin{bmatrix} 0 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

this shows us if $(A-2I)^2x=0$, then $x_2=\frac{1}{2}x_3+\frac{1}{2}x_4$. And hence $x=x_1(1,0,0,0)^T+x_3(0,\frac{1}{2},1,0)^T+x_4(0,\frac{1}{2},0,1)^T$, thus

$$\text{Nul}(A-2I)^2=\text{span}\left\{\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\2\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\\2\end{bmatrix}\right\}.$$

Note that $A-2I=\left[\begin{smallmatrix}0&-1&0&1\\0&1&-1&0\\0&1&-1&0\\0&-1&0&1\end{smallmatrix}\right]$, $(A-2I)(1,0,0,0)^T=0$, $(1,0,0,0)^T$ is not a suitable choice. Choose $v=(0,1,2,0)^T$, we find that $(A-2I)v=(-1,-1,-1,-1)^T\neq 0$. And then choose $u=(1,0,0,0)^T\in\text{Nul}(A-2I)$, then

$$\left\{\begin{bmatrix}-1\\-1\\-1\\-1\end{bmatrix},\begin{bmatrix}0\\1\\2\\0\end{bmatrix},\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\right\}$$

is the Jordan basis of A.

Remark. Although the eigenvalues in Example 4.3.19 are all real, don't forget our theory bases on the existence of at least one eigenvalue. Thus sometimes we get at least one complex eigenvalue, it is nothing wrong and don't hesitate to repeat what we have done here.

Theoretical Example

For the upcoming example we define the following:

Definition 4.3.20. Let $A\in M_{n\times n}(\mathbb{R})$. Denote $\sigma(A)$ the **spectrum** of A to be the collection of all eigenvalues,

$$\sigma(A):=\{\text{root of }\det(A-xI)\}\subseteq\mathbb{C}.$$

The **spectral radius**, is defined by

$$r(A):=\max\{|\lambda|:\lambda\in\sigma(A)\}.$$

Here $r(A)$ can always be defined as a matrix can just have finitely many eigenvalues.

Note that when $Ax=\lambda x$ and $|\lambda|<1$, then $A^kx\to 0$ as $k\to\infty$. So we can control the image A^kx if x is an eigenvector. Interestingly if the largest possible eigenvalue is small enough in magnitude, then we can control the image of A^k:

Example 4.3.21. Let A be an $n\times n$ matrix, we try to show that

$$\lim_{n\to\infty}A^nx=0,\quad\text{for all }x\in\mathbb{R}^n\iff r(A)<1.$$

For simplicity let's write $\lim_{n\to\infty}A^n=0$ to mean $\lim_{n\to\infty}A^nx=0$ for all $x\in\mathbb{R}^n$. We first finish the $(\Rightarrow)$ direction, although it is not of our main interest.

$(\Rightarrow)$. Let $\lambda\in\sigma(A)$ such that $|\lambda|=r(A)$. Since λ is an eigenvalue, $Ax=\lambda x$ for some $x\neq 0$. By hypothesis we have $\lim_{n\to\infty}A^nx=\lambda^nx=0$, hence there is an n_0 such that

$$\|\lambda^{n_0}x\|<\|x\|\implies|\lambda|<1.$$

Solution 1 of ($\Leftarrow$). By Theorem 4.3.1 we can upper-triangularize A by some invertible $P \in M_{n\times n}(\mathbb{C})$, i.e.,

$$U := P^{-1}AP = \begin{bmatrix} \lambda_1 & b_{12} & \cdots & b_{1n} \\ 0 & \lambda_2 & \cdots & b_{2n} \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix},$$

then $Ue_1 = \lambda_1 e_1$, and $U^j e_1 = \lambda_1^j e_1$ and hence $|\lambda_1| < 1 \implies U^k e_1 \to 0$. We complete the proof by induction, assume there is $k \in \mathbb{N}$ so that

$$\lim_{j\to\infty} U^j e_1, \dots, \lim_{j\to\infty} U^j e_{k-1} = 0.$$

We will show that $U^j e_k \to 0$.

Since $Ue_k = \sum_{i=1}^{k-1} b_{ik} e_i + \lambda_k e_k$, we apply U^j on both sides to get $U^{j+1}e_k = \sum_{i=1}^{k-1} b_{ik} U^j e_i + \lambda_k U^j e_k$, and hence

$$\|U^{j+1}e_k\| \le \sum_{i=1}^{k-1} |b_{ik}| \|U^j e_i\| + |\lambda_k| \|U^j e_k\|.$$

By induction hypothesis $\lim_{j\to\infty} U^j e_i = 0$ for $i = 1, 2, \dots, k-1$, so for every $\epsilon > 0$ there is an N such that

$$n \ge N \implies \|U^{j+1}e_k\| < \epsilon + |\lambda_k| \|U^j e_k\|. \tag{4.3.22}$$

For the sake of simplicity let's denote $\lambda = |\lambda_k|$ and $a_j = \|U^j e_k\|$, then (4.3.22) becomes

$$n \ge N \implies a_{j+1} < \epsilon + \lambda a_j,$$

where $0 < \lambda < 1$. A standard technique in elementary analysis shows us

$$\lim_{j\to\infty} a_j = \lim_{j\to\infty} \|U^j e_k\| = 0.$$

We conclude by induction that $\lim_{j\to\infty} U^j e_k = 0$, therefore $U^j \to 0$. Since $A^j = PU^jP^{-1}$, we conclude $A^j \to 0$ on $\mathbb{C}^n$, and of course, on $\mathbb{R}^n \subseteq \mathbb{C}^n$.

Remark. The first proof above is elementary in the sense that only the upper triangularization is needed which is an easy consequence of existence of at least one complex eigenvalue. The second proof below will be a standard proof to this result.

Solution 2 of ($\Leftarrow$). Let $\lambda_1, \lambda_2, \dots, \lambda_k$ be the eigenvalues of A. By Theorem 4.3.3 there is an invertible matrix $P \in M_{n\times n}(\mathbb{C})$ such that

$$J := P^{-1}AP = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_k \end{bmatrix},$$

where J_i is the Jordan form of L_A w.r.t. the cycles in $\mathcal{E}_{\lambda_i}$. Namely, there is a nilpotent matrix N_i such that $J_i = \lambda_i I + N_i$, where $N_i^{d_i} = 0$, $d_i = \dim \mathcal{E}_{\lambda_i}$. Note that by diagonal block multiplication,

$$J^m = \begin{bmatrix} J_1^m & & & \\ & J_2^m & & \\ & & \ddots & \\ & & & J_k^m \end{bmatrix},$$

to finish the proof it is enough to show that $J_i^m \to 0$ for each i. Indeed, since $J_i = \lambda_i I_{d_i} + N_i$, we have for large $m > d_1, d_2, \ldots, d_k$,

$$J_i^m = (\lambda_i I_{d_i} + N_i)^m = \sum_{r=0}^{m} \binom{m}{r} \lambda_i^{m-r} N_i^r = \sum_{r=0}^{d_i-1} \binom{m}{r} \lambda_i^{m-r} N_i^r.$$

For each r, since $\binom{m}{r}$ is just a product of r linear factors in m, we have $\binom{m}{r}\lambda_i^{m-r} \to 0$ when $m \to \infty$, therefore $J_i^m \to 0$, and we are done.

4.4 Exercises

Eigenvalues, Eigenvectors and Diagonalization

Problem 4.1. Let $A \in M_{n\times n}(\mathbb{R})$, show that there is $\delta > 0$ such that for every $t \in (0, \delta)$, $A - tI$ is invertible.

Problem 4.2. If A is diagonalizable, show that each of the following is also diagonalizable.

(i) $A^n, n \geq 1$.

(ii) $kA, k \in \mathbb{R}$.

(iii) $p(A)$, $p(x)$ is any polynomial.

(iv) $U^{-1}AU$, U is any invertible matrix.

Problem 4.3. Show that for $A \in M_{2\times 2}(\mathbb{R})$, we have

$$\det(A - \lambda I) = \lambda^2 - (\operatorname{Tr} A)\lambda + \det A,$$

hence show that

$$(\operatorname{Tr} A)^2 > 4 \det A$$

is a sufficient condition for A to be diagonalizable.

Problem 4.4. Let $A \in M_{n\times n}(\mathbb{R})$.

(i) Show that if λ is an eigenvalue of A, then λ^k is an eigenvalue of A^k.

(ii) Show that every eigenvalue of A is also an eigenvalue of A^T. Give an example that A and A^T have different eigenvectors.

Problem 4.5. Suppose $A \in M_{n\times n}(\mathbb{R})$ and that the sum of each row equals 1, show that 1 is an eigenvalue.

Problem 4.6. Let A be diagonalizable, show that $\det A$ is the product of all eigenvalues.

Problem 4.7. Construct a matrix that has no real eigenvalue.

Problem 4.8. Let $A \in M_{n\times n}(\mathbb{R})$, show that for any $\epsilon > 0$, there is t with $0 < |t| < \epsilon$ such that $A - tI$ is invertible.

Problem 4.9. Show that any rank one matrix $A \in M_{n\times n}(\mathbb{R})$ is of the form ab^T for some $a, b \in \mathbb{R}^n$. From this, prove that every rank one symmetric real matrix is diagonalizable.

Problem 4.10. Let $A \in M_{n\times n}(\mathbb{R})$, if $\operatorname{rank} A = k$, show that A has at most $k+1$ distinct eigenvalues. Give an example of rank k $n \times n$ matrix with $k+1$ distinct eigenvalues.

Problem 4.11. Let $A \in M_{m\times n}(\mathbb{R})$ and $B \in M_{n\times m}(\mathbb{R})$. Also we let I_n and I_m be $n \times n$ and $m \times m$ identity matrices respectively. Prove that

$$\det(I_m + AB) = \det(I_n + BA).$$

Problem 4.12. Let V be a finite dimensional real vector space and $T : V \to V$ linear. Suppose every nonzero vector in V is an eigenvector of T, show that then $T = kI$ for some $k \in \mathbb{R}$.

Hint. For each $v \in V$, let $g(v)$ denote the eigenvalue of v (we say "the" because each eigenvector cannot have two eigenvalues!). i.e., for each $v \in V \setminus \{0\}$, $Tv = g(v)v$. Show that g must be constant.

Problem 4.13. Let $T \in \mathcal{L}(V, V)$, show that for every pair of bases α, β of a finite dimensional vector space V, we have

$$\det\big([T]_\alpha\big) = \det\big([T]_\beta\big) \quad \text{and} \quad \det\big([T]_\alpha - tI\big) = \det\big([T]_\beta - tI\big).$$

Problem 4.14. Let

$$A = \begin{bmatrix} 1 & 2 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ \vdots & \vdots & \ddots & \vdots \\ n^2-n+1 & n^2-n+2 & \cdots & n^2 \end{bmatrix}.$$

Prove that the characteristic polynomial p_A of A is

$$p_A(x) = (-1)^n \left(x^n - \frac{n(n^2+1)}{2} x^{n-1} - \frac{n^3(n^2-1)}{12} x^{n-2} \right).$$

Hint. Show that $\operatorname{rank} A = 2$ and that $W := \operatorname{span}\{(1, 1, \ldots, 1)^T, (1, n+1, \ldots, n^2-n+1)^T\}$ is an invariant subspace of L_A, i.e., $Aw \in W$ for all $w \in W$.

Problem 4.15. Define $T \in \mathcal{L}(\mathbb{R}^3, \mathbb{R}^3)$ by

$$T(x_1, x_2, x_3) = (2x_2, 0, 5x_3),$$

find all eigenvalues and eigenvectors of T.

Problem 4.16. Consider the linear transformation

$$T : \mathbb{P} \to \mathbb{P}; \quad Tf(x) = xf'(x),$$

where $\mathbb{P}$ denotes the set of all polynomials.

(a) Find $\ker T$.

(b) Find a $p \in \mathbb{P} \setminus \operatorname{range} T$.

(c) Find all eigenvectors and eigenvalues of T.

Problem 4.17. Let V be finite dimensional, for a linear $T : V \to V$ we define its *trace* to be

$$\operatorname{Tr}(T) = \operatorname{Tr}[T]_\alpha$$

for any fixed basis α of V. It can be shown that the value $\operatorname{Tr}(T)$ is independent of the choices of basis, i.e., for any two bases α, β of V, $\operatorname{Tr}[T]_\alpha = \operatorname{Tr}[T]_\beta$ (cf. Problem 4.13).

Now for an $A \in M_{n\times n}(\mathbb{R})$, we define $L_A : M_{n\times n}(\mathbb{R}) \to M_{n\times n}(\mathbb{R})$ by

$$L_A(X) = AXA^T,$$

where $\cdot^T$ denotes the transpose of a matrix. Show that

$$\operatorname{Tr}(L_A) = (\operatorname{Tr} A)^2 \quad \text{and} \quad \det(L_A) = (\det A)^{2n}.$$

Singular Value Decomposition

Problem 4.18. Using SVD, prove that any matrix in $M_{m\times n}(\mathbb{C})$ is the limit of a sequence of full-rank matrices. Or in terms of analysis, prove that the set of full rank matrices is a dense subset of $M_{m\times n}(\mathbb{C})$.

Problem 4.19. By considering the SVD of $A \in M_{m\times n}(\mathbb{R})$, say $A = U\Sigma V^*$, find an eigenvalue decomposition of the $2m \times 2m$ symmetric matrix

$$\begin{bmatrix} O & A^T \\ A & O \end{bmatrix},$$

where O denotes a zero matrix.

Jordan Canonical Form

Problem 4.20. For each of the matrices A that follow, find a Jordan form J and an invertible matrix Q such that $J = Q^{-1}AQ$.

(a) $A = \begin{bmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{bmatrix}$

(b) $A = \begin{bmatrix} 0 & 1 & -1 \\ -4 & 4 & -2 \\ -2 & 1 & 1 \end{bmatrix}$

(c) $A = \begin{bmatrix} 0 & -1 & -1 \\ -3 & -1 & -2 \\ 7 & 5 & 6 \end{bmatrix}$

(d) $A = \begin{bmatrix} 0 & -3 & 1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & -3 & 1 & 4 \end{bmatrix}$

Problem 4.21. Let A be an $n \times n$ complex matrix. Prove that A and A^T have the same Jordan canonical form, and concldue that A and A^T are similar.

Hint. Use Theorem 4.3.18 and the fact that row rank = column rank.

Problem 4.22. Let $A \in M_{2\times 2}(\mathbb{R})$. Define

$$\sin A = A - \frac{A^3}{3!} + \frac{A^5}{5!} - \cdots .$$

RHS converges in the sense that each entry converges to a number. Determine whether it is possible that

$$\sin A = \begin{bmatrix} 1 & 2013 \\ 0 & 1 \end{bmatrix}.$$

Problem 4.23. Let $A \in M_{n\times n}(\mathbb{F})$ and $\operatorname{rank} A = r$. Suppose that

$$\operatorname{Tr}(A) = \operatorname{Tr}(A^2) = \cdots = \operatorname{Tr}(A^r) = 0,$$

prove that $A^{r+1} = 0$.

Chapter 5

Inner Product Spaces

Throughout the chapter we will follow the convention that:

$$\boxed{\mathbb{F} \text{ denotes } \mathbb{R} \text{ or } \mathbb{C}}$$

Instead of just being a vector space, we will impose one more structure on it such that many geometrically intuitive concept can be generalized to abstract spaces. We will also introduce the concept of orthogonal projection using orthogonal basis of a finite dimensional vector spaces to solve certain best approximation problem.

5.1 Inner Product

Definition 5.1.1. Let V be a a vector space over $\mathbb{F}$, an **inner product** on V is a function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ satisfying:

Linear in The First Variable
For every $\alpha \in \mathbb{F}$ and $u, v, w \in V$, $\langle u + \alpha w, v \rangle = \langle u, v \rangle + \alpha \langle w, v \rangle$.

Conjugate Linear in The Second Variable
For every $\alpha \in \mathbb{F}$ and $u, v, w \in V$, $\langle u, v + \alpha w \rangle = \langle u, v \rangle + \overline{\alpha} \langle u, w \rangle$.

Conjugate Symmetric
For every $u, v \in V$, $\langle u, v \rangle = \overline{\langle v, u \rangle}$.

Positive Definite
For every $v \in V$, $\langle v, v \rangle \geq 0$, and $\langle v, v \rangle = 0 \implies v = 0$.

When $\mathbb{F} = \mathbb{R}$, the linearity in the first variable and the conjugate linearity in the second variable are combined to called bilinearity. As a rule, whenever we mention a vector space that is not closed under complex scalar multiplication, every label $\mathbb{F}$ in our results and definitions should be replaced by $\mathbb{R}$ before we apply them.

Example 5.1.2 (Some Inner Products).

(i) For $u, v \in \mathbb{R}^n$, the **standard inner product** (also called **dot product**) on $\mathbb{R}^n$ is defined by

$$\langle u, v \rangle := u \cdot v = \sum_{i=1}^{n} u_i v_i.$$

(ii) For $u, v \in \mathbb{C}^n$, the **standard inner product** on $\mathbb{C}^n$, is defined by

$$\langle u, v\rangle := v^* u = \sum_{i=1}^{n} u_i \overline{v_i}.$$

(iii) We can define an inner product on $C([-1,1],\mathbb{F})$ by

$$\langle f, g\rangle = \int_{-1}^{1} f\overline{g}\, dx,$$

which is positive definite as $\langle f, f\rangle \geq 0$ and $\langle f, f\rangle = \int_{-1}^{1} f^2 dx = 0 \implies f = 0$ on $[-1,1]$.

(iv) On $\mathbb{R}^n$, every matrix $A \in M_{n\times n}(\mathbb{R})$ gives a bilinear functional

$$B(x, y) = x^T A y.$$

For it to be symmetric, we must require A be symmetric(*). For a nontrivial example that makes B into an inner product, let $n = 2$, set $A = \left[\begin{smallmatrix} 2 & -1 \\ -1 & 2 \end{smallmatrix}\right]$, then $B(x, y) = x^T A y = 2x_1y_1 - x_1y_2 - x_2y_1 + 2x_2y_2$ is bilinear and symmetric, moreover,

$$x \neq 0 \implies B(x, x) = (x_1 - x_2)^2 + x_1^2 + x_2^2 > 0.$$

(v) On $\mathbb{P}_2(\mathbb{R})$ the following define an inner product: for $p, q \in \mathbb{P}_2(\mathbb{R})$,

$$\langle p, q\rangle = p(-1)q(-1) + p(0)q(0) + p(1)q(1).$$

Note, however, that this does not define an inner product on $\mathbb{P}_3(\mathbb{R})$.

In fact there is a class of matrices that share the same feature with part (iv) of Example 5.1.2. We name this class of matrices in the following definition.

Definition 5.1.3. A matrix $A \in M_{n\times n}(\mathbb{R})$ is said to be **positive definite** if it satisfies the following two properties:

(i) A is symmetric.

(ii) $\langle Ax, x\rangle = \langle x, Ax\rangle = x^T Ax > 0$ for every $x \in \mathbb{R}^n \setminus \{0\}$.

Later in Theorem 5.7.2 we will learn a systematic way to determine a matrix is positive define or not.

Remark. These matrices will be found very useful in applications, for example, the second derivative test for multivariable calculus, the maximum principle for solutions of Partial Differential Equations with (uniform) ellipticity condition, the Lyapunov stability for linear systems of ordinary differential equations, etc.

Remark. In terms of dot product we have the following nice formula:

$$\langle Ax, y\rangle = \langle x, A^T y\rangle, \quad \langle A^T x, y\rangle = \langle x, Ay\rangle.$$

If $A \in M_{n\times n}(\mathbb{R})$ is positive definite, then $\langle x, y\rangle := x^T Ay$ defines an inner product on $\mathbb{R}^n$.

(*) This follows from the fact that $B(e_i, e_j) = B(e_j, e_i)$.

Several remarks concerning inner products are in order:

- By bilinearity, we can prove that $\langle 0, v\rangle = \langle v, 0\rangle = 0$.
- When $\mathbb{F} = \mathbb{R}$, suppose $\langle\cdot,\cdot\rangle$ is proved to be symmetric, then $\langle\cdot,\cdot\rangle$ is bilinear iff it is linear in one of the variables. When $\mathbb{F} = \mathbb{C}$, the conjugate linearity can be implied by linearity of the first variable and conjugate symmetricity.
- Usually we adopt other brackets to denote inner products when there are more than one in a vector space. Among the usual ones are $[x, y], (x, y), \langle x, y\rangle$, etc.
- Actually the matrix A in (iii) of Example 5.1.2 can be written as $A = P^T P$, where P is an invertible matrix given by

$$\frac{1}{4}\begin{bmatrix} -\sqrt{2}+\sqrt{6} & -\sqrt{2}-\sqrt{6} \\ \sqrt{2}+\sqrt{6} & \sqrt{2}-\sqrt{6} \end{bmatrix},$$

hence

$$(x, y) := x^T A y = x^T P^T P y = (Px)^T P y = \langle Px, Py\rangle, \tag{5.1.4}$$

where $\langle\cdot,\cdot\rangle$ denotes the dot product on $\mathbb{R}^n$. It follows that the bilinear functional $(x, y) := x^T A y$ is positive definite.

This is not a coincidence, Problem 5.6 provides us a complete characterization of **ALL** possible inner products on $\mathbb{R}^n$, each of them takes the same form as (5.1.4).

In this chapter we mainly study the following class of vector spaces.

Definition 5.1.5. A vector space over $\mathbb{F}$ endowed with an inner product is called an **inner product space**.

Example 5.1.6. $\mathbb{R}^n$ itself is a vector space, we give it a dot product to turn it into an inner product space.

Example 5.1.7. $C([0, 1], \mathbb{F})$ itself is a vector space, we give it an inner product

$$\langle f, g\rangle = \int_0^1 f(x)\overline{g(x)}\, dx$$

for every $f, g \in C([0, 1], \mathbb{F})$ to turn $C([0, 1], \mathbb{F})$ into an inner product space.

The way to turn a vector space into an inner product space is not unique. For every continuous function $w : [0, 1] \to (0, \infty)$ the inner product

$$(f, g) = \int_0^1 f(x)\overline{g(x)}w(x)\, dx$$

also turns $C[0, 1]$ into an inner product space.

Now we introduce a standard notation which helps us to distinguish different inner product spaces.

Convention. We always use the notation $(V, \langle\cdot,\cdot\rangle)$ to mean V is a vector space with inner product $\langle\cdot,\cdot\rangle$.

For example, the inner product spaces $(C([0,1],\mathbb{F}),\langle\cdot,\cdot\rangle)$ and $(C([0,1],\mathbb{F}),(\cdot,\cdot))$ in Example 5.1.7 are considered different.

Remark. Every subspace W of $(V,\langle\cdot,\cdot\rangle)$ is also an inner product space with inner product inherited from V, namely, we can turn W into $(W,\langle\cdot,\cdot\rangle)$.

Definition 5.1.8. By **Euclidean Space** we mean $\mathbb{R}^n$ equipped with the standard inner product, i.e., dot product.

Convention. From now on in $\mathbb{F}^n$, unless specified otherwise we always assume the notation $\langle\cdot,\cdot\rangle$ means the dot product.

The notation $\langle\cdot,\cdot\rangle$ is more convenient than the standard dot $\cdot$ notation, we demonstrate this in the following example.

Example 5.1.9. Let $A \in M_{n\times n}(\mathbb{R})$ be symmetric such that

$$-3A^2+5A-3I=0,$$

we try to show that A is positive definite.

We just need to verify $\langle Av,v\rangle > 0$ (dot product) for every $v\neq 0$. By the identity above, we have

$$\begin{aligned}5\langle Av,v\rangle &= \langle 5Av,v\rangle\\ &= \langle 3v+3A^2v,v\rangle && \text{(property of } A)\\ &= \langle 3v,v\rangle+\langle 3A^2v,v\rangle && \text{(bilinearity)}\\ &\overset{(?!)}{=\!=} 3\|v\|^2+3\|Av\|^2 \geq 0.\end{aligned}$$

(?!) is true because

$$\langle A^2v,v\rangle = \langle A(Av),v\rangle = \langle Av,A^Tv\rangle = \langle Av,Av\rangle = \|Av\|^2.$$

Finally, of course when $v\neq 0$, $\langle Av,v\rangle>0$, so we are done.

Definition 5.1.10. On a vector space X the function $x\mapsto\|x\|$ is said to be a **norm** if

(i) $\|x\|\geq 0$ and $\|x\|=0$ iff $x=0$. (**Positivity**)

(ii) For every $\alpha\in\mathbb{F}$ and $x\in X$, $\|\alpha x\|=|\alpha|\|x\|$. (**Scaling Property**)

(iii) For every $x,y\in X$, $\|x+y\|\leq\|x\|+\|y\|$. (**Triangle Inequality**)

Remark. By the way, a vector space endowed with a norm is called a **normed space**. Norms will not be intensively studied in this text, this will be brought into consideration only when the concept of convergence is involved which we study in mathematical analysis.

Definition 5.1.11. For $v\in(V,\langle\cdot,\cdot\rangle)$, we denote

$$\|v\|=\sqrt{\langle v,v\rangle}$$

the **"norm" induced by $\langle\cdot,\cdot\rangle$**.

The fact that $\|\cdot\|$ is a *true* norm follows from (ii) of Theorem 5.1.13. Thus we have no doubt to call $\|\cdot\|$ a *norm* which must satisfy properties listed in Definition 5.1.10.

Example 5.1.12. The norm induced by the inner product on $(V, \langle\cdot,\cdot\rangle)$ satisfies: for all $u, v \in V$,

$$\|u+v\|^2 = \|u\|^2 + \|v\|^2 + 2\operatorname{Re}\langle u, v\rangle.$$

This results from direct expansion:

$$\begin{aligned}\|u+v\|^2 &= \langle u+v, u+v\rangle \\ &= \langle u, u+v\rangle + \langle v, u+v\rangle \\ &= \|u\|^2 + \langle u, v\rangle + \langle v, u\rangle + \|v\|^2 \\ &= \|u\|^2 + \|v\|^2 + 2\operatorname{Re}\langle u, v\rangle.\end{aligned}$$

For complex vector space we note that

$$\operatorname{Re}\langle u, iv\rangle = \operatorname{Re}(-i\langle u, v\rangle) = \operatorname{Im}\langle u, v\rangle.$$

This formula is useful when we also want a statement in terms of $\operatorname{Im}\langle u, v\rangle$ instead of $\operatorname{Re}\langle u, v\rangle$. Next we derive the most fundamental properties of inner products.

Theorem 5.1.13. *In $(V, \langle\cdot,\cdot\rangle)$, the inner product $\langle\cdot,\cdot\rangle$ satisfies the following:*

(i) $|\langle u, v\rangle| \le \|u\|\|v\|$. ***(Cauchy-Schwarz Inequality)***

(ii) $\|u+v\| \le \|u\| + \|v\|$. ***(Triangle Inequality)***

(iii) $2(\|u\|^2 + \|v\|^2) = \|u+v\|^2 + \|u-v\|^2$. ***(Parallelogram Law)***

Proof. (i) Let $\alpha \in \mathbb{F}, |\alpha| = 1$ be such that $\alpha\langle u, v\rangle = |\langle u, v\rangle|$. For every $t \in \mathbb{R}$,

$$0 \le \|t\alpha u + v\|^2 = \|u\|^2 t^2 + 2|\langle u, v\rangle| t + \|v\|^2,$$

which means that the polynomial on the RHS either has one or has no real root, thus

$$(2|\langle u, v\rangle|)^2 - 4\|u\|^2\|v\|^2 \le 0 \iff |\langle u, v\rangle| \le \|u\|\|v\|.$$

(ii) By direct expansion,

$$\|u+v\| \le \|u\| + \|v\| \iff \|u+v\|^2 \le (\|u\| + \|v\|)^2 \iff \operatorname{Re}\langle u, v\rangle \le \|u\|\|v\|,$$

the latter one is true by (i).

(iii) It follows similarly from direct expansion. □

Remark. It is Parallelogram Law that's found to be also sufficient for a norm being induced by an inner product. Namely, we have the following result:

> *A norm $\|\cdot\|$ on a vector space X is induced by an inner product if and only if $\|\cdot\|$ satisfies the parallelogram law.*

The proof will not be presented here as it is not in the scope of this text. This is a standard result usually proved in analysis course which studies inner product spaces and, in particular, Hilbert spaces. The readers are left to learn the proof in these courses.

An inner product space is better than a vector space since many geometrical concept can be abstracted.

Definition 5.1.14. Let $(V, \langle\cdot,\cdot\rangle)$ be an inner product space.

(i) Let $u, v \in V$. u, v are said to be **orthogonal** if $\langle u, v\rangle = 0$, denoted by $u \perp v$.

(ii) $\{v_1, \ldots, v_n\}$ in V is said to be **orthogonal** if

$$\langle v_i, v_j\rangle = 0 \quad \text{whenever } i \neq j.$$

(iii) $\{v_1, \ldots, v_n\}$ in V is said to be **orthonormal** if it is orthogonal and $\|v_i\| = 1$ for $i = 1, 2, \ldots, n$.

Note that by definition, orthogonal set is allowed to contain a zero element, while orthonormal set does not.

Theorem 5.1.15. *Let $\{v_1, v_2, \ldots, v_n\} \subseteq V$ be an orthogonal set of nonzero vectors of $(V, \langle\cdot,\cdot\rangle)$, then $v_1, v_2, \ldots, v_n$ are linearly independent.*

Proof. Let $a_i \in \mathbb{R}$ be such that

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0,$$

we do inner product on both sides with a_i to get

$$\langle a_1v_1 + a_2v_2 + \cdots + a_nv_n, a_i\rangle = 0,$$

hence $a_i\|v_i\|^2 = 0$. As $v_i \neq 0$, $\|v_i\| \neq 0$, thus $a_i = 0$, for $i = 1, 2, \ldots, n$. □

Example 5.1.16 (Some Orthogonal Sets).

(i) The standard basis of $\mathbb{F}^n$ is orthonormal.

(ii) Define $\langle\cdot,\cdot\rangle$ on $\mathbb{P}_n(\mathbb{R})|_{[-1,1]} = \{p|_{[-1,1]} : p \in \mathbb{P}_n(\mathbb{R})\}$ by $\langle p, q\rangle = \int_{-1}^1 pq\,dx$. The **Legendre polynomials** on $[-1, 1]$ are defined recursively by

$$p_0 = 1, \quad p_1 = x \quad \text{and} \quad (n+1)p_{n+1} = (2n+1)xp_n - np_{n-1} \text{ for } n \geq 1.$$

p_k's are mutually orthogonal. Indeed, they satisfy

$$\int_{-1}^1 p_m(x)p_n(x)\,dx = \frac{2}{2n+1}\delta_{mn}.$$

Hence by Theorem 5.1.15, $p_0, \ldots, p_n$ forms a basis of $\mathbb{P}_n(\mathbb{R})|_{[-1,1]}$ since $\dim \mathbb{P}_n(\mathbb{R})|_{[-1,1]} = n+1$.

We give the first few Legendre polynomials here:

$$P_0(x) = 1$$

$$P_1(x) = x \qquad P_2(x) = \frac{1}{2}(3x^2 - 1)$$

$$P_3(x) = \frac{1}{2}(5x^3 - 3x) \qquad P_4(x) = \frac{1}{8}(35x^4 - 30x^2 + 3)$$

$$P_5(x) = \frac{1}{8}(63x^5 - 70x^3 + 15x) \qquad P_6(x) = \frac{1}{16}(231x^6 - 315x^4 + 105x^2 - 5).$$

They arise naturally in physics (when solving PDE) and come to be the solution of the 2nd order ODE:

$$\frac{d}{dx}\left((1-x^2)\frac{dy}{dx}\right) + n(n+1)y = 0. \tag{5.1.17}$$

Define the linear map

$$(Qf)(x) = \frac{d}{dx}\left((1-x^2)\frac{df}{dx}(x)\right),$$

solving (5.1.17) becomes an eigenvalue problem $Qy = -n(n+1)y$. The general study of the orthogonality among solutions corresponding to different eigenvalues is contained in Sturm-Liouville theory. One may google it for detail, this is important for physics students.

Orthonormal set provides us a natural decomposition of every vectors in an inner product space. Also with the help of orthonormal basis, all inner products look very similar to standard inner product on $\mathbb{F}^n$.

Theorem 5.1.18. *Let W be a subspace of $(V, \langle\cdot,\cdot\rangle)$ with orthonormal basis $\alpha = \{w_1, \dots, w_k\}$.*

(i) For every $w \in W$, $w = \sum_{i=1}^k \langle w, w_i\rangle w_i$.

(ii) For $x, y \in W$, $\langle x, y\rangle = \langle [x]_\alpha, [y]_\alpha\rangle$.

Proof. (i) Suppose $w = a_1w_1 + \cdots + a_kw_k$, then

$$\langle w, w_i\rangle = \langle a_1w_1 + \cdots + a_kw_k, w_i\rangle = a_i\|w_i\|^2 = a_i.$$

(ii) Let $x = \sum_{i=1}^k x_iw_i$ and $y = \sum_{i=1}^k y_iw_i$, then

$$\langle x, y\rangle = \left\langle \sum_{i=1}^k x_iw_i, \sum_{j=1}^k y_jw_j \right\rangle = \sum_{i=1}^k\sum_{j=1}^k x_i\overline{y_j}\langle w_i, w_j\rangle = \sum_{i=1}^k x_i\overline{y_i} = \langle [x]_\alpha, [y]_\alpha\rangle. \qquad \square$$

5.2 Orthogonal Complement

Definition 5.2.1. In $(V, \langle\cdot,\cdot\rangle)$, the set

$$S^\perp := \{v \in V : \langle v, s\rangle = 0, \text{ for all } s \in S\}$$

is called the **orthogonal complement** of S in V.

It will be seen very soon that orthogonal complement provides us a simple way to decompose a vector space into direct sum of subspaces. Before that we check that orthogonal complement always has a good linear algebraic structure.

Theorem 5.2.2. *In $(V, \langle\cdot,\cdot\rangle)$, let S be a subset of V, then $S^\perp$ is a subspace of V,*

Proof. It is a routine verification of (i), (ii) and (iii) in Definition 2.4.1. $\square$

In Theorem 5.2.2 we only require S be a set, not a subspace. If we also require S be a subspace, then we get more interesting properties:

Theorem 5.2.3 (Properties of Orthogonal Complement).

(i) Let $S \subseteq V$ and $0 \in S$, we have

$$S \cap S^{\perp} = \{0\}.$$

(ii) Let W_1, W_2 be subspaces of V, then

$$(W_1 + W_2)^{\perp} = W_1^{\perp} \cap W_2^{\perp}.$$

Proof. (i) Let $x \in S \cap S^{\perp}$, then $\langle x, s \rangle$ for every $s \in S$, take $s = x$, we have $\|x\| = 0$, so $x = 0$.

(ii) Let $x \in (W_1 + W_2)^{\perp}$, we try to show $x \in W_1^{\perp} \cap W_2^{\perp}$. Since $\langle x, v \rangle = 0$ for all $v \in W_1 + W_2$, $\langle x, v \rangle = 0$ for all $v \in W_1$ and also all $v \in W_2$, so $x \in W_1^{\perp} \cap W_2^{\perp}$, thus

$$(W_1 + W_2)^{\perp} \subseteq W_1^{\perp} \cap W_2^{\perp}.$$

Conversely, let $x \in W_1^{\perp} \cap W_2^{\perp}$, then for every $w_1 \in W_1$ and every $w_2 \in W_2$,

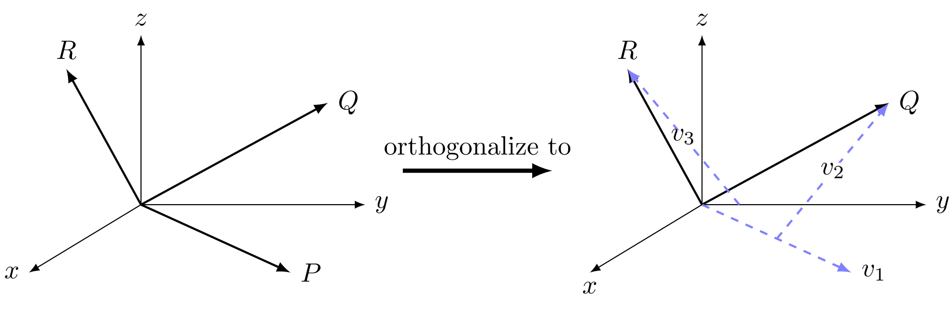
$$\langle x, w_1 \rangle, \langle x, w_2 \rangle = 0 \implies \langle x, w_1 + w_2 \rangle = 0,$$

so $\langle x, w \rangle = 0$ for all $w \in W_1 + W_2$, thus $x \in (W_1 + W_2)^{\perp}$, so

$$W_1^{\perp} \cap W_2^{\perp} \subseteq (W_1 + W_2)^{\perp}.$$ □

5.3 Gram-Schmidt Orthogonalization Process

Let's visualize our "orthogonalization" in $\mathbb{R}^3$. Let's consider a set of three vectors $\{P, Q, R\}$ (drawn below) that are linearly independent and we try to "orthogonalize" them.



Step 1. We fix a vector $v_1 = P$ as our "starting element".

Step 2. We search for a vector in $\text{span}\{v_1, Q\}$ that is orthogonal to v_1. To do this, we do "projection" of Q onto $\text{span}\{v_1\}$ to get $P_{\text{span}\{v_1\}}Q$, then we let

$$v_2 := Q - P_{\text{span}\{v_1\}}Q = Q - \frac{(Q \cdot v_1)v_1}{\|v_1\|^2}.$$

Step 3. We search for an element in $\operatorname{span}\{v_1, v_2, R\}$ that is orthogonal to both v_1 and v_2. For this, we project R onto $\operatorname{span}\{v_1, v_2\}$ to get $P_{\operatorname{span}\{v_1,v_2\}}R$, then we let

$$v_3 := R - P_{\operatorname{span}\{v_1,v_2\}}R = R - \left(\frac{(R\cdot v_1)v_1}{\|v_1\|^2} + \frac{(R\cdot v_2)v_2}{\|v_2\|^2}\right).$$

The process above can be generalized to every n dimensional subspace W of a vector space V provided a basis of W is already known.

Theorem 5.3.1 (Gram-Schmidt Process). *Let W be a finite dimensional subspace of $(V, \langle\cdot,\cdot\rangle)$. Given a basis $\{u_1, \dots u_n\}$ of W, $v_1, v_2, \dots, v_n$ constructed below*

$$\begin{aligned} v_1 &= u_1 \\ v_2 &= u_2 - \frac{\langle u_2, v_1\rangle}{\|v_1\|^2}v_1 \\ v_3 &= u_3 - \frac{\langle u_3, v_1\rangle}{\|v_1\|^2}v_1 - \frac{\langle u_3, v_2\rangle}{\|v_2\|^2}v_2 \\ &\vdots \\ v_p &= u_p - \sum_{i<p}\frac{\langle u_p, v_i\rangle}{\|v_i\|^2}v_i \end{aligned} \tag{5.3.2}$$

are mutually orthogonal, $p = 2, 3, \dots, n$, hence by Theorem 5.1.15, $\{v_1, \dots, v_n\}$ is an orthogonal basis of W.

Proof. The orthogonality is just a routine verification, we leave the proof as an exercise. □

Remark. Using (5.3.2) we can reduce any linearly independent set of vectors into an orthogonal set which spans the same space. Dividing each resulting vector by its norm (this process is called **normalization**), we get an orthonormal set.

Gram-Schmidt processes provides us with a partially constructive proof to the following important result:

Theorem 5.3.3 (Existence of Orthonormal Basis). *Every finite dimensional inner product space V admits an orthonormal basis.*

Proof. By Theorem 2.6.8 V has a basis, by (5.3.2) and normalization, we can reduce this basis into an orthonormal set. □

5.4 Orthogonal Projection

5.4.1 General Definition

To make sense of the upcoming definition one needs to know that whenever $T : V \to V$ satisfies $T^2 = T$,

$$V = \ker T \oplus \operatorname{range} T. \tag{5.4.1}$$

This is because for every $v \in V$,

$$v = (v - Tv) + Tv,$$

while $v - Tv \in \ker T$ and $Tv \in \operatorname{range} T$. Moreover, if $v \in \ker T \cap \operatorname{range} T$, one easily shows that $v = 0$, so the sum is actually a direct sum. In conclusion, every map $T : V \to V$ that satisfies $T^2 = T$ generates a direct sum decomposition of V.

Furthermore, suppose we can give V an inner product, we also study when the direct sum generated by such a map (satisfying $T^2 = T$) will be an orthogonal sum, namely, when will $\ker T \perp \operatorname{range} T$.

Definition 5.4.2. Let V be a vector space over $\mathbb{F}$ and $T : V \to V$ a linear map.

(i) We say that T is a **projection** if $T^2 = T$.

(ii) If $V = (V, \langle \cdot, \cdot \rangle)$, we say that T is an **orthogonal projection** if T is a projection and the direct sum
$$V = \ker T \oplus \operatorname{range} T$$
is orthogonal.

Example 5.4.3. Define $T : M_{n\times n}(\mathbb{R}) \to M_{n\times n}(\mathbb{R})$ by

$$T(A) = \frac{A + A^T}{2}, \quad \forall A \in M_{n\times n}(\mathbb{R}).$$

T is a projection. Indeed, for each $A \in M_{n\times n}(\mathbb{R})$,

$$T^2(A) = T\left(\frac{A + A^T}{2}\right) = \frac{\frac{A+A^T}{2} + \frac{A^T+A}{2}}{2} = \frac{A + A^T}{2} = T(A),$$

as desired. By the discussion preceding Definition 5.4.2 we have $M_{n\times n}(\mathbb{R}) = \ker T \oplus \operatorname{range} T$. Denote $\operatorname{Sym}_n(\mathbb{R}) = \{\text{symmetric matrices}\}$ and $\operatorname{Ssym}_n(\mathbb{R}) = \{\text{skew-symmetric matrices}\}$,

$$M_{n\times n}(\mathbb{R}) = \operatorname{range} T \oplus \ker T = \operatorname{Sym}_n(\mathbb{R}) \oplus \operatorname{Ssym}_n(\mathbb{R}).$$

Suppose we turn $M_{n\times n}(\mathbb{R})$ into an inner product space by defining $\langle A, B\rangle$ as in Problem 5.1 for $A, B \in M_{n\times n}(\mathbb{R})$, then the direct sum is easily shown to be orthogonal. Hence

$$T : (M_{n\times n}(\mathbb{R}), \langle \cdot, \cdot \rangle) \to (\operatorname{Sym}_n(\mathbb{R}), \langle \cdot, \cdot \rangle)$$

is an orthogonal projection.

5.4.2 Orthogonal Projection onto Finite Dimensional Subspaces

In the rest we mainly focus on the orthogonal projection defined in the following definition. Note that we just require W be finite dimensional, while V is as "big" as we want.

Definition 5.4.4. Let W be finite dimensional subspace of V and $\{w_1, \ldots, w_k\}$ its **orthogonal** basis, then we denote the linear map $\boldsymbol{P_W : V \to W}$ defined by

$$P_W v = \sum_{i=1}^{k} \frac{\langle v, w_i \rangle w_i}{\|w_i\|^2}, \quad \text{for each } v \in V. \tag{5.4.5}$$

We will prove that the map P_W is *well-defined*. Namely, the vector $P_W v$ is independent of the choices of orthogonal basis of W, therefore it makes sense to speak of P_W without specifying the orthogonal basis of W we use. We will state this result precisely in Corollary 5.4.8.

Remark. The reason to study orthogonal projection can be seen in Theorem 5.4.13. Namely, orthogonal projection gives us an explicit construction of a solution to optimization problems in linear algebra setting.

Remark. P_W defined in Definition 5.4.4 is usually called

$$\underline{\text{the}}\ \underline{\text{orthogonal projection}}\ \underline{\text{onto}}\ W.$$

The reason for using each underlined term will be clear after we go through Theorem 5.4.6, Corollary 5.4.7 and Corollary 5.4.8.

For Theorem 5.4.6 and Corollary 5.4.7 let's suppose P_W is defined by fixing a choice of an orthogonal basis $\{w_1, w_2, \ldots, w_k\}$ of W.

Theorem 5.4.6. *Let W be a finite dimensional subspace of $(V, \langle\cdot,\cdot\rangle)$, then:*

(i) $P_W^2 = P_W$. ***(Projection)***

(ii) $\langle P_W u, v\rangle = \langle u, P_W v\rangle$. ***(Self-Adjoint)***

(iii) $P_W\big|_W = I_W$.

(iv) $\operatorname{range} P_W = W$ *and* $\ker P_W = W^\perp$.

Proof. (i) Indeed,

$$\begin{aligned} P_W^2 v &= P_W\left(\sum_{i=1}^k \frac{\langle v, w_i\rangle w_i}{\|w_i\|^2}\right) = \sum_{i=1}^k \frac{\langle v, w_i\rangle}{\|w_i\|^2} P_W(w_i) \\ &= \sum_{i=1}^k\sum_{j=1}^k \frac{\langle v, w_i\rangle}{\|w_i\|^2}\frac{\langle w_i, w_j\rangle w_j}{\|w_j\|^2} = \sum_{i=1}^k \frac{\langle v, w_i\rangle w_i}{\|w_i\|^2} = P_W v, \end{aligned}$$

thus P_W is a projection.

(ii) By direct expansion,

$$\langle P_W u, v\rangle = \left\langle \sum_{i=1}^k \frac{\langle u, w_i\rangle w_i}{\|w_i\|^2}, v\right\rangle = \sum_{i=1}^k \frac{\langle u, w_i\rangle\langle w_i, v\rangle}{\|w_i\|^2} \overset{(*)}{=\!=} \sum_{i=1}^k \frac{\langle u, \langle v, w_i\rangle w_i\rangle}{\|w_i\|^2} = \langle u, P_W v\rangle.$$

Here $(*)$ holds since $\langle u, w_i\rangle\langle w_i, v\rangle = \langle u, w_i\rangle\overline{\langle v, w_i\rangle} = \langle u, \langle v, w_i\rangle w_i\rangle$.

(iii) suppose $x \in W$, then there are $a_1, \ldots, a_k \in \mathbb{F}$ such that

$$x = a_1 w_1 + \cdots + a_k w_k \implies \langle x, w_i\rangle = a_i\|w_i\|^2 \implies a_i = \frac{\langle x, w_i\rangle}{\|w_i\|^2},$$

thus

$$x = \sum_{i=1}^k a_i w_i = \sum_{i=1}^k \frac{\langle x, w_i\rangle}{\|w_i\|^2} w_i = P_W x,$$

as desired.

(iv) $\operatorname{range} P_W = W$ since $\operatorname{range} P_W \subseteq W$ and $P_W\big|_W = I_W$. For the next equality,

$$\begin{aligned} x \in \ker P_W &\iff P_W x = 0 \iff \langle P_W x, w\rangle = 0, \forall w \in W \\ &\iff \langle x, P_W w = w\rangle = 0, \forall w \in W \iff x \in W^\perp. \end{aligned}$$ □

Now we justify the name that P_W is indeed an orthogonal projection onto W.

Corollary 5.4.7. *Let W be a finite dimensional subspace of $(V, \langle\cdot,\cdot\rangle)$, then P_W defined in (5.4.5) is an orthogonal projection.*

Proof. By (i) of Theorem 5.4.6 P_W is a projection. By (ii) of Theorem 5.4.6 we have $\ker P_W \perp \operatorname{range} P_W$, it is because for $u \in \ker P_W$ and $P_W v \in \operatorname{range} P_W$,

$$\langle u, v\rangle = \langle u, P_W v\rangle = \langle P_W u, v\rangle = \langle 0, v\rangle = 0.$$ □

It is a natural to ask what happens if the orthogonal projections are constructed by two different orthogonal bases, will they be different? The answer is NO:

Corollary 5.4.8. *Let W be a finite dimensional subspace of $(V, \langle\cdot,\cdot\rangle)$, then P_W defined in Definition 5.4.4 is **well-defined**. That is, given two orthogonal bases $\{w_1, \dots, w_k\}, \{w_1', \dots . w_k'\}$ of W, we have*

$$\sum_{i=1}^k \frac{\langle v, w_i\rangle w_i}{\|w_i\|^2} = \sum_{i=1}^k \frac{\langle v, w_i'\rangle w_i'}{\|w_i'\|^2},$$

for all $v \in V$.

Proof. By (5.4.5) we get P_W by using the orthogonal basis $\{w_1, \dots, w_k\}$. Replacing w_i's in (5.4.5) by w_i''s, we get another orthogonal projection P_W'. Now Theorem 5.4.6 can be applied to both P_W and P_W', in particular, by (iv) of Theorem 5.4.6 for every $v \in V$,

$$v = \underbrace{P_W v}_{\in W} + \underbrace{(I - P_W)v}_{\in \ker P_W = W^\perp} = \underbrace{P_W' v}_{\in W} + \underbrace{(I - P_W')v}_{\in \ker P_W' = W^\perp}.$$

However, by (i) of Theorem 5.2.3, $W \cap W^\perp = \{0\}$, and also by (ii) of Proposition 2.4.10 the summing way is unique, i.e., $P_W v = P_W' v$. □

(i) and (iv) of Theorem 5.4.6 directly gives the decomposition:

Corollary 5.4.9. *If W is a **finite dimensional** subspace of V, then*

$$V = W \oplus W^\perp \quad \text{and} \quad (W^\perp)^\perp = W.$$

Usually we say that the direct sum $W \oplus W^\perp$ is orthogonal since for every $u \in W$ and $v \in W^\perp$, $\langle u, v\rangle = 0$.

Proof. Let α be an orthogonal basis of W and use it to construct $P_W : V \to W$, the orthogonal projection onto W. Then (i) of Theorem 5.4.6 says that P_W is a projection, thus by (5.4.1),

$$V = \operatorname{range} P_W \oplus \ker P_W,$$

then by (iv) of Theorem 5.4.6, $V = W \oplus W^\perp$.

It remains to check $(W^\perp)^\perp = W$, it follows from definition that $W \subseteq (W^\perp)^\perp$. Conversely, let $x \in (W^\perp)^\perp$, then there are $u \in W, v \in W^\perp$ such that $x = u + v$, then

$$v = x - u \in (W^\perp)^\perp + W = (W^\perp)^\perp \implies v \in (W^\perp)^\perp \cap W^\perp,$$

therefore $v = 0$ by (i) of Theorem 5.2.3 and thus $x = u \in W$, so $(W^\perp)^\perp \subseteq W$. $\square$

In the following example we use A^* to mean $(\overline{A})^T$, i.e., it is the **conjugate transpose** of A. For example, $\left[\begin{smallmatrix} i & 1 \\ 0 & 1 \end{smallmatrix}\right]^* = \left[\begin{smallmatrix} -i & 0 \\ 1 & 1 \end{smallmatrix}\right]$. It shares almost all features with transpose. For example, under standard inner product in $\mathbb{F}^n$, $\langle A^*x, y\rangle = \langle x, Ay\rangle$. We also use * to express the standard inner product on $\mathbb{F}^n$: $\langle x, y\rangle = y^*x$. When $\mathbb{F} = \mathbb{R}$, $y^*x = y^Tx$.

Example 5.4.10. Let $A \in M_{m\times n}(\mathbb{F})$, and $\mathbb{F}^m, \mathbb{F}^n$ be given standard inner products. Conjugate transpose and orthogonal complement are related by the following identities:

(i) $(\operatorname{Col} A)^\perp = \operatorname{Nul} A^*$

(ii) $(\operatorname{Nul} A)^\perp = \operatorname{Col} A^*$

(iii) $(\operatorname{Col} A^*)^\perp = \operatorname{Nul} A$

(iv) $(\operatorname{Nul} A^*)^\perp = \operatorname{Col} A$

To show these, we just need to prove (i) and the rest will then follow from this and Corollary 5.4.9. Now

$$\begin{aligned} x \in \operatorname{Nul} A^* \iff A^*x = 0 &\iff \langle A^*x, v\rangle = 0, \forall v \in \mathbb{F}^n \\ &\iff \langle x, Av\rangle = 0, \forall v \in \mathbb{F}^n \iff x \in (\operatorname{Col} A)^\perp, \end{aligned}$$

that said, $\operatorname{Nul} A^T = (\operatorname{Col} A)^\perp$.

Remark. A simple application of Example 5.4.10 gives

$$\boxed{A \text{ is onto}} \text{ iff } \operatorname{Col} A = \mathbb{F}^m \text{ iff } (\operatorname{Col} A)^\perp = (\mathbb{F}^m)^\perp \text{ iff } \operatorname{Nul} A^T = \{0\} \text{ iff } \boxed{A^T \text{ is 1-1.}}$$

The result $(W^\perp)^\perp = W$ in Corollary 5.4.9 **can be false if W is infinite dimensional**. In general it is easy to prove $W \subseteq (W^\perp)^\perp$. In analysis we further know $(W^\perp)^\perp = \overline{W}$, where $\overline{\cdot}$ denotes the **closure** with respect to the norm induced by the inner product. We give a specific counter example below which requires a result in real analysis.

Example 5.4.11. Let $P = \mathbb{P}(\mathbb{R})|_{[0,1]} = \{p|_{[0,1]} : p \in \mathbb{P}(\mathbb{R})\}$, then P is a subspace of the inner product space $C([0,1], \mathbb{R})$ with the inner product defined by $\langle f, g\rangle = \int_{-1}^1 fg\, dx$. Let $\cdot^\perp$ denote the orthogonal complement in $C([0,1], \mathbb{R})$, we try to prove that

$$(P^\perp)^\perp = C([0,1], \mathbb{R}).$$

By definition,

$$f \in (P^\perp)^\perp \iff \int_0^1 fg\, dx = 0 \quad \text{for all } g \in P^\perp.$$

What is $P^\perp$? Let $g \in P^\perp$, then

$$\int_0^1 gp\,dx = 0 \quad \text{for every polynomial } p \text{ on } [0,1].$$

But g is continuous on $[0,1]$, by Weierstrass approximation Theorem in analysis there is a sequence of polynomials $\{p_n\}$ such that $p_n \to g$ *uniformly* on $[0,1]$, thus

$$0 = \int_0^1 gp_n\,dx \quad \text{for all } n \implies 0 = \lim_{n\to\infty} \int_0^1 gp_n\,dx = \int_0^1 g^2\,dx,$$

hence by continuity $g = 0$ on $[0,1]$.

The logic says that $P^\perp \subseteq \{0\}$, thus $P^\perp = \{0\}$. Therefore

$$(P^\perp)^\perp = (\{0\})^\perp = C([0,1],\mathbb{R}).$$

Example 5.4.12. Let $v = (1,2,1)^T \in \mathbb{R}^3$, and $W = \operatorname{span}\{(1,0,1)^T, (1,1,0)^T\}$, let's compute $P_W v$.

Step 1 (Find an orthogonal basis of W). Let

$$u_1 = (1,0,1)^T \quad \text{and} \quad u_2 = (1,1,0)^T.$$

We use the Gram-Schmidt process (5.3.2),

$$v_1 = u_1 = \begin{bmatrix}1\\0\\1\end{bmatrix}, \quad \|v_1\|^2 = 2$$

next,

$$v_2 = u_2 - \frac{\langle u_2, v_1\rangle}{\|v_1\|^2} v_1 = \begin{bmatrix}1\\1\\0\end{bmatrix} - \frac{(1,1,0)^T \cdot (1,0,1)^T}{2} \begin{bmatrix}1\\0\\1\end{bmatrix} = \begin{bmatrix}1/2\\1\\-1/2\end{bmatrix}, \quad \|v_2\|^2 = \frac{3}{2}.$$

Step 2 (Project v to W). We apply the formula of P_W in (5.4.5) to get

$$P_W v = \sum \frac{\langle v, v_i\rangle}{\|v_i\|^2} v_i = \frac{\left[\begin{smallmatrix}1\\2\\1\end{smallmatrix}\right] \cdot \left[\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right]}{2} \begin{bmatrix}1\\0\\1\end{bmatrix} + \frac{\left[\begin{smallmatrix}1\\2\\1\end{smallmatrix}\right] \cdot \left[\begin{smallmatrix}1/2\\1\\-1/2\end{smallmatrix}\right]}{3/2} \begin{bmatrix}1/2\\1\\-1/2\end{bmatrix} = \frac{1}{3}\begin{bmatrix}5\\4\\1\end{bmatrix}.$$

5.4.3 Application of Orthogonal Projection to Obtain "Minimizer"

Theorem 5.4.13 explains why we spend time on orthogonal projection. The map $P_W : V \to W$ itself has many well properties explained in Theorem 5.4.6. Apart from that, certain minimization problems, possibly in calculus, can be translated to linear algebra setting, and the next theorem shows us linear algebra can settle the problem quickly.

Theorem 5.4.13. *Let W be a finite dimensional subspace of V, then $P_W v$ is an element such that*

$$\|v - P_W v\| \le \|v - w\| \quad \text{for all } w \in W.$$

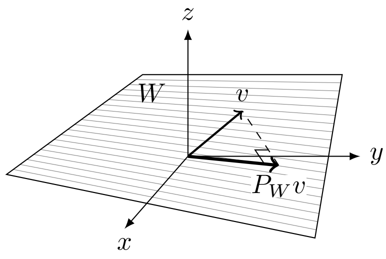
Remark. In Theorem 5.4.13, $P_W v \in W$ minimizes the distance $\|v - w\|$ for $w \in W$. We will show that such minimizer is unique in Theorem 5.4.14.

Proof. Let $v \in V$ and $w \in W$, then

$$\|v-w\|^2 = \|(v-P_W v)+(P_W v - w)\|^2 \overset{(*)}{=\!=} \|v-P_W v\|^2 + \|P_W v - w\|^2 \geq \|v - P_W v\|^2.$$

Here $(*)$ holds because $v - P_W v \in \ker P_W = W^\perp$, $P_W v - w \in W$ and $W \perp W^\perp$. $\square$

Theorem 5.4.13 has a very good geometric interpretation:



The picture also suggests that when w_0 is a *minimizer*, i.e., $\|v-w_0\| \leq \|v-w\|$ for all $w \in W$, then $(v-w_0) \perp w$ for every $w \in W$. Let's turn this geometrically straightforward observation into a rigorous proof.

Theorem 5.4.14 (Variational Principle). *Let W be a finite dimensional subspace of $(V, \langle \cdot, \cdot \rangle)$.*

(i) $w_0 \in W$ minimizes the distance from v to W:

$$\|v-w\|, \quad w \in W$$

if and only if $v - w_0 \in W^\perp$.

(ii) The minimizer above is unique.

Remark. The existence of $w_0 \in W$ is guaranteed by Theorem 5.4.13.

Proof. (i) ($\Rightarrow$) We fix a $w \in W$ and define a function $f : \mathbb{R} \to \mathbb{R}$ as follows:

$$f(t) = \|v - w_0 + tw\|^2 = \|v-w_0\|^2 + t^2\|w\|^2 + 2t\,\mathrm{Re}\langle v - w_0, w\rangle,$$

the second equality follows from Example 5.1.12. Now $f(t) \geq f(0)$ for every $t \in \mathbb{R}$, f attains a local extreme at 0, so $f'(0) = 0$. Since $f'(t) = 2t\|w\|^2 + 2\,\mathrm{Re}\langle v-w_0, w\rangle$, $f'(0) = 0$ becomes

$$\mathrm{Re}\langle v - w_0, w\rangle = 0.$$

When $\mathbb{F} = \mathbb{R}$ we are done. When $\mathbb{F} = \mathbb{C}$, we can replace w by iw (since $iw \in W$) to conclude

$$\mathrm{Im}\langle v - w_0, w\rangle = 0,$$

so $\langle v - w_0, w\rangle = 0$. Now this is true for each fixed $w \in W$, we conclude $v - w_0 \in W^\perp$.

($\Leftarrow$) Assume $v - w_0 \in W^\perp$, then for every $w \in W$,

$$\|v-w\|^2 = \|(v-w_0)+(w_0-w)\|^2 = \|v-w_0\|^2 + \|w_0 - w\|^2 \geq \|v-w_0\|^2,$$

therefore w_0 minimizes the distance from v to W.

(ii) Let w_0 be defined as in (i) and let $w' \in W$ be such that $\|v - w'\| \leq \|v - w\|$ for every $w \in W$, then $v - w' \in W^\perp$ by (i). Now both $v - w_0, v - w' \in W^\perp$, hence

$$w_0 - w' = (v - w') - (v - w_0) \in W \cap W^\perp = \{0\}. \qquad \square$$

Example 5.4.15. Let $y=(7,4,7)^T\in\mathbb{R}^3$ and let V be a subspace of $\mathbb{R}^3$ spanned by

$$u_1=(1,2,3)^T \quad\text{and}\quad u_2=(4,5,6)^T.$$

Let's find the distance from y to V in 4 different ways:

(a) Find a $u\in V$ that is closest to y by orthogonal projection.

(b) Find a $u\in V$ that is closest to y by constructing a **normal equation**.

(c) Find a $u\in V$ that is closest to y by the property of minimizer given in Theorem 5.4.14.

(d) Construct a matrix $P\in M_{3\times 3}(\mathbb{R})$ such that

$$\|x-Px\|\le\|x-v\|$$

for all $x\in\mathbb{R}^3$ and $v\in V$. What is Py?

(a) By Gram-Schmidt process we orthogonalize u_1 and u_2 to

$$v_1=\begin{bmatrix}1\\2\\3\end{bmatrix}\quad\text{and}\quad v_2=\frac{1}{7}\begin{bmatrix}12\\3\\-6\end{bmatrix}.$$

Where $\|v_1\|^2=14$ and $\|v_2\|^2=\frac{27}{7}$. If we use this orthogonal basis of V to construct the orthogonal projection: For each $x\in\mathbb{R}^3$,

$$Px=\frac{\langle x,v_1\rangle v_1}{\|v_1\|^2}+\frac{\langle x,v_2\rangle v_2}{\|v_2\|^2}. \tag{5.4.16}$$

The $u\in V$ we need is $Py\in V$, since $\|y-Py\|$ is least possible among $\{\|y-v\|:v\in V\}$. Now

$$u=Py=\frac{\langle y,v_1\rangle v_1}{\|v_1\|^2}+\frac{\langle y,v_2\rangle v_2}{\|v_2\|^2}=\frac{\left[\begin{smallmatrix}7\\4\\7\end{smallmatrix}\right]\cdot\left[\begin{smallmatrix}1\\2\\3\end{smallmatrix}\right]}{14}\begin{bmatrix}1\\2\\3\end{bmatrix}+\frac{\frac{1}{7}\left[\begin{smallmatrix}7\\4\\7\end{smallmatrix}\right]\cdot\left[\begin{smallmatrix}12\\3\\-6\end{smallmatrix}\right]}{\frac{27}{7}}\frac{1}{7}\begin{bmatrix}12\\3\\-6\end{bmatrix}=\begin{bmatrix}6\\6\\6\end{bmatrix}.$$

(b) Let's construct $A=\left[\begin{smallmatrix}1&4\\2&5\\3&6\end{smallmatrix}\right]$, then $\operatorname{Col}A=V$. The system $Ax=y$ has no solution, but the best possible that we can do is to choose an element $a\in\operatorname{Col}A$ such that a is closest to y. To do this, consider

$$A^TAx=A^Ty, \tag{5.4.17}$$

then the solution x_0 to this system will satisfy $\|y-v\|\ge\|y-Ax_0\|$, for all $v\in\operatorname{Col}A$. Thus what we want is $u=Ax_0$.

Let's try to solve (5.4.17), a direct computation shows that (5.4.17) is the same as

$$\begin{bmatrix}14&32\\32&77\end{bmatrix}x=\begin{bmatrix}36\\90\end{bmatrix},$$

a direct calculation yields $x=\left[\begin{smallmatrix}-2\\2\end{smallmatrix}\right]$. Hence $u=Ax=\left[\begin{smallmatrix}1&4\\2&5\\3&6\end{smallmatrix}\right]\left[\begin{smallmatrix}-2\\2\end{smallmatrix}\right]=\left[\begin{smallmatrix}6\\6\\6\end{smallmatrix}\right]$.

(c) An element $a\in\operatorname{Col}A$ minimizes the distance $\{\|y-v\|:v\in\operatorname{Col}A\}$ if and only if

$$y-a\perp v,\quad\forall v\in\operatorname{Col}A.^{(\dagger)}$$

(†) Essentially this is the idea that we use to construct normal equation in (b) since $y-a\in(\operatorname{Col}A)^\perp$ iff $A^T(y-a)=0$. But this "orthogonality method" also works for minimization problem that is not in $\mathbb{R}^n$. In particular, it works for some finite dimensional function spaces in which the language of matrices is not applicable, say the collection of all polynomials with degree at most n.

It is worth illustrating how simple the orthogonality method is. Let $a = x\begin{bmatrix}1\\2\\3\end{bmatrix} + y\begin{bmatrix}4\\5\\6\end{bmatrix}$ that minimizes the distance, then

$$\left\langle y - a, \begin{bmatrix}1\\2\\3\end{bmatrix}\right\rangle = \left\langle y - a, \begin{bmatrix}4\\5\\6\end{bmatrix}\right\rangle = 0 \implies \begin{cases} 14x + 32y = 36, \\ 32x + 77y = 90, \end{cases}$$

thus $x = -2$ and $y = 2$, so $u = \begin{bmatrix}6\\6\\6\end{bmatrix}$.

(d) The projection matrix is given by $P = A(A^TA)^{-1}A^T = \frac{1}{6}\begin{bmatrix}5 & 2 & -1\\2 & 2 & 2\\-1 & 2 & 5\end{bmatrix}$, so $u = Py = \begin{bmatrix}6\\6\\6\end{bmatrix}$. We will explain the formula in detail in Section 5.5.

Of course the computation of P above is very tedious.

Given an orthonormal basis, why don't we just find the standard matrix of the orthogonal projection constructed by this basis? Recall the formula in (5.4.16), we have (on simplification)

$$P(x) = \frac{x \cdot \begin{bmatrix}1\\2\\3\end{bmatrix}}{14}\begin{bmatrix}1\\2\\3\end{bmatrix} + \frac{x \cdot \begin{bmatrix}4\\1\\-2\end{bmatrix}}{21}\begin{bmatrix}4\\1\\-2\end{bmatrix},$$

so we get

$$\begin{aligned} Pe_1 &= \frac{1}{14}\begin{bmatrix}1\\2\\3\end{bmatrix} + \frac{4}{21}\begin{bmatrix}4\\1\\-2\end{bmatrix} = \frac{1}{6}\begin{bmatrix}5\\2\\-1\end{bmatrix} \\ Pe_2 &= \frac{2}{14}\begin{bmatrix}1\\2\\3\end{bmatrix} + \frac{1}{21}\begin{bmatrix}4\\1\\-2\end{bmatrix} = \frac{1}{6}\begin{bmatrix}2\\2\\2\end{bmatrix} \qquad \implies \qquad [P] = \frac{1}{6}\begin{bmatrix}5 & 2 & -1\\2 & 2 & 2\\-1 & 2 & 5\end{bmatrix}, \qquad (5.4.18) \\ Pe_3 &= \frac{3}{14}\begin{bmatrix}1\\2\\3\end{bmatrix} + \frac{(-2)}{21}\begin{bmatrix}4\\1\\-2\end{bmatrix} = \frac{1}{6}\begin{bmatrix}-1\\2\\5\end{bmatrix} \end{aligned}$$

where the computation is much simpler!

Remark. If $v_1, v_2 \in \mathbb{R}^3$ given are already **orthonormal** at the beginning, then the projection matrix is extremely easy to compute. Namely, let $A = [v_1 \quad v_2]$, then

$$P = A(A^TA)^{-1}A^T = AA^T.$$

Remark. The projection matrix in (5.4.18) is symmetric. Indeed the standard matrix of any orthogonal projection must be symmetric, see Problem 5.10 for detail.

Example 5.4.19. We try to find $p \in \mathbb{P}_3(\mathbb{R})$ such that $p(0) = 0$, $p'(0) = 0$ and

$$\int_0^1 (2 + 3x - p(x))^2\, dx$$

is as small as possible. Note that it is the same as finding p_0 in the vector space

$$W = \{p \in \mathbb{P}_3(\mathbb{R}) : p(0) = p'(0) = 0\} = \{a_3x^3 + a_2x^2 : a_3, a_2 \in \mathbb{R}\}$$

such that

$$\{\|2 + 3x - p\| : p \in W\}$$

is minimized by p_0, where the norm is induced by the inner product $\langle f, g\rangle = \int_0^1 fg\,dx$. We can find p_0 by two methods.

Method 1 (Projection method).

Step 1 (Find an orthogonal basis in W). It is clear $\{x^2, x^3\}$ is a basis of W. We use Gram-Schmidt process (5.3.2) to find an orthogonal basis of W.

$$f_1 = x^2, \quad \|f_1\|^2 = \int_0^1 (x^2)^2\,dx = \frac{1}{5}$$
$$f_2 = x^3 - \frac{\langle x^3, f_1\rangle}{\|f_1\|^2} f_1 = x^3 - \frac{\langle x^3, x^2\rangle}{\frac{1}{5}} x^2 = x^3 - \frac{5}{6}x^2, \quad \|f_2\|^2 = \frac{1}{252}.$$

Step 2 (Compute projection). Now the minimizing element is

$$\begin{aligned} p_0 = P_W(2+3x) &= \sum \frac{\langle 2+3x, f_i\rangle}{\|f_i\|^2} f_i \\ &= \frac{\langle 2+3x, x^2\rangle}{\frac{1}{5}} x^2 + \frac{\langle 2+3x, x^3 - \frac{5}{6}x^2\rangle}{\frac{1}{252}}\left(x^3 - \frac{5}{6}x^2\right) = -\frac{203}{10}x^3 + 24x^2. \end{aligned}$$

Method 2 (Orthogonality method). In (i) of Theorem 5.4.14 we have shown that p_0 is an minimizing element if and only if $2 + 3x - p_0 \in W^\perp$. Let $p_0 = a_3x^3 + a_2x^2$, then:

$$\begin{cases} \langle 2 + 3x - (a_3x^3 + a_2x^2), x^2\rangle = 0 \\ \langle 2 + 3x - (a_3x^3 + a_2x^2), x^3\rangle = 0 \end{cases} \implies \begin{cases} \dfrac{a_3}{6} + \dfrac{a_2}{5} = \dfrac{17}{12} \\ \dfrac{a_3}{7} + \dfrac{a_2}{6} = \dfrac{11}{10} \end{cases}$$

By solving it, we have $a_2 = 24$ and $a_3 = -203/10$.

5.5 Least Square Approximation

Let $A = [a_1 \quad \cdots \quad a_n] \in M_{m\times n}(\mathbb{R})$ with $a_1, a_2, \ldots, a_n \in \mathbb{R}^m$. Let $b \in \mathbb{R}^m$, although

$$Ax = b$$

may not have solution, generally we can still try to find out $a_0 \in \operatorname{Col} A$ such that $\|b - a_0\|$ is minimized. To find such a_0, we try to minimize

$$\|b - a\|, \quad a \in \operatorname{Col} A,$$

the minimizing element $a_0 \in \operatorname{Col} A$ exists by Theorem 5.4.13, also a_0 is such an element if and only if $b - a_0 \in (\operatorname{Col} A)^\perp$ by (i) of Theorem 5.4.14, hence a_0 is a minimizer if and only if

$$b - a_0 \perp a_1, a_2, \ldots, a_n,$$

or equivalently,

$$A^T(b - a_0) = 0.$$

Writing $a_0 = Ax_0$ for some $x_0 \in \mathbb{R}^n$, we obtain the **normal equation** (associated to the vector equation $Ax = b$)

$$(A^TA)x_0 = A^Tb^{(\ddagger)}.$$

(‡) Alternatively, we can obtain this equation by multivaribale calculus. Let $A = [a_1 \quad \cdots \quad a_n]$ and define $f(x) = \|b - Ax\|^2$, one can show that $f_{x_k}(x) = -2a_k^Tb - \sum_{j=1}^n x_j a_j^T a_k$, and hence $\begin{bmatrix} f_{x_1}(x) \\ \vdots \\ f_{x_n}(x) \end{bmatrix} = -2(A^Tb - A^TAx)$. So we get the normal equation when $\nabla f(x) = 0$.

WLOG we may assume the columns of A are linearly independent[(§)], in this case A is of full rank and necessarily $m \geq n$. Now A^TA is an $n \times n$ matrix and $\operatorname{rank} A^TA = \operatorname{rank} A = n$ (by Problem 2.21), hence A^TA is invertible, thus

$$x_0 = (A^TA)^{-1}A^Tb,$$

and the minimizer a_0 is $Ax_0 = A(A^TA)^{-1}A^Tb$. However, by Theorem 5.4.13, the orthogonal projection of $b \in \mathbb{R}^m$ onto $\operatorname{Col} A$ is also a minimizer, and Theorem 5.4.14 guarantees the uniqueness of such element, hence

$$P_{\operatorname{Col} A}b = A(A^TA)^{-1}A^Tb.$$

We summarize it as a theorem.

Theorem 5.5.1. *Let V be a proper subspace of $\mathbb{R}^n$ (i.e., $V \neq \mathbb{R}^n$) and $\{v_1, v_2, \ldots, v_k\}$ a basis of V. Then the orthogonal projection onto V is given by*

$$P_Vx = A(A^TA)^{-1}A^Tx,$$

where $A = [v_1 \quad \cdots \quad v_k]$.

5.6 Spectral Theorem

5.6.1 Linear Functional and Adjoint

Let V be a vector space, a map $\varphi \in \mathcal{L}(V, \mathbb{F})$ is called a **linear functional**. $\mathcal{L}(X, \mathbb{F})$ is also called the **dual space** of V, denoted by V^*. Dual space is an important concept in analysis, which provides us the notion of weak convergence, a weaker mode of convergence than the convergence in norm (which recovers "compactness" that starts to be lost in infinite dimensional vector spaces).

For finite dimensional vector space, every element in V^* can be easily understood.

Theorem 5.6.1 (Riesz Representation). *Let $(V, \langle \cdot, \cdot \rangle)$ be a finite dimensional inner product space, for every $\varphi \in V^* = \mathcal{L}(V, \mathbb{F})$, there is a unique $w \in V$ such that $\varphi(\cdot) = \langle \cdot, w \rangle$.*

Remark. The theorem actually holds for Hilbert space, a larger class of vector spaces than finite dimensional spaces, which we will not need in the rest of this text. Also there are several versions of Riesz representation theorem, mostly in real analysis, that are totally different from the statement we have, but they indeed bear the same last name.

Proof. We establish existence first. For this, let $\{w_1, \ldots, w_k\}$ be an orthonormal basis of V. Then for every linear functional $\varphi : V \to \mathbb{F}$ and for every $v \in V$, since

$$v = \sum_{i=1}^{k} \langle v, w_i \rangle w_i,$$

we have

$$\varphi(v) = \varphi\left(\sum_{i=1}^{k} \langle v, w_i \rangle w_i\right) = \sum_{i=1}^{k} \langle v, w_i \rangle \varphi(w_i) = \left\langle v, \sum_{i=1}^{k} \overline{\varphi(w_i)} w_i \right\rangle = \langle v, w \rangle,$$

(§) Otherwise we abandon finitely many of them, replace A by $A' = [a_{n_1} \quad \cdots \quad a_{n_k}]$, the problem is not changed.

for some $w \in V$ with

$$w = \sum_{i=1}^{k} \overline{\varphi(w_i)} w_i. \tag{5.6.2}$$

i.e., there is $w \in V$ such that $\varphi(\cdot) = \langle \cdot, w \rangle$. Moreover, such w must be unique since whenever $\langle \cdot, w \rangle = \langle \cdot, w' \rangle$ on V,

$$\langle v, w - w' \rangle = 0, \quad \forall v \in V \implies \|w - w'\| = 0 \implies w = w'. \qquad \square$$

Note that the proof of Theorem 5.6.1 provides us a explicit construction of the "w" using the formula (5.6.2).

Now we introduce the concept of adjoint operator. Given a linear map $T : V \to V$ we can define a $\varphi \in V^*$ by $\varphi(\cdot) = \langle T(\cdot), u \rangle$. Then there is a unique $w \in V$ such that $\varphi(\cdot) = \langle \cdot, w \rangle$. We note that this $w \in V$ corresponds only to T and u, we denote this w by $T^*(u)$. Therefore, for every $v \in V$ and every (fixed) $u \in V$,

$$\langle Tv, u \rangle = \langle v, T^* u \rangle. \tag{5.6.3}$$

Proposition 5.6.4. *$T^* : V \to V$ defined above is linear.*

Proof. By definition, fix $u, w \in V$, for every $\alpha \in \mathbb{F}$ and $v \in V$, we have

$$\begin{aligned}
\langle v, T^*(u + \alpha w) \rangle &= \langle Tv, u + \alpha w \rangle \\
&= \langle Tv, u \rangle + \overline{\alpha} \langle Tv, w \rangle \\
&= \langle v, T^* u \rangle + \langle v, \alpha T^* w \rangle \\
&= \langle v, T^* u + \alpha T^* w \rangle.
\end{aligned}$$

Therefore $\langle v, T^*(u + \alpha w) - (T^* u + \alpha T^* w) \rangle = 0$ for every $v \in V$, and hence

$$T^*(u + \alpha w) = T^* u + \alpha T^* w. \qquad \square$$

One can easily verify that the linear map from V to V that can satisfy (5.6.3) for all $u, v \in V$ is unique. Therefore we can define the following:

Definition 5.6.5. In an inner product space $(V, \langle \cdot, \cdot \rangle)$ the map $T^* : V \to V$ that corresponds to $T : V \to V$ is called the **adjoint** of T. Namely, $T^* : V \to V$ is the unique linear map such that

$$\langle Tv, u \rangle = \langle v, T^* u \rangle, \quad \text{for all } u, v \in V.$$

Taking adjoint is pretty much the same as taking transpose:

Proposition 5.6.6. *Let $(V, \langle \cdot, \cdot \rangle)$ be an finite dimensional inner product space and $S, T : V \to V$ linear. For $c \in \mathbb{F}$:*

(i) $(T + cS)^* = T^* + \overline{c} S^*$ *(ii)* $(TS)^* = S^* T^*$ *(iii)* $T^{**} = T$

Proof. (i) For every $u, v \in V$,

$$\langle u, (T + cS)^* v \rangle = \langle Tu + cSu, v \rangle = \langle u, T^* v \rangle + \langle u, \overline{c} S^* v \rangle = \langle u, (T^* + \overline{c} S^*) v \rangle.$$

As this is true for every $u \in V$, we have $(T+S)^* = T^* + S^*$.

(ii) It follows similarly.

(iii) We take complex conjugate on both sides of $\langle Tv, u\rangle = \langle v, T^*u\rangle$ to get $\langle u, Tv\rangle = \langle T^*u, v\rangle$, therefore for every $u, v \in V$,

$$\langle u, Tv\rangle = \langle T^*u, v\rangle = \langle u, T^{**}v\rangle. \qquad \square$$

The main property that we need for adjoint operator is (5.6.3). Bearing this property in mind, we go through some computational examples:

Example 5.6.7. Let $A \in M_{n\times n}(\mathbb{F})$, what is L_A^*? Let $x, y \in \mathbb{F}^n$, then

$$\langle x, L_A^* y\rangle = \langle L_A x, y\rangle = \langle Ax, y\rangle = \langle x, A^* y\rangle = \langle x, L_{A^*} y\rangle,$$

therefore $\boxed{L_A^* = L_{A^*}.}$ This shows that the use of the notation * for adjoint operator is consistent with conjugate transpose. Indeed adjoint and conjugate transpose are closely related, we shall see this in Theorem 5.6.9.

Example 5.6.8. Consider the linear operator $T : \mathbb{R}^3 \to \mathbb{R}^3$ given by

$$T(x, y, z)^T = (4x + y, 5y, 6z)^T.$$

What is $T^* : \mathbb{R}^3 \to \mathbb{R}^3$? To find this, let $x, y, z, a, b, c \in \mathbb{R}$, then

$$\begin{aligned}
\langle (x, y, z)^T, T^*(a, b, c)^T\rangle &= \langle T(x, y, z)^T, (a, b, c)^T\rangle \\
&= (4x + y)a + 5yb + 6zc \\
&= x(4a) + y(a + 5b) + z(6c) \\
&= \langle (x, y, z)^T, (4a, a + 5b, 6c)^T\rangle.
\end{aligned}$$

Therefore $T^*(a, b, c)^T = (4a, a + 5b, 6c)^T$.

The computation of T^* in general can be tedious, but this becomes very simple with the help of orthonormal basis.

Theorem 5.6.9. *Let $(V, \langle\cdot,\cdot\rangle)$ be a finite dimensional inner product space. For every orthonormal basis α, we have*

$$[T^*]_\alpha = [T]_\alpha^*.$$

Proof. First of all, given an orthonormal basis α of V, by (ii) of Theorem 5.1.18 for every $u, v \in V$,

$$\langle u, v\rangle = \langle [u]_\alpha, [v]_\alpha\rangle.$$

Therefore for every $x, y \in \mathbb{F}^n$, choose $u, v \in V$ such that $[u]_\alpha = x$ and $[v]_\alpha = y$, then

$$\begin{aligned}
\langle x, [T^*]_\alpha y\rangle &= \langle [u]_\alpha, [T^*]_\alpha [v]_\alpha\rangle \\
&= \langle u, T^* v\rangle \\
&= \langle Tu, v\rangle \\
&= \langle [T]_\alpha x, y\rangle \\
&= \langle x, [T]_\alpha^* y\rangle.
\end{aligned} \tag{5.6.10}$$

As this is true for every $x, y \in \mathbb{F}^n$, we are done. $\square$

Definition 5.6.11. Let $(V, \langle\cdot,\cdot\rangle)$ be a finite dimensional inner product space. A map $T : V \to V$ is said to be **self-adjoint** if $T^* = T$.

We have seen that projection map $P_W : V \to W$ onto a finite dimensional subspace is a self-adjoint linear map. In fact these self-adjoint linear maps can all be obtained from Hermitian matrices:

Theorem 5.6.12. *In a finite dimensional inner product space $(V, \langle\cdot,\cdot\rangle)$, let $T : V \to V$ be linear, the following are equivalent:*

(i) $T : V \to V$ is self-adjoint

(ii) For every orthonormal basis α of V, $[T]_\alpha^* = [T]_\alpha$.

Proof. (i) $\Rightarrow$ (ii) is just a direct application of Theorem 5.6.9. For (ii) $\Rightarrow$ (i) we imitate the computation in (5.6.10). $\square$

For example, every symmetric matrix $A \in M_{n\times n}(\mathbb{R})$ naturally gives a self-adjoint linear map from $\mathbb{R}^n$ to $\mathbb{R}^n$ because by Example 5.6.7,

$$L_A^* = L_{A^*} = L_{A^T} = L_A.$$

Every Hermitian matrix also gives a self-adjoint linear map from $\mathbb{C}^n$ to $\mathbb{C}^n$ due to the same reason. Later we will prove the important result, Spectral Theorem 5.6.19, which asserts that every self-adjoint linear map always has an orthonormal basis consisting of eigenvectors, therefore every symmetric matrix and Hermitian matrix do have a basis consisting of eigenvectors, i.e., they are diagonalizable. The development of this theorem usual starts with the class of normal operators in the next section:

5.6.2 Normal Operators

We start with a brief introduction to normal operator on finite dimensional inner product spaces. This serves as a transition to the proof of Spectral Theorem 5.6.19.

Definition 5.6.13. Let $(V, \langle\cdot,\cdot\rangle)$ be a finite dimensional inner product space. A linear operator $T : V \to V$ is said to be **normal** if

$$TT^* = T^*T.$$

For example, self-adjoint operators and unitary operators are obviously normal. We also define normal matrices due to the following result:

Proposition 5.6.14. *Let $A \in M_{n\times n}(\mathbb{F})$, the induced linear map L_A is normal if and only if $AA^* = A^*A$.*

Proof. This is simply because

$$L_A L_A^* = L_A^* L_A \iff L_A L_{A^*} = L_{A^*} L_A \iff AA^* = A^*A.$$

Here we take matrix representation w.r.t. standard basis in the last $\Leftrightarrow$. $\square$

Definition 5.6.15. A matrix $A \in M_{n\times n}(\mathbb{F})$ is said to be **normal** if

$$AA^* = A^*A.$$

The crucial property of normal operators that we frequently use is: They share the same set of eigenvectors with their adjoint:

Theorem 5.6.16. *Let $(V, \langle\cdot,\cdot\rangle)$ be a finite dimensional inner product space. If T is normal, then for $\lambda \in \mathbb{F}$ and $v \in V$,*

$$Tv = \lambda v \iff T^*v = \overline{\lambda}v.$$

In other words, T and T^* have slightly different eigenvalues and v is an eigenvector of T if and only if v is an eigenvector of T^*.

Proof. Suppose $Tv = \lambda v$, to prove $T^*v = \overline{\lambda}v$, we note that

$$\begin{aligned} T^*v = \overline{\lambda}v &\iff \langle T^*v - \overline{\lambda}v, T^*v - \overline{\lambda}v\rangle = 0 \\ &\iff \big[\langle T^*v, T^*v\rangle - \langle\overline{\lambda}v, T^*v\rangle\big] + \big[\langle\overline{\lambda}v, \overline{\lambda}v\rangle - \langle T^*v, \overline{\lambda}v\rangle\big] = 0. \end{aligned}$$

The last equality holds. Indeed, the first bracket vanishes because

$$\langle\overline{\lambda}v, T^*v\rangle = \langle v, T^*(\lambda v)\rangle = \langle v, T^*Tv\rangle = \langle v, TT^*v\rangle = \langle T^*v, T^*v\rangle.$$

Likewise the second bracket vanishes because

$$\langle\overline{\lambda}v, \overline{\lambda}v\rangle = \langle v, \overline{\lambda}(\lambda v)\rangle = \langle v, \overline{\lambda}Tv\rangle = \langle T^*v, \overline{\lambda}v\rangle.$$ ☐

We end this section with the basic properties of eigenvalues and eigenvectors of a self-adjoint operators.

Theorem 5.6.17. *Let $(V, \langle\cdot,\cdot\rangle)$ be a finite dimensional inner product space. If T is self-adjoint, then:*

(i) All eigenvalues of T are real.

(ii) Eigenvectors corresponding to different eigenvalues of T are orthogonal.

Proof. (i) Let $\lambda \in \mathbb{F}$ and $v \in V$ be nonzero, by Theorem 5.6.16 we have

$$\lambda v = Tv \overset{\text{self-adjoint}}{=\!=\!=} T^*v = \overline{\lambda}v,$$

therefore $(\lambda - \overline{\lambda})v = 0$. As $v \neq 0$, $\lambda - \overline{\lambda} = 0$.

(ii) Let $u, v \in V$ be nonzero and $\lambda_1, \lambda_2 \in \mathbb{F}$ be such that $Tu = \lambda_1 u, Tv = \lambda_2 v$ and $\lambda_1 \neq \lambda_2$. By (i) all eigenvalues are real, therefore $\lambda_i \in \mathbb{R}$, $i = 1, 2$, and hence

$$\lambda_1\langle u, v\rangle = \langle\lambda_1 u, v\rangle = \langle Tu, v\rangle \overset{\text{self-adjoint}}{=\!=\!=} \langle u, Tv\rangle = \langle u, \lambda_2 v\rangle = \lambda_2\langle u, v\rangle,$$

thus $(\lambda_1 - \lambda_2)\langle u, v\rangle = 0$. Since $\lambda_1 \neq \lambda_2$, necessarily $\langle u, v\rangle = 0$. ☐

5.6.3 The Spectral Theorem for Real and Complex Matrices

In this section we establish the existence of "eigenbasis" for several classes of operators on V. It will be made apparent that complex eigenvalue is an indispensable ingredient to the proof even for real vector spaces.

Recall that a subspace W of V is said to be ***T*-invariant** if $T(W) \subseteq W$. We have already used the concept of invariant subspace to decompose an operator in Section 4.3.

Lemma 5.6.18. *Let $(V, \langle\cdot,\cdot\rangle)$ be a finite dimensional inner product space. A subspace W is T-invariant if and only if $W^\perp$ is T^*-invariant.*

Proof. Suppose W is T-invariant, let $v \in W^\perp$, we show that $T^*v \in W^\perp$. Let $u \in W$, then

$$\langle u, T^*v\rangle = \langle Tu, v\rangle = 0,$$

the last equality holds because $Tu \in W$ and $v \in W^\perp$. Therefore $T^*v \in W^\perp$.

Now the converse follows because $T^{**} = T$. □

Theorem 5.6.19 (Spectral). *Let V be a finite dimensional inner product space.*

(i) If $\mathbb{F} = \mathbb{C}$ and $T : V \to V$ is an normal operator, then there is an orthonormal basis consisting of eigenvectors of T.

(ii) If $\mathbb{F} = \mathbb{R}$ and $T : V \to V$ is self-adjoint operator, then there is an orthonormal basis consisting of eigenvectors of T.

Proof. (i) We will prove by induction on $\dim V$. When $\dim V = 1$, the normalized nonzero vector in V will do. Suppose now the statement holds for every complex inner product space with dimensional less than $k := \dim V$.

By Lemma 5.6.20 below there is nonzero $w_1 \in V$ such that $Tv = \lambda w_1$, for some $\lambda \in \mathbb{C}$. Let $W = \operatorname{span}\{w_1\}$, as W is T-invariant, $W^\perp$ is T^* invariant by Lemma 5.6.18. Since

$$T^*|_{W^\perp} : W^\perp \to W^\perp$$

is normal (why?), by induction hypothesis there is an orthonormal basis $\{w_2, w_3, \ldots, w_{k-1}\}$ of $W^\perp$ consisting of eigenvectors of T^*. Since T is normal, by Theorem 5.6.16 $w_2, \ldots, w_k$ are eigenvectors of T.

(ii) We first show that T must have at least one eigenvector. Let α be an orthonormal basis of V, let $A = [T]_\alpha \in M_{n\times n}(\mathbb{R})$ which is symmetric by Theorem 5.6.9.

Claim. *Every symmetric matrix $S \in M_{n\times n}(\mathbb{R})$ has real eignevalues.*

Proof of the Claim. Consider S as a vector in $M_{n\times n}(\mathbb{C})$, then $\det(S - xI)$ has a root $\lambda \in \mathbb{C}$, so $L_S : \mathbb{C}^n \to \mathbb{C}^n$ has eigenvalue λ. Since L_S is self-adjoint (recall Example 5.6.7), λ must be real by Theorem 5.6.17. □

By the claim there is an eigenvalue $\lambda \in \mathbb{R}$ of A, so there is nonzero $x \in \mathbb{R}^n$ such that $Ax = \lambda x$. If we let $v \in V$ be such that $[v]_\alpha = x$, then $Tv = \lambda v$. Hence we have shown that every self-adjoint operator on real vector space[¶] has an eigenvector with real eigenvalue.

Up to this point we can repeat the argument in the second paragraph of (i) to finish the proof since T is normal, T and T^* share the same set of eigenvectors. $\square$

Lemma 5.6.20. *Let V be a finite dimensional complex vector space. Every linear operator $T : V \to V$ has at least one eigenvalue.*

Proof. Choose a basis α of V and consider the matrix $A = [T]_\alpha$, by Corollary 4.1.3 there is at least one eigenvalue $\lambda \in \mathbb{C}$, therefore $[T]_\alpha x = \lambda x$ for some nonzero $x \in \mathbb{C}^n$. Choose $v \in V \setminus \{0\}$ such that $[v]_\alpha = x$, then $Tv = \lambda v$. $\square$

For the next immediate corollary, we introduce the following terminology.

(i) We say that a matrix $A \in M_{n\times n}(\mathbb{R})$ is **orthogonally diagonalizable** if there is an orthogonal matrix $P \in M_{n\times n}(\mathbb{R})$ (i.e., $P^T P = I$) such that $P^T AP$ is diagonal.

(ii) We also say that a matrix $A \in M_{n\times n}(\mathbb{C})$ is **unitarily diagonalizable** if there is an unitary matrix $U \in M_{n\times n}(\mathbb{C})$ (i.e., $U^*U = I$) such that U^*AU is diagonal.

Theorem 5.6.19 tells us:

Corollary 5.6.21.

(i) Symmetric real matrices are orthogonally diagonalizable.

(ii) Hermitian complex matrices are unitarily diagonalizable with only real eigenvalues.

(iii) Unitary Matrices are unitarily diagonalizable.

Proof. Given a matrix $A \in M_{n\times n}(\mathbb{F})$, apply the Spectral Theorem 5.6.19 to L_A in each part. $\square$

If you want to solve the following on your own, please ignore the solution here for the moment and try to think about it first.

Example 5.6.22 (HKUST UG Math Competition Senior Level). Let A and B be 3×2 and 2×3 matrices respectively. If

$$AB = \begin{bmatrix} 8 & 2 & -2 \\ 2 & 5 & 4 \\ -2 & 4 & 5 \end{bmatrix},$$

then determine the rank of AB and determine all possible answers of BA.

Solution. Since AB is symmetric, by Corollary 5.6.21 we know that AB is diagonalizable. To find the rank, we may find all out all eigenvectors first.

Since $\det(AB - \lambda I) = -\lambda(\lambda - 9)^2$, the only eigenvalues are 0 and 9.

For $\lambda = 0$: The AM is 1 and thus the GM is also 1.

[¶] Actually with the same argument, every self-adjoint operator on $(V, \langle\cdot,\cdot\rangle)$ over $\mathbb{F}$ has a real eigenvalue.

For $\lambda = 9$: The AM is 2. However, AB is symmetric, it is diagonalizable, thus GM must also be 2.

Hence there are linearly independent eigenvectors v_1, v_2, v_3 of AB such that $ABv_1 = 0, ABv_2 = 9v_2$ and $ABv_3 = 9v_3$. Thus $\boxed{\operatorname{rank}(AB) = 2}$ and it follows that

$$BA(Bv_2) = 9Bv_2 \quad \text{and} \quad BA(Bv_3) = 9Bv_3.$$

Note that Bv_2 and Bv_3 are linearly independent since

$$xBv_2 + yBv_3 = 0 \implies xABv_2 + yABv_3 = 0 \implies 9xv_2 + 9yv_3 = 0 \implies x = y = 0.$$

Let $P = [Bv_2 \quad Bv_3]$, then

$$P^{-1}(BA)P = \begin{bmatrix} 9 & 0 \\ 0 & 9 \end{bmatrix} \implies BA = P(9I)P^{-1} = 9I,$$

where I is a 2×2 identity matrix.

Another linear algebra problem from the HKUST UG Math Competition is presented in Problem 5.8. You may take a look ☺.

5.7 Sylvester's Criterion for Positive Definiteness

In this section we focus on real symmetric matrices. Recall that from Definition 5.1.3 a matrix is said to be positive definite if it is symmetric and $x^T Ax > 0$ for all $x \neq 0$, moreover, by Corollary 5.6.21 all symmetric matrices are orthogonally diagonalizable.

Theorem 5.7.1. *A real symmetric matrix is positive definite if and only if all its eigenvalues are positive.*

Proof. Let $A \in M_{n\times n}(\mathbb{R})$ be symmetric and let $v_1, v_2, \ldots, v_n$ be orthonormal eigenvectors of A with $Av_i = \lambda_i v_i$, for some $\lambda_i \in \mathbb{R}$.

($\Rightarrow$) Suppose A is positive definite. Since $Av_i = \lambda_i v_i$, taking v_i^T on both sides,

$$0 < v_i^T Av_i = \lambda_i \|v_i\|^2 \implies \lambda_i > 0.$$

($\Leftarrow$) Suppose all eigenvalues are positive, then for $x = \sum_{i=1}^n a_i v_i \neq 0$,

$$x^T Ax = \sum_{i=1}^n \sum_{j=1}^n a_i a_j v_i^T Av_j = \sum_{i=1}^n \sum_{j=1}^n \lambda_j a_i a_j v_i^T v_j = \sum_{i=1}^n \lambda_i a_i^2 > 0. \qquad \square$$

Therefore to prove a symmetric is positive definite, it is sufficient (and also necessary) to show all of its eigenvalues are positive. We end this section by discussing the nice computational criterion for positive definiteness.

Theorem 5.7.2 (Sylvester's Criterion). *Let $A = [a_{ij}]_{n\times n}$ be real symmetric. Then A is positive definite if and only if*

$$\det[a_{ij}]_{1\times 1}, \quad \det[a_{ij}]_{2\times 2}, \quad \ldots, \quad \det[a_{ij}]_{n\times n} > 0.$$

The scalar $\det[a_{ij}]_{k\times k}$ is called the **kth principal minor** of A. Note that the assumption that A is symmetric doesn't affect its applicability since ALL quadratic polynomial in n variables can be rearranged to have "symmetric coefficients" (we demonstrate this in Example 5.9.3).

Proof of ($\Rightarrow$) of Theorem 5.7.2. This is simple because if we let

$$x = (x_1, x_2, \dots, x_k, 0, \dots, 0)^T = (\tilde{x}^T, 0, \dots, 0)^T, \quad \tilde{x} \in \mathbb{R}^k,$$

then

$$x^T A x = \sum_{i=1}^k \sum_{j=1}^k x_i x_j (e_i^T A e_j) = \sum_{i=1}^k \sum_{j=1}^k x_i x_j a_{ij} = \tilde{x}^T [a_{ij}]_{k\times k} \tilde{x}, \tag{5.7.3}$$

this shows us $A_k := [a_{ij}]_{k\times k}$ is symmetric and positive definite. By Theorem 5.7.1 all eigenvalues of A_k are positive. Since $\det A_k$ is the product of all eigenvalues of A_k, $\det A_k > 0$. ☐

Our proof to ($\Leftarrow$) direction of Theorem 5.7.2 will be adapted from George T. Gilbert, *Positive Definite Matrices and Sylvester's Criterion*, The American Mathematical Monthly, Vol. 98, No. 1, Jan., 1991, which proceeds with the following lemma:

Lemma 5.7.4. *Let $A \in M_{n\times n}(\mathbb{R})$ be a symmetric matrix. If there is a k dimensional subspace W of $\mathbb{R}^n$ such that $w^T A w > 0$ for every $w \in W \setminus \{0\}$, then A has at least k positive eigenvalues.*

Proof. Let $v_1, v_2, \dots, v_n$ be eigenvectors of A with $Av_i = \lambda_i v_i$, for some $\lambda_i \in \mathbb{R}$ (which always exists since A is symmetric). Relabelling if necessary, we assume

$$\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n.$$

If $\operatorname{span}\{v_n, v_{n-1}, \dots, v_{m+1}\}$ is too large (i.e., when m is too small), then it must intersect W nontrivially. Specifically, whenever $(n-m)+k > n$ (iff $k > m$), then Example 2.7.10 tells us

$$\operatorname{span}\{v_n, v_{n-1}, \dots, v_{m+1}\} \cap W \ne \{0\},$$

therefore there is $a_i \in \mathbb{R}$ such that $w = \sum_{i=m+1}^n a_i v_i \in W \setminus \{0\}$ and

$$0 < w^T A w = \sum_{i=m+1}^n \lambda_i a_i^2 \le \lambda_{m+1} \sum_{i=m+1}^n a_i^2.$$

Now necessarily $\lambda_{m+1} > 0$, i.e., $\lambda_1, \lambda_2, \dots, \lambda_{m+1} > 0$, we take $m = k-1$ to finish the proof. ☐

Proof of ($\Leftarrow$) of Theorem 5.7.2. We prove by induction on n, the case that $n = 1$ is trivial. Suppose now every $(n-1)\times(n-1)$ symmetric matrix with all principal minors positive is positive definite.

Let $A \in M_{n\times n}(\mathbb{R})$ be symmetric and have all principal minors positive, for every $x = (\tilde{x}^T, 0)^T$, $\tilde{x} \in \mathbb{R}^{n-1}$, one has

$$x^T A x = \tilde{x}^T \big([a_{ij}]_{(n-1)\times(n-1)}\big)\tilde{x}$$

from the computation in (5.7.3). By induction hypothesis, $[a_{ij}]_{(n-1)\times(n-1)}$ is positive definiteness, hence $x^T Ax > 0$ for all $x \in W = \{(\tilde{x}, 0) : \tilde{x} \in \mathbb{R}^{n-1}\}$. By Lemma 5.7.4, A has at least $n-1$ positive eigenvalues. Since $\det A > 0$, the remaining eigenvalue must be positive. □

If we examine every proof carefully, in each of the results when the word *real symmetric* is replaced by *Hermitian* and when $\mathbb{R}$ is replaced by $\mathbb{C}$, we find that nothing in the proof can go wrong. Therefore as a direct consequence of the proof we have:

Theorem 5.7.5 (Sylvester's Criterion). *Let $A = [a_{ij}]_{n\times n}$ be Hermitian. Then A is positive definite if and only if*

$$\det[a_{ij}]_{1\times 1}, \quad \det[a_{ij}]_{2\times 2}, \quad \dots, \quad \det[a_{ij}]_{n\times n} > 0.$$

5.8 Polar Decomposition

5.8.1 Positive Matrices and Unique Positive Square Root

In this section every matrix A such that $\langle Ax, x\rangle \geq 0$ for every x will be called a **positive matrix**. Since the Sylevester's Criterion work for real and complex matrices, in this section we pay all of our effort to $\mathbb{C}^n$, the complex Hilbert space. The notation $\langle x, y\rangle = y^*x$ will always denote the standard inner product on $\mathbb{C}^n$ which is conjugate linear in the second variable.

The first reason we stick with complex Hilbert spaces is due to the following result:

Theorem 5.8.1. *Let A be a matrix in $M_{n\times n}(\mathbb{C})$. If A is positive, i.e., if $\langle Ax, x\rangle \geq 0$ for every $x \in \mathbb{C}^n$, then A is self-adjoint.*

It is worth noting that the proof of below (including the claim) carries over to the general case when $\mathbb{C}^n$ is replaced by any complex Hilbert space H and A is replaced by any positive operator $T : H \to H$. Also note that positive matrices can be singular, they may not be positive definite.

Proof. First of all we claim that:

Claim. *If $\langle Ax, x\rangle = 0$ for every $x \in \mathbb{C}^n$, then $A = 0$.*

Proof. It follows from the following computations: For every $x, y \in \mathbb{C}^n$,

$$0 = \langle (A(x + iy), x + iy\rangle = -i\langle Ax, y\rangle + i\langle Ay, x\rangle$$

and

$$0 = \langle A(x + y), x + y\rangle = \langle Ax, y\rangle + \langle Ay, x\rangle,$$

therefore we have $\langle Ax, y\rangle = 0$ for every x, y. In paricular, $Ax = 0$ for every $x \in \mathbb{C}^n$.□

Now it is given that $\langle Ax, x\rangle \geq 0$, therefore $\langle Ax, x\rangle = \overline{\langle Ax, x\rangle} = \langle x, Ax\rangle = \langle A^*x, x\rangle$, and therefore $\langle (A - A^*)x, x\rangle = 0$ for every $x \in \mathbb{C}^n$. Now by the claim we are done. □

The following is an immediate application of Spectral Theorem:

Theorem 5.8.2. *Every positive matrix A has a unique positive matrix S such that $A = S^2$. We call S the positive square root of A.*

Proof. We show the existence first. By Theorem 5.8.1 A is self-adjoint, hence by Spectral Theorem in the previous section, $P^{-1}AP = D$ for some P invertible and some D diagonal. Since A is nonnegative definite, $D = \operatorname{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$, where $\lambda_i \geq 0$ for all i. If we define $D^{1/2} = \operatorname{diag}(\lambda_1^{1/2}, \lambda_2^{1/2}, \dots, \lambda_n^{1/2})$, then

$$S := PD^{1/2}P^{-1}$$

satisfies $S^2 = PDP^{-1} = A$, and of course S itself is positive.

As for uniqueness, let's still denote S a positive square root of A. Since T is self-adjoint, there are $\lambda_1, \dots, \lambda_k$ such that

$$\mathbb{C}^n = \bigoplus_{i=1}^{k} \ker(T - \lambda_i I).$$

Again by Spectral Theorem S is also diagonalizable, let $v \in \ker(S - \lambda I)$, then $Sv = \lambda v$ and thus $Tv = \lambda^2 v$, therefore $\lambda = \sqrt{\lambda_i}$ for some i. Moreover, since S is self-adjoint and since $\ker(S - \sqrt{\lambda_i} I) \subseteq \ker(T - \lambda_i I)$ for each i, this set inclusion cannot be proper due to the direct sum above, we conclude $\ker(S - \sqrt{\lambda_i} I) = \ker(T - \lambda_i I)$ for each i. Which means that $Sv = \sqrt{\lambda_i} v$ for $v \in \ker(T - \lambda_i I)$, S is uniquely determined. $\square$

Now we can discuss the main theorem of this section:

Theorem 5.8.3 (Polar Decomposition). *Let A be an $n \times n$ matrix over $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, then there is a unitary (orthogonal when $\mathbb{F} = \mathbb{R}$) matrix U and a positive matrix $P \in M_{n\times n}(\mathbb{F})$ such that*

$$A = UP,$$

where $P = \sqrt{A^*A}$, the unique positive square root of the positive matrix A^*A.

Proof. First we observe that

$$\|\sqrt{A^*A}x\|^2 = \langle \sqrt{A^*A}x, \sqrt{A^*A}x \rangle = \langle x, A^*Ax \rangle = \langle Ax, Ax \rangle = \|Ax\|^2,$$

therefore $\|\sqrt{A^*A}x\| = \|Ax\|$. Now we define an isometry:

$$S_1 : \operatorname{range} \sqrt{A^*A} \to \operatorname{range} A; \quad \sqrt{A^*A}x \mapsto Ax,$$

this map is automatically well-defined since it preserves norm. Namely, if $\sqrt{A^*A}x = \sqrt{A^*A}y$, then

$$\|\sqrt{A^*A}(x - y)\| = \|A(x - y)\| = 0,$$

so $Ax = Ay$.

Now if we can extend S_1 to a unitary operator S on $\mathbb{F}^n$, then we will have for every $x \in \mathbb{F}^n$,

$$S(\sqrt{A^*A}x) = S_1(\sqrt{A^*A}x) = Ax,$$

and we will be done. Since S_1 is injective, $\dim \operatorname{range} \sqrt{A^*A} = \dim \operatorname{range} S_1$ necessarily. We let $\{u_1, \dots, u_k\}$ be an orthonormal basis of $(\operatorname{range} \sqrt{A^*A})^\perp$ and $\{v_1, \dots, v_k\}$ be that of $(\operatorname{range} S_1)^\perp$. We now define

$$S_2 : (\operatorname{range} \sqrt{A^*A})^\perp \to (\operatorname{range} S_1)^\perp; \quad a_1u_1 + \cdots + a_ku_k \mapsto a_1v_1 + \cdots + a_kv_k.$$

Finally we define $S = S_1 \oplus S_2$. It is a direct verification that S preserves length: for $u \in \operatorname{dom} S_1$ and $v \in \operatorname{dom} S_2$, we have

$$\|S(u+v)\|^2 = \|Su + Sv\|^2 = \|S_1u + S_2v\|^2 = \|S_1u\|^2 + \|S_2v\|^2,$$

since $u = \sqrt{A^*A}x$ for some $x \in \mathbb{F}^n$ and $\|S_2v\| = \|v\|$, we have

$$\begin{aligned}\|S(u+v)\|^2 &= \|S_1(A^*Ax)\|^2 + \|v\|^2 = \|Ax\|^2 + \|v\|^2 \\ &= \|\sqrt{A^*A}x\|^2 + \|v\|^2 \\ &= \|u\|^2 + \|v\|^2 = \|u+v\|^2,\end{aligned}$$

as desired. Since preserving length is the same as preserving inner product, thus S must be unitary. □

For every $n \times n$ matrix A, the matrix $\sqrt{A^*A}$ is often called the positive part of A. Since it is analogues to decomposition of complex numbers that $z = e^{i\theta}|z|$, it is also common to denote $|A| = \sqrt{A^*A}$, therefore for every matrix A, there is a unitary matrix U such that $A = U|A|$. With this notation, it can be easily checked that a matrix is normal if and only if $|A| = |A^*|$ (set $A = UP$, say).

5.8.2 Second Proof of Singular Value Decomposition

In the following let's give a second proof of Singular Value Decomposition shown in Section 4.2. The proof below will not include the uniqueness of left and right singular vectors—which has been done in Section 4.2.

Theorem 5.8.4. *Every matrix $A \in M_{m\times n}(\mathbb{C})$ has a SVD:*

$$A = U\Sigma V^* \qquad \boxed{\begin{array}{ll} U \in M_{m\times m}(\mathbb{C}) & \textit{is unitary} \\ V \in M_{n\times n}(\mathbb{C}) & \textit{is unitary} \\ \Sigma \in M_{m\times n}(\mathbb{R}) & \textit{is “diagonal”} \end{array}}$$

Furthermore, the singular values σ_j's, $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_{\min\{m,n\}}$, are uniquely determined.

Proof. Let A be any $n \times n$ matrix over $\mathbb{F}$ first, then $A = S|A|$ for some unitary (orthogonal when $\mathbb{F} = \mathbb{R}$) matrix S. We may assume $A \neq 0$, since $|A|$ is positive definite, by Spectral Theorem there is a unitary matrix (orthogonal when $\mathbb{F} = \mathbb{R}$) V and diagonal Σ such that

$$A = S[V\Sigma V^*] = (SV)\Sigma V^* = U\Sigma V^*,$$

where $U = SV$ is unitary (orthogonal when $\mathbb{F} = \mathbb{R}$). We can further arrange columns of V such that $\Sigma = \operatorname{diag}(\sigma_1, \dots, \sigma_n)$ with $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n \geq 0$. They are unique since they are eigenvalues of the unique square root of $\sqrt{A^*A}$.

Now suppose that A is an $m \times n$ matrix. In order not to insert "(orthogonal when $\mathbb{F} = \mathbb{R}$)" everytime, let's use the term $\mathbb{F}$-unitary with obvious meaning.

W.l.o.g. let's assume $m > n$ (otherwise consider A^T). Extend A to a square by adjoining it an $m \times (m-n)$ 0 matrix O, then by what we have just proved there are $m \times m$ dimensional $\mathbb{F}$-unitary matrices U and V such that

$$\begin{bmatrix} A & O \end{bmatrix} = U \Sigma V^*, \tag{5.8.5}$$

where $\Sigma = \operatorname{diag}(\sigma_1, \ldots, \sigma_m)$ with $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_m \geq 0$. Note that Σ is uniquely corresponded to $\begin{bmatrix} A & O \end{bmatrix}$.

By our definition, for every $i > n$,

$$0 = U \Sigma V^* e_i = U \left(\sum_{k=1}^{m} \sigma_k e_k v_k^*(e_i) \right),$$

since U is invertible, we have

$$\sigma_k v_k^*(e_i) = 0 \text{ for each } k = 1, 2, \ldots, m \text{ and for each } i > n.$$

In particular, if $\operatorname{rank} A = r$, then $\sigma_{r+1} = 0$ (and then $\sigma_i = 0$ for every $i > r$), and we then have $v_k^*(e_i) = 0$ for every $k = 1, 2, \ldots, r$ and $i > n$. In other words,

$$v_1, \ldots v_r \in \mathbb{F}^n \times \{0_{m-n}\}. \tag{5.8.6}$$

Now multiplying both sides of (5.8.5) by $\begin{bmatrix} I_{n \times n} \\ O \end{bmatrix}$, we have

$$A = U \Sigma V_{m \times n}^*,$$

where $V_{m \times n}^*$ is the left $m \times n$ part of the matrix V^*. Denote $D = \operatorname{diag}(\sigma_1, \ldots, \sigma_n)$—the upper left $n \times n$ part of Σ, then

$$A = U \begin{bmatrix} D & O_{n,m-n} \\ O_{m-n,n} & O_{m-n,m-n} \end{bmatrix} V_{m \times n}^* = U \begin{bmatrix} D V_{n \times n}^* \\ O_{m-n,n} \end{bmatrix} = U \begin{bmatrix} D \\ O \end{bmatrix} V_{n \times n}^*,$$

where $V_{n \times n}^*$ denotes the upper left $n \times n$ part of V^*.

We are almost there, except the fact that $V_{n \times n}^*$ is not necessarily $\mathbb{F}$-unitrary. But we can always rearrange V, if necessary, to achieve this. For this, let's study the term $D V_{n \times n}^*$.

Since $\sigma_i = 0$ for $i > r$, we have

$$D V_{n \times n}^* = \begin{bmatrix} \sigma_1 v_1'^* \\ \vdots \\ \sigma_r v_r'^* \\ 0 \cdot v_{r+1}'^* \\ \vdots \\ 0 \cdot v_n'^* \end{bmatrix},$$

where v' means the first n coordinates of $v \in \mathbb{F}^m$. We may replace $v_{r+1}, \ldots, v_n \in \mathbb{F}^m$ freely such that $v_1, \ldots, v_n$ form an orthogonal basis of $\mathbb{F}^n \times \{0_{m-n}\}$ (recall (5.8.6)) without changing $D V_{n \times n}^*$, thus we may assume $V_{n \times n}^*$ itself is $\mathbb{F}$-unitary, and we are done. $\square$

5.9 Quadratic Forms

5.9.1 Definitions and Examples

Definition 5.9.1. Quadratic forms are homogeneous quadratic polynomials in n variables.

In general quadratic form in n variables takes the following form: for $x = (x_1, x_2, \ldots, x_n)^T$,

$$Q(x) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i a_{ij} x_j, \tag{5.9.2}$$

for some $a_{ij} \in \mathbb{R}$, $i, j = 1, 2, \ldots, n$. If we define $A = [a_{ij}]_{n \times n}$, a careful verification shows that

$$Q(x) = x^T A x.$$

Note that a_{ij}'s can always be arranged such that A is symmetric, thus every quadratic form gives us a symmetric form

$$B(x, y) = x^T A y,$$

where $x, y \in \mathbb{R}^n$. Note that when A is positive-definite, then B becomes an inner product. We have a nice criterion to determine positive definiteness in Theorem 5.7.2.

In application we need to get used to the way to arrange those coefficients into a symmetric matrix.

Example 5.9.3. Wr try to identify the conics represented by

$$2x^2 - 4xy + 5y^2 = 1. \tag{5.9.4}$$

We expect it is an ellipse. In view of (5.9.2), we see that the ith variable on the left corresponds to the ith row of our desired matrix:

$$2x^2 - 4xy + 5y^2 = \begin{matrix} 2xx - 2xy \\ -2yx + 5yy \end{matrix}$$

Note the coefficient of xy is divided by half so that the coefficients of xy and yx are equal, thus we get

$$2x^2 - 4xy + 5y^2 = [x \quad y] \underbrace{\begin{bmatrix} 2 & -2 \\ -2 & 5 \end{bmatrix}}_{:=A} \begin{bmatrix} x \\ y \end{bmatrix} = u^T A u, \tag{5.9.5}$$

where $u = (x, y)^T$. Now we will diagonalize A in order to get rid of all the cross terms.

Step 1 (Find all eigenvalues and eigenvectors). By direct computation, $p_A(t) = (t-6)(t-1)$, hence A is diagonalizable as there are enough eigenvectors.

When $t = 6$, the system $(A - 6I)v = 0$ gives $v = v_1(1, -2)^T$. When $t = 1$, the system $(A - I)v = 0$ gives $v = v_2(2, 1)^T$.

Step 2 (Orthogonalize eigenvectors to get an orthogonal matrix). Luckly $(1, -2)^T$ and $(2, 1)^T$ are already orthogonal. We divide them by their lengths to get orthonormal set, then

$$P = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}$$

is orthogonal, i.e., $P^T P = I$. We quickly see why we prefer orthogonality.

Step 3 (Simplify the quadratic form). Continuing from (5.9.5):

$$2x^2 - 4xy + 5y^2 = u^T A u = u^T \left(P \begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix} P^{-1} \right) u = (P^T u)^T \begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix} P^T u.$$

Let $P^T(x, y)^T = (x', y')^T$, then (5.9.4) becomes

$$\left(\frac{x'}{\frac{1}{\sqrt{6}}} \right)^2 + \left(\frac{y'}{1} \right)^2 = 1.$$

So (5.9.4) is an ellipse with major semi-axis of length 1 and minor semi-axis of length $1/\sqrt{6}$. The reason we require P be orthogonal is: our strategy is to "rotate" the coordinate axis in order to identify what the (5.9.4) represents, orthogonal matrices are indeed rotations!

5.9.2 Application of Quadratic Forms to Multivariable Second Derivative Test

Suppose f is defined near $a \in \mathbb{R}^n$ such that f has second order derivatives near at a. When f is nice enough, we expect the following approximation

$$T(x) = f(a) + \sum_{i=1}^n \frac{\partial f}{\partial x_i}(a)(x_i - a_i) + \frac{1}{2!} \sum_{i,j=1}^n \left(\frac{\partial^2 f}{\partial x_i \partial x_j}(a) \right) (x_i - a_i)(x_j - a_j)$$

is a second order approximation of f at a, i.e., we should have

$$\lim_{x \to a} \frac{|f(x) - T(x)|}{\|x - a\|^2} = 0.$$

To express the quadratic approximation neatly let's define **Hessian matrix** of f at a by

$$H_f(a) = \begin{bmatrix} \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \, \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_1 \, \partial x_n} \\ \frac{\partial^2 f}{\partial x_2 \, \partial x_1} & \frac{\partial^2 f}{\partial x_2^2} & \cdots & \frac{\partial^2 f}{\partial x_2 \, \partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_n \, \partial x_1} & \frac{\partial^2 f}{\partial x_n \, \partial x_2} & \cdots & \frac{\partial^2 f}{\partial x_n^2} \end{bmatrix} (a).$$

Therefore the quadratic approximation can be neatly written as

$$T(x) = f(a) + \nabla f(a) \cdot (x - a) + \frac{1}{2}(x - a)^T H_f(a)(x - a).$$

When a is a critical point, the quadratic approximation becomes

$$T(x) = f(a) + \frac{1}{2}(x - a)^T H_f(a)(x - a),$$

hence the study of maximality and minimality of $f(a)$ is the same as the study of positive definiteness of the quadratic form

$$h_a(x) = (x - a)^T H_f(a)(x - a).$$

Whom we have very good answer when $H_f(a)$ is a symmetric matrix. Therefore to apply the knowledge of linear algebra that we have developed we need to provide good sufficient conditions to make sure:

- $\dfrac{\partial^2 f}{\partial x_i \partial x_j}(a) = \dfrac{\partial^2 f}{\partial x_j \partial x_i}(a)$ for all $i, j = 1, 2, \ldots, n$;
- $T(x) := f(a) + \nabla f(a) \cdot (c-a) + \dfrac{1}{2}(x-a)^T H_f(a)(x-a)$ is a second order approximation.

For this, let's recall those standard results from multivariable calculus without proof. For simplicity let's denote

$$f_{x_i x_j} = \frac{\partial^2 f}{\partial x_j \partial x_i}.$$

Theorem 5.9.6. *Suppose $f(x, y)$ has first order partial derivatives near (x_0, y_0). If f_x and f_y are differentiable at (x_0, y_0), then*

$$f_{xy}(x_0, y_0) = f_{yx}(x_0, y_0).$$

To get second order approximation we further require those first order partial derivatives be continuous.

Theorem 5.9.7. *Suppose $f(x_1, x_2, \ldots, x_n)$ has continuous first order partial derivatives near a. If f_{x_i}'s are differentiable at a, then the quadratic approximation is a second order approximation in the sense that*

$$\lim_{x \to a} \frac{\left| f(x) - \left(f(a) + \nabla f(a) \cdot (x-a) + \frac{1}{2}(x-a)^T H_f(a)(x-a) \right) \right|}{\|x-a\|^2} = 0.$$

We summarize our discussion as a theorem.

Theorem 5.9.8. *Suppose $f(x_1, x_2, \ldots, x_n)$ has continuous first order partial derivatives near a and f_{x_i}'s are differentiable at a. Then $H_f(a)$ is symmetric and if $\nabla f(a) = 0$,*

*(i) $H_f(a)$ is **positive definite** $\implies$ $f(a)$ is a **local minimum**.*

*(ii) $H_f(a)$ is **negative definite** $\implies$ $f(a)$ is a **local maximum**.*

Remark. In application to apply Theorem 5.9.8 the minimal requirement that f_{x_i}'s are differentiable at a is usually replaced by a stronger condition that *all* second order partial derivatives are continuous at a.

5.10 Exercises

Inner Products

Problem 5.1. Show that $\langle A, B \rangle := \operatorname{Tr}(B^T A)$ defines an inner product on $M_{m \times n}(\mathbb{R})$ (recall Problem 1.4).

Problem 5.2. Use Cauchy-Schwarz inequality to prove that for all $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$,

$$\left(\sum_{k=1}^n a_k b_k \right)^2 \leq \left(\sum_{k=1}^n k a_k^2 \right)^2 \left(\sum_{k=1}^n \frac{b_k^2}{k} \right)^2.$$

Problem 5.3. Use Cauchy-Schwarz inequality to prove that all roots of $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ lie in the open disk

$$\{z \in \mathbb{C} : |z| < \sqrt{1 + |a_{n-1}|^2 + \cdots + |a_1|^2 + |a_0|^2}\}.$$

Problem 5.4. Let V be finite dimensional inner product space, prove that

$$\langle u, v\rangle = 0 \iff \|u\| \le \|u + \alpha v\|, \quad \text{for all } \alpha \in \mathbb{R}.$$

Problem 5.5. Let $A \in M_{n\times n}(\mathbb{R})$ be symmetric such that

$$A^3 - 3A^2 + 5A - 3I = 0.$$

Prove that A is positive definite. You may need to know Theorem 5.6.19.

Problem 5.6. Let $(\cdot,\cdot)$ be another inner product on $\mathbb{R}^n$ (with $\langle\cdot,\cdot\rangle$ denoting the dot product).

(i) Show that there is an invertible matrix $S \in M_{n\times n}(\mathbb{R})$ such that

$$(u, v) = \langle Su, Sv\rangle, \quad \text{for all } u, v \in \mathbb{R}^n.$$

This characterizes all possible inner products on $\mathbb{R}^n$.

(ii) From this, also prove that whenever A is positive definite, there is an invertible P such that $A = P^T P$.

Problem 5.7. Let $A, B \in M_{n\times n}(\mathbb{R})$ be positive definite, show that $\mathrm{Tr}(AB) \ge 0$.

Hint. What properties of positive definite matrices do we have? See Problem 5.6.

Problem 5.8 (HKUST UG Math Competition Junior Level).
Let H be an inner product space. Let n be a positive integer less than the dimension of H. If V and E are n and $n-1$ dimensional subspaces of H respectively, prove that there exists a nonzero $v \in V$ orthogonal to every $x \in E$.

Remark. The vector space H is possibly infinite dimensional.

Orthogonal Complement and Orthogonal Projection

Problem 5.9. Let V be an inner product space and W its subspace, show that

$$W \subseteq (W^\perp)^\perp.$$

Explain why $(W^\perp)^\perp = W$ when W is finite dimensional. Don't try to make the assumption that $\dim V < \infty$.

Problem 5.10. Let $A \in M_{n\times n}(\mathbb{R})$ be such that $A^2 = A$. Prove that the following are equivalent:

(i) A is an orthogonal projection (i.e., $\mathrm{Nul}\, A \perp \mathrm{Col}\, A$).

(ii) A is symmetric (i.e., $A^T = A$).

Problem 5.11. Let $A \in M_{m\times n}(\mathbb{R})$, prove that A is injective $\iff$ A^T is surjective.

Problem 5.12. Let U be a finite dimensional subspace of an inner product space V, show that

$$\dim U^\perp = \dim V - \dim U.$$

Problem 5.13. Let $\{v_1, v_2, \dots, v_n\}$ be any set of vector in $\mathbb{R}^n$. Show that for any $\epsilon > 0$, there is a basis $(u_1, u_2, \dots, u_n)$ of $\mathbb{R}^n$ such that

$$\|v_i - u_i\| < \epsilon, \quad i = 1, 2, \dots, n.$$

Problem 5.14. Show the **Bessel's Inequality**: let $\{v_1, v_2, \dots, v_n\}$ be an orthonormal set in an inner product space V, show that for every $v \in V$,

$$\sum_{i=1}^{n} |\langle v, v_i\rangle|^2 \leq \|v\|^2.$$

Problem 5.15. Find a polynomial $q \in \mathbb{P}_2(\mathbb{R})$ such that

$$\int_0^1 p(x)\cos(\pi x)\,dx = \int_0^1 p(x)q(x)\,dx$$

for every $p \in \mathbb{P}_2$.

Problem 5.16. Find $p_0 \in \mathbb{P}_5(\mathbb{R})$ that makes

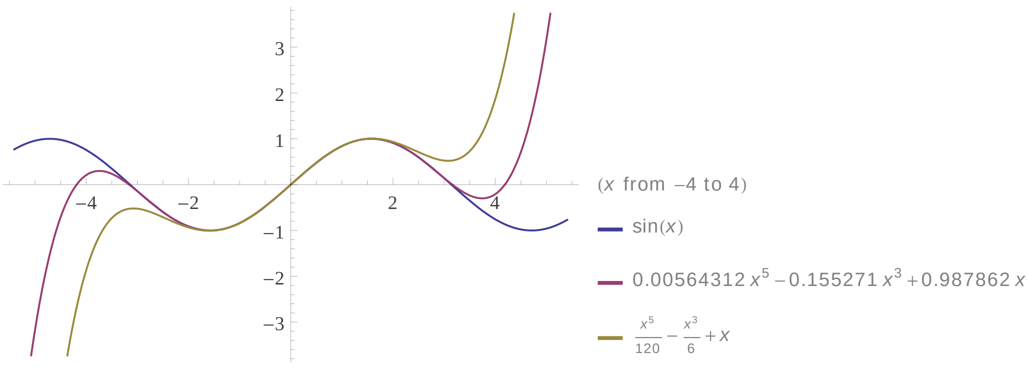
$$\int_{-\pi}^{\pi} (\sin x - p(x))^2\,dx$$

as small as possible. Don't do it by hands, use any software which can perform symbolic computation.

Answer:

$$p_0(x) = \begin{aligned}&\left(\frac{693}{8\pi^6} - \frac{72765}{8\pi^8} + \frac{654885}{8\pi^{10}}\right)x^5 + \left(\frac{39375}{4\pi^6} - \frac{315}{4\pi^6} - \frac{363825}{4\pi^8}\right)x^3 \\ &+ \left(\frac{105}{8\pi^2} - \frac{16065}{8\pi^4} + \frac{155925}{8\pi^6}\right)x\end{aligned}$$

Remark. Interestingly, among degree 5 polynomials p_0 gives a very good approximation of $\sin x$ on $[-\pi, \pi]$. Below is the graph of $\sin x, p_0(x)$ and $x - x^3/3! + x^5/5!$.



Knowledge in linear algebra provides us a much better approximation than calculus!

Problem 5.17 (Alternative Proof of Spectral Theorem). In this problem we prove Spectral Theorem using an important theorem in multivariable calculus:

> **Theorem (Lagrange Multiplier).** *Let $f, c_1, c_2, \ldots, c_m : \mathbb{R}^n \to \mathbb{R}$ be continuously differentiable function (i.e., all partial derivatives are continuous). If the local extreme of $f(x_1, \ldots, x_n)$ occurs at $x_0 \in \mathbb{R}^n$ subject to the constraints*
>
> $$c_1(x_1, \ldots, x_n) = 0, \quad c_2(x_1, \ldots, x_n) = 0, \quad \cdots, \quad c_m(x_1, \ldots, x_n) = 0,$$
>
> *then there are $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ such that*
>
> $$\nabla f(x_0) = \lambda_1 \nabla c_1(x_0) + \cdots + \lambda_m \nabla c_m(x_0).$$

Now we prove Spectral Theorem in the following step: Let A be a real $n \times n$ symmetric matrix.

Step 1. Let $\psi, c : \mathbb{R}^n \to \mathbb{R}$ be defined by $\psi(x) = x^T A x$ and $c(x) = x^T x - 1$ respectively. Show that for every $x \in \mathbb{R}^n$,

$$\nabla \psi(x) = 2x^T A \quad \text{and} \quad \nabla c(x) = 2x^T$$

Step 2. It is known that subject to the condition $c(x) = 0$, the local extreme $f(x)$ occurs for those x, say at x_0 (s.t. $x_0^T x_0 = 1$). By using Lagrange Multiplier Theorem, show that x_0 is an eigenvector of A.

Step 3. We will finish the proof by induction. Suppose that we already have orthonormal eigenvectors $v_1, \ldots, v_k \in \mathbb{R}^n$ of A. Show that the solution to the following constrained extreme problem (it is known that this exists)

$$\psi(x) = \max, \quad x^T x - 1 = 0, \quad x^T v_1 = 0, \quad x^T v_2 = 0, \quad \cdots, x^T v_k = 0$$

is also an eigenvector of A.

Step 4. Complete the proof by induction.