Linear Algebra

Wai Chee SHIU

Published by

Department of Mathematics
Hong Kong Baptist University
Kowloon Tong, Hong Kong

Printed in Hong Kong

Linear Algebra
Wai Chee Shiu

ISBN 978-988-13502-1-3

Contents

Preface

There are already many textbooks on linear algebra out there, so why are we writing another one? Based on our many years of teaching, having referred and adopted many textbooks in the field, we would categorize them into two classes. In the first class are books with a more abstract flavor and emphasis on mathematical rigor. In principle, they are very good books for mathematics majors. But since most concepts are treated in generalization, they may be too difficult for the average student today and are more suitably used as reference materials for advanced students.

Books of the second class are written for the most audience with the emphasis on finite dimensional space; mostly on $\mathbb{R}^n$, sometimes generalizing to $\mathbb{C}^n$. Concepts are treated in a more practical content with manipulation and theoretic on matrices. They are thus much easier to understand and particularly suitable for engineering majors. However, the restriction on $\mathbb{R}^n$ and $\mathbb{C}^n$ spaces would be too limiting for mathematics majors; without experience with more general vector spaces, they would find it difficult to progress onto advanced applications and research in the field. For example, the study of differential equations or functional analysis requires working in infinite dimensional function spaces and using inner product as opposed to dot product in $\mathbb{R}^n$; in computer science and coding theory, the most natural algebraic system is the finite field $\mathbb{Z}_2$, or vector spaces over $\mathbb{Z}_2$.

What we would like to adopt the best feature from both worlds and that is the motivation for this book. We begin with the ease to handle matrices, solving systems of linear equations in $\mathbb{R}^2$, then $\mathbb{R}^3$, eventually progressing to $\mathbb{F}^n$. Next we consider determinants and the eigenvalue problem. In the second half of the book, we discuss general vector space, including linear transformations, change of basis, diagonalization, Jorden normal forms, bilinear forms and quadratic forms, and inner product spaces. The first half (Chapters 1-5) of this book demonstrates how the matrix theory works and suits students who will not go to graduate schools. The second half (Chapters 6-10) of this book explains why matrix theory works and will lay the foundation for postgraduate studies.

For completeness, we have also added a Chapter zero at the start of the book, introducing the concept of fields, and the properties of integers and modules. Beginners in linear algebra may start with Chapters 1 and 2 treating the general field $\mathbb{F}$ as the real number field $\mathbb{R}$, before going back to Chapter zero. This may facilitate a gentler start, while eventually building up to a sound grasp of the general theory.

W.C. Shiu
January, 2019.

About the author

He graduated from National Taiwan University (NTU) and got master degree in 1983; got Diploma of education in 1985 at CUHK; M. Phil in 1989 and PhD in 1993 at HKU. He has taught in NTU as a full-time tutor. He was a teacher in Maria College in 1983. After getting the diploma of education, he was a part-time teaching assistant in 1985 at CUHK and a part-time demonstrator from 1986-89 in HKU. He worked in Hong Kong Baptist University as an assistant lecturer from 1989-93; a lecturer from 1993-95; an assistant professor from 1995-1999; an associate professor from 1999-2018 in HKBU and retired. Now he is working as a professor in Beijing Institute of Technology, Zhuhai. He has taught linear algebra, mathematical analysis, graph theory, algebra etc. in HKBU. Over 224 papers were published at international journals. There are some published books:

1. E.H. Li, C.K Liu and W.C. Shiu, *A first Course in Statistics* (in Chinese), Hong Kong Education Publishing Co., 1997.

2. W.C. Shiu and K.K. Poon, *Elementary Discrete Mathematics* (in Chinese), Chiu Chang Publishing Co., 2005.

3. K.K. Poon and W.C. Shiu, *Elementary Number Theory* (in Chinese), Canotta Publishing Co., 2008.

4. W.C. Shiu and M.L. Tang, *Introduction to Statistics* (in Chinese), Hong Kong Education Publishing Co., 2008.

5. W.C. Shiu and C.I. Chu, *Linear Algebra*, Asian Customized Ed., McGraw-Hill, 2012.

6. W.C. Shiu and L. Ling, *Smart Decisions*, Pearson, 2012.

7. W.C. Shiu and P.K. Sun, *A First Course in Graph Theory*, Department of Mathematics, Hong Kong Baptist University, 2014.

Chapter 0

Elementary Concepts

0.1 Real Numbers and Field

In this chapter, we shall introduce a concept called "field". The reader who first studies linear algebra may view the field as the set of all real numbers. After learning the first two chapters, we suggest the reader to reread this chapter.

Before introducing the concept of field we recall some properties of our usual number system — the system of real numbers.

Let $\mathbb{R}$ be the set of real numbers. For any real numbers a, b and c we have the following properties.

(1) $a + b \in \mathbb{R}$. (Closed under addition)

(2) $a + b = b + a$. (Commutative law of addition)

(3) $(a + b) + c = a + (b + c)$. (Associative law of addition)

(4) $a + 0 = a$. (Existence of additive identity)

(5) For each $x \in \mathbb{R}$, there is a real number y such that $x + y = 0$. The number y is denoted by $-x$. (Existence of additive inverse)

(6) $a \times b \in \mathbb{R}$. (Closed under multiplication)

(7) $a \times b = b \times a$. (Commutative law of multiplication)

(8) $(a \times b) \times c = a \times (b \times c)$. (Associative law of multiplication)

(9) $a \times 1 = a$. (Existence of multiplicative identity)

(10) For each $x \in \mathbb{R}$ with $x \neq 0$, there is a real number y such that $x \times y = 1$. The number y is denoted by $\frac{1}{x}$. (Existence of multiplicative inverse)

(11) $(b + c) \times a = (b \times a) + (c \times a)$. (Distribution law)

Based on these two operations we can define another two operations called subtraction "$-$" and division "$\div$". Namely for $a, b \in \mathbb{R}$, $a - b$ is defined by $a + (-b)$ and $a \div b$ is defined by $a \times \frac{1}{b}$ if $b \neq 0$. Note that "$-$" and "$\div$" do not satisfy associative law and commutative law.

Let $\mathbb{Z}$ be the set of integers. Let $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$ be the set of all rational numbers. It is easy to check that the above properties also hold in $\mathbb{Q}$. Now it is the time to generalize those concept to an abstract number system.

Definition 0.1.1 Let $\mathbb{F}$ be a non-empty set with two operations called *addition* and *multiplication*. Usually we denote these operations by "+" and "$\cdot$" respectively. The set $\mathbb{F}$ is called a *field* if it satisfies the following eleven axioms:

(A1) For any $a, b \in \mathbb{F}$, $a + b \in \mathbb{F}$. (Closed under addition)

(A2) For any $a, b \in \mathbb{F}$, $a + b = b + a$. (Commutative law of addition)

(A3) For any $a, b, c \in \mathbb{F}$, $(a + b) + c = a + (b + c)$. (Associative law of addition)

(A4) There is an element, denoted by 0, in $\mathbb{F}$ having the property that $a + 0 = a$ for any $a \in \mathbb{F}$. (Existence of additive identity)

(A5) For each $x \in \mathbb{F}$, there is an element $y \in \mathbb{F}$ such that $x + y = 0$. (Existence of additive inverse)

Note that such y is unique. It is denoted by $-x$.

(M1) For any $a, b \in \mathbb{F}$, $a \cdot b \in \mathbb{F}$. (Closed under multiplication)

(M2) For any $a, b \in \mathbb{F}$, $a \cdot b = b \cdot a$. (Commutative law of multiplication)

(M3) For any $a, b, c \in \mathbb{F}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (Associative law of multiplication)

(M4) There is an element not equal to 0, denoted by 1, in $\mathbb{F}$ such that $a \cdot 1 = a$ for any $a \in \mathbb{F}$.(Existence of multiplicative identity)

(M5) For each $x \in \mathbb{F}$ with $x \neq 0$, there is an element $y \in \mathbb{F}$ such that $x \cdot y = 1$. (Existence of multiplicative inverse)

Note that such y is unique. It is called the *inverse of* x and denoted by x^{-1}.

(D) $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$. (Distribution law)

So $\mathbb{R}$ and $\mathbb{Q}$ are fields under the usual addition and multiplication. Note that, by axioms (A4) and (M4) every field $\mathbb{F}$ contains at least 2 elements.

The notation $a \cdot b$ is always denoted by ab. Usually, the element $a + (-b)$ is written by $a - b$. But it is not common to use $a \div b$ to denote ab^{-1} for $b \neq 0$ in a field.

Proposition 0.1.2 *Let $\mathbb{F}$ be a field. There is a unique element satisfying the axiom* (A4) *and there is a unique element satisfying the axiom* (M4). Hence such elements are called the *zero* and *unity* of $\mathbb{F}$, respectively.

Proof: Suppose 0 and $0'$ satisfy the axiom (A4). Then

$$0' = 0' + 0 = 0 + 0' = 0.$$

Similarly, suppose 1 and $1'$ satisfy the axiom (M4). Then

$$1' = 1' \cdot 1 = 1 \cdot 1' = 1.$$

□

Proposition 0.1.3 *Let $\mathbb{F}$ be a field. The following statements hold.*

(a) For any $a \in \mathbb{F}$, $0a = 0$ and $(-1)a = -a$.

(b) For any $a, b \in \mathbb{F}$, $a(-b) = (-a)b = -(ab)$.

(c) For any nonzero elements a and b in $\mathbb{F}$, $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

(d) For any nonzero element $a \in \mathbb{F}$, $(a^{-1})^{-1} = a$.

(e) Suppose $ab = 0$ for some $a, b \in \mathbb{F}$. Then either $a = 0$ or $b = 0$.

Proof: The proof is left to the reader. □

Note that the contrapositive of Proposition 0.1.3 (e) is that
if both a and b are nonzero, then so is ab.

Example 0.1.4 Let $i = \sqrt{-1}$. It is easy to check that the set of complex numbers $\mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}\}$ is a field under the usual operations. □

Example 0.1.5 Consider the set $\mathbb{Z}$ under the usual addition and multiplication. It satisfies all conditions of field except the axiom (M5), for example there is no integer y such that $2 \times y = 1$. Thus $\mathbb{Z}$ is not a field. Note that a set with two operations satisfying all conditions of field except the axiom (M5) is called a *commutative ring with unity*[1]. Thus $\mathbb{Z}$ is a commutative ring with unity. □

Example 0.1.6 Consider the set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. We shall check that $\mathbb{Q}[\sqrt{2}]$ is a field.

For any $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, since sum and product of rational numbers are rational numbers,

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

and

$$(a + b\sqrt{2}) \times (c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Hence axioms (A1) and (M1) hold.

Since $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$, axioms (A2), (A3), (M2), (M3) and (D) hold automatically. Since $0 = 0 + 0\sqrt{2}$ and $1 = 1 + 0\sqrt{2}$ are in $\mathbb{Q}[\sqrt{2}]$, axioms (A4) and (M4) hold.

For any $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $(-a) + (-b)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. So axiom (A5) holds.

Let $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Suppose $a + b\sqrt{2} \neq 0$. Then $a \neq 0$ or $b \neq 0$. Since $a, b \in \mathbb{Q}$, $a^2 - 2b^2 \neq 0$. Thus

$$\frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2} \in \mathbb{Q}[\sqrt{2}] \text{ and } (a + b\sqrt{2}) \times \left(\frac{a - b\sqrt{2}}{a^2 - 2b^2}\right) = 1.$$

Thus axiom (M5) holds.

Hence $\mathbb{Q}[\sqrt{2}]$ is a field. □

Since $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ and their operations are the same, we call that $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{R}$. Following is the formal definition.

Definition 0.1.7 Let $\mathbb{F}$ be a field. Suppose $\mathbb{K}$ is a subset of $\mathbb{F}$. If $\mathbb{K}$ is a field under the same operations of $\mathbb{F}$, then $\mathbb{K}$ is called a *subfield of* $\mathbb{F}$.

[1] In this book, we do not discuss such algebraic object. The interested reader is referred to any book of abstract algebra or modern algebra. For example, N. Jacobson, *Basic Algebra I*, 2nd edition, Freeman, 1985.

Under the usual operations, $\mathbb{Q}$ is a subfield of $\mathbb{Q}[\sqrt{2}]$ and also a subfield of $\mathbb{R}$; and $\mathbb{R}$ is a subfield of $\mathbb{C}$. We have the following two propositions. The proofs are left to reader.

Proposition 0.1.8 *Suppose $\mathbb{K}$ is a subfield of a field $\mathbb{F}$. Then the zero and the unity of $\mathbb{K}$ are the same as those of $\mathbb{F}$.*

Proposition 0.1.9 *Suppose $\mathbb{F}$ is a field and $\mathbb{K}$ is a subset of $\mathbb{F}$. Under the same operations, $\mathbb{K}$ is a subfield of $\mathbb{F}$ if and only if $a - b \in \mathbb{K}$ for any $a, b \in \mathbb{K}$ and $ab^{-1} \in \mathbb{K}$ for any $a, b \in \mathbb{K}$ with $b \neq 0$.* Note that b^{-1} exists in $\mathbb{F}$.

All fields discussed in the above examples contain infinitely many elements. Does it exist a field which contains only finite element? The answer is yes. Here is an example.

Example 0.1.10 Let $\mathbb{Z}_2 = \{0, 1\}$. We define two commutative operations "$+$" and "$\cdot$" as follows:

$$0 + 0 = 0, \quad 1 + 0 = 1, \quad 1 + 1 = 0; \quad 0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 1 = 1.$$

We can write the above relations as the following tables which are called *addition table* and *multiplication table*, respectively.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

By these tables, one can see that all the axioms of field hold immediately except (A3), (M3) and (D). By checking all eight cases (by applying the commutative laws there are actually six cases), one can see that axioms (A3), (M3) and (D) hold. Hence under those two operations $\mathbb{Z}_2$ is a field. Since every field contains at least two elements, $\mathbb{Z}_2$ is a field of the smallest size. □

A field which contains finitely many elements is called a *finite field*. The following is another small finite field.

Example 0.1.11 Let $\mathbb{Z}_3 = \{0, 1, 2\}$. We define two commutative operations "$+$" and "$\cdot$" as follows:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

It is easy to see that 0 and 1 are the zero and unity respectively. The minus of 1 is 2, i.e., $-1 = 2$ and the minus of 2 is 1. The inverse of 1 is 1 and the inverse of 2 is 2, i.e., $2^{-1} = 2$. Verifying the rest axioms of field are left to the reader. So $\mathbb{Z}_3$ is a field. □

Note that although all symbols of $\mathbb{Z}_2$ are symbols of $\mathbb{Z}_3$, $\mathbb{Z}_2$ is not a subfield of $\mathbb{Z}_3$. The reason is that their operations are different, since there is some element a, for example 1 or 2, in $\mathbb{Z}_3$ such that $a + a \neq 0$ but there is no such kind of element in $\mathbb{Z}_2$. By the same reason, both $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are not subfields of $\mathbb{Q}$ or $\mathbb{R}$.

Exercise 0.1

0.1-1. Prove Proposition 0.1.3.

0.1-2. Prove Proposition 0.1.8.

0.1-3. Prove Proposition 0.1.9.

0.1-4. Complete Example 0.1.11.

0.1-5. Prove that $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ is a field (subfield of $\mathbb{R}$).

0.1-6. Prove that $\mathbb{Q}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$.

0.1-7. Prove that $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a field, where d is a square-free integer.

0.1-8. Prove that $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$

0.1-9. Let $\mathbb{Z}_2$ be the field defined in Example 0.1.10. Let α be an extra element and let $a + b\alpha$ be a formal sum, where $a, b \in \mathbb{Z}_2$. Let $\mathbb{Z}_2[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\}$. It is clear that $\mathbb{Z}_2[\alpha]$ contains 4 elements, namely $\mathbb{Z}_2[\alpha] = \{0, 1, \alpha, \alpha + 1\}$. Define the addition and multiplication as follows:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Prove that $\mathbb{Z}_2[\alpha]$ is a field under the operations defined above. Actually $\mathbb{Z}_2$ is a subfield of $\mathbb{Z}_2[\alpha]$.

0.2 Some Properties of Integers

An important property of the integers is the so-called Well Ordering Principle. Since we cannot prove it here, we will take it as an axiom. The interested reader is refereed to the book: N. Jacobson, *Basic Algebra I*, 2nd edition, W.H. Freeman and Company, 1985.

Well Ordering Principle: *Every nonempty set of nonnegative integers contains a smallest element.*

For convenience, we use $\mathbb{N}$ to denote the set of all natural numbers (i.e., positive integers). Note that some books use the notation $\mathbb{N}$ to denote the set of all nonnegative integers, however in this book we use $\mathbb{N}_0$, i.e., $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Definition 0.2.1 Suppose $a, b \in \mathbb{Z}$ and $b \neq 0$. If there is an integer x such that $a = bx$, then we call that a *is divisible by* b, or b *divides* a, or b *is a factor or divisor of* a, and we write $b|a$. In case a is not divisible by b, we write $b \not| a$.

Proposition 0.2.2 (Division Algorithm) *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.*

Proof: Let $S = \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\}$. If $a > 0$, then $a = a - b0 \in S$. If $a \leq 0$, then $a - b(2a) \in S$. Thus $S \neq \varnothing$.

Applying the Well Ordering Principle, let r be the smallest element in S. Then $r = a - bq$ for some $q \in \mathbb{Z}$. Thus $a = bq + r$ and $r \geq 0$. Suppose $r \geq b$. Then $a - b(q + 1) = r - b \geq 0$. Hence $r - b \in S$. Since $r - b < r$, it contradicts to the minimibility of r. Hence $r < b$.

Now we are going to prove the uniqueness of q and r. Suppose $bq + r = bq' + r'$. Without loss of generality, we may assume $r' - r \geq 0$. Then $b(q - q') = r' - r$. So $b|(r' - r)$ and $0 \leq r' - r < b$. It follows that $r' - r = 0$ and hence $r' = r$ and $q = q'$. □

Definition 0.2.3 An integer g is a *common divisor of b and c* if $g|b$ and $g|c$. Since there are only a finite number of divisors of any nonzero integer, there are only a finite number of common divisors of b and c, except $b = c = 0$. If at least one b and c is not zero, the greatest among their common divisors is called the *greatest common divisor of b and c* and is denoted by (b, c) or g.c.d.(b, c). Note that $(b, 0) = b$ if $b \neq 0$.

Remark 0.2.4 Suppose $g = (b, c)$. Then by definition $g \geq 1$. Suppose $d|b$ and $d|c$. Then $d \leq g$. In fact, $d|g$.

Lemma 0.2.5 *For any $x \in \mathbb{Z}$, $(a, b) = (b, a) = (a, -b) = (a, b + ax)$.*

Proof: Let $g = (a, b)$ and $d = (a, b + ax)$. By definition it is clear that $(b, a) = (a, -b) = g$. Since $g|a$ and $g|b$, $a = gs$ and $b = gt$ for some $s, t \in \mathbb{Z}$. Then $b + ax = g(t + sx)$. So $g|b + ax$ and hence $g \leq d$. Similarly, $a = dy$ and $b + ax = dz$ for some $y, z \in \mathbb{Z}$. Then $b = dz - ax = d(z - yx)$. So $d|b$ and hence $d \leq g$. Therefore, $g = d$. □

Note that $(a, 0) = a$ for $a > 0$. Thus by the Lemma above, on considering the g.c.d. of a and b we may assume that they are positive.

Theorem 0.2.6 (Euclidean Algorithm) *Given integers a and b with $a > b > 0$. There exist some integers $q_1, q_2, \ldots, q_{n+1}$ and $r_1, r_2, \ldots, r_n$ such that*

$$\begin{array}{rcll} a &=& bq_1 + r_1, & 0 < r_1 < b, \\ b &=& r_1q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 &=& r_2q_3 + r_3, & 0 < r_3 < r_2, \\ \vdots & & \vdots & \vdots \\ r_{n-2} &=& r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &=& r_nq_{n+1}. & \end{array} \tag{0.1}$$

The greatest common divisor $(a, b) = r_n$. Moreover, $r_n = as + bt$ for some $s, t \in \mathbb{Z}$.

The proof can be found in Appendix A.1.

Example 0.2.7 Find g.c.d.$(34567, 3210)$.

By using Euclidean Algorithm, we have the following table:

10	34567	3210	1
	32100	2467	
3	2467	743	3
	2229	714	
8	238	29	4
	232	24	
1	6	5	5
	5	5	
	1	0	

Thus $(34567, 3210) = 1$. Note that we have $q_1 = 10$, $q_2 = 1$, $q_3 = 3$, $q_4 = 3$, $q_5 = 8$, $q_6 = 4$, $q_7 = 1$, $q_8 = 5$, $r_1 = 2467$, $r_2 = 743$, $r_3 = 238$, $r_4 = 29$, $r_5 = 6$, $r_6 = 5$, $r_7 = 1$. □

Remark 0.2.8 According to the notations used in the proof of Theorem 0.2.6 (can be found in Appendix), if we let $s_{-1} = 1$, $s_0 = 0$, $t_{-1} = 0$ and $t_0 = 1$, then we have

$$s_i = s_{i-2} - q_i u_{i-2} = s_{i-2} - q_i s_{i-1}, 1 \leq i \leq n.$$

and

$$t_i = t_{i-2} - q_i t_{i-1}, 1 \leq i \leq n.$$

Then g.c.d.$(a, b) = as_n + bt_n$. Finding the integers s_i and t_i can be systematized. The following example demonstrates a convenient method.

Example 0.2.9 Find integers s and t to satisfy $34567s + 3210t = 1$.

i	-1	0	1	2	3	4	5	6	7	8
$-q_i$			-10	-1	-3	-3	-8	-4	-1	-5
s_i	1	0	1	-1	4	-13	108	-445	553	-3210
t_i	0	1	-10	11	-43	140	-1163	4792	-5955	34567

Therefore $s = 553$ and $t = -5955$, i.e., $34567 \times 553 + 3210 \times (-5955) = 1$. □

Exercise 0.2

0.2-1. Find s and t such that $as + bt = (a, b)$, where
(a) $a = 987$, $b = 68$;
(b) $a = 4530$, $b = 2004$.

0.2-2. Find an integral solution for each of the following integral equations:
(a) $73x - 52y = 1$;
(b) $243x + 198y = 9$;
(c) $6x + 8y + 9z = 1$.

0.2-3. Suppose $a, b, c \in \mathbb{Z}$. Prove the following statements:
(a) If $a|b$, then $a|kb$ for ant $k \in \mathbb{Z}$.
(b) If $a|b$ and $b|c$, then $a|c$.
(c) If $a|b$ and $a|c$, then $a|bx + cy$ for any $x, y \in \mathbb{Z}$.
(d) If $a|b$ and $b|a$, then $a = \pm b$.
(e) If $a|b$, $a > 0$ and $b > 0$, then $a \leq b$.

0.2-4. In this problem, we want to generalize the last result of Theorem 0.2.6 without using Euclidean Algorithm. Let $a, b \in \mathbb{Z}$ which are not all zero. Let

$$S = \{ax + by \mid x, y \in \mathbb{Z} \text{ and } ax + by > 0\}.$$

(a) Show that $S \neq \varnothing$.
(b) Show that the smallest element of S is (a, b).

0.2-5. Suppose $a, b \in \mathbb{Z}$ which are not all zero. For any positive integer c, show that $(ca, cb) = c(a, b)$.

0.2-6. Suppose $a, b \in \mathbb{Z}$ which are not all zero. If $d|a$ and $d|b$ and $d > 0$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$. Hence if $(a, b) = g$, then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

0.2-7. Suppose $a, b, c \in \mathbb{Z}$. Show that $(a, c) = (b, c) = 1$ if and only if $(ab, c) = 1$.

0.3 Equivalence Relations

An important arithmetic system called modular arithmetic will be introduced in the next section. Before introducing a notion called binary relation, we start with an example.

Example 0.3.1 Consider the set $\mathbb{N}$. Let $(a, b) \in \mathbb{N} \times \mathbb{N}$. We have introduced the notation $a|b$ in the previous section. Clearly $a|b$ does not guarantee $b|a$. Thus $2|2$; $2|4$; $3|6$; $5|25$; etc., but $4|2$ does not hold, i.e., $4 \not| 2$. Now we define that a is related to b if and only if a divides b. Therefore, 2 is related to 2; 2 is related to 4; 3 is related to 6 and 5 is related to 25, but 4 is not related to 2.

Now we define a subset R of $\mathbb{N} \times \mathbb{N}$ by

$$R = \{(a, b) \mid a \text{ divides } b\}.$$

This means that $a|b$ if and only if $(a, b) \in R$, i.e., R is considered a representation of the relationship "|". We shall call that R or | is a binary relation on $\mathbb{N}$. □

Relationship between elements of a set is represented using an algebraic structure called a binary relation. The usual way to express a relationship between two elements is to use ordered pair made up of two related elements. For this reason, sets of ordered pairs are called binary relations. Now let us make a formal definition of binary relation.

Definition 0.3.2 Let S be a set. Suppose $R \subseteq S \times S$. We say a *is related to* b *by* R if $(a, b) \in R$. The subset R is called a *binary relation* (or simply *relation*) *on* S. We shall use the same symbol R to denote the relation between elements. So if a is related to b by R, then we write aRb. Moreover, if $(a, b) \notin R$, then we say a is not related to b by R and is denoted by $a \not R b$.

Example 0.3.3 Consider the ring $\mathbb{Z}$. Let

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a - b \text{ is positive}\}.$$

Then R is a relation on $\mathbb{Z}$. Actually aRb is the same as $a > b$. □

Definition 0.3.4 Let R be a relation on a set S. Relation R is called
reflexive (or *reflective*) if for each $a \in S$, aRa;
symmetric if aRb implies bRa;
transitive if aRb and bRc implies aRc.

Example 0.3.5 The relation | defined in Example 0.3.1 is reflexive and transitive but not symmetric. The relation $>$ defined in Example 0.3.3 is a transitive but not reflexive nor symmetric. □

Example 0.3.6 Consider the ring $\mathbb{Z}$. Let $a \geq b$ if $a - b$ is nonnegative. Then $\geq$ is reflexive and transitive but not symmetric. □

Definition 0.3.7 A reflexive, symmetric and transitive relation is called an *equivalence relation.*

Example 0.3.8 The relation $=$ defined on $\mathbb{Z}$ is an equivalence relation. □

Example 0.3.9 Let $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$. We define $(x, y) \sim (u, v)$ if $x^2 + y^2 = u^2 + v^2$. It is easy to see that $\sim$ is an equivalence relation on $\mathbb{R}^2$. □

Consider the relation $\sim$ defined in Example 0.3.9. For a nonnegative real number a, let $C_a = \{(x, y) \mid x^2 + y^2 = a^2\}$ be the circle with radius a centered at the origin. One can see that each (x, y) must lie exactly on one such circle, and $(x, y) \sim (u, v)$ if and only if they lie on the same circle. It means that the collection $\{C_a \mid a \in \mathbb{R} \text{ and } a \geq 0\}$ forms a partition of $\mathbb{R}^2$. Equivalence points lie in the same class C_a for some $a \geq 0$.

We have a general property about equivalence relation and partition. Before stating some theorems, we give a formal definition of partition first.

Definition 0.3.10 Let S be a set. A *partition of* S is a collection $\mathscr{C}$ of nonempty subsets of S, namely $\mathscr{C} = \{A_i \subseteq S \mid i \in I\}$ for some index set I, such that

(P1) $\bigcup_{A \in \mathscr{C}} A \ (= \bigcup_{i \in I} A_i) = S$;

(P2) for $A, B \in \mathscr{C}$ if $A \neq B$, then $A \cap B = \varnothing$.

Theorem 0.3.11 *Let $\sim$ be an equivalence relation on a set S. For each $a \in S$, define $[a] = \{s \in S \mid a \sim s\}$. Then the collection $\mathscr{C} = \{[a] \mid a \in S\}$ is a partition of S.*

Proof: For each $a \in S$, since $a \sim a$, $a \in [a]$. Therefore, $S \subseteq \bigcup_{a \in S} [a]$. Since each $[a]$ is a subset of S, $S \supseteq \bigcup_{a \in S} [a]$. Hence (P1) holds.

To prove (P2) it is equivalent to prove that for $a, b \in S$ if $[a] \cap [b] \neq \varnothing$ then $[a] = [b]$. Since $[a] \cap [b] \neq \varnothing$, there is an element $s \in [a] \cap [b]$. Then $a \sim s$ and $b \sim s$. Since $\sim$ is symmetric, we have $s \sim b$. By the transitivity of $\sim$, we have $a \sim b$ and hence $b \in [a]$. For each $x \in [b]$, $b \sim x$. Since $a \sim b$, $a \sim x$ and hence $x \in [a]$. Therefore, $[b] \subseteq [a]$.

Similarly, we have $[a] \subseteq [b]$. Hence $[a] = [b]$. □

Note that the subset $[a]$ is called the *equivalence class of S with respect to the equivalence relation $\sim$ containing a* and the collection $\mathscr{C}$ is called the *quotient set of S with respect to $\sim$*. The collection $\mathscr{C}$ is often written by $S/\sim$.

Theorem 0.3.12 *Let $\mathscr{C}$ be a partition of a set S. Then there is an equivalence relation $\sim$ such that $\mathscr{C} = S/\sim$.*

Proof: A relation $\sim$ is defined on S by

$$a \sim b \text{ if } a \text{ and } b \text{ lie in the same subset } A \text{ for some } A \in \mathscr{C}.$$

We shall prove that $\sim$ is an equivalence relation and the quotient set $S/\sim$ is exactly the collection $\mathscr{C}$.

For each $a \in S$, since $\mathscr{C}$ is a partition of S, $a \in A$ for some $A \in \mathscr{C}$. By the definition of $\sim$, we have $a \sim a$. Hence $\sim$ is reflexive.

Suppose $a \sim b$ for some $a, b \in S$. Then a and b lie in A for some $A \in \mathscr{C}$. Thus b and a lie in A and hence $b \sim a$. Therefore, $\sim$ is symmetric.

Suppose $a \sim b$ and $b \sim c$ for some $a, b, c \in S$. Then $a, b \in A$ and $b, c \in B$ for some $A, B \in \mathscr{C}$. Then $b \in A \cap B$. Since $\mathscr{C}$ is a partition, $A = B$. Thus we have $a, c \in B$ and hence $a \sim c$. Therefore, $\sim$ is transitive.

Thus $\sim$ is an equivalence relation on S.

Now we are going to prove that $\mathscr{C} = S/\sim$. For each $[a] \in S/\sim$, since $\mathscr{C}$ is a partition of S, $a \in A$ for some $A \in \mathscr{C}$. For each $x \in [a]$, we have $a \sim x$. This means that both a and x lie in B for some

$B \in \mathscr{C}$. Then $a \in A \cap B$ and hence $A = B$. Therefore, $[a] \subseteq A$. Conversely, for each $y \in A$, since $a, y \in A$, we have $a \sim y$. Hence $A \subseteq [a]$. Finally, we have $[a] = A$ and then $S/\sim \subseteq \mathscr{C}$.

For each $A \in \mathscr{C}$, since $A \neq \varnothing$, there is $a \in A$. By the definition of $\sim$, we have $A \subseteq [a]$. By the same argument in the previous paragraph, we have $[a] \subseteq A$ and hence $A = [a]$. Therefore, $\mathscr{C} \subseteq S/\sim$. □

Exercise 0.3

0.3-1. Let $a, b \in \mathbb{R}$. Define $a \sim b$ if $a - b \in \mathbb{Z}$. Show that $\sim$ is an equivalence relation on $\mathbb{R}$. Describe the equivalence classes of $\mathbb{R}$ with respect to $\sim$.

0.3-2. Let $a, b \in \mathbb{Z}$. Define $a \sim b$ if $a + b$ is even, i.e., $a + b = 2k$ for some $k \in \mathbb{Z}$. Prove that $\sim$ is an equivalence relation on $\mathbb{Z}$. Describe the equivalence classes of $\mathbb{Z}$ with respect to $\sim$.

0.3-3. Let $S = \mathbb{Z} \times \mathbb{N}$.

(a) Define $(a, b) \sim (c, d)$ if $ad = bc$. Prove that $\sim$ is an equivalence relation.

(b) Let $[a, b]$ denote the equivalence class of S containing (a, b). Then the quotient set $S/\sim = \{[a, b] \mid (a, b) \in S\}$. Define addition "+" and multiplication "$\cdot$" on S by

$$[a, b] + [c, d] = [ad + bc, bd] \text{ and } [a, b] \cdot [c, d] = [ac, bd].$$

Prove that these two binary operations are well-defined.

(c) Prove that under the binary operations defined in (b), $S/\sim$ is a field. [Hint: $[0, 1] = [0, b]$ for any $b \in \mathbb{N}$ is the zero and $[1, 1] = [a, a]$ for any $a \in \mathbb{N}$ is the unity.]

0.4 Modular Arithmetic

Consider the set of integers $\mathbb{Z}$. Let m be a fixed integer m with $m \geq 2$. For $a \in \mathbb{Z}$, $a \mod m$, read "*a modulo m*", is the remainder upon dividing a by m. We often use the modular concept in combination with addition and multiplication.

Example 0.4.1 $10 \mod 4 = 2$; $\quad -5 \mod 4 = 3$;
$(7 + 2) \mod 6 = 3$; $\quad (3 \times 2) \mod 6 = 0$; $\quad 2 \times (3 + 2) \mod 7 = 3$. □

For the relation $a \mod m = b$, it is often written as $a \equiv b \pmod{m}$. Thus

$$10 \equiv 2 \pmod 4; \quad 7 + 2 \equiv 3 \pmod 6; \quad 2(3 + 2) \equiv 3 \pmod 7.$$

Now let us make a formal definition for the binary relation $\equiv \pmod m$ on $\mathbb{Z}$.

Definition 0.4.2 For a fixed integer m with $m \geq 2$, $a \equiv b \pmod m$, read "*a is congruent to b modulo m*", if $a - b$ is divisible by m. This means that the remainders upon dividing a and b by m are the same.

Theorem 0.4.3 *The relation* $\equiv \pmod m$ *is an equivalence relation on* $\mathbb{Z}$.

Proof: For convenience, we shall use '$\equiv$' instead of '$\equiv \pmod m$' in this proof.

For any integer a, $a - a = 0$ is always divisible by m. Thus $a \equiv a$.

Suppose $a \equiv b$. By the definition $a - b = km$ for some $k \in \mathbb{Z}$. Then $b - a = (-k)m$. Therefore, $b \equiv a$.

Suppose $a \equiv b$ and $b \equiv c$. By the definition $a - b = km$ and $b - c = hm$ for some $k, h \in \mathbb{Z}$. Then $a - c = (k + h)m$. Therefore, $a \equiv c$. □

Proposition 0.4.4 *Suppose* $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$. *Then* $a + c \equiv b + d \pmod m$ *and* $ac \equiv bd \pmod m$.

Proof: Since $a \equiv b \pmod m$ and $c \equiv d \pmod m$, $a = b + hm$ and $c = d + km$ for some $h, k \in \mathbb{Z}$. Then $a + c = b + d + (h + k)m$ and $ac = bd + (hd + kb + hkm)m$. Thus we have the proposition. □

What is the quotient set $\mathbb{Z}/\equiv \pmod m$? The remainder of a divided by m must be $0, 1, \ldots,$ or $m - 1$. Therefore, $a \equiv r \pmod m$ for some r with $0 \le r \le m - 1$. In the form of the last section it is written as $[a] = [r]$. Since the difference of two distinct integers i and j between 0 and $m - 1$ are not divisible by m, $i \not\equiv j \pmod m$ and hence $[i] \cap [j] = \varnothing$. Therefore, we have the following statement.

Theorem 0.4.5 *The quotient set* $\mathbb{Z}/\equiv \pmod m$ *is* $\{[0], [1], \ldots, [m - 1]\}$.

We shall use $\mathbb{Z}_m$ to denote $\mathbb{Z}/\equiv \pmod m$, i.e., $\mathbb{Z}_m = \{[0], [1], \ldots, [m - 1]\}$.

Now we want to define two binary operations, addition and multiplication, on $\mathbb{Z}_m$. For $[a], [b] \in \mathbb{Z}_m$, define $[a] + [b] = [a + b]$ and $[a][b] = [ab]$. This definition depends on the symbols a and b. But different symbols may represent the same element in $\mathbb{Z}_m$. For instance, $[1] = [7]$ in $\mathbb{Z}_6$. Thus we have to show that the definition of both addition and multiplication of $\mathbb{Z}_m$ are well-defined. This has been proved by Proposition 0.4.4.

Since the addition and the multiplication of $\mathbb{Z}_m$ come from the addition and the multiplication of $\mathbb{Z}$, it is easy to check that all the axioms of field hold except (M5). Moreover, [0] and [1] are the zero and the unity, respectively. So $\mathbb{Z}_m$ is a commutative ring with unity. In general, (M5) does not hold. For example, in $\mathbb{Z}_6$, [2] does not have inverse.

Theorem 0.4.6 *Suppose* p *is a prime. Then* $\mathbb{Z}_p$ *is a field.*

Proof: It suffices to verify (M5). For any $[a] \neq [0]$ in $\mathbb{Z}_p$, then a is not divisible by p. Since p is a prime, $(a, p) = 1$. By Theorem 0.2.6, there are $s, t \in \mathbb{Z}$ such that $as + pt = 1$. Then $as \equiv 1 \pmod p$, i.e., there exists $[s] \in \mathbb{Z}_p$ such that $[a][s] = [1]$. Thus $\mathbb{Z}_p$ is a field. □

For convenience we often write $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$.

Example 0.4.7 Find the inverse elements of 12 and 14 in $\mathbb{Z}_{31}$, respectively.

By Euclidean Algorithm, we have $31 \times (-5) + 12 \times 13 = 1$. Then 13 is the inverse of 12 in $\mathbb{Z}_{31}$. Similarly, we have $31 \times 5 + 14 \times (-11) = 1$. Since $[-11] = [-11 + 31] = [20]$. Then 20 is the inverse of 14 in $\mathbb{Z}_{31}$. □

Exercise 0.4

0.4-1. Find the inverses of 32 and 47 in $\mathbb{Z}_{67}$, respectively.

0.4-2. Prove that for every integer n, $n^3 \equiv n \pmod 6$.

0.4-3. If n is an odd integer, prove that $n^2 \equiv 1 \pmod 4$. Moreover, prove that $n^2 \equiv 1 \pmod 8$.

0.4-4. If it is 4:00 p.m. now, what time would it be 4000 hours from now?

0.4-5. Let $m, n \in \mathbb{N}$ with $(m, n) = 1$.

(a) Show that there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv 1 \pmod m, \\ x \equiv 0 \pmod n. \end{cases}$$

Similarly there exists $y \in \mathbb{Z}$ such that

$$\begin{cases} y \equiv 0 \pmod m, \\ y \equiv 1 \pmod n. \end{cases}$$

(b) Let $a, b \in \mathbb{Z}$. Show that there exists $z \in \mathbb{Z}$ such that

$$\begin{cases} z \equiv a \pmod m, \\ z \equiv b \pmod n. \end{cases}$$

The last assertion is known as the *Chinese Remainder Theorem*.

0.4-6. Solve the system of congruence equations

$$\begin{cases} z \equiv 3 \pmod 7, \\ z \equiv 4 \pmod{13}. \end{cases}$$

That is, find a z with $0 \le z \le 90$ satisfying the above congruence equations.

0.4-7. Solve the system of congruence equations

$$\begin{cases} z \equiv 3 \pmod 5, \\ z \equiv 4 \pmod 7 \\ z \equiv 2 \pmod{11}. \end{cases}$$

0.5 Polynomials over a Field

In elementary algebra an important object is polynomial. Polynomial is an expression such as $x^3 + 2x^2 + 1$ whose terms are grouped in powers of x. The exponents are nonnegative integers and the coefficients are real or complex numbers. In this section, we shall generalize this concept.

Definition 0.5.1 Let $\mathbb{F}$ be a field (more general, it can be a commutative ring such as $\mathbb{Z}$). An expression of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

is called a *polynomial in the indeterminate x with coefficients in* $\mathbb{F}$ or more simply, a *polynomial in x over* $\mathbb{F}$, where $a_i \in \mathbb{F}$. The expressions $a_k x^k$ for $k \in \mathbb{N}$ are called the *terms* of the polynomial. Note that $x^0 = 1$.

Polynomials in x are designated by symbols such as $f(x)$, $g(x)$, $q(x)$ and so on. If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. Then a_k is called the *coefficient of* x^k. The *degree* of $f(x)$, denoted by $\deg f$ or $\deg f(x)$, is the greatest n such that the coefficient of x^n is not zero. The polynomial whose coefficients are equal to zero is called the *zero polynomial* and is denoted by 0. It is the only polynomial whose degree is not defined (since it has no nonzero coefficient). For convenience, we define the degree of the zero polynomial by $-\infty$, i.e., $\deg 0 = -\infty$.

Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ with $a_n \neq 0$, i.e., $\deg f = n$. Then a_nx^n is called its *leading term* and a_n is called its *leading coefficient*, while a_0 is called its *constant term*. A polynomial whose leading coefficient is 1 is called a *monic polynomial*.

Two polynomials are *equal* if they have the same degree and corresponding coefficients are equal. We shall use $\mathbb{F}[x]$ to denote the set of all polynomials in x over $\mathbb{F}$.

The zero polynomial or a polynomial of degree zero is called a *constant polynomial*. Since each element of $\mathbb{F}$ can be viewed as a constant polynomial, $\mathbb{F}$ is always viewed as a subset of $\mathbb{F}[x]$. If there is no ambiguity, then we often use f instead of $f(x)$.

Definition 0.5.2 For $f, g \in \mathbb{F}[x]$ we define the *sum* of f and g as follows. Suppose $f(x) = \sum_{i=0}^{n} a_ix^i$ and $g(x) = \sum_{j=0}^{m} b_jx^j$. Without loss of generality, we may assume $m \geq n$. We let $a_k = 0$ for $n < k \leq m$. Define $c_j = a_j + b_j$ for $0 \leq j \leq m$. Then $(f + g)(x) = (g + f)(x) = \sum_{j=0}^{m} c_jx^j$.

The *product* of f and g is the polynomial $(fg)(x) = f(x)g(x) = d_0 + d_1x + \cdots + d_{n+m}x^{n+m}$, where $d_k = \sum_{i+j=k} a_ib_j$, $0 \leq k \leq n + m$. When $f(x) = a$ is a constant polynomial the multiplication is also called the *scalar multiplication*.

Under the addition and the multiplication defined above, one can check that $\mathbb{F}[x]$ satisfies all the axioms of field except (M5) (the unity is the constant polynomial 1). So it is a commutative ring with unity. It is called the *polynomial ring over* $\mathbb{F}$.

Proposition 0.5.3 *Suppose* $f, g \in \mathbb{F}[x]$. *Then* $\deg(fg) = \deg f + \deg g$.

Proof: Suppose both f and g are not the zero polynomial. Then by the definition of the product and Proposition 0.1.3 (e), it is easy to see that $\deg(fg) = \deg f + \deg g$. Suppose one of them is the zero polynomial, say $f = 0$. Then $\deg f = -\infty$. Then $\deg(fg) = \deg f + \deg g$ clearly holds. □

By the definition of the sum of two polynomials, we have

Proposition 0.5.4 *Suppose* $f, g \in \mathbb{F}[x]$. *Then* $\deg(f + g) \leq \max\{\deg f, \deg g\}$.

We have a theorem similar to the division algorithm for integer. And the proof is also similar.

Theorem 0.5.5 (Division Algorithm for Polynomials) *If* $a, b \in \mathbb{F}[x]$, *and* $b \neq 0$, *there exists unique polynomials* q *and* r *such that* $a = bq + r$, *where* $\deg r < \deg b$.

Proof: Suppose there is a polynomial $q \in \mathbb{F}[x]$ such that $a = bq$. Then let $r = 0$. Clearly, $-\infty = \deg r < \deg b$. So now we assume that $a - bk \neq 0$, i.e., $\deg(a - bk) \geq 0$, for all $k \in \mathbb{F}[x]$.

Consider the set $T = \{a - bk \mid k \in \mathbb{F}[x]\}$. Since $a = a - b0 \in T$, $T \neq \varnothing$. Let $S = \{\deg g \mid g \in T\}$. Since $T \neq \varnothing$, $S \neq \varnothing$. Applying the Well Ordering Principle, let s be the smallest integer in S. Then there exists a polynomial r in T, say $r = a - bq$ for some $q \in \mathbb{F}[x]$ and $\deg r = s$.

Suppose $\deg r \geq \deg b$. Let $b(x) = \sum_{i=0}^{n} b_i x^i$ and $r(x) = \sum_{i=0}^{s} r_i x^i$ with $b_n \neq 0$ and $r_s \neq 0$. Since $s \geq n$, $r'(x) = a(x) - b(x)q(x) - r_s b_n^{-1} x^{s-n} b(x) = r(x) - r_s b_n^{-1} x^{s-n} b(x)$ is a polynomial. (Note that, since $\mathbb{F}$ is a field, b_n^{-1} exists. If $\mathbb{F}$ is not a field, then this theorem does not hold.) It is clear that $r'(x) = a(x) - b(x)(q(x) + r_s b_n^{-1} x^{s-n}) \in T$ and $\deg r' < \deg r$. This contradicts the choice of r.

Suppose $a = bq + r = bq' + r'$ for some $q', r' \in \mathbb{F}[x]$. Then $b(q - q') = r' - r$. By Proposition 0.5.3 we have

$$\deg b + \deg(q - q') = \deg(r - r'). \tag{0.2}$$

By Proposition 0.5.4, we have $\deg(r - r') \leq \deg r$. Since $\deg b > \deg r$, Equation (0.2) holds only when $q - q' = 0$ and $r - r' = 0$. Thus q and r are unique. □

Proposition 0.5.6 (Cancellation Law) *Suppose $f, g, h \in \mathbb{F}[x]$ with $f \neq 0$. If $fg = fh$ then $g = h$.*

Proof: The identity $fg = fh$ implies $f(g - h) = 0$. By Proposition 0.5.3, $\deg f + \deg(g - h) = -\infty$. Since $\deg f \geq 0$, $\deg(g - h) = -\infty$. Hence $g = h$. □

Definition 0.5.7 Suppose $a, b \in \mathbb{F}[x]$. If there is a polynomial $c \in \mathbb{F}[x]$ such that $a = bc$, then b is called a *factor* of a (or a is *divisible* by b; or b *divides* a), and is denoted by $b|a$.

Definition 0.5.8 Let $f, g \in \mathbb{F}[x]$. A polynomial $d \in \mathbb{F}[x]$ is called a *common divisor of f and g*, if $d|f$ and $d|g$.

Lemma 0.5.9 *Suppose f and g are nonzero monic polynomials in $\mathbb{F}[x]$. If $f|g$ and $g|f$, then $f = g$.*

Proof: Since $f|g$ and $g|f$, then $g = af$ and $f = bg$ for some $a, b \in \mathbb{F}[x]$. Then $f = baf$. By Proposition 0.5.6, $ba = 1$. By Proposition 0.5.3, $a, b \in \mathbb{F}$. Since both f and g are monic, $a = b = 1$ and hence $f = g$. □

Theorem 0.5.10 *Let $f, g \in \mathbb{F}[x]$ with $f \neq 0$. There exists a unique polynomial $d \in \mathbb{F}[x]$ satisfying the following conditions:*

(1) d is monic;

(2) d is a common divisor of f and g;

(3) if h is a common divisor of f and g, then $h|d$;

(4) $d = fs + gt$ for some $s, t \in \mathbb{F}[x]$.

Proof: Let $T = \{fs + gt \mid s, t \in \mathbb{F}[x]\}$. This set contains nonzero polynomials (for example f^2) and thus contains monic polynomials. By an argument similar to the proof of Theorem 0.5.5, among all the monic polynomials in T, there exists $d = fs + gt$ which is one of smallest degree. Then (1) and (4) hold. (3) is an easy consequence of (4).

By Theorem 0.5.5, we have $f = dq + r$ with $\deg r < \deg d$. Then $r = f - dq = f - (fs + gt)q = (1 - qs)f - qtg$.

If $r \neq 0$ and a is the leading coefficient of r, then $a^{-1}r$ is a monic polynomial in T of smaller degree than d. This contradicts the choice of d, so $r = 0$ and $d|f$. Similarly, $d|g$. So (2) holds.

Finally, suppose d' is another polynomial satisfying (1), (2) and (3), then $d'|d$ and $d|d'$. By Lemma 0.5.9, $d = d'$. □

The monic polynomial d in Theorem 0.5.10 is called the *greatest common divisor of f and g* in $\mathbb{F}[x]$ and is denoted by g.c.d.(f, g). If g.c.d$(f, g) = 1$, f and g are said to be *relatively prime* in $\mathbb{F}[x]$.

Definition 0.5.11 Let $f \in \mathbb{F}[x]$ with $\deg f \geq 1$. The polynomial f is called *reducible in* $\mathbb{F}[x]$ or *reducible over* $\mathbb{F}$ if $f = p_1 p_2$, where $p_1, p_2 \in \mathbb{F}[x]$ with $\deg p_i < \deg f$ for $i = 1, 2$. A polynomial which is not reducible in $\mathbb{F}[x]$ is called *irreducible in* $\mathbb{F}[x]$ or *irreducible over* $\mathbb{F}$.

Thus, f is irreducible in $\mathbb{F}[x]$ if and only if whenever $p|f$ then either p is a constant polynomial or $p = cf$ where $c \in \mathbb{F}$.

Example 0.5.12 Suppose $f \in \mathbb{F}[x]$ with $\deg f = 1$. Suppose $f = pq$ for some $p, q \in \mathbb{F}[x]$. Since $f \neq 0$, $p \neq 0$ and $q \neq 0$. Hence $\deg p \geq 0$ and $\deg q \geq 0$. By Proposition 0.5.3, $1 = \deg p + \deg q$. Thus one of p and q is a constant polynomial. So f is irreducible. □

Theorem 0.5.13 *Let p be irreducible in $\mathbb{F}[x]$. If p divides a product fg, then p divides either f or g.*

Proof: Since $p|fg$, $pb = fg$ for some $b \in \mathbb{F}[x]$.

Let $d =$ g.c.d.(p, f). Then $d|p$. Since p is irreducible, either $\deg d = 0$ (so $d = 1$) or $\deg d = \deg p$. In the second case, $p = ad$ for some $a \in \mathbb{F}$. So $p|f$.

If $d = 1$, then by Theorem 0.5.10 we have $1 = ps + ft$ for some $s, t \in \mathbb{F}[x]$. Hence $g = gps + gft = gps + pbt = p(gs + bt)$. We have $p|g$. □

Theorem 0.5.14 *Let $f(x) \in \mathbb{F}[x]$. Suppose* $\deg f \geq 1$. *Then*

(1) $f(x) = ap_1(x)p_2(x)\cdots p_m(x)$, where $a \in \mathbb{F}$ and $p_i(x)$ is monic and irreducible for each i;

(2) the factorization in (1) is unique except for the order of the factors

Proof: For (1), it suffices to prove that $f(x) = q_1(x)q_2(x)\cdots q_m(x)$, where each $q_i(x)$ is irreducible. The reason is that suppose a_i is the leading coefficient of $q_i(x)$, we take $p_i(x) = a_i^{-1}q_i(x)$ and $a = a_1 a_2 \cdots a_m$.

We shall prove it by mathematical induction on $\deg f$. Suppose $\deg f = 1$. By Example 0.5.12, f is irreducible.

For $n > 1$, we assume that (1) holds for every polynomial $g(x)$ with $\deg g < n$. Suppose $\deg f = n$. If $f(x)$ is irreducible, then we are done. If $f(x)$ is reducible, then $f(x) = p(x)q(x)$ for some $p(x), q(x) \in \mathbb{F}[x]$ with $\deg p < \deg f$ and $\deg q < \deg f$. By induction assumption, both $p(x)$ and $q(x)$ are products of irreducible polynomials. And so is $f(x)$.

Now, we are going to prove (2) by contradiction. Suppose (2) does not hold. Let $f(x)$ be a nonconstant polynomial of minimal degree that has two different factorizations:

$$f(x) = ap_1(x)p_2(x)\cdots p_m(x) = bq_1(x)q_2(x)\cdots q_k(x), \tag{0.3}$$

where $a, b \in \mathbb{F}$ and $p_i(x)$'s, $q_j(x)$'s are monic irreducible polynomials in $\mathbb{F}[x]$. Since a and b are the leading coefficients of $f(x)$, $a = b$. Applying Theorem 0.5.13 repeatedly, we have that $p_1(x)|q_j(x)$ for some j, say $p_1(x)|q_1(x)$. Since $\deg p_1 \geq 1$ and $q_1(x)$ is irreducible, $cp_1(x) = q_1(x)$ for some $c \in \mathbb{F}$. Since $p_1(x)$ and $q_1(x)$ are monic, $c = 1$ and $p_1(x) = q_1(x)$. By Proposition 0.5.6, we have

$$g(x) = p_2(x)\cdots p_m(x) = q_2(x)\cdots q_k(x)$$

Then $g(x)$ has two different factorizations. But $\deg g < \deg f$. This contradicts the choice of $f(x)$. □

As we mentioned in the Definition 0.5.1, $\mathbb{F}$ need not be a field. So we consider the ring $(\mathbb{F}[x])[y]$ for another indeterminate y. This ring is called the *polynomial ring with two indeterminates x and y*. This ring is often denoted by $\mathbb{F}[x, y]$. Every element of $\mathbb{F}[x, y]$ has the form

$$f(x, y) = p_0(x) + p_1(x)y + p_2(x)y^2 + \cdots + p_n(x)y^n,$$

for some $n \in \mathbb{N}_0$ and $p_j(x) \in \mathbb{F}[x]$. If we write $p_j(x) = \sum_{i\geq 0} a_{ij}x^i$ as a finite sum, where $a_{ij} \in \mathbb{F}$, then $f(x, y)$ becomes a finite double sum:

$$f(x, y) = \sum_{i\geq 0}\sum_{j\geq 0} a_{ij}x^i y^j = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \cdots .$$

Moreover, each x and y commutes with the other and with every element of $\mathbb{F}$. Thus we may interchange the role of x and y, that is, $\mathbb{F}[x, y] = \mathbb{F}[y, x]$. Note that $f(x, y) \neq f(y, x)$ for $f(x, y) \in \mathbb{F}[x, y]$ in general. Follow the above process, one can define polynomial in n indeterminates $x_1, x_2, \ldots, x_n$ and the polynomial ring $\mathbb{F}[x_1, x_2, \ldots, x_n]$. We do not discuss here[2].

Exercise 0.5

0.5-1. If $f \in \mathbb{F}[x]$, and $c \in \mathbb{F}$ such that $f(c) = 0$, then c is called a *root* of f. Show that c is a root of f if and only if $x - c$ is a factor of $f(x)$.

0.5-2. Let $f \in \mathbb{F}[x]$ of degree n. Show by mathematical induction that f has at most n roots in $\mathbb{F}$.

0.5-3. Suppose that $\mathbb{F}$ is a field with $1 + 1 \neq 0$. Show that $f(x) = x^2 - 1$ has two distinct roots in $\mathbb{F}$.

0.5-4. Factor $x^4 - 4$ into irreducible factors over $\mathbb{Q}$, over $\mathbb{R}$, and over $\mathbb{C}$.

0.5-5. Factor $x^4 - 16$ into irreducible factors over $\mathbb{Q}$, over $\mathbb{R}$, and over $\mathbb{C}$.

0.5-6. Show that $x^2 + 2$ is irreducible over $\mathbb{Z}_5$ but reducible over $\mathbb{Z}_3$.

0.5-7. We can also apply Euclidean Algorithm on polynomials over a field. Try to find a monic polynomial $d(x)$ such that $d(x) =$g.c.d.$(f(x), g(x))$, where $f(x) = x^3 + 1$ and $g(x) = x^4 + x^3 + 2x^2 + x - 1$. Express this g.c.d. as a linear combination of the polynomials $f(x)$ and $g(x)$.

[2]The interested reader is referred to any book of abstract algebra or modern algebra. For example, N. Jacobson, *Basic Algebra I*, 2nd edition, Freeman, 1985; W.K. Nicholson, Introduction to Abstract Algebra, 2nd edition, Wiley, 1999.

Chapter 1

Matrices

1.1 Definitions and Notation

In geometry, if we want to find the intersection of two straight lines or to find the intersection of three planes, then we have to solve a system of equations. Those equations are called linear equation, since the degree of those unknowns are 1. Let us consider the following example.

Example 1.1.1 Let $3x + 6y = 1$, $y + z = 2$ and $-x + z = 3$ be equations of three planes in $\mathbb{R}^3$. Find the intersection point of these planes.

We have to solve the following equations simultaneously:

$$\begin{cases} 3x + 6y = 1, \\ y + z = 2, \\ -x + z = 3. \end{cases}$$

In secondary school we use some eliminations to solve it. Later we will introduce an efficient method which is modified from those eliminations. □

When apply the elimination to solve the above system of equations, we can see that only the coefficients of the unknowns and the constant term (the right hand side of the equations) involve the elimination. So for convenience we often arrange the coefficients and the constant terms into two arrays (called matrices) as follows:

$$A = \begin{pmatrix} 3 & 6 & 0 \\ 0 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} \qquad \boldsymbol{b} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}.$$

Now we are going to make the formal definition of matrix.

Definition 1.1.2 A *matrix* over a set S is a rectangular array of elements of S. A matrix with m rows and n columns is called an $m \times n$ *matrix* or *matrix of size* $m \times n$ (read as m by n matrix). If $m = n$, then the matrix is called a *square matrix of order* n (or *size* n). We use the notation

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

to describe an $m \times n$ matrix, where $a_{ij} \in S$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. For short, we use $A = (a_{ij})$. This notation indicates that A is the matrix whose general (i, j)-*th entry* (or *elements*) is a_{ij}. To avoid some confusion we shall use the notation $(A)_{i,j}$ to denote the (i, j)-th entry of A.

In the following we only consider the case that S is a field $\mathbb{F}$. For convenience, we denote $M_{m,n}(\mathbb{F})$ (or $\mathbb{F}^{m\times n}$) to be the set of all $m \times n$ matrices over $\mathbb{F}$. If $m = n$, then we use $M_n(\mathbb{F})$ instead of $M_{n,n}(\mathbb{F})$.

Definition 1.1.3 Two matrices A and B are said to be *equal*, which is denoted by $A = B$, if they are both of the same size and $(A)_{i,j} = (B)_{i,j} \quad \forall i, j$.

Example 1.1.4 $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ is a 2×3. $B = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$ is a square matrix of order 3. Suppose C is a 3×3 matrix with $(C)_{i,j} = i^j$. Then $C = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2^2 & 2^3 \\ 3 & 3^2 & 3^3 \end{pmatrix}$. Suppose D is a 2×4 matrix defined by $(D)_{i,j} = i - j$. Then $D = \begin{pmatrix} 0 & -1 & -2 & -3 \\ 1 & 0 & -1 & -2 \end{pmatrix}$. □

Definition 1.1.5 Suppose $A = (a_{ij}) \in M_{m,n}(\mathbb{F})$. For $1 \leq i \leq m$, the i-*th row* of A is the $1 \times n$ matrix $\begin{pmatrix} a_{i1} & \cdots & a_{in} \end{pmatrix}$ which is usually denoted by A_{i*}. For $1 \leq j \leq n$, the j-*th column* of A is the $m \times 1$ matrix $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ and is usually denoted by A_{*j}.

Example 1.1.6 Using Example 1.1.4, we have

$$A_{1*} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \quad A_{*2} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \quad B_{*3} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad C_{2*} = \begin{pmatrix} 2 & 2^2 & 2^3 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 8 \end{pmatrix}.$$

□

Definition 1.1.7 An $m \times n$ *zero matrix*, which is often denoted by O (or $O_{m,n}$), is a matrix whose entries are all zero. If $m = n$, then we use O_n instead of $O_{n,n}$. If $A = (a_{ij}) \in M_{m,n}(\mathbb{F})$, then the sequence of entries $\{a_{11}, a_{22}, \ldots, a_{tt}\}$, where $t = \min\{m, n\}$, is called the *main diagonal* of A. A square matrix with zero entries everywhere except in the main diagonal is called a *diagonal matrix*. The *identity matrix of order* n, which is often denoted by I or I_n, is a diagonal matrix of order n with all entries in the diagonal are all equal to 1.

For integers i, j, we define a notation δ_{ij} by

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

This is called the *Kronecker delta*. Then $(I_n)_{i,j} = \delta_{ij}$ for $1 \leq i, j \leq n$. Clearly, $\delta_{ij} = \delta_{ji}$.

Definition 1.1.8 Let U and L be $n \times n$ matrices. U is said to be *upper triangular* if $(U)_{i,j} = 0 \; \forall \; i > j$ and L is said to be *lower triangular* if $(L)_{i,j} = 0 \; \forall \; i < j$.

Therefore, a diagonal matrix is both upper and lower triangular matrix.

Some special notational conventions are described below. An element in $\mathbb{F}^n$ called a vector is usually denoted by $(x_1, \ldots, x_n)$. However, we use $n \times 1$ matrix $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ to represent this vector.

$\mathbf{0} = \mathbf{0}_n$ is a column vector of size $n \times 1$ whose entries are 0, i.e., $\mathbf{0}_n = O_{n,1}$.
$\mathbf{1} = \mathbf{1}_n$ is a column vector of size $n \times 1$ whose entries are 1.
The *standard unit vectors* of size $n \times 1$:

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \cdots, \boldsymbol{e}_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Note that the standard unit vectors are the columns of I_n.
$J = J_{m,n}$ is an $m \times n$ matrix whose entries are 1. Thus $\mathbf{1}_n = J_{n,1}$.

1.2 Algebra of Matrices

In this section we shall introduce addition, scalar multiplication, multiplication and transpose of matrices.

Definition 1.2.1 Let $A, B \in M_{m,n}(\mathbb{F})$. The *sum* of A and B, denoted by $A + B$, is an $m \times n$ matrix whose (i, j)-th entry is the sum of the (i, j)-th entries of A and B, i.e., $(A+B)_{i,j} = (A)_{i,j}+(B)_{i,j}$ $\forall\, 1 \leq i \leq m$, $1 \leq j \leq n$. The operation "+" is called the *addition* (of matrices).

Example 1.2.2 Let $A = \begin{pmatrix} 8 & -7 & 4 \\ -2 & 9 & -6 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 2 & 0 \\ -1 & -3 & -5 \end{pmatrix}$. Then

$$A + B = \begin{pmatrix} 11 & -5 & 4 \\ -3 & 6 & -11 \end{pmatrix}.$$ □

Proposition 1.2.3 *Let $A, B, C \in M_{m,n}(\mathbb{F})$. Then we have*

(1)	$A + B = B + A$	*Commutativity of addition*
(2)	$A + (B + C) = (A + B) + C$	*Associativity of addition*
(3)	$A + O = A$	*Identity of addition*
(4)	*there is a unique matrix A' such that $A + A' = O$*	*Inverse of addition*

Proof: We leave to the reader the proofs of (1), (2) and (3). Suppose $(A)_{i,j} = a_{ij}$. Let A' be an $m \times n$ matrix defined by $(A')_{i,j} = -a_{ij}$. Then it is clear that $A + A' = O$. Suppose there is a matrix $A'' \in M_{m,n}(\mathbb{F})$ such that $A + A'' = O$. Then

$$A'' = A'' + O = A'' + (A + A') = (A'' + A) + A' = O + A' = A'.$$

(4) is proved. □

Since the additive inverse of A is unique, we use $-A$ to denote it.

Definition 1.2.4 Let $A \in M_{m,n}(\mathbb{F})$ and $c \in \mathbb{F}$. We define $cA \in M_{m,n}(\mathbb{F})$ by $(cA)_{i,j} = c(A)_{i,j} \forall\ 1 \leq i \leq m,\ 1 \leq j \leq n$. This multiplication is called *scalar multiplication* and cA is called the *scalar product* of A by c.

Example 1.2.5 Let A be the matrix as in Example 1.2.2. Then

$$3A = \begin{pmatrix} 24 & -21 & 12 \\ -6 & 27 & -18 \end{pmatrix}. \qquad \square$$

Proposition 1.2.6 *Let $A, B \in M_{m,n}(\mathbb{F}), c, d \in \mathbb{F}$. Then we have*

(1) $c(A+B) = cA + cB$ *Left distributive law for scalar multiplication*
(2) $(c+d)A = cA + dA$ *Right distributive law for scalar multiplication*
(3) $(cd)A = c(dA)$ *Associativity of scalar multiplication*
(4) $1A = A$ *and* $(-1)A = -A$.
(5) Suppose $A \neq O$ *and* $cA = O$. *Then* $c = 0$.

Proof:

$$\begin{aligned} (c(A+B))_{i,j} &= c(A+B)_{i,j} && \text{definition of the scalar multiplication} \\ &= c((A)_{i,j} + (B)_{i,j}) && \text{definition of the addition} \\ &= c(A)_{i,j} + c(B)_{i,j} && \text{distributive law of field} \\ &= (cA + cB)_{i,j} && \text{definition of the addition} \end{aligned}$$

We leave the proofs of (2) and (3) to the reader.

By definition of the scalar multiplication, we have $1A = A$. By (2) and the definition, we have

$$A + (-1)A = (1 + (-1))A = 0A = O.$$

Since the inverse of addition is unique, $(-1)A = -A$. Hence (4) holds.

For (5), suppose $c \neq 0$. Then $c^{-1}(cA) = O$. This implies that $A = O$. It is a contradiction. $\square$

Consider the Example 1.1.1. If we arrange the unknowns as the matrix $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, then can we write the system as the form $AX = \boldsymbol{b}$? Here A and $\boldsymbol{b}$ are described in Example 1.1.1. To do this we have to introduce a multiplication for matrices.

Definition 1.2.7 Let $B \in M_{p,m}(\mathbb{F})$ and $A \in M_{m,n}(\mathbb{F})$. We define the *product* $BA \in M_{p,n}(\mathbb{F})$ by

$$(BA)_{k,j} = (B)_{k,1}(A)_{1,j} + (B)_{k,2}(A)_{2,j} + \cdots + (B)_{k,m}(A)_{m,j} = \sum_{i=1}^{m} (B)_{k,i}(A)_{i,j}$$

for $1 \leq k \leq p,\ 1 \leq j \leq n$.

Example 1.2.8 Let $B = \begin{pmatrix} -1 & 0 \\ 1 & -1 \\ 2 & -1 \\ 0 & 1 \end{pmatrix}$ $A = \begin{pmatrix} 8 & -7 & 4 \\ -2 & 9 & -6 \end{pmatrix}$. Then

$BA = \begin{pmatrix} -8 & 7 & -4 \\ 10 & -16 & 10 \\ 18 & -23 & 14 \\ -2 & 9 & -6 \end{pmatrix}$. Note that AB is undefined. $\square$

Remark 1.2.9 Note that B and A must be of the proper size in order that BA is defined. Even if AB is defined, AB may not equal to BA. For example, $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ then $AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Thus matrix multiplication is *not commutative*. Also note that the product of two nonzero matrices may be a zero matrix as the above example shown.

Proposition 1.2.10 *For matrices A, B and C (whenever the statement involves the matrix multiplication, the sizes of A, B, C and the identity matrix I are chosen properly), and $c \in \mathbb{F}$, we have*

(1)	$(cA)B = A(cB) = c(AB)$	*Scalar pull through*
(2)	$(AB)C = A(BC)$	*Associativity of multiplication*
(3)	$AI = A$, $IB = B$	*Identity for multiplication*
(4)	$A(B + C) = AB + AC$	*Left distributive law*
(5)	$(A + B)C = AC + BC$	*Right distributive law.*

Proof: We leave the proof of (1) to the reader. Suppose $A \in M_{p,m}(\mathbb{F})$, $B \in M_{m,n}$ and $C \in M_{n,q}(\mathbb{F})$. Then $AB \in M_{p,n}(\mathbb{F})$ and $BC \in M_{m,q}(\mathbb{F})$. Also it can be seen that $(AB)C$ and $A(BC)$ are matrices in $M_{p,q}(\mathbb{F})$. For any i, j with $1 \le i \le p$ and $1 \le j \le q$,

$$\begin{aligned}((AB)C)_{i,j} &= \sum_{r=1}^{n}(AB)_{i,r}(C)_{r,j} = \sum_{r=1}^{n}\sum_{s=1}^{m}[(A)_{i,s}(B)_{s,r}](C)_{r,j} \\ &= \sum_{r=1}^{n}\sum_{s=1}^{m}(A)_{i,s}[(B)_{s,r}(C)_{r,j}] = \sum_{s=1}^{m}\sum_{r=1}^{n}(A)_{i,s}[(B)_{s,r}(C)_{r,j}] \\ &= \sum_{s=1}^{m}(A)_{i,s}\left[\sum_{r=1}^{n}(B)_{s,r}(C)_{r,j}\right] = \sum_{s=1}^{m}(A)_{i,s}(BC)_{s,j} = (A(BC))_{i,j}.\end{aligned}$$

Hence $(AB)C = A(BC)$ and then (2) holds.

Suppose $A \in M_{m,n}(\mathbb{F})$ and $I = I_n$. Then $AI \in M_{m,n}(\mathbb{F})$. For any i, j with $1 \le i \le m$ and $1 \le j \le n$,

$$(AI)_{i,j} = \sum_{k=1}^{n}(A)_{i,k}(I)_{k,j} = \sum_{k=1}^{n}(A)_{i,k}\delta_{kj} = (A)_{i,j}.$$

Thus $AI = A$. The proof of $IB = B$ is left to the reader.

Suppose $A \in M_{p,m}(\mathbb{F})$, $B, C \in M_{m,n}$. Then $A(B + C)$, AB and AC are in $M_{p,n}(\mathbb{F})$. For any i, j with $1 \le i \le p$ and $1 \le j \le n$,

$$\begin{aligned}(A(B + C))_{i,j} &= \sum_{k=1}^{m}(A)_{i,k}(B + C)_{k,j} = \sum_{k=1}^{m}(A)_{i,k}[(B)_{k,j} + (C)_{k,j}] \\ &= \sum_{k=1}^{m}(A)_{i,k}(B)_{k,j} + (A)_{i,k}(C)_{k,j} \\ &= \sum_{k=1}^{m}(A)_{i,k}(B)_{k,j} + \sum_{k=1}^{m}(A)_{i,k}(C)_{k,j} = (AB)_{i,j} + (AC)_{i,j} \\ &= (AB + AC)_{i,j}.\end{aligned}$$

Hence (4) holds. Also we leave the proof of (5) to the reader. □

Example 1.2.11 We try to use changing variables to solve the problem in Example 1.1.1. Let

$$\begin{cases} x &= -a &+ 2b &- 2c, \\ y &= a &- b &+ c, \\ z &= -a &+ 2b &- c. \end{cases}$$

We have $X = B\begin{pmatrix} a \\ b \\ c \end{pmatrix}$, where $B = \begin{pmatrix} -1 & 2 & -2 \\ 1 & -1 & 1 \\ -1 & 2 & -1 \end{pmatrix}$ and $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$. Let $Y = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. Substituting into the equations we have $A(BY) = \boldsymbol{b}$. By the associative law, we have $(AB)Y = \boldsymbol{b}$. Since $AB = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, we get $\begin{pmatrix} 3a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$. That is $a = \frac{1}{3}, b = 2$ and $c = 3$. Hence $x = -\frac{7}{3}$, $y = \frac{4}{3}$ and $z = \frac{2}{3}$.

□

Note that, it is because that the associative law holds for addition, scalar multiplication and multiplication, we can omit the parentheses "( )". Let A be a square matrix and n a positive integer. A^n denotes the product of n A's, i.e., $A^n = \overbrace{AA\cdots A}^{n \text{ times}}$.

Definition 1.2.12 The *transpose* A^T of a matrix $A = (a_{ij}) \in M_{m,n}(\mathbb{F})$ is the matrix in $M_{n,m}(\mathbb{F})$ that whose (i,j)-th entry is a_{ji}. That is,

$$(A^T)_{i,j} = (A)_{j,i} \; \forall \; i = 1, \ldots, n, \; j = 1, \ldots, m.$$

Example 1.2.13 Let A be the matrix in Example 1.2.2. Then

$$A^T = \begin{pmatrix} 8 & -2 \\ -7 & 9 \\ 4 & -6 \end{pmatrix}.$$

□

Proposition 1.2.14 *For matrices A and B (when the statement includes the matrix multiplication, the sizes of A and B are chosen suitably), we have*

(1) $(A^T)^T = A$ *Transpose of the transpose*
(2) $(A+B)^T = A^T + B^T$ *Transpose of a sum*
(3) $(AB)^T = B^T A^T$ *Transpose of a product.*
(4) $(cA)^T = cA^T$ *for* $c \in \mathbb{F}$.

Proof: We only prove (3). Suppose $A \in M_{p,m}(\mathbb{F})$ and $B \in M_{m,n}$. Then $(AB)^T$ and $B^T A^T$ are $n \times p$ matrices. For $1 \le i \le n$ and $1 \le j \le p$,

$$\begin{aligned} ((AB)^T)_{i,j} = (AB)_{j,i} &= \sum_{k=1}^{m} (A)_{j,k}(B)_{k,i} = \sum_{k=1}^{m} (A^T)_{k,j}(B^T)_{i,k} \\ &= \sum_{k=1}^{m} (B^T)_{i,k}(A^T)_{k,j} = (B^T A^T)_{i,j}. \end{aligned}$$

Hence $(AB)^T = B^T A^T$. □

Definition 1.2.15 A square matrix S is called *symmetric* if $S^T = S$, i.e., $(S)_{i,j} = (S)_{j,i} \; \forall \; i,j$. A square matrix A is called *skew-symmetric* if $A^T = -A$, i.e., $(A)_{i,j} = -(A)_{j,i} \; \forall \; i,j$.

When in matrix computation we may only be interested in certain part of the matrix which we may save in the computer program. Sometimes when multiplying two matrices, it is much simpler when we partition matrices properly and then multiply the partitioned matrix just like the usual multiplication of matrices.

Let A be a matrix. By a *submatrix* of A, we mean any matrix obtained from A by deleting any number of rows and any number of columns. A matrix is always a submatrix of itself.

Example 1.2.16 Let $A = (a_{ij})$ be an $m \times n$ matrix. Recall that $A_{i*} = \begin{pmatrix} a_{i1} & \cdots & a_{in} \end{pmatrix}$. Thus $A = \left(\begin{array}{c} A_{1*} \\ \hline \vdots \\ \hline A_{m*} \end{array}\right)$. Hence $A^T = \left(\begin{array}{c|c|c} A_{1*}^T & \cdots & A_{m*}^T \end{array}\right)$. Also if $A_{*j} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$, then $A = \left(\begin{array}{c|c|c} A_{*1} & \cdots & A_{*n} \end{array}\right)$ and $A^T = \left(\begin{array}{c} A_{*1}^T \\ \hline \vdots \\ \hline A_{*n}^T \end{array}\right)$. □

Note that the lines between rows or columns are not necessary. Let $A \in M_{m,n}(\mathbb{F})$. Suppose that there are two partitions of m and n. Namely, $m = m_1 + \cdots + m_r$ and $n = n_1 + \cdots + n_s$ for some positive integers m_i, n_j $(1 \le i \le r,\ 1 \le j \le s)$. Then A can be partitioned into rs submatrices as the block form:

$$A = \left(\begin{array}{c|c|c} A^{1,1} & \cdots & A^{1,s} \\ \hline \vdots & \vdots & \vdots \\ \hline A^{r,1} & \cdots & A^{r,s} \end{array}\right), \text{ where each } A^{i,j} \text{ is an } m_i \times n_j \text{ submatrices of } A.$$

Suppose B is an $n \times p$ matrix of the block form $B = \left(\begin{array}{c|c|c} B^{1,1} & \cdots & B^{1,t} \\ \hline \vdots & \vdots & \vdots \\ \hline B^{s,1} & \cdots & B^{s,t} \end{array}\right)$, where $p = p_1 + \cdots + p_t$, $p_1, \ldots, p_t$ are positive integers and each $B^{j,k}$ is an $n_j \times p_k$ submatrices of B. Let $C = AB$. Then C is an $m \times p$ matrix which may be partitioned in the block form: $C = \left(\begin{array}{c|c|c} C^{1,1} & \cdots & C^{1,t} \\ \hline \vdots & \vdots & \vdots \\ \hline C^{r,1} & \cdots & C^{r,t} \end{array}\right)$, where each $C^{i,k}$ is an $m_i \times p_k$ submatrices of C. By a tedious but straightforward verification, one can show that $C^{i,k} = \sum_{j=1}^{s} A^{i,j}B^{j,k}$ for each i, k. The proof is put in the appendix. Such multiplication is usually referred as *partitioned multiplication* or *block multiplication*. Thus when we multiply two matrices in the block form, we may regard blocks as entries and multiply in the usual way.

Example 1.2.17 Let

$$A = \left(\begin{array}{ccc|cc|cc} 1 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & -1 & -1 & -1 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 2 & 3 & 1 & 2 \end{array}\right)$$

and

$$B = \left(\begin{array}{rrr|rrrr} 1 & 2 & 3 & 1 & 1 & 0 & 1 \\ 0 & 1 & 2 & -3 & -1 & 0 & -1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 2 & 2 & 1 & -3 & 0 & 0 & 0 \\ -2 & 3 & -1 & 0 & -1 & 1 & 2 \\ \hline 0 & 1 & 0 & 1 & 3 & 0 & 2 \\ 1 & 0 & 0 & 2 & 0 & -1 & 0 \end{array}\right).$$

Let $C = AB$. Then C can be written as a block form:

$$C = \left(\begin{array}{c|c|c} C^{1,1} & C^{1,2} & C^{1,3} \\ \hline C^{2,1} & C^{2,2} & C^{2,3} \\ \hline C^{3,1} & C^{3,2} & C^{3,3} \end{array}\right),$$

where $C^{1,1}$ is a 2×1 matrix, $C^{1,2}$ is a 2×2 matrix, $C^{1,3}$ is 2×4 matrix and so on. We consider the matrix $C^{1,3}$.

$$\begin{aligned} C^{1,3} &= A^{1,1}B^{1,3} + A^{1,2}B^{2,3} + A^{1,3}B^{3,3} \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 1 \\ -3 & -1 & 0 & -1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \\ &\quad + \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -3 & 0 & 0 & 0 \\ 0 & -1 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 0 & 2 \\ 2 & 0 & -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -2 & 0 & 0 & 0 \\ 3 & 0 & -1 & 0 \end{pmatrix} + \begin{pmatrix} -3 & -2 & 2 & 4 \\ 3 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 4 & 6 & -1 & 4 \\ 3 & 3 & -1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 4 & 1 & 8 \\ 9 & 3 & -2 & 2 \end{pmatrix}. \end{aligned}$$

One can compute all the $C^{i,j}$'s and obtains

$$C = \left(\begin{array}{rrr|rrrr} 0 & 13 & 4 & -1 & 4 & 1 & 8 \\ -2 & -2 & -3 & 9 & 3 & -2 & 2 \\ \hline 5 & 5 & 4 & 1 & 5 & 0 & 4 \\ 0 & 3 & -1 & 2 & 0 & 1 & 3 \\ \hline 0 & 15 & 1 & -4 & -1 & 1 & 7 \end{array}\right).$$

Also one can compute AB directly to verify the result. □

Example 1.2.18 Let A be an $m \times n$ matrix and B be an $n \times p$ matrix. Suppose B_{*j} is the j-th column of B. By using the block multiplication we have

$$AB = A(B_{*1}\ B_{*2}\ \cdots\ B_{*p}) = (AB_{*1}\ AB_{*2}\ \cdots\ AB_{*p}).$$

Thus AB records the product of A with B_{*1}, B_{*2}, $\ldots$, B_{*p}. Similarly if we suppose A_{i*} is the i-th row of A, then AB takes the form:

$$\begin{pmatrix} A_{1*}B \\ A_{2*}B \\ \vdots \\ A_{m*}B \end{pmatrix}.$$

□

Example 1.2.19 If $A = \left(\begin{array}{c|c} A^{1,1} & A^{1,2} \\ \hline A^{2,1} & A^{2,2} \end{array}\right)$. Then $A^T = \left(\begin{array}{c|c} (A^{1,1})^T & (A^{2,1})^T \\ \hline (A^{1,2})^T & (A^{2,2})^T \end{array}\right)$. □

The following two examples show that the block multiplication may simplify the computation process.

Example 1.2.20 Compute A^3, where $A = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & -1 & 1 \end{pmatrix}$.

Let $D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix}$. Then $A = \begin{pmatrix} D & O_{3,2} \\ O_{2,3} & B \end{pmatrix}$, $A^2 = \begin{pmatrix} D^2 & O_{3,2} \\ O_{2,3} & B^2 \end{pmatrix}$ and $A^3 = \begin{pmatrix} D^3 & O_{3,2} \\ O_{2,3} & B^3 \end{pmatrix}$.

It is easy to see that $D^3 = \begin{pmatrix} 8 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. We only need to compute B^3.

$B^2 = \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 9 \\ -3 & -2 \end{pmatrix}$ and hence

$B^3 = \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 9 \\ -3 & -2 \end{pmatrix} = \begin{pmatrix} -7 & 12 \\ -4 & -11 \end{pmatrix}$. Then

$$A^3 = \begin{pmatrix} 8 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -7 & 12 \\ 0 & 0 & 0 & -4 & -11 \end{pmatrix}.$$

□

Example 1.2.21 Let $A = \left(\begin{array}{c|c} O_k & I_k \\ \hline B & O_k \end{array}\right)$, where B is a $k \times k$ matrix. Then

$$A^2 = \begin{pmatrix} O_k & I_k \\ B & O_k \end{pmatrix}\begin{pmatrix} O_k & I_k \\ B & O_k \end{pmatrix} = \begin{pmatrix} B & O_k \\ O_k & B \end{pmatrix}.$$

$$A^4 = A^2A^2 = \begin{pmatrix} B^2 & O_k \\ O_k & B^2 \end{pmatrix}.$$

$$A^3 = A^2A = \begin{pmatrix} B & O_k \\ O_k & B \end{pmatrix}\begin{pmatrix} O_k & I_k \\ B & O_k \end{pmatrix} = \begin{pmatrix} O_k & B \\ B^2 & O_k \end{pmatrix}.$$

□

Exercise 1.2

1.2-1. Let $A = \begin{pmatrix} -2 & 1 & 3 \\ 4 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 3 & 1 \\ -4 & 0 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 2 & -1 \\ 0 & 6 \\ 2 & 3 \end{pmatrix}$, $D = \begin{pmatrix} 0 & 1 \\ 2 & 3 \\ -1 & -1 \end{pmatrix}$. Find the following matrices if they are defined
(a) $(-2)A$; (b) $A + 3B$; (c) $B + C$; (d) $BC - CB$; (e) $(A + B)C$;
(f) $A^T A$; (g) ADB.

1.2-2. Let $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Find A^k for $k \geq 1$.

1.2-3. Let $A = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$. Compute AA^T and $A^T A$.

1.2-4. Let $A = I_n + N$ be an $n \times n$ matrix with $N^r = O$ for some $r \geq 0$. Express A^k in terms of $I_n, N, N^2, \ldots, N^{r-1}$ for $k \geq r$.

1.2-5. Generalize the above problem. Let $A, N \in M_n(\mathbb{F})$. Suppose $N^r = O$ for some $r \geq 0$ and $AN = NA$. Find $(A + N)^k$ for $k \geq r$.

1.2-6. Complete the proof of Proposition 1.2.3.

1.2-7. Complete the proof of Proposition 1.2.6.

1.2-8. Complete the proof of Proposition 1.2.10.

1.2-9. Complete the proof of Proposition 1.2.14.

1.2-10. Let A and B be square matrices. Is $(A + B)^2 = A^2 + 2AB + B^2$? If so, prove it; if not, give a counterexample and state under what conditions the equation is true.

1.2-11. Let A and B be square matrices. Is $(A - B)(A + B) = A^2 - B^2$? If so, prove it; if not, give a counterexample and state under what conditions the equation is true.

1.2-12. Suppose $\boldsymbol{e}_j$'s are the standard unit vectors of size $n \times 1$, $1 \leq j \leq n$. Prove that if A in an $m \times n$ matrix, then $A\boldsymbol{e}_j = A_{*j}$.

1.2-13. Suppose $\boldsymbol{e}_i$'s are the standard unit vectors of size $m \times 1$, $1 \leq i \leq m$. Prove that if A in an $m \times n$ matrix, then $\boldsymbol{e}_i^T A = A_{i*}$.

1.2-14. Suppose A, B and C are nonzero matrices of suitable size such that the products can be defined. Give an example to show that $AB = AC$ does not imply $B = C$.

1.2-15. Let $A \in M_n(\mathbb{F})$. Define the *trace* of A by $\mathrm{Tr}(A) = \sum_{k=1}^{n} (A)_{k,k}$.

Suppose $A = \begin{pmatrix} 8 & -2 & 1 \\ -7 & 9 & 0 \\ 4 & -6 & -2 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & -1 & 4 \\ -3 & 6 & -3 \\ 0 & 1 & 1 \end{pmatrix}$. Find $\mathrm{Tr}(A)$, $\mathrm{Tr}(B)$, $\mathrm{Tr}(AB)$ and $\mathrm{Tr}(BA)$.

1.2-16. Suppose $A, B \in M_n(\mathbb{F})$.

(a) Prove that $\mathrm{Tr}(A^T) = \mathrm{Tr}(A)$.

(b) Prove that $\mathrm{Tr}(cA + dB) = c\mathrm{Tr}(A) + d\mathrm{Tr}(B)$ for all $c, d \in \mathbb{F}$.

(c) Prove that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

(d) Suppose A is skew-symmetric. Prove that entries in the diagonal of A are zero if $1 + 1 \neq 0$.

(e) Suppose $A \in M_{m,n}(\mathbb{F})$. Prove that both AA^T and A^TA are symmetric.

(f) Suppose A is a square matrix. Show that $A+A^T$ is symmetric and $A-A^T$ is skew-symmetric.

(g) If both A and B are two upper triangular (lower triangular) matrices, then so is AB.

1.2-17. Suppose $A \in M_n(\mathbb{F})$. Show that there exist a symmetric matrix S and a skew-symmetric matrix K such that $A = S + K$. Also show that such decomposition is unique. Here, we assume that $1 + 1 \neq 0$.

1.3 Non-singular Matrices

It is known that the identity matrix I is the multiplicative identity. Given a nonzero square matrix A. Can we always find a square matrix B such that $AB = I$? The answer is no. One can consider the matrices A and B defined in Remark 1.2.9. If there were a matrix C such that $AC = I$, then $O = OC = (BA)C = BI = B$. It yields a contradiction.

Definition 1.3.1 Let $A \in M_n(\mathbb{F})$. If there exists a matrix $B \in M_n(\mathbb{F})$ such that $AB = BA = I_n$, then we say that A is *invertible* or *non-singular*. A matrix which is not invertible is often called *singular*.

Lemma 1.3.2 *Let $A \in M_n(\mathbb{F})$. If there are $B, C \in M_n(\mathbb{F})$ such that $AB = CA = I$, then $B = C$.*

Proof: $B = IB = (CA)B = C(AB) = CI = C$. □

Thus the matrix B described in Definition 1.3.1 is unique. We called it the *inverse* of A and denote it by A^{-1}.

Remark 1.3.3 Note that if $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{n,m}(\mathbb{F})$ with $m \neq n$ such that $AB = I_m$ then BA may not be the identity matrix I_n. For example, let

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Then

$$AB = I_2 \text{ and } BA = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

In fact, we shall see that BA cannot be I_n.

Theorem 1.3.4 *Suppose A and B are non-singular matrices. Then*

(a) AB is non-singular and $(AB)^{-1} = B^{-1}A^{-1}$.

(b) A^{-1} is non-singular and $(A^{-1})^{-1} = A$.

(c) For $c \neq 0$, cA is non-singular and $(cA)^{-1} = c^{-1}A^{-1}$.

(d) A^T is non-singular and $(A^T)^{-1} = (A^{-1})^T$.

Proof:

(a) Since $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}IB = I$ and $(AB)(B^{-1}A^{-1}) = A(BB^{-1})(A^{-1}) = AIA^{-1} = I$, by Lemma 1.3.2 $(AB)^{-1} = B^{-1}A^{-1}$.

(b) By definition we have $A^{-1}A = I = AA^{-1}$. By Lemma 1.3.2 $(A^{-1})^{-1} = A$.

(c) We have $(c^{-1}A^{-1})(cA) = c^{-1}cA^{-1}A = I$. Similarly we have $(cA)(c^{-1}A^{-1}) = I$. By Lemma 1.3.2 we have $(cA)^{-1} = c^{-1}A^{-1}$.

(d) From Proposition 1.2.14 we have $(A^{-1})^T A^T = (AA^{-1})^T = I^T = I$. Similarly we have $A^T(A^{-1})^T = I$. By Lemma 1.3.2 we have $(A^T)^{-1} = (A^{-1})^T$. □

Theorem 1.3.5 *If A is non-singular then the equation $XA = B$ has unique solution if B is of the proper size (but not necessary a square matrix). Also the equation $AY = B$ has unique solution again with B of the proper size. However, these two solutions need not be equal even though B is a square matrix.*

Proof: Clearly BA^{-1} is a solution of $XA = B$ and $A^{-1}B$ is a solution of $AY = B$. The solution is unique since for any C such that $CA = B$ we have $C = CAA^{-1} = BA^{-1}$. Similarly, if $AD = B$, then $D = A^{-1}B$.

Let $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. It can be shown that $A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$. Then $X = BA^{-1} = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}$ and $Y = A^{-1}B = \begin{pmatrix} -3 & -2 \\ 2 & 1 \end{pmatrix}$. Thus $X \neq Y$. □

Example 1.3.6 Suppose A is an $n \times n$ matrix with the block form $A = \left(\begin{array}{c|c} B & C \\ \hline O & D \end{array}\right)$, where B, D are $k \times k$ and $(n-k) \times (n-k)$ matrices, respectively. By uniqueness of the inverse matrix it is easy to verify that if B and D are non-singular, then A is non-singular and A^{-1} has the block form $A^{-1} = \left(\begin{array}{c|c} B^{-1} & E \\ \hline O & D^{-1} \end{array}\right)$, where $E = -B^{-1}CD^{-1}$.

Lemma 1.3.7 *Suppose A has one row (column) of zeros, then A cannot be invertible.*

Proof: Without loss of generality, we may assume A has the form $\left(\begin{array}{c} A_1 \\ \hline A_2 \\ \hline A_3 \end{array}\right)$, where A_2 is a $1 \times n$ zero matrix which is the i-th row of A. Then for any $n \times n$ matrix X, consider $AX = \left(\begin{array}{c} A_1 \\ \hline A_2 \\ \hline A_3 \end{array}\right) X =$

$\left(\begin{array}{c} A_1X \\ \hline A_2X \\ \hline A_3X \end{array}\right) = \left(\begin{array}{c} A_1X \\ \hline O_{1,n} \\ \hline A_3X \end{array}\right)$. Thus $AX \neq I$ for any X. Hence A cannot be invertible.

The proof is similar if A has a zero column. □

Exercise 1.3

1.3-1. Suppose A is an $n \times n$ matrix over $\mathbb{R}$ satisfying the equation $A^2 - A + 2I = O$. Show that A is non-singular. Express A^{-1} as a linear combination of A and I. Suppose the matrix A is over the field $\mathbb{Z}_2$. Is it non-singular? Justify!

1.3-2. Suppose A is an $n \times n$ matrix over $\mathbb{F}$ satisfying the polynomial equation $f(x) = a_0 + a_1x + \cdots + a_mx^m = 0$, i.e., $f(A) = a_0I + a_1A + \cdots + a_mA^m = O$. Show that if $a_0 \neq 0$, then A is invertible. Express A^{-1} as a linear combination of I , A, $\ldots$, A^{m-1} over $\mathbb{F}$.

1.3-3. Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

(a) Compute $A^8 - 2A^7 + A^5 - A^3 + 3A + I$.

(b) Find $(A^3 - A + I)^{-1}$.

1.3-4. By a similar argument used in the proof of Lemma 1.3.7 show that if A is an $n \times n$ matrix having two rows (columns) that are in a ratio, say $A_{i*} = cA_{j*}$ for some $i \neq j$, then A cannot be invertible.

1.3-5. Suppose A, B and $A + B$ are invertible matrices. Prove that

(a) $A^{-1} + B^{-1}$ is invertible with the inverse $A(A + B)^{-1}B$.

(b) $A(A + B)^{-1}B = B(A + B)^{-1}A$.

1.3-6. Let $A_1, A_2, \ldots, A_r$ be invertible matrices (whose orders need not the same) over $\mathbb{F}$. Show that

$$A = \begin{pmatrix} A_1 & O & \cdots & O \\ O & A_2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_r \end{pmatrix} \text{ and } B = \begin{pmatrix} O & \cdots & O & A_1 \\ O & \cdots & A_2 & O \\ \vdots & \iddots & \vdots & \vdots \\ A_r & \cdots & O & O \end{pmatrix}$$

are invertible. Moreover,

$$A^{-1} = \begin{pmatrix} A_1^{-1} & O & \cdots & O \\ O & A_2^{-1} & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A_r^{-1} \end{pmatrix} \text{ and } B^{-1} = \begin{pmatrix} O & \cdots & O & A_r^{-1} \\ O & \cdots & A_{r-1}^{-1} & O \\ \vdots & \iddots & \vdots & \vdots \\ A_1^{-1} & \cdots & O & O \end{pmatrix}.$$

1.3-7. Use the above problem to find the inverse of the matrix

$$A = \begin{pmatrix} 2 & 3 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

over $\mathbb{R}$.

1.3-8. Find the inverse of the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 3 & 4 \end{pmatrix}$$

over $\mathbb{R}$.

1.4 Elementary Row Operations

To solve a system of linear equations (for example, Example 1.1.1) we can perform the following three operations:

(1) Multiply an equation by a nonzero scalar b.

(2) Multiply an equation by b and add to another equation. Note that the multiplied equation remains unchanged.

(3) Interchange two equations.

When applying the above operations there only involve the coefficients of the equations. So if we arrange the coefficients of the equations as the matrix A defined in Example 1.1.1, then the above operations can be translated into three operations on matrix A. Following are the general descriptions.

There are three types of the so-called *elementary row operations* on the rows of a matrix.

(1) Multiply the i-th row by a nonzero scalar b. We use "$b\mathcal{R}_i$" to denote this operation.

(2) Multiply the i-th row by b and add to the j-th row for $i \neq j$. We denote this operation by the notation "$b\mathcal{R}_i + \mathcal{R}_j$". Note that the i-th row does not change under this operation.

(3) Interchange the i-th and the j-th rows for $i \neq j$. We use "$\mathcal{R}_i \leftrightarrow \mathcal{R}_j$" to denote this operation.

Remark 1.4.1 Operation of type 3 is of no use in solving system of equations. However we need it to reduce a matrix to the reduced row echelon form that we shall discuss in the next section. Also operation of type 3 is redundant. It can be obtained by a series of operations of type 1 and type 2. This can be seen from the following (without loss of generality we assume $i < j$):

$$\begin{pmatrix} \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \vdots & \vdots \\ a_{j1} & \cdots & a_{jn} \\ \vdots & \vdots & \vdots \end{pmatrix} \xrightarrow{1\mathcal{R}_j+\mathcal{R}_i} \begin{pmatrix} \vdots & \vdots & \vdots \\ a_{i1}+a_{j1} & \cdots & a_{in}+a_{jn} \\ \vdots & \vdots & \vdots \\ a_{j1} & \cdots & a_{jn} \\ \vdots & \vdots & \vdots \end{pmatrix}$$

$$\xrightarrow{(-1)\mathcal{R}_i+\mathcal{R}_j} \begin{pmatrix} \vdots & \vdots & \vdots \\ a_{i1}+a_{j1} & \cdots & a_{in}+a_{jn} \\ \vdots & \vdots & \vdots \\ -a_{i1} & \cdots & -a_{in} \\ \vdots & \vdots & \vdots \end{pmatrix}$$

$$\xrightarrow{1\mathcal{R}_j+\mathcal{R}_i} \begin{pmatrix} \vdots & \vdots & \vdots \\ a_{j1} & \cdots & a_{jn} \\ \vdots & \vdots & \vdots \\ -a_{i1} & \cdots & -a_{in} \\ \vdots & \vdots & \vdots \end{pmatrix} \xrightarrow{(-1)\mathcal{R}_j} \begin{pmatrix} \vdots & \vdots & \vdots \\ a_{j1} & \cdots & a_{jn} \\ \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \vdots & \vdots \end{pmatrix}.$$

This means that $\mathcal{R}_i \leftrightarrow \mathcal{R}_j = [(-1)\mathcal{R}_j] \circ [1\mathcal{R}_j + \mathcal{R}_i] \circ [(-1)\mathcal{R}_i + \mathcal{R}_j] \circ [1\mathcal{R}_j + \mathcal{R}_i]$. It is easy to see that the expression is not unique. Nevertheless, this operation is direct and easy to use.

Definition 1.4.2 An *elementary matrix* is a matrix obtained by applying an elementary row operation to the identity matrix. The elementary matrix is said to be of *type* 1, 2, or 3 according to whether the elementary operation of type 1, 2 or 3 performed on I, respectively.

For fixed integers i, j, let $E^{i,j} \in M_m(\mathbb{F})$ whose (i, j)-entry is 1 and others are zero, where m fixed, i.e., $(E^{i,j})_{h,k} = \delta_{hi}\delta_{kj}$.

So an elementary matrix of type 1 is $(b\mathcal{R}_i)(I) = I + (b-1)E^{i,i}$ for $b \neq 0$ having the form

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ i \\ \\ n \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & & i & & n \end{array} \\ \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & b & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} \end{array}$$

An elementary matrix of type 2 is $(b\mathcal{R}_i + \mathcal{R}_j)(I) = I + bE^{j,i}$ for $i < j$ and $b \neq 0$ having the form

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ i \\ \\ j \\ \\ n \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & 2 & & i & & j & & n \end{array} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & b & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} \end{array}$$

An elementary matrix of type 3 is $(\mathcal{R}_i \leftrightarrow \mathcal{R}_j)(I) = I - E^{i,i} - E^{j,j} + E^{i,j} + E^{j,i}$ for $i < j$ having the form

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ i \\ \\ j \\ \\ n \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & 2 & & i & & j & & n \end{array} \\ \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} \end{array}$$

Theorem 1.4.3 *Let $A \in M_{m,n}(\mathbb{F})$ and suppose that B is obtained from A by performing an elementary row operation. Then there is an $m \times m$ elementary matrix E such that $B = EA$. In fact, E is obtained by performing the same row operation on I_m. Conversely, if E is an $m \times m$ elementary matrix, then EA is a matrix that can be obtained by performing the same elementary row operation on A.*

Proof: Suppose B is obtained from A by performing an elementary row operation of type 1, i.e., $B = (b\mathcal{R}_i)(A)$ for some i and $b \neq 0$. By definition $(B)_{h,k} = \begin{cases} b(A)_{h,k} & \text{if } h = i, \\ (A)_{h,k} & \text{if } h \neq i. \end{cases}$

Let $E = (b\mathcal{R}_i)(I) = I + (b-1)E^{i,i}$, i.e., $(E)_{h,k} = \begin{cases} b & \text{if } h = k = i, \\ 1 & \text{if } h = k \neq i, \\ 0 & \text{if } h \neq k. \end{cases}$. Then

$$\begin{aligned} (EA)_{h,k} &= \sum_{t=1}^{m} (E)_{h,t}(A)_{t,k} = (E)_{h,h}(A)_{h,k} = \begin{cases} b(A)_{h,k} & \text{if } h = i, \\ (A)_{h,k} & \text{if } h \neq i. \end{cases} \\ &= (B)_{h,k}. \end{aligned}$$

Hence $B = EA$.

Suppose B is obtained from A by performing an elementary row operation of type 2, i.e., $B = (b\mathcal{R}_i + \mathcal{R}_j)(A)$ for some $i \neq j$ and $b \neq 0$. By definition

$$(B)_{h,k} = \begin{cases} b(A)_{i,k} + (A)_{j,k} & \text{if } h = j, \\ (A)_{h,k} & \text{if } h \neq j. \end{cases}$$

Let $E = (b\mathcal{R}_i + \mathcal{R}_j)(I) = I + bE^{j,i}$, $i \neq j$ and $b \neq 0$. That is,

$$(E)_{h,k} = \begin{cases} b & \text{if } h = j, k = i, \\ 1 & \text{if } h = k, \\ 0 & \text{otherwise.} \end{cases}$$

For $h = j$, $(EA)_{h,k} = (EA)_{j,k} = \sum_{t=1}^{m}(E)_{j,t}(A)_{t,k} = (E)_{j,j}(A)_{j,k} + (E)_{j,i}(A)_{i,k} = (A)_{j,k} + b(A)_{i,k}$. For $h \neq j$, $(EA)_{h,k} = \sum_{t=1}^{m}(E)_{h,t}(A)_{t,k} = (E)_{h,h}(A)_{h,k} = (A)_{h,k}$. Hence $B = EA$.

Suppose B is obtained from A by performing an elementary row operation of type 3, i.e., $B = (\mathcal{R}_i \leftrightarrow \mathcal{R}_j)(A)$ for some $i \neq j$. By definition

$$(B)_{h,k} = \begin{cases} (A)_{j,k} & \text{if } h = i, \\ (A)_{i,k} & \text{if } h = j, \\ (A)_{h,k} & \text{otherwise.} \end{cases}$$

Let $E = (\mathcal{R}_i \leftrightarrow \mathcal{R}_j)(I) = I - E^{i,i} - E^{j,j} + E^{i,j} + E^{j,i}$.

$$\begin{aligned}(EA)_{h,k} &= (A - E^{i,i}A - E^{j,j}A + E^{i,j}A + E^{j,i}A)_{h,k} \\ &= (A)_{h,k} - \sum_{t=1}^{m}(E^{i,i})_{h,t}(A)_{t,k} - \sum_{t=1}^{m}(E^{j,j})_{h,t}(A)_{t,k} + \sum_{t=1}^{m}(E^{i,j})_{h,t}(A)_{t,k} \\ &\quad + \sum_{t=1}^{m}(E^{j,i})_{h,t}(A)_{t,k} \\ &= (A)_{h,k} - \delta_{ih}(A)_{i,k} - \delta_{jh}(A)_{j,k} + \delta_{ih}(A)_{j,k} + \delta_{jh}(A)_{i,k}.\end{aligned}$$

For $h = i$, $(EA)_{i,k} = (A)_{i,k} - (A)_{i,k} + (A)_{j,k} = (A)_{j,k}$. For $h = j$, $(EA)_{j,k} = (A)_{j,k} - (A)_{j,k} + (A)_{i,k} = (A)_{i,k}$. For $h \neq i$ and $h \neq j$, $(EA)_{h,k} = (A)_{h,k}$. Hence $B = EA$.

The converse is easy to see from the equalities above. □

Lemma 1.4.4 *For any integers i, j, h, k, $E^{i,j}E^{h,k} = \delta_{jh}E^{i,k}$.*

Proof: Suppose the matrices are of order n. Then

$$\begin{aligned}(E^{i,j}E^{h,k})_{x,y} &= \sum_{z=1}^{n}(E^{i,j})_{x,z}(E^{h,k})_{z,y} = \sum_{z=1}^{n}\delta_{xi}\delta_{zj}\delta_{zh}\delta_{yk} \\ &= \delta_{jh}\delta_{xi}\delta_{yk} = \delta_{jh}(E^{i,k})_{x,y}.\end{aligned}$$

Therefore, we have the lemma. □

Proposition 1.4.5 *Elementary matrices are non-singular and their inverses are also elementary matrices of the same type.*

Proof: Let E be an elementary matrix.

For the type 1 case, $E = I + (b-1)E^{i,i}$ for $b \neq 0$. Let $C = I + (b^{-1} - 1)E^{i,i}$. Then

$$\begin{aligned}EC &= [I + (b-1)E^{i,i}][I + (b^{-1} - 1)E^{i,i}] \\ &= I + (b-1)E^{i,i} + (b^{-1} - 1)E^{i,i} + (b-1)(b^{-1} - 1)E^{i,i}E^{i,i}.\end{aligned}$$

By Lemma 1.4.4, $EC = I + (b + b^{-1} - 2)E^{i,i} + (2 - b - b^{-1})\delta_{ii}E^{i,i} = I$. Similarly, one can check that $CE = I$. Hence $C = E^{-1}$.

For the type 2 case, $E = I + bE^{j,i}$ for $i \neq j$ and $b \neq 0$. Let $C = I - bE^{j,i}$. Since $i \neq j$, by Lemma 1.4.4 $E^{i,j}E^{i,j} = O$. So $EC = CE = I - b^2E^{i,j}E^{i,j} = I$.

For the type 3 case, one can check that $EE = I$, that is E is the inverse of E. We leave to the reader. □

Remark 1.4.6 Since $(E^{i,j})^T = E^{j,i}$, if E is an elementary matrix then so is E^T.

Definition 1.4.7 Suppose a matrix B is obtained from a matrix A by performing a finite sequence of elementary of row operations. Then we say that A is *row-equivalent* to B.

By using Theorem 1.4.3 and Proposition 1.4.5, it is easy to prove the following corollaries.

Corollary 1.4.8 *Let $A, B \in M_{m,n}(\mathbb{F})$. Then B is row-equivalent to A if and only if $B = PA$, where P is a product of $m \times m$ elementary matrices. Moreover, such P is invertible.*

Corollary 1.4.9 *Row-equivalence or being row-equivalent is an equivalence relation on $M_{m,n}(\mathbb{F})$.*

We can also define analogously the *elementary column operations* and the elementary matrices obtained by applying an elementary column operations to I. An elementary column operation on a matrix A can also be accomplished by multiplying A on the right by an elementary matrix which is obtained by applying a corresponding elementary column operation to I. This can be seen as follows. We first note that $AE = ((AE)^T)^T = (E^TA^T)^T$. We need to consider E^TA^T and then take transpose. If E is of type 1 or type 3, then as E is symmetric, so EA^T is just the same elementary row operations to rows of A^T, i.e., columns of A. Now if E is the elementary matrix obtained by multiplying the i-th column by b and add to the j-th column. Then E^T is the elementary matrix obtained by multiplying the i-th row by b and add to the j-th row. Thus the elementary matrix obtained by applying an elementary column operation to I is the transpose of the elementary matrix by applying the same elementary row operation to I. We shall use $b\mathcal{C}_i$, $b\mathcal{C}_i + \mathcal{C}_j$ and $\mathcal{C}_i \leftrightarrow \mathcal{C}_j$ to denote the elementary column operations of type 1, 2 and 3, respectively.

1.5 Reduced Row Echelon Form

Definition 1.5.1 A matrix is called in *reduced row echelon form* (*rref*) or *Hermite normal form* if it satisfies all of the following four conditions:

1. The zero rows, if any, are the last rows of the matrix.
2. The first nonzero entry in a nonzero row is a 1. It is called a *pivot* or *leading one*.
3. Suppose there are r nonzero rows. Let the pivot appearing in the i-th row lie at (i, k_i)-entry, $1 \leq i \leq r$. Then $1 \leq k_1 < k_2 < \cdots < k_r$.
4. In the k_i-th column, the only nonzero entry is the pivot in the i-th row. That is the k_i-th column is $\boldsymbol{e}_i$.

A column containing a pivot is called *leading column*. Suppose there are r nonzero rows. Then there are exactly r leading columns. Here is a general reduced row echelon form:

$$\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccccccc} & & & k_1 & & & & k_i & & & k_r & \\ \end{array} \\ \left(\begin{array}{cccccccccccc} 0 & \cdots & 0 & 1 & b_{1\,k_1+1} & \cdots & 0 & b_{1\,k_i+1} & \cdots & 0 & b_{1\,k_r+1} & \cdots \\ 0 & \cdots & 0 & 0 & * & \cdots & 0 & b_{2\,k_i+1} & \cdots & 0 & b_{2\,k_r+1} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & 1 & b_{i\,k_i+1} & \cdots & 0 & b_{i\,k_r+1} & \cdots \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 & * & \cdots & 0 & b_{i+1\,k_r+1} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 & \cdots & \cdots & 0 & b_{r-1\,k_r+1} & \cdots \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 & \cdots & \cdots & 1 & b_{r\,k_r+1} & \cdots \\ \hline 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 & \cdots & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 & \cdots & \cdots & 0 & \cdots & 0 \end{array}\right), \end{array} \tag{1.1}$$

where $*$ is either 0 or 1. If $*$ is a pivot, then every entry in this column differing from it is zero. Such matrix is called a *reduced row echelon matrix*.

Example 1.5.2 The following matrices are in reduced row echelon form:

$$I_n,\ O_{m,n},\ \begin{pmatrix} 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The following matrices are not in reduced row echelon form:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

□

Theorem 1.5.3 *Let $A \in M_{m,n}(\mathbb{F})$. There is a non-singular matrix P such that PA is in reduced row echelon form.*

Proof: We may assume $A \neq O$. The following algorithm is called *Gaussian elimination*. Using this algorithm we can reduce the matrix A to Hermite normal form H.

Gaussian Elimination (Gauss-Jordan Method)

Step 1: If the first column of the matrix is a zero column, cross it off mentally. Continue in this fashion until the left column of the remaining matrix has a nonzero entry or until the columns are exhausted. For the last case, go to Step 6.

Step 2: Interchange the first row with another row, if necessary, to put a nonzero entry to the top of the first column.

Step 3: By means of operation of type 1, make the nonzero entry found in Step 2 to be 1 (a pivot).

Step 4: By means of operations type 2 ($b\mathcal{R}_i + \mathcal{R}_j$), use the first row to obtain zeros in the remaining positions of the first column.

Step 5: Cross off the first row and the first column mentally. Begin with Step 1 applied to the submatrix that remains.

Step 6: Beginning with the last nonzero row, add multiples of this row to the rows above (operations type 2) such that the pivot in this row is the only nonzero entry in its column.

Step 7: Use operations type 2 to make the pivot in the next-to-last row the only nonzero entry in its column.

Step 8: Repeat Step 7 for each preceding row until the second row is performed.

By Theorem 1.4.3 there are elementary matrices $E_1, E_2, \ldots, E_s$ for some s such that $H = E_s \cdots E_2 E_1 A$. By Theorem 1.3.4, $P = E_s \cdots E_2 E_1$ is non-singular. □

Note that if we apply the Gaussian elimination on a square matrix and stop at Step 5, then we will obtain an upper triangular matrix. In general, if the matrix is not square, then it will be transformed to a *row echelon form* (or *trapezoidal form*).

Example 1.5.4

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & 3 & -1 \\ 2 & -1 & 5 & 2 \end{pmatrix} \xrightarrow[(-2)\mathcal{R}_1+\mathcal{R}_3]{(-2)\mathcal{R}_1+\mathcal{R}_2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -1 & 1 & -3 \\ 0 & -3 & 3 & 0 \end{pmatrix}$$

$$\xrightarrow[(-\frac{1}{3})\mathcal{R}_3]{(-1)\mathcal{R}_2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & 3 \\ 0 & 1 & -1 & 0 \end{pmatrix} \xrightarrow{(-1)\mathcal{R}_2+\mathcal{R}_3} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & 3 \\ 0 & 0 & 0 & -3 \end{pmatrix}$$

$$\xrightarrow{(-\frac{1}{3})\mathcal{R}_3} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[(-3)\mathcal{R}_3+\mathcal{R}_2]{(-1)\mathcal{R}_3+\mathcal{R}_1} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{(-1)\mathcal{R}_2+\mathcal{R}_1} \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Example 1.5.5 Let $A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & -1 & -1 & 1 & 1 \\ 0 & 1 & 1 & -1 & 2 \end{pmatrix}$. Then

$$A \xrightarrow[(-1)\mathcal{R}_1+\mathcal{R}_3]{1\mathcal{R}_1+\mathcal{R}_2} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & -2 & 1 \end{pmatrix} \xrightarrow{\frac{1}{2}\mathcal{R}_2} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -2 & 1 \end{pmatrix}$$
$$\xrightarrow[2\mathcal{R}_2+\mathcal{R}_3]{(-1)\mathcal{R}_2+\mathcal{R}_1} \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix} \xrightarrow{\frac{1}{3}\mathcal{R}_3} \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
$$\xrightarrow{(-1)\mathcal{R}_3+\mathcal{R}_2} \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that, sometimes we need not follow the steps of Gaussian elimination. □

By the definition of reduced row echelon form, we have the following two lemmas.

Lemma 1.5.6 *Suppose* $C = \begin{pmatrix} A & B \end{pmatrix}$ *is in rref, then* A *is also in rref.*

Lemma 1.5.7 *Suppose* $C = \begin{pmatrix} A \\ B \end{pmatrix}$ *is in rref, then* A *and* B *are also in rref.*

Theorem 1.5.8 *Suppose* A *and* B *are row-equivalent and are in rref. Let* A' *and* B' *be the result of removing the last* k *columns of* A *and* B*, respectively. Then* A' *and* B' *are row-equivalent and are in rref.*

Proof: By Lemma 1.5.6 A' and B' are in rref. Write $A = (A'|C)$ and $B = (B'|D)$. Since A is row-equivalent to B, there is a non-singular matrix P which is a product of elementary matrices such that $PA = B$. That is,

$$P(A'|C) = (B'|D).$$

By block multiplication, we have

$$(PA'|PC) = (B'|D).$$

Hence we have $PA' = B'$. By definition A' is row-equivalent to B'. □

Lemma 1.5.6 and Theorem 1.5.8 will be used in the next chapter.

Exercise 1.5

1.5-1. Complete the proof of Proposition 1.4.5. That is, prove that $EE = I$, where $E = I - E^{i,i} - E^{j,j} + E^{i,j} + E^{j,i}$ for $i \neq j$.

1.5-2. Let $A = \begin{pmatrix} 4 & 6 & 0 & 1 & -9 \\ 1 & 2 & -4 & 5 & 7 \\ 2 & 3 & 6 & 4 & 2 \\ 1 & 0 & 3 & 2 & -5 \end{pmatrix}$ be matrix over $\mathbb{R}$. Find rref(A).

1.5-3. Let $A = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 3 & 0 & 2 & 3 \\ 6 & 1 & 3 & 5 \\ 1 & 0 & 3 & 2 \end{pmatrix}$ be matrix over $\mathbb{Z}_7$. Find rref(A).

1.5-4. Let $A = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 1 & 3 & 2 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & -1 & 2 & 4 \\ 0 & 3 & 5 & 6 \\ 3 & 1 & 1 & 1 \end{pmatrix}$ be matrices over $\mathbb{Q}$. Find $\mathrm{rref}(A) + \mathrm{rref}(B)$ and $\mathrm{rref}(A + B)$.

1.5-5. Find all the reduced row echelon forms of 3×3 matrices.

Chapter 2

System of Linear Equations

2.1 Introduction

Suppose $\mathbb{F}$ is a field. We consider the problem of solving n scalars (in $\mathbb{F}$) $x_1, x_2, \ldots, x_n$ which satisfy the following m equations simultaneously:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \quad\quad \vdots \quad\quad \vdots \quad\quad \vdots \quad\quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{2.1}$$

where $b_1, b_2, \ldots, b_m$ and a_{ij} $(1 \leq i \leq m,\ 1 \leq j \leq n)$ are given scalars. Equation (2.1) is called a *system of m linear equations in n unknowns over $\mathbb{F}$* or an *$m \times n$ system of linear equations over $\mathbb{F}$*. The scalars a_{ij} $(1 \leq i \leq m,\ 1 \leq j \leq n)$ are called the *coefficients of the system*. An *n-tuple* $(x_1, x_2, \ldots, x_n) \in \mathbb{F}^n$ (for convenience we often write the n-tuple as a column matrix) which satisfies Equation (2.1) is called a *solution* of the system. The set of all solutions of a system of linear equations is called the *solution set*.

Let $A = (a_{ij})$ be an $m \times n$ matrix, $X = (x_1\ x_2\ \cdots\ x_n)^T$ and $\boldsymbol{b} = (b_1\ b_2\ \cdots\ b_m)^T$. Then Equation (2.1) can be written into a matrix form: $AX = \boldsymbol{b}$. The matrix A is called the *coefficient matrix* of Equation (2.1).

The above matrix equation can be generalized. Let $A \in M_{m,n}$ and $B \in M_{m,p}$ be two given matrices. Let $X = (x_{ij})$ be an $n \times p$ matrix whose entries are unknowns x_{ij}, $1 \leq i \leq n$ and $1 \leq j \leq p$. The equation $AX = B$ is called a *linear system*.

2.2 Linear System

In this section we shall discuss some properties of linear system. How to simplify the system and how to solve it?

Definition 2.2.1 A linear system $AX = B$ is called *homogeneous* if B is the zero matrix.

Definition 2.2.2 Let $A = (A_{ij}) \in M_{m,n}(\mathbb{F})$ and $B = (b_{ij}) \in M_{m,p}(\mathbb{F})$. By the *augmented matrix*

$(A|B)$ we mean the $m \times (n+p)$ matrix

$$\left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & b_{11} & b_{12} & \cdots & b_{1p} \\ a_{21} & a_{22} & \cdots & a_{2n} & b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_{m1} & b_{m2} & \cdots & b_{mp} \end{array}\right).$$

Theorem 2.2.3 *Let $A, B \in M_{m,n}(\mathbb{F})$ and $C, D \in M_{m,p}(\mathbb{F})$. The system $AX = C$ and $BX = D$ have the same solution sets if the augmented matrix $(A|C)$ is row-equivalent to the augmented matrix $(B|D)$.*

Proof: By definition there exist an invertible matrix P such that $P(A|C) = (B|D)$. Then $(PA|PC) = (B|D)$. Thus $PA = B$ and $PC = D$.

Suppose Y is a solution of the equation $AX = C$. Multiplying both sides by P we have $PAY = PC$. Then $BY = PAY = PC = D$, i.e., Y is a solution of the equation $BX = D$.

Similarly, if Y is a solution of $BX = D$, then $P^{-1}BY = P^{-1}D$. We have $AY = C$. Hence Y is a solution of the equation $AX = C$. □

Definition 2.2.4 A system $AX = B$ is said to be *consistent* if it has at least one solution, otherwise it is said to be *inconsistent*.

Suppose $(A|C)$ is row-equivalent to $(B|D)$. By Theorem 2.2.3 then the system $AX = C$ is consistent if and only if $BX = D$ is consistent.

Given a square matrix A we want to determine whether it is invertible or not. It is equivalent to determine the linear system $AX = I$ is consistent or not. Following are some equivalence statements of invertibility.

For a homogeneous system $AX = O_{m,p}$, where $A \in M_{m,n}(\mathbb{F})$, then $X = O_{n,p}$ is always a solution. This solution is called the *trivial solution* of the system. Other solution (if any) is called a *non-trivial solution*.

Theorem 2.2.5 *Let $A \in M_n(\mathbb{F})$. The followings are equivalent.*

(a) A is invertible.

(b) A is row-equivalent to I_n.

(c) A is a product of elementary matrices.

(d) For any $n \times p$ zero matrix O, the system $AX = O$ has only the trivial solution.

(e) For any given $n \times p$ matrix B, the system $AX = B$ has a unique solution.

Proof:
[(c)⇒ (a)]: It follows from Proposition 1.4.5 and Theorem 1.3.4.
[(a)⇒ (e)]: It follows from Theorem 1.3.5.
[(e)⇒ (d)]: It is trivial.
[(d)⇒ (b)]: Suppose that (d) holds. Let H be a reduced row echelon form which is row-equivalent to A. Let r be the number of non-zero rows of H. Suppose k_1-th, k_2-th, ..., k_r-th columns are the leading columns of H. Assume that $r < n$. Then there is a non-leading column, say the j-th column H_{*j}. Let $H_{*j} = \begin{pmatrix} c_1 & c_2 & \cdots & c_r & 0 & \cdots & 0 \end{pmatrix}^T$. Let $a_j = 1$, $a_{k_i} = -c_i$ for $1 \leq i \leq r$,

$a_t = 0$ if $t \notin \{j, k_1, k_2, \cdots, k_r\}$. Then $X = (\boldsymbol{\alpha}\ O_{n,(p-1)})$ is a nontrivial solution of $HX = O$, where $\alpha = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}^T$. By Theorem 2.2.3, $AX = O$ has non-trivial solution. Thus $r = n$. Since H is a (square) reduced row echelon form, $H = I_n$.
[(b)⇒(c)]: Suppose that (b) holds. Then $PA = I$ where $P = E_1E_2\cdots E_s$ is a product of elementary matrices for some $s \geq 0$ (note that if $s = 0$ then $P = I$). Multiply both sides by $E_s^{-1}\cdots E_2^{-1}E_1^{-1}$ we have $A = E_s^{-1}\cdots E_2^{-1}E_1^{-1}$. By Proposition 1.4.5, A is a product of elementary matrices. That is, (c) holds.

Hence, the proof is completed. □

Corollary 2.2.6 *Suppose A is a square matrix. If A has* right inverse*, i.e., there is a matrix B such that $AB = I$, then A is invertible.*

Proof: Let H be a reduced row echelon form which is row-equivalent to A. Then there is a invertible matrix P such that $PA = H$. Suppose A is not invertible. By Theorem 2.2.5, the last row of H must be a zero row. Let $H = \begin{pmatrix} H' \\ O \end{pmatrix}$. From $AB = I$, we have $PAB = P$. Then $HB = \begin{pmatrix} H' \\ O \end{pmatrix} B = \begin{pmatrix} H'B \\ O \end{pmatrix} = P$. By Lemma 1.3.7, P cannot be invertible. It is a contradiction. □

Remark 2.2.7 So by the above corollary, if $AB = I$ then $BA = I$. Moreover, B is invertible and $B = A^{-1}$.

Similarly, we have

Corollary 2.2.8 *Suppose A is a square matrix. If A has* left inverse*, i.e., there is a matrix C such that $CA = I$, then A is invertible.*

Remark 2.2.9 From Corollaries 2.2.6 and 2.2.8, if a square matrix has either right inverse or left inverse, then it has both and hence it is invertible. Moreover, the right inverse and the left inverse are the same.

Remark 2.2.10 For Corollaries 2.2.6 and 2.2.8 to be true, A must be a square matrix. Consider the following example:

Let $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ $Y = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$. Then $XY = I_2$ but $YX \neq I_3$.

Corollary 2.2.11 *Suppose A and B are square matrices. If $C = AB$ is invertible then both A and B are invertible.*

Proof: Since C is invertible, $C^{-1}AB = I$. By Corollaries 2.2.6 and 2.2.8, $C^{-1}A$ and B are non-singular. Since $C^{-1}A$ and C are invertible, by Theorem 1.3.4 $A = C(C^{-1}A)$ is invertible. □

Corollary 2.2.12 *If A is row-equivalent to B, then either both A and B are non-singular or they both are singular.*

Proof: This follows from Corollaries 1.4.8 and 2.2.11. □

Theorem 2.2.13 *Two matrices A and B are row-equivalent if and only if there is an invertible matrix P such that $PA = B$.*

Proof: The only if part is just Corollary 1.4.8. Suppose $PA = B$. Since P is invertible, by Theorem 2.2.5 P is a product of elementary matrices. By Corollary 1.4.8, B is row-equivalent to A. □

The proof of Theorem 2.2.5 provides us a method to find the inverse of an invertible matrix. Let A be an invertible matrix. Then by the proof of Theorem 2.2.5 there exist elementary matrices $E_1, \ldots, E_s$ such that $E_1 \cdots E_s A = I$. Thus we have $P = E_1 \cdots E_s I = A^{-1}$. So, to get A^{-1} we could apply successively the same elementary row operations that will reduce A to the reduced row echelon form to the identity matrix I. To carry out this procedure, we form an $n \times 2n$ augmented matrix $(A|I)$ and perform elementary row operations to the augmented matrix to get a matrix of the form $(I|B)$. Since $(I|B) = P(A|I) = (PA|P)$, $B = P = A^{-1}$.

Example 2.2.14 Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & -1 \\ 2 & 1 & -1 \end{pmatrix}$. Form the 3×6 matrix $(A|I_3)$ and perform as follows:

$$\left(\begin{array}{ccc|ccc} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 0 & 1 & 0 \\ 2 & 1 & -1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{\mathcal{R}_1 \leftrightarrow \mathcal{R}_2} \left(\begin{array}{ccc|ccc} 1 & 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & -1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{(-2)\mathcal{R}_1 + \mathcal{R}_3}$$

$$\left(\begin{array}{ccc|ccc} 1 & 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & -2 & 1 \end{array}\right) \xrightarrow{1\mathcal{R}_2 + \mathcal{R}_3} \left(\begin{array}{ccc|ccc} 1 & 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}\right)$$

$$\xrightarrow{1\mathcal{R}_3 + \mathcal{R}_1} \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & -1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}\right) \xrightarrow{(-1)\mathcal{R}_2 + \mathcal{R}_1} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}\right).$$

Thus $A^{-1} = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 0 \\ 1 & -2 & 1 \end{pmatrix}$. □

Suppose $A \in M_{m,n}(\mathbb{F})$. We would like to find an invertible matrix P such that $H = PA$, where H is row-equivalent to A. Again, we form the augmented matrix $(A|I_m)$. Then perform elementary row operations to $(A|I_m)$ to get $(H|B)$. Then $B = P$.

Similarly, to compute $A^{-1}B$, if A is invertible, we may form the augmented matrix $(A|B)$ and apply elementary row operations to it to get the matrix $(I|B')$. Then $B' = A^{-1}B$. If we still want to record A^{-1}, then we just simply apply elementary row operations to $(A|I|B)$ to get $(I|A^{-1}|A^{-1}B)$.

Exercise 2.2

2.2-1. Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 8 \\ 3 & 4 & 6 \end{pmatrix} \in M_3(\mathbb{Z}_{11})$. By using elementary row operations find A^{-1}.

2.2-2. Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 8 \\ 3 & 4 & 6 \end{pmatrix} \in M_3(\mathbb{Q})$. By using elementary row operations find A^{-1}.

2.2-3. Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Suppose $X = AX - A^2 + I$. Find X.

2.3 System of Linear Equations

Now we go back to consider systems of linear equations. In secondary school, we use Cramer's rule to solve $n \times n$ system of linear equations when n is small (for example, $n = 3$ or 4). We shall prove the Cramer's rule later. When n is large, Cramer's rule is not an efficient method. Also it cannot be applied to solve $m \times n$ system of linear equations when $m \neq n$. We will apply elementary row operations to solve the system.

From Theorem 2.2.3 the system $AX = \boldsymbol{c}$ and $BX = \boldsymbol{d}$ have the same solution set if and only if $(A|\boldsymbol{c})$ is row-equivalent to $(B|\boldsymbol{d})$.

Example 2.3.1 Consider the system $AX = \boldsymbol{b}$, where $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & -1 & -1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}$ and $\boldsymbol{b} = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$. Consider the augmented matrix $(A|\boldsymbol{b})$. By Example 1.5.5, it is row-equivalent to

$$\left(\begin{array}{cccc|c} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

The last row means $0x_1 + 0x_2 + 0x_3 + 0x_4 = 1$ which is absurd. So $AX = \boldsymbol{b}$ is inconsistent. □

Example 2.3.2 Solve the following system of linear equations over $\mathbb{R}$:

$$\begin{cases} x_1 + x_2 - 4x_3 + x_4 = 3 \\ 2x_1 - 3x_2 + 7x_3 + 7x_4 = -4 \\ x_2 - 3x_3 - x_4 = 2 \end{cases}$$

We first form the augmented matrix and then apply some elementary row operations.

$$\left(\begin{array}{cccc|c} 1 & 1 & -4 & 1 & 3 \\ 2 & -3 & 7 & 7 & -4 \\ 0 & 1 & -3 & -1 & 2 \end{array}\right) \xrightarrow{(-2)\mathcal{R}_1+\mathcal{R}_2} \left(\begin{array}{cccc|c} 1 & 1 & -4 & 1 & 3 \\ 0 & -5 & 15 & 5 & -10 \\ 0 & 1 & -3 & -1 & 2 \end{array}\right)$$

$$\xrightarrow[5\mathcal{R}_2+\mathcal{R}_3]{\mathcal{R}_2\leftrightarrow\mathcal{R}_3} \left(\begin{array}{cccc|c} 1 & 1 & -4 & 1 & 3 \\ 0 & 1 & -3 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{(-1)\mathcal{R}_2+\mathcal{R}_1} \left(\begin{array}{cccc|c} 1 & 0 & -1 & 2 & 1 \\ 0 & 1 & -3 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Thus the original system becomes

$$\begin{cases} x_1 - x_3 + 2x_4 = 1 \\ x_2 - 3x_3 - x_4 = 2 \end{cases} \quad \text{or} \quad \begin{cases} x_1 = x_3 - 2x_4 + 1 \\ x_2 = 3x_3 + x_4 + 2 \end{cases}$$

Thus, $x_1 = 1, x_2 = 2, x_3 = 0, x_4 = 0$ is a solution.

Clearly, $x_1 = 0, x_2 = 6, x_3 = 1, x_4 = 1$ is also a solution. So the solution of the system is not unique. The question is how to find all the solutions. We shall come back to this example later. □

Remark 2.3.3 Suppose we have k systems $AX_1 = \boldsymbol{b}_1$, $AX_2 = \boldsymbol{b}_2$, ..., $AX_k = \boldsymbol{b}_k$, where A is an $m \times n$ matrix, $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, ..., $\boldsymbol{b}_k$ are $m \times 1$ matrices. Then we can solve them together by forming the augmented matrix $(A|\boldsymbol{b}_1|\boldsymbol{b}_2|\cdots|\boldsymbol{b}_k)$ and apply the elementary row operations to it. Then the solutions of each system can be read accordingly.

Lemma 2.3.4 *If $(H|\boldsymbol{b})$ is in rref, then the system $HX = \boldsymbol{b}$ is inconsistent if and only if $\boldsymbol{b}$ is a leading column of $(H|\boldsymbol{b})$. Here $\boldsymbol{b} = (b_1\ b_2\ \cdots\ b_m)^T$.*

Proof: If $(H|\boldsymbol{b})$ is a zero matrix, then we are done. So we assume $(H|\boldsymbol{b})$ is not a zero matrix. Suppose the leading columns of $(H|\boldsymbol{b})$ are k_1-th, k_2-th, ..., and k_r-th columns, where $k_1 < k_2 < \cdots < k_r$ for some r with $1 \le r \le m$.

If $\boldsymbol{b}$ is a leading column, then the r-th row of $(H|\boldsymbol{b})$ is $(0\ 0\ \cdots\ 0\ 1)$. Then $HX = \boldsymbol{b}$ is inconsistent.

If $\boldsymbol{b}$ is not a leading column, then $b_j = 0$ if $m \ge j > r$ (if $r = m$, then no such b_j exists). Then $x_{k_i} = b_i$ for $i = 1, 2 \ldots, r$ and $x_j = 0$ otherwise constitute a solution of $HX = \boldsymbol{b}$. Hence the system is consistent. □

Lemma 2.3.5 *If $(H|\boldsymbol{b})$ and $(H|\boldsymbol{c})$ are in rref and are row-equivalent, then $\boldsymbol{b} = \boldsymbol{c}$.*

Proof: By Theorem 2.2.3 the systems $HX = \boldsymbol{b}$ and $HX = \boldsymbol{c}$ have the same solution sets. Hence they both are either consistent or inconsistent. Note that, by Lemma 1.5.6 H is in rref. Suppose H contains $r - 1$ nonzero rows, $r \ge 1$.

Suppose both of the systems are inconsistent. Then, by Lemma 2.3.4, $\boldsymbol{b}$ and $\boldsymbol{c}$ are leading columns. Then $\boldsymbol{b} = \boldsymbol{c} = \boldsymbol{e}_r$.

Suppose both of the systems are consistent. Let X_0 be a solution of $HX = \boldsymbol{b}$. Since X_0 is also a solution of $HX = \boldsymbol{c}$. Then $\boldsymbol{b} = HX_0 = \boldsymbol{c}$. □

Theorem 2.3.6 *If two $m \times n$ matrices A and B are in rref and are row-equivalent, then $A = B$.*

Proof: Suppose $A \ne B$. Let k be the least integer so that the k-th column of A does not agree with the k-th column of B. Consider the submatrices

$$\left(\begin{array}{ccc|c} A_{*1} & \cdots & A_{*(k-1)} & A_{*k} \end{array}\right) \quad \text{and} \quad \left(\begin{array}{ccc|c} B_{*1} & \cdots & B_{*(k-1)} & B_{*k} \end{array}\right).$$

By Theorem 1.5.8 the above matrices are in rref and are row-equivalent.

If $k = 1$, then $A_{*1} = \boldsymbol{0}_m$ or $\boldsymbol{e}_1$. Since A_{*1} is row-equivalent to B_{*1}, $A_{*1} = \boldsymbol{0}_m$ if and only if $B_{*1} = \boldsymbol{0}_m$. So if $A_{*1} = \boldsymbol{e}_1$, then B_{*1} is not a zero column. Thus it must a leading column. Hence $B_{*1} = \boldsymbol{e}_1$.

If $k > 1$, then by Lemma 2.3.5 $A_{*k} = B_{*k}$.

For both cases, we have $A_{*k} = B_{*k}$. It is a contradiction. □

By Theorem 2.3.6 the rref of a matrix A is unique. We will use $\mathrm{rref}(A)$ to denote the rref of A.

2.4 Rank of Matrix

Definition 2.4.1 Let $A \in M_{m,n}(\mathbb{F})$ and $H = \mathrm{rref}(A)$. The *rank* of A denoted by $\mathrm{rank}(A)$ is the number of nonzero rows (or equivalently the number of pivots, or the number of leading columns) of H. This is well-defined as H is unique.

From Theorem 2.2.5 we have that

Theorem 2.4.2 *An $n \times n$ matrix A is invertible if and only if* $\text{rank}(A) = n$.

By definition we have the following proposition.

Proposition 2.4.3 *Let $A \in M_{m,n}(\mathbb{F})$. Then* $\text{rank}(A) \leq \min\{m, n\}$.

Example 2.4.4 Clearly, $\text{rank}(I_n) = n$; $\text{rank}(J_{m,n}) = 1$; $\text{rank}(\boldsymbol{b}) = 1$ if $\boldsymbol{b} \neq \mathbf{0}$; $\text{rank}(A) = 0$ if and only if $A = O_{m,n}$ for some positive integers m and n. The rank of matrix considered in Example 2.2.14 is 3. The rank of matrix considered in Example 2.3.1 is 2. □

Proposition 2.4.5 *Two row-equivalent matrices have the same rref and hence have the same rank.*

Proof: It follows from row-equivalent being an equivalence relation and Theorem 2.3.6. □

Definition 2.4.6 Let A be a matrix and let $H = \text{rref}(A)$. Those columns of A are called the *leading columns* of A if the corresponding columns of H are leading columns. Those variables in the system $AX = \boldsymbol{b}$ that yield the leading columns are called *lead variables*. Other variables are called *free variables*.

Example 2.4.7 Consider Example 2.3.1. A_{*2} and A_{*4} are leading columns. If $X = (x_1\ x_2\ x_3\ x_4)^T$, then x_2 and x_4 are lead variables, and x_1 and x_3 are free variables.

Example 2.4.8 Let $A = \begin{pmatrix} 0 & 1 & -2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. The non-trivial equations in the system $AX = \mathbf{0}$ are

$$\begin{cases} x_2 - 2x_3 + x_5 = 0 \\ x_4 + 2x_5 = 0 \end{cases} \tag{2.2}$$

Here x_2, x_4 are lead variables and x_1, x_3, x_5 are free variables. If we let $x_1 = 1$, $x_3 = 0 = x_5$, then $x_2 = x_4 = 0$. It is a non-trivial solution of System (2.2). If we let $x_3 = 1$, $x_1 = x_5 = 0$, then $x_2 = 2$ and $x_4 = 0$. It is also a non-trivial solution of System (2.2).

Actually, it is easy to see that we can choose any values for x_1, x_3 and x_5 arbitrarily to determine the values of x_2 and x_4. □

Base on the method of finding solution described in the above example, we can prove the following theorem.

Theorem 2.4.9 *Let $A \in M_{m,n}(\mathbb{F})$. Then $AX = \mathbf{0}$ has a non-trivial solution if and only if* $\text{rank}(A) < n$.

Proof: For the if part, the proof is similar to the proof of Theorem 2.2.5 [(d) ⇒ (b)] part. We show here again. Suppose $r = \text{rank}(A)$ and $H = \text{rref}(A)$. Then the solution set of $HX = \mathbf{0}$ is the same as $AX = \mathbf{0}$. Suppose k_1-th, k_2-th, ..., k_r-th columns are the leading columns of H.

Assume that $r < n$. Then there is a non-leading column, say the j-th column H_{*j} corresponding to the free variable x_j. Let

$$H_{*j} = \begin{pmatrix} c_1 & c_2 & \cdots & c_r & 0 & \cdots & 0 \end{pmatrix}^T.$$

Then

$$x_j = 1, x_{k_i} = -c_i \text{ for } 1 \le i \le r, x_t = 0 \text{ if } t \notin \{j, k_1, k_2, \cdots, k_r\}$$

satisfy the equation $HX = \mathbf{0}$.

Conversely, suppose $r = n$. Then H must have the form $\begin{pmatrix} I_n \\ O \end{pmatrix}$. Then $HX = \begin{pmatrix} I_n X \\ \mathbf{0}_{m-n} \end{pmatrix} = \mathbf{0}$. So $I_n X = X = \mathbf{0}$ is the only solution. □

Theorem 2.4.10 *Suppose $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{n,p}(\mathbb{F})$. Then* $\operatorname{rank}(AB) \le \operatorname{rank} A$.

Proof: Suppose $r = \operatorname{rank}(A)$. There exists an invertible matrix P such that $PA = \begin{pmatrix} A' \\ O_{m-r,n} \end{pmatrix} = \operatorname{rref}(A)$. Then $PAB = \begin{pmatrix} A'B \\ O_{m-r,p} \end{pmatrix}$.

There is an invertible matrix Q' such that $Q'A'B = H' = \operatorname{rref}(A'B)$. Let $Q = \begin{pmatrix} Q' & O_{r,m-r} \\ O_{m-r,r} & I_{m-r} \end{pmatrix}$. Clearly Q is invertible with the inverse $\begin{pmatrix} Q'^{-1} & O_{r,m-r} \\ O_{m-r,r} & I_{m-r} \end{pmatrix}$. Then $QPAB = \begin{pmatrix} Q'A'B \\ O_{m-r,p} \end{pmatrix} = \begin{pmatrix} H' \\ O_{m-r,p} \end{pmatrix}$ is in rref. Thus the number of nonzero row of $QPAB$ is at most r. Hence the proof is completed. □

Theorem 2.4.11 *Suppose $A \in M_{m,n}(\mathbb{F})$. If $P \in M_m(\mathbb{F})$ and $Q \in M_n(\mathbb{F})$ are invertible, then* $\operatorname{rank}(PA) = \operatorname{rank}(A)$ *and* $\operatorname{rank}(AQ) = \operatorname{rank} A$.

Proof: The first part follows from Proposition 2.4.5.

By Theorem 2.4.10 $\operatorname{rank}(A) = \operatorname{rank}(AQQ^{-1}) \le \operatorname{rank}(AQ) \le \operatorname{rank}(A)$. Then the inequalities are equalities, and therefore $\operatorname{rank}(AQ) = \operatorname{rank}(A)$. □

Theorem 2.4.11 tells us that elementary row (or column) operations preserve the rank of matrices.

By the contrapositive of Theorem 2.4.11, $\operatorname{rank}(AQ) < \operatorname{rank}(A)$ implies Q is singular. However, the converse of Theorem 2.4.11 is false. Clearly A being a zero matrix is a counterexample. Following is another counterexample.

Example 2.4.12 Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Clearly, $\operatorname{rank}(A) = 1$ and then A is singular. Since $A^2 = A$, $\operatorname{rank}(A^2) = \operatorname{rank}(A) = 1$. □

Theorem 2.4.13 *Let $A \in M_{m,n}(\mathbb{F})$ and $\boldsymbol{b} \in M_{m,1}(\mathbb{F})$. The system $AX = \boldsymbol{b}$ is consistent if and only if* $\operatorname{rank}(A) = \operatorname{rank}(A|\boldsymbol{b})$. *Whenever a solution exists, all solutions can be expressed in terms of $n - r$ free variables, where $r = \operatorname{rank}(A)$.*

Proof: Let $r = \operatorname{rank}(A)$ and $H = \operatorname{rref}(A)$. Then $\operatorname{rref}(A|\boldsymbol{b}) = (H|\boldsymbol{c})$ for some $\boldsymbol{c}$. By Lemma 2.3.4 $HX = \boldsymbol{c}$ is consistent if and only if $\boldsymbol{c}$ is not a leading column. Then $\operatorname{rank}(A|\boldsymbol{b}) = \operatorname{rank}(H|\boldsymbol{c}) = \operatorname{rank}(H) = \operatorname{rank}(A)$.

Now we assume that the system has a solution. It was known that the solution set of $AX = \boldsymbol{b}$ is equal to the solution set of $HX = \boldsymbol{c}$. Suppose k_1-th, $\cdots$, k_r-th columns of H are the leading columns. Then each lead variable x_{k_j} appears only in the j-th equation of the system $HX = \boldsymbol{c}$ with unit coefficient. Thus the lead variables $x_{k_1}, \ldots, x_{k_r}$ can be expressed in terms of the rest $n - r$ unknowns which are free variables. □

We shall give other proofs for Theorems 2.4.9 and 2.4.13, together with explicit descriptions of lead variables in terms of free variables.

Corollary 2.4.14 *Suppose $A \in M_{m,n}(\mathbb{F})$ and the system $AX = \boldsymbol{b}$ is consistent. Then the solution is unique if and only if* $\operatorname{rank}(A) = n$.

Corollary 2.4.15 *Suppose $A \in M_{m,n}(\mathbb{F})$. If $m < n$ then the system $AX = \mathbf{0}$ has non-trivial solution.*

Proof: The system $AX = \mathbf{0}$ is always consistent. Since $\operatorname{rank}(A) \leq \min\{m, n\} = m < n$, by Corollary 2.4.14 the system has a solution other than $\mathbf{0}$. □

Corollary 2.4.16 *Suppose A is a square matrix. Then $AX = \boldsymbol{b}$ has a unique solution if and only if A is invertible.*

Proof: If A is invertible, then clearly $X = A^{-1}\boldsymbol{b}$ is the only solution.

Conversely, if $AX = \boldsymbol{b}$ has a unique solution, then by Corollary 2.4.14 A must be invertible. □

Note that the above corollary is just a special case of Theorem 2.2.5.

Example 2.4.17 Go back to Example 2.3.2. The general solution of the system

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

is $(x_1, x_2, x_3, x_4) = (c - 2d + 1, 3c + d + 2, c, d)$ for any $c, d \in \mathbb{R}$. The solution set is

$$\begin{aligned} &\{(c - 2d + 1, 3c + d + 2, c, d) \mid c, d \in \mathbb{R}\} \\ &= \{c(1, 3, 1, 0) + d(-2, 1, 0, 1) + (1, 2, 0, 0) \mid c, d \in \mathbb{R}\}. \end{aligned}$$ □

Exercise 2.4

2.4-1. Find the rank of the following matrices over $\mathbb{Q}$:

(a) $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & -2 & 0 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & 2 & 3 & 3 & 10 & 6 \\ 2 & 1 & 0 & 0 & 2 & 3 \\ 2 & 2 & 2 & 1 & 5 & 5 \\ -1 & 1 & 3 & 2 & 5 & 2 \end{pmatrix}$;

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 4 & 5 & \cdots & n+1 \\ 3 & 4 & 5 & 6 & \cdots & n+2 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ n-1 & n & n+1 & n+2 & \cdots & 2n-2 \end{pmatrix}_{(n-1)\times n}$.

2.4-2. Find the solution sets of the following systems over $\mathbb{R}$:

(a) $\begin{cases} x_1 - x_2 + x_3 + x_4 = 0 \\ 3x_2 + x_3 + 2x_4 = 0 \\ 3x_1 + 7x_3 + 14x_4 = 0 \\ x_1 - x_2 + 2x_3 = 0 \\ 2x_1 + x_2 + 5x_3 + 6x_4 = 0 \end{cases}$

(b) $\begin{cases} x_1 - 2x_3 + x_4 = 1 \\ 2x_1 - x_2 + x_3 - 3x_4 = -5 \\ 9x_1 - 3x_2 - x_3 - 7x_4 = -1 \end{cases}$

2.4-3. Suppose $A \in M_{m,n}(\mathbb{F})$ with $m < n$. Show that if $\operatorname{rank}(A) = m$, then there exists a $B \in M_{n,m}(\mathbb{F})$ such that $AB = I_m$.

2.5 Canonical Form

Suppose $H = \text{rref}(A)$. Then there is an invertible matrix P such that $PA = H$. Let r be the number of nonzero rows of H. We can apply the elementary column operation of type 3 on H to move the leading columns of H to be the first r columns in order, i.e,

$$H_c = HE_1^T E_2^T \cdots E_s^T = \left(\begin{array}{c|c} I_r & * \\ \hline O & O \end{array}\right),$$

where E_i is the elementary matrix of type 3. Since all the E_i are symmetric, $H_c = HE_1E_2\cdots E_s$ and $PAQ = H_c$ where $Q = E_1E_2\cdots E_s$. Note that Q is called a *permutation matrix*. H_c is called in *canonical form* and is denoted by $\text{can}(A)$.

Remark 2.5.1 Let H be in rref and let $H_c = \text{can}(H)$. Then $HQ = H_c$ for some permutation matrix $Q = E_1E_2\cdots E_s$. Then the system $HX = \boldsymbol{b}$ becomes $H_cQ^{-1}X = HQQ^{-1}X = \boldsymbol{b}$. Let $Y = Q^{-1}X = E_s^{-1}\cdots E_1^{-1}X$. Since $E_i^T = E_i = E_i^{-1}$ (see the proof of Proposition 1.4.5), $(y_1 \ \cdots \ y_n)^T = Y = E_s\cdots E_1X$. So the unknowns $y_1, \ldots, y_n$ are just a permutation of the original unknowns $x_1, \ldots, x_n$ or just rename the variables. $H_cY = \boldsymbol{b}$ represents exactly the same system as $HX = \boldsymbol{b}$.

Example 2.5.2 Consider Example 2.4.8 again. If we let $y_1 = x_2$, $y_2 = x_4$, $u_1 = x_1$, $u_2 = x_3$ and $u_3 = x_5$. Then the equation can be rewritten as

$$\left\{\begin{array}{rcrcrcl} y_1 & - & 2u_2 & + & u_3 & = & 0 \\ y_2 & & & + & 2u_3 & = & 0 \end{array}\right. \tag{2.3}$$

If we let $u_1 = 1$, $u_2 = u_3 = 0$, then $y_1 = y_2 = 0$. Then it is a non-trivial solution of System (2.3). Equivalently, $x_1 = 1$, $x_2 = x_3 = x_4 = x_5 = 0$ is a non-trivial solution of System (2.2). If we let $u_2 = 1$, $u_1 = u_3 = 0$, then $y_1 = 2$ and $y_2 = 0$. It is also a non-trivial solution of System (2.2). Equivalently, $x_1 = 0$, $x_2 = 2$, $x_3 = 1$, $x_4 = -2$, $x_5 = 0$ is a non-trivial solution of System (2.3).

Actually, it is easy to see that we can choose any values for u_1, u_2 and u_3 arbitrarily to determine the values of y_1 and y_2. □

Base on the method of finding solution described in the above example, we are going to give a simplier proof of Theorems 2.4.9 and 2.4.13.

Proof of Theorem 2.4.9: Let $H = \text{can}(A)$ and $r = \text{rank}(A)$. Then

$$H = \left(\begin{array}{c|c} I_r & C \\ \hline O_{m-r,r} & O_{m-r,n-r} \end{array}\right),$$

where $C = (c_{ij}) \in M_{r,n-r}(\mathbb{F})$. $AX = \boldsymbol{0}$ has a non-trivial solution if and only if $HY = \boldsymbol{0}$ has a non-trivial solution. For convenience, let $Y = (y_1 \ \cdots \ y_r \ u_1 \ \cdots \ u_{n-r})^T$. Then r non-trivial equations in $HY = \boldsymbol{0}$ are of the form

$$\left\{\begin{array}{rcl} y_1 + \sum_{j=1}^{n-r} c_{1j}u_j & = & 0 \\ \vdots \qquad\qquad \vdots & & \vdots \\ y_r + \sum_{j=1}^{n-r} c_{rj}u_j & = & 0 \end{array}\right. \tag{2.4}$$

If $r < n$, then let $u_1 = 1$, $u_j = 0$ if $j > 1$ and $y_i = -c_{i1}$ for $1 \leq i \leq r$. Then Y is a non-trivial solution of $HY = \mathbf{0}$. If $r = n$, then clearly $y_i = 0$ for all $1 \leq i \leq n$. □

Proof of Theorem 2.4.13: Let $r = \text{rank}(A)$ and $H = \text{rref}(A)$. Then $\text{rref}(A|\boldsymbol{b}) = (H|\boldsymbol{c})$ for some $\boldsymbol{c}$. By Lemma 2.3.4 $HX = \boldsymbol{c}$ is consistent if and only if $\boldsymbol{c}$ is not a leading column. Then $\text{rank}(A|\boldsymbol{b}) = \text{rank}(H|\boldsymbol{c}) = \text{rank}(H) = \text{rank}(A)$.

Now we assume that the system has a solution. It was known that the solution set of $AX = \boldsymbol{b}$ is equal to the solution set of $HX = \boldsymbol{c}$. After rearranging the unknowns we may assume the system becomes $H_cY = \boldsymbol{c}$, where $H_c = \text{can}(A)$ and $Y = (y_1 \ \cdots \ y_r \ u_1 \ \cdots \ u_{n-r})^T$. The non-trivial equations are of the form

$$\begin{cases} y_1 + \sum_{j=1}^{n-r} c_{1j}u_j = c_1 \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \\ y_r + \sum_{j=1}^{n-r} c_{rj}u_j = c_r \end{cases} \tag{2.5}$$

for some c_{ij} and c_k.

Since each y_i appears in but one equation with unit coefficient, when the remaining $n-r$ unknowns (free variables) u_j are given values arbitrarily then the corresponding values of y_i can be computed. □

By applying elementary column operations of type 2 to $\text{can}(A)$, it can be transformed into a simpler form. Namely, $\text{can}(A)F_1 \cdots F_t = \left(\begin{smallmatrix} I_r & O \\ O & O \end{smallmatrix}\right)$ for some elementary matrices F_j of type 2. Thus, we have the following theorem.

Theorem 2.5.3 *For any matrix $A \in M_{m,n}(\mathbb{F})$, there are two invertible matrices P and Q such that*

$$PAQ = \begin{pmatrix} I_r & O \\ O & O \end{pmatrix}$$

where r is the rank of A.

Suppose $A \in M_{m,n}(\mathbb{F})$. We would like to find invertible matrices P and Q such that $PAQ = \begin{pmatrix} I_r & O \\ O & O \end{pmatrix}$. Again, we form the augmented matrix $\left(\begin{array}{c|c} A & I_m \\ \hline I_n & \end{array}\right)$. Then perform elementary row operations and column operations to it to get $\left(\begin{array}{c|c} \left(\begin{smallmatrix} I_r & O \\ O & O \end{smallmatrix}\right) & P \\ \hline Q & \end{array}\right)$.

Example 2.5.4 Consider Example 1.5.4 again. Consider the augmented matrix and apply elementary row and column operations as follows:

$$\left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 3 & -1 & 0 & 1 & 0 \\ 2 & -1 & 5 & 2 & 0 & 0 & 1 \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right) \xrightarrow[(-2)\mathcal{R}_1+\mathcal{R}_3]{(-2)\mathcal{R}_1+\mathcal{R}_2} \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & 1 & -3 & -2 & 1 & 0 \\ 0 & -3 & 3 & 0 & -2 & 0 & 1 \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right)$$

$$\xrightarrow[(-\frac{1}{3})\mathcal{R}_3]{(-1)\mathcal{R}_2} \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 3 & 2 & -1 & 0 \\ 0 & 1 & -1 & 0 & \frac{2}{3} & 0 & -\frac{1}{3} \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right) \xrightarrow{(-1)\mathcal{R}_2+\mathcal{R}_3}$$

$$\left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 3 & 2 & -1 & 0 \\ 0 & 0 & 0 & -3 & -\frac{4}{3} & 1 & -\frac{1}{3} \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right) \xrightarrow{(-\frac{1}{3})\mathcal{R}_3} \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 3 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 & \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right)$$

$$\xrightarrow[(-3)\mathcal{R}_3+\mathcal{R}_2]{(-1)\mathcal{R}_3+\mathcal{R}_1} \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & \frac{5}{9} & \frac{1}{3} & -\frac{1}{9} \\ 0 & 1 & -1 & 0 & \frac{2}{3} & 0 & -\frac{1}{3} \\ 0 & 0 & 0 & 1 & \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right) \xrightarrow{(-1)\mathcal{R}_2+\mathcal{R}_1}$$

$$\left(\begin{array}{cccc|ccc} 1 & 0 & 2 & 0 & -\frac{1}{9} & \frac{1}{3} & \frac{2}{9} \\ 0 & 1 & -1 & 0 & \frac{2}{3} & 0 & -\frac{1}{3} \\ 0 & 0 & 0 & 1 & \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right) \xrightarrow{\mathcal{C}_3\leftrightarrow\mathcal{C}_4} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 2 & -\frac{1}{9} & \frac{1}{3} & \frac{2}{9} \\ 0 & 1 & 0 & -1 & \frac{2}{3} & 0 & -\frac{1}{3} \\ 0 & 0 & 1 & 0 & \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ \hline 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ 0 & 0 & 1 & 0 & & & \end{array}\right)$$

$$\xrightarrow[(-2)\mathcal{C}_1+\mathcal{C}_4]{\mathcal{C}_2+\mathcal{C}_4} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & -\frac{1}{9} & \frac{1}{3} & \frac{2}{9} \\ 0 & 1 & 0 & 0 & \frac{2}{3} & 0 & -\frac{1}{3} \\ 0 & 0 & 1 & 0 & \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ \hline 1 & 0 & 0 & -2 & & & \\ 0 & 1 & 0 & 1 & & & \\ 0 & 0 & 0 & 1 & & & \\ 0 & 0 & 1 & 0 & & & \end{array}\right).$$

Then $P = \begin{pmatrix} -\frac{1}{9} & \frac{1}{3} & \frac{2}{9} \\ \frac{2}{3} & 0 & -\frac{1}{3} \\ \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \end{pmatrix}$ and $Q = \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. □

To transform a matrix to canonical form, it is not necessary to follow the order of the Gaussian elimination steps.

Example 2.5.5 Consider Example 2.5.4 and start at the 2nd step.

$$\left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & 1 & -3 & -2 & 1 & 0 \\ 0 & -3 & 3 & 0 & -2 & 0 & 1 \\ \hline \multicolumn{4}{c|}{I_4} & & & \end{array}\right) \xrightarrow[(-\frac{1}{3})\mathcal{R}_3]{\mathcal{C}_3+\mathcal{C}_2} \left(\begin{array}{cccc|ccc} 1 & 2 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -3 & -2 & 1 & 0 \\ 0 & 0 & 1 & 0 & -\frac{2}{3} & 0 & \frac{1}{3} \\ \hline 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 1 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right)$$

$$\xrightarrow[(-1)\mathcal{R}_3+\mathcal{R}_2]{(-1)\mathcal{R}_3+\mathcal{R}_1} \left(\begin{array}{cccc|ccc} 1 & 2 & 0 & 1 & \frac{5}{3} & 0 & -\frac{1}{3} \\ 0 & 0 & 0 & -3 & -\frac{4}{3} & 1 & -\frac{1}{3} \\ 0 & 0 & 1 & 0 & -\frac{2}{3} & 0 & \frac{1}{3} \\ \hline 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 1 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right) \xrightarrow[\mathcal{C}_4\leftrightarrow\mathcal{C}_2]{(-\frac{1}{3})\mathcal{R}_2} \left(\begin{array}{cccc|ccc} 1 & 1 & 0 & 2 & \frac{5}{3} & 0 & -\frac{1}{3} \\ 0 & 1 & 0 & 0 & \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ 0 & 0 & 1 & 0 & -\frac{2}{3} & 0 & \frac{1}{3} \\ \hline 1 & 0 & 0 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ 0 & 0 & 1 & 1 & & & \\ 0 & 1 & 0 & 0 & & & \end{array}\right)$$

$$\xrightarrow[(-2)\mathcal{C}_1+\mathcal{C}_4]{(-1)\mathcal{C}_1+\mathcal{C}_2} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & \frac{5}{3} & 0 & -\frac{1}{3} \\ 0 & 1 & 0 & 0 & \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ 0 & 0 & 1 & 0 & -\frac{2}{3} & 0 & \frac{1}{3} \\ \hline 1 & -1 & 0 & -2 & & & \\ 0 & 0 & 0 & 1 & & & \\ 0 & 0 & 1 & 1 & & & \\ 0 & 1 & 0 & 0 & & & \end{array}\right)$$

Then $P = \begin{pmatrix} \frac{5}{3} & 0 & -\frac{1}{3} \\ \frac{4}{9} & -\frac{1}{3} & \frac{1}{9} \\ -\frac{2}{3} & 0 & \frac{1}{3} \end{pmatrix}$ and $Q = \begin{pmatrix} 1 & -1 & 0 & -2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$. Compare with Example 2.5.4 we see that such P and Q are not unique. □

Elementary row and column operations work in any field. We give an example working in finite field.

Example 2.5.6 Consider the same matrix of Example 2.5.4 but it is viewed as a matrix over $\mathbb{Z}_3 = \{0, 1, 2\}$. Note that $-1 = 5 = 2, 3 = 0$ in this case.

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & \\ 2 & 1 & 3 & -1 & I_3 \\ 2 & -1 & 5 & 2 & \end{array}\right) = \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & \\ 2 & 1 & 0 & 2 & I_3 \\ 2 & 2 & 2 & 2 & \end{array}\right)$$

$$\xrightarrow[\mathcal{R}_1+\mathcal{R}_2]{\mathcal{R}_1+\mathcal{R}_3} \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right) \xrightarrow{2\mathcal{R}_2} \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{2\mathcal{R}_2+\mathcal{R}_1} \left(\begin{array}{cccc|ccc} 1 & 0 & 2 & 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right)$$

Then $P = \begin{pmatrix} 2 & 1 & 0 \\ 2 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ and $PA = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. □

Theorem 2.5.7 *Let $A \in M_{m,n}(\mathbb{F})$. Then* $\text{rank}(A) = \text{rank}(A^T)$.

Proof: Suppose $r = \text{rank}(A)$. Then there are two invertible matrices P and Q such that

$$PAQ = \begin{pmatrix} I_r & O_{r,n-r} \\ O_{m-r,r} & O_{m-r,n-r} \end{pmatrix}.$$

Then

$$Q^T A^T P^T = \begin{pmatrix} I_r & O_{r,m-r} \\ O_{n-r,r} & O_{n-r,m-r} \end{pmatrix}.$$

Clearly $\text{rank}(Q^T A^T P^T) = r$. Since Q^T and P^T are invertible, by Theorem 2.4.11 $\text{rank}(Q^T A^T P^T) = \text{rank}(A^T)$. □

Theorem 2.5.8 *For every $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{q,m}(\mathbb{F})$, we have* $\text{rank}(BA) \leq \text{rank}(A)$.

Proof: Combining Theorems 2.5.7 and 2.4.10 we have

$$\text{rank}(BA) = \text{rank}((BA)^T) = \text{rank}(A^T B^T) \leq \text{rank}(A^T) = \text{rank}(A).$$

□

Remark 2.5.9 We only use elementary row operations to solve a system of linear equations since we do not want to mess up the unknown variables. However, if we want to change the variables, for example, in solving system of Diophantine equations in number theory, we may use elementary column operations. We shall elaborate this idea in the following example.

Example 2.5.10 Solve the following system of Diophantine equations. That is, find the integral solutions of this system.

$$\begin{cases} x + y + z = 15 \\ 2x + 4y + 5z = 50 \end{cases}$$

We start by forming a matrix

$$A = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 15 \\ 2 & 4 & 5 & 50 \\ \hline 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array}\right) \begin{matrix} \\ \\ x \\ y \\ z \end{matrix}$$

Then perform a sequence of elementary row operations on the first two rows of A for simplifying the system and column operations on the first three columns of A for changing variables.

$$A \xrightarrow{(-2)\mathcal{R}_1+\mathcal{R}_2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 15 \\ 0 & 2 & 3 & 20 \\ \hline 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array}\right) \begin{matrix} \\ \\ x \\ y \\ z \end{matrix} \xrightarrow[(-1)\mathcal{C}_1+\mathcal{C}_3]{(-1)\mathcal{C}_1+\mathcal{C}_2} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 15 \\ 0 & 2 & 3 & 20 \\ \hline 1 & -1 & -1 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array}\right) \begin{matrix} \\ \\ x \\ y \\ z \end{matrix}$$

$$\xrightarrow{(-1)\mathcal{C}_2+\mathcal{C}_3} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 15 \\ 0 & 2 & 1 & 20 \\ \hline 1 & -1 & 0 & \\ 0 & 1 & -1 & \\ 0 & 0 & 1 & \end{array}\right) \begin{matrix} \\ \\ x \\ y \\ z \end{matrix} \xrightarrow{\mathcal{C}_2\leftrightarrow\mathcal{C}_3} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 15 \\ 0 & 1 & 2 & 20 \\ \hline 1 & 0 & -1 & \\ 0 & -1 & 1 & \\ 0 & 1 & 0 & \end{array}\right) \begin{matrix} \\ \\ x \\ y \\ z \end{matrix}$$

$$\xrightarrow{(-2)C_2+\mathcal{C}_3} \begin{array}{ccc} u & v & w \end{array} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 15 \\ 0 & 1 & 0 & 20 \\ \hline 1 & 0 & -1 & \\ 0 & -1 & 3 & \\ 0 & 1 & -2 & \end{array}\right) \begin{matrix} \\ \\ x \\ y \\ z \end{matrix}$$

So we introduce new variables u, v, w. Hence we get $u = 15$, $v = 20$ and

$$\begin{aligned} x &= u - w = 15 - w \\ y &= -v + 3w = -20 + 3w \\ z &= v - 2w = 20 - 2w \end{aligned}$$

Here w is any integer. □

Remark 2.5.11 We may use elementary column operations to find the greatest common divisor of two integers a and b. We form a matrix $\left(\begin{array}{cc} a & b \\ \hline 1 & 0 \\ 0 & 1 \end{array}\right)$ and perform a sequence of elementary column

operation of types 2 and 3 until we get $\left(\begin{array}{c|c} r_n & 0 \\ \hline s & u \\ t & v \end{array}\right)$ or $\left(\begin{array}{c|c} 0 & r_n \\ \hline u & s \\ v & t \end{array}\right)$. Then we shall be able to find $r_n = (a, b)$ and integers s and t such that $r_n = sa + tb$.

Example 2.5.12 Let us redo Example 0.2.7 by using elementary column operations of types 2 and 3 as follows:

$$\left(\begin{array}{rr|r} 34567 & 3210 \\ \hline 1 & 0 \\ 0 & 1 \end{array}\right) \xrightarrow{(-10)\mathcal{C}_2+\mathcal{C}_1} \left(\begin{array}{rr|r} 2467 & 3210 \\ \hline 1 & 0 \\ -10 & 1 \end{array}\right) \xrightarrow{(-1)\mathcal{C}_1+\mathcal{C}_2} \left(\begin{array}{rr|r} 2467 & 743 \\ \hline 1 & -1 \\ -10 & 11 \end{array}\right)$$

$$\xrightarrow{(-3)\mathcal{C}_2+\mathcal{C}_1} \left(\begin{array}{rr|r} 238 & 743 \\ \hline 4 & -1 \\ -43 & 11 \end{array}\right) \xrightarrow{(-3)\mathcal{C}_1+\mathcal{C}_2} \left(\begin{array}{rr|r} 238 & 29 \\ \hline 4 & -13 \\ -43 & 140 \end{array}\right) \xrightarrow{(-8)\mathcal{C}_2+\mathcal{C}_1} \left(\begin{array}{rr|r} 6 & 29 \\ \hline 108 & -13 \\ -1163 & 140 \end{array}\right)$$

$$\xrightarrow{(-4)\mathcal{C}_1+\mathcal{C}_2} \left(\begin{array}{rr|r} 6 & 5 \\ \hline 108 & -445 \\ -1163 & 4792 \end{array}\right) \xrightarrow{(-1)\mathcal{C}_2+\mathcal{C}_1} \left(\begin{array}{rr|r} 1 & 5 \\ \hline 553 & -445 \\ -5955 & 4792 \end{array}\right) \xrightarrow{(-5)\mathcal{C}_1+\mathcal{C}_2} \left(\begin{array}{rr|r} 1 & 0 \\ \hline 553 & -3210 \\ -5955 & 34567 \end{array}\right).$$

Hence $d = 1$, $s = 553$ and $t = -5955$. One may see that we get the values of s_i's and t_i's obtained in Example 0.2.9. Also we do not need to carry out the last step as everyone knows that g.c.d$(5, 1) = 1$.

Exercise 2.5

2.5-1. Find invertible matrices P and Q over $\mathbb{R}$ such that PAQ is the canonical form of A, where A is

(a) $\begin{pmatrix} 1 & 3 & 2 & 4 \\ 4 & 2 & 3 & 1 \\ 1 & 0 & 2 & 1 \end{pmatrix}$; (b) $\begin{pmatrix} 3 & 2 & 3 & -1 \\ 4 & 0 & 3 & 2 \\ 2 & 4 & 1 & 3 \\ 1 & 1 & 0 & 1 \end{pmatrix}$; (c) $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & -1 \\ 4 & 2 & 0 \\ 2 & 4 & 1 \\ 3 & 1 & 1 \end{pmatrix}$.

2.5-2. Show that $A \in M_{m,n}(\mathbb{F})$ has rank at most 1 if and only if $A = BC$, where $B \in M_{m,1}(\mathbb{F})$ and $C \in M_{1,n}(\mathbb{F})$.

2.5-3. Suppose A is a square matrix of rank 1. Show that $A^2 = cA$ for some scalar c.

2.5-4. Let $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{n,m}(\mathbb{F})$. Show that if $m \neq n$, then AB and BA cannot both be the identity matrices.

2.5-5. We label the 26 alphabets A to Z by integers $1, 2 \ldots, 26$ and use 0 to denote a space. When we want to send a message, we put the content words (now are numbers) into a certain matrix starting from the first row. Let us call this matrix M. Now let S be a secret matrix only you and your friend know. Then your friend send an encoded message SM to you. Then you will be able to decode that message. Now let

$$S = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{pmatrix} \text{ and suppose } \begin{pmatrix} 41 & 40 & 80 & 24 \\ 90 & 104 & 197 & 67 \\ 74 & 79 & 138 & 43 \end{pmatrix}$$

be the message you received. What is the real message?

Chapter 3

Vector Spaces of $\mathbb{F}^n$

3.1 Introduction

In secondary school, we have learnt vectors. For examples, vectors in the plane; vectors in the space.

In the plane, we choose a point O called origin. The horizontal and vertical straight lines pass through the origin are called the x-axis and y-axis, respectively. Each point P in the plane can be represented by an ordered pair (x_0, y_0), where x_0 and y_0 are the distances from P to the y-axis and the x-axis, respectively. The ordered pair (x_0, y_0) is called the coordinate of P. The arrow starts from O and ends at P is called a vector and is also denoted by (x_0, y_0).

In physics, a 2-dimensional force $\boldsymbol{F}$ can be represented by (F_x, F_y), where $F_x, F_y \in \mathbb{R}$. The ordered pair (F_x, F_y) represents the direction of the force $\boldsymbol{F}$. The length of (F_x, F_y), which is $\sqrt{F_x^2 + F_y^2}$, is the magnitude of the force. Suppose there are two forces $\boldsymbol{F}_1 = (x_1, y_1)$ and $\boldsymbol{F}_2 = (x_2, y_2)$ acting on an object. The total force acting on the object is $\boldsymbol{F}_1 + \boldsymbol{F}_2 = (x_1 + x_2, y_1 + y_2)$. It is called the sum of the forces. Suppose $k > 0$. Then $k\boldsymbol{F}_1$ denotes a force whose magnitude is k times the magnitude of $\boldsymbol{F}_1$ and whose direction is the same as that of $\boldsymbol{F}$. It is known that $k\boldsymbol{F}_1 = (kx_1, ky_1)$. $-F_1 = (-x_1, -y_1)$ is the force with the same magnitude of $\boldsymbol{F}$ but opposite in direction. Thus $k\boldsymbol{F}$ has a physical meaning for each $k \in \mathbb{R}$. The set of all 2-dimensional vectors will be called a 2-dimensional vector space over $\mathbb{R}$.

For the space, a force $\boldsymbol{F}$ can be represented by (F_x, F_y, F_z), where $F_x, F_y, F_z \in \mathbb{R}$. The sum of two forces $\boldsymbol{F}_1 = (x_1, y_1, z_1)$ and $\boldsymbol{F}_2 = (x_2, y_2, z_2)$ are $\boldsymbol{F}_1 + \boldsymbol{F}_2 = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$. For each $k \in \mathbb{R}$, $kF_1 = (kx_1, ky_1, kz_1)$. The set of all 3-dimensional vectors will be called a 3-dimensional vector space over $\mathbb{R}$.

3.2 Vector Spaces of n-tuples

Now we are going to give a general definition of vector space of n-tuples. For a positive integer n, let $\mathbb{F}^n$ denote the set of all n-tuples $(x_1, \ldots, x_n)$ where $x_i \in \mathbb{F}$. For each point $P = (x_1, \ldots, x_n)$ in $\mathbb{F}^n$, we shall identify P with the vector OP, where O is the origin. Thus $\alpha = (x_1, \ldots, x_n)$ denotes the point P and is called a *vector*. The vector $\alpha = (x_1, \ldots, x_n)$ is often referred as vector form. In matrix

algebra, *we often write vectors in* $\mathbb{F}^n$ *in matrix form as an* $n \times 1$ *matrix* $\alpha = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. In other word, *we often identify the set* $\mathbb{F}^n$ *with* $M_{n,1}(\mathbb{F})$. The addition and the scalar multiplication in $\mathbb{F}^n$ are the same as those in $M_{n,1}(\mathbb{F})$. As a special type of matrix, we have the following proposition.

Proposition 3.2.1 *For any* $\alpha, \beta, \gamma \in \mathbb{F}^n$ *and* $a, b \in \mathbb{F}$, *we have*

(a) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$,

(b) $\alpha + \beta = \beta + \alpha$,

(c) $\alpha + \mathbf{0}_n = \alpha$,

(d) $a(\alpha + \beta) = a\alpha + a\beta$,

(e) $(a + b)\alpha = a\alpha + b\alpha$,

(f) $0\alpha = \mathbf{0}_n$.

Definition 3.2.2 A (nonempty) subset V of $\mathbb{F}^n$ is called a *vector space of* $\mathbb{F}^n$ if it satisfies the property:

$$\text{If } \alpha, \beta \in V, \text{ then } a\alpha + b\beta \in V \text{ for any } a, b \in \mathbb{F}.$$

Example 3.2.3 $\{\mathbf{0}_n\}$ and $\mathbb{F}^n$ are vector spaces of $\mathbb{F}^n$. □

Lemma 3.2.4 *Let* V *be a nonempty subset of* $\mathbb{F}^n$. *The following statements are equivalent:*

(a) If $\alpha, \beta \in V$, *then* $a\alpha + b\beta \in V$ *for any* $a, b \in \mathbb{F}$.

(b) If $\alpha, \beta \in V$, *then* $a\alpha + \beta \in V$ *for any* $a \in \mathbb{F}$.

(c) If $\alpha, \beta \in V$, *then* $\alpha + \beta \in V$ *and* $a\alpha \in V$ *for any* $a \in \mathbb{F}$.

Proof: Clearly (a) implies (b) by fixing $b = 1$.

Suppose (b) holds. If $\alpha, \beta \in V$, then by (b) $\alpha + \beta = 1\alpha + \beta \in V$ and $a\alpha = (a-1)\alpha + \alpha \in V$. Then (c) holds.

Suppose (c) holds. If $\alpha, \beta \in V$, then for any $a, b \in \mathbb{F}$ by (c) $a\alpha \in V$ and $b\beta \in V$. Since $a\alpha, b\beta \in V$, by (c) again $a\alpha + b\beta \in V$. So (a) holds. □

Example 3.2.5 For any given numbers a and b, all vectors of $\mathbb{R}^2$ lying on the line $ax + by = 0$ form a vector space of $\mathbb{R}^2$.

Solution: Let $V = \{(x, y) \in \mathbb{R}^2 \mid ax + by = 0\}$. Clearly, $(0, 0) \in V$. So V is not empty. For every $\alpha = (x_1, y_1)$, $\beta = (x_2, y_2) \in V$ and every $c \in \mathbb{R}$, $c\alpha + \beta = (cx_1 + x_2, cy_1 + y_2)$. Since $ax_i + by_i = 0$ for $i = 1, 2$, we have $a(cx_1 + x_2) + b(cy_1 + y_2) = c(ax_1 + by_1) + (ax_2 + by_2) = 0$. Thus $c\alpha + \beta \in V$. By Lemma 3.2.4, V is a vector space of $\mathbb{R}^2$. □

Proposition 3.2.6 *Let* $A \in M_{m,n}(\mathbb{F})$ *and* $V = \{X \in \mathbb{F}^n \mid AX = \mathbf{0}_m\}$. *Then* V *is a vector space of* $\mathbb{F}^n$.

Proof: Clearly, $\mathbf{0}_n \in V$. So $V \neq \varnothing$ (the empty set). For any $\alpha, \beta \in V$ and $a \in \mathbb{F}$,

$$A(a\alpha + \beta) = aA\alpha + A\beta = a\mathbf{0}_m + \mathbf{0}_m = \mathbf{0}_m.$$

Then $a\alpha + \beta \in V$. By Lemma 3.2.4, V is a vector space of $\mathbb{F}^n$. □

The space V defined in the previous proposition is called the *solution space of the linear system* $AX = \mathbf{0}$ or the *null space of* A.

Proposition 3.2.7 *Suppose V is a vector space of $\mathbb{F}^n$, then $\mathbf{0}_n \in V$.*

Proof: Since $V \neq \varnothing$, there exists $\alpha \in V$. Since V is a vector space, $\mathbf{0}_n = 0\alpha \in V$. □

In general, by Proposition 3.2.7 for a linear system $AX = \boldsymbol{b}$, if $\boldsymbol{b} \neq \mathbf{0}$ then the set of all solutions of $AX = \boldsymbol{b}$ is not a vector space.

Example 3.2.8 For any given numbers a, b and $c \neq 0$, the set V of all vectors in $\mathbb{R}^2$ lying on the line $ax + by + c = 0$ is not a vector space of $\mathbb{R}^2$.

Solution: Since $\mathbf{0}_2$ does not satisfy the equation $ax + by + c = 0$, $\mathbf{0}_2 \notin V$. □

Example 3.2.9 Let V be the set of vectors in $\mathbb{R}^3$ satisfying $x+y+z = 0$. Clearly $\alpha_1 = (-1, 0, 1)$ and $\alpha_2 = (-1, 1, 0)$ are in V. For any vector $\alpha = (a, b, c)$, we have $b + c = -a$. Then $\alpha = (-b - c, b, c) = b\alpha_1 + c\alpha_2$. So $V \subseteq \{b\alpha_1 + c\alpha_2 \mid b, c \in \mathbb{R}\}$.

For any vector $b\alpha_1 + c\alpha_2 = (-b - c, b, c)$, clearly it satisfies the equation $x + y + z = 0$. Therefore, $V = \{b\alpha_1 + c\alpha_2 \mid b, c \in \mathbb{R}\}$.

It has just been shown that any vector in V can be expressed as the form $b\alpha_1 + c\alpha_2$ for some $b, c \in \mathbb{R}$. We shall call this expression as a linear combination of α_1 and α_2. □

Definition 3.2.10 Let V be a vector space of $\mathbb{F}^n$. Suppose $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq V$. The expression

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k = \sum_{i=1}^{k} a_i\alpha_i$$

is called a *linear combination of* $\alpha_1, \alpha_2, \ldots, \alpha_k$ or a *linear combination of the set* S, where $a_1, a_2, \ldots, a_k \in \mathbb{F}$. We also call that β is *linearly dependent on* S. The set of all linear combinations of S is called the *span of* S and is denoted by $\text{span}\{\alpha_1, \alpha_2, \ldots, \alpha_k\} = \text{span}(S)$. If $V = \text{span}(S)$, then S is called a *spanning set of* V.

Theorem 3.2.11 *Let $\{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq \mathbb{F}^n$, $k \geq 1$. Then* $\text{span}\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ *is a vector space of* $\mathbb{F}^n$.

Proof: It is clear that $\mathbf{0} = 0\alpha_1 + \cdots + 0\alpha_k \in V$. So $V \neq \varnothing$. Let $\alpha, \beta \in V = \text{span}\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ and $a \in \mathbb{F}$. Then $\alpha = \sum_{i=1}^{k} a_i\alpha_i$ and $\beta = \sum_{j=1}^{k} b_j\alpha_j$ for some $a_i, b_j \in \mathbb{F}$.

$$a\alpha + \beta = \sum_{i=1}^{k} aa_i\alpha_i + \sum_{j=1}^{k} b_j\alpha_j = \sum_{i=1}^{k} (aa_i + b_i)\alpha_i \in V.$$

By Lemma 3.2.4, V is a vector space of $\mathbb{F}^n$. □

Example 3.2.12 It is clear that $\text{span}\{\mathbf{0}\} = \{\mathbf{0}\}$ and $\mathbb{F}^n = \text{span}\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$. The set V described in Example 3.2.9 is a span of $\{(-1\ 0\ 1), (-1\ 1\ 0)\}$. □

Exercise 3.2

3.2-1. By finding spanning sets, show that the following sets are vector spaces of $\mathbb{F}^n$.

(a) (a, b, c, d) with $a + b = 0$ and $c + d = 0$.

(b) (a, b, c, d) with $a + c + d = 0$.

(c) $(a, 2a, -3a, 0)$

3.2-2. Is $\mathbb{F}^3$ a vector space of $\mathbb{F}^4$? Is $\text{span}\{(1, 0, 0, 0),\ (0, 1, 0, 0)\ (0, 0, 1, 0)\}$ a vector space of $\mathbb{F}^4$?

3.2-3. Let $\alpha, \beta, \gamma \in \mathbb{F}^n$. Consider the set of all vectors of the form $\alpha + b\beta + c\gamma$, where $b, c \in \mathbb{F}$. Is this set a vector space of $\mathbb{F}^n$?

3.2-4. Let V and W be vector spaces of $\mathbb{F}^n$. Show that $V \cap W$ is a vector space of $\mathbb{F}^n$. Is $V \cup W$ a vector space of $\mathbb{F}^n$ in general? If not, give a counterexample. Also give conditions under which it is a vector space of $\mathbb{F}^n$.

3.2-5. Let V and W be vector spaces of $\mathbb{F}^n$. Define

$$V + W = \{v + w \mid v \in V, w \in W\}.$$

Show that $V + W$ is a vector space of $\mathbb{F}^n$. $V + W$ is called the *sum of* V *and* W.

3.2-6. Let $A \subseteq B$ be two subsets of a vector space of $\mathbb{F}^n$. Show that $\text{span}(A) \subseteq \text{span}(B)$.

3.3 Linear Independence, Bases and Dimension

Example 3.3.1 Let $v_1 = (1, 0)$, $v_2 = (1, 1)$ and $v_3 = (2, 1)$. Clearly,
$\mathbb{R}^2 = \text{span}\{v_1, v_2, v_3\}$. But actually $\mathbb{R}^2 = \text{span}\{v_1, v_2\} = \text{span}\{v_1, v_3\} = \text{span}\{v_2, v_3\}$. □

From the above example, we can see that there may have some vectors in the spanning set of a vector space that are redundant. We may remove the redundant vectors from the spanning set and the reduced set is also a spanning set of that vector space. Our purpose is to reduce the size of the spanning set of a vector space as small as possible.

Consider a set of vectors $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ in $\mathbb{F}^n$. Clearly $\mathbf{0}$ is always a linear combination of S, since $\mathbf{0} = 0\alpha_1 + 0\alpha_2 + \cdots + 0\alpha_k$.

Definition 3.3.2 Consider a set of vectors $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ in $\mathbb{F}^n$. An expression of the form $\sum_{i=1}^{n} a_i\alpha_i = \mathbf{0}$ is called a *linear relation* among the α's. A linear relation with all $a_i = 0$ is called *trivial*. A linear relation in which at least one $a_i \neq 0$ is called *non-trivial*.

Example 3.3.3 Let $\alpha = (3, 2, -3)$, $\beta = (-1, 0, 1)$ and $\gamma = (0, 1, 0)$ be three vectors in $\mathbb{R}^3$. Clearly, $\alpha + 3\beta + (-2)\gamma = (0, 0, 0) = \mathbf{0}$. It shows that there are three scalars a, b and c (in $\mathbb{R}$) which are not all zero such that $a\alpha + b\beta + c\gamma = \mathbf{0}$. Thus, there is a non-trivial linear relation among α, β and γ. In this case we can choose a vector suitably so that it is in terms of the other vector(s). For example, $\beta = -\frac{1}{3}\alpha + \frac{2}{3}\gamma$. That is, β depends on α and γ (in linear form). Note that, for this example we can choose anyone. □

Example 3.3.4 Let $\alpha = (3, 2, -3)$ and $\beta = (-1, 0, 1)$ be vectors in $\mathbb{R}^3$. Can we find two real numbers, say a and b, which are not all zero such that $a\alpha + b\alpha = \mathbf{0}$? If we can, then $(3a, 2a, -3a) + (-b, 0, b) = (0, 0, 0)$. Hence we have three equations:

$$\begin{cases} 3a - b = 0 \\ 2a \quad\;\; = 0 \\ -3a + b = 0 \end{cases}$$

Clearly, we have $a = 0 = b$. It contradicts a and b being not all zero. This means that α and β are not dependent on each other. In other words, they are independent (in linear form). □

Definition 3.3.5 Vectors $\alpha_1, \alpha_2, \ldots, \alpha_k$ are *linearly dependent over* $\mathbb{F}$ if there exist $a_1, a_2, \ldots, a_k$ in $\mathbb{F}$ not all zero such that $\sum_{i=1}^{k} a_i\alpha_i = \mathbf{0}$, i.e., there is a non-trivial linear relation among $\alpha_1, \alpha_2, \ldots, \alpha_k$. A set $S \subseteq V$, where V is a vector space of $\mathbb{F}^n$, is said to be *linearly dependent* if there exist $\alpha_1, \alpha_2, \ldots, \alpha_k \in S$ such that $\alpha_1, \alpha_2, \ldots, \alpha_k$ are linearly dependent over $\mathbb{F}$. A set is said to be *linearly independent* if it is not linearly dependent.

Remark: The set $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ being linearly independent is equivalent to the following statement:

$$\sum_{i=1}^{k} a_i\alpha_i = \mathbf{0} \text{ for some } a_i \in \mathbb{F} \text{ implies } a_i = 0 \text{ for all } i.$$

Example 3.3.6 Let $\alpha_1 = (1, 1, 1, 1)$, $\alpha_2 = (2, 1, 3, -2)$ and $\alpha_3 = (2, -1, 5, 2)$ in $\mathbb{R}^4$. Are α_1, α_2 and α_3 linearly independent over $\mathbb{R}$?
Answer: Suppose $a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 = (0, 0, 0, 0)$. Then we have

$$\begin{cases} a_1 + 2a_2 + 2a_3 = 0 \\ a_1 + a_2 - a_3 = 0 \\ a_1 + 3a_2 + 5a_3 = 0 \\ a_1 - 2a_2 + 2a_3 = 0 \end{cases}$$

By solving this system we have the only solution $a_1 = a_2 = a_3 = 0$. Thus $\alpha_1, \alpha_2, \alpha_3$ are linearly independent. □

Definition 3.3.7 Let $V \neq \{\mathbf{0}\}$ be a vector space of $\mathbb{F}^n$. A set $S \subset V$ is said to be a *basis of* V (or a *basis for* V) if S is a linearly independent spanning set of V, i.e., both a linearly independent set and a spanning set of V.

Example 3.3.8 Clearly $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ is a basis of $\mathbb{F}^n$. This basis is called the *standard basis for* $\mathbb{F}^n$. In particular, $\{(1, 0), (0, 1)\}$ is a basis of $\mathbb{F}^2$. Also $\{(1, 0), (1, 1)\}$ is a basis of $\mathbb{F}^2$. So we see that basis of a vectors space is not unique. □

Theorem 3.3.9 *The set* $\{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq \mathbb{F}^n$ *is linearly dependent if and only if the rank of the matrix* $A = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_k \end{pmatrix}$ *is less than* k.

Proof: $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ is linearly dependent

if and only if there exist $a_1, a_2, \ldots, a_k \in \mathbb{F}$ not all zero such that $\sum_{i=0}^{k} a_i\alpha_i = \mathbf{0}$

if and only if $A \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = \mathbf{0}$
if and only if $AX = \mathbf{0}$ has a non-trivial solution
if and only if $\text{rank}(A) < k$ (by Theorem 2.4.9). □

Corollary 3.3.10 *A square matrix A is nonsingular if and only if its columns (rows, respectively) are linearly independent.*

Corollary 3.3.11 *Suppose $S = \{\alpha_1, \ldots, \alpha_k\}$ is a subset of $\mathbb{F}^n$. If $n < k$, then S is linearly dependent.*

Theorem 3.3.12 *Suppose V is a vector space of $\mathbb{F}^n$ containing at least one nonzero vector. Then V has a basis.*

Proof: Since V contains a nonzero vector, say α, $\{\alpha\}$ is clearly linearly independent. Let S be any linearly independent set in V. By Corollary 3.3.11 S is a finite set with at most n elements. So we have $1 \leq |S| \leq n$. Let $\mathscr{B}$ be the maximal cardinality set among all the linearly independent sets in V, i.e.,

$$|\mathscr{B}| = \max\{|S| \mid S \text{ is a linearly independent set in } V\}.$$

We shall call this set to be a *maximal linearly independent set.*

Let $\mathscr{B} = \{\alpha_1, \ldots, \alpha_k\}$. For any $\beta \in V$. If $\beta \in \mathscr{B}$, then it is clear that $\beta \in \text{span}(\mathscr{B})$. If not, since $\mathscr{B}$ is a maximal linearly independent set, $\mathscr{B} \cup \{\beta\}$ is linearly dependent. There exist $b, a_1, \ldots, a_k \in \mathbb{F}$ not all zero such that

$$b\beta + a_1\alpha_1 + \cdots + a_k\alpha_k = \mathbf{0}.$$

If $b = 0$, then $\alpha_1, \ldots, \alpha_k$ has a non-trivial linear relation. It contradicts their linear independence. So $b \neq 0$ and hence

$$\beta = -b^{-1}\left(\sum_{i=1}^{k} a_i\alpha_i\right).$$

In this case, $\beta \in \text{span}(\mathscr{B})$.

Then $\text{span}(\mathscr{B}) = V$. So $\mathscr{B}$ is a basis of V. □

Proposition 3.3.13 *Suppose $\alpha_1, \ldots, \alpha_k$ are linearly independent. If $\beta = \sum_{i=1}^{k} a_i\alpha_i$ for some $a_1, \ldots, a_k \in \mathbb{F}$, then $a_1, \ldots, a_k$ are unique.*

Proof: Suppose $\beta = \sum_{i=1}^{k} a_i\alpha_i = \sum_{i=1}^{k} b_i\alpha_i$ for some $b_1, \ldots, b_k \in \mathbb{F}$. Then $\sum_{i=1}^{k}(a_i - b_i)\alpha_i = \mathbf{0}$. Since $\alpha_1, \ldots, \alpha_k$ are linearly independent, $a_i - b_i = 0$ for all i. So $a_i = b_i$ for all i. □

Corollary 3.3.14 *Suppose $\{\alpha_1, \ldots, \alpha_k\}$ is a basis for a vector space V. Then for each $\alpha \in V$, then there exist unique scalars $c_1, \ldots, c_k \in \mathbb{F}$ such that $\alpha = \sum_{i=1}^{k} c_i\alpha_i$.*

Theorem 3.3.15 *Let V be a vector space of $\mathbb{F}^n$. Suppose $\mathscr{A} = \{\alpha_1, \ldots, \alpha_k\}$ and $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$ are bases for V. Then $k = m$.*

Proof: Let $A = \begin{pmatrix} \alpha_1 & \cdots & \alpha_k \end{pmatrix}$ and $B = \begin{pmatrix} \beta_1 & \cdots & \beta_m \end{pmatrix}$. Since $\mathscr{A}$ is linearly independent, by Theorem 3.3.9 $\text{rank}(A) = k$. Similarly, we have $\text{rank}(B) = m$.

Since $\mathscr{B}$ is a basis, for each i, $1 \leq i \leq k$, there exist $c_{1i}, \ldots, c_{mi} \in \mathbb{F}$ such that

$$\alpha_i = \sum_{j=1}^{m} c_{ji}\beta_j = B \begin{pmatrix} c_{1i} \\ \vdots \\ c_{mi} \end{pmatrix}.$$

Let $\boldsymbol{c}_i = (c_{1i} \ \cdots \ c_{mi})^T$ and $C = \begin{pmatrix} \boldsymbol{c}_1 & \cdots & \boldsymbol{c}_k \end{pmatrix}$. Then

$$BC = \begin{pmatrix} B\boldsymbol{c}_1 & \cdots & B\boldsymbol{c}_k \end{pmatrix} = \begin{pmatrix} \alpha_1 & \cdots & \alpha_k \end{pmatrix} = A.$$

Therefore, $k = \text{rank}(A) = \text{rank}(BC) \leq \text{rank}(B) = m$.

Reversing the roles of $\mathscr{A}$ and $\mathscr{B}$ we obtain $m \leq k$. So we have $k = m$. □

From the above theorem, we know that the cardinality of a basis of a vector space is a constant. So we can make the following definition.

Definition 3.3.16 Let V be a vector space of $\mathbb{F}^n$. If $V \neq \{\mathbf{0}\}$, then the *dimension* of V, denoted by $\dim V$, is defined to be the cardinality of any basis of V. If $V = \{\mathbf{0}\}$, then we define $\dim V = 0$.

Corollary 3.3.17 *Suppose* $\dim V = k$. *If S is a linearly independent set in V and $|S| = k$, then S is a basis of V.*

Proof: By the same proof of Theorem 3.3.12 we know that S spans V. So it is a basis of V. □

Lemma 3.3.18 *Suppose* $\dim V = k$. *If $S \subseteq V$ and $|S| > k$, then S is linearly dependent.*

Proof: Since $|S| > k$, there are $\alpha_1, \alpha_2, \ldots, \alpha_{k+1} \in S$. Since k is the maximum cardinality of all linearly independent sets in V, $\alpha_1, \alpha_2, \ldots, \alpha_{k+1}$ are linearly dependent. So S is linearly dependent. □

Example 3.3.19 $\dim \mathbb{F}^n = n$. The dimension of V described in Example 3.2.9 is 2. According to Example 3.3.6, we let $V = \text{span}\{\alpha_1, \alpha_2, \alpha_3\}$. Then $\dim V = 3$. □

Example 3.3.20 Suppose H is in rref and of rank r. Let $\alpha_1, \cdots, \alpha_r$ be the r non-zero rows of H.

By Lemma 1.5.7, $A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \end{pmatrix}$ is in rref. By definition $\text{rank}(A) = r$. So we have $\text{rank}(A^T) = r$. Now $\alpha_1^T, \ldots, \alpha_r^T$ are the r columns of A^T. By Theorem 3.3.9, $\{\alpha_1^T, \ldots, \alpha_r^T\}$ is linearly independent. So $\alpha_1, \ldots, \alpha_r$ are linearly independent. □

Exercise 3.3

3.3-1. Which of the following sets are linearly independent? For those that are linearly dependent, find a linear relation among them.

(a) $\{(1,0,1),\ (1,1,1),\ (-1,1,-3)\}$ in $\mathbb{R}^3$.

(b) $\{(1,0,0),\ (1,1,-1),\ (1,1,3)\}$ in $\mathbb{R}^3$.

(c) $\{(3,1,1),\ (2,-1,5),\ (4,0,-3)\}$ in $\mathbb{R}^3$.

(d) $\{(2,0,1),\ (1,1,0),\ (0,1,1),\ (1,1,-1)\}$ in $\mathbb{R}^3$.

(e) $\{(1,1,0,1),\ (4,2,0,0),\ (0,0,1,0),\ (1,4,4,1)\}$ in $\mathbb{Z}_5^4$.

3.3-2. Find a linear relation among the columns of

$$A = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \\ -1 & 1 & 0 & 0 \end{pmatrix}.$$

3.3-3. For which values of a do the vectors $(a,-1,-1)$, $(-1,a,-1)$, $(-1,-1,a)$ form a linearly dependent set in $\mathbb{R}^3$?

3.3-4. Suppose $\{\alpha_1,\alpha_2,\alpha_3\}$ is linearly independent. Show that $\{\alpha_1,\alpha_2\}$ is also linearly independent. Generalize to sets of k vectors.

3.3-5. Suppose $\{\alpha_1,\alpha_2,\alpha_3\}$ is linearly dependent. Show $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ is also linearly dependent for any α_4. Generalize to sets of k vectors.

3.3-6. If α_0 is a linear combination of $\{\alpha_1,\ldots,\alpha_k\}$, show that the set $\{\alpha_0,\alpha_1,\ldots,\alpha_k\}$ is linearly dependent.

3.3-7. Given the linearly dependent set $\{\alpha_1,\alpha_2,\ldots,\alpha_k\}$ which does not contain zero vector $\mathbf{0}$ and $k>1$. Suppose the linear relation is

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k = \mathbf{0},$$

where $a_i \in \mathbb{F}$ for all i. Show that at least two a's are nonzero.

3.3-8. Find a basis for each of the space spanned by the set in Exercise 3.3-1.

3.3-9. Let α_1, α_2 α_3 be linearly independent vectors. Suppose $\beta_1 = \alpha_1+\alpha_2+\alpha_3$, $\beta_2 = \alpha_1 + a\alpha_2$, $\beta_3 = \alpha_1 + b\alpha_3$. Find condition that must be satisfied by $a,b \in \mathbb{R}$ in order that β_1, β_2 and β_3 are linearly independent.

3.3-10. Give an example of two vector spaces V and W of $\mathbb{R}^2$, such that $\dim(V) = \dim(W)$ but $V \neq W$.

3.3-11. Suppose $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ is a basis for $\mathbb{F}^n$ and A is invertible. Show that $\{A\alpha_1, A\alpha_2,\ldots,A\alpha_n\}$ is also a basis for $\mathbb{F}^n$. [Hint: Consider the product AX, where $X = \begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix}$.]

3.3-12. Let V and W be vector spaces of $\mathbb{F}^n$ and let $U = V + W$. Show that $\dim(U) \geq \dim(V)$. Similarly $\dim(U) \geq \dim(W)$.

3.3-13. If V is a vector space of $\mathbb{F}^n$ and $\dim(V) = n$, show that $V = \mathbb{F}^n$.

3.3-14. Show that a minimal (with respect to set inclusion) spanning set is a basis.

3.4 Subspace

Sometimes, we want to compare two vector spaces that they have inclusion relation. For this matter, we make the following definition.

Definition 3.4.1 Let W and V be two vector spaces of $\mathbb{F}^n$. If $W \subseteq V$, then we say that W is a *subspace* of V.

Note that V is always a subspace of itself. Vector space of $\mathbb{F}^n$ is always a subspace of $\mathbb{F}^n$.

Example 3.4.2 $\{\mathbf{0}_n\}$ is always a subspace of any vector space of $\mathbb{F}^n$. The vector space V described in Example 3.2.9 is a subspace of $\mathbb{R}^3$. □

We have an obvious lemma below.

Lemma 3.4.3 *Let W be a subspace of V. If $\alpha_1, \ldots, \alpha_s$ are linearly independent vectors in W, then they do so in V.*

Theorem 3.4.4 *Suppose W is a subspace of V. Then* $\dim W \leq \dim V$. *The equality holds if and only if $W = V$.*

Proof: Let $\dim W = s$ and let $\mathscr{B}$ be a basis of W. By Lemma 3.4.3 $\mathscr{B}$ is linearly independent in V. Since a basis of V is a maximal linearly independent set, $s \leq \dim V$.

If $s = \dim V$, then by Corollary 3.3.17 $\mathscr{B}$ is a basis of V. Then $W = \text{span}(\mathscr{B}) = V$. The converse is trivial. □

Remark 3.4.5 The condition $W \subseteq V$ is crucial. For taking $V = \text{span}\{(1,0)\}$ and $W = \text{span}\{(0,1)\}$, it is easy to see that $W \neq V$ yet $\dim W = \dim V = 1$.

3.5 Row Spaces and Column Spaces of Matrices

Definition 3.5.1 Let $A \in M_{m,n}(\mathbb{F})$. The *row space of A* is the vector space of $\mathbb{F}^n$ spanned by the rows of A and is denoted by $R(A)$. The *column space of A* is the vector space of $\mathbb{F}^m$ spanned by the columns of A and is denoted by $C(A)$. The dimension of $R(A)$ is called the *row rank of A* and is denoted by $\text{rowrank}(A)$. The dimension of $C(A)$ is called the *column rank of A* and is denoted by $\text{colrank}(A)$.

Remark 3.5.2 If $A \in M_{m,n}(\mathbb{F})$, then $R(A)$ is a subspace of $\mathbb{F}^n$ and $C(A)$ is a subspace of $\mathbb{F}^m$. $R(A) = C(A^T)$ and $C(A) = R(A^T)$.

Lemma 3.5.3 *Let $\{\alpha_1, \ldots, \alpha_s\}$ and $\{\beta_1, \ldots, \beta_t\}$ be two subsets of a vector space V of $\mathbb{F}^n$. If each β_j is a linear combination of $\{\alpha_1, \ldots, \alpha_s\}$, $1 \leq j \leq t$, then* $\text{span}\{\beta_1, \ldots, \beta_t\} \subseteq \text{span}\{\alpha_1, \ldots, \alpha_s\}$.

Proof: Let $\beta_j = \sum_{i=1}^{s} c_{ij}\alpha_i$. For each $\alpha \in \text{span}\{\beta_1, \ldots, \beta_t\}$,

$$\alpha = \sum_{j=1}^{t} a_j\beta_j = \sum_{j=1}^{t} a_j \sum_{i=1}^{s} c_{ij}\alpha_i = \sum_{i=1}^{s} \left(\sum_{j=1}^{t} c_{ij}a_j \right) \alpha_i.$$

Then $\alpha \in \text{span}\{\alpha_1, \ldots, \alpha_s\}$. □

Theorem 3.5.4 *If A and B are two row equivalent matrices, then $R(A) = R(B)$.*

Proof: Since B is row equivalent to A, there exist elementary matrices $E_1, \ldots, E_k$ such that $E_k E_{k-1} \cdots E_1 A = B$. Since elementary matrix of type 3 can be expressed as a product of elementary matrices of types 1 and 2, it suffices to show that $R(EA) = R(A)$ for any elementary matrix E of type 1 or 2.

Suppose E is an elementary matrix of type 1. Then

$$R(EA) = \text{span}\{A_{1*}, \ldots, bA_{i*}, \ldots, A_{m*}\},$$

for some $b \neq 0$. By Lemma 3.5.3, $R(EA) \subseteq R(A)$. Conversely, since $A_{i*} = b^{-1}(bA_{i*})$. So $R(A) \subseteq R(EA)$. Therefore, $R(EA) = R(A)$.

Suppose E is an elementary matrix of type 2. Then

$$R(EA) = \text{span}\{A_{1*}, \ldots, A_{i*}, \ldots, bA_{i*} + A_{j*}, \ldots, A_{m*}\},$$

for some $b \neq 0$. By Lemma 3.5.3, $R(EA) \subseteq R(A)$. Conversely, since $A_{j*} = (-b)A_{i*} + (bA_{i*} + A_{j*})$, by Lemma 3.5.3 again $R(A) \subseteq R(EA)$. Therefore, $R(EA) = R(A)$. □

Corollary 3.5.5 *The set of non-zero rows of* $\text{rref}(A)$ *is a basis for* $R(A)$. *Hence* $\text{rowrank}(A) = \text{rank}(A)$.

Proof: Since $R(A) = R(\text{rref}(A))$ and non-zero rows of $\text{rref}(A)$ are linearly independent (see Example 3.3.20), they form a basis of $R(\text{rref}(A)) = R(A)$. □

Remark 3.5.6 Since $\text{rref}(A)$ is unique, this basis described in the above corollary is unique. Such basis is called the *canonical basis* (or *standard basis*) of $R(A)$. To find a basis for $C(A)$, one can consider A^T and find the canonical basis for $R(A^T)$. This basis is called the *canonical basis* (or *standard basis*) of $C(A)$.

Example 3.5.7 Find the canonical basis of $C(A)$, where

$$A = \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 2 & -1 \\ 1 & 1 & 1 & 0 \\ -1 & 1 & 1 & 2 \\ -2 & 3 & 2 & 7 \end{pmatrix} \text{ over } \mathbb{R}.$$

Solution: Since

$$A^T = \begin{pmatrix} 1 & 0 & 1 & -1 & -2 \\ 0 & 1 & 1 & 1 & 3 \\ -1 & 2 & 1 & 1 & 2 \\ 1 & -1 & 0 & 2 & 7 \end{pmatrix} \xrightarrow[-\mathcal{R}_1+\mathcal{R}_4]{\mathcal{R}_1+\mathcal{R}_3} \begin{pmatrix} 1 & 0 & 1 & -1 & -2 \\ 0 & 1 & 1 & 1 & 3 \\ 0 & 2 & 2 & 0 & 0 \\ 0 & -1 & -1 & 3 & 9 \end{pmatrix}$$

$$\xrightarrow{\mathcal{R}_2 \leftrightarrow \mathcal{R}_3} \begin{pmatrix} 1 & 0 & 1 & -1 & -2 \\ 0 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 1 & 3 \\ 0 & -1 & -1 & 3 & 9 \end{pmatrix} \xrightarrow{\frac{1}{2}\mathcal{R}_2} \begin{pmatrix} 1 & 0 & 1 & -1 & -2 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 3 \\ 0 & -1 & -1 & 3 & 9 \end{pmatrix}$$

$$\xrightarrow[\mathcal{R}_2+\mathcal{R}_4]{-\mathcal{R}_2+\mathcal{R}_3} \begin{pmatrix} 1 & 0 & 1 & -1 & -2 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 3 & 9 \end{pmatrix} \xrightarrow{-3\mathcal{R}_3+\mathcal{R}_4} \begin{pmatrix} 1 & 0 & 1 & -1 & -2 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\mathcal{R}_3+\mathcal{R}_1} \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, the canonical basis of $C(A)$ is $\{(1\,0\,1\,0\,1)^T,\ (0\,1\,1\,0\,0)^T,\ (0\,0\,0\,1\,3)^T\}$. □

Corollary 3.5.8 $\text{colrank}(A) = \text{rank}(A) = \text{rowrank}(A)$.

Proof: $\text{colrank}(A) = \text{rowrank}(A^T) = \text{rank}(A^T) = \text{rank}(A) = \text{rowrank}(A)$. □

Remark 3.5.9 A and B are row equivalent do not imply $C(A) = C(B)$. For example, take $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Then A is row equivalent to $B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. $C(A) = \text{span}\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\}$ while $C(B) = \text{span}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\}$. These two vector spaces are different.

Corollary 3.5.10 *If A and B are row equivalent, then* $\text{colrank}(A) = \text{colrank}(B)$.

Proof: This follows from Theorem 3.5.4 and Corollary 3.5.8. □

Exercise 3.5

3.5-1. Find the canonical basis of $R(A)$, where A is described in Example 3.5.7.

3.5-2. Find the canonical bases of $R(A)$ and $C(A)$ respectively, where

$$A = \begin{pmatrix} 2 & 1 & 1 & -3 & 0 & 6 \\ -1 & 2 & 2 & 0 & -4 & 0 \\ 1 & 0 & 0 & -2 & 0 & 2 \\ 1 & 1 & 1 & -1 & 0 & 1 \end{pmatrix}.$$

3.5-3. Suppose A and B are two $m \times n$ matrices. Show that $\text{rank}(A + B) \leq \text{rank}(A) + \text{rank}(B)$.

3.6 Finding Bases

In this section, we shall provide some methods to find bases of some particular vector spaces.

Finding Maximal Linearly Independent Subset from a Given Set

Given a finite set of vectors S. Let $W = \text{span}(S)$. From Corollary 3.5.5 or Remark 3.5.6, it is easy to find a basis for W. But if we are required to find a basis of W from S, then it seems slightly more difficult. This problem is equivalent to find a maximal linearly independent subset from S. To solve this problem, we need the following lemma.

Lemma 3.6.1 *The set of leading columns of A is a basis for $C(A)$.*

Proof: Let $\text{rank}(A) = r$ and $H = \text{rref}(A)$. There is an invertible matrix P such that $PA = H$. Let $\alpha_1, \ldots, \alpha_r$ be the leading columns of H. Then $P^{-1}\alpha_1, \ldots, P^{-1}\alpha_r$ will be the leading columns of A. Since $P^{-1}(\alpha_1 \ \cdots \ \alpha_r)$ and $(\alpha_1 \ \cdots \ \alpha_r)$ have the same rank r, $P^{-1}\alpha_1, \ldots, P^{-1}\alpha_r$ are linearly independent. Let $W = \text{span}\{P^{-1}\alpha_1, \ldots, P^{-1}\alpha_r\}$. By definition $W \subseteq C(A)$. Since $\dim W = r = \text{rank}(A) = \dim C(A)$, $W = C(A)$. □

Remark 3.6.2 Row operations preserve linear relation among column vectors of a matrix A. Suppose $A = (A_{*1} \ \cdots \ A_{*n})$. Let $\sum_{i=1}^{n} a_i A_{*i}$ be a linear combination of A_{*i}'s, where $a_i \in \mathbb{F}$. Let P be any invertible matrix (which is a product of elementary matrices). Then

$$\mathbf{0}_m = \sum_{i=1}^{n} a_i A_{*i} \quad \Longleftrightarrow \quad \mathbf{0}_m = P(\sum_{i=1}^{n} a_i A_{*i}) = \sum_{i=1}^{n} a_i (PA_{*i}).$$

So in particular if P is such that $PA = \text{rref}(A)$, then PA_{*i} is the i-th column of $\text{rref}(A)$. So their linear relation can be easily inspected.

Remark 3.6.3 Let A be a given matrix. Suppose $\text{rref}(A)$ is of the form as (1.1). From that matrix, we have the following observations.

(a) The non-zero rows of $\text{rref}(A)$ form the standard basis of $R(A)$.

(b) By Remark 3.6.2 the linear relations among the columns of A can be easily seen from $\text{rref}(A)$.

From the above remarks and lemma, we can find a basis of $\text{span}(S)$ from S. Moreover, we can express the other vectors of S as a linear combination of the found basis (see Example 3.6.4).

To implement we are given a set S of vectors $\alpha_1, \ldots, \alpha_k$ in $\mathbb{F}^n$. To find the maximum number linearly independent vectors from S, we can simply put each vector in a row and form a $k \times n$ matrix and then perform elementary row operations to get rref. However, we are not sure which are linear dependent just from the rref. We get a basis of the $\text{span}(S)$ only. To find a linear relation (if they are linearly dependent), we better use these k vectors as columns vectors to form an $n \times k$ matrix $(\alpha_1 \ \cdots \ \alpha_k)$ and perform elementary row operations to get rref. In this way, we shall be able to tell which of the vectors are linearly independent (i.e., leading columns) and those dependent vectors and the linear relation.

We outline the above discussion as the following algorithm:

The Casting-out Method

Find a maximal linearly independent subset from a set of nonzero vectors $\{\alpha_1, \ldots, \alpha_k\}$.

Step 1: Form the matrix A with α_i as its i-th column vector.

Step 2: Find $\text{rref}(A)$.

Step 3: The set of all leading columns of A is the required subset. That is, cast out all the columns from the set that are not leading columns.

Example 3.6.4 Suppose $S = \{\alpha_1 = (1, 0, -1, 1), \ \alpha_2 = (0, 1, 2, -1), \ \alpha_3 = (1, 1, 1, 0), \ \alpha_4 = (-1, 1, 1, 2), \ \alpha_5 = (-2, 3, 2, 7)\}$.

Let $A = \begin{pmatrix} \alpha_1^T & \alpha_2^T & \alpha_3^T & \alpha_4^T & \alpha_5^T \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & -1 & -2 \\ 0 & 1 & 1 & 1 & 3 \\ -1 & 2 & 1 & 1 & 2 \\ 1 & -1 & 0 & 2 & 7 \end{pmatrix}$, which is the same matrix in Example 3.5.7. From Example 3.5.7 we have $\text{rref}(A) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Thus $\{\alpha_1, \alpha_2, \alpha_4\}$ is a maximal linearly independent subset of S. Note that it is neither the standard basis of $C(A)$ nor that of $R(A)$.

Moreover, let $H = \text{rref}(A)$. Since $H_{*3} = H_{*1} + H_{*2}$ and $H_{*5} = H_{*1} + 3H_{*4}$, we have $\alpha_3 = \alpha_1 + \alpha_2$ and $\alpha_5 = \alpha_1 + 3\alpha_4$. □

Extending a Basis

Given a linearly independent set S of $\mathbb{F}^n$ (obviously $0 \leq |S| \leq n$). We shall provide a method to extend S to a basis of $\mathbb{F}^n$.

Theorem 3.6.5 *Any linearly independent set of vectors in* $\mathbb{F}^n$ *can be extended to a basis of* $\mathbb{F}^n$.

Proof: Let $S = \{\alpha_1, \ldots, \alpha_k\}$ be a linearly independent set of $\mathbb{F}^n$. Let $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ be the standard basis for $\mathbb{F}^n$. Consider the matrix $B = (A|I_n)$, where $A = \begin{pmatrix} \alpha_1 & \cdots & \alpha_k \end{pmatrix}$. Since S is linearly independent, $\text{rank}(A) = k$.

Clearly $C(B) = \mathbb{F}^n$ and hence $\text{rank}(B) = n$. Let $H = \text{rref}(B) = (A'|C)$. By Lemma 1.5.6 $A' = \text{rref}(A)$. Since $\text{rank}(A) = k$, all columns of A' are leading columns.

Let $C_{*i_1}, \ldots, C_{*i_{n-k}}$ be columns of C that are leading columns of H. By Lemma 3.6.1 $\{\alpha_1, \ldots, \alpha_k, \boldsymbol{e}_{i_1}, \ldots, \boldsymbol{e}_{i_{n-k}}\}$ is a basis for $\mathbb{F}^n$. □

Remark 3.6.6 In the proof of the above theorem, we can choose any basis of $\mathbb{F}^n$ instead of the standard basis.

Example 3.6.7 Let $\alpha_1 = (1, 0 - 1, 1)$ and $\alpha_2 = (0, 1, 2, -1)$. Find a basis for $\mathbb{R}^4$ including α_1 and α_2.

Consider

$$B = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ -1 & 2 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[-\mathcal{R}_1+\mathcal{R}_4]{\mathcal{R}_1+\mathcal{R}_3} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow[\mathcal{R}_2+\mathcal{R}_4]{-2\mathcal{R}_2+\mathcal{R}_3} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 1 \end{pmatrix} \xrightarrow{\mathcal{R}_3+\mathcal{R}_4} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 1 \end{pmatrix}.$$

Although the last matrix is not in rref, we can see that the first 4 columns of B are leading columns. So $\{\alpha_1, \alpha_2, \boldsymbol{e}_1, \boldsymbol{e}_2\}$ is a basis for $\mathbb{R}^4$. □

Finding Basis for Null Space

Let $A \in M_{m,n}(\mathbb{F})$. The solution set of the linear system $AX = \mathbf{0}_m$, which is a subspace, is called the *null space* of A or the null space of the linear system and is denoted by $\text{null}(A)$. That is, $\text{null}(A) = \{\alpha \in \mathbb{F}^n \mid A\alpha = \mathbf{0}_m\}$. The dimension of $\text{null}(A)$ is called the *nullity* of A, written $\text{nullity}(A)$.

By Theorem 2.2.3 $\text{null}(A) = \text{null}(H)$, where $H = \text{rref}(A)$. Suppose $r = \text{rank}(A)$. After rearranging the unknowns (in practice, the rearrangement is not necessary), we have Equation (2.4). For $1 \leq i \leq n - r$, by setting $u_i = 1$ and $u_j = 0$ for $j \neq i$, we determine $y_1, \ldots, y_r$ and obtain a solution $\alpha_i = (x_1 \ \cdots \ x_n)^T$. It is clear that $\{\alpha_1, \ldots, \alpha_{n-r}\}$ is linearly independent. Thus we have the following lemma.

Lemma 3.6.8 *Let* $A \in M_{m,n}(\mathbb{F})$ *and* $\text{rank}(A) = r$. *Then* $AX = \mathbf{0}$ *has* $n - r$ *linearly independent solutions. Thus* $\text{nullity}(A) \geq n - r$.

Theorem 3.6.9 *Let* $A \in M_{m,n}(\mathbb{F})$ *and* $\text{rank}(A) = r$. *Then* $\text{nullity}(A) = n - r$ *or equivalently* $\text{rank}(A) + \text{nullity}(A) = n$.

Proof: Let $k = \text{nullity}(A)$ and $\{\alpha_1, \ldots, \alpha_k\}$ be a basis for null(A). By Theorem 3.6.5 there are $\beta_1, \ldots, \beta_{n-k}$ such that $\{\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_{n-k}\}$ is a basis of $\mathbb{F}^n$.

Let $Q = \begin{pmatrix} \alpha_1 & \cdots & \alpha_k & \beta_1 & \cdots & \beta_{n-k} \end{pmatrix}$. Then

$$AQ = \begin{pmatrix} \mathbf{0} & \cdots & \mathbf{0} & A\beta_1 & \cdots & A\beta_{n-k} \end{pmatrix}.$$

Since columns of Q are linearly independent, Q is invertible. By Theorem 2.4.11 we have rank$(AQ) =$ rank$(A) = r$. Thus AQ has at least r non-zero columns. However, AQ has at most $n-k$ non-zero columns. Hence $r \leq n-k$ or equivalently $k \leq n-r$. By Lemma 3.6.8, we have $k = n-r$. □

Example 3.6.10 Consider the homogeneous linear system

$$\begin{cases} x_1 - 2x_2 + 2x_3 - x_4 = 0 \\ -3x_1 + 6x_2 + x_3 + 10x_4 = 0 \\ x_1 - 2x_2 - 4x_3 - 7x_4 = 0 \end{cases}$$

over $\mathbb{R}$. The coefficient matrix of the system is

$$A = \begin{pmatrix} 1 & -2 & 2 & -1 \\ -3 & 6 & 1 & 10 \\ 1 & -2 & -4 & -7 \end{pmatrix}.$$

Then

$$\text{rref}(A) = \begin{pmatrix} 1 & -2 & 0 & -3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then we have

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

So a basis for null(A) is $\{(2 \ 1 \ 0 \ 0)^T, (3 \ 0 \ -1 \ 1)^T\}$ (or we can write it as $\{(2,1,0,0), (3,0,-1,1)\}$). □

Other Method on Finding Basis for Null Space

Alternative proof of Lemma 3.6.8: Since rank$(A) =$ rank$(A^T) = r$, there exists an invertible matrix P such that $PA^T = H = \text{rref}(A^T)$. Write $H = \begin{pmatrix} H_1 \\ \hline O_{n-r,m} \end{pmatrix}$, where $H_1 \in M_{r,m}(\mathbb{F})$ and has no zero rows. Now we partition P as $\begin{pmatrix} P_1 \\ \hline P_2 \end{pmatrix}$, where $P_1 \in M_{r,n}(\mathbb{F})$ and $P_2 \in M_{n-r,n}(\mathbb{F})$.

Consider $P(A^T|I_n) = (PA^T|P) = \left(\begin{array}{c|c} H_1 & P_1 \\ \hline O_{n-r,m} & P_2 \end{array}\right)$. Also

$$P(A^T|I_n) = \begin{pmatrix} P_1 \\ \hline P_2 \end{pmatrix}(A^T|I_n) = \left(\begin{array}{c|c} P_1A^T & P_1 \\ \hline P_2A^T & P_2 \end{array}\right).$$

So we have $P_2A^T = O_{n-r,m}$ or equivalently $AP_2^T = O_{m,n-r}$. Let $P_2 = \begin{pmatrix} P_{r+1\,*} \\ \vdots \\ P_{n\,*} \end{pmatrix}$. Then $P_2^T = \begin{pmatrix} P_{r+1\,*}^T & \cdots & P_{n\,*}^T \end{pmatrix}$ and hence $AP_{j*}^T = \mathbf{0}_m$ for $r+1 \leq j \leq n$.

$P_{r+1\,*}^T, \ldots, P_{n\,*}^T$ are the last $n-r$ columns of P^T. Since P^T is invertible, these columns are linearly independent. Hence nullity$(A) \geq n-r$. □

Remark 3.6.11 In the above proof, we do not really require that H_1 is in rref. We only need that $\text{rank}(H_1) = r$.

By the above discussions, we can find a basis of $\text{null}(A)$, the standard basis of $R(A^T) = C(A)$ and a basis of $C(A^T) = R(A)$ for a given matrix A. Moreover, that basis of $R(A)$ is chosen from the rows of A.

Example 3.6.12 Consider Example 3.6.10 again.

$$(A^T \mid I_4) = \left(\begin{array}{rrr|cccc} 1 & -3 & 1 & 1 & 0 & 0 & 0 \\ -2 & 6 & -2 & 0 & 1 & 0 & 0 \\ 2 & 1 & -4 & 0 & 0 & 1 & 0 \\ -1 & 10 & -7 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[\substack{-2\mathcal{R}_1+\mathcal{R}_3 \\ \mathcal{R}_1+\mathcal{R}_4}]{2\mathcal{R}_1+\mathcal{R}_2} \left(\begin{array}{rrr|cccc} 1 & -3 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 7 & -6 & -2 & 0 & 1 & 0 \\ 0 & 7 & -6 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow[\mathcal{R}_3 \leftrightarrow \mathcal{R}_2]{-\mathcal{R}_3+\mathcal{R}_4} \left(\begin{array}{rrr|cccc} 1 & -3 & 1 & 1 & 0 & 0 & 0 \\ 0 & 7 & -6 & -2 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & -1 & 1 \end{array}\right)$$

Thus $\text{null}(A) = \text{span}\{(2, 1, 0, 0), (3, 0, -1, 1)\}$. □

Example 3.6.13 Let $A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 0 & 2 & 2 \\ 0 & 1 & 1 & 3 \\ -1 & 1 & 0 & 2 \\ -2 & -1 & 1 & 1 \end{pmatrix}$. Then

$$(A^T \mid I_4) = \left(\begin{array}{rrrrr|cccc} 1 & 2 & 0 & -1 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 & 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 2 & 3 & 2 & 1 & 0 & 0 & 0 & 1 \end{array}\right).$$

After performing some elementary row operations we have

$$(A^T \mid I_4) \to (\text{rref}(A^T)|P) = \left(\begin{array}{rrrrr|cccc} 1 & 2 & 0 & -1 & 0 & 0 & 1 & 2 & -1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & -\frac{1}{2} & \frac{1}{2} \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 3 & -3 & 2 \end{array}\right).$$

Hence $\text{null}(A) = \text{span}\left\{\begin{pmatrix} 1 \\ 3 \\ -3 \\ 2 \end{pmatrix}\right\}$, $C(A) = \text{span}\left\{\begin{pmatrix} 1 \\ 2 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right\}$ and by casting-out method $C(A^T) = R(A) = \text{span}\{(1, 0, 1, 1), (0, 1, 1, 3), (-2, -1, 1, 1)\}$. □

Now we know how to find the basis of $\text{null}(A)$ for a given a matrix A. Conversely, given a set of vectors $S = \{\alpha_1, \ldots, \alpha_k\}$ in $\mathbb{F}^n$. Can we find a matrix $N \in M_{m,n}(\mathbb{F})$ for some m such that $\text{null}(N) = \text{span}(S)$?

To solve this problem, we first let $C = (\alpha_1 \ \cdots \ \alpha_k)$. If N is a required matrix, then NC is a zero matrix, i.e., $C^T N^T = O$. If we set $A^T = C$ in the alternative proof of Lemma 3.6.8, then applying Guassian elimination on $(C|I_n)$ we have $C^T P_2^T = O$. Then P_2 is a required matrix.

Example 3.6.14 Find a matrix A such that null(A) is spanned by

$$\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix}, \quad \begin{pmatrix}0\\-1\\0\\1\\1\end{pmatrix}, \quad \begin{pmatrix}-1\\1\\-1\\1\\-1\end{pmatrix}.$$

Consider the augmented matrix

$$\left(\begin{array}{ccc|ccccc} 1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

After performing some elementary row operations, it can be changed to row echelon form (not necessary reduced)

$$\left(\begin{array}{ccc|ccccc} 1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 0 & 0 & -2 & 1 & 4 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 1 & 0 & 1 \end{array}\right).$$

Then $A = \begin{pmatrix} -2 & 1 & 4 & 1 & 0 \\ -1 & 1 & 1 & 0 & 1 \end{pmatrix}$. □

Exercise 3.6

3.6-1. Find a maximal linearly independent subset $\mathscr{B}$ from

$$\{(1,1,1,3),\ (1,-2,4,0),\ (2,0,5,3),\ (3,4,6,-1)\ (0,3,2,-2),\ (1,3,5,7)\}.$$

Express the casted out vectors into the linear combination of vectors in $\mathscr{B}$.

3.6-2. Let $V = \text{span}\{(1,1,-1,2),\ (2,3,-4,2)\ (5,3,-3,3)\}$. Find a system $AX = \mathbf{0}$ of two equations in 4 unknowns so that V is the solution space.

3.6-3. Extend $\{(1,1,0),\ (-1,2,1)\}$ to a basis of $\mathbb{R}^3$.

3.6-4. Extend $\{(1,1,0,1),\ (-1,0,1,1)\}$ to a basis of $\mathbb{R}^4$.

3.6-5. Extend $\{(1,-2,0,1)\}$ to a basis of $\mathbb{R}^4$ by choosing vectors from

$$\{(1,0,0,1),\ (1,-2,1,1)\ (1,-1,0,1),\ (0,1,1,1)\}.$$

3.7 General Solution of Linear Systems

Now it is the time to consider how to find all the solutions of $AX = \boldsymbol{b}$.

Theorem 3.7.1 *Let $A \in M_{m,n}(\mathbb{F})$. Suppose $AX = \boldsymbol{b}$ has a solution β_p. Then any solution β of the system is of the form $\alpha + \beta_p$, where $\alpha \in \text{null}(A)$. That is,*

$$\{\beta \mid A\beta = \boldsymbol{b}\} = \{\alpha + \beta_p \mid A\alpha = \boldsymbol{0}\}.$$

Proof: Let $S = \{\beta \mid A\beta = \boldsymbol{b}\}$ and $T = \{\alpha + \beta_p \mid A\alpha = \boldsymbol{0}\}$. For each $\beta \in S$, $A(\beta - \beta_p) = \boldsymbol{b} - \boldsymbol{b} = \boldsymbol{0}$. Then $\beta \in T$, i.e., $S \subseteq T$.

Conversely, $\forall \alpha + \beta_p \in T$, $A(\alpha + \beta_p) = \boldsymbol{0} + \boldsymbol{b} = \boldsymbol{b}$. Then $\alpha + \beta_p \in S$, i.e., $S \supseteq T$. Hence $S = T$. □

Note that, β_p is called a *particular solution* of the system.

Recall that the system $AX = \boldsymbol{b}$ is consistent if and only if $\text{rank}(A) = \text{rank}(A|\boldsymbol{b})$.

Suppose $AX = \boldsymbol{b}$ is consistent, then after applying Guassian elimination on $(A|\boldsymbol{b})$ and rearranging the unknowns (in practice, the rearrangement is not necessary), we have Equation (2.5). If we set all the free variables to be 0, then we have $y_i = c_i$ for all $1 \leq i \leq r$. Then we obtain a particular solution β_p. Suppose $\{\alpha_1, \ldots, \alpha_{n-r}\}$ is the basis of $\text{null}(A)$. Then

$$\beta = \beta_p + \sum_{i=1}^{n-r} a_i \alpha_i$$

is a solution of the linear system $AX = \boldsymbol{b}$ for some $a_i \in \mathbb{F}$. It is called a *general solution* of the linear system.

Corollary 3.7.2 *Suppose the system $AX = \boldsymbol{b}$ is consistent. Then the solution is unique if and only if $AX = \boldsymbol{0}$ has unique solution.*

Example 3.7.3 Consider the linear system

$$\begin{cases} x_1 - 2x_2 + 2x_3 - x_4 = 2 \\ -3x_1 + 6x_2 + x_3 + 10x_4 = -13 \\ x_1 - 2x_2 - 4x_3 - 7x_4 = 8 \end{cases}$$

over $\mathbb{R}$.

After performing elementary row operations on the augmented matrix

$$\left(\begin{array}{cccc|c} 1 & -2 & 2 & -1 & 2 \\ -3 & 6 & 1 & 10 & -13 \\ 1 & -2 & -4 & -7 & 8 \end{array}\right),$$

we have the rref

$$\left(\begin{array}{cccc|c} 1 & -2 & 0 & -3 & 4 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

This means

$$\begin{cases} x_1 - 2x_2 - 3x_4 = 4 \\ x_3 + x_4 = -1 \end{cases}$$

We let the free variables x_2 and x_4 to be zero. So we have $x_1 = 4$, $x_2 = 0$, $x_3 = -1$ and $x_4 = 0$. That is, $\beta_p = (4, 0, -1, 0)$. The homogeneous part of this system was considered in Example 3.6.10. Since a basis for the null space of the system is $\{(2, 1, 0, 0),\ (3, 0, -1, 1)\}$. So the general solution of the system is

$$\{a(2, 1, 0, 0) + b(3, 0, -1, 1) + (4, 0, -1, 0) \mid a, b \in \mathbb{R}\}.$$ □

Definition 3.7.4 Suppose $A \in M_{m,n}(\mathbb{F})$. If $\text{colrank}(A) = n$, i.e., $\text{rank}(A) = n$, then we say that A has *full column rank*.

Corollary 3.7.5 *Suppose the system $AX = \boldsymbol{b}$ is consistent. The system has a unique solution if and only if A has full column rank if and only if* $\text{nullity}(A) = 0$.

Proof: The corollary follows from Theorems 2.4.9 and 3.6.9. □

Other Method on Finding General Solutions of Linear System

Theorem 3.7.6 *Suppose $A \in M_{m,n}(\mathbb{F})$. The system $AX = \boldsymbol{b}$ is consistent if and only if $\boldsymbol{b} \in C(A)$.*

Proof: The system $AX = \boldsymbol{b}$ is consistent
if and only if there exists $\alpha = (c_1, \ldots, c_n)$ such that $A\alpha^T = \begin{pmatrix} A_{*1} & \cdots & A_{*n} \end{pmatrix} \alpha^T = \boldsymbol{b}$
if and only if $\boldsymbol{b} = \sum_{i=1}^{n} c_i A_{*i}$
if and only if $\boldsymbol{b} \in \text{span}\{A_{*1}, \ldots, A_{*n}\}$. □

Now we would like to develop another method for finding the general solution of $AX = \boldsymbol{b}$, where $A \in M_{m,n}(\mathbb{F})$. When the system is consistent, there exists a solution $\boldsymbol{c}$ such that $A\boldsymbol{c} = \boldsymbol{b}$. It is equivalent to $\boldsymbol{c}^T A^T - \boldsymbol{b}^T = \mathbf{0}_m^T$. That is, $\boldsymbol{b}^T$ is a linear combination of the row vectors of A^T. Thus there exists a sequence of elementary row operations transforming $\left(\begin{array}{c} A^T \\ \hline -\boldsymbol{b}^T- \end{array}\right)$ to $\left(\begin{array}{c} A^T \\ \hline \mathbf{0}_m^T \end{array}\right)$. Also, there exists an invertible matrix P such that $PA^T = R$ is in rref. From this, we shall be able to find the general solutions of the linear system.

Indeed we have

$$\left(\begin{array}{c|c} P & \mathbf{0}_n \\ \hline \boldsymbol{c}^T & 1 \end{array}\right)\left(\begin{array}{c|c} A^T & I_n \\ \hline -\boldsymbol{b}^T- & \mathbf{0}_n^T \end{array}\right) = \left(\begin{array}{c|c} PA^T & P \\ \hline \boldsymbol{c}^T A^T - \boldsymbol{b}^T & \boldsymbol{c}^T \end{array}\right) = \left(\begin{array}{c|c} R & P \\ \hline \mathbf{0}_m^T & \boldsymbol{c}^T \end{array}\right) = \left(\begin{array}{c|c} R_1 & P_1 \\ \hline O & P_2 \\ \hline \mathbf{0}_m^T & \boldsymbol{c}^T \end{array}\right).$$

Hence we get a particular solution and the general solutions immediately.

Now, we form the $(n+1) \times (m+n)$ matrix $\left(\begin{array}{c|c} A^T & I_n \\ \hline -\boldsymbol{b}^T- & \mathbf{0}_n^T \end{array}\right)$ and perform elementary row operations to get the form

$$\left(\begin{array}{c|c} R_1 & P_1 \\ \hline O & P_2 \\ \hline \mathbf{0}_m^T & \boldsymbol{c}^T \end{array}\right).$$

Then we can read from this matrix that columns of P_2^T (i.e., rows of P_2) constitute a basis for the null space of A and $\boldsymbol{c}$ a particular solution of $AX = \boldsymbol{b}$.

Note that if $AX = \boldsymbol{b}$ is not consistent, we would not be able to find $\boldsymbol{c}$ and hence there is no way we can transform the last row to $(\mathbf{0}_m^T \mid \boldsymbol{c}^T)$.

Warning: We do not want to interchange the last row that has $-\boldsymbol{b}^T$ with any other rows. Nor do we want to multiply this row by any scalar.

Example 3.7.7 Consider Example 3.7.3 again. Let A be the coefficient matrix of the system. Then

$$\left(\begin{array}{c|c} A^T & I_4 \\ \hline -2 \quad 13 \quad -8 & \mathbf{0}_4^T \end{array}\right) \text{ is row equivalent to } \left(\begin{array}{ccc|ccccc} 1 & -3 & 1 & 1 & 0 & 0 & 0 \\ 0 & 7 & -6 & -2 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & -1 & 1 \\ \hline 0 & 0 & 0 & 4 & 0 & -1 & 0 \end{array}\right).$$

So $\boldsymbol{c} = (4\ 0\ -1\ 0)^T$ and the general solution is

$$a(2,1,0,0) + b(3,0,-1,1) + (4,0,-1,0),$$

where $a, b \in \mathbb{R}$. □

Example 3.7.8 Let A be the same matrix as in Example 3.7.7. Consider the linear system $AX = (2,3,8)^T$. Then

$$\left(\begin{array}{c|c} A^T & I_4 \\ \hline -2 \quad -3 \quad -8 & \mathbf{0}_4^T \end{array}\right) \text{ is row equivalent to } \left(\begin{array}{ccc|ccccc} 1 & -3 & 1 & 1 & 0 & 0 & 0 \\ 0 & 7 & -6 & -2 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & -1 & 1 \\ \hline 0 & -9 & -6 & 2 & 0 & 0 & 0 \end{array}\right).$$

It is clear that $(0,-9,-6)$ is not a linear combination of $(1,-3,1)$ and $(0,7,-6)$. So $(-2,-3,-8)$ is not in $R(A^T)$. Therefore, the system is inconsistent. □

Example 3.7.9 Let A be the same matrix as in Example 3.7.7. Find those vectors $\beta = (a,b,c)$ for which the system $AX = \beta^T$ is consistent.

$\left(\begin{array}{c|c} A^T & I_4 \\ \hline -\beta & \mathbf{0}_4^T \end{array}\right)$ is row equivalent to

$$\left(\begin{array}{ccc|cccc} 1 & -3 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -\frac{6}{7} & -\frac{2}{7} & 0 & \frac{1}{7} & 0 \\ \hline 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & -1 & 1 \\ \hline 0 & 0 & -\frac{1}{7}(11a+6b+7c) & \frac{1}{7}(13a+2b) & 0 & \frac{1}{7}(3a+b) & 0 \end{array}\right).$$

In order for the system to be consistent, it is necessary and sufficient that $11a + 6b + 7c = 0$. □

Exercise 3.7

3.7-1. Solve the system of linear equations

$$\begin{cases} x_1 + 2x_2 - 2x_3 - x_4 = 3 \\ 2x_1 + 3x_2 - 5x_3 + x_4 - 7x_5 = 4 \\ x_2 + x_3 - x_4 + x_5 = 2 \\ -x_1 + x_2 + 5x_3 - x_4 = 3 \end{cases}$$

over $\mathbb{R}$.

3.7-2. Find the value of a for which the system

$$\begin{cases} x_1 - 2x_2 + x_3 - 3x_4 = a \\ 2x_1 + x_2 + x_3 - 2x_4 = 2 \\ 7x_1 - 4x_2 + 5x_3 - 13x_4 = -8 \end{cases}$$

has solutions over $\mathbb{Q}$ and find the solution.

3.7-3. A man has a pocket full of coins of 10 cents, 50 cents and one dollar. If he has a total of 14 coins that worth \$8.90, how many coins of each type does he have?

3.7-4. Three species of fish are introduced into a fish-pond. The fishes are fed three types of food. Let a_{ij} be the average consumption per day of the j-th type of food by a fish of the i-th species $(i, j = 1, 2, 3)$. Given $A = (a_{ij}) = \begin{pmatrix} 2 & 1 & 2 \\ 3 & 2 & 1 \\ 3 & 1 & 5 \end{pmatrix}$ and that the supplies are 6,650, 4,350 and 2,550 units of food type 1, 2, and 3, respectively. Assuming that all food is consumed, how many fishes of each species can coexist in the pond?

Chapter 4

Determinants

4.1 Permutations

Determinant is a very useful tool. By using determinant we can check whether a matrix is invertible or not, we can find the inverse of an invertible matrix of lower order, we can find the characteristic polynomial of a matrix, etc.

Before giving a definition of determinant we have to introduce the concept of permutations.

Definition 4.1.1 A *permutation* θ of a set S is a bijection of S onto itself. For $n \in \mathbb{N}$, if $S = \{1, 2, \ldots, n\}$, then the set of all permutations on S is denoted by $\mathcal{S}_n$. We shall use the notation

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \theta(1) & \theta(2) & \cdots & \theta(n) \end{pmatrix}$$

to denote the permutation θ. Note that $\mathcal{S}_n$ has $n!$ elements.

Example 4.1.2 Let $n = 4$. Suppose $\theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ and $\theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$. Then $\theta_1 \circ \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ and $\theta_2 \circ \theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$. Thus $\theta_1 \circ \theta_2 \neq \theta_2 \circ \theta_1$ in general. □

Definition 4.1.3 The permutation that leaves all the elements of S fixed is called the *identity permutation* and is denoted by ι, i.e., $\iota(i) = i \; \forall \; i \in S$.

Note that for any $\theta \in \mathcal{S}_n$, since θ is a bijection, the inverse θ^{-1} exists.

Definition 4.1.4 Given $\theta \in \mathcal{S}_n$. If there is a pair of integers i, j with $1 \leq i < j \leq n$ such that $\theta(i) > \theta(j)$, then we say that θ performs an *inversion*. Let $k(\theta)$ be the total number of inversions performed by θ. Let $\text{sgn}(\theta) = (-1)^{k(\theta)}$, which is called the *sign* of θ. If $\text{sgn}(\theta) = 1$, then θ is called an *even permutation*; if $\text{sgn}(\theta) = -1$, then θ is called an *odd permutation*.

Example 4.1.5 Let θ_1 and θ_2 be defined in Example 4.1.2. Then $\theta_1(1) > \theta_1(4)$, $\theta_1(2) > \theta_1(3)$, $\theta_1(2) > \theta_1(4)$ and $\theta_1(3) > \theta_1(4)$. Hence $k(\theta_1) = 4$. Similarly one can compute that $k(\theta_2) = 2$. Both permutations are even. □

Theorem 4.1.6 *Let* $\theta, \sigma \in \mathcal{S}_n$. *Then* $\text{sgn}(\sigma \circ \theta) = \text{sgn}(\sigma)\text{sgn}(\theta)$.

Proof: Note that σ can be represented in the form

$$\begin{pmatrix} \cdots & \theta(i) & \cdots & \theta(j) & \cdots \\ \cdots & \sigma\circ\theta(i) & \cdots & \sigma\circ\theta(j) & \cdots \end{pmatrix} \text{ or } \begin{pmatrix} \cdots & \theta(j) & \cdots & \theta(i) & \cdots \\ \cdots & \sigma\circ\theta(j) & \cdots & \sigma\circ\theta(i) & \cdots \end{pmatrix},$$

because every element of $\{1, 2, \ldots, n\}$ appears in the top row. For a given pair $i < j$, we let N_1 and N be respectively the numbers of inversions of θ and $\sigma\circ\theta$ involving i and j. If N_2 is the number of inversions of σ involving $\theta(i)$ and $\theta(j)$, then we have the following table:

θ	σ	N_1	N_2	N
$\theta(i) < \theta(j)$	$\sigma(\theta(i)) < \sigma(\theta(j))$	0	0	0
$\theta(i) < \theta(j)$	$\sigma(\theta(i)) > \sigma(\theta(j))$	0	1	1
$\theta(i) > \theta(j)$	$\sigma(\theta(i)) < \sigma(\theta(j))$	1	0	1
$\theta(i) > \theta(j)$	$\sigma(\theta(i)) > \sigma(\theta(j))$	1	1	0

From the above table, we see that for each pair $i < j$, $N - N_1 - N_2 \equiv 0 \pmod 2$. Hence, after adding all the possible inversions, we have $k(\sigma\circ\theta) - k(\theta) - k(\sigma) \equiv 0 \pmod 2$. Thus

$$\text{sgn}(\sigma\circ\theta) = (-1)^{k(\sigma\circ\theta)} = (-1)^{k(\sigma)+k(\theta)} = (-1)^{k(\sigma)}(-1)^{k(\theta)} = \text{sgn}(\sigma)\text{sgn}(\theta).$$

□

Corollary 4.1.7 *Let $\theta \in \mathcal{S}_n$. Then* $\text{sgn}(\theta) = \text{sgn}(\theta^{-1})$.

The following are some properties of $\mathcal{S}_n$.

Proposition 4.1.8 *Let $\sigma \in \mathcal{S}_n$ and let $\sigma\mathcal{S}_n = \{\sigma\circ\theta \mid \theta \in \mathcal{S}_n\}$. Then $\sigma\mathcal{S}_n = \mathcal{S}_n$.*

Proof: Since the product of permutations is still a permutation, $\sigma\mathcal{S}_n \subseteq \mathcal{S}_n$.

$\forall\theta \in \mathcal{S}_n$, $\sigma^{-1}\circ\theta \in \mathcal{S}_n$. Let $\theta_1 = \sigma^{-1}\circ\theta$. Then $\theta = \sigma\circ\theta_1 \in \sigma S_n$. So $\mathcal{S}_n \subseteq \sigma\mathcal{S}_n$. Therefore, $\sigma\mathcal{S}_n = \mathcal{S}_n$. □

Proposition 4.1.9 *Let $\mathcal{T} = \{\sigma^{-1} \mid \sigma \in \mathcal{S}_n\}$. Then $\mathcal{T} = \mathcal{S}_n$.*

Proof: Since $\sigma^{-1} \in \mathcal{T}$ is a permutation for $\sigma \in \mathcal{S}_n$, $\sigma^{-1} \in \mathcal{S}_n$. Then $\mathcal{T} \subseteq \mathcal{S}_n$.

$\forall\sigma \in \mathcal{S}_n$, we know that $\sigma^{-1} \in \mathcal{S}_n$. Then $\sigma = (\sigma^{-1})^{-1} \in \mathcal{T}$. Thus $\mathcal{S}_n \subseteq \mathcal{T}$. Therefore, $\mathcal{T} = \mathcal{S}_n$. □

Let $\mathcal{A}_n$ be the set of all even permutations of $\mathcal{S}_n$, i.e.,

$$\mathcal{A}_n = \{\sigma \in \mathcal{S}_n \mid \text{sgn}(\sigma) = 1\}.$$

Proposition 4.1.10 *For any fixed odd permutation $\sigma \in \mathcal{S}_n$, $\mathcal{S}_n = \mathcal{A}_n \cup \sigma\mathcal{A}_n$ and $\mathcal{A}_n \cap \sigma\mathcal{A}_n = \varnothing$, where $\sigma\mathcal{A}_n = \{\sigma\circ\theta \mid \theta \in \mathcal{A}_n\}$.*

Proof: It is clear that $\mathcal{A}_n \cup \sigma\mathcal{A}_n \subseteq \mathcal{S}_n$.

$\forall\theta \in \mathcal{S}_n$, θ is either even or odd permutation. So either $\theta \in \mathcal{A}_n$ or $\theta \notin \mathcal{A}_n$. For the case $\theta \notin \mathcal{A}_n$, $\text{sgn}(\sigma^{-1}\circ\theta) = \text{sgn}(\sigma^{-1})\text{sgn}(\theta) = \text{sgn}(\sigma)\text{sgn}(\theta) = 1$. So $\sigma^{-1}\circ\theta = \theta_1 \in \mathcal{A}_n$. Hence $\theta = \sigma\circ\theta_1 \in \sigma\mathcal{A}_n$. Therefore, we have $\mathcal{S}_n = \mathcal{A}_n \cup \sigma\mathcal{A}_n$.

Since elements in $\sigma\mathcal{A}_n$ are odd permutations, $\mathcal{A}_n \cap \sigma\mathcal{A}_n = \varnothing$. □

Exercise 4.1

4.1-1. Let θ be the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$. Find $\text{sgn}\theta$.

4.1-2. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 4 & 2 \end{pmatrix}$ and $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$ be permutations in S_6. Find $\theta\circ\sigma$ and $\sigma\circ\theta$.

4.2 Definition and Properties of Determinants

Determinants can be defined recurrently. In this book, we shall define determinants by the classical way.

Definition 4.2.1 The *determinant* of an $n \times n$ matrix A is defined to be the scalar

$$\det A = \sum_{\theta \in \mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}(A)_{2,\theta(2)} \cdots (A)_{n,\theta(n)}.$$

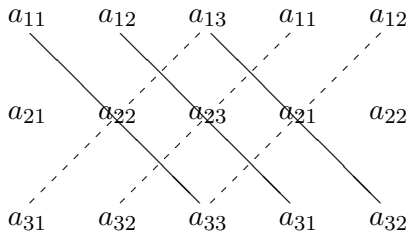
Each term in the sum is a product of n elements taken from each different row and different column of A and $\operatorname{sgn}(\theta)$. There are altogether $n!$ terms. Sometimes, we denote $\det A$ by $|A|$.

Suppose $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Then $\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$.

Suppose $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$. Then

$$\begin{aligned} \det A &= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \\ &= a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}. \end{aligned}$$

These six terms can also be obtained as follows. Repeat the first and the second columns of A. Form the sum of the products along the diagonal lines from left to right (the solid lines), and subtract from this number the products along the diagonal lines from right to left (the dash lines).



For $n \times n$ matrix A, $\det A$ has $n!$ terms. Thus $n \geq 4$, we do not have easy method to memorize all the terms.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$. It can be shown that the absolute value of $\det A$, i.e., $|\det A|$ is the area of the parallelogram determined by the vectors (a, b) and (c, d).

If A is a diagonal matrix, then by definition, it is easy to see that $\det A$ is the product of diagonal elements. In particular, $\det I = 1$.

Theorem 4.2.2 *Let $A \in M_n(\mathbb{F})$. Then $\det A^T = \det A$.*

Proof: Note that $(A^T)_{i,j} = (A)_{j,i}$. Suppose $\theta \in \mathcal{S}_n$, let $\theta(i) = i'$. Then $i = \theta^{-1}(i')$ and $(A^T)_{i,\theta(i)} = (A)_{\theta(i),i} = (A)_{i',\theta^{-1}(i')}$. Since θ varies in $\mathcal{S}_n$, so does θ^{-1} (see Proposition 4.1.9). Also $\operatorname{sgn}(\theta) = \operatorname{sgn}(\theta^{-1})$. Thus by definition,

$$\begin{aligned}\det A^T &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A^T)_{1,\theta(1)}(A^T)_{2,\theta(2)}\cdots(A^T)_{n,\theta(n)}\\ &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{\theta(1),1}(A)_{\theta(2),2}\cdots(A)_{\theta(n),n}\\ &= \sum_{\theta^{-1}\in\mathcal{S}_n} \operatorname{sgn}(\theta^{-1})(A)_{1',\theta^{-1}(1')}(A)_{2',\theta^{-1}(2')}\cdots(A)_{n',\theta^{-1}(n')}.\end{aligned}$$

Since θ is a permutation, some $i'_1 = 1, i'_2 = 2, \ldots$ etc.; also the multiplication in $\mathbb{F}$ is commutative, so after putting $\rho = \theta^{-1}$ we have

$$\det A^T = \sum_{\rho\in\mathcal{S}_n} \operatorname{sgn}(\rho)(A)_{1,\rho(1)}(A)_{2,\rho(2)}\cdots(A)_{n,\rho(n)} = \det A.$$

□

Theorem 4.2.3 *If B is the matrix obtained from A by multiplying a row (or a column) of A by a scalar c, then* $\det B = c\det A$.

Proof: Suppose $(B)_{k,j} = c(A)_{k,j}$ and $(B)_{i,j} = (A)_{i,j}$ if $i \neq k$. Then

$$\begin{aligned}\det B &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(B)_{1,\theta(1)}\cdots(B)_{k,\theta(k)}\cdots(B)_{n,\theta(n)}\\ &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}\cdots c(A)_{k,\theta(k)}\cdots(A)_{n,\theta(n)}\\ &= c\sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}\cdots(A)_{k,\theta(k)}\cdots(A)_{n,\theta(n)}\\ &= c\det A.\end{aligned}$$

□

Theorem 4.2.4 *If B is the matrix obtained from A by interchanging any two rows (or columns) of A, then* $\det B = -\det A$.

Proof: Suppose B is obtained from A by interchanging the i-th and the j-th rows of A, $i < j$. Then $B_{i*} = A_{j*}$, $B_{j*} = A_{i*}$ and $B_{r*} = A_{r*}$ if $r \neq i$ and $r \neq j$. Let ρ be the permutation that interchanges i with j and leaves others fixed. Then $\operatorname{sgn}(\rho) = -1$ and $\rho(i) = j$, $\rho(j) = i$, $\rho(r) = r$ for $r \neq i, j$. Now

$$\begin{aligned}\det B &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(B)_{1,\theta(1)}\cdots(B)_{i,\theta(i)}\cdots(B)_{j,\theta(j)}\cdots(B)_{n,\theta(n)}\\ &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}\cdots(A)_{j,\theta(i)}\cdots(A)_{i,\theta(j)}\cdots(A)_{n,\theta(n)}\\ &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta\circ\rho(1)}\cdots(A)_{j,\theta\circ\rho(j)}\cdots(A)_{i,\theta\circ\rho(i)}\cdots(A)_{n,\theta\circ\rho(n)}\\ &= \sum_{\theta\circ\rho\in\mathcal{S}_n} -\operatorname{sgn}(\theta\circ\rho)(A)_{1,\theta\circ\rho(1)}\cdots(A)_{i,\theta\circ\rho(i)}\cdots(A)_{j,\theta\circ\rho(j)}\cdots(A)_{n,\theta\circ\rho(n)}\\ &= -\det A,\end{aligned}$$

since $\theta\circ\rho$ runs over all the permutations in $\mathcal{S}_n$. □

Combining with Theorem 4.2.4 and Theorem 4.2.2 we have that if B is obtained from A by taking h interchanges of rows and k interchanges of columns then $\det B = (-1)^{h+k}\det A$.

Theorem 4.2.5 *If A has two identical rows (or columns), then* $\det A = 0$.

Proof: Since the matrix obtained from A by interchanging the two identical rows is still the same. Thus by Theorem 4.2.4, we have $\det A = -\det A$. Therefore $(1+1)\det A = 0$. If $1+1 \neq 0$, then $\det A = 0$.

If $1+1=0$, then $\operatorname{sgn}(\theta) = 1$ no matter whether θ is even or odd. Since there are two identical rows, so by the definition of $\det A$ in Definition 4.2.1, the terms in the summation can be grouped as a pair of equal terms. Since $1+1=0$. the sum of two equal terms is always 0. Thus $\det A = 0$. □

Theorem 4.2.6 *If B is the matrix obtained from A by adding a multiple of one row (or column) to another, then* $\det B = \det A$.

Proof: Let $B_{j*} = c(A_{i*}) + A_{j*}$, and $B_{r*} = A_{r*}$ if $r \neq j$, where $i \neq j$. Without loss of generality, we assume $i < j$. Then

$$\begin{aligned}
\det B &= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(B)_{1,\theta(1)}\cdots(B)_{i,\theta(i)}\cdots(B)_{j,\theta(j)}\cdots(B)_{n,\theta(n)} \\
&= \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}\cdots(A)_{i,\theta(i)}\cdots[c(A)_{i,\theta(j)} + (A)_{j,\theta(j)}]\cdots(A)_{n,\theta(n)} \\
&= c\sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}\cdots(A)_{i,\theta(i)}\cdots(A)_{i,\theta(j)}\cdots(A)_{n,\theta(n)} \\
&\quad + \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}\cdots(A)_{i,\theta(i)}\cdots(A)_{j,\theta(j)}\cdots(A)_{n,\theta(n)} \\
&= 0 + \sum_{\theta\in\mathcal{S}_n} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}\cdots(A)_{i,\theta(i)}\cdots(A)_{j,\theta(j)}\cdots(A)_{n,\theta(n)} \\
&= \det A.
\end{aligned}$$

The first sum vanishes because it is c times the determinant of a matrix with two identical rows.□

Theorem 4.2.7 *If E is an elementary matrix and A is a square matrix, then* $\det(EA) = \det E \det A = \det(AE)$.

Proof: Suppose E is the elementary matrix obtained by multiplying one row of I by a non-zero scalar c. Then by Theorem 4.2.3, we have $\det E = c$ and EA is the matrix obtained by multiplying the corresponding row by c. By Theorem 4.2.3 again, we have $\det(EA) = c\det A$. Thus $\det(EA) = \det E \det A$.

If E is obtained from I by interchanging two rows, then by Theorem 4.2.4 $\det E = -1$. Also by Theorem 4.2.4, we have $\det(EA) = -\det A = \det E \det A$.

Finally, if E is obtained by multiplying one row by a scalar and add to the other row, then $\det E = \det I = 1$ by Theorem 4.2.6. Also by Theorem 4.2.6 $\det(EA) = \det A$. Thus $\det(EA) = \det E \det A$.

Since E^T is an elementary matrix of the same type, by Theorem 4.2.2 we have $\det(AE) = \det(AE)^T = \det(E^T A^T) = \det E^T \det A^T = \det E \det A$. □

Theorem 4.2.8 *Let $A \in M_n(\mathbb{F})$. A is non-singular if and only if* $\det A \neq 0$.

Proof: Suppose A is non-singular. Then by Theorem 2.2.5, A is a product of elementary matrices, say $A = E_r \cdots E_1$. Then by Theorem 4.2.7 and induction, we have $\det A = \det E_r \cdots \det E_1$. From the proof of Theorem 4.2.7, we know that $\det E_i \neq 0$ for all i. Thus $\det A \neq 0$.

If A is singular, then $H = \text{rref}(A)$ has at least one zero row. Clearly, by the definition of determinant, $\det H = 0$. Let $H = E_r \cdots E_1 A$. By Theorem 4.2.7 and induction, $\det H = \det E_r \cdots \det E_1 \det A$. Since $\det E_i \neq 0$ for all i and $\det H = 0$, we have $\det A = 0$. □

Note that the 'if part' of the above theorem does not hold when $\mathbb{F}$ is not a field. For example, consider $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$. Then $\det A = 2 \neq 0$. But we cannot find a 2×2 matrix $B \in M_2(\mathbb{Z})$ such that $AB = BA = I_2$.

Theorem 4.2.9 *For $A, B \in M_n(\mathbb{F})$, $\det(AB) = \det A \det B = \det(BA)$.*

Proof: If A is non-singular, then $A = E_r \cdots E_1$ for some elementary matrices $E_1, \ldots, E_r$. Then by Theorem 4.2.7 and induction, we have

$$\det(AB) = \det(E_r \cdots E_1 B) = \det E_r \cdots \det E_1 \det B = \det(E_r \cdots E_1) \det B = \det A \det B.$$

If A is singular, then so is AB. By Theorem 4.2.8 $\det A = 0$ and $\det(AB) = 0$. Thus, in this case $\det(AB) = \det A \det B$.

Similarly, we have $\det(BA) = \det B \det A$. Since multiplication in $\mathbb{F}$ is commutative, we have $\det(AB) = \det A \det B = \det B \det A = \det(BA)$. □

Note that, the above theorem holds when $\mathbb{F} = \mathbb{Z}$. In general, the theorem holds when $\mathbb{F}$ is a commutative ring.

Exercise 4.2

4.2-1. Suppose $A = (a_{ij})$ is upper triangular. Compute $\det A$.

4.2-2. Suppose $A \in M_n(\mathbb{F})$ is invertible. Show that $\det(A^{-1}) = (\det A)^{-1}$.

4.2-3. Show that if A is a skew-symmetric $n \times n$ matrix, then $\det A^T = (-1)^n \det A$.

4.3 Cofactors

In order to evaluate the determinant of a square matrix, we shall expand the determinant into a linear combination of lower order determinants.

For a given pair i and j, let $S_{i,j} = \{\theta \in \mathcal{S}_n \mid \theta(i) = j\}$. Then for $A \in M_n(\mathbb{F})$,

$$\begin{aligned} \det A &= \sum_{\theta \in \mathcal{S}_n} \text{sgn}(\theta)(A)_{1,\theta(1)}(A)_{2,\theta(2)} \cdots (A)_{n,\theta(n)} \\ &= \sum_{\theta \in S_{i,j}} \text{sgn}(\theta)(A)_{1,\theta(1)}(A)_{2,\theta(2)} \cdots (A)_{n,\theta(n)} \\ &\quad + \sum_{\theta \in \mathcal{S}_n \setminus S_{i,j}} \text{sgn}(\theta)(A)_{1,\theta(1)}(A)_{2,\theta(2)} \cdots (A)_{n,\theta(n)}. \end{aligned}$$

Since for each $\theta \in S_{i,j}$, $(A)_{1,\theta(1)}(A)_{2,\theta(2)} \cdots (A)_{n,\theta(n)}$ has $(A)_{i,j}$ as a factor, we can write

$$\sum_{\theta \in S_{i,j}} \text{sgn}(\theta)(A)_{1,\theta(1)}(A)_{2,\theta(2)} \cdots (A)_{n,\theta(n)} = (A)_{i,j} A_{ij},$$

for some scalar A_{ij}.

Definition 4.3.1 The A_{ij} described above is called the *cofactor of* $(A)_{i,j}$.

Note that $(A)_{i,j}$ is the (i,j)-th entry of the matrix A and it is not A_{ij}.

Example 4.3.2 For $i = j = n$, we have

$$A_{nn} = \sum_{\theta \in S_{n,n}} \operatorname{sgn}(\theta)(A)_{1,\theta(1)}(A)_{2,\theta(2)} \cdots (A)_{(n-1),\theta(n-1)}.$$

Since $\theta \in S_{n,n}$, θ fixes n. Thus θ in $S_{n,n}$ defines a permutation ρ on $S' = \{1, 2, \ldots, n-1\}$, namely, $\rho = \theta\big|_{S'}$ (the restriction of θ on S'). Since no inversion of θ in $S_{n,n}$ involves the integer n, $\operatorname{sgn}(\theta) = \operatorname{sgn}(\rho)$. Thus

$$A_{nn} = \sum_{\rho \in \mathcal{S}_{n-1}} \operatorname{sgn}(\rho)(A)_{1,\rho(1)} \cdots (A)_{(n-1),\rho(n-1)}$$

is *the determinant of the* $(n-1) \times (n-1)$ *matrix obtained from* A *by crossing out the last row and the last column of* A. □

A similar procedure can be used to compute the cofactors A_{ij}. Interchanging successively adjacent rows and columns, we can obtain a matrix B with $(A)_{i,j}$ moved to the last row and last column. Thus, $(B)_{n,n} = (A)_{i,j}$. Since it takes $n - i$ interchanges of rows and $n - j$ interchanges of columns to get B, $\det B = (-1)^{n-i+n-j} \det A$. Then $\det A = (-1)^{i+j} \det B$. The cofactor A_{ij} of $(A)_{i,j}$ in A is the cofactor B_{nn} of $(B)_{n,n}$ in B. By Example 4.3.2, $B_{n,n}$ is the determinant of the $(n-1) \times (n-1)$ matrix obtained from B by crossing out the last row and the last column of B. This is the same determinant of the matrix obtained from A by crossing out the i-th row and the j-th column of A. This latter determinant is denoted by M_{ij} and is called the *minor of* A. Thus $A_{ij} = (-1)^{i+j} M_{ij}$.

Theorem 4.3.3 *The determinant* $\det A$ *can be expanded by cofactors using the* i*-th row of* A*, i.e.,*

$$\det A = \sum_{k=1}^{n} (A)_{i,k} A_{ik}.$$

Similarly, $\det A$ *can be expanded by cofactors using the* j*-th column of* A*, i.e.,*

$$\det A = \sum_{k=1}^{n} (A)_{k,j} A_{kj}.$$

Proof: Each term in the expansion of $\det A$ contains exactly one entry from each row and each column of A. Hence, for any given i, $\mathcal{S}_n = \bigcup_{k=1}^{n} S_{i,k}$, where the union is disjoint. Thus,

$$\det A = \sum_{k=1}^{n} \sum_{\theta \in S_{i,k}} \operatorname{sgn}\theta (A)_{1,\theta(1)} \cdots (A)_{n,\theta(n)} = \sum_{k=1}^{n} (A)_{i,k} A_{ik}.$$

Similarly, for any j, $\det A = \sum_{k=1}^{n} (A)_{k,j} A_{kj}$. □

For $n \geq 4$, it is usually very tedious to evaluate a determinant using cofactors. It is much easier to use elementary row (or column) operations to reduce one row (or column) to have at most one non-zero entry and then expand by cofactors using that row (or column).

Example 4.3.4 Evaluate $\begin{vmatrix} 1 & 2 & 0 & 5 \\ 3 & 4 & 1 & 7 \\ -2 & 5 & 2 & 0 \\ 0 & 1 & 2 & -7 \end{vmatrix}$.

$$\begin{vmatrix} 1 & 2 & 0 & 5 \\ 3 & 4 & 1 & 7 \\ -2 & 5 & 2 & 0 \\ 0 & 1 & 2 & -7 \end{vmatrix} \overset{\substack{(-3)\mathcal{R}_1+\mathcal{R}_2 \\ 2\mathcal{R}_1+\mathcal{R}_3}}{=} \begin{vmatrix} 1 & 2 & 0 & 5 \\ 0 & -2 & 1 & -8 \\ 0 & 9 & 2 & 10 \\ 0 & 1 & 2 & -7 \end{vmatrix} = \begin{vmatrix} -2 & 1 & -8 \\ 9 & 2 & 10 \\ 1 & 2 & -7 \end{vmatrix}$$

$$\overset{\substack{(-1)\mathcal{R}_2+\mathcal{R}_3 \\ (-2)\mathcal{R}_1+\mathcal{R}_2}}{=} \begin{vmatrix} -2 & 1 & -8 \\ 13 & 0 & 26 \\ -8 & 0 & -17 \end{vmatrix} = - \begin{vmatrix} 13 & 26 \\ -8 & -17 \end{vmatrix} = 13 \begin{vmatrix} 1 & 2 \\ 8 & 17 \end{vmatrix} = 13.$$

□

Example 4.3.5 To evaluate the *Vandermonde determinant*

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

we apply the sequence of elementary row operations
$(-x_1)\mathcal{R}_{n-1} + \mathcal{R}_n$, $(-x_1)\mathcal{R}_{n-2} + \mathcal{R}_{n-1}$, …, $(-x_1)\mathcal{R}_2 + \mathcal{R}_3$, $(-x_1)\mathcal{R}_1 + \mathcal{R}_2$ to get

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & x_2 - x_1 & \cdots & x_n - x_1 \\ 0 & x_2(x_2 - x_1) & \cdots & x_n(x_n - x_1) \\ \vdots & \vdots & \vdots & \vdots \\ 0 & x_2^{n-3}(x_2 - x_1) & \cdots & x_n^{n-3}(x_n - x_1) \\ 0 & x_2^{n-2}(x_2 - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{vmatrix}.$$

Then expanding by cofactors using the first column and factor out common factors to get

$$\left[\prod_{1<i\leq n} (x_i - x_1) \right] \begin{vmatrix} 1 & \cdots & 1 \\ x_2 & \cdots & x_n \\ x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots \\ x_2^{n-2} & \cdots & x_n^{n-2} \end{vmatrix}.$$

Continuing this process, we get that the Vandermonde determinant has value

$$\prod_{1\leq i<j\leq n} (x_j - x_i).$$

□

From Theorem 4.2.8 we know that A is invertible if and only if $\det A \neq 0$. Hence the matrix which defines the Vandermonde determinant is invertible if and only if all the x_i's are distinct. Such invertible matrix is called *Vandermonde matrix*. Following we shall show the relation between the inverse of A and $\det A$.

Proposition 4.3.6 *Let $A \in M_n(\mathbb{F})$ and let A_{ij} be the cofactor of $(A)_{i,j}$. Then $\sum_{j=1}^{n}(A)_{i,j}A_{kj} = \delta_{ik}\det A$ and $\sum_{i=1}^{n}(A)_{i,j}A_{ik} = \delta_{jk}\det A$.*

Proof: By Theorem 4.3.3 we have $\sum_{j=1}^{n}(A)_{i,j}A_{ij} = \det A$. For $i \neq k$, $\sum_{j=1}^{n}(A)_{i,j}A_{kj}$ by using Theorem 4.3.3 again is the determinant of a matrix whose i-th row and k-th row are the same. Hence it must be zero. Thus, $\sum_{j=1}^{n}(A)_{i,j}A_{kj} = 0$ if $i \neq k$. Hence $\sum_{j=1}^{n}(A)_{i,j}A_{kj} = \delta_{ik}\det A$. Similarly, we have $\sum_{i=1}^{n}(A)_{i,j}A_{ik} = \delta_{jk}\det A$. □

Definition 4.3.7 Suppose $A \in M_n(\mathbb{F})$ and let A_{ij} be the cofactor of $(A)_{i,j}$. Define $\mathrm{adj}A = \big(A_{ij}\big)^T \in M_n(\mathbb{F})$, i.e., $(\mathrm{adj}A)_{i,j} = A_{ji}$. This matrix is called the *classical adjoint* (for short, *adjoint*) of A.

Theorem 4.3.8 *Let $A \in M_n(\mathbb{F})$. Then $A(\mathrm{adj}A) = (\mathrm{adj}A)A = (\det A)I_n$.*

Proof: Let $C = A(\mathrm{adj}A)$. Then $(C)_{i,j} = \sum_{k=1}^{n}(A)_{i,k}A_{jk} = \delta_{ij}\det A$ for all i, j. Thus $A(\mathrm{adj}A) = (\det A)I_n$. Similarly, we have $(\mathrm{adj}A)A = (\det A)I_n$. □

Corollary 4.3.9 *Suppose A is invertible. Then $A^{-1} = (\det A)^{-1}\mathrm{adj}A$.*

Proof: By Theorem 4.2.8 we have $\det A \neq 0$. By Theorem 4.3.8 we have $A(\det A)^{-1}\mathrm{adj}A = I$. Hence $A^{-1} = (\det A)^{-1}\mathrm{adj}A$. □

Note that the cofactors of a square matrix can be defined even if $\mathbb{F}$ is a commutative ring, for example $\mathbb{F} = \mathbb{Z}$ or $\mathbb{F} = \mathbb{Z}_6$, etc.

Example 4.3.10

(1) Let $A = \begin{pmatrix} 3 & -2 & 1 \\ 5 & 6 & 2 \\ 1 & 0 & -3 \end{pmatrix} \in M_3(\mathbb{Q})$. Then $\det A = -94$. Thus A is invertible. The cofactors are

$$\begin{aligned} A_{11} &= -18, \quad A_{12} = 17, \quad A_{13} = -6; \\ A_{21} &= -6, \quad A_{22} = -10, \quad A_{23} = -2; \\ A_{31} &= -10, \quad A_{32} = -1, \quad A_{33} = 28. \end{aligned}$$

Hence $\mathrm{adj}A = \begin{pmatrix} -18 & -6 & -10 \\ 17 & -10 & -1 \\ -6 & -2 & 28 \end{pmatrix}$. Therefore, $A^{-1} = \begin{pmatrix} \frac{9}{47} & \frac{3}{47} & \frac{5}{47} \\ -\frac{17}{94} & \frac{5}{47} & \frac{1}{94} \\ \frac{3}{47} & \frac{1}{47} & -\frac{14}{47} \end{pmatrix}$. □

(2) Let $A = \begin{pmatrix} 3 & -2 & 1 \\ 5 & 6 & 2 \\ 1 & 0 & -3 \end{pmatrix} \in M_3(\mathbb{Z}_5)$. Then actually $A = \begin{pmatrix} 3 & 3 & 1 \\ 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}$. Then $\det A = 1$. Thus A is invertible. The cofactors are

$$\begin{aligned} A_{11} &= 2, \quad A_{12} = 2, \quad A_{13} = 4; \\ A_{21} &= 4, \quad A_{22} = 0, \quad A_{23} = 3; \\ A_{31} &= 0, \quad A_{32} = 4, \quad A_{33} = 3. \end{aligned}$$

Hence $\mathrm{adj}A = \begin{pmatrix} 2 & 4 & 0 \\ 2 & 0 & 4 \\ 4 & 3 & 3 \end{pmatrix}$.Therefore, $A^{-1} = \begin{pmatrix} 2 & 4 & 0 \\ 2 & 0 & 4 \\ 4 & 3 & 3 \end{pmatrix}$. □

(3) Let $A = \begin{pmatrix} 3 & -2 & 1 \\ 1 & -2 & 3 \\ 1 & 0 & -1 \end{pmatrix} \in M_3(\mathbb{Q})$. Then $\det A = 0$. Thus A is singular. We can also find the cofactors and the adjoint of A. The cofactors are

$$\begin{aligned} A_{11} &= 2, & A_{12} &= 4, & A_{13} &= 2; \\ A_{21} &= -2, & A_{22} &= -4, & A_{23} &= -2; \\ A_{31} &= -4, & A_{32} &= -8, & A_{33} &= -4. \end{aligned}$$

Hence $\mathrm{adj}A = \begin{pmatrix} 2 & -2 & -4 \\ 4 & -4 & -8 \\ 2 & -2 & -4 \end{pmatrix}$. One can check that $(\mathrm{adj}A)A = O = A(\mathrm{adj}A)$. □

Exercise 4.3

4.3-1. Evaluate

$$\begin{vmatrix} 1 & 4 & 9 & 16 \\ 4 & 9 & 16 & 25 \\ 9 & 16 & 25 & 36 \\ 16 & 25 & 36 & 49 \end{vmatrix}.$$

4.3-2. Show that

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & a_{43} & a_{44} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \times \begin{vmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{vmatrix}.$$

4.3-3. Evaluate the following determinants of $n \times n$ matrices ($n \geq 2$):

$$\begin{vmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \\ 3 & 4 & 5 & \cdots & 2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ n & 1 & 2 & \cdots & n-1 \end{vmatrix}, \quad \begin{vmatrix} 1-n & 1 & 1 & \cdots & 1 \\ 1 & 1-n & 1 & \cdots & 1 \\ 1 & 1 & 1-n & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1-n \end{vmatrix},$$

$$\begin{vmatrix} a_1 & a_2 & \cdots & \cdots & a_{n-1} & 0 \\ 1 & 0 & \cdots & \cdots & 0 & b_1 \\ 0 & 1 & 0 & \cdots & 0 & b_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 & b_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & b_{n-1} \end{vmatrix}.$$

4.3-4. Evaluate
$$\begin{vmatrix} a_1^n & a_1^{n-1}b_1 & \cdots & a_1b_1^{n-1} & b_1^n \\ a_2^n & a_2^{n-1}b_2 & \cdots & a_2b_2^{n-1} & b_2^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_n^n & a_n^{n-1}b_n & \cdots & a_nb_n^{n-1} & b_n^n \\ a_{n+1}^n & a_{n+1}^{n-1}b_{n+1} & \cdots & a_{n+1}b_{n+1}^{n-1} & b_{n+1}^n \end{vmatrix}.$$

4.3-5. Assume that $1+1 \neq 0$. Prove that if $A \in M_2(\mathbb{F})$ such that $A^2 = I$ and $\det A = 1$, then $A = \pm I$.

4.3-6. Suppose $A = \begin{pmatrix} B & C \\ O & D \end{pmatrix}$ be a square matrix over a ring (for example, $\mathbb{Z}$ or $\mathbb{F}[x]$), where B and D are square matrices. Show that $\det A = \det B \det D$.

4.3-7. Show that a matrix A is invertible if and only if $\mathrm{adj}A$ is invertible.

4.3-8. Show that for any $n \times n$ matrix A, $\det(\mathrm{adj}A) = (\det A)^{n-1}$.

4.3-9. Use the adjoint of A to find the inverse of $A = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 1 & -2 \\ 1 & 1 & 4 \end{pmatrix}$.

4.3-10. Let $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$ be of rank n. For $1 \leq r < n$, let $B = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{r1} & \cdots & a_{rn} \end{pmatrix}$. Put $X_i = \begin{pmatrix} A_{(r+i)1} \\ \vdots \\ A_{(r+i)n} \end{pmatrix}$ for $1 \leq i \leq n-r$, here A_{ij} is the cofactor of $(A)_{i,j}$. Show that $\{X_1, \ldots, X_{n-r}\}$ is a set of linearly independent solution of $BX = \mathbf{0}$.

4.3-11. Let $A \in M_n(\mathbb{Z})$ be a non-singular matrix. It means that there is a matrix $B \in M_n(\mathbb{Z})$ such that $AB = I = BA$. Note that $\mathbb{Z}$ is not a field.

(a) Show that $\mathrm{adj}A$ is also a matrix in $M_n(\mathbb{Z})$.

(b) Show that $A^{-1} \in M_n(\mathbb{Z})$ if and only if $\det A$ is either 1 or -1.

(c) Show that if $A \in M_n(\mathbb{Z})$ and $\det A = 1$, then $\mathrm{adj}(\mathrm{adj}A) = A$.

(d) Find nonzero integers x, y and z so that the inverse of the matrix $A = \begin{pmatrix} 3 & -1 & 2 \\ 1 & 1 & 5 \\ x & y & z \end{pmatrix}$ will contain only integers.

4.4 Cramer's Rule

Suppose we are given an $n \times n$ linear system:

$$\sum_{j=1}^{n} a_{ij}x_j = b_i \quad i = 1, 2, \ldots, n.$$

Put $A = (a_{ij})$, $\boldsymbol{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$, and $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Then the matrix form for the given system is $A\boldsymbol{x} = \boldsymbol{b}$. If the n equations are linearly independent, then A is invertible. By Corollary 4.3.9 $\boldsymbol{x} = A^{-1}\boldsymbol{b} = (\det A)^{-1}(\mathrm{adj}A)\boldsymbol{b}$. Then

$$x_k = (\det A)^{-1} \sum_{i=1}^{n} A_{ik} b_i, \quad k = 1, 2, \ldots, n.$$

We have the so-called *Cramer's rule*:

$$x_k = \frac{\begin{vmatrix} a_{11} & \cdots & b_1 & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & b_n & \cdots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & \cdots & a_{1k} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nk} & \cdots & a_{nn} \end{vmatrix}}, \quad k = 1, 2, \ldots, n.$$

Here the numerator is the determinant of the matrix obtained by replacing the k-th column of A by the column vector $\boldsymbol{b}$.

Example 4.4.1 Solve the following system of linear equations over $\mathbb{Q}$ by Cramer's rule:

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

Let $A = \begin{pmatrix} -2 & 3 & -1 \\ 1 & 2 & 1 \\ -2 & -1 & 1 \end{pmatrix}$. Then $\det A = -2$. Hence

$$x_1 = -\frac{1}{2}\begin{vmatrix} 1 & 3 & -1 \\ 0 & 2 & 1 \\ -1 & -1 & 1 \end{vmatrix} = -1, \quad x_2 = -\frac{1}{2}\begin{vmatrix} -2 & 1 & -1 \\ 1 & 0 & 1 \\ -2 & -1 & 1 \end{vmatrix} = -2,$$

$$x_3 = -\frac{1}{2}\begin{vmatrix} -2 & 3 & 1 \\ 1 & 2 & 0 \\ -2 & -1 & -1 \end{vmatrix} = -5.$$

□

Remark 4.4.2 Even if the coefficient matrix of the system is not square, we can still use Cramer's rule if the rows of A are linear independent. For example, consider the system

$$\begin{cases} 2x_1 - x_2 + 3x_3 = 4 \\ x_1 + 2x_2 - x_3 = 7 \end{cases}$$

over $\mathbb{Q}$. Transpose the x_3 term to the right, we have

$$\begin{cases} 2x_1 - x_2 = 4 - 3x_3 \\ x_1 + 2x_2 = 7 + x_3 \end{cases}$$

Then by Cramer'r rule,

$$x_1 = \frac{\begin{vmatrix} 4-x_3 & -1 \\ 7+x_3 & 2 \end{vmatrix}}{\begin{vmatrix} 2 & -1 \\ 1 & 2 \end{vmatrix}} = \frac{15-5x_3}{5} = 3 - x_3, \quad x_2 = \frac{\begin{vmatrix} 2 & 4-x_3 \\ 1 & 7+x_3 \end{vmatrix}}{\begin{vmatrix} 2 & -1 \\ 1 & 2 \end{vmatrix}} = \frac{10+5x_3}{5} = 2 + x_3,$$

x_3 arbitrary. □

The use of cofactors to find inverse and the Cramer's rule are not practical for $n \geq 4$. It is much simpler to use elementary row operations to reduce to the reduced row echelon form. However, the formula $A^{-1} = (\det A)^{-1}\text{adj}A$ and the Cramer's rule do tell analytically the relations of the inverse and solutions with the coefficients of the matrix, while the method of elementary row operations does not yield such an information.

Exercise 4.4

4.4-1. Use Cramer's rule to solve the system

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

4.4-2. Use Cramer's rule to solve the homogenous system

$$\begin{cases} x_1 + x_2 - x_3 = 0 \\ 3x_1 + 4x_2 - x_3 = 0 \\ x_1 + 2x_2 + x_3 = 0 \end{cases}$$

Chapter 5

Eigenvalue Problem

5.1 Eigenvalues and Eigenvectors

Eigenvectors and eigenvalues are useful throughout pure and applied mathematics. For instance, they are used to study differential equations and to solve systems of differential equations, to diagonalize matrices and to calculate powers of matrices, to study continuous and discrete dynamical system, they provide critical information in engineering design, and they arise naturally in other fields such as physics and chemistry.

Definition 5.1.1 Let $A \in M_n(\mathbb{F})$. A nonzero vector $\alpha \in \mathbb{F}^n$ is said to be an *eigenvector* (or a *characteristic vector*) of A if there exists a scalar $\lambda \in \mathbb{F}$ such that $A\alpha = \lambda\alpha$. The scalar λ is called the corresponding *eigenvalue* (or *characteristic value*). The scalar λ and the vector α related by $A\alpha = \lambda\alpha$ is called an *eigenpair*. The problem of finding λ and α is called an *eigenvalue problem*.

In this chapter we are interested in eigenvalue problem. So unless otherwise state, all matrices are square matrices.

Example 5.1.2 Let $A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then $\lambda = 1$ is an eigenvalue of A with eigenvector $\alpha = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. This is because $A\alpha = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. One can check that $\beta = \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}$ is also an eigenvector of A. □

Clearly, $A\alpha = \lambda\alpha$ for $\alpha \neq \mathbf{0}$ is equivalent to $(A - \lambda I)\alpha = \mathbf{0}$ for $\alpha \neq \mathbf{0}$. And it is equivalent to $A - \lambda I$ is singular, i.e., $\det(A - \lambda I) = 0$. So we have the following theorem.

Theorem 5.1.3 *The scalar λ is an eigenvalue of A if and only if λ is a root of the polynomial* $\det(A - xI)$.

Corollary 5.1.4 *The matrix A is singular if and only if* 0 *is an eigenvalue of A.*

Definition 5.1.5 Let $A \in M_n(\mathbb{F})$. Let $C_A(x) = \det(A - xI)$ (if no confusion can arise then $C(x)$ is written instead of $C_A(x)$). This polynomial is called the *characteristic polynomial* of A. The equation $C(x) = 0$ is called the *characteristic equation* of A.

Therefore, finding all eigenvalues of a matrix A is equivalent to finding all roots of the characteristic polynomial of A.

Example 5.1.6 Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. Then

$$C(x) = \begin{vmatrix} 1-x & 1 \\ 1 & 2-x \end{vmatrix} = (1-x)(2-x) - 1 = x^2 - 3x + 1.$$

Then $x = \dfrac{3 \pm \sqrt{5}}{2}$. That is $\lambda_1 = \dfrac{3+\sqrt{5}}{2}$ and $\lambda_2 = \dfrac{3-\sqrt{5}}{2}$ are eigenvalues of A. □

Example 5.1.7 Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $C(x) = x^2 + 1$. Thus A has no real eigenvalues, but it has two complex eigenvalues $\pm i$. □

Example 5.1.8 Let $A = \begin{pmatrix} 2 & -2 & -1 \\ 1 & -1 & -1 \\ -2 & 4 & 3 \end{pmatrix}$. Then $C(x) = -(x-1)^2(x-2)$. So 1 and 2 are all the eigenvalues of A. □

The determinant of an $n \times n$ matrix $A = (a_{ij})$ has $n!$ terms. Suppose a term of $\det A$ is $T = \operatorname{sgn}(\theta) a_{1\,\theta(1)} a_{2\,\theta(2)} \cdots a_{n\,\theta(n)}$. Suppose T contains the factor a_{ij} with $i \neq j$, i.e., T is not the "diagonal" term $a_{11}a_{22}\cdots a_{nn}$. Then T cannot contain the factors a_{ii} and a_{jj} (in fact it cannot contain any other factor from the i-th row and the j-th column). Thus, in the expansion of $\det(A - xI)$, every term contains at most $n-2$ factors with x except for the diagonal term. Hence we have

$$C(x) = (a_{11} - x)(a_{22} - x)\cdots(a_{nn} - x) + p(x), \tag{5.1}$$

where $p(x)$ is a polynomial of degree at most $n-2$.

Theorem 5.1.9 *The characteristic polynomial of $A \in M_n(\mathbb{F})$ is given by*

$$C(x) = (-1)^n x^n + (-1)^{n-1}\operatorname{Tr}(A)x^{n-1} + \cdots + \det A,$$

where $\operatorname{Tr}(A) = \sum_{i=1}^{n} (A)_{i,i}$ *is called the* trace *of A.*

Proof: By expanding Equation (5.1), we know that $\deg C = n$ and the coefficients of the first and the second terms are $(-1)^n$ and $(-1)^{n-1}\operatorname{Tr}(A)$, respectively. The last term of C is $C(0)$. It is equal to $\det A$. So we have the theorem. □

Corollary 5.1.10 *Let $A \in M_n(\mathbb{F})$. Suppose $\lambda_1, \lambda_2, \ldots, \lambda_n$ are all eigenvalues of A (not necessary distinct). Then* $\operatorname{Tr}(A) = \lambda_1 + \lambda_2 + \cdots + \lambda_n$ *and* $\det A = \lambda_1\lambda_2\cdots\lambda_n$.

Theorem 5.1.11 *If λ is an eigenvalue of $A \in M_n(\mathbb{F})$, then the set of all vectors satisfying $A\boldsymbol{x} = \lambda\boldsymbol{x}$ (including the zero vector $\mathbf{0}$) is the vector subspace $\mathscr{E}(\lambda) = \operatorname{null}(A - \lambda I)$ of $\mathbb{F}^n$. Moreover,* $\dim(\mathscr{E}(\lambda)) = n - \operatorname{rank}(A - \lambda I)$.

The vector space $\mathscr{E}(\lambda)$ is called the *eigenspace* of λ.

Definition 5.1.12 Let $A \in M_n(\mathbb{F})$ and $C(x)$ be the characteristic polynomial of A. Suppose $\lambda \in \mathbb{F}$ is an eigenvalue of A. Then $(x-\lambda)$ is a factor of $C(x)$. The *algebraic multiplicity*, denoted by $a_A(\lambda)$, is the largest integer m such that $(x-\lambda)^m$ divides $C(x)$. The dimension of $\mathscr{E}(\lambda)$, denoted by $g_A(\lambda)$, is called the *geometric multiplicity* of λ. If no confusion can arise, then $a(\lambda)$ and $g(\lambda)$ are written instead of $a_A(\lambda)$ and $g_A(\lambda)$, respectively.

Example 5.1.13 Let $A = J_n = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$. Then

$$C(x) = \begin{vmatrix} 1-x & 1 & \cdots & 1 \\ 1 & 1-x & \cdots & 1 \\ \vdots & & \ddots & \\ 1 & 1 & \cdots & 1-x \end{vmatrix} = \begin{vmatrix} n-x & 1 & \cdots & 1 \\ n-x & 1-x & \cdots & 1 \\ \vdots & & \ddots & \\ n-x & 1 & \cdots & 1-x \end{vmatrix}$$

$$= (n-x)\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1-x & \cdots & 1 \\ \vdots & & \ddots & \\ 1 & 1 & \cdots & 1-x \end{vmatrix} = (n-x)\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & -x & 0 & \cdots & 0 \\ 0 & 0 & -x & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \\ 0 & 0 & 0 & \cdots & -x \end{vmatrix}$$

$$= (-x)^{n-1}(n-x).$$

Thus eigenvalues are n and 0. Moreover, $a(n) = 1$ and $a(0) = n-1$. □

Example 5.1.14 Let $A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. It is clear that 1 is the only eigenvalue of A and $a(1) = 3$.

$$\left(\begin{array}{c|c} (A-I)^T & I_3 \end{array} \right) = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 \end{array} \right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{array} \right).$$

Thus $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T$ and $\begin{pmatrix} 0 & -2 & 1 \end{pmatrix}^T$ are two linearly independent eigenvectors of A corresponding to the eigenvalue 1. So $\mathscr{E}(1) = \text{span}\left\{ \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T, \begin{pmatrix} 0 & -2 & 1 \end{pmatrix}^T \right\}$ and $g(1) = 2$. □

Example 5.1.15 Let $A = \begin{pmatrix} 0 & -2 & 1 \\ -2 & 3 & -2 \\ 1 & -2 & 0 \end{pmatrix}$. Then $C(x) = -(x+1)^2(x-5)$. So the eigenvalues of A are -1 and 5. Moreover, $a(-1) = 2$ and $a(5) = 1$.

For $\lambda = -1$, then $A + I = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 4 & -2 \\ 1 & -2 & 1 \end{pmatrix}$.

$$\left(\begin{array}{c|c} (A+I)^T & I_3 \end{array} \right) \to \left(\begin{array}{ccc|ccc} 1 & -2 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \end{array} \right).$$

Thus $\mathscr{E}(-1) = \text{span}\left\{ \begin{pmatrix} -2 & 1 & 0 \end{pmatrix}^T, \begin{pmatrix} -1 & 0 & 1 \end{pmatrix}^T \right\}$ and $g(-1) = 2$.

For $\lambda = 5$, then $A - 5I = \begin{pmatrix} -5 & -2 & 1 \\ -2 & -2 & -2 \\ 1 & -2 & -5 \end{pmatrix}$.

$$\left(\begin{array}{c|c} (A-5I)^T & I_3 \end{array} \right) \to \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 2 & 0 & \frac{1}{6} & -\frac{1}{3} \\ \hline 0 & 0 & 0 & 1 & 2 & 1 \end{array} \right).$$

Thus $\mathscr{E}(5) = \text{span}\left\{ \begin{pmatrix} 1 & 2 & 1 \end{pmatrix}^T \right\}$ and $g(5) = 1$. □

Example 5.1.16 Let $A = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} \in M_2(\mathbb{C})$. Then the characteristic polynomial is $C(x) = x^2 + 1$. The eigenvalues are i and $-i$. The corresponding eigenvectors are $\begin{pmatrix} 1+i \\ -1 \end{pmatrix}$ and $\begin{pmatrix} i-1 \\ 1 \end{pmatrix}$, respectively. So $a(i) = g(i) = 1$ and $a(-i) = g(-i) = 1$ □

Example 5.1.17 Let $A = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} \in M_2(\mathbb{Z}_5)$. Then the characteristic polynomial is $C(x) = x^2 + 1 = (x-2)(x-3)$. The eigenvalues are 2 and 3. The corresponding eigenvectors are $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, respectively. Then $a(2) = g(2) = 1$ and $a(3) = g(3) = 1$. □

From the above examples, we see that $a(\lambda) \geq g(\lambda) \geq 1$ if λ is an eigenvalue of a matrix A. We shall show that this observation is true. Before showing this fact, we need two lemmas and a definition.

Definition 5.1.18 Two matrices A and B are said to be *similar* if there is an invertible matrix P such that $B = P^{-1}AP$.

Clearly, being similar is an equivalence relation defined on the set of square matrices of the same order.

Lemma 5.1.19 *Suppose A and B are similar. Then $C_A(x) = C_B(x)$.*

Proof: Since $B = P^{-1}AP$ for some invertible matrix P,

$$\begin{aligned} C_B(x) &= \det(B - xI) = \det(P^{-1}AP - xI) = \det(P^{-1}(A - xI)P) = \det((A - xI)P^{-1}P) \\ &= \det(A - xI) = C_A(x). \end{aligned}$$

□

Lemma 5.1.20 *Suppose $A\alpha = \lambda\alpha$ with $\alpha \neq \mathbf{0}$. Let P be an invertible matrix whose i-th column is α. Then the i-th column of $P^{-1}AP$ is $\lambda \boldsymbol{e}_i$.*

Proof: Let $A = \begin{pmatrix} A_1 & \cdots & A_i & \cdots & A_n \end{pmatrix}$ and $P = \begin{pmatrix} P_1 & \cdots & P_i & \cdots & P_n \end{pmatrix}$, where $P_i = \alpha$. Since $P^{-1}P = \begin{pmatrix} P^{-1}P_1 & \cdots & P^{-1}P_i & \cdots & P^{-1}P_n \end{pmatrix} = I_n$, $P^{-1}\alpha = P^{-1}P_i = \boldsymbol{e}_i$. Then we have

$$\begin{aligned} P^{-1}AP &= \begin{pmatrix} P^{-1}AP_1 & \cdots & P^{-1}AP_i & \cdots & P^{-1}AP_n \end{pmatrix} \\ &= \begin{pmatrix} P^{-1}AP_1 & \cdots & P^{-1}\lambda\alpha & \cdots & P^{-1}AP_n \end{pmatrix} \\ &= \begin{pmatrix} P^{-1}AP_1 & \cdots & \lambda \boldsymbol{e}_i & \cdots & P^{-1}AP_n \end{pmatrix}. \end{aligned}$$

Thus the i-th column of $P^{-1}AP$ is $\lambda \boldsymbol{e}_i$. □

Theorem 5.1.21 *If λ is an eigenvalue of A, then $a(\lambda) \geq g(\lambda) \geq 1$.*

Proof: There is at least one eigenvector corresponding to λ. So $g(\lambda) = \dim \mathscr{E}(\lambda) \geq 1$.

Suppose $g(\lambda) = s$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ be a basis of $\mathscr{E}(\lambda)$. Recall that every non-zero vector in $\mathscr{E}(\lambda)$ is an eigenvector of A correspondent to λ. Extend $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ to a basis of $\mathbb{F}^n$, say $\{\alpha_1, \alpha_2, \ldots, \alpha_s, \beta_{s+1}, \ldots, \beta_n\}$. Let $P = \begin{pmatrix} \alpha_1 & \cdots & \alpha_s & \beta_{s+1} & \cdots & \beta_n \end{pmatrix}$. Then P is invertible. By Lemma 5.1.20, with $i = 1, 2, \ldots, s$, we have

$$P^{-1}AP = \begin{pmatrix} \lambda \boldsymbol{e}_1 & \cdots & \lambda \boldsymbol{e}_s & * & \cdots & * \end{pmatrix} = \left(\begin{array}{c|c} \lambda I_s & C \\ \hline O & D \end{array}\right).$$

By Lemma 5.1.19,

$$C_A(x) = \det(P^{-1}AP - xI) = \left|\begin{array}{c|c} (\lambda - x)I_s & C \\ \hline O & D - xI_{n-s} \end{array}\right| = (\lambda - x)^s q(x)$$

for some polynomial q. So $a(\lambda) \geq s = g(\lambda)$. □

Suppose A is similar to B. From Lemma 5.1.19 we know that A and B have the same characteristic polynomial. So they have the same eigenvalues and $a_A(\lambda) = a_B(\lambda)$ for each eigenvalue λ. Moreover, they have the same geometric multiplicities. We describe it as follows.

Theorem 5.1.22 *Suppose A is similar to B and λ is an eigenvalue of A with $g_A(\lambda) = r$. Then λ is also an eigenvalue of B with $g_B(\lambda) = r$.*

Proof: Suppose $B = P^{-1}AP$ for some invertible matrix P. Let $\{\alpha_1, \ldots, \alpha_r\}$ be a set of linearly independent eigenvectors of A corresponding to λ. Consider the set $\{P^{-1}\alpha_1, \ldots, P^{-1}\alpha_r\}$. Since P is invertible, this set is linearly independent. Since

$$B(P^{-1}\alpha_i) = P^{-1}APP^{-1}\alpha_i = P^{-1}A\alpha_i = P^{-1}\lambda\alpha_i = \lambda P^{-1}\alpha_i,$$

$\{P^{-1}\alpha_1, \ldots, P^{-1}\alpha_r\}$ is a set of linearly independent eigenvectors of B correspondent to λ. Hence, we have $g_B(\lambda) \geq g_A(\lambda)$.

Since $A = (P^{-1})^{-1}BP^{-1}$, B is similar to A, so we have $g_A(\lambda) \geq g_B(\lambda)$. Thus they are equal. □

Exercise 5.1

5.1-1. Consider Example 5.1.13. Find $g(0)$.

5.1-2. Show that A and A^T have the same characteristic polynomial. Hence A and A^T have the same eigenvalues. How about their eigenvectors?

5.1-3. Suppose A and B are two square matrices of the same size. Show that AB and BA have the same eigenvalues. A challenge problem: Try to show that AB and BA have the same characteristic polynomial.

5.1-4. Construct 2×2 matrices A and B such that eigenvalues of AB are not product of eigenvalues of A and B.

5.1-5. Suppose A is non-singular. Show that if λ is an eigenvalue of A, then λ^{-1} is an eigenvalue of A^{-1}.

5.1-6. A matrix $A \in M_n(\mathbb{R})$ is called a *stochastic matrix* if $0 < (A)_{i,j} \leq 1$ and $\sum_{i=1}^{n} (A)_{i,j} = 1$ for all j. Show that if A is a stochastic matrix, then A has an eigenvalue 1.

5.2 Polynomials in Matrices

Recall that $\mathbb{F}[x]$ is the set of all polynomials in an indeterminate x whose coefficients are elements of $\mathbb{F}$. Let $p(x) = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$. Let $A \in M_n(\mathbb{F})$. We define $p(A) = a_m A^m + \cdots + a_1 A + a_0 I_n$. This is called a *polynomial in* A. There is a relation between the eigenvalues of polynomials in A and the eigenvalues of A. We start the special cases first.

Lemma 5.2.1 *If λ is an eigenvalue of A, then $\lambda + c$, λ^m and $c\lambda$ are eigenvalues of $A + cI$, A^m and cA, respectively, where $m \in \mathbb{N}_0$.* Note that A^0 is defined to be I.

Proof: Let α be an eigenvector of A corresponding to λ. Then

$$(A + cI)\alpha = A\alpha + cI\alpha = \lambda\alpha + c\alpha = (\lambda + c)\alpha.$$

So $\lambda + c$ is an eigenvalue of $A + cI$. For $m = 0$, this is obvious. For $m \geq 1$,

$$A^m\alpha = A^{m-1}(A\alpha) = A^{m-1}(\lambda\alpha) = \lambda A^{m-1}\alpha.$$

By induction, we have $A^m\alpha = \lambda^m\alpha$ and hence λ^m is an eigenvalue of A^m. Finally,

$$(cA)\alpha = c(A\alpha) = c\lambda\alpha.$$

So $c\alpha$ is an eigenvalue of cA. □

Theorem 5.2.2 *Let $p(x)$ be a polynomial over $\mathbb{F}$ and $A \in M_n(\mathbb{F})$. Suppose (λ, α) is an eigenpair of A. Then $(p(\lambda), \alpha)$ is an eigenpair of $p(A)$.*

Proof: Suppose $p(x) = \sum_{i=0}^{m} a_i x^i$. Then by Lemma 5.2.1

$$p(A)\alpha = \left(\sum_{i=0}^{m} a_i A^i\right)\alpha = \sum_{i=0}^{m} a_i A^i\alpha = \sum_{i=0}^{m} a_i \lambda^i \alpha = p(\lambda)\alpha.$$

□

In the previous sections, we only considered matrices whose entries are in a field $\mathbb{F}$. Now we extend this consideration to matrices whose entries are polynomials. By $A \in M_{m,n}(\mathbb{F}[x])$ we mean A

is an $m \times n$ matrix whose entries are in $\mathbb{F}[x]$. The addition, scalar multiplication and multiplication are similarly defined. All the elementary algebraic properties, such as commutative law for addition, associative law, distribution law, adjoint and determinant, etc., still hold.

Given a matrix $A \in M_{m,n}(\mathbb{F}[x])$. We can expand A into a polynomial of x whose coefficients are $m \times n$ matrices. We use the following example to illustrate this result.

Example 5.2.3 Let $A = \begin{pmatrix} x^2+1 & 3x & 2 \\ x^3-2x^2 & 3x+2 & 2x^2 \\ 4 & -x^2-2 & x+1 \\ x^3 & x^2-1 & x \end{pmatrix}$. Then

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} x^3 + \begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 2 \\ 0 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 3 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} x + \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 0 \\ 4 & -2 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

□

Theorem 5.2.4 (Cayley-Hamilton Theorem) *Suppose $C(x)$ is the characteristic polynomial of A. Then $C(A) = O$.*

Proof: Let $Y(x) = A - xI$. Since $Y(x) \in M_n(\mathbb{F}[x])$, $\text{adj}(Y(x)) \in M_n(\mathbb{F}[x])$. Moreover, the degree of each entry of $\text{adj}(Y(x))$ is at most $n-1$. Let

$$\text{adj}(Y(x)) = C_{n-1}x^{n-1} + C_{n-2}x^{n-2} + \cdots + C_1x + C_0,$$

where $C_0, C_1, \ldots, C_{n-1} \in M_n(\mathbb{F})$. By Theorem 4.3.8, we have

$$C(x)I = \det(Y(x))I = \text{adj}(Y(x))Y(x) = \text{adj}(Y(x))(A - xI) = \text{adj}(Y(x))A - \text{adj}(Y(x))x.$$

Suppose $C(x) = k_nx^n + k_{n-1}x^{n-1} + \cdots + k_1x + k_0$. Then

$$\begin{aligned} C(x)I &= k_nx^nI + k_{n-1}x^{n-1}I + \cdots + k_1xI + k_0I \\ &= C_{n-1}Ax^{n-1} + \cdots + C_1Ax + C_0A - C_{n-1}x^n - \cdots - C_1x^2 - C_0x \\ &= -C_{n-1}x^n + (-C_{n-2} + C_{n-1}A)x^{n-1} + \cdots + \\ &\quad + (-C_{n-i-1} + C_{n-i}A)x^{n-i} + \cdots + (-C_0 + C_1A)x + C_0A. \end{aligned}$$

Equating the coefficients of x's, we obtain

$$\begin{aligned} k_nI &= -C_{n-1} \\ k_{n-1}I &= -C_{n-2} + C_{n-1}A \\ &\vdots \\ k_{n-i+1}I &= -C_{n-i} + C_{n-i+1}A \\ &\vdots \\ k_1I &= -C_0 + C_1A \\ k_0I &= C_0A \end{aligned}$$

For each $i = 1, 2, \ldots, n+1$ multiply the i-th equation by A^{n-i+1} from the right respectively and add to obtain

$$\begin{aligned} C(A) = \sum_{i=1}^{n+1} k_{n-i+1} I A^{n-i+1} &= -C_{n-1}A^n + \left(\sum_{i=2}^{n} (-C_{n-i} + C_{n-i+1}A) A^{n-i+1} \right) + C_0 AI \\ &= -C_{n-1}A^n - \sum_{i=2}^{n} C_{n-i}A^{n-i+1} + \sum_{i=2}^{n} C_{n-i+1}A^{n-i+2} + C_0 A \\ &= -C_{n-1}A^n - \sum_{i=2}^{n} C_{n-i}A^{n-i+1} + \sum_{i=1}^{n-1} C_{n-i}A^{n-i+1} + C_0 A \\ &= -C_{n-1}A^n - C_0 A + C_{n-1}A^n + C_0 A = O. \end{aligned}$$

□

For a given matrix A, from Cayley-Hamilton Theorem we know that A satisfies a polynomial equation. That is, $f(A) = O$ for some $f(x) \in \mathbb{F}[x]$. Let

$$\operatorname{ann}(A) = \{ f(x) \in \mathbb{F}[x] \mid f(A) = O \}$$

(it is called the *annihilator of* A). We shall prove below that there exists a nonzero polynomial in $\operatorname{ann}(A)$ of minimal degree. The proof is similar to the proof of Theorem 0.5.5 (Division Algorithm for Polynomials).

Theorem 5.2.5 *There exists a nonzero polynomial $m(x) \in \operatorname{ann}(A)$ of minimal degree. Moreover, (1) for every $f(x) \in \operatorname{ann}(A)$, $m(x)$ is a factor of $f(x)$; (2) if $m(x)$ is monic, then it is unique.*

Proof: Let $S = \{\deg f \mid f \in \operatorname{ann}(A), f \neq 0\}$. Then by Well Ordering Principle, S contains the smallest nonnegative integer, say s. Hence there exists a nonzero polynomial $m(x) \in \operatorname{ann}(A)$ such that $\deg m = s$.

For each $f(x) \in \operatorname{ann}(A)$, by Theorem 0.5.5 there is $q(x), r(x) \in \mathbb{F}[x]$ such that $f(x) = m(x)q(x) + r(x)$, with $\deg r < \deg m$. Since $O = f(A) = m(A)q(A) + r(A) = r(A)$, $r(x) \in \operatorname{ann}(A)$. Since $m(x)$ is a nonzero polynomial of minimal degree in $\operatorname{ann}(A)$, $r(x)$ must be zero. Thus, $m(x)$ is a factor of $f(x)$.

Suppose there are two monic polynomials $m(x)$ and $m_1(x)$ in $\operatorname{ann}(A)$ of degree s. Then the degree of $g(x) = m(x) - m_1(x)$ is less than s. Since $g(A) = O$, by the same argument above g must be zero. Hence $m(x) = m_1(x)$. □

Definition 5.2.6 A polynomial $m(x) \in \operatorname{ann}(A)$ of minimal degree is called a *minimum polynomial of* A. Since the monic minimum polynomial of A is unique, we call the monic minimum polynomial of A to be *the minimum polynomial* of A.

Note that by the proof of Theorem 5.2.5, if $m(x)$ and $m_1(x)$ are minimum polynomials of A, then $m(x) = am_1(x)$ for some $a \in \mathbb{F}$.

Proposition 5.2.7 *Suppose A and B are similar. Then they have the same (monic) minimum polynomial.*

Proof: Suppose $B = P^{-1}AP$ for some invertible matrix P. For any polynomial $f \in \mathbb{F}[x]$, $f(B) = P^{-1}f(A)P$. Therefore, $f \in \operatorname{ann}(A)$ if and only if $f \in \operatorname{ann}(B)$. Thus A and B have the same minimum polynomial. □

Theorem 5.2.8 *Let $A \in M_n(\mathbb{F})$ and let $Y(x) = A - xI$. Let $g(x)$ be the greatest common divisor of the entries of* adj$(Y(x))$. *Then $g(x)$ divides the characteristic polynomial $C(x)$ and $h(x) = \frac{C(x)}{g(x)}$ is a minimum polynomial of A.*

Proof: Let adj$(Y(x)) = g(x)B(x)$, where $B(x)$ is a matrix whose entries are polynomials. Since $g(x)$ is the g.c.d. of the entries of adj$(Y(x))$, the entries of $B(x)$ have no non-scalar common factors. Since $C(x)I = \text{adj}(Y(x))Y(x) = g(x)B(x)Y(x)$, $g(x)$ divides $C(x)$ and $h(x)$ is a polynomial. Since $\deg g < n$, $\deg h \geq 1$. Suppose that $h(x) = h_{t+1}x^{t+1} + \cdots + h_1x + h_0$ with $h_{t+1} \neq 0$, $t \geq 0$. Then $\deg g = n - t - 1$. Thus $B(x)$ is matrix whose entries are polynomials in x of degree not greater than $n - 1 - (n - t - 1) = t$.

Let $B(x) = B_tx^t + B_{t-1}x^{t-1} + \cdots + B_1x + B_0$, where $B_i \in M_n(\mathbb{F})$, $0 \leq i \leq t$. Then

$$\begin{aligned} h(x)I = B(x)Y(x) &= B(x)(A - xI) = B(x)A - B(x)x \\ &= B_tAx^t + B_{t-1}Ax^{t-1} + \cdots + B_1Ax + B_0A \\ &\quad - B_tx^{t+1} - B_{t-1}x^t - \cdots - B_1x^2 - B_0x \\ &= -B_tx^{t+1} + (B_tA - B_{t-1})x^t + \cdots + (B_2A - B_1)x^2 + (B_1A - B_0)x + B_0A. \end{aligned}$$

Comparing the coefficients we obtain

$$\begin{aligned} h_{t+1}I &= -B_t \\ h_tI &= -B_{t-1} + B_tA \\ &\vdots \\ h_1I &= -B_0 + B_1A \\ h_0I &= B_0A \end{aligned}$$

Multiply each of these equations by $A^{t+1}, A^t, \ldots, A$ and I from the right respectively and add them. We obtain

$$\begin{aligned} h(A) &= h_{t+1}A^{t+1} + \cdots + h_0I \\ &= -B_tA^{t+1} - B_{t-1}A^t + B_tA^{t+1} - \cdots - B_0A + B_1A^2 + B_0A = O. \end{aligned}$$

Thus $h(x) \in \text{ann}(A)$. By Theorem 5.2.5, $h(x)$ is divisible by $m(x)$.

Consider the polynomial $m(x) - m(y) \in \mathbb{F}[x, y]$. Since it is a sum of terms of the form $c_i(x^i - y^i)$ for some $c_i \in \mathbb{F}$, each of which is divisible by $y - x$. So $m(x) - m(y) = (y - x)k(x, y)$ for some $k(x, y) \in \mathbb{F}[x, y]$. Since $(xI)A = A(xI)$, we can substitute xI to x and A to y, and obtain

$$m(x)I = m(xI) = m(xI) - m(A) = (A - xI)k(xI, A) = Y(x)k(xI, A).$$

Multiplying by adj$(Y(x))$ on the left, we obtain

$$m(x)\text{adj}(Y(x)) = \text{adj}(Y(x))Y(x)k(xI, A) = C(x)k(xI, A).$$

Hence $m(x)g(x)B(x) = h(x)g(x)k(xI, A)$. Thus $m(x)B(x) = h(x)k(xI, A)$. Since $h(x)$ divides every entry of $m(x)B(x)$ and the entries of $B(x)$ have no non-scalar common factors, $h(x)$ divides $m(x)$.

Thus $h(x)$ and $m(x)$ differ at most by a scalar factor. Hence $h(x)$ is a minimum polynomial of A.

□

Theorem 5.2.9 *Each irreducible factor of the characteristic polynomial $C(x)$ of A is also an irreducible factor of a minimum polynomial $m(x)$.*

Proof: As we have seen in the proof of Theorem 5.2.8, $m(x)I = Y(x)k(xI, A)$. Thus $\det(m(x)I) = \det(Y(x))\det(k(xI, A))$. Hence $m(x)^n = C(x)\det(k(xI, A))$. Thus every irreducible factor of $C(x)$ must divide $m(x)^n$, and therefore divides $m(x)$. □

Corollary 5.2.10 *The characteristic and minimal polynomials of A have the same roots except for multiplicities.*

Corollary 5.2.11 *Suppose the characteristic polynomial and the minimal polynomial of A are $C(x)$ and $m(x)$. If $C(x)$ has no repeated factors, then $m(x) = (-1)^n C(x)$.*

Example 5.2.12 Let $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Then

$$Y(x) = \begin{pmatrix} 1-x & 0 & 0 \\ 0 & 1-x & 1 \\ 0 & 0 & 1-x \end{pmatrix}, \qquad C(x) = (1-x)^3,$$

$$\operatorname{adj}(Y(x)) = \begin{pmatrix} (1-x)^2 & 0 & 0 \\ 0 & (1-x)^2 & -(1-x) \\ 0 & 0 & (1-x)^2 \end{pmatrix}.$$

Thus $g(x) = 1 - x$ and the minimum polynomial $h(x) = \frac{C(x)}{g(x)} = (1-x)^2$. □

Exercise 5.2

5.2-1. Let $A = \begin{pmatrix} x^2+x+1 & 2x^2-3 & -x^2-x-1 \\ x^2+4x-3 & 2x & -x^2+1 \end{pmatrix}$. Express A into polynomial of x with matrix coefficients.

5.2-2. Let $A = \begin{pmatrix} 3 & -1 & -1 \\ -12 & 0 & 5 \\ 4 & -2 & -1 \end{pmatrix}$. Find the characteristic polynomial of A. Verify the Cayley-Hamilton Theorem.

5.2-3. Let A be as in Problem 5.2-2. Find the eigenvalues of A and, their algebraic multiplicities and geometric multiplicities respectively.

5.2-4. Let $A \in M_n(\mathbb{F})$. Let $C(x) = (-1)^n x^n + k_{n-1}x^{n-1} + \cdots + k_1 x + k_0$ be the characteristic polynomial of A. Show that if $k_0 \neq 0$, then A is invertible and

$$A^{-1} = -k_0^{-1}\big\{(-1)^n A^{n-1} + k_{n-1}A^{n-2} + \cdots + k_1 I\big\}.$$

Hence adj$A$ can be expresses as a linear combination of A^{n-1}, A^{n-2}, ..., A and I.

5.2-5. Let $p(x) = (-1)^n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$. Use mathematical induction show that the matrix

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & (-1)^{n+1}a_0 \\ 1 & 0 & \cdots & 0 & (-1)^{n+1}a_1 \\ 0 & 1 & \cdots & 0 & (-1)^{n+1}a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & (-1)^{n+1}a_{n-1} \end{pmatrix}$$

has $p(x)$ as its characteristic polynomial. Matrix A is called the *companion matrix* of the polynomial $p(x)$.

5.3 Diagonalizable Matrices

In this section, we shall describe some necessary and sufficient conditions for diagonalizable matrices.

Theorem 5.3.1 *Suppose $\lambda_1, \ldots, \lambda_k$ are k distinct eigenvalues of A and $\alpha_1, \ldots, \alpha_k$ are corresponding eigenvectors, respectively. Then $\{\alpha_1, \ldots, \alpha_k\}$ is linearly independent.*

Proof: Suppose $\{\alpha_1, \ldots, \alpha_k\}$ is linearly dependent. Then there exists $m \geq 1$ such that $\{\alpha_1, \ldots, \alpha_m\}$ is linearly independent while α_{m+1} depends on $\alpha_1, \ldots, \alpha_m$. Hence there are $c_1, \ldots, c_m \in \mathbb{F}$ such that $\alpha_{m+1} = \sum_{i=1}^{m} c_i\alpha_i$.

Now

$$\begin{aligned} \mathbf{0} = (A - \lambda_{m+1}I)\alpha_{m+1} &= (A - \lambda_{m+1}I)\left(\sum_{i=1}^{m} c_i\alpha_i\right) \\ &= A\left(\sum_{i=1}^{m} c_i\alpha_i\right) - \sum_{i=1}^{m} c_i\lambda_{m+1}\alpha_i = \sum_{i=1}^{m} c_iA\alpha_i - \sum_{i=1}^{m} c_i\lambda_{m+1}\alpha_i \\ &= \sum_{i=1}^{m} c_i\lambda_i\alpha_i - \sum_{i=1}^{m} c_i\lambda_{m+1}\alpha_i = \sum_{i=1}^{m} c_i(\lambda_i - \lambda_{m+1})\alpha_i \end{aligned}$$

Since $\alpha_1, \ldots, \alpha_m$ are linearly independent, $c_i(\lambda_i - \lambda_{m+1}) = 0$ for all $i = 1, \ldots, m$. Since λ_i's are distinct, $c_i = 0$ for all $i = 1, \ldots, m$. Hence $\alpha_{m+1} = \mathbf{0}$. This is clearly impossible. □

Definition 5.3.2 A matrix $A \in M_n(\mathbb{F})$ is said to be *diagonalizable* over $\mathbb{F}$, if there exists an invertible matrix $P \in M_n(\mathbb{F})$ such that $P^{-1}AP$ is a diagonal matrix, i.e., A is similar to a diagonal matrix.

For convenience, an $n \times n$ diagonal matrix D will be written as $\text{diag}\{d_1, \ldots, d_n\}$, where $(D)_{i,i} = d_i$, $1 \leq i \leq n$.

Theorem 5.3.3 *Suppose $A \in M_n(\mathbb{F})$ has n linearly independent eigenvectors $\alpha_1, \ldots, \alpha_n$ with the corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$ respectively. Put $P = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix}$. Then $P^{-1}AP = D$ is a diagonal matrix. Indeed $D = \text{diag}\{\lambda_1, \ldots, \lambda_n\}$.*

Proof: This follows from Lemma 5.1.20. □

Definition 5.3.4 A matrix $A \in M_n(\mathbb{F})$ is said to be *simple* if A has n linearly independent eigenvectors in $\mathbb{F}^n$. Matrices that are not simple are called *defective*.

Corollary 5.3.5 *Suppose $A \in M_n(\mathbb{F})$. Then A is simple if and only if A is diagonalizable over $\mathbb{F}$.*

Proof: The "only if" part follows from Theorem 5.3.3.

For the "if" part, let $P^{-1}AP = D = \text{diag}\{\lambda_1, \ldots, \lambda_n\}$ for some $\lambda_i \in \mathbb{F}$. Let $P = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix}$. Then

$$AP = \begin{pmatrix} A\alpha_1 & \cdots & A\alpha_n \end{pmatrix} = PD = \begin{pmatrix} \lambda_1\alpha_1 & \cdots & \lambda_n\alpha_n \end{pmatrix}.$$

Then $\alpha_1, \ldots, \alpha_n$ are eigenvectors of A corresponding to eigenvalues $\lambda_1, \ldots, \lambda_n$ respectively. Since P is invertible, $\alpha_1, \ldots, \alpha_n$ are linearly independent. Hence A is simple. □

Theorem 5.3.6 (**First Test for Diagonalizability**) *Let $A \in M_n(\mathbb{F})$. Suppose the characteristic polynomial of A can be factorized as a product of linear factors in $\mathbb{F}[x]$. Then A is simple if and only if $a(\lambda) = g(\lambda)$ for each eigenvalue λ of A.*

Proof: Let A have k distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$.

Suppose A is simple. Then $\sum_{i=1}^{k} g(\lambda_i) = n$. By Theorem 5.1.21, we have $n \geq \sum_{i=1}^{k} a(\lambda_i) \geq \sum_{i=1}^{k} g(\lambda_i) = n$. Then the inequalities become equalities and hence $a(\lambda_i) = g(\lambda_i)$ for all i.

Conversely, if $k = 1$, then $a(\lambda_1) = n = g(\lambda_1)$. By definition A is simple. So we assume $k \geq 2$. We only prove the case for $k = 2$. For the general case the proof is just a slight modification of the proof for $k = 2$.

Since $k = 2$, $C(x) = (\lambda_1 - x)^r(\lambda_2 - x)^s$, where $r + s = n$. By assumption $g(\lambda_1) = r$ and $g(\lambda_2) = s$. Then there are two bases $\{\alpha_1, \ldots, \alpha_r\}$ and $\{\beta_1, \ldots, \beta_s\}$ for $\mathscr{E}(\lambda_1)$ and $\mathscr{E}(\lambda_2)$, respectively. We shall show that $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ is a basis of $\mathbb{F}^n$. It suffices to show that this set is linearly independent.

Suppose $(a_1\alpha_1 + \cdots + a_r\alpha_r) + (b_1\beta_1 + \cdots + b_s\beta_s) = \mathbf{0}$. Since $\alpha = (a_1\alpha_1 + \cdots + a_r\alpha_r) \in \mathscr{E}(\lambda_1)$ and $\beta = (b_1\beta_1 + \cdots + b_s\beta_s) \in \mathscr{E}(\lambda_2)$. By Theorem 5.3.1, α and β are linearly independent if they are eigenvectors of A. Since $\alpha + \beta = \mathbf{0}$, either α or β is not an eigenvector of A. Without loss of generality, we may assume α is not an eigenvector of A. Since $\alpha \in \mathscr{E}(\lambda_1)$, $\alpha = \mathbf{0}$. Hence $\beta = \mathbf{0}$. By the linear independence of basis we have $a_i = 0$ and $b_j = 0$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. Hence A is simple. □

Corollary 5.3.7 *Suppose $A \in M_n(\mathbb{F})$ has k distinct eigenvalues $\lambda_1, \ldots, \lambda_k$. Then A is diagonalizable over $\mathbb{F}$ if and only if $\sum_{i=1}^{k} g(\lambda_i) = n$.*

Corollary 5.3.8 *Suppose $A \in M_n(\mathbb{F})$ has n distinct eigenvalues. Then A is diagonalizable over $\mathbb{F}$.*

Example 5.3.9 Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in M_n(\mathbb{F})$. Then $C(x) = x^3$. So 0 is the only eigenvalue of A and $a(0) = 3$. Since $\text{rank}(A) = 2$, $\text{nullity}(A) = 1$. This means that $g(0) = 1$. Then A is defective. □

Theorem 5.3.6 provides us a condition on the algebraic and geometric multiplicities which is a necessary and sufficient condition for diagonalization of matrices. Following we shall show a condition on a minimum polynomial which is also a necessary and sufficient condition for diagonalization of matrices.

Theorem 5.3.10 (**Second Test for Diagonalizability**) *$A \in M_n(\mathbb{F})$ is diagonalizable over $\mathbb{F}$ if and only if the (monic) minimum polynomial of A has the form*

$$m(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_p),$$

where $\lambda_1, \lambda_2, \ldots, \lambda_p$ are distinct scalars (eigenvalues of A).

Proof: Suppose A is diagonalizable. Then A is similar to a diagonal matrix D. By Proposition 5.2.7, A and D have the same minimum polynomial, say $m(x)$. Also by Lemma 5.1.19, they have the same characteristic polynomial $C(x)$.

Suppose

$$D = \begin{pmatrix} \lambda_1 I_{k_1} & O & \cdots & O \\ O & \lambda_2 I_{k_2} & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & \lambda_p I_{k_p} \end{pmatrix},$$

where $\lambda_1, \lambda_2, \ldots, \lambda_p$ are distinct and $k_1 + k_2 + \cdots + k_p = n$. Then

$$C(x) = (-1)^n (x - \lambda_1)^{k_1} (x - \lambda_2)^{k_2} \cdots (x - \lambda_p)^{k_p}.$$

Let $g(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_p)$. By Theorem 5.2.9, $g(x) | m(x)$.

Since

$$g(D) = \begin{pmatrix} O & O & \cdots & O \\ O & (\lambda_2 - \lambda_1) I_{k_2} & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & (\lambda_p - \lambda_1) I_{k_p} \end{pmatrix} \begin{pmatrix} (\lambda_1 - \lambda_2) I_{k_1} & O & \cdots & O \\ O & O & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & (\lambda_p - \lambda_2) I_{k_p} \end{pmatrix}$$
$$\cdots \begin{pmatrix} (\lambda_1 - \lambda_p) I_{k_1} & O & \cdots & O \\ O & (\lambda_2 - \lambda_p) I_{k_2} & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & O \end{pmatrix} = O,$$

by Theorem 5.2.5 we have $m(x) | g(x)$. Since m and g are monic, $m(x) = g(x)$.

The converse will be proved in Chapter 8. □

Exercise 5.3

5.3-1. Complete the proof of Theorem 5.3.6.

5.3-2. Show that A is diagonalizable if and only if A^T is diagonalizable.

5.3-3. Let $A \in M_n(\mathbb{R})$ with eigenvalues $1, 2, \ldots, n$. Compute $\det(A + I)$.

5.3-4. Let $A_N \in M_{m,n}(\mathbb{R})$ for $N \geq 0$. The sequence of matrices $\{A_N\}$ is called *convergent* if for each pair (h, k) the sequence $\{(A_N)_{h,k}\}$ is convergent. The series of matrices $\sum_{i=0}^{\infty} A_i$ is called *convergent* if the sequence of the partial sums $\{\sum_{i=0}^{N} A_i\}$ is convergent. Let $A \in M_n(\mathbb{R})$. Show that $\sum_{i=0}^{\infty} \frac{1}{i!} A^i$ is convergent. The limit of this series is denoted by e^A. [Hint: Let $m = \max_{1 \leq h,k \leq n} \{|(A)_{h,k}|\}$. Show that each entry of A^i is less than or equal to $n^{i-1} m^i$ for $i \geq 1$.]

5.3-5. Let $A = \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ 1 & 0 & 1 \\ 0 & \frac{1}{2} & 0 \end{pmatrix}$

(a) Diagonalize A.

(b) Show that $A^{2n+1} = A$.

(c) Compute e^A.

5.3-6. The Fibonacci sequence is given by $F_0 = 1$, $F_1 = 1$, for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Find the general formula for F_n, i.e., a formula in terms of n. [Hint: Find a matrix A such that $\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = A^n \begin{pmatrix} F_1 \\ F_0 \end{pmatrix}$ for $n \geq 0$.]

5.3-7. Suppose $P \in M_n(\mathbb{F})$. P is called *idempotent* if $P^2 = P$. Show that

(a) $g(0) = \text{nullity}(P)$ and $g(1) = \text{nullity}(I - P)$.

(b) The column space $C(I - P)$ of $I - P$ is equal to the null space $\text{null}(P)$ of P.

5.3-8. Suppose $A \in M_n(\mathbb{F})$. A is called *involutory* if $A^2 = I$. Show that if P is idempotent, then $2P - I$ is involutory. Use this fact to prove that any involutory is diagonalizable.

5.4 Definite Matrices

Real symmetric matrices are the most frequently used matrices in real-world applications. For example, suppose that f is a real-valued function defined on $\mathbb{R}^3$ with continuous second-order partial derivatives. Then the Hessian of f at a point $\boldsymbol{p}$ is

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{pmatrix},$$

where $f_{ij} = \dfrac{\partial^2 f}{\partial x_i \partial x_j}(\boldsymbol{p})$. At a critical point, f has a relative minimum at $\boldsymbol{p}$ if the Hessian of f is positive definite in the sense defined below.

In this section, we assume that all matrices are real. Some properties about definite matrices will be stated in this section without proof. The proofs and the general discussions can be found in Chapters 9 and 10.

Definition 5.4.1 Let A be a symmetric (square) matrix over $\mathbb{R}$ of size n. A is said to be *positive definite* and *non-negative definite* (or *positive semi-definite*) if $X^TAX > 0$ and $X^TAX \geq 0$ respectively, for every nonzero vector $X \in \mathbb{R}^{n\times 1}$. Similarly, A is said to be *negative definite* and *non-positive definite* (or *negative semi-definite*) if $X^TAX < 0$ and $X^TAX \leq 0$ respectively, for every nonzero vector $X \in \mathbb{R}^{n\times 1}$.

Example 5.4.2 Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Then for any nonzero vector $X = \begin{pmatrix} x \\ y \end{pmatrix}$, $X^TAX = x^2 + 2y^2$. It is easy to see that $X^TAX > 0$. Hence A is positive definite.

Let $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Then for any nonzero vector $X = \begin{pmatrix} x \\ y \end{pmatrix}$, $X^TAX = x^2 \geq 0$. This value may be 0. For example, $(0,1)B \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$. Hence B is non-negative definite. □

Suppose A is negative definite. Then $-A$ is positive definite. So we only consider positive definite matrices.

Proposition 5.4.3 *Suppose A is positive definite. Then $(A)_{i,i} > 0$ for all i.*

Proof: The proposition follows from $(A)_{i,i} = \boldsymbol{e}_i^T A \boldsymbol{e}_i$. □

Proposition 5.4.4 *If a symmetric matrix A is positive definite, then $P^T AP$ is positive definite for every invertible matrix P.*

Proof: If $\boldsymbol{x} \neq \boldsymbol{0}$, then so is $P\boldsymbol{x}$, and we have $\boldsymbol{x}^T P^T AP\boldsymbol{x} = (P\boldsymbol{x})^T A(P\boldsymbol{x}) > 0$. □

Proposition 5.4.5 *Let A be a symmetric matrix. If $P^T AP$ is positive definite for some invertible matrix P, then A is positive definite.*

Proof: If $P^T AP$ is positive definite, then by Proposition 5.4.4 , $(P^{-1})^T (P^T AP)P^{-1} = A$ is positive definite. □

Corollary 5.4.6 *Let $A = \mathrm{diag}\{d_1, d_2, \ldots, d_n\}$. All d_i's are positive if and only if $P^T AP$ is positive definite for all invertible (real) matrices P.*

The following theorem is a special case of Corollary 9.4.17 in Chapter 9.

Theorem 5.4.7 *For any symmetric matrix A, there is an invertible matrix P such that $P^T AP$ is diagonal.*

Proof: We prove this theorem by mathematical induction on the order of A. Suppose A is a matrix of order 1. Then the theorem clearly holds. Suppose the theorem holds for any symmetric matrix of order $n-1$, where $n \geq 2$. Suppose $A = (a_{ij})$ is a symmetric matrix of order n.

Case 1: Suppose $a_{11} \neq 0$. Let

$$P_1 = \left(\begin{array}{c|ccc} 1 & c_2 & \cdots & c_n \\ \hline 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{array}\right),$$

where $c_i = -(a_{11})^{-1} a_{i1} = -(a_{11})^{-1} a_{1i}$, $2 \leq i \leq n$. Then

$$P_1^T AP_1 = \left(\begin{array}{c|ccc} a_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right), \tag{5.2}$$

for some symmetric matrix B of order $n-1$. By induction assumption, there is an invertible matrix P_2 of order $n-1$ such that $P_2^T BP_2$ is a diagonal matrix. Let $P = P_1 \begin{pmatrix} 1 & \boldsymbol{0}_{n-1}^T \\ \boldsymbol{0}_{n-1} & P_2 \end{pmatrix}$. Then $P^T AP$ is a diagonal matrix.

Case 2: Suppose $a_{11} = 0$ and $a_{ii} \neq 0$ for some $i \geq 2$. Let $Q = I_n - E^{1,1} - E^{i,i} + E^{1,i} + E^{i,1}$. Then the $(1,1)$-st entry of $Q^T AQ$ is a_{ii}. This case is reduced to Case 1.

Case 3: Suppose $a_{ii} = 0$ for all i. Suppose $a_{1j} = 0$ for all j. Then A is of the form in (5.2) with $a_{11} = 0$. By the same argument in Case 1, the theorem holds. Suppose $a_{1j} \neq 0$ for some $j \geq 2$. Let $Q = I_n + E^{j,1}$. Then the $(1,1)$-st entry of $Q^T AQ$ is $2a_{1j} \neq 0$. This case is reduced to Case 1. □

Example 5.4.8 Let $A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & -1 \\ 2 & -1 & 0 \end{pmatrix} = (a_{ij})$. Since $a_{11} = 0$, we let $Q = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then $A_1 = Q^T AQ = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 0 & 2 \\ -1 & 2 & 0 \end{pmatrix}$. Let $P_1 = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then $P_1^T A_1 P_1 = (QP_1)^T A(QP_1) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & -1 & 3 \\ 0 & 3 & -1 \end{array}\right)$. Consider the submatrix $B = \begin{pmatrix} -1 & 3 \\ 3 & -1 \end{pmatrix}$. Applying the method again, we let $R = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$. Then $R^T BR = \begin{pmatrix} -1 & 0 \\ 0 & 8 \end{pmatrix}$. Hence $P_2 = R$ and $P = QP_1 \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 3 \\ 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{c|cc} 0 & 1 & 3 \\ \hline -1 & -1 & 2 \\ 0 & 0 & 1 \end{array}\right)$. Then $P^T AP = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & -1 & 0 \\ 0 & 0 & 8 \end{array}\right)$. □

Remark 5.4.9 Suppose there is an invertible matrix P such that $P^T AP = D = \text{diag}\{d_1, d_2, \ldots, d_n\}$. The diagonal matrix D is not unique up to rearranging the entries of the main diagonal. It is because we can let $Q = \text{diag}\{q_1, q_2, \ldots, q_n\}$ for some $q_i \in \mathbb{R}$. Then $(PQ)^T APQ = \text{diag}\{d_1 q_1^2, d_2 q_2^2, \ldots, d_n q_n^2\}$.

Two square matrices A and B are called *congruent* if there is an invertible matrix P such that $B = P^T AP$.

Recall that two square matrices A and B are called similar if there is an invertible matrix P such that $B = P^{-1}AP$. It is also known that two similar matrices have the same list of eigenvalues (including the algebraic and geometric multiplicities).

Since P^T is not in general P^{-1},

the concepts of congruence and similarity are different.

However there are some very special P, that is

Definition 5.4.10 P is called an *orthogonal matrix* if $P^T = P^{-1}$, i.e., $P^T P = I = PP^T$.

The following theorem is a part of Theorem 10.5.20 in Chapter 10.

Theorem 5.4.11 *Suppose $A \in M_n(\mathbb{R})$ and is symmetric. Then there is an orthogonal matrix P such that $P^T AP$ is a diagonal matrix.*

Remark 5.4.12 Suppose $P^T AP = \text{diag}\{\lambda_1, \ldots, \lambda_n\}$. Since $P^T = P^{-1}$, according to Theorem 5.4.11, all the λ's are eigenvalues of A.

It is easy to get the following result (see Theorem 10.5.28).

Theorem 5.4.13 *Suppose $A \in M_n(\mathbb{R})$ and is symmetric. Then*

(1) A is positive definite if and only if all the eigenvalues of A are positive.

(2) A is non-negative definite if and only if all the eigenvalues of A are non-negative.

For a given symmetric real matrix A, we shall learn in Chapter 10 how to find an orthogonal matrix P such that P^TAP is diagonal.

Exercise 5.4

5.4-1. Find an invertible matrix P such that P^TAP is a diagonal matrix, where A is:

(a) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; (b) $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$; (c) $\begin{pmatrix} 3 & 1 & 2 \\ 1 & 4 & 0 \\ 2 & 0 & -1 \end{pmatrix}$.

5.4-2. Suppose A is a positive definite matrix. Prove that there is an invertible upper triangular matrix P such that P^TAP is diagonal.

Chapter 6

Vector Spaces

6.1 Definition and Some Basic Properties

In Chapter 3, we have learnt some properties of vector space of $\mathbb{F}^n$. In this chapter, we shall consider the concept of vector space in general. Now let us give a definition of a general vector space.

Definition 6.1.1 Let $\mathbb{F}$ be a field. A *vector space V over $\mathbb{F}$* is a non-empty set with two laws of combination called *vector addition* "+" (or simply addition) and *scalar multiplication* "$\cdot$" satisfying the following axioms:

(V1) $+ : V \times V \to V$ is a mapping and $+(\alpha, \beta)$ written by $\alpha + \beta$ is called the *sum* of α and β.

(V2) $+$ is associative.

(V3) $+$ is commutative.

(V4) There is an element, denoted by $\mathbf{0}$, such that $\alpha + \mathbf{0} = \alpha$ for all $\alpha \in V$. Note that such vector is unique (see Exercise 6.1-3). It is called the *zero vector* of V.

(V5) For each $\alpha \in V$ there is an element in V, denoted by $-\alpha$ such that $\alpha + (-\alpha) = \mathbf{0}$.

(V6) $\cdot : \mathbb{F} \times V \to V$ is a mapping which associates $a \in \mathbb{F}$ and $\alpha \in V$ a unique element denoted by $a \cdot \alpha$ or simply $a\alpha$ in V. This mapping is called the *scalar multiplication*.

(V7) Scalar multiplication is associative, i.e., $a(b\alpha) = (ab)\alpha$ for all $a, b \in \mathbb{F}$, $\alpha \in V$.

(V8) Scalar multiplication is distributive with respect to $+$, i.e., $a(\alpha + \beta) = a\alpha + a\beta$ for all $a \in \mathbb{F}$, $\alpha, \beta \in V$.

(V9) For each $a, b \in \mathbb{F}$, $\alpha \in V$, $(a + b)\alpha = a\alpha + b\alpha$.

(V10) For each $\alpha \in V$, $1 \cdot \alpha = \alpha$, where 1 is the unity of $\mathbb{F}$.

Elements of V and $\mathbb{F}$ are called *vectors* and *scalars*, respectively. In this book, vectors are often denoted by lower case Greek letters $\alpha, \beta, \gamma, \ldots$ and scalars are often denoted by lower case Latin letters $a, b, c, \ldots$.

Mathematical statements often contain quantifiers "$\forall$" and "$\exists$". The quantifier "$\forall$" is read "for each", "for every" or "for all" and the quantifier "$\exists$" is read "there exists", "there is" or "for some".

Lemma 6.1.2 (Cancellation Law) *Suppose α, β and γ are vectors in a vector space. If $\alpha + \beta = \alpha + \gamma$, then $\beta = \gamma$.*

Proof: By (V1), we have $-\alpha+(\alpha+\beta) = -\alpha+(\alpha+\gamma)$. By (V2), we have $(-\alpha+\alpha)+\beta = (-\alpha+\alpha)+\gamma$. By (V3), (V5) and (V4) we have the lemma. □

Corollary 6.1.3 *Suppose α and β are vectors in a vector space. If $\alpha + \beta = \alpha$, then $\beta = \mathbf{0}$.*

Proof: Since $\alpha + \beta = \alpha = \alpha + \mathbf{0}$, by Lemma 6.1.2 we have the corollary. □

Proposition 6.1.4 *Let V be a vector space over $\mathbb{F}$. We have*

(a) $\forall \alpha \in V$, $0\alpha = \mathbf{0}$.

(b) $\forall \alpha \in V$, $(-1)\alpha = -\alpha$.

(c) $\forall a \in \mathbb{F}$, $a\mathbf{0} = \mathbf{0}$.

Proof: By (V6) we know that $0\alpha \in V$. By (V9) we have $0\alpha = (0+0)\alpha = 0\alpha + 0\alpha$. By Corollary 6.1.3 we have (a).

By (V9), (V10) and (a) we have $(-1)\alpha + \alpha = [(-1) + 1]\alpha = 0\alpha = \mathbf{0}$. By the uniqueness of the inverse (see Exercise 6.1-4), we have $(-1)\alpha = -\alpha$.

By (V4) and (V8) we have $a\mathbf{0} = a(\mathbf{0} + \mathbf{0}) = a\mathbf{0} + a\mathbf{0}$. By Corollary 6.1.3 we have (c). □

The followings are examples of vector spaces. $\mathbb{F}$ is assumed to be a field. Reader can easily define $+$ and $\cdot$ and check that they satisfy all the axioms of vector space.

1. Let 0 be the zero of $\mathbb{F}$. Then $\{0\}$ is a vector space over $\mathbb{F}$.

2. Let $n \in \mathbb{N}$. $\mathbb{F}^n$ is a vector space over $\mathbb{F}$. In particular, $\mathbb{F}$ is a vector space over $\mathbb{F}$. $\mathbb{R}^n$ is a vector space over $\mathbb{R}$.

3. Let $m, n \in \mathbb{N}$. The set $M_{m,n}(\mathbb{F})$ is a vector space over $\mathbb{F}$ under the usual addition and scalar multiplication.

4. Let S be a non-empty set. Let V be the set of all functions from S into $\mathbb{F}$. For $f, g \in V$, $f + g$ is defined by the formula $(f + g)(a) = f(a) + g(a)\ \forall a \in S$. Also for $c \in \mathbb{F}$, cf is defined by $(cf)(a) = cf(a)\ \forall a \in S$. Then V is a vector space over $\mathbb{F}$.

5. Suppose $\mathscr{I}$ is an interval of $\mathbb{R}$. Let $C^0(\mathscr{I})$ be the set of all continuous real valued functions defined on $\mathscr{I}$. Then $C^0(\mathscr{I})$ is a vector space over $\mathbb{R}$.

6. Let $L[a, b]$ be the set of all integrable real valued functions defined on the closed interval $[a, b]$. Then $L[a, b]$ is a vector space over $\mathbb{R}$.

7. Recall that $\mathbb{F}[x]$ is the set of all polynomials in the indeterminate x over $\mathbb{F}$. Under the usual addition and scalar multiplication of polynomials, $\mathbb{F}[x]$ is a vector space over $\mathbb{F}$.

8. For $n \in \mathbb{N}$, let $P_n(\mathbb{F})$ be the subset of $\mathbb{F}[x]$ consisting of all polynomials in x of degree less than n (of course, together with the zero polynomial). Then $P_n(\mathbb{F})$ is a vector space over $\mathbb{F}$ with the same addition and scalar multiplication as in $\mathbb{F}[x]$ defined in the previous example. Namely, $P_n(\mathbb{F})$ can be written as $\left\{ \sum_{i=0}^{n-1} a_i x^i \;\middle|\; a_i \in \mathbb{F} \right\}$.

Exercise 6.1

6.1-1. Let α be any vector of a vector space. Prove that $\alpha + (-\alpha) = (-\alpha) + \alpha$ without using the commutative law (V3).

6.1-2. Let α be any vector of a vector space. Prove that $\mathbf{0} + \alpha = \alpha$ without using the commutative law (V3).

6.1-3. Prove that zero vector $\mathbf{0}$ of a vector space V is unique, i.e., if $\mathbf{0'}$ is an element in V such that $\alpha + \mathbf{0'} = \alpha$ for all $\alpha \in V$, then $\mathbf{0'} = \mathbf{0}$.

6.1-4. Prove that for each $\alpha \in V$, $-\alpha$ is unique, i.e., if $\beta \in V$ such that $\alpha + \beta = \mathbf{0}$, then $\beta = -\alpha$.

6.1-5. Determine whether or not the following are vector spaces over $\mathbb{R}$.

(a) The set of polynomials in $P_9(\mathbb{R})$ of even degree together with the zero polynomial.

(b) The set of polynomials in $P_4(\mathbb{R})$ with at least one real root.

(c) The set of all even real-valued functions defined on $[-1, 1]$.

6.1-6. Show that the set of solutions of differential equation $\dfrac{d^2y}{dx^2} + y = 0$ is a vector space over $\mathbb{R}$.

6.1-7. Show that $\mathbb{C}$ can be considered as a vector over $\mathbb{R}$. Also show that $\mathbb{R}$ can be considered as a vector space over $\mathbb{Q}$. Can $\mathbb{R}$ be a vector space over $\mathbb{C}$? Justify you answer.

6.1-8. Let V be any plane through the origin in $\mathbb{R}^3$. Show that points in V form a vector space under the standard addition and scalar multiplication of vectors in $\mathbb{R}^3$.

6.1-9. Let $V = \mathbb{R}^2$. Define scalar multiplication and addition on V by

$$c(x, y) = (cx, cy), \quad (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, 0),$$

where $c \in \mathbb{R}$. Is V a vector space over $\mathbb{R}$? Justify your answer.

6.1-10. Let $V = \mathbb{R}$. Define addition, denoted by $\oplus$, by $x \oplus y = \max\{x, y\}$ and scalar multiplication $c \cdot x = cx$, the usual multiplication of real numbers. Is V a vector space over $\mathbb{R}$? Justify!

6.1-11. Let V denote the set of all infinite sequences of real numbers. Define addition and scalar multiplication by

$$\{a_n\}_{n=1}^{\infty} + \{b_n\}_{n=1}^{\infty} = \{a_n + b_n\}_{n=1}^{\infty}, \quad c\{a_n\}_{n=1}^{\infty} = \{ca_n\}_{n=1}^{\infty}, \forall c \in \mathbb{R}.$$

Show that V is a vector space over $\mathbb{R}$.

6.1-12. Suppose W be the set of all convergent sequences of real numbers. Define addition and scalar multiplication as Exercise 6.1-11. Is W still a vector space over $\mathbb{R}$?

6.1-13. Let V be a vector space over $\mathbb{F}$.

(a) Show that if $a \in \mathbb{F}$, $a \neq 0$, $\alpha \in V$ and $a\alpha = \mathbf{0}$, then $\alpha = \mathbf{0}$.

(b) Show that if $a \in \mathbb{F}$, $\alpha \in V$, $\alpha \neq \mathbf{0}$, and $a\alpha = \mathbf{0}$, then $a = 0$.

6.2 Linear Dependence and Linear Independence

We have learnt the concept of linear combination and linear independence in Chapter 3. This concept can be extended in any vector space.

Definition 6.2.1 Let V be a vector space over $\mathbb{F}$. Suppose $\alpha_1, \alpha_2, \ldots, \alpha_n$ and β are vectors in V. β is said to be a *linear combination* of $\alpha_1, \alpha_2, \ldots, \alpha_n$ if there are scalars $a_1, a_2, \ldots, a_n$ such that $\beta = \sum_{i=0}^{n} a_i \alpha_i$. We also say that β is *linearly dependent on* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

By the above definition, $\mathbf{0}$ is always a linear combination of a set of vectors $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a vector space, since we can choose $a_i = 0$ for all $1 \leq i \leq n$.

Definition 6.2.2 Vectors $\alpha_1, \alpha_2, \ldots, \alpha_n$ are *linearly dependent over* $\mathbb{F}$ if there exist $a_1, a_2, \ldots, a_n$ in $\mathbb{F}$ not all zero such that $\sum_{i=0}^{n} a_i \alpha_i = \mathbf{0}$. Vectors $\alpha_1, \alpha_2, \ldots, \alpha_n$ are not linearly dependent over $\mathbb{F}$ is called *linearly independent over* $\mathbb{F}$. This is equivalent to the following statement:

$$\text{If } \sum_{i=0}^{n} a_i \alpha_i = \mathbf{0} \text{ for some } a_i \in \mathbb{F}, \text{ then } a_i = 0 \text{ for all } i.$$

A set $S \subseteq V$, where V is a vector space over $\mathbb{F}$, is said to be *linearly dependent* if there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in S$ such that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly dependent over $\mathbb{F}$. A set is said to be *linearly independent* if it is not linearly dependent.

Remark 6.2.3 Let V be a vector over a field $\mathbb{F}$.

1. Let S be a subset of V. If $\mathbf{0} \in S$, then S is linearly dependent.
2. For $\alpha \in V$ and $\alpha \neq \mathbf{0}$, the set $\{\alpha\}$ is linearly independent.
3. The empty set $\varnothing$ is always linearly independent.
4. Any set containing a linearly dependent subset is linearly dependent.
5. Any subset of a linearly independent set is linearly independent.

Examples 6.2.4

1. The set $\{1, x, x^2, x^2 + x + 1, x^3\}$ is linearly dependent in the vector space $\mathbb{F}[x]$ over $\mathbb{F}$.
2. The set $\{1, x, x^2, x^3\}$ is linearly independent in $\mathbb{F}[x]$ over $\mathbb{F}$.
3. In general, the set of monomials $\{1, x, x^2, x^3, \ldots\}$ is linearly independent in $\mathbb{F}[x]$ over $\mathbb{F}$. □

Theorem 6.2.5 *If α is linearly dependent on $\{\beta_1, \ldots, \beta_n\}$ and each β_i is linearly dependent on $\{\gamma_1, \ldots, \gamma_m\}$, then α is linearly dependent on $\{\gamma_1, \ldots, \gamma_m\}$.*

Proof: From the definition we have $\alpha = \sum_{i=1}^{n} a_i \beta_i$ and $\beta_i = \sum_{j=1}^{m} c_{ij} \gamma_j$ for some scalars a_i's and c_{ij}'s. Then

$$\alpha = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{m} c_{ij} \gamma_j \right) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_i c_{ij} \right) \gamma_j.$$

□

Theorem 6.2.6 *A set of non-zero vectors $\{\alpha_1, \ldots, \alpha_n\}$ is linearly dependent if and only if there is a vector α_k that is a linear combination of $\alpha_1, \alpha_2, \ldots, \alpha_j$ with $j < k$.*

Proof: Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is linearly dependent. Then $\exists a_1, \ldots, a_n \in \mathbb{F}$ not all zero such that $\sum_{i=1}^{n} a_i\alpha_i = \mathbf{0}$. Suppose k is the largest index such that $a_k \neq 0$. Clearly $k \geq 2$ (since $\alpha_1 \neq \mathbf{0}$). Thus

$$\alpha_k = -a_k^{-1}\left(\sum_{i=1}^{k-1} a_i\alpha_i\right) = \sum_{i=1}^{k-1}(-a_k^{-1}a_i)\alpha_i.$$

The converse is trivial. □

We rewrite the contrapositive of Theorem 6.2.6 below.

Theorem 6.2.7 *A set of non-zero vectors $\{\alpha_1, \ldots, \alpha_n\}$ is linearly independent if and only if for each k $(2 \leq k \leq n)$, α_k is not a linear combination of $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$.*

Exercise 6.2

6.2-1. For which values of λ do the vectors $(\lambda, -1, -1)$, $(-1, \lambda, -1)$, $(-1, -1, \lambda)$ form a linearly dependent set in $\mathbb{R}^3$?

6.2-2. Let $\alpha_1, \alpha_2, \alpha_3$ be linearly independent vectors. Suppose $\beta_1 = \alpha_1 + \alpha_2 + \alpha_3$, $\beta_2 = \alpha_1 + a\alpha_2$, $\beta_3 = \alpha_1 + b\alpha_3$. Find condition that must be satisfied by a, b in order that β_1, β_2 and β_3 are linearly independent.

6.2-3. Regarding $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Show that $\{1, \sqrt{2}, \sqrt{3}\}$ is linearly independent.

6.2-4. Let $C^0[a, b]$ be the space of all real continuous functions defined on the closed interval $[a, b]$.

(a) Show that $\sin x, \sin 2x, \sin 3x$ are linearly independent (over $\mathbb{R}$) in $C^0[0, 2\pi]$.

(b) Show that $2x$ and $|x|$ are linearly independent in $C^0[-1, 1]$.

(c) Show that $2x$ and $|x|$ are linearly dependent in $C^0[0, 1]$.

(d) Show that $e^x, e^{2x}, \ldots, e^{nx}$ are linearly independent in $C^0[0, 1]$.

6.2-5. Are the matrices A, B and C linearly independent? Here

$$A = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

6.2-6. Are the functions x, e^x, xe^x, $(2 - 3x)e^x$ linearly independent in $C^0(\mathbb{R})$ (over $\mathbb{R}$)?

6.2-7. Show that if $\{\alpha_1, \ldots, \alpha_n\}$ is linearly independent over $\mathbb{F}$ and if $\{\alpha_1, \ldots, \alpha_n, \beta\}$ is linearly dependent over $\mathbb{F}$, then β depends on $\alpha_1, \ldots, \alpha_n$.

6.2-8. Let V be a vector space over $\mathbb{R}$. Show that $\{\alpha,\ \beta,\ \gamma\}$ is linearly independent if and only if $\{\alpha + \beta,\ \beta + \gamma,\ \gamma + \alpha\}$ is linearly independent.

6.2-9. Given an example of three linearly dependent vectors in $\mathbb{R}^3$ such that any two of them are linearly independent.

6.2-10. Show that suppose $\alpha_1, \ldots, \alpha_n$ are linearly independent vectors and suppose $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ for some fixed scalars $a_1, \ldots, a_n$ in $\mathbb{F}$. Then the vectors $\alpha - \alpha_1, \alpha - \alpha_2, \ldots, \alpha - \alpha_n$ are linearly independent if and only if $a_1 + a_2 + \cdots + a_n \neq 1$.

6.2-11. Suppose $0 \leq \theta_1 < \theta_2 < \theta_3 < \frac{\pi}{2}$ are three constants. Let $f_i(x) = \sin(x + \theta_i)$, $i = 1, 2, 3$. Is $\{f_1, f_2, f_3\}$ linearly independent? Why?

6.2-12. Let $V \in \mathbb{R}[x]$. Let $f \in V$ be a polynomial of degree n. Is $\{f, f', f'', \ldots, f^{(n)}\}$ linearly independent? Justify! Here $f^{(k)}$ is the k-th derivative of f.

6.3 Subspaces

Definition 6.3.1 A *subspace* W of a vector space V is a non-empty subset of V which is itself a vector space with respect to the vector addition and scalar multiplication defined in V.

By the same proof of Lemma 3.2.4 we have the following lemma.

Lemma 6.3.2 *Suppose V is a vector space over $\mathbb{F}$ and W is a non-empty subset of V. The following statements are equivalent:*

(a) If $\alpha, \beta \in W$, then $a\alpha + b\beta \in W$ for any $a, b \in \mathbb{F}$.

(b) If $\alpha, \beta \in W$, then $a\alpha + \beta \in W$ for any $a \in \mathbb{F}$.

(c) If $\alpha, \beta \in W$, then $\alpha + \beta \in W$ and $a\alpha \in W$ for any $a \in \mathbb{F}$.

Proposition 6.3.3 *Suppose V is a vector space over $\mathbb{F}$ and W is a non-empty subset of V. Then W is a subspace of V if and only if for any $\alpha, \beta \in W$, $a \in \mathbb{F}$ we have $a\alpha + \beta \in W$.*

Proof: The only if part is trivial.

For the if part we have to check all the axioms of vector space. By Lemma 6.3.2, (V1) and (V6) hold. Since V is a vector space, axioms (V2), (V3), (V7), (V8), (V9) and (V10) hold automatically. Let $\alpha \in W$ (it exists since $W \neq \varnothing$). By Lemma 6.3.2, $0\alpha + 0\alpha = \mathbf{0} \in W$. Thus (V4) holds. For any $\alpha \in W$, since $\mathbf{0} \in W$, by the assumption $(-1)\alpha + \mathbf{0} = -\alpha \in W$. Thus (V5) holds. Therefore, W is a subspace of V. □

Examples 6.3.4

1. Let $V = \mathbb{R}^2$ and $W = \{(x, 0) \mid x \in \mathbb{R}\}$. Then W is a subspace of V.

2. The set $P_n(\mathbb{F})$ is a subspace of the vector space $\mathbb{F}[x]$ over $\mathbb{F}$.

3. $\mathbb{Q} \subset \mathbb{R}$ but $\mathbb{Q}$ is not a subspace of $\mathbb{R}$ over $\mathbb{R}$. It is because $\mathbb{Q}$ is not a vector space over $\mathbb{R}$. □

Theorem 6.3.5 *The intersection of any collection of subspaces is still a subspace.*

Proof: Let $\{W_\lambda \mid \lambda \in \Lambda\}$ be a collection of subspaces of a vector space V over $\mathbb{F}$. Let $W = \bigcap_{\lambda \in \Lambda} W_\lambda$. Since $\mathbf{0} \in W_\lambda$ for all $\lambda \in \Lambda$, $W \neq \varnothing$. $\forall \alpha, \beta \in W$, $a \in \mathbb{F}$, then $\alpha, \beta \in W_\lambda$, $\forall \lambda \in \Lambda$. Since W_λ is a subspace, $a\alpha + \beta \in W_\lambda$. Since it holds for each $\lambda \in \Lambda$, $a\alpha + \beta \in W$. Hence W is a subspace of V. □

Note that the union of two subspaces need not be a subspace. Can you provide an example?

From Chapter 3, we have learnt the concept about a spanning set of a vector space. In this chapter, we make a general definition of spanning set.

Definition 6.3.6 Let V be a vector space over $\mathbb{F}$. Suppose $S \subseteq V$. The *span of* S, denoted by $\text{span}(S)$, is defined as the intersection of all subspaces of V containing S. S is called a *spanning set of* $\text{span}(S)$.

By the above definition we have the following lemma.

Lemma 6.3.7 *Suppose $A \subseteq B \subseteq V$, where V is a vector space. Then* $\text{span}(A) \subseteq \text{span}(B)$.

For convenience, when S is a finite set, say $\{\alpha_1, \ldots, \alpha_n\}$, then we often write $\text{span}(S) = \text{span}\{\alpha_1, \ldots, \alpha_n\}$.

Remark 6.3.8 One can show that $\text{span}(S)$ is the smallest (with respect to set inclusion) subspace of V containing S. Hence if S is a subspace, then $\text{span}(S) = S$. Thus $\text{span}(\text{span}(A)) = \text{span}(A)$ for any subset A of V. Also, by the definition, $\text{span}(\varnothing) = \{\mathbf{0}\}$.

From Chapter 3, we know that if S is a finite set of a vector space, then $\text{span}(S)$ is the set of all linear combinations of vectors in S. Following we shall show that two definitions are consistent.

Theorem 6.3.9 *Let V be a vector space over $\mathbb{F}$. Suppose $\varnothing \neq S \subseteq V$. Then*

$$\text{span}(S) = \left\{ \sum_{i=1}^{n} a_i \alpha_i \;\middle|\; \alpha_i \in S, a_i \in \mathbb{F} \text{ and } n \in \mathbb{N} \right\}.$$

Proof: Let $U = \left\{ \sum_{i=1}^{n} a_i \alpha_i \;\middle|\; \alpha_i \in S, a_i \in \mathbb{F} \text{ and } n \in \mathbb{N} \right\}$. Clearly U is a subspace of V containing S. Since $\text{span}(S)$ is the smallest subspace of V containing S, $\text{span}(S) \subseteq U$.

On the other hand, suppose W is a subspace of V containing S. Then $\forall \alpha \in U$, $\alpha = \sum_{i=1}^{n} a_i \alpha_i$ for some $\alpha_i \in S$. Since $S \subseteq W$ and W is a subspace, $\alpha \in W$. Then we have $U \subseteq W$. In particular, $\text{span}(S) \supseteq U$. Hence we have the theorem. □

Lemma 6.3.10 *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a linearly independent set of a vector space V. Suppose $\alpha \in V \setminus \text{span}\{\alpha_1, \ldots, \alpha_n\}$. Then $\{\alpha_1, \ldots, \alpha_n, \alpha\}$ is linearly independent.*

Proof: By Theorem 6.2.7 α_k is not a linear combination of $\alpha_1, \ldots, \alpha_{k-1}$ for $2 \leq k \leq n$. Since $\alpha \notin \text{span}\{\alpha_1, \ldots, \alpha_n\}$, α is not a linear combination of $\alpha_1, \ldots, \alpha_n$. By Theorem 6.2.7 again $\{\alpha_1, \ldots, \alpha_n, \alpha\}$ is linearly independent. □

Theorem 6.3.11 *Let S be a subset of a vector space V over $\mathbb{F}$. If $\alpha \in S$ is linearly dependent on other vectors of S, then* $\text{span}(S) = \text{span}(S \setminus \{\alpha\})$.

Proof: By Lemma 6.3.7 we have $\text{span}(S \setminus \{\alpha\}) \subseteq \text{span}(S)$. On the other hand, since α is linearly dependent on other vectors of S, $\alpha = \sum_{i=1}^{n} a_i \alpha_i$ for some $\alpha_i \in S \setminus \{\alpha\}$, $a_i \in \mathbb{F}$ and $1 \leq i \leq n$. Hence $\alpha \in \text{span}(S \setminus \{\alpha\})$ and then $S \subseteq \text{span}(S \setminus \{\alpha\})$. By Remark 6.3.8, we have $\text{span}(S) \subseteq \text{span}(S \setminus \{\alpha\})$. This proves that $\text{span}(S) = \text{span}(S \setminus \{\alpha\})$. □

Exercise 6.3

6.3-1. Prove Lemma 6.3.7.

6.3-2. Let $C'[a,b]$ be the set of all real functions defined on $[a,b]$ and differentiable on (a,b). Let $C^1[a,b]$ be the subset of $C'[a,b]$ consisting of all continuously differentiable functions on (a,b). Show that $C'[a,b]$ is a subspace of $C^0[a,b]$ and $C^1[a,b]$ is a subspace of $C'[a,b]$.

6.3-3. Let $I[a,b]$ be the set of all integrable real functions defined on $[a,b]$. Show that $I[a,b]$ is a subspace of the space of all real functions defined on $[a,b]$.

6.3-4. Let V be the space of all 2×2 matrices. Let $S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$. What is $\text{span}(S)$?

6.3-5. $S = \{1 - x^2,\ x + 2,\ x^2\}$. Is $\text{span}(S) = P_3(\mathbb{R})$?

6.3-6. Let S_1 and S_2 be subsets of a vector space V. Assume that $S_1 \cap S_2 \neq \varnothing$. Is $\text{span}(S_1 \cap S_2) = \text{span}(S_1) \cap \text{span}(S_2)$?

6.4 Bases of Vector Spaces

Concept of basis was introduced in Chapter 3. In this section we shall study the properties of basis for a general vector space.

Definition 6.4.1 Let V be a vector space over $\mathbb{F}$. A subset $\mathscr{A}$ of V is said to be a *basis* of V if $\mathscr{A}$ is linearly independent over $\mathbb{F}$ and $\text{span}(\mathscr{A}) = V$.

Examples 6.4.2

1. We know that $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n\}$ is the standard basis of $\mathbb{F}^n$.
2. The vector space $P_n(\mathbb{F})$ has $\{1, x, \ldots, x^{n-1}\}$ as basis and is called the *standard basis* of $P_n(\mathbb{F})$.
3. The vector space $\mathbb{F}[x]$ has a basis $\{1, x, \ldots, x^k, \ldots\}$. This basis is called the *standard basis* of $\mathbb{F}[x]$.
4. Suppose W is a subspace of $\mathbb{F}^n$. The *standard basis* of W is a basis $\{\alpha_1, \ldots, \alpha_k\}$ of W so that the matrix $A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix}$ is in rref. □

By the same proof of Proposition 3.3.13 we have the following proposition and corollary.

Proposition 6.4.3 *Suppose $\alpha_1, \alpha_2, \ldots, \alpha_k$ are linearly independent vectors of a vector space over $\mathbb{F}$. If $\alpha = \sum_{i=1}^{k} a_i \alpha_i$ for some $a_1, a_2, \ldots, a_k \in \mathbb{F}$, then $a_1, a_2, \ldots, a_k$ are unique.*

Corollary 6.4.4 *Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis for a vector space V over $\mathbb{F}$. Then for every $\alpha \in V$ there exist unique scalars $a_1, \ldots, a_n \in \mathbb{F}$ such that $\alpha = \sum_{i=1}^{n} a_i \alpha_i$.*

Proposition 6.4.5 *Let $\mathscr{A}$ be a linearly independent set of a vector space. Suppose $\sum_{i=1}^{n} a_i\alpha_i = \sum_{j=1}^{m} b_j\beta_j$ for some distinct $\alpha_i \in \mathscr{A}$, some distinct $\beta_j \in \mathscr{A}$, and some non-zero scalars a_i, b_j. Then $n = m$ and $\{\alpha_1, \ldots, \alpha_n\} = \{\beta_1, \ldots, \beta_m\}$.*

Proof: We claim that $\{\alpha_1, \ldots, \alpha_n\} \cap \{\beta_1, \ldots, \beta_m\} \neq \varnothing$. For if not, then $\{\alpha_1, \ldots, \alpha_n\} \cup \{\beta_1, \ldots, \beta_m\} \subseteq \mathscr{A}$ is a linearly independent set. Then from $\sum_{i=1}^{n} a_i\alpha_i - \sum_{j=1}^{m} b_j\beta_j = \mathbf{0}$ we must have $a_i = 0$ and $b_j = 0$ for all i, j. This contradicts the assumption.

Thus $\{\alpha_1, \ldots, \alpha_n\} \cap \{\beta_1, \ldots, \beta_m\} \neq \varnothing$. After a suitable reordering we may assume that there exists a positive integer k, $1 \leq k \leq \min\{n, m\}$ such that $\alpha_i = \beta_i$ for $i = 1, \ldots, k$ and $\{\alpha_{k+1}, \ldots, \alpha_n\} \cap \{\beta_{k+1}, \ldots, \beta_m\} = \varnothing$. From the assumption we have

$$\sum_{i=1}^{k}(a_i - b_i)\alpha_i + \sum_{i=k+1}^{n} a_i\alpha_i - \sum_{j=k+1}^{m} b_j\beta_j = \mathbf{0}.$$

Since $\{\alpha_1, \ldots, \alpha_n, \beta_{k+1}, \ldots, \beta_m\} \subseteq \mathscr{A}$ is linearly independent, and all a_i's, b_j's are non-zero, we must have $a_i = b_i$ for $1 \leq i \leq k$ and $n \leq k$, $m \leq k$. Thus $n = m = k$. □

Theorem 6.4.6 (Steintz Replacement Theorem) *Let V be a vector space over $\mathbb{F}$. Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ spans V. Then every linearly independent set $\{\beta_1, \beta_2, \ldots, \beta_m\}$ contains at most n elements.*

Proof: Since $\beta_1 \in V$ and $V = \text{span}\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, $\beta_1 = \sum_{i=1}^{n} a_i\alpha_i$ for some $a_1, a_2, \ldots, a_n \in \mathbb{F}$. Since $\beta_1 \neq \mathbf{0}$, not all a_i can be zero. Without loss of generality, we may assume that $a_1 \neq 0$. Thus α_1 depends on $\{\beta_1, \alpha_2, \ldots, \alpha_n\}$. By Theorem 6.3.11 $V = \text{span}\{\beta_1, \alpha_2, \ldots, \alpha_n\}$.

Now as $\beta_2 \in V$, we have $\beta_2 = b_1\beta_1 + \sum_{i=2}^{n} c_i\alpha_i$ for some $b_1, c_2 \ldots, c_n \in \mathbb{F}$. Since β_1 and β_2 are linearly independent, at least one of c_i is non-zero. Again, we assume that $c_2 \neq 0$. Hence α_2 depends on $\{\beta_1,\ \beta_2,\ \alpha_3,\ \ldots,\ \alpha_n\}$. So by Theorem 6.3.11 $V = \text{span}\{\beta_1, \beta_2, \alpha_3, \ldots, \alpha_n\}$.

Continuing this process, at the k-th step ($k \leq n$) we have

$$V = \text{span}\{\beta_1, \beta_2, \ldots, \beta_k, \alpha_{k+1}, \ldots, \alpha_n\}.$$

So if $k < n$, then by the above argument $\{\beta_1, \beta_2, \ldots, \beta_k, \beta_{k+1}, \alpha_{k+1}, \ldots, \alpha_n\}$ is linearly dependent and so one of α_i, $i > k$, depends on the other vectors. After renumbering $\{\alpha_{k+1}, \ldots, \alpha_n\}$ if necessary, we may assume that it is α_{k+1}. Then we replace α_{k+1} by β_{k+1} and obtain that $V = \text{span}\{\beta_1, \beta_2, \ldots, \beta_k, \beta_{k+1}, \alpha_{k+2}, \ldots, \alpha_n\}$. Now if $n < m$, then the above process enables us to obtain a spanning set $\{\beta_1, \beta_2, \ldots, \beta_n\}$. But $\beta_{n+1} \in V$, so β_{n+1} depends on $\beta_1, \beta_2, \ldots, \beta_n$. This contradicts the fact that $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is linearly independent. Therefore, we have $m \leq n$. □

Corollary 6.4.7 *If a vector space has one basis with n elements, then all the other bases also have n elements.*

Due to the above corollary we can make the following definition.

Definition 6.4.8 A vector space V over $\mathbb{F}$ with a finite basis is called a *finite dimensional vector space* and the number of elements in a basis is called the *dimension* of V over $\mathbb{F}$ and is denoted by $\dim_{\mathbb{F}} V$ (or $\dim V$). V is called *infinite dimensional vector space* if V is not of finite dimension.

Examples 6.4.9

(a) $\dim_{\mathbb{F}} \mathbb{F}^n = n$.

(b) $\dim_{\mathbb{C}} \mathbb{C} = 1$ but $\dim_{\mathbb{R}} \mathbb{C} = 2$ with $\{1, i\}$ as a basis.

(c) $\dim_{\mathbb{F}} P_n(\mathbb{F}) = n$ and $\dim_{\mathbb{F}} \mathbb{F}[x] = \infty$.

(d) The vector space $\{\mathbf{0}\}$ has the empty set as a spanning set which is linearly independent and therefore $\varnothing$ is a basis of $\{\mathbf{0}\}$. Thus $\dim\{\mathbf{0}\} = 0$. □

By using the Steintz Replacement Theorem we have the following corollary.

Corollary 6.4.10 *Suppose $m > n$. Then any m vectors in an n-dimensional vector space must be linearly dependent.*

Theorem 6.4.11 *Let V be an n-dimensional vector space and $\mathscr{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a set of vectors in V. Then the following statements are equivalent:*

(a) $\mathscr{A}$ is a basis.

(b) $\mathscr{A}$ is linearly independent.

(c) $V = \text{span}(\mathscr{A})$.

Proof:

[(a)⇒(b)] Clear.

[(b)⇒(c)] If $\text{span}(\mathscr{A}) \neq V$, then there is an $\alpha \in V \setminus \text{span}(\mathscr{A})$. By Lemma 6.3.10 $\mathscr{A} \cup \{\alpha\}$ is linearly independent with $n+1$ elements. By Corollary 6.4.10 it is impossible.

[(c)⇒(a)] Suppose $V = \text{span}(\mathscr{A})$. We have to show that $\mathscr{A}$ is linearly independent. Suppose not, then by Theorem 6.2.6 some α_k depends on $\alpha_1, \ldots, \alpha_{k-1}$. Also by Theorem 6.3.11 $V = \text{span}\{\alpha_1, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_n\}$. By Theorem 6.4.6 $\dim V \leq n-1$. This is impossible. □

Corollary 6.4.12 *Suppose W_1 and W_2 are two subspaces of V. If $W_1 \subseteq W_2$ and $\dim W_1 = \dim W_2 < \infty$, then $W_1 = W_2$.*

Proof: Suppose $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of W_1. Then $\{\alpha_1, \ldots, \alpha_m\} \subset W_2$ is linearly independent. Since $\dim W_1 = \dim W_2$, by Theorem 6.4.11 it is also a basis of W_2. Therefore, $W_1 = W_2$. □

Note that two vector spaces having the same dimension may not be the same vector space. Here the condition that $W_1 \subseteq W_2$ is crucial.

Theorem 6.4.13 *In a finite dimensional vector space, every spanning set contains a basis.*

Proof: Let S be a spanning set of an n-dimensional vector space V. If $\dim V = 0$, then the empty set is a basis of V. If $V \neq \{\mathbf{0}\}$, then S must contain at least one non-zero vector, say α_1. If $\text{span}\{\alpha_1\} = V$, then $\{\alpha_1\}$ is a basis of V. If $\text{span}\{\alpha_1\} \neq V$, then there exists $\alpha_2 \in S \setminus \text{span}\{\alpha_1\}$. By Lemma 6.3.10 $\{\alpha_1, \alpha_2\}$ is linearly independent. If $\text{span}\{\alpha_1, \alpha_2\} = V$, then $\{\alpha_1, \alpha_2\}$ is already a basis. Otherwise, we continue the above process as long as we can. This process must stop as we cannot find more than n linearly independent vectors in S. □

Alternative proof: Let S be a spanning set of an n-dimensional vector space V. Let $\mathscr{A}$ be a maximal linearly independent subset of S, i.e., there is no linearly independent subset B of S such that $\mathscr{A} \subset B$ (such $\mathscr{A}$ must exist it is because by Theorem 6.4.6 every linearly independent subset of S containing at most n vectors). We shall show that $\mathscr{A}$ is a basis of V.

If $S \subseteq \text{span}(\mathscr{A})$, then by Lemma 6.3.7 we have $V = \text{span}(S) \subseteq \text{span}(\text{span}(\mathscr{A})) = \text{span}(\mathscr{A})$ and hence $\text{span}(\mathscr{A}) = V$. So $\mathscr{A}$ is a basis. If S is not a subset of $\text{span}(\mathscr{A})$, then let $\alpha \in S \setminus \text{span}(\mathscr{A})$. By Lemma 6.3.10 $\mathscr{A} \cup \{\alpha\}$ is linearly independent. This contradicts to the assumption that $\mathscr{A}$ is a maximal linearly independent subset of S. □

From Chapter 3 we know that we can extend a linearly independent set of $\mathbb{F}^n$ to a basis of $\mathbb{F}^n$. Following we shall extend this result to a general vector space.

Theorem 6.4.14 *In a finite dimensional vector space, any linearly independent set of vectors can be extended to a basis.*

Proof: Let $\{\beta_1, \ldots, \beta_m\}$ be a linearly independent set in an n-dimensional vector space V. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of V. Clearly $m \leq n$ and $\{\beta_1, \ldots, \beta_m, \alpha_1, \ldots, \alpha_n\}$ spans V. If $m = 0$, then there is nothing to prove. So we assume $m > 0$. Thus $\{\beta_1, \ldots, \beta_m, \alpha_1, \ldots, \alpha_n\}$ is linearly dependent. Then there are $b_1, \ldots, b_m, a_1, \ldots, a_n \in \mathbb{F}$ not all zero such that $\sum_{i=1}^{m} b_i\beta_i + \sum_{j=1}^{n} a_j\alpha_j = \mathbf{0}$. We claim that at least one $a_j \neq 0$. For otherwise, if all the a_j's are zero, then we have $\sum_{i=1}^{m} b_i\beta_i = \mathbf{0}$ and by the assumption, $b_1 = \cdots = b_m = 0$. This is impossible.

Thus by Theorem 6.3.11 $\{\beta_1, \ldots, \beta_m, \alpha_1, \ldots, \alpha_{j-1}, \ \alpha_{j+1}, \ldots \alpha_n\}$ still spans V. If $m > 1$, then this set is linearly dependent and we can apply the above argument to discard another α_j and still obtain a spanning set of V. We continue this process until we get n spanning vectors, m of which are $\beta_1, \ldots, \beta_m$. This is a required basis. □

Remark 6.4.15 From the proof above, we see that there are more than one way of extending a linearly independent set to a basis.

Let V be a finite dimensional vector space and let W be a subspace of V. What is the dimension of W? That means whether W contains a basis. Is there any relation between the dimension of W and the dimension of V? We shall answer these questions below.

Theorem 6.4.16 *A subspace W of an n-dimensional vector space V is a finite dimensional vector space of dimension at most n.*

Proof: If $W = \{\mathbf{0}\}$, then W is 0-dimensional.

Assume $W \neq \{\mathbf{0}\}$. Then there exists $\alpha_1 \in W$ with $\alpha_1 \neq \mathbf{0}$. If $\text{span}\{\alpha_1\} = W$, then W is 1-dimensional. Otherwise, choose $\alpha_2 \in W \setminus \text{span}\{\alpha_1\}$. By Lemma 6.3.10 $\{\alpha_1, \alpha_2\}$ is linearly independent. Continuing in this fashion, after k steps, we have a linearly independent set $\{\alpha_1, \ldots, \alpha_k\}$ and $\text{span}\{\alpha_1, \ldots, \alpha_k\} \neq W$. Choose $\alpha_{k+1} \in W \setminus \text{span}\{\alpha_1, \ldots, \alpha_k\}$. By Lemma 6.3.10 $\{\alpha_1, \ldots, \alpha_k, \alpha_{k+1}\}$ is linearly independent.

This process cannot go on infinitely, for otherwise we would obtain more than n linearly independent vectors in V. Hence there must be an integer m such that $\text{span}\{\alpha_1, \ldots, \alpha_m\} = W$. Thus $\dim W = m$ and clearly $m \leq n$. □

Theorem 6.4.17 *Let W be a subspace of V with a basis $\mathscr{B} = \{\alpha_1, \ldots, \alpha_m\}$. Assume that $\dim V = n$. Then there exists a basis $\mathscr{B} \cup \{\alpha_{m+1}, \ldots, \alpha_n\}$ of V for some vectors $\alpha_{m+1}, \ldots, \alpha_n$ in V.*

Proof: This follows from Theorem 6.4.14. □

Remark 6.4.18 Every infinite dimensional vector space also has a basis. However to show this, we have to apply Zorn's lemma, which is beyond the scope of in this book.

Exercise 6.4

6.4-1. Let V be the vector space spanned by $\alpha_1 = \cos^2 x$, $\alpha_2 = \sin^2 x$ and $\alpha_3 = \cos 2x$. Is $\{\alpha_1, \alpha_2, \alpha_3\}$ a basis of V? If not, find a basis of V.

6.4-2. Let $\mathbb{F} = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Show that (i) $\mathbb{F}$ is a field, (ii) $\mathbb{F}$ is a vector space over $\mathbb{Q}$, (iii) $\dim_{\mathbb{Q}} \mathbb{F} = 2$.

6.4-3. Show that a maximal (with respect to set inclusion) linearly independent set is a basis.

6.4-4. Show that a minimal (with respect to set inclusion) spanning set is a basis.

6.4-5. Find a basis for the subspace W in $\mathbb{Q}^4$ consisting of all vectors of the form $(a + b, a - b + 2c, b, c)$.

6.4-6. Let W be the set of all polynomials of the form $ax^2 + bx + 2a + 3b$. Show that W is a subspace of $P_3(\mathbb{F})$. Find a basis for W.

6.4-7. Let $V = M_n(\mathbb{R})$. Let W be the set of all symmetric matrices.

(a) Show that W is a subspace of V.

(b) Compute $\dim W$.

6.4-8. Show that if W_1 and W_2 are subspaces, then $W_1 \cup W_2$ is a subspace if and only if one is a subspace of the other.

6.4-9. Let S, T and T' be three subspaces of a vector space V for which (a) $S \cap T = S \cap T'$, (b) $S + T = S + T'$, (c) $T \subseteq T'$. Show that $T = T'$.

6.5 Sums and Direct Sums of Subspaces

Sometimes we want to consider a new subspace which is spanned by two subspaces. For example, we have two lines L_1 and L_2 in $\mathbb{R}^3$ which pass through the origin. Suppose L_1 and L_2 are not the same. Then the subspace span by these two lines is a plane passing through the origin. We shall denote this plane by $L_1 + L_2$. Now we make a definition of such concept.

Definition 6.5.1 Let $W_1, \ldots, W_k$ be k subsets of a vector space V. We put

$$W_1 + \cdots + W_k = \sum_{i=1}^{k} W_i = \left\{ \sum_{i=1}^{k} \alpha_i \;\middle|\; \alpha_i \in W_i, 1 \leq i \leq k \right\}.$$

By definition, it is easy to have the following lemma.

Lemma 6.5.2 *Suppose $A_1 \subseteq B_1$ and $A_2 \subseteq B_2$ are nonempty subsets of a vector space. Then $A_1 + A_2 \subseteq B_1 + B_2$.*

Proposition 6.5.3 *If $W_1, \ldots, W_k$ are subspaces of a vector space, then so is $\sum_{i=1}^{k} W_i$.*

Proof: Suppose $\alpha, \beta \in \sum_{i=1}^{k} W_i$ and $a \in \mathbb{F}$. Then $\alpha = \sum_{i=1}^{k} \alpha_i$, $\beta = \sum_{i=1}^{k} \beta_i$ for some $\alpha_i, \beta_i \in W_i$. Now we have

$$a\alpha + \beta = a\sum_{i=1}^{k} \alpha_i + \sum_{i=1}^{k} \beta_i = \sum_{i=1}^{k} (a\alpha_i + \beta_i).$$

Since $\alpha_i, \beta_i \in W_i$ and W_i is a subspace, $a\alpha_i + \beta_i \in W_i$. Thus, $a\alpha + \beta \in \sum_{i=1}^{k} W_i$. By Proposition 6.3.3, $\sum_{i=1}^{k} W_i$ is a subspace. □

Definition 6.5.4 If $W_1, \ldots, W_k$ are subspaces of a vector space, then $\sum_{i=1}^{k} W_i$ is called the *sum of the subspaces* $W_1, \ldots, W_k$.

Theorem 6.5.5 *Suppose $W_1, \ldots, W_k$ are subspaces of a vector space. Then*

(a) $\sum_{i=1}^{k} W_i = \text{span}\left(\bigcup_{i=1}^{k} W_i\right)$;

(b) if $\text{span}(A_i) = W_i$ *for* $1 \leq i \leq k$, *then* $\text{span}\left(\bigcup_{i=1}^{k} A_i\right) = \sum_{i=1}^{k} W_i$.

Proof: For simplicity we shall assume that $k = 2$. The general case follows easily by mathematical induction.

To prove (a) we first note that $\mathbf{0} \in W_1$, so $W_2 = \{\mathbf{0}\} + W_2 \subseteq W_1 + W_2$. Similarly we have $W_1 \subseteq W_1 + W_2$. By Lemma 6.3.7 and Remark 6.3.8 $\text{span}(W_1 \cup W_2) \subseteq W_1 + W_2$. On the other hand, since $W_1 \subseteq \text{span}(W_1 \cup W_2)$, $W_2 \subseteq \text{span}(W_1 \cup W_2)$ and $\text{span}(W_1 \cup W_2)$ is a subspace, $W_1 + W_2 \subseteq \text{span}(W_1 \cup W_2)$. Thus $W_1 + W_2 = \text{span}(W_1 \cup W_2)$.

To prove (b) we first note that from Lemma 6.3.7 we have $W_1 = \text{span}(A_1) \subseteq \text{span}(A_1 \cup A_2)$, $W_2 = \text{span}(A_2) \subseteq \text{span}(A_1 \cup A_2)$. By Lemma 6.3.7 and Remark 6.3.8 we have $\text{span}(W_1 \cup W_2) \subseteq \text{span}(A_1 \cup A_2)$. But as $A_1 \subseteq W_1$ and $A_2 \subseteq W_2$ we have $A_1 \cup A_2 \subseteq W_1 \cup W_2$. Thus by Lemma 6.3.7 again we have $\text{span}(A_1 \cup A_2) \subseteq \text{span}(W_1 \cup W_2)$. Therefore, $\text{span}(A_1 \cup A_2) = \text{span}(W_1 \cup W_2)$. From (a) we obtain (b). □

Theorem 6.5.6 *Let W_1 and W_2 be any two subspaces of a finite dimensional vector space. Then* $\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$.

Proof: Let $\dim(W_1 \cap W_2) = r$, $\dim W_1 = r + s$ and $\dim W_2 = r + t$. Suppose $\{\alpha_1, \ldots, \alpha_r\}$ is a basis of $W_1 \cap W_2$. We extend it to bases $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ and $\{\alpha_1, \ldots, \alpha_r, \gamma_1, \ldots, \gamma_t\}$ of W_1 and W_2, respectively. Clearly

$$\text{span}\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s, \gamma_1, \ldots, \gamma_t\} = W_1 + W_2.$$

We have only to show that $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s, \gamma_1, \ldots, \gamma_t\}$ is linearly independent.

Suppose

$$\sum_{i=1}^{r} a_i\alpha_i + \sum_{j=1}^{s} b_j\beta_j + \sum_{k=1}^{t} c_k\gamma_k = \mathbf{0} \text{ for some } a_i, b_j, c_k \in \mathbb{F}.$$

Then $\sum_{k=1}^{t} c_k\gamma_k = -\left(\sum_{i=1}^{r} a_i\alpha_i + \sum_{j=1}^{s} b_j\beta_j\right) \in W_1$. Also $\sum_{k=1}^{t} c_k\gamma_k \in W_2$. Thus $\sum_{k=1}^{t} c_k\gamma_k \in W_1 \cap W_2$. Hence $\sum_{k=1}^{t} c_k\gamma_k = \sum_{i=1}^{r} d_i\alpha_i$ for some $d_i \in \mathbb{F}$. But then $\sum_{i=1}^{r} d_i\alpha_i - \sum_{k=1}^{t} c_k\gamma_k = \mathbf{0}$ and since $\{\alpha_1, \ldots, \alpha_r, \gamma_1, \ldots, \gamma_t\}$ is a linearly independent, $d_i = 0$, $c_k = 0\ \forall i, k$. Thus we have

$$\sum_{i=1}^{r} a_i\alpha_i + \sum_{j=1}^{s} b_j\beta_j = \mathbf{0}.$$

Since $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ is linearly independent, $a_i = 0$ and $b_j = 0\ \forall i, j$. Thus $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s, \gamma_1, \ldots, \gamma_t\}$ is a basis of $W_1 + W_2$. Therefore,
$\dim(W_1 + W_2) = r + s + t = (r + s) + (r + t) - r = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$. □

Example 6.5.7 Let $V = \mathbb{R}^3$. Suppose W_1 and W_2 are subspaces of dimension 2. Then

$$\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = 4.$$

If $\dim(W_1 + W_2) = 3$, then $\dim(W_1 \cap W_2) = 1$. So W_1 and W_2 intersect in a line.

If $\dim(W_1 + W_2) = 2$, then $\dim(W_1 \cap W_2) = 2$. But $W_1 \cap W_2 \subseteq W_1$, they have the same dimension. So $W_1 \cap W_2 = W_1$. Similarly, we also have $W_1 \cap W_2 = W_2$ and then $W_1 = W_2$. □

Example 6.5.8 Let $V = \mathbb{R}^3$. Suppose

$$W_1 = \text{span}\{(1, 0, 2), (1, 2, 2)\}, W_2 = \text{span}\{(1, 1, 0), (0, 1, 1)\}.$$

We would like to use the idea of the proof of Theorem 6.5.6 to find a basis for $W_1 + W_2$. By an easy inspection we see that both dimensions of W_1 and W_2 are 2. Let $\alpha \in W_1 \cap W_2$. Since $\alpha \in W_1$, $\alpha = a(1, 0, 2) + b(1, 2, 2) = (a + b, 2b, 2a + 2b)$ for some $a, b \in \mathbb{R}$. Also, since $\alpha \in W_2$, $\alpha = c(1, 1, 0) + d(0, 1, 1) = (c, c + d, d)$ for some $c, d \in \mathbb{R}$. Then

$$\begin{cases} a + b &= c \\ 2b &= c + d \\ 2a + 2b &= d \end{cases}$$

Solving this system, we get $b = -3a$,$c = -2a$, $d = -4a$. Thus $\alpha = -2a(1, 3, 2)$. This shows that $\{(1, 3, 2)\}$ is a basis of $W_1 \cap W_2$. Since $\dim W_1 = 2$, and $(1, 3, 2)$, $(1, 0, 2)$ are linearly independent, $\{(1, 3, 2), (1, 0, 2)\}$ is a basis of W_1. Similarly $\{(1, 3, 2), (1, 1, 0)\}$ is a basis of W_2. Hence $\{(1, 3, 2), (1, 0, 2), (1, 1, 0)\}$ is a basis of $W_1 + W_2$.

Note that, by Theorem 6.5.5 (b) $W_1 + W_2 = \text{span}\{(1, 0, 2), (1, 2, 2), (1, 1, 0), (0, 1, 1)\}$. We can use Casting-out Method to find a basis of $W_1 + W_2$. Please refer to Chapter 3. □

Definition 6.5.9 Let W_1 and W_2 be subspaces of a vector space. The sum $W_1 + W_2$ is called a *direct sum* of W_1 and W_2 if $W_1 \cap W_2 = \{\mathbf{0}\}$. In this case $W_1 + W_2$ is denoted by $W_1 \oplus W_2$. Note that $W_1 \oplus W_2 = W_2 \oplus W_1$.

Proposition 6.5.10 *Let W_1 and W_2 be subspaces of a finite dimensional vector space. Then*

(a) $\dim(W_1 \oplus W_2) = \dim W_1 + \dim W_2$.

(b) The sum $W_1 + W_2$ is direct if and only if for each $\alpha \in W_1 + W_2$, α is decomposed in a unique way as $\alpha = \alpha_1 + \alpha_2$ with $\alpha_1 \in W_1$ and $\alpha_2 \in W_2$.

Proof: (a) is trivial. We have to prove (b) only.

Suppose $\alpha \in W_1 + W_2$ and $\alpha = \alpha_1 + \alpha_2 = \beta_1 + \beta_2$, where $\alpha_1, \beta_1 \in W_1$ and $\alpha_2, \beta_2 \in W_2$. Then since $\alpha_1 - \beta_1 = \alpha_2 - \beta_2 \in W_1 \cap W_2 = \{\mathbf{0}\}$, we have $\alpha_1 = \beta_1$ and $\alpha_2 = \beta_2$.

Conversely, suppose for each $\alpha \in W_1 + W_2$, $\alpha = \alpha_1 + \alpha_2$ in a unique way with $\alpha_1 \in W_1$ and $\alpha_2 \in W_2$. We have to show that $W_1 \cap W_2 = \{\mathbf{0}\}$. For $\alpha \in W_1 \cap W_2$, from $\alpha = \alpha + \mathbf{0} = \mathbf{0} + \alpha \in W_1 + W_2$ and the uniqueness of decomposition we have that $\alpha = \mathbf{0}$. Thus, $W_1 \cap W_2 = \{\mathbf{0}\}$ and the sum is direct. □

Definition 6.5.11 Suppose W_1 and W_2 are subspace of a vector space V. If $V = W_1 \oplus W_2$, then we say that W_1 and W_2 are *complementary* and that W_2 is a *complementary subspace of* W_1 or *complement of* W_1. The *codimension* of W_1 is defined to be the dimension of W_2 and denoted by $\operatorname{codim} W_1$.

Theorem 6.5.12 *If W is a subspace of an n-dimensional vector space V, then there exists a subspace W' such that $V = W \oplus W'$.*

Proof: Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis of W. By Theorem 6.4.14 (or Theorem 6.4.17) we can extend this linearly independent set to a basis $\{\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n\}$ of V. Put $W' = \operatorname{span}\{\alpha_{m+1}, \ldots, \alpha_n\}$. Clearly $V = W \oplus W'$. □

Thus every subspace of a finite dimensional vector space has a complementary subspace. However, the complementary subspace is not unique, for there are more than one way to extend a linearly independent set to a basis of the whole space. For example, $W_1 = \operatorname{span}\{(0,1)\}$ and $W_2 = \operatorname{span}\{(1,1)\}$ are two different complementary subspaces of $W = \operatorname{span}\{(1,0)\}$ in $\mathbb{R}^2$.

Definition 6.5.13 Let $W_1, \ldots, W_k$ be subspaces of a vector space. The sum $W_1 + \cdots + W_k$ is said to be *direct* if for each i, $W_i \cap \left(\sum_{\substack{1 \le j \le k \\ j \ne i}} W_j \right) = \{\mathbf{0}\}$. We denote this sum by $W_1 \oplus \cdots \oplus W_k$ or $\bigoplus_{j=1}^{k} W_j$.

Proposition 6.5.14 *Let $W_1, \ldots, W_k$ be subspaces of a vector space. The sum $W_1 + \cdots + W_k$ is direct if and only if for each $\alpha \in W_1 + \cdots + W_k$, α can be expressed uniquely in the form $\alpha = \alpha_1 + \cdots + \alpha_k$ with $\alpha_i \in W_i$, $1 \le i \le k$.*

We leave the proof to reader (exercise).

Theorem 6.5.15 *Suppose $W_1, \ldots, W_k$ are subspaces of a finite dimensional vector space. Then the sum $\sum_{i=1}^{k} W_i$ is direct if and only if $\dim \left(\sum_{i=1}^{k} W_i \right) = \sum_{i=1}^{k} \dim W_i$.*

Proof: It is easy to show by mathematical induction that $\dim \left(\sum_{i=1}^{r} W_i \right) \le \sum_{i=1}^{r} \dim W_i$ for each $r \ge 1$.

We prove the "if" part first. For each j,

$$\begin{aligned}
\sum_{i=1}^{k} \dim W_i = \dim \left(\sum_{i=1}^{k} W_i \right) &= \dim \left(W_j + \sum_{i \ne j} W_i \right) \\
&= \dim W_j + \dim \left(\sum_{i \ne j} W_i \right) - \dim \left(W_j \cap \sum_{i \ne j} W_i \right) \\
&\le \dim W_j + \left(\sum_{i \ne j} \dim W_i \right) - \dim \left(W_j \cap \sum_{i \ne j} W_i \right).
\end{aligned}$$

This implies that $\dim\left(W_j \cap \sum_{i\neq j} W_i\right) = 0$ or equivalently $W_j \cap \sum_{i\neq j} W_i = \{\mathbf{0}\}$.

Now, we prove the "only if" part by mathematical induction on k. For $k = 1$, the statement is trivial. Assume the statement is true for $k \geq 1$. That is, if $\sum_{i=1}^{k} W_i$ is direct, then $\dim\left(\sum_{i=1}^{k} W_i\right) = \sum_{i=1}^{k} \dim W_i$.

Now we assume that $\sum_{i=1}^{k+1} W_i$ is direct.

$$\begin{aligned}\dim\left(\sum_{i=1}^{k+1} W_i\right) &= \dim\left(\sum_{i=1}^{k} W_i + W_{k+1}\right)\\ &= \dim\left(\sum_{i=1}^{k} W_i\right) + \dim W_{k+1} - \dim\left(W_{k+1} \cap \sum_{i=1}^{k} W_i\right)\\ &= \dim\left(\sum_{i=1}^{k} W_i\right) + \dim W_{k+1}. \qquad (6.1)\end{aligned}$$

Since $\sum_{i=1}^{k+1} W_i$ is direct, for each j with $1 \leq j \leq k$

$$\{\mathbf{0}\} \subseteq W_j \cap \left(\sum_{\substack{1\leq i\leq k\\ i\neq j}} W_i\right) \subseteq W_j \cap \left(\sum_{\substack{1\leq i\leq k+1\\ i\neq j}} W_i\right) = \{\mathbf{0}\}.$$

Hence $\sum_{i=1}^{k} W_i$ is direct. So by the induction hypothesis, $\dim\left(\sum_{i=1}^{k} W_i\right) = \sum_{i=1}^{k} \dim W_i$. Therefore, Equation (6.1) becomes $\dim\left(\sum_{i=1}^{k+1} W_i\right) = \sum_{i=1}^{k+1} \dim W_i$. □

Exercise 6.5

6.5-1. Prove the Proposition 6.5.14.

6.5-2. Let $W_1 = \text{span}\{(1,1,2,0),\ (-2,1,2,0)\}$ and $W_2 = \text{span}\{(2,0,1,1),\ (-3,2,0,4)\}$ be two subspaces of $\mathbb{R}^4$. Is $W_1 + W_2$ direct?

6.5-3. Let $W = \text{span}\{(1,1,0,1),\ (-1,0,1,1)\}$. Find a subspace W' such that $W \oplus W' = \mathbb{R}^4$.

6.5-4. Let V be the vector space of all real functions defined on $\mathbb{R}$. Let W_1 be the set of all even functions in V and W_2 be the set of all odd functions in V.

(a) Prove that W_1 and W_2 are subspaces of V.

(b) Show that $W_1 + W_2 = V$.

(c) Is the sum in (b) direct?

6.5-5. Let W_1 and W_2 are subspaces of a finite dimensional vector space V. Show that

$$\text{codim}(W_1 \cap W_2) = \text{codim}W_1 + \text{codim}W_2$$

if and only if $W_1 + W_2 = V$.

Chapter 7

Linear Transformations and Matrix Representations

7.1 Linear Transformations

We want to compare two vector spaces. So we need a corresponding between two vector spaces which preserves the structure of vector space. Such corresponding is called homomorphism in the theory of algebra. But in linear algebra it is often called linear transformation. Following is its definition.

Definition 7.1.1 Let U and V be vector spaces over $\mathbb{F}$. A *linear transformation σ of U into V* is a mapping of U into V such that

$$\forall \alpha, \beta \in U, a \in \mathbb{F},\ \sigma(a\alpha + \beta) = a\sigma(\alpha) + \sigma(\beta).$$

Note that if σ is a linear transformation, then $\forall \alpha, \beta \in U,\ \forall a, b \in \mathbb{F},\ \sigma(a\alpha + b\beta) = a\sigma(\alpha) + b\sigma(\beta)$.

Proposition 7.1.2 *If σ is a linear transformation, then $\sigma(\mathbf{0}) = \mathbf{0}$.*

Proof: Since $\sigma(\mathbf{0}) = \sigma(\mathbf{0} + \mathbf{0}) = \sigma(\mathbf{0}) + \sigma(\mathbf{0})$, by Corollary 6.1.3 we have $\sigma(\mathbf{0}) = \mathbf{0}$. □

Definition 7.1.3 Suppose $\sigma : U \to V$ is a linear transformation. If σ is injective (i.e., one to one), then σ is called a *monomorphism*. If σ is surjective (i.e., onto), then σ is called an *epimorphism*. A linear transformation that is both an epimorphism and a monomorphism is called an *isomorphism*.

Theorem 7.1.4 *Let $\sigma : U \to V$ be an isomorphism. Then $\sigma^{-1} : V \to U$ is also an isomorphism.*

Proof: We have only to show that σ^{-1} is linear.

Let $\alpha', \beta' \in V$ and $a \in \mathbb{F}$. Since σ is surjective, $\exists \alpha, \beta \in U$ such that $\sigma(\alpha) = \alpha'$ and $\sigma(\beta) = \beta'$. Since σ is linear, $\sigma(a\alpha + \beta) = a\sigma(\alpha) + \sigma(\beta) = a\alpha' + \beta'$. Thus by the definition of inverse mapping we have

$$\sigma^{-1}(a\alpha' + \beta') = a\alpha + \beta = a\sigma^{-1}(\alpha') + \sigma^{-1}(\beta').$$ □

Example 7.1.5 Let $U = V = \mathbb{F}[x]$. For $\alpha \in U$, $\alpha = \sum_{k=0}^{n} a_k x^k$ for some n, define $\sigma(\alpha) = \sum_{k=1}^{n} k a_k x^{k-1}$. Note that if $\mathbb{F} = \mathbb{R}$, then $\sigma = \frac{d}{dx}$ is the derivative operator of real value functions. It is easy to check that σ is linear.

Suppose $\mathbb{F} = \mathbb{R}$. Define $\tau(\alpha) = \sum_{k=0}^{n} \frac{a_k}{k+1} x^{k+1}$. Then τ is also linear. Note that σ is surjective but not injective and τ is injective but not surjective. □

Example 7.1.6 For vector space $U = V$ and a fixed $a \in \mathbb{F}$, define the mapping $\sigma : U \to V$ by $\sigma(\alpha) = a\alpha$. Then σ is a linear transformation and is called a *scalar transformation.* If $a = 1$, then we have the *identity linear transformation.* □

Proposition 7.1.7 *Let U, V and W be vector spaces over $\mathbb{F}$. Suppose $\sigma : U \to V$ and $\tau : V \to W$ are linear. Then the composition $\tau \circ \sigma : U \to W$ is linear.*

Proof: The proof is straightforward. □

Proposition 7.1.8 *Let U and V be vector spaces over $\mathbb{F}$. If $\sigma, \tau : U \to V$ are two linear transformations and $a \in \mathbb{F}$, then $\sigma + \tau$ and $a\sigma$ are linear. Here $\sigma + \tau$ is the sum of σ and τ and $a\sigma$ is the map defined by $(a\sigma)(\alpha) = a\sigma(\alpha)$ for each $\alpha \in U$.*

Proof: The proof is trivial. □

Example 7.1.9 Let V be an n-dimensional vector space over $\mathbb{F}$. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of V. For each $\alpha \in V$ there exist unique $a_1, \ldots, a_n \in \mathbb{F}$ such that $\alpha = \sum_{i=1}^{n} a_i \alpha_i$. Define a mapping $\sigma : V \to \mathbb{F}^n$ (respectively $\mathbb{F}^{n\times 1}$) by assigning α to $(a_1, \ldots, a_n)$ (respectively $(a_1 \ \cdots \ a_n)^T$). Then σ is an isomorphism of V onto $\mathbb{F}^n$ (respectively $\mathbb{F}^{n\times 1}$). □

Theorem 7.1.10 *Suppose $\sigma : U \to V$ is a linear transformation. Then $\sigma(U)$, the image of U under σ, is a subspace of V.*

Proof: The proof is left to reader as an exercise. □

Corollary 7.1.11 *Keep the notation and assumption of Theorem 7.1.10. If U_1 is a subspace of U, then $\sigma(U_1)$ is a subspace of V.*

The rank of a matrix was defined in Chapter 2. Following we define the rank of a linear transformation. We will obtain a result similar to Proposition 2.4.3.

Definition 7.1.12 Let $\sigma : U \to V$ be a linear transformation. The *rank* of σ is defined to be the dimension of $\sigma(U)$ and is denoted by $\text{rank}(\sigma)$.

Theorem 7.1.13 *Let $\sigma : U \to V$ be a linear transformation. Suppose* $\dim(U) = n$ *and* $\dim(V) = m$. *Then* $\text{rank}(\sigma) \leq \min\{n, m\}$.

Proof: Since $\text{rank}(\sigma) = \dim(\sigma(U))$ and $\sigma(U)$ is a subspace of V, by Theorem 6.4.16 we have $\text{rank}(\sigma) \leq m$.

We first note that if $\{\alpha_1, \ldots, \alpha_s\}$ is linearly dependent in U then $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_s)\}$ is linearly dependent in V. Since U is n-dimensional, there cannot have more than n linearly independent vectors in U. Thus if $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_s)\}$ is linearly independent in $\sigma(U)$, then $s \leq n$. Hence $\dim(\sigma(U)) \leq n$. Therefore, $\text{rank}(\sigma) \leq n$. □

Proposition 7.1.14 *Suppose $\sigma : U \to V$ is a linear transformation and W is a subspace of V. Then $\sigma^{-1}[W] = \{\alpha \in U \mid \sigma(\alpha) \in W\}$, the pre-image of W under σ, is a subspace of U.*

Proof: The proof is left to reader as an exercise. □

Corollary 7.1.15 $\sigma^{-1}[\{\mathbf{0}\}]$ *is a subspace of* U.

The nullity of a matrix was defined in Chapter 3. Now we define the nullity of a linear transformation. We will obtain a result similar to Theorem 3.6.9.

Definition 7.1.16 Suppose $\sigma : U \to V$ is a linear transformation. $\sigma^{-1}[\{\mathbf{0}\}]$ is called the *kernel* of σ and is denoted by $\ker(\sigma)$. The dimension of $\ker(\sigma)$ is called the *nullity* of σ and is denoted by $\text{nullity}(\sigma)$.

Theorem 7.1.17 *Let* U *and* V *be vector spaces over* $\mathbb{F}$ *and let* $\sigma : U \to V$ *be a linear transformation. Suppose* $\dim U = n$. *Then* $\text{rank}(\sigma) + \text{nullity}(\sigma) = n$.

Proof: Since $\ker(\sigma)$ is a subspace of U, it is finite dimensional. Suppose $\text{nullity}(\sigma) = k$. Choose a basis $\{\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n\}$ of U such that $\{\alpha_1, \ldots, \alpha_k\}$ is a basis of $\ker(\sigma)$.

For each $\alpha \in U$, $\alpha = \sum_{i=1}^{n} a_i\alpha_i$ for some $a_i \in \mathbb{F}$. Thus $\sigma(\alpha) = \sum_{i=k+1}^{n} a_i\sigma(\alpha_i)$. That is, $\text{span}\{\sigma(\alpha_{k+1}), \ldots, \sigma(\alpha_n)\} = \sigma(U)$.

If $\sum_{i=k+1}^{n} c_i\sigma(\alpha_i) = \mathbf{0}$ for some $c_i \in \mathbb{F}$, then from the linearity of σ we have $\sigma\left(\sum_{i=k+1}^{n} c_i\alpha_i\right) = \mathbf{0}$. This implies that $\sum_{i=k+1}^{n} c_i\alpha_i \in \ker(\sigma)$. Hence $\sum_{i=k+1}^{n} c_i\alpha_i = \sum_{j=1}^{k} d_j\alpha_j$ for some $d_j \in \mathbb{F}$. From this, we have $\sum_{j=1}^{k} d_j\alpha_j - \sum_{i=k+1}^{n} c_i\alpha_i = \mathbf{0}$. By the linearly independence of basis, we must have $c_i = 0\ \forall i$. Thus $\{\sigma(\alpha_{k+1}), \ldots, \sigma(\alpha_n)\}$ is a basis of $\sigma(U)$. By definition $\text{rank}(\sigma) = n - k$. Thus $\text{rank}(\sigma) + \text{nullity}(\sigma) = n$. □

Theorem 7.1.18 *Let* U *and* V *be finite dimensional vector spaces. Let* $\sigma : U \to V$ *be a linear transformation. Then*

(a) σ *is a monomorphism if and only if* $\text{nullity}(\sigma) = 0$;

(b) σ *is an epimorphism if and only if* $\text{rank}(\sigma) = \dim V$.

Proof:

(a) Suppose σ is injective. Let $\alpha \in \ker(\sigma)$. Then $\sigma(\alpha) = \mathbf{0}$. Since $\sigma(\mathbf{0}) = \mathbf{0}$ and σ is injective, $\alpha = \mathbf{0}$. Thus, $\ker(\sigma) = \{\mathbf{0}\}$ and hence $\text{nullity}(\sigma) = 0$.

Conversely, suppose $\ker(\sigma) = \{\mathbf{0}\}$. If $\alpha, \beta \in U$ are such that $\sigma(\alpha) = \sigma(\beta)$, then $\sigma(\alpha - \beta) = \mathbf{0}$. Then $\alpha - \beta \in \ker(\sigma)$. Hence $\alpha - \beta = \mathbf{0}$. Therefore, σ is injective.

(b) If σ is surjective, then $\sigma(U) = V$. So $\text{rank}(\sigma) = \dim(\sigma(U)) = \dim V$.

Conversely, if $\text{rank}(\sigma) = \dim V$, then since $\sigma(U) \subseteq V$, by Corollary 6.4.12 we have $\sigma(U) = V$. That is, σ is surjective. □

Note that if $\dim U < \dim V$, then by Theorem 7.1.17 $\text{rank}(\sigma) = \dim U - \text{nullity}(\sigma) \leq \dim U < \dim V$. Thus σ cannot be an epimorphism. If $\dim U > \dim V$, then $\text{nullity}(\sigma) = \dim U - \text{rank}(\sigma) \geq \dim U - \dim V > 0$. Thus σ cannot be a monomorphism. Consequently,

$$\boxed{\text{if } \sigma \text{ is an isomorphism, then } \dim(U) = \dim(V).}$$

Theorem 7.1.19 *Let U and V be finite dimensional vector spaces of the same dimension. Suppose $\sigma : U \to V$ is a linear transformation. Then the following statements are equivalent:*

(a) σ is an isomorphism;

(b) σ is a monomorphism;

(c) σ is an epimorphism.

Proof:

[(a)⇒(b)] It is clear.

[(b)⇒(c)] By Theorem 7.1.18 $\text{nullity}(\sigma) = 0$. By Theorem 7.1.17,

$$\dim(\sigma(U)) = \text{rank}(\sigma) = \dim U = \dim V.$$

Thus σ is surjective.

[(c)⇒(a)] It suffices to show that σ is injective. Since σ is surjective, $\text{rank}(\sigma) = \dim V$. Hence $\text{nullity}(\sigma) = \dim U - \text{rank}(\sigma) = \dim U - \dim V = 0$. By Theorem 7.1.18 σ is injective. □

Let A and B be sets and let $f : A \to B$ be a mapping. Suppose $C \subseteq A$. Let $g : C \to B$ be defined by $g(c) = f(c)$ for all $c \in C$. The mapping g is called the *restriction of f on C* and is denoted by $g = f|_C$.

Theorem 7.1.20 *Let U, V and W be finite dimensional vector spaces. Let $\sigma : U \to V$ and $\tau : V \to W$ be linear transformations. Then*

$$\text{rank}(\sigma) = \text{rank}(\tau \circ \sigma) + \dim(\sigma(U) \cap \ker(\tau)).$$

Proof: Let $\phi = \tau|_{\sigma(U)} : \sigma(U) \to W$. Then $\ker(\phi) = \sigma(U) \cap \ker(\tau)$. Also,

$$\text{rank}(\phi) = \dim(\phi(\sigma(U)) = \dim((\tau \circ \sigma)(U)) = \text{rank}(\tau \circ \sigma).$$

By Theorem 7.1.17 we have

$$\text{rank}(\phi) + \text{nullity}(\phi) = \dim(\sigma(U)) = \text{rank}(\sigma).$$

Therefore,

$$\text{rank}(\sigma) = \text{rank}(\tau \circ \sigma) + \text{nullity}(\phi) = \text{rank}(\tau \circ \sigma) + \dim(\sigma(U) \cap \ker(\tau)).$$ □

Corollary 7.1.21 *Keep the same hypothesis as Theorem 7.1.20. Then*

$$\text{rank}(\tau \circ \sigma) = \dim(\sigma(U) + \ker(\tau)) - \text{nullity}(\tau).$$

Proof: Since

$$\begin{aligned}\dim(\sigma(U) + \ker(\tau)) &= \dim(\sigma(U)) + \dim(\ker(\tau)) - \dim(\sigma(U) \cap \ker(\tau)) \\ &= \text{rank}(\sigma) + \text{nullity}(\tau) - (\text{rank}(\sigma) - \text{rank}(\tau \circ \sigma)) \\ &= \text{nullity}(\tau) + \text{rank}(\tau \circ \sigma),\end{aligned}$$

we have the corollary. □

Corollary 7.1.22 *Keep the same hypothesis as Theorem 7.1.20. If* $\ker(\tau) \subseteq \sigma(U)$*, then*

$$\text{rank}(\sigma) = \text{rank}(\tau \circ \sigma) + \text{nullity}(\tau).$$

Theorem 7.1.23 *Let* $\sigma : U \to V$ *and* $\tau : V \to W$ *be linear transformations. Then* $\text{rank}(\tau \circ \sigma) \leq \min\{\text{rank}(\sigma), \text{rank}(\tau)\}$*, where* U, V *and* W *are finite dimensional.*

Proof: By definition, $\text{rank}(\tau \circ \sigma) = \dim((\tau \circ \sigma)(U)) = \dim(\tau(\sigma(U)) \leq \dim(\tau(V)) = \text{rank}(\tau)$.

It is easy to see from the equality in Theorem 7.1.20 that $\text{rank}(\tau \circ \sigma) \leq \text{rank}(\sigma)$. Thus the theorem holds. □

Theorem 7.1.24 *Let* $\sigma : U \to V$ *and* $\tau : V \to W$ *be linear transformations. If* σ *is surjective, then* $\text{rank}(\tau \circ \sigma) = \text{rank}(\tau)$*. If* τ *is injective, then* $\text{rank}(\tau \circ \sigma) = \text{rank}(\sigma)$*. Here* U, V *and* W *are finite dimensional.*

Proof: If σ is surjective, then $\ker(\tau) \subseteq V = \sigma(U)$. So by Corollary 7.1.22

$$\text{rank}(\tau \circ \sigma) = \text{rank}(\sigma) - \text{nullity}(\tau) = \dim V - \text{nullity}(\tau) = \text{rank}(\tau).$$

If τ is injective, then $\ker(\tau) = \{\mathbf{0}\}$. By Theorem 7.1.20 $\text{rank}(\tau \circ \sigma) = \text{rank}(\sigma)$. □

Corollary 7.1.25 *The rank of a linear transformation is not changed by composing with an isomorphism on either side.*

Theorem 7.1.26 *Let* $\{\alpha_1, \ldots, \alpha_n\}$ *be any basis of a vector space* U*. Suppose* $\beta_1, \ldots, \beta_n$ *are any* n *vectors (not necessary distinct) in a vector space* V*. Then there exists a unique linear transformation* $\sigma : U \to V$ *such that* $\sigma(\alpha_i) = \beta_i$ *for* $i = 1, 2, \ldots, n$*.*

Proof: For $\alpha \in U$, $\alpha = \sum_{i=1}^{n} a_i \alpha_i$ for uniquely determined scalars $a_1, \ldots, a_n$. Define $\sigma(\alpha) = \sum_{i=1}^{n} a_i \beta_i$. Then it is easy to check that σ is linear and $\sigma(\alpha_i) = \beta_i$ for $i = 1, 2, \ldots, n$. Clearly, σ is unique. □

Corollary 7.1.27 *Let* $\{\alpha_1, \ldots, \alpha_k\}$ *be any linearly independent set in an* n*-dimensional vector space* U*. Suppose* $\beta_1, \ldots, \beta_k$ *are any* k *vectors (not necessary distinct) in a vector space* V*. Then there exists a linear transformation* $\sigma : U \to V$ *such that* $\sigma(\alpha_i) = \beta_i$ *for* $i = 1, 2, \ldots, k$*.*

Proof: Extend $\{\alpha_1, \ldots, \alpha_k\}$ to a basis $\{\alpha_1, \ldots, \alpha_k, \ldots, \alpha_n\}$ of U. Define $\sigma(\alpha_i) = \beta_i$ for $i = 1, 2, \ldots, k$ and $\sigma(\alpha_j)$ arbitrarily for $j = k+1, \ldots, n$. Extend σ linearly to get a required linear transformation. Note that such σ is not unique if $k < n$. □

Under what condition will the left or the right cancellation law hold for composition of linear transformations?

We shall use O to denote the zero linear transformation, i.e., $O(\alpha) = \mathbf{0}$ for every vector α in the domain of O.

Theorem 7.1.28 *Let* V *be an* m*-dimensional vector space and* $\sigma : U \to V$ *be a linear transformation. Then* σ *is surjective if and only if for any linear transformation* $\tau : V \to W$*,* $\tau \circ \sigma = O$ *implies* $\tau = O$*.*

Proof:

[⇒] Suppose σ is surjective. Assume $\tau : V \to W$ is a linear transformation such that $\sigma \circ \tau = O$. $\forall \beta \in V$, since σ is surjective, $\exists \alpha \in U$ such that $\sigma(\alpha) = \beta$. Then $\tau(\beta) = \tau(\sigma(\alpha)) = O(\alpha) = \mathbf{0}$. So $\tau = O$.

[⇐] Suppose σ is not surjective. Then $\sigma(U) \subset V$. Hence we can find a basis $\{\alpha_1, \ldots, \alpha_k, \ldots, \alpha_m\}$ of V such that $\{\alpha_1, \ldots, \alpha_k\}$ is a basis of $\sigma(U)$. Clearly $k < m$. By Theorem 7.1.26 there exists a linear transformation $\tau : V \to V$ such that $\tau(\alpha_i) = \mathbf{0}$ for $i \leq k$ and $\tau(\alpha_i) = \alpha_i$ for $k < i \leq m$. Then $\tau \circ \sigma = O$ with $\tau \neq O$. □

Corollary 7.1.29 *A linear transformation $\sigma : U \to V$ is surjective if and only if $\tau_1 \circ \sigma = \tau_2 \circ \sigma$ implies $\tau_1 = \tau_2$ for any linear transformations $\tau_1, \tau_2 : V \to W$. Here V is finite dimensional.*

Theorem 7.1.30 *Let U be an n-dimensional vector space and $\sigma : U \to V$ be a linear transformation. Then σ is injective if and only if for any linear transformation $\eta : S \to U$, $\sigma \circ \eta = O$ implies $\eta = O$.*

Proof:

[⇒] Suppose σ is injective. Assume $\eta : S \to U$ is a linear transformation such that $\sigma \circ \eta = O$. $\forall \alpha \in S$ by assumption $\sigma(\eta(\alpha)) = \mathbf{0}$. Since σ is injective, $\eta(\alpha) = \mathbf{0}$. So $\eta = O$.

[⇐] Suppose σ is not injective. Then by Theorem 7.1.18 $\ker(\sigma) \supset \{\mathbf{0}\}$. That is, $\exists \alpha \in \ker(\sigma)$ such that $\alpha \neq \mathbf{0}$. Let $S = U$ and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of U. By Theorem 7.1.26 there exists a linear transformation $\eta : U \to U$ such that $\eta(\alpha_i) = \alpha$ for $1 \leq i \leq n$. Then $\eta \neq O$ but $(\sigma \circ \eta)(\alpha_i) = \sigma(\alpha) = \mathbf{0}$ for all i. This means that $\sigma \circ \eta = O$. □

Corollary 7.1.31 *A linear transformation $\sigma : U \to V$ is injective if and only if $\sigma \circ \eta_1 = \sigma \circ \eta_2$ implies $\eta_1 = \eta_2$ for any linear transformations $\eta_1, \eta_2 : S \to U$. Here U is finite dimensional.*

Following we shall introduce a linear transformation called projection. This transformation will be used in decomposition of a vector space.

Definition 7.1.32 A linear transformation $\pi : V \to V$ is called a *projection* on V if $\pi^2 = \pi \circ \pi = \pi$.

Theorem 7.1.33 *If π is projection on V, then $V = \pi(V) \oplus \ker(\pi)$ and $\pi(\alpha) = \alpha$ for every $\alpha \in \pi(V)$.*

Proof: First we note that if $\beta \in V$, then $\pi(\pi(\beta)) = \pi^2(\beta) = \pi(\beta)$. Thus $\pi(\alpha) = \alpha$ for every $\alpha \in \pi(V)$. Now suppose $\beta \in V$. Put $\gamma = \beta - \pi(\beta)$. Then $\pi(\gamma) = \pi(\beta) - \pi^2(\beta) = \mathbf{0}$. Thus $\gamma \in \ker(\pi)$. Hence $V = \pi(V) + \ker(\pi)$. The sum is also direct, for if $\alpha \in \pi(V) \cap \ker(\pi)$, then $\alpha = \pi(\alpha) = \mathbf{0}$. □

Exercise 7.1

7.1-1. Prove Theorem 7.1.10.

7.1-2. Prove Proposition 7.1.14.

7.1-3. Let $\sigma : P_3(\mathbb{R}) \to P_3(\mathbb{R})$ be defined by $\sigma(f) = f'' + 2f' - f$. Here f' is the derivative of f. Is σ surjective? Can you find a polynomial $f \in P_3(\mathbb{R})$ such that $f''(x) + 2f'(x) - f(x) = x$ (i.e., $x \in \sigma(P_3(\mathbb{R}))$)? If so, find f.

7.1-4. Determine whether the following linear transformations are (a) injective; (b) surjective.

(1) $\sigma : \mathbb{R}^3 \to \mathbb{R}^2$; $\sigma(x, y, z) = (x - y, z)$.

(2) $\sigma : \mathbb{R}^2 \to \mathbb{R}^3$; $\sigma(x, y) = (x + y, 0, 2x - y)$.

(3) $\sigma : \mathbb{R}^3 \to \mathbb{R}^3$; $\sigma(x, y, z) = (x, x + y, x + y + z)$.

(4) $\sigma : P_4(\mathbb{R}) \to M_2(\mathbb{R})$, for $f \in P_4(\mathbb{R})$, let $\sigma(f) = \begin{pmatrix} f(1) & f(2) \\ f(3) & f(4) \end{pmatrix}$.

7.1-5. Define $\sigma : P_3(\mathbb{R}) \to \mathbb{R}^4$ by $\sigma(f) = (f(1), f'(0), \int_0^1 f(x)dx, \int_{-1}^1 xf(x)dx)$. Find $\ker(\sigma)$.

7.1-6. Define $\sigma : M_2(\mathbb{R}) \to P_3(\mathbb{R})$ by $\sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a+b+2dx+bx^2$. Find $\ker(\sigma)$ and also find $\text{nullity}(\sigma)$ and $\text{rank}(\sigma)$.

7.2 Coordinates

From now on, we shall assume all the vector spaces are finite dimensional unless otherwise stated.

In coordinate geometry, coordinate axes play an indispensable role. In a vector space, basis plays a similar role. Each vector in a vector space can be expressed by a unique linear combination of a given ordered basis vectors. These coefficients in the combination determine a column matrix.

For a linear transformation σ from vector space U to vector space V, we would like to give σ 'clothes', that is, the representing matrix via ordered bases of U and V respectively. This way we shall be able to make full use of the matrix algebra to study linear transformation.

Let $\mathscr{A}$ be a basis of a finite dimensional vector space V. We say that $\mathscr{A}$ is an *ordered basis* if $\mathscr{A}$ is viewed as an ordered set (i.e., a finite sequence). Note that, from now on the order is very important.

Definition 7.2.1 Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ be an ordered basis of V over $\mathbb{F}$. For $\alpha \in V$ there exist $a_1, \ldots, a_n \in \mathbb{F}$ such that $\alpha = \sum_{i=1}^{n} a_i\alpha_i$. We define the *coordinate of α relative to $\mathscr{A}$*, denoted $[\alpha]_{\mathscr{A}}$, by

$$[\alpha]_{\mathscr{A}} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{F}^{n\times 1}.$$

The scalar a_i is called the *i-th coordinate of α relative to $\mathscr{A}$*.

Note that we normally identify the element $(a_1, \ldots, a_n) \in \mathbb{F}^n$ with the column vector $(a_1 \ \cdots \ a_n)^T$.

Proposition 7.2.2 *Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ be an ordered basis of V over $\mathbb{F}$. For $\alpha, \beta \in V$ and $a \in \mathbb{F}$, $[a\alpha + \beta]_{\mathscr{A}} = a[\alpha]_{\mathscr{A}} + [\beta]_{\mathscr{A}}$.*

Proof: Suppose $\alpha = \sum_{i=1}^{n} a_i\alpha_i$, and $\beta = \sum_{i=1}^{n} b_i\alpha_i$ for some $a_i, b_i \in \mathbb{F}$. Then

$$a\alpha + \beta = a\sum_{i=1}^{n} a_i\alpha_i + \sum_{i=1}^{n} b_i\alpha_i = \sum_{i=1}^{n}(aa_i + b_i)\alpha_i.$$

Thus, $[a\alpha + \beta]_{\mathscr{A}} = \begin{pmatrix} aa_1 + b_1 \\ aa_2 + b_2 \\ \vdots \\ aa_n + b_n \end{pmatrix} = a\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a[\alpha]_{\mathscr{A}} + [\beta]_{\mathscr{A}}$. □

Corollary 7.2.3 *Keeping the hypothesis of Proposition 7.2.2, the mapping $\alpha \mapsto [\alpha]_{\mathscr{A}}$ is an isomorphism from V onto $\mathbb{F}^n$.*

Suppose U and V are finite dimensional vector spaces over $\mathbb{F}$. Let $L(U,V)$ be the set of all linear transformations from U to V. Now we are going to study the structure of $L(U,V)$. Note that under the addition and scalar multiplication defined in Proposition 7.1.8 $L(U,V)$ is a vector space over $\mathbb{F}$.

Theorem 7.2.4 *Suppose U and V are finite dimensional vector spaces over $\mathbb{F}$ with ordered bases $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ and $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$, respectively. Then with respect to these bases, there is a bijection between $L(U,V)$ and $M_{m,n}(\mathbb{F})$.*

Proof: Let $\sigma \in L(U,V)$. Since $\sigma(\alpha_j) \in V$, $\sigma(\alpha_j) = \sum_{i=1}^{m} a_{ij}\beta_i$ for some $a_{ij} \in \mathbb{F}$. Thus we obtain a matrix $A = (a_{ij}) \in M_{m,n}(\mathbb{F})$.

Conversely, suppose $A = (a_{ij}) \in M_{m,n}(\mathbb{F})$. Then by Theorem 7.1.26 there exists a unique linear transformation $\sigma \in L(U,V)$ such that $\sigma(\alpha_j) = \sum_{i=1}^{m} a_{ij}\beta_i$ for $j = 1, 2, \ldots, n$.

Therefore, the mapping $\sigma \mapsto (a_{ij})$ is a bijection. □

Definition 7.2.5 With the notation defined in the proof of Theorem 7.2.4, we call that σ is *represented by A with respect to the ordered bases $\mathscr{A}$ and $\mathscr{B}$* and write $A = [\sigma]_{\mathscr{B}}^{\mathscr{A}}$. If $U = V$ and $\mathscr{A} = \mathscr{B}$, we call that σ is *represented by A with respect to the ordered basis $\mathscr{A}$*, we simplify the notation $A = [\sigma]_{\mathscr{A}}^{\mathscr{A}}$ to $A = [\sigma]_{\mathscr{A}}$.

Note that any matrix representation of a linear transformation must be relative to some ordered bases. Thus by bases we shall mean ordered bases for any linear transformation representation.

Note also that the entries of the j-th column of A are the coefficients of $\sigma(\alpha_j)$ with respect to basis $\mathscr{B}$, i.e., $A_{*j} = [\sigma(\alpha_j)]_{\mathscr{B}}$. Here α_j is the j-th vector in $\mathscr{A}$.

Theorem 7.2.6 *Let the bijection $\varphi : \sigma \mapsto A = [\sigma]_{\mathscr{B}}^{\mathscr{A}}$ be defined in the proof of Theorem 7.2.4. Then φ is an isomorphism.*

Proof: It suffices to show that φ is linear. Suppose $\sigma, \tau \in L(U,V)$. Let $\mathscr{A}$ and $\mathscr{B}$ be the bases defined in Theorem 7.2.4 and let $A = (a_{ij}) = [\sigma]_{\mathscr{B}}^{\mathscr{A}} = \varphi(\sigma)$ and $B = (b_{ij}) = [\tau]_{\mathscr{B}}^{\mathscr{A}} = \varphi(\tau)$. For any $c \in \mathbb{F}$,

$$(c\sigma + \tau)(\alpha_j) = c\sigma(\alpha_j) + \tau(\alpha_j) = c\sum_{i=1}^{m} a_{ij}\beta_i + \sum_{i=1}^{m} b_{ij}\beta_i = \sum_{i=1}^{m} (ca_{ij} + b_{ij})\beta_i.$$

Thus $[c\sigma + \tau]_{\mathscr{B}}^{\mathscr{A}} = (ca_{ij} + b_{ij}) = cA + B = c[\sigma]_{\mathscr{B}}^{\mathscr{A}} + [\tau]_{\mathscr{B}}^{\mathscr{A}}$. That is, $\varphi(c\sigma + \tau) = c\varphi(\sigma) + \varphi(\tau)$. □

Examples 7.2.7

1. Let $U = V = \mathbb{R}^2$. Suppose σ is the rotation through an angle θ in the anticlockwise direction. Then σ maps $(1,0)$ to $(\cos\theta, \sin\theta)$ and $(0,1)$ to $(-\sin\theta, \cos\theta)$, respectively. Thus σ is represented by

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

with respect to the standard (ordered) basis.

2. Let $U = V = \mathbb{R}^2$. Suppose σ is the reflection about the line $x = y$. Then $\sigma(x, y) = (y, x)$. Thus $\sigma(1, 0) = (0, 1)$ and $\sigma(0, 1) = (1, 0)$. Hence σ is represented by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to the standard basis.

3. The zero transformation represented by the zero matrix with respect to any bases. The identity transformation is represented by the identity matrix with respect to any basis. Note that if we choose two difference bases $\mathscr{A}$ and $\mathscr{B}$ for the same vector space, then the identity transformation is represented by a non-identity matrix. We shall discuss this fact later.

4. Let $A \in M_{m,n}(\mathbb{F})$. We define $\sigma_A : \mathbb{F}^n \to \mathbb{F}^m$ by $\sigma_A(X) = AX$ for all $X \in \mathbb{F}^n$ (which is identified with $\mathbb{F}^{n\times 1}$). Then with respect to the standard bases $\mathscr{S}_n$ and $\mathscr{S}_m$ of $\mathbb{F}^n$ and $\mathbb{F}^m$ respectively, $[\sigma_A]_{\mathscr{S}_m}^{\mathscr{S}_n} = A$. This means that for any $m \times n$ matrix, it is a matrix representation of a linear transformation of some suitable vector spaces with respect to some suitable bases. □

Example 7.2.8 Let $\sigma : \mathbb{R}^3 \to \mathbb{R}^2$ be defined by $\sigma(x, y, z) = (x - z,\ 3x - 2y + z)$ for each $(x, y, z) \in \mathbb{R}^3$.

Now we first verify that σ is linear. For any $\alpha = (x_1, y_1, z_1),\ \beta = (x_2, y_2, z_2) \in \mathbb{R}^3,\ c \in \mathbb{R}$, $c\alpha + \beta = (cx_1 + x_2,\ cy_1 + y_2,\ cz_1 + z_2)$. Then

$$\begin{aligned}\sigma(c\alpha + \beta) &= \big((cx_1 + x_2) - (cz_1 + z_2),\ 3(cx_1 + x_2) - 2(cy_1 + y_2) + (cz_1 + z_2)\big)\\ &= \big(cx_1 - cz_1,\ 3cx_1 - 2cy_1 + cz_1\big) + \big(x_2 - z_2,\ 3x_2 - 2y_2 + z_2\big)\\ &= c(x_1 - z_1,\ 3x_1 - 2y_1 + z_1) + (x_2 - z_2,\ 3x_2 - 2y_2 + z_2) = c\sigma(\alpha) + \sigma(\beta).\end{aligned}$$

Hence σ is linear.

Suppose $\mathscr{A} = \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ and $\mathscr{B} = \{\boldsymbol{e}'_1, \boldsymbol{e}'_2\}$ be the standard bases of $\mathbb{R}^3$ and $\mathbb{R}^2$, respectively. Then

$$\begin{aligned}\sigma(\boldsymbol{e}_1) &= \sigma(1, 0, 0) = (1, 3) = \boldsymbol{e}'_1 + 3\boldsymbol{e}'_2,\\ \sigma(\boldsymbol{e}_2) &= \sigma(0, 1, 0) = (0, -2) = -2\boldsymbol{e}'_2,\\ \sigma(\boldsymbol{e}_3) &= \sigma(0, 0, 1) = (-1, 1) = -\boldsymbol{e}'_1 + \boldsymbol{e}'_2.\end{aligned}$$

Hence $[\sigma]_{\mathscr{B}}^{\mathscr{A}} = \begin{pmatrix} 1 & 0 & -1 \\ 3 & -2 & 1 \end{pmatrix}$.

Clearly the matrix obtained above is of rank 2. So $\operatorname{rank}(\sigma) = 2$ and hence $\operatorname{nullity}(\sigma) = 3 - 2 = 1$. □

Theorem 7.2.9 *Let $\sigma \in L(U, V)$ and $\tau \in L(V, W)$. Suppose $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$, $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$ and $\mathscr{C} = \{\gamma_1, \ldots, \gamma_p\}$ are bases of U, V and W, respectively. Then $[\tau \circ \sigma]_{\mathscr{C}}^{\mathscr{A}} = [\tau]_{\mathscr{C}}^{\mathscr{B}}[\sigma]_{\mathscr{B}}^{\mathscr{A}}$.*

Proof: Let $[\sigma]_{\mathscr{B}}^{\mathscr{A}} = (a_{ij}) \in M_{m,n}(\mathbb{F})$ and $[\tau]_{\mathscr{C}}^{\mathscr{B}} = (b_{ki}) \in M_{p,m}(\mathbb{F})$. Then

$$\sigma(\alpha_j) = \textstyle\sum_{i=1}^{m} a_{ij}\beta_i, \quad \text{and} \quad \tau(\beta_i) = \sum_{k=1}^{p} b_{ki}\gamma_k.$$

Then

$$\begin{aligned}(\tau \circ \sigma)(\alpha_j) = \tau(\sigma(\alpha_j)) &= \tau\left(\sum_{i=1}^{m} a_{ij}\beta_i\right)\\ &= \sum_{i=1}^{m} a_{ij}\tau(\beta_i) = \sum_{i=1}^{m} a_{ij}\sum_{k=1}^{p} b_{ki}\gamma_k = \sum_{k=1}^{p}\left(\sum_{i=1}^{m} b_{ki}a_{ij}\right)\gamma_k.\end{aligned}$$

Thus we have the theorem. □

This theorem explains why the multiplication of matrices is so defined.

Corollary 7.2.10 *Let $\sigma \in L(U,V)$ be an isomorphism. Suppose $\mathscr{A}$ and $\mathscr{B}$ are bases of U and V, then $[\sigma]_{\mathscr{B}}^{\mathscr{A}}$ is an invertible matrix.*

Proof: Since $\sigma^{-1} \circ \sigma = \iota$, the identity transformation from U to U and $[\iota]_{\mathscr{A}} = I$, the corollary follows. □

Theorem 7.2.11 *Let $\sigma \in L(U,V)$. Suppose $\mathscr{A}$ and $\mathscr{B}$ are bases of U and V, respectively. Then for $\alpha \in U$, $[\sigma(\alpha)]_{\mathscr{B}} = [\sigma]_{\mathscr{B}}^{\mathscr{A}}[\alpha]_{\mathscr{A}}$.*

Proof: Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$, $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$. Let

$$[\sigma]_{\mathscr{B}}^{\mathscr{A}} = (a_{ij}) \text{ and } [\alpha]_{\mathscr{A}} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Then we have

$$\sigma(\alpha) = \sum_{j=1}^{n} x_j \sigma(\alpha_j) = \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij}\beta_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij}x_j \right) \beta_i.$$

Thus

$$[\sigma(\alpha)]_{\mathscr{B}} = \begin{pmatrix} \sum_{j=1}^{n} a_{1j}x_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj}x_j \end{pmatrix} = [\sigma]_{\mathscr{B}}^{\mathscr{A}}[\alpha]_{\mathscr{A}}.$$

□

Corollary 7.2.12 *Keep the notation as in Theorem 7.2.11. If $[\sigma(\alpha)]_{\mathscr{B}} = A[\alpha]_{\mathscr{A}}$ for all $\alpha \in U$, then $A = [\sigma]_{\mathscr{B}}^{\mathscr{A}}$.*

Proof: From the assumption and Theorem 7.2.11 we have $(A - [\sigma]_{\mathscr{B}}^{\mathscr{A}})[\alpha]_{\mathscr{A}} = \mathbf{0}$ in $\mathbb{F}^n$. Since α is arbitrary and from Corollary 7.2.3, $(A - [\sigma]_{\mathscr{B}}^{\mathscr{A}})\boldsymbol{x} = \mathbf{0}$ for all $\boldsymbol{x} \in \mathbb{F}^n$. By setting $\boldsymbol{x} = \boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$, we have $A - [\sigma]_{\mathscr{B}}^{\mathscr{A}} = O$. Hence the corollary holds. □

Suppose $\sigma : U \to V$ is linear. Let $\beta \in V$. To solve the linear problem $\sigma(\alpha) = \beta$, we choose ordered bases $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ of U and $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$ of V. Then the unknown vector α is represented by $n \times 1$ matrix X, given vector β by $m \times 1$ matrix $\boldsymbol{b}$ and linear transformation σ by $m \times n$ matrix A. Thus we convert the linear problem to the matrix equation $AX = \boldsymbol{b}$. If we can find $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, then we have found $\alpha = \sum_{i=1}^{n} x_i\alpha_i$ as our solution.

As another application of the representing matrix we can compute nullity(σ) without knowing $\ker(\sigma)$. Since $\operatorname{rank}(\sigma) = \dim \operatorname{span}\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ which is the dimension of $C(A)$ and can be easily seen via the 'new clothes', i.e., the rref of A. Then nullity(σ) $= n - \operatorname{rank}(\sigma)$ is determined immediately.

Exercise 7.2

7.2-1. Let $\mathscr{A}$ and $\mathscr{B}$ be the standard bases of $\mathbb{R}^n$ and $\mathbb{R}^m$, respectively. Show that the following maps σ are linear and compute $[\sigma]_{\mathscr{B}}^{\mathscr{A}}$, $\text{rank}(\sigma)$ and $\text{nullity}(\sigma)$.

(a) $\sigma : \mathbb{R}^2 \to \mathbb{R}^3$ is defined by $\sigma(x, y) = (2x - y, 3x + 4y, x)$.

(b) $\sigma : \mathbb{R}^3 \to \mathbb{R}^3$ is defined by $\sigma(x, y, z) = (x - y + 2z, 2x + y, -x - 2y + 2z)$.

(c) $\sigma : \mathbb{R}^3 \to \mathbb{R}$ is defined by $\sigma(x, y, z) = 2x + y - z$.

(d) $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ is defined by $\sigma(x_1, x_2, \ldots, x_n) = (x_1, x_1, \ldots, x_1)$.

(e) $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ is defined by $\sigma(x_1, x_2, \ldots, x_n) = (x_n, x_{n-1}, \ldots, x_1)$.

7.2-2. Let $\mathscr{A} = \{(1, 2),\ (2, 3)\}$ and $\mathscr{B} = \{(1, 1, 0),\ (0, 1, 1),\ (2, 2, 3)\}$. Show that $\mathscr{A}$ and $\mathscr{B}$ are bases of $\mathbb{R}^2$ and $\mathbb{R}^2$, respectively. Define $\sigma : \mathbb{R}^2 \to \mathbb{R}^3$ by $\sigma(x, y) = (x - y, x + y, y)$. Compute $[\sigma]_{\mathscr{B}}^{\mathscr{A}}$.

7.2-3. Define $\sigma : M_2(\mathbb{R}) \to P_3(\mathbb{R})$ by $\sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a+b) + 2dx + bx^2$. Let $\mathscr{A} = \{E^{1,1}, E^{1,2}, E^{2,1}, E^{2,2}\}$ and $\mathscr{B} = \{1, x, x^2\}$ be the standard bases of $M_2(\mathbb{R})$ and $P_3(\mathbb{R})$, respectively. Show that σ is linear and compute $[\sigma]_{\mathscr{B}}^{\mathscr{A}}$.

7.2-4. Define $\sigma : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ by $\sigma(X) = AX - XA$, here $A = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$.

(a) Show that σ is linear.

(b) Represent σ by matrix using the standard basis of $M_2(\mathbb{R})$ (see Problem 7.2-3).

(c) Find the eigenpairs of the matrix obtained from (b) (note that, these eigenpairs are called *eigenpairs of* σ).

(d) Find all X such that $AX = XA$.

7.2-5. Define $\sigma : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ by $\sigma(A) = A^T$. Show that σ is linear and compute $[\sigma]_{\mathscr{A}}$, where $\mathscr{A}$ is the standard basis of $M_2(\mathbb{R})$.

7.2-6. Define $\sigma : M_2(\mathbb{R}) \to \mathbb{R}$ by $\sigma(A) = \text{Tr}(A)$. Show that σ is linear and compute $[\sigma]_{\mathscr{B}}^{\mathscr{A}}$, where $\mathscr{A}$ and $\mathscr{B}$ are the standard bases of $M_2(\mathbb{R})$ and $\mathbb{R}$ respectively.

7.2-7. Let V be a vector space with ordered basis $\mathscr{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Put $\alpha_0 = \mathbf{0}$. Suppose $\sigma : V \to V$ is a linear transformation such that $\sigma(\alpha_j) = \alpha_j + \alpha_{j-1}$ for $1 \leq j \leq n$. Compute $[\sigma]_{\mathscr{A}}$.

7.2-8. Let $D : P_3(\mathbb{R}) \to P_3(\mathbb{R})$ be the differential operator $\dfrac{d}{dx}$. Find the matrix representation of D with respect to the bases $\{1,\ 1 + 2x,\ 4x^2 - 3\}$ and $\{1, x, x^2\}$.

7.2-9. Let $\mathscr{A} = \{(2, 4),\ (3, 1)\}$ be a basis of $\mathbb{R}^2$. What is the 2×1 matrix X that represents the vector $(2, 1)$ with respect to $\mathscr{A}$?

7.2-10. Find the formula of the reflection about the line $y = \sqrt{3}x$ in the xy-plane.

7.3 Change of Basis

The 'clothes' of a linear transformation $\sigma : U \to V$ is just the matrix representing the transformation via bases of U and V respectively. The 'look' of the transformation depends on the bases chosen. If we change 'clothes' the transformation will have a different 'look'. Let us consider the identity transformation first.

Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$, $\mathscr{B} = \{\beta_1, \ldots, \beta_n\}$ be two bases of U. For avoiding confusion, we let U' be the vector space U with the ordered basis $\mathscr{B}$. Since $\beta_j \in U$ for $1 \leq j \leq n$, there exist $p_{ij} \in \mathbb{F}$ such that $\beta_j = \sum_{i=1}^{n} p_{ij}\alpha_i$. The associated matrix $P = (p_{ij})$ is called the *matrix of transition from $\mathscr{A}$ to $\mathscr{B}$* or *transition matrix from $\mathscr{A}$ to $\mathscr{B}$*.

Consider the identity transformation $\iota : U' \to U$. Since $\iota(\beta_j) = \beta_j = \sum_{i=1}^{n} p_{ij}\alpha_i$, $[\iota]_{\mathscr{A}}^{\mathscr{B}} = P$. On the other hand, we consider the identity transformation $\iota : U \to U'$ and want to find $[\iota]_{\mathscr{B}}^{\mathscr{A}}$.

Let $Q = [\iota]_{\mathscr{B}}^{\mathscr{A}} = (q_{ki})$, i.e., $\alpha_i = \sum_{k=1}^{n} q_{ki}\beta_k$. Then for each i,

$$\alpha_i = \sum_{k=1}^{n} q_{ki}\beta_k = \sum_{k=1}^{n} q_{ki} \sum_{j=1}^{n} p_{jk}\alpha_j = \sum_{j=1}^{n} \left(\sum_{k=1}^{n} p_{jk}q_{ki} \right) \alpha_j.$$

Thus we have $\sum_{k=1}^{n} p_{jk}q_{ki} = \delta_{ji}$. Hence $PQ = I$. That is, $[\iota]_{\mathscr{B}}^{\mathscr{A}} = P^{-1}$.

Let $\alpha \in U = U'$. By Theorem 7.2.11

$$[\alpha]_{\mathscr{A}} = [\iota(\alpha)]_{\mathscr{A}} = [\iota]_{\mathscr{A}}^{\mathscr{B}}[\alpha]_{\mathscr{B}} = P[\alpha]_{\mathscr{B}} \text{ or } [\alpha]_{\mathscr{B}} = P^{-1}[\alpha]_{\mathscr{A}}. \tag{7.1}$$

So the above formula shows the relation of the coordinates between different bases.

Theorem 7.3.1 *Suppose $\sigma \in L(U, V)$. Suppose $A = [\sigma]_{\mathscr{C}}^{\mathscr{A}}$, where $\mathscr{A}$ and $\mathscr{C}$ are bases of U and V, respectively. Suppose $A' = [\sigma]_{\mathscr{D}}^{\mathscr{B}}$, where $\mathscr{B}$ and $\mathscr{D}$ are other bases of U and V, respectively. Let $P = [\iota_U]_{\mathscr{A}}^{\mathscr{B}}$ and $Q = [\iota_V]_{\mathscr{C}}^{\mathscr{D}}$ be matrices of transition from $\mathscr{A}$ to $\mathscr{B}$ and $\mathscr{C}$ to $\mathscr{D}$, respectively. Here ι_U and ι_V denote the identity transformation of U and V, respectively. Then $A' = Q^{-1}AP$.*

Proof: Since $\iota_V \circ \sigma = \sigma = \sigma \circ \iota_U$ and by Theorem 7.2.9,

$$[\iota_V]_{\mathscr{C}}^{\mathscr{D}}[\sigma]_{\mathscr{D}}^{\mathscr{B}} = [\sigma]_{\mathscr{C}}^{\mathscr{B}} = [\sigma]_{\mathscr{C}}^{\mathscr{A}}[\iota_U]_{\mathscr{A}}^{\mathscr{B}}.$$

Thus $QA' = [\sigma]_{\mathscr{C}}^{\mathscr{B}} = AP$, hence $A' = Q^{-1}AP$. □

Corollary 7.3.2 *Let us keep the notation in Theorem 7.3.1. If $\mathscr{A} = \mathscr{B}$, then $A' = Q^{-1}A$.*

Keeping the notation in Theorem 7.3.1. Suppose $U = V$, $\mathscr{A} = \mathscr{C}$ and $\mathscr{B} = \mathscr{D}$. Then by Theorem 7.3.1 we have the following corollary:

Corollary 7.3.3 *Suppose $\sigma \in L(V, V)$. Let $\mathscr{A}$ and $\mathscr{B}$ be two bases of V. Let P be the matrix of transition from $\mathscr{A}$ to $\mathscr{B}$. Then $[\sigma]_{\mathscr{B}} = P^{-1}[\sigma]_{\mathscr{A}}P$.*

Example 7.3.4 Let $\sigma : \mathbb{R}^3 \to \mathbb{R}^2$ be a linear transformation that $\sigma(\boldsymbol{e}_1) = (1, 1)$, $\sigma(\boldsymbol{e}_2) = (0, -2)$ and $\sigma(\boldsymbol{e}_3) = (1, 3)$. Let $\mathscr{B} = \{(1, 1, 1),\ (1, 0, -1),\ (0, 0, 1)\}$ and $\mathscr{D} = \{(1, -1),\ (1, 1)\}$ be bases of $\mathbb{R}^3$ and $\mathbb{R}^2$, respectively. Find $[\sigma]_{\mathscr{D}}^{\mathscr{B}}$.

Let $\mathscr{A} = \mathscr{S}_3$ and $\mathscr{C} = \mathscr{S}_2$ be the standard bases of $\mathbb{R}^3$ and $\mathbb{R}^2$, respectively. By the definition of σ we can easy to see that

$$A = [\sigma]_{\mathscr{S}_2}^{\mathscr{S}_3} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix}.$$

It is also easy to see that the matrix transition from $\mathscr{S}_3$ to $\mathscr{B}$ is $P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & -1 & 1 \end{pmatrix}$. The matrix transition from $\mathscr{S}_2$ to $\mathscr{D}$ is $Q = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. Then

$$[\sigma]_{\mathscr{D}}^{\mathscr{B}} = Q^{-1}AP = \tfrac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ 2 & -1 & 2 \end{pmatrix}. \qquad \square$$

Theorem 7.3.5 *Suppose $\sigma \in L(U,V)$. Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ and $\mathscr{C} = \{\beta_1, \ldots, \beta_m\}$ be bases of U and V, respectively. Then* $\operatorname{rank}(\sigma) = \operatorname{rank}([\sigma]_{\mathscr{C}}^{\mathscr{A}})$.

Proof: Choose a basis $\mathscr{B} = \{\alpha'_1, \ldots, \alpha'_n\}$ of U such that $\{\alpha'_{r+1}, \ldots, \alpha'_n\}$ is a basis of $\ker(\sigma)$. Since $\operatorname{rank}(\sigma) = r$, $\{\sigma(\alpha'_1), \ldots, \sigma(\alpha'_r)\}$ is a basis of $\sigma(U)$ and hence can be extended to a basis $\mathscr{D} = \{\beta'_1, \ldots, \beta'_m\}$ of V. Hence $\sigma(\alpha'_i) = \beta'_i$ for $i = 1, 2 \ldots, r$ and $\sigma(\alpha'_j) = \mathbf{0}$ for $j = r+1, \ldots, n$. Let $A' = [\sigma]_{\mathscr{D}}^{\mathscr{B}}$. Then

$$Q^{-1}AP = A' = \left(\begin{array}{c|c} I_r & O_{r,n-r} \\ \hline O_{m-r,r} & O_{m-r,n-r} \end{array}\right),$$

where P and Q are the respective transition matrices. Then $\operatorname{rank}(A') = r$. Since P and Q are invertible, by Theorem 2.4.11 $\operatorname{rank}(A) = r$. $\square$

Alternative proof of Theorem 7.3.5: Let $\alpha \in \ker(\sigma)$ and $A = [\sigma]_{\mathscr{C}}^{\mathscr{A}}$. Then $\mathbf{0}_m = [\sigma(\alpha)]_{\mathscr{C}} = A[\alpha]_{\mathscr{A}}$. Hence $[\alpha]_{\mathscr{A}} \in \ker(A)$. It is known that the mapping $\beta \mapsto [\beta]_{\mathscr{A}}$ is an isomorphism. So its restriction on $\ker(\sigma)$ is a monomorphism. For any $X = (x_1 \ \cdots \ x_n)^T \in \ker(A)$, let $\alpha = \sum_{i=1}^n x_i\alpha_i$. Then $[\sigma(\alpha)]_{\mathscr{C}} = AX = \mathbf{0}_m$. Hence $\alpha \in \ker(\sigma)$. Therefore, the mapping $\alpha \mapsto [\alpha]_{\mathscr{A}}$ is an isomorphism. Hence $\operatorname{nullity}(\sigma) = \operatorname{nullity}(A)$. By Theorems 7.1.17 and 3.6.9 we have $\operatorname{rank}(\sigma) = \operatorname{rank}(A)$. $\square$

Suppose $A \in M_{m,n}(\mathbb{F})$. We can choose a basis $\mathscr{A}$ of an n-dimensional vector space U (for example $\mathbb{F}^n$) and a basis $\mathscr{C}$ of an m dimensional vector space V (for example $\mathbb{F}^m$). Then by Theorem 7.1.26, we can define a linear transformation $\sigma : U \to V$ such that $[\sigma]_{\mathscr{C}}^{\mathscr{A}} = A$. If $\operatorname{rank}(A) = r$, then by Theorem 7.3.5 $\operatorname{rank}(\sigma) = r$.

The main purpose of changing basis is to make the linear transformation $\sigma : U \to V$ looks nicer, for example, upper triangular or diagonal. To do this we may have to change the basis of U. This is equivalent to multiply the representing matrix on the left by a non-singular matrix. To attain this goal, we may simply apply a sequence of elementary row operations to the representing matrix. Or we would like to change basis of V which can sometimes be obtained by applying a sequence of elementary column operations.

When $U = V$, the representing matrix of σ is a square matrix. Diagonalizing a square matrix is just choosing the right basis of U so that the new representing matrix is diagonal if this is possible.

Exercise 7.3

7.3-1. Find the matrix of transition in $P_3(\mathbb{R})$ from the basis $\mathscr{A} = \{1,\ 1+2x,\ 4x^2-3\}$ to $\mathscr{S} = \{1,\ x,\ x^2\}$. [Hint: Find the matrices of transitions from $\mathscr{S}$ to $\mathscr{A}$ first.]

7.3-2. Suppose $\mathscr{A} = \{x^2-x+1,\ x+1,\ x^2+1\}$ and $\mathscr{B} = \{x^2+x+4,\ 4x^2-3x+2,\ 2x^2+3\}$ are bases of $P_3(\mathbb{Q})$. What is the matrix of transition from $\mathscr{A}$ to $\mathscr{B}$? [Hint: Find the transition matrices from the standard basis $\mathscr{S} = \{1,\ x,\ x^2\}$ to $\mathscr{A}$ and to $\mathscr{B}$, respectively.]

7.3-3. Let $\sigma : P_3(\mathbb{R}) \to P_2(\mathbb{R})$ be defined by $\sigma(p) = p'$, the derivative of $p \in P_3(\mathbb{R})$. Let $\mathscr{A} = \{x^2-x+1,\ x+1,\ x^2+1\}$ and $\mathscr{C} = \{1+x,\ 1-x\}$ be bases of $P_3(\mathbb{R})$ and $P_2(\mathbb{R})$, respectively. Using transition matrices find $[\sigma]_{\mathscr{C}}^{\mathscr{A}}$.

7.3-4. Let σ be the linear transformation from $\mathbb{R}^3$ to $\mathbb{R}^3$ defined by

$$\sigma(x,y,z) = (3x-y-2z,\ 2x-2z,\ 2x-y-z).$$

Find the matrix A representing σ with respect to the basis

$$\{(1,1,1),\ (1,2,0),\ (0,-2,1)\}.$$

Chapter 8

Diagonal Form and Jordan Form

8.1 Diagonal Form

In Chapter 7, we knew that the matrix representation of a linear transformation between two vector spaces U and V depends on the choice of bases. In this chapter, we consider the special case when $U = V$. In this case we choose the same (ordered) basis $\mathscr{A}$ for U and V. If we change the basis from $\mathscr{A}$ to $\mathscr{B}$, then for $\sigma \in L(V, V)$ we knew from Theorem 7.3.1 or Corollary 7.3.3 that

$$[\sigma]_{\mathscr{B}} = P^{-1}[\sigma]_{\mathscr{A}}P,$$

where P is the matrix of transition from $\mathscr{A}$ to $\mathscr{B}$. In this chapter, we want to find a basis of V such that the matrix representation of σ is as simple as possible. In matrix theory terminology, it is equivalent to finding an invertible matrix P such that $P^{-1}AP$ as simple as possible for a given square matrix A. The simplest form is diagonal matrix. So our question is whether A is diagonalizable. We have discussed this topic in Chapter 5. We have two tests for the diagonalizability of A in Theorems 5.3.6 and 5.3.10. However the proof of Theorem 5.3.10 has not yet completed. We shall finish the proof of it. In this chapter, all vector spaces are finite dimensional and all linear transformations are in $L(V, V)$ for some vector space V.

Let $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ and $\sigma \in L(V, V)$. We define that

$$f(\sigma) = a_k\sigma^k + \cdots + a_1\sigma + a_0\iota,$$

where ι is the identity mapping and $\sigma^i = \overbrace{\sigma \circ \cdots \circ \sigma}^{i \text{ times}}$ for $i \geq 1$.

Since the characteristic polynomials of two similar matrices are the same, we can make the following definition.

Definition 8.1.1 The characteristic polynomial of any matrix representing the linear transformation σ is called the *characteristic polynomial of* σ. This is well defined since any two representing matrices are similar and hence have the same characteristic polynomial. We shall write the characteristic polynomial of σ as $C_\sigma(x)$ or $C(x)$.

It is easy to see that the (monic) minimum polynomials of two similar matrices are the same (Proposition 5.2.7). So we say that the *monic minimum polynomial* of a linear transformation σ is the minimum polynomial of any matrix representing it. For short, we call the monic minimum polynomial of a linear transformation the *minimum polynomial*.

Only the zero matrix represents the zero linear transformation and vice versa. Suppose $f(x)$ is the characteristic or minimum polynomial of a linear transformation σ. Then $f(\sigma) = O$, the zero linear transformation.

Definition 8.1.2 Let $\sigma \in L(V, V)$. A nonzero vector $\alpha \in V$ is called an *eigenvector of* σ *corresponding to eigenvalue* λ, for some $\lambda \in \mathbb{F}$, if $\sigma(\alpha) = \lambda\alpha$. σ is *diagonalizable* if there is a basis $\mathscr{B}$ of V such that $[\sigma]_{\mathscr{B}}$ is a diagonal matrix. That is, the basis $\mathscr{B}$ consists of eigenvectors of σ.

Theorem 5.3.10 (**Second Test for Diagonalizability**) *$A \in M_n(\mathbb{F})$ is diagonalizable over $\mathbb{F}$ if and only if the monic minimum polynomial of A has the form*

$$m(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_p),$$

where $\lambda_1, \lambda_2, \ldots, \lambda_p$ are distinct scalars (eigenvalues of A).

Proof: It remains to prove the " if" part as the "only if" part had been done in Chapter 5. By Example 7.2.7 we can choose a linear transformation $\sigma_A : V \to V$ such that A is its representing matrix. Suppose

$$m(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_p)$$

is the minimum polynomial of A with λ_i all distinct.

If $p = 1$, then $\sigma = \lambda_1\iota$. Hence it is diagonalizable. So we assume $p \geq 2$. Let $M_j = \ker(\sigma - \lambda_j\iota)$, $1 \leq j \leq p$. Nonzero vectors in M_j are eigenvectors of σ corresponding to λ_j. By Theorem 5.3.1 $M_j \cap \sum_{i \neq j} M_i = \{\mathbf{0}\}$. Thus the sum $\sum_{j=1}^{p} M_j$ is direct. Let $m_j = \dim M_j = \text{nullity}(\sigma - \lambda_j\iota)$ and $\text{rank}(\sigma - \lambda_j\iota) = r_j$. Since $M_1 \oplus \cdots \oplus M_p \subseteq V$, we have $m_1 + \cdots + m_p \leq n$. By Theorem 7.1.17 we have

$$r_j = \text{rank}(\sigma - \lambda_j\iota) = n - \text{nullity}(\sigma - \lambda_j\iota) = n - m_j.$$

Also, by Theorem 7.1.20

$$\begin{aligned}\dim\big([(\sigma - \lambda_1\iota) \circ (\sigma - \lambda_2\iota)](V)\big) &= \text{rank}[(\sigma - \lambda_1\iota) \circ (\sigma - \lambda_2\iota)] \\ &= \text{rank}(\sigma - \lambda_2\iota) - \dim\big[(\sigma - \lambda_2\iota)(V) \cap \ker(\sigma - \lambda_1\iota)\big] \\ &\geq r_2 - m_1 = n - (m_2 + m_1).\end{aligned}$$

Repeating use of the same idea, we have

$$0 = \dim(m(\sigma)(V)) = \dim\big([(\sigma - \lambda_1\iota) \circ \cdots \circ (\sigma - \lambda_p\iota)](V)\big) \geq n - \sum_{j=1}^{p} m_j.$$

Hence $m_1 + \cdots + m_p \geq n$. Therefore, $m_1 + \cdots + m_p = n$. This show that $V = M_1 \oplus \cdots \oplus M_p$. Since every nonzero vector of M_j is an eigenvector of σ, V has a basis consisting of eigenvectors of σ. Hence σ is diagonalizable, i.e., A is diagonalizable. □

This theorem is not useful in practice as it is usually very tedious to find a minimum polynomial. In fact, we may just go ahead to find a basis consisting of eigenvectors if such a basis exists. If so, then the matrix is diagonalizable. Otherwise, it is not.

The subspace $\ker(\sigma - \lambda\iota)$ for some eigenvalue λ in the proof of Theorem 5.3.10 is called the *eigenspace of* λ and is denoted by $\mathscr{E}(\lambda)$. This concept is agreed with the eigenspace defined in Chapter 5. So we use the same notation.

Examples 8.1.3

1. Let $A = \begin{pmatrix} -1 & 2 & 2 \\ 2 & 2 & 2 \\ -3 & -6 & -6 \end{pmatrix} \in M_3(\mathbb{Q})$. Then the eigenvalues are $-2, -3$ and 0. By Corollary 5.3.8 A is diagonalizable. In fact, we can find three linearly independent eigenvectors $\alpha_1 = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}$, $\alpha_2 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ and $\alpha_3 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$ corresponding to the eigenvalues -2, -3 and 0, respectively. Thus

$$P = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix} \text{ and } P^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -2 & -2 \\ 1 & 2 & 1 \end{pmatrix},$$

and hence

$$P^{-1}AP = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

□

2. Let $A = \begin{pmatrix} 1 & 1 & -1 \\ -1 & 3 & -1 \\ -1 & 2 & 0 \end{pmatrix} \in M_3(\mathbb{Q})$. Then the eigenvalues are $2, 1$ and 1. An eigenvector corresponding to $\lambda_1 = 2$ is $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$. However, for $\lambda_2 = 1$, we can only obtain one linearly independent eigenvector $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$. Thus A is not diagonalizable. □

Definition 8.1.4 Let V be a vector space and $\sigma \in L(V, V)$. A subspace W of V is said to be *invariant under* σ if $\sigma(W) \subseteq W$. W is also called an *invariant subspace*.

Clearly, if $\sigma \in L(V, V)$, then V, $\{\mathbf{0}\}$, eigenspaces and their sums are invariant subspaces.

Theorem 8.1.5 *Let V be a vector space with a basis consisting of eigenvectors of $\sigma \in L(V, V)$. If W is a subspace of V invariant under σ, then W also has a basis consisting of eigenvectors of σ.*

Proof: Suppose $\{\beta_1, \ldots, \beta_n\}$ is a basis of V consisting of eigenvectors of σ. Let $\alpha \in W$. Then $\alpha = \sum_{i=1}^{n} a_i\beta_i$ for some scalar $a_1, \ldots, a_n$. Suppose $a_i \neq 0$, $a_j \neq 0$ and $\beta_i, \beta_j \in \mathscr{E}(\lambda)$. Then $\gamma = a_i\beta_i + a_j\beta_j \in \mathscr{E}(\lambda)$. We do this for each i with $a_i \neq 0$. Then we can represent α as $\alpha = \sum_{i=1}^{p} \gamma_i$ for some p, where γ_i are eigenvectors of σ corresponding to distinct eigenvalues λ_i, respectively.

Since W is invariant under σ, W is invariant under $\sigma - k\iota$ for any scalar k. Thus $\big[(\sigma - \lambda_2\iota) \circ \cdots \circ (\sigma - \lambda_p\iota)\big](\alpha) \in W$. But

$$\begin{aligned}\big[(\sigma - \lambda_2\iota) \circ \cdots \circ (\sigma - \lambda_p\iota)\big](\alpha) &= \big[(\sigma - \lambda_2\iota) \circ \cdots \circ (\sigma - \lambda_p\iota)\big]\left(\sum_{i=1}^{p} \gamma_i\right) \\ &= \sum_{i=1}^{p} \big[(\sigma - \lambda_2\iota) \circ \cdots \circ (\sigma - \lambda_p\iota)\big](\gamma_i) \\ &= (\lambda_1 - \lambda_2)(\lambda_1 - \lambda_3) \cdots (\lambda_1 - \lambda_p)\gamma_1.\end{aligned}$$

Since $\lambda_j \neq \lambda_1$ for all $j \neq 1$, we have $\gamma_1 \in W$.

Similarly, we can show that $\gamma_2, \ldots, \gamma_p \in W$. Since α is arbitrary, this shows that W is spanned by eigenvectors of σ in W. Thus W contains a basis consisting of eigenvectors of σ. □

Theorem 8.1.6 *Let $\sigma \in L(V, V)$. If V has a basis consisting of eigenvectors of σ, then for every invariant subspace S there is an invariant subspace T such that $V = S \oplus T$.*

Proof: Suppose $\mathscr{B} = \{\beta_1, \ldots, \beta_n\}$ is a basis of V consisting of eigenvectors of σ. Let S be any invariant subspace of V. By Theorem 8.1.5 S has a basis consisting of eigenvectors of σ, say $\{\gamma_1, \ldots, \gamma_s\}$. Using the method used in the proof of the Steintz Replacement Theorem (Theorem 6.4.6) we obtain a basis $\{\gamma_1, \ldots, \gamma_s, \beta'_{s+1}, \ldots, \beta'_n\}$, where $\{\beta'_{s+1}, \ldots, \beta'_n\} \subseteq \mathscr{B}$. Put $T = \operatorname{span}(\beta'_{s+1}, \ldots, \beta'_n)$. Then clearly T is invariant under σ and $V = S \oplus T$. □

In general, the converse of the above theorem is not true. But it is true for vector spaces over $\mathbb{C}$.

Theorem 8.1.7 *Let V be a vector space over $\mathbb{C}$ and let $\sigma \in L(V, V)$. Suppose that for every subspace S invariant under σ there is a subspace T also invariant under σ such that $V = S \oplus T$. Then V has a basis consisting of eigenvectors of σ.*

Proof: We shall prove this theorem by mathematical induction on $n = \dim V$.

If $n = 1$, then any nonzero vector is an eigenvector of σ and hence the theorem is true.

Assume the theorem holds for vector spaces of dimension less than n, $n \geq 2$. Now suppose V is an n-dimensional vector space over $\mathbb{C}$ satisfying the hypothesis of this theorem. By fundamental theorem of algebra, the characteristic polynomial of σ has at least one root λ_1, i.e., λ_1 is an eigenvalue of σ. Let α_1 be an eigenvector corresponding to λ_1. Clearly, the subspace $S_1 = \operatorname{span}(\alpha_1)$ is invariant under σ. By the assumption, there is a subspace T_1 invariant under σ such that $V = S_1 \oplus T_1$. Clearly $\dim T_1 = n - 1$. To apply the induction hypothesis we have to show that every subspace S_2 of T_1 invariant under $\sigma_1 = \sigma\big|_{T_1}$ there is a subspace T_2 of T_1 which is invariant under σ_1.

Now suppose S_2 is a subspace of T_1 invariant under σ_1. Then $\sigma(S_2) = \sigma_1(S_2) \subseteq S_2$. That is, S_2 is invariant under σ. Thus by the hypothesis there exists a subspace T'_2 of V invariant under σ such that $V = S_2 \oplus T'_2$. Since $S_2 \subseteq T_1$,

$$T_1 = T_1 \cap V = T_1 \cap (S_2 \oplus T'_2) = (T_1 \cap S_2) \oplus (T_1 \cap T'_2) = S_2 \oplus (T_1 \cap T'_2)$$

(we leave the proof of the above equalities to the reader). Since $T_1 \cap T'_2$ is invariant under σ, it is invariant under σ_1. Put $T_2 = T_1 \cap T'_2$. By induction hypothesis T_1 has a basis $\{\alpha_2, \ldots, \alpha_n\}$ consisting of eigenvectors of σ_1. Since these vectors are in T_1, they are also eigenvectors of σ. Thus $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of V consisting of eigenvectors of σ. □

Note that we do not require $\mathbb{F} = \mathbb{C}$ in the above theorem. All we need is σ has all its eigenvalues in $\mathbb{F}$. That means the characteristic polynomial $C_\sigma(x)$ can be written as a product of linear factors over $\mathbb{F}$. In this case, we say that $C_\sigma(x)$ *splits* over $\mathbb{F}$.

Example 8.1.8 Let $A = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix} \in M_2(\mathbb{Q})$. We want to find A^k for $k \in \mathbb{N}$.

Solution: It is easy to see that the eigenvalues of A are 1 and 2. Since the eigenvalues are distinct, A is diagonalizable. It is easy to see that if $P = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}$, then $P^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix}$ and $P^{-1}AP = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = D$. Now since $A = PDP^{-1}$,

$$A^k = (PDP^{-1})^k = \underbrace{(PDP^{-1})(PDP^{-1})\cdots(PDP^{-1})}_{k \text{ times}} = PD^kP^{-1}$$

$$= \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 2-2^k & 2-2^{k+1} \\ -1+2^k & -1+2^{k+1} \end{pmatrix}.$$

□

Example 8.1.9 Prove that if $A \in M_n(\mathbb{Q})$ such that $A^3 = A$ then A is diagonalizable over $\mathbb{Q}$. Moreover, the eigenvalues of A are either 0, 1 or -1.

Proof: Let $g(x) = x^3 - x$. Then $g(A) = O$. So if $m(x)$ is the minimum polynomial of A (remind that it is the monic one), then $m(x)|g(x) = x(x-1)(x+1)$. Thus $m(x)$ must factor into distinct linear factors. Hence A is diagonalizable.

Thus, there exists an invertible matrix P such that $P^{-1}AP = D$, a diagonal matrix. Then

$$D^3 = (P^{-1}AP)^3 = P^{-1}A^3P = P^{-1}AP = D.$$

Put $D = \operatorname{diag}\{d_1, d_2, \ldots, d_n\}$. Then we have $d_i^3 = d_i$ for all i. Thus $d_i = 0, 1$ or -1. Since d_i are just the eigenvalues of A, hence our assertion is proved. Note that this result also follows from Theorem 5.2.9 and Corollary 5.2.9. □

Example 8.1.10 Characterize all the real 2×2 matrices A for which $A^2 - 3A + 2I = O$.

Solution: Let $g(x) = x^2 - 3x + 2 = (x-1)(x-2)$. From $g(A) = O$ we see that the minimum polynomial $m(x)$ of A must be one of form: $x-1$, $x-2$ or $(x-1)(x-2)$.

If $m(x) = x - 1$, then $A = I$.

If $m(x) = x - 2$, then $A = 2I$.

If $m(x) = (x-1)(x-2)$, then A is diagonalizable and hence similar to $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. □

Exercise 8.1

8.1-1. Let $\sigma \in L(V, V)$. Prove that if $g(x) \in F[x]$ and α is an eigenvector of σ corresponding to eigenvalue λ, then $g(\sigma)(\alpha) = g(\lambda)\alpha$.

8.1-2. Show that if every vector in V is an eigenvector of σ, then σ must be a scalar transformation, i.e., $\sigma = k\iota$ for some $k \in \mathbb{F}$.

8.1-3. Let $A = \begin{pmatrix} -3 & 1 & 5 \\ 7 & 2 & -6 \\ 1 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{R})$. Find A^k for $k \in \mathbb{N}$.

8.1-4. Let $A = \begin{pmatrix} 4 & 1 & 1 \\ 0 & 4 & 5 \\ 0 & 3 & 6 \end{pmatrix} \in M_3(\mathbb{R})$. Find a matrix B such that $B^2 = A$. [Hint: First, find an invertible matrix P such that $P^{-1}AP = D$, a diagonal matrix. Next, find C such that $C^2 = D$.

8.1-5. Let $x_0 = 0, x_1 = \frac{1}{2}$ and $x_k = \frac{1}{2}(x_{k-1} + x_{k-2})$ for $k \geq 2$. Find a formula for x_k by setting a matrix A and diagonalize it. Also find $\lim_{k\to\infty} x_k$.

8.1-6. Show that the matrix $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ with $c \neq 0$ is not diagonalizable.

8.1-7. Prove that the matrix J_n is similar to $\begin{pmatrix} n & \mathbf{0}_{n-1}^T \\ \mathbf{0}_{n-1} & O_{n-1} \end{pmatrix}$.

8.1-8. Can you find two matrices that have the same characteristic polynomial but are not similar?

8.1-9. Prove that two diagonal matrices are similar if and only if the diagonal elements of one are simply a rearrangement of the diagonal elements of the other.

8.2 Jordan Form

There are some matrices that cannot be diagonalized. The best possible simple form that we can get is so-called Jordan form. Before introducing Jordan form, we define some concepts first.

Definition 8.2.1 Let $\sigma \in L(V, V)$. A nonzero vector $\alpha \in V$ is called a *generalized eigenvector* of σ if there exists a scalar λ and positive integer s such that $(\sigma - \lambda\iota)^s(\alpha) = \mathbf{0}$. We say that α is a *generalized eigenvector corresponding to* λ. Hence, an eigenvector is also a generalized eigenvector.

Note that if α is a generalized eigenvector corresponding to λ, then λ is an eigenvalue of σ. If s is the smallest positive integer such that $(\sigma - \lambda\iota)^s(\alpha) = \mathbf{0}$, then $\beta = (\sigma - \lambda\iota)^{s-1}(\alpha) \neq \mathbf{0}$ is an eigenvector of σ corresponding to the eigenvalue λ.

Definition 8.2.2 Let $\sigma \in L(V, V)$. Suppose α is a generalized eigenvector of σ corresponding to eigenvalue λ. If s denotes the smallest positive integer such that $(\sigma - \lambda\iota)^s(\alpha) = \mathbf{0}$, then the ordered set

$$Z(\alpha; \sigma, \lambda) = \{(\sigma - \lambda\iota)^{s-1}(\alpha), (\sigma - \lambda\iota)^{s-2}(\alpha), \ldots, (\sigma - \lambda\iota)(\alpha), \alpha\} = (Z(\alpha; \lambda) \text{ for short})$$

is called a *cycle of generalized eigenvectors of* σ *corresponding to* λ. The elements $(\sigma - \lambda\iota)^{s-1}(\alpha)$ and α are called the *initial vector* and the *end vector* of the cycle, respectively. Also we say that *length of the cycle* is s.

Let λ be an eigenvalue of $\sigma \in L(V, V)$ and α be a generalized eigenvector corresponding to λ. Then each element of $Z(\alpha; \lambda)$ is a generalized eigenvector of σ. Let

$$\begin{aligned} \mathscr{K}(\lambda) &= \{\alpha \in V \mid \alpha \text{ is a generalized eigenvector corresponding to } \lambda\} \cup \{\mathbf{0}\} \\ &= \{\alpha \in V \mid (\sigma - \lambda\iota)^s(\alpha) = \mathbf{0} \text{ for some nonnegative integer } s\}. \end{aligned}$$

Then $Z(\alpha; \lambda) \subseteq \mathscr{K}(\lambda)$. In the following we shall consider the set $\mathscr{K}(\lambda)$. Under some condition we try to partition it into a collection of mutually disjoint cycles of generalized eigenvectors.

Theorem 8.2.3 *Let λ be an eigenvalue of $\sigma \in L(V,V)$. The set $\mathscr{K}(\lambda)$ is a subspace of V containing the eigenspace $\mathscr{E}(\lambda)$ and is invariant under σ.*

Proof: Clearly $\mathscr{E}(\lambda) \subseteq \mathscr{K}(\lambda)$. Suppose $\alpha, \beta \in \mathscr{K}(\lambda)$ and $c \in \mathbb{F}$. There are nonnegative integers s and t such that $(\sigma - \lambda\iota)^s(\alpha) = \mathbf{0}$ and $(\sigma - \lambda\iota)^t(\beta) = \mathbf{0}$. Then $(\sigma - \lambda\iota)^r(c\alpha + \beta) = \mathbf{0}$, where $r = \max\{s,t\}$. Hence $\mathscr{K}(\lambda)$ is a subspace of V. For each $\alpha \in \mathscr{K}(\lambda)$, there is a nonnegative integer s such that $(\sigma - \lambda\iota)^s(\alpha) = \mathbf{0}$. Then

$$(\sigma - \lambda\iota)^s(\sigma(\alpha)) = [(\sigma - \lambda\iota)^s \circ \sigma](\alpha) = [\sigma \circ (\sigma - \lambda\iota)^s](\alpha) = \sigma((\sigma - \lambda\iota)^s(\alpha)) = \mathbf{0}.$$

Therefore, $\sigma(\alpha) \in \mathscr{K}(\lambda)$ and hence $\mathscr{K}(\lambda)$ is invariant under σ. □

Definition 8.2.4 The subspace $\mathscr{K}(\lambda)$ is called the *generalized eigenspace corresponding to* λ.

Theorem 8.2.5 *Let the ordered set $\{\alpha_1, \ldots, \alpha_k\}$ be a cycle of generalized eigenvectors of σ corresponding to eigenvalue λ. Then the initial vector α_1 is an eigenvector and α_i is not an eigenvector of σ for each $i \geq 2$. Also $\{\alpha_1, \ldots, \alpha_k\}$ is linearly independent.*

Proof: We only need to prove that $\{\alpha_1, \ldots, \alpha_k\}$ is linearly independent. To do this, we prove by mathematical induction on k, the length of the cycle.

If $k = 1$, then the theorem is trivial.

Assume $k \geq 2$ and that cycles of length less than k are linearly independent.

Let $\{\alpha_1, \ldots, \alpha_k\}$ be a cycle of generalized eigenvectors of σ corresponding to λ. Suppose $a_1, \ldots, a_k$ are scalars such that $\sum_{i=1}^{k} a_i\alpha_i = \mathbf{0}$. By the definition of cycle, we have $\alpha_i = (\sigma - \lambda\iota)^{k-i}(\alpha_k)$ for $1 \leq i \leq k$. Now

$$\mathbf{0} = (\sigma - \lambda\iota)\left(\sum_{i=1}^{k} a_i\alpha_i\right) = \sum_{i=1}^{k} a_i(\sigma - \lambda\iota) \circ (\sigma - \lambda\iota)^{k-i}(\alpha_k) = \sum_{i=2}^{k} a_i(\sigma - \lambda\iota)^{k-i+1}(\alpha_k) = \sum_{i=2}^{k} a_i\alpha_{i-1}.$$

This is a linear relation among the ordered set $Z = \{\alpha_1, \ldots, \alpha_{k-1}\}$. Clearly Z is a cycle of generalized eigenvectors of σ corresponding to eigenvalue λ of length $k-1$. Thus by mathematical induction hypothesis, we have $a_i = 0$ for $2 \leq i \leq k$. This shows that $a_1 = 0$ as well, so $\{\alpha_1, \ldots, \alpha_k\}$ is linearly independent. □

Let $\sigma \in L(V,V)$. Suppose that there is a basis $\mathscr{B}$ of V such that

$$J = [\sigma]_{\mathscr{B}} = \begin{pmatrix} J_1 & O & \cdots & O \\ O & J_2 & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & J_p \end{pmatrix}$$

for some $p \geq 1$, where J_i is an $m_i \times m_i$ matrix of the form $(\lambda)_{1\times 1}$ when $m_i = 1$ or

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \ddots & \ddots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix} \quad \text{when } m_i \geq 2,$$

for some eigenvalue λ of σ. Such a matrix J_i is called a *Jordan block corresponding to* λ, and the matrix J is called a *Jordan canonical form of* σ or *Jordan form* for short. $\mathscr{B}$ is called a *Jordan canonical basis corresponding to* σ or *Jordan basis corresponding to* σ for short.

Example 8.2.6 Let

$$J = \left(\begin{array}{|ccc|c|cc|cc} \hline 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}\right).$$

Then J is a Jordan form. Let $\sigma \in L(\mathbb{C}^8, \mathbb{C}^8)$ defined by $\sigma(X) = JX$ for $X \in \mathbb{C}^8$. Then $[\sigma]_{\mathscr{S}} = J$, where $\mathscr{S}$ is the standard basis of $\mathbb{C}^8$ over $\mathbb{C}$.

It is clear that $C_J(x) = C_\sigma(x) = (3-x)^3(2-x)^3x^2$. One can check that the minimum polynomial of σ is $(x-3)^3(x-2)^2x^2$. By Theorem 5.3.10 σ is not diagonalizable. Also we observe that of the vectors $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_8$ only $\boldsymbol{e}_1, \boldsymbol{e}_4, \boldsymbol{e}_5, \boldsymbol{e}_7$ are eigenvectors of σ.

Consider $\eta = \sigma - 3\iota$. Then

$$\eta(\boldsymbol{e}_3) = (\sigma - 3\iota)(\boldsymbol{e}_3) = \sigma(\boldsymbol{e}_3) - 3\boldsymbol{e}_3 = 3\boldsymbol{e}_3 + \boldsymbol{e}_2 - 3\boldsymbol{e}_3 = \boldsymbol{e}_2; \quad \eta^2(\boldsymbol{e}_3) = \eta(\boldsymbol{e}_2) = \boldsymbol{e}_1.$$

So $Z(\boldsymbol{e}_3; 3) = \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$. Similarly $Z(\boldsymbol{e}_4; 2) = \{\boldsymbol{e}_4\}$, $Z(\boldsymbol{e}_6; 2) = \{\boldsymbol{e}_5, \boldsymbol{e}_6\}$ and $Z(\boldsymbol{e}_8; 0) = \{\boldsymbol{e}_7, \boldsymbol{e}_8\}$. □

From the above example, we see that a Jordan basis of V corresponding to σ is a disjoint union of cycles of generalized eigenvectors. The converse is clearly true. It is true in general. Now we state and prove this theorem.

Theorem 8.2.7 *Let $\mathscr{B}$ be a basis of V and let $\sigma \in L(V,V)$. Then $\mathscr{B}$ is a Jordan basis for V corresponding to σ if and only if $\mathscr{B}$ is a disjoint union of cycles of generalized eigenvectors of σ.*

Proof: Suppose $[\sigma]_{\mathscr{B}} = J = \begin{pmatrix} J_1 & O & \cdots & O \\ \vdots & \ddots & \ddots & \vdots \\ O & \ddots & \ddots & O \\ O & O & \cdots & J_p \end{pmatrix}$, where J_i's are Jordan blocks, $1 \leq i \leq p$. Suppose J_i is an $m_i \times m_i$ matrix. Then $n = \sum_{i=1}^{p} m_i$. We partition $\mathscr{B}$ into p classes $\mathscr{B}_1, \ldots, \mathscr{B}_p$ corresponding to the sizes of the Jordan blocks, i.e., $\mathscr{B}_1$ consists of the first m_1 vectors of $\mathscr{B}$, $\mathscr{B}_2$ consists the next m_2 vectors of $\mathscr{B}$, and so on. Let

$$\mathscr{B}_i = \{\beta_1, \ldots, \beta_{m_i}\} \text{ and } J_i = \begin{pmatrix} \lambda & 1 & \cdots & 0 \\ 0 & \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

Then by the definition of $[\sigma]_{\mathscr{B}}$,

$$\begin{aligned}\sigma(\beta_{m_i}) &= \lambda\beta_{m_i} + \beta_{m_i-1};\\ \sigma(\beta_{m_i-1}) &= \lambda\beta_{m_i-1} + \beta_{m_i-2};\\ &\vdots\\ \sigma(\beta_2) &= \lambda\beta_2 + \beta_1;\\ \sigma(\beta_1) &= \lambda\beta_1.\end{aligned}$$

If we let $\eta = \sigma - \lambda\iota$, then

$$\eta(\beta_{m_i}) = \beta_{m_i-1},\ \eta^2(\beta_{m_i}) = \beta_{m_i-2},\ \ldots,\ \eta^{m_i-1}(\beta_{m_i}) = \beta_1,\ \eta^{m_i}(\beta_{m_i}) = \mathbf{0}.$$

Then $\mathscr{B}_i = Z(\beta_{m_i}; \lambda)$. Therefore, $\mathscr{B}$ is a disjoint union of cycles of generalized eigenvectors of σ.

The "if" part is trivial. □

Lemma 8.2.8 *Let $\sigma \in L(V,V)$ and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be distinct eigenvalues of σ. For each i, $1 \le i \le k$, let $\alpha_i \in \mathscr{K}(\lambda_i)$. If $\alpha_1 + \alpha_2 + \cdots + \alpha_k = \mathbf{0}$, then $\alpha_i = \mathbf{0}$ for all i.*

Proof: We prove the lemma by mathematical induction on k. It is trivial for $k = 1$. Assume that the lemma holds for any $k-1$ distinct eigenvalues, where $k \ge 2$.

Suppose $\alpha_i \in \mathscr{K}(\lambda_i)$ for $1 \le i \le k$ satisfying $\alpha_1 + \alpha_2 + \cdots + \alpha_k = \mathbf{0}$. Suppose $\alpha_1 \ne \mathbf{0}$. For each i, let s_i be the smallest nonnegative integer for which $(\sigma - \lambda_i\iota)^{s_i}(\alpha_i) = \mathbf{0}$. Since $\alpha_1 \ne \mathbf{0}$, $s_1 \ge 1$. Let $\beta = (\sigma - \lambda_1\iota)^{s_1-1}(\alpha_1)$. Then β is an eigenvector of σ corresponding to λ_1. Let $g(x) = (x-\lambda_2)^{s_2}\cdots(x-\lambda_k)^{s_k}$. Then $g(\sigma)(\alpha_i) = \mathbf{0}$ for all $i > 1$. By the result of Exercise 8.1-1,

$$g(\sigma)(\beta) = g(\lambda_1)\beta = (\lambda_1-\lambda_2)^{s_2}\cdots(\lambda_1-\lambda_k)^{s_k}\beta \ne \mathbf{0}.$$

On the other hand,

$$\begin{aligned}g(\sigma)(\beta) &= g(\sigma)\big((\sigma-\lambda_1\iota)^{s_1-1}(\alpha_1)\big) = [g(\sigma)\circ(\sigma-\lambda_1\iota)^{s_1-1}](\alpha_1)\\ &= -(\sigma-\lambda_1\iota)^{s_1-1}\big(g(\sigma)(\alpha_2+\cdots+\alpha_k)\big) = \mathbf{0}.\end{aligned}$$

This is a contradiction. So α_1 must be $\mathbf{0}$ and then $\alpha_2+\cdots+\alpha_k = \mathbf{0}$. By induction assumption, $\alpha_i = \mathbf{0}$ for all i, $2 \le i \le k$. The lemma follows. □

Corollary 8.2.9 *The sum $\mathscr{K}(\lambda_1) + \mathscr{K}(\lambda_2) + \cdots + \mathscr{K}(\lambda_k)$ is direct.*

Proof: This corollary follows from Proposition 6.5.14 and Lemma 8.2.8. □

Lemma 8.2.10 *Let $\sigma \in L(V,V)$ with distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$. For each $i = 1, 2, \ldots, k$, let S_i be a linearly independent subset of $\mathscr{K}(\lambda_i)$. Then $S_1, S_2, \ldots, S_k$ are pairwise disjoint and $S = S_1 \cup S_2 \cup \cdots \cup S_k$ is a linearly independent subset of V.*

Proof: Suppose $\alpha \in S_i \cap S_j$ for some $i \ne j$. Then $\alpha \in \mathscr{K}(\lambda_i) \cap \mathscr{K}(\lambda_j)$. Since $\mathscr{K}(\lambda_i) + \mathscr{K}(\lambda_j)$ is direct, $\alpha = \mathbf{0}$. This contradicts the fact that α lies in a linearly independent set. Thus $S_i \cap S_j = \varnothing$ for $i \ne j$.

Suppose $S_i = \{\alpha_{i,1}, \ldots, \alpha_{i,m_i}\}$. Then $S = \{\alpha_{i,j} \mid 1 \le j \le m_i, 1 \le i \le k\}$. Suppose $\sum_{i=1}^{k}\sum_{j=1}^{m_i} a_{i,j}\alpha_{i,j} = \mathbf{0}$. Let $\beta_i = \sum_{j=1}^{m_i} a_{i,j}\alpha_{i,j}$. Then $\beta_i \in \mathscr{K}(\lambda_i)$ for each i and $\beta_1 + \cdots + \beta_k = \mathbf{0}$. By Lemma 8.2.8

$\beta_i = \mathbf{0}$ for all i. Since S_i is linearly independent for each i, $a_{i,j} = 0$ for all j. Therefore, S is linearly independent. □

Is $\mathscr{K}(\lambda_1) \oplus \mathscr{K}(\lambda_2) \oplus \cdots \oplus \mathscr{K}(\lambda_k) = V$ for some k? The answer is not affirmative. We have to impose some condition on the characteristic polynomial of the linear transformation σ.

Theorem 8.2.11 *Let $\sigma \in L(V,V)$. For each i with $1 \le i \le q$ let Z_i be a cycle of generalized eigenvectors of σ corresponding to the same λ with initial vector β_i. If $\{\beta_1, \ldots, \beta_q\}$ is linearly independent, then Z_i's are pairwise disjoint and $Z = \bigcup_{i=1}^{q} Z_i$ is linearly independent.*

Proof: Suppose $\alpha \in Z_i \cap Z_j$. There are two nonnegative integers s, t such that $(\sigma - \lambda\iota)^s(\alpha) = \beta_i$ and $(\sigma - \lambda\iota)^t(\alpha) = \beta_j$. Suppose $s \le t$. Then $\beta_i = (\sigma - \lambda\iota)^s(\alpha) \in Z_j$. Since β_i and β_j are eigenvectors of σ and β_j is the only eigenvector in Z_j, $\beta_i = \beta_j$ and hence $i = j$. Thus $Z_i \cap Z_j = \varnothing$ if $i \ne j$.

We prove the linearly independence of Z by mathematical induction on $|Z| = n$. If $n = 1$, then this is trivial. Assume that for $n \ge 2$, the result is true for $|Z| < n$.

Now suppose $|Z| = n$. Let $W = \operatorname{span}(Z)$ and let $\eta = \sigma - \lambda\iota$. Clearly W is invariant under η and $\dim W \le n$. Let $\phi = \eta\big|_W : W \to W$. For each i let Z_i' denote the cycle obtained from Z_i by deleting the end vector. Then $Z_i' = \phi(Z_i) \setminus \{\mathbf{0}\}$. Let $Z' = \bigcup_{i=1}^{q} Z_i'$. Then $\operatorname{span}(Z') = \phi(W)$. Since $|Z'| = n - q < n$ and the set of initial vectors of Z_i''s are the same as those of Z_i's. By induction assumption Z' is linearly independent. Then $\operatorname{rank}(\phi) = \dim(\phi(W)) = n - q$.

Since $\phi(\beta_i) = \eta(\beta_i) = \mathbf{0}$, $\beta_i \in \ker(\phi)$. Since $\{\beta_1, \ldots, \beta_q\}$ is linearly independent, $\dim(\ker(\phi)) = \operatorname{nullity}(\phi) \ge q$. By Theorem 7.1.17,

$$n \ge \dim W = \operatorname{rank}(\phi) + \operatorname{nullity}(\phi) \ge n - q + q = n.$$

So $\dim W = n$ and Z is a basis of W, and hence Z is linearly independent. □

Lemma 8.2.12 *Let $\sigma \in L(V,V)$ and let W be an invariant subspace of V under σ. Then the characteristic polynomial of $\sigma\big|_W$ divides the characteristic polynomial of σ.*

Proof: Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_k\}$ be a basis of W. Extend $\mathscr{A}$ to a basis $\mathscr{B}$ of V. Let $A = [\sigma]_{\mathscr{B}}$ and $B = \left[\sigma\big|_W\right]_{\mathscr{A}}$. Then it is clear that $A = \begin{pmatrix} B & C \\ O & D \end{pmatrix}$ for some matrices C and D. Then by Exercise 4.3-6 we have

$$C_A(x) = \det(A - xI) = \det \begin{pmatrix} B - xI & C \\ O & D - xI \end{pmatrix} = C_B(x) C_D(x).$$

Thus the lemma follows. □

Theorem 8.2.13 *Let V be an n-dimensional vector space over $\mathbb{F}$ and let $\sigma \in L(V,V)$. If the characteristic polynomial $C_\sigma(x)$ splits over $\mathbb{F}$, then there is a Jordan basis for V corresponding to σ; i.e., there is a basis for V that is a disjoint union of cycles of generalized eigenvectors of σ.*

Proof: We prove the theorem by mathematical induction on n. Clearly, the theorem is true for $n = 1$. Assume that the theorem is true for any vector space of dimension less than $n > 1$. Suppose $\dim V = n$. Since $C_\sigma(x)$ splits over $\mathbb{F}$, there is an eigenvalue λ_1 of σ. Let $r = \operatorname{rank}(\sigma - \lambda_1\iota)$. Since λ_1 is an eigenvalue, $U = (\sigma - \lambda_1\iota)(V)$ is an r-dimensional invariant subspace of V under σ and $r < n$. Let $\phi = \sigma\big|_U$. By Lemma 8.2.12 we have $C_\phi(x) | C_\sigma(x)$ and hence $C_\phi(x)$ splits over $\mathbb{F}$. By induction assumption, there is a Jordan basis $\mathscr{A}$ for U corresponding to ϕ as well as to σ.

We want to extend $\mathscr{A}$ to be a Jordan basis for V. Suppose σ has k distinct eigenvalues $\lambda_1, \ldots, \lambda_k$. For each j let S_j consist of the generalized eigenvectors in $\mathscr{A}$ corresponding to λ_j. Since $\mathscr{A}$ is a basis, S_j is linearly independent that is a disjoint union of cycles of generalized eigenvectors of λ_j. Let $Z_1 = Z(\alpha_1; \lambda_1)$, $Z_2 = Z(\alpha_2; \lambda_1)$, $\ldots$, $Z_p = Z(\alpha_p; \lambda_1)$ be the disjoint cycles whose union is S_1, $p \geq 1$. For each i, since $Z_i \subseteq (\sigma - \lambda_1\iota)(V)$, there is a $\beta_i \in V$ such that $(\sigma - \lambda_1\iota)(\beta_i) = \alpha_i$. Then $Z_i' = Z_i \cup \{\beta_i\} = Z(\beta_i; \lambda_1)$ is a cycle of generalized eigenvectors of σ corresponding λ_1 with end vector β_i.

Let γ_i be the initial vector of Z_i for each i. Then $\{\gamma_1, \ldots, \gamma_p\}$ is a linearly independent subset of $\ker(\sigma - \lambda_1\iota)$, and this set can be extended to a basis $\{\gamma_1, \ldots, \gamma_p, \ldots, \gamma_{n-r}\}$ for $\ker(\sigma - \lambda_1\iota)$. If $p < n - r$, then let $Z_j' = \{\gamma_j\}$ for $p < j \leq n - r$. Then $Z_1', \ldots, Z_{n-r}'$ is a collection of disjoint cycles of generalized eigenvectors corresponding to λ_1.

Let $S_1' = \bigcup_{i=1}^{n-r} Z_i'$. Since the initial vectors of these cycles form a linearly independent set, by Theorem 8.2.11 S_1' is linearly independent. Then $\mathscr{B} = S_1' \cup S_2 \cdots \cup S_k$ is obtained from $\mathscr{A}$ by adjoining $n - r$ vectors. By Theorem 8.2.7, $\mathscr{B}$ is a Jordan basis for V corresponding to σ. □

In the proof of Theorem 8.2.13 the cycles Z_i''s were constructed so that the set of their initial vectors $\{\gamma_1, \ldots, \gamma_{n-r}\}$ is a basis of $\ker(\sigma - \lambda_1\iota) = \mathscr{E}(\lambda_1)$. Then, in the context of the construction of the proof of Theorem 8.2.13, the number of cycles corresponding to λ equals $\dim \mathscr{E}(\lambda)$. These relations are true for any Jordan basis. We do not want to prove it in this textbook[1].

Following we investigate the connection between the generalized eigenspaces $\mathscr{K}(\lambda)$ and the characteristic polynomial $C_\sigma(x)$ of σ.

Theorem 8.2.14 *Let V be an n-dimensional vector space over $\mathbb{F}$. Let $\sigma \in L(V, V)$ be such that $C_\sigma(x)$ splits over $\mathbb{F}$. Suppose $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of σ with algebraic multiplicities $m_1, \ldots, m_k$, respectively. Then*

(a) $\dim \mathscr{K}(\lambda_i) = m_i$ *for all* i, $1 \leq i \leq k$.

(b) For each i, if $\mathscr{A}_i$ is a basis of $\mathscr{K}(\lambda_i)$, then $\mathscr{A} = \mathscr{A}_1 \cup \cdots \cup \mathscr{A}_k$ is a basis of V.

(c) If $\mathscr{B}$ is a Jordan basis of V corresponding to σ, then for each i, $\mathscr{B}_i = \mathscr{B} \cap \mathscr{K}(\lambda_i)$ is a basis of $\mathscr{K}(\lambda_i)$.

(d) $\mathscr{K}(\lambda_i) = \ker((\sigma - \lambda_i\iota)^{m_i})$ *for all* i.

(e) σ is diagonalizable if and only if $\mathscr{E}(\lambda_i) = \mathscr{K}(\lambda_i)$ for all i.

Proof: We shall prove (a), (b) and (c) simultaneously. Let $J = [\sigma]_{\mathscr{B}}$ be a Jordan form, and let $r_i = \dim \mathscr{K}(\lambda_i)$ for $1 \leq i \leq k$.

For each i, the vectors in $\mathscr{B}_i$ are in one-to-one correspondence with the columns of J that contain λ_i as the diagonal entry. Since $C_\sigma(x) = C_J(x)$ and J is an upper triangular matrix, the number of occurrence of λ_i on the diagonal is m_i. Therefore, $|\mathscr{B}_i| = m_i$. Since $\mathscr{B}_i$ is a linearly independent subset of $\mathscr{K}(\lambda_i)$, $m_i \leq r_i$ for all i.

Since $\mathscr{A}_i$'s are linearly independent and mutually disjoint, by Lemma 8.2.10 $\mathscr{A}$ is linearly independent. So we have $n = \sum_{i=1}^{k} m_i \leq \sum_{i=1}^{k} r_i \leq n$. Hence we have $m_i = r_i$ for all i and $\sum_{i=1}^{k} r_i = n$. Then

[1]The interested reader may refer to the book: S.H. Friedberg, A.J. Insel and L.E. Spence *Linear Algebra*, 2nd editor, Prentice-Hall, 1989.

$|\mathscr{A}| = n$ and $\mathscr{A}$ is a basis of V. Since $m_i = r_i$, each $\mathscr{B}_i$ is a basis of $\mathscr{K}(\lambda_i)$. Therefore, (a), (b) and (c) hold.

It is clear that $\ker((\sigma - \lambda_i\iota)^{m_i}) \subseteq \mathscr{K}(\lambda_i)$. Suppose $\alpha \in \mathscr{K}(\lambda_i)$. By Theorem 8.2.5, $Z(\alpha; \lambda_i)$ is linearly independent. Since $\dim \mathscr{K}(\lambda_i) = m_i$, by (c) the length of $Z(\alpha; \lambda_i)$ cannot be greater than m_i. Thus $(\sigma - \lambda_i\iota)^{m_i}(\alpha) = \mathbf{0}$, i.e., $\alpha \in \ker((\sigma - \lambda_i\iota)^{m_i})$. So (d) is proved.

σ is diagonalizable if and only if there is a basis $\mathscr{C}$ of V consisting of eigenvectors of σ. By (c) $\mathscr{K}(\lambda_i)$ has a basis $\mathscr{C}_i = \mathscr{C} \cap \mathscr{K}(\lambda_i)$ consists of eigenvectors of σ corresponding to λ_i. Then $m_i = |\mathscr{C}_i| \leq \dim \mathscr{E}(\lambda_i)$. Since $\mathscr{E}(\lambda_i) \subseteq \mathscr{K}(\lambda_i)$, they are equal. Conversely, if $\mathscr{E}(\lambda_i) = \mathscr{K}(\lambda_i)$ for all i, then by (a) $\dim \mathscr{E}(\lambda_i) = m_i$ for all i. By (b), V has a basis consisting of eigenvectors of σ. So σ is diagonalizable. Hence (e) is proved. □

Corollary 8.2.15 *Let V be a vector space over $\mathbb{F}$. Let $\sigma \in L(V, V)$ be such that $C_\sigma(x)$ splits over $\mathbb{F}$. Suppose $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of σ. Then*

$$V = \mathscr{K}(\lambda_1) \oplus \cdots \oplus \mathscr{K}(\lambda_k).$$

By the fundamental theorem of algebra, we have the following corollaries.

Corollary 8.2.16 *Let V be a vector space over $\mathbb{C}$. Let $\sigma \in L(V, V)$. Then there is Jordan basis of V corresponding to σ.*

Corollary 8.2.17 *Suppose $A \in M_n(\mathbb{C})$. Then there is an invertible matrix $P \in M_n(\mathbb{C})$ such that $P^{-1}AP$ is in Jordan form.*

Suppose V has a Jordan basis corresponding to σ. Let $\mathscr{K}(\lambda)$ be one of the generalized eigenspace of V. By Theorem 8.2.14 (c) and Theorem 8.2.7 $\mathscr{K}(\lambda)$ has a basis $\mathscr{B}(\lambda)$ which is a disjoint union of cycles of generalized eigenvectors of σ. Suppose $\mathscr{B}(\lambda) = Z_1 \cup \cdots \cup Z_k$ and the length of the cycle Z_i is l_i. Without loss of generality, we may assume $l_1 \geq \cdots \geq l_k$.

It can be shown that the sequence $l_1, \ldots, l_k$ is uniquely determined by σ. The interested reader may refer to the book written by S.H Friedberg et al. Thus under this ordering of the basis of $\mathscr{K}(\lambda)$, the Jordan form of σ is uniquely determined.

Exercise 8.2

8.2-1. Let $\sigma \in L(V, V)$, where V is a finite dimensional vector space over $\mathbb{F}$. Prove that

(a) $\ker(\sigma) \subseteq \ker(\sigma^2) \subseteq \cdots \subseteq \ker(\sigma^k) \subseteq \ker(\sigma^{k+1}) \subseteq \cdots$.

(b) If $\operatorname{rank}(\sigma^m) = \operatorname{rank}(\sigma^{m+1})$ for some $m \in \mathbb{N}$, then $\operatorname{rank}(\sigma^k) = \operatorname{rank}(\sigma^m)$ for $k \geq m$.

(c) If $\operatorname{rank}(\sigma^m) = \operatorname{rank}(\sigma^{m+1})$ for some $m \in \mathbb{N}$, then $\ker(\sigma^k) = \ker(\sigma^m)$ for $k \geq m$.

(d) Let λ be an eigenvalue of σ. Prove that if $\operatorname{rank}((\sigma - \lambda\iota)^m) = \operatorname{rank}((\sigma - \lambda\iota)^{m+1})$ for some $m \in \mathbb{N}$, then $\mathscr{K}(\lambda) = \ker((\sigma - \lambda\iota)^m)$.

(e) (*Third Test for Diagonalizability*) Suppose $C_\sigma(x)$ splits over $\mathbb{F}$. Suppose $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of σ. Then σ is diagonalizable if and only if $\operatorname{rank}(\sigma - \lambda_i\iota) = \operatorname{rank}((\sigma - \lambda_i\iota)^2)$ for all i.

8.2-2. Let $Z = Z(\alpha; \sigma, \lambda)$ be a cycle of generalized eigenvectors of $\sigma \in L(V, V)$. Prove that $\operatorname{span}(Z)$ is an invariant subspace under σ.

8.3 Algorithms for Finding Jordan Basis

Jordan form is very useful in solving differential equation. So we provide two algorithms for finding the Jordan form of a given linear transformation or a square matrix. Since for a given square matrix A we can define a linear transformation σ such that A represents σ. Conversely, for a given linear transformation σ, it can be represented by a square matrix. Thus in the following we only talk about finding an invertible P such that $P^{-1}AP$ is in Jordan form, where $A \in M_n(\mathbb{F})$ whose characteristic polynomial splits over $\mathbb{F}$. To find P is equivalent to find a Jordan basis of $\mathbb{F}^n$. So in this section, we assume the characteristic polynomial of any matrix splits over $\mathbb{F}$.

Recurrent Algorithm:

Let $A \in M_n(\mathbb{F})$ with λ as an eigenvalue of algebraic multiplicity m. Suppose $\{X_1, \ldots, X_k\}$ is a cycle of generalized eigenvectors corresponding to λ. Then

$$\begin{aligned} (A-\lambda I)X_1 &= \mathbf{0} \\ (A-\lambda I)X_2 &= X_1 \\ &\vdots \\ (A-\lambda I)X_k &= X_{k-1} \end{aligned} \tag{8.1}$$

Thus we have to choose X_1 properly so that the second equation of Equation (8.1) has a solution X_2. Furthermore, when X_i is chosen, the equation $(A-\lambda I)X = X_i$ has a solution X_{i+1} for $i = 1, \ldots, k-1$. We proceed as follows:

Step 1: Form the augmented matrix $\big(A - \lambda I | B\big)$, where $B = \big(y_1 \ \cdots \ y_n\big)^T$.

Step 2: Use elementary row operations to reduce $\big(A - \lambda I | B\big)$ to the row reduced echelon form.

Step 3: If nullity$(A - \lambda I) = m$, then we get m linearly independent eigenvectors immediately by putting $B = \mathbf{0}$ and then go to Step 2 for another unconsidered eigenvalue, else go to Step 4.

Step 4: Assume that nullity$(A - \lambda I) = \nu < m$. Then after Step 2, the augmented matrix $\big(A - \lambda I | B\big)$ is row-equivalent to

$$\left(\begin{array}{c|c} H & \begin{matrix} f_1 \\ \vdots \\ f_{n-\nu} \end{matrix} \\ \hline O & \begin{matrix} f_{n-\nu+1} \\ \vdots \\ f_n \end{matrix} \end{array}\right),$$

where H is in rref and $f_1, \ldots, f_n$ are linear functions of $y_1, \ldots, y_n$. Since $\nu < m$, some eigenvector will generate a cycle of length larger than 1. Thus to find an initial vector X_1 of the cycle, we cannot simply put $B = \mathbf{0}$. We have to take the conditions $f_{n-\nu+1} = 0, \ldots, f_n = 0$ into consideration. We may use the coefficients of $y_1, \ldots, y_n$ in the linear equations $f_{n-\nu+1} =$

$0, \ldots, f_n = 0$ to form a matrix K. Then reduce the matrix

$$\left(\begin{array}{c|c} H & \begin{matrix} f_1 \\ \vdots \\ f_{n-\nu} \end{matrix} \\ \hline K & O \end{array}\right) \text{ to } \left(\begin{array}{c|c} H' & \begin{matrix} f_1' \\ \vdots \\ f_r' \end{matrix} \\ \hline O & \begin{matrix} f_{r+1}' \\ \vdots \\ f_n' \end{matrix} \end{array}\right).$$

From this rref, we may choose the right eigenvector X_1 by putting $y_1 = \cdots = y_n = 0$ if the length of the cycle is 2. If the length of the cycle is larger than 2, then this procedure can be continued.

Step 5: After $X_1 = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}^T$ has been chosen properly, we may put $B = X_1$ into the linear functions $f_1(y_1, \ldots, y_n), \ldots, f_{n-\nu}(y_1, \ldots, y_n)$ and compute X_2 from

$$\left(\begin{array}{c|c} H & \begin{matrix} f_1(y_1, \ldots, y_n) \\ \vdots \\ f_{n-\nu}(y_1, \ldots, y_n) \end{matrix} \end{array}\right).$$

If this X_2 will generate X_3, then we have to take the conditions $f_{r+1}'(y_1, \ldots, y_n) = 0$, $\ldots$, $f_n'(y_1, \ldots, y_n) = 0$ into consideration.

Step 6: This algorithm terminates if there is no new linear relation among $y_1, \ldots, y_n$ required. Thus, we shall be able to find a cycle of generalized eigenvectors corresponding to λ.

Step 7: If $\nu > 1$, then we can choose another eigenvector X_1' independent of X_1 and go to Step 4.

Step 8: After we have done with λ, we go to Step 2 for another unconsidered eigenvalue.

Step 9: Finally we obtain a Jordan basis of $\mathbb{F}^n$ and hence an invertible matrix P such that $P^{-1}AP$ is in Jordan form.

We use the following examples to illustrate the algorithm. We assume all the matrices considered in the following examples are over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

Example 8.3.1 Let $A = \begin{pmatrix} 5 & -3 & -2 \\ 8 & -5 & -4 \\ -4 & 3 & 3 \end{pmatrix}$. Then $C(x) = -(x-1)^3$.

Steps 1-3: Reduce the augmented matrix

$$(A - I|B) = \left(\begin{array}{ccc|c} 4 & -3 & -2 & y_1 \\ 8 & -6 & -4 & y_2 \\ -4 & 3 & 2 & y_3 \end{array}\right) \to \left(\begin{array}{ccc|c} 4 & -3 & -2 & y_1 \\ 0 & 0 & 0 & -2y_1+y_2 \\ 0 & 0 & 0 & y_1 \quad +y_3 \end{array}\right). \tag{8.2}$$

In practice, we do not need to reduce to the rref. Thus we have two cycles. (In this stage, we know that one of length 1 and the other length 2.)

Step 4: In order to find the cycle of length 2, we have to choose x_1, x_2, x_3 such that

$$\begin{cases} 4x_1 - 3x_2 - 2x_3 = 0 \\ -2x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \end{cases}.$$

To do this, we form the matrix $\begin{pmatrix} 4 & -3 & -2 \\ -2 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ and reduce to $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$. Hence choose $X_1 = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$.

Step 5: Then put $y_1 = 1, y_2 = 2, y_3 = -1$. Hence X_2 can be chosen from $\left(\begin{array}{ccc|c} 4 & -3 & -2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$. We choose $X_2 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$.

Step 7: To find the other linearly independent eigenvector, we go back to Equation (8.2). By putting $y_1 = y_2 = y_3 = 0$ we obtain $x_1 = 1$, $x_2 = 0$, $x_3 = 2$. That is $X_3 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$ which is linearly independent of X_1.

Step 9: Therefore, $P = \begin{pmatrix} 1 & 0 & 1 \\ 2 & -1 & 0 \\ -1 & 1 & 2 \end{pmatrix}$ and $J = P^{-1}AP = \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$. □

Example 8.3.2 Let $A = \begin{pmatrix} 3 & 1 & 0 & 0 \\ -4 & -1 & 0 & 0 \\ 7 & 1 & 2 & 1 \\ -7 & -6 & -1 & 0 \end{pmatrix}$. Then $C(x) = (x-1)^4$.

Steps 1-3: Reduce the matrix

$$(A - I|B) = \left(\begin{array}{cccc|c} 2 & 1 & 0 & 0 & y_1 \\ -4 & -2 & 0 & 0 & y_2 \\ 7 & 1 & 1 & 1 & y_3 \\ -7 & -6 & -1 & -1 & y_4 \end{array}\right) \to \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \frac{1}{2}y_1 + \frac{1}{10}(y_3 + y_4) \\ 0 & 1 & 0 & 0 & -\frac{1}{5}(y_3 + y_4) \\ 0 & 0 & 1 & 1 & -\frac{7}{2}y_1 + \frac{1}{2}y_3 - \frac{1}{2}y_4 \\ 0 & 0 & 0 & 0 & 2y_1 + y_2 \end{array}\right). \quad (8.3)$$

Thus, there is only one linearly independent eigenvector and hence there is a cycle of length 4. To achieve this, we have to assume $2x_1 + x_2 = 0$. Since there is only one linearly independent eigenvector, it is not necessary to continue the reducing process for finding the condition of the eigenvector. That is, the condition $2x_1 + x_2 = 0$ will hold until the final step. So we only put $y_1 = y_2 = y_3 = 0 = y_4 = 0$ in Equation (8.3) to get $X_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$.

Step 5: Put $y_1 = 0, y_2 = 0, y_3 = 1, y_4 = -1$ into Equation (8.3) we obtain X_2 easily from $\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$, namely, $X_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$.

Step 5: X_3 may be chosen from $\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \frac{1}{10} \\ 0 & 1 & 0 & 0 & -\frac{1}{5} \\ 0 & 0 & 1 & 1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$ to be $X_3 = \begin{pmatrix} \frac{1}{10} \\ -\frac{1}{5} \\ 0 \\ \frac{1}{2} \end{pmatrix}$. Finally, X_4 may be chosen from $\left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \frac{1}{10} \\ 0 & 1 & 0 & 0 & -\frac{1}{10} \\ 0 & 0 & 1 & 1 & -\frac{3}{5} \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$ to be $X_4 = \begin{pmatrix} \frac{1}{10} \\ -\frac{1}{10} \\ -\frac{3}{5} \\ 0 \end{pmatrix}$.

Step 9: Thus $P = \begin{pmatrix} 0 & 0 & \frac{1}{10} & \frac{1}{10} \\ 0 & 0 & -\frac{1}{5} & -\frac{1}{10} \\ 1 & 1 & 0 & -\frac{3}{5} \\ -1 & 0 & \frac{1}{2} & 0 \end{pmatrix}$ and $J = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

□

Example 8.3.3 Let $A = \begin{pmatrix} 1 & 0 & -1 & 1 & 0 \\ -4 & 1 & -3 & 2 & 1 \\ -2 & -1 & 0 & 1 & 1 \\ -3 & -1 & -3 & 4 & 1 \\ -8 & -2 & -7 & 5 & 4 \end{pmatrix}$. Then $C(x) = -(x-2)^5$.

Step 1: Consider $\big(A - 2I|B\big) = \left(\begin{array}{ccccc|c} -1 & 0 & -1 & 1 & 0 & y_1 \\ -4 & -1 & -3 & 2 & 1 & y_2 \\ -2 & -1 & -2 & 1 & 1 & y_3 \\ -3 & -1 & -3 & 2 & 1 & y_4 \\ -8 & -2 & -7 & 5 & 2 & y_5 \end{array}\right)$.

Step 4: Reduce it to the form

$$\left(\begin{array}{ccccc|l} 1 & 0 & 0 & 0 & 0 & y_1 - y_2 + y_3 \\ 0 & 1 & 0 & 1 & -1 & 2y_1 \quad -y_3 \\ 0 & 0 & 1 & -1 & 0 & -2y_1 + y_2 - y_3 \\ 0 & 0 & 0 & 0 & 0 & -2y_1 - y_2 - y_3 \quad +y_5 \\ 0 & 0 & 0 & 0 & 0 & -y_1 \quad -y_3 + y_4 \end{array}\right). \tag{8.4}$$

There are only two linearly independent eigenvectors and hence two cycles of generalized eigenvectors. In order to get generalized eigenvectors we have to introduce two conditions

$$\left\{\begin{array}{l} -2x_1 - x_2 - x_3 \quad +x_5 = 0 \\ -x_1 \quad -x_3 + x_4 \quad = 0 \end{array}\right.$$

Step 5: Applying elementary row operation, we have

$$\left(\begin{array}{rrrrr|r} 1 & 0 & 0 & 0 & 0 & y_1-y_2+y_3 \\ 0 & 1 & 0 & 1 & -1 & 2y_1 \quad -y_3 \\ 0 & 0 & 1 & -1 & 0 & -2y_1+y_2-y_3 \\ -2 & -1 & -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 1 & 0 & 0 \end{array}\right) \rightarrow \left(\begin{array}{rrrrr|r} 1 & 0 & 0 & 0 & 0 & y_1-y_2+y_3 \\ 0 & 1 & 0 & 1 & -1 & 2y_1 \quad -y_3 \\ 0 & 0 & 1 & -1 & 0 & -2y_1+y_2-y_3 \\ 0 & 0 & 0 & 0 & 0 & 2y_1-y_2 \\ 0 & 0 & 0 & 0 & 0 & y_1 \end{array}\right). \quad (8.5)$$

Thus there are two cycles of length greater than 1. (In this case, we know that one is of length 3 and the other is of length 2.)

Step 5: Applying elementary row operations again, we obtain

$$\left(\begin{array}{rrrrr|r} 1 & 0 & 0 & 0 & 0 & y_1-y_2+y_3 \\ 0 & 1 & 0 & 1 & -1 & 2y_1 \quad -y_3 \\ 0 & 0 & 1 & -1 & 0 & -2y_1+y_2-y_3 \\ 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \rightarrow \left(\begin{array}{rrrrr|r} 1 & 0 & 0 & 0 & 0 & y_1-y_2+y_3 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & -2y_1+y_2-y_3 \\ 0 & 0 & 0 & 1 & -1 & 2y_1 \quad -y_3 \\ 0 & 0 & 0 & 0 & 0 & -y_1+y_2-y_3 \end{array}\right). \quad (8.6)$$

Here we can see again that there is only one cycle of length greater than 2. If we put the condition $-x_1 + x_2 - x_3 = 0$ into consideration, then we reduce the augmented matrix

$$\left(\begin{array}{rrrrr|r} 1 & 0 & 0 & 0 & 0 & y_1-y_2+y_3 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & -2y_1+y_2-y_3 \\ 0 & 0 & 0 & 1 & -1 & 2y_1 \quad -y_3 \\ -1 & 1 & -1 & 0 & 0 & 0 \end{array}\right) \rightarrow \left(\begin{array}{c|r} I_5 & \begin{array}{r} y_1-y_2 \ +y_3 \\ 0 \\ 0 \\ 2y_1-y_2 \ -y_3 \\ -y_2+2y_3 \end{array} \end{array}\right)$$

There is no other linear relation among $y_1, \ldots, y_5$ required. So there is no cycle of length greater than 3.

Step 6: We find a cycle of length 3 first. To find X_1, we put $y_i = 0$ for $i = 1, \ldots, 5$ in Equation (8.6) to get $X_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \end{pmatrix}^T$.

Then put $y_1 = 0, y_2 = 0, y_3 = y_4 = y_5 = 1$ in Equation (8.5) to get $X_2 = \begin{pmatrix} 1 & -1 & -1 & 0 & 0 \end{pmatrix}^T$. Similarly, put the data of X_2 into Equation (8.4) we get $X_3 = \begin{pmatrix} 1 & 3 & -2 & 0 & 0 \end{pmatrix}^T$.

Step 7: We try to get another cycle. Since this cycle will be of length 2. So we start from Equation (8.5). Put $y_i = 0$ for all i we obtain $X_4 = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \end{pmatrix}^T$ which is linearly independent of X_1. Thus by putting this data of X_4 into Equation (8.4) we obtain $X_5 = \begin{pmatrix} -1 & 0 & 1 & 0 & 0 \end{pmatrix}^T$.

Step 9: Hence $P = \begin{pmatrix} 0 & 1 & 1 & 0 & -1 \\ 0 & -1 & 3 & 1 & 0 \\ 1 & -1 & -2 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$ and $J = \left(\begin{array}{rrr|rr} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{array}\right)$. □

Example 8.3.4 Let $A = \begin{pmatrix} 5 & -1 & -3 & 2 & -5 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & -2 \\ 0 & -1 & 0 & 3 & 1 \\ 1 & -1 & -1 & 1 & 1 \end{pmatrix}$. Then $C(x) = -(x-2)^3(x-3)^2$.

Step 1: Consider $\big(A-2I|B\big)=\left(\begin{array}{ccccc|c} 3 & -1 & -3 & 2 & -5 & y_1\\ 0 & 0 & 0 & 0 & 0 & y_2\\ 1 & 0 & -1 & 1 & -2 & y_3\\ 0 & -1 & 0 & 1 & 1 & y_4\\ 1 & -1 & -1 & 1 & -1 & y_5 \end{array}\right)$.

Step 4: We reduce it to the form

$$\left(\begin{array}{ccccc|l} 1 & 0 & -1 & 0 & -2 & -y_4+y_5\\ 0 & 1 & 0 & 0 & -1 & y_3-y_5\\ 0 & 0 & 0 & 1 & 0 & y_3+y_4-y_5\\ 0 & 0 & 0 & 0 & 0 & y_1-y_3+y_4-2y_5\\ 0 & 0 & 0 & 0 & 0 & y_2 \end{array}\right) \tag{8.7}$$

There are two linearly independent eigenvectors, hence there are two cycles, one of length 1 and the other of length 2. In order to find a proper eigenvector, we have to take the conditions $x_1-x_3+x_4-2x_5=0$ and $x_2=0$ into consideration. Thus we form the matrix $\left(\begin{array}{ccccc|l} 1 & 0 & -1 & 0 & -2 & -y_4+y_5\\ 0 & 1 & 0 & 0 & -1 & y_3-y_5\\ 0 & 0 & 0 & 1 & 0 & y_3+y_4-y_5\\ 1 & 0 & -1 & 1 & -2 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right)$ and reduce it to

$$\left(\begin{array}{ccccc|l} 1 & 0 & -1 & 0 & 0 & -2y_3-y_4+y_5\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & y_3+y_4-y_5\\ 0 & 0 & 0 & 0 & 1 & -y_3+y_5\\ 0 & 0 & 0 & 0 & 0 & -y_3+2y_5 \end{array}\right).$$

Thus we choose $X_1=\big(1\,0\,1\,0\,0\big)^T$.

Step 5: Now put $y_1=y_3=1$ and $y_2=y_4=y_5=0$ in Equation (8.7). Then we get $X_2=\big(0\;1\;0\;1\;0\big)^T$. For the other cycle, we put $y_i=0$ for all i in Equation (8.7) and get $X_3=\big(2\,1\,0\,0\,1\big)^T$.

Steps 1-4: For $\lambda=3$, we again reduce $\big(A-3I|B\big)$ to

$$\left(\begin{array}{ccccc|l} 1 & 0 & 0 & 1 & 0 & -4y_2-y_3+2y_4+2y_5\\ 0 & 1 & 0 & 0 & 0 & -y_2\\ 0 & 0 & 1 & 0 & 0 & -y_2-y_3+y_5\\ 0 & 0 & 0 & 0 & 1 & -y_2+y_4\\ 0 & 0 & 0 & 0 & 0 & y_1-y_2-y_3+y_4-y_5 \end{array}\right).$$

There is only one linearly independent eigenvector, hence only one cycle of length 2. Choose $X_4=\big(-1\,0\,0\,1\,0\big)^T$. It is clear that it satisfies the condition $x_1-x_2-x_3+x_4-x_5=0$. So we can compute X_5.

Step 5: By the data of X_4 and the above matrix, we solve that $X_5=\big(2\,0\,0\,0\,1\big)^T$.

Step 9: Thus $P = \begin{pmatrix} 1 & 0 & 2 & -1 & 2 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$ and hence $J = \begin{pmatrix} \boxed{\begin{matrix} 2 & 1 \\ 0 & 2 \end{matrix}} & 0 & 0 & 0 \\ 0 & \boxed{2} & 0 & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 3 & 1 \\ 0 & 3 \end{matrix}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. □

Example 8.3.5 Let

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 2 & 6 & 0 & -27 & 9 & 0 \\ 0 & -2 & -10 & 1 & 50 & -18 & 0 \\ 0 & 0 & -4 & 2 & 18 & -6 & 0 \\ 0 & 0 & -4 & 0 & 20 & -6 & 0 \\ 0 & 2 & -4 & -1 & 22 & -4 & 0 \\ 0 & 2 & 1 & -1 & 0 & 1 & 2 \end{pmatrix}.$$

Then $C(x) = -(x-2)^7$. After applying some elementary row operations on $[A - 2I \mid Y]$ we have

$$A = \left(\begin{array}{ccccccc|l} 0 & 1 & 0 & 0 & 0 & 2 & 0 & y_1 - 3y_2 - 2y_3 + y_4 - 2y_7 \\ 0 & 0 & 1 & 0 & 0 & -3 & 0 & 18y_2 + 9y_3 + 2y_4 + 9y_7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2y_1 + 10y_2 + 5y_3 + y_4 + 4y_7 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 3y_2 + 2y_3 - y_4 + 2y_7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2y_2 + 3y_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2y_2 + y_3 - y_4 + y_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -y_4 + y_5 \end{array}\right). \tag{8.8}$$

Since the nullity of $A - 2I$ is 3, there are 3 cycles of generalized eigenvectors.

For cycle of length greater than 1, we have to take the last three linear relations into consideration. After taking some elementary row operation we have

$$A = \left(\begin{array}{ccccccc|l} 0 & 1 & 0 & 0 & 0 & 0 & 0 & -3y_1 - 17y_2 - 8y_3 - 3y_4 - 2y_7 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 6y_1 + 39y_2 + 18y_3 + 8y_4 + 15y_7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2y_1 + 10y_2 + 5y_3 + y_4 + 4y_7 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2y_1 + 10y_2 + 5y_3 + y_4 + 4y_7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2y_1 + 7y_2 + 3y_3 + 2y_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4y_2 + y_3 + 3y_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2y_2 - 3y_4 - y_7 \end{array}\right). \tag{8.9}$$

Thus, there are only two cycles of length greater than 1. For cycle of length greater than 2, we take the last two linear relations into consideration. After taking some elementary row operations we have

$$A = \left(\begin{array}{ccccccc|l} 0 & 1 & 0 & 0 & 0 & 0 & 0 & -3y_1 - 17y_2 - 8y_3 - 3y_4 - 2y_7 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 6y_1 + 39y_2 + 18y_3 + 8y_4 + 15y_7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2y_1 + 10y_2 + 5y_3 + y_4 + 4y_7 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2y_1 + 10y_2 + 5y_3 + y_4 + 4y_7 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2y_1 + 7y_2 + 3y_3 + 2y_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4y_2 + y_3 + 3y_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -y_2 - y_3 + y_4 - 3y_7 \end{array}\right). \tag{8.10}$$

Thus, there is only one cycle of length greater than 2. Hence, there is precisely one cycle of length 1, one of length 2 and the other of length 4.

To get a cycle of length 4, put $y_1 = \cdots = y_7 = 0$ into Equation (8.10) and get an initial vector $X_1 = (1\ 0\ 0\ 0\ 0\ 0\ 0)^T$. Now put $y_1 = 1$, $y_2 = \cdots = y_7 = 0$ into Equation (8.10) and get $X_2 = (0\ -3\ 6\ 2\ 2\ 2\ 0)^T$. Putting this data into Equation (8.9) and get $X_3 = (0\ -3\ 7\ 2\ 2\ 1\ 0)^T$. Substitute the data into Equation (8.8) and get $X_4 = (\ -3\ 1\ 3\ 7\ 3\ 0\ 0)^T$.

To get a cycle of length 2, put $y_i = 0$ into Equation (8.9) and get an initial vector $X_5 = (0\ 0\ 0\ 0\ 0\ 0\ 1)^T$. Put $y_1 = \cdots = y_6 = 0$ and $y_7 = 1$ into Equation (8.8) and get $X_6 = (0\ -2\ 9\ 4\ 2\ 0\ 0)^T$.

Finally, it is easy to see from Equation (8.8) that the cycle of length 1 consists of the vector $X_7 = (0\ -2\ 3\ 0\ 1\ 1\ 0)^T$. □

Null Space Algorithm:

Let $\sigma \in L(V, V)$. Suppose V has a Jordan basis $\mathscr{B}$ corresponding to σ. Let λ be an eigenvalue of σ. Suppose $k = \text{nullity}(\sigma - \lambda\iota)$, the geometric multiplicity of λ. We know that there are k cycles of generalized eigenvectors of σ corresponding to λ. From Exercise 8.2-1 (d) we know that if $\text{rank}((\sigma - \lambda\iota)^j) = \text{rank}((\sigma - \lambda\iota)^{j+1})$ for some $j \in \mathbb{N}$, then $\mathscr{K}(\lambda) = \ker((\sigma - \lambda\iota)^j)$. How can we determine the length of each of the cycles? How do we find the initial vector of each cycle?

Let $J = [\sigma]_{\mathscr{B}}$. Suppose that $J_1, \ldots, J_t$ are the Jordan blocks. Without loss of generality, we may assume that the first k Jordan blocks whose diagonal entries are λ. Let m_i be the size of J_i for $1 \le i \le t$. Without loss of generality, we may assume $m_1 \ge \cdots \ge m_k$. For convenience, we let $\eta = \sigma - \lambda\iota$, $N = J - \lambda I$ and $N_i = J_i - \lambda I_{m_i}$ for $1 \le i \le t$. Also we denote N by $\text{diag}\{N_1, \ldots, N_k, \ldots, N_t\}$. Then it is easy to see that $N_i^{m_i} = O$ but $N_i^{m_i - 1} \neq O$ for $1 \le i \le k$. Since N_j is invertible for $j \ge k+1$, so is N_j^s for $s \ge 0$. Then $\dim \mathscr{K}(\lambda) = \text{nullity}(N^{m_1})$.

Let $Z(\alpha_1), \ldots, Z(\alpha_k)$ be the cycles of generalized eigenvectors of σ corresponding to λ. In order to determine these cycles we have to find all the α_i's. If $m_i = m_1$, then $\eta^{m_1 - 1}\alpha_i \neq \mathbf{0}$ but $\eta^{m_1}\alpha_i = \mathbf{0}$. Hence $\alpha_i \in \ker(\eta^{m_1}) \setminus \ker(\eta^{m_1 - 1})$. So we can determine the end vectors of the cycles whose length are m_1. Let m_{h+1} be the second large number of the sequence $m_1, \ldots, m_k$. The rank of $\eta^{m_1 - 2}$ must be greater than $\text{rank}(\eta^{m_1 - 1})$ by at least h. If $\text{rank}(\eta^{m_1 - 2}) > \text{rank}(\eta^{m_1 - 1}) + h$ or equivalently $\text{nullity}(\eta^{m_1 - 2}) < \text{nullity}(\eta^{m_1 - 1}) + h$, then there are some end vectors of the cycles whose length are m_{h+1}. Then we can determine all such end vectors. If $\text{rank}(\eta^{m_1 - 2}) = \text{rank}(\eta^{m_1 - 1}) + h$, then consider the rank of $\eta^{m_1 - 3}$. This process can be continued until all the end vectors have been found.

Following is the algorithm. Let $A \in M_n(\mathbb{F})$ be such that $C_A(x)$ splits over $\mathbb{F}$. Let λ be an eigenvalue of A. Then $\dim \mathscr{K}(\lambda)$ is the algebraic multiplicity of λ. Later, it will be denoted by n_m.

Step 1: Let $N = A - \lambda I$. Starting with $i = 1$, compute N^i and $n_i = \text{nullity}(N^i)$ until $n_{i+1} = n_i$. Let m be the least positive integer such that $n_{m+1} = n_m$. Let $\mathscr{N}_i = \text{null}(N^i)$ for $1 \le i \le m$ and let $n_0 = 0$. Define $d_i = n_i - n_{i-1}$ for $1 \le i \le m$. Set the banks $\mathscr{B}_i = \varnothing$ for $1 \le i \le m$. Set a counter $k = m$.

Step 2: Find a basis $\mathscr{A}_m$ for $\mathscr{N}_m$. Find d_m linearly independent vectors from $N^{m-1}(\mathscr{A}_m)$. Let them be $\beta_1, \ldots, \beta_{d_m}$. Trace back these vectors to the basis $\mathscr{A}_m$ and denote them by $\alpha_1, \ldots, \alpha_{d_m}$ accordingly. Note that $\beta_j = N^{m-1}(\alpha_j)$ for $1 \le i \le d_m$. Put $N^i(\alpha_j)$ into $\mathscr{B}_{m-i}$ for $1 \le j \le d_m$ and $0 \le i \le m - 1$.

Step 3: Subtract the counter k by 1. If $k = 0$, then go to Step 1 for another unconsidered eigenvalue until all eigenvalues have been considered. If $d_k - d_{k+1} = 0$ then repeat this step, otherwise go to Step 4.

Step 4: Extend the set $\bigcup_{i=1}^{k} \mathscr{B}_i$ to a basis $\mathscr{A}_k$ for $\mathscr{N}_k$. Find the maximal linearly independent subset $\mathscr{L}$ from $N^{k-1}(\mathscr{A}_k)$ containing $\mathscr{B}_1 = \{\beta_1, \ldots, \beta_{d_{k+1}}\}$. Let the vectors in $\mathscr{L}$ but not in $\mathscr{B}_1$ be denoted by $\beta_{d_{k+1}+1}, \ldots, \beta_{d_k}$. Trace back these $d_k - d_{k+1}$ vectors to $\mathscr{A}_k$. Let the corresponding vectors be $\alpha_{d_{k+1}+1}, \ldots, \alpha_{d_k}$. Put $N^i(\alpha_j)$ into $\mathscr{B}_{k-i}$ for $d_{k+1}+1 \le j \le d_k$ and $0 \le i \le k-1$. Go to Step 3.

Note that by the choice of $\mathscr{B}_1$, it guarantees that $\mathscr{B}_1$ is linearly independent. Since $d_1 = \dim \mathscr{E}(\lambda)$, $\mathscr{B}_1$ is a basis of $\mathscr{E}(\lambda)$. Each β_j is the initial vector of $Z(\alpha_j; \lambda)$. Since $\bigcup_{j=1}^{d_1} Z(\alpha_j; \lambda) = \bigcup_{i=1}^{m} \mathscr{B}_i$ and the construction of $\mathscr{B}_i$, we have $\left|\bigcup_{j=1}^{d_1} Z(\alpha_j; \lambda)\right| = \sum_{i=1}^{m} |\mathscr{B}_i| = \sum_{i=1}^{m} d_i = n_m = \dim \mathscr{K}(\lambda)$. Thus $\bigcup_{j=1}^{d_1} Z(\alpha_j; \lambda)$ is a basis of $\mathscr{K}(\lambda)$.

We use the following examples to illustrate the algorithm. We assume all the matrices considered in the following examples are over $\mathbb{F}$, where $\mathbb{F}$ is $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

Example 8.3.6 We consider Example 8.3.2 again.

Step 1: $N = A - I = \begin{pmatrix} 2 & 1 & 0 & 0 \\ -4 & -2 & 0 & 0 \\ 7 & 1 & 1 & 1 \\ -7 & -6 & -1 & -1 \end{pmatrix}$. $\operatorname{rref}(N) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Then $n_1 = 1$.

$N^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 \\ 10 & 10 & 0 & 0 \end{pmatrix}$. Then $n_2 = 2$.

$N^3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 20 & 10 & 0 & 0 \\ -20 & -10 & 0 & 0 \end{pmatrix}$. Then $n_3 = 3$ and $N^4 = O$. Hence $n_4 = 4 = n_5$. So $m = 4$ and $d_4 = d_3 = d_2 = d_1 = 1$.

Step 2: Since $\mathscr{N}_4 = \mathbb{F}^4$. We let $\mathscr{A}_4$ be the standard basis. Since $d_4 = 1$ and $N^3 \boldsymbol{e}_2 \neq \mathbf{0}$, we choose $\alpha_1 = \boldsymbol{e}_2$ (since $N^3 \boldsymbol{e}_1 \neq \mathbf{0}$, we may also choose $\boldsymbol{e}_1$).

Step 3: Since $d_4, d_3, d_2, d_1 = 1$ are the same, no other step is needed.

Then $Z(\boldsymbol{e}_2) = \{(0\ 0\ 10\ -10)^T,\ (0\ 0\ 0\ 10)^T,\ (1\ -2\ 1\ -6)^T,\ (0\ 1\ 0\ 0)^T\}$ and

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 1 \\ 10 & 0 & 1 & 0 \\ -10 & 10 & -6 & 0 \end{pmatrix}.$$

Then $P^{-1}AP$ is in Jordan form as in Example 8.3.2. □

Example 8.3.7 We consider Example 8.3.3 again.

Step 1: $N = A - 2I = \begin{pmatrix} -1 & 0 & -1 & 1 & 0 \\ -4 & -1 & -3 & 2 & 1 \\ -2 & -1 & -2 & 1 & 1 \\ -3 & -1 & -3 & 2 & 1 \\ -8 & -2 & -7 & 5 & 2 \end{pmatrix}$. After taking row operations we have

$\mathrm{rref}(N) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Thus $n_1 = 2$.

$N^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 1 & 0 \\ -1 & 0 & -1 & 1 & 0 \\ -1 & 0 & -1 & 1 & 0 \end{pmatrix}$ and $\mathrm{rref}(N^2) = \begin{pmatrix} 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Thus $n_2 = 4$.

$N^3 = O$. Thus $n_3 = 5 = n_4$. So $m = 3$ and $d_3 = 1$, $d_2 = 2$, $d_1 = 2$.

Step 2: Since $\mathscr{N}_3 = \mathbb{F}^5$, we let $\mathscr{A}_3$ be the standard basis.
$N^2\boldsymbol{e}_1 = (0\ 0\ -1\ -1\ -1)^T = N^2\boldsymbol{e}_3 = -N^2\boldsymbol{e}_4$ and $N^2\boldsymbol{e}_2 = N^2\boldsymbol{e}_5 = \mathbf{0}$. So we may choose any one vector from $\boldsymbol{e}_1, \boldsymbol{e}_3$ and $\boldsymbol{e}_4$. Now we choose $\alpha_1 = \boldsymbol{e}_1$. Then $\mathscr{B}_3 = \{\boldsymbol{e}_1\}$, $\mathscr{B}_2 = \{N\boldsymbol{e}_1 = (-1\ -4\ -2\ -3\ -8)^T\}$ and $\mathscr{B}_1 = \{N^2\boldsymbol{e}_1 = \beta_1 = (0\ 0\ -1\ -1\ -1)^T\}$.

Step 3: $k = 2$, $d_2 - d_3 = 1$. There is one new vector.

Step 4: Now $\{\boldsymbol{e}_5,\ \boldsymbol{e}_2,\ \gamma_1 = (-1\ 0\ 1\ 0\ 0)^T,\ \gamma_2 = (1\ 0\ 0\ 1\ 0)^T\}$ is a basis of $\mathscr{N}_2$. Consider $\{N\boldsymbol{e}_1, N^2\boldsymbol{e}_1, \boldsymbol{e}_5, \boldsymbol{e}_2, \gamma_1, \gamma_2\}$. By casting-out method we obtain $\mathscr{A}_2 = \{N\boldsymbol{e}_1, N^2\boldsymbol{e}_1, \boldsymbol{e}_5, \boldsymbol{e}_2\}$ as a basis of $\mathscr{N}_2$. $N(\mathscr{A}_2) = \{N^2\boldsymbol{e}_1, \mathbf{0}, N\boldsymbol{e}_5 = (0\ 1\ 1\ 1\ 2)^T, N\boldsymbol{e}_2 = -(0\ 1\ 1\ 1\ 2)^T\}$. Then $\mathscr{L} = \{N^2\boldsymbol{e}_1, N\boldsymbol{e}_5 = (0\ 1\ 1\ 1\ 2)^T\}$ is a maximal linearly independent subset of $N(\mathscr{A}_2)$. Thus we choose $\alpha_2 = \boldsymbol{e}_5$ and hence $\beta_2 = N\boldsymbol{e}_5$.

$\mathscr{B}_2 = \{N\boldsymbol{e}_1, \boldsymbol{e}_5\}$ and $\mathscr{B}_1 = \{\beta_1, \beta_2\}$. (In practice, since we have already found 5 linearly independent vectors in $\mathscr{K}(2)$, we stop here.)

Step 3: $k = 1$, $d_1 - d_2 = 0$. Repeat Step 3. Since $k = 0$, stop.

So

$$Z(\alpha_1) = \{(0\ 0\ -1\ -1\ -1)^T,\ (-1\ -4\ -2\ -3\ -8)^T,\ (1\ 0\ 0\ 0\ 0)^T\},$$
$$Z(\alpha_2) = \{(0\ 1\ 1\ 1\ 2)^T,\ (0\ 0\ 0\ 0\ 1)^T\}.$$

Thus

$$P = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 \\ 0 & -4 & 0 & 1 & 0 \\ -1 & -2 & 0 & 1 & 0 \\ -1 & -3 & 0 & 1 & 0 \\ -1 & -8 & 0 & 2 & 1 \end{pmatrix},$$

and $P^{-1}AP$ is in Jordan form as in Example 8.3.3. □

Example 8.3.8 We consider Example 8.3.4 again.

Consider the case $\lambda = 2$.

Step 1: Then $N = A - 2I = \begin{pmatrix} 3 & -1 & -3 & 2 & -5 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 1 & -2 \\ 0 & -1 & 0 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 \end{pmatrix}$. From Example 8.3.4 we know that $n_1 = 2$.

$$N^2 = \begin{pmatrix} 1 & 0 & -1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & -1 & 2 & 0 \\ 1 & -1 & -1 & 1 & -1 \end{pmatrix} \text{ and } \operatorname{rref}(N^2) = \begin{pmatrix} 1 & 0 & -1 & 0 & -2 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{8.11}$$

So $n_2 = 3$.

$N^3 = \begin{pmatrix} 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 2 & -3 & -2 & 3 & -1 \\ 1 & -1 & -1 & 1 & -1 \end{pmatrix}$. We can compute that $n_3 = 3$. Then $m = 3$, $d_2 = 1$ and $d_1 = 2$.

Step 2: By Equation (8.11) we obtain $\mathscr{A}_2 = \{(1\ 0\ 1\ 0\ 0)^T,\ (0\ 1\ 0\ 1\ 0)^T,\ (2\ 1\ 0\ 0\ 1)^T\}$. $N(\mathscr{A}_2) = \{\mathbf{0},\ (1\ 0\ 1\ 0\ 0)^T,\ \mathbf{0}\}$. Then we choose $\alpha_1 = (0\ 1\ 0\ 1\ 0)^T$. Hence $\beta_1 = (1\ 0\ 1\ 0\ 0)^T$. $\mathscr{B}_2 = \{\alpha_1\}$ and $\mathscr{B}_1 = \{\beta_1\}$.

Step 3-4: Now $k = 1$. From Equation (8.7) we obtain that $\{(1\ 0\ 1\ 0\ 0)^T,\ (2\ 1\ 0\ 0\ 1)^T\}$ is a basis of $\mathscr{N}$. So $\mathscr{A}_1 = \{(1\ 0\ 1\ 0\ 0)^T, (2\ 1\ 0\ 0\ 1)^T\}$. Then $\alpha_2 = (2\ 1\ 0\ 0\ 1)^T = \beta_2$. And $\mathscr{B}_1 = \{\beta_1, \beta_2\}$.

Then $Z(\alpha_1; 2) = \{(1\ 0\ 1\ 0\ 0)^T,\ (0\ 1\ 0\ 1\ 0)^T\}$ $\quad Z(\alpha_2; 2) = \{(2\ 1\ 0\ 0\ 1)^T\}$.

Consider the case $\lambda = 3$.

Step 1: $N = A - 3I = \begin{pmatrix} 2 & -1 & -3 & 2 & -5 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & -2 & 1 & -2 \\ 0 & -1 & 0 & 0 & 1 \\ 1 & -1 & -1 & 1 & -2 \end{pmatrix}$. By Example 8.3.4 we know that $n_1 = 1$.

$N^2 = \begin{pmatrix} -4 & 2 & 5 & -4 & 8 \\ 0 & 1 & 0 & 0 & 0 \\ -2 & 0 & 3 & -2 & 4 \\ 1 & 0 & -1 & 1 & -2 \\ -1 & 1 & 1 & -1 & 2 \end{pmatrix}$ and $\operatorname{rref}(N^2) = \begin{pmatrix} 1 & 0 & 0 & 1 & -2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. So $n_2 = 2$.

$N^3 = \begin{pmatrix} 5 & -2 & -6 & 5 & -10 \\ 0 & -1 & 0 & 0 & 0 \\ 3 & 0 & -4 & 3 & -6 \\ -1 & 0 & 1 & -1 & 2 \\ 1 & -1 & -1 & 1 & -2 \end{pmatrix}$ and $n_3 = 2$. So $m = 2$. (In fact, we need not compute N^3. It is because that the algebraic multiplicity of $\lambda = 3$ is 2. Then the maximum length of any cycle is 2.)

Step 2: $\mathscr{A}_2 = \{(1\ 0\ 0\ -1\ 0)^T,\ (2\ 0\ 0\ 0\ 1)^T\}$. Since $N(\mathscr{A}_2) = \{\mathbf{0},\ (-1\ 0\ 0\ 1\ 0)^T\}$. We choose $\alpha_1 = (2\ 0\ 0\ 0\ 1)^T$ and then $\beta_1 = (-1\ 0\ 0\ 1\ 0)^T$.

Hence we have

$$Z(\alpha_1; 3) = \{(-1\ 0\ 0\ 1\ 0)^T,\ (2\ 0\ 0\ 0\ 1)^T\}.$$

Finally, we have a Jordan basis

$$\mathscr{B} = \{(1\ 0\ 1\ 0\ 0)^T,\ (0\ 1\ 0\ 1\ 0)^T,\ (2\ 1\ 0\ 0\ 1)^T,\ (-1\ 0\ 0\ 1\ 0)^T, (2\ 0\ 0\ 0\ 1)^T\}$$

of $\mathbb{F}^5$ corresponding to a linear transformation induced by A. Coincidentally, it is the same as what we have found in Example 8.3.4. □

Example 8.3.9 Consider Example 8.3.5 again. Let $N = A - 2I$. We compute n_i first. Since

$$\mathrm{rref}(N) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathrm{rref}(N^2) = \begin{pmatrix} 0 & 1 & 0 & -\frac{1}{2} & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & -\frac{9}{2} & \frac{3}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathrm{rref}(N^3) = \begin{pmatrix} 0 & 1 & 0 & -\frac{1}{2} & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and $N^4 = O$. Thus $n_1 = 3$, $n_2 = 5$, $n_3 = 6$, $n_4 = 7 = n_5$ and hence $m = 4$, $d_4 = 1$, $d_3 = 1$, $d_2 = 2$, $d_1 = 3$.

Let $\mathscr{A}_4$ be the standard basis of $\mathbb{F}^7 = \mathscr{N}_4$. Since $N^3\boldsymbol{e}_4 = \boldsymbol{e}_1$, we choose $\alpha_1 = \boldsymbol{e}_4$ and put it into $\mathscr{B}_4$. Put $N\boldsymbol{e}_4 = (0\ 0\ 1\ 0\ 0\ -1\ -1)^T$ into $\mathscr{B}_3$, $N^2\boldsymbol{e}_4 = (-1\ -3\ 6\ 2\ 2\ 2\ 0)^T$ into $\mathscr{B}_2$ and $\beta_1 = N^3\boldsymbol{e}_4 = \boldsymbol{e}_1$ into $\mathscr{B}_1$.

From $\mathrm{rref}(N^2)$ we have that $\{\boldsymbol{e}_1,\ \boldsymbol{e}_7,\ (0,1,0,2,0,0,0),\ (0,-4,9,0,2,0,0),\ (0,0,-3,0,0,2,0)\}$ is a basis of $\mathscr{N}_2$ (note that, for convenience we write the column vectors as 7-tuples). Then we have

$$\mathscr{A}_2 = \{\boldsymbol{e}_1,\ (-1,-3,6,2,2,2,0),\ \boldsymbol{e}_7,\ (0,1,0,2,0,0,0),\ (0,-4,9,0,2,0,0)\}.$$

Then $N(\mathscr{A}_2) = \{\mathbf{0},\ \boldsymbol{e}_1,\ \mathbf{0},\ \boldsymbol{e}_1,\ (-2,0,0,0,0,0,1)\}$. So we choose $\alpha_2 = (0,-4,9,0,2,0,0)$. Hence $\beta_2 = (-2,0,0,0,0,0,1)$. Then
$\mathscr{B}_2 = \{(-1,-3,6,2,2,2,0),\ (0,-4,9,0,2,0,0)\}$, $\mathscr{B}_1 = \{\boldsymbol{e}_1,\ (-2,0,0,0,0,0,1)\}$.

From $\mathrm{rref}(N)$ we have that $\{\boldsymbol{e}_1,\ \boldsymbol{e}_7,\ (0,-2,3,0,1,1,0)\}$ is a basis of $\mathscr{N}_1$. Then
$\mathscr{A}_1 = \{\boldsymbol{e}_1, (-2,0,0,0,0,0,1), (0,-2,3,0,1,1,0)\}$. Hence $\alpha_3 = \beta_3 = (0,-2,3,0,1,1,0)$ and $\mathscr{B}_1 = \{\boldsymbol{e}_1, (-2,0,0,0,0,0,1), (0,-2,3,0,1,1,0)\}$.

Therefore,

$$\begin{aligned} Z(\alpha_1) &= \{\boldsymbol{e}_1,\ (-1,-3,6,2,2,2,0),\ (0,0,1,0,0,-1,-1),\ \boldsymbol{e}_4\}, \\ Z(\alpha_2) &= \{(-2,0,0,0,0,0,1),\ (0,-4,9,0,2,0,0)\}, \\ Z(\alpha_3) &= \{(0,-2,3,0,1,1,0)\}. \end{aligned}$$

□

Exercise 8.3

8.3-1. Let $A = \begin{pmatrix} 1 & -3 & 0 & 3 \\ -2 & -6 & 0 & 13 \\ 0 & -3 & 1 & 3 \\ -1 & -4 & 0 & 8 \end{pmatrix}$ over $\mathbb{C}$. Find an invertible matrix P such that $P^{-1}AP$ is in Jordan form.

8.3-2. Put the matrix $A = \begin{pmatrix} -3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix} \in M_4(\mathbb{C})$ into Jordan form.

8.3-3. Put the matrix $A = \begin{pmatrix} -1 & 1 & 0 & 0 \\ -5 & 3 & 1 & 0 \\ 3 & 0 & -1 & 1 \\ 11 & -3 & -3 & 3 \end{pmatrix} \in M_4(\mathbb{Q})$ into Jordan form.

8.3-4. Let $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 5 & -1 & -1 & 1 \\ 10 & -2 & -4 & 3 \end{pmatrix} \in M_4(\mathbb{R})$. Find an invertible matrix P such that $P^{-1}AP$ is in Jordan form.

8.3-5. Let $A = \begin{pmatrix} -2 & 1 & 0 & 0 \\ -4 & 2 & 0 & 0 \\ 3 & 0 & -2 & 1 \\ 12 & -3 & -4 & 2 \end{pmatrix} \in M_4(\mathbb{R})$. Find an invertible matrix P such that $P^{-1}AP$ is in Jordan form.

Chapter 9

Linear and Quadratic Forms

For real problem we always need to find a numerical data or value of a function. To find an approximate value of a given function, the usual method is linear approximation. If we need to have a more precise value, the higher order approximation is used. The usual higher approximation is quadratic approximation. In mathematical language, suppose there is an n-variable function $f : \mathbb{R}^n \to \mathbb{R}$. For a fixed point $\boldsymbol{c} \in \mathbb{R}^n$, we know the exact value $f(\boldsymbol{c})$ but do not know the value of $\boldsymbol{x}$ that near the point $\boldsymbol{c}$. So we need to find an approximate value of $f(\boldsymbol{x})$ for $\boldsymbol{x}$ close to $\boldsymbol{c}$. The usual linear approximation is

$$f(\boldsymbol{x}) \cong f(\boldsymbol{c}) + \nabla f(\boldsymbol{c}) \cdot (\boldsymbol{x} - \boldsymbol{c}).$$

The quadratic approximation is

$$f(\boldsymbol{x}) \cong f(\boldsymbol{c}) + \nabla f(\boldsymbol{c}) \cdot (\boldsymbol{x} - \boldsymbol{c}) + (\boldsymbol{x} - \boldsymbol{c})^T D^2 f(\boldsymbol{c})(\boldsymbol{x} - \boldsymbol{c}),$$

where $D^2 f(\boldsymbol{c}) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}(\boldsymbol{c})\right)$ is the second derivative matrix of f at $\boldsymbol{c}$. If $\nabla f(\boldsymbol{c}) = \boldsymbol{0}$, then the positivity of the matrix $D^2 f(\boldsymbol{c})$ determines the property of the extrema.

The functions $\nabla f(\boldsymbol{c}) \cdot (\boldsymbol{x} - \boldsymbol{c})$ and $(\boldsymbol{x} - \boldsymbol{c})^T D^2 f(\boldsymbol{c})(\boldsymbol{x} - \boldsymbol{c})$ are a linear form and a quadratic form, respectively. In this chapter we shall discuss linear forms and quadratic forms.

9.1 Linear Forms

In this section we study linear forms first. Let V and W be vectors spaces over $\mathbb{F}$. We know that $L(V, W)$ is a vector space over $\mathbb{F}$. In particular if we choose $W = \mathbb{F}$, then $L(V, \mathbb{F})$ is a vector space. We shall use $\widehat{V}$ to denote $L(V, \mathbb{F})$.

Definition 9.1.1 Let V be a vector space over $\mathbb{F}$. A linear transformation of V into $\mathbb{F}$ is called a *linear form* or *linear functional* on V. The space $\widehat{V} = L(V, \mathbb{F})$ is called the *dual space* of V.

Let V and W be n and m dimensional vectors spaces over $\mathbb{F}$. From Theorems 7.2.4 and 7.2.6 we know that $L(V, W)$ is isomorphic to $M_{m,n}(\mathbb{F})$. Let $E^{i,j}$ be the matrix defined in Section 1.5 for $1 \leq i \leq m$ and $1 \leq j \leq n$. Then it is easy to see that

$$\{E^{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

is a basis of $M_{m,n}(\mathbb{F})$. This means that $\dim L(V, W) = \dim M_{m,n}(\mathbb{F}) = mn$. So combining with Theorem 7.1.8 we have the following theorem.

Theorem 9.1.2 *Let V be a vector space (not necessary finite dimensional) over $\mathbb{F}$. Then $\widehat{V}$ is a vector space over $\mathbb{F}$. If $\dim V = n$, then $\dim \widehat{V} = n$.*

From the above discussion we have a basis for $M_{m,n}(\mathbb{F})$. Use the proof of Theorem 7.2.4 we should have a corresponding basis for $L(V,W)$. Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ and $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$ be bases of V and W, respectively. From the proof of Theorem 7.2.4 and 7.2.6 we know that the corresponding is $\Lambda : \sigma \mapsto [\sigma]_{\mathscr{B}}^{\mathscr{A}}$. So the basis for $L(V,W)$ should be the linear transformations whose images under Λ are the matrices $E^{i,j}$. Precisely, we define $\sigma_{i,j} : V \to \mathbb{F}$ by

$$\sigma_{i,j}(\alpha_j) = \beta_i \text{ and } \sigma_{i,j}(\alpha_k) = \mathbf{0} \text{ for } k \neq j.$$

Hence $\{\sigma_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for $L(V,W)$ and $[\sigma_{i,j}]_{\mathscr{B}}^{\mathscr{A}} = E^{i,j}$.

For the linear functional case, we choose $\mathscr{B} = \{1\}$ as the basis of $\mathbb{F}$. Then the corresponding basis of $\widehat{V}$ is $\phi_j : V \to \mathbb{F}$ which is defined by $\phi_j(\alpha_j) = 1$ and $\phi_j(\alpha_k) = 0$ for $k \neq j$. In other word,

$$\phi_j(\alpha_k) = \delta_{jk} \cdot 1 = \delta_{jk}, \text{ for } 1 \leq j \leq n.$$

Then $[\phi_j]_{\mathscr{B}}^{\mathscr{A}} = \boldsymbol{e}_j$, where $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ is the standard basis of $\mathbb{F}^{1\times n}$. The linear form ϕ_j is called the *j-th coordinate function.*

Definition 9.1.3 The basis $\{\phi_1, \ldots, \phi_n\}$ constructed above is called the *basis dual to $\mathscr{A}$* or the *dual basis of $\mathscr{A}$*. They are characterized by the relations $\phi_i(\alpha_j) = \delta_{ij}$ for all $1 \leq i, j \leq n$.

Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ be a basis of V and let $\Phi = \{\phi_1, \ldots, \phi_n\}$ be the dual basis of $\mathscr{A}$. Suppose $\phi \in \widehat{V}$ and $\alpha \in V$. There are $b_i, x_j \in \mathbb{F}$, $1 \leq i, j \leq n$, such that $\phi = \sum_{i=1}^{n} b_i\phi_i$ and $\alpha = \sum_{j=1}^{n} x_j\alpha_j$. Then

$$\phi(\alpha) = \left(\sum_{i=1}^{n} b_i\phi_i\right)\left(\sum_{j=1}^{n} x_j\alpha_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} b_ix_j\phi_i(\alpha_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} b_ix_j\delta_{ij} = \sum_{i=1}^{n} b_ix_i.$$

Thus if we use the matrix $B = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}^T$ to represent ϕ and the matrix $X = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}^T$ to represent α, i.e., $[\phi]_\Phi = B$ and $[\alpha]_{\mathscr{A}} = X$, then

$$\phi(\alpha) = B^TX. \tag{9.1}$$

Note that if we view ϕ as a vector in $\widehat{V}$, then $[\phi]_\Phi = B$ is the coordinate vector of ϕ relative to the basis Φ. However if we view ϕ as a linear transformation from V to $\mathbb{F}$, then $[\phi]_{\mathscr{B}}^{\mathscr{A}} = B^T$ (which is a row vector). So $[\phi(\alpha)]_{\mathscr{B}} = [\phi]_{\mathscr{B}}^{\mathscr{A}}[\alpha]_{\mathscr{A}} = B^TX$. This agrees with (9.1) whose right hand side is the product of two matrices.

Suppose $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ is a basis of V. Let $\{\phi_1, \ldots, \phi_n\}$ be the dual basis of $\mathscr{A}$. Let $\alpha \in V$. Then $\alpha = \sum_{j=1}^{n} a_j\alpha_j$ for some $a_j \in \mathbb{F}$. Then $\phi_i(\alpha) = \sum_{j=1}^{n} a_j\phi_i(\alpha_j) = \sum_{j=1}^{n} a_j\delta_{ij} = a_i$. So

$$\alpha = \sum_{j=1}^{n} \phi_j(\alpha)\alpha_j. \tag{9.2}$$

Suppose $\phi \in \widehat{V}$. Then $\phi = \sum_{i=1}^{n} b_i\phi_i$ for some $b_i \in \mathbb{F}$. Then
$\phi(\alpha_j) = \sum_{i=1}^{n} b_i\phi_i(\alpha_j) = \sum_{i=1}^{n} b_i\delta_{ij} = b_j$. So $\phi = \sum_{i=1}^{n} \phi(\alpha_i)\phi_i$.

Example 9.1.4 Let $t_1, \ldots, t_n$ be any distinct real numbers and $c_1, \ldots, c_n$ be any real numbers. Find a polynomial $f \in \mathbb{R}[x]$ such that $f(t_i) = c_i$ for all i and $\deg f < n$.

Solution: Let $V = P_n(\mathbb{R})$. For $p \in V$, define $\phi_i(p) = p(t_i)$ for $i = 1, \ldots, n$. Then clearly $\phi_i \in \widehat{V}$.

Suppose $\sum_{i=1}^{n} a_i\phi_i = O$, then $\left(\sum_{i=1}^{n} a_i\phi_i\right)(p) = 0$ for all $p \in V$. In particular, for $p = x^j$ with $0 \le j \le n-1$, we have $\sum_{i=1}^{n} a_i t_i^j = 0$ for $0 \le j \le n-1$. Since the matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ t_1 & t_2 & \cdots & t_n \\ \vdots & \vdots & \cdots & \vdots \\ t_1^{n-1} & t_2^{n-1} & \cdots & t_n^{n-1} \end{pmatrix}$$

is non-singular (see Example 4.3.5), we have $a_1 = \cdots = a_n = 0$. Thus $\{\phi_1, \ldots, \phi_n\}$ is a basis of $\widehat{V}$.

Since $\phi_i(x^j) = t_i^j \neq \delta_{ij}$ in general, $\{\phi_1, \ldots, \phi_n\}$ is not a basis dual to the standard basis $\{1, x, \ldots, x^{n-1}\}$. Let

$$\begin{aligned} p_1(x) &= \frac{(x-t_2)(x-t_3)\cdots(x-t_n)}{(t_1-t_2)(t_1-t_3)\cdots(t_1-t_n)} \\ &\vdots \\ p_i(x) &= \frac{(x-t_1)\cdots(x-t_{i-1})(x-t_{i+1})\cdots(x-t_n)}{(t_i-t_1)\cdots(t_i-t_{i-1})(t_1-t_{i+1})\cdots(t_i-t_n)} \\ &\vdots \\ p_n(x) &= \frac{(x-t_1)(x-t_2)\cdots(x-t_{n-1})}{(t_n-t_1)(t_n-t_2)\cdots(t_n-t_{n-1})}. \end{aligned}$$

It is easy to see that $\{p_1, \ldots, p_n\}$ is linearly independent and hence a basis of V, and $\{\phi_1, \ldots, \phi_n\}$ is its dual basis.

Then by Equation (9.2) the required polynomial is $f = \sum_{j=1}^{n} c_j p_j$. This is called the *Lagrange interpolation*. Note that the above method works in any field that contains at least n elements. □

Exercise 9.1

9.1-1. Find the dual basis of the basis $\{(1,0,1),\ (-1,1,1),\ (0,1,1)\}$ of $\mathbb{R}^3$.

9.1-2. Let V be a vector space of finite dimension $n \ge 2$ over $\mathbb{F}$. Let α and β be two vectors in V such that $\{\alpha, \beta\}$ is linearly independent. Show that there exists a linear form ϕ such that $\phi(\alpha) = 1$ and $\phi(\beta) = 0$.

9.1-3. Show that if α is a nonzero vector in a finite dimensional vector space, then there is a linear form ϕ such that $\phi(\alpha) \neq 0$.

9.1-4. Let W be a proper subspace of a finite dimensional vector space V. Let $\alpha \in V \setminus W$. Show that there is a linear form ϕ such that $\phi(\alpha) = 1$ and $\phi(\beta) = 0$ for all $\beta \in W$.

9.1-5. Let α, β be vectors in a finite dimensional vector space V such that whenever $\phi \in \widehat{V}$, $\phi(\beta) = 0$ implies $\phi(\alpha) = 0$. Show that α is a multiple of β.

9.1-6. Find a polynomial $f(x) \in P_5(\mathbb{R})$ such that $f(0) = 2$, $f(1) = -1$, $f(2) = 0$, $f(-1) = 4$ and $f(4) = 3$.

9.2 The Dual Space

Let V be a vector space. For a fixed vector $\alpha \in V$ we define a function $J(\alpha)$ on the space $\widehat{V}$ by $J(\alpha)(\phi) = \phi(\alpha)$ for all $\phi \in \widehat{V}$. It is clear that $J(\alpha)$ is linear. So $J(\alpha) \in \widehat{\widehat{V}}$, the dual space of $\widehat{V}$.

Theorem 9.2.1 *Let V be a finite dimensional vector space over $\mathbb{F}$ and let $\widehat{\widehat{V}}$ be the space of all linear forms on $\widehat{V}$. Let $J : V \to \widehat{\widehat{V}}$ be defined by $J(\alpha)(\phi) = \phi(\alpha)$ for all $\alpha \in V$ and $\phi \in \widehat{V}$. Then J is an isomorphism between V and $\widehat{\widehat{V}}$ and is sometimes referred as the natural isomorphism.*

Proof: Let $\alpha, \beta \in V$, $a \in \mathbb{F}$ and $\phi \in \widehat{V}$. Then

$$J(a\alpha + \beta)(\phi) = \phi(a\alpha + \beta) = a\phi(\alpha) + \phi(\beta) = aJ(\alpha)(\phi) + J(\beta)(\phi) = [aJ(\alpha) + J(\beta)](\phi).$$

Since $\phi \in \widehat{V}$ is chosen arbitrarily, we have $J(a\alpha + \beta) = aJ(\alpha) + J(\beta)$. So J is linear.

Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of V and $\{\phi_1, \ldots, \phi_n\}$ its dual basis. Let $\alpha \in V$, $\alpha = \sum_{j=1}^{n} a_j\alpha_j$ for some $a_j \in \mathbb{F}$. If $J(\alpha) = O$, then $J(\alpha)(\phi) = 0\ \forall \phi \in \widehat{V}$. In particular, $J(\alpha)(\phi_i) = 0\ \forall i$. That is, $0 = \phi_i(\alpha) = a_i\ \forall i$. Hence $\alpha = \mathbf{0}$ and J is a monomorphism. Since $\dim \widehat{\widehat{V}} = \dim \widehat{V} = \dim V = n$, By Theorem 7.1.19 J is an isomorphism between V and $\widehat{\widehat{V}}$. □

Corollary 9.2.2 *Let V be a finite dimensional vector space and let $\widehat{V}$ be its dual space. Then every basis of $\widehat{V}$ is the dual basis of some basis of V.*

Proof: Let $\{\phi_1, \ldots, \phi_n\}$ be a basis of $\widehat{V}$. By Theorem 9.1.2 we can find its dual basis $\{\Phi_1, \ldots, \Phi_n\}$ in $\widehat{\widehat{V}}$. By means of the isomorphism J defined above we can find $\alpha_1, \ldots, \alpha_n \in V$ such that $J(\alpha_i) = \Phi_i$ for $i = 1, \ldots, n$. Then $\{\alpha_1, \ldots, \alpha_n\}$ is the required basis. This is because $\phi_j(\alpha_i) = J(\alpha_i)(\phi_j) = \Phi_i(\phi_j) = \delta_{ij}$. □

By the above theorem, we can identify V with $\widehat{\widehat{V}}$, and consider V as the space of all linear forms on $\widehat{V}$. Thus V and $\widehat{V}$ are called *dual spaces*. A basis $\{\alpha_1, \ldots, \alpha_n\}$ of V and a basis $\{\phi_1, \ldots, \phi_n\}$ of $\widehat{V}$ are called *dual bases* if $\phi_i(\alpha_j) = \delta_{ij}$ for all i, j.

Suppose $\mathscr{A}$ and $\mathscr{B}$ are bases of a finite dimensional vector space V and Φ and Ψ are their dual bases, respectively. It is known that there is a linear relation between the bases $\mathscr{A}$ and $\mathscr{B}$. Namely, there is a matrix of transition P from $\mathscr{A}$ to $\mathscr{B}$. Similarly there is a matrix of transition Q from Φ to Ψ. What is the relation between P and Q?

Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$, $\mathscr{B} = \{\beta_1, \ldots, \beta_n\}$, $\Phi = \{\phi_1, \ldots, \phi_n\}$ and $\Psi = \{\psi_1, \ldots, \psi_n\}$. Suppose $P = (p_{ij})$ and $Q = (q_{ij})$. Then

$$\beta_j = \sum_{i=1}^{n} p_{ij}\alpha_i \text{ and } \psi_k = \sum_{r=1}^{n} q_{rk}\phi_r,\ 1 \le j, k \le n.$$

Now observe that $\psi_k(\alpha_j) = \sum_{r=1}^{n} q_{rk}\phi_r(\alpha_j) = \sum_{r=1}^{n} q_{rk}\delta_{rj} = q_{jk}$. Then

$$\delta_{kj} = \psi_k(\beta_j) = \psi_k\left(\sum_{i=1}^{n} p_{ij}\alpha_i\right) = \sum_{i=1}^{n} p_{ij}\psi_k(\alpha_i) = \sum_{i=1}^{n} p_{ij}q_{ik} = \sum_{i=1}^{n} (Q^T)_{k,i}(P)_{i,j}.$$

Thus $Q^TP = I$ or equivalently $P^TQ = I$. Hence $P^T = Q^{-1}$ is the matrix of transition from Ψ to Φ. Thus $\phi_i = \sum_{j=1}^{n} p_{ij}\psi_j$.

Let $B = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}^T$ and $B' = \begin{pmatrix} b'_1 & \cdots & b'_n \end{pmatrix}^T$ be the coordinate vectors of the linear form ϕ with respect to the bases Φ and Ψ, respectively. That is, $[\phi]_\Phi = B$ and $[\phi]_\Psi = B'$. Then

$$\sum_{j=1}^{n} b'_j\psi_j = \phi = \sum_{i=1}^{n} b_i\phi_i = \sum_{i=1}^{n} b_i \left(\sum_{j=1}^{n} p_{ij}\psi_j \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} b_i p_{ij} \right) \psi_j.$$

Thus $B'^T = B^TP$ or $B' = P^TB = Q^{-1}B$. That is, $[\phi]_\Psi = Q^{-1}[\phi]_\Phi = P^T[\phi]_\Phi$.

Example 9.2.3 Let $V = \mathbb{R}^3$ and $\beta_1 = (1, 0, -1)$, $\beta_2 = (-1, 1, 0)$ and $\beta_3 = (0, 1, 1)$. Then clearly $\mathscr{B} = \{\beta_1, \beta_2, \beta_3\}$ is a basis of V. From Equation (9.1) we know that $\phi(x, y, z) = b_1x + b_2y + b_3z$ for some $b_i \in \mathbb{R}$. To find the dual basis $\Psi = \{\psi_1, \psi_2, \psi_3\}$ of $\mathscr{B}$ we can solve b_i by considering the equations $\psi_i(\beta_j) = \delta_{i,j}$ for all $1 \leq i, j \leq 3$.

Now we would like to use the result above to find the dual basis of $\mathscr{B}$. Let $\mathscr{S}$ be the standard basis of V. Let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the dual basis of $\mathscr{S}$. Then $[\psi_1]_\Psi = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $[\psi_2]_\Psi = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $[\psi_3]_\Psi = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and $[\phi_1]_\Phi = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $[\phi_2]_\Phi = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $[\phi_3]_\Phi = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. That is, $\phi_1(x, y, z) = x$, $\phi_2(x, y, z) = y$ and $\phi_3(x, y, z) = z$. The transition matrix P from $\mathscr{S}$ to $\mathscr{B}$ is $\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}$. Then $Q = (P^T)^{-1} = \frac{1}{2}\begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & 1 \\ -1 & -1 & 1 \end{pmatrix}$. Thus, the required dual basis will consist of

$$[\psi_1]_\Phi = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \quad [\psi_2]_\Phi = \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \quad [\psi_3]_\Phi = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}.$$

That is, $\psi_1 = \frac{1}{2}\phi_1 + \frac{1}{2}\phi_2 - \frac{1}{2}\phi_3$, etc. Equivalently, $\psi_1(x, y, z) = \frac{1}{2}x + \frac{1}{2}y - \frac{1}{2}z$, etc. □

In Chapter 2, we were asked to find the null space of a matrix. The equivalent question was asked in Chapter 7. It asked us to find the kernel of a given linear transformation. In this chapter, we are concerned on linear form. Let V be a finite dimensional space. We may be asked to find the solution space of $\phi(\alpha) = 0$ for a given linear form ϕ. On the other hand, α can be viewed as a linear form of $\widehat{V}$. So we may also be asked to find all the solutions $\phi \in \widehat{V}$ such that $\phi(\alpha) = 0$.

Definition 9.2.4 Let V be a vector space. Let S be a subset of V (S can be empty). The set of all linear forms ϕ satisfying the condition that $\phi(\alpha) = 0$ $\forall \alpha \in S$ is called the *annihilator of* S and denoted by S^0. Any linear form $\phi \in S^0$ is called an *annihilator of* S.

Theorem 9.2.5 *The annihilator W^0 of a subset W is a subspace of $\widehat{V}$. In addition, suppose W is a subspace of V and if* $\dim V = n$ *and* $\dim W = r$, *then* $\dim W^0 = n - r$.

Proof: Let $\phi, \psi \in W^0$ and $a \in \mathbb{F}$. Then $(a\phi + \psi)(\alpha) = a\phi(\alpha) + \psi(\alpha) = 0\ \forall \alpha \in W$. Thus W^0 is a subspace of $\widehat{V}$.

Suppose W is a subspace of V. Let $\{\alpha_1, \ldots, \alpha_r\}$ be a basis of W. Extend it to a basis $\{\alpha_1, \ldots, \alpha_n\}$ of V. Let $\{\phi_1, \ldots, \phi_n\}$ be its dual basis. We shall show that $\phi_{r+1}, \ldots, \phi_n$ span W^0 and hence form a basis of W^0.

Suppose $\alpha \in W$. Then $\alpha = \sum_{i=1}^{r} a_i\alpha_i$ for some $a_i \in \mathbb{F}$. If $r+1 \le j \le n$, $\phi_j(\alpha) = \sum_{i=1}^{r} a_i\phi_j(\alpha_i) = 0$. Thus $\phi_{r+1}, \ldots, \phi_n \in W^0$.

Suppose $\phi \in W^0$. Then $\phi \in \widehat{V}$ and so $\phi = \sum_{i=1}^{n} b_i\phi_i$ for some $b_i \in \mathbb{F}$. Then for $1 \le j \le r$, $0 = \phi(\alpha_j) = b_j$. Thus $\phi = \sum_{i=r+1}^{n} b_i\phi_i$. Thus $W^0 = \text{span}\{\phi_{r+1}, \ldots, \phi_n\}$. □

Example 9.2.6 Let $W = \text{span}\{(1,0,-1),\ (-1,1,0),\ (0,1,-1)\}$ be a subspace of $\mathbb{R}^3$. We would like to find a basis of W^0.

We first observe that $\dim W = 2$ and W has a basis $\{(1,0,-1),\ (-1,1,0)\}$. Extend this basis to a basis $\{(1,0,-1),\ (-1,1,0),\ (0,1,1)\}$ of $\mathbb{R}^3$. By Example 9.2.3 we obtain the dual basis $\{\psi_1, \psi_2, \psi_3\}$. Then by the proof of Theorem 9.2.5 we see that $\{\psi_3\}$ is a basis of W^0. That is, $\psi_3(x,y,z) = \frac{1}{2}(x+y+z)$. Note that we can also let $[\phi_3]_\Phi = \begin{pmatrix} b_1 & b_2 & b_3 \end{pmatrix}^T$ or $\phi(x,y,z) = b_1x + b_2y + b_3z$ in W^0 and use definition to determine b_1, b_2, b_3. □

Since the dual space $\widehat{V}$ of V is also a vector space. We can also consider the annihilator of a subset S of $\widehat{V}$ (S can be empty). The annihilator S^0 is a subspace of $\widehat{\widehat{V}}$. Since we have identified $\widehat{\widehat{V}}$ with V, S^0 is viewed as a subspace of V. Namely, $S^0 = \{\alpha \in V \mid \phi(\alpha) = 0\ \forall \phi \in S\}$. By Theorem 9.2.5 we have

Theorem 9.2.7 *Let S be a subspace of $\widehat{V}$. If $\dim V = n$ and $\dim S = s$, then $\dim S^0 = n - s$.*

Theorem 9.2.8 *If W is a subset of a vector space V, then $W \subseteq (W^0)^0$. If W is a subspace and $\dim V$ is finite, then $(W^0)^0 = W$.*

Proof: It is clear that $W \subseteq (W^0)^0 = \{\alpha \in V \mid \phi(\alpha) = 0\ \forall \phi \in W^0\}$.

If $\dim W < \infty$, then $\dim(W^0)^0 = \dim \widehat{V} - \dim W^0 = n - (n - \dim W) = \dim W$. Hence $(W^0)^0 = W$. □

Theorem 9.2.9 *Let W_1 and W_2 be two subsets containing $\mathbf{0}$ in a finite dimensional vector space V. Then $(W_1 + W_2)^0 = W_1^0 \cap W_2^0$. If W_1 and W_2 are subspaces, then $(W_1 \cap W_2)^0 = W_1^0 + W_2^0$.*

Proof: Suppose $\phi \in (W_1 + W_2)^0$. Then for $\alpha_1 \in W_1$, since $\mathbf{0} \in W_2$, $\alpha_1 = \alpha_1 + \mathbf{0} \in W_1 + W_2$. Thus $\phi(\alpha_1) = 0$ and hence $\phi \in W_1^0$. Similarly, $\phi \in W_2^0$. Hence $\phi \in W_1^0 \cap W_2^0$ and $(W_1 + W_2)^0 \subseteq W_1^0 \cap W_2^0$.

Conversely, suppose $\phi \in W_1^0 \cap W_2^0$. Then for $\alpha \in W_1 + W_2$, $\alpha = \alpha_1 + \alpha_2$ with $\alpha_1 \in W_1$ and $\alpha_2 \in W_2$, $\phi(\alpha) = \phi(\alpha_1) + \phi(\alpha_2) = 0$. Hence $\phi \in (W_1 + W_2)^0$ and $W_1^0 \cap W_2^0 \subseteq (W_1 + W_2)^0$.

Suppose W_1 and W_2 are subspaces. Then $W_1 \cap W_2 = (W_1^0)^0 \cap (W_2^0)^0$. Since both W_1^0 and W_2^0 contain O in $\widehat{V}$, $(W_1^0 + W_2^0)^0 = (W_1^0)^0 \cap (W_2^0)^0$ by what we have just proved. Thus, $W_1 \cap W_2 = (W_1^0 + W_2^0)^0$. By Theorem 9.2.8 we have $(W_1 \cap W_2)^0 = W_1^0 + W_2^0$. □

Remark: In establishing the second equality of Theorem 9.2.9, we do need W_1 and W_2 to be subspaces. For, if we let $V = \mathbb{R}^2$, $W_1 = \{(0,0),\ (1,0)\}$ and $W_2 = \{(0,0),\ (-1,0)\}$, then $W_1 \cap W_2 = \{(0,0)\}$ and hence $(W_1 \cap W_2)^0 = \widehat{V}$. However, $W_1^0 = W_2^0$, so $W_1^0 + W_2^0$ is of dimension one.

Exercise 9.2

9.2-1. Let V be a finite dimensional vector space. Suppose S is a proper subspace of $\widehat{V}$. Let $\phi \in \widehat{V} \setminus S$. Show that there exists an $\alpha \in V$ such that $\phi(\alpha) = 1$ and $\psi(\alpha) = 0$ for all $\psi \in S$.

9.2-2. Let $\phi, \psi \in \widehat{V}$ be such that $\phi(\alpha) = 0$ always implies $\psi(\alpha) = 0$ for all $\alpha \in V$. Show that ψ is a multiplies of ϕ, i.e., there is a scalar $c \in \mathbb{F}$ such that $\psi = c\phi$.

9.2-3. Let $W = \text{span}\{(1, 0, -1),\ (1, -1, 0),\ (0, 1, -1)\}$ be a real vector subspace. Find W^0.

9.2-4. Let $W_1 = \{(1, 2, 3, 0),\ (0, 1, -1, 1)\}$ and $W_2 = \{(1, 0, 1, 2)\}$ be real vector subspaces. Find $(W_1 + W_2)^0$ and $W_1^0 \cap W_2^0$.

9.2-5. Show that if S and T are subspaces of V such that $V = S + T$, then $S^0 \cap T^0 = \{\mathbf{0}\}$.

9.2-6. Show that if S and T are subspaces of V such that $V = S \oplus T$, then $\widehat{V} = S^0 \oplus T^0$.

9.3 The Dual of a Linear Transformation

For vector spaces U and V, we will study the relation of $L(U, V)$ and $L(\widehat{V}, \widehat{U})$ in this section.

Theorem 9.3.1 *Let U and V be vector spaces and $\sigma \in L(U, V)$. The mapping $\hat{\sigma} : \widehat{V} \to \widehat{U}$ defined by $\hat{\sigma}(\phi) = \phi \circ \sigma$ for $\phi \in \widehat{V}$ is linear.*

Proof: Since $\sigma \in L(U, V)$ and $\phi \in \widehat{V} = L(V, \mathbb{F})$, $\phi \circ \sigma : U \to \mathbb{F}$ is linear and hence $\hat{\sigma}(\phi) = \phi \circ \sigma \in \widehat{U}$.

For any $\phi, \psi \in \widehat{V}$ and $a \in \mathbb{F}, \alpha \in U$, we have

$$\begin{aligned}\big(\hat{\sigma}(a\phi + \psi)\big)(\alpha) &= \big((a\phi + \psi) \circ \sigma\big)(\alpha) = (a\phi + \psi)(\sigma(\alpha)) = a\phi(\sigma(\alpha)) + \psi(\sigma(\alpha)) \\ &= \big(a\hat{\sigma}(\phi)\big)(\alpha) + \big(\hat{\sigma}(\psi)\big)(\alpha) = \big(a\hat{\sigma}(\phi) + \hat{\sigma}(\psi)\big)(\alpha).\end{aligned}$$

Thus $\hat{\sigma}(a\phi + \psi) = a\hat{\sigma}(\phi) + \hat{\sigma}(\psi)$. □

Definition 9.3.2 The mapping $\hat{\sigma}$ defined in Theorem 9.3.1 is called the *dual* of σ.

Suppose $\sigma \in L(U, V)$ is represented by the matrix $A = (a_{ij})$ with respect to the bases $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ of U and $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$, respectively.

Let $\Phi = \{\phi_1, \ldots, \phi_n\}$ be the basis in $\widehat{U}$ dual to $\mathscr{A}$ and let $\Psi = \{\psi_1, \ldots, \psi_m\}$ be the basis in $\widehat{V}$ dual to $\mathscr{B}$. Let $G = (g_{ij}) = [\hat{\sigma}]_{\Phi}^{\Psi}$. Now consider

$$\begin{aligned}\big(\hat{\sigma}(\psi_i)\big)(\alpha_j) = (\psi_i \circ \sigma)(\alpha_j) = \psi_i\big(\sigma(\alpha_j)\big) &= \psi_i\left(\sum_{k=1}^{m} a_{kj}\beta_k\right) \\ &= \sum_{k=1}^{m} a_{kj}\psi_i(\beta_k) = \sum_{k=1}^{m} a_{kj}\delta_{ik} = a_{ij} = (A)_{i,j} = (A^T)_{j,i}.\end{aligned}$$

On the other hand, we have $\hat{\sigma}(\psi_i) = \sum_{s=1}^{n} g_{si}\phi_s$ and hence

$$\big(\hat{\sigma}(\psi_i)\big)(\alpha_j) = \left(\sum_{s=1}^{n} g_{si}\phi_s\right)(\alpha_j) = \sum_{s=1}^{n} g_{si}\phi_s(\alpha_j) = \sum_{s=1}^{n} g_{sj}\delta_{sj} = g_{ji} = (G)_{j,i}.$$

This shows the following theorem:

Theorem 9.3.3 *Suppose $\mathscr{A}$ and $\mathscr{B}$ are bases of finite dimensional vector spaces U and V, respectively. Let Φ and Ψ be the dual bases of $\mathscr{A}$ and $\mathscr{B}$, respectively. If $\sigma \in L(U,V)$, then $\hat{\sigma} \in L(\widehat{V},\widehat{U})$ and $[\hat{\sigma}]_{\Phi}^{\Psi} = \big([\sigma]_{\mathscr{B}}^{\mathscr{A}}\big)^T$.*

Let G and A be as defined in the above theorem. If we use the $m \times 1$ matrix X to represent ψ (i.e., $[\psi]_{\Psi}$) and the $n \times 1$ matrix Y to represent ϕ (i.e., $[\phi]_{\Phi} = Y$), then the matrix equation for $\hat{\sigma}(\psi) = \phi$ will have the form $GX = Y$. But as $G = A^T$, we have $X^T A = Y^T$.

The dual linear transformation $\hat{\sigma}$ of a linear transformation σ has many same properties as what σ has. We shall show some of them below.

Theorem 9.3.4 *Let $\sigma \in L(U,V)$. Then* $\ker(\hat{\sigma}) = (\sigma(U))^0$.

Proof:

$$\begin{aligned} \psi \in \ker(\hat{\sigma}) \quad & \text{if and only if} \quad \hat{\sigma}(\psi) = O \\ & \text{if and only if} \quad \big(\hat{\sigma}(\psi)\big)(\alpha) = \mathbf{0}\ \forall \alpha \in U \\ & \text{if and only if} \quad \psi\big(\sigma(\alpha)\big) = \mathbf{0}\ \forall \alpha \in U \\ & \text{if and only if} \quad \psi \in (\sigma(U))^0. \end{aligned}$$

□

Corollary 9.3.5 *Suppose V is finite dimensional and suppose $\sigma \in L(U,V)$. The linear problem $\sigma(\xi) = \beta$ has a solution if and only if $\beta \in (\ker(\hat{\sigma}))^0$.*

Theorem 9.3.6 *Let $\sigma \in L(U,V)$, V finite dimensional and $\beta \in V$. Then either there is $\xi \in U$ such that $\sigma(\xi) = \beta$ or there is $\phi \in \widehat{V}$ such that $\hat{\sigma}(\phi) = O$ and $\phi(\beta) = 1$.*

Proof: Let $\beta \in V$. If $\beta \in \sigma(U)$, then there exists $\xi \in U$ such that $\sigma(\xi) = \beta$. Now suppose not, then by Corollary 9.3.5 that $\beta \notin (\ker(\hat{\sigma}))^0$. Thus there exists $\psi \in \ker(\hat{\sigma})$ such that $\psi(\beta) = c \neq 0$. Let $\phi = c^{-1}\psi$. Then $\hat{\sigma}(\phi) = O$ and $\phi(\beta) = 1$. □

Theorem 9.3.7 *Let U and V be finite dimensional vector spaces. Suppose $\sigma \in L(U,V)$. Then* $\operatorname{rank}(\sigma) = \operatorname{rank}(\hat{\sigma})$.

Proof: This is because

$$\operatorname{rank}(\hat{\sigma}) = \dim \widehat{V} - \operatorname{nullity}(\hat{\sigma}) = \dim V - \dim(\ker(\hat{\sigma})) = \dim\big((\ker(\hat{\sigma}))^0\big) = \dim(\sigma(U)) = \operatorname{rank}(\sigma).$$ □

Theorem 9.3.8 *Let $\sigma \in L(V,V)$. If W is a subspace invariant under σ, then W^0 is a subspace of $\widehat{V}$ also invariant under $\hat{\sigma}$.*

Proof: Let $\phi \in W^0$. Then for each $\alpha \in W$, $\big(\hat{\sigma}(\phi)\big)(\alpha) = \phi(\sigma(\alpha)) = 0$ since $\sigma(\alpha) \in W$ and $\phi \in W^0$. Thus $\hat{\sigma}(\phi) \in W^0$. □

Lemma 9.3.9 *Let $\sigma, \tau \in L(U,V)$, $c \in \mathbb{F}$. Then $\widehat{c\sigma + \tau} = c\hat{\sigma} + \hat{\tau}$.*

Proof: To prove the lemma, we have to prove that for each $\phi \in \widehat{V}$, linear forms $(\widehat{c\sigma + \tau})(\phi)$ and $(c\hat{\sigma} + \hat{\tau})(\phi)$ in $\widehat{U}$ are equal.

For each $\alpha \in U$, we have

$$\begin{aligned} \big((\widehat{c\sigma + \tau})(\phi)\big)(\alpha) &= \big(\phi \circ (c\sigma + \tau)\big)(\alpha) = \phi\big((c\sigma + \tau)(\alpha)\big) = \phi\big(c\sigma(\alpha) + \tau(\alpha)\big) \\ &= \phi\big(c\sigma(\alpha)\big) + \phi\big(\tau(\alpha)\big) = c\phi\big(\sigma(\alpha)\big) + \phi\big(\tau(\alpha)\big) \\ &= c(\phi \circ \sigma)(\alpha) + (\phi \circ \tau)(\alpha) = c\big(\hat{\sigma}(\phi)\big)(\alpha) + \big(\hat{\tau}(\phi)\big)(\alpha) \\ &= \big(c\hat{\sigma}(\phi)\big)(\alpha) + \big(\hat{\tau}(\phi)\big)(\alpha) = \big(c\hat{\sigma}(\phi) + \hat{\tau}(\phi)\big)(\alpha) = \big((c\hat{\sigma} + \hat{\tau})(\phi)\big)(\alpha) \end{aligned}$$

Thus $\widehat{c\sigma+\tau} = c\hat{\sigma}+\hat{\tau}$. □

From the above lemma, it shows that the mapping $\sigma \mapsto \hat{\sigma}$ is a linear transformation from $L(U,V)$ to $L(\widehat{V},\widehat{U})$. It is easy to show that this linear transformation is an isomorphism.

Theorem 9.3.10 *Suppose V is a finite dimensional vector space and $\sigma \in L(V,V)$. If λ is an eigenvalue of σ, then λ is also an eigenvalue of $\hat{\sigma}$.*

Proof: Let λ be an eigenvalue of σ and put $\eta = \sigma - \lambda\iota$. By Theorem 9.3.7 $\text{rank}(\eta) = \text{rank}(\hat{\eta})$. Since η is singular, $\text{rank}(\eta) < \dim V = \dim \widehat{V}$. Thus $\text{rank}(\hat{\eta}) < \dim \widehat{V}$ and $\hat{\eta}$ is singular. Clearly, by Lemma 9.3.9 $\hat{\eta} = \hat{\sigma} - \lambda\hat{\iota}$. It is clear that $\hat{\iota}$ is the identity mapping on $\widehat{V}$. Therefore, λ is an eigenvalue of $\hat{\sigma}$. □

This is an expected result, since we know that if λ is an eigenvalue of A then λ is also an eigenvalue of A^T.

Assume that U and V are two finite dimensional vector spaces. Let $\sigma \in L(U,V)$. Then $\hat{\sigma} \in L(\widehat{V},\widehat{U})$. Let $\hat{\hat{\sigma}}$ be the dual of $\hat{\sigma}$. Then $\hat{\hat{\sigma}} \in L(\widehat{\widehat{U}},\widehat{\widehat{V}})$. Let $\sigma' : U \to V$ be the mapping $J_V^{-1} \circ \hat{\hat{\sigma}} \circ J_U$, where $J_U : U \to \widehat{\widehat{U}}$ and $J_V : V \to \widehat{\widehat{V}}$ are the isomorphisms in Theorem 9.2.1. Now for $\alpha \in U$, $\phi \in \widehat{V}$, we have

$$\Big(\hat{\hat{\sigma}}(J_U(\alpha))\Big)(\phi) = \big(J_U(\alpha)\big)(\hat{\sigma}(\phi)) = \big(\hat{\sigma}(\phi)\big)(\alpha) = \phi(\sigma(\alpha)) = \big(J_V(\sigma(\alpha))\big)(\phi).$$

Thus $\hat{\hat{\sigma}}(J_U(\alpha)) = J_V(\sigma(\alpha))$ for all $\alpha \in U$. Hence $\hat{\hat{\sigma}} \circ J_U = J_V \circ \sigma$. That is, $\sigma = J_V^{-1} \circ \hat{\hat{\sigma}} \circ J_U = \sigma'$. Thus, we may regard σ as the dual of $\hat{\sigma}$.

Example 9.3.11 It is known that every functional ϕ on $\mathbb{F}^n$ is of the form $\phi(x_1,\ldots,x_n) = \sum_{i=1}^{n} a_i x_i$ for some $a_i \in \mathbb{F}$. Let us consider a simpler case. Let $U = \mathbb{R}^2$ and $V = \mathbb{R}^3$. Suppose $\sigma \in L(U,V)$ defined by $\sigma(x,\ y) = (x+y,\ x-2y,\ -x)$. For any $\phi \in \widehat{V}$, $\phi(x,y,z) = ax+by+cz$ for some $a,b,c \in \mathbb{R}$. Then $\hat{\sigma}(\phi)$ is a linear functional on U. By definition we have

$$\begin{aligned}\hat{\sigma}(\phi)(x,\ y) &= \phi(\sigma(x,\ y)) = \phi(x+y,\ x-2y,\ -x)\\ &= a(x+y)+b(x-2y)+c(-x) = (a+b-c)x+(a-2b)y.\end{aligned}$$ □

Exercise 9.3

9.3-1. Let $\mathbb{F}$ be a field and let ϕ be the linear functional on $\mathbb{F}^2$ defined by $\phi(x,y) = ax+by$. For each of the following linear transformation σ, let $\psi = \hat{\sigma}(\phi)$, find $\hat{\sigma}$ and $\psi(x,y)$.

(a) $\sigma(x,y) = (x,0)$.

(b) $\sigma(x,y) = (-y,x)$.

(c) $\sigma(x,y) = (x-y,x+y)$.

9.3-2. Let $V = \mathbb{R}[x]$. Let a and b be fixed real numbers and let ϕ be the linear functional on V defined by $\phi(p) = \int_a^b p(t)dt$. If D is the differentiation operation on V, what is $\hat{D}(\phi)$?

9.3-3. Let $V = M_n(\mathbb{F})$ and let $B \in V$ be fixed. Let $\sigma \in L(V,V)$ be defined by $\sigma(A) = AB - BA$. Let $\phi =$Tr be the trace function. What is $\hat{\sigma}(\phi)$?

9.4 Quadratic Forms

Let $A \in M_{m,n}(\mathbb{F})$. $F(X,Y) = X^T AY$, for $X \in \mathbb{F}^m$ and $Y \in \mathbb{F}^n$, is a function defined on $\mathbb{F}^m \times \mathbb{F}^n$. If we fix Y as a constant vector, then $f(X) = F(X,Y)$ is a linear form defined on $\mathbb{F}^m$. Similarly, if we fix X as a constant, then $g(Y) = F(X,Y)$ is a linear from on $\mathbb{F}^n$. Such F is called a bilinear form.

Definition 9.4.1 Let U and V be vector spaces over $\mathbb{F}$. A mapping $f : U \times V \to \mathbb{F}$ is said to be *bilinear* if f is linear in each variable, that is,

(1) $f(a\alpha_1 + \alpha_2, \beta) = af(\alpha_1, \beta) + f(\alpha_2, \beta)$ and

(2) $f(\alpha, b\beta_1 + \beta_2) = bf(\alpha, \beta_1) + f(\alpha, \beta_2)$

for all $\alpha, \alpha_1, \alpha_2 \in U$, $\beta, \beta_1, \beta_2 \in V$ and $a, b \in \mathbb{F}$. f is called a *bilinear form.*

Example 9.4.2 Let $U = V = \mathbb{R}^n$ and $\mathbb{F} = \mathbb{R}$. Suppose $\alpha = (x_1, \ldots, x_n)$ and $\beta = (y_1, \ldots, y_n)$. Define $f(\alpha, \beta) = \sum_{i=1}^{n} x_i y_i$. Then f is a bilinear form. It is known as an *inner product* and is called the *dot product.* □

Example 9.4.3 Let $U = V$ be the space of all real valued continuous functions on $[0,1]$. Let $\mathbb{F} = \mathbb{R}$. Define $f(\alpha, \beta) = \int_0^1 \alpha(x)\beta(x)dx$. Then f is a bilinear form. Note that it is also an inner product on U. We shall discuss inner product in Chapter 10. □

Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_m\}$ be a basis of U and let $\mathscr{B} = \{\beta_1, \ldots, \beta_n\}$ be a basis of V. Then for $\alpha \in U$ and $\beta \in V$, we have $\alpha = \sum_{i=1}^{m} x_i\alpha_i$ and $\beta = \sum_{j=1}^{n} y_j\beta_j$ with $x_i, y_j \in \mathbb{F}$. Then

$$f(\alpha, \beta) = f\left(\sum_{i=1}^{m} x_i\alpha_i,\ \sum_{j=1}^{n} y_j\beta_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} x_i y_j f(\alpha_i, \beta_j).$$

Put $b_{ij} = f(\alpha_i, \beta_j)\ \forall i, j$. This defines an $m \times n$ matrix $B = (b_{ij})$. B is called the *matrix representing f with respect to bases $\mathscr{A}$ and $\mathscr{B}$.* We denote this matrix by $\{f\}_{\mathscr{B}}^{\mathscr{A}}$.

Suppose $[\alpha]_{\mathscr{A}} = X = (x_1, \cdots, x_m)^T$ and $[\beta]_{\mathscr{B}} = Y = (y_1, \cdots, y_n)^T$, then

$$f(\alpha, \beta) = X^T BY = ([\alpha]_{\mathscr{A}})^T \{f\}_{\mathscr{B}}^{\mathscr{A}} [\beta]_{\mathscr{B}}.$$

Now suppose $\mathscr{A}' = \{\alpha_1', \ldots, \alpha_m'\}$ is another basis of U with transition matrix $P = (p_{ij})$ and suppose $\mathscr{B}' = \{\beta_1', \ldots, \beta_n'\}$ is another basis of V with transition matrix $Q = (q_{ij})$. Suppose $\{f\}_{\mathscr{B}'}^{\mathscr{A}'} = B' = (b_{ij}')$. Then

$$b_{ij}' = f(\alpha_i', \beta_j') = f\left(\sum_{r=1}^{m} p_{ri}\alpha_r,\ \sum_{s=1}^{n} q_{sj}\beta_s\right) = \sum_{r=1}^{m} p_{ri}\left(\sum_{s=1}^{n} q_{sj} f(\alpha_r, \beta_s)\right) = \sum_{r=1}^{m}\sum_{s=1}^{n} p_{ri} b_{rs} q_{sj}.$$

Thus $B' = P^T BQ$. Hence $\operatorname{rank}(B') = \operatorname{rank}(B)$.

In particular, when $U = V$ we can choose $\mathscr{A} = \mathscr{B}$ and $\mathscr{A}' = \mathscr{B}'$. Then $Q = P$ and $B' = P^T BP$.

Definition 9.4.4 Two square matrices A and B are said to be *congruent* if there exists a non-singular matrix P such that $B = P^T AP$.

Proposition 9.4.5 *For a fixed natural number n, congruence is an equivalence relation on $M_{n,n}(\mathbb{F})$.*

Definition 9.4.6 A bilinear form $f : V \times V \to \mathbb{F}$ is said to be *symmetric* if $f(\alpha, \beta) = f(\beta, \alpha)$ $\forall \alpha, \beta \in V$. f is said to be *skew-symmetric* if $f(\alpha, \alpha) = 0$ $\forall \alpha \in V$.

Theorem 9.4.7 *For a finite dimensional vector space V, bilinear form f is symmetric if and only if any representing matrix is symmetric.*

Proof: Suppose the bilinear form $f : V \times V \to \mathbb{F}$ is symmetric. Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ be a basis of V. Let $\{f\}^{\mathscr{A}}_{\mathscr{A}} = B = (b_{ij})$. Since f is symmetric, $b_{ij} = f(\alpha_i, \alpha_j) = f(\alpha_j, \alpha_i) = b_{ji}$ $\forall i, j$. Thus B is symmetric.

Conversely, suppose $B = \{f\}^{\mathscr{A}}_{\mathscr{A}}$ is a symmetric matrix. For $\alpha, \beta \in V$, let $[\alpha]_{\mathscr{A}} = X$ and $[\beta]_{\mathscr{A}} = Y$, we have $f(\alpha, \beta) = X^T BY = (X^T BY)^T = Y^T B^T X = Y^T BX = f(\beta, \alpha)$. □

Note that if A is another matrix representing f, then $A = P^T BP$ for some invertible matrix P. Hence B is symmetry if and only if A is symmetry.

Theorem 9.4.8 *If a bilinear form f on a finite dimensional vector space is skew-symmetric, then any matrix B representing f is skew-symmetric.*

Proof: Let $\alpha, \beta \in V$. Then

$$0 = f(\alpha + \beta, \alpha + \beta) = f(\alpha, \alpha) + f(\alpha, \beta) + f(\beta, \alpha) + f(\beta, \beta) = f(\alpha, \beta) + f(\beta, \alpha).$$

Thus $f(\alpha, \beta) = -f(\alpha, \beta)$. Hence, for any basis $\{\alpha_1, \ldots, \alpha_n\}$ of V, we have

$$b_{ij} = f(\alpha_i, \alpha_j) = -f(\alpha_j, \alpha_i) = -b_{ji}\ \forall i, j.$$

That is, $B^T = -B$. □

For the converse of the above theorem, we need an additional condition.

Theorem 9.4.9 *If $1 + 1 \neq 0$ in $\mathbb{F}$ and the matrix B representing f is skew-symmetric, then f is skew-symmetric.*

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of a vector space such that B represents f with respect to this basis. Since $B^T = -B$, $f(\alpha_i, \alpha_j) = -f(\alpha_j, \alpha_i)$ $\forall i, j$. Hence $f(\alpha, \beta) = -f(\beta, \alpha)$ $\forall \alpha, \beta \in V$. In particular, $f(\alpha, \alpha) = -f(\alpha, \alpha)$ $\forall \alpha \in V$. Thus $(1 + 1)f(\alpha, \alpha) = 0$. Since $1 + 1 \neq 0$, $f(\alpha, \alpha) = 0$. Therefore, f is skew-symmetric. □

For convenience, we shall use 2 to denote $1 + 1$ in any field. Thus $2 = 0$ in the field $\mathbb{Z}_2$.

Theorem 9.4.10 *If the field is such that $2 \neq 0$, then any bilinear from $f : V \times V \to \mathbb{F}$ can be expressed uniquely as a sum of symmetric bilinear form and a skew-symmetric bilinear form.*

Proof: Define $g, h : V \times V \to \mathbb{F}$ by

$$g(\alpha, \beta) = 2^{-1}[f(\alpha, \beta) + f(\beta, \alpha)] \quad \text{and} \quad h(\alpha, \beta) = 2^{-1}[f(\alpha, \beta) - f(\beta, \alpha)], \alpha, \beta \in V.$$

Then it is easy to see that g is a symmetric bilinear form, h is a skew-symmetric bilinear form and $f = g + h$. To show the uniqueness, suppose $f = g_1 + h_1$ is another such decomposition with g_1 symmetric and h_1 skew-symmetric. Then by the definitions of g and g_1,

$$\begin{aligned} g(\alpha, \beta) &= 2^{-1}[f(\alpha, \beta) + f(\beta, \alpha)] = 2^{-1}[g_1(\alpha, \beta) + h_1(\alpha, \beta) + g_1(\beta, \alpha) + h_1(\beta, \alpha)] \\ &= 2^{-1}[2g_1(\alpha, \beta)] = g_1(\alpha, \beta). \end{aligned}$$

Hence $h_1 = f - g_1 = f - g = h$. □

Note that if $2 \neq 0$ in a field $\mathbb{F}$, then for any square matrix A over $\mathbb{F}$, A can always be expressed uniquely as $A = B+C$ with B symmetric and C skew-symmetric. We can simply put $B = 2^{-1}(A+A^T)$ and $C = 2^{-1}(A - A^T)$.

Definition 9.4.11 A function q from a vector space V into the scalar field $\mathbb{F}$ is called a *quadratic form* if there exists a bilinear form $f : V \times V \to \mathbb{F}$ such that $q(\alpha) = f(\alpha, \alpha)$.

Remark 9.4.12 Suppose the bilinear form f is of the form $g + h$ with g symmetric and h skew-symmetric. Then $q(\alpha) = f(\alpha, \alpha) = g(\alpha, \alpha)$. Thus q is determined by the symmetric part of f only.

Theorem 9.4.13 *Suppose* $2 \neq 0$. *There is a bijection between symmetric bilinear forms and quadratic forms.*

Proof: Let S be the set of symmetric bilinear forms on a vector space V and let Q be the set of quadratic forms on V. For each $f \in S$, let $q(\alpha) = f(\alpha, \alpha)$ for each $\alpha \in V$. Then $q \in Q$. So we may define a mapping $\phi : S \to Q$ by $\phi(f) = q$.

Note that, suppose q is a quadratic form defined by a symmetric bilinear form f. Then by definition

$$\begin{aligned} q(\alpha + \beta) - q(\alpha) - q(\beta) &= f(\alpha + \beta, \alpha + \beta) - f(\alpha, \alpha) - f(\beta, \beta) \\ &= f(\alpha, \beta) + f(\beta, \alpha) = 2f(\alpha, \beta). \end{aligned} \tag{9.3}$$

Suppose there are two symmetric bilinear forms f and f_1 both mapped to the same quadratic form q under ϕ. Then by Equation (9.3) we have $2f(\alpha, \beta) = 2f_1(\alpha, \beta)$ for all $\alpha, \beta \in V$. Since $2 \neq 0$, $f = f_1$. Thus, ϕ is an injection.

Suppose q is a quadratic form. By definition there is a bilinear from f such that $q(\alpha) = f(\alpha, \alpha)$ for $\alpha \in V$. Since $2 \neq 0$, by Theorem 9.4.10 we have the symmetric part g of f. From Remark 9.4.12 we have $g(\alpha, \alpha) = q(\alpha)$ for $\alpha \in V$. So $\phi(g) = q$. This means that ϕ is a surjection. □

A matrix representing a quadratic form is a symmetric matrix which represents the corresponding symmetric bilinear form given by Theorem 9.4.13. Here, we assume that $2 \neq 0$.

Example 9.4.14 Let $q : \mathbb{R}^2 \to \mathbb{R}$ be defined by $q(x, y) = x^2 - 4xy + 3y^2$. Then q is a quadratic, since $q(x, y) = f((x, y),\ (x, y))$, where $f((x, y), (u, v)) = (x, y)\begin{pmatrix} 1 & 0 \\ -4 & 3 \end{pmatrix}\begin{pmatrix} u \\ v \end{pmatrix}$ is a bilinear form. We can choose a symmetric bilinear form

$$g((x, y), (u, v)) = (x, y)\begin{pmatrix} 1 & -2 \\ -2 & 3 \end{pmatrix}\begin{pmatrix} u \\ v \end{pmatrix}.$$

It is easy to see that $q(x, y) = g((x, y),\ (x, y))$. □

In general, if $2 \neq 0$, then the quadratic form $X^T AX = q(x_1, \ldots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j$ has the representing matrix $S = (s_{ij})$ with $s_{ij} = 2^{-1}(a_{ij} + a_{ji})$.

Example 9.4.15 Let $V = \mathbb{Z}_2^2$. Let f be a bilinear form whose representing matrix is $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to the standard basis. Clearly f is symmetric. f determines the quadratic form $q(x, y) = x^2$. One can see that there is another symmetric f_1 whose representing matrix is $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ determining q.

□

Given a quadratic form, we want to change the variables such that the quadratic form becomes as simple as possible. Any quadratic form can be represented by a symmetric matrix A. If we change the basis of the domain space of the quadratic form, then the representing matrix becomes P^TAP for some invertible matrix P. So the problem becomes to find an invertible matrix P such that P^TAP is in the simplest form.

Theorem 9.4.16 *Let f be a symmetric bilinear form on V, where V is finite dimensional vector space over $\mathbb{F}$. If $2 \neq 0$ in $\mathbb{F}$, then there is a basis $\mathscr{B}$ of V such that $\{f\}_{\mathscr{B}}^{\mathscr{B}}$ is diagonal.*

Proof: Let $\mathscr{A}$ be a basis of V. Let $A = \{f\}_{\mathscr{A}}^{\mathscr{A}}$.

We shall prove the theorem by mathematical induction on n, the dimension of V. If $n = 1$, then the theorem is obvious.

Suppose the theorem holds for all symmetric bilinear forms on vector spaces of dimension $n-1$. Let f be a symmetric bilinear form on V with $\dim V = n > 1$. If $A = O$, then it is already diagonal. Thus we assume $A \neq O$.

Let q be the quadratic form induced from f. Then $f(\alpha, \beta) = 2^{-1}[q(\alpha+\beta) - q(\alpha) - q(\beta)]$. If $q(\alpha) = 0\ \forall \alpha \in V$, then $f(\alpha, \beta) = 0\ \forall \alpha, \beta \in V$. Since $A \neq O$, there exists $\beta_1 \in V$ such that $q(\beta_1) = d_1 \neq 0$. Define $\phi : V \to \mathbb{F}$ by $\phi(\alpha) = f(\beta_1, \alpha)$. Then ϕ is a nonzero linear form since $\phi(\beta_1) = d_1 \neq 0$.

Let $W = \ker(\phi)$. Then $\dim W = n - 1$. Suppose g is the restriction of f on $W \times W$. Then g is a symmetric bilinear form on W. By induction assumption, there is a basis $\mathscr{B}_1 = \{\beta_2, \ldots, \beta_n\}$ of W such that $\{g\}_{\mathscr{B}_1}^{\mathscr{B}_1}$ is diagonal. That is, $g(\beta_i, \beta_j) = 0$, for $i \neq j$, $2 \leq i, j \leq n$. However, for $i \geq 2$, $f(\beta_i, \beta_1) = f(\beta_1, \beta_i) = \phi(\beta_i) = 0$. Thus $f(\beta_i, \beta_j) = 0$, for $i \neq j$, $1 \leq i, j \leq n$. Let $\mathscr{B} = \{\beta_1\} \cup \mathscr{B}_1$. Then $\{f\}_{\mathscr{B}}^{\mathscr{B}} = \operatorname{diag}\{d_1, d_2, \ldots, d_n\}$, for some $d_2, \ldots, d_n \in \mathbb{F}$. □

For any given symmetric matrix A, it is a representing matrix of a bilinear form on some finite dimensional vector space. For example, we may choose $V = \mathbb{F}^n$, $\mathscr{A}$ is the standard basis of $\mathbb{F}^n$ and $f(X, Y) = X^TAY$ for all $X, Y \in \mathbb{F}^n$. By Theorem 9.4.16 if we let P be the matrix of transition from $\mathscr{A}$ to $\mathscr{B}$, then we have the following corollary.

Corollary 9.4.17 *Let $\mathbb{F}$ be a field such that $2 \neq 0$. Then for any symmetric matrix A over $\mathbb{F}$, there is an invertible matrix P such that P^TAP is diagonal.*

The above result may not hold if $1 + 1 = 0$. For example, $\mathbb{F} = \mathbb{Z}_2$ and $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then we cannot find an invertible matrix such that P^TAP is diagonal.

Note that, the d_i's along the main diagonal of $\{f\}_{\mathscr{B}}^{\mathscr{B}} = P^TAP$ (for some P) described in the proof of Theorem 9.4.16 are not unique. We can introduce a third basis $\mathscr{C} = \{\gamma_1, \ldots, \gamma_n\}$ by putting $\gamma_i = a_i\beta_i$ with $a_i \neq 0$ for all i. Then the matrix of transition Q from $\mathscr{B}$ to $\mathscr{C}$ is $\operatorname{diag}\{a_1, \ldots, a_n\}$. Then the matrix representing f with respect to $\mathscr{C}$ is $(PQ)^TAPQ = \operatorname{diag}\{a_1^2d_1, \ldots, a_n^2d_n\}$. Thus the elements in the main diagonal may be multiplied by arbitrary non-zero squares from $\mathbb{F}$.

Theorem 9.4.18 *If $\mathbb{F} = \mathbb{C}$, then every symmetric matrix is congruent to a diagonal matrix in which all the non-zero elements are 1's.*

Proof: We simply choose a_i for each i for which $d_i \neq 0$ such that $a_i^2d_i = 1$. □

In practice, how do we find an invertible matrix P or the diagonal form D? We shall provide three methods for finding such matrices.

Inductive method

Let $A = (a_{ij})$ be a symmetric matrix. We shall use the idea used in the proof of Theorem 9.4.16 to find an invertible matrix P such that P^TAP is diagonal. As before, A determines a symmetric bilinear form f and a quadratic form q with respect to some basis $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$ of some vector space V. Here $2 \neq 0$ in $\mathbb{F}$.

First choose β_1 such that $f(\beta_1, \beta_1) = q(\beta_1) \neq 0$. If $a_{11} \neq 0$, then we let $\beta_1 = \alpha_1$, for $a_{11} = f(\alpha_1, \alpha_1)$. If $a_{11} = 0$ but $a_{22} \neq 0$, then we let $\beta_1 = \alpha_2$. If $a_{11} = a_{22} = 0$ but $a_{12} \neq 0$, then we let $\beta_1 = \alpha_1 + \alpha_2$. Then $f(\beta_1, \beta_1) = f(\alpha_1, \alpha_1) + 2f(\alpha_1, \alpha_2) + f(\alpha_2, \alpha_2) = 2a_{12}$. If $a_{11} = a_{12} = a_{22} = 0$ but $a_{33} \neq 0$, then we let $\beta_1 = \alpha_3$. Thus, unless $A = O$, this process enables us to choose β_1 such that $f(\beta_1, \beta_1) \neq 0$.

Define $\phi_1 \in \widehat{V}$ by $\phi_1(\alpha) = f(\beta_1, \alpha)\ \forall \alpha \in V$. Now suppose $[\beta_1]_{\mathscr{A}} = \begin{pmatrix} p_{11} \\ \vdots \\ p_{n1} \end{pmatrix}$ and $[\alpha]_{\mathscr{A}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. That is, $\beta_1 = \sum_{i=1}^{n} p_{i1}\alpha_i$ and $\alpha = \sum_{i=1}^{n} x_i\alpha_i$. Then $\phi_1(\alpha) = \sum_{j=1}^{n}\sum_{i=1}^{n} p_{i1}a_{ij}x_j$. Thus ϕ_1 is represented by the $1 \times n$ matrix $\begin{pmatrix} p_{11} & \cdots & p_{n1} \end{pmatrix} A$.

Next we put $W_1 = \ker(\phi_1)$. If $q\big|_{W_1} = O$, then we are done by choosing any basis $\{\beta_2, \ldots, \beta_n\}$ of W_1. Otherwise, choose $\beta_2 \in W_1$ such that $q(\beta_2) = f(\beta_2, \beta_2) \neq 0$. Define $\phi_2 \in \widehat{V}$ by $\phi_2(\alpha) = f(\beta_2, \alpha)\ \forall \alpha \in V$. Suppose $[\beta_2]_{\mathscr{A}} = \begin{pmatrix} p_{12} \\ \vdots \\ p_{n2} \end{pmatrix}$, then by the above argument, ϕ_2 is represented by the $1 \times n$ matrix $\begin{pmatrix} p_{12} & \cdots & p_{n2} \end{pmatrix} A$.

Let $W_2 = W_1 \cap \ker(\phi_2)$. If $q\big|_{W_2} = O$, then we are done. Otherwise, choose $\beta_3 \in W_2$ such that $q(\beta_3) = f(\beta_3, \beta_3) \neq 0$. Define $\phi_3 \in \widehat{V}$ by $\phi_3(\alpha) = f(\beta_3, \alpha)\ \forall \alpha \in V$. This process can be continued until we have found $\{\beta_1, \ldots, \beta_n\}$ and $\{\phi_1, \ldots, \phi_n\}$ so that

$$D = P^TAP = \operatorname{diag}\{\phi_1(\beta_1), \phi_2(\beta_2), \ldots, \phi_n(\beta_n)\}.$$

Here $\phi_i(\beta_i) = f(\beta_i, \beta_i)$ and $P = (p_{ij})$.

Example 9.4.19 Let $A = \begin{pmatrix} 0 & 1 & -1 & 2 \\ 1 & 1 & 0 & -1 \\ -1 & 0 & -1 & 1 \\ 2 & -1 & 1 & 0 \end{pmatrix}$ over $\mathbb{R}$.

For convenience to compute, we usually choose $\mathscr{A}$ to be the standard basis (of $\mathbb{R}^4$). Let f and q be the corresponding bilinear form and quadratic form, respectively. Since $(A)_{1,1} = 0$ and $(A)_{2,2} = 1 \neq 0$, we put $\beta_1 = \boldsymbol{e}_2 = (0, 1, 0, 0)$. Now the linear form ϕ_1 is represented by

$$\begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} A = \begin{pmatrix} 1 & 1 & 0 & -1 \end{pmatrix}.$$

Thus $\phi_1(\beta_1) = 1$. Next, we have to choose β_2 such that $\phi_1(\beta_2) = 0$ and $f(\beta_2, \beta_2) \neq 0$, if possible.

If $\beta_2 = (x_1, x_2, x_3, x_4)$, then $\phi_1(\beta_2) = 0$ implies $x_1 + x_2 - x_4 = 0$. Since $\dim(\ker(\phi_1)) = 3$, we may find three linearly independent vectors forming a basis of $\ker(\phi_1)$. Consider these three vectors we may find β_2 such that $q(\beta_2) \neq 0$ or $q|_{\ker(\phi_1)} = O$. If we choose $\beta_2 = (1, 0, 0, 1)$ then the linear form ϕ_2 is represented by

$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} A = \begin{pmatrix} 2 & 0 & 0 & 2 \end{pmatrix}.$$

In this case, $f(\beta_2, \beta_2) = 4 \neq 0$. Next we have to choose β_3 such that $\phi_1(\beta_3) = \phi_2(\beta_3) = 0$ but $f(\beta_3, \beta_3) \neq 0$, if possible.

If $\beta_3 = (x_1, x_2, x_3, x_4)$, then

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

Solving this system we get two linearly independent vectors. Similar to the above case, we may choose $\beta_3 = (1, -2, 0, -1)$ so that $\phi_3(\beta_3) = -8 \neq 0$. Thus ϕ_3 is represented by

$$\begin{pmatrix} 1 & -2 & 0 & -1 \end{pmatrix} A = \begin{pmatrix} -4 & 0 & -2 & 4 \end{pmatrix}.$$

Finally, we choose β_4 such that $\phi_1(\beta_4) = \phi_2(\beta_4) = \phi_3(\phi_4) = 0$. Hence we have to solve the system

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

It is easy to see that we can choose $\beta_4 = (-1, 2, 4, 1)$. Then ϕ_4 is defined by

$$\begin{pmatrix} -1 & 2 & 4 & 1 \end{pmatrix} A = \begin{pmatrix} 0 & 0 & -2 & 0 \end{pmatrix}.$$

Thus $\phi_4(\beta_4) = -8$. So

$$P = \begin{pmatrix} 0 & 1 & 1 & -1 \\ 1 & 0 & -2 & 2 \\ 0 & 0 & 0 & 4 \\ 0 & 1 & -1 & 1 \end{pmatrix} \quad \text{and} \quad D = P^T A P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & -8 & 0 \\ 0 & 0 & 0 & -8 \end{pmatrix}.$$

□

Elementary row and column operations method

We shall use the elementary row operations and elementary column operations to reduce a symmetric matrix to a diagonal matrix. Let A be a symmetric matrix. By Corollary 9.4.17, there exists an invertible matrix P such that $P^T A P = D$ a diagonal matrix. Since P is invertible, by Theorem 2.2.5 $P = E_1 E_2 \cdots E_r$ is a product of elementary matrices. Thus,

$$D = (E_1 E_2 \cdots E_r)^T A (E_1 E_2 \cdots E_r) = E_r^T \Big(\cdots \big(E_2^T (E_1^T A E_1) E_2 \big) \cdots \Big) E_r.$$

Note that E_1^T is also an elementary matrix and $E_1^T A$ is obtained from A by applying an elementary row operation to A. Hence $(E_1^T A)E_1$ is obtained by applying the same column operation to $E_1^T A$. Thus the diagonal form will be obtained after successive use of elementary operations and the corresponding column operations.

In practice, we form the augmented matrix $\big(A|I\big)$, where the function of I is to record the product of elementary matrices $E_1^T, E_2^T, \ldots, E_r^T$. After applying an elementary row operation (or a sequence of elementary row operations) to $\big(A|I\big)$ we also apply the same elementary column operation (or the same sequence of column operations) to A. This process is to be continued until A becomes a diagonal matrix. At this time I becomes the matrix $E_1^T E_2^T \cdots E_r^T$, i.e., P^T. Note that we need $1 + 1 \neq 0$ in $\mathbb{F}$. Also note that exchanging two rows is always of no use, since we have to exchange the corresponding columns.

Example 9.4.20 Let $A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}$ over $\mathbb{R}$. Then

$$
\begin{aligned}
(A|I) &= \left(\begin{array}{ccc|ccc} 0 & 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow{1\mathcal{R}_2+\mathcal{R}_1} \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \\
&\xrightarrow{1\mathcal{C}_2+\mathcal{C}_1} \left(\begin{array}{ccc|ccc} 2 & 1 & 3 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow[-\frac{3}{2}\mathcal{R}_1+\mathcal{R}_3]{-\frac{1}{2}\mathcal{R}_1+\mathcal{R}_2} \left(\begin{array}{ccc|ccc} 2 & 1 & 3 & 1 & 1 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & -\frac{9}{2} & -\frac{3}{2} & -\frac{3}{2} & 1 \end{array}\right) \\
&\xrightarrow[-\frac{3}{2}\mathcal{C}_1+\mathcal{C}_3]{-\frac{1}{2}\mathcal{C}_1+\mathcal{C}_2} \left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 1 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & -\frac{9}{2} & -\frac{3}{2} & -\frac{3}{2} & 1 \end{array}\right) \xrightarrow{(-1)\mathcal{R}_2+\mathcal{R}_3} \left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 1 & 0 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & -4 & -1 & -2 & 1 \end{array}\right) \\
&\xrightarrow{(-1)\mathcal{C}_2+\mathcal{C}_3} \left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 1 & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & -4 & -1 & -2 & 1 \end{array}\right).
\end{aligned}
$$

Thus $P^T = \begin{pmatrix} 1 & 1 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -1 & -2 & 1 \end{pmatrix}$ and $P^T AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & -4 \end{pmatrix}$. □

For comparison, we shall use elementary row and column operation method to reduce the matrix in Example 9.4.19 to diagonal form.

Example 9.4.21 Let A be the matrix in Example 9.4.19.

$$
\begin{aligned}
&\left(\begin{array}{cccc|cccc} 0 & 1 & -1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 2 & -1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow{1\mathcal{R}_4+\mathcal{R}_1} \left(\begin{array}{cccc|cccc} 2 & 0 & 0 & 2 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 2 & -1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \\
&\xrightarrow{1\mathcal{C}_4+\mathcal{C}_1} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 2 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 2 & -1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow{-\frac{1}{2}\mathcal{R}_1+\mathcal{R}_4} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 2 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & -1 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{array}\right) \\
&\xrightarrow{-\frac{1}{2}\mathcal{C}_1+\mathcal{C}_4} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & -1 & -\frac{1}{2} & 0 & 0 & \frac{1}{2} \end{array}\right) \xrightarrow{1\mathcal{R}_2+\mathcal{R}_4} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -2 & -\frac{1}{2} & 1 & 0 & \frac{1}{2} \end{array}\right) \\
&\xrightarrow{1\mathcal{C}_2+\mathcal{C}_4} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -2 & -\frac{1}{2} & 1 & 0 & \frac{1}{2} \end{array}\right) \xrightarrow{1\mathcal{R}_3+\mathcal{R}_4} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & -\frac{1}{2} & 1 & 1 & \frac{1}{2} \end{array}\right) \\
&\xrightarrow{1\mathcal{C}_3+\mathcal{C}_4} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & -\frac{1}{2} & 1 & 1 & \frac{1}{2} \end{array}\right) \xrightarrow[2\mathcal{C}_4]{2\mathcal{R}_4} \left(\begin{array}{cccc|cccc} 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -4 & -1 & 2 & 2 & 1 \end{array}\right).
\end{aligned}
$$

In this case, $P^T = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 2 & 2 & 1 \end{pmatrix}$, i.e., $P = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 1 \end{pmatrix}$, and

$$P^T AP = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -4 \end{pmatrix}.$$

Note that, actually the last step is not necessary. It only makes the involved numbers are integers. □

Completing square method

Consider the quadratic form

$$X^T AX = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i a_{ij} x_j = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\left(\sum_{1\le i<j\le n} a_{ij}x_i x_j\right).$$

Of course we assume $2 \neq 0$ in $\mathbb{F}$.

Case 1. Suppose $a_{kk} \neq 0$ for some k. Put $x'_k = \sum\limits_{j=1}^{n} a_{kj}x_j$. Then

$$\begin{aligned} X^T AX - a_{kk}^{-1}x_k'^2 &= \sum_{i=1}^{n} a_{ii}x_i^2 + 2\left(\sum_{1\le i<j\le n} a_{ij}x_i x_j\right) \\ &\quad - a_{kk}^{-1}\left[\sum_{j=1}^{n} a_{kj}^2 x_j^2 + 2\left(\sum_{1\le i<j\le n} a_{ki}a_{kj}x_i x_j\right)\right]. \\ &= \sum_{i=1}^{n}\left(a_{ii} - a_{kk}^{-1}a_{ki}^2\right)x_i^2 + 2\left[\sum_{1\le i<j\le n}\left(a_{ij} - a_{ki}a_{kj}a_{kk}^{-1}\right)x_i x_j\right] \\ &= \sum_{\substack{i=1 \\ i\neq k}}^{n}\left(a_{ii} - a_{kk}^{-1}a_{ki}^2\right)x_i^2 + 2\left[\sum_{\substack{1\le i<j\le n \\ i\neq k,\, j\neq k}}\left(a_{ij} - a_{ki}a_{kj}a_{kk}^{-1}\right)x_i x_j\right]. \end{aligned}$$

This is a quadratic form which does not involve x_k, thus the inductive steps apply.

Case 2. Suppose $a_{kk} = 0\ \forall k = 1, 2, \ldots, n$. Then $X^T AX = 2\left(\sum\limits_{1\le i<j\le n} a_{ij}x_i x_j\right)$.

Suppose $a_{rs} \neq 0$ for some $r < s$. Put $x'_r = x_r + x_s$ and $x'_s = x_r - x_s$. That is, $x_r = 2^{-1}(x'_r + x'_s)$, $x_s = 2^{-1}(x'_r - x'_s)$ and $x_r x_s = 2^{-2}(x_r'^2 - x_s'^2)$. Thus

$$X^T AX = 2\left(\sum_{1\le i<j\le n} a_{ij}x_i x_j\right) = 2^{-1}a_{rs}(x_r'^2 - x_s'^2) + \cdots.$$

Then, we can apply Case 1.

Example 9.4.22 Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & -1 \\ 3 & -1 & 1 \end{pmatrix}$ be a real matrix. Then $X^TAX = x_1^2 + x_3^2 + 4x_1x_2 + 6x_1x_3 - 2x_2x_3$. Since $(A)_{1,1} = 1 \neq 0$, we let $x_1' = x_1 + 2x_2 + 3x_3$. Then

$$X^TAX - x_1'^2 = -4x_2^2 - 14x_2x_3 - 8x_3^2 = -4(x_2^2 + \tfrac{7}{2}x_2x_3 + \tfrac{49}{16}x_3^2) + \tfrac{17}{4}x_3^2.$$

If we put $x_2' = x_2 + \frac{7}{4}x_3$ and $x_3' = x_3$, then

$$X^TAX = x_1'^2 - 4x_2'^2 + \tfrac{17}{4}x_3'^2.$$

So we have

$$X' = \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & \frac{7}{4} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

If we write $X^TAX = \big(X^T(P^{-1})^T(P^TAP)P^{-1}X)\big) = X'^TDX'$, where $D = \mathrm{diag}\{1, -4, \frac{17}{4}\}$. Then $X' = P^{-1}X$ and the transition matrix

$$P = \begin{pmatrix} 1 & -2 & \frac{1}{2} \\ 0 & 1 & -\frac{7}{4} \\ 0 & 0 & 1 \end{pmatrix}. \qquad \square$$

Exercise 9.4

9.4-1. Consider elements of $\mathbb{R}^2$ as column vectors. Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by $f(X, Y) = \det\begin{pmatrix} X & Y \end{pmatrix}$. Here $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ and $\begin{pmatrix} X & Y \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$. Is f bilinear?

9.4-2. Define $f : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ by $f\big((x_1, x_2, x_3),\ (y_1, y_2, y_3)\big) = x_1y_1 - 2x_2y_2 + 2x_2y_1 - x_3y_3$. Show that f is bilinear. Also find the matrix representing f with respect to the basis $\mathscr{A} = \{(1, 0, 1),\ (1, 0, -1),\ (0, 1, 0)\}$.

9.4-3. Let $V = M_{2,2}(\mathbb{F})$. Define $f : V \times V \to V$ by $f(A, B) = \mathrm{Tr}(A)\mathrm{Tr}(B)$. Show that f is bilinear. Also find the matrix representing f with respect to the basis

$$\mathscr{A} = \left\{ E^{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ E^{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ E^{2,1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ E^{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

9.4-4. Show that a skew-symmetric matrix over $\mathbb{F}$ of odd order must be singular.

9.4-5. Show that if A is skew-symmetric and congruent to a diagonal matrix, then $A = O$. Here $2 \neq 0$.

9.4-6. Reduce the following matrices to diagonal form which are congruent to them.

(a) $\begin{pmatrix} 1 & 3 & 0 \\ 3 & -2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ 2 & -2 & 1 \end{pmatrix}$; (c) $\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$.

9.5 Real Quadratic Forms

In this section and the following section we only consider finite dimensional vector space. In this section we only consider vector space over $\mathbb{R}$.

From the previous section we knew that given a quadratic form q we can choose a basis such that the matrix representing q is diagonal. On the diagonal of this diagonal matrix, we shall show that the numbers of positive and negative numbers are independent of the bases chosen.

Theorem 9.5.1 *Let q be a quadratic form over $\mathbb{R}$. Let P and N be the number of positive terms and negative terms in a diagonalized representation of q, respectively. Then these two numbers are independent of the representations chosen.*

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of a vector space V which yields a diagonalized representation of q with P positive terms and N negative terms in the main diagonal.

Without loss of generality, we may assume that the first P elements of the main diagonal are positive. Suppose $\{\beta_1, \ldots, \beta_n\}$ is another basis yielding a diagonalized representation of q with the first P' elements of the main diagonal positive.

Let $U = \text{span}\{\alpha_1, \ldots, \alpha_P\}$ and $W = \text{span}\{\beta_{P'+1}, \ldots, \beta_n\}$. For $\alpha \in U$, $\alpha = \sum_{i=1}^{P} a_i\alpha_i$ for some $a_i \in \mathbb{R}$. Then

$$q(\alpha) = \sum_{i=1}^{P}\sum_{j=1}^{P} a_i a_j f(\alpha_i, \alpha_j) = \sum_{i=1}^{P} a_i^2 f(\alpha_i, \alpha_i) \geq 0,$$

here f is the symmetric bilinear form determining q. Thus $q(\alpha) = 0 \Leftrightarrow a_i = 0\ \forall i = 1, \ldots, P$. That is, $q(\alpha) = 0 \Leftrightarrow \alpha = \mathbf{0}$. Also, if $\beta \in W$, then by the definition, $q(\beta) \leq 0$. Thus $U \cap W = \{\mathbf{0}\}$. Since $\dim U = P$, $\dim W = n - P'$ and $\dim(U + W) \leq n$, we have $P + n - P' = \dim U + \dim W = \dim(U + W) \leq n$. Therefore, $P \leq P'$.

Similarly, we can show $P' \leq P$. Thus $P = P'$ and $N = r - P = r - P' = N'$, here r is the rank of the representation matrix. □

Remark 9.5.2 For a symmetric matrix $A \in M_n(\mathbb{R})$, define $q(X) = X^T AX$ for $X \in \mathbb{R}^n$. Then q is a quadratic form with representing matrix A with respect to the standard basis of $\mathbb{R}^n$. By Theorem 9.5.1 if A is congruent to a diagonal matrix D, i.e., $Q^T AQ = D$ for some non-singular matrix Q, then the number of positive terms and negative terms in the diagonal of D are independent of the choice of Q.

Definition 9.5.3 The number $S = P - N$ is called the *signature* of the quadratic form q. By Theorem 9.5.1, S is well-defined. A quadratic form q is called *non-negative definite* if $S = r$, where r is the rank of the matrix representing q. If $S = n$, then q is said to be *positive definite*. Similarly, if $S = -r$, then q is called *non-positive definite*; and if $S = -n$, then q is said to be *negative definite*.

Remark 9.5.4 Since $r = P + N$, q is non-negative definite if and only if $P - N = S = P + N$ if and only if $N = 0$. Also q is positive definite if and only if $S = n$ if and only if $P - N = n$ if and only if $P = n$ and $N = 0$. Similarly, q is non-positive definite if and only if $P = 0$; and q is negative definite if and only if $N = n$ and $P = 0$.

Proposition 9.5.5 *Suppose A is real symmetric matrix which represents a positive definite quadratic form. Then* $\det A > 0$.

Proof: By Corollary 9.4.17 there exists an invertible matrix P such that $P^TAP = D$ is diagonal. Since q is positive definite, all the diagonal entries of D are positive. Thus, $\det D > 0$. But $\det D = \det(P^TAP) = (\det P)^2(\det A)$. Hence $\det A > 0$. □

Definition 9.5.6 A symmetric real matrix is called *positive definite*, *negative definite*, *non-negative definite* or *non-positive definite* if it represents a positive definite, negative definite, non-negative definite or non-positive definite quadratic form, respectively. The *signature* of a symmetric real matrix is the signature of quadratic form it defines.

Definition 9.5.7 Let V be a vector space over $\mathbb{R}$. Suppose q is a quadratic form on V and f is the symmetric bilinear form such that $q(\alpha) = f(\alpha, \alpha)\ \forall \alpha \in V$. The *Gram determinant* of the vectors $\alpha_1, \ldots, \alpha_k$ with respect to q is defined to be the determinant

$$G(\alpha_1, \ldots, \alpha_k) = \begin{vmatrix} f(\alpha_1, \alpha_1) & f(\alpha_1, \alpha_2) & \cdots & f(\alpha_1, \alpha_k) \\ \vdots & \vdots & \vdots & \vdots \\ f(\alpha_k, \alpha_1) & f(\alpha_k, \alpha_2) & \cdots & f(\alpha_k, \alpha_k) \end{vmatrix}.$$

Theorem 9.5.8 *Let V be a vector space over $\mathbb{R}$ with a positive definite quadratic form q. Then $\alpha_1, \ldots, \alpha_k$ are linearly independent if and only if $G(\alpha_1, \ldots, \alpha_k) > 0$.*

Proof: Let q be the quadratic form induced from a symmetric bilinear form f.

Suppose $\alpha_1, \ldots, \alpha_k$ are linearly independent. Let $W = \text{span}\{\alpha_1, \ldots, \alpha_k\}$. Then $\mathscr{B} = \{\alpha_1, \ldots, \alpha_k\}$ is a basis of W. Let $q' = q\big|_W$. Then q' is a positive definite quadratic form on W. With respect to the basis $\mathscr{B}$, q' is represented by the $k \times k$ matrix $A = (a_{ij})$, where $a_{ij} = f(\alpha_i, \alpha_j)$. Since q' is positive definite, by Proposition 9.5.5 $\det A > 0$. That is, $G(\alpha_1, \ldots, \alpha_k) > 0$.

Conversely, suppose $\alpha_1, \ldots, \alpha_k$ are linearly dependent. Then there exist real numbers $c_1, \ldots, c_k$ not all zero such that $\sum_{i=1}^{k} c_i\alpha_i = \mathbf{0}$. Hence $f\Big(\alpha_j, \sum_{i=1}^{k} c_i\alpha_i\Big) = 0\ \forall j = 1, 2, \ldots, k$. Hence the system of linear equations

$$\begin{cases} f(\alpha_1, \alpha_1)x_1 + & \cdots & + & f(\alpha_1, \alpha_k)x_k & = 0 \\ f(\alpha_2, \alpha_1)x_1 + & \cdots & + & f(\alpha_2, \alpha_k)x_k & = 0 \\ & \vdots & & & \\ f(\alpha_k, \alpha_1)x_1 + & \cdots & + & f(\alpha_k, \alpha_k)x_k & = 0 \end{cases}$$

has non-trivial solution $(c_1, c_2, \ldots, c_k)$. Thus the determinant of the coefficient matrix must be zero. That is, $G(\alpha_1, \ldots, \alpha_k) = 0$. □

Note that, from the above proof we can see that the Gram determinant with respect to a positive definite quadratic form must be non-negative.

Exercise 9.5

9.5-1. Find the signature of the following matrices.

(a) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; (b) $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$; (c) $\begin{pmatrix} 3 & 1 & 2 \\ 1 & 4 & 0 \\ 2 & 0 & -1 \end{pmatrix}$.

9.5-2. Suppose A is a real symmetric matrix. Suppose $A^2 = O$. Is $A = O$? Why?

9.5-3. Reduce the quadratic form $q(x_1, x_2, x_3) = 2x_1x_2 + 4x_1x_3 - x_2^2 + 6x_2x_3 + 4x_3^2$ to diagonal form. That is, find an invertible matrix P such that if $Y = P^{-1}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$, then $q(x_1, x_2, x_3)$ is a quadratic form with variables y_1, y_2 and y_3 but with no mixed terms y_iy_j for $i \neq j$.

9.5-4. Reduce the quadratic form $q(x, y, z, w) = x^2 - 2xy - y^2 + 4yw + w^2 - 6zw + z^2$ to diagonal form.

9.6 Hermitian Forms

After considering real quadratic forms, in this section we consider complex quadratic forms which are called Hermitian quadratic forms. They will have similar properties as real quadratic forms.

Definition 9.6.1 Let $\mathbb{F} \subseteq \mathbb{C}$ and let V be a vector space over $\mathbb{F}$. A mapping $f : V \times V \to \mathbb{C}$ is called a *Hermitian form* if $\forall \alpha, \beta, \beta_1, \beta_2 \in V$, $b \in \mathbb{F}$

(1) $\overline{f(\alpha, \beta)} = f(\beta, \alpha)$, where $\bar{z}$ is the complex conjugate of z, and

(2) $f(\alpha, b\beta_1 + \beta_2) = bf(\alpha, \beta_1) + f(\alpha, \beta_2)$.

That is, f is linear in the second variable and *conjugate linear* in the first variable. For a given Hermitian form f, the mapping $q : V \to \mathbb{C}$ defined by $q(\alpha) = f(\alpha, \alpha)$ is called a *Hermitian quadratic form*. Note that $q(\alpha) \in \mathbb{R}$.

Definition 9.6.2 Let $\mathscr{B} = \{\alpha_1, \ldots, \alpha_n\}$ be a basis of V. Define $h_{ij} = f(\alpha_i, \alpha_j)$ $\forall i, j = 1, \ldots, n$. Put $H = (h_{ij})$. Then H is the representing matrix of f with respect to $\mathscr{B}$. Since $h_{ji} = f(\alpha_j, \alpha_i) = \overline{f(\alpha_i, \alpha_j)} = \overline{h_{ij}}$, $H^T = \overline{H}$ where $\overline{H} = (\overline{h_{ij}})$. Such a matrix is called a *Hermitian matrix*.

For any square matrix A over $\mathbb{C}$, we denote $A^* = \overline{A}^T = \overline{A^T}$. Thus, H is Hermitian if and only if $H^* = H$. Note that if H is Hermitian, then $(H)_{i,i} \in \mathbb{R}$. Also if H is a real matrix, then H is Hermitian if any only if H is symmetric.

Proposition 9.6.3 *Let $H = (h_{ij})$ be the matrix representing a Hermitian form f with respect to a basis $\mathscr{A} = \{\alpha_1, \ldots, \alpha_n\}$. Suppose $\mathscr{B} = \{\beta_1, \ldots, \beta_n\}$ is another basis and suppose $P = (p_{ij})$ is the matrix of transition from $\mathscr{A}$ to $\mathscr{B}$. If $K = (k_{ij})$ is the matrix representing f with respect to the basis $\mathscr{B}$, then $K = P^*HP$.*

Proof: Since $\beta_j = \sum_{i=1}^{n} p_{ij}\alpha_i$ for each j, we have

$$k_{ij} = f(\beta_i, \beta_j) = f\Big(\sum_{r=1}^{n} p_{ri}\alpha_r, \sum_{s=1}^{n} p_{sj}\alpha_s\Big) = \sum_{r=1}^{n}\sum_{s=1}^{n} \overline{p_{ri}} f(\alpha_r, \alpha_s)p_{sj} = \sum_{r=1}^{n}\sum_{s=1}^{n} \overline{p_{ri}} h_{rs} p_{sj}. \qquad \square$$

Definition 9.6.4 Two matrices H and K are said to be *Hermitian congruent* if there exists an invertible matrix P such that $P^*HP = K$.

Note that it is easy to see that Hermitian congruence is an equivalence relation.

Theorem 9.6.5 *For a given Hermitian matrix H over $\mathbb{C}$, there is an invertible matrix P such that $P^*HP = D$ is a diagonal matrix.*

Proof: Choose a vector space V and a basis $\mathscr{A}$. Then with respect to this basis, H defines a Hermitian form f and hence a Hermitian quadratic form q. The relation between f and q is

$$f(\alpha,\beta)=\frac{1}{4}[q(\alpha+\beta)-q(\alpha-\beta)-iq(\alpha+i\beta)+iq(\alpha-i\beta)].$$

As in the proof of Theorem 9.4.16, choose $\beta_1 \in V$ such that $q(\beta_1)\neq 0$. If this is not possible, then $f=0$ and we are finished.

Define a linear form ϕ on V by the formula $\phi(\alpha)=f(\beta_1,\alpha)\ \forall\alpha\in V$. If β_1 is represented by $\begin{pmatrix}p_{11} & \cdots & p_{n1}\end{pmatrix}^T$ and α by $\begin{pmatrix}x_1 & \cdots & x_n\end{pmatrix}^T$ with respect to $\mathscr{A}$, then $\phi(\alpha)=\sum\limits_{j=1}^{n}\left(\sum\limits_{k=1}^{n}\overline{p_{k1}}h_{kj}\right)x_j$. Thus ϕ is represented by the matrix $\begin{pmatrix}\overline{p_{11}} & \cdots & \overline{p_{n1}}\end{pmatrix}H$.

The rest of the proof is very much the same as that of the proof of Theorem 9.4.16 and hence we shall omit it. □

Note that, if H is a real Hermitian matrix, then the above theorem is just Theorem 9.4.16. From the proof of Theorem 9.6.5, it is easy to see that the field to which entries of H belong is not necessary the whole complex field $\mathbb{C}$. It can be any subfield of $\mathbb{C}$ that containing i.

We can use the inductive method or row and column operations method to reduce a Hermitian matrix to a diagonal matrix. But when using the elementary row and column operations method, we have only to make one modification. That is, whenever we multiple one row by a complex numbers c we have to multiply the corresponding column by $\bar{c}$. Also, instead of getting P^T we get P^*.

Example 9.6.6 Let $H=\begin{pmatrix}1 & i & 0\\ -i & 1 & i\\ 0 & -i & 1\end{pmatrix}$. We shall apply the elementary row and column operations method to find an invertible matrix P such that P^*HP is diagonal.

$$(H|I)\xrightarrow{i\mathcal{R}_1+\mathcal{R}_2}\left(\begin{array}{ccc|ccc}1 & i & 0 & 1 & 0 & 0\\ 0 & 0 & i & i & 1 & 0\\ 0 & -i & 1 & 0 & 0 & 1\end{array}\right)\xrightarrow{-i\mathcal{C}_1+\mathcal{C}_2}\left(\begin{array}{ccc|ccc}1 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & i & i & 1 & 0\\ 0 & -i & 1 & 0 & 0 & 1\end{array}\right)$$

$$\xrightarrow{1\mathcal{R}_3+\mathcal{R}_2}\left(\begin{array}{ccc|ccc}1 & 0 & 0 & 1 & 0 & 0\\ 0 & -i & 1+i & i & 1 & 1\\ 0 & -i & 1 & 0 & 0 & 1\end{array}\right)\xrightarrow{1\mathcal{C}_3+\mathcal{C}_2}\left(\begin{array}{ccc|ccc}1 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 1+i & i & 1 & 1\\ 0 & 1-i & 1 & 0 & 0 & 1\end{array}\right)$$

$$\xrightarrow{(-1+i)\mathcal{R}_2+\mathcal{R}_3}\left(\begin{array}{ccc|ccc}1 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 1+i & i & 1 & 1\\ 0 & 0 & -1 & -1-i & -1+i & i\end{array}\right)$$

$$\xrightarrow{(-1-i)\mathcal{C}_2+\mathcal{C}_3}\left(\begin{array}{ccc|ccc}1 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & i & 1 & 1\\ 0 & 0 & -1 & -1-i & -1+i & i\end{array}\right).$$

Hence $P^*=\begin{pmatrix}1 & 0 & 0\\ i & 1 & 1\\ -1-i & -1+i & i\end{pmatrix}$, so $P=\begin{pmatrix}1 & -i & -1+i\\ 0 & 1 & -1-i\\ 0 & 1 & -i\end{pmatrix}$ and $P^*HP=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix}$. □

Remark 9.6.7 Since the diagonal matrix $P^*HP=D=\operatorname{diag}\{d_1,\ldots,d_n\}$ is Hermitian, the diagonal entries are real. However, these diagonal entries are not unique. We can transform D into another diagonal matrix D' by means of a diagonal matrix $Q=\operatorname{diag}\{a_1,\ldots,a_n\}$ with $a_i\neq 0\ \forall i$. Then

$$D'=Q^*DQ=\operatorname{diag}\{d_1|a_1|^2,\ldots d_r|a_r|^2,0,\ldots,0\}.$$

Here $r = \text{rank}(H)$. Note that even though we are dealing with complex numbers, the transformation multiplies the diagonal entries of D by positive real numbers.

Definition 9.6.8 A Hermitian form or a Hermitian matrix is said to be *positive definite* (respectively, *non-negative definite*, *negative definite* or *non-positive definite*) if the associated quadratic form is positive definite (respectively, non-negative definite, negative definite or non-positive definite). By Remark 9.6.7 and the fact that the associated quadratic form is a real quadratic form, we see that these definitions are well defined.

The definition of the *signature* of a Hermitian quadratic or Hermitian matrix is the same as that of the real quadratic form or symmetric real matrix.

Remark 9.6.9 For infinite dimensional vector space V, a quadratic form q is said to be *positive definite* (*negative definite* respectively) if the corresponding Hermitian form f satisfied the condition that $f(\alpha, \alpha) > 0$ ($f(\alpha, \alpha) < 0$ respectively) $\forall \alpha \in V \setminus \{\mathbf{0}\}$. q is said to be *non-negative definite* (*non-positive definite* respectively) if $q(\alpha) \geq 0$ ($q(\alpha) \leq 0$ respectively) $\forall \alpha \in V$. For finite dimensional vector spaces, these two definitions are easily seen to be equivalent. Thus suppose A is a real symmetric (Hermitian respectively) matrix. Then A is positive definite if and only if $X^T AX > 0$ ($X^* AX > 0$) for all non-zero $n \times 1$ matrix X. The definition of the other definite or definite matrix is similarly defined.

Exercise 9.6

9.6-1. Reduce the following matrices to diagonal form which are Hermitian congruent to them. Also find their signatures.

(a) $\begin{pmatrix} 1 & i & 1-i \\ -i & -1 & 0 \\ 1+i & 0 & 1 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & i & 1+i \\ -i & 1 & i \\ 1-i & -i & 1 \end{pmatrix}$

9.6-2. Show that if H is a positive definite Hermitian matrix, then there exists an invertible matrix P such that $H = P^* P$. Also show that if H is real then we can choose P to be real.

9.6-3. Show that if A is an invertible matrix, then $A^* A$ is positive definite Hermitian matrix.

9.6-4. Show that if A is a square matrix, then $A^* A$ is Hermitian non-negative definite.

9.6-5. Show that if H is a Hermitian non-negative definite matrix, then there exists a matrix R such that $H = R^* R$. Moreover, if H is real, then R can be chosen to be real.

9.6-6. Show that if A is a square matrix such that $A^* A = O$, then $A = O$.

9.6-7. Let $H_1, \ldots, H_k$ be Hermitian matrices. Show that if $H_1^2 + \cdots + H_k^2 = O$, then $H_1 = \cdots = H_k = O$.

9.6-8. Let A be an $n \times n$ Hermitian non-negative definite matrix. Show that if $\text{rank}\, A = 1$, then there exists an $1 \times n$ matrix X such that $A = X^* X$.

9.6-9. Suppose A is a real $m \times n$ matrix with $\text{rank}(A) = n$. Show that $A^T A$ is positive definite.

Chapter 10

Inner Product Spaces and Unitary Transformations

10.1 Inner Product

In secondary school we have learnt dot product in $\mathbb{R}^3$. This is one of the inner product in $\mathbb{R}^3$. We shall generalize this concept to some general vector spaces.

In this chapter, we shall denote $\mathbb{F}$ to be the field $\mathbb{C}$ or a subfield of $\mathbb{C}$.

Definition 10.1.1 Let V be a vector space over $\mathbb{F}$. An *inner product* or *scalar product* on V is a positive definite Hermitian form f on V. Since f will be fixed throughout our discussion, we write $\langle \alpha, \beta \rangle$ instead $f(\alpha, \beta)$. For $\alpha \in V$, we define the *norm* or *length* of α by $\|\alpha\| = \sqrt{\langle \alpha, \alpha \rangle}$. Since the inner product is positive definite, $\|\alpha\| \geq 0 \ \forall \alpha \in V$. Also $\|\alpha\| = 0$ if and only if $\alpha = \mathbf{0}$.

Examples 10.1.2

1. Let $V = \mathbb{R}^n$. For $\alpha = (x_1, \ldots, x_n)$, $\beta = (y_1, \ldots, y_n)$ in V, define $\langle \alpha, \beta \rangle = \sum_{i=1}^{n} x_i y_i$. Then it is easy to see that this defines an inner product on $\mathbb{R}^n$, sometimes called the dot product, $\|\alpha\| = \sqrt{\sum_{i=1}^{n} x_i^2}$.

2. Let $V = \mathbb{C}^n$. For $\alpha = (x_1, \ldots, x_n)$, $\beta = (y_1, \ldots, y_n)$ in V, define $\langle \alpha, \beta \rangle = \sum_{i=1}^{n} \bar{x}_i y_i$. Again, this defines an inner product on $\mathbb{C}^n$, $\|\alpha\| = \sqrt{\sum_{i=1}^{n} |x_i|^2}$.

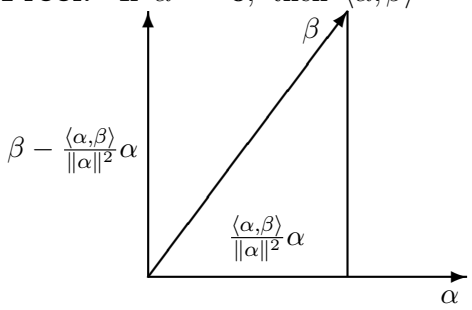
3. Let V be the vector space of all complex valued continuous functions defined on the closed interval $[a, b]$. Then it is easy to see that the formula $\langle f, g \rangle = \int_a^b \overline{f(x)} g(x) dx$ defines an inner product on V. Also $\|f\|^2 = \int_a^b |f(x)|^2 dx$.

4. Let $V = M_{m,n}(\mathbb{R})$. Let $A, B \in V$. Define $\langle A, B \rangle = \mathrm{Tr}(A^T B)$. It is easy to check that this defines an inner product on V. If we view $M_{m,n}(\mathbb{F})$ as $\mathbb{F}^{mn}$, then actually this inner product is the dot product. □

Definition 10.1.3 A vector space with an inner product is called an *inner product space*. A *Euclidean space* is a finite dimensional inner product space over $\mathbb{R}$. A finite dimensional inner product space over $\mathbb{C}$ is called a *unitary space*.

Theorem 10.1.4 (**Cauchy-Schwarz's inequality**) *Let V be an inner product space. Then for $\alpha, \beta \in V$, $|\langle \alpha, \beta \rangle| \leq \|\alpha\| \|\beta\|$.*

Proof: If $\alpha = \mathbf{0}$, then $\langle \alpha, \beta \rangle = 0$ and thus the inequality holds. If $\alpha \neq \mathbf{0}$, then $\|\alpha\| \neq 0$.



From

$$0 \leq \left\| \frac{\langle \alpha, \beta \rangle}{\|\alpha\|^2} \alpha - \beta \right\|^2 = \|\beta\|^2 - \frac{|\langle \alpha, \beta \rangle|^2}{\|\alpha\|^2},$$

we get $|\langle \alpha, \beta \rangle|^2 \leq \|\alpha\|^2 \|\beta\|^2$. That is, $|\langle \alpha, \beta \rangle| \leq \|\alpha\| \|\beta\|$. □

Remark 10.1.5 The equality holds if and only if β is a multiple of α or $\alpha = \mathbf{0}$. For, in the proof of Theorem 10.1.4, we see that the equality holds only if $\alpha = \mathbf{0}$ or $\frac{\langle \alpha, \beta \rangle}{\|\alpha\|^2} \alpha - \beta = \mathbf{0}$. Conversely, if $\alpha = \mathbf{0}$ or $\beta = c\alpha$ for some scalar c, then the equality holds.

Theorem 10.1.6 (**Triangle inequality**) *Let V be an inner product space. Then for $\alpha, \beta \in V$, $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$. The equality holds if and only if $\alpha = \mathbf{0}$ or $\beta = c\alpha$ for some non-negative real number c.*

Proof: Consider

$$\begin{aligned} \|\alpha + \beta\|^2 &= \langle \alpha + \beta, \alpha + \beta \rangle = \|\alpha\|^2 + 2\mathrm{Re}\langle \alpha, \beta \rangle + \|\beta\|^2 \leq \|\alpha\|^2 + 2|\langle \alpha, \beta \rangle| + \|\beta\|^2 \\ &\leq \|\alpha\|^2 + 2\|\alpha\|\|\beta\| + \|\beta\|^2 = (\|\alpha\| + \|\beta\|)^2. \end{aligned}$$

Hence $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$.

Note that the equality holds if and only if $\mathrm{Re}\langle \alpha, \beta \rangle = |\langle \alpha, \beta \rangle| = \|\alpha\| \|\beta\|$. By Remark 10.1.5, $|\langle \alpha, \beta \rangle| = \|\alpha\| \|\beta\|$ if and only if $\alpha = \mathbf{0}$ or $\beta = c\alpha$ for some $c \in \mathbb{C}$.

If $\beta = c\alpha$, then $\langle \alpha, \beta \rangle = \langle \alpha, c\alpha \rangle = c\|\alpha\|^2$. However, $\mathrm{Re}\langle \alpha, \beta \rangle = |\langle \alpha, \beta \rangle|$ if and only if $\langle \alpha, \beta \rangle$ is real and non-negative. Hence the equality holds if and only if $\alpha = \mathbf{0}$ or $\beta = c\alpha$ for some $c \geq 0$. □

Definition 10.1.7 Let V be an inner product space. Two vectors $\alpha, \beta \in V$ are said to be *orthogonal* if $\langle \alpha, \beta \rangle = 0$. A vector α is said to be a *unit vector* if $\|\alpha\| = 1$. A set $S \subseteq V$ is called an *orthogonal set* if all pairs of distinct vectors in S are orthogonal. An orthogonal set S is called an *orthonormal set* if all the vectors in S are unit vectors. A basis of V is said to be an *orthogonal basis* (*orthonormal basis*) if it is also an orthogonal set (orthonormal set).

Theorem 10.1.8 *Let V be an inner product space. Suppose S (finite set or infinite set) is an orthogonal set of non-zero vectors. Then S is a linearly independent set.*

Proof: Suppose $\xi_1, \ldots, \xi_k \in S$ are distinct and that $\sum_{i=1}^{k} c_i \xi_i = \mathbf{0}$. Then for each j, $1 \leq j \leq k$,

$$0 = \langle \xi_j, \mathbf{0} \rangle = \left\langle \xi_j, \sum_{i=1}^{k} c_i \xi_i \right\rangle = \sum_{i=1}^{k} c_i \langle \xi_j, \xi_i \rangle = c_j \|\xi_j\|^2.$$

Since $\|\xi_j\|^2 \neq 0$, each $c_j = 0$. Thus S is a linearly independent set. □

Corollary 10.1.9 *Let V be an inner product space. Suppose S is an orthonormal set. Then S is linearly independent.*

Theorem 10.1.10 (**Gram-Schmidt orthonormalization process**)
Suppose $\{\alpha_1, \ldots, \alpha_s\}$ *is a linearly independent set in an inner product space* V*. Then there exists an orthonormal set* $\{\xi_1, \ldots, \xi_s\}$ *such that for each* k

$$\xi_k = \sum_{i=1}^{k} a_{ik}\alpha_i \text{ for some scalars } a_{ik} \tag{10.1}$$

and $\text{span}\{\alpha_1, \ldots, \alpha_s\} = \text{span}\{\xi_1, \ldots, \xi_s\}$.

Proof: Since $\alpha_1 \neq \mathbf{0}$, $\|\alpha_1\| > 0$. Put $\xi_1 = \frac{\alpha_1}{\|\alpha_1\|}$. Then $\|\xi_1\| = 1$.

Suppose an orthonormal set $\{\xi_1, \ldots, \xi_r\}$ has been found so that each ξ_k, $k = 1, \ldots, r$ satisfies (10.1) and $\text{span}\{\alpha_1, \ldots, \alpha_r\} = \text{span}\{\xi_1, \ldots, \xi_r\}$. Assume $r < s$. Let

$$\alpha'_{r+1} = \alpha_{r+1} - \sum_{j=1}^{r} \langle \xi_j, \alpha_{r+1}\rangle \xi_j.$$

Then for each ξ_i, $1 \leq i \leq r$,

$$\langle \xi_i, \alpha'_{r+1}\rangle = \langle \xi_i, \alpha_{r+1}\rangle - \sum_{j=1}^{r} \langle \xi_j, \alpha_{r+1}\rangle \langle \xi_i, \xi_j\rangle = \langle \xi_i, \alpha_{r+1}\rangle - \sum_{j=1}^{r} \langle \xi_j, \alpha_{r+1}\rangle \delta_{ij} = 0.$$

Since each $\xi_k \in \text{span}\{\alpha_1, \ldots, \alpha_k\}$ for $1 \leq k \leq r$, $\alpha'_{r+1} \in \text{span}\{\alpha_1, \ldots, \alpha_r, \alpha_{r+1}\}$. Also $\alpha'_{r+1} \neq \mathbf{0}$, for otherwise α_{r+1} will be a linear combination of $\alpha_1, \ldots, \alpha_r$.

Put $\xi_{r+1} = \frac{\alpha'_{r+1}}{\|\alpha'_{r+1}\|}$. $\{\xi_1, \ldots, \xi_{r+1}\}$ is an orthonormal set with the desired properties. Also as $\alpha_{r+1} \in \text{span}\{\xi_1, \ldots, \xi_r, \alpha'_{r+1}\} = \text{span}\{\xi_1, \ldots, \xi_r, \xi_{r+1}\}$ we have

$$\text{span}\{\alpha_1, \ldots, \alpha_{r+1}\} = \text{span}\{\xi_1, \ldots, \xi_{r+1}\}$$

We continue this process until $r = s$. □

Applying the Gram-Schmidt process to a basis of a finite dimensional inner product space we have the following corollary:

Corollary 10.1.11 *Let* V *be a finite dimensional inner product space. Then* V *has an orthonormal basis.*

Corollary 10.1.12 *Let* V *be a finite dimensional inner product space. For any given unit vector* α*, there is an orthonormal basis with* α *as the first element.*

Proof: Extend the linearly independent set $\{\alpha\}$ to be a basis of V with α as the first element. Applying the Gram-Schmidt process to this basis we obtain a desired orthonormal basis. □

Examples 10.1.13

1. Let $V = \mathbb{R}^4$. It is clear that $\alpha_1 = (0, 1, 1, 0)$, $\alpha_2 = (0, 5, -3, -2)$ and $\alpha_3 = (-3, -3, 5, -7)$ are linearly independent. We would like to find an orthonormal basis of $\text{span}\{\alpha_1, \alpha_2, \alpha_3\}$.

   Put $\xi_1 = \frac{\alpha_1}{\|\alpha_1\|} = \frac{1}{\sqrt{2}}(0, 1, 1, 0)$.

   Let $\alpha'_2 = \alpha_2 - \langle \xi_1, \alpha_2\rangle \xi_1 = 2(0, 2, -2, -1)$. Thus $\xi_2 = \frac{\alpha'_2}{\|\alpha'_2\|} = \frac{1}{3}(0, 2, -2, -1)$.

   Let $\alpha'_3 = \alpha_3 - \langle \xi_1, \alpha_3\rangle \xi_1 - \langle \xi_2, \alpha_3\rangle \xi_2 = (-3, -2, 2, -8)$. Hence $\xi_3 = \frac{\alpha'_3}{\|\alpha'_3\|} = \frac{1}{9}(-3, -2, 2, -8)$. □

2. Let V be the vector space of all real continuous functions defined on closed interval $[0,1]$. V has an inner product defined by $\langle f,g\rangle = \int_0^1 f(x)g(x)dx$. We would like to find an orthonormal basis of span$\{1,x,x^2\}$.

   Let $f_1(x)=1, f_2(x)=x, f_3(x)=x^2$. Then $\|f_1\| = \displaystyle\int_0^1 dx = 1$. Put $g_1 = f_1$.

   Let $\widetilde{f_2}(x) = f_2(x) - \langle g_1, f_2\rangle g_1 = x - \displaystyle\int_0^1 x dx = x - \frac{1}{2}$, so

   $\|\widetilde{f_2}\| = \sqrt{\displaystyle\int_0^1 \left(x-\frac{1}{2}\right)^2 dx} = \frac{1}{2\sqrt{3}}$. Put $g_2(x) = \dfrac{\widetilde{f_2}}{\|\widetilde{f_2}\|} = 2\sqrt{3}(x-\frac{1}{2})$.

   Let $\widetilde{f_3}(x) = f_3(x) - \langle g_1, f_3\rangle g_1(x) - \langle g_2, f_3\rangle g_2(x)$

   $$= x^2 - \int_0^1 x^2 dx - \left[2\sqrt{3}\int_0^1 x^2\left(x-\frac{1}{2}\right)dx\right] 2\sqrt{3}\left(x-\frac{1}{2}\right) = x^2 - x + \frac{1}{6}.$$

   Then $\|\widetilde{f_3}\| = \sqrt{\displaystyle\int_0^1 \left(x^2 - x + \frac{1}{6}\right)^2 dx} = \frac{1}{6\sqrt{5}}$.

   Put $g_3(x) = \dfrac{\widetilde{f_3}}{\|\widetilde{f_3}\|} = 6\sqrt{5}\left(x^2 - x + \dfrac{1}{6}\right)$.

   The required orthonormal basis is $\left\{1, 2\sqrt{3}(x-\frac{1}{2}), 6\sqrt{5}(x^2-x+\frac{1}{6})\right\}$. □

Application–QR decomposition

Let $\alpha_1,\ldots,\alpha_s$ be s linearly independent vectors in an inner product space V. By the Gram-Schmidt process, we obtain

$$\alpha_1' = \alpha_1,\ \xi_1 = \frac{\alpha_1'}{\|\alpha_1'\|},\ \text{and for } k>1, \alpha_k' = \alpha_k - \langle\xi_1,\alpha_k\rangle\xi_1 - \cdots - \langle\xi_{k-1},\alpha_k\rangle\xi_{k-1},\ \xi_k = \frac{\alpha_k'}{\|\alpha_k'\|}.$$

Put $r_{kk} = \|\alpha_k'\|$ for $k=1,\ldots,s$ and $r_{ik} = \langle\xi_i,\alpha_k\rangle$ for $i<k$, $k=2,\ldots,s$. Thus, $\alpha_1 = \alpha_1' = \|\alpha_1'\|\xi_1 = r_{11}\xi_1$. Also from $\alpha_k' = \|\alpha_k'\|\xi_k = r_{kk}\xi_k = \alpha_k - r_{1k}\xi_1 - \cdots - r_{k-1\,k}\xi_{k-1}$ for $k=2,\ldots,s$, we have

$$\alpha_k = r_{1k}\xi_1 + \cdots + r_{k-1\,k}\xi_{k-1} + r_{kk}\xi_k \text{ for } k=1,2,\ldots,s. \tag{10.2}$$

Suppose $\dim V = m$ and with respect to some basis α_k and ξ_k have coordinate vectors $\begin{pmatrix} a_{1k}\\ \vdots \\ a_{mk}\end{pmatrix}$ and $\begin{pmatrix} q_{1k}\\ \vdots \\ q_{mk}\end{pmatrix}$, respectively. Then the relations (10.2) in the matrix form are

$$\begin{pmatrix} a_{1k}\\ \vdots \\ a_{jk}\\ \vdots \\ a_{mk}\end{pmatrix} = \begin{pmatrix} \sum_{i=1}^k r_{ik}q_{1i}\\ \vdots \\ \sum_{i=1}^k r_{ik}q_{ji}\\ \vdots \\ \sum_{i=1}^k r_{ik}q_{mi}\end{pmatrix} = \begin{pmatrix} \sum_{i=1}^k q_{1i}r_{ik}\\ \vdots \\ \sum_{i=1}^k q_{ji}r_{ik}\\ \vdots \\ \sum_{i=1}^k q_{mi}r_{ik}\end{pmatrix}.$$

Thus

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{ms} \end{pmatrix} = \begin{pmatrix} q_{11}r_{11} & q_{11}r_{12}+q_{12}r_{22} & \cdots & \sum_{i=1}^{s} q_{1i}r_{is} \\ q_{21}r_{11} & q_{21}r_{12}+q_{22}r_{22} & \cdots & \sum_{i=1}^{s} q_{2i}r_{is} \\ \vdots & \vdots & \vdots & \vdots \\ q_{m1}r_{11} & q_{m1}r_{12}+q_{m2}r_{22} & \cdots & \sum_{i=1}^{s} q_{mi}r_{is} \end{pmatrix}$$

$$= \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1s} \\ q_{21} & q_{22} & \cdots & q_{2s} \\ \vdots & \vdots & \vdots & \vdots \\ q_{m1} & q_{m2} & \cdots & q_{ms} \end{pmatrix} \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1s} \\ 0 & r_{22} & \cdots & r_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r_{ss} \end{pmatrix} = QR.$$

Here $Q = (q_{ij})$ is an $m \times s$ matrix with orthonormal columns and $R = (r_{ij})$ is an $s \times s$ invertible upper triangular matrix. Therefore, we have proved the so-called *QR decomposition theorem*:

Theorem 10.1.14 *Suppose A is an $m \times n$ matrix of rank n. Then $A = QR$, where Q is an $m \times n$ matrix with orthonormal columns and R is an $n \times n$ invertible upper triangle matrix.*

Example 10.1.15 Let $A = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 3 \\ 1 & 2 & 1 \\ 1 & 1 & 6 \end{pmatrix}$. Clearly, $\operatorname{rank}(A) = 3$. In this case, we let $V = \mathbb{R}^4$ under the usual dot product. And we choose the standard basis as an orthonormal basis for V.

Then $\alpha_1 = (1,1,1,1) = \alpha_1'$, $\xi_1 = \frac{1}{2}(1,1,1,1)$. Thus $\alpha_1 = 2\xi_1$.

Now $\alpha_2 = (1,2,2,1)$, $\alpha_2' = \alpha_2 - \langle \xi_1, \alpha_2 \rangle \xi_1 = \alpha_2 - 3\xi_1 = \frac{1}{2}(-1,1,1,-1)$. Hence $\xi_2 = \frac{1}{2}(-1,1,1,-1)$ and $\alpha_2 = 3\xi_1 + \xi_2$.

$\alpha_3 = (2,3,1,6)$, $\alpha_3' = \alpha_3 - \langle \xi_1, \alpha_3 \rangle \xi_1 - \langle \xi_2, \alpha_3 \rangle \xi_2 = \alpha_3 - 6\xi_1 + 2\xi_2 = (-2,1,-1,2)$. Hence $\xi_3 = \frac{1}{\sqrt{10}}(-2,1,-1,2)$ and $\alpha_3 = 6\xi_1 - 2\xi_2 + \sqrt{10}\xi_3$.

Thus $Q = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & -\frac{2}{\sqrt{10}} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{\sqrt{10}} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{\sqrt{10}} \\ \frac{1}{2} & -\frac{1}{2} & \frac{2}{\sqrt{10}} \end{pmatrix}$, $R = \begin{pmatrix} 2 & 3 & 6 \\ 0 & 1 & -2 \\ 0 & 0 & \sqrt{10} \end{pmatrix}$ and $A = QR$. □

Definition 10.1.16 Let $\{\xi_1, \xi_2, \ldots, \}$ be an orthonormal set in an inner product space V and let $\alpha \in V$. The scalars $a_i = \langle \xi_i, \alpha \rangle$, $i = 1, 2, \ldots$, are called the *Fourier coefficients of α with respect to this orthonormal set.*

Suppose ξ is a unit vector in $\mathbb{R}^3$ (or generally in $\mathbb{R}^n$). The absolute value of Fourier coefficient $\langle \xi, \alpha \rangle$ of α is the length of α projected onto the vector ξ. If we identify the point P with its position vector α, then $\alpha - \langle \xi, \alpha \rangle \xi$ is a vector orthogonal to ξ. The distance from P to the straight line passing through the origin with the direction ξ is the length (norm) of the vector $\alpha - \langle \xi, \alpha \rangle \xi$. This geometrical property can be generalized to project a point onto a plane passing through the origin (a subspace) in a general inner product space.

Theorem 10.1.17 *Let V be an inner product space. Suppose $\{\xi_1, \ldots, \xi_k\}$ is an orthonormal set in V. For $\alpha \in V$, we have $\min\limits_{\substack{x_i \in \mathbb{F} \\ 1 \le i \le k}} \left\| \alpha - \sum_{i=1}^{k} x_i \xi_i \right\| = \left\| \alpha - \sum_{i=1}^{k} a_i \xi_i \right\|$, where $a_i = \langle \xi_i, \alpha \rangle$ are the Fourier*

coefficients of α. *Moreover,* $\left\|\alpha - \sum_{i=1}^{k} x_i\xi_i\right\| = \left\|\alpha - \sum_{i=1}^{k} a_i\xi_i\right\|$ *if and only if* $x_i = a_i$ *for all* i. *Also* $\sum_{i=1}^{k} |a_i|^2 \leq \|\alpha\|^2$ *and* $\left\langle \xi_j, \alpha - \sum_{i=1}^{k} a_i\xi_i \right\rangle = 0$, $\forall j = 1, \ldots, k$. *Hence, we see that* $\alpha - \sum_{i=1}^{k} a_i\xi_i$ *is orthogonal to each vector in* $\text{span}\{\xi_1, \ldots, \xi_k\}$.

Proof: Consider

$$\left\|\alpha - \sum_{i=1}^{k} x_i\xi_i\right\|^2 = \left\langle \alpha - \sum_{i=1}^{k} x_i\xi_i, \alpha - \sum_{i=1}^{k} x_i\xi_i \right\rangle = \langle \alpha, \alpha\rangle - \sum_{i=1}^{k} \bar{x}_i a_i - \sum_{i=1}^{k} x_i \bar{a}_i + \sum_{i=1}^{k} \bar{x}_i x_i$$
$$= \|\alpha\|^2 + \sum_{i=1}^{k} (\bar{a}_i - \bar{x}_i)(a_i - x_i) - \sum_{i=1}^{k} |a_i|^2 = \|\alpha\|^2 + \sum_{i=1}^{k} |a_i - x_i|^2 - \sum_{i=1}^{k} |a_i|^2.$$

Thus $\left\|\alpha - \sum_{i=1}^{k} x_i\xi_i\right\|^2 \geq \|\alpha\|^2 - \sum_{i=1}^{k} |a_i|^2 = \left\|\alpha - \sum_{i=1}^{k} a_i\xi_i\right\|^2$. The equality holds if and only if $\sum_{i=1}^{k} |a_i - x_i|^2 = 0$. This is equivalent to $x_i = a_i$ $\forall i = 1, \ldots, k$. That is, the minimum of $\left\|\alpha - \sum_{i=1}^{k} x_i\xi_i\right\|$ is attained when $x_i = a_i$ $\forall i = 1, \ldots, k$. Since $\|\alpha\|^2 - \sum_{i=1}^{k} |a_i|^2 = \left\|\alpha - \sum_{i=1}^{k} a_i\xi_i\right\|^2 \geq 0$, we have $\sum_{i=1}^{k} |a_i|^2 \leq \|\alpha\|^2$. It is clear that $\left\langle \xi_j, \alpha - \sum_{i=1}^{k} a_i\xi_i \right\rangle = 0$ for all j. □

Application–least squares problem

Let V be an inner product space with W as its finite dimensional subspace. Given $\alpha \in V \setminus W$. We want to find $\beta \in W$ such that $\|\alpha - \beta\| = \min_{\xi \in W} \|\alpha - \xi\|$. One way of doing this is to find an orthonormal basis of W and proceed as above.

An alternative method is to pick any basis, say $\mathscr{A} = \{\eta_1, \ldots, \eta_k\}$, of W. Suppose $\beta = \sum_{j=1}^{k} x_j\eta_j \in W$ is the required vector, its existence is asserted in Theorem 10.1.17 yet to be determined. Then by Theorem 10.1.17 we have $\langle \eta_i, \alpha - \beta\rangle = 0$ $\forall i = 1, \ldots, k$. So $\left\langle \eta_i, \alpha - \sum_{j=1}^{k} x_j\eta_j \right\rangle = 0$ and then $\langle \eta_i, \alpha\rangle = \sum_{j=1}^{k} \langle \eta_i, \eta_j\rangle x_j$. This system has the matrix form $GX = N$, where $X = \begin{pmatrix} x_1 & \cdots & x_k \end{pmatrix}^T$, $N = \begin{pmatrix} \langle \eta_1, \alpha\rangle & \cdots & \langle \eta_k, \alpha\rangle \end{pmatrix}^T$ and $G = (\langle \eta_i, \eta_j\rangle)$ which is the representing matrix of the inner product with respect to $\mathscr{A}$. The matrix G is called the *Gram matrix* of $\mathscr{A}$. $\det(G)$ is the Gram determinant of the vectors $\eta_1, \ldots, \eta_k$ with respect to the inner product. By Theorem 9.5.8, G is invertible and hence we have a unique solution β. Such vector β is called the *best approximation to* α in the least squares sense.

Example 10.1.18 Let $W = \{(x, y, z, w) \in \mathbb{R}^4 \mid x - y - z + w = 0\}$ be a subspace of $\mathbb{R}^4$ under the usual inner product (i.e., the dot product). Find a vector in W that is closest to $\alpha = (-2, 1, 2, 1)$.
Solution: Clearly $\{\eta_1 = (1, 1, 0, 0),\ \eta_2 = (1, 0, 1, 0),\ \eta_3 = (-1, 0, 0, 1)\}$ is a basis of W. Then $G = \left(\langle \eta_i, \eta_j\rangle\right) = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$ and $N = \begin{pmatrix} -1 \\ 0 \\ 3 \end{pmatrix}$. Solve the equation $GX = N$ we get

$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$. Thus, the required vector is $0\eta_1 + 1\eta_2 + 2\eta_3 = (-1, 0, 1, 2)$. □

In most applications, our inner product space V is $\mathbb{R}^m$ and the corresponding inner product is the usual dot product. In this content, we rephrase the least squares problem as follows:

Given $A \in M_{m,k}(\mathbb{R})$ and $B \in M_{m,1}(\mathbb{R})$. We want to find a matrix $X_0 \in M_{k,1}(\mathbb{R})$ such that $\|AX_0 - B\|$ is minimum among all $k \times 1$ matrices X. Let $W = C(A)$ be the column space of A, i.e., $W = \{AX \mid X \in \mathbb{R}^k\}$. By Theorem 10.1.17, we know that there is an X_0 such that $AX_0 - B$ is orthogonal to each vector in W. Thus using the dot product as our inner product, we must have

$$(AX)^T(AX_0 - B) = 0 \text{ for all } X \in \mathbb{R}^k.$$

That is, $X^T A^T(AX_0 - B) = 0$ for all X. This could happen only if $A^T(AX_0 - B) = \mathbf{0}$. That means X_0 is a solution of the so-called *normal equation*

$$A^T AX = A^T B.$$

Moreover if $\text{rank}(A) = k$, then $A^T A$ is non-singular (Exercise 9.6-9) and the normal equation has unique solution in $X_0 = (A^T A)^{-1}(A^T B)$.

Geometrically the solution of the normal equation enables us to find the vector in W that has the least distance from B. Thus, AX_0 is just the 'projection' of B onto the subspace W. As B varies, we get the so-called *projection matrix*

$$P = A(A^T A)^{-1} A^T.$$

It is easy to see that $P^2 = P$ and P is symmetric.

Example 10.1.19 Let $W = \text{span}\{(1, 1, 1, 1)^T, (-1, 0, 1, 2)^T, (0, 1, 2, 3)^T\}$ and let $B = (0, 2, 1, 2)^T$. Then

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Then the normal equation $A^T AX = A^T B$ takes the form

$$\begin{pmatrix} 4 & 2 & 6 \\ 2 & 6 & 8 \\ 6 & 8 & 14 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \\ 10 \end{pmatrix}.$$

One can get a solution $x_1 = 1$, $x_2 = \frac{1}{2}$ and $x_3 = 0$. Then the vector in W that yields the least distance is given by

$$AX_0 = \begin{pmatrix} \frac{1}{2} \\ 1 \\ \frac{3}{2} \\ 2 \end{pmatrix}.$$

Thus the least distance is $\sqrt{(\frac{1}{2} - 0)^2 + (1 - 2)^2 + (\frac{3}{2} - 1)^2 + (2 - 2)^2} = \frac{\sqrt{6}}{2}$. □

Following example is a well-known problem in statistics called regression.

Example 10.1.20 We would like to find a polynomial of degree n such that it fits given m points $(x_1, y_1), \ldots, (x_m, y_m)$ in the plane in the least squares sense, in general, $m > n+1$. We put $y = \sum_{j=0}^{n} c_j x^j$, where c_j's are to be determined such that $\sum_{i=1}^{m} (\hat{y}_i - y_i)^2$ is the least. Put $\hat{y}_i = \sum_{j=0}^{n} c_j x_i^j$, $i = 1, \ldots, m$. Then we have to solve the system

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_m & x_m^2 & \cdots & x_m^n \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} \hat{y}_1 \\ \hat{y}_2 \\ \vdots \\ \hat{y}_m \end{pmatrix}$$

in the least squares sense. Thus we need to find an X_0 such that

$$\|AX_0 - B\| = \min_{X \in \mathbb{R}^{n+1}} \|AX - B\|$$

with

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_m & x_m^2 & \cdots & x_m^n \end{pmatrix}, \quad X = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}.$$

When $n = 1$, the problem is called the *linear regression problem*. In this case

$$A = \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \\ \vdots & \vdots \\ 1 & x_m \end{pmatrix}, \quad X = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}.$$

Now $W = \operatorname{span}(1, 1, \ldots, 1)^T$, $(x_1, x_2, \ldots, x_m)^T$. In practice as, $x_1, \ldots, x_m$ are not all equal, so $\dim W = 2$. Then

$$A^T A = \begin{pmatrix} m & \sum_{i=1}^{m} x_i \\ \sum_{i=1}^{m} x_i & \sum_{i=1}^{m} x_i^2 \end{pmatrix} = \begin{pmatrix} m & m\bar{x} \\ m\bar{x} & \sum_{i=1}^{m} x_i^2 \end{pmatrix}, \quad A^T B = \begin{pmatrix} \sum_{i=1}^{m} y_i \\ \sum_{i=1}^{m} x_i y_i \end{pmatrix} = \begin{pmatrix} m\bar{y} \\ \sum_{i=1}^{m} x_i y_i \end{pmatrix},$$

where $\bar{x} = \frac{1}{m} \sum_{i=1}^{m} x_i$ and $\bar{y} = \frac{1}{m} \sum_{i=1}^{m} y_i$.

Then $\det(A^T A) = m \sum_{i=1}^{m} x_i^2 - m^2 \bar{x}^2 = m \sum_{i=1}^{m} (x_i - \bar{x})^2$. Hence

$$X_0 = (A^T A)^{-1} (A^T B) = \frac{1}{m \sum_{i=1}^{m} (x_i - \bar{x})^2} \begin{pmatrix} m\bar{y} \sum_{i=1}^{m} x_i^2 - m\bar{x} \sum_{i=1}^{m} x_i y_i \\ m \sum_{i=1}^{m} x_i y_i - m^2 \bar{x}\bar{y} \end{pmatrix}.$$

So

$$c_1 = \frac{\sum_{i=1}^{m} x_i y_i - m\bar{x}\bar{y}}{\sum_{i=1}^{m} (x_i - \bar{x})^2} = \frac{\sum_{i=1}^{m} (x_i - \bar{x})(y_i - \bar{y})}{\sum_{i=1}^{m} (x_i - \bar{x})^2} \quad \text{and} \quad c_0 = \frac{\bar{y} \sum_{i=1}^{m} x_i^2 - \bar{x} \sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} (x_i - \bar{x})^2}.$$

□

Exercise 10.1

10.1-1. Let V be an inner product space over $\mathbb{F}$. Prove the following *polarization identities*:

(a) If $\mathbb{F} \subseteq \mathbb{R}$, then
$$\langle \alpha, \beta \rangle = \frac{1}{4}\|\alpha+\beta\|^2 - \frac{1}{4}\|\alpha-\beta\|^2, \ \forall \alpha, \beta \in V.$$

(b) If $i \in \mathbb{F} \subseteq \mathbb{C}$, then
$$\langle \alpha, \beta \rangle = \frac{1}{4}\|\alpha+\beta\|^2 - \frac{1}{4}\|\alpha-\beta\|^2 - \frac{i}{4}\|\alpha+i\beta\|^2 + \frac{i}{4}\|\alpha-i\beta\|^2 = \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\alpha+i^n\beta\|^2, \ \forall \alpha, \beta \in V.$$

10.1-2. Let V be an inner product space over $\mathbb{F}$, where $\mathbb{F} \subseteq \mathbb{R}$ or $i \in \mathbb{F} \subseteq \mathbb{C}$. Prove the *parallelogram law*:
$$\|\alpha+\beta\|^2 + \|\alpha-\beta\|^2 = 2\|\alpha\|^2 + 2\|\beta\|^2, \ \forall \alpha, \beta \in V.$$

10.1-3. Let V be a real inner product space. Show that if $\alpha, \beta \in V$ are orthogonal if and only if $\|\alpha+\beta\|^2 = \|\alpha\|^2 + \|\beta\|^2$ (Pythagoream theorem).

10.1-4. Given the basis $\{(1,0,1,0),\ (1,1,0,0),\ (0,1,1,1),\ (0,1,1,0)\}$ of $\mathbb{R}^4$. Apply the Gram-Schmidt process to obtain an orthonormal basis.

10.1-5. Find an orthonormal basis of $\mathbb{R}^3$ starting with $\frac{1}{\sqrt{3}}(1,2,-1)$.

10.1-6. Let $V = C^0[0,1]$ be the inner product space of real continuous defined on $[0,1]$. The inner product is defined by
$$\langle f, g \rangle = \int_0^1 f(t)g(t)dt.$$
Apply the Gram-Schmidt process to the standard basis $\{1, x, x^2, x^3\}$ of the subspace $P_4(\mathbb{R})$.

10.1-7. Let S be a finite set of mutually non-zero orthogonal vectors in an inner product space V. Show that if the only vector orthogonal to each vector in S is the zero vector, then S is a basis of V.

10.1-8. Find an orthonormal basis for the plane $x + y + 2z = 0$ in $\mathbb{R}^3$.

10.1-9. Let $W = \text{span}\{(1,1,0,1),\ (3,1,1,-1)\}$. Find a vector in W that is closest to $(0,1,-1,1)$.

10.1-10. Find the minimum distance of $(1,1,1,1)$ to the subspace
$\{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4 \mid x_1+x_2+x_3+x_4 = 0\}$.

10.1-11. Find a linear equation that fits the data $(0,1),\ (3,4),\ (6,5)$ in the least squares sense.

10.1-12. Find a quadratic equation that fits the data $(1,4),\ (2,0),\ (-1,1),\ (0,2)$ in the least squares sense.

10.1-13. Find the least squares solution to each of the following system:

(a) $\begin{pmatrix} 1 & 1 \\ 2 & -3 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \\ 1 \\ 2 \end{pmatrix}$;

(c) $\begin{pmatrix} 1 & 1 & 3 \\ -1 & 3 & 1 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ 8 \end{pmatrix}$.

10.1-14. Find the QR decomposition of $\begin{pmatrix} 1 & \sqrt{2} & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$.

10.2 The Adjoint Transformation

An inner product on a vector space V is a positive definite Hermitian form. So if we fix the first variable of the inner product, then it becomes a linear form. We shall show that this is a one-one corresponding between V and $\widehat{V}$ if V is finite dimensional.

Theorem 10.2.1 *Let V be a finite dimensional inner product space. Then for any linear form $\phi \in \widehat{V}$, there exists a unique $\gamma \in V$ such that $\phi(\alpha) = \langle \gamma, \alpha \rangle$.*

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be an orthonormal basis of V and let $\{\phi_1, \ldots, \phi_n\}$ be the dual basis. Then $\phi = \sum_{i=1}^{n} b_i \phi_i$ with $b_i = \phi(\alpha_i)$. Define $\gamma = \sum_{i=1}^{n} \bar{b}_i \alpha_i$. Then for each α_j,

$$\langle \gamma, \alpha_j \rangle = \left\langle \sum_{i=1}^{n} \bar{b}_i \alpha_i, \alpha_j \right\rangle = \sum_{i=1}^{n} b_i \langle \alpha_i, \alpha_j \rangle = b_j = \phi(\alpha_j).$$

By Theorem 7.1.26, two linear transformations ϕ and $\langle \gamma, \cdot \rangle$ are the same, i.e., $\phi(\alpha) = \langle \gamma, \alpha \rangle$.

If γ' is another vector in V such that $\phi(\alpha) = \langle \gamma', \alpha \rangle$, then $\langle \gamma, \alpha \rangle = \langle \gamma', \alpha \rangle \ \forall \alpha \in V$. That is, $\langle \gamma - \gamma', \alpha \rangle = 0 \ \forall \alpha \in V$. In particular, for $\alpha = \gamma - \gamma'$, we have $\langle \gamma - \gamma', \gamma - \gamma' \rangle = \|\gamma - \gamma'\|^2 = 0$. Hence $\gamma = \gamma'$. □

Of course, if V is inner product space with another inner product, then the vector γ must be changed.

Theorem 10.2.2 *Let V be a finite dimensional inner product space. Let $\Lambda : \widehat{V} \to V$ be the map which associates each $\phi \in \widehat{V}$ a unique $\gamma \in V$ such that $\phi(\alpha) = \langle \Lambda(\phi), \alpha \rangle = \langle \gamma, \alpha \rangle$. Then Λ is bijective and conjugate linear, that is, $\Lambda(a\phi + \psi) = \bar{a}\Lambda(\phi) + \Lambda(\psi)$. Also Λ^{-1} is conjugate linear.*

Proof: Suppose $\beta \in V$. Define $\phi : V \to \mathbb{F}$ by $\phi(\alpha) = \langle \beta, \alpha \rangle$. Clearly, $\phi \in \widehat{V}$ and by Theorem 10.2.1, $\Lambda(\phi) = \beta$. Thus Λ is surjective. Suppose $\phi, \psi \in \widehat{V}$ are such that $\Lambda(\phi) = \Lambda(\psi)$. Then by the definition of Λ, $\phi(\alpha) = \langle \Lambda(\phi), \alpha \rangle = \langle \Lambda(\psi), \alpha \rangle = \psi(\alpha) \ \forall \alpha \in V$. Thus $\phi = \psi$ and hence Λ is injective.

Now let $\phi, \psi \in \widehat{V}$, $a \in \mathbb{F}$ and $\alpha \in V$. Consider

$$\langle \Lambda(a\phi + \psi), \alpha \rangle = (a\phi + \psi)(\alpha) = a\phi(\alpha) + \psi(\alpha) = a\langle \Lambda(\phi), \alpha \rangle + \langle \Lambda(\psi), \alpha \rangle = \langle \bar{a}\Lambda(\phi) + \Lambda(\psi), \alpha \rangle.$$

Hence $\langle \Lambda(a\phi + \psi) - \bar{a}\Lambda(\phi) - \Lambda(\psi), \alpha \rangle = 0 \ \forall \alpha \in V$. Therefore, $\Lambda(a\phi + \psi) = \bar{a}\Lambda(\phi) + \Lambda(\psi)$. Similarly, Λ^{-1} is conjugate linear. □

Corollary 10.2.3 *If $\mathbb{F}$ is a subfield of $\mathbb{R}$, then Λ is linear and hence an isomorphism. Thus for Euclidean space V, any linear form on V is an inner product with a fixed vector in V.*

Theorem 10.2.4 *Let $\sigma \in L(V, V)$, where V is a finite dimensional inner product space. Then there exists a unique $\sigma^* \in L(V, V)$ such that $\langle \sigma^*(\alpha), \beta \rangle = \langle \alpha, \sigma(\beta) \rangle \ \forall \alpha, \beta \in V$.*

Proof: For $\alpha \in V$, define $\phi \in \widehat{V}$ by $\phi(\beta) = \langle \alpha, \sigma(\beta)\rangle$ for $\beta \in V$. Put $\sigma^*(\alpha) = \Lambda(\phi)$, where Λ is defined in Theorem 10.2.2. Then we have $\langle \sigma^*(\alpha), \beta\rangle = \langle \Lambda(\phi), \beta\rangle = \phi(\beta) = \langle \alpha, \sigma(\beta)\rangle$. Now for $\alpha_1, \alpha_2, \beta \in V$, $a \in \mathbb{F}$,

$$\begin{aligned}\langle \sigma^*(a\alpha_1 + \alpha_2), \beta\rangle &= \langle a\alpha_1 + \alpha_2, \sigma(\beta)\rangle = \bar{a}\langle \alpha_1, \sigma(\beta)\rangle + \langle \alpha_2, \sigma(\beta)\rangle \\ &= \bar{a}\langle \sigma^*(\alpha_1), \beta\rangle + \langle \sigma^*(\alpha_2), \beta\rangle = \langle a\sigma^*(\alpha_1) + \sigma^*(\alpha_2), \beta\rangle.\end{aligned}$$

Since β is arbitrary, we have $\sigma^*(a\alpha_1 + \alpha_2) = a\sigma^*(\alpha_1) + \sigma^*(\alpha_2)$. It is easy to see that σ^* with this property is unique. □

Note that if there exists a linear transformation $\sigma^* \in L(V, V)$ such that $\langle \sigma^*(\alpha), \beta\rangle = \langle \alpha, \sigma(\beta)\rangle$ $\forall \alpha, \beta \in V$ for a given $\sigma \in L(V, V)$, where V is a general inner product space, then σ^* is unique.

Definition 10.2.5 Let $\sigma \in L(V, V)$, where V is an inner product space. The unique linear transformation $\sigma^* : V \to V$ defined by $\langle \sigma^*(\alpha), \beta\rangle = \langle \alpha, \sigma(\beta)\rangle$ $\forall \alpha, \beta \in V$ is called the *adjoint of* σ.

By Theorem 10.2.4, for finite dimensional inner product space V and any linear transformation on V, the adjoint always exists.

Theorem 10.2.6 *Let $\sigma \in L(V, V)$, where V is an inner product space. Suppose σ^* exists. Then $\sigma^{**} = (\sigma^*)^*$ exists and equals σ.*

Proof: Let $\alpha, \beta \in V$. Then from the definition of adjoint transformation, we must have that

$$\langle \alpha, \sigma^*(\beta)\rangle = \overline{\langle \sigma^*(\beta), \alpha\rangle} = \overline{\langle \beta, \sigma(\alpha)\rangle} = \langle \sigma(\alpha), \beta\rangle.$$

Since α, β are arbitrary, we have σ^{**} exists and $\sigma^{**} = \sigma$. □

Suppose V is a finite dimensional inner product space. Let $\sigma : V \to V$ be a linear transformation. Recall that $\hat{\sigma} : \widehat{V} \to \widehat{V}$ is defined by $\hat{\sigma}(\phi) = \phi \circ \sigma$ for $\phi \in \widehat{V}$. Now for $\alpha, \beta \in V$, we have

$$\begin{aligned}\langle \Lambda \circ \hat{\sigma} \circ \Lambda^{-1}(\alpha), \beta\rangle &= \langle \Lambda(\hat{\sigma} \circ \Lambda^{-1}(\alpha)), \beta\rangle = (\hat{\sigma} \circ \Lambda^{-1}(\alpha))(\beta) \\ &= \Lambda^{-1}(\alpha)(\sigma(\beta)) = \langle \alpha, \sigma(\beta)\rangle = \langle \sigma^*(\alpha), \beta\rangle.\end{aligned}$$

Hence $\sigma^* = \Lambda \circ \hat{\sigma} \circ \Lambda^{-1}$. Let $A = (a_{ij})$ and $A' = (a'_{ij})$ be respectively matrices representing σ and σ^* with respect to some orthonormal basis $\{\xi_1, \ldots, \xi_n\}$. Then

$$\langle \sigma^*(\xi_j), \xi_k\rangle = \langle \xi_j, \sigma(\xi_k)\rangle = \left\langle \xi_j, \sum_{i=1}^{n} a_{ik}\xi_i \right\rangle = \sum_{i=1}^{n} a_{ik}\langle \xi_j, \xi_i\rangle = a_{jk}.$$

On the other hand

$$\langle \sigma^*(\xi_j), \xi_k\rangle = \left\langle \sum_{i=1}^{n} a'_{ij}\xi_i, \xi_k \right\rangle = \sum_{i=1}^{n} \overline{a'_{ij}}\langle \xi_i, \xi_k\rangle = \overline{a'_{kj}}.$$

Thus $A' = \bar{A}^T = A^*$.

Example 10.2.7 Let $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ be given by $\sigma(x, y) = (x+y, 2x-y)$. Then with the standard basis of $\mathbb{R}^2$, σ has the representing matrix $A = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}$. Thus σ^* is represented by A^T with respect to the standard basis.

Now $\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+2y \\ x-y \end{pmatrix}$. Hence $\sigma^*(x, y) = (x + 2y, x - y)$. □

Proposition 10.2.8 *Let V be a finite dimensional inner product space. Suppose W is a subset of V. Then $\Lambda(W^0)$ is a subspace of V. Moreover,*

$$\Lambda(W^0) = \{\beta \in V \mid \langle \beta, \alpha \rangle = 0 \ \forall \alpha \in W\}.$$

Proof: Let $\phi, \psi \in W^0 \subseteq \widehat{V}$, $a \in \mathbb{F}$. Then $a\Lambda(\phi) + \Lambda(\psi) = \Lambda(\bar{a}\phi + \psi) \in \Lambda(W^0)$ since W^0 is a subspace of $\widehat{V}$. Let $U = \{\beta \in V \mid \langle \beta, \alpha \rangle = 0 \ \forall \alpha \in W\}$. From Theorem 10.2.2 for any $\beta \in V$ there is a unique $\phi \in \widehat{V}$ such that $\beta = \Lambda(\phi)$. Then $\beta \in \Lambda(W^0)$ if and only if $\beta = \Lambda(\phi)$ for some $\phi \in W^0$. This is equivalent to $\langle \beta, \alpha \rangle = \phi(\alpha) = 0 \ \forall \alpha \in W$. Hence $\Lambda(W^0) = U$. □

In general inner product space V, we shall use $W^\perp$ to denote the subspace

$$\{\beta \in V \mid \langle \beta, \alpha \rangle = 0 \ \forall \alpha \in W\}$$

in the sequel, where $W \subseteq V$.

Theorem 10.2.9 *Let V be an n-dimensional inner product space. If W is a subspace of V of dimension r, then $W^\perp$ is a subspace of V of dimension $n - r$. Moreover, $W \cap W^\perp = \{\mathbf{0}\}$ and hence $V = W \oplus W^\perp$.*

Proof: Let $\alpha \in W \cap W^\perp$. Then by the definition of $W^\perp$, $0 = \langle \alpha, \alpha \rangle = \|\alpha\|^2$. Hence $\alpha = \mathbf{0}$. Thus $W \cap W^\perp = \{\mathbf{0}\}$. Thus it suffices to show that $V = W + W^\perp$.

For $\alpha \in V$, by Theorem 10.1.17 there is a unique $\beta \in W$ such that β is the best approximation to α that lies in W. Moreover $\alpha - \beta$ is orthogonal to any vector in W, i.e., $\alpha - \beta \in W^\perp$. Then

$$\alpha = \beta + (\alpha - \beta) \in W + W^\perp.$$

Hence we have the theorem. □

In the proof above, if we denote the best approximation vector β to α in W as $\sigma(\alpha)$, then one can show that $\sigma \in L(V, V)$. The vector $\beta = \sigma(\alpha)$ is also called the *orthogonal projection of α on W*. The linear transformation σ is called the *orthogonal projection of V on W*.

Definition 10.2.10 Suppose W_1 and W_2 are subspaces of an inner product space V. If $V = W_1 + W_2$ and vectors of W_1 are orthogonal to vectors of W_2, then W_1 is said to be an *orthogonal complement of W_2* and is denoted by $V = W_1 \perp W_2$. Note that $W_1 \cap W_2 = \{\mathbf{0}\}$.

Theorem 10.2.11 *Let V be a finite dimensional inner product space. Then any subspace W of V has a unique orthogonal complement.*

Proof: The existence of orthogonal complement follows from Theorem 10.2.9. The uniqueness is left as an exercise. □

Theorem 10.2.12 *Suppose W is a subspace of an inner product space V invariant under a linear transformation σ. Then $W^\perp$ is invariant under σ^*, the adjoint transformation of σ.*

Proof: Let $\alpha \in W^\perp$. Then for $\beta \in W$, we have $\langle \sigma^*(\alpha), \beta \rangle = \langle \alpha, \sigma(\beta) \rangle = 0$ since $\sigma(\beta) \in W$ and $\alpha \in W^\perp$. Hence $\sigma^*(\alpha) \in W^\perp$. □

Theorem 10.2.13 *Let $\sigma \in L(V, V)$, where V is an inner product space, and let σ^* be its adjoint transformation. Then* $\ker(\sigma^*) = \sigma(V)^\perp$.

Proof: Let $\alpha \in \ker(\sigma^*)$. Then $\sigma^*(\alpha) = \mathbf{0}$. Thus $\forall \beta \in V$, $\langle \alpha, \sigma(\beta)\rangle = \langle \sigma^*(\alpha), \beta\rangle = 0$. That is, $\alpha \in \sigma(V)^\perp$.

Conversely, suppose $\alpha \in \sigma(V)^\perp$. Then $\langle \sigma^*(\alpha), \sigma^*(\alpha)\rangle = \langle \alpha, \sigma(\sigma^*(\alpha))\rangle = 0$. Thus $\sigma^*(\alpha) = \mathbf{0}$. That is, $\alpha \in \ker(\sigma^*)$. □

Theorem 10.2.14 *Let V be a finite dimensional inner product space. For each conjugate bilinear form f, there exists a unique linear transformation σ on V such that $f(\alpha, \beta) = \langle \alpha, \sigma(\beta)\rangle$ $\forall \alpha, \beta \in V$.*

Proof: For each $\alpha \in V$, $f(\alpha, \beta)$ is linear in β. Thus by Theorem 10.2.1, there exists a unique vector γ such that $f(\alpha, \beta) = \langle \gamma, \beta\rangle \ \ \forall \beta \in V$.

Let $\tau : V \to V$ be the mapping which associates α to γ. We claim that τ is linear. For any $\alpha_1, \alpha_2, \beta \in V$ and $a \in \mathbb{F}$,

$$\langle \tau(a\alpha_1+\alpha_2), \beta\rangle = f(a\alpha_1+\alpha_2, \beta) = \bar{a}f(\alpha_1, \beta)+f(\alpha_2, \beta) = \langle a\tau(\alpha_1), \beta\rangle+\langle \tau(\alpha_2), \beta\rangle = \langle a\tau(\alpha_1)+\tau(\alpha_2), \beta\rangle.$$

Thus $\tau(a\alpha_1 + \alpha_2) = a\tau(\alpha_1) + \tau(\alpha_2)$.

Let $\sigma = \tau^*$. Then we have $f(\alpha, \beta) = \langle \tau(\alpha), \beta\rangle = \langle \alpha, \sigma(\beta)\rangle$. Thus, σ is the required linear transformation. Clearly, σ is unique. □

The linear transformation σ defined above is called the *linear transformation associated with the conjugate bilinear form f*.

Theorem 10.2.15 *Let V be a finite dimensional inner product space. Suppose f is a conjugate bilinear form on V and σ is the associated linear transformation. Then f and σ are represented by the same matrix with respect to an orthonormal basis.*

Proof: Let $\{\xi_1, \ldots, \xi_n\}$ be an orthonormal basis and let $A = (a_{ij})$ be the matrix representing σ with respect to this basis. Then

$$f(\xi_i, \xi_j) = \langle \xi_i, \sigma(\xi_j)\rangle = \left\langle \xi_i, \sum_{k=1}^{n} a_{kj}\xi_k \right\rangle = a_{ij}.$$ □

By the above theorem we can define that the *eigenvalues and eigenvectors* of a conjugate bilinear form as the eigenvalues and eigenvectors of the associated linear transformation. It is easy to see that there is a bijection between linear transformations and conjugate bilinear forms.

Definition 10.2.16 A linear transformation $\sigma : V \to V$ is said to be *self-adjoint* if $\sigma^* = \sigma$.

Proposition 10.2.17 *Suppose V is a finite dimensional inner product space. A linear transformation $\sigma : V \to V$ is self-adjoint if and only if the matrix representing σ with respect to an orthonormal basis is Hermitian.*

Proof: This follows from the paragraph between Theorem 10.2.6 and Example 10.2.7. □

Exercise 10.2

10.2-1. Suppose W_1 and W_2 are two subspace of an inner product space V. Prove that if $W_1 \subseteq W_2$, then $W_1^\perp \supseteq W_2^\perp$.

10.2-2. Suppose V is an inner product space. Show that if U, W and W' are subspaces of V such that $U \perp W = U \perp W'$, then $W = W'$.

10.2-3. Let V be a finite dimensional inner product space. Show that if $\sigma \in L(V, V)$ is an isomorphism, then $(\sigma^*)^{-1} = (\sigma^{-1})^*$.

10.3 Isometry Transformations

In the real world ($\mathbb{R}^3$), there are many motions of rigid objects. For example, translations and rotations (rotational dynamics in physics). They preserve angle of any two vectors. Now we shall consider an abstract case in mathematical sense called orthogonal and unitary transformations. They will preserve the inner product, and hence preserve angles between vectors.

Definition 10.3.1 Let V be an inner product space over $\mathbb{F}$. A linear transformation $\sigma : V \to V$ is called an *isometry* if $\|\sigma(\alpha)\| = \|\alpha\|\ \forall \alpha \in V$. If $\mathbb{F} = \mathbb{R}$, then σ is called an *orthogonal transformation*. If $\mathbb{F} = \mathbb{C}$, then σ is called a *unitary transformation*. Note that an isometry is always injective.

Theorem 10.3.2 *Let $\sigma \in L(V, V)$, where V is an inner product space over $\mathbb{F}$ with $\mathbb{F} \subseteq \mathbb{R}$ or $i \in \mathbb{F}$. Then σ is an isometry if and only if σ preserves inner product; that is, $\langle \sigma(\alpha), \sigma(\beta)\rangle = \langle \alpha, \beta\rangle\ \forall \alpha, \beta \in V$.*

Proof: If $\langle \sigma(\alpha), \sigma(\beta)\rangle = \langle \alpha, \beta\rangle$ for $\alpha, \beta \in V$, then in particular, when $\alpha = \beta$, we have $\|\sigma(\alpha)\|^2 = \|\alpha\|^2$. Hence σ is an isometry.

Now suppose σ is an isometry. For $\mathbb{F} \subseteq \mathbb{R}$, by polarization identity we have

$$\begin{aligned}\langle \alpha, \beta\rangle &= \frac{1}{4}\|\alpha + \beta\|^2 - \frac{1}{4}\|\alpha - \beta\|^2 = \frac{1}{4}\|\sigma(\alpha + \beta)\|^2 - \frac{1}{4}\|\sigma(\alpha - \beta)\|^2 \\ &= \frac{1}{4}\|\sigma(\alpha) + \sigma(\beta)\|^2 - \frac{1}{4}\|\sigma(\alpha) - \sigma(\beta)\|^2 = \langle \sigma(\alpha), \sigma(\beta)\rangle.\end{aligned}$$

For $i \in \mathbb{F} \subseteq \mathbb{C}$, by polarization identity we have

$$\begin{aligned}\langle \alpha, \beta\rangle &= \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\alpha + i^n\beta\|^2 \\ &= \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\sigma(\alpha + i^n\beta)\|^2 \\ &= \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\sigma(\alpha) + i^n\sigma(\beta)\|^2 \\ &= \langle \sigma(\alpha), \sigma(\beta)\rangle.\end{aligned}$$

□

Corollary 10.3.3 *Let V be a finite dimensional inner product space over $\mathbb{F}$, where $\mathbb{F} \subseteq \mathbb{R}$ or $i \in \mathbb{F} \subseteq \mathbb{C}$. If $\sigma \in L(V, V)$ is an isometry, then σ maps orthonormal basis to orthonormal basis.*

We shall obtain a stronger result of the converse of the above corollary. It is stated as follows.

Theorem 10.3.4 *Let σ be a linear transformation on an inner product space V. If σ maps orthonormal basis onto orthonormal basis, then σ is an isometry.*

Proof: Let $\{\xi_i\}_{i\in I}$ be an orthonormal basis of V such that $\{\sigma(\xi_i)\}_{i\in I}$ is also an orthonormal basis. Let $\alpha \in V$. Then $\alpha = \sum_{k=1}^{m} a_{i_k}\xi_{i_k}$ for some m. Hence

$$\begin{aligned}\|\sigma(\alpha)\|^2 = \langle \sigma(\alpha), \sigma(\alpha)\rangle &= \left\langle \sum_{k=1}^{m} a_{i_k}\sigma(\xi_{i_k}), \sum_{j=1}^{m} a_{i_j}\sigma(\xi_{i_j})\right\rangle \\ &= \sum_{k=1}^{m}\sum_{j=1}^{m} \overline{a_{i_k}}a_{i_j}\left\langle \sigma(\xi_{i_k}), \sigma(\xi_{i_j})\right\rangle = \sum_{k=1}^{m} |a_{i_k}|^2 = \|\alpha\|^2.\end{aligned}$$

□

Theorem 10.3.5 *Suppose V is a finite dimensional inner product space over $\mathbb{F}$ with $\mathbb{F} \subseteq \mathbb{R}$ or $i \in \mathbb{F}$ and $\sigma \in L(V,V)$. Then σ is an isometry if and only if $\sigma^* = \sigma^{-1}$.*

Proof: Suppose σ is an isometry. By Theorem 10.3.2, $\langle \sigma(\alpha), \sigma(\beta)\rangle = \langle \alpha, \beta\rangle \ \forall \alpha, \beta \in V$. By Theorem 10.2.4, $\langle \sigma(\alpha), \sigma(\beta)\rangle = \langle \sigma^*(\sigma(\alpha)), \beta\rangle$. Thus $(\sigma^* \circ \sigma)(\alpha) = \alpha \ \forall \alpha \in V$. Hence $\sigma^* \circ \sigma$ is the identity mapping. So σ is injective. Since V is finite dimension, σ is an isomorphism. Thus σ^{-1} exists. Hence $\sigma^* = \sigma^{-1}$.

Conversely, suppose $\sigma^* = \sigma^{-1}$. Then $\langle \sigma(\alpha), \sigma(\beta)\rangle = \langle \sigma^*(\sigma(\alpha)), \beta\rangle = \langle \alpha, \beta\rangle \ \forall \alpha, \beta \in V$. Thus σ is an isometry. □

Following we shall study the matrix representing a unitary transformation or an orthogonal transformation.

Theorem 10.3.6 *Let V be a unitary space. Then a complex matrix U represents a unitary transformation σ with respect to an orthonormal basis $\mathscr{A}$ if and only if $U^* = U^{-1}$.*

Proof: By the hypothesis, $U = [\sigma]_{\mathscr{A}}$. By the discussion between Theorem 10.2.6 and Example 10.2.7 we have $U^* = [\sigma^*]_{\mathscr{A}}$. By Theorem 10.3.5, σ is a unitary transformation if and only if $\sigma^* = \sigma^{-1}$, if and only if $U^* = U^{-1}$. □

By the same proof we have

Corollary 10.3.7 *Let V be a Euclidean space. Then a real matrix U represents an orthogonal transformation with respect to an orthonormal basis if and only if $U^T = U^{-1}$.*

Definition 10.3.8 A complex matrix U is said to be *unitary* if $U^*U = I$. If U is a real matrix and $U^* = U^T = U^{-1}$, then U is called an *orthogonal matrix*.

Proposition 10.3.9 *Let $U \in M_n(\mathbb{F})$. Then the followings are equivalent:*

(1) U is unitary (or orthogonal).

(2) The columns of U are orthonormal.

(3) The rows of U are orthonormal.

Proof: Since $U^*U = I$, we have $UU^* = I$. Thus

$$\sum_{r=1}^{n} \overline{(U)_{r,i}}(U)_{r,j} = \delta_{ij} = \sum_{s=1}^{n} (U)_{i,s}\overline{(U)_{j,s}} \ \forall i, j.$$ □

Theorem 10.3.10 *The matrix of transition from one orthonormal basis to another is unitary (or orthogonal if $\mathbb{F} \subseteq \mathbb{R}$).*

Proof: Suppose $\mathscr{A} = \{\xi_1, \ldots, \xi_n\}$ and $\mathscr{B} = \{\zeta_1, \ldots, \zeta_n\}$ are two orthonormal bases with $P = (p_{ij})$ as the matrix of transition from $\mathscr{A}$ to $\mathscr{B}$. Then $\zeta_j = \sum_{r=1}^{n} p_{rj}\xi_r$. Thus

$$\delta_{ij} = \langle \zeta_i, \zeta_j\rangle = \left\langle \sum_{r=1}^{n} p_{ri}\xi_r, \sum_{s=1}^{n} p_{sj}\xi_s \right\rangle = \sum_{r=1}^{n} \overline{p_{ri}}p_{rj}.$$

Hence $P^*P = I$. □

Definition 10.3.11 Two square matrices A and B are *unitary* (respectively *orthogonal*) *similar* if there exists a unitary (respectively orthogonal) matrix P such that $B = P^{-1}AP = P^*AP$ (or $B = P^{-1}AP = P^TAP$).

It is easy to see that unitary similar and orthogonal similar are equivalence relations on $M_n(\mathbb{F})$.

Exercise 10.3

10.3-1. Show that the product of unitary (respectively orthogonal) matrices is unitary (respectively orthogonal).

10.3-2. Let $\{\xi_1, \xi_2, \xi_3\}$ be an orthonormal basis of V over $\mathbb{R}$ or $\mathbb{C}$. Find an isometry that maps ξ_1 onto $\frac{1}{3}(\xi_1 + 2\xi_2 + 2\xi_3)$.

10.3-3. Let A be an orthogonal matrix. Suppose A_{ij} is the cofactor of $(A)_{i,j}$. Show that $A_{ij} = (A)_{i,j} \det A$.

10.4 Upper Triangular Form

Given a square matrix A over $\mathbb{C}$ we know that it is similar to a Jordan form, that is there is an invertible matrix P such that $P^{-1}AP$ is in Jordan form. Jordan form is a particular upper triangular matrix. In this section we shall show that every square matric over $\mathbb{C}$ is unitary similar to an upper triangular matrix. For the real case, we know that if characteristic polynomial of a real square matrix A factors into linear factors, then it is similar to a Jordan form. Similar to the complex case, we shall show that every real square matrix is orthogonal similar to an upper triangular matrix.

Theorem 10.4.1 *Let V be a unitary space. Suppose $\sigma \in L(V, V)$. Then there exists an orthonormal basis with respect to which the matrix representing σ is in the upper triangular form, that is, each entry below the main diagonal is zero.*

Proof: We shall prove by mathematical induction on $n = \dim V$. Clearly, the theorem holds for $n = 1$.

Assume the theorem holds for $\dim V < n$ with $n \geq 2$. Suppose $\dim V = n$. Since V is a vector space over $\mathbb{C}$, σ^* has at least one eigenvalue. Let λ be an eigenvalue of σ^* with unit vector ξ_n as its corresponding eigenvector. Put $W = \text{span}(\xi_n)^\perp$. Then W is of dimension $n-1$. By Theorems 10.2.6 and 10.2.12 W is invariant under $(\sigma^*)^* = \sigma$. Thus, by induction hypothesis, there is an orthonormal basis $\{\xi_1, \ldots, \xi_{n-1}\}$ of W such that $\sigma(\xi_k) = \sum_{i=1}^{k} a_{ik}\xi_i$ for $k = 1, \ldots, n-1$. Clearly, $\{\xi_1, \ldots, \xi_n\}$ is a required basis. □

Corollary 10.4.2 *Over the field $\mathbb{C}$, every square matrix is unitary similar to an upper triangular matrix.*

Now we are going to consider the real case.

Theorem 10.4.3 *Let V be a Euclidean space. Suppose $\sigma \in L(V, V)$ whose characteristic polynomial factors into real linear factors. Then there is an orthonormal basis of V with respect to which the matrix representing σ is in the upper triangular form.*

Proof: Again, we shall prove by mathematical induction on $n = \dim V$. Clearly, the theorem holds for $n = 1$.

Now we assume that the theorem holds for all Euclidean space of dimension less than n with $n \geq 2$. Let λ be an eigenvalue of σ with unit vector ξ_1 as its corresponding eigenvector. By the Gram-Schmidt process, we obtain an orthonormal basis $\{\xi_1, \ldots, \xi_n\}$ of V.

Let $W = \text{span}\{\xi_2, \ldots, \xi_n\}$. We define a mapping $\tau : V \to W$ as follows. For each $\alpha = \sum_{i=1}^{n} a_i\xi_i \in V$, defined $\tau(\alpha) = \sum_{i=2}^{n} a_i\xi_i$. Then clearly, τ is linear and $\tau(\alpha) = \alpha \ \forall \alpha \in W$.

Let $\sigma' = (\tau \circ \sigma)\big|_W$. Then $\sigma' \in L(W, W)$. To apply the induction hypothesis we have to show that the characteristic polynomial of σ' factors into real linear factors.

First, we note that if $\alpha \in W$, then $(\tau \circ \sigma)(\alpha) = (\tau \circ \sigma \circ \tau)(\alpha)$. If $\alpha = c\xi_1$ for $c \in \mathbb{R}$, then $(\tau \circ \sigma)(\alpha) = \lambda c\tau(\xi_1) = \mathbf{0} = (\tau \circ \sigma \circ \tau)(\alpha)$. Thus $\tau \circ \sigma = \tau \circ \sigma \circ \tau$. Hence by an easy induction, we can show that

$$(\tau \circ \sigma)^k = \tau \circ \sigma^k, \ k = 1, 2, \ldots.$$

Suppose $f(x) = k_n x^n + k_{n-1}x^{n-1} + \cdots + k_1 x + k_0$ is the characteristic polynomial of σ. Then for $\alpha \in W$,

$$\begin{aligned} f(\sigma')(\alpha) &= k_n\sigma'^n(\alpha) + k_{n-1}\sigma'^{n-1} + \cdots + k_1\sigma'(\alpha) + k_0\alpha \\ &= k_n(\tau \circ \sigma)^n(\alpha) + k_{n-1}(\tau \circ \sigma)^{n-1} + \cdots + k_1(\tau \circ \sigma)(\alpha) + k_0\tau(\alpha) \\ &= k_n(\tau \circ \sigma^n)(\alpha) + k_{n-1}(\tau \circ \sigma^{n-1}) + \cdots + k_1(\tau \circ \sigma)(\alpha) + k_0\tau(\alpha) \\ &= \tau(k_n\sigma^n(\alpha) + k_{n-1}\sigma^{n-1}(\alpha) + \cdots + k_1\sigma(\alpha) + k_0\alpha) = \tau(f(\sigma)(\alpha)) = \mathbf{0}. \end{aligned}$$

Thus $f(\sigma') = O$. Hence the minimum polynomial of σ' divides $f(x)$. Since $f(x)$ factors into real linear factors, the minimum polynomial of σ' also factors into linear factors. Thus the characteristic polynomial of σ' must also factor into real linear factors. By the induction hypothesis, W has an orthonormal basis $\{\zeta_2, \ldots, \zeta_n\}$ such that $\sigma'(\zeta_k) = \sum_{i=2}^{k} a_{ik}\zeta_i$ for $k = 2, \ldots, n$. Let $\zeta_1 = \xi_1$. Then $\sigma(\zeta_1) = \sigma(\xi_1) = \lambda\zeta_1$. For $k \geq 2$, since $\sigma(\zeta_k) = \sum_{j=2}^{n} b_{jk}\zeta_j + b_{1k}\zeta_1$ for some $b_{jk} \in \mathbb{R}$,

$$\sigma'(\zeta_k) = \sum_{i=2}^{k} a_{ik}\zeta_i = \tau(\sigma(\zeta_k)) = \sum_{j=2}^{n} b_{jk}\tau(\zeta_j) + \mathbf{0} = \sum_{j=2}^{n} b_{jk}\zeta_j, \text{ for some } a_{ik} \in \mathbb{R}.$$

Thus $b_{jk} = 0$ for $j > k$, i.e., $\sigma(\zeta_k) = b_{1k}\zeta_1 + \sum_{j=2}^{k} b_{jk}\zeta_j$. Hence $\{\zeta_1, \zeta_2, \ldots, \zeta_n\}$ is a required basis. □

Corollary 10.4.4 *Every real square matrix whose characteristic polynomial factors into real linear factors is orthogonal similar to an upper triangular matrix.*

Theorems 10.4.1 and 10.4.3 are usually referred as *Schur's Theorems.*

Given a square real matrix whose eigenvalues are all real. Following we provide an algorithm for finding an upper triangular matrix which is orthogonal similar to this square matrix.

Let $A \in M_n(\mathbb{R})$ be such that all its eigenvalues are real. Then by Corollary 10.4.4 A is orthogonal similar to an upper triangular matrix. To put A into an upper triangular from, we proceed as follows.

Step 1. Find one eigenvalue λ_1 and choose a corresponding eigenvector ξ_1 with unit length.

Step 2. Extend ξ_1 to an orthonormal basis $\{\xi_1, \ldots, \xi_n\}$ of $\mathbb{R}^n$. Form the transition matrix P_1, which is an orthogonal matrix. Indeed, the i-th column is ξ_i.

Step 3. Compute $P_1^T A P_1$, which is of the form

$$\left(\begin{array}{c|ccc} \lambda_1 & \cdots & \cdots & \cdots \\ \hline 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{array}\right).$$

Here A_1 is a real $(n-1)\times(n-1)$ matrix whose eigenvalues are also eigenvalues of A, hence they are all real. If A_1 is already upper triangular, then we are done.

Step 4. Suppose A_1 is not upper triangular, then we apply Step 1 and Step 2 to A_1 to obtain an $(n-1)\times(n-1)$ orthogonal matrix Q_1 such that $Q_1^T A_1 Q_1$ is of the form

$$\left(\begin{array}{c|ccc} \lambda_2 & \cdots & \cdots & \cdots \\ \hline 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{array}\right),$$

for some eigenvalue λ_2 and some $(n-2)\times(n-2)$ matrix A_2 whose eigenvalues are also eigenvalues of A. Now let

$$P_2 = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{array}\right).$$

Clearly P_2 is orthogonal and

$$P_2^T P_1^T A P_1 P_2 = \left(\begin{array}{cc|ccc} \lambda_1 & * & \cdots & \cdots & \cdots \\ 0 & \lambda_2 & \cdots & \cdots & \cdots \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & A_2 & \\ 0 & 0 & & & \end{array}\right).$$

Note that $P_1 P_2$ is an orthogonal matrix (see Exercise 10.3-1.)

Step 5. If A_2 is upper triangular, then we are done. Otherwise, we repeat the above steps until we obtain an upper triangular matrix.

Example 10.4.5 Let $A = \begin{pmatrix} 2 & 2 & -1 \\ -1 & -1 & 1 \\ -1 & -2 & 2 \end{pmatrix}$. Then 1 is an eigenvalue of A. $\xi_1 = \frac{1}{\sqrt{2}}(1,0,1)$ is a corresponding eigenvector of unit length. By Gram-Schmidt process, we have an orthonormal basis $\left\{\frac{1}{\sqrt{2}}(1,0,1),\ \frac{1}{\sqrt{2}}(1,0,-1),\ (0,1,0)\right\}$ of $\mathbb{R}^3$.

Put $P_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \end{pmatrix}$. Then $P_1^T A P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 2\sqrt{2} \\ 0 & -\sqrt{2} & -1 \end{pmatrix}$. Now consider the 2×2 matrix $\begin{pmatrix} 3 & 2\sqrt{2} \\ -\sqrt{2} & -1 \end{pmatrix}$. This matrix has an eigenvalue 1 and a corresponding eigenvector $\frac{1}{\sqrt{3}}(\sqrt{2},-1)$. By an easy inspection, we see that $\left\{\frac{1}{\sqrt{3}}(\sqrt{2},-1),\ \frac{1}{\sqrt{3}}(1,\sqrt{2})\right\}$ is an orthonormal basis of $\mathbb{R}^2$.

Form $P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\frac{2}{3}} & \sqrt{\frac{1}{3}} \\ 0 & -\sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} \end{pmatrix}$. Then $P_2^T P_1^T A P_1 P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3\sqrt{2} \\ 0 & 0 & 1 \end{pmatrix}$. □

Exercise 10.4

10.4-1. Let $A = \begin{pmatrix} 1 & 1 & -1 \\ -1 & 3 & -1 \\ -1 & 2 & 0 \end{pmatrix}$. Find an orthogonal matrix P such that $P^T AP$ is upper triangular.

10.5 Normal Linear Transformations

We learned that every matrix whose minimum polynomial can be factorized into linear factors is similar to a diagonal matrix. We also learned every symmetric or Hermitian matrix is congruent to a diagonal matrix. Under what condition can a matrix be simultaneously similar and congruent to a diagonal matrix, i.e., unitary or orthogonal similar to a diagonal matrix?

Definition 10.5.1 A linear transformation $\sigma \in L(V, V)$, where V is an inner product space, is called a *normal linear transformation* if $\sigma \circ \sigma^* = \sigma^* \circ \sigma$.

Theorem 10.5.2 *Let V be an inner product space over $\mathbb{F}$, where $\mathbb{F} \subseteq \mathbb{R}$ or $i \in \mathbb{F}$. Suppose $\sigma \in L(V, V)$. Then the followings are equivalent:*

(1) σ is normal.

(2) $\langle \sigma(\alpha), \sigma(\beta) \rangle = \langle \sigma^*(\alpha), \sigma^*(\beta) \rangle \ \forall \alpha, \beta \in V$.

(3) $\|\sigma(\alpha)\| = \|\sigma^*(\alpha)\| \ \forall \alpha \in V$.

Proof:

(1)⇒(2): This is because $\langle \sigma(\alpha), \sigma(\beta) \rangle = \langle \sigma^* \circ \sigma(\alpha), \beta \rangle = \langle \sigma \circ \sigma^*(\alpha), \beta \rangle = \langle \sigma^*(\alpha), \sigma^*(\beta) \rangle$.

(2)⇒(1): Since $\langle \alpha, \sigma \circ \sigma^*(\beta) \rangle = \langle \sigma^*(\alpha), \sigma^*(\beta) \rangle = \langle \sigma(\alpha), \sigma(\beta) \rangle = \langle \alpha, \sigma^* \circ \sigma(\beta) \rangle \ \forall \alpha, \beta \in V$, so $\sigma \circ \sigma^* = \sigma^* \circ \sigma$.

(2)⇒(3): Just put $\alpha = \beta$ in (2).

(3)⇒(2): We have to consider the following two cases:

Case 1: $\mathbb{F} \subseteq R$. Then

$$\begin{aligned} \langle \sigma(\alpha), \sigma(\beta) \rangle &= \frac{1}{4} \left(\|\sigma(\alpha + \beta)\|^2 - \|\sigma(\alpha - \beta)\|^2 \right) \\ &= \frac{1}{4} \left(\|\sigma^*(\alpha + \beta)\|^2 - \|\sigma^*(\alpha - \beta)\|^2 \right) = \langle \sigma^*(\alpha), \sigma^*(\beta) \rangle. \end{aligned}$$

Case 2: $i \in \mathbb{F}$. Then

$$\begin{aligned}\langle \sigma(\alpha), \sigma(\beta)\rangle &= \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\sigma(\alpha) + i^n\sigma(\beta)\|^2 = \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\sigma(\alpha + i^n\beta)\|^2 \\ &= \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\sigma^*(\alpha + i^n\beta)\|^2 = \frac{1}{4}\sum_{n=0}^{3} \overline{i^n}\|\sigma^*(\alpha) + i^n\sigma^*(\beta)\|^2 \\ &= \langle \sigma^*(\alpha), \sigma^*(\beta)\rangle. \end{aligned}$$

□

Theorem 10.5.3 *Let $\sigma : V \to V$ be a normal linear transformation of an inner product space V. Then $\ker(\sigma) = \ker(\sigma^*)$. Moreover, if V is finite dimensional, then $\sigma(V) = \sigma^*(V)$.*

Proof: By the proof of Theorem 10.5.2, $\|\sigma(\alpha)\| = \|\sigma^*(\alpha)\|$. Thus $\sigma(\alpha) = \mathbf{0}$ if and only if $\sigma^*(\alpha) = \mathbf{0}$. Hence $\ker(\sigma) = \ker(\sigma^*)$.

By Theorem 10.2.13, $\ker(\sigma^*) = \sigma(V)^\perp$ and $\ker(\sigma) = \sigma^*(V)^\perp$. Hence from $\ker(\sigma) = \ker(\sigma^*)$ if V is finite dimensional, then by the uniqueness of orthogonal complement we have $\sigma(V) = \sigma^*(V)$. □

Theorem 10.5.4 *Let $\sigma : V \to V$ be a normal linear transformation on an inner product space V. If ξ is an eigenvector of σ corresponding to eigenvalue λ, then ξ is also an eigenvector of σ^* corresponding to eigenvalue $\overline{\lambda}$.*

Proof: Since σ is normal, by Theorem 10.5.2 $\langle \sigma(\xi), \sigma(\xi)\rangle = \langle \sigma^*(\xi), \sigma^*(\xi)\rangle$. Thus

$$\begin{aligned} 0 &= \|\sigma(\xi) - \lambda\xi\|^2 = \langle \sigma(\xi) - \lambda\xi, \sigma(\xi) - \lambda\xi\rangle = \langle \sigma(\xi), \sigma(\xi)\rangle - \overline{\lambda}\langle \xi, \sigma(\xi)\rangle - \lambda\langle \sigma(\xi), \xi\rangle + |\lambda|^2\langle \xi, \xi\rangle \\ &= \langle \sigma^*(\xi), \sigma^*(\xi)\rangle - \overline{\lambda}\langle \sigma^*(\xi), \xi\rangle - \lambda\langle \xi, \sigma^*(\xi)\rangle + |\lambda|^2\langle \xi, \xi\rangle = \|\sigma^*(\xi) - \overline{\lambda}\xi\|^2. \end{aligned}$$

Thus $\sigma^*(\xi) = \overline{\lambda}\xi$. □

By applying the above theorem we have

Theorem 10.5.5 *Let $\sigma : V \to V$ be a normal linear transformation of an inner product space V. Suppose ξ_1 and ξ_2 are eigenvectors corresponding to eigenvalues λ_1 and λ_2, respectively. If $\lambda_1 \neq \lambda_2$, then $\langle \xi_1, \xi_2\rangle = 0$.*

Proof: Since

$$\lambda_2\langle \xi_1, \xi_2\rangle = \langle \xi_1, \lambda_2\xi_2\rangle = \langle \xi_1, \sigma(\xi_2)\rangle = \langle \sigma^*(\xi_1), \xi_2\rangle = \langle \overline{\lambda_1}\xi_1, \xi_2\rangle = \lambda_1\langle \xi_1, \xi_2\rangle,$$

$(\lambda_1 - \lambda_2)\langle \xi_1, \xi_2\rangle = 0$. Since $\lambda_1 \neq \lambda_2$, $\langle \xi_1, \xi_2\rangle = 0$. □

Lemma 10.5.6 *Let $\sigma : V \to V$ be a normal linear transformation of an inner product space V. If S is a set of eigenvectors of σ, then $S^\perp$ is invariable under σ.*

Proof: Let $\alpha \in S^\perp$. Suppose ξ is an eigenvector in S corresponding to eigenvalue λ. Then $\langle \sigma(\alpha), \xi\rangle = \langle \alpha, \sigma^*(\xi)\rangle = \langle \alpha, \overline{\lambda}\xi\rangle = \overline{\lambda}\langle \alpha, \xi\rangle = 0$. Thus $\sigma(\alpha) \in S^\perp$. □

Lemma 10.5.7 *Let $\sigma : V \to V$ be a normal linear transformation of an inner product space V. If W is a subspace invariant under both σ and σ^*, then σ', the restriction of σ on W is a normal linear transformation on W.*

Proof: Let $\alpha, \beta \in W$. Since $\langle \sigma^*(\alpha), \beta\rangle = \langle \alpha, \sigma(\beta)\rangle = \langle \alpha, \sigma'(\beta)\rangle$, $\sigma'^* = \sigma^*\big|_W$ by uniqueness.

Let $\alpha, \beta \in W$. $\langle \sigma'(\alpha), \sigma'(\beta)\rangle = \langle \sigma(\alpha), \sigma(\beta)\rangle = \langle \sigma^*(\alpha), \sigma^*(\beta)\rangle = \langle \sigma'^*(\alpha), \sigma'^*(\beta)\rangle$. Thus by Theorem 10.5.2 σ' is normal linear transformation on W. □

Theorem 10.5.8 *Let V be a unitary space and $\sigma : V \to V$ a normal linear transformation. If W is a subspace invariant under σ, then W is also invariant under σ^*. Hence $\sigma\big|_W$ is a normal linear transformation on W.*

Proof: We shall prove by mathematical induction on $n = \dim V$. Clearly, the theorem holds for $n = 1$.

Now for $n \geq 2$, we assume the theorem holds for all unitary spaces of dimension less than n. Suppose V is a unitary space of dimension n and let W be a subspace invariant under σ. If $W = V$, then we are done. So we assume that $\dim W \leq n - 1$. Then by Theorems 10.2.9 and 10.2.12, $\dim W^\perp \geq 1$ and $W^\perp$ is invariant under σ^*. Since $W^\perp$ is also a finite dimensional vector space over $\mathbb{C}$, σ^* has at least one eigenvector ξ in $W^\perp$. By Theorem 10.5.4, ξ is also an eigenvector of σ. By Lemma 10.5.6, $\text{span}\{\xi\}^\perp$ is invariant under both σ and σ^*. Then by Lemma 10.5.7, σ is a normal linear transformation on $\text{span}\{\xi\}^\perp$. Since $\text{span}\{\xi\} \subseteq W^\perp$, $W \subseteq \text{span}\{\xi\}^\perp$ and $\dim(\text{span}\{\xi\}^\perp) = n - 1$, the induction hypothesis applies. Thus W is invariant under σ^* and σ is a normal linear transformation on W. □

Theorem 10.5.9 *Let V be a finite dimensional inner product space and let $\sigma \in L(V, V)$. If V has an orthonormal basis consisting of eigenvectors of σ, then σ is a normal linear transformation.*

Proof: It follows from Theorem 10.5.2(2). □

Theorem 10.5.10 *If V is a unitary space and $\sigma : V \to V$ is a normal linear transformation, then V has an orthonormal basis consisting of eigenvectors of σ.*

Proof: We shall prove by mathematical induction on $n = \dim V$. For $n = 1$, the theorem is clear, for any unit vector will do.

Now for $n \geq 2$, we assume the theorem holds for all unitary spaces of dimension less than n. Suppose V is a unitary space of dimension n. Since V is a finite dimensional vector space over $\mathbb{C}$, σ has at least one eigenvalue λ and hence has a corresponding eigenvector ξ_1 of unit length. By Lemma 10.5.6 $W = \text{span}\{\xi_1\}^\perp$ is invariant under σ. By Theorem 10.5.8, $\sigma\big|_W$ is a normal linear transformation on W. Since $\dim W = n - 1$, so by induction hypothesis, W has an orthonormal basis $\{\xi_2, \ldots, \xi_n\}$ consisting of eigenvectors of $\sigma\big|_W$. Since $V = \text{span}\{\xi_1\} \perp W$, $\{\xi_1, \xi_2, \ldots, \xi_n\}$ is an orthonormal basis of V consisting of eigenvector of σ. □

Note that in Theorem 10.5.9, we do not require that $\mathbb{F} = \mathbb{C}$. However in the proof of Theorem 10.5.10 we do not need $\mathbb{F} = \mathbb{C}$ to ensure eigenvalues exist.

Theorem 10.5.11 *Let V be a unitary space and let σ be a normal linear transformation on V. Then σ is self-adjoint if and only if all its eigenvalues are real.*

Proof: Suppose σ is self-adjoint. Let λ be an eigenvalue of σ with ξ as a corresponding eigenvector. Then by Theorem 10.5.4 we have $\lambda\xi = \sigma(\xi) = \sigma^*(\xi) = \bar{\lambda}\xi$ and therefore $(\lambda - \bar{\lambda})\xi = \mathbf{0}$. Hence $\lambda = \bar{\lambda}$. That is, λ must be real.

Conversely, suppose all the eigenvalue of σ are real. By Theorem 10.5.10 V has an orthonormal basis $\{\xi_1, \ldots, \xi_n\}$ consisting of eigenvectors of σ. Let λ_i be the eigenvalue corresponding to ξ_i. Then $\sigma^*(\xi_i) = \overline{\lambda_i}\xi_i = \lambda_i\xi_i = \sigma(\xi_i)$. Since σ and σ^* agree on a basis of V, $\sigma = \sigma^*$. □

Theorem 10.5.12 *Let V be an inner product space. Then all the eigenvalues of an isometry on V are of absolute value* 1. *If* $\dim V$ *is finite and $\sigma \in L(V,V)$ is normal whose eigenvalues are of absolute value* 1, *then σ is an isometry.*

Proof: Suppose σ is an isometry. Let λ be an eigenvalue of σ with ξ as a corresponding eigenvector. Then $\|\xi\| = \|\sigma(\xi)\| = \|\lambda\xi\| = |\lambda|\|\xi\|$. Hence $|\lambda| = 1$. So we have the first part of the theorem.

Now suppose V is finite dimensional and σ is a normal linear transformation on V whose eigenvalues are of absolute value 1. By Theorem 10.5.10 V has an orthonormal basis $\{\xi_1, \ldots, \xi_n\}$ consisting of eigenvectors of σ. Let λ_i be the eigenvalue corresponding to ξ_i. Then $\langle \sigma(\xi_i), \sigma(\xi_j)\rangle = \langle \lambda_i\xi_i, \lambda_j\xi_j\rangle = \overline{\lambda_i}\lambda_j\langle \xi_i, \xi_j\rangle = \delta_{ij}$. Since σ maps orthonormal basis onto orthonormal basis, by Theorem 10.3.4 σ is isometry. □

Now let us consider the matrix counterpart.

Definition 10.5.13 A square matrix A for which $A^*A = AA^*$ is called a *normal* matrix. Thus, a matrix that represents a normal linear transformation must be normal.

Example 10.5.14 Unitary matrices and Hermitian matrices are normal matrices. Also, diagonal matrices are normal matrices. □

Lemma 10.5.15 *An upper triangular matrix A is normal if and only if A is diagonal.*

Proof: Suppose $A = (a_{ij})$ is a normal matrix with $a_{ij} = 0$ if $i > j$. If A were not diagonal, then there would be a smallest positive integer r for which there exists an integer $s > r$ such that $a_{rs} \neq 0$. This implies that for any $i < r$, we would have $a_{ir} = 0$. Then

$$(A^*A)_{r,r} = \sum_{i=1}^{n} \overline{a_{ir}}a_{ir} = \sum_{i=1}^{n} |a_{ir}|^2 = |a_{rr}|^2 \text{ and } (AA^*)_{r,r} = \sum_{j=1}^{n} a_{rj}\overline{a_{rj}} = \sum_{j=r}^{n} |a_{rj}|^2.$$

Thus we would have $|a_{rr}|^2 = |a_{rr}|^2 + \cdots + |a_{rs}|^2 + \cdots + |a_{rn}|^2$. Since $|a_{rs}|^2 > 0$, this is clearly a contradiction.

The conversely is clear. □

Lemma 10.5.16 *A matrix that is unitary similar to a normal matrix is also normal.*

Proof: Suppose A is normal and $B = U^*AU$ for some unitary matrix U. Then

$$B^*B = (U^*AU)^*(U^*AU) = U^*A^*UU^*AU = U^*A^*AU = U^*AA^*U = U^*AUU^*A^*U = BB^*. \quad \square$$

Theorem 10.5.17 *A square matrix A that is unitary similar to a diagonal matrix if and only if A is normal.*

Proof: Suppose A is normal. By Corollary 10.4.2 A is unitary similar to an upper triangular matrix S. Then by Lemma 10.5.16 S is normal. By Lemma 10.5.15 S must be diagonal.

Conversely, suppose A is unitary similar to a diagonal matrix D. Then since D is normal, by Lemma 10.5.16 A must be normal. □

Theorem 10.5.18 *Suppose H is a Hermitian matrix. Then H is unitary similar to a diagonal matrix and all its eigenvalues are real. Conversely, if H is normal and all its eigenvalues are real, then H is Hermitian.*

Proof: Suppose H is Hermitian. Then H is normal, and by Theorem 10.5.17 H is unitary similar to a diagonal matrix D. That is, $D = U^*HU$ for some unitary matrix U. Since

$$D^* = (U^*HU)^* = U^*H^*U = U^*HU = D,$$

the diagonal entries of D are real. Since the diagonal entries of D are also eigenvalues of H, all the eigenvalues of H are real.

Conversely, if H is normal with real eigenvalues, then $D = U^*HU$ with U unitary and D a real diagonal matrix. Hence $H = UDU^*$ and $H^* = UD^*U^* = UDU^* = H$ as $D = D^*$. Thus H is Hermitian. □

Theorem 10.5.19 *If A is unitary, then A is similar to a diagonal matrix and the eigenvalues of A are of absolute value* 1*. Conversely, if A is normal and all eigenvalues are of absolute value* 1*, then A is unitary.*

Proof: Suppose A is unitary. Then A is normal, so by Theorem 10.5.17 there exists a unitary matrix U and a diagonal matrix D such that $U^*AU = D$. Since D is a product of unitary matrices, D is unitary. Therefore, $I = D^*D = \overline{D}D$, where $\overline{D}$ is the matrix obtained from D by taking complex conjugate of all entries of D. Hence the diagonal entries of D are of absolute value 1. Since the diagonal entries of D are also eigenvalues of A, we have the first part of the theorem.

Conversely, suppose A is normal and all eigenvalues of A are of absolute value 1. Then by Theorem 10.5.17 A is unitary similar to a diagonal matrix D whose diagonal entries are eigenvalues of A. Thus $D^*D = \overline{D}D = I$, D is unitary. Therefore, A is also unitary. □

If A is orthogonal, then it is not necessary that A is orthogonal similar to a diagonal matrix. For consider the matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. A is an orthogonal matrix with eigenvalues i and $-i$. Thus there cannot exist orthogonal matrix P such that $P^TAP = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

Theorem 10.5.20 *Let $A \in M_n(\mathbb{R})$. A is symmetric if and only if A is orthogonal similar to a diagonal matrix.*

Proof: Suppose A is symmetric. Then A is Hermitian. By Theorem 10.5.18 all the eigenvalues of A are real. Thus, by Corollary 10.4.4 A is orthogonal similar to an upper triangular matrix S. Thus there exists an orthogonal (real) matrix P such that $S = P^TAP$. Thus S is real matrix and

$$S^*S = S^TS = P^TA^TPP^TAP = P^TAA^TP = SS^T = SS^*.$$

Thus S is normal and by Lemma 10.5.15 is a diagonal matrix.

Conversely, suppose A is orthogonal similar to a diagonal matrix D, then there exists an orthogonal matrix P such that $P^TAP = D$. Then $A = PDP^T$ and hence $A^T = PD^TP^T = PDP^T = A$. Thus A is symmetric. □

Theorem 10.5.21 *Suppose $A \in M_n(\mathbb{R})$. Then A is symmetric if and only if A is a normal and all its eigenvalues are real.*

Proof: Suppose A is symmetric. Obviously A is normal. By Theorem 10.5.20 A is orthogonal similar to a diagonal matrix whose diagonal entries are eigenvalues of A. Hence all the eigenvalues of A are real.

Conversely, suppose A is normal and all the eigenvalues of A are real. Then by Corollary 10.4.4 and Lemma 10.5.15, A is orthogonal similar to a diagonal matrix. Hence A is symmetric. □

In practice, how do we find an orthogonal matrix to reduce a given symmetric or Hermitian matrix into diagonal form? We shall use the following examples to demonstrate.

Example 10.5.22 The matrix $A = \begin{pmatrix} 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 3 \\ 3 & 1 & 0 & 0 \\ 1 & 3 & 0 & 0 \end{pmatrix}$ is a real symmetric matrix which has four distinct eigenvalues, namely, $-4, -2, 2$ and 4. The corresponding eigenvectors are

$$(-1,-1,1,1),\ (1,-1,-1,1),\ (-1,1,-1,1) \text{ and } (1,1,1,1),$$

respectively. Since the eigenvalues are distinct, these eigenvectors are mutually orthogonal. Thus, we obtain an orthonormal basis

$$\{\tfrac{1}{2}(-1,-1,1,1),\ \tfrac{1}{2}(1,-1,-1,1),\ \tfrac{1}{2}(-1,1,-1,1),\ \tfrac{1}{2}(1,1,1,1)\}$$

and the orthogonal matrix of transition is

$$P = \frac{1}{2}\begin{pmatrix} -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$ □

Example 10.5.23 The symmetric matrix $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ 2 & -2 & 1 \end{pmatrix}$ has characteristic polynomial $-(x-3)^2(x+3)$. For the eigenvalue -3, we obtain the eigenvector $(1,-1,-1)$. For the eigenvalue 3, we obtain two linearly independent eigenvectors $(1,1,0)$ and $(1,0,1)$. Apply the Gram-Schmidt process to these two vectors we obtain an orthonormal set $\{\frac{1}{2}(1,1,0),\ \frac{1}{\sqrt{6}}(1,-1,2)\}$ also consisting of eigenvectors. Thus

$$\{\tfrac{1}{\sqrt{3}}(1,-1,-1),\ \tfrac{1}{2}(1,1,0),\ \tfrac{1}{\sqrt{6}}(1,-1,2)\}$$

is an orthonormal basis of eigenvectors. The orthogonal matrix of transition is

$$P = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \end{pmatrix}.$$ □

Example 10.5.24 Let $A = \begin{pmatrix} 1 & 1-i \\ 1+i & 3 \end{pmatrix}$. Then A is Hermitian and its characteristic polynomial is $(x-4)(x-1)$. For eigenvalue 1, we obtain eigenvector $(-1+i,1)$. For eigenvalue 4, we obtain eigenvector $(1,1+i)$. Thus, an orthonormal basis of eigenvectors is $\{\frac{1}{\sqrt{3}}(-1+i,1),\ \frac{1}{\sqrt{3}}(1,1+i)\}$. The unitary matrix of transition is

$$U = \frac{1}{\sqrt{3}}\begin{pmatrix} -1+i & 1 \\ 1 & 1+i \end{pmatrix}.$$ □

Example 10.5.25 Let $A = \begin{pmatrix} \cos\theta & 0 & -\sin\theta \\ 0 & 1 & 0 \\ \sin\theta & 0 & \cos\theta \end{pmatrix}$, where $0 < \theta < \pi$. Then A is an orthogonal matrix that is not symmetric. It is easy to see that the characteristic polynomial of A is $-(x-1)(x^2 - 2x\cos\theta + 1)$. The eigenvalues are 1, $\cos\theta + i\sin\theta$ and $\cos\theta - i\sin\theta$. The corresponding eigenvectors are $(0,1,0)$, $(1,0,-i)$ and $(1,0,i)$, respectively. Since the eigenvalues are distinct, these eigenvectors are mutually orthogonal. After normalizing, we obtain the orthonormal basis $\{(0,1,0),\ \frac{1}{\sqrt{2}}(1,0,-i),\ \frac{1}{\sqrt{2}}(1,0,i)\}$. The unitary matrix of transition is $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 1 \\ \sqrt{2} & 0 & 0 \\ 0 & -i & i \end{pmatrix}$. □

Example 10.5.26 Determine the type of the conic curve $2x^2 - 4xy + 5y^2 - 36 = 0$.

Solution: The associated quadratic form is $2x^2 - 4xy + 5y^2$ which has the representing matrix $B = \begin{pmatrix} 2 & -2 \\ -2 & 5 \end{pmatrix}$. Then there exists an orthogonal matrix $P = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix}$, so that $P^T BP = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$. Putting

$$X' = \begin{pmatrix} x' \\ y' \end{pmatrix} = P^{-1} \begin{pmatrix} x \\ y \end{pmatrix} \text{ or } \begin{pmatrix} x \\ y \end{pmatrix} = PX' = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Thus $x = \frac{1}{\sqrt{5}}(2x' - y')$ and $y = \frac{1}{\sqrt{5}}(x + 2y')$. Substitute x, y into the original equation, we get $(x')^2 + 6(y')^2 = 36$. This is an ellipse. □

Remark 10.5.27 In the above example, we have used a rotation of the axis to the major axis of the conic. We do not change the conic at all. While if we use the 'congruent' as in Chapter 9, we can reduce the conic to the form $2x'^2 + 3y'^2 = 36$ via the non-singular matrix $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Even though the curve changes its shape, but it is still an ellipse.

By applying Theorems 10.5.20 and 9.5.1 we have

Theorem 10.5.28 *Suppose $A \in M_n(\mathbb{R})$ and symmetric. Then*

(1) A is positive definite if and only if all the eigenvalues of A are positive.

(2) A is non-negative definite if and only if all the eigenvalues of A are non-negative.

Theorem 10.5.29 *Let A and B be two real symmetric $m \times m$ matrices. Then A and B are congruent if and only if A and B have the same numbers of positive, negative and zero eigenvalues.*

Proof: Let p, n, z and p', n', z' be respectively the numbers of positive, negative and zero eigenvalues of A and B.

Suppose A and B are congruent. Then there exists an invertible matrix Q such that $B = Q^T AQ$. By Remark 9.5.2 we have $p = p$; and $n = n'$, hence $z = z'$.

Conversely, there are orthogonal matrices Q and Q' such that

$$Q^T AQ = D = \operatorname{diag}\{\lambda_1, \ldots, \lambda_p, \lambda_{p+1}, \ldots, \lambda_{p+n}, 0, \ldots, 0\} \text{ and}$$
$$Q'^T BQ' = D' = \operatorname{diag}\{\lambda'_1, \ldots, \lambda'_p, \lambda'_{p+1}, \ldots, \lambda'_{p+n}, 0, \ldots, 0\}.$$

Let $d_j = (\lambda'_j)^{-1}\lambda_j$, $1 \le j \le p+n$, then $d_j > 0$. Let $P = \operatorname{diag}\{\sqrt{d_1}, \ldots, \sqrt{d_{p+n}}, 1, \ldots, 1\}$. Then $QP^T Q'^T BQ'PQ^T = A$. □

Application – Hessenberg form

We denote vectors in $\mathbb{R}^n$ by column vectors $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $Z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$, etc. Assume that $\mathbb{R}^n$ is endowed with the usual inner product $\langle X, Z\rangle = X^T Z = \sum_{i=1}^{n} x_i z_i$. Suppose Z is a unit vector in $\mathbb{R}^n$. Put $H = I - 2ZZ^T$. Then it is easy to see that H is a symmetric orthogonal matrix. Such a matrix H is usually called a *Householder matrix*.

Now $HX = (I - 2ZZ^T)X = X - 2Z(Z^T X)$. So geometrically, HX is just the reflection of X with respect to the space $\operatorname{span}\{Z\}^\perp$. (For the complex case, we consider $H = I - 2ZZ^*$, then H is Hermitian and unitary.)

Let $X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix}^T$ and $\boldsymbol{e}_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T$ be given. We would like to find a unit vector $Z = \begin{pmatrix} z_1 & z_2 & \cdots & z_n \end{pmatrix}^T$ such that Householder matrix $H = I - 2ZZ^T$ satisfies $HX = a\boldsymbol{e}_1$ for some $a \in \mathbb{R}$. Since H is orthogonal, $\|X\| = \|HX\| = \|a\boldsymbol{e}_1\| = |a|$. Thus, $|a| = \|X\|$ is a necessary condition.

Without loss of generality, we may assume $a > 0$. From $HX = a\boldsymbol{e}_1$ we have

$$X = H^T HX = H^2 X = H(a\boldsymbol{e}_1) = a(\boldsymbol{e}_1 - 2z_1 Z).$$

Comparing coordinates, we have

$$\begin{aligned} x_1 &= a(1 - 2z_1^2) \\ x_2 &= -2az_1 z_2 \\ &\vdots \\ x_n &= -2az_1 z_n. \end{aligned}$$

If $x_1 = a$, then $x_2 = \cdots = x_n = 0$. In this case choose $Z = \boldsymbol{e}_2$ and we are done.

Assume that $x_1 \neq a$, in fact $x_1 < a$. Then from the above equations we have $z_1 = \pm\sqrt{\frac{a - x_1}{2a}}$ and $z_i = -\frac{x_i}{2az_1}$ for $i = 2, 3, \ldots, n$. Now we choose $z_1 = -\sqrt{\frac{a-x_1}{2a}}$ and set $b = a(a - x_1)$. Then $-2az_1 = \sqrt{2a(a - x_1)} = \sqrt{2b}$. It follows that

$$Z = -\frac{1}{2az_1}\begin{pmatrix} -2az_1^2 & x_2 & \cdots & x_n \end{pmatrix}^T = \frac{1}{\sqrt{2b}}\begin{pmatrix} x_1 - a & x_2 & \cdots & x_n \end{pmatrix}^T.$$

Put $W = \begin{pmatrix} x_1 - a & x_2 & \cdots & x_n \end{pmatrix}^T$. Then $Z = \frac{1}{\sqrt{2b}}W$ and $\|W\| = \sqrt{2b}$. Therefore, $H = I - 2ZZ^T = I - \frac{1}{b}WW^T$ is a matrix such that $HX = a\boldsymbol{e}_1$. The matrix H defines the so-called *Householder transformation* which enables us to transform a matrix into the upper triangular form.

In general, given $X = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}^T$, we want to zero out the last $n-k$ components of X, $1 \leq k \leq n$. To do this, we write $X = \begin{pmatrix} X^{(1)} \\ X^{(2)} \end{pmatrix}$, where $X^{(1)} = \begin{pmatrix} x_1 & \cdots & x_{k-1} \end{pmatrix}^T$ and $X^{(2)} = \begin{pmatrix} x_k & \cdots & x_n \end{pmatrix}^T$. Then by the above argument, we construct an $(n-k+1) \times (n-k+1)$ Householder matrix $H_k^{(2)} = I^{(2)} - \frac{1}{b_k} W_k W_k^T$ satisfying $H_k^{(2)} X^{(2)} = \|X^{(2)}\| \boldsymbol{e}_1^{(2)}$, where $I^{(2)} = I_{n-k+1}$, W_k is a unit vector in $\mathbb{R}^{n-k+1}$ and $\boldsymbol{e}_1^{(2)} = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T$ in $\mathbb{R}^{n-k+1}$. Let $H_k = \begin{pmatrix} I^{(1)} & O \\ O & H_k^{(2)} \end{pmatrix}$, where $I^{(1)} = I_{k-1}$. Then $H_k X = \begin{pmatrix} I^{(1)} & O \\ O & H_k^{(2)} \end{pmatrix} \begin{pmatrix} X^{(1)} \\ X^{(2)} \end{pmatrix} = \begin{pmatrix} X^{(1)} \\ H_k^{(2)} X^{(2)} \end{pmatrix} = \begin{pmatrix} x_1 & \cdots & x_{k-1} & \sum_{i=k}^{n} x_i^2 & 0 & \cdots & 0 \end{pmatrix}^T$.

Let $Y = \begin{pmatrix} y_1 & \cdots & y_{k-1} & y_k & \cdots & y_n \end{pmatrix}^T$. Then $H_k Y = \begin{pmatrix} Y^{(1)} \\ H_k^{(2)} Y^{(2)} \end{pmatrix}$, where $Y^{(1)} = \begin{pmatrix} y_1 & \cdots & y_{k-1} \end{pmatrix}^T$ and $Y^{(2)} = \begin{pmatrix} y_k & \cdots & y_n \end{pmatrix}^T$. Thus H_k acts like the identity on the first $k-1$ coordinates of any vector Y. In particular, if $Y^{(2)} = \mathbf{0}$, then $H_k Y = Y$.

Example 10.5.30 Let $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$. Find a Householder matrix H so that HA is upper triangular.

Solution: First let $X = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $a = \|X\| = 1$, $x_1 = 0$ and $b = 1$. Thus $W = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$. Then $WW^T = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. So,

$$H_1 = I - \frac{1}{b} WW^T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } H_1 A = \left(\begin{array}{c|cc} 1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ 0 & -1 & 0 \end{array}\right).$$

Next we consider $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$. Let $X = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. In this case, $a = \|X\| = \sqrt{2}$ and $b = \sqrt{2}(\sqrt{2}-1) = 2 - \sqrt{2}$. Thus, $W = \begin{pmatrix} 1-\sqrt{2} \\ 1 \end{pmatrix}$ and $WW^T = \begin{pmatrix} (1-\sqrt{2})^2 & \sqrt{2}-1 \\ \sqrt{2}-1 & 1 \end{pmatrix}$.

$$I - \tfrac{1}{b} WW^T = \begin{pmatrix} \frac{\sqrt{2}-1}{2-\sqrt{2}} & -\frac{\sqrt{2}-1}{2-\sqrt{2}} \\ -\frac{\sqrt{2}-1}{2-\sqrt{2}} & -\frac{\sqrt{2}-1}{2-\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

So,

$$H_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & -1 \end{pmatrix}.$$

Therefore, $H_2 H_1 A = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & 0 & \sqrt{2} \\ 0 & 2 & 1 \\ 0 & 0 & -1 \end{pmatrix}$. □

We may also use Householder transformation to put an $m \times n$ real matrix A with $m \geq n$ into a matrix of the form R if $m = n$ and $\begin{pmatrix} R \\ O \end{pmatrix}$ if $m > n$, where R is an upper triangular matrix. We proceed as follows.

First, we find a Householder transformation $H_1 = I_m - \frac{1}{b_1} W_1 W_1^T$ which when applies to the first column of A gives a multiple of $\boldsymbol{e}_1$. Then $H_1 A$ has the form

$$\begin{pmatrix} * & * & \cdots & * \\ 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{pmatrix}.$$

Then we can find a Householder transformation H_2 that zeros out the last $m-2$ entries in the second column of $H_1 A$ while leaving the first entry in the second column and all the entries in the first column unchanged. Then $H_2 H_1 A$ is of the form

$$\begin{pmatrix} * & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ 0 & 0 & & & \\ \vdots & \vdots & & A_3 & \\ 0 & 0 & & & \end{pmatrix}.$$

Continuing in this fashion, we obtain at most $n-1$ Householder matrices $H_1, \ldots, H_{n-1}$ such that $H_{n-1} \cdots H_1 A = R$ if $m = n$. (Note that this yields an alternative method to find the QR decomposition.) If $m > n$, then we obtain at most n Householder matrix $H_1, \ldots, H_n$ such that $H_n \cdots H_1 A = \begin{pmatrix} R \\ O \end{pmatrix}$.

Theorem 10.5.31 *Let $A \in M_n(\mathbb{R})$. Then there exists $P = H_1 \cdots H_{n-2}$, a product of Householder matrices so that $H = PAP$ is of the Hessenberg form, i.e., $(H)_{i,j} = 0$ if $i > j + 1$.*

Proof: As in the above discussion, we find a Householder matrix H_1 which zeros out the last $n-2$ entries in the first column of A. Then $H_1 = \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & H' \end{pmatrix}$, where H' is an $(n-1) \times (n-1)$ matrix. It is easy to see that $H_1 A$ and $H_1 A H_1$ have the same first column. Thus applying this procedure to the second, third, ..., and $(n-2)$-th columns respectively, we obtain $H_2, \ldots, H_{n-2}$ so that $H_{n-2} \cdots H_1 A H_1 \cdots H_{n-2}$ has the desired form. □

Application – Singular value decomposition

Theorem 10.5.32 *Let $A \in M_{m,n}(\mathbb{R})$ with $m > n$. Then there exist an $m \times m$ orthogonal matrix U and an $n \times n$ orthogonal matrix V such that $U^T A V$ is of the form*

$$S = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \\ 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \quad \text{with } d_1 \geq d_2 \geq \cdots \geq d_n \geq 0.$$

Proof: Since A^TA is non-negative definite (see Exercise 9.6-4) , A^TA has non-negative eigenvalues, say $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$. Put $d_i = \sqrt{\lambda_i}$, $i = 1, 2, \ldots, n$. Suppose $\operatorname{rank}(A^TA) = r$, then $d_1 \geq d_2 \geq \cdots \geq d_r > 0$ and $d_{r+1} = \cdots = d_n = 0$. Since A^TA is symmetric, there is an orthogonal matrix V such that $V^TA^TAV = D$, an $n \times n$ diagonal matrix of the form $\operatorname{diag}\{d_1^2, \ldots, d_r^2, 0, \ldots, 0\}$. Let S be the $m \times n$ matrix $\begin{pmatrix} S_r & O \\ O & O \end{pmatrix}$, where S_r is an $r \times r$ diagonal matrix $\operatorname{diag}\{d_1, d_2, \ldots, d_r\}$. Then we have $D = S^TS$.

Let $V_1, \ldots, V_n$ be the columns of V. Then V_i is an eigenvector of A^TA with eigenvalue d_i^2 for $i = 1, 2, \ldots, r$ and $V_{r+1}, \ldots, V_n$ are eigenvectors corresponding to eigenvalue 0.

Let $V^{(1)} = \begin{pmatrix} V_1 & V_2 & \cdots & V_r \end{pmatrix}$ be the $n \times r$ matrix and $V^{(2)} = \begin{pmatrix} V_{r+1} & \cdots & V_n \end{pmatrix}$ be the $n \times (n-r)$ matrix. Clearly, $\big(V^{(1)}\big)^TV^{(1)} = I_r$ and $\big(V^{(2)}\big)^TV^{(2)} = I_{n-r}$. Since $A^TAV_i = \mathbf{0}$ for $i = r+1, \ldots, n$, we have

$$\big(AV^{(2)}\big)^TAV^{(2)} = \big(V^{(2)}\big)^TA^TAV^{(2)} = O$$

and hence $AV^{(2)} = O$. Since $A^TAV^{(1)} = V^{(1)}S_r^2$, we have

$$S_r^{-1}\big(V^{(1)}\big)^TA^TAV^{(1)}S_r^{-1} = I_r.$$

Now we put $U^{(1)} = AV^{(1)}S_r^{-1}$. Then $\big(U^{(1)}\big)^TU^{(1)} = I_r$. Hence $U^{(1)}$ is an $m \times r$ matrix with orthonormal columns $U_1, \ldots, U_r$, say. Extend $\{U_1, \ldots, U_r\}$ to an orthonormal basis $\{U_1, \ldots, U_r, \ldots, U_m\}$ of $\mathbb{R}^m$. Let $U = \begin{pmatrix} U_1 & \cdots & U_m \end{pmatrix}$ be the $m \times m$ matrix and $U^{(2)} = \begin{pmatrix} U_{r+1} & \cdots & U_m \end{pmatrix}$ be the $m \times (m-r)$ matrix. Thus $U = \begin{pmatrix} U^{(1)} & U^{(2)} \end{pmatrix}$. Now we consider

$$\begin{aligned} U^TAV &= \begin{pmatrix} \big(U^{(1)}\big)^T \\ \big(U^{(2)}\big)^T \end{pmatrix} A \begin{pmatrix} V^{(1)} & V^{(2)} \end{pmatrix} = \begin{pmatrix} \big(U^{(1)}\big)^T \\ \big(U^{(2)}\big)^T \end{pmatrix} \begin{pmatrix} AV^{(1)} & AV^{(2)} \end{pmatrix} \\ &= \begin{pmatrix} \big(U^{(1)}\big)^T \\ \big(U^{(2)}\big)^T \end{pmatrix} \begin{pmatrix} AV^{(1)} & O \end{pmatrix} = \begin{pmatrix} \big(U^{(1)}\big)^TAV^{(1)} & O \\ \big(U^{(2)}\big)^TAV^{(1)} & O \end{pmatrix}. \end{aligned}$$

Since $\big(U^{(1)}\big)^TAV^{(1)} = S_r^{-1}\big(V^{(1)}\big)^TA^TAV^{(1)} = S_r$ and $\big(U^{(2)}\big)^TAV^{(1)} = \big(U^{(2)}\big)^TU^{(1)}S_r = O$, we have $U^TAV = \begin{pmatrix} S_r & O \\ O & O \end{pmatrix}$. □

Remark 10.5.33

(1) Since the diagonal entries of S are non-negative square roots of the eigenvalues of A^TA, hence are unique. The d_i's are called *singular values* of A and the factorization $A = USV^T$ is called the *singular value decomposition* (SVD) of A.

(2) The matrices U and V are not unique as we can easily see from the proof of Theorem 10.5.32.

(3) Since $U^TAA^TU = SS^T$ is diagonal, U diagonalizes AA^T and hence the columns of U are eigenvectors of AA^T.

(4) Since

$$\begin{pmatrix} AV_1 & \cdots & AV_n \end{pmatrix} = A\begin{pmatrix} V_1 & \cdots & V_n \end{pmatrix} = AV = US$$

$$= \begin{pmatrix} U_1 & \cdots & U_m \end{pmatrix} \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \\ 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} = \begin{pmatrix} d_1U_1 & \cdots & d_nU_n \end{pmatrix},$$

we have $AV_j = d_jU_j$ for $j = 1, 2, \ldots, n$.

Also from the matrix equation $A^TU = VS^T$ we have

$$\begin{aligned} A^TU_j &= d_jV_j \quad \text{for } j = 1, 2, \ldots, n; \\ A^TU_j &= \mathbf{0} \qquad \text{for } j = n+1, \ldots, m. \end{aligned}$$

Therefore, $AA^TU_j = d_jAV_j = d_j^2U_j = \lambda_jU_j$ for $j = 1, 2, \ldots, n$ and $AA^TU_j = \mathbf{0}$ for $j = n+1, \ldots, m$. Hence U_j for $j = 1, 2, \ldots, m$ are eigenvectors of AA^T and for $j = n+1, \ldots, m$, U_j's are eigenvectors corresponding to eigenvalue 0.

Example 10.5.34 Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}$. We want to compute the singular values and the singular value decomposition of A.

$A^TA = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$ has eigenvalues 4 and 0. Consequently, the singular values of A are 2 and 0. An eigenvector corresponding to 4 is $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and an eigenvector corresponding to 0 is $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Then the orthogonal matrix $V = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ diagonalizes A^TA.

Let $U_1 = AV_1S_1^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}\left(\frac{1}{2}\right) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$. The remaining columns of U must be eigenvectors of AA^T corresponding to the eigenvalue 0.

Now $AA^T = \begin{pmatrix} 2 & 2 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ has $U_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$ and $U_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ as eigenvectors whose eigenvalues are 0. Then

$$A = USV^T = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

is a singular value decomposition of A. □

Example 10.5.35 Find a singular value decomposition of $A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$.

Here $m = 4$, $n = 3$ and $A^TA = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 5 & 4 \\ 0 & 4 & 5 \end{pmatrix}$. Then the characteristics polynomial of A^TA is $-(x-4)(x-1)(x-9)$. Thus the eigenvalues are $9, 4$ and 1 and the singular values are $3, 2$ and 1.

A unit eigenvector corresponding to 9 is $V_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$. A unit eigenvector corresponding to 4 is $V_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. A unit eigenvector corresponding to 1 is $V_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$. Then $V^{(1)} = V = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & \sqrt{2} & 0 \\ 1 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix}$ diagonalizes A^TA. Since $S_3 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $S_3^{-1} = \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$. So we obtain

$$U^{(1)} = AV^{(1)}S_3^{-1} = AVS_3^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & \sqrt{2} & 0 \\ 1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix}.$$

To obtain U_4 we have to find an eigenvector corresponding to the zero eigenvalue of AA^T. Now $AA^T = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 5 & 4 & 0 \\ 0 & 4 & 5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. From this, we obtain $U_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ as a unit eigenvector corresponding to 0. Thus, we have $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & \sqrt{2} & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & \sqrt{2} \end{pmatrix}$. □

For complex matrices, we consider A^*A instead of A^TA and proceed as in the real case with proper modifications.

Exercise 10.5

10.5-1. Show that every real skew-symmetric matrix is normal. Find a complex symmetric matrix which is not normal.

10.5-2. Find an orthogonal transformation to reduced the quadratic form $x^2 + 6xy - 2y^2 - 2yz + z^2$ to diagonal form.

10.5-3. Let $A = \begin{pmatrix} 8 & 4 & -1 \\ 4 & -7 & 4 \\ -1 & 4 & 8 \end{pmatrix}$. Find an orthogonal matrix P such that P^TAP is diagonal.

10.5-4. Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(a) Find an orthogonal matrix P such that $P^T AP$ is diagonal.

(b) Compute e^A.

10.5-5. Let $A = \begin{pmatrix} 1 & i & 0 \\ -i & 1 & i \\ 0 & -i & 1 \end{pmatrix}$. Find a unitary matrix U such that $U^* AU$ is diagonal.

10.5-6. Let $A = \frac{1}{3}\begin{pmatrix} 2 & -2 & 1 \\ 2 & 1 & -2 \\ 1 & 2 & 2 \end{pmatrix}$. Find a unitary matrix U such that $U^* AU$ is diagonal.

10.5-7. $A = \begin{pmatrix} 0 & 1 & -3 & 0 \\ 1 & 0 & 0 & -3 \\ -3 & 0 & 0 & 1 \\ 0 & -3 & 1 & 0 \end{pmatrix}$. Find an orthogonal matrix P such that $P^T AP$ is diagonal.

10.5-8. Let A and B be real symmetric matrices with A positive definite. For real x, define the polynomial $f(x) = \det(B - xA)$. Show that there exist an invertible matrix Q such that $Q^T AQ = I$ and $Q^T BQ$ is a diagonal matrix whose diagonal elements are roots of $f(x)$.

10.5-9. Show that every real skew-symmetric matrix has the form $A = P^T BP$ where P is orthogonal and B^2 is a diagonal.

10.5-10. Show that every non-zero real skew-symmetric matrix cannot be orthogonal similar to a diagonal matrix.

10.5-11. Show that the eigenvalues of a normal matrix A are all equal if and only if A is a scalar multiple of the identity matrix.

10.5-12. Let $W = \begin{pmatrix} 9 \\ 1 \\ 5 \\ 1 \end{pmatrix}$. Find H the Householder matrix defined by W. Also find the reflection of $X = \begin{pmatrix} 3 \\ 1 \\ 5 \\ 1 \end{pmatrix}$ with respect to subspace $\text{span}(W)^{\perp}$.

10.5-13. Prove that if A is a real symmetric matrix with eigenvalues $\lambda_1, \ldots, \lambda_n$, then the singular values of A are $|\lambda_1|, \ldots, |\lambda_n|$.

10.5-14. Find the singular value decomposition of $\begin{pmatrix} 1 & 3 \\ 3 & 1 \\ 0 & 0 \end{pmatrix}$.

10.5-15. Show that if A is a real symmetric positive define matrix, then there is an upper triangular matrix R such that $A = R^T R$.

10.5-16. Suppose that A has eigenvalues 0, 1 and 2 corresponding to eigenvectors $\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, respectively. Find A. Is A normal? Why?

10.5-17. Show that Theorem 10.5.5 is false if σ is not normal.

10.5-18. Show that if A is normal and $A^k = O$ for some positive integer k, then $A = O$.

10.5-19. Show that the product of two upper triangular matrices is upper triangular. Also, show that the inverse of an invertible upper triangular matrix is upper triangular. Hence show that each symmetric positive definite matrix A has the factorization $A = LL^T$, where L^T is upper triangular.

Appendices

§A.1 Greatest Common Division

Proof of Theorem 0.2.6: Applying the Division Algorithm repeatedly, since $r_i \geq 0$ and $b > r_1 > r_2 > \cdots$, the process will stop. Thus we obtain recurrence relations (0.1).

By Lemma 0.2.5,

$$(a,b) = (a - bq_1, b) = (r_1, b) = (r_1, b - r_1q_2) = (r_1, r_2) = (r_1 - r_2q_3, r_2) = (r_3, r_2).$$

Continuing this process, we get $(a,b) = (r_{n-1}, r_n) = (r_n, 0) = r_n$.

Since

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix}, \quad \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix},$$
$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} \quad \cdots, \quad \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix},$$
$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} q_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n \\ 0 \end{pmatrix},$$

we have

$$\begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \quad \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix},$$
$$\begin{pmatrix} r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_3 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}, \quad \cdots, \quad \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix},$$
$$\begin{pmatrix} r_n \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n+1} \end{pmatrix} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}.$$

Therefore,

$$\begin{pmatrix} r_n \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

for some $s, t, u, v \in \mathbb{Z}$. This completes the proof. □

Proof of Remark 0.2.8: From the proof of Theorem 0.2.6, for $0 \leq i \leq n$, we have

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

for some $s_i, t_i, u_i, v_i \in \mathbb{Z}$, where $r_0 = b$, $\begin{pmatrix} s_0 & t_0 \\ u_0 & v_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$ and

$$\begin{pmatrix} s_i & t_i \\ u_i & v_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} s_{i-1} & t_{i-1} \\ u_{i-1} & v_{i-1} \end{pmatrix} = \begin{pmatrix} u_{i-1} & v_{i-1} \\ s_{i-1} - q_{i+1}u_{i-1} & t_{i-1} - q_{i+1}v_{i-1} \end{pmatrix}.$$

For convenience, let $s_{-1} = 1$, $s_0 = 0$, $t_{-1} = 0$ and $t_0 = 1$, then the above equation holds for $0 \leq i \leq n$. So we have

$$s_i = u_{i-1}, t_i = v_{i-1}, u_i = s_{i-1} - q_{i+1}u_{i-1}, \text{ and } v_i = t_{i-1} - q_{i+1}v_{i-1}.$$

Then we have

$$s_i = s_{i-2} - q_i u_{i-2} = s_{i-2} - q_i s_{i-1}, 1 \leq i \leq n.$$

Similarly,

$$t_i = t_{i-2} - q_i t_{i-1}, 1 \leq i \leq n.$$

Then g.c.d.$(a, b) = r_n = as_n + bt_n$. □

§A.2 Block Matrix Multiplication

Theorem A.2.1 *Let $A \in M_{m,n}(\mathbb{F})$ and $B \in M_{n,p}(\mathbb{F})$. Suppose A and B are partitioned as follows:*

$$A = \left(\begin{array}{c|c|c} A^{1,1} & \cdots & A^{1,s} \\ \hline \vdots & \vdots & \vdots \\ \hline A^{r,1} & \cdots & A^{r,s} \end{array}\right), \qquad B = \left(\begin{array}{c|c|c} B^{1,1} & \cdots & B^{1,t} \\ \hline \vdots & \vdots & \vdots \\ \hline B^{s,1} & \cdots & B^{s,t} \end{array}\right),$$

where each $A^{i,j}$ is an $m_i \times n_j$ submatrices of A, each $B^{j,k}$ is an $n_j \times p_k$ submatrices of B, $m = m_1 + \cdots + m_r$, $n = n_1 + \cdots + n_s$ and $p = p_1 + \cdots p_t$ for some positive integers r, s, t. Let $C = AB$. Then there are $C^{i,k} = \sum_{j=1}^{s} A^{i,j}B^{j,k} \in M_{m_i,p_k}(\mathbb{F})$ such that $C = \left(\begin{array}{c|c|c} C^{1,1} & \cdots & C^{1,t} \\ \hline \vdots & \vdots & \vdots \\ \hline C^{r,1} & \cdots & C^{r,t} \end{array}\right)$, $1 \leq i \leq r$, $1 \leq k \leq t$.

Proof: To prove this theorem, we first define a number $q(A, B) = r + s + t$. Clearly $q(A, B) \geq 3$.

We shall prove the theorem by induction on $q(A, B)$.

When $q(A, B) = 3$. Then $r = s = t = 1$. The theorem is always true.

When $q(A, B) = 4$. Then there are 3 cases as below:

Case 1: Suppose $t = 2$, $s = r = 1$. Then $B = \begin{pmatrix} B_1 & B_2 \end{pmatrix}$, where

$$B_1 = \begin{pmatrix} B_{*1} & \cdots & B_{*p_1} \end{pmatrix} \in M_{n,p_1}(\mathbb{F}) \text{ and } B_2 = \begin{pmatrix} B_{*(p_1+1)} & \cdots & B_{*p} \end{pmatrix} \in M_{n,p_2}(\mathbb{F}).$$

Thus,

$$\begin{aligned} AB &= A \begin{pmatrix} B_{*1} & \cdots & B_{*p_1} & B_{*(p_1+1)} & \cdots & B_{*p} \end{pmatrix} \\ &= \begin{pmatrix} AB_{*1} & \cdots & AB_{*p_1} & AB_{*(p_1+1)} & \cdots & AB_{*p} \end{pmatrix} = \begin{pmatrix} AB_1 & AB_2 \end{pmatrix}. \end{aligned}$$

Let $C^{1,1} = AB_1$ and $C^{1,2} = AB_2$. Then we have the theorem for this case.

Case 2: Suppose $r = 2$, $s = t = 1$. Then $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$. Consider $C^T = (AB)^T = B^T A^T$. By Case 1 we have $C^T = \begin{pmatrix} B^T(A_1)^T & B^T(A_2)^T \end{pmatrix}$. Thus $C = \begin{pmatrix} A_1B \\ A_2B \end{pmatrix}$. So by putting $C^{1,1} = A_1B$ and $C^{2,1} = A_2B$ we have the theorem for this case.

Case 3: Suppose $s = 2$, $r = t = 1$. Then $A = \begin{pmatrix} A_1 & A_2 \end{pmatrix}$ and $B = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$, where A_1, A_2, B_1 and B_2 are $m \times n_1$, $m \times n_2$, $n_1 \times p$ and $n_2 \times p$ matrices respectively. Then

$$(C)_{i,k} = \sum_{j=1}^{n} (A)_{i,j}(B)_{j,k} = \sum_{j=1}^{n_1} (A)_{i,j}(B)_{j,k} + \sum_{j=n_1+1}^{n} (A)_{i,j}(B)_{j,k}.$$

Now

$$\sum_{j=1}^{n_1} (A)_{i,j}(B)_{j,k} = (A_1B_1)_{i,k} \text{ and } \sum_{j=n_1+1}^{n} (A)_{i,j}(B)_{j,k} = (A_2B_2)_{i,k}.$$

So we have

$$(C)_{i,k} = (A_1B_1 + A_2B_2)_{i,k}$$

and hence $C = C^{1,1} = A_1B_1 + A_2B_2$.

Thus, the theorem holds for $q(A, B) = 4$.

Suppose the theorem holds for $q(A, B) \leq q$, where $q \geq 4$. Now we assume $q(A, B) = q + 1$. Then one of r, s and t must be greater than 1.

Case 1: Suppose $t \geq 2$. Then we rewrite B as $B = \begin{pmatrix} B_1 & B_2 \end{pmatrix}$, where

$$B_1 = \begin{pmatrix} B^{1,1} & \cdots & B^{1,t-1} \\ \vdots & \vdots & \vdots \\ B^{s,1} & \cdots & B^{s,t-1} \end{pmatrix} \text{ and } B_2 = \begin{pmatrix} B^{1,t} \\ \vdots \\ B^{s,t} \end{pmatrix}.$$

Then $AB = A\begin{pmatrix} B_1 & B_2 \end{pmatrix}$. In this case, $q(A, B) = 1 + 1 + 2 = 4$. By induction $AB = \begin{pmatrix} AB_1 & AB_2 \end{pmatrix}$.

Since $q(A, B_1) = r + s + (t - 1) = q$, by induction again

$$C = \left(\begin{array}{c|c|c} C^{1,1} & \cdots & C^{1,t-1} \\ \hline \vdots & \vdots & \vdots \\ \hline C^{r,1} & \cdots & C^{r,t-1} \end{array}\right)$$

where $C^{i,k} = \sum_{j=1}^{s} A^{i,j}B^{j,k} \in M_{m_i,p_k}(\mathbb{F})$ for $1 \leq i \leq r$ and $1 \leq k \leq t - 1$.

Similarly, since $q(A, B_2) = r + s + 1 \leq q$, we have

$$AB_2 = \begin{pmatrix} C^{1,t} \\ \vdots \\ C^{r,t} \end{pmatrix}, \text{ where } C^{i,t} = \sum_{j=1}^{s} A^{i,j}B^{j,t} \in M_{m_i,p_t}(\mathbb{F}),$$

for $1 \leq i \leq r$.

Combine these two results we have the theorem for this case.

Case 2: Suppose $r \geq 2$. Then consider $C^T = B^T A^T$. We will get the result.

Case 3: Suppose $r = t = 1$ and $s \geq 2$. Then

$$A = \left(\begin{array}{ccc|c} A^{1,1} & \cdots & A^{1,s-1} & A^{1,s} \end{array} \right) \text{ and } B = \left(\begin{array}{c} B^{1,1} \\ \vdots \\ \hline B^{s,1} \end{array} \right).$$

We rewrite $A = \begin{pmatrix} A_1 & A^{1,s} \end{pmatrix}$ and $B = \begin{pmatrix} B_1 \\ B^{s,1} \end{pmatrix}$. By induction $AB = A_1B_1 + A^{1,s}B^{s,t}$. Since $q(A_1, B_1) = 1 + (s-1) + 1 = s + 1 = q$, by induction $A_1B_1 = \sum_{j=1}^{s-1} A^{1,j}B^{j,1}$. Thus we have $C = C^{1,1} = \sum_{j=1}^{s} A^{1,j}B^{j,1}$.

Therefore, by induction the theorem holds for $q(A, B) \geq 3$. □

§A.3 Jacobian Matrix

In finite dimensional calculus we define the derivative of a mapping f from $\mathbb{R}^n$ into $\mathbb{R}^m$ as a linear transformation.

Suppose $f : \mathbb{R}^n \to \mathbb{R}^m$ is a mapping. f is said to be *differentiable* at $\boldsymbol{x} \in \mathbb{R}^n$ if there exists a linear transformation $\sigma_{\boldsymbol{x}} \in L(\mathbb{R}^n, \mathbb{R}^m)$ such that for $\boldsymbol{h} \in \mathbb{R}^n \setminus \{\boldsymbol{0}\}$ we have

$$\frac{\|f(\boldsymbol{x} + \boldsymbol{h}) - f(\boldsymbol{x}) - \sigma_{\boldsymbol{x}}(\boldsymbol{h})\|_m}{\|\boldsymbol{h}\|_n} \to 0 \text{ as } \|\boldsymbol{h}\|_n \to 0.$$

Here $\|\cdot\|_m$ and $\|\cdot\|_n$ are the usual norms of $\mathbb{R}^m$ and $\mathbb{R}^n$, respectively. One can easily check that if such $\sigma_{\boldsymbol{x}}$ exists then it is unique and we shall denote it by $Df(\boldsymbol{x})$.

Definition A.3.1 Let $f : \mathbb{R}^n \to \mathbb{R}^m$ be a mapping and $\boldsymbol{x} \in \mathbb{R}^n$. Let $\boldsymbol{h}$ be a unit vector in $\mathbb{R}^n$. Then the *directional derivative of f at $\boldsymbol{x}$ in the direction $\boldsymbol{h}$*, denoted by $D_{\boldsymbol{h}}f(\boldsymbol{x})$, is defined by

$$D_{\boldsymbol{h}}f(\boldsymbol{x}) = \lim_{t \to 0} \frac{f(\boldsymbol{x} + t\boldsymbol{h}) - f(\boldsymbol{x})}{t}.$$

Proposition A.3.2 *Let $f : \mathbb{R}^n \to \mathbb{R}^m$ be differentiable at $\boldsymbol{x}$. Then for each unit vector $\boldsymbol{h} \in \mathbb{R}^n$, $D_{\boldsymbol{h}}f(\boldsymbol{x})$ exists and $D_{\boldsymbol{h}}f(\boldsymbol{x}) = \big(Df(\boldsymbol{x})\big)(\boldsymbol{h})$.*

In particular, if $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ and $\boldsymbol{h} = \boldsymbol{e}_j$ in $\mathbb{R}^n$, then $D_{\boldsymbol{e}_j}f(\boldsymbol{x})$ is the usual partial derivative with respect to x_j.

Proposition A.3.3 *Let $f : \mathbb{R}^n \to \mathbb{R}^m$ be a mapping. Suppose that for $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, $f(\boldsymbol{x}) = (f_1(\boldsymbol{x}), \ldots, f_m(\boldsymbol{x}))$. Let $\mathscr{A} = \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ and $\mathscr{B} = \{\boldsymbol{e}_1^*, \ldots, \boldsymbol{e}_m^*\}$ be standard bases of $\mathbb{R}^n$ and $\mathbb{R}^m$ respectively. If f is differentiable at $\boldsymbol{x}_0$, then*

$$[Df(\boldsymbol{x}_0)]_{\mathscr{B}}^{\mathscr{A}} = \left(\frac{\partial f_i(\boldsymbol{x}_0)}{\partial x_j} \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}.$$

Proof: Let $[Df(\boldsymbol{x}_0)]_{\mathscr{B}}^{\mathscr{A}} = (a_{ij})$. Then $Df(\boldsymbol{x}_0)(\boldsymbol{e}_j) = \sum_{i=1}^{m} a_{ij}\boldsymbol{e}_i^*$, $1 \le j \le n$. Since

$$Df(\boldsymbol{x}_0)(\boldsymbol{e}_j) = D_{\boldsymbol{e}_j} f(\boldsymbol{x}_0) = \left(\frac{\partial f_1(\boldsymbol{x}_0)}{\partial x_j}, \cdots, \frac{\partial f_m(\boldsymbol{x}_0)}{\partial x_j} \right) = \sum_{i=1}^{m} \frac{\partial f_i(\boldsymbol{x}_0)}{\partial x_j} \boldsymbol{e}_i^*.$$

Thus $a_{ij} = \dfrac{\partial f_i(\boldsymbol{x}_0)}{\partial x_j}$ for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. □

The matrix $[Df(\boldsymbol{x})]_{\mathscr{B}}^{\mathscr{A}}$ is called the *Jacobian matrix of f at $\boldsymbol{x}$*.

Corollary A.3.4 *If $f : \mathbb{R}^n \to \mathbb{R}$ is differentiable at $\boldsymbol{x}$. Then with respect to the standard bases of $\mathbb{R}^n$ and $\mathbb{R}$, $Df(\boldsymbol{x})$ has representing matrix*

$$\begin{pmatrix} \frac{\partial f(\boldsymbol{x})}{\partial x_1} \\ \vdots \\ \frac{\partial f(\boldsymbol{x})}{\partial x_n} \end{pmatrix}.$$

Remark A.3.5 With the same notation as above, $Df(\boldsymbol{x})$ is a linear functional on $\mathbb{R}^n$. By Theorem 10.2.1 there exists a unique vector denoted by $\nabla f(\boldsymbol{x}) \in \mathbb{R}^n$ such that $Df(\boldsymbol{x})(\boldsymbol{v}) = \nabla f(\boldsymbol{x}) \cdot \boldsymbol{v}$. Here $\boldsymbol{v} \in \mathbb{R}^n$ and " $\cdot$ " is the usual dot product in $\mathbb{R}^n$. $\nabla f(\boldsymbol{x})$ is called the *gradient vector of f at $\boldsymbol{x}$*. In standard basis of $\mathbb{R}^n$, $\nabla f(\boldsymbol{x}) = \left(\dfrac{\partial f}{\partial x_1}, \ldots, \dfrac{\partial f}{\partial x_n} \right)$.

Numerical Answers

Chapter 0

Exercise 0.2

0.2-1. (a)

i	-1	0	1	2	3	4	5
$-q_i$			-14	-1	-1	-16	-2
s_i	1	0	1	-1	2	-33	68
t_i	0	1	-14	15	-29	479	-987

$s = -33$, $t = 479$

(b)

i	-1	0	1	2	3	4	5	6	7
$-q_i$			-2	-3	-1	-5	-4	-1	-2
s_i	1	0	1	-3	4	-23	96	-119	334
t_i	0	1	-2	7	-9	52	-217	269	-755

$s = -119$, $t = 269$

0.2-2. (a)

i	-1	0	1	2	3	4
$-q_i$			-1	-2	-2	-10
s_i	1	0	1	-2	5	-52
t_i	0	1	-1	3	-7	73

$x = 5$, $y = 7$

(b)

i	-1	0	1	2	3	4
$-q_i$			-1	-4	-2	-2
s_i	1	0	1	-4	9	-22
t_i	0	1	-1	5	-11	27

$x = -11$, $y = 9$

(c) $x = -4$, $y = 4$, $z = 1$

Exercise 0.4

0.4-1. The inverse of 32 is 44; the inverse of 47 is 10

0.4-4. 8:00am

0.4-6. $z = 17$

0.4-7. $z = 123 + 385s \ \forall s \in \mathbb{N}_0$

Exercise 0.5

0.5-4. $(x^2-2)(x^2+2)$ over $\mathbb{Q}$; $(x-\sqrt{2})(x+\sqrt{2})(x^2+2)$ over $\mathbb{R}$; $(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}i)(x+\sqrt{2}i)$ over $\mathbb{C}$

0.5-5. $(x-2)(x+2)(x^2+4)$ over $\mathbb{Q}$; $(x-2)(x+2)(x^2+4)$ over $\mathbb{R}$; $(x-2)(x+2)(x-2i)(x+2i)$ over $\mathbb{C}$

0.5-7.

x	$+1$	x^4	$+x^3$	$+2x^2$	$+x$	-1	x^3	$+1$	$\frac{1}{2}x$
		x^4	$+x^3$		$+x$	$+1$	x^3 $-x$		
$2x$				$2x^2$		-2	x	$+1$	$-\frac{1}{2}$
				$2x^2$	$+2x$		x	$+1$	
					$-2x$	-2		0	

-1	0	1	2	3	4
		$-x-1$	$-\frac{1}{2}x$	$-2x$	$\frac{1}{2}$
1	0	1	$-\frac{1}{2}x$	x^2+1	$\frac{1}{2}x^2-\frac{1}{2}x+\frac{1}{2}$
0	1	$-x-1$	$\frac{1}{2}x(x+1)+1$	$-x^3-x^2-3x-1$	$-\frac{1}{2}x^3-x+\frac{1}{2}$

Then $(x^2+1)g(x)+(-x^3-x^2-3x-1)f(x)=-2x-2$

Chapter 1

Exercise 1.2

1.2-1. (a) $\begin{pmatrix} 4 & -2 & -6 \\ -8 & -2 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 4 & 10 & 6 \\ -8 & 1 & 3 \end{pmatrix}$

(c) It cannot work, since the size of B is different from C

(d) It cannot work, since the size of BC is different from CB

(e) $\begin{pmatrix} 8 & 36 \\ 2 & 9 \end{pmatrix}$

(f) $\begin{pmatrix} 20 & 2 & -6 \\ 2 & 2 & 3 \\ -6 & 3 & 9 \end{pmatrix}$

(g) $\begin{pmatrix} 6 & -3 & -3 \\ -24 & 6 & 9 \end{pmatrix}$

1.2-2. $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ k & 0 & 1 & 0 \\ 0 & k & 0 & 1 \end{pmatrix}$

1.2-3. $AA^T=(a^2+b^2+c^2+d^2)I_4=A^TA$

1.2-4. $\sum_{i=0}^{r-1}\binom{k}{i}N^i$ (since $IN=NI$)

1.2-5. $\sum_{i=0}^{r-1} \binom{k}{i} A^{k-i} N^i$

1.2-14. $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$

1.2-15. $\mathrm{Tr}(A) = 15$, $\mathrm{Tr}(AB) = 8$, $\mathrm{Tr}(AB) = 107$, $\mathrm{Tr}(BA) = 107$

Exercise 1.3

1.3-2. $-\frac{1}{a_0}(a_1 I + a_2 A + \cdots + a_m A^{m-1})$

1.3-3. (a) $\begin{pmatrix} 3 & 16 & -9 \\ 0 & 69 & -41 \\ 0 & -41 & 28 \end{pmatrix}$

(b) $(A^3 - A + I)^{-1} = A^{-1} = -A^2 + 2I = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

1.3-7. $\begin{pmatrix} -\frac{1}{4} & \frac{3}{4} & 0 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

1.3-8. $\begin{pmatrix} 0 & 0 & 0 & \frac{1}{4} & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$

Exercise 1.5

1.5-2. $\begin{pmatrix} 1 & 0 & 0 & 0 & -\frac{736}{85} \\ 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & \frac{11}{85} \\ 0 & 0 & 0 & 1 & \frac{139}{85} \end{pmatrix}$

1.5-3. I_4

1.5-4. $\mathrm{rref}(A) + \mathrm{rref}(B) = \begin{pmatrix} 2 & 0 & 5 & \frac{32}{31} \\ 0 & 2 & -1 & -\frac{23}{31} \\ 0 & 0 & 1 & \frac{51}{31} \end{pmatrix}$, $\mathrm{rref}(A+B) = \begin{pmatrix} 1 & 0 & 0 & -\frac{23}{71} \\ 0 & 1 & 0 & \frac{5}{71} \\ 0 & 0 & 1 & \frac{70}{71} \end{pmatrix}$

1.5-5. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & * & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Chapter 2

Exercise 2.2

2.2-1. $\begin{pmatrix} 9 & 0 & 1 \\ 0 & 8 & 4 \\ 1 & 2 & 8 \end{pmatrix}$

2.2-2. $\begin{pmatrix} -2 & 0 & 1 \\ 0 & -3 & 4 \\ 1 & 2 & -3 \end{pmatrix}$

2.2-3. $\begin{pmatrix} 2 & 0 & 1 \\ 0 & 3 & 0 \\ 1 & 0 & 2 \end{pmatrix}$

Exercise 2.4

2.4-1. (a) 3

(b) 3

(c) 2

2.4-2. (a) $\{(0,0,0,0)\}$

(b) $\{(1,2,t,\frac{193-4t}{10},\frac{69-2t}{2}) \mid t \in \mathbb{R}\}$

Exercise 2.5

2.5-1. (a) $P = \begin{pmatrix} -\frac{4}{15} & \frac{2}{5} & -\frac{1}{3} \\ \frac{1}{3} & 0 & -\frac{1}{3} \\ \frac{2}{15} & -\frac{1}{5} & \frac{2}{3} \end{pmatrix}$, $Q = \begin{pmatrix} -\frac{4}{15} & \frac{2}{15} & -\frac{1}{3} & 1 \\ \frac{1}{3} & 0 & -\frac{1}{3} & -1 \\ \frac{2}{15} & -\frac{1}{5} & \frac{2}{3} & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(b) $P = \begin{pmatrix} \frac{1}{7} & 0 & 0 & -\frac{2}{7} \\ \frac{1}{7} & -\frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ 0 & \frac{1}{5} & \frac{2}{5} & \frac{9}{35} \\ -\frac{2}{7} & \frac{1}{5} & -\frac{8}{5} & \frac{16}{35} \end{pmatrix}$, $Q = \begin{pmatrix} \frac{1}{7} & 0 & -\frac{3}{7} & \frac{10}{7} \\ \frac{1}{7} & -\frac{1}{5} & \frac{6}{35} & \frac{1}{35} \\ 0 & \frac{1}{5} & \frac{2}{5} & -\frac{8}{5} \\ -\frac{2}{7} & \frac{1}{5} & \frac{9}{35} & -\frac{16}{35} \end{pmatrix}$

(c) $P = \begin{pmatrix} -\frac{13}{14} & -\frac{5}{7} & \frac{12}{7} \\ \frac{5}{14} & \frac{4}{7} & -\frac{3}{7} \\ -\frac{5}{7} & \frac{1}{7} & \frac{6}{7} \\ \frac{1}{14} & \frac{2}{7} & \frac{2}{7} \\ \frac{3}{14} & -\frac{1}{7} & \frac{1}{7} \end{pmatrix}$, $Q = \begin{pmatrix} -\frac{1}{9} & -\frac{1}{9} & \frac{5}{18} \\ \frac{2}{9} & \frac{2}{9} & -\frac{1}{18} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{3}{8} \end{pmatrix}$

2.5-5. $M = \begin{pmatrix} 25 & 15 & 21 & 0 \\ 8 & 1 & 22 & 5 \\ 0 & 23 & 15 & 14 \end{pmatrix}$. "you have won"

Chapter 3

Exercise 3.3

3.3-1. (a), (b), (c) and (e) are linearly independent sets.
For (d), $(2,0,1) = 5(1,1,0) - 2(0,1,1) - 3(1,1,-1)$

3.3-2. $(1,2,3,0)^T = (1,1,2,-1)^T + (1,0,1,1)^T + (-1,1,0,0)^T$

3.3-3. $a = 1$ or 2

3.3-9. $\{\beta_1, \beta_2, \beta_3\}$ is linearly independent if and only if $ab + a + b \neq 0 \ \forall a, b \in \mathbb{R}$

3.3-10. $V = \text{span}\{(1,0)\}$ and $W = \text{span}\{(0,1)\}$

Exercise 3.5

3.5-1. $\{(1,0,0,-1),\ (0,1,0,3),\ (0,0,1,-2)\}$

3.5-2. $R(A) = \text{span}\{(1,0,0,0,2,0),\ (0,1,1,0,-1,0)\ (0,0,0,1,1,0),\ (0,0,0,0,0,1)\}$
$C(A) = \text{span}\{(1,0,0,0)^T,\ (0,1,0,0)^T\ (0,0,1,0)^T,\ (0,0,0,1)^T\}$

Exercise 3.6

3.6-1. We choose $\{(1,1,1,3),\ (1,-2,4,0),\ (2,0,5,3),\ (3,4,6,1)\}$ as a basis. Then
$(0,3,2,-2) = \frac{17}{3}(1,1,1,3) - \frac{13}{3}(1,-2,4,0) + 5(2,0,5,3)$
$(1,3,5,7) = -\frac{181}{21}(1,1,1,3) - \frac{170}{21}(1,-2,4,0) + \frac{74}{7}(2,0,5,3) - \frac{8}{7}(3,4,6,-1)$

3.6-2. By using row operation,
$$\left(\begin{array}{ccc|c} 1 & 2 & 5 & \\ 1 & 3 & 3 & \\ -1 & -4 & -3 & I_4 \\ 2 & 2 & 3 & \end{array}\right) \text{ becomes } \left(\begin{array}{ccc|cccc} 1 & 2 & 5 & 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0.5 & -1 & -0.5 & 0 \\ \hline 0 & 0 & 0 & 1.5 & -9 & -5.5 & 1 \end{array}\right).$$
So $A = \begin{pmatrix} 1.5 & -9 & -5.5 & 1 \end{pmatrix}$ or equivalently $A = \begin{pmatrix} 3 & -18 & -11 & 2 \end{pmatrix}$

3.6-3. $\{(1,1,0,\ (-1,2,1),\ (0,1,0)\}$

3.6-4. $\{(1,1,0,1),\ (-1,0,1,1,),\ (0,0,1,0),\ (0,0,0,1)\}$

3.6-5. $\{(1,-2,0,1),\ (1,0,0,1),\ (1,-2,1,1),\ (0,1,1,1)\}$ or
$\{(1,-2,0,1),\ (1,-2,1,1),\ (1,-1,0,1),\ (0,1,1,1)\}$

Exercise 3.7

3.7-1. $(x_1, x_2, x_3, x_4, x_5) = (-1 + 4t - s,\ 2 + 2s - t,\ t,\ 3s,\ s)$

3.7-2. $a = -4$

3.7-3. four 10 cents, three 50 cents, seven 1 dollar

3.7-4. $(250 - 3t, 2050 + t, t)$, where $t \in \mathbb{N}$ and $0 \leq t \leq 83$

Chapter 4

Exercise 4.1

4.1-1. -1

4.1-2. $\theta \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 4 & 5 & 1 \end{pmatrix}$, $\sigma \circ \theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix}$

Exercise 4.2

4.2-1. $\det A = \prod_{i=1}^{n} a_{ii}$, where A is an $n \times n$ matrix

Exercise 4.2

4.2-1. 0

4.2-3. $(-1)^{\frac{1}{2}n(n-1)}\frac{1}{2}n^{n-1}(n+1),\ 0,\ (-1)^n \sum_{i=1}^{n} a_i b_i$

4.2-4. $\prod_{i=1}^{n}\prod_{j=i}^{n+1}\begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix}$

4.2-8. $\begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \\ -\frac{1}{3} & 0 & \frac{1}{3} \end{pmatrix}$

4.2-10. (d) For nonzero integers x, y, z satisfying the equation $7x + 13y - 4z = \pm 1$. For example, $x = 2$, $y = 1$ and $z = 7$

Exercise 4.3

4.3-1. $(x_1, x_2, x_3) = (-1, -\frac{1}{2}, -\frac{7}{2})$

4.3-2. $(x_1, x_2, x_3) = (t, -\frac{2t}{3}, \frac{t}{3})$

Chapter 5

Exercise 5.1

5.1-1. $n - 1$

Exercise 5.2

5.2-1. $\begin{pmatrix} 1 & 2 & -1 \\ 1 & 0 & -1 \end{pmatrix} x^2 + \begin{pmatrix} 1 & 0 & -1 \\ 4 & 2 & 0 \end{pmatrix} x + \begin{pmatrix} 1 & -3 & -1 \\ -3 & 0 & 1 \end{pmatrix}$

5.2-2. $-x^3 + 2x^2 + x - 2 = -(x-2)(x-1)(x+1)$

5.2-3. 2, 1, -1. The algebraic and geometric multiplicities of each eigenvalue are 1

5.2-5. $(-1)^n p(x)$

Exercise 5.3

5.3-3. $(n+1)!$

5.3-5. (a) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

(c) $\frac{1}{4}\begin{pmatrix} e + e^{-1} & -e + e^{-1} & e + e^{-1} \\ -2e + 2e^{-1} & 2e + 2e^{-1} & -2e + e^{-1} \\ e + e^{-1} & -e + e^{-1} & e + e^{-1} \end{pmatrix}$

5.3-6. $\dfrac{1}{2^n\sqrt{5}}\begin{pmatrix} C_k^{n+1}5^{\frac{k}{2}} & C_k^n 5^{\frac{k-1}{2}} \\ 2C_k^{n+1}5^{\frac{k}{2}} & 2C_k^n 5^{\frac{k-1}{2}} \end{pmatrix}$

Chapter 6

Exercise 6.2

6.2-1. $\lambda = 2$ or -1

6.2-2. $-a + ab - b \neq 0$

6.2-5. Yes

6.2-6. No

6.2-11. Yes

Exercise 6.3

6.3-4. $\text{span}(S) = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F} \right\}$

6.3-5. Yes

Exercise 6.4

6.4-1. No. $\{\alpha_1, \alpha_2\}$ is a basis of V

6.4-5. $\{(1,1,0,0),\ (1,-1,1,0),\ (0,2,0,1)\}$

6.4-6. $\{x^2+2, x+3\}$

6.4-7. $\frac{n(n+1)}{2}$

Exercise 6.5

6.5-2. Yes

6.5-3. $W' = \text{span}\{(0,0,1,0),\ (0,0,0,1)\}$

Chapter 7

Exercise 7.1

7.1-3. σ is onto. $f = -(x+2)$

7.1-4. (1) surjective, (2) injective, (3) injective and surjective, (4) injective and surjective

7.1-5. $\{0\}$

7.1-6. $\ker(\sigma) = \left\{ \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} \;\middle|\; c \in \mathbb{R} \right\}$, $\text{nullity}(\sigma) = 1$, $\text{rank}(\sigma) = 2$

Exercise 7.2

7.2-1. (a) $[\sigma]_{\mathscr{B}}^{\mathscr{A}} = \begin{pmatrix} 2 & -1 \\ 3 & 4 \\ 1 & 0 \end{pmatrix}$, $\operatorname{rank}(\sigma) = 2$, $\operatorname{nullity}(\sigma) = 0$

(b) $\begin{pmatrix} 1 & -1 & 2 \\ 2 & 1 & 0 \\ -1 & -2 & 2 \end{pmatrix}$, $\operatorname{rank}(\sigma) = 3$, $\operatorname{nullity}(\sigma) = 0$

(c) $\begin{pmatrix} 2 & 1 & -1 \end{pmatrix}$, $\operatorname{rank}(\sigma) = 1$, $\operatorname{nullity}(\sigma) = 2$

(d) $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}$, $\operatorname{rank}(\sigma) = 1$, $\operatorname{nullity}(\sigma) = n - 1$

(e) $\begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & \iddots & \iddots & 0 \\ 0 & \iddots & \iddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}$, $\operatorname{rank}(\sigma) = n$, $\operatorname{nullity}(\sigma) = 0$

7.2-2. $\begin{pmatrix} \frac{1}{3} & 1 \\ 4 & 6 \\ -\frac{2}{3} & -1 \end{pmatrix}$

7.2-3. $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

7.2-4. (b) $[\sigma]_{\mathscr{A}} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 1 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

(c) Eigenvalues: $-1, 0, 0, 1$ and

their corresponding eigenvectors: $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix}$

(d) $a \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + b \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}$ for all $a, b \in \mathbb{R}$

7.2-5. $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

7.2-6. $\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$

7.2-7. $\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$

7.2-8. $\begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 8 \\ 0 & 0 & 0 \end{pmatrix}$

7.2-9. $\begin{pmatrix} \frac{1}{10} \\ \frac{3}{5} \end{pmatrix}$

7.2-10. $\begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$

Exercise 7.3

7.3-1. $\begin{pmatrix} 1 & -\frac{1}{2} & \frac{3}{4} \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix}$

7.3-2. $\begin{pmatrix} 2 & 1 & 1 \\ 3 & -2 & 1 \\ -1 & 3 & 1 \end{pmatrix}$

7.3-3. $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 1 \\ -\frac{3}{2} & \frac{1}{2} & -1 \end{pmatrix}$

7.3-4. $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Chapter 8

Exercise 8.1

8.1-3. $\frac{1}{70}\begin{pmatrix} 72(-4)^k + 3^k \times 40 - 42 & 35(3^k - 1) & -72(-4)^k - 3^k \times 5 + 77 \\ -82(-4)^k + 3^k \times 40 + 42 & 35(3^k + 1) & 82(-4)^k - 3^k \times 5 - 77 \\ 2(-4)^k + 3^k \times 40 - 42 & 35(3^k - 1) & -2(-4)^k - 3^k \times 5 + 77 \end{pmatrix}$

8.1-4. $\begin{pmatrix} 2 & \frac{7}{30} & \frac{1}{6} \\ 0 & \frac{7}{4} & \frac{5}{4} \\ 0 & \frac{3}{4} & \frac{9}{4} \end{pmatrix}$

8.1-5. $A = \begin{pmatrix} 0 & 1 \\ 0.5 & 0.5 \end{pmatrix}$, $x_k = \frac{1}{6}(2 + (0.5)^{k-1})$, $\lim_{k\to\infty} x_k = \frac{1}{3}$

8.1-8. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and O_2, their characteristic polynomials are x^2

Exercise 8.3

8.3-1. $P = \begin{pmatrix} 3 & 0 & 7 & 6 \\ 1 & -2 & 2 & 2 \\ 3 & 0 & 0 & 0 \\ 1 & -1 & 2 & 2 \end{pmatrix}$, $P^{-1}AP = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

8.3-2. $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -3+3i & 0 \\ 0 & 0 & 0 & -3-3i \end{pmatrix}$

8.3-3. $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

8.3-4. $P = \begin{pmatrix} 0 & 1 & 0 & -\frac{1}{5} \\ 0 & 1 & 1 & 0 \\ 5 & 0 & 0 & 0 \\ 10 & 1 & 1 & 1 \end{pmatrix}$, $P^{-1}AP = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

8.3-5. $P = \begin{pmatrix} -2 & 1 & 0 & 0 \\ -4 & 0 & 0 & 0 \\ 1 & 1 & -2 & 1 \\ 8 & 0 & -4 & 0 \end{pmatrix}$, $P^{-1}AP = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

Chapter 9

Exercise 9.1

9.1-1. $\phi_1(x,y,z) = -y+z,\ \phi_2 = -x-y+z,\ \phi_3 = x+2y-z$

9.1-6. $-\frac{31}{120}x^4 + \frac{27}{20}x^3 - \frac{29}{120}x^2 - \frac{77}{20}x + 2$

Exercise 9.2

9.2-3. $\{\psi(x,y,z) = a(x+y+z) \mid a \in \mathbb{R}\}$

9.2-4. $\{\psi(x,y,z,w) = a(3x-z-w) \mid a \in \mathbb{R}\}\ \ \forall f \in \mathbb{R}[x]$

Exercise 9.3

9.3-1. (a) ax (b) $bx - ay$ (c) $(a+b)x - (a-b)y$

9.3-2. $\big(\widehat{D}(\phi)\big)(f) = \phi(D \circ f) = f(b) - f(a)$

9.3-3. $\widehat{\sigma}(\phi) = O$ (the zero map)

Exercise 9.4

9.4-1. Yes

9.4-2. $\begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}$

9.4-3. $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$

9.4-6. (a) $\begin{pmatrix} 4 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & \frac{3}{2} \end{pmatrix}$ with $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & -\frac{1}{2} \\ 1 & 0 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 9 \end{pmatrix}$ with $P = \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix}$ with $P = \begin{pmatrix} 1 & \frac{1}{2} & -1 & \frac{1}{2} \\ 1 & -\frac{1}{2} & -2 & 0 \\ 0 & 0 & 1 & \frac{3}{2} \\ 0 & 0 & 0 & -1 \end{pmatrix}$

Exercise 9.5

9.5-1. (a) 0 (b) 3 (c) 1

9.5-3. $P = \begin{pmatrix} 1 & 0 & -3 \\ 1 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$, $q(y_1, y_2, y_3) = y_1^2 - y_2^2 - 14y_3^2$

9.5-4. $q(x', y', z', w') = x'^2 - 2y'^2 + 3z'^2 - 2w'^2$, where $x = x' + y' + z' + w'$, $y = y' + z' + w'$, $z = z' + w'$ and $w = w'$

Exercise 9.6

9.6-1. (a) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ with $P = \begin{pmatrix} 1 & -i & -\frac{1}{2} + \frac{1}{2}i \\ 0 & 1 & \frac{1}{2} + \frac{1}{2}i \\ 0 & 0 & 1 \end{pmatrix}$, 0

(b) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & \frac{5}{3} \end{pmatrix}$ with $P = \begin{pmatrix} 1 & -1 - 2i & 1 - \frac{1}{3}i \\ 0 & 1 & -\frac{2}{3} + \frac{2}{3}i \\ 0 & 1 & \frac{1}{3} + \frac{2}{3}i \end{pmatrix}$, 1

Chapter 10

Exercise 10.1

10.1-4. $\frac{1}{\sqrt{2}}(1, 0, 1, 0)$, $\frac{1}{6}(1, 2, -1, 0)$, $\frac{1}{\sqrt{21}}(-2, 2, 2, 3)$, $\frac{1}{7}(-2, -5, 2, -4)$

10.1-6. $\{1,\ 2\sqrt{3}(x - \frac{1}{2}),\ 6\sqrt{5}(x^2 - x + \frac{1}{6}),\ 10\sqrt{28}(x^3 - \frac{3}{2}x^2 + \frac{3}{5}x - \frac{1}{20})\}$

10.1-8. $\{\frac{1}{\sqrt{3}}(1, 1, -1),\ \frac{1}{\sqrt{2}}(-1, 1, 0)\}$

10.1-9. $(0, \frac{2}{3}, -\frac{1}{3}, \frac{4}{3}\}$

10.1-10. 2

10.1-11. $3y = 2x + 4$

10.1-12. $y = \frac{1}{2}(4 + x - x^2)$

10.1-13. (a) $(2, 1)$
(b) $\frac{1}{5}(8, 3, 6)$
(c) $(2, 1, 0)$

10.1-14. $Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $R = \begin{pmatrix} 1 & \sqrt{2} & 0 \\ 0 & -\sqrt{2} & -\sqrt{2} \\ 0 & 0 & \sqrt{2} \\ 0 & 0 & 0 \end{pmatrix}$

Exercise 10.3

10.3-2. $\xi_2 \mapsto \frac{1}{3}(-2\xi_1 + 2\xi_2 - \xi_3)$, $\xi_3 \mapsto \frac{1}{3}(-2\xi_1 - \xi_2 + 2\xi_3)$

Exercise 10.4

10.4-1. $P = \begin{pmatrix} 1 & \frac{1}{4} & \frac{1}{2} \\ 0 & \frac{1}{4} & -\frac{3}{2} \\ 0 & 0 & 2 \end{pmatrix}$; $P^T A P = \begin{pmatrix} 1 & \frac{1}{2} & -3 \\ 0 & \frac{1}{4} & -\frac{5}{2} \\ 0 & 0 & 2 \end{pmatrix}$

Exercise 10.5

10.5-2. $x = x' - \frac{1}{4}y'$, $y = -\frac{1}{12}y'$, $-\frac{1}{12}y' - z'$; $x'^2 - \frac{1}{16}y'^2 + z'^2$

10.5-3. $\begin{pmatrix} 1 & 1 & 1 \\ -4 & \frac{1}{4} & -4 \\ 1 & 0 & -17 \end{pmatrix}$

10.5-4. (a) $\begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$

(b) $\frac{1}{2}\begin{pmatrix} e^{-1} + e & -e^{-1} + e & 0 \\ -e^{-1} + e & e^{-1} + e & 0 \\ 0 & 0 & e \end{pmatrix} = \begin{pmatrix} \cosh 1 & \sinh 1 & 0 \\ \sinh 1 & \cosh 1 & 0 \\ 0 & 0 & e \end{pmatrix}$

10.5-5. $\begin{pmatrix} -\frac{1}{2} & \frac{1}{\sqrt{2}} & -\frac{1}{2} \\ -\frac{i}{\sqrt{2}} & i & \frac{i}{\sqrt{2}} \\ \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} \end{pmatrix}$

10.5-6. $\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{i}{2} & -\frac{i}{2} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{i}{2} & \frac{i}{2} \end{pmatrix}$

10.5-7. $\begin{pmatrix} 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{pmatrix}$

10.5-12. $H = I - 2WW^T = \begin{pmatrix} -161 & -18 & -90 & -18 \\ -18 & -1 & -10 & -2 \\ -90 & -10 & -49 & -10 \\ -18 & -2 & -10 & -1 \end{pmatrix}$, $HX = \begin{pmatrix} -969 \\ -107 \\ -535 \\ -107 \end{pmatrix}$

10.5-14. $U = \begin{pmatrix} -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $S = \begin{pmatrix} 4 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}$, $V = \begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$; $A = USV^T$

10.5-16. $\begin{pmatrix} -\frac{4}{25} & -\frac{2}{25} & 0 \\ -\frac{2}{25} & \frac{1}{25} & 0 \\ 0 & 0 & 2 \end{pmatrix}$

Note: If you find some wrong answers, please send an e-mail to tell the author Dr. W.C. Shiu (wcshiu@hkbu.edu.hk) for correction.