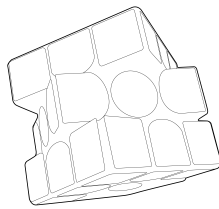


# Linear Algebra

Snochi Song



*This page intentionally left blank.*

# Contents

<b>1</b>	<b>Vector Spaces</b>	
1.1	Vector Spaces . . . . .	4
1.2	Subspaces . . . . .	5
1.3	Linear Combinations and Span . . . . .	5
1.4	Linear Independence . . . . .	6
1.5	Bases and Dimension . . . . .	7
<b>2</b>	<b>Linear Transformations and Matrices</b>	
2.1	Linear Transformations . . . . .	12
2.2	Matrix Representations of Linear Transformations . . . . .	15
2.3	Compositions of Linear Transformations . . . . .	17
2.4	Invertibility and Isomorphisms . . . . .	21
2.5	The Change of Basis . . . . .	24
<b>3</b>	<b>Linear Equations</b>	
3.1	Elementary Matrix Operations and Elementary Matrices . . . . .	26
3.2	The Rank and Inverse of a Matrix . . . . .	26
3.3	Four Fundamental Subspaces of a Matrix . . . . .	29
3.4	Systems of Linear Equations . . . . .	30
<b>4</b>	<b>Determinants</b>	
4.1	Determinants . . . . .	38
4.2	Properties of Determinants . . . . .	41
<b>5</b>	<b>Polynomials</b>	
5.1	Algebras . . . . .	46
5.2	Algebra of Polynomials . . . . .	47
5.3	Lagrange Interpolation . . . . .	49
5.4	Polynomial Ideals . . . . .	51
<b>6</b>	<b>Diagonalization</b>	
6.1	Eigenvectors and Eigenvalues . . . . .	60
6.2	Diagonalization . . . . .	61
<b>7</b>	<b>Elementary Canonical Forms</b>	
7.1	Eigenvalues . . . . .	68
7.2	Annihilating Polynomials . . . . .	69
7.3	Triangulation and Diagonalization . . . . .	71
7.4	Direct Sum Decompositions . . . . .	74
7.5	Invariant Direct Sum . . . . .	77

7.6	Primary Decomposition Theorem . . . . .	81
<b>8</b>	<b>The Rational and Jordan Form</b>	
8.1	Cyclic Subspaces and Annihilators . . . . .	86
8.2	Cyclic Decomposition and the Rational Form . . . . .	91
8.3	Jordan Form . . . . .	101
<b>9</b>	<b>Bilinear Forms</b>	
9.1	Bilinear Forms . . . . .	108
9.2	Symmetric Bilinear Form . . . . .	114
9.3	Skew-Symmetric Bilinear Form . . . . .	120
9.4	Groups Preserving Bilinear Forms . . . . .	123
<b>10</b>	<b>Inner Product Spaces</b>	
10.1	Inner Products . . . . .	126
10.2	Inner Product Spaces . . . . .	130
10.3	Linear Functionals and Adjoint . . . . .	138
10.4	Unitary Operators . . . . .	143
10.5	Normal Operators . . . . .	149
10.6	Spectral Theory . . . . .	153

# 1.

## Vector Spaces

- 
- 1.1 Vector Spaces
  - 1.2 Subspaces
  - 1.3 Linear Combinations and Span
  - 1.4 Linear Independence
  - 1.5 Bases and Dimension
-

## Vector Spaces

### Def'n. Vector Space over a Field

A **vector space** over a field  $\mathbb{F}$  is a set with two binary operations, addition  $V \times V \rightarrow V$  and scalar multiplication  $\mathbb{F} \times V \rightarrow V$  such that the following holds. Let  $x, y, z \in V$  and  $a, b, c \in \mathbb{F}$ .

- (a) Commutativity of addition:

$$x + y = y + x.$$

- (b) Associativity of addition:

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

- (c) Existence of additive identity: There exists  $0 \in V$  such that

$$0 + v = v + 0 = v$$

for all  $v \in V$ .

- (d) Existence of additive inverse: There exists  $-v \in V$  such that

$$-v + v = v + (-v) = 0$$

for all  $v \in V$ .

- (e) Existence of identity of scalar multiplication:

$$1x = x,$$

where  $1 \in \mathbb{F}$  is the unity of  $\mathbb{F}$ .

- (f) Compatibility of scalar multiplication with field multiplication:

$$a(bx) = (ab)x.$$

- (g) Distributivity of scalar multiplication with respect to addition:

$$a(x + y) = ax + ay.$$

- (h) Distributivity of scalar multiplication with respect to field addition:

$$(a + b)x = ax + bx.$$

**Remark 1.1.** For convenience, we shall consistently use  $\mathbb{F}$  to denote an arbitrary field. Moreover, unless otherwise specified,  $\mathbb{F}$  is the underlying field of any vector space that we are going to discuss.

### Def'n. Vector, Scalar

Let  $V$  be a vector space over  $\mathbb{F}$ . We call an element  $v \in V$  a **vector** and  $c \in \mathbb{F}$  a **scalar**.

### Proposition 1.1. Cancellative Property of Vector Addition

Let  $V$  be a vector space and  $x, y, z \in V$ . Suppose  $x + z = y + z$ . Then  $x = y$ .

*Proof.* By definition, there exists  $v \in V$  such that  $z + v = 0$ , the additive inverse of  $z$ . Thus,

$$x = x + 0 = x + (z + v) = (x + z) + v = (y + z) + v = y + (z + v) = y.$$



## Subspaces

**Remark 1.2.** In study of algebraic structure, often times it is of interest to examine subsets that possess the same structure as its superset.

### Def'n. Subspace of a Vector Space

Let  $V$  be a vector space over  $\mathbb{F}$ . We say a subset  $W \subseteq V$  is a **subspace** of  $V$  if  $W$  is a vector space over the same field  $\mathbb{F}$  with operations on  $V$ .

### Proposition 1.2. Subspace Test

*Let  $V$  be a vector space and  $W$  be a subset of  $V$ . Then  $W$  is a subspace of  $V$  if and only if the following hold.*

- (a)  $0 \in W$ .
- (b)  $x + y \in W$  whenever  $x \in W$  and  $y \in W$ .
- (c)  $cx \in W$  whenever  $c \in \mathbb{F}$  and  $x \in W$ .

*Proof.* For the forward direction, suppose  $W$  is a subspace of  $V$ . But this means that the operations on  $W$  are closed, so (2) and (3) hold. Furthermore, there is  $0' \in W$  such that for every  $x \in W$ ,  $x + 0 = x$ . But since  $V$  is a vector space, there is  $0 \in V$ , so  $0' + 0 = 0 = 0'$ , proving (1). Moreover, for the reverse direction, suppose (1), (2), and (3) hold. Then we only have to ensure that the existence of additive inverse for each element. But clearly,

$$(-1)x = -x \in W$$

whenever  $x \in W$  by (3). ♠

### Proposition 1.3. Intersection of Subspaces Is a Subspace

*Any intersection of subspaces of a vector space  $V$  is a subspace of  $V$ .*

*Proof.* Let  $C$  be the set of some arbitrary subspaces of  $V$  and  $W$  be the intersection of the subspaces in  $C$ . Since every subspace has  $0$ ,  $0 \in W$ . Moreover, let  $x, y \in W$  and  $a \in \mathbb{F}$ . Since every subspace is closed under addition and scalar multiplication, every subspace has  $x + y$  and  $ax$ , so  $(x + y), ax \in W$ . ♠

## Linear Combinations and Span

### Def'n. Linear Combination of Vectors

Let  $V$  be a vector space and let  $v_1, v_2, \dots, v_n \in V$ . We say  $v \in V$  is a **linear combination** of  $v_1, v_2, \dots, v_n$  if there exists some  $c_1, c_2, \dots, c_n \in \mathbb{F}$  such that

$$v = \sum_{i=1}^n c_i v_i.$$

**Remark 1.3.** From the definition, it is implicitly stated that any linear combination involves only finite number of vectors.

### Def'n. Span of a Set of Vectors

Let  $V$  be a vector space and let  $S \subseteq V$  be a nonempty subset. We define the **span** of  $S$ , denoted as  $\text{span}(S)$ , to be the set of linear combinations of vectors in  $S$ .

**Proposition 1.4.**  
 $\text{span}(S)$  **Is a Subspace**

Let  $V$  be a vector space and let  $S \subseteq V$  be a subset. Then  $\text{span}(S) \subseteq V$  is a subspace and any subspace  $W \subseteq V$  with  $S \subseteq W$  also satisfies  $\text{span}(S) \subseteq W$ .

*Proof.* Notice that the result is trivial for  $S = \emptyset$ , since  $\text{span}(\emptyset) = \{0\}$ , which is a subspace for any vector space. So suppose that  $S \neq \emptyset$ . First notice that

$$0 \in \text{span}(S),$$

since  $0v$  for any  $v \in S$  is a linear combination of  $v$ . Moreover, let  $x, y \in \text{span}(S)$  and  $c$  be any scalar. Since  $x$  and  $y$  are linear combinations of vectors in  $S$ , clearly  $x + y$  and  $cx$  are both linear combinations of vectors in  $S$  as well. So  $\text{span}(S)$  is a subspace of  $V$ . For the second part of the proposition, suppose  $W$  is a subspace of  $V$  which contains  $S$ . For the sake of contradiction, further assume that  $W$  does not contain  $\text{span}(S)$ . Then, for some vectors  $s_1, s_2, \dots, s_n \in S$  and scalars  $a_1, a_2, \dots, a_n \in \mathbb{F}$ ,

$$a_1 s_1 + a_2 s_2 + \dots + a_n s_n \notin W.$$

But clearly each  $a_i s_i \in W$ , since  $W$  contains  $S$  and  $W$  is closed under scalar multiplication. So  $a_1 s_1 + a_2 s_2 + \dots + a_n s_n \in W$ , which is a contradiction. Thus  $\text{span}(S) \subseteq W$ , as desired. ♠

## Linear Independence

**Remark 1.4.** Let  $V$  be a vector space and suppose that  $S \subseteq V$  is a spanning set of  $V$ . Then, we have some number of expression to describe vectors in  $V$ . For instance, if  $S$  has  $n$  elements  $s_1, s_2, \dots, s_n \in S$ , then for any  $v \in V$ ,

$$v = \sum_{i=1}^n c_i s_i$$

for some  $c_1, c_2, \dots, c_n \in \mathbb{F}$ . But the question is, is  $S$  the minimal spanning subset of  $V$ ? That is, we are interested to find out if there is a subset of  $V$  which has less than  $n$  elements and spans  $V$ . To answer this question, we introduce the following definition.

**Def'n. Linearly Independent, Linearly Dependent Vectors**

Let  $V$  be a vector space. We say  $v_1, v_2, \dots, v_n \in V$  are **linearly dependent** if there exist nonzero  $(c_1, c_2, \dots, c_n) \in \mathbb{F}^n$  ( $\mathbb{F}^n$  is the set of  $n$ -tuples where each entry is an element of  $\mathbb{F}$ ; we say  $x \in \mathbb{F}^n$  is zero if every entry of  $x$  is zero) such that

$$\sum_{i=1}^n c_i v_i = 0.$$

We say  $v_1, v_2, \dots, v_n$  are **linearly independent** otherwise.

**Remark 1.5.** We also say that a subset  $S \subseteq V$  is linearly dependent if there exist finite number of elements  $s_1, s_2, \dots, s_n \in S$  such that

$$\sum_{i=1}^n c_i s_i = 0$$

for some nonzero  $(c_1, c_2, \dots, c_n) \in \mathbb{F}$ . Of course,  $S$  is linearly independent if no such elements exist.

**Remark 1.6.** Another way to think linear independence is the following. Let  $v_1, v_2, \dots, v_n \in V$  for some vector space  $V$ . Then  $v_1, v_2, \dots, v_n$  are linearly independent if and only if the only linear combination of  $v_1, v_2, \dots, v_n$  equal to 0 is the trivial representation. That is,

$$\sum_{i=1}^n 0v_i = 0.$$



**Proposition 1.5.**

*Let  $V$  be a vector space. If  $S_1 \subseteq S_2 \subseteq V$  and  $S_1$  is linearly dependent, then  $S_2$  is linearly dependent.*

*Proof.* Suppose  $S_1 = \{v_1, \dots, v_n\} \in V$  be linearly dependent. Then there is a nonzero  $(a_1, \dots, a_n) \in \mathbb{F}^n$  such that

$$\sum_{i=1}^n a_i v_i = 0.$$

Therefore, if we define  $a_{n+1} = a_{n+2} = \dots = a_m = 0$ , where  $m = |S_2| \in \mathbb{N}$ , then

$$\sum_{i=1}^m a_i v_i = \sum_{i=1}^n a_i v_i = 0,$$

which is not the trivial representation. ♠

**Corollary 1.5.1.**

*Let  $V$  be a vector space. If  $S_1 \subseteq S_2 \subseteq V$  and  $S_2$  is linearly independent, then  $S_1$  is linearly independent.*

**Remark 1.7.** Now suppose  $S_n \subseteq V$  is a subset of  $V$  containing  $n$  elements and spans  $V$ . If  $S_n$  is linearly dependent, then there must be a vector  $s_n$  which can be written as a linear combination of other vectors in  $S_n$ . So it turns out that

$$\text{span}(S_{n-1}) = \text{span}(S_n) = V,$$

where  $S_{n-1} = S_n \setminus \{s_n\}$ . We may continue this process until  $S_k$  is independent. But once we hit here, there is no way  $\text{span}(S_{k-1}) = \text{span}(S_k)$ . Thus it turns out that the smallest spanning set of  $V$  must be independent. This idea can be written alternatively as the following proposition.

**Proposition 1.6.**

*Let  $S$  be linearly independent subset of a vector space  $V$ , and let  $v \in V$  with  $v \notin S$ . Then  $S \cup \{v\}$  is linearly dependent if and only if  $v \in \text{span } S$ .*

*Proof.* First, write  $S = \{v_1, \dots, v_n\} \subseteq S$  for convenience. For the forward direction, suppose that  $S \cup \{v\}$  is linearly dependent. Then there must exist nonzero  $(a_1, \dots, a_{n+1}) \in \mathbb{F}^{n+1}$  such that

$$\sum_{i=1}^n a_i v_i + a_{n+1} v = 0.$$

But this means

$$-a_{n+1} v = \sum_{i=1}^n a_i v_i \iff v = \sum_{i=1}^n -\frac{a_i}{a_{n+1}} v_i$$

so  $v \in \text{span}\{v_1, \dots, v_n\}$ . For the reverse direction, suppose that  $v \in \text{span}(S)$ . Then there exists  $(a_1, \dots, a_n) \in \mathbb{F}^n$  such that

$$v = \sum_{i=1}^n a_i v_i,$$

so we have nontrivial representation of zero

$$\sum_{i=1}^n a_i v_i + 1v = 0. \quad \spadesuit$$

## Bases and Dimension

**Remark 1.8.** From the last section, we have seen that the smallest spanning set of any vector space must be linearly independent. Indeed, there are many pleasurable behaviors of linearly independent spanning sets that would be discussed in this section.

**Def'n. Basis** for a Vector Space

Let  $V$  be a vector space and  $\beta \subseteq V$ . We say  $\beta$  is a **basis** for  $V$  if  $\beta$  is linearly dependent and spans  $V$ . We also say vectors of  $\beta$  form a basis for  $V$ .

**Remark 1.9.** One important property of basis  $\beta$  for a vector space  $V$  is that any  $v \in V$  can be uniquely written as a linear combination of vectors in  $\beta$ .

**Proposition 1.7.**  
Unique  
Representation of a  
Vector

Let  $V$  be a vector space and  $\beta = \{v_1, v_2, \dots, v_n\} \subseteq V$ . Then  $\beta$  is a basis for  $V$  if and only if there exists unique scalars  $c_1, c_2, \dots, c_n \in \mathbb{F}$  such that

$$v = c_1 v_1 + c_2 v_2 + \dots + c_n v_n$$

for all  $v \in V$ .

*Proof.* For the forward direction, suppose that  $\beta$  is a basis for  $V$ , and for the sake of contradiction, suppose that there exist  $d_1, d_2, \dots, d_n \in \mathbb{F}$  such that

$$v = \sum_{i=1}^n d_i v_i$$

and  $d_j \neq c_j$  for some  $i \in \{1, 2, \dots, n\}$ . But this means

$$\sum_{i=1}^n (d_i - c_i) v_i = v - v = 0$$

where  $d_j - c_j \neq 0$ , so we have a contradiction. For the reverse direction, suppose that we have unique representation of each vector in  $V$  by  $\beta$ . Then  $\text{span}(\beta) = V$ , and  $\beta$  is linearly independent, since

$$\sum_{i=1}^n 0 v_i = 0$$

is the unique representation of  $0 \in V$ . ♠

**Proposition 1.8.**  
Maximal Linearly  
Independent Subset

Let  $V$  be a vector space. If  $\beta \subseteq V$  is a maximal linearly independent subset, then  $\beta$  is a basis for  $V$ .

*Proof.* For the sake of contradiction, suppose that  $\text{span}(\beta) \subsetneq V$ . Then there exists  $v \in V \setminus \text{span}(\beta)$ . But this means  $\beta \cup \{v\}$  is linearly independent, which violates the maximality of  $\beta$ , so we have a contradiction. ♠

**Theorem 1.9.**  
Existence of Basis

Let  $V$  be a vector space. Then there exists a basis  $\beta$  for  $V$ .

*Proof.* Let  $S \subseteq \mathcal{P}(V)$  be the set of every linearly independent subsets of  $V$ . Then  $S$  is nonempty, since  $\emptyset \in S$ . Moreover,  $(S, \preceq)$  is a partially ordered set. Let  $C \subseteq S$  be a chain and let

$$u = \bigcup_{c \in C} c.$$

We claim that  $u$  is an upper bound for  $C$ . To verify this, we have to show that  $c \in u$  for any  $c \in C$  (which is clear from the definition) and that  $u \in S$ . So for the sake of contradiction, suppose that  $u \notin S$ , which means  $u$  is linearly dependent. Then there exist  $v_1, v_2, \dots, v_n \in u$  such that

$$\sum_{i=1}^n a_i v_i = 0$$

for some nonzero  $(a_1, a_2, \dots, a_n) \in \mathbb{F}^n$ . But for each  $i \in \{1, 2, \dots, n\}$ , there exist  $c_i \in C$  such that

$$v_i \in c_i.$$

Since  $C$  is a chain, there must exist  $c \in C$  which contains  $c_1, c_2, \dots, c_n$ . But  $c \in C \subseteq S$ , so  $c$  is linearly independent, and we have a contradiction. Thus by Zorn's lemma, there exists a maximal  $\beta \in S$ , which is a maximal linearly independent subset of  $V$ . By Proposition 1.8,  $\beta$  is a basis for  $V$ . ♠

**Theorem 1.10.**  
**Replacement**  
**Theorem**

*Let  $V$  be a vector space. Suppose  $G \subseteq V$  with  $|G| = n \in \mathbb{N}$  is a spanning set and let  $L \subseteq V$  be a linearly independent subset with  $|L| = m \in \mathbb{N}$ . Then  $m \leq n$  and there exists  $H \subseteq G$  with  $|H| = n - m$  such that  $\text{span}(L \cup H) = V$ .*

*Proof.* Write  $G = \{v_1, v_2, \dots, v_n\}$  and let  $L = \{u_1, u_2, \dots, u_m\}$ . For the sake of contradiction, suppose  $n < m$ . Since  $G$  is a spanning set, there exist  $a_1, a_2, \dots, a_n \in \mathbb{F}$  such that

$$u_1 = \sum_{i=1}^n a_i v_i.$$

Since  $u_1 \neq 0$ , some  $a_i \neq 0$ . Without loss of generality, suppose  $a_1 \neq 0$ . Then

$$v_1 = \frac{\sum_{i=2}^n a_i v_i - u_1}{-a_1},$$

which means  $\{u_1, v_2, v_3, \dots, v_n\}$  spans  $V$ . Then, for  $u_2$ , there exist  $b_1, b_2, \dots, b_n \in \mathbb{F}$  such that

$$u_2 = \sum_{i=2}^n b_i v_i + b_1 u_1$$

where  $b_i \neq 0$  for some  $i \in \{2, 3, \dots, n\}$ , since  $u_1$  and  $u_2$  are linearly independent and  $u_2 \neq 0$ . So suppose  $b_2 \neq 0$  without loss of generality. Then again,  $\{u_1, u_2, v_3, v_4, \dots, v_n\}$  spans  $V$ . By continuing this process, we obtain  $\{u_1, u_2, \dots, u_n\}$  as a spanning set for  $V$ . But this means there exist  $c_1, c_2, \dots, c_n \in \mathbb{F}$  such that

$$\sum_{i=1}^n c_i u_i = u_{n+1},$$

which is a contradiction, since  $L$  is linearly independent. So  $m \leq n$ . Observe that  $H$  can be found in an analogous way. For, we may obtain a spanning set

$$\{u_1, u_2, \dots, u_m, v_{m+1}, \dots, v_n\}$$

for any  $m \leq n$ . ♠

**Def'n. Finite-Dimensional, Infinite-Dimensional Vector Space**

Let  $V$  be a vector space. We say  $V$  is *finite-dimensional* if there exists a finite spanning set for  $V$ . We say  $V$  is *infinite-dimensional* otherwise.

**Corollary 1.10.1.**

*Let  $V$  be finite-dimensional. Then every basis for  $V$  has the same number of vectors.*

**Remark 1.10.** Corollary 1.10.1 enables the following definition.

**Def'n. Dimension of a Finite-Dimensional Vector Space**

Let  $V$  be a finite-dimensional vector space. Then the unique number of elements  $n \in \mathbb{N}$  of any basis for  $V$ , denoted as  $\dim(V)$ , is called the *dimension* of  $V$ .

**Proposition 1.11.**  
**Properties of**  
**Finite-Dimensional**  
**Vector Space**

*Let  $V$  be a vector space with dimension  $n$ . Then the following holds.*

- (a) *Any finite generating set for  $V$  contains at least  $n$  vectors, and a generating set for  $V$  containing  $n$  vectors is a basis of  $V$ .*
- (b) *Any linearly independent subset of  $V$  that contains exactly  $n$  vectors is a basis for  $V$ .*
- (c) *Every linearly independent subset of  $V$  can be extended to a basis for  $V$ .*

*Proof.* The result follows immediately from replacement theorem (Theorem 1.10), Corollary 1.10.1, and the definition of basis. ♠

**Proposition 1.12.**

*Let  $W$  be a subspace of a finite-dimensional vector space  $V$ . Then  $W$  is finite-dimensional and  $\dim(W) \leq \dim(V)$ . Moreover, if  $\dim(W) = \dim(V)$ , then  $V = W$ .*

*Proof.* Let  $\beta = \{v_1, v_2, \dots, v_n\}$  be a basis for  $V$ . Since the result is clear when  $W = \{0\}$ , assume that  $W \neq \{0\}$ . Then there exist some  $v_i$  such that  $v_i \in W$ . Without loss of generality, suppose  $v_1, v_2, \dots, v_m \in W$  for some  $m \leq n$ . We claim that  $\alpha = \{v_1, v_2, \dots, v_m\}$  is a basis for  $W$ . To verify this, observe that  $\alpha$  is linearly independent. Moreover, for the sake of contradiction, suppose there exists  $w \in W$  such that  $w$  cannot be expressed as a linear combination of  $v_1, v_2, \dots, v_m$ . Since  $w \in V$ , there exist  $c_1, c_2, \dots, c_n \in \mathbb{F}$  such that

$$\sum_{i=1}^n c_i v_i = w,$$

and there exists  $i \in \{m+1, \dots, n\}$  such that  $c_i \neq 0$  by assumption. But this means  $v_i \in W$ , which is a contradiction. Thus  $\text{span}(\alpha) = W$ , so  $\dim(W) \leq \dim(V)$ . If  $\dim(W) = \dim(V)$ , then given a basis  $\alpha = \{w_1, w_2, \dots, w_n\}$  for  $W$  and  $\beta = \{v_1, v_2, \dots, v_n\}$  for  $V$ , we may replace each  $w_i \in \alpha$  with  $v_i \in \beta$ . That is,  $\text{span}(\beta) = V = W$ . ♠

**Theorem 1.13.**  
**Basis Extension**  
**Theorem**

*If  $W$  is a subspace of finite-dimensional vector space  $V$ , then any basis for  $W$  can be extended to a basis for  $V$ .*

*Proof.* This is a direct result of the replacement theorem (Theorem 1.10). For, if  $\alpha$  is a basis for  $W$ , then  $\alpha$  is a linearly independent subset of  $V$ . Thus, for any basis  $\beta$  for  $V$ , we may find a set  $\gamma \subseteq \beta$  with  $|\gamma| = \dim(V) - \dim(W)$  vectors such that  $\alpha \cup \gamma$  is a basis for  $V$ . ♠

## **2.**

# **Linear Transformations and Matrices**

- 
- 2.1 Linear Transformations
  - 2.2 Matrix Representations of Linear Transformations
  - 2.3 Compositions of Linear Transformations
  - 2.4 Invertibility and Isomorphisms
  - 2.5 The Change of Basis
-

## Linear Transformations

**Remark 2.1.** In previous section, we developed the theory of abstract vector space. It is now natural to consider those functions defined on vector spaces that, in some sense, preserve the structure.

### Def'n. Linear Transformation on Vector Spaces

Let  $V, W$  be vector spaces over the same field  $\mathbb{F}$ . We say a function  $T : V \rightarrow W$  is a **linear transformation** from  $V$  to  $W$  if  $T$  preserves the operations. That is, for any  $v \in V$ ,  $w \in W$ , and  $c \in \mathbb{F}$ ,

$$(a) \quad T(v + u) = Tv + Tu \text{ and}$$

$$(b) \quad Tcv = cTv.$$

### Def'n. Linear Operator on a Vector Space

Let  $V$  be a vector space. A linear transformation  $T : V \rightarrow V$  from  $V$  to  $V$  is called a **linear operator**.

**Remark 2.2.** We denote the set of linear transformations from  $V$  to  $W$  by  $\mathcal{L}(V, W)$ ,

$$\mathcal{L}(V, W) = \{T : V \rightarrow W \mid T \text{ is linear}\}$$

In case of  $V = W$ , we write  $\mathcal{L}(V)$  for simplicity.

### Proposition 2.1. Properties of Linear Transformations

Let  $V, W$  be vector spaces over the same field  $\mathbb{F}$  and let  $T : V \rightarrow W$ .

(a) If  $T$  is linear, then  $T(0) = 0$ .

(b)  $T$  is linear if and only if  $T(cv + u) = cTv + Tu$  for all  $v, u \in V$  and  $c \in \mathbb{F}$ .

(c) If  $T$  is linear, then  $T(v - u) = Tv - Tu$  for all  $v, u \in V$ .

(d)  $T$  is linear if and only if

$$T\left(\sum_{i=1}^n c_i v_i\right) = \sum_{i=1}^n c_i T v_i$$

for all  $c_1, c_2, \dots, c_n \in \mathbb{F}$  and  $v_1, v_2, \dots, v_n \in V$ . That is,  $T$  preserves linear combinations.

*Proof.* For (a), let  $v \in V$ . Observe that  $T(0) = T(0v) = 0Tv = 0$ . For (b), suppose that  $T$  is linear. Then

$$T(cv + u) = Tcv + Tu = cTv + Tu.$$

On the other hand, if  $T(cv + u) = cTv + Tu$  for all  $v, u \in V$  and  $c \in \mathbb{F}$ , then for any  $x, y \in V$ ,

$$T(x + y) = T(1x + y) = 1Tx + Ty = Tx + Ty$$

and for any  $d \in \mathbb{F}$ ,

$$Tdx = T(dx + 0) = dTx + T(0) = dTx$$

by (a). (c) and (d) are direct consequences of (b). 

### Def'n. Null Space (Kernel), Range (Image) of a Linear Transformation

Let  $V, W$  be vector spaces and let  $T : V \rightarrow W$  be a linear transformation. We define the **null space** (or **kernel**) of  $T$ , denoted as  $\ker(T)$ , by

$$\ker(T) = \{v \in V : Tv = 0\} \subseteq V.$$

In other words,  $\ker(T)$  is the set of vectors in  $V$  which are mapped to 0 by  $T$ . Moreover, we define the

**range** (or **image**) of  $T$ , denoted as  $\text{image}(T)$ , by

$$\text{image}(T) = \{w \in W : \exists v \in V [w = Tv]\} \subseteq W.$$

**Remark 2.3.** An important property of the null space and range of a linear transformation is that they are subspaces of their respective supersets.

**Proposition 2.2.**  
**Null Space and Range Are Subspaces**

*Let  $V, W$  be vector spaces and let  $T : V \rightarrow W$  be linear. Then  $\ker(T) \subseteq V$  and  $\text{image}(T) \subseteq W$  are subspaces.*

*Proof.* To verify that  $\ker(T) \subseteq V$  is a subspace, first observe that  $0 \in \ker(T)$ , since  $T(0) = 0$ . Moreover, if  $v, u \in \ker(T)$  and  $c \in \mathbb{F}$ , then

$$T(cv + u) = cTv + Tu = 0$$

so  $cv + u \in \ker(T)$  as well. To verify that  $\text{image}(T) \subseteq W$  is a subspace, observe that  $T(0) = 0 \in \text{image}(T)$ . Moreover, if  $w, z \in \text{image}(T)$  and  $c \in \mathbb{F}$ , then there exist  $v, u \in V$  such that  $w = Tv$  and  $z = Tu$ . That is,

$$cw + z = cTv + Tu = T(cv + u) \in \text{image}(T). \spadesuit$$

**Remark 2.4.** The following proposition provides a method for finding a spanning set for the range of a linear transformation.

**Proposition 2.3.**

*Let  $V$  and  $W$  be vector spaces, and let  $T : V \rightarrow W$  be linear. If  $\beta = \{v_1, v_2, \dots, v_n\}$  is a basis for  $V$ , then*

$$\ker(T) = \text{span}(T(\beta)) = \text{span}\{Tv_1, Tv_2, \dots, Tv_n\}.$$

*Proof.* Suppose  $\text{image}(T) \neq \text{span}(T\beta)$ . Then there exists  $Tv \in \text{image}(T)$  such that

$$Tv \neq a_1Tv_1 + a_2Tv_2 + \dots + a_nTv_n$$

for any  $(a_1, a_2, \dots, a_n) \in \mathbb{F}^n$ . So

$$Tv \neq T \sum_{i=1}^n a_i v_i,$$

which means

$$v \neq \sum_{i=1}^n a_i v_i$$

for any  $(a_1, a_2, \dots, a_n) \in \mathbb{F}^n$ . This is a contradiction, since  $\beta$  is a basis for  $V$ .  $\spadesuit$

**Def'n. Nullity, Rank of a Linear Transformation**

Let  $V, W$  be vector spaces and let  $T : V \rightarrow W$  be linear. We define the **nullity** of  $T$ , denoted as  $\text{nullity}(T)$ , by

$$\text{nullity}(T) = \dim(\ker(T)),$$

if  $\ker(T)$  is finite-dimensional. Moreover, we define the **rank** of  $T$ , denoted as  $\text{rank}(T)$ , by

$$\text{rank}(T) = \dim(\text{image}(T)),$$

if  $\text{image}(T)$  is finite-dimensional. That is, the nullity and rank of a linear transformation are the dimension of the associated null space and the range.

**Remark 2.5.** By thinking the definition of null space and kernel, one may find it intuitive to think that, given a linear transformation, larger the nullity, smaller the rank. In other words, more vectors are mapped to 0, the smaller the range. The next theorem address the balance between the rank and nullity of a linear transformation.

**Theorem 2.4.**  
**Rank-Nullity Theorem**  
**(Dimension Theorem)**

Let  $V$  and  $W$  be vector spaces, and let  $T : V \rightarrow W$  be linear. If  $V$  is finite-dimensional, then

$$\text{nullity}(T) + \text{rank}(T) = \dim(V).$$

*Proof.* Let  $n = \dim(V)$ ,  $k = \text{nullity}(T) \in \mathbb{N}$  for convenience. Let  $\beta_N = \{v_1, v_2, \dots, v_k\}$  be a basis for  $\ker(T)$ . By basis extension theorem, there exists vectors  $v_{k+1}, v_{k+2}, \dots, v_n \in V$  such that

$$\beta = \beta_N \cup \{v_{k+1}, v_{k+2}, \dots, v_n\}$$

where  $\beta$  is a basis for  $V$ . Now the claim is that  $\beta_R = \{v_{k+1}, v_{k+2}, \dots, v_n\}$  is a basis for  $\text{image}(T)$ . To verify this claim, first observe that  $\text{span}(T\beta) = \text{image}(T)$  implies that

$$\text{image}(T) = \text{span}(T\beta) = \text{span}(T(\beta \setminus \beta_N)) = \text{span}(T(\beta_R)),$$

since  $T(v_i) = 0$  for all  $v_i \in \beta_N$ . For the linear independence part, consider

$$\sum_{k+1}^n c_i T v_i = 0$$

for some  $c_i \in \mathbb{F}$ . Since  $T$  is linear,

$$T \sum_{k+1}^n c_i v_i = 0$$

so  $\sum_{k+1}^n c_i v_i \in \ker(T)$ . Therefore, there exist  $b_1, b_2, \dots, b_k \in \mathbb{F}$  such that

$$\sum_{k+1}^n c_i v_i = \sum_1^k b_i v_i$$

which can be also written as

$$\sum_{k+1}^n c_i v_i + \sum_1^k b_i v_i = 0.$$

But since  $\beta$  is linearly independent,  $(b_1, b_2, \dots, b_k), (c_1, c_2, \dots, c_n) = 0$ . So  $\beta_R$  is linearly independent. Thus

$$\dim(\text{image}(T)) = \text{rank}(T) = n - k$$

as desired. ♠

**Recall. Injective, Surjective, Bijective Function**

Let  $A, B$  sets and let  $f : A \rightarrow B$  a function. We say  $f$  is **injective** if for all  $y \in B$ , there exist a unique  $x \in A$  such that  $f(x) = y$ . We say  $f$  is **surjective** if there exist  $x \in A$  such that  $f(x) = y$  for all  $y \in B$ . We say  $f$  is **bijective** if  $f$  is injective and surjective.

**Proposition 2.5.**  
 **$T$  Is Surjective If and**  
**Only If  $T$  Is Injective**

Let  $V, W$  be vector spaces over  $F$  and let  $T : V \rightarrow W$  be linear. Then  $T$  is surjective if and only if  $\ker(T) = \{0\}$ .

*Proof.* For the forward direction, suppose that  $T$  is surjective and let  $x \in \ker(T)$  be arbitrary. Then  $Tx = 0 = T(0)$ , so by definition of surjection,  $x = 0$ . For the reverse direction, suppose  $\ker(T) = \{0\}$  and  $Tx = Ty$ . Then

$$Tx - Ty = T(x - y) = 0$$

so it must be that  $x - y \in \{0\}$ . That is,  $x = y$ , which means  $T$  is surjective, as desired. ♠



**Proposition 2.6.**

Let  $V$  and  $W$  be vector spaces over  $\mathbb{F}$  of equal finite dimension, and let  $T : V \rightarrow W$  be linear. Then the following are equivalent.

- (a)  $T$  is injective.
- (b)  $T$  is surjective.
- (c)  $\text{rank}(T) = \dim(V)$ .

*Proof.* Proposition 2.5 supplies (a)  $\iff$  (b). Observe that

$$T \text{ is injective} \iff \ker(T) = \{0\} \iff \text{nullity}(T) = 0 \iff \text{rank}(T) = \dim(V).$$



**Remark 2.6.** One of the most important properties of a linear transformation is that it is completely determined by its action on a basis. This result follows from the next theorem and corollary.

**Theorem 2.7.**  
**Characterization of a**  
**Linear**  
**Transformation**

Let  $V$  and  $W$  be vector spaces over  $\mathbb{F}$  and let  $\{v_1, v_2, \dots, v_n\}$  be a basis for  $V$ . Moreover, let  $w_1, w_2, \dots, w_n \in W$ . Then there exists a unique linear  $T : V \rightarrow W$  such that

$$Tv_i = w_i$$

for all  $i \in \{1, 2, \dots, n\}$ .

*Proof.* Define  $T : V \rightarrow W$  by

$$v = \sum_{i=1}^n c_i v_i \mapsto \sum_{i=1}^n c_i w_i.$$

We claim that  $T$  is the desired linear transformation. To verify this, let  $x, y \in V$  and  $c \in \mathbb{F}$ . Then  $x = \sum_{i=1}^n a_i v_i$  and  $y = \sum_{j=1}^n b_j v_j$  for some  $a_1, a_2, \dots, a_n, b_1, \dots, b_n \in \mathbb{F}$ , and

$$\begin{aligned} T(cx + y) &= T\left(c \sum_{i=1}^n a_i v_i + \sum_{i=1}^n b_i v_i\right) = T \sum_{i=1}^n (ca_i + b_i) v_i \\ &= \sum_{i=1}^n (ca_i + b_i) w_i = c \sum_{i=1}^n a_i w_i + \sum_{i=1}^n b_i w_i = cTx + Ty. \end{aligned}$$

Moreover, clearly

$$Tv_i = w_i.$$

To verify the uniqueness, let  $S : V \rightarrow W$  be an arbitrary linear transformation satisfying  $Sv_i = w_i$ . Then

$$Sx = S \sum_{i=1}^n a_i v_i = \sum_{i=1}^n a_i Sv_i = \sum_{i=1}^n a_i w_i = Tx,$$

as desired.


**Corollary 2.7.1.**

Let  $V, W$  be a finite-dimensional vector spaces,  $\{v_1, v_2, \dots, v_n\}$  be a basis for  $V$ , and  $T, U : V \rightarrow W$  be linear transformations satisfying  $Tv_i = Uv_i$  for all  $i \in \{1, 2, \dots, n\}$ . Then  $T = U$ .

## Matrix Representations of Linear Transformations

**Remark 2.7.** Until now, every linear transformation is described by examining its range and null space. In this section, we begin another yet useful approach to describe linear transformation over a vector space: matrix representation of a linear transformation. In fact, we are going to show that there is a special kind of bijection (called isomorphism) between matrices and linear transformations.

**Def'n. Orderd Basis** of a Vector Space

Let  $V$  be a finite-dimensional vector space. An **ordered basis** for  $V$  is a basis for  $V$  endowed with a specific order.

**Remark 2.8.** Given any ordered basis, we may describe any vector in the vector space by using coordinate vectors,  $n$ -tuples ( $n = \dim(V)$ ) that identify abstract vectors in  $V$ . For, if  $\beta = \{v_1, v_2, \dots, v_n\}$  is an ordered basis for a vector space  $V$  over  $\mathbb{F}$ , then there exists a unique representation of any  $v \in V$  as a linear combination of  $v_1, v_2, \dots, v_n$ ,

$$v = \sum_{i=1}^n a_i v_i$$

for some  $a_1, a_2, \dots, a_n$ .

**Def'n. Coordinate Vector** in an Orderd Basis

Let  $\beta = \{v_1, v_2, \dots, v_n\}$  be an ordered basis for a vector space  $V$  over  $\mathbb{F}$ . A unique  $n$ -tuple  $(a_1, a_2, \dots, a_n)$  such that

$$v = \sum_{i=1}^n a_i v_i$$

is called the **coordinate vector** of  $v$  relative to  $\beta$  and denoted by

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = [v]_{\beta}.$$

**Remark 2.9.** We shall show later that the function  $[\cdot]_{\beta} : V \rightarrow \mathbb{F}^n$  for any ordered basis  $\beta$  for  $V$  is linear.

**Def'n. Matrix** over a Field

We say an  $m \times n$  rectangular array  $A$

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

of scalars  $A_{ij} \in \mathbb{F}$  a **matrix** over  $\mathbb{F}$ .

**Remark 2.10.** We shall consistently denote the set of  $m \times n$  matrices over  $\mathbb{F}$  by  $M_{m \times n}(\mathbb{F})$  and the entry on  $i$ th row and  $j$ th column of a matrix  $A \in M_{m \times n}(\mathbb{F})$  by  $A_{ij}$ .

**Remark 2.11.** Similar to how a vector is represented as a coordinate vector in an ordered basis, we may represent a linear transformation as a matrix in an ordered basis. That is, if  $V, W$  are finite-dimensional vector spaces with ordered basis  $\beta = \{v_1, v_2, \dots, v_n\}$  and  $\gamma = \{w_1, w_2, \dots, w_m\}$ . Then for each  $j \in \{1, 2, \dots, n\}$  there exists unique scalars  $a_{ij} \in \mathbb{F}$  such that

$$Tv_j = \sum_{i=1}^m a_{ij} w_i.$$

**Def'n. Matrix Representation** of a Linear Transformation

Consider Remark 2.11. We say the matrix  $A \in M_{m \times n}(\mathbb{F})$  defined by  $A_{ij} = a_{ij}$  the **matrix representation**

of  $T$  in the ordered bases  $\beta$  and  $\gamma$ . We denote the matrix representation of  $T$  by

$$A = [T]_{\beta}^{\gamma}.$$

**Remark 2.12.** When  $V = W$  and  $\beta = \gamma$ , we write

$$[T]_{\beta} = [T]_{\beta}^{\beta}$$

for convenience.

**Remark 2.13.** By Corollary 2.7.1, if  $T, U : V \rightarrow W$  are linear transformations satisfying  $[T]_{\beta}^{\gamma} = [U]_{\beta}^{\gamma}$  then  $T = U$ . Moreover, observe that  $j$ th column of  $[T]_{\beta}^{\gamma}$  is  $[Tv_j]_{\gamma}$ , the coordinate vector of  $Tv_j$  relative to  $\gamma$ . In other words,

$$[T]_{\beta}^{\gamma} = \begin{bmatrix} [Tv_1]_{\gamma} & [Tv_2]_{\gamma} & \cdots & [Tv_n]_{\gamma} \end{bmatrix}.$$

**Remark 2.14.** Now that we have defined an association from linear transformations to matrices, we are going to prove that

$$[\cdot]_{\beta}^{\gamma} : \mathcal{L}(V, W) \rightarrow M_{m \times n}(\mathbb{F})$$

for any ordered basis  $\beta$  for  $V$  and  $\gamma$  for  $W$  is linear, where  $V, W$  are finite-dimensional vector spaces. But to do so, we first show that  $\mathcal{L}(V, W)$  is a vector space under the following operations: Define addition and scalar multiplications such that

$$(cT + U)v = cTv + Uv$$

for any  $T, U \in \mathcal{L}(V, W)$ ,  $c \in \mathbb{F}$ , and  $v \in V$ . Then it is a routine computation to show that  $cT + U : V \rightarrow W$  is linear (and hence  $\mathcal{L}(V, W)$  is closed under the provided operations) and that  $\mathcal{L}(V, W)$  is a vector space.

**Proposition 2.8.**

$[\cdot]_{\beta}^{\gamma} : \mathcal{L}(V, W) \rightarrow$

$M_{m \times n}(\mathbb{F})$  **Is Linear**

*Let  $V, W$  be finite-dimensional vector spaces with ordered bases  $\beta$  and  $\gamma$ , respectively, and let  $T, U : V \rightarrow W$  be linear. Then*

$$[cT + U]_{\beta}^{\gamma} = c[T]_{\beta}^{\gamma} + [U]_{\beta}^{\gamma}.$$

*Proof.* Consider writing  $\beta = \{v_1, v_2, \dots, v_n\}$  and  $\gamma = \{w_1, w_2, \dots, w_m\}$ . Then there exist unique scalars  $a_{ij}, b_{ij}$  such that  $Tv_j = \sum_{i=1}^m a_{ij}w_i$  and  $Uv_j = \sum_{i=1}^m b_{ij}w_i$  for all  $j \in \{1, 2, \dots, n\}$ . Hence

$$(cT + U)v_j = cTv_j + Uv_j = c \sum_{i=1}^m a_{ij}w_i + \sum_{i=1}^m b_{ij}w_i = \sum_{i=1}^m (ca_{ij} + b_{ij})w_i.$$

Thus for all  $i \in \{1, 2, \dots, m\}$  and  $j \in \{1, 2, \dots, n\}$ ,

$$\left([cT + U]_{\beta}^{\gamma}\right)_{ij} = ca_{ij} + b_{ij} = c \left([T]_{\beta}^{\gamma}\right)_{ij} + \left([U]_{\beta}^{\gamma}\right)_{ij}.$$

as desired. ♠

## Compositions of Linear Transformations

**Remark 2.15.** For simplicity, we shall write  $TU$  to denote the composition of linear transformations  $T$  and  $U$ .

**Proposition 2.9.**  
**The Composition of**  
**Linear**  
**Transformations Is**  
**Linear**

Let  $V, W, Z$  be vector spaces over  $\mathbb{F}$  and let  $T : V \rightarrow W$  and  $U : W \rightarrow Z$  be linear. Then  $UT : V \rightarrow Z$  is linear.

*Proof.* Let  $x, y \in V$  and  $c \in \mathbb{F}$  be arbitrary. Then observe that

$$UT(cx + y) = U(T(cx + y)) = U(cTx + Ty) = cU(Tx) + U(Ty) = cUTx + UTy. \quad \spadesuit$$

**Proposition 2.10.**  
**Properties of the**  
**Composition of**  
**Linear**  
**Transformations**

Let  $V$  be a vector space and let  $T, U_1, U_2 : V \rightarrow V$  be linear operators.

- (a)  $T(U_1 + U_2) = TU_1 + TU_2$  and  $(U_1 + U_2)T = U_1T + U_2T$ .
- (b)  $(TU_1)U_2 = T(U_1U_2)$ .
- (c)  $TI = IT = T$ , where  $I$  is the identity operator. That is,  $Iv = v$  for all  $v \in V$ .
- (d)  $a(U_1U_2) = (aU_1)U_2 = U_1(aU_2)$  for all  $a \in \mathbb{F}$ .

**Remark 2.16.** Although we have stated Proposition 2.10 in terms of linear operators for simplicity, (a), (b), and (d) are valid for any linear transformations  $T, U_1, U_2$  such that the provided compositions are well-defined.

**Remark 2.17.** Aside from the addition of matrices and scalar multiplication, an important operation that is not yet introduced is matrix product. Suppose  $T : V \rightarrow W$  and  $U : W \rightarrow Z$  are linear, where  $\alpha = \{v_1, v_2, \dots, v_n\}, \beta = \{w_1, w_2, \dots, w_m\}, \gamma = \{z_1, z_2, \dots, z_p\}$  are bases of  $V, W, Z$ , respectively. Given this, the motivation is to define the product of  $[T]_\alpha^\beta$  and  $[U]_\beta^\gamma$  to be

$$[U]_\beta^\gamma [T]_\alpha^\beta = [UT]_\alpha^\gamma.$$

**Def'n. Product of Matrices**

Let  $A \in M_{m \times n}(\mathbb{F})$  and  $B \in M_{n \times p}(\mathbb{F})$ . We define the **product** of  $A$  and  $B$ , denoted by  $AB$ , to be the  $m \times p$  matrix with entries

$$(AB)_{ij} = \sum_{k=1}^n A_{ik} B_{kj}.$$

**Remark 2.18.** We verify that the above definition of matrix multiplication is consistent with our motivation.

**Proposition 2.11.**

Let  $V, W, Z$  be finite-dimensional vector spaces with ordered bases  $\alpha, \beta, \gamma$ , respectively, and let  $T : V \rightarrow W$  and  $U : W \rightarrow Z$  be linear. Then

$$[U]_\beta^\gamma [T]_\alpha^\beta = [UT]_\alpha^\gamma.$$

*Proof.* Write  $\alpha = \{v_1, v_2, \dots, v_m\}, \beta = \{w_1, w_2, \dots, w_n\}, \gamma = \{z_1, z_2, \dots, z_p\}$  for convenience. Then

$$Tv_i = \sum_{j=1}^n \left( [T]_\alpha^\beta \right)_{ji} w_j$$

and

$$Tw_j = \sum_{k=1}^p \left( [U]_\beta^\gamma \right)_{kj} z_k$$

for all  $i \in \{1, 2, \dots, m\}$  and  $j \in \{1, 2, \dots, n\}$ . That is,

$$\begin{aligned} UTv_i &= U \sum_{j=1}^n \left([T]_{\alpha}^{\beta}\right)_{ji} w_j = \sum_{j=1}^n \left([T]_{\alpha}^{\beta}\right)_{ji} \sum_{k=1}^p \left([U]_{\beta}^{\gamma}\right)_{kj} z_k \\ &= \sum_{j=1}^n \sum_{k=1}^p \left([U]_{\beta}^{\gamma}\right)_{kj} \left([T]_{\alpha}^{\beta}\right)_{ji} z_k = \sum_{k=1}^p \left([U]_{\beta}^{\gamma} [T]_{\alpha}^{\beta}\right)_{ki} z_k \end{aligned}$$

for each  $i \in \{1, 2, \dots, m\}$ , as desired. ♠

**Remark 2.19.** Matrix multiplication is not commutative nor cancellative. That is, given  $A, B \in M_{n \times n}(\mathbb{F})$ , it need not be the case which  $AB = BA$ , and there exist some nonzero  $C \in M_{m \times n}(\mathbb{F})$  and  $D \in M_{n \times p}(\mathbb{F})$  such that  $CD = 0$ , the  $m \times p$  zero matrix.

### Def'n. Transpose of a Matrix

Let  $A \in M_{m \times n}(\mathbb{F})$ . We define the *transpose* of  $A$ , denoted as  $A^T \in M_{n \times m}(\mathbb{F})$ , by

$$A_{ij}^T = A_{ji}.$$

**Remark 2.20.** Here are some remarks about the transpose operation. Let  $A, B \in M_{m \times n}(\mathbb{F})$  and  $c \in \mathbb{F}$ . Then

$$(cA + B)_{ij}^T = (cA + B)_{ji} = cA_{ji} + B_{ji} = cA_{ij}^T + B_{ij}^T.$$

That is,

$$(cA + B)^T = cA^T + B^T.$$

Moreover, let  $C \in M_{m \times n}(\mathbb{F})$  and  $D \in M_{n \times p}(\mathbb{F})$ . Then observe that

$$(CD)_{ij}^T = CD_{ji} = \sum_{k=1}^n C_{jk} D_{ki} = \sum_{k=1}^n D_{ki} C_{jk} = \sum_{k=1}^n D_{ik}^T C_{kj}^T = (D^T C^T)_{ij}.$$

That is,  $(CD)^T = D^T C^T$ .

### Def'n. Kronecker Delta

The *Kronecker delta*  $\delta_{ij}$  is defined as

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

**Remark 2.21.** We have a natural analogue of an identity operator. That is, if we define  $I \in M_{n \times n}(\mathbb{F})$  by

$$I_{ij} = \delta_{ij},$$

then it is an easy computation to verify that

$$IA = AI = A$$

for any  $A \in M_{n \times n}(\mathbb{F})$ .

### Proposition 2.12. Properties of Matrix Product

Let  $A \in M_{m \times n}(\mathbb{F})$ ,  $B, C \in M_{n \times p}(\mathbb{F})$ , and  $D, E \in M_{q \times m}(\mathbb{F})$ .

(a)  $A(B + C) = AB + AC$  and  $(D + E)A = DA + EA$ .

(b)  $a(AB) = (aA)B = A(aB)$  for any  $a \in \mathbb{F}$ .

(c)  $I_m A = A I_n = A$ , where  $I_k \in M_{k \times k}(\mathbb{F})$  is the  $k \times k$  identity matrix.

(d) Let  $V$  be a finite-dimensional vector space,  $I : V \rightarrow V$  be the identity operator, and let  $\beta$  be an ordered basis for  $V$ . Then  $[I]_\beta = I$ .

**Proposition 2.13.**

Let  $V$  and  $W$  be vector spaces with ordered bases  $\beta$  and  $\gamma$ , respectively, and let  $T : V \rightarrow W$  be linear. Then,

$$[Tv]_\gamma = [T]_\beta^\gamma [v]_\beta.$$

*Proof.* Write  $\beta = \{v_1, v_2, \dots, v_n\}$  and  $\gamma = \{w_1, w_2, \dots, w_m\}$ . Let

$$v = \sum_{i=1}^n a_i v_i$$

for some  $a_1, a_2, \dots, a_n \in \mathbb{F}$ . Then  $([v]_\beta)_i = a_i$  and

$$\begin{aligned} Tv &= T \sum_{i=1}^n a_i v_i = \sum_{i=1}^n ([v]_\beta)_i \sum_{j=1}^m ([T]_\beta^\gamma)_{ji} w_j \\ &= \sum_{j=1}^m \sum_{i=1}^n ([T]_\beta^\gamma)_{ji} ([v]_\beta)_i w_j = \sum_{j=1}^m ([T]_\beta^\gamma [v]_\beta)_j w_j, \end{aligned}$$

as desired. ♠

**Remark 2.22.** Let  $A \in M_{m \times n}(\mathbb{F})$ . Then Proposition 2.13 suggests that there exist a function  $L_A : \mathbb{F}^n \rightarrow \mathbb{F}^m$  defined by

$$v \mapsto Av.$$

**Def'n. Left Multiplication Transformation of a Matrix**

Consider Remark 2.22. We say  $L_A$  the *left multiplication transformation* of  $A$ .

**Remark 2.23.** We shall consistently write  $L_A$  to denote the left multiplication transformation of  $A \in M_{m \times n}(\mathbb{F})$ .

**Proposition 2.14.**

Let  $A \in M_{m \times n}(\mathbb{F})$  and  $L_A : \mathbb{F}^n \rightarrow \mathbb{F}^m$  be the left multiplication transformation of  $A$ . Then  $L_A$  is linear. Moreover, let  $B \in M_{m \times n}(\mathbb{F})$  and let  $L_B : \mathbb{F}^n \rightarrow \mathbb{F}^m$ .

(a)  $[L_A]_\beta = A$ .

(b)  $L_A = L_B$  if and only if  $A = B$ .

(c)  $L_{A+B} = L_A + L_B$  and  $L_{aA} = aL_A$  for all  $a \in \mathbb{F}$ .

(d) If  $T : \mathbb{F}^n \rightarrow \mathbb{F}^m$  is linear, then there exists a unique  $C \in M_{m \times n}(\mathbb{F})$  such that  $T = L_C$ . In fact,  $C = [T]_\beta^\gamma$ .

(e) If  $E \in M_{n \times p}(\mathbb{F})$ , then  $L_{AE} = L_A L_E$ .

(f)  $L_I = I$ .

Here,  $\beta$  and  $\gamma$  denotes the standard ordered bases for  $\mathbb{F}^n$  and  $\mathbb{F}^m$ , respectively.

**Proposition 2.15.**  
**Matrix Multiplication**  
**Is Associative**

Let  $A, B, C$  be matrices such that  $A(BC)$  is defined. Then  $(AB)C$  is also defined and  $A(BC) = (AB)C$ . That is, matrix product is associative.

*Proof.* Let  $A \in M_{m \times n}(\mathbb{F})$  then for  $A(BC)$  to be defined,  $(BC) \in M_{n \times q}(\mathbb{F})$ . That is,  $B \in M_{n \times p}(\mathbb{F})$  and  $C \in M_{p \times q}(\mathbb{F})$ . So  $AB$  is defined, and  $AB \in M_{m \times p}$ , so  $(AB)C$  is defined as well. From (e) of Proposition 2.14,

$$L_A(L_{BC}) = L_A(L_B L_C) = (L_A L_B) L_C = (L_{AB}) L_C.$$

Then the result follows from (b) of Proposition 2.14. ♠

## Invertibility and Isomorphisms

**Remark 2.24.** By utilizing invertibility of functions, we may investigate inverse of a matrix by using linear transformation  $L_A = A$ . In particular, if  $T$  is linear, then  $T^{-1}$  is linear, so  $L_A^{-1}$  can be used to determine properties of  $A^{-1}$ . It turns out that the concept of isomorphism is related to invertibility, which is discussed in this section as well. Consider the following definition.

**Def'n. Inverse of a Linear Transformation**

Let  $V, W$  be vector spaces and let  $T : V \rightarrow W$  be linear. We say a function  $U : W \rightarrow V$  is the *inverse* of  $T$  if  $TU = I : W \rightarrow W$  and  $UT = I : V \rightarrow V$ . If such  $U$  exists, then we say  $T$  is *invertible*, and denote  $U$  by  $T^{-1}$ .

**Remark 2.25.** Suppose that  $f$  and  $g$  are invertible functions such that  $fg$  is well-defined. Then

- (a)  $(fg)^{-1} = g^{-1}f^{-1}$  and
- (b)  $(f^{-1})^{-1} = f$ . In particular,  $f^{-1}$  is invertible.

An important property of invertible function is that  $f$  is invertible if and only if  $f$  is bijective. Combining this with Proposition 2.6 shows that, a linear transformation  $T : V \rightarrow W$  is invertible if and only if  $\dim(V) = \text{rank}(T)$ , where  $V, W$  are some vector spaces. Moreover, it turns out that  $T^{-1} : W \rightarrow V$  is linear as well.

**Proposition 2.16.**  
 **$T^{-1}$  Is Linear**

Let  $V, W$  be vector spaces and let  $T : V \rightarrow W$  be linear. Then  $T^{-1} : W \rightarrow V$  is linear.

*Proof.* Let  $v, u \in V$  and  $c \in \mathbb{F}$  be arbitrary. Then

$$T^{-1}(cTv + Tu) = T^{-1}(T(cv + u)) = cv + u = cT^{-1}(Tv) + T^{-1}(Tu). \quad \spadesuit$$

**Remark 2.26.** We also have a natural matrix analogue of the inverse of a linear transformation.

**Def'n. Inverse of a Matrix**

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $A$  is *invertible* if there exists  $B \in M_{n \times n}(\mathbb{F})$  such that  $AB + BA = I$ . Such  $B$  is unique and we denote  $B = A^{-1}$ .

**Proposition 2.17.**

Let  $V, W$  be finite-dimensional vector spaces. Then there exists an invertible  $T : V \rightarrow W$  if and only if  $\dim(V) = \dim(W)$ .

*Proof.* From Remark 2.25,  $T$  is invertible if and only if  $\dim(V) = \text{rank}(T)$ . But by Proposition 2.6,  $T$  is invertible if and only if  $T$  is surjective, which exactly means  $\text{rank}(T) = \dim(W)$ . For the reverse direction, if  $\dim(V) = \dim(W)$ , and  $\{v_1, v_2, \dots, v_n\}$  and  $\{w_1, w_2, \dots, w_n\}$  are bases for  $V$  and  $W$  respectively, then  $T : V \rightarrow W$  defined by

$$v_i \mapsto w_i$$

is clearly invertible. ♠

**Proposition 2.18.**  
 **$T$  Is Invetible If and**  
**Only If  $[T]^\gamma_\beta$  Is**  
**Invertible**

*Let  $V, W$  be finite-dimensional vector spaces with ordered bases  $\beta$  and  $\gamma$ , respectively. Let  $T : V \rightarrow W$  be linear. Then  $T$  is invertible if and only if  $[T]^\gamma_\beta$  is invertible. Furthermore,  $[T^{-1}]^\beta_\gamma = ([T]^\gamma_\beta)^{-1}$ .*

*Proof.* For the forward direction, suppose that  $T$  is invertible. Then by Proposition 2.17,  $\dim(V) = \dim(W) = n$ , so  $[T]^\gamma_\beta \in M_{n \times n}(\mathbb{F})$ . Since  $T^{-1} : W \rightarrow V$  satisfies  $TT^{-1} = I : W \rightarrow W$ ,

$$[T]^\gamma_\beta [T^{-1}]^\beta_\gamma = [TT^{-1}]^\gamma_\gamma = [I]^\gamma_\gamma$$

so  $[T]^\gamma_\beta$  is invertible and  $([T]^\gamma_\beta)^{-1} = [T^{-1}]^\beta_\gamma$ . For the reverse direction, suppose  $A = ([T]^\gamma_\beta)$  is invertible. Then there is  $B \in M_{n \times n}(\mathbb{F})$  such that  $AB = BA = I$ . Then there exists a unique  $U : W \rightarrow V$  such that

$$Uw_j = \sum_{i=1}^n B_{ij}v_i,$$

for all  $j \in \{1, 2, \dots, n\}$ , where  $\gamma = \{w_1, w_2, \dots, w_n\}$  and  $\beta = \{v_1, v_2, \dots, v_n\}$ . By definition,  $B = [U]^\beta_\gamma$ , and

$$[UT]^\beta_\beta = [U]^\beta_\gamma [T]^\gamma_\beta = BA = I = [I]^\beta_\beta$$

so  $UT = I$  and, similarly,  $TU = I$ . ♠

**Corollary 2.18.1.**

*Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $A$  is invertible if and only if  $L_A$  is invertible. Furthermore,  $L_A^{-1} = L_{A^{-1}}$ .*

**Def'n. Isomorphism on Vector Spaces**

Let  $V, W$  be vector spaces. We say  $T : V \rightarrow W$  is an **isomorphism** if  $T$  is linear and invertible. If such  $T$  exists, then we say that  $V$  and  $W$  are **isomorphic**, denoted as

$$V \cong W.$$

**Remark 2.27.** Isomorphism is an equivalence relation.

**Proposition 2.19.**  
 **$V \cong W$  If and Only If**  
 **$\dim(V) = \dim(W)$**

*Let  $V, W$  be finite-dimensional vector spaces. Then  $V$  and  $W$  are isomorphic to each other if and only if  $\dim V = \dim W$ .*

*Proof.* For the forward direction, suppose that  $T : V \rightarrow W$  is an isomorphism. Then  $\text{nullity}(T) = 0$  so by rank-nullity theorem,

$$\dim(V) = \text{rank}(T) = \dim(W).$$

For the reverse direction, suppose  $\dim(V) = \dim(W)$ . Then there exists a linear transformation  $T : V \rightarrow W$  that satisfies

$$Tv_i = w_i,$$



where  $\{v_1, v_2, \dots, v_n\}$  and  $\{w_1, w_2, \dots, w_n\}$  are bases of  $V$  and  $W$ , respectively. Then  $T$  is an isomorphism, since

$$\text{image}(T) = \text{span}\{w_1, w_2, \dots, w_n\} = W. \quad \spadesuit$$

**Corollary 2.19.1.**

*Let  $V$  be a finite-dimensional vector space over  $\mathbb{F}$ . Then  $V \cong \mathbb{F}^n$  if and only if  $\dim(V) = n$ .*

**Remark 2.28.** We proceed to discuss the natural isomorphism between  $\mathcal{L}(V, W)$  and  $M_{m \times n}(\mathbb{F})$ , where  $\dim(V) = n$  and  $\dim(W) = m$ , as mentioned in Remark 2.7.

**Theorem 2.20.**

$$\mathcal{L}(V, W) \cong M_{m \times n}(\mathbb{F})$$

*Let  $V$  and  $W$  be finite dimensional vector spaces with  $\dim(V) = n$  and  $\dim(W) = m$ , and let  $\beta$  and  $\gamma$  be ordered bases for  $V$  and  $W$ , respectively. Then the function  $[\cdot]_\beta^\gamma : \mathcal{L}(V, W) \rightarrow M_{m \times n}(\mathbb{F})$  is an isomorphism.*

*Proof.* The linearity of  $[\cdot]_\beta^\gamma$  is supplied by Proposition 2.8. Now the claim is that  $[\cdot]_\beta^\gamma$  is surjective. To verify this, let  $A \in M_{m \times n}(\mathbb{F})$  be arbitrary. Then there exists a (unique) linear  $T : V \rightarrow W$  such that

$$Tv_j = \sum_{i=1}^m A_{ij}w_i$$

for all  $j \in \{1, 2, \dots, n\}$ . It follows from Proposition 2.6 that  $[\cdot]_\beta^\gamma$  is bijective.  $\spadesuit$

**Corollary 2.20.1.**

*Let  $V, W$  be finite-dimensional vector spaces with  $\dim(V) = n$  and  $\dim(W) = m$ . Then*

$$\dim(\mathcal{L}(V, W)) = mn.$$

**Remark 2.29.** Similar to how we define a natural isomorphism in terms of ordered bases,  $[\cdot]_\beta : V \rightarrow \mathbb{F}^n$  for any ordered basis  $\beta$  for a finite-dimensional vector space  $V$  is also an isomorphism. The linearity of  $[\cdot]_\beta$  follows immediately from the definition of the coordinate vector, and  $[\cdot]_\beta$  is surjective, since for any  $(c_1, c_2, \dots, c_n) \in \mathbb{F}^n$ ,

$$v = \sum_{i=1}^n c_i v_i \in V$$

is the unique representation of  $v$  as a linear combination of vectors in an ordered basis  $\beta = \{v_1, v_2, \dots, v_n\}$  for  $V$ .

**Def'n. Standard Representation of a Vector Space**

Let  $V$  be a  $n$ -dimensional vector space and let  $\beta$  be an ordered basis for  $V$ . The *standard representation* of  $V$  with respect to  $\beta$  is the isomorphism  $[\cdot]_\beta : V \rightarrow \mathbb{F}^n$ .

**Remark 2.30.** By using standard representation, we may restate Proposition 2.13 as follows.

**Proposition 2.21.**

*Let  $V, W$  be finite-dimensional vector spaces with  $\dim(V) = n$  and  $\dim(W) = m$ , and let  $\beta$  and  $\gamma$  be ordered bases for  $V$  and  $W$ , respectively. Let  $T : V \rightarrow W$  be linear and let  $A = [T]_\beta^\gamma$ . Then*

$$L_A [\cdot]_\beta = [\cdot]_\gamma T.$$

## The Change of Basis

### Proposition 2.22.

Let  $V$  be a finite-dimensional vector space and let  $\beta$  and  $\gamma$  be ordered bases for  $V$ . Let  $Q = [I]_{\gamma}^{\beta}$ . Then  $Q$  is invertible, and

$$[v]_{\beta} = Q[v]_{\gamma}$$

for all  $v \in V$ .

*Proof.* The invertibility of  $Q$  is a direct consequence of the invertibility of  $I : V \rightarrow V$ . Moreover, by Proposition 2.13,

$$[v]_{\beta} = [Iv]_{\beta} = [I]_{\gamma}^{\beta} [v]_{\gamma} = Q[v]_{\gamma}. \quad \spadesuit$$

### Def'n. Change of Basis Matrix

Consider Proposition 2.22. We call  $Q$  the *change of basis matrix* from  $\gamma$  to  $\beta$ .

**Remark 2.31.** Let  $V$  be a finite-dimensional vector space and let  $\beta = \{v_1, v_2, \dots, v_n\}$  and  $\gamma = \{u_1, u_2, \dots, u_n\}$  be ordered bases for  $V$ . Let  $Q \in M_{n \times n}(\mathbb{F})$  be the change of basis matrix from  $\gamma$  to  $\beta$ . Then

$$u_j = \sum_{i=1}^n Q_{ij} v_i$$

for all  $j \in \{1, 2, \dots, n\}$ . That is, the  $j$ th column of  $Q$  is  $[u_j]_{\beta}$ . Moreover  $Q^{-1}$  is the change of basis matrix from  $\beta$  to  $\gamma$ .

### Proposition 2.23.

Let  $T$  be a linear operator on  $V$  and  $\beta$  and  $\gamma$  be ordered bases for  $V$ . Suppose that  $Q$  is the change of basis matrix from  $\gamma$  to  $\beta$ . Then,

$$[T]_{\gamma} = Q^{-1} [T]_{\beta} Q.$$

*Proof.* Observe that

$$Q[T]_{\gamma} = [I]_{\gamma}^{\beta} [T]_{\gamma} = [IT]_{\gamma}^{\beta} = [TI]_{\gamma}^{\beta} = [T]_{\beta} [T]_{\gamma}^{\beta} = [T]_{\beta} Q.$$

That is,  $[T]_{\gamma} = Q^{-1} [T]_{\beta} Q$ . ♠

### Corollary 2.23.1.

Let  $A \in M_{n \times n}(\mathbb{F})$  and  $\gamma$  be an ordered basis for  $\mathbb{F}^n$ . Then  $[L_A]_{\gamma} = Q^{-1} A Q$ , where  $Q$  is the matrix whose  $j$ th column is the  $j$ th vector of  $\gamma$ .

**Remark 2.32.** Proposition 2.23 and Corollary 2.23.1 motivates the following definition.

### Def'n. Similar Matrices

Let  $A, B \in M_{n \times n}(\mathbb{F})$ . We say  $A$  and  $B$  are *similar* if there exists an invertible  $P \in M_{n \times n}(\mathbb{F})$  such that  $B = P^{-1} A P$ .

# 3.

## Linear Equations

- 
- 3.1 Elementary Matrix Operations and Elementary Matrices
  - 3.2 The Rank and Inverse of a Matrix
  - 3.3 Four Fundamental Subspaces of a Matrix
  - 3.4 Systems of Linear Equations
-

## Elementary Matrix Operations and Elementary Matrices

### Def'n. Elementary Operations on Matrix

Let  $A \in M_{m \times n}(\mathbb{F})$ . We define the three *elementary row operations* on  $A$  as follows.

- (a) Interchange any two rows of  $A$ .
- (b) Multiply any row of  $A$  by a nonzero scalar  $c \in \mathbb{F}$ .
- (c) Add a scalar multiple of any row of  $A$  to another row of  $A$ .

We say (a) is a *type 1* operation, (b) is a *type 2* operation, and (c) is a *type 3* operation.

**Remark 3.1.** We have an analogous definition for the three elementary column operations.

### Def'n. Elementary Matrix

We say a matrix  $E \in M_{n \times n}(\mathbb{F})$  is an *elementary matrix* if  $E$  is obtained by applying any elementary operation on  $I$ . Depending on which type of operation is used, we call that  $E$  is a *type 1*, *type 2*, or *type 3* elementary matrix, respectively.

**Remark 3.2.** Any elementary matrix can be obtained by at least two ways. That is, if  $E \in M_{n \times n}(\mathbb{F})$  is obtained by applying an elementary row operation on  $I$ , then there is an elementary column operation of the same type by applying which  $E$  is obtained from  $I$ .

### Theorem 3.1.

Let  $A \in M_{m \times n}(\mathbb{F})$ , and suppose that  $B$  is obtained from  $A$  by performing an elementary column [row] operation on  $A$ . Then there exists an  $n \times n$  [ $m \times m$ ] elementary matrix  $E$  such that  $B = AE$  [ $B = EA$ ]. In fact,  $E$  is obtained from  $I$  by performing the same elementary column [row] operation. Conversely, for any  $n \times n$  [ $m \times m$ ] elementary matrix  $E$ ,  $B = AE$  [ $B = EA$ ] is the matrix obtained by performing an elementary column [row] operation on  $I$  to obtain  $E$ .

### Proposition 3.2. Invertibility of Elementary Matrices

Let  $E \in M_{n \times n}(\mathbb{F})$  be elementary. Then  $E$  is invertible and  $E^{-1}$  is an elementary matrix of the same type.

*Proof.* Let  $E \in M_{n \times n}(\mathbb{F})$  be invertible. Then  $E$  can be obtained from  $I$  by performing elementary operations, so  $I$  can be obtained from  $E$  by reversing the operations. Then by Theorem 3.1, there exists an  $E' \in M_{n \times n}(\mathbb{F})$  such that  $EE' = E'E = I$ . Therefore  $E$  is invertible and  $E' = E^{-1}$ . ♠

## The Rank and Inverse of a Matrix

### Def'n. Rank of a Matrix

Let  $A \in M_{n \times n}(\mathbb{F})$ . We define the *rank* of  $A$ , denoted by  $\text{rank}(A)$ , to be the rank of the left multiplication transformation  $L_A : \mathbb{F}^n \rightarrow \mathbb{F}^m$ .

### Theorem 3.3. Invertible Matrix Theorem I

Let  $A \in M_{m \times n}(\mathbb{F})$ , and let  $P \in M_{m \times m}(\mathbb{F})$ ,  $Q \in M_{n \times n}(\mathbb{F})$  be invertible.

- (a)  $\text{rank}(AQ) = \text{rank}(A)$ .
- (b)  $\text{rank}(PA) = \text{rank}(A)$ .

$$(c) \operatorname{rank}(PAQ) = \operatorname{rank}(A).$$

*Proof.* For (a), observe that

$$\operatorname{rank}(AQ) = \operatorname{rank}(L_A Q) = \operatorname{rank}(L_A L_Q) = \dim(L_A L_Q(\mathbb{F}^n)) = \dim(L_A(\mathbb{F}^n)) = \operatorname{rank}(A),$$

since  $Q$  is an invertible matrix so  $L_Q$  is an isomorphism and  $L_Q(\mathbb{F}^n) = \operatorname{image}(L_Q) = \mathbb{F}^n$ . Similar argument can be used for (b). Observe that (c) is an immediate consequence of (a) and (b). ♠

### Corollary 3.3.1.

Let  $A \in M_{m \times n}(\mathbb{F})$ . Then, for all elementary  $E \in M_{n \times n}, F \in M_{m \times m}$ ,

$$\operatorname{rank}(A) = \operatorname{rank}(AE) = \operatorname{rank}(AF).$$

### Theorem 3.4. Invertible Matrix Theorem II

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $A$  is invertible if and only if  $\operatorname{rank}(A) = n$ .

*Proof.* For the forward direction, suppose that  $A$  is invertible. Then  $L_A$  is an isomorphism, so  $\operatorname{rank}(A) = \operatorname{rank}(L_A) = \dim(\mathbb{F}^n) = n$ . For the reverse direction, suppose  $\operatorname{rank}(A) = n$  then  $\operatorname{rank}(A) = n = \dim(\mathbb{F}^n)$  so  $L_A : \mathbb{F}^n \rightarrow \mathbb{F}^n$  is an isomorphism, and thus  $A$  is invertible. ♠

### Proposition 3.5. Rank of a Matrix Is the Maximal Number of Independent Columns

Let  $A \in M_{m \times n}(\mathbb{F})$ . Then  $\operatorname{rank}(A)$  is equal to the maximal number of independent columns.

*Proof.* Write  $A = [A_1 \ A_2 \ \cdots \ A_n]$  and let  $\alpha = \{A_1, A_2, \dots, A_n\}$ , the set of columns of  $A$ . Moreover, let  $\beta = \{e_1, e_2, \dots, e_n\}$  be the standard basis for  $\mathbb{F}^n$ . Then

$$\begin{aligned} \operatorname{rank}(A) &= \operatorname{rank}(L_A) = \dim(\operatorname{image}(L_A)) = \dim(L_A(\mathbb{F}^n)) = \dim(\operatorname{span}(L_A(\beta))) \\ &= \dim(\operatorname{span}\{Ae_1, Ae_2, \dots, Ae_n\}) = \dim(\operatorname{span}\{A_1, A_2, \dots, A_n\}) = \dim(\operatorname{span}(\alpha)). \end{aligned}$$

But  $\dim(\operatorname{span}(\alpha))$  is the maximal number of independent vectors of  $\alpha$ , which is the desired result. ♠

**Remark 3.3.** An important restatement of Proposition 3.5 is that, for any  $A \in M_{m \times n}(\mathbb{F})$ ,  $\operatorname{rank}(A)$  is the dimension of the subspace of  $\mathbb{F}^m$  that the columns of  $A$  span.

### Theorem 3.6. Matrix Elimination

Let  $A \in M_{m \times n}(\mathbb{F})$ . Then by finite number of elementary operations  $E_1, E_2, \dots, E_p$  on  $A$ ,  $A$  can be transformed into

$$E_p E_{p-1} \cdots A \cdots E_2 E_1 = \begin{bmatrix} I_r & O_1 \\ O_2 & O_3 \end{bmatrix},$$

where  $O_1, O_2, O_3$  are zero matrices and  $0 \leq r = \operatorname{rank}(A) \leq \min(m, n)$ .

*Proof.* Consider splitting the theorem into two cases. First suppose that  $A = 0$  then the proof is done. So suppose that  $A \neq 0$ . Then there must be a nonzero entry, by type 1 operations which can be moved to  $(1, 1)$  position. Then, by a type 2 operation, it can be turned into 1, and all  $(n, 1)$  entries can be made zero by type 3 operations. Observe that we have made a matrix of the form

$$\begin{bmatrix} I_1 & O \\ O & A' \end{bmatrix}.$$

So by proceeding on  $A'$  inductively, at most  $\min(m, n)$  times, we have the desired result. Moreover, since the number of inductive process is finite, we also observe that the number of elementary operations that are used to obtain a matrix of the desired form is finite. Lastly,

$$\text{rank}(A) = \text{rank}(I_r) = r$$

by Lemma 3.5 and invertible matrix theorem I, so  $0 \leq r = \text{rank}(A) \leq \min(m, n)$ . ♠

**Corollary 3.6.1.**

*For any  $A \in M_{m \times n}(\mathbb{F})$ , there exist invertible  $P \in M_{m \times m}(\mathbb{F})$  and  $Q \in M_{n \times n}(\mathbb{F})$  such that  $PAQ$  is of the form*

$$\begin{bmatrix} I_r & O \\ O & O \end{bmatrix}.$$

**Corollary 3.6.2.**

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

- (a)  $\text{rank}(A) = \text{rank}(A^T)$ .*
- (b)  $\text{rank}(A)$  is the number of maximal independent rows.*
- (c) Columns and rows of  $A$  span subspaces of  $\mathbb{F}^m$  of equal dimension.*

*Proof.* For (a), let  $P \in M_{m \times m}(\mathbb{F})$  and  $Q \in M_{n \times n}$  be invertible matrices discussed in Corollary 3.6.1. Then,

$$\text{rank}(A) = \text{rank}(PAQ) = \text{rank}((PAQ)^T) = \text{rank}(Q^T A^T P^T) = \text{rank}(A^T).$$

Observe that (b) and (c) are immediate consequences of (a) and Lemma 3.5. ♠

**Corollary 3.6.3.**  
**An Invertible Matrix Is a Product of Elementary Matrices**

*Let  $A \in M_{n \times n}(\mathbb{F})$  be invertible. Then  $A$  is a product of elementary matrices.*

*Proof.* Since  $A$  is invertible, by invertible matrix theorem II,  $\text{rank} A = n$ , and by Theorem 3.6 and Corollary 3.6.1, there exist invertible  $P = \prod_{i=1}^p E_i, Q = \prod_{j=1}^q F_j \in M_{n \times n}(\mathbb{F})$  such that

$$PAQ = I.$$

That is,

$$A = P^{-1}IQ^{-1} = P^{-1}Q^{-1} = E_p^{-1}E_{p-1}^{-1} \cdots E_2^{-1}E_1^{-1}F_q^{-1}F_{q-1}^{-1} \cdots F_2^{-1}F_1^{-1},$$

where each  $E_i^{-1}$  and  $F_i^{-1}$  are elementary matrices by Proposition 3.2. ♠

**Proposition 3.7.**

*Let  $A \in M_{m \times n}(\mathbb{F})$  and  $B \in M_{n \times p}(\mathbb{F})$ . Then*

$$\text{rank}(AB) = \min(\text{rank}(A), \text{rank}(B)).$$

*Proof.* First, suppose  $\text{rank}(A) \leq \text{rank}(B)$ . Observe that

$$\text{rank}(AB) = \text{rank}(L_{AB}) = \text{rank}(L_A L_B) = \dim(L_A(\text{image}(L_B)))$$

where  $\text{image}(L_B) \subseteq \mathbb{F}^n$  so  $L_A(\text{image}(L_B)) \subseteq L_A(\mathbb{F}^n)$ . Thus

$$\dim(L_A(\text{image}(L_B))) \leq \dim(L_A(\mathbb{F}^n)) = \dim(\text{image}(L_A)) = \text{rank}(A).$$

When  $\text{rank}(B) \leq \text{rank}(A)$ , the same argument can be used by taking the transpose of  $AB, B^T A^T$ . ♠

## Four Fundamental Subspaces of a Matrix

**Def'n. Column Space, Row Space, Null Space, Left Null Space** of a Matrix

Let  $A \in M_{m \times n}(\mathbb{F})$ . Define the *column space* of  $A$ ,  $\text{image}(A)$ , by

$$\text{image}(A) = \text{span} \{x \in \mathbb{F}^m : x \text{ column of } A\} \subseteq \mathbb{F}^m.$$

Similarly, define the *row space* of  $A$ ,  $\text{image}(A^T)$ , by

$$\text{image}(A^T) = \text{span} \{x \in \mathbb{F}^n : x \text{ row of } A\} \subseteq \mathbb{F}^n.$$

Moreover, define the *null space* of  $A$ ,  $\ker(A)$ , by

$$\ker(A) = \{x \in \mathbb{F}^n : Ax = 0\} \subseteq \mathbb{F}^n.$$

Lastly, define the *left null space* of  $A$ ,  $\ker(A^T)$ , by

$$\ker(A^T) = \{x \in \mathbb{F}^m : A^T x = 0\} \subseteq \mathbb{F}^m.$$

$\text{image}(A)$ ,  $\text{image}(A^T)$ ,  $\ker(A)$ ,  $\ker(A^T)$  together are called the *four fundamental subspaces* of  $A$ .

### Proposition 3.8. Properties of Four Fundamental Subspaces

Let  $A \in M_{m \times n}(\mathbb{F})$ . Then the following holds.

- (a)  $\text{image}(A)$  and  $\ker(A^T)$  are subspaces of  $\mathbb{F}^m$  and  $\text{image}(A^T)$  and  $\ker(A)$  are subspaces of  $\mathbb{F}^n$ .
- (b)  $\text{rank}(A) = \dim(\text{image}(A^T)) = \dim(\text{image}(A))$ .
- (c)  $\dim(\text{image}(A)) + \dim(\ker(A^T)) = m$  and  $\dim(\text{image}(A^T)) + \dim(\ker(A)) = n$ .
- (d)  $\text{image}(A) \oplus \ker(A^T) = \mathbb{F}^m$  and  $\text{image}(A^T) \oplus \ker(A) = \mathbb{F}^n$ .

*Proof.* For (a), use Proposition 1.7 for each set. For (b), observe that

$$\begin{aligned} \text{rank}(A) &= \text{the number of linearly independent columns of } A \\ &= \dim(\text{span} \{\text{Col}_1(A), \dots, \text{Col}_n(A)\}) = \dim(\text{Col}(A)), \end{aligned}$$

and similar proof holds for  $\text{rank}(A) = \dim(\text{image}(A^T))$ . For (c), observe that

$$\dim(\mathbb{F}^n) = \dim(\text{image}(L_A)) + \dim(\ker(L_A)) = \text{rank}(A) + \dim(\ker(A)) = \dim(\text{image}(A^T)) + \dim(\ker(A)),$$

by rank-nullity theorem, and similar proof holds for the remaining part of the statement. For (d), observe that

$$\text{image}(A^T) \cap \ker(A) = \{0\},$$

so  $\text{image}(A^T) \oplus \ker(A)$  is well defined. Then we have

$$\dim(\text{image}(A^T) \oplus \ker(A)) = \dim(\text{image}(A^T)) + \dim(\ker(A)) - \dim(\text{image}(A^T) \cap \ker(A)) = n,$$

where  $\text{image}(A^T) \oplus \ker(A) \subseteq \mathbb{F}^n$ , so  $\text{image}(A^T) \oplus \ker(A) = \mathbb{F}^n$ . Again, similar proof holds for the remaining part of the statement. ♠

**Theorem 3.9.**  
**Invertible Matrix**  
**Theorem III**

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then the following are equivalent.

- (a)  $A$  is invertible.
- (b) Columns of  $A$  form a basis for  $\mathbb{F}^n$ .
- (c) Rows of  $A$  form a basis for  $\mathbb{F}^n$ .
- (d)  $A$  is a product of elementary matrices.

*Proof.* Consider showing that (a) is equivalent to other statements. For (a)  $\iff$  (b), observe that

$$\begin{aligned} A \text{ is invertible} &\iff \text{rank}(A) = n \\ &\iff \text{maximal number of independent columns is } n \\ &\iff \text{columns of } A \text{ form a basis for } \mathbb{F}^n. \end{aligned}$$

Observe that similar proof holds for (a)  $\iff$  (c). (a)  $\implies$  (d) is provided by Corollary 3.6.3. (d)  $\implies$  (a) is also clear, since each elementary matrix is invertible. ♠

**Def'n. Augmented Matrix**

A matrix of the form  $[A \mid B]$  for some  $A \in M_{m \times n}(\mathbb{F})$  and  $B \in M_{m \times p}(\mathbb{F})$  is called an *augmented matrix*.

**Proposition 3.10.**  
**Computing the**  
**Inverse Matrix**

Let  $A \in M_{n \times n}(\mathbb{F})$  be invertible. Then the following hold.

- (a) There exists finite number of row operations that transforms  $[A \mid I]$  into  $[I \mid A^{-1}]$ .
- (b) If there exists  $B \in M_{n \times n}(\mathbb{F})$  such that  $[I \mid B]$  is obtained from  $[A \mid I]$  by a finite number of row operations, then  $A$  is invertible and  $B = A^{-1}$ .

*Proof.* For (a), write  $C = [A \mid I] = [C_1 \ C_2 \ \cdots \ C_m]$  for convenience. Then for any  $B \in M_{n \times n}(\mathbb{F})$ ,

$$BC = [BC_1 \ BC_2 \ \cdots \ BC_m],$$

so

$$A^{-1}[A \mid I] = [I \mid A^{-1}],$$

where  $A^{-1} = E_1 E_2 \cdots E_p$  for some elementary matrices  $E_1, \dots, E_p \in M_{n \times n}(\mathbb{F})$  by Theorem 3.9. That is,

$$E_1 \cdots E_p [A \mid I] = [I \mid A^{-1}]$$

which means there exist corresponding row operations to  $E_1, \dots, E_p$  that transform  $[A \mid I]$  into  $[I \mid A^{-1}]$ . For (b), observe that there are elementary matrices  $G_1, \dots, G_q$  corresponding to row operations that transform  $[A \mid I]$  into  $[I \mid B]$ . That is,

$$G_1 \cdots G_q [A \mid I] = [G_1 \cdots G_q A \mid G_1 \cdots G_q I] = [I \mid B],$$

so  $G_1 \cdots G_q = A^{-1}$  and thus  $B = G_1 \cdots G_q = A^{-1}$ , as desired. ♠

## Systems of Linear Equations



**Def'n. System of Linear Equations**

A collection of linear equations of the form

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

where  $a_{ij}, b_i \in \mathbb{F}$  for all  $i \in \{1, \dots, m\}, j \in \{1, \dots, n\}$  and  $x_1, \dots, x_n$  are  $n$  variables taking values in  $\mathbb{F}$ , is called a **system of linear equations** in  $n$  unknowns over  $\mathbb{F}$ .

**Def'n. Coefficient Matrix, Augmented Matrix, Solution, Solution Set of a System**

Any system can be written as a matrix product  $Ax = b$ , where

$$Ax = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = b.$$

Moreover, the matrix  $A$  and  $[A \mid b]$  are called the **coefficient matrix** and **augmented matrix** of the system, respectively. We say  $c \in \mathbb{F}^n$  is a **solution** of the system if it satisfies  $Ac = b$ . The set of all solutions  $\{c \in \mathbb{F}^n : Ac = b\}$  is called the **solution set** of the system.

**Def'n. Consistent, Inconsistent, Homogeneous, Inhomogeneous System**

A system  $Ax = b$  is called **consistent** if its solution set is nonempty and **inconsistent** otherwise. Moreover, it is called **homogeneous** if  $b = 0$  and **inhomogeneous** otherwise.

**Proposition 3.11.**  
**The Solution Set of a Homogeneous System Is a Subspace**

Let  $A \in M_{m \times n}(\mathbb{F})$  and consider  $Ax = 0$ . Then the solution set  $K_H$  of the system is a subspace of  $\mathbb{F}^n$  and

$$\dim(K_H) = n - \text{rank}(A).$$

*Proof.* Observe that  $A0 = 0$  so  $0 \in K_H$ . For closure under subtraction, let  $v, u \in K_H$  then

$$A(v - u) = Av - Au = 0 - 0 = 0$$

so  $(v - u) \in K_H$ . For closure under multiplication, let  $c \in \mathbb{F}$  then

$$A(cv) = c(Av) = c0 = 0$$

so  $cv \in K_H$ . Moreover, observe that  $K_H = \ker(L_A)$ , so by the rank-nullity theorem

$$n = \dim(\mathbb{F}^n) = \text{nullity}(L_A) + \text{rank}(L_A) = \dim(\ker(L_A)) + \text{rank}(A) = \dim(K_H) + \text{rank}(A)$$

rearranging which in terms of  $\dim(K_H)$  gives

$$\dim(K_H) = n - \text{rank}(A).$$



**Corollary 3.11.1.**  
**Properties of the**  
**Solution Set of a**  
**Homogeneous**  
**System**

Let  $K_H$  be the solution set to  $Ax = 0$ . Then the following hold.

- (a)  $K_H \neq \emptyset$ . In particular,  $0 \in K_H$ .
- (b)  $K_H = \{0\} \iff \text{rank}(A) = n$ .
- (c) If  $m < n$ , then the system has a nonzero solution.

**Def'n. Full Column Rank of a System**

We say a system  $Ax = b$  is of **full column rank** if it satisfies (b) of Corollary 3.11.1.

**Proposition 3.12.**  
 **$K = K_H + \{c\}$  for any**  
**Particular Solution  $c$**

Suppose  $A \in M_{m \times n}(\mathbb{F})$  and  $b \in \mathbb{F}^m$ . Let  $K$  and  $K_H$  be the solution sets for  $Ax = b$  and  $Ax = 0$ , respectively. Then for any solution  $c$  to  $Ax = b$ , we have

$$K = \{c\} + K_H = \{c + k : k \in K_H\}.$$

*Proof.* Let  $x \in \mathbb{F}^n$  such that  $Ax = b$ . Then for any  $k \in K_H$ , observe that

$$A(x + k) = Ax + Ak = Ax + 0 = Ax = b,$$

so  $(x + k) \in K$ . Moreover, if  $z \in \mathbb{F}^n$  such that  $Az = b$ , then

$$A(x - z) = b - b = 0$$

so  $(x - z) \in K_H$ . In other words, there exists  $w = (x - z) \in K_H$  such that

$$x = z + w. \quad \spadesuit$$

**Theorem 3.13.**  
**Invertible Matrix**  
**Theorem IV**

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $A$  is invertible if and only if  $Ax = b$  has a unique solution.

*Proof.* For the forward direction, suppose that  $A$  is invertible. From  $Ax = b$ , we have

$$A^{-1}b = A^{-1}Ax = Ix = x,$$

so  $Ax = b$  has a unique solution  $x = A^{-1}b$ . For the reverse direction, suppose  $Ax = b$  has a unique solution  $c \in \mathbb{F}^n$ . Let  $K_H$  and  $K$  be the solution sets for  $Ax = 0$  and  $Ax = b$ , respectively. By Proposition 3.12,

$$K = \{c\} = \{c\} + K_H$$

so  $K_H = \{0\}$  and  $\dim(K_H) = 0$ . Since

$$\dim(K_H) = n - \text{rank}(A),$$

it follows that  $\text{rank}(A) = n$ , which means  $A$  is invertible.  $\spadesuit$

**Proposition 3.14.**  
**A System Is**  
**Consistent If and**  
**Only If**  
 $\text{rank}(A) = \text{rank}[A \mid b]$

Let  $Ax = b$  be a system of linear equations. Then the system is consistent if and only if  $\text{rank}(A) = \text{rank}[A \mid b]$ .

*Proof.* Observe that

$$\begin{aligned}
 Ax = b & \text{ has a solution} \\
 \iff b & \in \text{image}(L_A) \\
 \iff b & \in \text{span}\{\text{Col}_1(A), \dots, \text{Col}_n(A)\} \\
 \iff \text{span}\{\text{Col}_1(A), \dots, \text{Col}_n(A)\} &= \text{span}\{\text{Col}_1(A), \dots, \text{Col}_n(A), b\} \\
 \iff \dim(\text{span}\{\text{Col}_1(A), \dots, \text{Col}_n(A)\}) &= \dim(\text{span}\{\text{Col}_1(A), \dots, \text{Col}_n(A), b\}) \\
 \iff \text{rank}(A) &= \text{rank}[A \mid b],
 \end{aligned}$$

which is the desired result. ♠

### Def'n. Equivalent Systems

Two systems of linear equations are called **equivalent** if they have the same solution set.

### Proposition 3.15. $C Ax = C b$ Is Equivalent to $Ax = b$ Whenever $C$ Is Invertible

Let  $Ax = b$  be a system of  $m$  linear equations in  $n$  unknowns and let  $C \in M_{m \times n}(\mathbb{F})$  be invertible. Then the system  $(CA)x = Cb$  is equivalent to  $Ax = b$ .

*Proof.* Let  $K_H$  be the solution set of  $Ax = b$  and suppose that  $x \in K_H$ . Then

$$(CA)x = C(Ax) = Cb,$$

so  $x$  is in the solution set of  $C Ax = C b$  as well. Moreover, suppose that  $x$  is in the solution set of  $(CA)x = Cb$ , then

$$CAx = Cb \iff C^{-1}CAx = C^{-1}Cb \iff Ax = b.$$

Thus  $x \in K_H$ , which is the desired result. ♠

### Corollary 3.15.1.

Let  $Ax = b$  be a system of  $m$  linear equations in  $n$  unknowns. If  $[A' \mid b']$  is obtained from  $[A \mid b]$  by a finite number of elementary row operations, then the system  $A'x = b'$  is equivalent to  $Ax = b$ .

### Def'n. Reduced Row Echelon Form (RREF), Leading One

A matrix is said to be in **reduced row echelon form** if the following three conditions are satisfied.

- Any row containing nonzero entry precedes any row in which all the entries are zero, if any.
- The first nonzero entry in each row is the only nonzero entry in its column.
- The first nonzero entry in each row is 1, called the **leading one** of the row, and it occurs a column to the right of the first nonzero entry in the preceding row.

**Remark 3.4.** Given  $A \in M_{m \times n}(\mathbb{F})$ , we may obtain an RREF from  $A$  as follows.

- In the leftmost nonzero column, use elementary row operations to get 1 in the first row.
- By means of type 3 elementary row operations, use the first row to obtain zeroes in the remaining entries of the leftmost nonzero column.
- Consider the submatrix consisting of the columns to the right of the column we just modified and the rows beneath the row that just got a leading one. Use elementary row operations - if necessary - to get a leading one in the top of the first nonzero column of this submatrix.

- (d) Use elementary row operations to obtain zeroes below the one created in the preceding step.
- (e) Repeat (c) and (d) until no nonzero rows remain.
- (f) Work upward, beginning with the last nonzero row and add multiples of each row above to create zeroes above the first nonzero in each row.
- (g) Repeat the process in (f) for each preceding row until it is performed with the second row, at which time the reduction process is complete.

### Def'n. Gaussian Elimination

We call the procedure described in Remark 3.4 the *Gaussian elimination*.

### Proposition 3.16. Gaussian Elimination

*Gaussian elimination transforms any matrix to its RREF, and the RREF of a matrix is unique.*

### Def'n. Free Variable

Let  $R$  be the RREF of a coefficient matrix of a system of linear equations  $Ax = b$ . If the  $j$ th column of  $R$  does not contain a leading one, then  $x_j$  is called a *free variable*.

### Proposition 3.17. Number of Free Variables Is Equal to $n - \text{rank}(A)$

*Let  $A \in M_{m \times n}(\mathbb{F})$ ,  $b \in \mathbb{F}$ , and  $B$  be the RREF of  $A$ . Then the following holds.*

$$\text{number of free variables} = n - \text{number of leading ones} = n - \text{rank}(A).$$

*Proof.* Observe that

$$\text{rank}(A) = \text{rank}(B) = \text{number of leading ones of } B = \text{number of nonzero rows of } B. \quad \spadesuit$$

**Remark 3.5.** Let  $A \in M_{m \times n}(\mathbb{F})$  and  $b \in \mathbb{F}$ . Consider solving the system  $Ax = b$  by the following algorithm.

- (a) Write the augmented matrix  $[A \mid b]$  for the system.
- (b) Use elementary row operations (e.g. Gaussian elimination) to transform the augmented matrix into its RREF  $[A' \mid b']$ .
- (c) Write the system of linear equations to the RREF.
- (d) If the system contain an equation of the form  $0 = 1$ , then the system is inconsistent.
- (e) Otherwise, assign values  $t_1, \dots, t_{n-r}$  to the free variables and then solve the remaining variables in terms of the free variables. Here  $r = \text{rank}(A') = \text{rank}(A)$  is the number of nonzero rows of  $A'$ .
- (f) Then an arbitrary solution to  $Ax = b$  is of the form

$$x = x_0 + \sum_{i=1}^{n-r} t_i u_i$$

where  $r$  is the number of nonzero rows in  $A'$ .

Then  $K$  is given by

$$K = \left\{ x \in \mathbb{F}^n : x = x_0 + \sum_{i=1}^{n-r} t_i u_i \right\}.$$

**Def'n. Parametric Value** Assigned to Free Variables

The values  $t_1, \dots, t_{n-r}$  assigned to free variables in (e) of Remark 3.4 are called *parametric values*.

**Proposition 3.18.**

Let  $[A \mid b]$  be a consistent system of  $m$  linear equations in  $n$  variables. Suppose that the RREF of  $[A \mid b]$  has  $r$  nonzero rows. If the general solution to  $Ax = b$  obtained by the procedure described in Remark 3.4 is of the form

$$x = x_0 + \sum_{i=1}^{n-r} t_i u_i,$$

then  $x_0 \in \mathbb{F}^n$  is a solution to  $Ax = b$  and  $\{u_1, \dots, u_{n-r}\}$  is a basis for the solution set of the corresponding homogeneous system  $Ax = 0$ .

*Proof.* To verify that  $x_0$  is a solution to  $Ax = b$ , observe that, by setting  $t_1, \dots, t_{n-r} = 0$ ,

$$x = x_0 + \sum_{i=1}^{n-r} 0u_i = x_0.$$

So, we may verify that  $\{u_1, \dots, u_{n-r}\}$  generates  $K_H$  the following. First, write

$$K = \{x_0\} + K_H,$$

where  $K_H$  and  $K$  are solution sets of  $Ax = 0$  and  $Ax = b$ , respectively. Observe that

$$K = \left\{ x : x = x_0 + \sum_{i=1}^{n-r} t_i u_i \right\} = \{x_0\} + \left\{ x : x = \sum_{i=1}^{n-r} t_i u_i \right\},$$

so it must be the case which  $K_H = \left\{ x : x = \sum_{i=1}^{n-r} t_i u_i \right\}$ . But this means  $K_H = \text{span}\{u_1, \dots, u_{n-r}\}$ . Lastly, to verify that  $\{u_1, \dots, u_{n-r}\}$  is linearly independent, observe that

$$\dim(K_H) = n - \text{rank}(A) = n - r$$

by Proposition 3.11. ♠

*This page intentionally left blank.*

# 4.

## Determinants

- 
- 4.1 Determinants
  - 4.2 Properties of Determinants
-

## Determinants

### Def'n. Determinant, Cofactor, Cofactor Expansion

Let  $A \in M_{n \times n}(\mathbb{F})$ . We define the **determinant** of  $A$ , denoted by  $\det A$  or  $|A|$ , as follows.

(a) If  $n = 1$ , then

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

(b) For each  $n \in \mathbb{N} \setminus \{1\}$ ,  $\det A$  is defined recursively as

$$\det(A) = \sum_{i=1}^n (-1)^{1+i} A_{i1} \left( \det \tilde{A}_{i1} \right),$$

where  $\tilde{A}_{ij}$  is the  $(n-1) \times (n-1)$  matrix obtained by removing  $i$ th row and  $j$ th column.

The scalar  $(-1)^{i+j} \det(\tilde{A}_{ij})$  is called the **cofactor** of the entry of  $A$  in row  $i$  and column  $j$ . The above determinant equation is also known as the **cofactor expansion along the first column** of  $A$ .

**Remark 4.1.** The expression

$$\sum_{i=1}^n (-1)^{j+i} A_{ij} \left( \det(\tilde{A}_{ij}) \right)$$

is called the cofactor expansion along the  $j$ th column of  $A$ .

**Remark 4.2.** For  $A \in M_{2 \times 2}(\mathbb{F})$ , we have

$$\det(A) = A_{11}A_{22} - A_{12}A_{21}.$$

**Remark 4.3.** For simplicity, we are going to write

$$A = [A_1, A_2, \dots, A_n]$$

to denote  $A \in M_{n \times n}(\mathbb{F})$  with rows  $A_1, A_2, \dots, A_n$ .

### Proposition 4.1. $n$ -Linearity of Determinants

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then the determinant of  $A$  is a linear function of each row, when the remaining rows are held fixed. That is, for each  $k \in \{1, \dots, n\}$ , we have

$$\det[A_1, \dots, B_k + \alpha C_k, \dots, A_n] = \det[A_1, \dots, B_k, \dots, A_n] + \alpha \det[A_1, \dots, C_k, \dots, A_n].$$

*Proof.* Write

$$A = [A_1, \dots, B_k + \alpha C_k, \dots, A_n] \quad B = [A_1, \dots, B_k, \dots, A_n] \quad C = [A_1, \dots, C_k, \dots, A_n].$$

Then by definition,

$$\begin{aligned} \det(A) &= \sum_{i=1}^n (-1)^{1+i} A_{i1} \det(\tilde{A}_{i1}) \\ &= \sum_{i=1, i \neq k}^n (-1)^{1+i} A_{i1} \det(\tilde{A}_{i1}) + (-1)^{1+k} A_{k1} \det(\tilde{A}_{k1}). \end{aligned}$$

Observe that

$$\tilde{A}_{k1} = \tilde{B}_{k1} = \tilde{C}_{k1} \quad \text{and} \quad A_{k1} = B_{k1} + \alpha C_{k1}.$$



For  $i \neq k$ , the matrices  $\tilde{A}_{i1}, \tilde{B}_{i1}, \tilde{C}_{i1}$  have the same rows, except for one row  $i_0 = k - 1$  if  $i < k$  and  $i_0 = k$  if  $j > k$ . Moreover, row  $i_0$  of  $\tilde{A}_{i1}, \tilde{B}_{i1}, \tilde{C}_{i1}$  is  $(B_k + \alpha C_k), B_k, C_k$ , respectively. So by induction hypothesis,


$$\det(\tilde{A}_{i1}) = \det(\tilde{B}_{i1}) + \alpha \det(\tilde{C}_{i1})$$

and

$$A_{i1} = B_{i1} = C_{i1}$$

for each  $i \neq k$ . Plugging these equalities into the cofactor expansion along the first column of  $A$ , we get

$$\begin{aligned} \det(A) &= \sum_{i=1}^n (-1)^{1+i} A_{i1} \cdot \det(\tilde{A}_{i1}) \\ &= \sum_{i=1, i \neq k}^n (-1)^{1+i} A_{i1} \cdot \det(\tilde{A}_{i1}) + (-1)^{1+k} A_{k1} \cdot \det(\tilde{A}_{k1}) \\ &= \sum_{i=1, i \neq k}^n (-1)^{1+i} A_{i1} \cdot (\det(\tilde{B}_{i1}) + \alpha \det(\tilde{C}_{i1})) \\ &\quad + (-1)^{1+k} (B_{k1} + \alpha C_{k1}) \cdot \det(\tilde{A}_{k1}) \\ &= \sum_{i=1}^n (-1)^{1+i} B_{i1} \cdot \det(\tilde{B}_{i1}) + \alpha \sum_{i=1}^n (-1)^{1+i} C_{i1} \cdot \det(\tilde{C}_{i1}) \\ &= \det(B) + \alpha \det(C), \end{aligned}$$

which is the desired result. 

**Corollary 4.1.1.**  
**Determinant Is Zero A**  
**If Has a Zero Row**


*Let  $A \in M_{n \times n}(\mathbb{F})$ . If  $A$  has a zero row, then  $\det(A) = 0$ .*

*Proof.* Write

$$A = [R_1, \dots, R_k, \dots, R_n]$$

where  $R_k = 0$ . Then,

$$\begin{aligned} \det A &= \det [R_1, \dots, R_k, \dots, R_n] = \det [R_1, \dots, 2R_k, \dots, R_n] \\ &= 2 \det [R_1, \dots, R_k, \dots, R_n] = 2 \det(A) \end{aligned}$$

so  $\det(A) = 0$ . 

**Corollary 4.1.2.**  
**Determinants after a**  
**Type 2 Elementary**  
**Row Operation**


*Let  $A \in M_{n \times n}(\mathbb{F})$  and  $Q \in M_{n \times n}(\mathbb{F})$  be the matrix obtained from  $A$  by multiplying a row of  $A$  by a scalar  $\alpha \in \mathbb{F}$ . Then  $\det(Q) = \alpha \det(A)$ .*

*Proof.* Write

$$A = [R_1, \dots, R_n]$$

and suppose that  $Q$  is obtained by multiplying row  $k$  of  $A$ ,  $R_k$ , by  $\alpha$ . Then

$$\det(Q) = \det [R_1, \dots, \alpha R_k, \dots, R_n] = \alpha \det [R_1, \dots, R_k, \dots, R_n] = \alpha \det A,$$

which is the desired result. 

**Lemma 4.2.**  
 **$\det(A) = 0$  If Two**  
**Adjacent Rows Are**  
**Equal**

*Let  $A \in M_{n \times n}(\mathbb{F})$ . If two adjacent rows of  $A$  are equal, then  $\det A = 0$ .*

*Proof.* We proceed by induction. Let  $P(n)$  be the predicate that every  $A \in M_{n \times n}(\mathbb{F})$  that has two equal adjacent rows satisfies  $\det A = 0$ . For  $n = 2$ , if  $A \in M_{2 \times 2}(\mathbb{F})$  has two equal adjacent rows, then we may write

$$\begin{bmatrix} A_{11} & A_{11} \\ A_{21} & A_{21} \end{bmatrix}$$

so

$$\det(A) = A_{11}A_{21} - A_{11}A_{21} = 0.$$

Now, suppose  $P(k)$  for some  $k \in \{n \in \mathbb{N} : n > 2\}$ . Further suppose that  $A \in M_{(k+1) \times (k+1)}(\mathbb{F})$  such that  $A$  has two equal adjacent rows, row  $p$  and row  $p+1$ . Then, for each  $i \in \{1, \dots, k+1\} \setminus \{p, p+1\}$ ,  $\tilde{A}_{il}$  has two equal adjacent rows, so  $\det(\tilde{A}_{il}) = 0$  by induction hypothesis. Moreover,  $\tilde{A}_{p1} = \tilde{A}_{(p+1)1}$ , since  $\text{Row}_p(A) = \text{Row}_{p+1}(A)$  and they are adjacent. Thus,

$$\begin{aligned} \det(A) &= \sum_{i=1}^{k+1} (-1)^{1+i} A_{i1} \det(\tilde{A}_{il}) \\ &= \sum_{i=1, i \neq p, p+1}^{k+1} (-1)^{1+i} A_{i1} \det(\tilde{A}_{il}) + (-1)^{1+p} A_{p1} \det(\tilde{A}_{p1}) \\ &\quad + (-1)^{1+p+1} A_{(p+1)1} \det(\tilde{A}_{(p+1)1}) \\ &= (-1)^{1+p} A_{p1} \det(\tilde{A}_{p1}) + (-1)^{1+p+1} A_{(p+1)1} \det(\tilde{A}_{(p+1)1}) \\ &= ((-1)^{1+p} + (-1)^{2+p}) A_{p1} \det(\tilde{A}_{p1}) = 0, \end{aligned}$$

since  $(-1)^{1+p} + (-1)^{2+p} = 0$  for any  $p \in \mathbb{Z}$ . ♠

#### Lemma 4.3.

$\det(B) = -\det(A)$  if  $B$  is obtained by exchanging two adjacent rows of  $A$

Let  $A \in M_{n \times n}(\mathbb{F})$  and  $B \in M_{n \times n}(\mathbb{F})$  be the matrix obtained by exchanging row  $i$  and row  $i+1$  of  $A$  for some  $i \in \{1, \dots, n-1\}$ . Then  $\det(B) = -\det(A)$ .

*Proof.* Let  $R_1, \dots, R_n$  be the rows of  $A$ . Define

$$C = [R_1, \dots, R_i + R_{i+1}, R_i + R_{i+1}, \dots, R_n]$$

then  $\det(C) = 0$  by Lemma 4.2. That is,

$$\begin{aligned} \det(C) &= \det[R_1, \dots, R_i + R_{i+1}, R_i + R_{i+1}, \dots, R_n] \\ &= \det[R_1, \dots, R_i, R_i, \dots, R_n] + \det[R_1, \dots, R_{i+1}, R_{i+1}, \dots, R_n] \\ &\quad + \det[R_1, \dots, R_i, R_{i+1}, \dots, R_n] + \det[R_1, \dots, R_{i+1}, R_i, \dots, R_n] \\ &= \det[R_1, \dots, R_{i+1}, R_{i+1}, \dots, R_n] + \det[R_1, \dots, R_i, R_i, \dots, R_n] \\ &= \det(A) + \det(B) = 0, \end{aligned}$$

which exactly means  $\det(B) = -\det(A)$ . ♠

#### Lemma 4.4.

Determinant is zero if  $A$  has two identical rows

Let  $A \in M_{n \times n}(\mathbb{F})$ . If  $A$  has two identical rows, then  $\det(A) = 0$ .

*Proof.* Suppose that  $A$  has two identical rows. Then by means of type 1 elementary row operations,  $A$  can be transformed into a matrix which has two adjacent identical rows, denote which  $A'$ . Suppose  $n$  type 1 elementary row operations are used. Then by Lemma 4.2 and Lemma 4.3,

$$\det(A) = (-1)^n \det(A') = 0. \quad \spadesuit$$

**Proposition 4.5.**  
**Determinants after a**  
**Type 1 Elementary**  
**Row Operation**


Let  $A \in M_{n \times n}(\mathbb{F})$  and suppose that  $B \in M_{n \times n}(\mathbb{F})$  is obtained by exchanging row  $i$  and row  $j$  of  $A$ . Then  $\det(B) = -\det(A)$ .

*Proof.* Without loss of generality, suppose  $i < j$  and let  $R_1, \dots, R_n$  be the rows of  $A$ . Define

$$C = [R_1, \dots, R_i + R_j, \dots, R_i + R_j, \dots, R_n]$$

then

$$\begin{aligned} \det(C) &= \det[R_1, \dots, R_i + R_j, \dots, R_i + R_j, \dots, R_n] \\ &= \det[R_1, \dots, R_i, \dots, R_i, \dots, R_n] + \det[R_1, \dots, R_j, \dots, R_j, \dots, R_n] \\ &\quad + \det[R_1, \dots, R_i, \dots, R_j, \dots, R_n] + \det[R_1, \dots, R_j, \dots, R_i, \dots, R_n] \\ &= \det[R_1, \dots, R_i, \dots, R_j, \dots, R_n] + \det[R_1, \dots, R_j, \dots, R_i, \dots, R_n] \\ &= \det(A) + \det(B) = 0. \end{aligned}$$

Thus  $\det(B) = -\det(A)$ . 

**Proposition 4.6.**  
**Determinants after a**  
**Type 3 Elementary**  
**Row Operation**


Let  $A \in M_{n \times n}(\mathbb{F})$ . Suppose that  $B$  is obtained from  $A$  by adding scalar multiple of row  $j$  to row  $i$  of  $A$ . Then  $\det(B) = \det(A)$ .

*Proof.* Without loss of generality, suppose  $i < j$  and let  $R_1, \dots, R_n$  be the rows of  $A$ . Then

$$B = [R_1, \dots, R_i + cR_j, \dots, R_j, \dots, R_n]$$

for some  $c \in \mathbb{F}$ . Thus

$$\begin{aligned} \det(B) &= \det[R_1, \dots, R_i + cR_j, \dots, R_j, \dots, R_n] \\ &= \det[R_1, \dots, R_i, \dots, R_j, \dots, R_n] + c \det[R_1, \dots, R_j, \dots, R_j, \dots, R_n] \\ &= \det[R_1, \dots, R_i, \dots, R_j, \dots, R_n] = \det(A), \end{aligned}$$

which is the desired result. 

## Properties of Determinants

**Theorem 4.7.**  
**Characterization of**  
**Determinants**

As a function of each row, the determinant of a square matrix is a unique function  $\mathbb{F}^n \times \mathbb{F}^n \times \dots \times \mathbb{F}^n \rightarrow \mathbb{F}$  that satisfies the following.

(a) Determinant is a  $n$ -linear function. In other words, if  $A = [A_1, A_2, \dots, A_n]$

$$\det(A_1, \dots, cA_i, \dots, A_n) = c \det(A_1, \dots, A_i, \dots, A_n) = c \det(A)$$

for each  $i \in \{1, 2, \dots, n\}$ .

(b) Whenever there exists  $i \in \{1, \dots, n-1\}$  such that  $A_i = A_{i+1}$ ,  $\det(A) = 0$ .

(c)  $\det(I) = 1$ .

**Corollary 4.7.1.**  
**Determinant of an Elementary Matrix and Its Transpose**

Let  $E_i$  be an elementary matrix obtained by type  $i$  elementary row operation. Then the following holds.

- (a)  $\det(E_1) = -1$ .
- (b)  $\det(E_2) = c$ , where  $c \in \mathbb{R} \setminus \{0\}$  is the coefficient multiplied to a row.
- (c)  $\det(E_3) = 1$ .
- (d)  $\det(E_i^T) = \det(E_i)$ .

*Proof.* Observe that (1), (2), and (3) are direct results of Proposition 5, Corollary 1.2, Proposition 6, respectively, with (3) of Proposition 7. For (4), it is sufficient to recall that  $E^T$  is an elementary matrix of the same type as  $E$ , provided that  $E$  is an elementary matrix. ♠

**Corollary 4.7.2.**

Let  $E \in M_{n \times n}(\mathbb{F})$  be an elementary matrix. Then  $\det(E) \neq 0$ .

**Corollary 4.7.3.**

Let  $A \in M_{n \times n}(\mathbb{F})$  and  $E \in M_{n \times n}(\mathbb{F})$  be an elementary matrix. Then  $\det(EA) = \det(E)\det(A)$ .

**Corollary 4.7.4.**

Let  $A \in M_{n \times n}(\mathbb{F})$  and  $E_1, \dots, E_p \in M_{n \times n}(\mathbb{F})$  be elementary matrices. Then

$$\det(E_1 E_2 \cdots E_p A) = \det(E_1) \det(E_2) \cdots \det(E_p) \det(A).$$

In particular,

$$\det(E_1 E_2 \cdots E_p) = \det(E_1) \det(E_2) \cdots \det(E_p).$$

**Theorem 4.8.**  
**Invertible Matrix Theorem V**

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $A$  is invertible if and only if  $\det(A) \neq 0$ .

*Proof.* For the forward direction, suppose that  $A$  is invertible. Then there exists elementary matrices  $E_1, \dots, E_p \in M_{n \times n}(\mathbb{F})$  such that  $A = E_1 E_2 \cdots E_p$ , so  $\det(A) = \det(E_1) \det(E_2) \cdots \det(E_p) \neq 0$ . For the reverse direction, suppose that  $\det(A) \neq 0$ . Further suppose that  $A$  is not invertible for the sake of contradiction. Then there exists elementary matrices  $F_1, F_2, \dots, F_q \in M_{n \times n}(\mathbb{F})$  such that

$$F_1 F_2 \cdots F_q A = \begin{bmatrix} I_r & O \\ O & O \end{bmatrix},$$

where  $r = \text{rank}(A) < n$ . But  $\det \begin{bmatrix} I_r & O \\ O & O \end{bmatrix} = 0$ , which is a contradiction, since  $\det(A) \neq 0$  by assumption and  $F_1, F_2, \dots, F_q$  are elementary matrices. ♠

**Corollary 4.8.1.**  
**Determinant and Rank**

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $\det(A) = 0$  if and only if  $\text{rank}(A) < n$ .

**Proposition 4.9.**  
**Determinant of a Matrix Product**

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

*Proof.* First suppose that  $\det(A) = 0$  or  $\det(B) = 0$ . Then clearly  $\det(AB) = 0$ , since  $AB$  is not invertible. So suppose that  $\det(A), \det(B) \neq 0$ . Then  $A$  and  $B$  are invertible, so there exist elementary  $E_1, \dots, E_p, F_1, \dots, F_q \in M_{n \times n}(\mathbb{F})$  such that  $A = E_1 E_2 \cdots E_p$  and  $B = F_1 F_2 \cdots F_q$ . Therefore,

$$\begin{aligned}\det(AB) &= \det(E_1 E_2 \cdots E_p F_1 F_2 \cdots F_q) \\ &= \det(E_1 \det E_2 \cdots \det E_p) (\det F_1 \det F_2 \cdots \det F_q) = \det(A) \det(B),\end{aligned}$$

which is the desired result. ♠

**Proposition 4.10.**  
Determinant of a  
Matrix and Its  
Transpose

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $\det(A) = \det(A^T)$ .

*Proof.* Suppose that  $A$  is not invertible. Then so  $A^T$  is not, and we have  $\det A = 0 = \det A^T$ . So suppose that  $A$  is invertible. Then there are elementary matrices  $E_1, \dots, E_p \in M_{n \times n}(\mathbb{F})$  such that

$$\begin{aligned}\det(A^T) &= \det(E_1 E_2 \cdots E_p)^T = \det(E_p^T E_{p-1}^T \cdots E_1^T) \\ &= \det(E_p^T) \det(E_{p-1}^T) \cdots \det(E_1^T) \\ &= \det(E_p) \det(E_{p-1}) \cdots \det(E_1) \\ &= \det(E_1) \det(E_2) \cdots \det(E_p) = \det(E_1 E_2 \cdots E_p) = \det(A),\end{aligned}$$

as desired. ♠

**Theorem 4.11.**  
Cofactor Expansion  
Theorem

The determinant of  $A$  can be evaluated by cofactor expansion along any column. That is, for any  $j \in \{1, \dots, n\}$ ,

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

*Proof.* Write  $A = [C_1, C_2, \dots, C_j, \dots, C_n]$ . Observe that it takes  $(j-1)$  type 1 elementary column operations to transform  $A$  into  $A' = [C_j, C_1, C_2, \dots, C_n]$ . Therefore,  $\det(A) = (-1)^{j-1} \det(A')$  and by using cofactor expansion,

$$(-1)^{j-1} \sum_{i=1}^n (-1)^{1+i} A'_{i1} \det(\tilde{A}'_{i1}) = \sum_{i=1}^n (-1)^{i+j} A'_{i1} \det(\tilde{A}'_{i1}) = \sum_{i=1}^n (-1)^{i+j} A_{ij} \det(\tilde{A}_{ij}),$$

since  $A'_{i1} = A_{ij}$  and  $\tilde{A}'_{i1} = \tilde{A}_{ij}$  for all  $i \in \{1, \dots, n\}$  by construction. A more general result involving cofactor expansion along any row can be shown by taking the transpose of  $A$ . ♠

*This page intentionally left blank.*

# 5.

## Polynomials

- 
- 5.1 Algebras
  - 5.2 Algebra of Polynomials
  - 5.3 Lagrange Interpolation
  - 5.4 Polynomial Ideals
-

## Algebras

### Def'n. Algebra over a Field

We say  $\mathcal{A}$  is **algebra** over a field  $\mathbb{F}$  if  $\mathcal{A}$  is a vector space over  $\mathbb{F}$  equipped with a binary operation  $\mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$  called multiplication that has the following properties. Let  $\alpha, \beta, \gamma \in \mathcal{A}$  and  $c \in \mathbb{F}$ .

- (a) Multiplication is distributive with respect to addition.

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma \quad (\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha.$$

- (b) Multiplication is compatible with respect to scalar multiplication.

$$c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta).$$

### Def'n. Associative, Commutative Algebra

We say an algebra  $\mathcal{A}$  is **associative** if the multiplication on  $\mathcal{A}$  is associative. That is, for any  $\alpha, \beta, \gamma \in \mathcal{A}$ ,

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma.$$

Moreover, we say  $\mathcal{A}$  is **commutative** if the multiplication on  $\mathcal{A}$  is commutative. That is, for any  $\alpha, \beta \in \mathcal{A}$ ,

$$\alpha\beta = \beta\alpha.$$

### Def'n. Unity of an Algebra

An element  $\alpha \in \mathcal{A}$  such that

$$\forall \beta \in \mathcal{A} [\alpha\beta = \beta\alpha = \beta]$$

is called the **unity** of  $\mathcal{A}$ . If such element exists, then it is unique, and we say  $\mathcal{A}$  is **unital**.

**Remark 5.1.** The rest of this section will be devoted to the construction of the polynomial algebra. Recall that the set of all functions from  $\mathbb{N} \cup \{0\}$  to  $\mathbb{F}$  is a vector space, which we denote by  $\mathbb{F}^\infty$ . Then, any  $f \in \mathbb{F}^\infty$  can be represented as an infinite sequence

$$f = (f_0, f_1, \dots)$$

where  $f_n = f(n)$  for each  $n \in \mathbb{N} \cup \{0\}$ .

### Proposition 5.1. Algebra of Sequences

Let  $\mathbb{F}^\infty$  be the algebra of all sequences in  $\mathbb{F}$ . That is, an element  $f \in \mathbb{F}^\infty$  can be represented as

$$f = (f_0, f_1, \dots) \in \mathbb{F}^\infty,$$

where  $f : \mathbb{N} \cup \{0\} \rightarrow \mathbb{F}$  satisfy that  $f_k = f(k)$  for any  $k \in \mathbb{N}$ . Define addition and scalar multiplication to be componentwise. Further define multiplication  $\mathbb{F}^\infty \times \mathbb{F}^\infty \rightarrow \mathbb{F}^\infty$  to be such that

$$(fg)_n = \sum_{i=0}^n f_i g_{n-i}.$$

Then  $\mathbb{F}^\infty$  is an infinite-dimensional, unital, and commutative algebra over  $\mathbb{F}$ .

*Proof.* To verify that  $\mathbb{F}^\infty$  is infinite-dimensional, observe that

$$\{e_k : k \in \mathbb{N}\} \subseteq \mathbb{F}^\infty$$



is linearly independent. We verify other necessary properties componentwise. To verify distributivity, let  $f = (f_0, f_1, \dots), g = (g_0, g_1, \dots), h = (h_0, h_1, \dots) \in \mathbb{F}^\infty$ . Then,

$$(f(g+h))_n = \sum_{i=0}^n f_i(g+h)_{n-i} = \sum_{i=0}^n f_i(g_{n-i} + h_{n-i}) = \sum_{i=0}^n f_i g_{n-i} + \sum_{i=0}^n f_i h_{n-i} = (fg)_n + (fh)_n.$$

Similar proof holds for compatibility. To verify commutativity,

$$(fg)_n = \sum_{i=0}^n f_i g_{n-i} = \sum_{i=0}^n g_i f_{n-i} = (gf)_n.$$

We claim that

$$1_{\mathbb{F}^\infty} = (1, 0, \dots)$$

is the unity of  $\mathbb{F}^\infty$ . To verify this, observe that

$$(1_{\mathbb{F}^\infty} f)_n = \sum_{i=0}^n (1_{\mathbb{F}^\infty})_i f_{n-i} = \sum_{i=0}^n \delta_{0i} f_{n-i} = f_n.$$

To verify the associativity, observe that

$$\begin{aligned} [(fg)h]_n &= \sum_{i=0}^n (fg)_i h_{n-i} = \sum_{i=0}^n \left( \sum_{j=0}^i f_j g_{i-j} \right) h_{n-i} = \sum_{i=0}^n \sum_{j=0}^i f_j g_{i-j} h_{n-i} \\ &= \sum_{j=0}^n \sum_{i=j}^n f_j g_{i-j} h_{n-i} = \sum_{j=0}^n f_j \left( \sum_{i=j}^n g_{i-j} h_{n-i} \right) \\ &= \sum_{j=0}^n f_j \left( \sum_{l=0}^{n-j} g_l h_{n-j-l} \right) = \sum_{j=0}^n f_j (gh)_{n-j} = [f(gh)]_n, \end{aligned}$$

which is the desired result. ♠

**Remark 5.2.** The vector

$$x = (0, 1, 0, \dots)$$

plays a distinguished role in what follows, and we shall consistently denote it by  $x$ . The product of  $x$  with itself  $n$  times,

$$x^n := \underbrace{x \cdot x \cdots x}_{n \text{ multiplicands}} = \underbrace{(0, 0, \dots, 0, 1, 0, \dots)}_{n+1 \text{th entry is 1}},$$

shall be denoted by  $x^n$ . Notice that  $x^0 = 1$  is the unity.

## Algebra of Polynomials

### Def'n. Algebra of Polynomials, Polynomial

We call the subspace of  $\mathbb{F}^\infty$  spanned by  $\{1, x, x^2, \dots\}$ , denoted by  $\mathbb{F}[x]$ , the *algebra of polynomials*. An element  $f \in \mathbb{F}[x]$  of the algebra is called a *polynomial*.

**Remark 5.3.** Notice that  $f \in \mathbb{F}^\infty$  is a polynomial if there exists  $a_0, a_1, \dots, a_n \in \mathbb{F}$  with  $a_n \neq 0$  such that

$$f = a_0 1 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

for some  $n \in \mathbb{N} \cup \{0\}$ .

**Remark 5.4.**  $\mathbb{F}[x] \subsetneq \mathbb{F}^\infty$ . Moreover,  $\mathbb{F}[x]$  is infinite-dimensional and the spanning set  $\{1, x, x^2, \dots\}$  is linearly independent. That is,  $\{1, x, x^2, \dots\}$  is a basis for  $\mathbb{F}[x]$ .

**Def'n. Degree** of a Polynomial

Let  $f \in \mathbb{F}$  be nonzero. Write

$$f = a_0 1 + a_1 x + a_2 x^2 + \cdots .$$

If  $n \in \mathbb{N}$  is the largest element such that  $a_n \neq 0$  (which clearly is unique), we say  $n$  is the **degree** of  $f$  and denote as  $\deg(f) = n$ .

**Remark 5.5.** We do not assign a degree to  $0 \in \mathbb{F}[x]$ .

**Def'n. Coefficient, Leading Coefficient** of a Polynomial

Let

$$f = a_0 1 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{F}[x].$$

Then we say  $a_0, a_1, \dots, a_n \in \mathbb{F}$  are **coefficients** of  $f$  and, in particular,  $a_n$  with  $n = \deg(f)$  is called the **leading coefficient** of  $f$ .

**Def'n. Scalar, Monic** Polynomial

We say  $f \in \mathbb{F}[x]$  is **scalar** if  $f = 0$  or  $\deg(f) = 0$ . Moreover, we say  $f \in \mathbb{F}[x]$  is **monic** if the leading coefficient of  $f$  is 1.

**Proposition 5.2.**  
**Properties of**  
**Polynomials**

Let  $f, g \in \mathbb{F}[x]$  be nonzero. Then the following holds.

- (a)  $fg \neq 0$ . In fact,  $\deg(fg) = \deg(f) + \deg(g)$ .
- (b)  $fg$  is monic if  $f$  and  $g$  are monic.
- (c)  $fg$  is scalar if  $f$  and  $g$  are scalar.
- (d)  $f + g = 0$  or  $\deg(f + g) \leq \max(\deg(f), \deg(g))$ . Equality occurs whenever  $\deg(f) \neq \deg(g)$ .

*Proof.* To verify (a), let  $n = \deg(f)$ ,  $m = \deg(g)$ , and  $k \in \mathbb{N} \cup \{0\}$ . Observe that

$$(fg)_{n+m+k} = \sum_{i=0}^{n+m+k} f_i g_{n+m+k-i},$$

where  $f_i = 0$  if  $i > n$  and  $g_{n+m+k-i} = 0$  if  $n+m+k-i > m \iff i < n+k$ . That is, when  $k \geq 1$ , we have

$$(fg)_{n+m+k} = 0.$$

When  $k = 0$ ,

$$(fg)_{n+m+k} = (fg)_{n+m} = \sum_{i=0}^{n+m} f_i g_{n+m-i} = f_n g_m \neq 0.$$

Thus  $\deg(fg) = n + m = \deg(f) + \deg(g)$ . It follows that (b) and (c) are true as well. To verify (d), suppose that  $\deg(f) = n \geq m = \deg(g)$  without loss of generality. Then for each  $k \in \mathbb{N}$ ,

$$(f + g)_{n+k} = f_{n+k} + g_{n+k} = 0 + 0 = 0. \quad \spadesuit$$

**Corollary 5.2.1.**  
 **$\mathbb{F}[x]$  Is Commutative**  
**and Unital**

$\mathbb{F}[x]$  is a commutative, unital algebra.

*Proof.* Observe that the associativity of  $\mathbb{F}[x]$  is guaranteed by the associativity of  $\mathbb{F}^\infty$ . Let  $f, g \in \mathbb{F}$  with  $\deg(f) = n$  and  $\deg(g) = m$ . Then  $fg \in \mathbb{F}[x]$ , where

$$f = \sum_{i=0}^n a_i x^i \quad g = \sum_{j=0}^m b_j x^j$$

for some  $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m \in \mathbb{F}$ . So

$$fg = \sum_{i=0}^n \sum_{j=0}^m a_i b_j x^{i+j} = \sum_{p=0}^{n+m} \left( \sum_{l=0}^p a_l b_{p-l} x^p \right) = gf. \quad \spadesuit$$

**Remark 5.6.** (a) of Proposition 5.2 and Corollary 5.2.1 shows that  $\mathbb{F}[x]$  (as a ring) is an integral domain. That is,  $\mathbb{F}[x]$  is unital, commutative, and cancellative.

**Remark 5.7.** Let  $\mathcal{A}$  be a unital algebra over  $\mathbb{F}$ . Let  $f \in \mathbb{F}[x]$ . We evaluate  $f$  on an element  $\alpha \in \mathcal{A}$  as follows. Denote

$$\alpha^n = \underbrace{\alpha \cdot \alpha \cdots \alpha}_{n \text{ multiplicands}}$$

for each  $n \in \mathbb{N}$ , and  $\alpha^0 = 1$ . Moreover, write

$$f = \sum_{i=0}^n c_i x^i \in \mathbb{F}[x],$$

where  $c_0, c_1, \dots, c_n \in \mathbb{F}$ . We define  $f(\alpha) \in \mathcal{A}$  to be

$$f(\alpha) := \sum_{i=0}^n c_i \alpha^i = c_0 1 + c_1 \alpha + c_2 \alpha^2 + \cdots + c_n \alpha^n.$$

**Proposition 5.3.**  
Properties of  
Evaluating  
Polynomials on  $\alpha \in \mathcal{A}$

Let  $f, g \in \mathbb{F}[x]$  and let  $\mathcal{A}$  be a unital linear algebra over  $\mathbb{F}$ . Let  $\alpha \in \mathcal{A}$  and  $c \in \mathbb{F}$ .

$$(a) \quad (cf + g)(\alpha) = cf(\alpha) + g(\alpha).$$

$$(b) \quad (fg)(\alpha) = f(\alpha)g(\alpha).$$

*Proof.* (a) is a direct result of componentwise addition. To verify (b), write

$$f = \sum_{i=0}^n f_i x^i \quad g = \sum_{j=0}^m g_j x^j$$

where  $n = \dim(f)$  and  $m = \dim(g)$ . Then,

$$(fg)(\alpha) = \sum_{i,j} f_i g_j \alpha^{i+j} = \left( \sum_{i=0}^n f_i \alpha^i \right) \left( \sum_{j=0}^m g_j \alpha^j \right) = f(\alpha)g(\alpha). \quad \spadesuit$$

## Lagrange Interpolation

**Remark 5.8.** Let  $n \in \mathbb{N}$ . Throughout this section, we shall assume that  $\mathbb{F}$  is a field with at least  $n+1$  distinct elements  $t_0, t_1, \dots, t_n \in \mathbb{F}$ . Moreover, we shall denote the subspace of  $\mathbb{F}[x]$  containing polynomials of degree less than or equal to  $n$ , together with  $0 \in \mathbb{F}[x]$ , by

$$\mathbb{F}_n[x] = \{f \in \mathbb{F}[x] : \deg(f) \leq n \vee f = 0\}.$$

**Recall. Linear Functional** on a Vector Space

Let  $V$  be a vector space over  $\mathbb{F}$ . A **linear functional** (or **linear form**) is a linear transformation  $T : V \rightarrow \mathbb{F}$  from  $V$  to its field of scalars  $\mathbb{F}$ .

*Remark 5.8 is continued here.*

Define a function  $L_i : \mathbb{F}_n[x] \rightarrow \mathbb{F}$  by

$$f \mapsto f(t_i)$$

for all  $i \in \{0, 1, \dots, n\}$ . Then each  $L_i$  is a linear functional on  $\mathbb{F}_n[x]$ . Now, what we intend to show here is that  $\gamma = \{L_0, L_1, \dots, L_n\}$  is a basis for  $\mathbb{F}_n[x]^*$ , the dual space of  $\mathbb{F}_n[x]$ . Of course, it is sufficient to show that there exists a basis  $\beta = \{p_0, p_1, \dots, p_n\}$  for  $\mathbb{F}_n[x]^*$  such that  $\gamma = \beta^*$ . If such basis exists, then it is characterized by the fact that

$$L_j(p_i) = p_i(t_j) = \delta_{ij}$$

for all  $i \in \{0, 1, \dots, n\}$ . A way to construct such polynomials is by

$$p_i = \prod_{j=0, j \neq i}^n \left( \frac{x - t_j}{t_i - t_j} \right) \in \mathbb{F}_n[x].$$

In particular, if  $f \in \mathbb{F}_n[x]$  is  $\sum_{i=0}^n c_i p_i$  for some  $c_0, c_1, \dots, c_n \in \mathbb{F}$ , then for each  $j \in \{0, 1, \dots, n\}$ ,

$$f(t_j) = \sum_{i=0}^n c_i p_i(t_j) = c_j.$$

This shows that  $p_0, p_1, \dots, p_n$  are linearly independent, since  $0 \in \mathbb{F}_n[x]$  has the property that  $0(t) = 0$  for any  $t \in \mathbb{F}$ . That is, if  $f = 0$ , then  $c_0 = c_1 = \dots = c_n = 0$ . Clearly,  $\{1, x, \dots, x^n\}$  is a basis for  $\mathbb{F}_n[x]$ , so  $\dim(\mathbb{F}_n[x]) = n + 1$ . Thus  $\beta$  is a basis for  $\mathbb{F}_n[x]$ , and, accordingly,  $\gamma = \beta^*$  is also a basis for  $\mathbb{F}_n[x]^*$ .

**Theorem 5.4.**  
**Lagrange**  
**Interpolation**

Let  $t_0, t_1, \dots, t_n \in \mathbb{F}$  be distinct. Define

$$L_j(f) = f(t_j)$$

for each  $j \in \{0, 1, \dots, n\}$ . Then  $\{L_0, L_1, \dots, L_n\}$  is a basis for  $\mathbb{F}_n[x]^*$ .

**Corollary 5.4.1.**  
**Characterization of a**  
**Polynomial**

Let  $c_0, c_1, \dots, c_n \in \mathbb{F}$ . Then there exists a unique polynomial  $f \in \mathbb{F}_n[x]$  such that

$$f(t_i) = c_i.$$

**Corollary 5.4.2.**  
**Lagrange's**  
**Interpolation Formula**

Let  $\mathbb{F}$  be a field with at least  $n + 1$  distinct elements and suppose we have constructed  $p_0, p_1, \dots, p_n$  as described in Remark 5.8. Then for each  $f \in \mathbb{F}[x]$ ,

$$f = \sum_{i=0}^n f(t_i) p_i.$$

*Proof.* Suppose

$$f = \sum_{i=0}^n c_i p_i.$$

Then by Remark 5.8,  $f(t_j) = c_j$ . Thus

$$f = \sum_{i=0}^n f(t_i) p_i.$$



**Def'n. Polynomial Function**

Let  $f \in \mathbb{F}[x]$  be a polynomial. We define a *polynomial function*  $\tilde{f} : \mathbb{F} \rightarrow \mathbb{F}$  by the mapping

$$t \mapsto f(t),$$

where  $f(t)$  is the evaluation of the polynomial  $f$  at  $t$ .

**Remark 5.9.** By definition, every polynomial function is constructed in this way. However, it may happen that  $\tilde{f} = \tilde{g}$  for two distinct polynomials  $f, g \in \mathbb{F}$ . Fortunately, this only occurs in the case where  $\mathbb{F}$  is a finite field.

**Remark 5.10.** In order to describe in a precise way the relation between polynomials and polynomial functions, we proceed to define the product of two polynomial functions. Let  $f, g \in \mathbb{F}[x]$  then we define the product of  $\tilde{f}$  and  $\tilde{g}$  by the mapping  $t \mapsto \tilde{f}(t)\tilde{g}(t)$ . Equivalently,

$$(\tilde{f}\tilde{g})(t) = \tilde{f}(t)\tilde{g}(t).$$

From Proposition 5.3,  $(fg)(t) = f(t)g(t)$ , and thus

$$(\widetilde{fg})(t) = \tilde{f}(t)\tilde{g}(t).$$

It follows that  $\tilde{f}\tilde{g} = \widetilde{fg}$ .

## Polynomial Ideals

### Theorem 5.5. Division Algorithm

Let  $f, d \in \mathbb{F}[x]$  with  $d \neq 0$ . Then there exist unique polynomials  $q, r \in \mathbb{F}[x]$  such that

$$f = dq + r$$

where  $r = 0$  or  $\deg(r) < \deg(d)$ .

### Lemma 5.5.1.

Let  $f, d \in \mathbb{F}[x]$  be nonzero such that  $\deg(f) \geq \deg(d)$ . Then there exists  $g \in \mathbb{F}[x]$  such that  $f - dg = 0$  or  $\deg(f - dg) < \deg(f)$ .

*Proof.* Write

$$f = \sum_{i=0}^n a_i x^i \quad d = \sum_{j=0}^m b_j x^j$$

where  $\deg(f) = n \geq m = \deg(d)$ . So  $a_n, b_m \neq 0$ , which means

$$g = \frac{a_n}{b_m} x^{n-m}$$

is a well-defined expression. Moreover,

$$f - dg = \sum_{i=0}^n a_i x^i - \frac{a_n}{b_m} x^{n-m} \sum_{j=0}^m b_j x^j = a_n x^n - \left( \frac{a_n}{b_m} x^{n-m} b_m x^m \right) + \dots = 0 + \dots$$

by construction, so  $\deg(f - dg) < \deg(f)$ . ♠

### Proof of Theorem 5.5 Begins Here

*Proof.* When  $\deg(f) < \deg(d)$ , we have  $q = 0, r = f$  and their uniqueness is trivial. So suppose  $\deg(f) \geq \deg(d)$ . We verify the existence of  $q, r \in \mathbb{F}[x]$  with  $\deg(r) < \deg(d)$  or  $r = 0$  such that

$$f = dq + r$$

first. By Lemma 5.5.1, there exists  $q_1 \in \mathbb{F}[x]$  such that

$$\deg(f) > \deg(f - dq_1).$$

If  $\deg(d) > \deg(f - dq_1)$  or  $f - dq_1 = 0$ , we are done. Otherwise, there exists another  $q_2 \in \mathbb{F}[x]$  such that

$$\deg(f) > \deg(f - dq_1) > \deg(f - dq_1 - dq_2).$$

Since this is a strict inequality, by continuing this process, we get polynomials  $q_1, q_2, \dots, q_n \in \mathbb{F}[x]$  such that

$$\deg(d) > \deg(f - dq_1 - dq_2 - \dots - dq_n)$$

or, if  $\deg(d) = 0$ ,

$$f - dq_1 - dq_2 - \dots - dq_n = 0.$$

That is,  $q = q_1 + q_2 + \dots + q_n$  and  $r = f - dq_1 - dq_2 - \dots - dq_n$  satisfy the listed conditions. To verify uniqueness, suppose that there exist another  $q' \in \mathbb{F}[x]$  such that

$$f = dq' + r'$$

where  $r' = 0$  or  $\deg(r') < \deg(d)$ . For the sake of contradiction, suppose that  $q \neq q'$ . Then  $r - r' = (f - dq) - (f - dq') = dq' - dq \neq 0$  and we have

$$\deg(r - r') = \deg(d) \deg(q' - q).$$

But clearly

$$\deg(r - r') \leq \max(\deg(r), \deg(r')) < \deg(d),$$

so we have a contradiction. Thus  $q' = q$  and, consequently,  $r = r'$ , which verifies the uniqueness. ♠

#### Def'n. Divisor, Quotient, Remainder

Let  $f, d, q, r \in F[x]$  satisfy conditions listed in Theorem 5.5. Then we call  $d \neq 0$  the **divisor**,  $q$  the **quotient**, and  $r$  the **remainder**.

#### Def'n. Divides

Let  $f \in \mathbb{F}[x]$ . We say  $d \in \mathbb{F}[x]$  **divides**  $f$ , denoted by  $d \mid f$ , if there exists  $q \in \mathbb{F}[x]$  such that

$$f = dq.$$

**Remark 5.11.** Let  $f \in \mathbb{F}[x]$  and suppose  $d \mid f$  for some  $d \in \mathbb{F}[x]$ . Then Theorem 5.5 guarantees the existence and uniqueness of  $q \in \mathbb{F}[x]$  such that  $f = dq$ .

#### Corollary 5.5.2. Remainder Theorem

Let  $f \in \mathbb{F}[x]$  and  $c \in \mathbb{F}$ . Then

$$(x - c) \mid f \iff f(c) = 0.$$

*Proof.* By division algorithm,

$$f = (x - c)q + r$$

for some unique  $q, r \in \mathbb{F}[x]$ . Notice that  $r$  is a scalar, since if  $r \neq 0$ , then  $\deg(r) < \deg(x - c) = 1$ . That is,

$$f(c) = (c - c)q(c) + r = r,$$

which means  $f(c) = 0 \iff r = 0$ . But  $r = 0$  exactly means  $(x - c) \mid f$ , as desired. ♠

#### Def'n. Root of a Polynomial

Let  $f \in \mathbb{F}[x]$ . We say  $c \in \mathbb{F}$  is a **root** of  $f$  if  $f(c) = 0$ .

**Corollary 5.5.3.**  
**Nonzero  $f$  Has at**  
**Most  $\deg(f)$  Roots**

Let  $f \in F[x]$  be nonzero and let  $n = \deg(f)$ . Then  $f$  has at most  $n$  roots.

*Proof.* We proceed by induction. When  $\deg(f) = 0$ ,  $f = a_0 1$  so  $f \neq 0$  for all  $c \in \mathbb{F}$ . When  $\deg(f) = 1$ ,  $f = a_0 1 + a_1 x$ . That is

$$f(c) = 0 \iff c = -\frac{a_1}{a_0}.$$

Now suppose that every  $f \in \mathbb{F}[x]$  with  $\deg(f) = k$  has at most  $k$  roots. Let  $g \in \mathbb{F}[x]$  be such that  $\deg(g) = k + 1$ . If  $g$  does not have any root, then we are done. So suppose  $g$  has a root  $c \in \mathbb{F}$ . Then by the remainder theorem,

$$g = (x - c)q$$

for some unique  $q \in \mathbb{F}[x]$  with  $\deg(q) = k$ . But by induction hypothesis,  $q$  has at most  $k$  roots, so  $g$  has at most  $k + 1$  roots, as desired. ♠

**Remark 5.12.** If  $\deg(f) > 1$ , there needs not exist any roots.

**Def'n. Algebraically Closed Field**

Let  $\mathbb{F}$  be a field. We say  $\mathbb{F}$  is **algebraically closed** if every polynomial  $f \in \mathbb{F}[x]$  over  $\mathbb{F}$  has a root.

**Def'n. Formal Derivative of a Polynomial**

Define linear operator  $D : \mathbb{F}[x] \rightarrow \mathbb{F}[x]$  by

$$\sum_{i=0}^n a_i x^i \mapsto \sum_{i=1}^n i a_i x^{i-1}$$

For any  $f \in \mathbb{F}[x]$ , we call  $Df$  the **formal derivative** of  $f$ .

**Theorem 5.6.**  
**Binomial Theorem**

Let  $\mathcal{A}$  be an commutative algebra over  $\mathbb{F}$  with characteristic zero and let  $\alpha, \beta \in \mathcal{A}$ . Then

$$(\alpha + \beta)^n = \sum_{r=0}^n \binom{n}{r} \alpha^{n-r} \beta^r.$$

*Proof.* We proceed inductively. Observe that

$$(\alpha + \beta)^1 = \alpha + \beta = \binom{1}{0} \alpha^1 \beta^0 + \binom{1}{1} \alpha^0 \beta^1 = \sum_{k=0}^1 \binom{1}{k} \alpha^{1-k} \beta^k.$$

Now suppose

$$(\alpha + \beta)^k = \sum_{r=0}^k \binom{k}{r} \alpha^{k-r} \beta^r.$$

Then,

$$(\alpha + \beta)^{k+1} = (\alpha + \beta) \sum_{r=0}^k \binom{k}{r} \alpha^{k-r} \beta^r = \sum_{r=0}^k \binom{k}{r} \alpha^{k+1-r} \beta^r + \sum_{r=0}^k \binom{k}{r} \alpha^{k-r} \beta^{r+1}.$$

Since  $\mathbb{F}$  has zero characteristic, the coefficient of the term  $\alpha^{k+1-r} \beta^r$  is given by the expression

$$\binom{k}{r} + \binom{k}{r-1} = \binom{k+1}{r},$$

which exactly means

$$\sum_{r=0}^k \binom{k}{r} \alpha^{k+1-r} \beta^r + \sum_{r=0}^k \binom{k}{r} \alpha^{k-r} \beta^{r+1} = \sum_{r=0}^{k+1} \binom{k+1}{r} \alpha^{k+1-r} \beta^r.$$

So by the principle of mathematical induction,

$$(\alpha + \beta)^n = \sum_{r=0}^n \binom{n}{r} \alpha^{n-r} \beta^r,$$

as desired. ♠

**Theorem 5.7.**  
**Taylor's Formula**

Let  $\mathbb{F}$  be a field with characteristic zero and let  $f \in \mathbb{F}[x]$  be a nonzero polynomial with  $\deg(f) \leq n$  for some  $n \in \mathbb{N}$ . Then,

$$f = \sum_{k=0}^n \frac{D^k f}{k!}(c)(x-c)^k$$

for any  $c \in \mathbb{F}$ .

*Proof.* We first verify the result for the standard basis vectors  $1, x, x^2, \dots \in \mathbb{F}[x]$ . Let  $f = x^m$  for some  $m \leq n$ . Then,

$$\begin{aligned} \sum_{k=0}^n \frac{D^k f}{k!}(c)(x-c)^k &= \sum_{k=n+1}^n \frac{D^k f}{k!}(c)(x-c)^k + \sum_{k=0}^m \frac{D^k f}{k!}(c)(x-c)^k \\ &= \sum_{k=0}^m \frac{\frac{m!}{(m-k)!} c^{m-k}}{k!}(x-c)^k = \sum_{k=0}^m \binom{m}{k} c^{m-k} (x-c)^k = (c + (x-c))^m = x^m. \end{aligned}$$

That is, for any  $f = \sum_{p=0}^m a_p x^p$  for some  $m \leq n$ ,

$$\begin{aligned} \sum_{k=0}^n \frac{D^k f}{k!}(c)(x-c)^k &= \sum_{k=0}^n \frac{D^k \left( \sum_{p=0}^m a_p x^p \right)}{k!}(c)(x-c)^k = \sum_{k=0}^n \sum_{p=0}^m \frac{a_p D^k(x^p)}{k!}(c)(x-c)^k \\ &= \sum_{p=0}^m a_p \sum_{k=0}^n \frac{D^k(x^p)}{k!}(c)(x-c)^k = \sum_{p=0}^m a_p x^p = f, \end{aligned}$$

as desired. ♠

**Def'n. Multiplicity of a Root**

Let  $f \in \mathbb{F}[x]$  and  $c \in \mathbb{F}$ . We say  $m \in \mathbb{N}$  is the **multiplicity** of  $c$  provided that  $(x-c)^m \mid f$  and  $(x-c)^{m+1} \nmid f$ .

**Proposition 5.8.**

Let  $\mathbb{F}$  be a field with characteristic zero and  $f \in \mathbb{F}[x]$ . Then  $c \in \mathbb{F}$  is a root with multiplicity  $r$  if and only if  $D^i f(c) = 0$  for each  $i \in \{0, 1, \dots, r-1\}$  and  $D^r f(c) \neq 0$ .

*Proof.* For the forward direction, suppose  $c \in \mathbb{F}$  is a root of multiplicity  $r$ . Write  $f = (x-c)^r q$  where  $\deg(f) = n$ ,  $\deg(q) = n-r$ , and  $q(c) \neq 0$ . By Taylor's formula,

$$f = (x-c)^r q = (x-c)^r \sum_{k=0}^{n-r} \frac{D^k q}{k!}(c)(x-c)^k = \sum_{k=0}^{n-r} \frac{D^k q}{k!}(c)(x-c)^{k+r}.$$

Since  $\{1, (x-c), (x-c)^2, \dots\}$  is a basis for  $\mathbb{F}[x]$ , the above expression is the unique representation of  $f$  as a linear combination of  $1, (x-c), (x-c)^2, \dots, (x-c)^n$ . So

$$\sum_{k=0}^n \frac{D^k f}{k!}(c)(x-c)^k = \sum_{k=0}^{n-r} \frac{D^k q}{k!}(c)(x-c)^{k+r} = \sum_{k=r}^n \frac{D^{k-r} q}{(k-r)!}(c)(x-c)^k.$$

It follows that  $D^r f(c) = r! q(c) \neq 0$  and  $\frac{D^k f}{k!}(c) = 0$  for each  $k \in \{0, 1, \dots, r-1\}$ . For the reverse direction, suppose that  $D^k f(c) = 0$  for each  $k \in \{0, 1, \dots, r-1\}$  and  $D^r f(c) \neq 0$ . Then

$$f = \sum_{k=0}^n \frac{D^k f}{k!}(c)(x-c)^k = \sum_{k=r}^n \frac{D^k f}{k!}(c)(x-c)^k = (x-c)^r \sum_{k=r}^n \frac{D^k f}{k!}(c)(x-c)^{k-r}$$

so  $(x-c)^r \mid f$  but  $(x-c)^{r+1} \nmid f$ , as desired. ♠



**Def'n. Ideal** of a Polynomial Space

We say a subspace  $M \subseteq \mathbb{F}[x]$  is an **ideal** of  $\mathbb{F}[x]$  if

$$f \in M \wedge g \in \mathbb{F}[x] \implies fg \in M.$$

**Theorem 5.9.**  
**Ideal Test**

Let  $M \subseteq \mathbb{F}[x]$ . Then  $M$  is an ideal of  $\mathbb{F}[x]$  if the following holds.

- (a) For each  $f, g \in M$ ,  $f - g \in M$ .
- (b) For each  $f \in M$  and  $h \in \mathbb{F}[x]$ ,  $fh = hf \in M$ .

**Def'n. Generator** of an Ideal

Let  $M \subseteq \mathbb{F}[x]$  be an ideal. We say  $\{d_1, d_2, \dots, d_n\} \subseteq \mathbb{F}[x]$  is a generator of  $M$  if

$$M = \left\{ \sum_{i=1}^n d_i f : f \in \mathbb{F}[x] \right\}.$$

For such case, we say  $M$  is the ideal **generated** by  $\{d_1, d_2, \dots, d_n\}$  and we often denote  $M$  by  $\langle d_1, d_2, \dots, d_n \rangle$ .

**Def'n. Principal Ideal**

Let  $d \in \mathbb{F}[x]$ . We say  $\langle d \rangle$  is the **principal ideal** generated by  $d$  of  $\mathbb{F}[x]$ .

**Def'n. Trivial Ideal**

For any polynomial space  $\mathbb{F}[x]$ ,  $\{0\}$  is an ideal, which we call the **trivial ideal**.

**Proposition 5.10.**  
 **$\mathbb{F}[x]$  Is a Principal**  
**Idean Domain**

Let  $M \subseteq \mathbb{F}[x]$  be a nontrivial ideal. Then  $M = \langle d \rangle$  for some monic  $d \in \mathbb{F}[x]$ .

*Proof.* Let  $d \in M$  be a monic polynomial with minimum degree. We claim that  $\langle d \rangle = M$ . Clearly  $\langle d \rangle \subseteq M$ . Let  $f \in M$  be nonzero. By division algorithm,

$$f = dq + r$$

for some  $q, r \in \mathbb{F}[x]$  with  $\deg(d) > \deg(r)$  or  $r = 0$ . By the closure under subtraction of vector spaces,  $r = f - dq \in M$ . So if  $r \neq 0$ , we violate the minimality of  $d$ , since  $\deg(d) > \deg(r)$ . That is,  $f = dq$  for some  $q \in \mathbb{F}[x]$ , so  $f \in \langle d \rangle$ , as desired. ♠

**Corollary 5.10.1.**  
**Uniqueness of the**  
**Monic Generator**

Let  $p_1, p_2, \dots, p_k \in \mathbb{F}[x]$  be nonzero. Then there exists a unique monic  $d \in \mathbb{F}[x]$  that satisfies

- (a)  $d \in \langle p_1, p_2, \dots, p_k \rangle$ .
- (b)  $d \mid p_1 \wedge d \mid p_2 \wedge \dots \wedge d \mid p_k$ .
- (c)  $\forall f \in \mathbb{F}[x] [f \mid p_1 \wedge f \mid p_2 \wedge \dots \wedge f \mid p_k \implies f \mid d]$ .

*Proof.* We claim that the monic generator  $d \in \mathbb{F}[x]$  of  $\langle p_1, p_2, \dots, p_k \rangle$  uniquely satisfies (a), (b), and (c). Notice that  $\langle d \rangle = \langle p_1, p_2, \dots, p_k \rangle$  means  $d \in \langle p_1, p_2, \dots, p_k \rangle$  and (b) is a direct result of Proposition 5.10. To verify that  $d$  satisfies (c), observe that  $d = \sum_{i=1}^k p_i f_i$  for some  $f_1, f_2, \dots, f_k \in \mathbb{F}[x]$  and, for each  $i \in \{1, 2, \dots, k\}$ ,  $p_i = f q_i$  for some  $q_i \in \mathbb{F}[x]$ . So,

$$d = \sum_{i=1}^k p_i f_i = \sum_{i=1}^k f q_i f_i = f \sum_{i=1}^k q_i f_i$$

is divisible by  $f$ . To verify the uniqueness, suppose  $d' \in \mathbb{F}[x]$  satisfies (a), (b), and (c). Then by (b),  $d' \mid p_1 \wedge d' \mid p_2 \wedge \dots \wedge d' \mid p_k$ , so  $d' \mid d$  by (c). But by symmetry  $d \mid d'$  as well. Since both  $d$  and  $d'$  are monic, it follows that  $d = d'$ , as required. ♠

**Def'n. Greatest Common Divisor** of Polynomials

Let  $p_1, p_2, \dots, p_k \in \mathbb{F}[x]$  be nonzero. We call the unique monic generator  $d \in \mathbb{F}[x]$  of  $\langle p_1, p_2, \dots, p_k \rangle$  the **greatest common divisor** of  $p_1, p_2, \dots, p_k$ , denoted as  $d = \gcd(p_1, p_2, \dots, p_k)$ .

**Def'n. Coprime Polynomials**

We say nonzero  $p_1, p_2, \dots, p_k$  are **coprime** if  $\gcd(p_1, p_2, \dots, p_k) = 1$ .

**Proposition 5.11.**  
Alternative  
Definitions of  
Coprime Polynomials

Let  $p_1, p_2, \dots, p_k \in \mathbb{F}[x]$ . Then the following are equivalent.

- (a)  $p_1, p_2, \dots, p_k$  are coprime.
- (b) There exists  $q_1, q_2, \dots, q_k \in \mathbb{F}[x]$  such that  $\sum_{i=1}^k p_i q_i = 1$ .
- (c)  $\langle p_1, p_2, \dots, p_k \rangle = \mathbb{F}[x]$ .

**Theorem 5.12.**  
Bezout's Lemma for  
Polynomials

Let  $M \subseteq \mathbb{F}[x]$  be an ideal. For each  $p, q \in M$ ,  $\gcd(p, q) = d$  if and only if  $d \mid p$ ,  $d \mid q$ , and  $\exists f, g \in \mathbb{F}[x]$  such that  $d = fp + gq$ .

**Def'n. Reducible, Irreducible, Prime Polynomials**

Let  $f \in \mathbb{F}[x]$ . We say  $f$  is **reducible** if there exist  $g, h \in \mathbb{F}[x]$  such that  $\deg(g), \deg(h) \geq 1$  and  $f = gh$ . Otherwise, we say  $f$  is **irreducible**. An irreducible  $f$  is **prime** if  $\deg(f) \geq 1$ .

**Remark 5.13.** Every polynomial with degree 1 is prime.

**Proposition 5.13.**  
Alternative Definition  
of Prime

Let  $f, g, h \in \mathbb{F}[x]$ . If  $f$  is prime and  $f \mid gh$ , then  $f \mid g$  or  $f \mid h$ .

*Proof.* Without loss of generality, suppose  $f$  is monic. Let  $d = \gcd(g, h)$ . Then  $d$  is a monic polynomial that divides  $f$ , so  $d = f$  or  $d = 1$ . Since if  $d = f$ , then  $f \mid g$  and  $f \mid h$ , suppose  $d = 1$ . It follows that  $f$  is relatively prime with  $g$  or  $h$ , so without loss of generality, suppose  $f$  is relatively prime with  $g$ . Then there are  $f', g' \in \mathbb{F}[x]$  such that  $ff' + gg' = 1$ . By multiplying both sides by  $h$  we get

$$h = ff'h + gg'h = f(f'h) + (gh)g'.$$

Clearly  $f \mid f(f'h)$  and  $f \mid gh$ . That is,  $f \mid h$ , as required. ♠

**Corollary 5.13.1.**  
If  $f$  Is Prime, Then  
 $f \mid \prod_{i=1}^n p_i \implies f \mid p_k$   
for Some  
 $k \in \{1, 2, \dots, n\}$

Let  $f, p_1, p_2, \dots, p_n \in \mathbb{F}[x]$  be such that  $f$  is prime and  $f \mid \prod_{i=1}^n p_i$ . Then there is  $k \in \{1, 2, \dots, n\}$  such that  $f \mid p_k$ .

*Proof.* We proceed inductively. When  $n = 1$  the result holds trivially. Suppose that the result holds for  $n = m$  and  $f \mid \prod_{i=1}^m p_i$ . Then by Proposition 5.13,

$$f \mid \prod_{i=1}^m p_i \vee f \mid p_{m+1}$$

If  $f \mid p_{m+1}$ , then  $k = m + 1$  and we are done. If  $f \mid \prod_{i=1}^m p_i$ , then the result follows by the induction hypothesis. ♠

**Theorem 5.14.**  
**Unique Factorization**  
**of Monic Polynomials**

Let  $f \in \mathbb{F}[x]$  be nonscalar and monic. Then there exist unique monic, prime  $p_1, p_2, \dots, p_n \in \mathbb{F}[x]$  such that  $f = \prod_{i=1}^n p_i$ .

*Proof.* We proceed inductively. When  $\deg(f) = 1$ ,  $f$  itself is prime. For some  $k \in \mathbb{N}$ , suppose the result for all  $f \in \mathbb{F}[x]$  with  $\deg(f) \leq k$ . Let  $g \in \mathbb{F}[x]$  be monic with  $\deg(g) = k + 1$ . If  $g$  is prime, then we are done. So suppose that  $g$  is not prime. Then there are monic  $p, q \in \mathbb{F}[x]$  with  $\deg(p), \deg(q) \geq 1$  such that  $g = pq$ . Clearly  $\deg(p), \deg(q) \leq k$ , so there exist unique primes  $p_1, p_2, \dots, p_r, p_{r+1}, \dots, p_n$  such that  $p = \prod_{i=1}^r p_i$  and  $q = \prod_{i=r+1}^n p_i$ . That is,  $g = \prod_{i=1}^n p_i$ . To verify uniqueness, suppose that there exist monic, prime  $q_1, q_2, \dots, q_n \in \mathbb{F}[x]$  such that  $g = \prod_{j=1}^n q_j$ . Then for each  $i \in \{1, 2, \dots, n\}$ ,

$$p_i \mid \prod_{j=1}^n q_j$$

so  $p_i \mid q_j$  for some  $j \in \{1, 2, \dots, n\}$ . But both  $p_i$  and  $q_j$  are prime and monic, which means  $p_i = q_j$ . By symmetry, for each  $j \in \{1, 2, \dots, n\}$ ,  $q_j = p_i$  for some  $i \in \{1, 2, \dots, n\}$ . It follows that  $n = r$ , and by some renumbering,

$$\forall i \in \{1, 2, \dots, n\} [p_i = q_i],$$

as desired. ♠

**Remark 5.14.** Let  $f \in \mathbb{F}[x]$  be a nonscalar monic polynomial. Then Theorem 5.14 guarantees a unique representation of  $f$  in terms of products of monic prime polynomials, some of which may be repeated. In other words, if  $p_1, p_2, \dots, p_k \in \mathbb{F}[x]$  are the distinct primes which occur in the factorization of  $f$ , then

$$f = \prod_{i=1}^k p_i^{n_i}$$

for some  $n_1, n_2, \dots, n_k \in \mathbb{N}$ .

**Def'n. Primary Decomposition** of a Monic Polynomial

Consider Remark 5.14. We call

$$f = \prod_{i=1}^k p_i^{n_i}$$

the **primary decomposition** of  $f$ .

**Proposition 5.15.**

Let  $f \in \mathbb{F}[x]$  be a nonscalar monic polynomial and let

$$f = \prod_{i=1}^k p_i^{n_i}$$

be the primary decomposition of  $f$ . For each  $j \in \{1, 2, \dots, k\}$ , let

$$f_j = \frac{f}{p_j^{n_j}} = \prod_{i=1, i \neq j}^k p_i^{n_i}.$$

Then  $f_1, f_2, \dots, f_n$  are coprime.

*Proof.* For the sake of contradiction, suppose that there exists prime  $p \in \mathbb{F}[x]$  such that

$$p \mid f_i$$

for each  $i \in \{1, 2, \dots, k\}$ . It is clear that  $p = p_j$  for some  $j \in \{1, 2, \dots, k\}$  by Theorem 5.14. But this is a contradiction, since clearly

$$p_j \nmid f_j. \quad \spadesuit$$

**Proposition 5.16.**  
*f* Is a Product of  
 Distinct Primes If and  
 Only If *f* and *Df* Are  
 Coprime

Let  $f \in \mathbb{F}[x]$ . Then  $f$  is a product of distinct primes if and only if  $\gcd(f, Df) = 1$ .

*Proof.* For the forward direction, suppose that there exist distinct primes  $p_1, p_2, \dots, p_n \in \mathbb{F}[x]$  such that  $f = \prod_{i=1}^n p_i$ . By product rule,

$$Df = \sum_{j=1}^n D(p_j) \prod_{i=1, i \neq j}^n p_i.$$

Clearly  $p_j \nmid Dp_j$  since  $\deg(p_j) > \deg(Dp_j)$ . That is, for each  $j \in \{1, 2, \dots, n\}$ ,  $p_j \nmid Df$ , or,  $f$  and  $Df$  are coprime. For the reverse direction, suppose that there exists a prime  $p_j \in \mathbb{F}[x]$  such that  $f = p_j^k \prod_{i=1, i \neq j}^n p_i$  for some  $k \geq 2$ . By product rule and chain rule,

$$Df = \left( \sum_{s=1, s \neq j}^n D(p_s) \prod_{i=1, i \neq s}^n p_i \right) + k p_j^{k-1} D(p_j) \prod_{i=1, i \neq j}^n p_i,$$

where  $p_j$  divides both summands. So  $\gcd(f, Df) \neq 1$ , as desired. ♠

**Def'n. Algebraically Closed Field**

Let  $\mathbb{F}$  be a field. We say  $\mathbb{F}$  is **algebraically closed** if every nonscalar  $f \in \mathbb{F}[x]$  has a root  $c \in \mathbb{F}$ .

**Proposition 5.17.**  
 Alternative  
 Definitions of  
 Algebraic Closure

Let  $\mathbb{F}$  be a field. Then the following are equivalent.

(a)  $\mathbb{F}$  is algebraically closed.

(b) For each  $f \in \mathbb{F}[x]$ ,

$$f = c \prod_{i=1}^n (x - c_i)^{p_i}$$

for some  $c, c_1, c_2, \dots, c_n \in \mathbb{F}$  and  $p_1, p_2, \dots, p_n \in \mathbb{N}$ .

(c) Every prime polynomial of  $\mathbb{F}[x]$  has degree 1.

# 6.

## Diagonalization

---

6.1 Eigenvectors and Eigenvalues

6.2 Diagonalization

---

## Eigenvectors and Eigenvalues

### Def'n. Eigenvector, Eigenvalue, Eigenspace of a Matrix

Let  $A \in M_{n \times n}(\mathbb{F})$ . A nonzero  $v \in \mathbb{F}^n$  is called an **eigenvector** of  $A$  if there exists  $c \in \mathbb{F}$  such that

$$Av = cv.$$

Such  $c$  is called the **eigenvalue** corresponding to  $v$ . For any eigenvalue  $c \in \mathbb{F}$  of  $A$ , the set

$$E_c = \{u \in \mathbb{F}^n : Au = cu\} \cup \{0\}$$

is a subspace of  $\mathbb{F}^n$  and called the **eigenspace** corresponding to  $c$ .

**Remark 6.1.** Let  $A \in M_{n \times n}(\mathbb{F})$  and suppose  $c \in \mathbb{F}$  is an eigenvalue of  $A$ . Then the eigenspace corresponding to  $c$  is the null space of  $cI - A$ ,  $\ker(cI - A)$ . For, any eigenvector  $v \in \mathbb{F}^n$  of  $A$  corresponding to  $c$  satisfies  $Av = cv$ , which exactly means  $(cI - A)v = 0$ .

**Proposition 6.1.**  
 **$c$  Is an Eigenvalue If and Only If**  
 $\det(cI - A) = 0$

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $c \in \mathbb{F}$  is an eigenvalue of  $A$  if and only if  $\det(cI - A) = 0$ .

*Proof.* The forward direction follows easily from Remark 6.1. For the reverse direction, if  $\det(cI - A) = 0$ , then  $cI - A$  is not invertible, so there exists some  $v \in \mathbb{F}^n$  such that

$$(cI - A)v = 0.$$

But this exactly means  $Av = cv$ , so  $c$  is an eigenvalue of  $A$ . ♠

**Remark 6.2.** Proposition 6.1 motivates the following.

### Def'n. Characteristic Polynomial of a Matrix

Let  $A \in M_{n \times n}(\mathbb{F})$ . The  $n$ th degree polynomial  $\det(xI - A)$  in the indeterminate  $x$  is called the **characteristic polynomial** of  $A$ .

**Proposition 6.2.**  
**Properties of Characteristic Polynomials**

Let  $A \in M_{n \times n}(\mathbb{F})$  and let  $f \in \mathbb{F}[x]$  be the characteristic polynomial of  $A$ .

(a)  $f$  is a monic polynomial of  $\deg(f) = n$ .

(b)  $A$  has at most  $n$  eigenvalues.

(c) If  $B \in M_{n \times n}(\mathbb{F})$  is similar to  $A$ , then the characteristic polynomial of  $B$  is  $f$ .

*Proof.* For (a), use the cofactor expansion along any row or column. (b) is a direct consequence of a property of polynomials, that a polynomial of degree  $n$  has at most  $n$  roots. For (c), since  $B = QAQ^{-1}$  for some invertible  $Q \in M_{n \times n}(\mathbb{F})$ ,

$$\begin{aligned} \det(cI - B) &= \det(cI - QAQ^{-1}) = \det(QcIQ^{-1} - QAQ^{-1}) = \det(Q(cI - A)Q^{-1}) \\ &= \det(Q)\det(cI - A)\det(Q^{-1}) = \det(cI - A), \end{aligned}$$

as desired. ♠

**Remark 6.3.** Let  $V$  be a finite-dimensional vector space. Observe that (c) of Proposition 6.2 enables us to define an eigenvalue and eigenvector of a linear operator  $T : V \rightarrow V$  as an eigenvalue and eigenvector of its matrix representation  $[T]_\beta$  for any ordered basis  $\beta$  for  $V$ .

**Def'n. Eigenvalue, Eigenvector** of a Linear Operator

Let  $T : V \rightarrow V$  be a linear operator on  $V$ . A scalar  $c \in \mathbb{F}$  is called an **eigenvalue** of the linear operator  $T$  if there exists a nonzero  $v \in V$  such that  $Tv = cv$ . Such vector  $v$  is called an **eigenvector** of  $T$  corresponding to  $c$ .

**Def'n. Characteristic Polynomial** of a Linear Operator

Let  $T : V \rightarrow V$  be a linear operator on  $V$ . We define the **characteristic polynomial** of  $T$  to be the characteristic polynomial of any matrix representation  $[T]_\beta$  of  $T$ , where  $\beta$  is an ordered basis for  $V$ .

**Remark 6.4.** We see that the uniqueness of characteristic polynomial of a linear operator  $T : V \rightarrow V$  on a finite-dimensional vector space  $V$  is guaranteed by (c) of Proposition 6.2. For, if  $\beta$  and  $\gamma$  are ordered bases for  $V$ , then  $[T]_\beta$  and  $[T]_\gamma$  are similar.

**Proposition 6.3.**

Let  $T : V \rightarrow V$  be a linear operator on  $V$ .

- (a) A scalar  $c \in \mathbb{F}$  is an eigenvalue of  $T$  if and only if  $cI - T$  is not invertible.
- (b) Let  $c$  be an eigenvalue of  $T$ . A vector  $v \in V$  is an eigenvector of  $T$  corresponding to  $c$  if and only if  $v \neq 0$  and  $v \in \ker(cI - T)$ .

*Proof.* (a) follows easily from Proposition 6.1. For (b), if  $v$  is an eigenvector corresponding to  $c$ , then  $Tv = cv$  or  $(cI - T)v = 0$ . Conversely, for any nonzero  $v \in \ker(cI - T)$ , we have  $Tv = cv$ . ♠

## Diagonalization

**Def'n. Diagonalizable** Linear Operator

Let  $V$  be a finite-dimensional vector space. A linear operator  $T : V \rightarrow V$  is called **diagonalizable** if there is an ordered basis  $\beta$  for  $V$  such that  $[T]_\beta$  is a diagonal matrix. Moreover  $A \in M_{n \times n}(\mathbb{F})$  is called **diagonalizable** if its left multiplication operator  $L_A : \mathbb{F}^n \rightarrow \mathbb{F}^n$  is diagonalizable.

**Remark 6.5.** Another way to state the diagonalizability of a (square) matrix is that  $A \in M_{n \times n}(\mathbb{F})$  is diagonalizable if and only if  $A$  is similar to a diagonal  $B$  over  $\mathbb{F}$ .

**Proposition 6.4.**  
 $T : V \rightarrow V$  Is  
 Diagonalizable If and  
 Only If a Eigenbasis  
 for  $V$  Exists

Let  $T : V \rightarrow V$  be a linear operator on an  $n$ -dimensional vector space  $V$ . Then  $T$  is diagonalizable if and only if there exists an ordered basis  $\beta$  for  $V$  consisting of eigenvectors of  $T$ .

*Proof.* For the forward direction, suppose that  $T$  is diagonalizable. Then there exists ordered basis  $\beta = \{v_1, v_2, \dots, v_n\}$  such that  $[T]_\beta$  is diagonal. So  $([T]_\beta)_{ii} = c_i$  for some  $c_i \in \mathbb{F}$ , and  $([T]_\beta)_{ij} = 0$  whenever  $i \neq j$ . That is,

$$Tv_i = c_i v_i$$

so  $v_i$  is an eigenvector of  $T$  for each  $i \in \{1, 2, \dots, n\}$ . For the reverse direction, suppose that  $\beta = \{v_1, v_2, \dots, v_n\}$  is consisting of eigenvectors. Then  $Tv_i = c_i v_i$  for some  $c_i \in \mathbb{F}$ , which exactly means

$$[T]_\beta = \begin{bmatrix} c_1 & 0 & \cdots & 0 \\ 0 & c_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & c_n \end{bmatrix}.$$

♠

**Corollary 6.4.1.**

Let  $A \in M_{n \times n}(\mathbb{F})$ . Then  $A$  is diagonalizable if and only if there is an ordered basis for  $\mathbb{F}^n$  consisting of eigenvectors of  $A$ .

**Proposition 6.5.  
Eigenvectors  
Corresponding to  
Distinct Eigenvalues  
Are Linearly  
Independent**

Let  $T : V \rightarrow V$  be a linear operator where  $\dim(V) = n$ . Let  $c_1, c_2, \dots, c_m$  be distinct eigenvalues of  $T$ . If  $v_1, v_2, \dots, v_m$  are eigenvectors of  $T$  corresponding to  $c_1, c_2, \dots, c_m$ , then  $\{v_1, v_2, \dots, v_m\}$  is linearly independent.

*Proof.* We proceed by induction on  $m$ . When  $m = 1$ , observe that  $\{v_1\}$  is linearly independent, since any eigenvector is nonzero. Moreover, suppose that  $\{v_1, v_2, \dots, v_k\}$  is linearly independent for some  $k \leq m - 1$ . For the sake of contradiction, further suppose that  $\{v_1, v_2, \dots, v_{k+1}\}$  is linearly dependent. Then there exists  $(a_1, \dots, a_k) \in \mathbb{F}^k$  such that

$$v_{k+1} = \sum_{i=1}^k a_i v_i.$$

Then

$$c_{k+1} v_{k+1} = T v_{k+1} = T \sum_{i=1}^k a_i v_i = \sum_{i=1}^k a_i T v_i = \sum_{i=1}^k a_i c_i v_i,$$

so

$$v_{k+1} = \sum_{i=1}^k a_i \frac{c_i}{c_{k+1}} v_i,$$

where each  $\frac{c_i}{c_{k+1}} \neq 1$  since each eigenvalue is distinct, so we have two different representation of  $v_{k+1}$  as a linear combination of  $v_1, v_2, \dots, v_k$ , which contradicts the linear independence of  $v_1, v_2, \dots, v_k$ . Thus  $\{v_1, v_2, \dots, v_m\}$  is linearly independent. ♠

**Corollary 6.5.1.  
Diagonalizable If  
 $n = \dim(V)$  Distinct  
Eigenvalues**

Let  $T : V \rightarrow V$  be a linear operator where  $\dim(V) = n$ . If  $T$  has  $n$  distinct eigenvalues, then  $T$  is diagonalizable.

*Proof.* Let  $c_1, c_2, \dots, c_n$  be distinct eigenvalues of  $T$  and  $v_1, v_2, \dots, v_n$  be the corresponding eigenvectors. Then  $\{v_1, v_2, \dots, v_n\}$  is linearly independent by Proposition 6.7, so is a basis for  $V$ , which exactly means  $T$  is diagonalizable by Corollary 6.5.1. ♠

**Proposition 6.6.**

Let  $V$  be a finite-dimensional vector space and let  $T : V \rightarrow V$  be diagonalizable. Then the characteristic polynomial of  $T$  can be written as a product of linear polynomials in  $\mathbb{F}$ .

*Proof.* Observe that there exists an ordered basis  $\beta$  for  $V$  such that  $[T]_\beta$  is diagonal with  $([T]_\beta)_{ii} = c_i$  for some  $c_1, c_2, \dots, c_n \in \mathbb{F}$ . That is,

$$\prod_{i=1}^n (x - c_i)$$

is the characteristic polynomial of  $T$ . ♠

**Def'n. Algebraic Multiplicity, Geometric Multiplicity of an Eigenvalue**

Let  $c$  be an eigenvalue of a linear operator  $T : V \rightarrow V$  on an  $n$ -dimensional vector space  $V$  and let  $p(t)$  be the characteristic polynomial of  $T$ . The **algebraic multiplicity** of  $c$  is the largest  $k \in \mathbb{N}$  such that  $(t - c)^k | p(t)$ . Moreover, the **geometric multiplicity** is  $\dim(E_c)$ , the dimension of the eigenspace corresponding to  $c$ .



**Proposition 6.7.**

Let  $T : V \rightarrow V$  be a linear operator where  $\dim(V) = n$  and let  $c$  be an eigenvalue of  $T$  having algebraic multiplicity  $m$ . Let  $E_c \subseteq V$  be the eigenspace corresponding to  $c$ . Then

$$1 \leq \dim(E_c) \leq m.$$

*Proof.* For convenience, let  $k = \dim(E_c)$  and let  $\{v_1, v_2, \dots, v_k\}$  be a basis for  $E_c$ . By the basis extension theorem, add  $v_{k+1}, v_{k+2}, \dots, v_n$  to form  $\beta = \{v_1, v_2, \dots, v_n\}$ , an ordered basis for  $V$ . Then,

$$[T]_\beta = \begin{bmatrix} cI & B \\ 0 & C \end{bmatrix}$$

for some  $B \in M_{k \times (n-k)}(\mathbb{F})$  and  $C \in M_{(n-k) \times (n-k)}(\mathbb{F})$ , since  $Tv_i = cv_i$  for each  $i \in \{1, 2, \dots, k\}$ . Therefore

$$f = \det(xI - [T]_\beta) = \det \begin{bmatrix} (x-c)I & B \\ 0 & xI - C \end{bmatrix} = \det((x-c)I) \det(xI - C) = (x-c)^k \det(xI - C)$$

is the characteristic polynomial of  $T$ . Thus  $(x-c)^k | f$ , which exactly means  $k \leq m$ , as desired. ♠

**Proposition 6.8.**

Let  $T$  be a linear operator and let  $c_1, c_2, \dots, c_n$  be distinct eigenvalues of  $T$ . For each  $i \in \{1, 2, \dots, k\}$ , let  $v_i$  be an eigenvector corresponding to  $c_i$ . If

$$\sum_{i=1}^k v_i = 0$$

then  $v_i = 0$  for all  $i \in \{1, 2, \dots, k\}$ .

*Proof.* It is clear that  $v_1, v_2, \dots, v_k$  are linearly independent. Thus, if

$$\sum_{i=1}^k v_i = 0,$$

then it must be the case that  $v_i = 0 \in E_{c_i}$  for each  $i \in \{1, 2, \dots, k\}$ , which is the desired result. ♠

**Proposition 6.9.**

Let  $T : V \rightarrow V$  be a linear operator and let  $c_1, c_2, \dots, c_k$  be distinct eigenvalues of  $T$ . For each  $i \in \{1, 2, \dots, k\}$ , let  $S_i$  be a finite linearly independent subset of the eigenspace  $E_{c_i}$ . Then

$$S = \bigcup_{i=1}^k S_i$$

is linearly independent.

*Proof.* Let  $n_i = |S_i|$  and write  $S_i = \{S_{i1}, S_{i2}, \dots, S_{in_i}\}$  for convenience. Then

$$S = \{S_{ij} : 1 \leq i \leq k, 1 \leq j \leq n_i\}.$$

For the sake of contradiction, suppose that  $S$  is linearly dependent. That is, there exist nonzero  $a_{ij} \in \mathbb{F}$  such that

$$\sum_{i=1}^k \sum_{j=1}^{n_i} a_{ij} S_{ij} = 0.$$

Define  $v_i = \sum_{j=1}^{n_i} a_{ij} S_{ij}$  then

$$T(v_i) = T\left(\sum_{j=1}^{n_i} a_{ij} S_{ij}\right) = \sum_{j=1}^{n_i} a_{ij} T(S_{ij}) = \sum_{j=1}^{n_i} a_{ij} c_i S_{ij} = c_i \sum_{j=1}^{n_i} a_{ij} S_{ij} = c_i v_i,$$

so each  $v_i$  is an eigenvector corresponding to  $c_i$ , and  $\{v_1, v_2, \dots, v_k\}$  is linearly independent. But this means

$$\sum_{i=1}^k v_i = \sum_{i=1}^k \sum_{j=1}^{n_i} a_{ij} S_{ij} \neq 0,$$

which is a contradiction. Thus  $S$  is linearly independent, as desired. ♠

**Proposition 6.10.**

*Let  $T : V \rightarrow V$  be a linear operator such that the characteristic polynomial  $f$  of  $T$  is a product of linear polynomials over  $\mathbb{F}$  and  $\dim(V) = n$ . Let  $c_1, c_2, \dots, c_k$  be all distinct eigenvalues of  $T$ .*

- (a)  *$T$  is diagonalizable if and only if the algebraic multiplicity of  $c_i$  is equal to the geometric multiplicity of  $c_i$  for all  $i \in \{1, 2, \dots, k\}$ .*
- (b) *If  $T$  is diagonalizable and each  $\beta_i$  is an ordered basis for the eigenspace corresponding to  $c_i$ , then  $\beta = \beta_1 \cup \beta_2 \cup \dots \cup \beta_k$  is an eigenbasis for  $V$ .*

*Proof.* Write

$$f = \prod_{i=1}^k (x - c_i)^{m_i}$$

where  $\sum_{i=1}^k m_i = \deg(f) = n$  by the assumption. For the forward direction of (a), suppose that  $T$  is diagonalizable. Let  $\beta$  be an ordered basis for  $V$  and let each  $E_i \subseteq V$  be the eigenspace corresponding to  $c_i$ . Define  $\beta_i = \beta \cap E_i$  then  $|\beta_i| \leq \dim(E_i)$ , since  $\beta_i$  is linearly independent. Moreover,  $\dim(E_i) \leq m_i$  by the previous proposition. So we have

$$\sum_{i=1}^k |\beta_i| \leq \sum_{i=1}^k \dim(E_i) \leq \sum_{i=1}^k m_i = n,$$

but clearly  $\sum_{i=1}^k |\beta_i| = n$  as well, since  $\beta_i \cap \beta_j = \emptyset$  whenever  $i \neq j$ . Therefore

$$\sum_{i=1}^k [m_i - \dim(E_i)] = 0,$$

but since  $m_i \geq \dim(E_i)$  for each  $i \in \{1, 2, \dots, k\}$ , it must be the case that  $m_i = \dim(E_i)$ . For the reverse direction of (a), suppose  $m_i = \dim(E_i)$  for each  $i \in \{1, 2, \dots, k\}$ . We simultaneously show that  $T$  is diagonalizable and prove (b). For each  $i \in \{1, 2, \dots, k\}$ , let  $\beta_i$  be an ordered basis for  $E_i$ , and let  $\beta = \beta_1 \cup \beta_2 \cup \dots \cup \beta_k$ . Then  $\beta$  is linearly independent by Proposition 6.11. Furthermore, since  $\dim\{E_i\} = |\beta_i| = m_i$  for each  $i \in \{1, 2, \dots, k\}$ ,

$$|\beta| = \sum_{i=1}^k |\beta_i| = \sum_{i=1}^k m_i = n.$$

Therefore  $\beta$  is an ordered basis for  $V$  containing eigenvectors of  $T$ , which means  $T$  is diagonalizable. ♠

**Remark 6.6.** Proposition 6.10 provides the following way of checking whether a linear operator  $T : V \rightarrow V$  is diagonalizable or not.

**Proposition 6.11.**  
**Diagonalizability Test**

*Let  $T : V \rightarrow V$  is diagonalizable if and only if the following conditions hold.*

- (a) *The characteristic polynomial of  $T$  is a product of linear factors.*
- (b) *For each eigenvalue  $c$  of  $T$ , the algebraic multiplicity of  $c$  equals  $\dim(V) - \text{rank}(cI - T)$ .*

**Proposition 6.12.**  
**Eigendecomposition**

Let  $A \in M_{n \times n}(\mathbb{F})$  be diagonalizable,  $c_1, c_2, \dots, c_k$  be all distinct eigenvalues, and  $\beta_1, \beta_2, \dots, \beta_k$  be bases for the corresponding eigenspaces  $E_1, E_2, \dots, E_n$ . Let

$$\beta = \beta_1 \cup \beta_2 \cup \dots \cup \beta_k,$$

let  $P \in M_{n \times n}(\mathbb{F})$  be such that  $\text{Col}_j(P) \in \beta$  for each  $j \in \{1, 2, \dots, n\}$  and  $\text{Col}_j(P) \neq \text{Col}_k(P)$  whenever  $j \neq k$ , and let  $D \in M_{n \times n}(\mathbb{F})$  be a diagonal matrix whose diagonal entries are eigenvalues corresponding to the columns of  $P$ . Then  $A = PDP^{-1}$ .

*This page intentionally left blank.*

# 7.

## Elementary Canonical Forms

- 
- 7.1 Eigenvalues
  - 7.2 Annihilating Polynomials
  - 7.3 Triangulation and Diagonalization
  - 7.4 Direct Sum Decompositions
  - 7.5 Invariant Direct Sum
  - 7.6 Primary Decomposition Theorem
-

**Remark 7.1.** Throughout this chapter, let  $V$  denote a finite-dimensional vector space over a field  $\mathbb{F}$ , unless otherwise specified.

**Remark 7.2.** The goal of this chapter is to find an ordered basis  $\beta$  for  $V$  provided a linear operator  $T : V \rightarrow V$  such that  $[T]_\beta$  is in a simple form (i.e. diagonal, triangular, ...).

## Eigenvalues

**Proposition 7.1.**  
 *$f(T)v = f(c)v$  for any  
 Eigenpair  $(c, v)$*

*Let  $T$  be a linear operator on  $V$ ,  $v \in V$  be an eigenvector of  $T$ , and  $c \in \mathbb{F}$  be the eigenvalue corresponding to  $v$ . Then  $f(T)v = f(c)v$  for any  $f \in \mathbb{F}[x]$ .*

*Proof.* Write  $f = \sum_{i=0}^n a_i x^i \in \mathbb{F}[x]$ . Then

$$f(T)v = \left( \sum_{i=0}^n a_i T^i \right) v = \sum_{i=0}^n a_i T^i(v) = \sum_{i=0}^n a_i (cv)^i = \left( \sum_{i=0}^n a_i c^i \right) v = f(c)v. \quad \spadesuit$$

**Proposition 7.2.**

*Let  $T : V \rightarrow V$  be a linear operator. Let  $c_1, c_2, \dots, c_k \in \mathbb{F}$  be distinct eigenvalues of  $T$  and let  $W_1, W_2, \dots, W_k$  be the corresponding eigenspaces, respectively. Then*

$$\dim(W_1 + W_2 + \dots + W_k) = \sum_{i=1}^k \dim(W_i).$$

*In particular, if  $\beta_1, \beta_2, \dots, \beta_k$  are bases for  $W_1, W_2, \dots, W_k$ , respectively, then*

$$\beta = \bigcup_{i=1}^k \beta_i$$

*is a basis for  $W = W_1 + W_2 + \dots + W_k$ .*

*Proof.* Notice that  $W_i \cap W_j = \{0\}$  for any distinct  $i, j \in \{1, 2, \dots, k\}$ , since each eigenspace is characterized by the corresponding eigenvalue. It follows that any bases  $\beta_i$  for  $W_i$  and  $\beta_j$  for  $W_j$  are linearly independent. Thus we conclude  $\beta = \bigcup_{i=1}^k \beta_i$  is a basis for  $W$ . It follows that  $\dim(W) = \sum_{i=1}^k \dim(W_i)$ .  $\spadesuit$

**Proposition 7.3.**  
 Alternative  
 Definitions of  
 Diagonalizability

*Let  $T : V \rightarrow V$  be a linear operator. The following are equivalent.*

- (a)  $T$  is diagonalizable.
- (b) There exist  $c_1, c_2, \dots, c_k \in \mathbb{F}$  such that

$$f = \prod_{i=1}^k (x - c_i)^{m_i}$$

*is the characteristic polynomial of  $T$ , where  $m_i$  is the dimension of the eigenspace  $W_i$  corresponding to  $c_i$ .*

- (c)  $\sum_{i=1}^k \dim(W_i) = \dim(V)$ .

*Proof.* (a)  $\implies$  (b) is a direct result of the fact that the diagonal entries of a diagonal matrix is the eigenvalues of the matrix. (b)  $\implies$  (c) is clear, since

$$\dim(V) = \deg(f) = \sum_{i=1}^k m_i = \sum_{i=1}^k \dim(W_i).$$

Notice that (c)  $\implies$  (a) is a direct result of Proposition 7.2. ♠

## Annihilating Polynomials

### Def'n. Annihilating Polynomial of a Linear Operator

Let  $V$  be a vector space and  $T : V \rightarrow V$  be a linear operator. We say  $f \in \mathbb{F}[x]$  is an *annihilating polynomial* of  $T$  if  $f(T) = 0$ .

### Proposition 7.4. Set of Annihilating Polynomial Is an Ideal

Let  $T : V \rightarrow V$ . Then the set of annihilating polynomials of  $T$ ,

$$M_T = \{f \in \mathbb{F}[x] : f(T) = 0\},$$

is an ideal of  $\mathbb{F}[x]$ .

*Proof.* Let  $f, g \in M_T$  and  $h \in \mathbb{F}[x]$ . Clearly  $(f - g)(T) = f(T) - g(T) = 0 - 0 = 0$ . Moreover,  $(fh)(T) = f(T)h(T) = 0h(T) = 0$  so  $fh \in M$ . Thus by the ideal test,  $M_T \subseteq \mathbb{F}[x]$  is an ideal of  $\mathbb{F}[x]$ . ♠

**Remark 7.3.** If  $V$  is an arbitrary vector space and  $T : V \rightarrow V$  is linear, then  $T$  need not have an annihilating polynomial except for  $0 \in \mathbb{F}[x]$ . But when  $V$  is finite-dimensional,  $T$  always has a nonzero annihilating polynomial. This can be shown as follows. Let  $n = \dim(V) \in \mathbb{N}$  then  $\dim(\mathcal{L}(V, V)) = n^2$ , so  $T^0, T^1, \dots, T^{n^2}$  are linearly dependent. This means there exists nonzero  $(c_0, c_1, \dots, c_{n^2}) \in \mathbb{F}^{n^2+1}$  such that

$$\sum_{i=0}^{n^2} c_i T^i = 0.$$

But this exactly means

$$f = \sum_{i=0}^{n^2} c_i x^i \in \mathbb{F}[x]$$

is an annihilating polynomial of  $T$ . Then Proposition 5.10 and Corollary 5.10.1 guarantee that there exists a unique  $p \in \mathbb{F}[x]$  which generates the ideal of annihilating polynomials of  $T$ ,  $M_T$ . This motivates the following definition.

### Def'n. Minimal Polynomial of a Linear Operator

Let  $T : V \rightarrow V$  be linear. We say  $p \in \mathbb{F}[x]$  is the *minimal polynomial* of  $T$  if  $p$  is the unique monic generator of  $M_T$ .

**Remark 7.4.** Observe that the minimal polynomial  $p \in \mathbb{F}[x]$  of a linear operator  $T : V \rightarrow V$  is uniquely determined by the following.

- (a)  $p$  is monic.
- (b)  $p(T) = 0$ .
- (c) No polynomial over  $\mathbb{F}$  which annihilates  $T$  has smaller degree than  $p$  has.

The name *minimal* stems from (c).

### Def'n. Minimal Polynomial of a Matrix

Let  $A \in M_{n \times n}(\mathbb{F})$ . We say  $p \in \mathbb{F}[x]$  is the *minimal polynomial* of  $A$  if  $p$  is the unique monic generator of the ideal of annihilating polynomials of  $A$  over  $\mathbb{F}$ .

**Remark 7.5.** Let  $T : V \rightarrow V$  be a linear operator and let  $\beta$  be an ordered basis for  $V$ . Then it is clear that the minimal polynomial of  $T$  and  $[T]_\beta$  are identical, since

$$[f(T)]_\beta = f[T]_\beta$$

for any  $f \in \mathbb{F}[x]$ , so  $f(T) = 0$  if and only if  $f[T]_\beta = 0$ . Furthermore, this result also shows that, if  $A, B \in M_{n \times n}(\mathbb{F})$  are similar, then  $A$  and  $B$  have the same minimal polynomial.

**Remark 7.6.** Let  $T : V \rightarrow V$  be diagonalizable and let  $c_1, c_2, \dots, c_k \in \mathbb{F}$  be the distinct eigenvalues of  $T$ . Then it is easy to see that

$$p = \prod_{i=1}^k (x - c_i)$$

is the minimal polynomial of  $T$ . To verify this, let  $v \in V$  be arbitrary. Then by Proposition 7.2, there exist eigenvectors  $v_1, v_2, \dots, v_k \in V$  corresponding to  $c_1, c_2, \dots, c_k$ , respectively, such that

$$v = \sum_{i=1}^k v_i.$$

Then, for any  $f \in \mathbb{F}[x]$ ,

$$f(T)v = f(T) \sum_{i=1}^k v_i = \sum_{i=1}^k f(T)v_i = \sum_{i=1}^k f(c_i) v_i,$$

so if  $f(T)v = 0$ , then  $f(c_i) = 0$  for all  $i \in \{1, 2, \dots, k\}$ . This means  $p \mid f$ . But it is clear that  $p$  is the polynomial of minimum degree which satisfies the above equation.

**Proposition 7.5.**  
Minimal Polynomial  
of any Diagonalizable  
Operator Is a Product  
of Linear Factors

*Let  $V$  be a vector space over  $\mathbb{F}$  and let  $T : V \rightarrow V$  be a diagonalizable linear operator with eigenvalues  $c_1, c_2, \dots, c_n \in \mathbb{F}$ . Then*

$$p = \prod_{i=1}^k (x - c_i)$$

*is the minimal polynomial of  $T$ .*

**Remark 7.7.** We will discuss that the converse of Proposition 7.5 is also true later. That is,  $T$  is diagonalizable if and only if its minimal polynomial is a product of linear factors of degree 1.

**Proposition 7.6.**  
The Characteristic  
and Minimal  
Polynomials Have the  
Same Roots

*Let  $T : V \rightarrow V$  be linear. Then the characteristic polynomial and minimal polynomial have the same roots.*

*Proof.* Let  $p \in \mathbb{F}[x]$  be the minimal polynomial of  $T$ . Notice that it is equivalent to prove that  $p(c) = 0$  if and only if  $c \in \mathbb{F}$  is an eigenvalue of  $T$ . For the forward direction, suppose  $p(c) = 0$ . It follows that  $p = (x - c)q$  for some  $q \in \mathbb{F}[x]$ , where  $q(T) \neq 0$  by the minimality of  $p$ . Let  $v \in V$  be such that  $q(T)v \neq 0$ . Then

$$p(T)v = (T - cI)q(T)v = 0$$

so  $T - cI$  is not invertible and  $c$  is an eigenvalue of  $T$ . The reverse direction is a direct consequence of Proposition 7.1. ♠

**Theorem 7.7.**  
Cayley-Hamilton  
Theorem

*Let  $T : V \rightarrow V$  be a linear operator. If  $p$  is the characteristic polynomial of  $T$ , then  $p(T) = 0$ . Equivalently, the minimal polynomial divides the characteristic polynomial.*



*Proof.* Let  $K$  be a commutative, unital algebra over  $\mathbb{F}$ . Let  $(v_1, v_2, \dots, v_n)$  be an ordered basis for  $V$  and  $A = [T]_\beta$ . Then

$$T(v_i) = \sum_{j=1}^n A_{ji} v_j$$

or, equivalently,

$$\sum_{j=1}^n (T - A_{ji}I)(v_j) = 0.$$

Define  $B \in M_{n \times n}(K)$  by  $B_{ij} = T - A_{ji}I$ . Then  $\det(B) = f(T)$ . Now the claim is that  $\det(B)v_i = 0$  for each  $i \in \{1, 2, \dots, n\}$ . To verify this, let  $\tilde{B} = \text{adj}(B)$ . By definition,  $\sum_{j=1}^n B_{ij}v_j = 0$ , so

$$\sum_{j=1}^n \tilde{B}_{ki} B_{ij} v_j = 0$$

for each  $k, i \in \{1, 2, \dots, n\}$ . By summing over  $i$ ,

$$\sum_{i=1}^n \sum_{j=1}^n \tilde{B}_{ki} B_{ij} v_j = \sum_{j=1}^n \left( \sum_{i=1}^n \tilde{B}_{ki} B_{ij} \right) v_j = 0.$$

Since  $\tilde{B}B = \text{adj}(B)B = \det(B)I$  by definition,

$$\tilde{B}_{ki} B_{ij} = \delta_{kj} \det(B).$$

That is,

$$\sum_{j=1}^n \det(B) v_j = \det(B) v_k = 0$$

for each  $k \in \{1, 2, \dots, n\}$ . Thus by the linearity of  $\det(B) = f(T)$ ,

$$f(T)v = 0$$

for all  $v \in V$ , as desired. ♠

## Triangulation and Diagonalization

### Def'n. $T$ -Invariant Subspace

Let  $V$  be a vector space and  $T : V \rightarrow V$  be a linear operator on  $V$ . We say a subspace  $W \subseteq U$  is  *$T$ -invariant* if  $T(W) \subseteq W$ . Equivalently,

$$\forall w \in W [Tw \in W].$$

**Remark 7.8.** Whenever  $W \subseteq V$  is  $T$ -invariant, we may restrict  $T$  to  $W$ . That is, there is a  $T_W : W \rightarrow W$  by  $w \mapsto Tw$ . In terms of matrices, suppose  $\alpha = \{v_1, v_2, \dots, v_k\}$  is an ordered basis for  $W$ . By basis extension, there exist  $v_{k+1}, v_{k+2}, \dots, v_n \in V$  such that  $\beta = \{v_1, v_2, \dots, v_n\}$  is an ordered basis for  $V$ . Then

$$[T]_\beta = \begin{bmatrix} [T_W]_\alpha & B \\ O & C \end{bmatrix}$$

for some  $B \in M_{k \times (n-k)}(\mathbb{F})$ ,  $C \in M_{(n-k) \times (n-k)}$  and zero matrix  $O$ .

### Def'n. Restriction of a Linear Operator on an Invariant Subspace

Let  $T : V \rightarrow V$  be a linear operator and let  $W \subseteq V$  be a  $T$ -invariant subspace. The linear operator  $T_W : W \rightarrow W$  defined by

$$w \mapsto Tw$$

is called the *restriction* of  $T$  on  $W$ .

**Remark 7.9.** For any linear operator  $T : V \rightarrow V$ ,  $\{0\}$  and  $V$  are  $T$ -invariant. Moreover,  $\ker(T)$ ,  $\text{image}(T) \subseteq V$  are  $T$ -invariant as well.

**Remark 7.10.** Here is a generalization of Remark 7.8. Let  $T, U : V \rightarrow V$  linear operators such that  $T$  and  $U$  commute. Then  $\ker(U)$  and  $\text{image}(U)$  are  $T$ -invariant. That is, if  $v \in \text{image}(U)$ , say  $v = Uw$  for some  $w \in V$ , then

$$Tv = TUw = UTw \in \text{image}(U).$$

Similarly, if  $v \in \ker(U)$ , then

$$UTv = TUv = T_0 = 0,$$

which means  $Tv \in \ker(U)$ . A particular type of operators which commute with  $T$  is a polynomial in  $T$ . For instance,  $U = T - cI$  for some eigenvalue  $c \in \mathbb{F}$  for  $T$  (suppose  $T$  has an eigenvalue) is a polynomial in  $T$ , and  $\ker(U)$  is the eigenspace corresponding to  $c$ . That is, any eigenspace of a linear operator  $T$  is  $T$ -invariant.

**Proposition 7.8.**

Let  $T : V \rightarrow V$  be linear and let  $W \subseteq V$  be  $T$ -invariant. Let  $T_W : W \rightarrow W$  be the restriction of  $T$  on  $W$ . Let  $p, f \in \mathbb{F}[x]$  be the minimal and characteristic polynomials for  $T$  and let  $p_W, f_W \in \mathbb{F}[x]$  be the minimal and characteristic polynomials for  $T_W$ . Then  $p_W \mid p$  and  $f_W \mid f$ .

*Proof.* Consider the block matrix

$$[T]_\beta = \begin{bmatrix} [T_W]_\alpha & B \\ O & C \end{bmatrix}$$

from Remark 7.8. It is clear that

$$f = \det(xI - [T]_\beta) = \det(xI - [T_W]_\alpha) \det(xI - C) = f_W \det(xI - C)$$

so  $f_W \mid f$ . Moreover, for any  $k \in \mathbb{N}$ ,

$$[T]_\beta^k = \begin{bmatrix} [T_W]_\alpha^k & B' \\ O & C^k \end{bmatrix}$$

for some  $B' \in M_{r \times n-r}(\mathbb{F})$ . Therefore, any annihilating polynomial of  $[T]_\beta$  annihilates  $[T_W]_\alpha$  as well. That is,  $p_W \mid p$ . ♠

**Def'n.  $T$ -Conductor,  $T$ -Annihilator of a Vector**

Let  $V$  be an  $n$ -dimensional vector space and let  $T : V \rightarrow V$  be a linear operator. Let  $W \subseteq V$  be a  $T$ -invariant subspace of  $V$  and  $v \in V$ . Define

$$S_T(v; W) = \{f \in \mathbb{F}[x] : f(T)v \in W\}$$

which we call the  **$T$ -conductor** of  $v$  into  $W$ . If  $W = \{0\}$ , we say  $S_T(v; W)$  is a  **$T$ -annihilator** of  $v$ . Moreover, the unique monic generator of  $S_T(v; W)$ , denoted as  $s_T(v; W)$ , is unique and also called the  **$T$ -conductor** of  $v$  into  $W$ .

**Proposition 7.9.**  
 **$T$ -Conductor Is an Ideal**

Let  $T : V \rightarrow V$  be linear and  $W \subseteq V$  be a  $T$ -invariant subspace. Then  $S_T(v; W)$  is an ideal of  $\mathbb{F}[x]$ .

*Proof.* Let  $f, g \in S_T(v; W)$  and  $h \in \mathbb{F}[x]$ . Then

$$(f - g)(T)v = (f(T) - g(T))v = f(T)v - g(T)v \in W,$$

so  $f - g \in S_T(v; W)$ . Moreover,

$$(fh)(T)v = (hf)(T)v = h(T)(f(T)v) \in W,$$

so  $fh \in S_T(v; W)$ , as desired. ♠

**Def'n. Triangulable Linear Operator**

Let  $T : V \rightarrow V$  be a linear operator on a finite-dimensional vector space  $V$ . We say  $T$  is *triangulable* if there is an ordered basis  $\beta$  for  $V$  such that  $[T]_\beta$  is triangular.

**Proposition 7.10.**

Let  $V$  be a finite-dimensional vector space over  $\mathbb{F}$  and let  $T : V \rightarrow V$  be a linear operator. Suppose the minimal polynomial  $p \in \mathbb{F}[x]$  of  $T$  is a product of linear factors, that

$$p = \prod_{i=1}^k (x - c_i)^{r_i}$$

for some  $c_1, c_2, \dots, c_k \in \mathbb{F}$  and  $r_1, r_2, \dots, r_k \in \mathbb{N}$ . Let  $W \subsetneq V$  be a  $T$ -invariant proper subspace of  $V$ . Then there exists  $v \in V$  such that

(a)  $v \notin W$  and

(b)  $(T - cI)v \in W$  for some eigenvalue  $c \in \mathbb{F}$  of  $T$ .

*Proof.* Let  $u \in V$  be such that  $u \notin W$  and let  $g$  be the  $T$ -conductor of  $u$  into  $W$ . Then  $g \mid p$ , so  $g = \prod_{i=1}^k (x - c_i)^{s_i}$  for some  $s_1, s_2, \dots, s_k$  where  $0 \leq s_i \leq r_i$  for each  $i \in \{1, 2, \dots, k\}$  and at least one  $s_i$  is nonzero. Then

$$g = (x - c_i)h$$

for some  $i \in \{1, 2, \dots, k\}$  and  $h \in \mathbb{F}[x]$ . By minimality of  $g$ ,  $v = h(T)(u) \notin W$ . However,

$$(T - c_i I)(v) = (T - c_i I)h(T)(u) = g(T)(v) \in W$$

by construction. ♠

**Remark 7.11.** Notice that  $(T - c_i I)(v) = (x - c_i)(T)(v)$ . So if  $(T - c_i I)(v) \in W$ , the  $T$ -conductor of  $v$  into  $W$  is a linear polynomial  $(x - c_i)$ .

**Theorem 7.11.**  
 **$T$  Is Triangulable If  
 and Only If Its  
 Minimal Polynomial  
 Splits**

Let  $V$  be a finite-dimensional vector space over  $\mathbb{F}$  and let  $T : V \rightarrow V$  be a linear operator. Then  $T$  is triangulable if and only if the minimal polynomial of  $T$  is a product of linear polynomials over  $\mathbb{F}$ .

*Proof.* For the forward direction, suppose  $T$  is triangulable. Then the characteristic polynomial of  $T$  is a product of linear factors, so minimal polynomial is also a product of linear factors. For the reverse direction, we proceed inductively. Suppose that  $p$ , the minimal polynomial of  $T$ , is a product of linear factors. Observe that  $W_0 = \{0\}$  is a proper  $T$ -invariant subspace, so there exists  $v_1 \in V \setminus W_0$  such that  $(T - cI)v_1 \in W_0$  for some eigenvalue  $c$  by Proposition 7.10. We also see that  $\beta_1 = \{v_1\}$  spans a  $T$ -invariant subspace, since

$$(T - cI)v_1 \in W_0 \iff Tv_1 = cv_1 \iff Tv_1 \in \text{span}\{v_1\}.$$

Now suppose that  $\beta_k = \{v_1, v_2, \dots, v_k\}$  is a basis for  $T$ -invariant proper subspace  $W_k$ . Then by Proposition 7.10, there exists  $v_{k+1} \in V \setminus W_k$  such that  $(T - cI)v_{k+1} \in W_k$ . It follows that

$$(T - cI)v_{k+1} \in W_k \iff Tv_{k+1} = cv_{k+1} + \sum_{i=1}^k a_i v_i \iff Tv_{k+1} \in \text{span}\{v_1, v_2, \dots, v_{k+1}\}.$$

But this exactly means  $W_{k+1}$  is  $T$ -invariant. So continuing this process, we have a basis  $\beta = \{v_1, v_2, \dots, v_n\}$ . Moreover, the  $T$ -invariance of  $W_1, W_2, \dots, W_{n-1}$  guarantees that  $[T]_\beta$  is upper-triangular, as required. ♠

**Theorem 7.12.**  
 **$T$  Is Diagonalizable If and Only If Its Minimal Polynomial Is a Product of Distinct Linear Factors**

Let  $V$  be a finite-dimensional vector space and let  $T : V \rightarrow V$  be a linear operator. Then  $T$  is diagonalizable if and only if the minimal polynomial of  $T$  is of the form

$$\prod_{i=1}^k (x - c_i).$$

*Proof.* The forward direction is supplied by Proposition 7.5. For the reverse direction, suppose

$$p = \prod_{i=1}^k (x - c_i)$$

is the minimal polynomial. Let  $W \subseteq V$  be the subspace of  $V$  generated by every eigenvectors of  $T$ . For the sake of contradiction, suppose  $W \subsetneq V$ . Then there exists  $v \in V \setminus W$  such that  $(T - cI)v \in W$  by Proposition 7.10, since a subspace generated by eigenvectors is  $T$ -invariant. Let  $u = (T - cI)v \in W$ . Then,

$$u = \sum_{i=1}^k v_i$$

for some  $v_1, v_2, \dots, v_k \in W$  satisfying  $Tv_i = c_i v_i$  for all  $i \in \{1, 2, \dots, k\}$ . Then for any  $f \in \mathbb{F}[x]$ ,

$$f(T)u = f(T) \sum_{i=1}^k v_i = \sum_{i=1}^k f(T)v_i = \sum_{i=1}^k f(c_i)v_i$$

is an element of  $W$ . Now  $p = (x - c_j)q$  for some eigenvalue  $c_j \in \mathbb{F}$  and  $q \in \mathbb{F}[x]$ . Also,

$$q - q(c_j) = (x - c_j)g$$

for some  $g \in \mathbb{F}[x]$ , since  $q(c_j) - q(c_j) = 0$ . So we have

$$(q - q(c_j))(T)v = (T - c_j I)g(T)v = g(T)u.$$

But  $g(T)u \in W$ , and since

$$0 = p(T)v = (T - c_j I)q(T)v,$$

$q(T)v$  is an eigenvector corresponding to  $c_j$ . That is,  $q(T)v \in W$ . So clearly  $q(c_j)v \in W$  as well, but  $v \notin W$  so  $q(c_j) = 0$ . This is a contradiction, since  $p = (x - c_j)q$  is a product of linear factors of degree 1. Thus  $W = V$ , which exactly means that  $T$  is diagonalizable. ♠

**Remark 7.12.** We shall give a different proof of Theorem 7.12 later.

## Direct Sum Decompositions

**Remark 7.13.** At the beginning of the chapter, we introduced that our goal is to find an ordered basis in which the matrix representation of a linear operator assumes a simple form. Now, we shall describe our goal as follows: To decompose the underlying space  $V$  into a direct sum of  $T$ -invariant subspaces such that the restriction operators on those subspaces are simple.

### Def'n. Independent Subspaces

Let  $V$  be a vector space and let  $W_1, W_2, \dots, W_k \subseteq V$  be subspaces. We say  $W_1, W_2, \dots, W_k$  are *independent* if

$$\sum_{i=1}^k w_i = 0 \implies w_1 = w_2 = \dots = w_k = 0,$$

provided that each  $w_i \in W_i$ .

**Remark 7.14.** When  $k = 2$ , the meaning of independence is merely  $\{0\}$  intersection. When  $k > 2$ , it means more than that:

$$\forall j \in \{1, 2, \dots, k\} [W_j \cap (W_1 + W_2 + \dots + W_{j-1} + W_{j+1} + \dots + W_k) = \{0\}].$$

The significance of independence can be shown as follows. If  $W_1 + W_2 + \dots + W_k = W \subseteq V$ , then there exist  $w_1 \in W_1, w_2 \in W_2, \dots, w_k \in W_k$  such that

$$w = \sum_{i=1}^k w_i$$

for all  $w \in W$ .

**Proposition 7.13.**  
**Alternative**  
**Definitions of**  
**Independence**

Let  $V$  be a finite-dimensional vector space and let  $W_1, W_2, \dots, W_k \subseteq V$  be subspaces, where  $W = W_1 + W_2 + \dots + W_k$ . Then the following are equivalent.

- (a)  $W_1, W_2, \dots, W_k$  are independent.
- (b)  $\forall j \in \{2, 3, \dots, k\} [W_j \cap (W_1 + W_2 + \dots + W_{j-1}) = \{0\}]$ .
- (c) If  $\beta_1, \beta_2, \dots, \beta_k$  are ordered bases for  $W_1, W_2, \dots, W_k$ , then  $\beta = (\beta_1, \beta_2, \dots, \beta_k)$  is an ordered basis for  $W$ .

*Proof.* For (a)  $\implies$  (b), suppose  $W_1, W_2, \dots, W_k$  are independent. Then for any  $j \in \{1, 2, \dots, k\}$ ,

$$W_j \cap (W_1 + W_2 + \dots + W_{j-1} + W_{j+1} + \dots + W_k) = \{0\}$$

by Remark 7.14. It follows that (b) is true as well. For (b)  $\implies$  (c), let  $w \in W$ . Then there exist  $w_1 \in W_1, w_2 \in W_2, \dots, w_k \in W_k$  such that

$$w = \sum_{i=1}^k w_i.$$

This is a unique representation of  $w$  as a sum of elements of  $W_1, W_2, \dots, W_k$ , since (b) implies that  $w_i \notin W_j$  whenever  $i \neq j$ . This exactly means  $\beta = (\beta_1, \beta_2, \dots, \beta_k)$  is an ordered basis for  $W$ . For (c)  $\implies$  (a), suppose  $\beta = (\beta_1, \beta_2, \dots, \beta_k)$  is an ordered basis for  $W$ . Then  $\beta_1, \beta_2, \dots, \beta_k$  are linearly independent, so whenever we have a linear relation

$$\sum_{i=1}^k w_i = 0,$$

where each  $w_i \in W_i$  for each  $i \in \{1, 2, \dots, k\}$ ,  $w_1 = w_2 = \dots = w_k = 0$ . But this exactly means that  $W_1, W_2, \dots, W_k$  are independent. ♠

**Def'n. Direct Sum of Subspaces**

Let  $V$  be a vector space and let  $W_1, W_2, \dots, W_k \subseteq V$  be subspaces. If  $W_1, W_2, \dots, W_k$  are independent, then we say the sum

$$W = W_1 + W_2 + \dots + W_k$$

is **direct**. Moreover, we write

$$W = W_1 \oplus W_2 \oplus \dots \oplus W_k = \bigoplus_{i=1}^k W_i$$

to indicate that  $W$  is the direct sum of  $W_1, W_2, \dots, W_k$ .

**Def'n. Projection** of a Vector Space

Let  $V$  be a vector space. A linear operator  $E : V \rightarrow V$  is called a **projection** of  $V$  if  $E^2 = E$ .

**Proposition 7.14.**  
**Properties of**  
**Projections**

Let  $V$  be a vector space and let  $E : V \rightarrow V$  be a projection. Then the following hold.

(a) For any  $v \in V$ ,  $v \in \text{image}(E)$  if and only if  $Ev = v$ .

(b)  $V = \text{image}(E) \oplus \ker(E)$ . In particular,

$$Ev + (v - Ev) = v \in V$$

is the unique representation for any  $v \in V$  as a sum of vectors in  $\text{image}(E)$  and  $\ker(E)$ .

**Corollary 7.14.1.**  
**Projection on  $R$  along**  
 **$N$** 

Let  $V$  be a vector space and let  $R, N \subseteq V$  be subspaces satisfying  $R \oplus N = V$ . Then there exists a unique projection  $E : V \rightarrow V$  such that  $\text{image}(E) = R$  and  $\ker(E) = N$ .

**Def'n. Projection** on  $R$  along  $N$ 

Consider Corollary 7.14.1. We say  $E : V \rightarrow V$  the **projection** on  $R$  along  $N$ .

**Remark 7.15.** Any projection is trivially diagonalizable. Let  $E : V \rightarrow V$  be a projection and let  $\beta_R, \beta_N$  be ordered bases for  $\text{image}(E)$  and  $\ker(E)$ . Then

$$[E]_{(\beta_R, \beta_N)} = \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix},$$

where  $k = \dim(\text{image}(E)) = |\beta_R|$ .

**Remark 7.16.** Projections can be used to conveniently describe direct sum decompositions of vector spaces. Let  $V$  be a vector space and suppose

$$V = \bigoplus_{i=1}^k W_i$$

where  $W_1, W_2, \dots, W_k \subseteq V$  are subspaces. Then we shall define linear operators  $E_1, E_2, \dots, E_k : V \rightarrow V$  such that

$$E_i(v) = w_i$$

provided that  $v = \sum_{i=1}^k w_i$  for some  $w_1 \in W_1, w_2 \in W_2, \dots, w_k \in W_k$ . It can be easily verified that each  $E_i$  is a projection on  $W_i$  along  $\bigoplus_{j=1, j \neq i}^k W_j$ . Moreover,

$$\forall v \in V \left[ v = \sum_{i=1}^k E_i v \right],$$

or, equivalently,

$$I = \sum_{i=1}^k E_i.$$

Lastly,

$$E_i E_j = 0$$

whenever  $i \neq j$ . We summarize our observations and prove its converse in the following theorem.

**Theorem 7.15.**  
**Direct Sum**  
**Decomposition**

Let  $V$  be a vector space and let  $W_1, W_2, \dots, W_k \subseteq V$  be subspaces such that  $V = \bigoplus_{i=1}^k W_i$ . Then there exist linear operations  $E_1, E_2, \dots, E_k : V \rightarrow V$  such that the following hold.

- (a) Each  $E_i$  is a projection.
- (b)  $E_i E_j = 0$  whenever  $i \neq j$ .
- (c)  $I = \sum_{i=1}^k E_i$ .
- (d)  $\text{image}(E_i) = W_i$ .

Conversely, if  $E_1, E_2, \dots, E_k : V \rightarrow V$  are linear operators satisfying (a), (b), and (c), then

$$V = \bigoplus_{i=1}^k \text{image}(E_i).$$

*Proof.* We only have to prove the converse statement. By (c),

$$\forall v \in V \exists E_1 v \in \text{image}(E_1) \exists E_2 v \in \text{image}(E_2) \cdots \exists E_k v \in \text{image}(E_k) \left[ v = Iv = \sum_{i=1}^k E_i v \right].$$

This means

$$V = \text{image}(E_1) + \text{image}(E_2) + \cdots + \text{image}(E_k).$$

This sum is unique, since the representation  $v = \sum_{i=1}^k E_i v$  is the unique representation of  $v$  as a sum of vectors in  $\text{image}(E_1), \text{image}(E_2), \dots, \text{image}(E_k)$ . To verify this, suppose

$$v = \sum_{i=1}^k w_i$$

for some  $w_1 \in \text{image}(E_1), w_2 \in \text{image}(E_2), \dots, w_k \in \text{image}(E_k)$ . Then

$$E_i v = E_i \sum_{j=1}^k w_j = \sum_{j=1}^k E_i w_j = E_i w_i = w_i.$$

Thus  $\text{image}(E_1), \text{image}(E_2), \dots, \text{image}(E_k)$  are independent and

$$V = \bigoplus_{i=1}^k \text{image}(E_i).$$



## Invariant Direct Sum

**Remark 7.17.** We are primarily interested in direct sum decompositions  $V = \bigoplus_{i=1}^k W_i$  such that each subspace  $W_i \subseteq V$  is invariant under some linear operator  $T : V \rightarrow V$ . Given such decompositions,  $T$  induces a linear operator  $T_{W_i} : W_i \rightarrow W_i$  on each  $W_i$  by restriction. Recall that given  $v \in V$ , the representation

$$v = \sum_{i=1}^k w_i$$

as a sum of vectors from  $W_1, W_2, \dots, W_k$  is unique, provided that  $\bigoplus_{i=1}^k W_i$ . Then,

$$Tv = \sum_{i=1}^k T w_i = \sum_{i=1}^k T_{W_i} w_i.$$

We describe this situation as follows.

**Def'n. Direct Sum** of Linear Operators

Consider the case in Remark 7.17. We say  $T$  is the **direct sum** of linear operators  $T_{W_1}, T_{W_2}, \dots, T_{W_k}$ .

**Remark 7.18.** One should note that the direct sum of operators is different from the addition of linear operators, since each  $T_{W_i}$  has  $W_i$  as its domain and range. We also have a matrix analogue of this.

**Def'n. Direct Sum** of Matrices

Let  $A \in M_{n \times n}(\mathbb{F})$  and suppose

$$A = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}$$

for some square matrices  $A_1, A_2, \dots, A_k$  over  $\mathbb{F}$ . Then we call  $A$  the **direct sum** of  $A_1, A_2, \dots, A_k$ .

**Remark 7.19.** Most often, we shall describe each subspace  $W_i$  by means of the associated projection  $E_i$ . In other words, we need to phrase the invariance of  $W_i$  in terms of  $E_i$ .

**Proposition 7.16.**  
**A Subspace Is**  
 **$T$ -Invariant If and**  
**Only If  $T$  Commutes**  
**with the Associated**  
**Projection**

Let  $V$  be a finite-dimensional vector space and let  $T : V \rightarrow V$  be a linear operator. Let  $W_1, W_2, \dots, W_k$  be subspaces such that

$$V = \bigoplus_{i=1}^k W_i$$

and let  $E_i : V \rightarrow V$  be the associated projection for each  $i \in \{1, 2, \dots, k\}$ . Then each subspace  $W_i$  is invariant under  $T$  if and only if  $T$  commutes with each  $E_i$ .

*Proof.* For the reverse direction, suppose  $T$  commutes with each  $E_i$ . Then for any  $w_i \in W_i$ ,

$$Tw_i = TE_iw_i = E_iTw_i$$

so  $Tw_i \in \text{image}(E_i) = W_i$ , which exactly means that  $W_i$  is invariant under  $T$ . For the forward direction, suppose that each  $W_i$  is  $T$ -invariant. Then for any  $v \in V$ ,

$$\sum_{i=1}^k E_i v$$

and so

$$Tv = T \sum_{i=1}^k E_i v = \sum_{i=1}^k TE_i v.$$

Since each  $W_i$  is  $T$ -invariant, there exists  $w_i \in W_i$  such that  $TE_i v = E_i w_i$ . Moreover,

$$E_j TE_i v = \begin{cases} 0 & \text{if } i \neq j \\ E_j^2 w_j & \text{otherwise} \end{cases}$$

so

$$E_j Tv = \sum_{i=1}^k E_j TE_i v = E_j^2 w_j = E_j w_j = TE_j v,$$

which exactly means that  $T$  commutes with each  $E_i$ , as desired. ♠

**Remark 7.20.** We now proceed to describe diagonalizable linear operator  $T$  in terms of a direct sum decomposition of invariant subspaces by using projections that commute with  $T$ .



**Theorem 7.17.**

Let  $V$  be a vector space and let  $T : V \rightarrow V$  be diagonalizable. Let  $c_1, c_2, \dots, c_k \in \mathbb{F}$  be the distinct eigenvalues of  $T$ . Then there exists linear operators  $E_1, E_2, \dots, E_k : V \rightarrow V$  such that the following hold.

- (a)  $T = \sum_{i=1}^k c_i E_i$ .
- (b)  $I = \sum_{i=1}^k E_i$ .
- (c)  $E_i E_j = 0$  whenever  $i \neq j$ .
- (d)  $E_i^2 = E_i$ .
- (e)  $\text{image}(E_i)$  is the eigenspace corresponding to  $c_i$ .

Conversely, if there exist  $k$  distinct scalars  $c_1, c_2, \dots, c_k \in \mathbb{F}$  and  $k$  nonzero linear operators  $E_1, E_2, \dots, E_k : V \rightarrow V$  satisfying (a), (b), and (c), then  $T$  is diagonalizable,  $c_1, c_2, \dots, c_k$  are eigenvalues of  $T$ , and conditions (d) and (e) are satisfied as well.

*Proof.* Suppose that  $T$  is diagonalizable and  $c_1, c_2, \dots, c_k \in \mathbb{F}$  are  $k$  distinct eigenvalues of  $T$ . For each  $i \in \{1, 2, \dots, k\}$ , let  $W_i$  denote the eigenspace corresponding to  $c_i$  and let  $E_i : V \rightarrow V$  be the associated projection. Then the conditions (b), (c), (d), and (e) are satisfied by construction. To verify (a), notice that

$$\forall v \in V \left[ v = \sum_{i=1}^k E_i v \right]$$

so

$$\forall v \in V \left[ T v = T \sum_{i=1}^k E_i v = \sum_{i=1}^k T E_i v = \sum_{i=1}^k c_i E_i v \right].$$

But this exactly means  $T = \sum_{i=1}^k c_i E_i$ . To verify the converse statement, suppose that there exist  $k$  distinct scalars  $c_1, c_2, \dots, c_k$  and  $k$  distinct linear operators  $E_1, E_2, \dots, E_k : V \rightarrow V$  satisfying (a), (b), (c). Then

$$E_i = E_i I = E_i \sum_{j=1}^k E_j = E_i^2$$

so (d) is satisfied. To show that each  $c_i$  is an eigenvalue, notice that there exists  $E_i v \in \text{image}(E_i)$  such that

$$T E_i v = \sum_{j=1}^k c_j E_j E_i v = c_i E_i^2 v = c_i E_i v.$$

Notice that  $E_i$  is nonzero by assumption, so there must exist a nonzero element in  $W_i$ , the eigenspace corresponding to  $c_i$ . Furthermore, the above equation shows that  $\text{image}(E_i) \subseteq W_i$ . We also see that  $T$  is diagonalizable, since

$$\forall v \in V \left[ v = I v = \sum_{i=1}^k E_i v \right]$$

so  $\text{span} \left( \bigcup_{i=1}^k \text{image}(E_i) \right) = V$ . That is, eigenvectors of  $T$  span  $V$ . To verify that  $c_1, c_2, \dots, c_k$  are the only eigenvalues of  $T$ , suppose

$$T v = c v$$

for some  $c \in \mathbb{F}$  and  $v \in V$ . Then  $(T - cI)v = 0$  so

$$(T - cI)v = \left( \sum_{i=1}^k c_i E_i - c \sum_{i=1}^k E_i \right) v = \sum_{i=1}^k (c_i - c) E_i v = 0.$$

So  $(c_j - c)E_j v = 0$  for each  $j \in \{1, 2, \dots, k\}$ . If  $v \neq 0$ , then  $E_i v \neq 0$  for some  $i$ . Notice that this  $i$  is unique, since

$$T v = \sum_{i=1}^k c_i E_i v = c v = \sum_{i=1}^k c E_i v.$$

So in order for  $c_1, c_2, \dots, c_k$  to be distinct, there must be only one  $i$  such that  $E_i v \neq 0$ . This means  $c = c_i$  for some  $i \in \{1, 2, \dots, k\}$  whenever  $c$  is an eigenvalue of  $T$ . To verify that  $W_i \subseteq \text{image}(E_i)$ , let  $v \in W_i$ . Then

$$Tv = \sum_{j=1}^k c_j E_j v = c_i v = c_i \sum_{j=1}^k E_j v = \sum_{i=1}^k c_i E_j v.$$

So

$$\sum_{j=1}^k (c_j - c_i) E_j v = 0.$$

It follows that  $E_j v = 0$  whenever  $i \neq j$  so

$$v = Iv = \sum_{j=1}^k E_j v = E_i v \in \text{image}(E_i),$$

as desired. ♠

**Remark 7.21.** Theorem 7.17 shows that for a diagonalizable linear operator  $T$ , the scalars  $c_1, c_2, \dots, c_k \in \mathbb{F}$  and linear operators  $E_1, E_2, \dots, E_k : V \rightarrow V$  are uniquely determined by (a), (b), (c), the fact that each  $c_i$  is distinct, and the fact that each  $E_i \neq 0$ . One of the pleasant features of the decomposition

$$T = \sum_{i=1}^k E_i$$

is that, for any polynomial  $f \in \mathbb{F}[x]$ ,

$$f(T) = \sum_{i=1}^k f(c_i) E_i.$$

This can be verified by checking the result for each powers of  $x$ . This is analogous to the fact that, given a diagonal  $A \in M_{n \times n}(\mathbb{F})$ , then

$$[f(A)]_{ii} = f(A_{ii}).$$

**Remark 7.22.** Consider applying Lagrange interpolation to distinct scalars  $c_1, c_2, \dots, c_k \in \mathbb{F}$ . Define

$$p_j = \prod_{i=1, i \neq j}^k \frac{(x - c_i)}{(c_j - c_i)}$$

then we have  $p_j(c_i) = \delta_{ij}$ , which means

$$p_j(T) = \sum_{i=1}^k p_j(c_i) E_i = \sum_{i=1}^k \delta_{ij} E_i = E_j.$$

Since  $E_j = p_j(T)$  is a polynomial in  $T$ , it follows that  $E_i$  commutes not only with  $T$  but with polynomials in  $T$  as well. This enables us to give an alternative proof to Theorem 7.12.

**Theorem 7.12.**  
 **$T$  Is Diagonalizable If and Only If Its Minimal Polynomial Is a Product of Distinct Linear Factors**

*Let  $V$  be a finite-dimensional vector space and let  $T : V \rightarrow V$  be a linear operator. Then  $T$  is diagonalizable if and only if the minimal polynomial of  $T$  is of the form*

$$\prod_{i=1}^k (x - c_i).$$

*Proof.* For the forward direction, suppose  $T$  is diagonalizable. Then for any  $f \in \mathbb{F}[x]$ ,

$$f(T) = \sum_{i=1}^k f(c_i) E_i$$

where  $c_1, c_2, \dots, c_k \in \mathbb{F}$  are distinct eigenvalues of  $T$  and each  $E_i$  is the associated projection to the age space corresponding to  $c_i$ . It follows that  $f(c_i) = 0$  for each  $i \in \{1, 2, \dots, k\}$  provided that  $f(T) = 0$ , and in particular, the minimal polynomial is

$$p = \prod_{i=1}^k (x - c_i).$$

For the reverse direction, suppose

$$p = \prod_{i=1}^k (x - c_i)$$

for some distinct  $c_1, c_2, \dots, c_k \in \mathbb{F}$  is the minimal polynomial of  $T$ . We form the Lagrange polynomial

$$p_j = \prod_{i=1, i \neq j}^k \frac{x - c_i}{c_j - c_i}$$

for each  $j \in \{1, 2, \dots, k\}$ . Recall that the Lagrange polynomials have the properties that  $p_j(c_i) = \delta_{ij}$  and

$$g = \sum_{j=1}^k g(c_j) p_j$$

provided that  $\deg(g) \leq k - 1$ . Then

$$1 = \sum_{i=1}^k p_i \quad x = \sum_{j=1}^k c_j p_j.$$

Notice that we may not define  $x$  as  $\sum_{j=1}^k c_j p_j$  if  $k = 1$ . However, if  $k = 1$ , then  $p = (x - c_1)$  and the proof is trivial. So we may safely assume  $k \geq 2$ . Now let  $E_i = p_i(T)$  then

$$I = \sum_{i=1}^k E_i \quad T = \sum_{i=1}^k c_i E_i.$$

Observe that  $p \mid p_i p_j$  whenever  $i \neq j$ , since  $c_i c_j$  has every factor that  $p$  has. Thus

$$(p_i p_j) T = E_i E_j = 0.$$

Furthermore, observe that  $E_i \neq 0$  for each  $i \in \{1, 2, \dots, k\}$ , since  $\deg(p_i) < \deg(p)$ . Notice that we just proved the necessary conditions for the converse statement of Theorem 7.12 to hold. That is,  $T$  is diagonalizable. ♠

## Primary Decomposition Theorem

**Remark 7.23.** When we try to study a linear operator  $T : V \rightarrow V$  on a finite-dimensional vector space  $V$  in terms of its characteristic values, we are confronted with two particular problems.

- (a) The minimal polynomial of  $T$  may not decompose into a product of linear factors. This is certainly a deficiency in the field  $\mathbb{F}$ , since we cannot guarantee algebraic closure.
- (b) Even if we find the characteristic polynomial to be decomposed into a product of linear factors, there is no guarantee that the direct sum of the corresponding eigenspaces is equal to  $V$ .

However, one can verify that a weaker version of (b) always holds. Namely, given a linear operator  $T$  with the characteristic polynomial

$$p = \prod_{i=1}^k (x - c_i)^{r_i}$$

for some  $c_1, c_2, \dots, c_k \in \mathbb{F}$  and  $r_1, r_2, \dots, r_k \in \mathbb{N}$ , it is always the case that

$$V = \bigoplus_{i=1}^k \ker((T - c_i I)^{r_i}).$$

In fact, we are going to prove more general version of this idea.

**Theorem 7.18.**  
**Primary**  
**Decomposition**  
**Theorem**

Let  $V$  be a finite-dimensional vector space and let  $T : V \rightarrow V$  be a linear operator. Suppose

$$p = \prod_{i=1}^k p_i^{r_i}$$

is the minimal polynomial of  $T$ , where  $p_1, p_2, \dots, p_k$  are distinct irreducible monic polynomials and  $r_i \in \mathbb{N}$  for each  $i$ . Let

$$W_i = \ker(p_i(T)^{r_i})$$

for each  $i$ . Then the following hold.

- (a)  $V = \bigoplus_{i=1}^k W_i$ .
- (b) Each  $W_i$  is  $T$ -invariant.
- (c) If  $T_i$  is the induced operator on  $W_i$  by  $T$ , then the minimal polynomial for  $T_i$  is  $p_i^{r_i}$ .

*Proof.* For each  $i \in \{1, 2, \dots, k\}$ , define

$$f_i = \frac{p}{p_i^{r_i}} = \prod_{j=1, j \neq i}^k p_j^{r_j}$$

then  $f_1, f_2, \dots, f_k$  are coprime by construction. So there exist  $g_1, g_2, \dots, g_k \in \mathbb{F}[x]$  such that

$$\sum_{i=1}^k f_i g_i = 1$$

by (b) of Proposition 5.11. Define  $E_i = f_i(T)g_i(T)$  for each  $i$ . Notice that  $p \mid h_i h_j$  whenever  $i \neq j$ , so  $E_i E_j = 0$  whenever  $i \neq j$  and  $\sum_{i=1}^k E_i = I$ . It follows that  $E_i = E_i I = E_i \sum_{j=1}^k E_j = E_i^2$ , so each  $E_i$  is a projection. Now the claim is that  $\text{image}(E_i) = W_i = \ker(p_i(T)^{r_i})$ . To verify this, observe that if  $v \in \text{image}(E_i)$ , then  $v = E_i v = f_i(T)g_i(T)v$  and

$$p_i(T)^{r_i} v = p_i(T)^{r_i} f_i(T)g_i(T)v = p(T)g_i(T)v = 0.$$

Moreover, notice that  $p_i(T)^{r_i} \nmid E_j$  whenever  $i \neq j$ . It follows that if  $v \in \ker(p_i(T)^{r_i})$ , then  $E_j v = 0$  for each  $j \neq i$ . So

$$v = Iv = \sum_{j=1}^k E_j v = E_i v.$$

Then  $\bigoplus_{i=1}^k W_i = V$  by Theorem 7.15. Furthermore, notice that each  $W_i$  is  $T$ -invariant by definition, since if  $p_i(T)^{r_i} v = 0$ , then

$$p_i(T)^{r_i} T v = T p_i(T)^{r_i} v = 0,$$

since  $T$  commutes with any polynomial in  $T$ . So define  $T_i$  be the induced operator on  $W_i$  by  $T$ . Clearly  $p_i(T)^{r_i} = 0$ , since  $p_i^{r_i}$  annihilates  $T$  on  $W_i$  by definition. Moreover, suppose  $q_i$  is an annihilating polynomial of  $T_i$ . Then  $q_i f_i$  annihilates  $T$ , so  $p \mid q_i f_i$ . But  $p = p_i^{r_i} f_i$ , so

$$p_i^{r_i} f_i \mid q_i f_i$$

which means  $p_i^{r_i} \mid q_i$  as well. Thus  $p_i^{r_i} = q_i$  is the minimal polynomial for  $T_i$ , as desired. ♠

**Corollary 7.18.1.**

If  $E_1, E_2, \dots, E_k$  are projections associated with the primary decomposition of  $T$ , then each  $E_i$  is a projection in  $T$ , and any linear operator  $U$  commutes with  $T$  commutes with  $E_i$ . In particular, the associated subspace  $W_i = \text{image}(E_i)$  is  $U$ -invariant.

**Def'n. Diagonalizable Part** of a Linear Operator

Consider analyzing a special case of the Theorem 7.18, when each factor  $p_i$  of the minimal polynomial is linear (i.e. each  $p_i = x - c_i$ ). Define

$$D = \sum_{i=1}^k c_i E_i : V \rightarrow V$$

then  $D$  is a diagonalizable operator by Theorem 7.15, which we call the *diagonalizable part* of  $T$ .

**Remark 7.24.** Let  $T$  be a linear operator with the characteristic polynomial

$$\prod_{i=1}^k (x - c_i)^{r_i}$$

and let  $D$  be the diagonalizable part of  $T$ . Further define

$$N = T - D = \sum_{i=1}^k (T - c_i I) E_i.$$

Clearly

$$N^r = \sum_{i=1}^k (T - c_i I)^r E_i,$$

since each  $E_i$  is a projection. Notice that

$$(T - c_i I)^r E_i = 0$$

whenever  $r \geq r_i$ . It follows that

$$N^r = \sum_{i=1}^k (T - c_i I)^{r_i} E_i = 0$$

provided that  $r \geq r_i$  for all  $i \in \{1, 2, \dots, k\}$ . This motivates the following definition.

**Def'n. Nilpotent** Linear Operator

Let  $V$  be a vector space and let  $N : V \rightarrow V$  be a linear operator. We say  $N$  is *nilpotent* if there exists  $r \in \mathbb{N}$  such that  $N^r = 0$ .

**Theorem 7.19.**  
**Nilpotent**  
**Decomposition**

*Let  $V$  be a finite-dimensional vector space and let  $T : V \rightarrow V$  be a linear operator. If the minimal polynomial of  $T$  decomposes into a product of linear polynomials, then there exist diagonalizable  $D : V \rightarrow V$  and  $N : V \rightarrow V$  such that the following holds.*

$$(a) \quad T = D + N.$$

$$(b) \quad DN = ND.$$

*Moreover,  $D$  and  $N$  are polynomials in  $T$  uniquely determined by (a) and (b).*

*Proof.* We have already shown the existence of  $D, N : V \rightarrow V$  satisfying the listed conditions in Remark 7.24. Namely, take diagonalizable part of  $T$  to be  $D$  and define  $N = T - D$ . To verify the uniqueness, suppose that there exist diagonalizable  $D' : V \rightarrow V$  and nilpotent  $N' : V \rightarrow V$  satisfying the listed properties. Then

$$N + D = N' + D'$$

so

$$D - D' = N' - N.$$

We see that both  $D$  and  $D'$  are diagonalizable and  $DD' = D'D$ , so  $D - D'$  is diagonalizable. Moreover, since both  $N'$  and  $N$  are nilpotent, it follows that  $N' - N$  is nilpotent. This can be verified easily by using

binomial theorem, since  $N'$  and  $N$  commute. It follows that  $D - D'$  is nilpotent, so the minimal polynomial for  $D - D'$  is  $x^r$  for some  $r \in \mathbb{N}$ . But  $D - D'$  is diagonalizable, so  $r = 1$  and  $x$  is its minimal polynomial. Thus  $D - D' = 0$ , and we have  $D = D'$  and  $N = N'$ , as desired. ♠

**Corollary 7.19.1.**

*Let  $V$  be a finite-dimensional vector space over an algebraically closed field  $\mathbb{F}$ . Then every operator  $T : V \rightarrow V$  can be uniquely written as a sum of diagonalizable  $D : V \rightarrow V$  and nilpotent  $N : V \rightarrow V$ , where both  $D$  and  $N$  are polynomials in  $T$ .*

# 8.

## The Rational and Jordan Form

- 
- 8.1 Cyclic Subspaces and Annihilators
  - 8.2 Cyclic Decomposition and the Rational Form
  - 8.3 Jordan Form
-

**Remark 8.1.** For simplicity, we shall adapt the following notation for this chapter. Unless otherwise specified, let  $V$  denote a finite-dimensional vector space over a field  $\mathbb{F}$  and let  $T : V \rightarrow V$  denote a linear operator on  $V$ .

## Cyclic Subspaces and Annihilators

**Remark 8.2.** Let  $v \in V$  and consider finding the smallest  $T$ -invariant subspace  $W \subseteq V$  that contains  $v$ . Clearly,  $Tv \in W$ . Not only that, for any  $f \in \mathbb{F}[x]$ ,  $f(T)v \in W$ , since

$$\{f(T)v : f \in \mathbb{F}[x]\}$$

for any  $v \in V$  is a subspace of  $V$ , we conclude that  $W = \{f(T)v : f \in \mathbb{F}[x]\}$  is the smallest  $T$ -invariant subspace of  $V$ . This motivates the following definition.

**Def'n.  $T$ -Cyclic Subspace** Generated by a Vector

Let  $v \in V$ . We say the subspace

$$Z(v; T) = \{f(T)v : f \in \mathbb{F}[x]\} \subseteq V$$

the  *$T$ -cyclic subspace* generated by  $v$ .

**Remark 8.3.** Sometimes there exist  $v \in V$  such that  $Z(v; T) = V$ . Although this need not be the case for every linear operator  $T : V \rightarrow V$ , it is certainly important to give a name for it.

**Def'n. Cyclic Vector** of a Linear Operator

Let  $v \in V$ . We say  $v$  is a *cyclic vector* of  $T$  if  $Z(v; T) = V$ .

**Remark 8.4.** An alternative way to define  $Z(v; T)$  is that,

$$Z(v; T) = \text{span} \left\{ T^k v : k \in \mathbb{N} \cup \{0\} \right\}.$$

Thus  $v$  is a cyclic vector of  $T$  whenever  $V = \text{span} \{T^k v : k \in \mathbb{N} \cup \{0\}\}$ .

**Example 8.5.** Consider the following examples:

- (a)  $Z(0; T) = \{0\}$ .
- (b)  $\dim(Z(v; T)) = 1$  if and only if  $v$  is an eigenvector of  $T$ .
- (c)  $\dim(Z(v; I)) = 1$  for any  $v \in V$ . That is, the identity operator of  $V$  does not have a cyclic vector if  $\dim(V) > 1$ .
- (d) Let  $\beta = \{e_1, e_2\}$ . Suppose a linear operator  $T : \mathbb{F}^2 \rightarrow \mathbb{F}^2$  satisfies

$$[T]_{\beta} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Then clearly  $v = (1, 0) \in \mathbb{F}^2$  is a cyclic vector of  $T$ , since

$$\text{span} \{T^0 v, T^1 v, \dots\} = \text{span} \{(1, 0), (0, 1), \dots\} = \mathbb{F}^2.$$



**Remark 8.6.** For any  $v \in V$ , we shall be interested in linear relations

$$\sum_{i=0}^k c_i T^i v = 0$$

between  $T^0 v, T^1 v, \dots, T^k v$ . That is, we are interested in the polynomials

$$f = \sum_{i=0}^k c_i x^i \in \mathbb{F}[x]$$

such that  $f(T)v$ . Recall the following definitions.

**Recall.  $T$ -Annihilator of a Vector**

Let  $v \in V$ . We call the polynomial ideal

$$M(v; T) = \{f \in \mathbb{F}[x] : f(T)v = 0\} \subseteq \mathbb{F}[x]$$

the  $T$ -*annihilator* of  $v$ . Moreover, the unique monic generator of  $M(v; T)$ , denoted as  $m(v; T)$ , is also called the  $T$ -*annihilator* of  $v$ .

**Remark 8.7.** Let  $p \in \mathbb{F}[x]$  be the minimal polynomial for  $T$ . Then  $p(T) = 0$  so  $p(T)v = 0$ . It follows that  $m(v; T) \mid p$ . One should also note that  $\deg(m(v; T)) > 0$  whenever  $v \neq 0$ .

**Proposition 8.1.**

*Let  $v \in V$  be nonzero and let  $p_v = m(v; T)$ . Then the following hold.*

- (a)  $\deg(p_v) = \dim(Z(v; T))$ .
- (b)  $\{v, Tv, \dots, T^{k-1}v\}$  is a basis for  $Z(v; T)$  provided that  $\dim(Z(v; T)) = k$ .
- (c) If  $U : Z(v; T) \rightarrow Z(v; T)$  is the linear operator on  $Z(v; T)$  induced by  $T$ , then the minimal polynomial for  $U$  is  $p_v$ .

*Proof.* We verify (b) first, which verifies (a) as well. Let  $z \in Z(v; T)$ . Then  $z = f(T)v$  for some  $f \in \mathbb{F}[x]$ . Notice that

$$f = dp_v + r$$

for some  $d, r \in \mathbb{F}[x]$  satisfying  $r = 0$  or  $\deg(r) < \deg(p_v)$  by the division algorithm. That is,

$$r = \sum_{i=0}^{k-1} c_i x^i$$

for some  $c_0, c_1, \dots, c_{k-1} \in \mathbb{F}$ , provided that  $\deg(p_v) > k$ . It follows that  $f(T)v \in \text{span}\{v, Tv, \dots, T^{k-1}v\}$ , since

$$f(T)v = (dp_v)(T)v + r(T)v = r(T)v.$$

Notice that  $\{v, Tv, \dots, T^{k-1}v\}$  is linearly independent by the minimality of the unique monic generator  $p_v = m(v; T)$  of  $M(v; T)$ . This verifies (b) and, hence, (a). To verify (c), let  $z \in Z(v; T)$ . Then  $z = f(T)v$  for some  $f \in \mathbb{F}[x]$ . Moreover,  $p_v(U)z = p_v(T)z$ , since  $U$  is the restriction operator on  $Z(v; T)$  induced by  $T$ . Thus

$$p_v(U)z = p_v(T)z = p_v(T)f(T)v = f(T)p_v(T)v = 0,$$

as desired. ♠

**Def'n. Cyclic Basis**

Notice that (b) of Theorem 8.1 guarantees that, given a cyclic vector  $v \in V$  of  $T$ ,

$$\{v, Tv, \dots, T^{n-1}v\}$$

is a basis for  $V$ , provided that  $\dim(V) = n$ . We call this a *cyclic basis* for  $V$ .

**Remark 8.8.** A particular consequence of Theorem 8.1 is as follows. If  $v \in V$  is a cyclic vector of  $T$ , then

$$\deg(p_v) = \dim(Z(v; T)) = \dim(V).$$

Since  $p_v$  divides the characteristic polynomial  $p$  of  $T$ , and

$$\deg(p) \leq \dim(V),$$

we have  $p_v = p$ .

**Remark 8.9.** Our plan is to study general linear operator by linear operators which have a cyclic vector. So let  $W$  be a  $k$ -dimensional vector space and consider a linear operator  $U : W \rightarrow W$  which has a cyclic vector  $w \in W$ . Then

$$\beta = \{T^i w : i \in \{0, 1, \dots, n-1\}\}$$

is a basis for  $W$  by Theorem 8.1. For convenience, let  $w_i = T^i w$ . Then the action of  $U$  on the ordered basis  $\beta$  is

$$Uw_i = w_{i+1}$$

for all  $i < k-1$ , and

$$Uw_{k-1} = -\sum_{i=0}^{k-1} c_i w_i$$

provided that  $p_v = x^k + \sum_{i=0}^{k-1} c_i x^i \in \mathbb{F}[x]$ . This is because

$$p_v(U)w = U^k w + \sum_{i=0}^{k-1} c_i U^i w = 0.$$

Thus the matrix representation of  $U$  in  $\beta$  is

$$[U]_\beta = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{k-1} \end{bmatrix}.$$

This motivates the following definition.

**Def'n. Companion Matrix of a Monic Polynomial**

Let  $p = \sum_{i=0}^k c_i x^i \in \mathbb{F}[x]$  be monic. We define the *companion matrix* of  $p$  as

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{k-1} \end{bmatrix}.$$

**Theorem 8.2.**  
 **$U$  Has a Cyclic Vector**  
**If and Only If There**  
**Exists  $\beta$  Such That**  
 **$[U]_\beta$  Is the**  
**Companion Matrix of**  
**the Minimal**  
**Polynomial**

Let  $W$  be a finite-dimensional vector space and let  $U : W \rightarrow W$  be a linear operator. Then  $U$  has a cyclic vector if and only if there exists an ordered basis  $\beta$  for  $W$  such that  $[U]_\beta$  is the companion matrix of the minimal polynomial.

*Proof.* Notice that the forward direction is supplied by Remark 8.9. To prove the reverse direction, suppose that there exists an ordered basis  $\beta = \{w_1, w_2, \dots, w_n\}$  for  $W$  such that

$$[U]_\beta = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{k-1} \end{bmatrix}$$

where  $p = \sum_{i=0}^k c_i x^i$  is the minimal polynomial for  $U$ . Then it is clear that  $w_1 \in \beta$  is a cyclic vector of  $U$ . ♠

**Corollary 8.2.1.**

If  $A \in M_{n \times n}(\mathbb{F})$  is the companion matrix of a monic  $p \in \mathbb{F}[x]$ , then  $p$  is both the minimal and the characteristic polynomial of  $A$ .

*Proof.* By the isomorphism between  $M_{n \times n}(\mathbb{F})$  and  $\mathcal{L}(\mathbb{F}^n)$ , there exists a unique linear operator  $T : \mathbb{F}^n \rightarrow \mathbb{F}^n$  such that

$$[T]_\beta = A$$

where  $\beta = \{e_1, e_2, \dots, e_n\}$  is the standard ordered basis for  $\mathbb{F}^n$ . Then clearly  $e_1$  is a cyclic vector of  $T$ , since  $T^k e_1 = e_{k+1}$  so  $\{e_1, Te_1, \dots, T^{n-1} e_1\}$  is a basis for  $\mathbb{F}^n$ . Moreover,  $p$  is the  $T$ -annihilator of  $e_1$ , since

$$p(T)e_1 = 0$$

by definition, and, since  $\{e_1, Te_1, \dots, T^{n-1} e_1\}$  is a basis for  $\mathbb{F}^n$ , any  $f \in \mathbb{F}[x]$  such that

$$f(T)e_1 = 0$$

satisfies  $\deg(f) \geq n$ . But  $\deg(p) = n$  and  $p$  is monic, so  $p$  must be the  $T$ -annihilator of  $e_1$ . Furthermore,  $Z(e_1; T) = V$ , so  $T$  itself is the linear operator induced on  $Z(e_1; T)$  by  $T$ . So the minimal polynomial for  $T$  is  $p$  by Theorem 8.1. Thus by the Cayley-Hamilton theorem,  $p$  is also the characteristic polynomial of  $T$ , as required. ♠

**Remark 8.10.** Let  $v \in V$ . Then the linear operator  $U : Z(v; T) \rightarrow Z(v; T)$  induced by  $T$  on  $Z(v; T)$  has a cyclic vector, namely  $v$ . That is, there exists an ordered basis  $\beta$  for  $Z(v; T)$  such that  $[U]_\beta$  is the companion matrix of  $p_v$ , the  $T$ -annihilator of  $v$ .

**Example 8.11.** Suppose  $\dim(V) = n$  and let  $N : V \rightarrow V$  be nilpotent, where  $N^{n-1} \neq 0$ . Further let  $v \in V$  be such that  $N^{n-1}v \neq 0$ . Prove that  $v$  is a cyclic vector of  $N$ .

*Proof.* For the sake of contradiction, suppose there exists nonzero  $(c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}^n$  be such that

$$\sum_{i=0}^{n-1} c_i N^i v = 0.$$

This is a contradiction, since

$$N^{n-1} \sum_{i=0}^{n-1} c_i N^i v = c_0 N^{n-1} v \neq 0.$$

Thus  $\{v, Nv, \dots, N^{n-1}v\}$  is linearly independent, which means  $v$  is a cyclic vector of  $N$ , as desired. ♠

**Example 8.12.** Suppose that  $\dim(V) = n$  and that  $T$  is diagonalizable.

- (a) Prove that if  $T$  has a cyclic vector, then  $T$  has  $n$  distinct eigenvalues.
- (b) Prove that if  $T$  has  $n$  distinct eigenvalues and if  $\{v_1, v_2, \dots, v_n\}$  is an eigenbasis for  $V$ , then

$$v = \sum_{i=1}^n v_i \in V$$

is a cyclic vector of  $v$ .

*Proof.* To prove (a), let  $v \in V$  be a cyclic vector of  $T$ . Then the minimal polynomial  $p \in \mathbb{F}[x]$  of  $T$  is of the form

$$p = \prod_{i=1}^k (x - c_i)$$

for some  $k \leq n$  by Theorem 2.14. Moreover,  $p$  is the characteristic polynomial by Remark 8.8, so  $k = n$  and  $T$  has  $n$  distinct eigenvalues. To verify (b), let  $c_1, c_2, \dots, c_n \in \mathbb{F}$  be the eigenvalues corresponding to  $v_1, v_2, \dots, v_n$ . Then

$$T^k v = \sum_{i=1}^n c_i^k v_i.$$

Now the claim is that  $\{v, Tv, \dots, T^{n-1}v\}$  is linearly independent. To verify this, suppose

$$\sum_{p=0}^{n-1} a_p T^p v = 0$$

for some nonzero  $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}^n$  for the sake of contradiction. Then

$$\sum_{p=0}^{n-1} a_p \sum_{i=1}^n c_i^p v_i = \sum_{p=0}^{n-1} \sum_{i=1}^n a_p c_i^p v_i = \sum_{i=1}^n \sum_{p=0}^{n-1} a_p c_i^p v_i = 0.$$

Since  $v_1, v_2, \dots, v_n$  are linearly independent, it must be the case that

$$\sum_{p=0}^{n-1} a_p c_i^p = 0$$

for all  $i \in \{1, 2, \dots, n\}$ . That is, we have a nonzero solution to the system

$$\begin{bmatrix} 1 & c_1 & c_1^2 & \cdots & c_1^{n-1} \\ 1 & c_2 & c_2^2 & \cdots & c_2^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & c_n & c_n^2 & \cdots & c_n^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

However, the rows are linearly independent, since  $c_1, c_2, \dots, c_n$  are distinct. Thus the solution set to the system is  $\{0\}$ , which is a contradiction. ♠

**Example 8.13.** Suppose that  $T$  has a cyclic vector. Prove that if  $U : V \rightarrow V$  commutes with  $T$ , then  $U$  is a polynomial in  $T$ .

*Proof.* Let  $v \in V$  be a cyclic vector of  $T$ . Then by Theorem 8.1,  $\{v, Tv, \dots, T^{n-1}v\}$  is a basis for  $V$ , where  $n = \dim(V)$ . So there exists  $f \in \mathbb{F}[x]$  with  $\deg(f) \leq n-1$  such that

$$Uv = f(T)v,$$

since  $Uv \in V$ . Moreover, for any  $T^k \in \{T^1, T^2, \dots, T^{n-1}\}$ ,

$$UT^k v = T^k Uv = T^k f(T)v = f(T)T^k v.$$

Since  $\{v, Tv, \dots, T^{n-1}v\}$  is a basis for  $V$ , it follows that

$$U = f(T),$$

as desired. ♠

## Cyclic Decomposition and the Rational Form

**Remark 8.14.** The primary purpose of this section is to prove that if  $T$  is any linear operator on  $V$ , then there exist  $v_1, v_2, \dots, v_r \in V$  such that

$$V = \bigoplus_{i=1}^r Z(v_i; T).$$

In other words, we desire to prove that  $V$  is a direct sum of  $T$ -cyclic subspaces, which will show that  $T$  is the direct sum of a finite number of linear operators, each of which has a cyclic vector. The cyclic decomposition theorem is deeply related to the following question: which  $T$ -invariant subspace  $W \subseteq V$  has the property that there exists a  $T$ -invariant  $W' \subseteq V$  such that

$$V = W \oplus W'.$$

### Def'n. Complementary Subspace

Let  $W \subseteq V$  be a subspace. We say  $W' \subseteq V$  is a **complementary subspace** of  $W$  if  $V = W \oplus W'$ .

**Remark 8.15.** Suppose that  $V = W \oplus W'$  for some  $T$ -invariant  $W, W' \subseteq V$  and see what we can discover about  $W$ . Notice that each  $v \in V$  is of the form

$$v = w + w'$$

for some  $w \in W$  and  $w' \in W'$ . If  $f \in \mathbb{F}[x]$ , then

$$f(T)v = f(T)w + f(T)w'.$$

Since  $W$  and  $W'$  are  $T$ -invariant subspaces, it follows that  $f(T)v \in W$  if and only if  $f(T)w' = 0$ . Equivalently,  $f(T)v \in W$  if and only if  $f(T)v = f(T)w$ . This motivates the following definition.

### Def'n. $T$ -Admissible Subspace

Let  $W \subseteq V$  be a  $T$ -invariant subspace. We say  $W$  is  **$T$ -admissible** if there exists  $w \in W$  such that  $f(T)v = f(T)w$  whenever  $v \in V$  is such that  $f(T)v \in W$ .

**Remark 8.16.** By Remark 8.15, if  $W$  is a  $T$ -invariant and has a complementary subspace, then  $W$  is  $T$ -admissible. One of the consequences of the cyclic decomposition theorem is the converse: the admissibility characterizes those  $T$ -invariant subspaces with  $T$ -invariant complements.

**Remark 8.17.** Let us indicate how the admissibility is involved in the attempt to obtain a decomposition

$$V = \bigoplus_{i=1}^r Z(v_i; T).$$

One basic method is to select  $v_1, v_2, \dots, v_r \in V$  inductively. Suppose that we have selected  $v_1, v_2, \dots, v_j \in V$  and

$$W = \bigoplus_{i=1}^j Z(v_i; T) \subsetneq V$$

is proper. We desire to find  $v_{j+1} \in V$  such that

$$W \cap Z(v_{j+1}; T) = \{0\},$$

because then  $\dim(W \cap Z(v_{j+1}; T)) > \dim(W)$ , allowing us to come at least one dimension nearer to exhausting  $V$ . But why such  $v_{j+1} \in V$  always exist? Rather than answering this question directly, we observe the following: if  $v_1, v_2, \dots, v_j \in V$  are chosen such that  $W = \bigoplus_{i=1}^j Z(v_i; T)$  is  $T$ -admissible, then it is much easier to find a suitable  $v_{j+1} \in V$ . To explain this, let us take one step back and suppose  $W \subsetneq V$  is a proper  $T$ -invariant subspace, and consider finding a nonzero  $v \in V$  such that

$$W \cap Z(v; T) = \{0\}.$$

Let  $u \in V \setminus W$  and let  $f = s(u; W)$ , the unique monic generator of the  $T$ -conductor of  $u$  into  $W$ ,  $S(u; W)$ . Clearly  $f(T)u \in W$ . Now, if  $W$  is  $T$ -admissible, then there exists  $w \in W$  such that

$$f(T)u = f(T)w.$$

Let  $v = u - w$  and let  $g = \mathbb{F}[x]$ . Since  $u - v = w \in W$ ,  $g(T)u \in W$  if and only if  $g(T)v \in W$ . That is,

$$S(u; W) = S(v; W)$$

and  $s(u; W) = f = s(v; W)$ , the  $T$ -conductor of  $v$  into  $W$ . But

$$f(T)v = f(T)(u - w) = f(T)u - f(T)w = 0,$$

which means  $g(T)v = 0$  whenever  $g \in S(v; W)$ . But since any element of  $Z(v; T)$  is of the form  $g(T)v$  for some  $g \in \mathbb{F}[x]$ , it follows that

$$W \cap Z(v; T) = \{0\}$$

which is what we desired.

**Theorem 8.3.**  
**Cyclic Decomposition**  
**Theorem**

Let  $W_0 \subsetneq V$  be a proper  $T$ -invariant subspace. Then there exist nonzero  $v_1, v_2, \dots, v_r \in V$  with respective  $T$ -annihilators  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  that satisfies the following:

- (a)  $V = W_0 \oplus (\bigoplus_{i=1}^r Z(v_i; T))$ .
- (b) For all  $i \in \{2, 3, \dots, r\}$ ,  $p_i \nmid p_{i-1}$ .

Moreover, the integer  $r \in \mathbb{N}$  and the  $T$ -annihilators  $p_1, p_2, \dots, p_r$  are uniquely determined by (a), (b), and the fact that  $v_1, v_2, \dots, v_r$  are nonzero.

**Lemma 8.3.1.**

There exist nonzero  $u_1, u_2, \dots, u_r \in V$  such that

- (a)  $V = W_0 + \sum_{i=1}^r Z(u_i; T)$  and
- (b) if we define  $W_k = W_0 + \sum_{i=1}^k Z(u_i; T)$  for each  $k \in \{1, 2, \dots, r\}$ , then the  $T$ -conductor  $p_k = s(u_i; W_{k-1})$  has maximum degree among all  $T$ -conductors into the subspace  $W_{k-1}$ . That is,

$$\deg(p_k) = \max_{v \in V} (\deg(s(v; W_{k-1}))).$$

*Proof.* Clearly,  $W_k$  is a proper  $T$ -invariant subspace for all  $k \in \{0, 1, \dots, r-1\}$ . So,

$$0 < \max_{v \in V} (\deg(s(v; W_{k-1}))) \leq \dim(V)$$

for all  $k \in \{1, 2, \dots, r\}$ , and we can certainly choose  $v_k \in V$  such that

$$\deg(s(v_k; W_{k-1})) = \max_{v \in V} (\deg(s(v; W_{k-1}))).$$

But  $0 < \deg(s(v_k; W_{k-1}))$  means  $v_k \notin W_{k-1}$ , and so

$$\dim(W_{k-1} + Z(v_k; T)) > \dim(W_{k-1}).$$

Thus by repeating the above process at most  $r$  times, we have the desired result by construction. ♠

**Lemma 8.3.2.**

Suppose  $u_1, u_2, \dots, u_k \in V$  are nonzero vectors satisfying (a) and (b) of Lemma 8.3.1. Fix  $k \in \{1, 2, \dots, r\}$ . Let  $u \in V$  be arbitrary and let  $f = s(v_k; W_{k-1})$ . If

$$f(T)u = u_0 + \sum_{i=1}^{k-1} g_i(T)u_i$$

for some  $g_1, g_2, \dots, g_{k-1} \in \mathbb{F}[x]$  and  $u_0 \in W_0$ , then

- (a)  $f \mid g_i$  for all  $i \in \{1, 2, \dots, k-1\}$  and
- (b)  $u_0 = f(T)w_0$  for some  $w_0 \in W_0$ .

*Proof.* When  $k = 1$ , notice that  $f(T)u = u_0$ , so we only have to verify

$$f(T)u = u_0 = f(T)w_0$$

for some  $w_0 \in W_0$ , which is true since  $W_0$  is  $T$ -admissible. For each  $k \in \{2, 3, \dots, r\}$  and  $i \in \{1, 2, \dots, k-1\}$ , write

$$g_i = fh_i + r_i$$

for some  $h_i, r_i \in \mathbb{F}[x]$  satisfying  $r_i = 0$  or  $\deg(r_i) < \deg(f)$  by the division algorithm. For the sake of contradiction, suppose that there exists  $i \in \{1, 2, \dots, k-1\}$  such that  $r_i \neq 0$ , and let  $j \in \{1, 2, \dots, k-1\}$  be the greatest such index,

$$j = \max \{i \in \{1, 2, \dots, k-1\} : r_i \neq 0\}.$$

Let

$$w = u - \sum_{i=1}^{k-1} h_i(T)u_i \in V,$$

then clearly  $w - u = -\sum_{i=1}^{k-1} h_i(T)u_i \in W_{k-1}$ . Recall from Remark 8.17 that, this means

$$s(w; W_{k-1}) = s(u; W_{k-1}) = f.$$

Moreover, observe that

$$\begin{aligned} f(T)w &= f(T)u - \sum_{i=1}^{k-1} f(T)h_i(T)u_i \\ &= u_0 + \sum_{i=1}^{k-1} (fh_i + r_i)(T)u_i - \sum_{i=1}^{k-1} (fh_i)(T)u_i = u_0 + \sum_{i=1}^{k-1} r_i(T)u_i. \end{aligned}$$

Since  $r_{j+1}, r_{j+2}, \dots, r_{k-1} = 0$ ,

$$f(T)w = u_0 + \sum_{i=1}^j r_i(T)u_i,$$

where  $\deg(r_j) < \deg(f)$ . Let  $p = s(w; W_{j-1})$ . Since  $W_{k-1} \supseteq W_{j-1}$ , it follows that  $f = s(w; W_{k-1})$  divides  $p$ . That is,

$$p = fg$$

for some  $g \in \mathbb{F}[x]$ . Then

$$p(T)w = g(T)f(T)w = g(T)u_0 + \sum_{i=1}^{j-1} g(T)r_i(T)u_i + g(T)r_j(T)u_j.$$

But  $g(T)u_0 + \sum_{i=1}^{j-1} g(T)r_i(T)u_i \in W_{j-1}$  and  $p(T)w \in W_{j-1}$  by definition, so  $g(T)r_j(T)u_j \in W_{j-1}$  as well. This means  $p_j \mid gr_j$  so  $\deg(gr_j) \geq \deg(s(u_j; W_{j-1}))$ . Furthermore,  $\deg(s(u_j; W_{j-1})) \deg(s(w; W_{j-1}))$  by the maximality of  $s(u_j; W_{j-1})$  that (b) of Lemma 8.3.1 guarantees. But  $s(u_j; W_{j-1}) = p_j$  and  $s(w; W_{j-1}) = p = fg$ , so

$$\deg(gr_j) \leq \deg(p_j) \leq \deg(p) = \deg(fg).$$

But this means  $\deg(r_j) \geq \deg(f)$ , which is a contradiction. Thus  $f$  divides  $g_i$  for each  $i \in \{1, 2, \dots, r-q\}$ . It follows that

$$u_0 = u_0 + \sum_{i=1}^{k-1} r_i(T)u_i = f(T)w,$$

so by taking  $w_0 = w \in W_0$ , we have  $u_0 = f(T)w_0$  for some  $w_0 \in W_0$ , as desired. ♠

### Proof of Theorem 8.3 Begins Here

*Proof of Theorem 8.3.* We first verify the existence part. Let  $u_1, u_2, \dots, u_k \in V$  be nonzero vectors satisfying (a) and (b) of Lemma 8.3.1. Fix  $k \in \{1, 2, \dots, r\}$  and let  $p_k = s(u_k; W_{k-1})$ , the  $T$ -conductor of  $u_k$  into  $W_{k-1}$ . Then

$$p_k(T)u_k = p_k(T)w_0 + \sum_{i=1}^{k-1} p_i(T)h_i(T)u_i$$

for some  $w_0 \in W_0$  and  $h_1, h_2, \dots, h_{k-1} \in \mathbb{F}[x]$  by Lemma 8.3.2. Let

$$v_k = u_k - w_0 - \sum_{i=1}^{k-1} h_i(T)u_i.$$

Then since

$$p_k(T)v_k = p_k(T) \left( u_k - w_0 - \sum_{i=1}^{k-1} h_i(T)u_i \right) = p_k(T)u_k - p_k(T) \left( u_i + \sum_{i=1}^{k-1} h_i(T)u_i \right) = 0,$$

we have

$$W_{k-1} \cap Z(v_k; T) = \{0\}.$$

That is, since the choice of  $k \in \{1, 2, \dots, r\}$  is arbitrary,  $W_0, Z(v_1; T), Z(v_2; T), \dots, Z(v_r; T)$  are independent and the sum

$$V = W_0 \oplus \left( \bigoplus_{i=1}^k Z(v_i; T) \right)$$

is direct, and that the polynomials  $p_1, p_2, \dots, p_r$  are the respective  $T$ -annihilators of  $v_1, v_2, \dots, v_r$ . Therefore, the vectors  $v_1, v_2, \dots, v_r$  determine the subspaces  $W_1, W_2, \dots, W_r$  as do the vectors  $u_1, u_2, \dots, u_r$ , and the  $T$ -conductor  $p_k = s(v_k; W_{k-1})$  - which really is the  $T$ -annihilator - is maximal by (b) of Lemma 8.3.1. The vectors  $v_1, v_2, \dots, v_r$  have an additional property that  $W_0, Z(v_1; T), Z(v_2; T), \dots, Z(v_r; T)$  are independent. That is,

$$W_k = W_0 \oplus \left( \bigoplus_{i=1}^k Z(v_i; T) \right)$$

for all  $k \in \{1, 2, \dots, r\}$ . Moreover, since  $p_i(T)v_i = 0$  for all  $i \in \{1, 2, \dots, r\}$  by definition, we have a trivial linear relation

$$p_k(T)v_k = 0 + \sum_{i=1}^{k-1} p_i(T)v_i$$

and by Lemma 8.3.2,  $p_k \mid p_i$  for all  $i < k$ . To verify the uniqueness part, suppose there exist nonzero  $z_1, z_2, \dots, z_s \in V$  and the respective  $T$ -annihilators  $q_1, q_2, \dots, q_s \in \mathbb{F}[x]$  for some  $s \in \mathbb{N}$  that satisfy (a) and (b). We first show that  $p_1 = q_1$ . Define

$$S(V; W) = \{f \in \mathbb{F}[x] : \forall v \in V [f(T)v \in W]\} \subseteq \mathbb{F}[x]$$

for any subspace  $W \subseteq V$ . Now the claim is that  $S(V; W)$  is an ideal of  $\mathbb{F}[x]$ . To verify this, let  $\alpha, \beta \in S(V; W)$  and  $\gamma \in \mathbb{F}[x]$ . Then

$$(\alpha - \beta)(T)v = \alpha(T)v - \beta(T)v \in W$$



and

$$(\alpha\gamma)(T)v = \alpha(\gamma(T)v) \in W.$$

Since any  $v \in V$  is of the form

$$v = w_0 + \sum_{i=1}^s f_i(T)z_i$$

for some  $w_0 \in W_0$  and  $f_1, f_2, \dots, f_s \in \mathbb{F}[x]$ ,

$$q_1(T)v = q_1(T)w_0 + \sum_{i=1}^s q_1(T)f_i(T)z_i = q_1(T)w_0,$$

which follows from the fact that  $q_1 \mid q_i$  so  $q_1(T)z_i = 0$  for all  $i \in \{1, 2, \dots, s\}$ . Thus  $q_1 \in S(V; W)$ . Notice that  $q_1$  is the polynomial of least degree such that

$$q_1(T)z_1 \in W_0,$$

since  $Z(z_1; T)$  and  $W_0$  are independent. Therefore,  $q_1$  is the unique monic generator of  $S(V; W)$ . But by symmetry,  $p_1$  is also the unique monic generator of  $S(V; W)$ , so  $p_1 = q_1$ . Now we proceed inductively to show  $r = s$  and  $p_i = q_i$  for all  $i \in \{2, 3, \dots, r\}$ . But before doing so, we first have to prove the following lemma.

**Lemma 8.3.3.**

*Let  $f \in \mathbb{F}[x]$ . We define*

$$f(T)W = \{f(T)w \mid w \in W\}$$

*for any subspace  $W \subseteq V$ . Then the following hold:*

(a) *Let  $v \in V$  be arbitrary. Then  $f(T)Z(v; T) = Z(f(T)v; T)$ .*

(b) *If  $V = \bigoplus_{i=1}^k V_i$  for some  $T$ -invariant  $V_1, V_2, \dots, V_k \subseteq V$ , then  $f(T)V = \bigoplus_{i=1}^k f(T)V_i$ .*

(c) *If  $v, z \in V$  have the same  $T$ -annihilator, then  $f(T)v$  and  $f(T)z$  have the same  $T$ -annihilator. That is,*

$$\dim(Z(f(T)v; T)) = \dim(Z(f(T)z; T)).$$

*Proof.* For (a), notice that

$$y \in f(T)Z(v; T) \iff \exists g \in \mathbb{F}[x] [y = f(T)g(T)v] \iff \exists g \in \mathbb{F}[x] [y = g(T)f(T)v] \iff y \in Z(f(T)v; T).$$

For (b), let  $v \in V$ . Then there exist  $f_1, f_2, \dots, f_k \in \mathbb{F}[x]$  and  $v_1 \in V_1, v_2 \in V_2, \dots, v_k \in V_k$  such that

$$v = \sum_{i=1}^k f_i(T)v_i.$$

So

$$f(T)v = f(T) \sum_{i=1}^k f_i(T)v_i = \sum_{i=1}^k f_i(T)f(T)v_i.$$

Since the choice of  $v \in V$  is arbitrary, it follows that

$$V = \bigoplus_{i=1}^k V_i.$$

For (c), let  $p \in \mathbb{F}[x]$  be the common  $T$ -annihilator of  $v$  and  $z$ , and let  $q_v \in \mathbb{F}[x]$  be the  $T$ -annihilator of  $f(T)v$ . Then

$$q_v(T)f(T)v = 0$$

so  $q_v(T)v = 0$  or  $f(T)v = 0$ . Notice that we may disregard the case which  $f(T)v = 0$  easily, since  $p \mid f$  by definition and thus  $f(T)z = 0$  as well. Therefore  $f(T)v$  and  $f(T)z$  have the same  $T$ -annihilator, namely  $1 \in \mathbb{F}[x]$ . So suppose  $q_v(T)v = 0$ . But this means  $q_v(T)z = 0$  as well, since  $p \mid q_v$ . So by symmetry, if we let  $q_z \in \mathbb{F}[x]$  be the  $T$ -annihilator of  $f(T)z$ , then  $q_z(T)v = 0$  as well. It follows that  $q_v = q_z$ , and the result

$$\dim(Z(f(T)v; T)) = \dim(Z(f(T)z; T)).$$

easily follows as well. ♠

**Proof of Theorem 8.3 Is Continued Here**

*Proof of Theorem 8.3 Cont'd.* Let  $k \in \{2, 3, \dots, r\}$  and suppose  $W_{k-2}$  is  $T$ -invariant and  $p_{k-1} = q_{k-1}$ . Notice that we have proven the base case which  $k = 2$ . Moreover, notice that

$$\dim(W_{k-2}) + \dim(Z(v_{k-1}; T)) < \dim(V).$$

Since  $p_{k-1} = q_{k-1}$ ,  $\dim(Z(v_{k-1}; T)) = \dim(Z(z_{k-1}; T))$  by (c) of Lemma 8.3.3, and so

$$\dim(W_{k-2}) + \dim(Z(z_{k-1}; T)) < \dim(V)$$

which shows  $s \geq k$  as well. Notice that

$$\begin{cases} p_k(T)V = p_k(T)W_k \oplus Z(p_k(T)v_{k-1}; T) \\ p_k(T)V = p_k(T)W_k \oplus (\bigoplus_{i=k-1}^s Z(p_k(T)v_{k-1}; T)) \end{cases}$$

by (a) and (b) of Lemma 8.3.3. But

$$\dim(Z(p_k(T)v_{k-1}; T)) = \dim(Z(p_k(T)z_{k-1}; T))$$

by (c) of Lemma 8.3.3, so it is apparent that

$$\dim(Z(p_k(T)z_i)) = 0$$

for all  $i \in \{k, k+1, \dots, s\}$ . Thus  $p_k(T)z_k = 0$  and so  $q_k \mid p_k$ . But by symmetry,  $p_k \mid q_k$  as well. Thus  $p_k = q_k$  for all  $k \in \{1, 2, \dots, r\}$  and  $r = s$ , as desired. ♠

**Corollary 8.3.4.**

Every  $T$ -admissible  $W \subseteq V$  has a  $T$ -invariant complementary  $W' \subseteq V$ .

*Proof.* If  $W = V$ , then  $W' = \{0\}$ . Otherwise, by Theorem 8.3,

$$V = W \oplus \left( \bigoplus_{i=1}^r Z(v_i; T) \right)$$

for some  $v_1, v_2, \dots, v_r \in V$ . Then clearly

$$W' = \bigoplus_{i=1}^r Z(v_i; T)$$

is a  $T$ -invariant subspace such that  $W \oplus W' = V$ . ♠

**Corollary 8.3.5.**

There exists  $v \in V$  such that the  $T$ -annihilator of  $v$  is the minimal polynomial of  $T$ .

*Proof.* By Theorem 8.3,

$$V = \bigoplus_{i=1}^r Z(v_i; T)$$

for some  $v_1, v_2, \dots, v_r \in V$ , where the respective  $T$ -annihilators  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  satisfy  $p_i \mid p_{i-1}$  for all  $i \in \{2, 3, \dots, r\}$ . Then it is clear that  $p = p_1$  is the minimal polynomial of  $T$ , since for any  $v \in V$ , we have  $z_1 \in Z(v_1; T), z_2 \in Z(v_2; T), \dots, z_r \in Z(v_r; T)$  such that

$$v = \sum_{i=1}^r z_i$$

so

$$p(T)v = p(T) \sum_{i=1}^r z_i = \sum_{i=1}^r p(T)z_i = 0$$

which follows from the fact that  $p_i \mid p$  for any  $i \in \{1, 2, \dots, r\}$ . Moreover, from the definition,  $p = p_1$  is the monic polynomial of least degree which sends  $v_1$  to  $\{0\}$ . This is because the decomposition  $V = \bigoplus_{i=1}^r Z(v_i; T)$  is essentially

$$V = \{0\} \oplus \left( \bigoplus_{i=1}^r Z(v_i; T) \right).$$

Thus  $v = v_1$  is a vector such that  $s(v; \{0\})$  is the minimal polynomial of  $T$ , as desired. ♠

#### Corollary 8.3.6.

*$T$  has a cyclic vector if and only if the minimal and the characteristic polynomials of  $T$  are identical.*

*Proof.* The forward direction is supplied by Remark 8.8. To verify the reverse direction, suppose that the minimal and characteristic polynomials of  $T$  coincide, and let  $p$  be the minimal polynomial of  $T$ . Then by Corollary 8.3.5, there exists  $v \in V$  such that the  $T$ -annihilator of  $v$  is  $p$ . Since  $p$  is also the characteristic polynomial, it follows that  $\{v, Tv, \dots, T^{n-1}v\}$  is a basis for  $V$ , where  $n = \dim(V)$ . But this exactly means  $v$  is a cyclic vector of  $T$ . ♠

#### Theorem 8.4. Generalized Cayley-Hamilton Theorem

*Let  $p, f \in \mathbb{F}[x]$  be the minimal and characteristic polynomials of  $T$ , respectively. Then the following hold.*

- (a)  $p \mid f$ .
- (b)  $p$  and  $f$  have the same prime factors, except for the multiplicities.
- (c) If

$$p = \prod_{i=1}^k f_i^{r_i}$$

*for some monic  $f_1, f_2, \dots, f_k \in \mathbb{F}[x]$  and  $r_1, r_2, \dots, r_k \in \mathbb{N}$  is the prime factorization of  $p$ , then*

$$f = \prod_{i=1}^k f_i^{d_i}$$

*where*

$$d_i = \frac{\text{nullity}(f_i(T)^{r_i})}{\deg(f_i)}.$$

*Proof.* By the cyclic decomposition theorem, write

$$V = \bigoplus_{i=1}^r Z(v_i; T)$$

for some  $v_1, v_2, \dots, v_r \in V$ , and let  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  be the respective  $T$ -annihilators. Then  $p = p_1$  as we have seen in Corollary 8.3.5. Moreover, if we define  $T_i : Z(v_i; T) \rightarrow Z(v_i; T)$  to be the restriction operator induced by  $T$  for each  $i \in \{1, 2, \dots, r\}$ , then

$$T = \bigoplus_{i=1}^r T_i$$

and the minimal and characteristic polynomials of each  $T_i$  are  $p_i$ , the  $T$ -annihilator (and thus  $T_i$ -annihilator) of  $v_i$ . It follows that

$$f = \prod_{i=1}^r p_i$$

is the characteristic polynomial for  $T$ . But from the above expression, it is clear that  $p = p_1$  divides  $f$  and any prime factor which divides  $f$  divides some  $p_i$ 's, which in turn divide  $p = p_1$ . This verifies (a) and (b). To verify (c), notice that

$$V = \bigoplus_{i=1}^k N(f_i(T)^{r_i})$$

and each  $f_i^{r_i}$  is the minimal polynomial of the restriction operator  $T_i : N(f_i(T)^{r_i}) \rightarrow N(f_i(T)^{r_i})$  induced by  $T$  by the primary decomposition theorem (Theorem 2.20). Then by (b), it must be the case

$$f = \prod_{i=1}^k f_i^{d_i}$$

for some  $d_1, d_2, \dots, d_k \in \mathbb{N}$ , where

$$d_i = \frac{\text{nullity}(f_i(T)^{r_i})}{\deg(f_i)},$$

since the characteristic polynomial  $\varphi_i \in \mathbb{F}[x]$  of each  $T_i$  satisfies  $\varphi_i = f_i^{d_i}$ . That is,

$$\text{nullity}(f_i(T)^{r_i}) = \dim(N(f_i(T)^{r_i})) = \deg(\varphi_i) = d_i \deg(f_i).$$

Thus by rearranging the above equality in terms of  $d_i$ , we have the desired result. ♠

#### Corollary 8.4.1.

*Let  $N : V \rightarrow V$  be nilpotent. Then the characteristic polynomial of  $N$  is  $x^n$ , where  $n = \dim(V)$ .*

*Proof.* It is clear that  $N^k = 0$  for some  $k \in \{1, 2, \dots, n\}$ . Then by (b) of the generalized Cayley-Hamilton theorem,  $x^n$  is the characteristic polynomial of  $N$ . ♠

**Remark 8.18.** Let us take a look at the matrix analogue of the cyclic decomposition theorem. Consider a cyclic decomposition

$$V = \bigoplus_{i=1}^r Z(v_i; T)$$

for some  $v_1, v_2, \dots, v_r \in V$ , and let  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  be the respective  $T$ -annihilators. Now, for each  $i \in \{1, 2, \dots, r\}$ , let

$$\beta_i = \{v_i, Tv_i, \dots, T^{k_i-1}v_i\}$$

be a cyclic basis for  $Z(v_i; T)$ , where  $k_i = \dim(Z(v_i; T)) = \deg(p_i)$ . Moreover, if we define  $T_i : Z(v_i; T) \rightarrow Z(v_i; T)$  to be the operator induced by  $T$ , then  $[T_i]_{\beta_i}$  is the companion matrix of  $p_i$ . Thus, if we define

$$\beta = \{\beta_1, \beta_2, \dots, \beta_r\},$$

then

$$[T]_{\beta} = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{bmatrix},$$

where each  $A_i = [T_i]_{\beta_i}$ . This motivates the following definition.

#### Def'n. Rational Form

Let  $A \in M_{n \times n}(\mathbb{F})$ . We say  $A$  is in *rational form* if

$$A = \bigoplus_{i=1}^r A_i,$$

where each  $A_i$  is the companion matrix of a nonscalar monic  $p_i \in \mathbb{F}[x]$  satisfying  $p_i \mid p_{i-1}$  for all  $i \in \{2, 3, \dots, r\}$ .

**Theorem 8.5.**  
Every  $B \in M_{n \times n}(\mathbb{F})$  is  
Similar over  $\mathbb{F}$  to a  
Unique  $A \in M_{n \times n}(\mathbb{F})$  in  
Rational Form

Let  $B \in M_{n \times n}(\mathbb{F})$ . Then there exists a unique  $A \in M_{n \times n}(\mathbb{F})$  in rational form such that  $B$  and  $A$  are similar.

*Proof.* Let  $\beta$  be the standard ordered basis for  $\mathbb{F}^n$  and let  $T : \mathbb{F}^n \rightarrow \mathbb{F}^n$  be the unique linear operator such that  $[T]_{\beta} = B$ . By using the construction in Remark 8.18, there exist  $v_1, v_2, \dots, v_r \in \mathbb{F}^n$  and the respective  $T$ -annihilators  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  satisfying  $p_i \mid p_{i-1}$  for all  $i \in \{2, 3, \dots, r\}$  such that

$$\mathbb{F}^n = \bigoplus_{i=1}^r Z(v_i; T),$$

where  $\alpha = \{T^k v_i : 0 \leq k < \deg(p_i) = \dim(Z(v_i; T))\}$  is a basis for  $\mathbb{F}^n$  such that  $[T]_{\alpha}$  is in rational form. Now suppose there exists another ordered basis  $\gamma$  for  $V$  such that  $[T]_{\gamma}$  is in rational form. Notice that

$$[T]_{\gamma} = \bigoplus_{i=1}^s C_i$$

for some  $s \in \mathbb{N}$  and  $C_1, C_2, \dots, C_s$ , which are the respective companion matrices of some monic nonscalar  $q_1, q_2, \dots, q_s \in \mathbb{F}[x]$ . Then by Corollary 8.2.1, each  $q_i$  is the characteristic and the minimal polynomial of  $C_i$ , so by Corollary 8.3.5, there exists  $z_i \in V$  such that the  $T$ -annihilator of  $z_i$  is  $q_i$ . So we have nother cyclic decomposition

$$\mathbb{F}^n = \bigoplus_{i=1}^s Z(z_i; T),$$

which means  $r = s$  and  $p_i = q_i$  for all  $i \in \{1, 2, \dots, r\}$  by the uniqueness part of the cyclic decomposition theorem. Thus  $[T]_{\alpha} = [T]_{\gamma}$ , as desired. ♠

#### Def'n. Invariant Factor of a Matrix

Let  $B \in M_{n \times n}(\mathbb{F})$  and let  $T : \mathbb{F}^n \rightarrow \mathbb{F}^n$  satisfy  $[T]_{\beta} = B$ , where  $\beta$  is the standard ordered basis for  $\mathbb{F}^n$ . Then for any cyclic decomposition

$$\mathbb{F}^n = \bigoplus_{i=1}^r Z(v_i; T)$$

for some  $v_1, v_2, \dots, v_r \in \mathbb{F}^n$ , the respective  $T$ -annihilators  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  is the same regardless of the choice of  $v_1, v_2, \dots, v_r$ . We call these polynomials  $p_1, p_2, \dots, p_r$  the *invariant factors* of  $B$ .

**Remark 8.19.** We shall discuss an algorithm for calculating invariant factors later. The fact that invariant factors can be computed by means of finite number of rational operations on the entries of a matrix is what gives rational form its name.

**Example 8.20.** Suppose  $\dim(V) = 2$ . Observe that the possibilities for the cyclic decomposition of  $V$  is very limited. Let  $p \in \mathbb{F}[x]$  be the minimal polynomial of  $T$ . If  $\deg(p) = 2 = \dim(V)$ , then  $p$  is also the characteristic polynomial of  $T$ , and thus  $T$  has a cyclic vector. That is, there exists some ordered basis  $\beta$  for  $V$  such that  $[T]_\beta$  is the companion matrix of  $p$ . On the other hand, if  $\deg(p) = 1$ , then  $T = cI$  for some  $c \in \mathbb{F}$ , and thus for any linearly independent  $v_1, v_2 \in V$ , we have

$$V = Z(v_1; T) \oplus Z(v_2; T)$$

and the respective  $T$ -annihilators  $p_1, p_2 \in \mathbb{F}[x]$  are such that

$$p_1 = p_2 = p = x - c.$$

That is, in terms of matrices in  $M_{2 \times 2}(\mathbb{F})$ , every  $A \in M_{2 \times 2}(\mathbb{F})$  is similar to exactly one matrix of the types

$$\begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & -c_0 \\ 1 & -c_1 \end{bmatrix}$$

over  $\mathbb{F}$ , for some  $c, c_0, c_1 \in \mathbb{F}$ .

**Example 8.21.** Suppose  $T : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  satisfies

$$[T]_\beta = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$$

where  $\beta$  is the standard ordered basis. By some calculations, we can show that

$$f = (x - 1)(x - 2)^2$$

is the characteristic polynomial of  $T$  and

$$p = (x - 1)(x - 2)$$

is the minimal polynomial of  $T$ . So if we consider a cyclic decomposition

$$\mathbb{R}^3 = \bigoplus_{i=1}^r Z(v_i; T)$$

it is clear that the  $T$ -annihilator of  $v_1$  is  $p_1 = p$ . Moreover, since

$$\dim(Z(v_1; T)) = \deg(p_1) = \deg(p) = 2,$$

it follows that

$$\mathbb{R}^3 = Z(v_1; T) \oplus Z(v_2; T)$$

where  $\dim(Z(v_2; T)) = 1$ . But this exactly means that  $v_2$  is an eigenvector of  $T$ , which the corresponding eigenvalue is 2, since we must have  $f = p_1 p_2$  where  $p_2 \in \mathbb{F}[x]$  is the  $T$ -annihilator of  $v_2$ . It follows immediately that

$$[T]_{\alpha} = \begin{bmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

where  $\alpha = \{v_1, Tv_1, v_2\}$ . But how do we actually compute  $v_1$  and  $v_2$ ? TO answer this question, notice that any  $v_1 \in V$  such that  $\dim(Z(v_1; T)) = 2$  and any  $v_2 \in V \setminus Z(v_1; T)$  such that  $Tv_2 = 2v_2$  are suitable. For instance, if we take  $v_1 = (1, 0, 0)$ , then

$$Tv_1 = \begin{bmatrix} 5 \\ -1 \\ 3 \end{bmatrix}$$

which clearly is linearly independent of  $v_1$ . To find  $v_2$ , notice that

$$T \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = 2 \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}$$

if and only if  $u_1 = 2u_2 + 2u_3$  by some calculations, and an example of such  $v_2$  is  $v_2 = (2, 1, 0)$ . By direct calculations, it can be verified that

$$[T]_{\alpha} = \begin{bmatrix} 0 & -2 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

when  $\alpha = \{(1, 0, 0), (5, -1, 3), (2, 1, 0)\}$ .

## Jordan Form

**Remark 8.22.** Consider analyzing a cyclic decomposition of a nilpotent linear operator. Let  $N : V \rightarrow V$  be nilpotent. By the cyclic decomposition theorem, there exist  $v_1, v_2, \dots, v_r \in V$  and the corresponding  $N$ -annihilators  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  such that

$$V = \bigoplus_{i=1}^r Z(v_i; N)$$

and  $p_i \mid p_{i-1}$  for all  $i \in \{2, 3, \dots, r\}$ . Since  $N$  is nilpotent, the minimal polynomial for  $N$  is  $x^k$  for some  $k \in \{1, 2, \dots, n\}$  by Corollary 8.4.1. It follows that  $p_i = x^{k_i}$  for some  $k_i \in \mathbb{N}$  such that

$$k_1 \geq k_2 \geq \dots \geq k_r$$

and  $k_1 = k$ . The companion matrix  $C_i \in M_{k_i \times k_i}(\mathbb{F})$  of  $p_i = x^{k_i}$  is

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

the matrix with 1's at the entries directly below the main diagonal and 0's at every other entries. Therefore, the cyclic decomposition theorem provides a basis  $\beta$  for  $V$  such that

$$[N]_{\beta} = \bigoplus_{i=1}^r C_i,$$

a direct sum of elementary nilpotent matrices, the sizes of which nonincreases as  $i$  increases. Moreover,  $r \in \mathbb{N}$  and  $p_1, p_2, \dots, p_r \in \mathbb{F}[x]$  are unique, so with a nilpotent operator  $N$  on a  $n$ -dimensional vector space, we see that the number  $r \in \mathbb{N}$  of the cyclic subspaces involved in a decomposition and some  $k_1, k_2, \dots, k_r \in \mathbb{N}$  such that  $\sum_{i=1}^r k_i = n$  and  $k_1 \geq k_2 \geq \dots \geq k_r$  uniquely determine the rational form of the linear operator up to similarity. Moreover, here is one more thing that we would like to point out. That is,

$$r = \text{nullity}(N).$$

In fact, the  $r$  vectors  $N^{k_1-1}v_1, N^{k_2-1}v_2, \dots, N^{k_r-1}v_r$  form a basis for  $\ker(N)$ . To see this, let

$$v = \sum_{i=1}^r f_i(N)v_i \in \ker(N)$$

for some  $f_1, f_2, \dots, f_r \in \mathbb{F}[x]$  and denote  $\alpha = \{N^{k_1-1}v_1, N^{k_2-1}v_2, \dots, N^{k_r-1}v_r\}$  for convenience. Since  $\dim(Z(v_i; T))$ , we may assume  $\deg(f_i) < k_i$  without loss of generality. Since  $Nv = 0$ ,

$$Nf_i(N)v_i = (xf_i)(N)v_i = 0$$

for each  $i \in \{1, 2, \dots, r\}$ , which means  $p_i \mid f_i$  for all  $i \in \{1, 2, \dots, r\}$ . But each  $p_i = x^{k_i}$  and  $\deg(f_i) < k_i$ , so each

$$f_i = c_i x^{k_i-1}$$

for some  $c_i \in \mathbb{F}$ . Then,

$$v = \sum_{i=1}^r c_i N^{k_i-1}v_i$$

so clearly  $\ker(N) \subseteq \text{span}(\alpha)$ . On the other hand,

$$N \sum_{i=1}^r c_i N^{k_i-1}v_i = \sum_{i=1}^r c_i N^{k_i}v_i = 0,$$

so  $\text{span}(\alpha) \subseteq \ker(N)$ . Since  $\alpha$  is linearly independent, it follows that  $\alpha$  is a basis for  $\ker(N)$ .

**Remark 8.23.** Now, we are going to combine the results of Remark 8.23 and the primary decomposition theorem (Theorem 2.20). Suppose that the characteristic polynomial  $f \in \mathbb{F}[x]$  factors over  $\mathbb{F}$  as

$$f = \prod_{i=1}^k (x - c_i)^{d_i}$$

for some distinct  $c_1, c_2, \dots, c_k \in \mathbb{F}$  and  $d_1, d_2, \dots, d_k \in \mathbb{N}$ . Then the minimal polynomial  $p \in \mathbb{F}[x]$  of  $T$  would be

$$p = \prod_{i=1}^k (x - c_i)^{r_i}$$

where  $1 \leq r_i \leq d_i$  for each  $i \in \{1, 2, \dots, k\}$ . Let  $W_i = \ker(T_i - c_i I)^{r_i}$ . Then by the primary decomposition theorem,

$$V = \bigoplus_{i=1}^k W_i$$

and the linear operator  $T_i : W_i \rightarrow W_i$  induced by  $T$  has minimal polynomial  $(x - c_i)^{r_i}$  for each  $i \in \{1, 2, \dots, k\}$ . Now, define

$$N_i = T_i - c_i I : W_i \rightarrow W_i$$



for each  $i \in \{1, 2, \dots, k\}$ . Then  $N_i$  is nilpotent and has minimal polynomial  $x^{r_i}$ . On  $W_i$ ,  $T$  acts like  $N_i + c_i I$ . That is, if we choose a basis  $\beta$  for  $W_i$  corresponding to the cyclic decomposition for  $N_i$ , then  $[T_i]_\beta$  would be the direct sum of matrices of the form

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

each with  $c = c_i$ . Furthermore, the sizes of these matrices would nonincrease as one reads from left to right. We use the following terminology to specify such matrices.

**Def'n. Elementary Jordan Matrix with Eigenvalue**

We call a matrix of the form

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

an *elementary Jordan matrix* with eigenvalue  $c$ .

*Remark 8.23 is continued here*

Now, if we define

$$\beta = \{\beta_1, \beta_2, \dots, \beta_k\},$$

where each  $\beta_i$  is an ordered basis for  $W_i$  such that  $\{T_i\}_{\beta_i}$  is a direct sum of elementary Jordan matrices, then  $\beta$  is a basis for  $V$ . Then the matrix representation  $[T]_\beta$  of  $T$  would be the direct sum

$$[T]_\beta = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{bmatrix}$$

where each  $A \in M_{d_i \times d_i}(\mathbb{F})$  is of the form

$$\bigoplus_{j=1}^{n_i} J_{ij}$$

where each  $J_{ij}$  is an elementary Jordan matrix with eigenvalue  $c_i$ . Moreover, the sizes of elementary Jordan matrices  $J_{i1}, J_{i2}, \dots, J_{ij}$  are nonincreasing as one reads from left to right. This motivates the following definition.

**Def'n. Jordan Form**

Let  $c_1, c_2, \dots, c_k \in \mathbb{F}$  be distinct and suppose  $A \in M_{n \times n}(\mathbb{F})$  is a direct sum of  $A_1, A_2, \dots, A_k$ , each  $A_i$  of which is a direct sum of elementary Jordan matrices with eigenvalue  $c_i$ , the sizes of which are nonincreasing as one reads from left to right. Such matrix  $A$  is said to be in *Jordan form*.

**Remark 8.24.** So in summary, we have shown that any linear operator  $T$  on a finite-dimensional vector space  $V$  for which the characteristic polynomial  $f \in \mathbb{F}[x]$  factors over  $\mathbb{F}$  has an ordered basis  $\beta$  for  $V$

such that  $[T]_\beta$  is in Jordan form. What we now want to point out is that, this Jordan form  $[T]_\beta$  of  $T$  is something uniquely associated with  $T$ , up to the order which the eigenvalues of  $T$  are written down. In other words, if  $A, B \in M_{n \times n}(\mathbb{F})$  are similar and in Jordan form, then they only differ in the order which the eigenvalues  $c_1, c_2, \dots, c_k \in \mathbb{F}$  are written down.

**Proposition 8.6.**  
**Uniqueness of**  
**Jordan form up to**  
**Reordering**  
**Eigenvalues**

*Let  $T : V \rightarrow V$  be a linear operator such that the characteristic polynomial of  $T$  factors over  $\mathbb{F}$ . Then there exists an ordered basis  $\alpha$  for  $V$  such that  $[T]_\alpha$  is in Jordan form. Moreover, if  $\beta$  is a basis for  $V$  such that  $[T]_\beta$  is in Jordan form, then  $[T]_\alpha$  and  $[T]_\beta$  are same up to reordering the eigenvalues  $c_1, c_2, \dots, c_k \in \mathbb{F}$  of  $T$ .*

*Proof.* The existence part is supplied by Remark 8.23. To verify the uniqueness up to reordering, first write

$$A = \bigoplus_{i=1}^k A_i \in M_{d_i \times d_i}(\mathbb{F})$$

where each

$$A_i = \bigoplus_{j=1}^{r_i} J_{ij}$$

for some elementary Jordan matrices  $J_{i1}, J_{i2}, \dots, J_{ir_i}$ , the sizes of which are nonincreasing as we read from left to right. Then  $A$  is lower triangular and

$$f = \prod_{j=1}^{r_i} (x - c_i)^{d_i}$$

is the characteristic polynomials for  $A$ , since each  $c_i$  is repeated  $d_i$  times on the main diagonal. This verifies that  $c_1, c_2, \dots, c_k$  and  $d_1, d_2, \dots, d_k$  are unique up to reordering. The fact that  $A$  is the direct sum of  $A_1, A_2, \dots, A_k$  provides a direct sum decomposition

$$V = \bigoplus_{i=1}^k W_i$$

by the primary decomposition theorem (Theorem 2.20), where  $W_i = \ker(A_i - c_i I)^{r_i}$ . Now the claim is

$$W_i = \ker(T - c_i I)^n.$$

To verify this, first observe that

$$\ker(T - c_i I)^n \subseteq W_i.$$

This is because there exists unique  $v_1 \in W_1, v_2 \in W_2, \dots, v_k \in W_k$  such that

$$v = \sum_{i=1}^k v_i$$

for any  $v \in V$  by the direct sum decomposition of  $V$ . Therefore, if  $v \in \ker(T - c_i I)^n$ , then

$$(T - c_i I)^n v = \sum_{j=1}^k (T - c_i I)^n v_j = \sum_{j=1}^k (T_j - c_i I)^n v_j = 0,$$

which means

$$(T_j - c_i I)^n v_j = 0$$

for all  $j \in \{1, 2, \dots, n\}$ . But  $T_j - c_i I$  is invertible whenever  $j \neq i$ , so it follows that  $v_j = 0$  whenever  $j \neq i$  and thus  $v = v_i \in W_i$ . Moreover, observe that

$$\ker(T_i - c_i I)^{r_i} \subseteq \ker(T_i - c_i I)^n$$

where  $T_i : W_i \rightarrow W_i$  is the operator induced by  $T$ , since  $r_i \leq n$  and

$$v \in \ker(T_i - c_i I)^{r_i} \implies (T_i - c_i I)^{r_i} v = 0 \implies (T_i - c_i I)^n v = (T_i - c_i I)^{n-r_i} (T_i - c_i I)^{r_i} v = 0.$$

Thus we have

$$W_i = \ker(A_i - c_i I)^{r_i} = \ker(T_i - c_i)^{r_i} \subseteq \ker(T_i - c_i)^n \subseteq \ker(T - c_i I)^n \subseteq W_i$$

verifying our claim. This means  $W_1, W_2, \dots, W_k$  are also unique up to reordering. Since each  $W_i$  is  $T$ -invariant, the Jordan form of  $T_i$  is unique. Thus the Jordan form of  $T$ , which is a direct sum of Jordan form of  $T_1, T_2, \dots, T_k$  is unique up to reordering. ♠

*This page intentionally left blank.*

# 9.

## Bilinear Forms

- 
- 9.1 Bilinear Forms
  - 9.2 Symmetric Bilinear Form
  - 9.3 Skew-Symmetric Bilinear Form
  - 9.4 Groups Preserving Bilinear Forms
-

## Bilinear Forms

**Remark 9.1.** For this and next section, unless otherwise specified, let  $V$  denote a finite-dimensional vector space.

### Recall. Linear Functional on a Vector Space

Let  $V$  be a vector space. We say a function  $L : V \rightarrow \mathbb{F}$  is a **linear functional** on  $V$  if  $L$  is linear.

### Def'n. Bilinear Form on a Vector Space

Let  $V$  be a vector space. We say a function  $f : V \times V \rightarrow \mathbb{F}$  is a **bilinear form** on  $V$  if

$$\begin{cases} f(cv + u, w) = cf(v, w) + f(u, w) \\ f(v, cu + w) = cf(v, u) + f(v, w) \end{cases}$$

In other words,  $f(v, u)$  is bilinear if  $f$  is a linear functional of  $v$  when  $u$  is fixed and vice versa.

**Example 9.2.** Clearly the zero function  $0 : V \times V \rightarrow \mathbb{F}$  is a bilinear form on  $V$ .

**Remark 9.3.** Let  $f, g : V \times V \rightarrow \mathbb{F}$  be bilinear and let  $c \in \mathbb{F}$ . Then

$$cf + g : V \times V \rightarrow \mathbb{F}$$

is also bilinear. In fact, if  $f_1, f_2, \dots, f_n : V \times V \rightarrow \mathbb{F}$  are bilinear, then

$$\sum_{i=1}^n c_i f_i : V \times V \rightarrow \mathbb{F}$$

is also bilinear. Together with Example 9.1, it follows that the set of bilinear forms on  $V$ , denoted as  $\mathcal{L}(V, V, \mathbb{F})$ , is a subspace of the vector space  $\mathbb{F}^{V \times V}$ .

**Example 9.4.** Let  $V$  be a vector space and let  $L_1, L_2 : V \rightarrow \mathbb{F}$  be linear functionals on  $V$ . Then

$$f(v, u) = L_1(v)L_2(u)$$

is bilinear, since  $f$  is a linear functional of  $v$  when  $u$  is fixed and vice versa.

**Example 9.5.** Let  $m, n \in \mathbb{N}$  and let  $V = M_{m \times n}(\mathbb{F})$ . Let  $A \in M_{m \times m}(\mathbb{F})$ . Define

$$f_A(X, Y) = \text{tr}(X^T A Y),$$

then  $f_A$  is a linear functional on  $V$ . For, if  $X, Y, Z \in V$  and  $c \in \mathbb{F}$ , then

$$f_A(cX + Y, Z) = \text{tr}((cX + Y)^T A Z) = \text{tr}(cX^T A Z) + \text{tr}(Y^T A Z) = f_A(cX, Z) + f_A(Y, Z).$$

In particular, when  $n = 1$ , the matrix  $X^T A Y$  is  $1 \times 1$ , and the bilinear form is simply

$$f_A(X, Y) = X^T A Y = \sum_{i,j} A_{ij} X_i Y_j.$$

We shall presently show that every bilinear form on the space  $M_{m \times 1}(\mathbb{F})$  is of this type, for some  $A \in M_{m \times m}(\mathbb{F})$ .

**Example 9.6.** Let us find all bilinear forms on  $\mathbb{F}^2$ . Suppose  $f : \mathbb{F}^2 \times \mathbb{F}^2 \rightarrow \mathbb{F}$  is bilinear. If we let

$$v = (v_1, v_2), u = (u_1, u_2) \in \mathbb{F}^2,$$

then

$$\begin{aligned} f(v, u) &= f(v_1 e_1 + v_2 e_2, u) = v_1 f(e_1, u) + v_2 f(e_2, u) = v_1 f(e_1, u_1 e_1 + u_2 e_2) + v_2 f(e_2, u_1 e_1 + u_2 e_2) \\ &= v_1 u_1 f(e_1, e_1) + v_1 u_2 f(e_1, e_2) + v_2 u_1 f(e_2, e_1) + v_2 u_2 f(e_2, e_2), \end{aligned}$$

where each  $e_i \in \mathbb{F}^2$  is the  $i$ th element of the standard ordered basis for  $\mathbb{F}^2$ . That is,  $f$  is completely determined by  $a_{ij} = f(e_i, e_j)$ 's, such that

$$f(v, u) = \sum_{i,j} a_{ij} v_i u_j.$$

If  $X$  and  $Y$  are the coordinate matrices of  $v$  and  $u$ , respectively, and if  $A \in M_{2 \times 2}(\mathbb{F})$  with entries

$$A_{ij} = a_{ij} = f(e_i, e_j),$$

then

$$f(v, u) = X^T A Y.$$

Thus we see that any bilinear form on  $\mathbb{F}^2$  is precisely of the form which we discussed in Example 9.4.

**Remark 9.7.** We may generalize the results of Example 9.5 as follows. Let  $\beta = \{v_1, v_2, \dots, v_n\}$  be an ordered basis for  $V$  and let  $f : V \times V \rightarrow \mathbb{F}$  be bilinear. If

$$x = \sum_{i=1}^n x_i v_i, y = \sum_{i=1}^n y_i v_i \in V$$

for some  $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n \in \mathbb{F}$ , then

$$f(x, y) = f\left(\sum_i x_i v_i, y\right) = \sum_i x_i f(v_i, y) = \sum_i x_i f\left(v_i, \sum_j y_j v_j\right) = \sum_{i,j} x_i y_j f(v_i, v_j).$$

That is, if we let  $A_{ij} = f(v_i, v_j)$ , then

$$f(x, y) = \sum_{i,j} A_{ij} x_i y_j = X^T A Y$$

where  $X$  and  $Y$  are the coordinate matrices of  $x$  and  $y$  in the ordered basis  $\beta$  for  $V$ , respectively. Thus every bilinear form on  $V$  is of the type

$$f(x, y) = [x]_{\beta} A [y]_{\beta}$$

for some  $A \in M_{n \times n}(\mathbb{F})$  and an ordered basis  $\beta$  for  $V$ . Conversely, if  $A \in M_{n \times n}(\mathbb{F})$  is given, then clearly the above equation defines a bilinear form  $f : V \times V \rightarrow \mathbb{F}$  such that

$$A_{ij} = f(v_i, v_j).$$

This motivates the following definition.

**Def'n. Matrix of a Bilinear Function with Respect to an Ordered Basis**

Let  $f : V \times V \rightarrow \mathbb{F}$  be bilinear and let  $\beta = \{v_1, v_2, \dots, v_n\}$  be an ordered basis for  $V$ . Then we define the *matrix* of  $f$  with respect to  $\beta$  by

$$([f]_{\beta})_{ij} = f(v_i, v_j).$$

**Theorem 9.1.**  
 $[\ ]_\beta : \mathcal{L}(V, V, \mathbb{F}) \rightarrow M_{n \times n}(\mathbb{F})$  **Is an Isomorphism**

Let  $\beta$  be an ordered basis for  $V$ . Then  $[\ ]_\beta : \mathcal{L}(V, V, \mathbb{F}) \rightarrow M_{n \times n}(\mathbb{F})$  is an isomorphism.

*Proof.* The bijectivity of  $[\ ]_\beta$  is supplied by Remark 9.5. To verify the linearity, let  $f, g \in \mathcal{L}(V, V, \mathbb{F})$  and  $c \in \mathbb{F}$ . Then

$$([cf + g]_\beta)_{ij} = (cf + g)(v_i, v_j) = cf(v_i, v_j) + g(v_i, v_j) = (c[f]_\beta)_{ij} + ([g]_\beta)_{ij}.$$

But this exactly means

$$[cf + g]_\beta = c[f]_\beta + [g]_\beta,$$

as desired. ♠

**Recall. Dual of an Ordered Basis**

Let  $\beta = \{v_1, v_2, v_n\}$  be an ordered basis for  $V$ . Then the **dual** of  $\beta$ , denoted as  $\beta^* = \{L_1, L_2, \dots, L_n\}$  is such that

$$L_i(v) = ([v]_\beta)_i$$

for all  $v \in V$  and  $i \in \{1, 2, \dots, n\}$ .

**Corollary 9.1.1.**

Let  $\beta = \{v_1, v_2, \dots, v_n\}$  be a basis for  $V$  and let  $\beta^* = \{L_1, L_2, \dots, L_n\}$  be the dual of  $\beta$ . Then

$$\{f_{ij} = L_i L_j : i, j \in \{1, 2, \dots, n\}\}$$

is a basis for  $\mathcal{L}(V, V, \mathbb{F})$ . In particular,

$$\dim(\mathcal{L}(V, V, \mathbb{F})) = n^2.$$

*Proof.* For convenience, write

$$\alpha = \{f_{ij} = L_i L_j : i, j \in \{1, 2, \dots, n\}\}.$$

Notice that each  $f_{ij}$  is defined by

$$f_{ij}(x, y) = L_i(x)L_j(y)$$

is a bilinear form on  $V$  by Example 9.3. That is, if

$$x = \sum_{i=1}^n x_i v_i, y = \sum_{i=1}^n y_i v_i \in V,$$

then

$$f_{ij}(x, y) = x_i y_j.$$

Now, let  $f : V \times V \rightarrow \mathbb{F}$  be bilinear and let  $A = [f]_\beta$ . Then

$$f(x, y) = \sum_{i,j} A_{ij} x_i y_j$$

which exactly means

$$f = \sum_{i,j} A_{ij} f_{ij}.$$

Thus  $\alpha$  is a basis for  $\mathcal{L}(V, V, \mathbb{F})$ , as required. ♠



**Remark 9.8.** In terms of matrix point of view, one may rephrase Corollary 9.1.1 as follows: the matrix of each  $f_{ij}$  with respect to  $\beta$  is such that

$$\left([f_{ij}]_{\beta}\right)_{rs} = \begin{cases} 1 & \text{if } r = i \wedge s = j \\ 0 & \text{otherwise} \end{cases}.$$

In other words,

$$\left\{[f_{ij}]_{\beta} : i, j \in \{1, 2, \dots, n\}\right\}$$

is a set of  $n \times n$  matrices whose entries are all zero except for the entry  $\left([f_{ij}]_{\beta}\right)_{ij} = 1$ , which clearly is a basis for  $M_{n \times n}(\mathbb{F})$ . Thus it follows from Theorem 9.1 that  $\alpha$  is a basis for  $\mathcal{L}(V, V, \mathbb{F})$ .

**Remark 9.9.** The concept of the matrix of a bilinear form in an ordered basis is similar to that of the matrix representation of a linear operator. Just as for linear operators, we shall be interested in what happens to the matrix representing a bilinear form, as we change from one ordered basis to another. So suppose

$$\beta = \{v_1, v_2, \dots, v_n\}, \gamma = \{u_1, u_2, \dots, u_n\} \subseteq V$$

are ordered basis for  $V$  and let  $f : V \times V \rightarrow \mathbb{F}$  be bilinear. How are the matrices  $[f]_{\beta}$  and  $[f]_{\gamma}$  related? First, write

$$u_i = \sum_{j=1}^n a_{ij} v_j$$

for each  $j \in \{1, 2, \dots, n\}$ . For all  $v \in V$ , there exists  $c_1, c_2, \dots, c_n \in \mathbb{F}$  such that

$$v = \sum_{i=1}^n c_i u_i.$$

That is,

$$v = \sum_{i=1}^n c_i u_i = \sum_{i=1}^n c_i \sum_{j=1}^n a_{ij} v_j = \sum_{i,j} c_i a_{ij} v_j,$$

which means

$$\begin{aligned} \left([v]_{\beta}\right)_j &= \sum_{i=1}^n c_i a_{ij} \\ \left([v]_{\gamma}\right)_j &= c_j. \end{aligned}$$

So if  $P_{ij} = a_{ij}$ , then

$$[v]_{\beta} = P[v]_{\gamma}.$$

This matrix is unique, and for all  $v, u \in V$ ,

$$f(v, u) = [v]_{\beta}^T [f]_{\beta} [v]_{\beta} = \left(P[u]_{\gamma}\right)^T [f]_{\beta} P[v]_{\gamma} = [u]_{\gamma}^T \left(P^T [f]_{\beta} P\right) [v]_{\gamma}.$$

Thus by the definition and uniqueness of the matrix  $[f]_{\gamma}$ , it follows that

$$[f]_{\gamma} = P^T [f]_{\beta} P.$$

**Example 9.10.** Define  $f : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$  by

$$f(x, y) = x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2$$

provided that  $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$ . Then  $x = x_1 e_1 + x_2 e_2$  and  $y = y_1 e_1 + y_2 e_2$  where  $\beta = \{e_1, e_2\}$  is the standard ordered basis for  $\mathbb{R}^2$ . So

$$f(e_1, e_1) = f(e_1, e_2) = f(e_2, e_1) = f(e_2, e_2) = 1$$

which means

$$[f]_{\beta} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Now let  $v_1 = (1, -1), v_2 = (1, 1) \in \mathbb{R}^2$  and let  $\gamma = \{v_1, v_2\}$  be an ordered basis for  $\mathbb{R}^2$ . If  $P \in M_{2 \times 2}(\mathbb{R})$  is the change of basis matrix, then

$$\begin{aligned} v_1 = (1, -1) &= P_{11}e_1 + P_{21}e_2 \implies P_{11} = 1, P_{21} = -1 \\ v_2 = (1, 1) &= P_{11}e_1 + P_{21}e_2 \implies P_{12} = P_{22} = 1. \end{aligned}$$

Thus,

$$[f]_{\gamma} = P^T [f]_{\beta} P = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 4 \end{bmatrix}.$$

What this means is that, if  $x = x_1 v_1 + x_2 v_2$  and  $y = y_1 v_1 + y_2 v_2$ , then

$$f(x, y) = 4x_2 y_2.$$

**Remark 9.11.** One consequence of the change of basis equation

$$[f]_{\gamma} = P^T [f]_{\beta} P$$

is the following. If  $A, B \in M_{n \times n}(\mathbb{F})$  represents the same bilinear form on  $V$ , then  $A$  and  $B$  have the same rank. For, if

$$B = P^T A P$$

for some invertible  $P \in M_{n \times n}(\mathbb{F})$ , it is clear that  $A$  and  $B$  have the same rank. This makes it possible to define the rank of a bilinear form  $f$  on  $V$  to be the rank of  $[f]_{\beta}$  for some ordered basis  $\beta$  on  $V$ . However, it is more desirable to give more intrinsic definition of the rank of a bilinear form. This can be done as follows. Suppose  $f(v, u)$  is a bilinear form on  $V$ . If we fix  $v \in V$ , then  $f(v, u)$  becomes a linear functional on  $V$ ; let us denote this by  $L_f(v)$ . This provides us a linear transformation  $L_f : V \rightarrow V^*$  by the mapping

$$v \mapsto L_f(v).$$

On the other hand, if we fix  $u \in V$ , then we also get a linear functional  $R_f(u) : V \rightarrow \mathbb{F}$ , and  $R_f$  is a linear transformation. After we prove that

$$\text{rank}(L_f) = \text{rank}(R_f),$$

we shall define the rank of a bilinear form on a finite-dimensional vector space to be the rank of the associated linear transformations.

**Proposition 9.2.**

$$\text{rank}(L_f) = \text{rank}(R_f)$$

*Let  $f$  be a bilinear form on  $V$  and define linear transformations*

$$L_f, R_f : V \rightarrow V^*$$

*as Remark 9.9. Then  $\text{rank}(L_f) = \text{rank}(R_f)$ .*

*Proof.* To prove  $\text{rank}(L_f) = \text{rank}(R_f)$ , it is sufficient to prove that  $\text{nullity}(L_f) = \text{nullity}(R_f)$  by rank-nullity theorem. Let  $\beta$  be an ordered basis for  $V$  and let  $A = [f]_\beta$ . Then

$$f(x, y) = X^T [f]_\beta Y,$$

where  $X$  and  $Y$  are the coordinate matrix of  $x$  and  $y$ , respectively. So if  $L_f(x) = 0$ , then

$$\left( X^T [f]_\beta \right) Y = 0$$

for any  $Y \in M_{n \times 1}(\mathbb{F})$ . Clearly this means

$$X^T [f]_\beta = 0,$$

or, equivalently,

$$[f]^T \beta X = 0.$$

This means

$$\text{nullity}(L_f) = \dim \left\{ X \in M_{n \times 1}(\mathbb{F}) : [f]_\beta^T X = 0 \right\}.$$

Similar argument shows that

$$\text{nullity}(R_f) = \dim \left\{ Y \in M_{n \times 1}(\mathbb{F}) : [f]_\beta Y = 0 \right\}.$$

Since  $[f]_\beta^T$  and  $[f]_\beta$  have the same column rank, they have the same dimension of solution space of homogeneous equations. That is,

$$\text{nullity}(L_f) = \text{nullity}(R_f),$$

as desired. 

#### **Def'n. Rank** of a Bilinear Form

Let  $f$  be a bilinear form on  $V$  and let  $L_f, R_f : V \rightarrow V^*$  be linear transformations provided by Remark 9.9. Then we define the rank of  $f$  by

$$\text{rank}(f) = \text{rank}(L_f) = \text{rank}(R_f),$$

where the second equality holds by Proposition 9.2.

#### **Corollary 9.2.1.**

$\text{rank}(f) = \text{rank}[f]_\beta$

*Let  $f$  be a bilinear form on  $V$  and let  $\beta$  be an ordered basis for  $V$ . Then*


$$\text{rank}(f) = \text{rank}[f]_\beta.$$

*Proof.* From the proof of Proposition 9.2,

$$\text{nullity}(f) = \dim \left\{ X \in M_{n \times 1}(\mathbb{F}) : [f]_\beta X = 0 \right\}.$$

But it is clear that

$$\dim \left\{ X \in M_{n \times 1}(\mathbb{F}) : [f]_\beta X = 0 \right\} = \text{nullity}[f]_\beta.$$

Thus  $\text{rank}(f) = \text{rank}[f]_\beta$  by rank-nullity theorem, as desired. 

**Corollary 9.2.2.**

Let  $f$  be a bilinear form on  $V$ . Then the following are equivalent.

- (a)  $\text{rank}(f) = \dim(V)$ .
- (b)  $\forall v \in V \setminus \{0\} \exists u \in V [f(v, u) \neq 0]$ .
- (c)  $\forall u \in V \setminus \{0\} \exists v \in V [f(v, u) \neq 0]$ .

*Proof.* Observe that (a), (b), and (c) are all equivalent to the statement

$$\text{nullity}(L_f) = \text{nullity}(R_f) = 0.$$

**Def'n. Nondegenerate Bilinear Form**

Let  $f$  be a bilinear form on an arbitrary vector space  $V$ . We say  $f$  is **nondegenerate** if it satisfies (b) and (c) of Corollary 9.2.2.

**Remark 9.12.** As Corollary 9.2.2 implies, if  $f$  is a bilinear form on a finite-dimensional vector space  $V$ , then  $f$  is nondegenerate if it satisfies one of (a), (b), and (c). In particular,  $f$  is nondegenerate if and only if  $[f]_\beta$  is invertible for any ordered basis  $\beta$  for  $V$ .

**Def'n. Dot Product**

Let  $V = \mathbb{F}^n$  and let  $f$  be a bilinear form on  $V$  defined by

$$f(x, y) = \sum_{i=1}^n x_i y_i,$$

where  $x_i$  and  $y_i$  are the  $i$ th entries of  $x$  and  $y$ , respectively. Then  $f$  is nondegenerate on  $V$ . Moreover, if  $\beta$  is the standard ordered basis for  $\mathbb{F}^n$ , then

$$[f]_\beta = I.$$

That is,

$$f(x, y) = [x]_\beta^T [y]_\beta.$$

We call such  $f$  the **dot product**.

**Symmetric Bilinear Form**

**Remark 9.13.** The main purpose of this section is to answer the following question: if  $f$  is a bilinear form on  $V$ , when does an ordered basis  $\beta$  for  $V$  such that  $[f]_\beta$  is diagonal exist? We shall prove that such  $\beta$  exists if and only if  $f(v, u) = f(u, v)$  for all  $v, u \in V$ . The result is proved only when the field underlying  $V$  has characteristic zero.

**Def'n. Symmetric Bilinear Form**

Let  $f$  be a bilinear form. We say  $f$  is **symmetric** if

$$f(v, u) = f(u, v)$$

for all  $v, u \in V$ .

**Recall. Characteristic of a Field**

Let  $\mathbb{F}$  be a field. We say  $n \in \mathbb{N}$  is the *characteristic* of  $\mathbb{F}$ , denoted as  $\text{char}(\mathbb{F})$ , if  $n$  is the minimum positive integer such that adding 1  $n$  times is zero,

$$1 + 1 + \cdots + 1 = 0.$$

If no such  $n$  exists, we say  $\mathbb{F}$  has *characteristic zero*.

**Remark 9.14.** If  $V$  is finite-dimensional, then a bilinear form  $f$  is symmetric if and only if  $[f]_\beta$  is symmetric for some ordered basis  $\beta$  for  $V$ . To see this, first suppose that  $f$  is symmetric. Then,

$$f(x, y) = X^T A Y$$

where  $X$  and  $Y$  are the coordinate matrices of  $x$  and  $y$ , respectively. Since  $f$  is symmetric,  $f(x, y) = f(y, x)$  for any  $x, y \in V$ , so

$$X^T A Y = Y^T A X.$$

But  $X^T A Y, Y^T A X \in M_{1 \times 1}(\mathbb{F})$ , which means

$$X^T A Y = Y^T A X = (Y^T A X)^T = X^T A^T Y$$

for any  $X, Y \in M_{n \times 1}(\mathbb{F})$ . Thus it is clear from the above equation that  $A = A^T$ . The converse statement is clear, since  $X^T A Y, Y^T A X \in M_{1 \times 1}(\mathbb{F})$ , so

$$X^T A Y = (X^T A Y)^T = Y^T A^T X = Y^T A X.$$

One particular result is that, if  $[f]_\beta$  is diagonal for some ordered basis  $\beta$  for  $V$ , then  $f$  is symmetric, since any diagonal matrix is symmetric. Whenever a bilinear form is symmetric, we are allowed to make the following definition.

**Def'n. Quadratic Form Associated with a Symmetric Bilinear Form**

Let  $f$  be a symmetric bilinear form on  $V$ . Then we define the *quadratic form* associated with  $f$  to be

$$q(v) = f(v, v) : V \rightarrow \mathbb{F}$$

for all  $v \in V$ .

**Remark 9.15.** If  $\mathbb{F} \subseteq \mathbb{C}$  is a subfield, the symmetric bilinear form  $f$  is completely determined by its associated quadratic form, that

$$f(v, u) = \frac{1}{4}q(v+u) - \frac{1}{4}q(v-u).$$

The establishment of the above equation is a routine computation, so we shall omit it.

**Def'n. Polarization Identity**

We call the equation

$$f(v, u) = \frac{1}{4}q(v+u) - \frac{1}{4}q(v-u),$$

where  $f$  is a symmetric bilinear form on  $V$  over a subfield of  $\mathbb{C}$  and  $q$  is the quadratic form of  $f$ , the *polarization identity*.

**Example 9.16.** Suppose the bilinear form  $f$  over  $\mathbb{F}^n$  is the dot product. Then the associated quadratic form is

$$q(x_1, x_2, \dots, x_n) = \sum_{i=1}^n x_i^2.$$

In other words, the geometric interpretation is that  $q(x)$  is the square of the length of  $v$ . Moreover, notice that for any symmetric bilinear form  $f_A(x, y) = XA^TY$ , the associated quadratic form is

$$q_A(x) = X^TAX = \sum_{i,j} A_{ij}x_i x_j.$$

**Remark 9.17.** One important class of symmetric bilinear forms consists of inner products on a vector space over  $\mathbb{R}$  or  $\mathbb{C}$ .

### Def'n. Inner Product

Let  $V$  be a vector space over a subfield of  $\mathbb{C}$ . An **inner product**  $f$  on  $V$  is a symmetric bilinear form which is positive definite. That is,

$$q(v) = f(v, v) > 0$$

for any nonzero  $v \in V$ .

### Def'n. Orthogonal Vectors

Let  $v, u \in V$ . We say  $v$  and  $u$  are **orthogonal** with respect to an inner product  $f$  if

$$f(v, u) = 0.$$

*Remark 9.17 is continued here.*

The motivation for the definition of orthogonal vectors is clear: notice that if  $f$  is the dot product - which is a special form of inner products -, then

$$f(v, u) = 0$$

whenever  $v$  and  $u$  are orthogonal. The above definition is a generalization of this result. The quadratic form of an inner product  $q(v) = f(v, v)$  takes only nonnegative values by positive definiteness, and is usually thought as the square of the length of  $v$ . More discussions of inner product will be done in the following chapter.

**Theorem 9.3.**  
If  $f$  is a Symmetric Bilinear Form, Then  $[f]_\beta$  Is Diagonal for Some Ordered Basis  $\beta$

*Let  $V$  be a finite-dimensional vector space over  $\mathbb{F}$  of characteristic zero and let  $f$  be a symmetric bilinear form on  $V$ . Then there exists an ordered basis  $\beta$  for  $V$  such that  $[T]_\beta$  is diagonal.*

*Proof.* We proceed inductively. Observe that if  $f = 0$ , then the proof is trivial, so suppose that  $f$  is nonzero. When  $\dim(V) = 1$ , then  $[f]_\beta$  is diagonal for any ordered basis  $\beta$  for  $V$ . Now suppose that the result holds for any bilinear form  $f$  on a  $k$ -dimensional vector space. Let  $V$  be a vector space with  $\dim(V) = k + 1$ . Then there exists  $v_{k+1} \in V$  such that  $f(v_{k+1}, v_{k+1}) = q(v_{k+1}) \neq 0$ , where  $q$  is the quadratic form of  $f$ , since any symmetric bilinear form can be written as

$$f(v, u) = \frac{1}{4}q(v+u) - \frac{1}{4}q(v-u)$$

by the polarization identity, and it is clear from the above equation that  $q(v_{k+1}) \neq 0$  for some  $v_{k+1} \in V$ . Let  $W = \text{span}(v_{k+1})$ , then  $\dim(W) = 1$ . Moreover, let

$$W_\perp = \{w \in V : f(v_{k+1}, w) = 0\}.$$

Now the claim is that  $V = W \oplus W_\perp$ . To verify this, first observe that  $W_\perp$  is a subspace of  $V$ . For,  $f(v_{k+1}, 0) = 0$  and if  $w_1, w_2 \in W_\perp$  and  $c \in \mathbb{F}$ , then

$$f(v_{k+1}, cw_1 + w_2) = cf(v_{k+1}, w_1) + f(v_{k+1}, w_2) = 0$$

so  $cw_1 + w_2 \in W_\perp$ , which means  $W_\perp$  is closed under addition and scalar multiplication. Therefore,  $W_\perp$  is a subspace of  $V$ . It is clear that  $W$  and  $W_\perp$  are independent, since if  $w \in W$ , then  $w = cv$  for some  $c \in \mathbb{F}$ . So if  $w = cv \in W_\perp$ , then

$$f(v, cv) = cf(v, v) = 0$$

which means  $c = 0$  and  $w = cv = 0$ . To see that every  $v \in V$  can be written as

$$v = w + w_\perp$$

for some  $w \in W$  and  $w_\perp \in W_\perp$ , observe that if we define

$$w_\perp = v - \frac{f(v, v_{k+1})}{f(v_{k+1}, v_{k+1})}v_{k+1},$$

then

$$f(v_{k+1}, w_\perp) = f(v_{k+1}, v) - \frac{f(v, v_{k+1})}{f(v_{k+1}, v_{k+1})}f(v_{k+1}, v_{k+1})$$

and since  $f$  is symmetric,  $f(v, w_\perp) = 0$ . That is,  $w_\perp \in W_\perp$ . In other words, every  $v \in V$  can be written as

$$v = \frac{f(v, v_{k+1})}{f(v_{k+1}, v_{k+1})}v_{k+1} + w_\perp$$

for some  $\frac{f(v, v_{k+1})}{f(v_{k+1}, v_{k+1})}v_{k+1} \in W$  and  $w_\perp \in W_\perp$ . Thus  $V = W \oplus W_\perp$ , as claimed. By induction hypothesis,  $W_\perp$  has an ordered basis  $\beta_\perp = \{v_1, v_2, \dots, v_k\}$  such that  $[f_\perp]_{\beta_\perp}$  is diagonal. But this exactly means

$$([f_\perp]_{\beta_\perp})_{ij} = f(v_i, v_j) = 0$$

whenever  $i \neq j$ . Thus, if we define  $\beta = \{v_1, v_2, \dots, v_k, v_{k+1}\}$ , then  $\beta$  is the ordered basis for  $V$  by direct sum decomposition  $V = W \oplus W_\perp$ , and we have diagonal  $[f]_\beta$  by construction. ♠

### Corollary 9.3.1.

Let  $\mathbb{F} \subseteq \mathbb{C}$  be a subfield and let  $A \in M_{n \times n}(\mathbb{F})$ . Then there exists invertible  $P \in M_{n \times n}(\mathbb{F})$  such that  $P^T A P$  is diagonal.

### Theorem 9.4. Diagonalization of a Symmetric Bilinear Form on a Real Vector Space where Nonzero Entries Are $\pm 1$

Let  $V$  be a finite-dimensional vector space over  $\mathbb{R}$  and let  $f$  be a symmetric bilinear form on  $V$  with  $\text{rank}(f) = r \in \mathbb{N}$ . Then there exists an ordered basis  $\beta = \{v_1, v_2, \dots, v_n\}$  for  $V$  such that  $[f]_\beta$  is diagonal and

$$f(v_i, v_i) = \begin{cases} \pm 1 & \text{if } i \in \{1, 2, \dots, r\} \\ 0 & \text{otherwise} \end{cases}.$$

Furthermore, the number of  $v_i \in \beta$  such that  $f(v_i, v_i) = 1$  is independent of the choice of an ordered basis  $\beta$  for  $V$ .

*Proof.* By Theorem 9.3, there exists an ordered basis  $\alpha$  for  $V$  such that  $[f]_\alpha$  is diagonal. Since

$$\text{rank}(f) = \text{rank}[f]_\alpha,$$

it follows that exactly  $r$  entries on the main diagonal of  $[f]_\alpha$  are nonzero. That is, we may rearrange the elements of  $\alpha$  to obtain an ordered basis  $\gamma$  for  $V$  such that  $[f]_\gamma$  is diagonal and

$$([f]_\gamma)_{ii} = \begin{cases} 1 & \text{if } i \in \{1, 2, \dots, r\} \\ 0 & \text{otherwise} \end{cases}.$$

Write  $\gamma = \{u_1, u_2, \dots, u_n\}$  for convenience. For all  $i \in \{1, 2, \dots, n\}$ , define

$$v_i = \begin{cases} \frac{1}{\sqrt{|f(u_i, u_i)|}} u_i & \text{if } i \in \{1, 2, \dots, r\} \\ u_i & \text{otherwise} \end{cases}$$

and let  $\beta = \{v_1, v_2, \dots, v_r\}$ . Then

$$f(v_i, v_i) = ([f]_\beta)_{ii} = \begin{cases} \pm 1 & \text{if } i \in \{1, 2, \dots, r\} \\ 0 & \text{otherwise} \end{cases}$$

as desired. To prove the uniqueness of the number of  $v_i \in \beta$  such that

$$f(v_i, v_i) = ([f]_\beta)_{ii} = 1,$$

let  $p \in \mathbb{N}$  be the number of such  $v_i \in \beta$ . Also, let

$$V_+ = \text{span}\{v_i \in \beta : f(v_i, v_i) = 1\}, V_- = \text{span}\{v_i \in \beta : f(v_i, v_i) = -1\} \subseteq V$$

be subspaces. Now  $p = \dim(V_+)$ , so what we should verify is the uniqueness of the dimension of  $V_+$ . But first, notice that  $f$  is positive definite on  $V_+$ . That is,

$$\forall v \in V_+ \setminus \{0\} [f(v, v) > 0].$$

Similarly,  $f$  is negative definite on  $V_-$ . Moreover, if we define

$$V_\perp = \text{span}\{v_i \in \beta : f(v_i, v_i) = 0\} \subseteq V,$$

then  $V_\perp$  is also the subspace of  $V$ , and clearly we have

$$\forall v \in V_\perp [f(v, v) = 0].$$

Since the union of bases of  $V_+, V_-, V_\perp$  is  $\beta$ , and it is clear from the above constructions that  $V_+, V_-, V_\perp$  are independent, we have

$$V = V_+ \oplus V_- \oplus V_\perp.$$

Now the claim is that, if  $W \subseteq V$  is any subspace on which  $f$  is positive definite, then  $W, V_-, V_\perp$  are independent. To verify this claim, suppose  $w \in W, v_- \in V_-, v_\perp \in V_\perp$  satisfy

$$w + v_- + v_\perp = 0.$$

Then,

$$\begin{cases} f(w, w + v_-, v_\perp) &= f(w, w) + f(w, v_-) + f(w, v_\perp) = 0 \\ f(v_-, w + v_-, v_\perp) &= f(v_-, w) + f(v_-, v_-) + f(v_-, v_\perp) = 0 \end{cases}.$$

Since  $v_\perp \in V_\perp$ ,  $f(w, v_\perp) = f(v_-, v_\perp) = 0$ ,

$$\begin{cases} f(w, w) + f(w, v_-) &= 0 \\ f(v_-, w) + f(v_-, v_-) &= 0 \end{cases},$$

and  $f$  is symmetric, it follows that  $f(w, w) = f(v_-, v_-)$ . Moreover, since  $f$  is positive definite on  $W$  and negative definite on  $V_-$ , we obtain

$$f(w, w) = f(v_-, v_-) = 0.$$



So it must be the case that

$$w = v_- = v_\perp = 0,$$

verifying the claim. Then by the direct sum decomposition

$$V = V_+ \oplus v_- \oplus V_\perp,$$

we have  $\dim(V_+) \geq \dim(W)$ . On the other hand, if  $\zeta$  is another ordered basis which satisfy the property

$$([f]_\zeta)_{ii} = \begin{cases} \pm 1 & \text{if } i \in \{1, 2, \dots, r\} \\ 0 & \text{otherwise} \end{cases},$$

then we get another direct sum decomposition

$$V = W_+ \oplus W_- \oplus W_\perp,$$

where  $f$  is positive definite on  $W_+$ , negative definite on  $W_-$ , and zero on  $W_\perp$ . So we have

$$\dim(V_+) \geq \dim(W_+).$$

But by symmetry,

$$\dim(W_+) \geq \dim(V_+),$$

which means  $\dim(W_+) = \dim(V_+)$ . Thus

$$p = \dim(W_+) = \dim(V_+)$$

is unique, as desired. ♠

**Remark 9.18.** Let  $f$  be a symmetric bilinear form on a finite dimensional vector space  $V$  over  $\mathbb{R}$  and let  $\beta$  and

$$V = V_+ \oplus V_- \oplus V_\perp$$

be as described in Theorem 9.4. Now let  $V_0 \subseteq V$  be subspace such that

$$\forall v_0 \in V_0 \forall v \in V [f(v_0, v) = 0].$$

We claim that  $V_\perp = V_0$ . To verify this, first observe that Theorem 9.4 provides  $V_\perp \subseteq V_0$  by construction. On the other hand, it is clear that which means

$$\dim(V_\perp) = \dim(V) - (\dim(V_+) + \dim(V_-)) = \dim(V) - \text{rank}(f),$$

so it must be the case that every  $v_0 \in V$  such that  $f(v_0, v) = 0$  for all  $v \in V$  are such that  $v_0 \in V_\perp$ . Thus  $V_0 \subseteq V_\perp$ , verifying our claim. Thus we also see that  $V_\perp$  is unique. On the other hand, the subspaces  $V_+$  and  $V_-$  are not unique. However, their dimension is unique as Theorem 9.4 shows, allowing us to make the following definition.

**Def'n. Signature** of a Symmetric Bilinear Form on a Finite-Dimensional Real Vector Space

Let  $f$  be a symmetric bilinear form on  $V$ , a finite-dimensional vector space over  $\mathbb{R}$ , and let  $V_+, V_-, V_\perp \subseteq V$  be subspaces such that

$$V = V_+ \oplus V_- \oplus V_\perp$$

and as described in Theorem 9.4. Then we define the *signature* of  $f$  by

$$\dim(V_+) - \dim(V_-).$$

**Remark 9.19.** Let  $V$  is a finite-dimensional vector space over  $\mathbb{R}$  and let  $V_1, V_2, V_3 \subseteq V$  be such that

$$V = \bigoplus_{i=1}^3 V_i.$$

Let  $f_1, f_2$  be an inner product on  $V_1, V_2$ , respectively. Then, we may define a symmetric bilinear form  $f$  on  $V$  as follows. If  $v, u \in V$ , then write

$$v = \sum_{i=1}^3 v_i, u = \sum_{i=1}^3 u_i \in V$$

for some  $v_1, u_1 \in V_1, v_2, u_2 \in V_2, v_3, u_3 \in V_3$ . Then a direct sum decomposition

$$V = V_+ \oplus V_- \oplus V_\perp$$

for  $f$ , as described in Theorem 9.4, would be,  $V_+ = V_1, V_- = V_2, V_\perp = V_3$ . Of course,  $V_+$  and  $V_-$  need not be  $V_1$  and  $V_2$ , respectively;  $V_1$  and  $V_2$  are some suitable candidates. In fact, Theorem 9.4 guarantees that every symmetric bilinear form on  $V$  can be constructed in this way. Moreover, the part which states that

$$([f]_\beta)_{ii} \begin{cases} \pm 1 & \text{if } i \in \{1, 2, \dots, r\} \\ 0 & \text{otherwise} \end{cases},$$

for some ordered basis  $\beta$  for  $V$ , is that any inner product can be represented by the identity matrix in some ordered basis for  $V$ .

**Remark 9.20.** If  $V$  is instead a finite-dimensional vector space over  $\mathbb{C}$ , then we may further simplify the matrix of a bilinear form.

**Corollary 9.4.1.**

*Let  $V$  be a finite-dimensional vector space over  $\mathbb{C}$  and let  $f$  be a symmetric bilinear form on  $V$  with  $\text{rank}(f) = r \in \mathbb{N}$ . Then there exists an ordered basis  $\beta = \{v_1, v_2, \dots, v_n\}$  for  $V$  such that  $[f]_\beta$  is diagonal and*

$$f(v_i, v_i) = \begin{cases} 1 & \text{if } i \in \{1, 2, \dots, r\} \\ 0 & \text{otherwise} \end{cases}.$$

*Proof.* A suitable proof for Corollary 9.4.1 can be done in an analogously to the proof of Theorem 9.4 above. The only difference is that, since  $\mathbb{C}$  is an algebraically closed field, we are allowed to take a square root of  $f(u_i, u_i)$ , and that we define

$$v_i = \begin{cases} \frac{1}{\sqrt{f(u_i, u_i)}} u_i & \text{if } i \in \{1, 2, \dots, r\} \\ u_i & \text{otherwise} \end{cases}.$$



*Remark 9.20 is continued here.*

In fact, the proof of Corollary 9.4.1 is valid for any algebraically closed field, or, any field closed under the operation of taking the square root.

## Skew-Symmetric Bilinear Form

**Remark 9.21.** Throughout this section, let  $V$  be a vector space over a subfield  $\mathbb{F} \subseteq \mathbb{C}$ .

**Def'n. Skew-Symmetric Bilinear Form**

Let  $f$  be a bilinear form. We say  $f$  is *skew-symmetric* if

$$f(v, u) = -f(u, v)$$

for all  $v, u \in V$ .

**Remark 9.22.** We claim that any bilinear form  $f$  on  $V$  can be written as a sum of a symmetric bilinear form  $g$  on  $V$  and a skew-symmetric bilinear form  $h$  on  $V$ . To verify this, let

$$g = \frac{1}{2}(f(v, u) + f(u, v))$$

$$h = \frac{1}{2}(f(v, u) - f(u, v)),$$

then  $g$  and  $h$  are symmetric and skew-symmetric by definition and clearly  $f = g + h$ . Moreover, it turns out that  $g$  and  $h$  are unique. That is, if  $S$  is the set of symmetric bilinear forms on  $V$  and  $K$  is the set of skew-symmetric bilinear forms on  $V$ , then

$$\mathcal{L}(V, V, \mathbb{F}) = S \oplus K.$$

**Remark 9.23.** If  $f$  is a skew-symmetric bilinear form on  $V$ , then for any ordered basis  $\beta$  for  $V$ ,  $[f]_\beta$  is skew-symmetric.

**Remark 9.24.** Let  $f$  be a skew-symmetric bilinear form on  $V$ . Similear to linear operators and symmetric bilinear forms, we are interested in finding an ordered basis  $\beta$  such that  $[f]_\beta$  is simple, if such  $\beta$  exists. We proceed as follows. If  $f$  is nonzero, then there exists  $v, u \in V$  such that

$$f(v, u) = 1.$$

To see this, one may first pick  $v', u \in V$  such that  $f(v', u) \neq 0$ , since  $f$  is nonzero. Then it is clear that

$$v = \frac{v'}{f(v', u)}$$

satisfies the above condition. Let

$$x = av + bu \in \text{span}\{v, u\} \subseteq V$$

for some  $a, b \in \mathbb{F}$ . Then

$$f(x, v) = f(av + bu, v) = bf(u, v) = -b$$

$$f(x, u) = f(av + bu, u) = af(u, u) = a,$$

and so

$$x = av + bu = f(x, u)v - f(x, v)u.$$

The above equation shows that  $a = f(x, u)$  and  $b = f(x, v)$  are zero whenever  $x = 0$ , so  $v$  and  $u$  are linearly independent and  $\dim(W) = 2$ . Moreover, let

$$W_\perp = \{w_\perp \in V : f(w_\perp, v) = f(w_\perp, u) = 0\} \subseteq V.$$

We claim that

$$V = W \oplus W_\perp.$$

To verify this, let  $y \in V$  be arbitrary, and let

$$\begin{aligned} w &= f(y, u)v - f(y, v)u \\ w_{\perp} &= y - w. \end{aligned}$$

Then  $w \in \text{span}(v, u) = W$  and  $w_{\perp} \in W_{\perp}$ , since

$$f(w_{\perp}, v) = f(y - f(y, u)v + f(y, v)u, v) = f(y + f(y, v)u, v) = f(y, v) + f(y, v)f(u, v) = 0,$$

and we can show that  $f(w_{\perp}, u) = 0$  in a similar way. Thus any  $y \in V$  can be written by the form  $y = w + w_{\perp}$  for some  $w \in W$  and  $w_{\perp} \in W_{\perp}$ . Moreover, it is clear from the definition of  $W$  and  $W_{\perp}$  that  $W \cap W_{\perp} = \{0\}$ . That is,

$$V = W \oplus W_{\perp},$$

as claimed. Now, let  $f_{\perp}$  be the restriction of  $f$  on  $W_{\perp}$ . Then  $f_{\perp}$  is a skew-symmetric bilinear form on  $W_{\perp}$ . That is, if  $f_{\perp}$  is nonzero, then we may further decompose  $V$  as

$$V = W_1 \oplus W_2 \oplus W_{\perp_2}$$

by repeating the process above, where  $W_1 = W$ . In other words, if  $V$  is finite-dimensional, we are going to get a decomposition

$$V = \left( \bigoplus_{i=1}^k W_i \right) \oplus W_0$$

at the end, where each  $W_1, W_2, \dots, W_k \subseteq V$  is spanned by two vectors  $v_i, u_i \in V$  such that

- (a)  $f(v_i, u_i) = 1$ ,
- (b)  $f(v_i, v_j) = f(u_i, u_j) = f(v_i, u_j) = 0$  for any  $j \in \{1, 2, \dots, k\}$  with  $j \neq i$ ,
- (c) for all  $w_0 \in W_0$ ,  $w_0$  is *orthogonal* to any  $v \in V$ , which means  $f(v, w_0) = 0$ , and
- (d) the restriction of  $f$  into  $W_0$  is zero.

The following theorem summarizes the matrix analogue of this result.

**Theorem 9.5.**

*Let  $f$  be a skew-symmetric bilinear form on  $V$ . Then  $r = \text{rank}(f) = 2k$  for some  $k \in \mathbb{N} \cup \{0\}$ , and there exists an ordered basis  $\beta$  for  $V$  such that*

$$[f]_{\beta} = \left( \bigoplus_{i=1}^k \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right) \oplus O,$$

*where  $O \in M_{n-r \times n-r}(\mathbb{F})$  is the zero matrix.*

**Corollary 9.5.1.**

*If there exists nondegenerate skew-symmetric bilinear form  $f$  on  $V$ , then  $n = \dim(V)$  is even. Moreover, there exists an ordered basis  $\beta$  for  $V$  such that*

$$[f]_{\beta} = \left( \bigoplus_{i=1}^{\frac{n}{2}} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right).$$

**Remark 9.25.** Theorem 9.5 also provides the following standard matrix representation of a nondegenerate skew-symmetric bilinear form  $f$  on  $V$ . That is, if  $\beta = \{v_1, u_1, v_2, u_2, \dots, v_{\frac{n}{2}}, u_{\frac{n}{2}}\}$  is an ordered basis for  $V$  such that  $[f]_\beta$  is as described in Corollary 9.5.1, then  $\alpha = \{v_1, v_2, \dots, v_{\frac{n}{2}}, u_1, \dots, u_{\frac{n}{2}}\}$  is such that

$$[f]_\alpha = \begin{bmatrix} 0 & J \\ -J & 0 \end{bmatrix},$$

where  $J \in M_{\frac{n}{2} \times \frac{n}{2}}(\mathbb{R})$  is

$$J = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \cdots & 0 & 0 \end{bmatrix}.$$

## Groups Preserving Bilinear Forms

### Def'n. Preserve

Let  $f$  be a bilinear form on a vector space  $V$  and let  $T : V \rightarrow V$  be linear. We say  $T$  **preserves**  $f$  if

$$f(Tv, Tu) = f(v, u)$$

for all  $v, u \in V$ .

**Remark 9.26.** Notice that for any bilinear form  $f$  and linear operator  $T$  on  $V$ ,

$$g(v, u) = f(Tv, Tu)$$

is a bilinear form. Thus  $T$  preserves  $f$  if and only if  $g = f$ .

**Remark 9.27.** Clearly  $f(Iv, Iu) = f(v, u)$ . Moreover, if  $T, S : V \rightarrow V$  preserve  $f$  then

$$f(STv, STu) = f(Tv, Tu) = f(v, u)$$

so  $ST$  preserves  $f$  as well. That is, if

$$M_f = \{T \in \mathcal{L}(V) : T \text{ preserves } f\},$$

then  $(M_f, \circ)$  is a monoid, where  $\circ$  is the usual composition operation. In general, there is not much to talk about monoids of linear operators. However, if  $f$  is nondegenerate, then we have the following.

**Proposition 9.6.**  
Set of Linear  
Operator Preserving  
Nondegenerate  $f$  Is a  
Group

Let  $f$  be a nondegenerate bilinear form on a vector space  $V$ , and let

$$G_f = \{T \in \mathcal{L}(V) : T \text{ preserves } f\},$$

Then  $G_f$  is a group under the usual composition operation of linear operators.

*Proof.* Remark 9.27 provides that  $G_f$  is a monoid, so we only have to prove that every  $T \in G_f$  has an inverse  $T^{-1}$ . Let  $T \in G_f$  be and let  $v \in \ker(T)$ . Then for any  $u \in V$ ,

$$f(v, u) = f(Tv, Tu) = f(0, Tu) = 0.$$

Since  $f$  is nondegenerate,  $v = 0$ . That is,  $v = 0$  whenever  $Tv = 0$ , which means that  $T$  is invertible. Moreover,

$$f(T^{-1}v, T^{-1}u) = f(TT^{-1}v, TT^{-1}u) = f(v, u)$$

for any  $v, u \in V$ , so  $T^{-1}$  preserves  $f$ , or  $T^{-1} \in G_f$ , as desired. ♠

**Remark 9.28.** When  $V$  is finite-dimensional, an immediate consequence of Proposition 9.6 is that

$$G = \{[T]_\beta \in M_{n \times n}(\mathbb{F}) : T \text{ preserves } f\}$$

is a group under usual matrix composition, where  $n = \dim(V)$ . However, there is an alternative way of describing matrices which preserve  $f$ .

**Corollary 9.6.1.**

*Let  $A \in M_{n \times n}(\mathbb{F})$  be invertible. Then*

$$G = \{M \in M_{n \times n}(\mathbb{F}) : M^T A M = A\}$$

*is a group under usual matrix composition.*

*Proof.* We have shown that  $[\ ]_\beta : \mathcal{L}(V, V, \mathbb{F}) \rightarrow M_{n \times n}(\mathbb{F})$  is an isomorphism, where  $\dim(V) = n$  and  $\beta$  is an ordered basis for  $V$ , and also that

$$\text{rank}(f) = \text{rank}[f]_\beta$$

for any bilinear form  $f$  on  $V$ . That is, if  $A \in M_{n \times n}(\mathbb{F})$  is invertible and if we fix an ordered basis  $\beta$  for  $V$ , then there exists unique bilinear form  $f$  on  $V$  such that  $A = [f]_\beta$ . Moreover, the isomorphism  $[\ ]_\beta : \mathcal{L}(V) \rightarrow M_{n \times n}(\mathbb{F})$ , there exists unique linear operator  $T : V \rightarrow V$  such that  $M = [T]_\beta$ . Observe that

$$f(x, y) = X^T A Y,$$

where  $X = [x]_\beta$  and  $Y = [y]_\beta$  by definition. But  $A = M^T A M$ , so

$$\begin{aligned} f(x, y) &= X^T A Y = X^T M^T A M Y = (M X)^T A (M Y) \\ &= ([T]_\beta [x]_\beta)^T [f]_\beta ([T]_\beta [y]_\beta) = [Tx]_\beta^T [f]_\beta [Ty]_\beta = f(Tx, Ty), \end{aligned}$$

which means  $T$  preserves  $f$ . Since the set  $G_f$  of linear operators preserving  $f$  is a group,  $G$  is also a group by isomorphism  $[\ ]_\beta$ . ♠

**Remark 9.29.** Consider the case which  $f$  is a symmetric nondegenerate bilinear form over a vector space  $V$  over a subfield  $\mathbb{F} \subset \mathbb{C}$ . Then a linear operator  $T$  on  $V$  preserves  $f$  if and only if  $T$  preserves

$$q(v) = f(v, v),$$

the quadratic form associated with  $f$ . This can be verified as follows. If  $T$  preserves  $f$ , then it is clear that

$$q(Tv) = f(Tv, Tv) = f(v, v) = q(v).$$

Conversely, if  $T$  preserves  $q$ , then by the polarization identity

$$f(v, u) = \frac{1}{4}q(v+u) - \frac{1}{4}q(v-u),$$

$T$  preserves  $f$ .

# 10.

## Inner Product Spaces

- 
- 10.1 Inner Products
  - 10.2 Inner Product Spaces
  - 10.3 Linear Functionals and Adjoint
  - 10.4 Unitary Operators
  - 10.5 Normal Operators
  - 10.6 Spectral Theory
-

## Inner Products

**Remark 10.1.** Throughout this section, we are going to discuss about vector spaces over  $\mathbb{R}$  or  $\mathbb{C}$ . For this reason, we shall consistently use  $\mathbb{K}$  to denote  $\mathbb{R}$  or  $\mathbb{C}$ , when there is no need to distinguish between two fields.

### Recall. Dot Product on $\mathbb{R}^n$

We define the *dot product* on  $\mathbb{R}^n$  by

$$x \cdot y = \sum_{i=1}^n x_i y_i$$

for all  $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{R}^n$ .

**Remark 10.2.** There is an important geometric interpretation of  $x \cdot y$ . If we let  $\|x\|, \|y\|$  be the length of  $x$  and  $y$ , respectively, and let  $\theta$  be the angle between  $x$  and  $y$ , then

$$x \cdot y = \|x\| \|y\| \cos(\theta).$$

The motivation for an inner product is to generalize the notion of length and angle to any vector space over  $\mathbb{K}$ . However, our discussions about angle will be restricted to the concept of orthogonality of vectors.

### Def'n. Inner Product on a Vector Space

Let  $V$  be a vector space over  $\mathbb{K}$ . An *inner product* on  $V$  is a function  $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{K}$  that satisfies the following properties. Suppose  $u, v, w \in V$  and  $c \in \mathbb{K}$ .

- (a)  $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$ .
- (b)  $\langle cv, u \rangle = c \langle v, u \rangle$ .
- (c)  $\langle v, u \rangle = \overline{\langle u, v \rangle}$ , where the bar represents the complex conjugate.
- (d)  $\langle v, v \rangle > 0$  whenever  $v \neq 0$ .

**Remark 10.3.** By using (a), (b), and (c) of the definition above, one can deduce

$$\langle u, cv + w \rangle = \bar{c} \langle u, v \rangle + \langle u, w \rangle.$$

In case of  $\mathbb{K} = \mathbb{R}$ , the bars can be ignored; the purpose of including complex conjugate in the definition is to make an inner product positive definite on  $\mathbb{C}$  as well. For instance, without complex conjugate, if

$$\langle v, v \rangle > 0,$$

for some  $v \in V$ , then

$$\langle iv, iv \rangle = i \langle v, iv \rangle = -1 \langle v, v \rangle < 0$$

which is inconsistent with (d).

**Remark 10.4.** Notice that the definition of inner product here is consistent with the one provided in Chapter 9. That is, if  $f(v, u) = \langle v, u \rangle$ , then  $f$  is bilinear by (a), (b), and (c), symmetric by (c), and positive definite by (d).



**Def'n. Standard Inner Product on  $\mathbb{K}^n$** 

We define the *standard inner product*  $\langle \cdot, \cdot \rangle$  on  $\mathbb{K}^n$  by

$$\langle x, y \rangle = \sum_{i=1}^n x_i \overline{y_i},$$

where  $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{K}^n$ .

**Remark 10.5.** In case of  $\mathbb{K} = \mathbb{R}$ , the standard inner product on  $\mathbb{K}^n$  is the inner product.

**Remark 10.6.** Consider the space of square  $n \times n$  matrices,  $M_{n \times n}(\mathbb{K})$ . Then  $M_{n \times n}(\mathbb{K}) \cong \mathbb{K}^{n^2}$  in a natural way. Thus we may use the definition of standard inner product on  $\mathbb{K}^n$  to define an inner product

$$\langle A, B \rangle = \sum_{i,j} A_{ij} \overline{B_{ij}}$$

on  $M_{n \times n}(\mathbb{K})$ . To simplify this further, we introduce the following definition.

**Def'n. Complex Conjugate of a Complex Matrix**

Let  $A \in M_{n \times n}(\mathbb{K})$ . We define the *complex conjugate* of  $A$ , denoted as  $A^*$ , by

$$A_{ij}^* = \overline{A_{ji}}.$$

Then, the above definition of an inner product on  $M_{n \times n}(\mathbb{K})$  can be alternatively written as

$$\langle A, B \rangle = \text{tr}(AB^*) = \text{tr}(B^*A),$$

since

$$\langle A, B \rangle = \sum_{i,j} A_{ij} \overline{B_{ij}} = \sum_{i,j} A_{ij} B_{ji}^* = \sum_i (AB^*)_{ii} = \text{tr}(AB^*),$$

and the second equality holds by definition of trace.

**Remark 10.7.** Suppose  $Q \in M_{n \times n}(\mathbb{K})$  is invertible. Then for any  $X, Y \in M_{n \times 1}(\mathbb{K})$ , let

$$\langle X, Y \rangle = X^* Q^* Q Y.$$

Then  $\langle X, Y \rangle$  is an inner product on  $M_{n \times 1}(\mathbb{K})$ . Moreover, when  $Q = I$ , the identity matrix, then the above definition is essentially identical to the definition of the standard inner product on  $\mathbb{K}^n$ .

**Def'n. Standard Inner Product on  $\mathbb{K}^n$** 

We call the inner product

$$\langle X, Y \rangle = X^* Y$$

on  $M_{n \times 1}(\mathbb{K})$  the *standard inner product* on  $\mathbb{K}^n$ .

**Example 10.8.** Let

$$V = \{f : \mathbb{C} \rightarrow \mathbb{C} : f \text{ continuous on } [0, 1]\}.$$

Then

$$\langle f, g \rangle = \int_0^1 f(t) \overline{g(t)} dt$$

is an inner product.

**Remark 10.9.** By using the following method, one may define a new inner product from a given one. Let  $U$  and  $V$  be vector spaces over  $\mathbb{K}$  and suppose  $\langle \cdot, \cdot \rangle$  is an inner product on  $U$ . If  $T : V \rightarrow U$  is an isomorphism, then

$$p_T(v, u) = \langle Tv, Tu \rangle : V \times V \rightarrow \mathbb{K}$$

*Remark 10.6 is continued here.*

is an inner product on  $V$ . The inner product shown in Remark 10.7 is a special case of this result.

**Example 10.10.** Let  $V$  be an  $n$ -dimensional vector space over  $\mathbb{K}$  and let

$$\beta = \{v_1, v_2, \dots, v_n\}$$

be an ordered basis for  $V$ . Then there exists a natural isomorphism  $\phi$  in between  $V$  and  $\mathbb{K}^n$  by the mapping

$$v_i \mapsto e_i$$

for each  $i \in \{1, 2, \dots, n\}$ , where  $e_i \in \{e_1, e_2, \dots, e_n\}$ , the standard ordered basis for  $\mathbb{K}^n$ . Then by the standard inner product on  $\mathbb{K}^n$  and the method described in Remark 10.9, one may define an inner product

$$p_\phi \left( \sum_i x_i v_i, \sum_j y_j v_j \right) = \sum_i x_i \bar{y}_i$$

for any  $x = \sum_i x_i v_i, y = \sum_j y_j v_j \in V$ . That is, for any ordered basis  $\beta = \{v_1, v_2, \dots, v_n\}$  for  $V$ , there exists an inner product  $\langle \cdot, \cdot \rangle$  on  $V$  such that

$$\langle v_i, v_j \rangle = \delta_{ij}$$

for all  $i, j \in \{1, 2, \dots, n\}$ .

**Example 10.11.** We take a look at Example 10.8 again. Let

$$V = \{f : \mathbb{C} \rightarrow \mathbb{C} : f \text{ continuous on } [0, 1]\}$$

and let  $T : V \rightarrow V$  be defined by the mapping

$$f(t) \mapsto tf(t).$$

It can be easily verified that  $T$  is linear. Moreover,  $T$  is invertible, since if  $Tf(t) = 0$ , then

$$\forall t \in [0, 1], tf(t) = 0,$$

which means

$$\forall t \in (0, 1], f(t) = 0.$$

But  $f$  is continuous, so  $f(0) = 0$ , or,  $f = 0$  on  $[0, 1]$ . Thus  $T$  is an isomorphism, and

$$p_T(f, g) = \langle Tf, Tg \rangle = \int_0^1 t^2 fg \, dt$$

is an inner product.

**Remark 10.12.** We now turn into some general observation about inner products on a complex vector space. Let  $V$  be a vector space over  $\mathbb{C}$  with an inner product  $\langle \cdot, \cdot \rangle$ . Then for all  $v, u \in V$ ,

$$\langle v, u \rangle = \operatorname{Re} \langle v, u \rangle + i \operatorname{Im} \langle v, u \rangle.$$

where  $\operatorname{Re} \langle v, u \rangle$  and  $\operatorname{Im} \langle v, u \rangle$  are the real and imaginary parts of  $\langle v, u \rangle$ , respectively. Observe that for any  $z \in \mathbb{C}$ ,

$$\operatorname{Im}(z) = \operatorname{Re}(-iz).$$

It follows that

$$\operatorname{Im} \langle v, u \rangle = \operatorname{Re}(-i \langle v, u \rangle) = \operatorname{Re} \langle v, -iu \rangle.$$

Thus the inner product  $\langle v, u \rangle$  is completely determined by its real part, such that

$$\langle v, u \rangle = \operatorname{Re} \langle v, u \rangle + i \operatorname{Re} \langle v, -iu \rangle.$$

**Remark 10.13.** Occasionally, it is very useful to know that an inner product  $\langle \cdot, \cdot \rangle$  on a vector space  $V$  is completely determined by the quadratic form associated with  $\langle \cdot, \cdot \rangle$ . The definition is similar to how we define a quadratic form associated with a bilinear form. However, for inner products, we utilize the following concept.

**Def'n. Norm on a Vector Space**

Let  $V$  be a vector space on  $\mathbb{K}$  and let  $\langle \cdot, \cdot \rangle$  be an inner product on  $V$ . We define the *norm* with respect to  $\langle \cdot, \cdot \rangle$  by

$$\|v\| = \sqrt{\langle v, v \rangle} : V \rightarrow \mathbb{K}.$$

*Remark 10.13 is continued here.*

By looking at the standard inner product on  $\mathbb{K}^n$  (in particular, when  $n \in \{1, 2, 3\}$ ), it should be convincing that the norm  $\|v\|$  of a vector  $v \in V$  is a generalization of length.

**Def'n. Quadratic Form of an Inner Product**

We define the quadratic form of an inner product  $\langle \cdot, \cdot \rangle$  on a vector space  $V$  by the mapping

$$v \mapsto \|v\|^2$$

for all  $v \in V$ , where  $\|\cdot\|$  is the norm with respect to  $\langle \cdot, \cdot \rangle$ .

*Remark 10.13 is continued here.*

It follows from the properties of inner product that

$$\|v \pm u\|^2 = \|v\|^2 \pm 2 \operatorname{Re} \langle v, u \rangle + \|u\|^2,$$

provided that  $v, u \in V$  and  $\|\cdot\|$  is the norm with respect to  $\langle \cdot, \cdot \rangle$ . When  $V$  is over  $\mathbb{R}$ ,

$$\langle v, u \rangle = \frac{1}{4} \|v + u\|^2 - \frac{1}{4} \|v - u\|^2.$$

When  $V$  is over  $\mathbb{C}$ , we get a more complicated result that

$$\langle v, u \rangle = \frac{1}{4} \|v + u\|^2 - \frac{1}{4} \|v - u\|^2 + \frac{i}{4} \|v + iu\|^2 - \frac{i}{4} \|v - iu\|^2 = \frac{1}{4} \sum_p i^p \|v + i^p u\|^2$$

The above equations are unsurprisingly called the polarization identities; observe that the equation when  $V$  is over  $\mathbb{R}$  is a special case of the polarization identity of bilinear forms, as discussed in Chapter 4.

**Remark 10.14.** The discussions so far apply to every vector space  $V$  over  $\mathbb{K}$ , regardless of the dimension. We now turn to the case when  $V$  is finite-dimensional. As one might guess, an inner product on a finite-dimensional vector space can be represented by a matrix with respect to an ordered basis for  $V$ . To show this, suppose  $V$  is finite-dimensional and let  $\beta = \{v_1, v_2, \dots, v_n\}$  be an ordered basis for  $V$ , where  $n = \dim(V)$ . Let  $\langle \cdot, \cdot \rangle$  be an inner product on  $V$ . Now the claim is that  $\langle \cdot, \cdot \rangle$  is completely determined by the scalars

$$g_{ij} = \langle v_i, v_j \rangle \in \mathbb{K},$$

where  $i, j \in \{1, 2, \dots, n\}$ . To verify this, let  $x = \sum_j x_j v_j, y = \sum_i y_i v_i \in V$  for some  $x_1, x_2, \dots, x_n, y_1, \dots, y_n \in \mathbb{K}$ . Then

$$\langle x, y \rangle = \left\langle \sum_j x_j v_j, y \right\rangle = \sum_j x_j \langle v_j, y \rangle = \sum_j x_j \sum_i \bar{y}_i \langle v_j, v_i \rangle = \sum_{i,j} \bar{y}_i g_{ij} x_j = Y^* G X,$$

where  $Y = [y]_\beta$  and  $X = [x]_\beta$ , and  $G \in M_{n \times n}(\mathbb{K})$  is defined by

$$G_{ij} = g_{ij}$$

for each  $i, j \in \{1, 2, \dots, n\}$ . This motivates the following definition.

**Def'n. Matrix of an Inner Product**

Let  $\langle \cdot, \cdot \rangle$  be an inner product on an  $n$ -dimensional vector space  $V$  over  $\mathbb{K}$  and let  $\beta$  be an ordered basis for  $V$ . If we define  $G \in M_{n \times n}(\mathbb{K})$  as described in Remark 10.14, then we call  $G$  the **matrix** of  $\langle \cdot, \cdot \rangle$ .

**Remark 10.15.** Suppose  $G \in M_{n \times n}(\mathbb{K})$  is a matrix of an inner product  $\langle \cdot, \cdot \rangle$  on a finite-dimensional vector space  $V$  over  $\mathbb{K}$ . Then by definition of the entries of  $G$ ,

$$G_{ij} = \langle v_j, v_i \rangle,$$

$G$  has the property that  $G = G^*$ .

**Def'n. Hermitian matrix**

Let  $G \in M_{n \times n}(\mathbb{K})$ . We say  $G$  is **Hermitian** if  $G = G^*$ .

*Remark 10.15 is continued here.*

However,  $G$  is a rather special kind of Hermitian matrix, that  $G$  satisfies

$$X^*GX > 0$$

for any nonzero  $X \in M_{n \times 1}(\mathbb{K})$ . In particular,  $G$  is invertible, since if  $G$  is singular, then there exists  $X \in M_{n \times 1}(\mathbb{K})$  such that  $GX = 0$ . More explicitly, the above inequality implies that for any nonzero  $x = (x_1, x_2, \dots, x_n) \in \mathbb{K}^n$ ,

$$\sum_{i,j} \bar{x}_i G_{ij} x_j > 0.$$

An immediate consequence of this result is that the diagonal entries are positive,

$$G_{ii} > 0$$

for all  $i \in \{1, 2, \dots, n\}$ . However, this condition solely does not guarantee

$$X^*GX > 0$$

for all  $X \in M_{n \times 1}(\mathbb{K})$ . Sufficient conditions on  $G$  such that the above inequality holds will be provided later.

## Inner Product Spaces

**Def'n. Inner Product Space, Euclidean Space, Unitary Space**

Let  $V$  be a vector space over  $\mathbb{K}$  and let  $\langle \cdot, \cdot \rangle$  be an inner product on  $V$ . Then  $(V, \langle \cdot, \cdot \rangle)$  is called an **inner product space**. In particular, in case of  $V = \mathbb{K}^n$  for some  $n \in \mathbb{N}$ , we say  $(\mathbb{K}^n, \langle \cdot, \cdot \rangle)$  is an **Euclidean space** if  $\mathbb{K} = \mathbb{R}$  and a **unitary space** if  $\mathbb{K} = \mathbb{C}$ .

**Theorem 10.1.**  
**Properties of the**  
**Associated Norm on**  
**an Inner Product**  
**Space**

*Let  $(V, \langle \cdot, \cdot \rangle)$  be an inner product space over  $\mathbb{K}$  and let  $\|\cdot\|$  be the norm associated with  $\langle \cdot, \cdot \rangle$ . Then the following holds. Suppose  $v, u \in V$  and  $c \in \mathbb{K}$  are arbitrary.*

- (a)  $\|cv\| = |c| \|v\|$ .
- (b)  $\|v\| > 0$  if  $v \neq 0$ .
- (c)  $|\langle v, u \rangle| \leq \|v\| \|u\|$ .
- (d)  $\|v + u\| \leq \|v\| + \|u\|$ .

*Proof.* Notice that (a) and (b) immediately follow from the definition of an inner product. To verify (c), first fix  $u \in V$  without loss of generality. Since the result is trivially valid when  $v = 0$ , suppose  $v \neq 0$ . Let

$$w = u - \frac{\langle u, v \rangle}{\|v\|^2} v,$$

then  $\langle w, v \rangle = 0$  and

$$0 \leq \|w\|^2 = \left\langle u - \frac{\langle u, v \rangle}{\|v\|^2} v, u - \frac{\langle u, v \rangle}{\|v\|^2} v \right\rangle = \langle u, u \rangle - \frac{\langle u, v \rangle \langle v, u \rangle}{\|v\|^2} = \|u\|^2 - \frac{|\langle v, u \rangle|^2}{\|v\|^2},$$

rearranging which gives

$$|\langle v, u \rangle| \leq \|v\| \|u\|.$$

Now, using the inequality above, we find

$$\begin{aligned} \|v + u\|^2 &= \|v\|^2 + \langle v, u \rangle + \langle u, v \rangle + \|u\|^2 = \|v\|^2 + \operatorname{Re} \langle v, u \rangle + \|u\|^2 \\ &\leq \|v\|^2 + 2\|v\| \|u\| + \|u\|^2 = (\|v\| + \|u\|)^2. \end{aligned}$$

Thus

$$\|v + u\| \leq \|v\| + \|u\|,$$

as desired. 

### Def'n. Cauchy-Schwarz Inequality

The inequality

$$|\langle v, u \rangle| \leq \|v\| \|u\|$$

from (c) of Theorem 10.1 is known as the **Cauchy-Schwarz inequality**.

**Remark 10.16.** The proof of the Cauchy-Schwarz inequality shows that, when  $v, u \neq 0$ , then the strict inequality

$$|\langle v, u \rangle| < \|v\| \|u\|$$

applies unless

$$u = \frac{\langle v, u \rangle}{\|v\|^2} v.$$

In other words, the equality occurs if and only if  $v$  and  $u$  are linearly dependent.

### Def'n. Orthogonal Vectors

Let  $V$  be an inner product space. We say  $v, u \in V$  are **orthogonal** with respect to  $\langle \cdot, \cdot \rangle$  if  $\langle v, u \rangle = 0$ .

### Def'n. Orthogonal, Orthonormal Set

Let  $V$  be an inner product space. We say a subset  $S \subseteq V$  is **orthogonal** if every pair of vectors in  $S$  are orthogonal. That is,

$$\forall v, u \in S [\langle v, u \rangle = 0].$$

If  $S$  has an additional property that every vector has the unit norm,

$$\forall v \in S [\langle v, v \rangle = \|v\|^2 = \|v\| = 1],$$

we say  $S$  is **orthonormal**.

**Example 10.17.** For any inner product space,  $0 \in V$  is the unique vector orthogonal to every  $v \in V$ .

**Example 10.18.** The standard ordered basis for  $\mathbb{K}^n$  is an orthonormal set.

**Example 10.19.** Let  $\langle \cdot, \cdot \rangle$  be the inner product described in Remark 10.8, and let

$$\beta = \left\{ E^{pq} \in M_{n \times n}(\mathbb{C}) : E_{ij}^{pq} = \begin{cases} 1 & \text{if } i = p \wedge j = q \\ 0 & \text{otherwise} \end{cases} \right\}.$$

Then  $\beta$  is an orthonormal set with respect to  $\langle \cdot, \cdot \rangle$ . For, if  $p, q, r, s \in \{1, 2, \dots, n\}$ , then

$$\langle E^{pq}, E^{rs} \rangle = \text{tr}(E^{pq} E^{rs*}) = \text{tr}(E^{pq} E^{sr}) = \delta_{qs} \delta_{pr}.$$

**Remark 10.20.** The two examples of orthogonal sets above are linearly independent. We show that this is true for all orthogonal sets containing nonzero elements.

**Theorem 10.2.**  
**Orthogonality Implies**  
**Linear Independence**

*Let  $V$  be an inner product space and let  $S \subseteq V$  be orthogonal such that every  $v \in S$  is nonzero. Then  $S$  is linearly independent.*

*Proof.* Let  $v_1, v_2, \dots, v_n \in S$  for some  $n \in \mathbb{N}$  be arbitrary and let

$$v = \sum_{i=1}^n c_i v_i$$

for some  $c_1, c_2, \dots, c_n \in \mathbb{K}$ . Then for all  $k \in \{1, 2, \dots, n\}$ ,

$$\langle v, v_k \rangle = \left\langle \sum_{i=1}^n c_i v_i, v_k \right\rangle = \sum_{i=1}^n c_i \langle v_i, v_k \rangle = c_k \langle v_k, v_k \rangle.$$

Therefore,

$$c_k = \frac{\langle v, v_k \rangle}{\|v_k\|^2},$$

which means that, if  $v = 0$ , then  $c_1 = c_2 = \dots = c_n = 0$ , verifying the linear independence of  $\{v_1, v_2, \dots, v_n\} \in S$ . Since we have shown that every finite subset of  $S$  is linearly independent,  $S$  is linearly independent. ♠

**Corollary 10.2.1.**

*Let  $V$  and  $S$  be define as Theorem 10.2 and let  $v_1, v_2, \dots, v_n \in S$ . If  $v \in V$  is a linear combination of  $v_1, v_2, \dots, v_n$  then*

$$v = \sum_{i=1}^n \frac{\langle v, v_i \rangle}{\|v_i\|^2} v_i.$$

**Corollary 10.2.2.**

*Let  $V$  be a finite-dimensional inner product space and let  $\{v_1, v_2, \dots, v_k\} \subseteq V$  be diagonal. Then  $\dim(V) \leq k$ .*

**Remark 10.21.** One possible - and geometrically important - interpretation of Corollary 10.2.2 is that the number of mutually perpendicular directions of an inner product space does not exceed the dimension of the space. Also, it is intuitive to think that the maximum number of mutually perpendicular direction is the dimension of the space; however, we only know that it cannot exceed the dimension of the space so far. It is a particular corollary to the upcoming theorem.

**Theorem 10.3.**  
**Gram-Schmidt**  
**Orthogonalization**  
**Process**

Let  $V$  be an inner product space. Then for any linearly independent

$$\beta = \{v_1, v_2, \dots, v_n\} \subseteq V,$$

there exists an orthogonal set

$$\alpha = \{u_1, u_2, \dots, u_n\} \subseteq V$$

such that  $\{u_1, u_2, \dots, u_k\}$  is a basis for  $\text{span}\{v_1, v_2, \dots, v_k\}$  for any  $k \in \{1, 2, \dots, n\}$ .

*Proof.* Fix  $n \in \mathbb{N}$ . We proceed inductively to construct vectors  $u_1, u_2, \dots, u_n$ . Clearly  $\{u_1\} = \{v_1\}$  is an orthogonal set which spans  $\text{span}\{v_1\}$ . Now suppose that, for some  $m \in \mathbb{N}$ ,  $\{u_1, u_2, \dots, u_m\}$  is orthogonal and such that

$$\text{span}\{u_1, u_2, \dots, u_k\} = \text{span}\{v_1, v_2, \dots, v_k\}$$

for all  $k \in \{1, 2, \dots, m\}$ . Then define

$$u_{m+1} = v_{m+1} - \sum_{i=1}^m \frac{\langle v_{m+1}, u_i \rangle}{\|u_i\|^2} u_i.$$

We claim that  $\{u_1, u_2, \dots, u_{m+1}\}$  is a basis for  $\{v_1, v_2, \dots, v_{m+1}\}$ . To verify this, first notice that  $u_{m+1} \neq 0$ , since

$$\text{span}\{u_1, u_2, \dots, u_m\} = \text{span}(\beta \setminus \{v_{m+1}\})$$

and  $\beta$  is linearly independent. Moreover, for any  $j \in \{1, 2, \dots, m\}$ ,

$$\begin{aligned} \langle v_{m+1}, u_j \rangle &= \left\langle v_{m+1} - \sum_{i=1}^m \frac{\langle v_{m+1}, u_i \rangle}{\|u_i\|^2} u_i, u_j \right\rangle \\ &= \langle v_{m+1}, u_j \rangle - \sum_{i=1}^m \frac{\langle v_{m+1}, u_i \rangle}{\|u_i\|^2} \langle u_i, u_j \rangle = \langle v_{m+1}, u_j \rangle - \frac{\langle v_{m+1}, u_j \rangle}{\|u_j\|^2} \langle u_j, u_j \rangle = 0, \end{aligned}$$

so  $u_{m+1}$  is orthogonal to every  $v_i \in \{u_1, u_2, \dots, u_m\}$ . Thus

$$\{u_1, u_2, \dots, u_{m+1}\}$$

is an orthogonal set containing  $m+1$  vectors, so by Theorem 10.2, is a basis for  $\text{span}\{v_1, v_2, \dots, v_{m+1}\}$ . Thus by induction we have the desired result. ♠

**Corollary 10.3.1.**  
**Existence of**  
**Orthonormal Basis**

Every finite-dimensional inner product space has an orthonormal basis.

*Proof.* Let  $\{v_1, v_2, \dots, v_n\}$  be a basis for  $V$ , and  $n$ -dimensional inner product space over  $\mathbb{K}$ . Then by Theorem 10.3, one may construct an orthogonal set

$$\{u_1, u_2, \dots, u_n\} \subseteq V.$$

Then,

$$\left\{ \frac{u_1}{\|u_1\|}, \frac{u_2}{\|u_2\|}, \dots, \frac{u_n}{\|u_n\|} \right\}$$

is an orthonormal basis for  $V$ , as required. ♠

**Remark 10.22.** One of the main advantages of orthonormal basis is that computations involving coordinates are simpler. To demonstrate this, suppose  $V$  is a finite-dimensional inner product space, and let

Since the inner product of an inner product space is fixed, we may proceed in the reverse direction of Remark 10.14.

$\{v_1, v_2, \dots, v_n\}$  be an ordered basis for an inner product space  $V$  over  $\mathbb{K}$ . Then we may associate a matrix  $G$  with  $\beta$  by

$$G_{ij} = \langle v_j, v_i \rangle.$$

In particular, when  $\beta$  is orthonormal,

$$G_{ij} = \langle v_j, v_i \rangle = \delta_{ji},$$

which means  $G = I$ , the identity matrix. So by using an orthonormal basis, we may treat the inner product  $\langle \cdot, \cdot \rangle$  on  $V$  as the standard inner product on  $\mathbb{K}^n$ .

**Remark 10.23.** It is interesting to note that the Gram-Schmidt process can be used to determine linear independence. To show this, suppose  $v_1, v_2, \dots, v_n \in V$  are linearly dependent, where  $V$  is an inner product space over  $\mathbb{K}$ . To make the case nontrivial, suppose that  $v_1 \neq 0$ . Let  $m \in \mathbb{N}$  be the greatest integer such that  $v_1, v_2, \dots, v_m$  are linearly independent. Then it is clear from the construction that  $u_{m+1} = 0$ , since  $v_{m+1} \in \text{span}\{v_1, v_2, \dots, v_m\}$  and so

$$u_{m+1} \in \text{span}\{v_1, v_2, \dots, v_{m+1}\} = \text{span}\{v_1, v_2, \dots, v_m\} = \text{span}\{u_1, u_2, \dots, u_m\}.$$

But, this means  $u_{m+1}$  is orthogonal to every  $v \in \text{span}\{u_1, u_2, \dots, u_m\}$ , and as we mentioned in Example 10.17, 0 is the unique vector with this property.

**Remark 10.24.** In essence, the Gram-Schmidt process consists of a basic geometric operation called orthogonal projection, and it is best understood from this point of view. The method of orthogonal projection also arises naturally in the solution of an important approximation problem, which is described as follows. Let  $V$  be an inner product space and let  $W \subseteq V$  be a subspace. The problem is to find the best possible approximation  $w \in W$  for any  $v \in V$ . That is,

$$\forall u \in W \quad [\|v - w\| \leq \|v - u\|].$$

By looking at this problem in  $\mathbb{R}^2$  or in  $\mathbb{R}^3$ , it is intuitive to conclude that a  $w \in W$  such that  $v - w$  is perpendicular to every vector in  $W$  is the best approximation, and there is a unique such  $w \in W$ . Although this conclusion is valid for any finite-dimensional inner product space, it is not valid for some infinite-dimensional case. Since the precise situation is too complicated, we shall only prove the following.

#### Theorem 10.4. Orthogonal Approximation

Let  $V$  be an inner product space and let  $W \subseteq V$  be a subspace. Let  $v \in V$  be arbitrary. Then the following hold.

- (a)  $w \in W$  is a best approximation to  $v$  on  $W$  if and only if  $v - w$  is orthogonal to every  $u \in W$ .
- (b) If a best approximation  $w \in W$  of  $v$  exists, then it is unique.
- (c) If  $V$  is finite-dimensional and if  $\beta = \{w_1, w_2, \dots, w_n\}$  is any orthonormal basis for  $W$ , then

$$w = \sum_i \frac{\langle v, w_i \rangle}{\|w_i\|^2} w_i$$

is the best approximation of  $v$  by vectors in  $W$ .

*Proof.* For the reverse direction of (a), suppose that  $v - w$  is orthogonal to  $W$ , and let  $u \in W$ . Then  $v - u = (v - w) + (w - u)$  and

$$\|v - u\|^2 = \|v - w\|^2 + 2\text{Re} \langle v - w, w - u \rangle + \|w - u\|^2,$$



where the equality occurs if and only if  $w = u$ . For the forward direction, suppose that

$$\|v - w\| \leq \|v - u\|$$

for all  $u \in W$ . Then we claim that

$$2\operatorname{Re}\langle v - w, y \rangle + \|y\|^2 \geq 0$$

for any  $y \in W$ . This can be verified by observing that any  $y \in W$  can be written as  $w - u$  for some  $u \in W$  and by using

$$\|v - u\|^2 = \|v - w\|^2 + 2\operatorname{Re}\langle v - w, w - u \rangle + \|w - u\|^2.$$

In particular, if  $w \neq u$ , let

$$y = -\frac{\langle v - w, w - u \rangle}{\|w - u\|^2}(w - u).$$

Then the inequality becomes

$$\begin{aligned} & 2\operatorname{Re}\left\langle v - w, -\frac{\langle v - w, w - u \rangle}{\|w - u\|^2}(w - u) \right\rangle + \left\| -\frac{\langle v - w, w - u \rangle}{\|w - u\|^2}(w - u) \right\|^2 \\ &= 2\operatorname{Re}\left( -\frac{\overline{\langle v - w, w - u \rangle}}{\|w - u\|^2} \langle v - w, w - u \rangle \right) + \left| \frac{\langle v - w, w - u \rangle}{\|w - u\|^2} \right|^2 \|w - u\|^2 \\ &= -2\frac{|\langle v - w, w - u \rangle|^2}{\|w - u\|^2} + \frac{|\langle v - w, w - u \rangle|^2}{\|w - u\|^2} \geq 0, \end{aligned}$$

which is true if and only if  $\langle v - w, w - u \rangle = 0$  for all  $w - u \in W$ . For (b), suppose  $w_1, w_2 \in W$  are best approximations to  $v \in V$  on  $W$ . Write

$$v - w_1 = (v - w_2) + (w_2 - w_1).$$

Then,

$$\|v - w_1\| \leq \|v - w_2\| + \|w_2 - w_1\|.$$

But by symmetry,

$$\|v - w_2\| \leq \|v - w_1\| + \|w_1 - w_2\|,$$

where  $\|w_1 - w_2\| = \|w_2 - w_1\|$ . Thus we conclude

$$\|w_1 - w_2\| = \|w_2 - w_1\| = 0,$$

or  $w_1 = w_2$ . For (c), let  $k \in \{1, 2, \dots, n\}$ . Then

$$\langle v - w, w_k \rangle = \left\langle v - \sum_i \frac{\langle v, w_i \rangle}{\|w_i\|^2} w_i, w_k \right\rangle = \langle v, w_k \rangle - \sum_i \frac{\langle v, w_i \rangle}{\|w_i\|^2} \langle w_i, w_k \rangle = \langle v, w_k \rangle - \langle v, w_k \rangle = 0.$$

The uniqueness is provided by (b). ♠

### Def'n. Orthogonal Complement

Let  $V$  be an inner product space and let  $S \subseteq V$  be a subset. We say  $S_\perp \subseteq V$  is an *orthogonal complement* to  $S$  if

$$\forall s_\perp \forall s \in S [\langle s_\perp, s \rangle = 0].$$

**Remark 10.25.** For any inner product space  $V$ ,  $V_\perp = \{0\}$  and, conversely,  $\{0\}_\perp = V$ . Moreover, if  $S \subseteq V$ , then  $S_\perp$  is a subspace of  $V$ , since  $0 \in S_\perp$  and whenever  $v, u \in S_\perp$  and  $c \in \mathbb{K}$ ,

$$\langle cv + u, w \rangle = c\langle v, w \rangle + \langle u, w \rangle = 0$$

for any  $w \in V$ . In Theorem 10.4, the property which characterizes the best approximation  $w \in W$  of  $v \in V$  on  $W$  is that  $w$  is the unique vector in  $W$  such that  $v - w \in W_\perp$ .

**Def'n. Orthogonal Projection** of a Vector on a Subspace

Let  $V$  be an inner product space and let  $v \in V$ . If the best approximation  $w \in W$  of  $v$  on  $W$  exists, then we say  $w$  is the *orthogonal projection* of  $v$  on  $W$ .

**Def'n. Orthogonal Projection** of an Inner Product Space on a Subspace

Let  $V$  be an inner product space. If for all  $v \in V$  there exists  $w \in W$  such that  $w$  is the orthogonal projection of  $v$ , then we call the unique function  $P : V \rightarrow V$  defined by the mapping

$$v \mapsto w$$

the *orthogonal projection* of  $V$  on  $W$ .

**Remark 10.26.** By Theorem 10.4, the orthogonal projection of  $V$  on  $W$  always exists when  $V$  is a finite-dimensional inner product space and  $W \subseteq V$ . But Theorem 10.4 also provides the following result.

**Corollary 10.4.1.**

*Let  $V$  be an inner product space and let  $W \subseteq V$  be a finite-dimensional subspace. Let  $P : V \rightarrow V$  be the orthogonal projection of  $V$  on  $W$ . Then the mapping*

$$v \mapsto v - Pv$$

*defines the orthogonal projection of  $V$  on  $W^\perp$ .*

*Proof.* Let  $v \in V$  be arbitrary. Then it is clear that

$$v - Pv \in W^\perp$$

from the definition of orthogonal projection. To verify that  $v - Pv$  is the best approximation of  $v$  on  $W^\perp$ , let  $w_\perp \in W^\perp$  be arbitrary. Then

$$\begin{aligned} \|v - w_\perp\|^2 &= \langle v - w_\perp, v - w_\perp \rangle = \langle (v - w_\perp - Pv) + Pv, (v - w_\perp - Pv) + Pv \rangle \\ &= \|v - w_\perp - Pv\|^2 + \langle v - w_\perp - Pv, Pv \rangle + \langle Pv, v - w_\perp - Pv \rangle + \|Pv\|^2 \\ &= \|v - w_\perp - Pv\|^2 + \|Pv\|^2 \geq \|Pv\|^2 = \|v - (v - Pv)\|^2, \end{aligned}$$

where the equality holds if and only if  $w_\perp = v - Pv$ . Thus  $v - Pv$  is the best approximation of  $v$  on  $W^\perp$ , as desired. ♠

**Remark 10.27.** We now proceed to prove some properties of the orthogonal projection.

**Def'n. Idempotent** Linear Operator

Let  $V$  be a vector space and let  $T : V \rightarrow V$  be a linear operator. We say  $T$  is *idempotent* if  $T^n = T$  for all  $n \in \mathbb{N}$ .

**Proposition 10.5.**  
**Properties of**  
**Orthogonal**  
**Projection**

*Let  $W \subseteq V$  be a subspace of an inner product space  $V$  and let  $P : V \rightarrow V$  be the orthogonal projection of  $V$  on  $W$ . Then the following holds.*

- (a)  *$P$  is an idempotent linear operator.*
- (b)  *$\text{image}(P) = W$  and  $\ker(P) = W^\perp$ .*
- (c)  *$V = W \oplus W^\perp$ .*

*Proof.* To prove linearity, let  $v, u \in V$  and  $c \in \mathbb{K}$  be arbitrary. Then

$$cPv + Pu = c \sum_i \frac{\langle v, w_i \rangle}{\|w_i\|^2} w_i + \sum_i \frac{\langle u, w_i \rangle}{\|w_i\|^2} w_i = \sum_i \frac{c\langle v, w_i \rangle + \langle u, w_i \rangle}{\|w_i\|^2} w_i = \sum_i \frac{\langle cv + u, w_i \rangle}{\|w_i\|^2} w_i = P(cv + u)$$

by Theorem 10.4, provided that  $\{w_1, w_2, \dots, w_n\}$  is an orthonormal basis for  $W$ . To prove that  $P$  is idempotent, first notice that  $\text{image}(P) = W$  by definition. Then, for any  $w \in W$ , it is clear that  $w$  is the best approximation. To see this algebraically, notice that

$$P \sum_j c_j w_j = \sum_i \frac{\langle \sum_j c_j w_j, w_i \rangle}{\|w_i\|^2} w_i = \sum_i \frac{\sum_j c_j \langle w_j, w_i \rangle}{\|w_i\|^2} w_i = \sum_i \frac{c_i \langle w_i, w_i \rangle}{\|w_i\|^2} w_i = \sum_i c_i w_i$$

for any  $c_1, c_2, \dots, c_n \in \mathbb{K}$ . To show that  $\ker(P) = W_\perp$ , suppose  $Pv = 0$ . Since  $v - Pv \in W_\perp$  by definition, it follows that  $v \in W_\perp$ . Conversely, if  $v \in W_\perp$ , then

$$\langle v, w_i \rangle = 0$$

for all  $i \in \{1, 2, \dots, n\}$ , so  $Pv = 0$  and  $v \in \ker(P)$ . The direct sum

$$V = W \oplus W_\perp$$

follows from the fact that  $v = Pv + (v - Pv)$  for any  $v \in V$  and that  $W \cap W_\perp = \{0\}$ . ♠

### Corollary 10.5.1.

*Assume the conditions of Proposition 10.5. Then  $I - P : V \rightarrow V$  is the orthogonal projection of  $V$  on  $W_\perp$ . Moreover,  $I - P$  is idempotent and  $\ker(I - P) = W$ .*

*Proof.* The first part of this corollary is supplied by Corollary 10.4.1. To show that  $I - P$  is idempotent, notice that

$$(I - P)^2 = I^2 - 2P + P^2 = I - P,$$

since  $P$  is idempotent. The result  $\ker(I - P) = W$  easily follows from the fact that  $(I - P)v = 0$  if and only if  $v = Pv$ , which exactly means  $v \in W$ . ♠

**Remark 10.28.** The Gram-Schmidt process can now be described geometrically in the following way. Given an inner product space  $V$  and  $v_1, v_2, \dots, v_n \in V$ , let  $P_k$  be the orthogonal projection of  $V$  on the orthogonal complement of the subspace  $\text{span}\{v_1, v_2, \dots, v_{k-1}\} \subseteq V$  for each  $k \in \{2, 3, \dots, n+1\}$  and let  $P_1 = I$ . Then the vectors  $u_1, u_2, \dots, u_n \in V$  one obtains from the orthogonalization process is defined by

$$u_i = P_i v_i$$

for each  $i \in \{1, 2, \dots, n\}$ .

### Corollary 10.5.2. Bessel's Inequality

*Let  $V$  be an inner product space and let  $\{v_1, v_2, \dots, v_n\} \subseteq V$  be an orthogonal set of nonzero vectors. Then for any  $v \in V$ ,*

$$\sum_i \frac{|\langle v, v_i \rangle|^2}{\|v_i\|^2} \leq \|v\|^2$$

*and the equality holds if and only if*

$$v = \sum_i \frac{\langle v, v_i \rangle}{\|v_i\|^2} v_i.$$

*Proof.* Let

$$w = \sum_i \frac{\langle v, v_i \rangle}{\|v_i\|^2} v_i,$$

the orthogonal projection of  $v$  on  $W = \text{span}\{v_1, v_2, \dots, v_n\}$ . Then

$$v = w + w_\perp$$

for some  $w_\perp \in W_\perp$ , where  $W_\perp$  is the orthogonal complement of  $W$ . So,

$$\|v\| = \|w\| + \|w_\perp\| = \sum_i \frac{|\langle v, v_i \rangle|^2}{\|v_i\|^2} + \|w_\perp\|$$

which proves the inequality. In particular, the equality

$$\|v\| = \sum_i \frac{|\langle v, v_i \rangle|^2}{\|v_i\|^2}$$

occurs if and only if  $w_\perp = 0$ . But this exactly means

$$v = \sum_i \frac{\langle v, v_i \rangle}{\|v_i\|^2} v_i. \quad \spadesuit$$

**Remark 10.29.** In the special case which  $\{v_1, v_2, \dots, v_n\} \subseteq V$  is an orthonormal set of an inner product space  $V$ , Bessel's inequality can be written as

$$\sum_i |\langle v, v_i \rangle|^2 \leq \|v\|^2$$

for any  $v \in V$ , and that  $v \in \text{span}\{v_1, v_2, \dots, v_n\}$  if and only if

$$v = \sum_i \langle v, v_i \rangle v_i.$$

In particular, if  $V$  is finite-dimensional, and  $\beta = \{v_1, v_2, \dots, v_n\}$  is an orthonormal basis for  $V$ , then the above equation implies that

$$([v]_\beta)_i = \langle v, v_i \rangle.$$

## Linear Functionals and Adjoint

**Remark 10.30.** We proceed to discuss linear functionals in an inner product space  $(V, \langle \cdot, \cdot \rangle)$ . In particular, what we will discover is that any linear functional  $f : V \rightarrow \mathbb{K}$  can be defined by

$$v \mapsto \langle v, u \rangle$$

for some fixed  $u \in V$ , provided that  $V$  is finite-dimensional. We then use this result to prove that for all linear operator  $T : V \rightarrow V$  there exists a unique linear operator  $T^* : V \rightarrow V$  such that

$$\langle Tv, u \rangle = \langle v, T^*u \rangle.$$

This *adjoint* operations on linear operators  $T$  and  $T^*$  is identified with the operation of forming the conjugate transpose of a matrix.

**Theorem 10.6.**  
**Linear Functional Is**  
**an Inner Product with**  
**a Fixed Argument**

Let  $V$  be a finite-dimensional inner product space, and let  $f : V \rightarrow \mathbb{K}$  be a linear functional. Then there exists a unique  $u \in V$  such that

$$\forall v \in V [f(v) = \langle v, u \rangle].$$

*Proof.* Let  $\{v_1, v_2, \dots, v_n\}$  be an orthonormal basis for  $V$  and let

$$u = \sum_i \overline{f(v_i)} v_i.$$

Define  $f_u : V \rightarrow \mathbb{K}$  by

$$v \mapsto \langle v, u \rangle.$$

Then,

$$f_u(v_i) = \left\langle v_i, \sum_j \overline{f(v_j)} v_j \right\rangle f(v_i)$$

for all  $i \in \{1, 2, \dots, n\}$ , which means

$$f(v) = f_u(v) = \langle v, u \rangle$$

for all  $v \in V$ . To verify the uniqueness, suppose there exists  $w \in W$  such that

$$f(v) = \langle v, w \rangle$$

for all  $v \in V$ . In particular,  $\langle v, w \rangle = \langle v, u \rangle$  for any  $v \in V$ , and so

$$\langle u - w, u - w \rangle = (\langle u, u \rangle - \langle u, w \rangle) + (\langle w, w \rangle - \langle w, u \rangle) = 0,$$

which exactly means  $u = w$ , as desired. ♠

**Remark 10.31.** Here is another proof of Theorem 10.6 in terms of the representation of a linear functional in an ordered basis. For any  $x = \sum_i x_i v_i, y = \sum_j y_j v_j \in V$ , we have

$$\langle x, y \rangle = \sum_i x_i \overline{y_i}$$

by Remark 10.22. Since any linear functional  $f : V \rightarrow \mathbb{K}$  is of the form

$$f(x) = \sum_i c_i v_i$$

for some  $c_1, c_2, \dots, c_n \in \mathbb{K}$  determined by the basis. That is,

$$c_i = f(v_i)$$

for all  $i \in \{1, 2, \dots, n\}$ . So we may find  $y \in V$  such that  $f(x) = \langle x, y \rangle$  by observing that  $\overline{y_i} = c_i$ , or,

$$\overline{f(v_i)} = y_i$$

for all  $i \in \{1, 2, \dots, n\}$ . Thus we find

$$y = \sum_i \overline{f(v_i)} v_i$$

satisfies  $f(x) = \langle x, y \rangle$  for all  $x \in V$ .

**Remark 10.32.** The proof of Theorem 10.6 fails to emphasize the essential geometric fact that  $u \in V$  such that  $f(v) = \langle v, u \rangle$  for all  $v \in V$  is an element of the orthogonal complement of the null space of  $f$ . To show this, let  $W = \ker(f)$  and let  $W_\perp$  be the orthogonal complement of  $W$ . Now the claim is that

$$f(v) = f(Pv)$$

for all  $v \in V$ , where  $P : V \rightarrow V$  is the orthogonal projection of  $V$  on  $W$ . To verify this, first observe that  $V = W \oplus W_\perp$ , since if  $\{w_1, w_2, \dots, w_k\}$  is an orthogonal basis for  $W$ , then we may choose  $v_{k+1}, v_{k+2}, \dots, v_n \in V$  such that  $\{w_1, w_2, \dots, w_k, v_{k+1}, \dots, v_n\}$  is a basis for  $V$ . Then by the Gram-Schmidt process, we may find  $w_{k+1}, w_{k+2}, \dots, w_n \in W_\perp$  such that  $\{w_1, w_2, \dots, w_n\}$  is an orthogonal basis for  $V$ . It follows that  $\{w_{k+1}, w_{k+2}, \dots, w_n\}$  is a basis for  $W_\perp$ , and

$$W \oplus W_\perp = V,$$

as claimed. That is, for any

$$v = \sum_{i=1}^n c_i w_i \in V$$

we have

$$f(v) = f\left(\sum_{i=1}^n c_i w_i\right) = \sum_{i=1}^n c_i f(w_i) = \sum_{i=k+1}^n c_i f(w_i) = f\left(\sum_{i=k+1}^n c_i w_i\right) = f(Pv).$$

Moreover,

$$\dim(W_\perp) = \dim(V) - \dim(W) = \dim(V) - \text{nullity}(f) = \text{rank}(f) = \dim(\mathbb{K}) = 1,$$

if we suppose that  $f$  is nonzero. So any nonzero  $w_\perp \in W_\perp$  satisfies

$$Pv = \frac{\langle v, w_\perp \rangle}{\|w_\perp\|^2} w_\perp$$

for all  $v \in V$  by (c) of Theorem 10.4. Thus, for any  $v \in V$ ,

$$f(v) = f(Pv) = f\left(\frac{\langle v, w_\perp \rangle}{\|w_\perp\|^2} w_\perp\right) = \frac{\langle v, w_\perp \rangle}{\|w_\perp\|^2} f(w_\perp) = \langle v, w_\perp \rangle \frac{f(w_\perp)}{\|w_\perp\|^2},$$

and thus

$$u = \frac{\overline{f(w_\perp)} w_\perp}{\|w_\perp\|}$$

is the unique vector in  $V$  such that  $f(v) = \langle v, u \rangle$  for all  $v \in V$  by Remark 10.31.

**Remark 10.33.** We now turn to the concept of the adjoint of a linear operator.

**Theorem 10.7.**  
**Existence and**  
**Uniqueness of**  
**Adjoint**

*Let  $V$  be a finite-dimensional inner product space. Then for any linear operator  $T : V \rightarrow V$  there exists a unique linear operator  $T^* : V \rightarrow V$  such that*

$$\langle Tv, u \rangle = \langle v, T^*u \rangle$$

*for all  $v, u \in V$ .*

*Proof.* Consider the mapping

$$v \mapsto \langle Tv, u \rangle$$

which defines a linear functional  $f : V \rightarrow \mathbb{K}$ . Then Theorem 10.6 provides a unique  $w \in V$  such that

$$f(v) = \langle Tv, u \rangle = \langle v, w \rangle.$$

That is, if  $T^* : V \rightarrow V$  is a function defined by

$$u \mapsto w$$

for all  $u \in V$ ,  $\langle Tv, u \rangle = \langle u, T^* \rangle$  for all  $v, u \in V$ . To show that the constructed  $T^*$  is linear, let  $x, y \in V$  and  $c \in \mathbb{K}$  be arbitrary. Then

$$\langle v, T^*(cx + y) \rangle = \langle Tv, cx + y \rangle = \bar{c} \langle Tv, x \rangle + \langle Tv, y \rangle = \langle v, T^*x \rangle + \langle v, T^*y \rangle = \langle v, cT^*x + T^*y \rangle$$

for all  $v \in V$ . Thus  $T^*(cx + y) = cT^*(x) + T^*(y)$ . The uniqueness of  $T^*$  easily follows from Theorem 10.6 and the above construction. ♠

**Proposition 10.8.**  
Matrix  
Representation of a  
Linear Operator in an  
Orthogonal Basis

Let  $V$  be a finite-dimensional inner product space and let  $\beta = \{v_1, v_2, \dots, v_n\}$  be an orthonormal ordered basis. Then for any linear operator  $T : V \rightarrow V$ ,

$$([T]_\beta)_{ij} = \langle Tv_j, v_i \rangle.$$

*Proof.* Since  $\beta$  is an orthonormal basis, we have

$$v = \sum_i \langle v, v_i \rangle v_i$$

for any  $v \in V$  by Remark 10.29. So

$$Tv_j = \sum_i \langle Tv_j, v_i \rangle v_i = \sum_i ([T]_\beta)_{ij} v_i,$$

where the second equality holds by the definition of the matrix representation of a linear operator. ♠

**Corollary 10.8.1.**

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a linear operator. Then for any orthonormal ordered basis  $\beta$  for  $V$ ,

$$[T]_\beta^* = [T^*]_\beta.$$

*Proof.* By Proposition 10.8,

$$\begin{cases} ([T]_\beta)_{ij} &= \langle Tv_j, v_i \rangle \\ ([T^*]_\beta)_{ij} &= \langle T^*v_j, v_i \rangle \end{cases},$$

provided that  $\beta = \{v_1, v_2, \dots, v_n\}$ . But by definition,

$$\overline{([T]_\beta)} = \overline{\langle Tv_j, v_i \rangle} = \overline{\langle v_j, T^*v_i \rangle} = \langle T^*v_i, v_j \rangle = ([T^*]_\beta)_{ij},$$

which exactly means  $[T]_\beta^* = [T^*]_\beta$ . ♠

**Def'n. Adjoint of a Linear Operator**

Let  $V$  be an inner product space and let  $T : V \rightarrow V$  be a linear operator. If there exists a linear operator  $T^* : V \rightarrow V$  such that

$$\langle Tv, u \rangle = \langle v, T^*u \rangle$$

for all  $v, u \in V$ , then we call  $T^*$  the **adjoint** of  $T$ .

**Remark 10.34.** By Theorem 10.7, any linear operator on a finite-dimensional inner product space has a unique adjoint. In an infinite-dimensional case, some linear operator does not have an adjoint. But in any case, there is at most one adjoint of a linear operator.

**Remark 10.35.** Here are some general comments about the finite-dimensional case.

- (a) The adjoint of a linear operator  $T$  depends not only on  $T$  but also the inner product of the space.
- (b) In case of  $\beta$  is an arbitrary ordered basis for the inner product space, it need not be the case which

$$[T]_{\beta}^* = [T^*]_{\beta}.$$

**Remark 10.36.** There is a natural analogue in between taking the complex conjugate of a complex number and taking the adjoint of a linear operator on an inner product space, as the following proposition shows.

**Proposition 10.9.**  
Properties of the  
Adjoint Operation

*Let  $V$  be a finite-dimensional inner product space. Then the following holds for any linear operators  $T, S : V \rightarrow V$  and  $c \in \mathbb{K}$ .*

$$(a) \quad (T + S)^* = T^* + S^*.$$

$$(b) \quad (cT)^* = \bar{c}T^*.$$

$$(c) \quad (TS)^* = S^*T^*.$$

$$(d) \quad (T^*)^* = T.$$

*Proof.* We treat (a) and (b) together. Observe that

$$\langle v, (cT + S)u \rangle = \langle (cT + S)v, u \rangle = c\langle Tv, u \rangle + \langle Sv, u \rangle = \langle v, \bar{c}T^*v \rangle + \langle v, S^*u \rangle = \langle v, (\bar{c}T^* + S^*) \rangle.$$

For (c),

$$\langle v, (TS)^*u \rangle = \langle (TS)v, u \rangle = \langle T(Sv), u \rangle = \langle Sv, T^*u \rangle = \langle v, T^*S^*u \rangle.$$

For (d),

$$\langle v, (T^*)^*u \rangle = \langle T^*v, u \rangle = \overline{\langle u, T^*v \rangle} = \overline{\langle Tu, v \rangle} = \langle v, Tu \rangle. \quad \spadesuit$$

**Remark 10.37.** Proposition 10.9 is often phrased as follows. The adjoint operation  $(\cdot)^* : \mathcal{L}(V) \rightarrow \mathcal{L}(V)$  is a conjugate linear

$$(cT + U)^* = \bar{c}T^* + U^*$$

antiisomorphism

$$(TU)^* = U^*T^*$$

of period 2

$$(T^*)^* = T.$$

Of course, the analogy with complex conjugation is based upon the observation that, if  $w, z \in \mathbb{C}$ , then  $\overline{(w+z)} = \bar{w} + \bar{z}$ ,  $\overline{(wz)} = \bar{w}\bar{z}$ , and  $\overline{(\bar{z})} = z$ . One should be careful about the reversal of order in a product, that

$$(TU)^* = U^*T^*.$$

This is analogous to the transpose of a matrix product. We might also mention that  $z \in \mathbb{C}$  satisfies  $\bar{\bar{z}} = z$  if and only if

$$\bar{\bar{z}} = z,$$

so one might expect that there exists some linear operator  $T : V \rightarrow V$  such that

$$T^* = T$$



and that  $T$  behaves like real numbers. This is in fact the case. If  $T : V \rightarrow V$  is a linear operator, where  $V$  is an inner product space over  $\mathbb{C}$ , then  $T$  can be written as

$$T = T_1 + iT_2$$

for some  $T_1, T_2 : V \rightarrow V$  satisfying  $T_1^* = T_1$  and  $T_2^* = T_2$ . Thus, in some sense,  $T_1$  is the *real part* of  $T$  and  $T_2$  is the *imaginary part* of  $T$ . Such  $T_1$  and  $T_2$  are unique, and we may obtain them by

$$T_1 = \frac{1}{2}(T + T^*)$$

$$T_2 = \frac{1}{2}(T - T^*).$$

### Def'n. Hermitian (Self-Adjoint) Linear Operator

Let  $V$  be an inner product space. We say a linear operator  $T : V \rightarrow V$  is **Hermitian** (or **self-adjoint**) if  $T^* = T$ .

*Remark 10.37 is continued here.*

If  $T : V \rightarrow V$  is Hermitian and  $\beta$  is an orthonormal ordered basis for  $V$ , then  $[T]_\beta$  is also Hermitian. That is,  $[T]_\beta$  is equal to its conjugate transpose,

$$[T]_\beta = [T]_\beta^*.$$

Hermitian operators are important for the following reasons:

- (a) Hermitian operators have many special properties. For instance, Hermitian operators have orthonormal eigenbasis.
- (b) Many linear operators which arise in practice are Hermitian.

We shall discuss the special properties of Hermitian operators later.

## Unitary Operators

**Remark 10.38.** In this section we consider the concept of isomorphisms between two inner product spaces. Recall that an isomorphism between two algebraic structures of the same type (e.g. group, ring, vector space, ...) is a bijective function which preserves the operations defined on the structures. That being said, an isomorphism between inner product spaces is a vector space isomorphism with an additional property that it preserves inner products.

### Def'n. Isometry

Let  $(V, \langle \cdot, \cdot \rangle_V), (W, \langle \cdot, \cdot \rangle_W)$  be inner product spaces over  $\mathbb{K}$ . We say function  $\phi : V \rightarrow W$  is an **isometry** if  $\phi$  is a vector space isomorphism which preserves inner products. That is,

$$\langle Tv, Tu \rangle_W = \langle v, u \rangle_V$$

for all  $v, u \in V$ .

**Remark 10.39.** Let  $V$  and  $W$  be inner product spaces over  $\mathbb{K}$ . If a linear transformation  $T : V \rightarrow W$  preserves inner products, then it must be the case that

$$\|Tv\| = \|v\|,$$

which means  $T$  is invertible (i.e. bijective).

**Remark 10.40.** If  $T : V \rightarrow W$  is an isometry, then  $T^{-1} : W \rightarrow V$  is an isometry, since

$$\|T^{-1}v\| = \|TT^{-1}v\| = \|v\|.$$

That is, if  $V$  is isometric to  $W$ , then  $W$  is isometric to  $V$ , and vice versa. So an isometry is an equivalence relation.

**Proposition 10.10.**  
**Alternative**  
**Definitions of**  
**Isometry**

*Let  $V, W$  be finite-dimensional inner product spaces over  $\mathbb{K}$  satisfying  $\dim(V) = \dim(W)$ . If  $T : V \rightarrow W$  is linear, then the following are equivalent.*

- (a)  $T$  preserves inner products.
- (b)  $T$  is an isometry.
- (c)  $T$  carries some orthonormal basis for  $V$  onto an orthonormal basis for  $W$ .
- (d)  $T$  carries every orthonormal basis for  $V$  onto an orthonormal basis for  $W$ .

*Proof.* We shall proceed in the order (a)  $\implies$  (b)  $\implies$  (d)  $\implies$  (c)  $\implies$  (a). Notice that (a)  $\implies$  (b) is supplied by Remark 10.39. For (b)  $\implies$  (d), let  $\beta = \{v_1, v_2, \dots, v_n\}$  be an orthonormal basis for  $V$ . Then for any  $i, j \in \{1, 2, \dots, n\}$ ,

$$\langle Tv_i, Tv_j \rangle = \langle v_i, v_j \rangle = \delta_{ij}$$

which verifies that  $T\beta = \{Tv_1, Tv_2, \dots, Tv_n\}$  is an orthonormal basis for  $W$ . (d)  $\implies$  (c) requires no comment. For (c)  $\implies$  (a), suppose  $\beta = \{v_1, v_2, \dots, v_n\}$  is an orthonormal basis for  $V$  such that  $T\beta$  is an orthonormal basis for  $W$ . Then for any  $i, j \in \{1, 2, \dots, n\}$ ,

$$\langle Tv_i, Tv_j \rangle = \langle v_i, v_j \rangle = \delta_{ij}.$$

Let  $x = \sum_{i=1}^n x_i v_i, y = \sum_{i=1}^n y_i v_i \in V$  for some  $x_1, x_2, \dots, x_n, y_1, \dots, y_n \in \mathbb{K}$ . Then

$$\langle x, y \rangle = \sum_i x_i \bar{y}_i$$

and

$$\langle Tx, Ty \rangle = \left\langle \sum_i x_i v_i, \sum_j y_j Tv_j \right\rangle = \sum_i x_i \bar{y}_i$$

by Remark 10.22. ♠

**Corollary 10.10.1.**

*Let  $V$  and  $W$  be finite-dimensional inner product spaces over  $\mathbb{K}$ . Then  $V$  and  $W$  are isometry if and only if  $\dim(V) = \dim(W)$ .*

*Proof.* The forward direction easily follows from the fact that if  $V$  and  $W$  are isometric, then they are vector space isomorphic. For the reverse direction, we may find orthonormal bases  $\beta_V = \{v_1, v_2, \dots, v_n\}$  for  $V$  and  $\beta_W = \{w_1, w_2, \dots, w_n\}$  for  $W$  by a slight variant of the Gram-Schmidt process. Then if we define a linear transformation  $T : V \rightarrow W$  by

$$v_i \mapsto w_i,$$

$T$  is an isometry by Proposition 10.10. ♠

**Example 10.41.** If  $V$  is an  $n$ -dimensional inner product space, then each orthonormal ordered basis  $\beta = \{v_1, v_2, \dots, v_n\}$  determines an isometry  $T : V \rightarrow \mathbb{K}^n$  with the standard inner product. The isometry is simply

$$T\left(\sum_i x_i v_i\right) = \sum_i x_i e_i.$$

**Proposition 10.11.**  
 **$T$  Preserves Inner  
 Products If and Only  
 If  $T$  Preserves Norms**

*Let  $V$  and  $W$  be inner product spaces over  $\mathbb{K}$  and let  $T : V \rightarrow W$  be a linear transformation. Then  $T$  preserves inner products if and only if  $T$  preserves norms.*

*Proof.* The forward direction is supplied by Remark 10.39. For the reverse direction, suppose

$$\|Tv\| = \|v\|$$

for all  $v \in V$ . Then

$$\|Tv\|^2 = \|v\|^2$$

so by using the appropriate polarization identity, one may show that  $\langle Tv, Tu \rangle = \langle v, u \rangle$  for all  $v, u \in V$ . ♠

**Def'n. Unitary Operator**

Let  $V$  be an inner product space. We say a linear operator  $T : V \rightarrow V$  is **unitary** if  $T$  is an isometry.

**Remark 10.42.** Let  $V$  be an inner product space. If  $T_1, T_2 : V \rightarrow V$  are unitary operators then  $T_1 T_2$  and  $T_2 T_1$  are unitary, since

$$\|T_1 T_2 v\| = \|T_2 v\| = \|v\| - \|T_1 v\| = \|T_2 T_1 v\|$$

by Proposition 10.11. It is also clear that  $I : V \rightarrow V$  is unitary, and we also have that, if  $T : V \rightarrow V$  is unitary, then  $T^{-1} : V \rightarrow V$  is unitary by Remark 10.40. Thus

$$\{T \in \mathcal{L}(V) : T \text{ is an isometry}\}$$

is a group under the usual composition.

**Remark 10.43.** If  $V$  is a finite-dimensional inner product space and  $T : V \rightarrow V$  is linear, then  $T$  is unitary if and only if

- (a)  $\langle Tv, Tu \rangle = \langle v, u \rangle$  for all  $v, u \in V$  or
- (b) there exists an orthonormal basis  $\beta$  for  $V$  such that  $T\beta$  is an orthonormal basis for  $V$ .

**Proposition 10.12.**

*Let  $V$  be an inner product space. Then a linear operator  $T : V \rightarrow V$  is unitary if and only if there exists the adjoint  $T^* : V \rightarrow V$  of  $T$  which satisfies  $TT^* = I$ .*

*Proof.* For the forward direction, observe that if  $T$  is unitary, then  $T$  is invertible and so

$$\langle Tv, u \rangle = \langle Tv, TT^{-1}u \rangle = \langle v, T^{-1}u \rangle$$

for any  $v, u \in V$ , which means  $T^{-1} = T^*$ . For the reverse direction, if  $TT^* = I$ , then  $T^* = T^{-1}$  so  $T$  is invertible. Moreover,

$$\langle Tv, Tu \rangle = \langle v, T^*Tu \rangle = \langle v, T^{-1}Tu \rangle = \langle v, u \rangle$$

for any  $v, u \in V$ , which means  $T$  is unitary. ♠

**Example 10.44.** Let  $(M_{n \times 1}(\mathbb{C}), \langle \cdot, \cdot \rangle)$  be an inner product space with

$$\langle X, Y \rangle = Y^* X$$

for all  $X, Y \in M_{n \times 1}(\mathbb{C})$ . Let  $A \in M_{n \times n}(\mathbb{C})$  and let  $T : M_{n \times 1}(\mathbb{C}) \rightarrow M_{n \times 1}(\mathbb{C})$  be the left multiplication operator of  $A$ . Then

$$\langle TX, TY \rangle = (AY)^* (AX) = Y^* A^* A X$$

for all  $X, Y \in M_{n \times 1}(\mathbb{C})$ . That is,  $T$  is unitary if and only if  $A^* A = I$ .

**Def'n. Unitary Matrix**

Let  $A \in M_{n \times n}(\mathbb{K})$ . We say  $A$  is *unitary* if  $AA^* = I$ .

**Proposition 10.13.**

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a linear operator. Then  $T$  is unitary if and only if there exists an ordered basis  $\beta$  for  $V$  such that  $[T]_\beta$  is unitary.

*Proof.* Let  $\beta$  be an orthonormal basis for  $V$ . Then it is clear that  $TT^* = I$  if and only if  $[T]_\beta [T]_\beta^* = I$  by a slight modification of Example 10.44. The rest of the proof is completely supplied by the proof of Proposition 10.12 above. ♠

**Remark 10.45.** Let  $A \in M_{n \times n}(\mathbb{K})$ . The statement that  $A$  is unitary merely means

$$(A^*A)_{ij} = \sum_k A_{ik}^* A_{kj} = \sum_k \overline{A_{ki}} A_{kj} = \delta_{ij}.$$

In other words, the columns of  $A$  form an orthonormal set of column matrices, with respect to the standard inner product

$$\langle X, Y \rangle = Y^* X$$

of  $M_{n \times 1}(\mathbb{K})$ . Since  $A^*A = I$  if and only if  $AA^* = I$  we also see that  $A$  is unitary if and only if the rows of  $A$  form an orthonormal set with respect to the standard inner product. In conclusion,  $A \in M_{n \times n}(\mathbb{K})$  is unitary if and only if the rows and columns of  $A$  form orthonormal sets. In particular, in case which  $\mathbb{K} = \mathbb{R}$ , we see that  $AA^* = I$  if and only if  $AA^T = I$  if and only if the rows and columns of  $A$  form orthonormal sets.

**Def'n. Orthogonal Matrix**

Let  $A \in M_{n \times n}(\mathbb{K})$ . We say  $A$  is *orthogonal* if  $AA^T = I$ .

**Remark 10.46.** If  $A \in M_{n \times n}(\mathbb{R})$  is orthogonal, then it is unitary. A  $B \in M_{n \times n}(\mathbb{K})$  is unitary if and only if each  $B_{ij} \in \mathbb{R}$ .

**Example 10.47.** The relations between trigonometric functions show that the matrix

$$A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

is orthogonal. If  $\theta \in \mathbb{R}$ ,  $A$  is the matrix representation of the rotation operator  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  through angle  $\theta$  in the standard ordered basis for  $\mathbb{R}^2$ . Since  $A$  is orthogonal  $A$  is unitary and preserves the standard inner product of  $\mathbb{R}^2$  (i.e. the dot product).

**Remark 10.48.** Recall that the set of unitary operators on an inner product space  $V$ ,

$$\{T : V \rightarrow V \mid T \text{ is unitary}\}$$

We shall consistently use  $U(n)$  to denote the following group from now on.

$$U(n) = \{U \in M_{n \times n}(\mathbb{C}) : U \text{ is unitary}\}$$

is a group under the usual composition. The Gram-Schmidt process in  $\mathbb{C}^n$  has an interesting consequence for  $U(n)$ .

**Proposition 10.14.**

Let  $A \in M_{n \times n}(\mathbb{C})$  be invertible. Then there exists a unique lower triangular  $M \in M_{n \times n}(\mathbb{C})$  with positive entries on the main diagonal such that  $MA$  is unitary.

*Proof.* Write

$$A = [A_1 \ A_2 \ \cdots \ A_n],$$

where each  $A_i \in \mathbb{C}^n$  is the  $i$ th column of  $A$ . Since  $A$  is invertible,  $\{A_1, A_2, \dots, A_n\}$  is a basis for  $\mathbb{C}^n$ . Then by Gram-Schmidt process, we may obtain an orthogonal basis  $\{v_1, v_2, \dots, v_n\}$  for  $\mathbb{C}^n$  such that

$$\text{span}\{A_1, A_2, \dots, A_n\} = \text{span}\{v_1, v_2, \dots, v_n\}$$

for any  $k \in \{1, 2, \dots, n\}$ , where

$$v_i = A_i - \sum_{j=1}^{i-1} \frac{\langle A_i, v_j \rangle}{\|v_j\|^2} v_j.$$

By some calculations, we may show that each  $v_i$  is a linear combination of  $A_1, A_2, \dots, A_i$ . Since  $\{A_1, A_2, \dots, A_i\}$  is linearly independent, there exist unique  $c_{i1}, c_{i2}, \dots, c_{ii} \in \mathbb{K}$  such that

$$v_i = \sum_{j=1}^i c_{ij} A_j = A_i - \sum_{j=1}^{i-1} c_{ij} A_j.$$

Let  $M \in M_{n \times n}(\mathbb{C})$  be defined by

$$M_{ij} = \begin{cases} -\frac{1}{\|v_i\|} c_{ij} & \text{if } j < i \\ \frac{1}{\|v_i\|} & \text{if } j = i \\ 0 & \text{otherwise} \end{cases},$$

then  $M$  is lower triangular and each  $M_{ii} > 0$  by definition. Moreover,

$$\sum_{j=1}^i M_{ij} A_j = \frac{A_i}{\|v_i\|} + \sum_{j=1}^{i-1} M_{ij} A_j = \frac{A_i + \sum_{j=1}^{i-1} \|v_i\| M_{ij} A_j}{\|v_i\|} = \frac{A_i - \sum_{j=1}^{i-1} c_{ij} A_j}{\|v_i\|} = \frac{v_i}{\|v_i\|},$$

which exactly means

$$MA = \begin{bmatrix} \frac{v_1}{\|v_1\|} & \frac{v_2}{\|v_2\|} & \cdots & \frac{v_n}{\|v_n\|} \end{bmatrix}$$

We shall consistently use  $T(n)^+$  to denote the following group from now on.

which clearly is unitary. To verify the uniqueness, we first claim that

$$T(n)^+ = \{B \in M_{n \times n}(\mathbb{C}) : \forall i, j \in \{1, 2, \dots, n\} [i < j \implies B_{ij} = 0 \wedge B_{ii} > 0]\},$$

the set of lower triangular matrices with positive entries on the main diagonal, is a group under the usual composition. To verify this, observe that  $I \in T(n)^+$ . Moreover, for any  $B, C \in T(n)^+$ , it is clear that  $BC$  is lower triangular and

$$(BC)_{ii} = \sum_{j=1}^n B_{ij} C_{ji} = B_{ii} C_{ii} > 0.$$

Lastly, if  $B \in T(n)^+$ , then  $B$  is invertible, since  $B$  is triangular and every entry on the main diagonal is nonzero, and  $B^{-1} \in T(n)^+$ , since  $BB^{-1} = I$  and so

$$(BB^{-1})_{ii} = I_{ii} = 1 > 0 \implies B_{ii}^{-1} > 0$$

for all  $i \in \{1, 2, \dots, n\}$ , and it is clear that  $B^{-1}$  is lower triangular as well. Since

$$U(n) = \{U \in M_{n \times n}(\mathbb{C}) : U \text{ is unitary}\}$$

is also a group under usual composition, if there exists  $N \in T(n)^+$  such that  $NA$  is unitary, then  $(MA)(NA)^{-1} \in U(n)$  and so

$$(MA)(NA)^{-1} = MAA^{-1}N^{-1} = MN^{-1} \in U(n).$$

That is,  $MN^{-1}$  satisfies

$$(MN^{-1})^{-1} = (MN^{-1})^*.$$

But  $(MN^{-1})^{-1} \in T(n)^+$  is upper triangular by definition, so it follows that  $(MN^{-1})^{-1}$ , or,  $MN^{-1}$  is simultaneously upper and lower triangular, which means  $MN^{-1}$  is diagonal. But a diagonal matrix is unitary if and only if every entry on the main diagonal is 1 or  $-1$ . But  $MN^{-1} \in T(n)^+$  so  $(MN^{-1})_{ii} = 1$  for all  $i \in \{1, 2, \dots, n\}$ . Thus  $MN^{-1} = I$  and  $M = N$ , as desired. ♠

**Remark 10.49.** Observe that Proposition 10.14 is about the following group of matrices:

$$GL(n) = \{A \in M_{n \times n}(\mathbb{C}) : A \text{ is invertible}\}.$$

It can be easily shown that  $GL(n)$  is a group under the usual composition. For,  $I \in GL(n)$ ,  $AB$  is invertible whenever  $A$  and  $B$  are invertible, and  $A^{-1}$  is invertible whenever  $A$  is invertible.

### Def'n. General Linear Group

The group of  $n \times n$  complex invertible matrices, denoted by  $GL(n)$ , is called a **general linear group**.

### Corollary 10.14.1. LU Decomposition

For each  $A \in GL(n)$ , there exist unique  $L \in T^+(n)$  and  $U \in U(n)$  such that  $A = LU$ .

*Proof.* By Proposition 10.14, there exists unique  $M \in T(n)^+$  such that  $MB \in U(n)$ . Let  $U = MA$  and  $L = M^{-1}$ . Then it is clear that

$$LU = M^{-1}MA = A.$$

Observe that the uniqueness of  $U$  and  $L$  easily follows from the uniqueness of  $M$ . ♠

**Remark 10.50.** Let us consider briefly the change of basis in an inner product space. Let  $V$  be a finite dimensional inner product space and let  $\beta = \{v_1, v_2, \dots, v_n\}$  and  $\gamma = \{u_1, u_2, \dots, u_n\}$  be orthonormal ordered bases for  $V$ . Then there exists a unique invertible  $P \in M_{n \times n}(\mathbb{K})$  such that

$$[v]_\gamma = P^{-1} [v]_\beta$$

for all  $v \in V$ . If  $U : V \rightarrow V$  is defined by

$$v_i \mapsto u_i,$$

then  $[u]_\beta = P$ , since

$$u_i = \sum_j P_{ji} v_j.$$

Since  $\beta$  and  $\gamma$  are orthonormal bases,  $P$  and  $U$  are unitary by Proposition 10.10. Then for any linear operator  $T : V \rightarrow V$ ,

$$[T]_\gamma = P^{-1} [T]_\beta P = P^* [T]_\beta P.$$

This motivates the following definition.

### Def'n. Unitarily Equivalent, Orthogonally Equivalent Matrices

We say  $A, B \in M_{n \times n}(\mathbb{K})$  are **unitarily equivalent** if there exists a unitary  $P \in M_{n \times n}(\mathbb{K})$  such that

$$A = P^{-1}BP = P^*BP$$

and say **orthogonally equivalent** if there exists an orthogonal  $Q \in M_{n \times n}(\mathbb{K})$  such that

$$A = Q^{-1}BQ = Q^T BQ.$$

## Normal Operators

**Remark 10.51.** The main purpose of this section is to find out under which conditions a linear operator  $T : V \rightarrow V$  in a finite-dimensional inner product space satisfies that, there exists an orthogonal ordered basis  $\beta$  such that  $[T]_\beta$  is diagonal. In other words, we wish to find out the sufficient conditions on  $T$  such that there exist  $n = \dim(V)$  linearly independent eigenvectors  $v_1, v_2, \dots, v_n \in V$  with  $\langle v_i, v_j \rangle = 0$  whenever  $i \neq j$  and  $\|v_i\| = 1$  for all  $i, j \in \{1, 2, \dots, n\}$ . Then, there exist  $c_1, c_2, \dots, c_n \in \mathbb{K}$  such that

$$Tv_i = c_i v_i$$

for all  $i \in \{1, 2, \dots, n\}$ , and we have

$$[T]_\beta = \begin{bmatrix} c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_n \end{bmatrix}.$$

Then, the adjoint operator  $T^* : V \rightarrow V$  of  $T$  is represented by

$$[T^*]_\beta = [T]_\beta^* = \begin{bmatrix} \overline{c_1} & & & \\ & \overline{c_2} & & \\ & & \ddots & \\ & & & \overline{c_n} \end{bmatrix}.$$

That is, if  $c_1, c_2, \dots, c_n \in \mathbb{R}$ , then  $[T]_\beta = [T^*]_\beta$ , which means  $T$  is Hermitian. If some  $c_i \notin \mathbb{R}$ , then  $T$  is not Hermitian, but it still satisfies the property that

$$TT^* = T^*T,$$

since any diagonal matrices commute. It is, however, a remarkable fact that the above condition implies the existence of an orthonormal ordered basis in which  $T$  is represented by a diagonal matrix.

### Def'n. Normal Linear Operator

Let  $T : V \rightarrow V$  be a linear operator. We say  $T$  is **normal** if  $T$  commutes with the adjoint operator  $T^* : V \rightarrow V$ ,

$$TT^* = T^*T.$$

*Remark 10.51 is continued here.*

Any Hermitian or unitary operator is normal. However, sums and products of normal operators need not be normal. Although it is by no means necessary, we shall begin our discussions normal operators by considering Hermitian operators.

### Proposition 10.15.

*Let  $V$  be an inner product space and let  $T : V \rightarrow V$  be Hermitian. Then every eigenvalue of  $T$  is real, and if  $v, u \in V$  are eigenvectors corresponding to distinct eigenvalues, then  $v$  and  $u$  are orthogonal.*

*Proof.* Suppose that  $c \in \mathbb{K}$  is an eigenvalue of  $T$  and let  $v \in V$  be an eigenvector corresponding to  $c$ . Then

$$c \langle v, v \rangle = \langle cv, v \rangle = \langle Tv, v \rangle = \langle v, Tv \rangle = \langle v, cv \rangle = \bar{c} \langle v, v \rangle,$$

which exactly means  $c = \bar{c}$ , or, equivalently,  $c \in \mathbb{R}$ . Now, suppose that  $d \in \mathbb{K}$  with  $d \neq c$  is also an eigenvalue of  $T$  and  $u \in V$  is a corresponding eigenvector. Then,

$$c \langle v, u \rangle = \langle cv, u \rangle = \langle Tv, u \rangle = \langle v, Tu \rangle = \langle v, du \rangle = \bar{d} \langle v, u \rangle.$$

But  $c \neq d = \bar{d}$ , so it follows that  $\langle v, u \rangle = 0$ . ♠

**Remark 10.52.** It should be pointed out that Proposition 10.15 does not provide any information about the existence of eigenvalues of a Hermitian operator.

**Proposition 10.16.**  
Every Hermitian  
Operators on a  
Finite-Dimensional  
Inner Product Space  
Has an Eigenvalue

*Let  $V$  be a finite-dimensional inner product space over  $\mathbb{K}$ . Then every Hermitian  $T : V \rightarrow V$  has an eigenvalue.*

*Proof.* Let  $f \in \mathbb{K}[x]$  be the characteristic polynomial of  $T$ . If  $\mathbb{K} = \mathbb{C}$ , then by the fundamental theorem of algebra, there exists  $c \in \mathbb{C}$  such that  $f(c) = 0$ . But  $T$  is Hermitian, so Proposition 10.15 implies that  $c \in \mathbb{R}$ . This means  $c$  is also an eigenvalue of  $T$  when  $\mathbb{K} = \mathbb{R}$ . ♠

**Remark 10.53.** Here are few things we wish to point out about Proposition 10.16:

- (a) In case of  $\mathbb{K} = \mathbb{C}$ , the fundamental theorem of algebra is sufficient to show that  $T$  has an eigenvalue. But when  $\mathbb{K} = \mathbb{R}$ , the self-adjointness of  $T$  is used very heavily.
- (b) The proof of Proposition 10.16 above shows that the characteristic polynomial of any Hermitian operator has real coefficients, although the matrix representation of  $T$  in an ordered basis almost always has a complex entry.
- (c) The assumption that  $V$  is finite-dimensional is necessary. That is, a Hermitian operator over an infinite-dimensional inner product space need not have an eigenvalue.

**Proposition 10.17.**

*Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be linear. Let  $W \subseteq V$  be a  $T$ -invariant subspace. Then the orthogonal complement  $W_{\perp} \subseteq V$  of  $W$  is  $T^*$ -invariant.*

*Proof.* Let  $w \in W$  and  $w_{\perp} \in W_{\perp}$ . Then,

$$\langle w, T^* w_{\perp} \rangle = \langle Tw, w_{\perp} \rangle.$$

But  $Tw \in W$  by the  $T$ -invariance of  $W$ , so it follows that

$$\langle w, T^* w_{\perp} \rangle = \langle Tw, w_{\perp} \rangle = 0,$$

which exactly means that  $w$  and  $T^* w_{\perp}$  are orthogonal, or, equivalently, that  $W_{\perp}$  is  $T^*$ -invariant. ♠

**Theorem 10.18.**  
Every Hermitian  
Operator Has an  
Orthonormal  
Eigenbasis

*Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a Hermitian operator. Then there exists an orthonormal eigenbasis for  $V$ .*

*Proof.* We proceed inductively. First, assume  $n = \dim(V) \neq 0$  without loss of generality. In case of  $n = 1$ , Proposition 10.16 provides an eigenvector  $v \in V$  of  $T$ , so  $\left\{ \frac{v}{\|v\|} \right\}$  is the desired basis. Now suppose the result for all  $n \in \{1, 2, \dots, k-1\}$  for some  $k \in \mathbb{N}$ . Select an eigenvector  $u_1 \in V$  of  $T$  by Proposition 10.16 and let  $W = \text{span}(u_1)$ . Then  $v_1 = \frac{u_1}{\|u_1\|}$  also spans  $W$ . Let  $W_{\perp} \in V$  be the orthogonal complement



of  $W$ . Then  $W_\perp$  is  $T^*$ -invariant by Proposition 10.17. But  $T$  is Hermitian, so  $T = T^*$  and  $W_\perp$  is  $T$ -invariant. So we may define the linear operator  $T_\perp : W_\perp \rightarrow W_\perp$ , the restriction of  $T$  on  $W_\perp$ . By the induction hypothesis, there exists an orthonormal eigenbasis  $\{v_2, v_3, \dots, v_k\}$  for  $W_\perp$ . Since  $V = W \oplus W_\perp$ , and clearly  $v_1$  is orthogonal to  $v_i$  for all  $i \in \{2, 3, \dots, k\}$ , it follows that  $\{v_1, v_2, \dots, v_k\}$  is the desired basis. ♠

**Corollary 10.18.1.**

*Let  $A \in M_{n \times n}(\mathbb{K})$  be Hermitian. Then there exists a unitary  $P \in M_{n \times n}(\mathbb{K})$  such that  $P^{-1}AP$  is diagonal.*

*Proof.* By Theorem 10.18, there exists an orthonormal eigenbasis  $\beta$  for  $V$ . So if  $T : \mathbb{K}^n \rightarrow \mathbb{K}^n$  is the left multiplication operator of  $A$ , then  $[T]_\beta$  is diagonal, and there exists an invertible  $P \in M_{n \times n}(\mathbb{K})$  such that

$$[T]_\beta = P^{-1}AP.$$

We claim that  $P$  preserves the standard inner product of  $\mathbb{K}^n$ . To verify this, observe that  $P$  is characterized by

$$Pe_i = v_i$$

for all  $i \in \{1, 2, \dots, n\}$ , where  $\{e_1, e_2, \dots, e_n\}$  is the standard ordered basis for  $\mathbb{K}^n$  and  $\{v_1, v_2, \dots, v_n\} = \beta$ . But  $\{e_1, e_2, \dots, e_n\}$  is an orthonormal basis, so  $P$  preserves the standard inner product by Proposition 10.10. Thus  $P$  is unitary, as required. ♠

**Remark 10.54.** Together with Remark 10.52, Theorem 10.18 shows that a linear operator  $T : V \rightarrow V$  on a real finite-dimensional inner product space  $V$  has an orthonormal eigenbasis for  $V$  if and only if  $T$  is Hermitian. This, however, is false when  $V$  is over  $\mathbb{C}$ .

**Remark 10.55.** We now return to the study of normal operators in general. In particular, we shall prove a result for normal operators analogous to Theorem 10.18, in the complex case.

**Proposition 10.19.**

*Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be normal. Then  $v \in V$  is an eigenvector of  $T$  corresponding to  $c \in \mathbb{K}$  if and only if  $v$  is an eigenvector of  $T^*$  corresponding to  $\bar{c}$ .*

*Proof.* We claim that any normal  $U : V \rightarrow V$  satisfies  $\|Uv\| = \|U^*v\|$  for all  $v \in V$ . To verify this, observe that

$$\|Uv\|^2 = \langle Uv, Uv \rangle = \langle v, U^*Uv \rangle = \langle U^*v, U^*v \rangle = \|U^*v\|^2.$$

Moreover, for any  $d \in \mathbb{K}$ ,  $T - dI$  is normal. For  $TT^* = T^*T$ . Thus,

$$\|(T - dI)v\| = \|(T^* - \bar{d}I)v\|$$

which implies the result. ♠

**Def'n. Normal Matrix**

Let  $A \in M_{n \times n}(\mathbb{K})$ . We say  $A$  is **normal** if  $AA^* = A^*A$ .

**Remark 10.56.** It is not so obvious what normality of linear operators or matrices really means. However, it might be helpful to find that a triangular matrix is normal if and only if it is diagonal.

**Proposition 10.20.**

*Let  $V$  be a finite-dimensional inner product space and let  $T$  be linear. If  $\beta$  is an orthonormal basis for  $V$  such that  $[T]_\beta$  is upper triangular, then  $[T]_\beta$  is diagonal if and only if  $T$  is normal.*

*Proof.* The forward direction is clear, since any diagonal matrix commutes with its adjoint. For the reverse direction, suppose that  $T$  is normal and that  $[T]_\beta$  is upper triangular, and for convenience, write  $\beta = \{v_1, v_2, \dots, v_n\}$ . Then

$$Tv_1 = \sum_{i=1}^n ([T]_\beta)_{i1} v_i = ([T]_\beta)_{11} v_1.$$

This means  $v_1$  is an eigenvector of  $T$  corresponding to  $([T]_\beta)_{11}$ , so by Proposition 10.19,

$$T^*v_1 = ([T]_\beta)_{11} v_1 = ([T]_\beta^*)_{11} v_1.$$

But we also know that

$$T^*v_1 = \sum_{i=1}^n ([T]_\beta^*)_{i1} v_i.$$

That is,

$$([T]_\beta^*)_{21} = ([T]_\beta^*)_{31} = \dots = ([T]_\beta^*)_{n1} = 0.$$

And in particular,

$$Tv_2 = ([T]_\beta)_{22} v_2.$$

Thus by continuing this for  $v_2, v_3, \dots, v_n$ , we have the desired result. ♠

**Proposition 10.21.**

*Let  $V$  be a finite-dimensional inner product space over  $\mathbb{C}$  and let  $T : V \rightarrow V$  be linear. Then there exists an orthonormal basis for  $V$  such that  $[T]_\beta$  is upper triangular.*

*Proof.* We proceed inductively. The result is trivial for 1-dimensional inner product spaces. Now suppose that the result holds for all  $k$ -dimensional inner product space, and suppose  $\dim(V) = k + 1$ . Since  $V$  is finite-dimensional and is over  $\mathbb{C}$ , there exists an eigenvector  $v \in V$  of  $T^*$  corresponding to some  $c \in \mathbb{C}$ . Let  $W$  be the orthogonal complement of  $\text{span}(v)$ . Then by Proposition 10.17,  $W$  is  $T$ -invariant, so we may define the restriction operator  $T_W : W \rightarrow W$ . By the inductive hypothesis, there exists an orthonormal basis  $\beta_W = \{v_2, v_3, \dots, v_{k+1}\}$  for  $W$  such that  $[T]_{\beta_W}$  is upper triangular. Thus it follows that  $\beta = \left\{ \frac{v}{\|v\|}, v_2, \dots, v_{k+1} \right\}$  is the desired basis. ♠

**Corollary 10.21.1.**

*For every  $A \in M_{n \times n}(\mathbb{C})$  there exists a unitary  $U \in M_{n \times n}(\mathbb{C})$  such that  $U^{-1}AU$  is upper triangular.*

**Remark 10.57.** A possible proof of Corollary 10.21.1 is very similar to the proof of Corollary 10.18.1.

**Remark 10.58.** Combining Proposition 10.20 and 10.21 provides the following result.

**Theorem 10.22.**

*Let  $V$  be a finite-dimensional inner product space over  $\mathbb{C}$  and let  $T : V \rightarrow V$  be normal. Then there exists an orthonormal eigenbasis for  $V$ .*

*Proof.* This is a direct consequence of Proposition 10.20 and 10.21. ♠

**Corollary 10.22.1.**

*For every normal  $A \in M_{n \times n}(\mathbb{C})$  there exists a unitary  $U \in M_{n \times n}(\mathbb{C})$  such that  $U^{-1}AU$  is diagonal.*

## Spectral Theory

**Remark 10.59.** In this section, we pursue the implications of Theorem 10.18 and 10.22 concerning the diagonalization of Hermitian and normal operators. One may find it helpful to read Elementary Canonical Forms (Chapter 2), especially the parts concerning eigendecomposition or projections.

### Theorem 10.23. Spectral Theorem

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be Hermitian if  $V$  is over  $\mathbb{R}$  or normal if  $V$  is over  $\mathbb{C}$ . Let  $c_1, c_2, \dots, c_k \in \mathbb{K}$  be the distinct eigenvalues of  $T$ , let  $W_1, W_2, \dots, W_k \subseteq V$  be the associated eigenspaces, and let  $E_1, E_2, \dots, E_k : V \rightarrow V$  be the orthogonal projections of  $V$  on  $W_1, W_2, \dots, W_k$ . Then the following holds.

- (a) For all  $i, j \in \{1, 2, \dots, k\}$ ,  $W_i$  and  $W_j$  are orthogonal whenever  $i \neq j$ .
- (b)  $V = \bigoplus_{i=1}^k W_i$ .
- (c)  $T = \sum_{i=1}^k c_i E_i$ .

*Proof.* For (a), let  $w_i \in W_i$  and let  $w_j \in W_j$ , where  $i \neq j$ . If  $V$  is over  $\mathbb{R}$ , then

$$c_i \langle w_i, w_j \rangle = \langle c_i w_i, w_j \rangle = \langle T w_i, w_j \rangle = \langle w_i, T w_j \rangle = \langle w_i, c_j w_j \rangle = c_j \langle w_i, w_j \rangle$$

since  $T$  is Hermitian. But  $c_i \neq c_j$ , so  $\langle w_i, w_j \rangle = 0$ . Furthermore, if  $V$  is over  $\mathbb{C}$ , then

$$c_i \langle w_i, w_j \rangle = \langle c_i w_i, w_j \rangle = \langle T w_i, w_j \rangle = \langle w_i, T^* w_j \rangle = \langle w_i, \overline{c_j} w_j \rangle = c_j \langle w_i, w_j \rangle$$

by the normality of  $T$ , so  $\langle w_i, w_j \rangle = 0$ . For (b) and (c), first notice that  $V = \sum_{i=1}^k W_i$ , since Theorem 10.18 and 10.22 provide an eigenbasis for  $V$ . Now suppose that

$$v = \sum_{j=1}^k v_j = 0$$

for some  $v_1 \in W_1, v_2 \in W_2, \dots, v_k \in W_k$ . Then

$$\|v_i\|^2 = \langle v_i, v_i \rangle = \sum_j \langle v_i, v_j \rangle = \left\langle v_i, \sum_j v_j \right\rangle = \langle v_i, v \rangle = 0,$$

for each  $i \in \{1, 2, \dots, k\}$ , so  $v_1 = v_2 = \dots = v_k = 0$ , which means  $V = \bigoplus_{i=1}^k W_i$ . Thus

$$I = \sum_i E_i$$

and

$$T = \sum_i T E_i = \sum_i c_i E_i.$$



### Def'n. Spectral Resolution, Spectrum of a Linear Operator

Suppose the conditions of Theorem 10.23. We call the decomposition

$$T = \sum_i c_i E_i$$

the *spectral resolution* of  $T$ . Moreover, we call

$$\{c_1, c_2, \dots, c_k\},$$

the set of eigenvalues of  $T$ , the *spectrum* of  $T$ .

**Remark 10.60.** Let  $T : V \rightarrow V$  be a linear operator on a finite-dimensional inner product space and consider

$$T = \sum_{i=1}^k c_i E_i,$$

the spectral resolution of  $T$ . The next result shows that the linear operators  $E_1, E_2, \dots, E_k$  satisfying the above equation are canonically associated with  $T$ . In fact, they are polynomials in  $T$ .

**Corollary 10.23.1.**  
Uniqueness of  
Spectral Resolution  
of a Linear Operator

Consider the case in Remark 10.60. Then each  $E_i : V \rightarrow V$  is such that

$$E_i = \prod_{j=1, j \neq i}^k \frac{T - c_j}{c_j - c_i}.$$

In other words, if we define each

$$e_i = \prod_{j=1, j \neq i}^k \frac{x - c_j}{c_j - c_i} \in \mathbb{K}[x],$$

then  $e_i(T) = E_i$ .

*Proof.* Notice that  $E_i E_j \neq 0$  whenever  $i \neq j$ . So, for any  $n \in \mathbb{N} \cup \{0\}$ ,

$$T^n = \left( \sum_{i=1}^k c_i E_i \right)^n = \sum_{i=1}^k c_i^n E_i^n = \sum_{i=1}^k c_i^n E_i.$$

Therefore, for any  $f \in \sum_{i=0}^p d_i x^i \in \mathbb{K}[x]$ , where  $p \in \mathbb{N}$  and  $d_1, d_2, \dots, d_p \in \mathbb{K}$ ,

$$\begin{aligned} f(T) &= \sum_{i=0}^p d_i T^i = \sum_{i=0}^p d_i \sum_{j=1}^k c_j^i E_j \\ &= \sum_{i=0}^p \sum_{j=1}^k d_i c_j^i E_j = \sum_{j=1}^k \left( \sum_{i=0}^p d_i c_j^i \right) E_j = \sum_{j=1}^k f(c_j) E_j. \end{aligned}$$

Since  $e_i$  is a polynomial such that  $e_i(c_j) = \delta_{ij}$ , it follows that

$$e_i(T) = \sum_{j=1}^k e_i(c_j) E_j = \sum_{j=1}^k \delta_{ij} E_j = E_i. \quad \spadesuit$$

**Remark 10.61.** If

$$T = \sum_{i=1}^k c_i E_i$$

is the spectral resolution of  $T$ , a linear operator on a finite-dimensional inner product space, then

$$I = \sum_{i=1}^k E_i.$$

The fact that  $E_1, E_2, \dots, E_k$  are canonically associated with  $T$  motivates the following definition.

**Def'n. Resolution of the Identity Operator by a Linear Operator**

Consider Remark 10.61. We say the decomposition

$$I = \sum_{i=1}^k E_i$$

the *resolution of the identity* by  $T$ .

**Remark 10.62.** The proof of the spectral theorem (Theorem 10.23) provided here is derived from the diagonalization of Hermitian and normal operators (Theorem 10.18 and 10.22). We shall give a more algebraic proof utilizing the primary decomposition theorem later.

**Def'n. Function** in a Linear Operator

Let  $T : V \rightarrow V$  be a diagonalizable normal operator on a finite-dimensional inner product space and let  $S$  be the spectrum of  $T$ . If  $f : \text{domain}(f) \rightarrow \mathbb{K}$  is such that

$$S \subseteq \text{domain}(f),$$

then we define  $f(T)$ , the **function**  $f$  in  $T$ , by

$$f(T) = \sum_{i=1}^k f(c_i) E_i,$$

provided that

$$T = \sum_{i=1}^k c_i E_i$$

is the spectral resolution of  $T$ .

**Proposition 10.24.**

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a diagonalizable normal operator with spectrum  $S \subseteq \mathbb{K}$ . If  $f : \text{domain}(f) \rightarrow \mathbb{K}$  satisfies

$$S \subseteq \text{domain}(f),$$

then  $f(T) : V \rightarrow V$  is a diagonalizable normal operator with spectrum  $f(S)$ .

*Proof.* It is clear that  $f(T)$  is diagonalizable, since if  $v \in V$  is an eigenvector of  $T$  corresponding to  $c_i$ , then

$$f(T)v = \sum_{i=1}^k f(c_i) E_i v = f(c_i) v,$$

and  $f(T)v$  is normal as well, since every diagonalizable operator is normal. Now let  $P$  be the spectrum of  $f(T)$ . For any  $i \in \{1, 2, \dots, k\}$ ,

$$f(T)E_i v = f(c_i) E_i v$$

for all  $v \in V$ . But any eigenvector of  $T$  is of the form  $E_i v$  for some  $i \in \{1, 2, \dots, k\}$ , so it follows that  $f(c_i) \in P$  whenever  $c_i$  is an eigenvalue of  $T$ . On the other hand, suppose  $v \in V$  is an eigenvector of  $f(T)$  corresponding to  $d \in P$ ,

$$f(T)v = dv.$$

Since  $v = \sum_{i=1}^k E_i v$ ,

$$f(T)v = f(T) \sum_{i=1}^k E_i v = \sum_{i=1}^k f(T)E_i v = \sum_{i=1}^k f(c_i) E_i v.$$

But

$$f(T)v = dv = \sum_{i=1}^k d E_i v,$$

so it follows that

$$\sum_{i=1}^k (f(c_i) - d) E_i v = 0,$$

which means  $f(c_i) - d = 0$  or  $E_i v = 0$  for all  $i \in \{1, 2, \dots, k\}$ . But since  $v$  is an eigenvector of  $f(T)$ ,  $v \neq 0$ , so it follows that there must exist  $E_i v \neq 0$  for some  $i \in \{1, 2, \dots, k\}$ , which exactly means  $d = c_i$ . Thus  $P = f(S)$  is the spectrum of  $f(T)$ , as desired. ♠

**Remark 10.63.** Consider Proposition 10.24. We may find the spectral resolution of  $f(T)$  as follows. We have shown that

$$f(S) = \{d_1, d_2, \dots, d_r\} \subseteq \mathbb{K}$$

is the spectrum of  $f(T)$ , where, obviously,  $r \leq k$ . Let  $X_j$  be the set of  $i \in \{1, 2, \dots, k\}$  such that  $f(c_i) = d_j$ ,

$$X_j = \{i \in \{1, 2, \dots, k\} : f(c_i) = d_j\}.$$

Moreover, define

$$P_j = \sum_{i \in X_j} E_i : V \rightarrow V.$$

Then  $P_j$  is the orthogonal projection of  $V$  onto the eigenspace corresponding to  $d_j$ . Thus,

$$f(T) = \sum_{j=1}^r d_j P_j$$

is the spectral resolution of  $f(T)$ .

#### Def'n. Unitary Transformation

Let  $V, V'$  be inner product spaces over  $\mathbb{K}$  and let  $T : V \rightarrow V'$  be a linear transformation. We say  $T$  is **unitary** if  $T$  preserves inner products.

#### Proposition 10.25.

Let  $V, V'$  be finite-dimensional inner product spaces and let  $T : V \rightarrow V$  be a diagonalizable normal operator. Let  $U : V \rightarrow V'$  be a unitary transformation and let  $T' = UTU^{-1}$ . Then  $S$  is the spectrum of  $T'$  and

$$f(T') = Uf(T)U^{-1}.$$

*Proof.* Let  $v \in V$ . Observe that the equation

$$Tv = cv$$

for some  $c \in \mathbb{K}$  holds if and only if

$$T'Uv = UTv = Ucv = cUv,$$

which exactly means  $v \in V$  is an eigenvector of  $T$  corresponding to  $c \in \mathbb{K}$  if and only if  $Uv \in V'$  is an eigenvector of  $T'$  corresponding to  $c$ . Thus  $S$  is the spectrum of  $T'$ , and  $U$  maps each eigenspace of  $T$  onto the corresponding eigenspace of  $T'$ . In fact, for each  $i \in \{1, 2, \dots, k\}$ ,

$$E'_i = UE_iU^{-1}$$

is the orthogonal projection of  $V'$  onto the eigenspace corresponding to  $c_i$ , and hence

$$T' = \sum_{i=1}^k c_i E'_i = \sum_{i=1}^k c_i UE_iU^{-1}$$

is the spectral resolution of  $T'$ . Thus

$$f(T') = \sum_{i=1}^k f(c_i) UE_iU^{-1} = U \left( \sum_{i=1}^k f(c_i) E_i \right) U^{-1} = Uf(T)U^{-1}. \quad \spadesuit$$

#### Corollary 10.25.1.

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a diagonalizable normal operator such that

$$[T]_{\beta} = \begin{bmatrix} d_{11} & & & \\ & d_{22} & & \\ & & \ddots & \\ & & & d_{nn} \end{bmatrix}$$

for some  $d_{11}, d_{22}, \dots, d_{nn} \in \mathbb{K}$ , where  $\beta = \{v_1, v_2, \dots, v_n\}$  is an ordered basis for  $V$ . Then, if  $f : \text{domain}(f) \rightarrow \mathbb{K}$  is such that

$$S \subseteq \text{domain}(f),$$

where  $S$  is the spectrum of  $T$ , then

$$[f(T)]_\beta = \begin{bmatrix} f(d_{11}) & & & \\ & f(d_{22}) & & \\ & & \ddots & \\ & & & f(d_{nn}) \end{bmatrix}.$$

If  $\gamma = \{u_1, u_2, \dots, u_n\}$  is an ordered basis for  $V$  and  $P \in M_{n \times n}(\mathbb{K})$  is the change of coordinate matrix defined by

$$u_j = \sum_i P_{ij} v_i,$$

then  $P^{-1}[f(T)]_\beta P = [f(T)]_\gamma$ .

*Proof.* Let  $c_1, c_2, \dots, c_k \in \mathbb{K}$  be the distinct eigenvalues of  $T$  and let  $E_1, E_2, \dots, E_k : V \rightarrow V$  be the orthogonal projections of  $V$  onto the associated eigenspace, respectively. Then for each  $i \in \{1, 2, \dots, n\}$ , there exists a unique  $j \in \{1, 2, \dots, k\}$  such that  $v_i \in E_j(V)$  and  $d_{ii} = c_j$ . Thus  $f(T)v_i = f(d_{ii})v_i$  for all  $i \in \{1, 2, \dots, n\}$  and

$$\begin{aligned} f(T)u_j &= f(T) \sum_i P_{ij} v_i = \sum_i P_{ij} f(T)v_i = \sum_i d_{ii} P_{ij} v_i = \sum_i ([T]_\beta P)_{ij} v_i \\ &= \sum_i ([T]_\beta P)_{ij} \sum_k P_{ki}^{-1} u_k = \sum_k (P^{-1} [T]_\beta P)_{kj} u_k, \end{aligned}$$

which exactly means

$$P^{-1} [f(T)]_\beta P = [f(T)]_\gamma. \quad \spadesuit$$

**Remark 10.64.** It follows from Corollary 10.24.1 that one can define a function in a normal matrix. For, if  $A \in M_{n \times n}(\mathbb{K})$  is normal, then there exists an invertible, in fact unitary,  $P \in M_{n \times n}(\mathbb{K})$  such that  $D = PAP^{-1}$  is diagonal. Then for any  $f : \text{domain}(f) \rightarrow \mathbb{K}$  such that

$$\{D_{11}, D_{22}, \dots, D_{nn}\} \subseteq \text{domain}(f),$$

we may define  $f(D)$  by

$$f(D) = \begin{bmatrix} f(D_{11}) & & & \\ & f(D_{22}) & & \\ & & \ddots & \\ & & & f(D_{nn}) \end{bmatrix}.$$

#### Def'n. Function in a Matrix

Let  $A \in M_{n \times n}(\mathbb{K})$  be normal and diagonalizable and let  $P \in M_{n \times n}(\mathbb{K})$  be unitary such that  $PAP^{-1}$  is diagonal. Then we define  $f(A)$ , the function in  $A$ , by

$$f(A) = P^{-1} f(PAP^{-1}) P^{-1}.$$

**Remark 10.65.** The matrix  $f(A)$ , where  $A$  is diagonalizable and normal and the domain of  $f$  contains the set of eigenvalues of  $A$ , can be characterized in a different way. In doing so, we first state a matrix analogue of the spectral theorem (Theorem 10.23) and Corollary 10.23.1 without a proof.

**Proposition 10.26.**

Let  $A \in M_{n \times n}(\mathbb{K})$  be a diagonalizable normal matrix and let  $c_1, c_2, \dots, c_k \in \mathbb{K}$  be distinct eigenvalues of  $A$ . Let

$$e_i = \prod_{j=1, j \neq i}^k \frac{x - c_j}{c_i - c_j}$$

and let  $E_i = e_i(A)$  for all  $i \in \{1, 2, \dots, k\}$ . Then the following holds.

- (a)  $E_i E_j = 0$  whenever  $i \neq j$ ,  $i, j \in \{1, 2, \dots, k\}$ .
- (b)  $E_i^2 = E_i$  for all  $i \in \{1, 2, \dots, k\}$ .
- (c)  $I = \sum_{i=1}^k E_i$ .
- (d) If  $f : \text{domain}(f) \rightarrow \mathbb{K}$  satisfies  $\{c_1, c_2, \dots, c_k\} \subseteq \text{domain}(f)$ , then

$$f(A) = \sum_{i=1}^k f(c_i) E_i.$$

In particular,

$$A = \sum_{i=1}^k c_i E_i.$$

**Def'n. Positive, Nonnegative, Negative, Nonpositive Linear Operator**

Let  $V$  be an inner product space and let  $T : V \rightarrow V$  be a linear operator. We say  $T$  is

- (a) **positive** if  $\langle Tv, v \rangle > 0$  for all nonzero  $v \in V$ ,
- (b) **nonnegative** if  $\langle Tv, v \rangle \geq 0$  for all  $v \in V$ ,
- (c) **negative** if  $\langle Tv, v \rangle < 0$  for all nonzero  $v \in V$ , and
- (d) **nonpositive** if  $\langle Tv, v \rangle \leq 0$  for all  $v \in V$ .

**Proposition 10.27.**

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a diagonalizable normal operator. Let  $c_1, c_2, \dots, c_k \in \mathbb{K}$  be distinct eigenvalues. Then the following holds.

- (a)  $T$  is Hermitian if and only if  $c_1, c_2, \dots, c_k \in \mathbb{R}$ .
- (b)  $T$  is nonnegative if and only if  $c_1, c_2, \dots, c_k \geq 0$ .
- (c)  $T$  is unitary if and only if  $|c_1| = |c_2| = \dots = |c_k| = 1$ .

*Proof.* Let  $E_1, E_2, \dots, E_k : V \rightarrow V$  be such that

$$T = \sum_{i=1}^k c_i E_i$$

is the spectral resolution of  $T$ . Then by the normality of  $T$ ,

$$T^* = \sum_{i=1}^k \bar{c}_i E_i$$

is the spectral resolution of  $T^*$ . If  $T$  is Hermitian, then  $T = T^*$ , and

$$T - T^* = \sum_{i=1}^k (c_i - \bar{c}_i) E_i = 0,$$



which means  $c_i = \bar{c}_i \in \mathbb{R}$  for each  $i \in \{1, 2, \dots, k\}$ . The converse is trivial. If  $T$  is nonnegative, then for any eigenvector  $v \in V$  corresponding to  $c_i$  for some  $i \in \{1, 2, \dots, k\}$ ,

$$c_i \langle v, v \rangle = \langle c_i v, v \rangle = \langle T v, v \rangle \geq 0$$

so by the positive definiteness of  $\langle \cdot, \cdot \rangle$ ,  $c_i \geq 0$  for all  $i \in \{1, 2, \dots, k\}$ . Conversely, if  $c_1, c_2, \dots, c_k \geq 0$ , then for any  $v \in V$ ,

$$\langle T v, v \rangle = \left\langle \sum_{i=1}^k c_i E_i v, \sum_{j=1}^k E_j v \right\rangle = \sum_{i=1}^k \sum_{j=1}^k c_i \langle E_i v, E_j v \rangle = \sum_{i=1}^k c_i \langle E_i v, E_i v \rangle \geq 0,$$

where the last inequality holds by the positive definiteness of  $\langle \cdot, \cdot \rangle$ . If  $T$  is unitary, then  $T T^* = I$  and so

$$\sum_{i=1}^k E_i = I = T T^* = \sum_{i=1}^k c_i E_i \sum_{j=1}^k \bar{c}_j E_j = \sum_{i=1}^k |c_i|^2 E_i,$$

which exactly means

$$\sum_{i=1}^k (|c_i|^2 - 1) E_i = 0,$$

so  $|c_1| = |c_2| = \dots = |c_k| = 1$ . The converse is clear as well. ♠

**Remark 10.66.** A result like Proposition 10.27 serves to strengthen the analogy between the adjoint operation on linear operators and the conjugate operation on  $\mathbb{C}$ . A  $z \in \mathbb{C}$  is real if and only if  $z = \bar{z}$  and is of absolute value 1 if and only if  $z\bar{z} = 1$ . Analogously, eigenvalues of a diagonalizable normal operator  $T : V \rightarrow V$  on a finite-dimensional inner product space are real if and only if  $T = T^*$  and are of absolute value 1 if and only if  $T T^* = I$ . We shall also prove two propositions, which are analogous to the following statements.

- (a) For all nonnegative  $a \in \mathbb{R}$ , there exists a unique nonnegative  $b \in \mathbb{R}$  such that  $a = b^2$  (i.e.  $\sqrt{a} = b$ ).
- (b) For all  $z \in \mathbb{C}$ , there exist nonnegative  $r \in \mathbb{R}$  and  $u \in \mathbb{C}$  of absolute value  $|u| = 1$  such that  $z = ru$ . This is the polar decomposition of complex numbers,

$$z = r e^{i\theta}.$$

**Proposition 10.28.**  
**Square Root of a**  
**Nonnegative**  
**Operator**

*Let  $V$  be an inner product space and let  $T : V \rightarrow V$  be a nonnegative operator. Then there exists a unique nonnegative operator  $N : V \rightarrow V$  such that  $T = N^2$ .*

*Proof.* Let  $E_1, E_2, \dots, E_k : V \rightarrow V$  and  $c_1, c_2, \dots, c_k \in \mathbb{R}$  be such that

$$T = \sum_{i=1}^k c_i E_i$$

is the spectral resolution of  $T$ . Then by Proposition 10.27,  $c_1, c_2, \dots, c_k \geq 0$ . Since  $\text{domain}(\sqrt{\cdot}) = [0, \infty)$ ,  $\sqrt{c_1}, \sqrt{c_2}, \dots, \sqrt{c_k} \in \mathbb{R}$  are well-defined, and so

$$N = \sqrt{T} = \sum_{i=1}^k \sqrt{c_i} E_i$$

is well-defined as well. It is clear from the definition that  $N$  is nonnegative. Moreover,

$$N^2 = \sum_{i=1}^k (\sqrt{c_i})^2 E_i = \sum_{i=1}^k c_i E_i = T.$$

Now suppose that there exist a nonnegative  $M : V \rightarrow V$  with spectral resolution

$$M = \sum_{j=1}^r d_j F_j$$

satisfies  $M^2 = T$ . But this means  $M^2 = T = N^2$ , so

$$\sum_{j=1}^r d_j^2 F_j = \sum_{i=1}^k (\sqrt{c_i})^2 E_i.$$

Thus by the uniqueness of the spectral resolution of  $T$ ,  $r = k$  and for each  $i \in \{1, 2, \dots, k\}$ , there exists unique  $j \in \{1, 2, \dots, k\}$  such that  $d_j = \sqrt{c_i}$  and  $F_j = E_i$ , which exactly means  $M = N$ . ♠

**Theorem 10.29.**  
**Polar Decomposition**

*Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be linear. Then there exist a unitary  $U : V \rightarrow V$  and a nonnegative  $N : V \rightarrow V$  such that  $T = UN$ . Moreover,  $N$  is unique, and if  $T$  is invertible, then  $U$  is unique.*

*Proof.* Observe that  $T^*T : V \rightarrow V$  is nonnegative, since

$$\langle T^*Tv, v \rangle = \langle Tv, Tv \rangle \geq 0$$

for all  $v \in V$  by the positive definiteness of  $\langle \cdot, \cdot \rangle$ . We first consider the case which  $T$  is invertible. By Proposition 10.28, let  $N : V \rightarrow V$  be the unique nonnegative operator such that  $T^*T = N^2$ . We see that  $N$  is invertible, since

$$\langle Nv, Nv \rangle = \langle N^*Nv, v \rangle = \langle N^2v, v \rangle = \langle T^*Tv, v \rangle = \langle Tv, Tv \rangle,$$

so  $Tv = 0$  if and only if  $Nv = 0$ . Moreover, define  $U : V \rightarrow V$  by

$$U = TN^{-1}.$$

It can easily shown that  $U$  is unitary. For,

$$\begin{aligned} UU^* &= TN^{-1} (N^{-1})^* T^* = \left( (TN^{-1} (N^{-1})^* T^*)^{-1} \right)^{-1} = \left( (T^*)^{-1} N^* N T^{-1} \right)^{-1} \\ &= \left( (T^*)^{-1} N^2 T^{-1} \right)^{-1} = \left( (T^*)^{-1} T^* T T^{-1} \right)^{-1} = I^{-1} = I. \end{aligned}$$

To show the uniqueness of  $N$  and  $U$ , suppose  $T = QM$  for some unitary  $Q : V \rightarrow V$  and nonnegative  $M : V \rightarrow V$ . Then

$$T^*T = M^*Q^*QM = M^2$$

so it follows  $N = M$  by the uniqueness of the square root of  $T^*T$ . Thus  $Q = TM^{-1} = TN^{-1} = U$  as well. We now consider the case which  $T$  is singular. As before, let  $N : V \rightarrow V$  be the unique nonnegative operator such that  $T^*T = N^2$ . We construct  $U$  as follows. First, define  $U_1$  be such that  $\text{domain}(U_1) = \text{image}(N)$ . In particular, let  $U_1$  be defined by

$$w \mapsto Tv$$

provided that  $v \in V$  is such that  $w = Nv \in \text{image}(N)$ . The motivation for this is that one of the desired properties of  $U$  is

$$UNv = Tv$$

for all  $v \in V$ . We see that  $U_1$  is well-defined, since  $Tv = 0$  if and only if  $Nv = 0$ . Therefore, for any  $v, v' \in V$  such that  $Nv = Nv'$ ,

$$Nv = Nv' \iff N(v - v') = 0 \iff T(v - v') = 0 \iff Tv = Tv',$$

which exactly means that  $Uw = UNv = Tv$  is well-defined.  $U$  is clearly linear as well. Moreover, let  $W, Z \subseteq V$  be the orthogonal complements of  $\text{image}(N)$  and  $\text{image}(T)$ , respectively. Then  $\dim(W) = \text{nullity}(N)$  and  $\dim(Z) = \text{nullity}(T)$  by the rank-nullity theorem, where  $\text{nullity}(N) = \text{nullity}(T)$  by the fact that  $\ker(N) = \ker(T)$ . Thus  $W \cong Z$ , and there exists an isometry  $U_2 : W \rightarrow Z$ . We then define  $U : V \rightarrow V$  by the direct sum of  $U_1$  and  $U_2$ ,

$$U = U_1 \oplus U_2,$$

since

$$V = \text{image}(N) \oplus W = \text{image}(T) \oplus Z$$

by definition. In other words, if  $v \in V$ , then there exist unique  $y \in V$  (so that  $Ny \in \text{image}(N)$ ) and  $w \in W$  such that

$$v = Ny + w$$

by the direct sum decomposition above, and we define

$$Uv = Ty + U_2w.$$

This  $U$  is clearly linear, for  $U_1$  and  $U_2$  are linear, and we also verified that  $U$  is well-defined as well. Furthermore,

$$\begin{aligned} \langle Uv, Uv \rangle &= \langle Ty + U_2w, Ty + U_2w \rangle = \langle Ty, Ty \rangle + \langle U_2w, U_2w \rangle \\ &= \langle Ny, Ny \rangle + \langle w, w \rangle = \langle Ny + w, Ny + w \rangle = \langle v, v \rangle \end{aligned}$$

so  $U$  is unitary, and by definition

$$UNv = Tv$$

for all  $v \in V$ , as desired. ♠

#### Def'n. Polar Decomposition of a Linear Operator

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a linear operator. Then by Theorem 10.29 there exist unitary  $U : V \rightarrow V$  and nonnegative  $N : V \rightarrow V$  such that

$$T = UN,$$

which we call a *polar decomposition* of  $T$ .

**Remark 10.67.** Let  $T : V \rightarrow V$  an invertible linear operator on a finite-dimensional inner product space and suppose

$$T = UN$$

is the unique polar decomposition of  $T$ . It turns out that  $U$  and  $N$  commute if and only if  $T$  is normal. For, if  $T$  is normal, then

$$UN^2U^* = UNN^*U^* = TT^* = T^*T = N^2,$$

so

$$UN^2U = UN^2U^*(U^2) = N^2U^2 = (NU)^2,$$

which means  $NU = UN$ . Conversely, if  $NU = UN$ , then

$$TT^* = (NU)(NU)^* = NUU^*N^* = N^2 = T^*T$$

so  $T$  is normal.

**Remark 10.68.** We now proceed to prove a stronger result of the primary decomposition theorem for normal operators.

**Theorem 10.30.**  
**Primary**  
**Decomposition**  
**Theorem for Normal**  
**Operators**

Let  $V$  be a finite-dimensional inner product space and let  $N : V \rightarrow V$  be a normal operator. Let  $p \in \mathbb{K}[x]$  be the minimal polynomial of  $N$  and let  $p_1, p_2, \dots, p_k \in \mathbb{K}[x]$  be the distinct prime factors of  $p$ . Then

$$p = \prod_{i=1}^k p_i$$

Let  $W_i = \ker(p_i(N))$  for all  $i \in \{1, 2, \dots, k\}$ . Then the following hold.

- (a)  $W_i$  and  $W_j$  are orthogonal whenever  $i \neq j$ ,  $i, j \in \{1, 2, \dots, k\}$ .
- (b)  $V = \bigoplus_{i=1}^k W_i$ .
- (c)  $W_i$  is  $N$ -invariant and  $p_i$  is the minimal polynomial of the restriction of  $N$  to  $W_i$  for each  $i \in \{1, 2, \dots, k\}$ .
- (d) There exists  $e_i \in \mathbb{K}[x]$  such that  $e_i(N)$  is the orthogonal projection of  $V$  onto  $W_i$ .

**Lemma 10.30.1.**

Let  $V$  be an inner product space and let  $N : V \rightarrow V$  be normal. Then the following hold.

- (a)  $\ker(N)$  is the orthogonal complement of  $\text{image}(N)$ .
- (b) If  $v \in V$  is such that  $N^p v = 0$ , then  $Nv = 0$ .
- (c) For any  $f \in \mathbb{K}[x]$ ,  $f(N) : V \rightarrow V$  is normal.
- (d) If  $f, g \in \mathbb{K}[x]$  are coprime, then for any  $v, u \in V$  such that  $f(N)v = 0$  and  $g(N)u = 0$ ,  $\langle v, u \rangle = 0$ .

*Proof.* For (a), suppose  $v \in V$  is such that  $v$  is orthogonal to every vector in  $\text{image}(N)$ . Then for any  $u \in V$ ,  $\langle v, Nu \rangle = 0$  and so

$$\langle N^* v, u \rangle = \langle v, Nu \rangle = 0,$$

which means  $N^* v = 0$ . So  $v$  is an eigenvector of  $N^*$  corresponding to 0, so by the normality of  $N$ ,  $v$  is an eigenvector of  $N$  corresponding to  $\bar{0} = 0$ . This exactly means  $Nv = 0$ . Conversely, if  $v \in \ker(N)$ , then for any  $Nu \in \text{image}(N)$ ,

$$\langle v, Nu \rangle = \langle N^* v, u \rangle = \langle Nv, u \rangle = 0.$$

For (b), suppose that  $N^p v = 0$ . observe that  $N^{p-1}v = NN^{p-2}v \in \text{image}(N)$  and since  $N^p v = NN^{p-1}v = 0$ ,  $N^{p-1}v \in \ker(N)$  as well. So by (a),  $N^{p-1}v = 0$ . So by an induction argument,  $Nv = 0$ . For (c), let

$$f = \sum_{i=0}^k c_i x^i \in \mathbb{K}[x]$$

for some  $c_1, c_2, \dots, c_k \in \mathbb{K}$ . Then

$$f(N) = \sum_{i=0}^k c_i N^i$$

and

$$f(N)^* = \left( \sum_{i=0}^k c_i N^i \right)^* = \sum_{i=0}^k c_i (N^*)^i.$$

So  $f(N)$  and  $f(N)^*$  commute since  $N$  and  $N^*$  commute. For (d), let  $f, g \in \mathbb{K}[x]$  be coprime and let  $v, u \in V$  such that  $f(N)v = 0$  and  $g(N)u = 0$ . Then there exist  $\alpha, \beta \in \mathbb{K}[x]$  such that

$$\alpha f = \beta g = 1.$$

Therefore,

$$\alpha(N)f(N) + \beta(N)f(N) = I,$$

so

$$v = Iv = \alpha(N)f(N)v + \beta(N)g(N)v = \beta(N)g(N)v.$$

It follows that

$$\langle v, u \rangle = \langle \beta(N)g(N)v, u \rangle = \langle g(N)\beta(N)v, u \rangle = \langle \beta(N)v, g(N)^*u \rangle.$$

Since  $g(N)u = 0$ , the normality of  $g(N)$  by (c) implies that  $g(N)^* = 0$  as well. Thus  $\langle v, u \rangle = 0$ . ♠

**Proof of Theorem  
10.30 Begins Here**

*Proof of Theorem 10.30.* We first verify that

$$p = \prod_{i=1}^k p_i.$$

Suppose, for the sake of contradiction, there exists  $i \in \{1, 2, \dots, k\}$  such that

$$p_i^s \mid p$$

for some  $s \in \mathbb{N}$ ,  $s \geq 2$ . Then there exists  $g \in \mathbb{K}[x]$  such that

$$p = p_i^s g,$$

and for all  $v \in V$ ,

$$p(N)v = p_i^s(N)g(N)v = 0.$$

By (c) of Lemma 10.30.1,  $p_i^s(N)$  is normal. Thus by (b) of Lemma 10.30.1,

$$p_i(N)g(N)v = 0,$$

which clearly is a contradiction., since the minimality of  $p$  is violated. Thus

$$p = \prod_{i=1}^k p_i.$$

Of course,  $\deg(p_i) \leq 2$  for each  $i \in \{1, 2, \dots, k\}$ . For (a), observe that (d) of Lemma 10.30.4 is equivalent to the result that, if  $f, g \in \mathbb{K}[x]$  are coprime, then  $\ker(f(T))$  and  $\ker(g(T))$  are orthogonal, whenever  $T : V \rightarrow V$  is normal. But since  $p_1, p_2, \dots, p_k$  are distinct prime polynomials,  $p_i$  and  $p_j$  are coprime whenever  $i \neq j$ . So  $W_i = \ker(p_i(N))$  and  $W_j = \ker(p_j(N))$  are orthogonal. For (b), let

$$f_i = \prod_{j=1, j \neq i}^k p_j \in \mathbb{K}[x]$$

then  $f_1, f_2, \dots, f_k$  are coprime by construction, so there exist  $g_1, g_2, \dots, g_k \in \mathbb{K}[x]$  such that

$$\sum_{i=1}^k f_i g_i = 1.$$

So for any  $v \in V$ ,

$$v = Iv = \left( \sum_{i=1}^k f_i(N)g_i(N) \right) v = \sum_{i=1}^k f_i(N)g_i(N)v.$$

But  $p = p_i f_i$  for any  $i \in \{1, 2, \dots, k\}$ , so  $p_i(N)f_i(N) = p(N) = 0$ . It follows that

$$p_i(N)f_i(N)g_i(N)v = 0,$$

so  $f_i(N)g_i(N)v \in \ker(p_i(N)) = W_i$  for all  $i \in \{1, 2, \dots, k\}$ ,  $v \in V$ . But (a) provides that  $W_1, W_2, \dots, W_k$  are independent, so

$$V = \bigoplus_{i=1}^k W_i.$$

For (c), let  $i \in \{1, 2, \dots, k\}$ , let  $N_i : W_i \rightarrow W_i$  be the restriction of  $N$  to  $W_i$ , and let  $w_i \in W_i$ . Then  $p_i(N)w_i = 0$  and so

$$p_i(N)Nw_i = Np_i(N)w_i = 0,$$

so  $W_i$  is  $N$ -invariant. Moreover, since  $p_i(N_i) = p_i(N) = 0$  on  $W_i$  by definition,  $p_i$  divides the minimal polynomial of  $N_i$ . But  $p_i$  is prime, so  $p_i$  is the minimal polynomial of  $N_i$ . For (d), let  $i \in \{1, 2, \dots, k\}$  and let  $e_i = f_i g_i \in \mathbb{K}[x]$ . Then for any  $v \in V$ ,  $e_i(N)v = f_i(N)g_i(N)v \in W_i$  and


$$v = \sum_{j=1}^k f_j(N)g_j(N)v = \sum_{j=1}^k e_j(N)v$$

which exactly means

$$v - e_i(N)v = \sum_{j=1, j \neq i}^k e_j(N)v.$$

But  $W_j$  is orthogonal to  $W_i$  whenever  $i \neq j$ ,  $j \in \{1, 2, \dots, k\}$ , so

$$v - e_i(N)v - \sum_{j=1, j \neq i}^k e_j(N)v \in W_{i\perp},$$

where  $W_{i\perp}$  is the orthogonal complement of  $W_i$ . Thus it follows Corollary 10.4.1 that  $e_i(N)$  is the projection of  $V$  on  $W_i$ . 

**Def'n. Primary Component** of an Inner Product Space under a Normal Operator

Consider Theorem 10.30. We call  $W_1, W_2, \dots, W_k \subseteq V$  the **primary component** of  $V$  under  $T$ .


### Corollary 10.30.2.

Let  $T : V \rightarrow V$  be a normal operator on a finite-dimensional inner product space  $V$  and let  $W_1, W_2, \dots, W_k \subseteq V$  be the primary components of  $W$  under  $T$ . Suppose  $W \subseteq V$  is a  $T$ -invariant subspace. Then

$$W = \sum_{i=1}^k W \cap W_i.$$

*Proof.* It is clear that each  $W \cap W_i \subseteq W$  so  $\sum_{i=1}^k W \cap W_i \subseteq W$ . To show that  $W \subseteq \sum_{i=1}^k W \cap W_i$ , observe that  $W$  is invariant under any polynomial in  $T$ , and, in particular,  $W$  is invariant under each  $e_i(T)$ , the projection of  $V$  on  $W_i$ . Since

$$w = \sum_{i=1}^k e_i(T)w$$

for any  $w \in W$ , where each  $e_i(T)w \in W \cap W_i$ , it follows that  $W \subseteq \sum_{i=1}^k W \cap W_i$ . Thus  $W = \sum_{i=1}^k W \cap W_i$ , as desired. 

**Remark 10.69.** Theorem 10.30 shows that every normal operator  $T : V \rightarrow V$  on a finite-dimensional inner product space is canonically associated with normal operators  $T_1, T_2, \dots, T_k$  on  $W_1, W_2, \dots, W_k \subseteq V$ , the primary components of  $V$  under  $T$ . Moreover, the minimal polynomial  $p_i \in \mathbb{K}[x]$  for  $W_i$  is prime over  $\mathbb{K}$ . To complete our understanding of normal operators, it is necessary to study normal operators of this particular type. A normal operator whose minimal polynomial is of degree 1 is clearly a scalar multiple of the identity operator (indeed, any operator is a scalar multiple of the identity if its minimal polynomial is of degree 1). On the other hand, when the minimal polynomial of a normal operator is of degree 2, the situation is more complicated.

**Example 10.70.** Let  $r \in \mathbb{R}$  be positive and let  $\theta \in \mathbb{R}$  be such that  $\theta \neq k\pi$  for any  $k \in \mathbb{Z}$ . Let  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  be such that

$$[T]_\beta = r \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix},$$

where  $\beta$  is the standard ordered basis for  $\mathbb{R}^2$ . Then  $T$  is orthogonal, and, hence, normal. Let  $p \in \mathbb{R}[x]$  be the characteristic polynomial of  $T$ . Then

$$\begin{aligned} p(x) &= \det(xI - [T]_\beta) = \det \begin{bmatrix} x - r\cos(\theta) & r\sin(\theta) \\ -r\sin(\theta) & x - r\cos(\theta) \end{bmatrix} = (x - r\cos(\theta))^2 + r^2\sin^2(\theta) \\ &= x^2 - 2r\cos(\theta)x + r^2\cos^2(\theta) + r^2\sin^2(\theta) = x^2 - 2r\cos(\theta)x + r^2. \end{aligned}$$

Let  $a = r\cos(\theta)$ ,  $b = r\sin(\theta)$ , and  $c = a + bi$ . Then  $b = r\sin(\theta) \neq 0$  since  $\theta \neq k\pi$  for any  $k \in \mathbb{Z}$ ,  $c = re^{i\theta} \in \mathbb{C}$ , and

$$[T]_\beta = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Moreover,  $p = (x - c)(x - \bar{c})$ , so  $p$  is prime over  $\mathbb{R}$ . Since  $p$  is divisible by the minimal polynomial, it follows that  $p$  is the minimal polynomial of  $T$  as well.

**Proposition 10.31.**

*Let  $T : V \rightarrow V$  be a normal operator on a finite-dimensional inner product space  $V$  over  $\mathbb{R}$  and let  $p \in \mathbb{R}[x]$  be the minimal polynomial of  $T$ . Suppose*

$$p = (x - a)^2 + b^2$$

*for some  $a, b \in \mathbb{R}$ ,  $b \neq 0$ . Then there exists  $k \in \mathbb{N}$  such that  $p^k \in \mathbb{R}[x]$  is the characteristic polynomial for  $T$ . Moreover, there exists subspaces  $W_1, W_2, \dots, W_k \in V$  such that*

- (a)  $W_i$  and  $W_j$  are orthogonal whenever  $i \neq j$ ,  $i, j \in \{1, 2, \dots, k\}$ ,
- (b)  $V = \bigoplus_{i=1}^k W_i$ , and
- (c) each  $W_i$  has an orthonormal basis  $\{v_i, w_i\}$  such that

$$\begin{cases} Tv_i &= av_i + bw_i \\ Tw_i &= -bv_i + aw_i \\ T^*v_i &= av_i - bw_i \\ T^*w_i &= bv_i + aw_i \end{cases}.$$

**Lemma 10.31.1.**

*Let  $V$  be an inner product space over  $\mathbb{R}$  and let  $T : V \rightarrow V$  be a normal operator such that  $T^2 + I = 0$ . Let  $v \in V$  be arbitrary and let  $w = Tv \in \text{image}(T)$ . Then*

$$\begin{cases} T^*v &= -w \\ T^*w &= v \end{cases},$$

*$\langle v, w \rangle = 0$ , and  $\|v\| = \|w\|$ .*

*Proof.* Observe that

$$T^2v = T^2v - (T^2 + I)v = -v$$

and  $Tv = w$  by definition. So  $\|Tv - w\| = \|T^2v + v\| = \|Tw + v\| = 0$ , and so

$$\begin{aligned} 0 &= \|Tv - w\|^2 + \|Tw + v\|^2 = \langle Tv - w, Tv - w \rangle + \langle Tw + v, Tw + v \rangle \\ &= \|Tv\|^2 - 2\langle Tv, w \rangle + \|w\|^2 + \|Tw\|^2 + \langle Tw, v \rangle + \|v\|^2. \end{aligned}$$

Since  $T$  is normal,  $\|Tz\|^2 = \|Tdz\|^2$  and  $\langle Ty, z \rangle = \langle z, Ty \rangle = \langle T^*z, y \rangle$  for any  $y, z \in V$ , and so

$$\begin{aligned} 0 &= \|Tv\|^2 - 2\langle Tv, w \rangle + \|w\|^2 + \|Tw\|^2 + \langle Tw, v \rangle + \|v\|^2 \\ &= \|T^*v\|^2 - 2\langle T^*w, v \rangle + \|w\|^2 + \|T^*w\|^2 + \langle T^*v, w \rangle + \|v\|^2 \\ &= \|T^*v\|^2 + 2\langle T^*v, w \rangle + \|w\|^2 + \|T^*w\|^2 - \langle T^*w, v \rangle + \|v\|^2 \\ &= \|T^*v + w\|^2 + \|T^*w - v\|^2. \end{aligned}$$

So  $T^*v = -w$  and  $T^*w = v$ . Moreover,

$$\langle v, w \rangle = \langle T^*w, w \rangle = \langle w, Tw \rangle = \langle w, T^2v \rangle = \langle w, -v \rangle = \langle -v, w \rangle = -\langle v, w \rangle,$$

which exactly means  $\langle v, w \rangle = 0$ . Similarly,

$$\|v\|^2 = \langle v, v \rangle = \langle T^*w, v \rangle = \langle w, Tv \rangle = \langle w, w \rangle = \|w\|^2,$$

as desired. ♠

### Proof of Proposition 10.31 Begins Here

*Proof of Proposition 10.31.* Let  $W_1, W_2, \dots, W_k \subseteq V$  be subspaces such that  $k \in \mathbb{N}$  is the maximum number of subspaces satisfying (a) and (c). Let  $W = \bigoplus_{i=1}^k W_i$ . We claim that  $W = V$ . To verify this, suppose  $W \subsetneq V$  for the sake of contradiction. Then  $W_\perp \neq \{0\}$ , the orthogonal complement of  $W$ . Moreover, (c) implies that  $W$  is invariant under  $T$  and  $T^*$ ,  $W_\perp$  is invariant under  $T^*$  and  $(T^*)^* = T$ . Now, let

$$S = \frac{1}{b}(T - aI) : V \rightarrow V.$$

Then  $S^* = \frac{1}{b}(T^* - aI)$ ,  $S$  is normal, and  $W_\perp$  is invariant under  $S$  and  $S^*$ . Since  $p(T) = (T - aI)^2 + b^2I = 0$ , it follows that

$$S^2 + I = \frac{1}{b^2}(T - aI)^2 + I = \frac{1}{b}((T - aI)^2 + bI) = 0.$$

Let  $v \in W_\perp$  be any unit vector (i.e.  $\|v\| = 1$ ) and let  $w = Sv$ . Then  $w \in W_\perp$  and  $Sw = -v$ . Since

$$aI + bS = aI + b\left(\frac{1}{b}(T - aI)\right) = T,$$

we have

$$\begin{cases} Tv &= (aI + bS)v = av + bw \\ Tw &= (aI + bS)w = aw - bv = -bv + aw \end{cases}.$$

By Lemma 10.31.1,  $S^*v = -w$ ,  $S^*w = v$ ,  $\langle v, w \rangle = 0$  and  $\|w\| = \|v\| = 1$ . But  $T^* = aI + bS^*$ , it follows that

$$\begin{cases} T^*v &= av - bw \\ T^*w &= bv + aw \end{cases}.$$

However, this means  $Z = \text{span}\{v, w\}$  is a subspace which satisfies (a) and (c). This violates the maximality of  $k$ , so we have a contradiction. Thus,

$$V = W = \bigoplus_{i=1}^k W_i,$$

and it is clear that each  $T_i : W_i \rightarrow W_i$ , the restriction of  $T$  on  $W_i$ , has characteristic polynomial  $p_i = p = (x - a)^2 + b^2$ . Thus it follows from the above direct sum decomposition that

$$\det(xI - T) = \left((x - a)^2 + b^2\right)^k$$



is the characteristic polynomial of  $T$ . ♠

**Remark 10.71.** Consider Proposition 10.31. Another way to state the proposition is that, if  $r, \theta \in \mathbb{R}$  are such that  $r = \sqrt{a^2 + b^2}$ ,  $a = r \cos(\theta)$ , and  $b = r \sin(\theta)$ , then  $V$  is a direct sum

$$V = \bigoplus_{i=1}^k W_i$$

of orthogonal 2-dimensional subspaces  $W_i$ , and on each  $W_i$   $T$  acts as  $r$  times rotation through the angle  $\theta$ .

**Corollary 10.31.2.**

Consider Proposition 10.31. Then  $T$  is invertible and

$$T^* = (a^2 + b^2) T^{-1}.$$

*Proof.* Observe that

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a^2 + b^2 & 0 \\ 0 & a^2 + b^2 \end{bmatrix}.$$

So by (c) of Proposition 10.31,  $TT^* = (a^2 + b^2)I$ . Thus  $T$  is invertible and  $T^* = (a^2 + b^2) T^{-1}$ . ♠

**Proposition 10.32.**

Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a normal operator.

- (a) Any linear  $S : V \rightarrow V$  commutes with  $T$  commutes with  $T^*$ .
- (b) Any  $T$ -invariant subspace  $W \subseteq V$  is also  $T^*$ -invariant.

*Proof.* For (a), let  $i \in \{1, 2, \dots, k\}$ ,  $W_i \subseteq V$  be a primary component of  $V$  under  $T$ , and  $E_i : W_i \rightarrow W_i$  be the orthogonal projection of  $V$  on  $W_i$ . Then  $E_i$  is a polynomial in  $T$ , so  $S$  commutes with  $E_i$ . Therefore,

$$E_i S E_i = S E_i^2 = S E_i,$$

which means  $W_i$  is  $S$ -invariant. Let  $T_i, S_i : W_i \rightarrow W_i$  be the restrictions of  $T$  and  $S$  on  $W_i$ , respectively. Then  $S_i$  commutes with  $T_i$ . By Theorem 10.30, the minimal polynomial  $p_i \in \mathbb{K}[x]$  of  $T_i$  is of degree 1 or 2. If  $\deg(p_i) = 1$ , then  $T_i = c_i I$  for some  $c_i \in \mathbb{K}$  and clearly  $S_i$  commutes with  $T_i^* = \overline{c_i} I$ . So suppose  $\deg(p_i) = 2$ . Then by Corollary 10.31.2, there exist  $a_i, b_i \in \mathbb{K}$  such that

$$T_i^* = (a_i^2 + b_i^2) T_i^{-1}.$$

Since  $S_i$  commutes with  $T_i$  if and only if  $S_i$  commutes with  $T_i^{-1}$ , it follows that  $S_i$  commutes with  $T_i^{-1}$  as well. So in conclusion,  $S_i$  commutes with  $T_i$  regardless of  $\deg(p_i)$ . Also,  $T_i^*$  commutes with  $E_i$ , and so

$$E_i T_i^* E_i = T_i^* E_i^2 = T_i^* E_i,$$

which means  $W_i$  is a  $T_i^*$ -invariant. Moreover, for any  $v_i, w_i \in W_i$ ,

$$\langle T_i v_i, w_i \rangle = \langle T v_i, w_i \rangle = \langle v_i, T^* w_i \rangle = \langle v_i, T_i^* w_i \rangle,$$

so  $T_i^* : W_i \rightarrow W_i$  is the restriction of  $T^*$  on  $W_i$ . Thus,

$$S T^* w_i = S_i T_i^* w_i = T_i^* S_i w_i = T^* S w_i$$

for any  $w_i \in W_i$ . But  $V = \bigoplus_{i=1}^k W_i$ , so

$$ST^*v = T^*Sv$$

for any  $v \in V$ . So  $U$  commutes with  $T^*$ . For (b), suppose that  $W \subseteq V$  is a  $T$ -invariant subspace and let  $Z_i = W \cap W_i$  for each  $i \in \{1, 2, \dots, k\}$ . Then  $Z_i$  is  $T_i$ -invariant. Moreover, by Corollary 10.30.2,  $W = \sum_{i=1}^k Z_i$ , so it is sufficient to verify that each  $Z_i$  is  $T_i^*$ -invariant. If  $\deg(p_i) = 1$ , then  $T_i = c_i I$  for some  $c_i \in \mathbb{K}$ , and clearly  $Z_i$  is invariant under  $T_i^* = \bar{c}_i I$ . On the other hand, if  $\deg(p_i) = 2$ , then  $T_i$  is invertible and

$$T_i^* = (a_i^2 + b_i^2) T_i^{-1}$$

for some  $a_i, b_i \in \mathbb{K}$ . But by the invertibility of  $T_i$  and  $T_i$ -invariance of  $Z_i$ ,  $Z_i$  is  $T_i^{-1}$ -invariant, and hence  $T^*$ -invariant as well. ♠

**Remark 10.72.** Suppose  $T : V \rightarrow V$  is a normal operator on a finite-dimensional inner product space  $V$  and let  $W \subseteq V$  be a  $T$ -invariant subspace. Then (b) of Proposition 10.32 shows that  $W$  is invariant under  $T^*$ , and that  $W_\perp \subseteq V$ , the orthogonal complement of  $W$ , is invariant under  $T^*$  and  $T^{**} = T$ . One can use this fact to provide a stronger version of the cyclic decomposition theorem of normal operators.

**Theorem 10.33.**  
**Cyclic Decomposition**  
**Theorem for Normal**  
**Operators**

*Let  $V$  be a finite-dimensional inner product space and let  $T : V \rightarrow V$  be a normal operator. Then there exists nonzero  $v_1, v_2, \dots, v_k \in V$  and respective  $T$ -annihilators  $e_1, e_2, \dots, e_k \in \mathbb{K}[x]$  for some  $k \in \mathbb{N}$  such that the following holds.*

- (a)  $V = \bigoplus_{i=1}^k Z(v_i; T)$ .
- (b) For each  $i \in \{2, 3, \dots, k\}$ ,  $e_{i+1} \mid e_i$ .
- (c)  $Z(v_i; T)$  is orthogonal to  $Z(v_j; T)$  whenever  $i \neq j$ .
- (d) The integer  $k$  and the  $T$ -annihilators  $e_1, e_2, \dots, e_k$  are uniquely determined by (a), (b), and the fact that every  $v_i$  is nonzero.

*Proof.* Let  $p \in \mathbb{K}[x]$  be the minimal polynomial of  $T$ . Then the cyclic decomposition theorem provides that there exists  $v_1 \in V$  such that  $e_1 = p_1$  is the  $T$ -annihilator of  $v_1$ . Since  $Z(v_1; T)$  is  $T$ -invariant, it is also  $T^*$ -invariant. Moreover, Remark 10.71 provides that  $W$ , the orthogonal complement of  $Z(v_1; T)$ , is also invariant under  $T$  and  $T^*$ , and  $T_W : W \rightarrow W$ , the restriction of  $T$  on  $W$ , is normal. Then the cyclic decomposition theorem provides again that there exists  $v_2 \in W$  such that the minimal polynomial  $p_2 \in \mathbb{K}[x]$  of  $T_W$  is such that  $e_2 = p_2$  is the  $T_W$ -annihilator of  $v_2$ . Since  $p_1$  annihilates  $T$ , it annihilates  $T_W$  as well, so  $p_2 \mid p_1$ . Furthermore,  $Z(v_1; T)$  and  $Z(v_2; T) = Z(v_2; T_W)$  are orthogonal by construction. Thus by continuing this process, we get

$$V = \bigoplus_{i=1}^k Z(v_i; T)$$

which satisfies (b) and (c). Moreover, (d) is provided by the cyclic decomposition theorem. ♠

**Def'n. Unitarily Equivalent Linear Operators**

Let  $V$  and  $V'$  be inner product spaces over  $\mathbb{K}$  and let  $T : V \rightarrow V$  and  $T' : V' \rightarrow V'$  be linear. We say  $T$  and  $T'$  are **unitarily equivalent** if there exists a unitary transformation  $U : V \rightarrow V'$  such that

$$UTU^{-1} = T'.$$

**Proposition 10.34.**

Let  $V$  and  $V'$  be finite-dimensional inner product spaces over  $\mathbb{K}$  and let  $T : V \rightarrow V$ ,  $T' : V' \rightarrow V'$  be linear. Then  $T$  is unitarily equivalent to  $T'$  if and only if there exist orthonormal bases  $\beta$  and  $\beta'$  for  $V$  and  $V'$ , respectively, such that

$$[T]_{\beta} = [T']_{\beta'}.$$

*Proof.* For the forward direction, suppose that there exists a unitary transformation  $U : V \rightarrow V$  such that

$$UTU^{-1} = T'.$$

Let  $\beta = \{v_1, v_2, \dots, v_n\}$  be any orthonormal basis for  $V$  and let

$$\beta' = \{v'_1, v'_2, \dots, v'_n\} = U\beta = \{Uv_1, Uv_2, \dots, Uv_n\}.$$

Since  $U$  is unitary,  $\beta'$  is an orthonormal basis for  $V'$ . Moreover,  $[T]_{\beta}$  is characterized by the fact that

$$Tv_i = \sum_{j=1}^n ([T]_{\beta})_{ji} v_j$$

for all  $i \in \{1, 2, \dots, n\}$ . But

$$T'v'_i = UTU^{-1}v_i = U \sum_{j=1}^n ([T]_{\beta})_{ji} v_j = \sum_{j=1}^n ([T]_{\beta})_{ji} Uv_j = \sum_{j=1}^n ([T]_{\beta})_{ji} v'_j,$$

so  $[T]_{\beta} = [T']_{\beta'}$ . For the reverse direction, let  $\beta = \{v_1, v_2, \dots, v_n\}$  and  $\beta' = \{v'_1, v'_2, \dots, v'_n\}$  be orthonormal bases for  $V$  and  $V'$ , respectively, such that

$$[T]_{\beta} = [T']_{\beta'}.$$

Define  $U : V \rightarrow V'$  by

$$v_i \mapsto v'_i$$

for each  $i \in \{1, 2, \dots, n\}$ . Then

$$UTU^{-1}v'_i = UTv_i = U \sum_{j=1}^n ([T]_{\beta})_{ji} v_j = \sum_{j=1}^n ([T]_{\beta})_{ji} Uv_j = \sum_{j=1}^n ([T]_{\beta})_{ji} v'_j.$$

But  $[T]_{\beta} = [T']_{\beta'}$ , so it follows that  $T' = UTU^{-1}$ , as desired. ♠

**Remark 10.73.** An immediate consequence of Proposition 10.34 is that unitarily equivalent operators on finite-dimensional inner product spaces have the same characteristic polynomial. For normal unitarily equivalent operators, the converse is also true.

**Theorem 10.35.**

Let  $V$  and  $V'$  be finite-dimensional inner product spaces over  $\mathbb{K}$  and let  $T : V \rightarrow V$  and  $T' : V' \rightarrow V'$  be normal operators. Then  $T$  and  $T'$  are unitarily equivalent if and only if  $T$  and  $T'$  have the same characteristic polynomials.

*Proof.* Observe that the forward direction is supplied by Remark 10.73. To verify the reverse direction, suppose that  $T$  and  $T'$  have the same characteristic polynomial  $f \in \mathbb{K}[x]$ . Let  $W_1, W_2, \dots, W_k \subseteq V$  be the primary components of  $V$  under  $T$  and  $T_1, T_2, \dots, T_k$  be the restriction of  $T$  on  $W_1, W_2, \dots, W_k$ . Then

$$f = \prod_{i=1}^k \det(xI_i - T_i),$$

where each  $I_i$  is the identity operator on  $W_i$ . Let  $i \in \{1, 2, \dots, k\}$  and  $p_i \in \mathbb{K}[x]$  be the minimal polynomial for  $T_i$ . If  $\deg(p_i) = 1$ , then it is clear that

$$\det(xI_i - T_i) = p_i^{s_i} = (x - c_i)^{s_i}$$

for some  $c_i \in \mathbb{K}$  and  $s_i = \dim(W_i)$ . If  $\deg(p_i) = 2$ , then  $p_i = (x - a_i)^2 + b_i^2$  for some  $a_i, b_i \in \mathbb{R} \subseteq \mathbb{K}$ ,  $b_i \neq 0$ , and

$$\det(xI_i - T_i) = \left((x - a_i)^2 + b_i^2\right)^{s_i},$$

where  $s_i = \frac{1}{2} \dim(W_i) \in \mathbb{N}$ . Therefore,

$$f = \prod_{i=1}^k p_i^{s_i}.$$

But we may also calculate  $f$  by the same method using the primary components of  $V'$  under  $T'$ . Since  $p_1, p_2, \dots, p_k$  are distinct prime polynomials, the uniqueness of prime factorization of polynomials implies that there exist  $k$  primary components  $W'_1, W'_2, \dots, W'_k \subseteq V'$  of  $V'$  under  $T'$ , and by reordering, they can be indexed such that  $p'_i = p_i$  is the minimal polynomial for  $T'_i$ , the restriction of  $T'$  on  $W'_i$ , for all  $i \in \{1, 2, \dots, k\}$ . Let  $i \in \{1, 2, \dots, k\}$  be arbitrary. If  $\deg(p_i) = 1$ , then  $p = x - c_i$  for some  $c_i \in \mathbb{K}$ , and it is clear that

$$T'_i = c_i I'_i$$

and

$$T_i = c_i I_i$$

are unitarily equivalent, where  $I_1, I_2, \dots, I_k$  are the identity operators on  $W_1, W_2, \dots, W_k$ , respectively. On the other hand, if  $\deg(p_i) = 2$ , then  $p_i = (x - a_i)^2 + b_i^2$  for some  $a_i, b_i \in \mathbb{R} \subseteq \mathbb{K}$ ,  $b_i \neq 0$ . But (c) of Proposition 10.31 guarantees the existence of orthonormal bases  $\beta_i$  and  $\beta'_i$  for  $W_i$  and  $W'_i$ , respectively, such that

$$[T_i]_{\beta_i} = [T'_i]_{\beta'_i}.$$

But this exactly means

$$[T]_{\beta} = \bigoplus_{i=1}^k [T_i]_{\beta_i} = \bigoplus_{i=1}^k [T'_i]_{\beta'_i} = [T']_{\beta'},$$

where  $\beta = \{\beta_1, \beta_2, \dots, \beta_k\}$  and  $\beta' = \{\beta'_1, \beta'_2, \dots, \beta'_k\}$ . ♠

**Remark 10.74.** Another way to show that  $T$  and  $T'$  are unitarily equivalent is to construct  $U : V \rightarrow V'$  by mappings

$$\begin{aligned} v_i &\mapsto v'_i \\ w_i &\mapsto w'_i \end{aligned}$$

provided that  $\beta_i = \{v_i, w_i\}$  and  $\beta'_i = \{v'_i, w'_i\}$  satisfying

$$[T_i]_{\beta_i} = [T'_i]_{\beta'_i}.$$