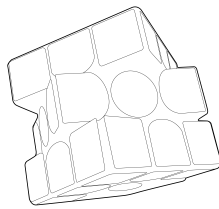


Linear Algebra II

Snochi Song



This page intentionally left blank.

Contents

1	Polynomials	
1.1	Algebras	4
1.2	Polynomial Space	5
1.3	Lagrange Interpolation	7
1.4	Polynomial Ideals	8
2	Elementary Canonical Forms	
2.1	Annihilating Polynomials	18
2.2	Characteristic Polynomial and Cayley-Hamilton Theorem	18
2.3	Triangulation and Diagonalization	21
2.4	Direct Sum Decompositions	23
2.5	Invariant Direct Sum	26
2.6	Primary Decomposition Theorem	30
3	The Rational and Jordan Form	
3.1	Cyclic Subspaces and Annihilators	36
3.2	Cyclic Decomposition and the Rational Form	41
3.3	Jordan Form	51
4	Bilinear Form	
4.1	Bilinear Forms	58
4.2	Symmetric Bilinear Form	64
4.3	Skew-Symmetric Bilinear Form	70
4.4	Groups Preserving Bilinear Forms	73
5	Inner Product Spaces	
5.1	Inner Products	76
5.2	Inner Product Spaces	80
5.3	Linear Functionals and Adjoints	88
5.4	Unitary Operators	93

This page intentionally left blank.

1. Polynomials

-
- 1.1 Algebras
 - 1.2 Polynomial Space
 - 1.3 Lagrange Interpolation
 - 1.4 Polynomial Ideals
-

Algebras

Def'n. Linear Algebra over a Field

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

(a) Multiplication is associative.

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

(b) Multiplication is distributive with respect to addition.

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

(c) Multiplication is compatible with respect to scalar multiplication.

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

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 1.1. 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}^∞ . 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 1.1. Space of Sequences

Let \mathbb{F}^∞ be the space 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}^∞ is an infinite-dimensional, unital, and commutative algebra over \mathbb{F} .

Proof. To verify that \mathbb{F}^∞ 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}^∞ . 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 1.2. 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.

Polynomial Space

Def'n. Polynomial Space

We call the subspace of \mathbb{F}^∞ spanned by $\{1, x, x^2, \dots\}$ the *polynomial space* and denote which by $\mathbb{F}[x]$. Notice that $f \in \mathbb{F}^\infty$ is an element of $\mathbb{F}[x]$ 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 $n \in \mathbb{N}$.

Remark 1.3.

- (a) $\mathbb{F}[x] \subsetneq \mathbb{F}^\infty$.
- (b) $\mathbb{F}[x]$ 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 $a_n \neq 0$, we say n is the *degree* of f and denote as $\deg(f) = n$.

Remark 1.4. 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 1.2.
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 $\deg(f + g) \leq \max(\deg(f), \deg(g))$.

Proof. To verify (1), 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 (2) and (3) are true as well. To verify (4), suppose that $\deg(f) = n \geq m = \deg(g)$ without loss of generality. Then for each $k \in \mathbb{N}$,

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

Remark 1.5. (1) of Proposition 1.2 shows that $\mathbb{F}[x]$ is an integral domain. That is, $\mathbb{F}[x]$ has a cancellative property.

Corollary 1.2.1.
 $\mathbb{F}[x]$ 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}^∞ . 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 1.6. 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 1.3.
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 $c \in \mathbb{F}$. Then the following hold.

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

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

Proof. (1) is a direct result of componentwise addition. To verify (2), 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

Theorem 1.4.
Lagrange
Interpolation

Let $F_n[x]$ be the vector space spanned by $\{1, x, x^2, \dots, x^n\}$ over a field \mathbb{F} with at least $n+1$ elements. Let $t_0, t_1, \dots, t_n \in \mathbb{F}$ be distinct. Define linear $L_j : F_n[x] \rightarrow \mathbb{F}$ by

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

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

Proof. We proceed to show that $\{L_0, L_1, \dots, L_n\}$ is the dual of a basis for $F_n[x]$. For each $j \in \{0, 1, \dots, n\}$, define $p_i \in F_n[x]$ by

$$p_i = \prod_{j=0, j \neq i}^n \frac{x - t_j}{t_i - t_j}.$$

This is well-defined since each t_j is distinct. Then,

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

by construction. Let $f = \sum_{i=0}^n c_i p_i \in \text{span}\{p_0, p_1, \dots, p_n\}$. Then,

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

Since $0 \in \mathbb{F}_n[x]$ has the property

$$\forall c \in \mathbb{F} [0(t) = 0],$$

it follows that $\{p_0, p_1, \dots, p_n\}$ is linearly independent. Moreover, since

$$|\{p_0, p_1, \dots, p_n\}| = n + 1 = \dim(\mathbb{F}_n[x]),$$

$\{p_0, p_1, \dots, p_n\}$ is a basis for $\mathbb{F}_n[x]$. Notice that

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

by construction. That is, $\{L_0, L_1, \dots, L_n\}$ is the dual of $\{p_0, p_1, \dots, p_n\}$, as desired. ♠

Corollary 1.4.1.
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 1.4.2.
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 Theorem 1.4. Then for each $f \in \mathbb{F}[x]$,

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

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 1.7. 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 1.8. 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 1.3, $(fg)(t) = f(t)g(t)$, and thus

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

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

Polynomial Ideals

Lemma 1.5.

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 $\deg(f - dg) < \deg(f)$. ♠

Theorem 1.6.
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 $\deg(r) < \deg(d)$.

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 1.5, 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 1.6. 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

$$f = dq.$$

By Theorem 1.6, the existence of such q guarantees its uniqueness.

Corollary 1.6.1. 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 1.6.2. 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 1.9. 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

$$\forall f \in \{p \in \mathbb{F}[x] : \deg(p) \geq 1\} [\exists c \in \mathbb{F}, f(c) = 0].$$

In other words, every polynomial of nonzero degree always have a root when it is defined over an algebraically closed field.

Def'n. Formal Differentiation

The linear operator $D : \mathbb{F}[x] \rightarrow \mathbb{F}[x]$ defined as

$$D \left[\sum_{i=0}^n a_i x^i \right] := \sum_{i=1}^n i a_i x^{i-1}$$

is called the *formal differentiation*.

**Theorem 1.7.
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 1.8.
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 1.9. Characterization of Multiplicity

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

$$[\forall i \in \{0, 1, \dots, r-1\} [D^i f(c) = 0]] \wedge [D^r f(c) \neq 0].$$

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 1.10. 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 1.11.
Every Nontrivial Ideal
Is Principal and
Generated by a Monic
Polynomial

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 1.11.1.
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 1.10. 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 1.12.
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 1.13.
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 1.10. Every polynomial with degree 1 is prime.

Proposition 1.14.
Alternative Definition
of Prime

Let $f, g, h \in \mathbb{F}[x]$ and f be prime. Then $f \mid gh \implies f \mid g \vee f \mid h$.

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 1.14.1.
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 1.13,

$$f \mid \prod_{i=1}^m p_i \vee f \mid p_{m+1}$$

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 1.15.
Primary
Decomposition of a
Monic Polynomial

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 $\deg(p), \deg(q) \leq m$, 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 $j \in \{1, 2, \dots, r\}$, $q_j = p_i$ 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. ♠

Proposition 1.16.
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 1.17.
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 $f \in \mathbb{F}[x]$, $f = c(x - c_1)^{p_1}(x - c_2)^{p_2} \cdots (x - c_n)^{p_n}$ for some $c_1, c_2, \dots, c_n \in \mathbb{F}$ and $p_1, p_2, \dots, p_n \in \mathbb{N}$.
- (c) Every prime polynomial of $\mathbb{F}[x]$ has degree 1.

Exercises

Exercise 1.11. Verify the existence of the formal differentiation $D : \mathbb{F}[x] \rightarrow \mathbb{F}[x]$.

Exercise 1.12. Verify the formula

$$\sum_{i,j} f_i g_j x^{i+j} = \left(\sum_{i=0}^n f_i x^i \right) \left(\sum_{j=1}^m g_j x^j \right).$$

Exercise 1.13. For any $c \in \mathbb{F}$, verify $\{1, (x-c), (x-c)^2, \dots, (x-c)^k\}$ is a basis for $\mathbb{F}_n[x]$.

Exercise 1.14. Let V be a n -dimensional vector space over \mathbb{F} , β be an ordered basis for V , and $T : V \rightarrow V$ be a linear operator. Verify that

$$[f(T)]_{\beta} = f\left([T]_{\beta}\right).$$

Exercise 1.15. Let $d_1, d_2, \dots, d_n \in \mathbb{F}[x]$. Verify that $\langle d_1, d_2, \dots, d_n \rangle$ is an ideal of $\mathbb{F}[x]$

Exercise 1.16. Verify that $f = x^2 + 1 \in \mathbb{R}[x]$ is prime.

2.

Elementary Canonical Forms

-
- 2.1 Annihilating Polynomials
 - 2.2 Characteristic Polynomial and Cayley-Hamilton Theorem
 - 2.3 Triangulation and Diagonalization
 - 2.4 Direct Sum Decompositions
 - 2.5 Invariant Direct Sum
 - 2.6 Primary Decomposition Theorem
-

Annihilating Polynomials

Def'n. Annihilating Polynomial

Let \mathcal{A} be a unital algebra over \mathbb{F} and let $\alpha \in \mathcal{A}$. We say $f \in \mathbb{F}[x]$ is an *annihilating* polynomial for α if $f(\alpha) = 0$.

Proposition 2.1. Set of Annihilating Polynomial Is an Ideal

Let \mathcal{A} be a unital algebra over \mathbb{F} and let $\alpha \in \mathcal{A}$. Then

$$M_\alpha = \{f \in \mathbb{F}[x] : f(\alpha) = 0\}$$

is an ideal of $\mathbb{F}[x]$.

Proof. Let $f, g \in M_\alpha$ and $h \in \mathbb{F}[x]$. Clearly $(f - g)(\alpha) = f(\alpha) - g(\alpha) = 0 - 0 = 0$. Moreover, $(fh)(\alpha) = f(\alpha)h(\alpha) = 0h(\alpha) = 0$ so $fh \in M$. Thus by the ideal test, $M_\alpha \subseteq \mathbb{F}[x]$ is an ideal of $\mathbb{F}[x]$. ♠

Def'n. Minimal Polynomial for $\alpha \in \mathcal{A}$

Let $\alpha \in \mathcal{A}$. Then M_α is generated by a unique monic polynomial $d \in \mathbb{F}[x]$, which we call the *minimal polynomial* for α .

Remark 2.1. In other words, the minimal polynomial for α is the monic polynomial of minimum degree that annihilates α .

Proposition 2.2. If \mathcal{A} Is Finite-Dimensional Then M_α Is Nontrivial

If \mathcal{A} is finite-dimensional, then $M_\alpha \neq \{0\}$ for any $\alpha \in \mathcal{A}$.

Proof. Suppose that $\dim(\mathcal{A}) = n \in \mathbb{N}$. Then $\alpha^0, \alpha^1, \dots, \alpha^n$ are $n + 1$ elements of \mathcal{A} , so they are linearly dependent. So there is a nonzero $(a_0, a_1, \dots, a_n) \in \mathbb{F}^{n+1}$ such that

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

It follows that

$$f = \sum_{i=0}^n a_i x^i$$

is an annihilating polynomial for α , which is nonzero since $(a_0, a_1, \dots, a_n) \neq 0$. But this means M_α is nontrivial. ♠

Characteristic Polynomial and Cayley-Hamilton Theorem

Lemma 2.3. $f(T)v = f(c)v$ 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

$$f(T)v = \left(\sum_{i=0}^n a_i T^i \right) v = \sum_{i=0}^n a_i T^i(v) = \sum_{i=0}^n a_i (cv)^i = \left(\sum_{i=0}^n a_i c^i \right) v = f(c)v. \quad \spadesuit$$

Lemma 2.4.

Let V be a finite-dimensional vector space and 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 β_i for W_i and β_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 $\dim(W) = \sum_{i=1}^k \dim(W_i)$. ♠

Proposition 2.5.
Alternative
Definitions of
Diagonalizability

Let V be a finite-dimensional vector space and 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

$$p_T = \prod_{i=1}^k (x - c_i)^{m_i}$$

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

$$\dim(V) = \deg(p_T) = \sum_{i=1}^k m_i = \sum_{i=1}^k \dim(W_i).$$

Notice that (c) \implies (a) is a direct result of Lemma 2.4. ♠

Proposition 2.6.
Every Linear
Operator on a
Finite-Dimensional
Vector Space Has an
Annihilating
Polynomial

Let V be a finite-dimensional vector space and let $T : V \rightarrow V$ be a linear operator. Then there exists $f \in \mathbb{F}[x]$ such that $f(T) = 0$.

Proof. Let $n = \dim(V)$. Observe that the space of linear operators on V has dimension n^2 . That is, $\{1, T, T^2, \dots, T^{n^2}\}$ is a linearly dependent subset of V , so there exist nonzero $a_0, a_1, \dots, a_{n^2} \in \mathbb{F}$ such that

$$\sum_{i=0}^{n^2} a_i T^i = 0.$$

But this exactly means $f = \sum_{i=0}^{n^2} a_i x^i \in \mathbb{F}[x]$ is an annihilating polynomial of T , as desired. ♠

Lemma 2.7.
The Characteristic
and Minimal
Polynomials Have the
Same Roots

Let V be a finite-dimensional vector space and let T be a linear operator on V . 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 Lemma 2.3. ♠

Proposition 2.8.
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 $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{F}$. Then

$$p = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$$

is the minimal polynomial of T .

Proof. Let $v_i \in V$ be an eigenvector of T . Then there exists an eigenvalue λ_i corresponding to v_i , so

$$p(T)v_i = (T - \lambda_1 I)(T - \lambda_2 I) \cdots (T - \lambda_i I) \cdots (T - \lambda_n I) = 0.$$

Since T is diagonalizable, $\{v_1, v_2, \dots, v_n\}$ forms an eigenbasis for V . That is, $p(T)v = 0$ for any $v \in V$, or, $p(T) = 0$. Since $\lambda_1, \lambda_2, \dots, \lambda_n$ are the roots of the minimal polynomial, it follows that p is the minimal polynomial of T . ♠

Remark 2.2. We will discuss that the converse of Proposition 2.8 is also true. That is, T is diagonalizable if and only if its minimal polynomial is a product of linear factors of degree 1.

Theorem 2.9.
Cayley-Hamilton
Theorem

Let V be a finite-dimensional vector space and 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,

$$\forall w \in W [T(w) \in W].$$

Remark 2.3. Whenever $W \subseteq V$ is T -invariant, we may restrict T to W . That is, there is a $T_W : W \rightarrow W$ by $w \rightarrow T(w)$. 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

$$[T]_\beta = \begin{bmatrix} [T]_\alpha & B \\ O & C \end{bmatrix}$$

for some $B \in M_{k \times (n-k)}(\mathbb{F})$, $C \in M_{(n-k) \times (n-k)}$ and zero matrix O .

Remark 2.4. For any linear operator $T : V \rightarrow V$, $\{0\}$ and V are T -invariant.

Remark 2.5. If $W \subseteq V$ is T -invariant and $\dim(W) = 1$, then W is spanned by an eigenvector of T .

Proposition 2.10. Null Space and Range Are T -Invariant

Let $T : V \rightarrow V$ be a linear operator on V . Then $\ker(T)$ and $\text{image}(T)$ are T -invariant.

Proof. Suppose $v \in \ker(T)$. Then $T(v) = 0 \in \ker(T)$. Furthermore, suppose $u \in \text{image}(T)$. Then $u \in V$ as well so $T(u) \in \text{image}(T)$. ♠

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

$$S_T(v, W) = \{f \in F[x] : f(T)v \in W\}$$

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 2.11.
 T -Conductor Is an Ideal

$S_T(v, W)$ 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,

$$(fh)(T)v = (f(T)h(T))v = h(T)(f(T)v) \in W,$$

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 β for V such that $[T]_\beta$ is triangular.

Lemma 2.12.

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 $v \in V \setminus W$ such that $(T - cI)(v) \in W$ 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 2.6. 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 2.13.
Characterization of Triangulable Linear Operator

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. It follows that the 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 Lemma 2.12. 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 Lemma 2.12 again, 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 2.14.
Characterization of
Diagonalizability

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 of Theorem 2.14 is supplied by Proposition 2.8. 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 Lemma 2.12, 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. ♠

Direct Sum Decompositions

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

$$\forall w_1 \in W_1 \forall w_2 \in W_2 \cdots \forall w_k \in W_k \left[\sum_{i=1}^k w_i = 0 \implies w_1 = w_2 = \cdots = w_k = 0 \right].$$

Remark 2.7. 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

$$\forall w \in W \exists w_1 \in W_1 \exists w_2 \in W_2 \dots \exists w_k \in W_k \left[w = \sum_{i=1}^k w_i \right].$$

Lemma 2.15.
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 2.7. 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 on a Vector Space

Let V be a vector space. A linear operator $E : V \rightarrow V$ is called a **projection** on V if $E^2 = E$.

Proposition 2.16.
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 2.16.1.
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

The unique linear operator $E : V \rightarrow V$ satisfying the condition in Corollary 2.16.1 is called the **projection** on R along N .

Remark 2.8. Any projection is trivially diagonalizable. Let $E : V \rightarrow V$ be a projection and let β_R, β_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 2.9. 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 2.17.
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 2.10. 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 2.10. We say T is the **direct sum** of linear operators $T_{W_1}, T_{W_2}, \dots, T_{W_k}$.

Remark 2.11. 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

Consider the case in Remark 2.10 and let β_i be an ordered basis for W_i for each $i \in \{1, 2, \dots, k\}$. Form $\beta = (\beta_1, \beta_2, \dots, \beta_k)$ then

$$[T]_{\beta} = \begin{bmatrix} [T_{W_1}]_{\beta_1} & & & \\ & [T_{W_2}]_{\beta_2} & & \\ & & \ddots & \\ & & & [T_{W_k}]_{\beta_k} \end{bmatrix}$$

We also describe this by saying that $[T]_{\beta}$ is the **direct sum** of $[T_{W_1}]_{\beta_1}, [T_{W_2}]_{\beta_2}, \dots, [T_{W_k}]_{\beta_k}$.

Remark 2.12. 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 2.18.
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 2.13. 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 2.19.

$T = \sum_{i=1}^k c_i E_i$
Decomposition

Let V be a vector space and let $T : V \rightarrow V$ be a linear operator. If T is diagonalizable and if $c_1, c_2, \dots, c_k \in \mathbb{F}$ are the distinct characteristic values of T , then there exist 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

$$Tv = \sum_{i=1}^k c_i E_i v = cv = \sum_{i=1}^k c E_i v.$$

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 2.14. Theorem 2.19 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 2.15. 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

$$p_j(T) = \sum_{i=1}^k p_j(c_i) E_i = \sum_{i=1}^k \delta_{ij} E_i = E_j$$

by Remark 2.14. Since $p_j(T)$ 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 2.14.

Theorem 2.14.
Characterization of
Diagonalizability

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 diagonal sizable. 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 2.19 to hold. That is, T is diagonal sizable. ♠

Primary Decomposition Theorem

Remark 2.16. 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.

- 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.
- 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

$$p = \prod_{i=1}^k (x - c_i)^{r_i},$$

it is always the case that

$$V = \bigoplus_{i=1}^k N((T - c_i I)^{r_i}).$$

In fact, we are going to prove more general version of this idea.

Theorem 2.20.
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

$$W_i = N(p_i(T)^{r_i})$$

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 Bezout's lemma. 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 $\text{image}(E_i) = W_i = N(p_i(T)^{r_i})$. 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 $p_i(T)^{r_i} \mid E_j$ whenever $i \neq j$. It follows that if $v \in N(p_i(T)^{r_i})$, 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 2.17. 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 2.20.1.

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 2.20, when each factor p_i of the minimal polynomial is linear (i.e. $p_i = x - c_i$). Now

$$\text{image}(E_i) = W_i = \ker(T - c_i I).$$

Define

$$D = \sum_{i=1}^k c_i E_i$$

then D is a diagonalizable operator by Theorem 2.19, which we call the **diagonalizable part** of T .

Remark 2.17. 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 2.21.
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) $T = D + N$.

(b) $DN = ND$.

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 2.17. 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 2.21.1.

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 .

This page intentionally left blank.

3.

The Rational and Jordan Form

-
- 3.1 Cyclic Subspaces and Annihilators
 - 3.2 Cyclic Decomposition and the Rational Form
 - 3.3 Jordan Form
-

Notations

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 .

End of Notations

Cyclic Subspaces and Annihilators

Remark 3.1. 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 3.2. 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 3.3. 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 3.4. 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 3.5. 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 3.6. 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 3.1.

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 3.1 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 3.7. A particular consequence of Theorem 3.1 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 3.8. 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 3.1. For convenience, let $w_i = T^i w$. Then the action of U on the ordered basis β 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 β 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 3.2.
 U Has a Cyclic Vector
If and Only If There
Exists β 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 β for W such that $[U]_\beta$ is the companion matrix of the minimal polynomial.

Proof. Notice that the forward direction is supplied by Remark 3.8. 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 3.2.1.

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 3.1. Thus by the Cayley-Hamilton theorem, p is also the characteristic polynomial of T , as required. ♠

Remark 3.9. 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 β for $Z(v; T)$ such that $[U]_\beta$ is the companion matrix of p_v , the T -annihilator of v .

Exercises

Exercise 3.10. 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. ♠

Exercise 3.11. 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 3.7, 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. ♠

Exercise 3.12. 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 3.1, $\{v, Tv, \dots, T^{n-1}v\}$ 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 3.13. 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 3.14. 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 3.15. By Remark 3.14, 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 3.16. 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 3.3.
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 3.3.1.

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 3.3.2.

Suppose $u_1, u_2, \dots, u_k \in V$ are nonzero vectors satisfying (a) and (b) of Lemma 3.3.1. 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 3.16 that, this means

$$s(w; W_{k-1}) = s(u; W_{k-1}) = f.$$

Moreover, observe that

$$f(T)w = f(T)u - \sum_{i=1}^{k-1} f(T)h_i(T)u_i = u_0 + \sum_{i=1}^{k-1} (fh_i + r_i)(T)u_i - \sum_{i=1}^{k-1} (fh_i)(T)u_i = u_0 + \sum_{i=1}^{k-1} r_i(T)u_i.$$

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, $\deg(s(u_j; W_{j-1})) \geq \deg(s(w; W_{j-1}))$ by

the maximality of $s(u_j; W_{j-1})$ that (b) of Lemma 3.3.1 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 3.3 Begins Here

Proof of Theorem 3.3. 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 3.3.1. 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 3.3.2. 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 3.3.1. 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 3.3.2, $p_k \mid p_i$ 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 $z \in \mathbb{N}$ 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 3.3.3.

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 3.3 Is Continued Here

Proof of Theorem 3.3 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 3.3.3, 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 3.3.3. But

$$\dim(Z(p_k(T)v_{k-1}; T)) = \dim(Z(p_k(T)z_{k-1}; T))$$

by (c) of Lemma 3.3.3, 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 3.3.4.

Every T -admissible $W \subseteq V$ has a T -invariant complementary $W' \subseteq V$.

Proof. If $W = V$, then $W' = \{0\}$. Otherwise, by Theorem 3.3,

$$V = W \oplus \left(\bigoplus_{i=1}^r Z(v_i; T) \right)$$

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 3.3.5.

There exists $v \in V$ such that the T -annihilator of v is the minimal polynomial of T .

Proof. By Theorem 3.3,

$$V = \bigoplus_{i=1}^r Z(v_i; T)$$

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 3.3.6.

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 3.7. 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 3.3.5, 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 3.4.
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 3.3.5. 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 3.4.1.

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 3.17. 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

$$[T]_{\beta} = \begin{bmatrix} [T_1]_{\beta_1} & & & \\ & [T_2]_{\beta_2} & & \\ & & \ddots & \\ & & & [T_r]_{\beta_r} \end{bmatrix} = \bigoplus_{i=1}^r [T_i]_{\beta_i}.$$

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 3.5.

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 β 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 3.17, 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 γ 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 3.2.1, each q_i is the characteristic and the minimal polynomial of C_i , so by Corollary 3.3.5, there exists $z_i \in V$ such that the T -annihilator of z_i is q_i . So we have another 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 β 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 3.18. 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 3.19. 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 β 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 3.20. 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 β 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 $\alpha = \{v_1, T v_1, v_2\}$. 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 $T v_2 = 2v_2$ are suitable. For instance, if we take $v_1 = (1, 0, 0)$, then

$$T v_1 = \begin{bmatrix} 5 \\ -1 \\ 3 \end{bmatrix}$$

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 3.21. 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 3.4.1. 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 β 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 α is linearly independent, it follows that α is a basis for $\ker(N)$.

Remark 3.22. Now, we are going to combine the results of Remark 3.22 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 β 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 3.22 is continued here

Now, if we define

$$\beta = \{\beta_1, \beta_2, \dots, \beta_k\},$$

where each β_i is an ordered basis for W_i such that $\{T_i\}_{\beta_i}$ is a direct sum of elementary Jordan matrices, then β 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 3.23. 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 β 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 3.6.
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 α for V such that $[T]_\alpha$ is in Jordan form. Moreover, if β 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 3.22. 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

$$(T - c_i I)^n v = \sum_{j=1}^k (T - c_i I)^n v_j = \sum_{j=1}^k (T_j c_i)^n v_j = 0,$$

which means

$$(T_j - c_i I)^n v = 0$$

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.

4.

Bilinear Form

-
- 4.1 Bilinear Forms
 - 4.2 Symmetric Bilinear Form
 - 4.3 Skew-Symmetric Bilinear Form
 - 4.4 Groups Preserving Bilinear Forms
-

Bilinear Forms

Remark 4.1. 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 4.2. Clearly the zero function $0 : V \times V \rightarrow \mathbb{F}$ is a bilinear form on V .

Remark 4.3. 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 4.1, 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 4.4. 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 4.5. 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 bilinear form 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 1×1 , 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 4.6. 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 4.4.

Remark 4.7. We may generalize the results of Example 4.5 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 β 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 β 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 β by

$$([f]_{\beta})_{ij} = f(v_i, v_j).$$

Theorem 4.1.

$[\cdot]_{\beta} : \mathcal{L}(V, V, \mathbb{F}) \rightarrow M_{n \times n}(\mathbb{F})$ is an isomorphism

Let β be an ordered basis for V . Then $[\cdot]_{\beta} : \mathcal{L}(V, V, \mathbb{F}) \rightarrow M_{n \times n}(\mathbb{F})$ is an isomorphism.

Proof. The bijectivity of $[\cdot]_{\beta}$ is supplied by Remark 4.5. 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 β , 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 4.1.1.

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 β . 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 4.3. 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 α is a basis for $\mathcal{L}(V, V, \mathbb{F})$, as required. ♠

Remark 4.8. In terms of matrix point of view, one may rephrase Corollary 4.1.1 as follows: the matrix of each f_{ij} with respect to β 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 4.1 that α is a basis for $\mathcal{L}(V, V, \mathbb{F})$.

Remark 4.9. 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 4.10. 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 4.11. 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 β 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 4.2.

$$\text{rank}(L_f) = \text{rank}(R_f)$$

Let f be a bilinear form on V and define linear transformations

$$L_f, R_f : V \rightarrow V^*$$

as Remark 4.9. 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 β 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

$$(X^T [f]_\beta) Y = 0$$

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 4.9. 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 4.2.

Corollary 4.2.1.

$\text{rank}(f) = \text{rank}[f]_\beta$

Let f be a bilinear form on V and let β be an ordered basis for V . Then


$$\text{rank}(f) = \text{rank}[f]_\beta.$$

Proof. From the proof of Proposition 4.2,

$$\text{nullity}(f) = \dim \left\{ X \in M_{n \times 1}(\mathbb{F}) : [f]_\beta X = 0 \right\}.$$

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 4.2.2.

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 4.2.2.

Remark 4.12. As Corollary 4.2.2 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 β 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 β 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 4.13. 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 β for V such that $[f]_\beta$ is diagonal exist? We shall prove that such β 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 4.14. If V is finite-dimensional, then a bilinear form f is symmetric if and only if $[f]_\beta$ is symmetric for some ordered basis β 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 β 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 4.15. 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 4.16. 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

$$q_A(x) = X^TAX = \sum_{i,j} A_{ij}x_ix_j.$$

Remark 4.17. 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 4.17 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 4.3.
If f is a Symmetric Bilinear Form, Then $[f]_\beta$ Is Diagonal for Some Ordered Basis β

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 β 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 β 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

$$w_\perp = v - \frac{f(v, v_{k+1})}{f(v_{k+1}, v_{k+1})}v,$$

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 β is the ordered basis for V by direct sum decomposition $V = W \oplus W_\perp$, and we have diagonal $[f]_\beta$ by construction. ♠

Corollary 4.3.1.

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 4.4. Diagonalization of a Symmetric Bilinear Form on a Real Vector Space where Nonzero Entries Are ± 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 β for V .

Proof. By Theorem 4.3, there exists an ordered basis α 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 α to obtain an ordered basis γ 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 β , 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 ζ 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 4.18. Let f be a symmetric bilinear form on a finite dimensional vector space V over \mathbb{R} and let β and

$$V = V_+ \oplus V_- \oplus V_\perp$$

be as described in Theorem 4.4. 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 4.4 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 4.4 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 4.4. Then we define the *signature* of f by

$$\dim(V_+) - \dim(V_-).$$

Remark 4.19. 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 4.4, 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 4.4 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 β for V , is that any inner product can be represented by the identity matrix in some ordered basis for V .

Remark 4.20. If V is instead a finite-dimensional vector space over \mathbb{C} , then we may further simplify the matrix of a bilinear form.

Corollary 4.4.1.

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 4.4.1 can be done in an analogously to the proof of Theorem 4.4 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 4.20 is continued here.

In fact, the proof of Corollary 4.4.1 is valid for any algebraically closed field, or, any field closed under the operation of taking the square root.

Skew-Symmetric Bilinear Form

Remark 4.21. 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 4.22. 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 4.23. If f is a skew-symmetric bilinear form on V , then for any ordered basis β for V , $[f]_\beta$ is skew-symmetric.

Remark 4.24. 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 β such that $[f]_\beta$ is simple, if such β 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 4.5.

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 β 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 4.5.1.

If there exists nondegenerate skew-symmetric bilinear form f on V , then $n = \dim(V)$ is even. Moreover, there exists an ordered basis β for V such that

$$[f]_{\beta} = \left(\bigoplus_{i=1}^{\frac{n}{2}} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right).$$

Remark 4.25. Theorem 4.5 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 4.5.1, 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 4.26. 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 4.27. 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 4.6.
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 4.27 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 4.28. When V is finite-dimensional, an immediate consequence of Proposition 4.6 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 4.6.1.

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 $\llbracket_{\beta} : \mathcal{L}(V, V, \mathbb{F}) \rightarrow M_{n \times n}(\mathbb{F})$ is an isomorphism, where $\dim(V) = n$ and β 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 β for V , then there exists unique bilinear form f on V such that $A = [f]_{\beta}$. Moreover, the isomorphism $\llbracket_{\beta} : \mathcal{L}(V) \rightarrow M_{n \times n}(\mathbb{F})$, 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

$$\begin{aligned} f(x, y) &= X^T A Y = X^T M^T A M Y = (M X)^T A (M Y) \\ &= \left([T]_{\beta} [x]_{\beta} \right)^T [f]_{\beta} \left([T]_{\beta} [y]_{\beta} \right) = [Tx]_{\beta}^T [f]_{\beta} [Ty]_{\beta} = f(Tx, Ty), \end{aligned}$$

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 \llbracket_{β} . ♠

Remark 4.29. 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 .

5.

Inner Product Spaces

-
- 5.1 Inner Products
 - 5.2 Inner Product Spaces
 - 5.3 Linear Functionals and Adjoint
 - 5.4 Unitary Operators
-

Inner Products

Remark 5.1. 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 5.2. 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 θ 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 5.3. 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 5.4. Notice that the definition of inner product here is consistent with the one provided in Chapter 4. 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 5.5. In case of $\mathbb{K} = \mathbb{R}$, the standard inner product on \mathbb{K}^n is the inner product.

Remark 5.6. 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 5.7. 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 5.8. 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 5.9. 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 $T : V \rightarrow W$ is an isomorphism, then

$$p_T(v, u) = \langle Tv, Tw \rangle : V \times V \rightarrow \mathbb{K}$$

Remark 5.6 is continued here.

is an inner product on V . The inner product shown in Remark 5.7 is a special case of this result.

Example 5.10. 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 ϕ 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 5.9, 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 5.11. We take a look at Example 5.8 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 5.12. 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 5.13. 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 5.13 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 5.13 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 5.14. 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 β be an ordered basis for V . If we define $G \in M_{n \times n}(\mathbb{K})$ as described in Remark 5.14, then we call G the **matrix** of $\langle \cdot, \cdot \rangle$.

Remark 5.15. 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 5.15 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 5.1.
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 5.1 is known as the **Cauchy-Schwarz inequality**.

Remark 5.16. 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 5.17. For any inner product space, $0 \in V$ is the unique vector orthogonal to every $v \in V$.

Example 5.18. The standard ordered basis for \mathbb{K}^n is an orthonormal set.

Example 5.19. Let $\langle \cdot, \cdot \rangle$ be the inner product described in Remark 5.8, 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 β 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 5.20. The two examples of orthogonal sets above are linearly independent. We show that this is true for all orthogonal sets containing nonzero elements.

Theorem 5.2.
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 5.2.1.

Let V and S be define as Theorem 5.2 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 5.2.2.

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 5.21. One possible - and geometrically important - interpretation of Corollary 5.2.2 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 5.3.
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 β 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 5.2, is a basis for $\text{span}\{v_1, v_2, \dots, v_{m+1}\}$. Thus by induction we have the desired result. ♠

Corollary 5.3.1.
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 5.3, 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 5.22. 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 5.14.

$\{v_1, v_2, \dots, v_n\}$ be an ordered basis for an inner product space V over \mathbb{K} . Then we may associate a matrix G with β by

$$G_{ij} = \langle v_j, v_i \rangle.$$

In particular, when β 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 5.23. 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 5.17, 0 is the unique vector with this property.

Remark 5.24. 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 5.4. 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 5.25. 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 5.4, 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 5.26. By Theorem 5.4, the orthogonal projection of V on W always exists when V is a finite-dimensional inner product space and $W \subseteq V$. But Theorem 5.4 also provides the following result.

Corollary 5.4.1.

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 5.27. 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 5.5.
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 5.4, 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 5.5.1.

Assume the conditions of Proposition 5.5. 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 5.4.1. 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 5.28. 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 5.5.2. 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 5.29. 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 5.30. 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 5.6.
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 5.31. Here is another proof of Theorem 5.6 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 5.22. Since any linear functional $f : V \rightarrow \mathbb{K}$ is of the form

$$f(x) = \sum_i c_i x_i$$

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 5.32. The proof of Theorem 5.6 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 5.4. 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 5.31.

Remark 5.33. We now turn to the concept of the adjoint of a linear operator.

Theorem 5.7.
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 5.6 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 5.6 and the above construction. ♠

Proposition 5.8.
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 β is an orthonormal basis, we have

$$v = \sum_i \langle v, v_i \rangle v_i$$

for any $v \in V$ by Remark 5.29. 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 5.8.1.

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 β for V ,

$$[T]_\beta^* = [T^*]_\beta.$$

Proof. By Proposition 5.8,

$$\begin{cases} ([T]_\beta)_{ij} &= \langle Tv_j, v_i \rangle \\ ([T^*]_\beta)_{ij} &= \langle T^*v_j, v_i \rangle \end{cases},$$

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 5.34. By Theorem 5.7, 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 5.35. 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 β is an arbitrary ordered basis for the inner product space, it need not be the case which

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

Remark 5.36. 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 5.9.
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) $(T + S)^* = T^* + S^*$.
- (b) $(cT)^* = \bar{c}T^*$.
- (c) $(TS)^* = S^*T^*$.
- (d) $(T^*)^* = T$.

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 5.37. Proposition 5.9 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 $z \in \mathbb{R}$ if and only if

$$\bar{z} = z,$$

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

$$T_1 = \frac{1}{2}(T + T^*)$$

$$T_2 = \frac{1}{2i}(T - T^*).$$

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 5.37 is continued here.

If $T : V \rightarrow V$ is Hermitian and β 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 5.38. 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.