LECTURE 18

Invariant Subspaces

Recall the *range* of a linear transformation $T : V \to W$ is the set

$$range\,(T) = \{w \in W \mid w = T\,(v) \text{ for some } v \in V\}$$

Sometimes we say $range\,(T)$ is the *image of V by T* to communicate the same idea. We can also generalize this notion by considering the image of a particular subspace U of V. We usually denote the image of a subspace as follows

$$T\,(U) = \{w \in W \mid w = T\,(v) \text{ for some } u \in U\}$$

This notion of the image of a subspace is also appplicable when T be a linear tranformation from a vector space V into itself; and in this situation both U and $T\,(U)$ are subspaces of V. All this motivates the following definition.

Definition 18.1. *A subspace W of a vector space V is said to be* ***invariant*** *with respect to a linear transformation $T \in L\,(V,V)$ if $T\,(W) \subseteq W$.*

Of course, the parent vector space V is always invariant with respect to a $T \in L\,(V,V)$ since the range of T will always be a subspace of V.

Also, if v is an eigenvector of T with eigenvalue λ, then its span will be an invariant subspace of T since

$$v' \in span\,(v) \quad v' = \alpha v \quad \Rightarrow \quad T\,(v') = T\,(\alpha v) = \alpha T\,(v) = (\alpha\lambda)\,v \in span\,(v)$$

In fact,

Proposition 18.2. *Let V_λ be the λ-eigenspace of $T \in L\,(V,V)$;*

$$V_\lambda = \{v \in V \mid T\,(v) = \lambda v\}$$

Then any subspace of V_λ is an invariant subspace of T.

Proof. Let W be a subspace of V_λ. Each vector $w \in W \subseteq V_\lambda$ will satisfy

$$T\,(w) = \lambda w \in W \qquad \text{since } W \text{ is closed under scalar multiplication.}$$

Therefore $T\,(W) \subseteq W$. $\square$

As a particular example of the preceding proposition, consider the 0-eigenspace of a $T \in L\,(V,V)$:

$$V_0 = \{v \in V \mid T\,(v) = 0_{\mathbb{F}} \cdot v = \mathbf{0}_V\} = \ker\,(T)$$

So any subspace of the kernel of a linear transformation $T \in L\,(V,V)$ will be an invariant subspace.[1]

Definition 18.3. *Let $V_1, \ldots, V_k$ be subspaces of V. The space V is said to be the* ***direct sum*** *of $V_1, \ldots, V_k$ if*

[1]Actually, we have a slight inconsistency if $V_0 = \{\mathbf{0}_V\}$. For if we allow $\mathbf{0}_V$ to be interpretable as an eigenvector, it is then an eigenvector for all possible eigenvalues

$$T\,(\mathbf{0}_V) = \mathbf{0}_V = \lambda \cdot \mathbf{0}_V \quad \forall\, \lambda \in \mathbb{F}$$

So we normally don't regard the zero vector as an eigenvector; nor V_0 as an eigenspace when $V_0 = \{\mathbf{0}_V\}$.

(a) *Every vector $v \in V$ can be expressed as*

(1) $$v = v_1 + v_2 + \cdots + v_k \quad \text{with } v_i \in V_i \ \text{ for each } i \in \{1, \ldots, k\}\,.$$

(b) *The expansion of a vector v in the form (1) is unique.*

We write

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

or

$$V = \bigoplus_{i=1}^{k} V_i$$

when V is a direct sum of $V_1, V_2, \ldots, V_k$.

Example 18.4. Let $B = \{w_1, \ldots, w_n\}$ be a basis for V and set

$$V_i = span\,(w_i) \quad , \quad i = 1, 2, \ldots, n \quad .$$

Then

$$V = \bigoplus V_i$$

Lemma 18.5. *Let $V_1, \ldots, V_k$ be subspaces of V. Then $V = \bigoplus_{i=1}^{k} V_i$ if and only if*

(i) *Every vector in v can be expressed at least one way as $v = v_1 + \cdots + v_k$ with $v_i \in V_i$, $i = 1, \ldots, k$.*

(ii) *If $v_i \in V_i$ for $i = 1, \ldots, k$ and*

$$v_1 + v_2 + \cdots + v_k = \mathbf{0}_V \qquad \Rightarrow \qquad v_1 = \mathbf{0}_V \quad , \quad v_2 = \mathbf{0}_V \quad , \quad \ldots \quad , \quad v_k = \mathbf{0}_V \quad .$$

Proof.

$\Rightarrow$ Suppose $V = \bigoplus_{i=1}^{k} V_i$. Statement (i) of the lemma is the same as property (a) of the definition of the direct sum. We need to deduce property (ii) of the Lemma. Since each V_i is a subspace of V each V_i contains $\mathbf{0}_V$. If we set $v_i = \mathbf{0}_V$ for each $i \in \{1, \ldots, k\}$ we can then write

$$V \ni \mathbf{0}_V = \mathbf{0}_V + \mathbf{0}_V \ + \cdots + \mathbf{0}_V = v_1 + v_2 + \cdots + v_k$$

Applying the uniqueness property (b) of Definition 17.3 we can infer that the only way to get a sum like $v_1 + \cdots + v_k$ to produce the $\mathbf{0}$ vector is to take $v_1 = \mathbf{0}_V\ , \ldots, v_k = \mathbf{0}_V$. Thus, statement (ii) of the Lemma follows.

$\Rightarrow$ Suppose statements (i) and (ii) of the Lemma hold. Since statement (i) of the lemma is the same as statement (b) of the definition of direct sum, we just have to show that statement (b) of the Definition holds. Suppose

$$\begin{aligned} v &= v_1 + \cdots + v_k \\ v &= w_1 + \cdots + w_k \end{aligned}$$

are two expansions of v of the form (1). Then subtracting the two equations we get

(*) $$\mathbf{0}_V = (v_1 - w_1) + \cdots + (v_k - w_k)$$

Since the V_i are subspaces, $v_i, w_i \in V_i$ implies $v_i - w_i \in V_i$ and so (*) is an expression in the form (1). Statement (ii) says that for such an equation to be valid we must have each term $v_i - w_i = \mathbf{0}_V$. Thus, $v_i = w_i$ for $i = 1, \ldots, k$ and property (b) of the definition follows.

□

Lemma 18.6. *Let V be a vector space over $\mathbb{F}$, and suppose there exists non-zero linear transformations $E_1, \ldots, E_k$ in $L(V, V)$ such that*

(a) $\mathbf{1} = E_1 + E_2 + \cdots + E_k$

(b) $E_iE_j = E_jE_i = \mathbf{0}$ *if* $i \neq j$, $1 \leq i, j \leq k$

Then

(i) $E_i^2 = E_i$ *for* $i = 1, \ldots, k$
(ii) V *is the direct sum*

$$V = \bigoplus_{i=1}^{k} E_i\left(V\right)$$

and each $E_i\left(V\right)$ *is non-zero.*

Proof.

(i) We have

$$\begin{aligned} E_i &= E_i \cdot \mathbf{1} = E_i \cdot \left(E_1 + \cdots + E_i + \cdots + E_k\right) \qquad \text{(using part (a) of hypotheis)} \\ &= E_i^2 + \sum_{i \neq j} E_iE_j \\ &= E_i^2 + \sum_{i \neq j} \mathbf{0} \qquad \text{(using part (b) of hypothesis)} \\ &= E_i^2 \end{aligned}$$

(ii) Since each E_i is a non-zero linear transformation each $E_i\left(V\right)$ is a non-zero subspace of V. Let $v \in V$.

$$\begin{aligned} v &= \mathbf{1} \cdot v = \left(E_1 + \cdots + E_k\right)\left(v\right) \\ &= E_1\left(v\right) + \cdots + E_k\left(v\right) \end{aligned}$$

Thus, each element of V can be expressed sum $w_1 + \cdots + w_k$ with each $v_i \in E_i\left(V\right)$. Now suppose $v_1 \in E_1\left(V\right), \ldots, v_k \in E_k\left(V\right)$ and

$$\mathbf{0}_V = v_1 + \cdots + v_k$$

Then, for each $i = 1, \ldots, k$ we have

$$\mathbf{0}_V = E_i\left(\mathbf{0}_V\right) = E_i\left(v_1\right) + \cdots + E_iv_i + \cdots + E_iv_k$$

Now if $v_j \in E_j\left(V\right) \quad \Rightarrow \quad v_j = E_j\left(w_j\right)$ for some $w_j \in V$. So we have

$$\mathbf{0}_V = E_i\left(\mathbf{0}_V\right) = E_iE_1\left(w_1\right) + \cdots + E_iE_i\left(w_i\right) + \cdots + E_iE_k\left(w_k\right)$$

Since $E_iE_j = \mathbf{0}$ if $i \neq j$, the only possibly non-zero term on the right hand side is $E_iE_i\left(w_i\right) = E_i\left(w_i\right) = v_i$. So we must have

$$\mathbf{0}_V = v_i$$

This argument holds for each $i = 1, \ldots, k$. Hence,

$$\mathbf{0}_V = v_1 + \cdots + v_k \qquad \Rightarrow \qquad v_1 = \mathbf{0}_V \quad , \quad v_2 = \mathbf{0}_V \quad , \quad \ldots \quad , \quad v_k = \mathbf{0}_V$$

and so

$$V = \bigoplus_{i=1}^{k} E_i\left(V\right)$$

by Lemma 17.5. □

1. Digression: More on Polynomials

Before we procede further, it will might be helpful to review a bit of polynomial algebra. We gave a suitably abstract definition of polynomials over a field back in Lecture 16, recall that the ring $\mathbb{F}\left[x\right]$ of polynomials with coefficients in a field $\mathbb{F}$ is not only a vector space over $\mathbb{F}$ but an integral ring (a commutative ring with identity without zero divisors). In this commutative ring setting we have

THEOREM 18.7 (Division Algorithm for $\mathbb{F}[x]$). *Let f, g be polynomials in $\mathbb{F}[x]$, not both $0_{\mathbb{F}}$. Then there exists unique polynomials $q, r \in \mathbb{F}[x]$ such that*

(i) $f = qg + r$
(ii) *Either* $r = 0_{\mathbb{F}}$ *or* $\deg(r) < \deg(g)$.

We write

$$f \mid g \qquad (\text{"}f \text{ divides } g\text{"})$$

whenever there is a polynomial q such that $g = qf$.

DEFINITION 18.8. *Two polynomials $f, g \in \mathbb{F}[x]$ are called **associate** if $g = cf$ for some $c \in \mathbb{F}$.*

DEFINITION 18.9. *Let $f, g \in \mathbb{F}[x]$ not both zero. The **greatest common divisor** of f and g is the (unique) monic polynomial of highest degree that divides both f and g.*

THEOREM 18.10. *Let $f, g \in \mathbb{F}[x]$. Then there exist polynomials $u, v \in \mathbb{F}[x]$ such that*

$$GCD(f, g) = uf + vg$$

COROLLARY 18.11. *If $f_1, f_2, \ldots, f_k \in \mathbb{F}[x]$ have no common factors then there exist polynomials $u_1, u_2, \ldots, u_k \in \mathbb{F}[x]$ such that*

$$1_{\mathfrak{F}} = u_1 f_1 + u_2 f_2 + \cdots + u_k f_k$$

Recall that an integer $p \in \mathbb{Z}$ is **prime** if its only divisors are ± 1 and $\pm p$. The analogous concept for polynomials is that of an *irreducible polynomial.*

DEFINITION 18.12. *A non-constant polynomial p is **irreducible** if its only divisors are the constants and its associates:*

$$\text{if } p \text{ is irreducible, } q \mid p \quad \Rightarrow \quad q \in \mathbb{F} \text{ or } q = cp \text{ for some } c \in \mathbb{F}$$

THEOREM 18.13. *Every non-constant polynomial is factorizable as a product of irreducible polynomials. This factorization is unique up to reordering of factors and replacing factors by their associates.*

DEFINITION 18.14. *Let R be an $\mathbb{F}$-algebra (a vector space over $\mathbb{F}$ with its own internal multiplication). Then for each $f \in \mathbb{F}[x]$ we have a function $\widetilde{f} : R \to R$ defined by*

$$r \quad \longmapsto \quad \widetilde{f}(r) = a_0 + a_1 \cdot r + a_2 \cdot r^2 + \cdots + a_n \cdot r^n \in R$$

when

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \quad .$$

DEFINITION 18.15. *A **root** of a polynomial in R is an element $r \in R$ such that*

$$\widetilde{f}(r) = 0_R$$

THEOREM 18.16. *Suppose $a \in R$ is a root of $f \in \mathbb{F}[x]$, then $x - a$ is a factor of f.*

Proof. *By the Division Algorithm there exist unique polynomials q and r such that*

$$f = q(x - a) + r$$

Evaluating both sides at $x = a$, we see

$$\widetilde{f}(a) = 0 + \widetilde{r}(a)$$

So

$$a \text{ is a root of} \quad \Longleftrightarrow \quad \widetilde{f}(a) = 0 \quad \Longleftrightarrow \quad \widetilde{r}(a) = 0 \quad \Longleftrightarrow \quad r = 0_{\mathbb{F}} \quad \Longleftrightarrow \quad (x - a) \mid f$$

□

As remarked in Lecture 16, the point of using indeterminates in the definition of a polynomial is so that we have some choice in how we evaluate a polynomial function; and the the basics of polynomial arithmetic (like Theorems 17.7, 17.10, 17.11, 17.13, and 17.16 above) still remain in force. Note, however, whether or not there are roots of a polynomial f in a given ring R is as much a property of the ring R as it is of the polynomial f. Consider for example,

$$f = x^2 + 1$$

It's well known that f has no roots in $\mathbb{R}$, but it does have the roots $\pm i \in \mathbb{C}$. It also has roots

$$\left(\begin{array}{cc} 0 & \pm 1 \\ \mp 1 & 0 \end{array} \right) \in M_2 (\mathbb{R})$$

On the other hand, since it always makes sense to evaluate a polynomial $f \in \mathbb{F}[x]$ at an element $a \in \mathbb{F}$, the question as to whether $f \in \mathbb{F}[x]$ has a root in $\mathbb{F}$ is a property of $\mathbb{F}$ alone. When it is always possible to find a root of a polynomial $f \in \mathbb{F}[x]$ in the underlying field f we say that $\mathbb{F}$ is *algebraically closed.*

2. Back to Linear Transformations

THEOREM 18.17. *Let $T \in L(V, V)$ and let*

$$m_T(x) = p_1(x)^{s_1} \cdots p_k(x)^{s_k}$$

be a factorization of the minimal polynomial of T in terms of distinct irreducible elements of $\mathbb{F}[x]$. Then there exist polynomials $\{f_1, \ldots, f_k\}$ in $\mathbb{F}[x]$ such that the linear transformations E_i defined by

$$E_i = f_i(T) \qquad , \qquad i = 1, \ldots, k$$

satisfy

(i) $\mathbf{1} = E_1 + E_2 + \cdots + E_k$
(ii) $E_i E_j = E_j E_i = \mathbf{0}$ *if* $i \neq j$
(iii) $E_i \neq 0$
(iv) *Each $E_i V$ is a T-invariant subspace of V and we have the following direct sum decomposition of V*

$$V = E_1(V) \oplus E_2(V) \oplus \cdots \oplus E_k(V)$$

(v) $E_i(V) = \ker(p_i^{s_i})$ *for* $i = 1, \ldots, k$.

Proof.

(i) Let

$$q_i(x) = \frac{m_T(x)}{p_i(x)^{s_i}} = p_1(x)^{s_1} \cdots p_{i-1}(x)^{s_{i-1}} p_{i+1}(x)^{s_{i+1}} \cdots p_k(x)^{s_k}$$

Then the polynomials $q_i(x)$ have no common factors[2], then by Corollary 17.11 above, there exist polynomials $a_1 \ldots, a_k \in \mathbb{F}[x]$ such that

$$1_{\mathbb{F}} = a_1 q_1 + \cdots + a_k q_k \quad .$$

Substituting T into both sides of this last equation we have

$$\mathbf{1} = a_1(T) q_1(T) + \cdots + a_k(T) q_k(T) \quad .$$

So if we set

$$f_i(x) = a_i(x) q_i(x)$$

and

$$E_i = f_i(T)$$

[2]Although pairs of these polynomials will have multiple common factors of the form $(p_k(x)^{s_k})$, there will be no such factor common to **all** of the $q_i(x)$. The latter circumstance is what allows us to apply Corollary 11.7,

we have

$$\mathbf{1} = E_1 + \cdots + E_k \quad .$$

(ii) Next we note whenever $i \neq j$, m_T divides $f_i f_j$; for when we construct f_i we retain all the factors $(p_k)^{s_k}$ except $(p_i)^{s_i}$ and similarly for f_j when we construct it. So in the product $f_i f_j$ all the factor $(p_k)^{s_k}$ occur at least once (every factor except $(p_i)^{s_i}$ and $(p_j)^{s_j}$ appear at least twice). Thus,

$$m_T \mid f_i f_j \quad \Rightarrow \quad f_i(T) f_j(T) = 0 \quad \Rightarrow \quad E_i E_j = \mathbf{0}$$

(iii) In order to apply Lemma 17.6 in order to conclude

$$V = E_1(V) \oplus E_2(V) \oplus \cdots \oplus E_k(V)$$

let us now show that each of the linear transformations E_i are non-zero. Suppose $E_i(V) = 0$ for some i. Then

$$\begin{aligned} V &= \mathbf{1}_V(V) = (E_1 + \cdots E_{i-1} + \mathbf{0} + E_{i+1} + \cdots + E_k)(V) \\ &= \left(\sum_{i \neq j} E_i\right)(V) \end{aligned}$$

But then

$$\begin{aligned} q_i(T)(V) &= \sum_{i \neq j} q_i(T) E_j(V) \\ &= \sum_{i \neq j} \left(p_1^{s_1}(T) \cdots \widehat{p_i^{s_i}(T)} \cdots p_k^{s_k}(T)\right)\left(a_j(T) p_1^{s_1}(T) \cdots \widehat{p_j^{s_j}(T)} \cdots p_k^{s_k}(T)\right) \\ &= \sum_{i \neq j} m_T(T)\left(a_j(T) p_1^{s_1}(T) \cdots \widehat{p_i^{s_i}}(T) \cdots \widehat{p_j^{s_j}(T)} \cdots_j p_k^{s_k}(T)\right) \\ &= 0 \end{aligned}$$

since $m_T(T) = 0$. On the other hand,

$$q_i = \frac{m_T}{p_i^{r_i}} \quad \Rightarrow \quad \deg(q_i) < \deg(m_T)$$

contradicting the hypothesis that m_T is the minimal polynomial for T. Thus, we cannot have $E_i(V) = 0$.

(iv) Since the operator E_i have now been shown to satisfy the hypothesis on the operators in Lemma 17.6, we can conclude

$$V = E_1(V) \oplus E_2(V) \oplus \cdots \oplus E_k(V) \quad .$$

To see that the subspaces $E_i(V)$ are T-invariant, we simply observe

$$T E_i(V) = T f_i(T)(V) = f_i(T) T(V) = E_i T(V) \subseteq range(E_i) = E_i(V)$$

It remains to show that

(v) $$\ker(p_i(T)^{s_i}) = E_i(V)$$

Now

$$\begin{aligned} (p_i(T))^{s_i} E_i &= (p_i(T))^{s_i}\left(a_i(T)(p_1(T))^{s_1} \cdots \widehat{(p_i(T))}^{s_i} \cdots (p_k(T))^{s_k}\right) \\ &= a_i(T) m_T(T) \\ &= 0 \end{aligned}$$

This shows that the range of E_i lives in in the kernel of $(p_i(T))^{s_i}$; which is to say

(*) $$E_i(V) \subseteq \ker(p_i(T)^{s_i}) \quad , \quad i = 1, \ldots, k$$

If we can show the opposite inclusion

$$\ker(p_i(T)^{s_i}) \subseteq E_i(V)$$

then (v) will follow.

Let $v \in \ker\left(p_i(T)^{s_i}\right)$ and decompose it with respect to the direct sum composition (4) of v :

$$v = E_1 v + E_2 v + \cdots + E_i v + \cdots + E_k v$$

Note if we can show that

$$(^{**}) \qquad v \in \ker\left(p_i(T)^{s_i}\right) \quad \Rightarrow \quad E_j v = 0 \quad \forall\ j \neq i$$

then our conclusion will follows; because in this situation

$$\begin{aligned} \ker\left(p_i(T\ )^{s_i}\right) \quad \ni \quad v \quad &\Rightarrow \quad v = 0 + \cdots + 0 + E_i v_i + 0 + \cdots + 0 \\ &\Rightarrow \quad v = E_i v \\ &\Rightarrow \quad v \in E_i(V) \end{aligned}$$

To prove (**), we first note that since p_i and p_j are distinct irreducible polynomials when $i \neq j$, $(p_i)^{s_i}$ and $(p_j)^{s_j}$ have no common factors and so there are polynomials $b_i, b_j \in \mathbb{F}[x]$ such that

$$1_{\mathbb{F}[x]} = GCD\left(p_i^{s_i}, p_j^{s_j}\right) = b_i(p_i)^{s_i} + b_j(p_j)^{s_i}.$$

Now let $v \in \ker\left(p_i(T)^{s_i}\right)$ and consider

$$E_j v = 1 \cdot E_j v = \left(b_i(T)\, p_i(T)^{s_i} + b_j(T)\, p_j(T)^{s_j}\right) E_j v \qquad , \qquad i \neq j$$

We have, on the one hand,

$$b_i(T)\, p_i(T)^{s_i}\, E_j v = b_i(T)\, E_j p_i(T)^{s_i}\, v = 0 \qquad \text{since } v \in \ker\left(p_i(T)^{s_i}\right)$$

and, on the other hand, since as we showed in (*), $E_j(V) \subseteq \ker\left(p_j(T)^{s_j}\right)$,

$$b_j(T)\, p_j(T)^{s_j}\, E_j v = 0$$

Thus

$$\begin{aligned} E_j v \quad &= \quad = b_i(T)\, p_i(T)^{s_i}\, E_j(v) + b_j(T)\, p_j(T)^{s_j}\, E_j v \\ &= \quad 0 + 0 \\ &= \quad 0 \end{aligned}$$

Thus,

$$\begin{aligned} v \quad &= \quad E_1 v + E_2 v + \cdots + E_i v + \cdots + E_k v \\ &= \quad 0 + \cdots + 0 + E_i v + 0 + \cdots + 0 \\ &= \quad E_i v \end{aligned}$$

So any $v \in \ker\left(p_i(T)^{s_i}\right)$ lies in $E_i(V)$, thus (**) holds.

$\square$

3. Diagonalization

Definition 18.18. *A linear transformation $T : V \to V$ is* ***diagonalizable*** *if there exists a basis B of V consisting of eigenvectors of T. (Equivalently, T is diagonalizable if the number of linearly independent eigenvectors equals the dimension of V.)*

Theorem 18.19. *A linear transformation $T : V \to V$ is diagonalizable if and only if the minimal polynomial $m_T(x)$ of T has the form*

$$m(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_k)$$

with the ξ_i being the distinct roots of $m(x)$ in $\mathbb{F}$.

Proof.

$\Rightarrow$ Suppose T is diagonalizable, and let $\{v_1, \ldots, v_n\}$ be a basis for V which we can take to be a basis of T-eigenvectors:

$$T(v_i) = \lambda_i v_i \qquad \text{with } \lambda_i \in \{\xi_1, \ldots, \xi_k\}$$

Since each λ_i must be chosen from the set $\{\xi_1, \ldots, \xi_k\}$, each of the vectors v_i must be annihilated by one of the operators

$$S_j = T - \xi_j \mathbf{1}$$

for

$$S_j (v_i) = T (v_i) - \xi_j v_i = \left(\lambda_i - \xi_j\right) v_i = \mathbf{0}_V \quad \text{when } \lambda_i = \xi_j . \tag{6}$$

So all of the v_i are annihilated by the product of the S_j

$$(S_1 S_2 \cdots S_k) v_i = \mathbf{0}_V \qquad \forall \ i$$

(note that we are using both (6) and the easy observation that the operators S_i all commute with one another). Hence, if we expand an arbitrary vector v with respect to the basis $\{v_1, \ldots, v_n\}$ we'll have

$$\begin{aligned} (S_1 \cdots S_k)(v) &= (S_1 \cdots S_k)(a_1 v_1 + \cdots + a_n v_n) \\ &= a_1 (S_1 \cdots S_k)(v_1) + \cdots + a_n (S_1 \cdots S_k)(v_n) \\ &= a_1 \cdot \mathbf{0}_V + \cdots + a_n \mathbf{0}_V \\ &= \mathbf{0}_V \end{aligned}$$

Since v is arbitrary, we must have

$$S_1 \cdots S_k = \mathbf{0}_{L(V,V)} \quad .$$

Note

$$S_1 \cdots S_k = m(T)$$

where $m(x)$ is a polynomial in the form specified in the statement of the Lemma.

We'll now show that $m(x)$ is indeed the minimal polynomial of T. By Theorem 16.8 and Definition 16.9, the minimal polynomial $m_T(x)$ of T must be a factor of any other polynomial $f(x)$ such that $f(T) = \mathbf{0}_{L(V,V)}$. In particular, $m_T(x)$ must divide $m(x) = (x - \xi_1) \cdots (x - \xi_k)$. Since we are already displaying $m(x)$ in terms of its complete factorization, it's clear that $m_T(x)$ if it is to be a factor of $m(x)$ must be factorizable in a similar way, except that some of factors $(x - \xi_k)$ that appear in $m(x)$ might not appear in $m_T(x)$. However, if one removes any factor $(x - \xi_i)$ from $m(x)$, one ends up with an operator

$$S_1 \cdots S_{i-1} S_{i+1} \cdots S_k$$

that does not vanish on the ξ_i-eigenspace of T. Thus, the minimal polynomial of T actually coincides with the polynomial $m(x)$.

$\Longleftarrow$ If the minimal polnomial of T takes the specied form

$$m_T(x) = (x - \xi_1) \cdots (x - \xi_k)$$

then by Theorem 17.17, the above factorization of $m_T(x)$ leads to operators E_i such that

$$V = E_1(V) \oplus E_2(V) \oplus \cdots \oplus E_k(V) \tag{7}$$

with

$$E_i(V) = \ker (T - \xi_i \mathbf{1}) \tag{8}$$

It's pretty clear that (7) and (8) say that V has a direct sum decomposition into eigenspaces of T (as each $\ker(T - \xi_i \mathbf{1})$ is exactly the ξ_i-eigenspace of T). If we chose a basis $\left\{v_1^{(i)}, \ldots, v_\ell^{(i)}\right\}$ for each subspace $E_i(V)$, it is clear that (1) each basis vector is an eigenvector of T, (2) that the basis vectors for different subspaces $E_i(V)$ and $E_j(V)$ are linearly independent, and (3) that the union of the bases of the individual $E_i(V)$ will span V. Thus, we can form a basis for V consisting of T-eigenvectors Hence, V is diagonalizable.

$\square$

3.1. An Algorithm for Diagonalizing Matrices. Unfortunately, the diagonalizability criterion given in Theorem 17.19 is really only readily applicable in the situation where the characteristic polynomial

$$p_T(x) = \det(T - x\mathbf{1})$$

has $n = \dim V$ distinct roots. If there are factors like $(x-\xi_i)^m$ in the characteristic polynomial, it may **or** may not happen that the transformation T is diagonalizable; because the minimal polynomial might not **or** might also have factor of the form $(x-\xi_i)^k$ (or even a factor that is a irreducible polynomial of degree ≥ 2). The basic problem is the fact that we don't yet have a general algorithm that provides us the minimal polynomial $m_T(x)$ for a given linear transformation ; in fact, about all we know about $m_T(x)$ is that it has to divide the characteristic polynomial $p_T(x)$.

To make up for this deficiency in Theorem 17.19, I'll now describe a general algorithm for diagonalizing a matrix.

Let $p_T(x)$ be the characteristic polynomial of a linear transformation $T : V \to V$. In what follows, we shall suppose that $p_T(x)$ has a complete factorization in the form

$$p_T(x) = (x-\xi_1)^{m_1}(x-\xi_2)^{m_2}\cdots(x-\xi_k)^{m_k}$$

with

$$m_1 + m_2 + \cdots + m_k = n \equiv \dim V \quad . \tag{9}$$

(Such a factorization of $p_T(x)$ will always be possible when we are working over $\mathbb{C}$ or any other algebraically closed field.). Recall that each of the ξ_i will be an eigenvalue of T and that the exponents m_i of $(x-\xi_i)$ in the characteristic polynomial is referred to as the *algebraic multiplicity* $m_A(\xi_i)$ of the eigenvalue ξ_i.

The *geometric multiplicity* $m_G(\xi_i)$ of an eigenvalue ξ_i, on the other hand, is defined as

$$m_G(\xi_i) = \dim\ker(T - \xi_i\mathbf{1}) = \text{dimension of the } \xi_i\text{-eigenspace}$$

We always have,

$$1 \leq m_G(\xi_i) \leq m_A(\xi_i) \quad .$$

If the upper bound $m_G(\xi_i) = m_A(\xi_i)$ holds for all the eigenvalues ξ_i, then, by (9) we will have as many linearly independent eigenvectors as the dimension n of V; and so V will be diagonalizable. In other words,

$$\text{dimension of } \ker(T - \xi_i\mathbf{1}) = \#\text{ of factors of } (x-\xi_i) \text{ in } p_T(x) \text{ for each } i = 1,\ldots,k \quad \Rightarrow \quad T \text{ is diagonalizable} \tag{10}$$

So how does one construct the corresponding basis of eigenvectors? Well, this will just be a matter of determining all the eigenvectors of T, as we did in §16.3.3. More explicitly, we carry the following steps (working with a matrix representation of T).

(1) Factorize $p_T(x)$ to identify all the eigenvalues $\{\xi_1,\ldots,\xi_k\}$ of T.
(2) For each $\xi_i \in \{\xi_1,\ldots,\xi_k\}$ solve the homogeneous linear system

$$(T - \xi_i\mathbf{1})\,\mathbf{x} = \mathbf{0}$$

and express the solution in terms of a basis $\left\{v_1^{(i)},\ldots,v_{m_G(\xi_i)}^{(i)}\right\}$ for the solution space. Note that each of these basis vector will be an eigenvector of T with eigenvalue ξ_i, and the total number of eigenvectors found this way will be (by definition) the geometric multiplicity of ξ_i. Now if the number $m_G(\xi_i) \neq m_A(\xi_i)$ you may as well stop, because you will not have enough linearly independent eigenvectors for form a basis for V.
(3) On the other hand, if $m_G(\xi_i)$ always equals $m_A(\xi_i)$, then you will have found enough linearly independent eigenvectors to construct a basis of V. Moreover, you can also construct a *change-of-basis* matrix $\mathbf{C}$ that maps you from your original basis to a basis of eigenvectors. This matrix is formed by using the eigenvectors just found as its columns. Suppose for example that you found

n linearly independent eigenvectors $v_1, \ldots, v_n$ and $\lambda_1, \ldots \lambda_n$ are there corresponding eigenvalues. Then the matrix

$$\mathbf{C} = \begin{pmatrix} | & | & & | & | \\ | & | & & | & | \\ \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_{n-1} & \mathbf{v}_n \\ | & | & & | & | \\ | & | & & | & | \end{pmatrix}$$

will convert the i^{th} standard basis vector for $\mathbb{R}^n$ to the i^{th} eigenvector for T, and so allow one to carry out a change of coordinates from the standard basis to a basis of eigenvectors.

Example 18.20. Find the matrix $\mathbf{C}$ that diagonalizes the matrix $\mathbf{A} = \begin{pmatrix} -1 & 0 & 1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{pmatrix}$, characteristic polynomial: $X^3 + 2X^2$

- I'll just run the highlights of the method described above.

$$\det(\mathbf{A} - \lambda \mathbf{I}) = \det \begin{pmatrix} -1-\lambda & 0 & 1 \\ 3 & -\lambda & -3 \\ 1 & 0 & -1-\lambda \end{pmatrix} = 0 - \lambda \det \begin{pmatrix} 1-\lambda & 1 \\ 1 & 1-\lambda \end{pmatrix} = -\lambda^2 (\lambda + 2)$$

So we have two eigenvalues $\lambda = 0, -2$. The corresponding eigenvectors are

$$\begin{aligned} \lambda &= 0 \quad \Rightarrow \quad NullSp\left(\mathbf{A} - (0)\,\mathbf{I}\right) = span\left(\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right) \\ \lambda &= 1 \quad \Rightarrow \quad NullSp\left(\mathbf{A} - (1)\,\mathbf{I}\right) = span\left(\begin{bmatrix} -1 \\ 3 \\ 1 \end{bmatrix} \right) \end{aligned}$$

Thus, we three linearly independent eigenvectors

$$\begin{aligned} v_1 &= \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \quad \text{with eigenvalue } 0 \\ v_2 &= \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \text{with eigenvalue } 0 \\ v_3 &= \begin{bmatrix} -1 \\ 3 \\ 1 \end{bmatrix} \quad \text{with eigenvalue } 1 \end{aligned}$$

The diagonalization matrix $\mathbf{C}$ should thus be

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 1 \end{pmatrix}$$

,Computing the inverse of $\mathbf{C}$, one finds

$$\mathbf{C}^{-1} = \begin{pmatrix} \frac{3}{2} & 1 & -\frac{3}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$$

Then, one can verify, via matrix multiplication, that

$$\mathbf{C}^{-1}\mathbf{A}\mathbf{C} = \begin{pmatrix} \frac{3}{2} & 1 & -\frac{3}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} -1 & 0 & 1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

$\square$

EXAMPLE 18.21. An application. Solving systems of linear first order ordinary differential equations.

Suppose you are given the followinng system of ODEs

$$\begin{aligned}\frac{dx_1}{dt} &= 2x_1 - 3x_2 + 7x_3 \\ \frac{dx_2}{dt} &= 5x_2 + x_3 \\ \frac{dx_3}{dt} &= -x_3\end{aligned}$$

How would you solve it?

- Let's write the system of ODEs in matrix form

$$\frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 & -3 & 7 \\ 0 & 5 & 1 \\ 0 & 0 & -1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

or, more compactly,

$$\frac{d}{dt}\mathbf{x} = \mathbf{A}\mathbf{x} \quad .$$

Now if the coefficient matrix had been diagonal this system would have been easy to solve

(11) $$\frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \quad \Rightarrow \quad \begin{array}{lcl} \frac{dx_1}{dt} = \lambda_1 x_1 & \Rightarrow & x_1(t) = c_1 e^{\lambda_1 t} \\ \frac{dx_2}{dt} = \lambda_2 x_2 & \Rightarrow & x_2(t) = c_2 e^{\lambda_2 t} \\ \frac{dx_3}{dt} = \lambda_3 x_3 & \Rightarrow & x_3(t) = c_3 e^{\lambda_3 t} \end{array}$$

On the other hand, if the coefficient matrix $\mathbf{A}$ is diagonalizable, then we'll be able to construct a matrix $\mathbf{C}$ from the eigenvectors of $\mathbf{A}$, so that

$$\mathbf{C}^{-1}\mathbf{A}\mathbf{C} = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix} \equiv \mathbf{D}$$

where $\lambda_1, \lambda_2, \lambda_3$ are the eigenvalues of $\mathbf{A}$.

Now consider the vector function

(12) $$\mathbf{y}(t) = \mathbf{C}^{-1}\mathbf{x}(t)$$

It will satisfy

$$\frac{d}{dt}\mathbf{y} = \frac{d}{dt}\left(\mathbf{C}^{-1}\mathbf{x}\right) = \mathbf{C}^{-1}\left(\frac{d}{dt}\mathbf{x}\right) = \mathbf{C}^{-1}\mathbf{A}\mathbf{x} = \mathbf{C}^{-1}\mathbf{A}\mathbf{C}\mathbf{C}^{-1}\mathbf{x} = \left(\mathbf{C}^{-1}\mathbf{A}\mathbf{C}\right)\left(\mathbf{C}^{-1}\mathbf{x}\right) = \mathbf{D}\mathbf{y}$$

Since, $\mathbf{D}$ is a diagonal matrix, the vector function $\mathbf{y}$ has an easy solution as determined by (11).

$$\mathbf{y}(t) = \begin{bmatrix} c_1 e^{\lambda_1 t} \\ c_2 e^{\lambda_2 t} \\ c_3 e^{\lambda_3 t} \end{bmatrix}$$

But then we can recover the original vector function $\mathbf{x}(t)$ from this $\mathbf{y}(t)$ by multiplying both sides of (12) by $\mathbf{C}$

$$\mathbf{x}(t) = \mathbf{C}\mathbf{y}(t) = \mathbf{C}\begin{bmatrix} c_1 e^{\lambda_1 t} \\ c_2 e^{\lambda_2 t} \\ c_3 e^{\lambda_3 t} \end{bmatrix}$$

So the general solution of a system of ODEs of the form

$$\frac{d\mathbf{x}}{dt} = \mathbf{A}\mathbf{x}$$

where $\mathbf{A}$ is a constant coefficient matrix is readily solvable once you know the eigenvectors of $\mathbf{A}$ (these give you the columns of $\mathbf{C}$) and the eigenvalues of $\mathbf{A}$ (the give you the exponential functions $e^{\lambda_i t}$)