Structure of a Linear Operator

May 7, 2009

1 Where to look for invariant subspaces of a linear operator? Let $T\colon V \to V$ be a linear operator. If $S\colon V \to V$ is another operator *and* T *commutes* with S, i.e., if

$$[S,T] := ST - TS = 0, \tag{1}$$

then both the *range*, $\mathsf{R}[S]$, and the eigenspaces,

$$\mathsf{E}_\lambda[S] := \{v \in V \mid Sv = \lambda v\} \tag{2}$$

are T-invariant for any $\lambda \in F$.

Indeed, if $v \in \mathsf{R}[S]$, then $v = Su$ for some $u \in V$ and

$$Tv = T(Su) = (TS)u = (ST)u = S(Tu) \quad \in \mathsf{R}[S].$$

Similarly, if $v \in \mathsf{E}_\lambda[S]$, then

$$S(Tv) = (ST)v = (TS)v = T(Sv) = T(\lambda v) = \lambda Tv,$$

i.e., Tv is a λ-eigenvector for S.

2 Projections Even better if one can find a *projection*[1] $P\colon V \to V$ which commutes with T. For a projection one has the direct sum decomposition

$$V = \mathsf{N}[P] \oplus \mathsf{R}[P] \tag{3}$$

and both the null space and the range of P are T-invariant.

***Verification of* (3).** *For any $v \in V$, one has*

$$v = (v - Pv) + Pv = (I - P)v + Pv$$

and

$$P(v - Pv) = Pv - P^2v = Pv - Pv = 0$$

shows that $(I-P)v \in \mathsf{N}[P]$. Vice-versa, if $v \in \mathsf{N}[P]$, then $v = (I-P)v$ and hence

$$\mathsf{N}[P] = \mathsf{R}[I-P] \qquad \textit{and} \qquad \mathsf{R}[P] = \mathsf{N}[I-P].$$

It follows that if $v \in \mathsf{N}[P] \cap \mathsf{R}[P] = \mathsf{N}[P] \cap \mathsf{N}[I-P]$, then

$$v = (I-P)v + Pv = 0 + 0 = 0$$

This completes the verification of (3).

So, the next question is

3 Where to look for operators commuting with a given operator? Let us begin by observing that if S and S' commute with T, then $S+S'$ and SS' do.[2] In particular, for any polynomial $f(x) \in F[x]$,

$$f(x) = a_nx^n + \cdots + a_1x + a_0 \qquad (a_i \in F) \tag{4}$$

T commutes with

$$f(T) := a_nT^n + \cdots + a_1T + a_0I$$

[1] A linear operator $P\colon V \to V$ is called a *projection* if $P^2 = P$.

[2] Verify that! It is straightforwrd to do that.

4 The annihilator ideal (of an operator) For any operator $T \in \mathcal{L}(V)$, the set of polynomials *annihilating* T,

$$\operatorname{ann} T := \{f(x) \in F[x] \mid f(T) = 0\} \tag{5}$$

is closed wit respect to addition and multiplication by *any* polynomial in $F[x]$. Such subsets are called *ideals* (in the *ring* of polynomials, $F[x]$).

If V is finite dimensional, say of dimension n, then the ring of all linear operators $\mathcal{L}(V)$ is of dimension n^2. In particular, $n^2 + 1$ elements of $\mathcal{L}(V)$:

$$I,\, T,\, \dots,\, T^{n^2}$$

must be linearly dependent, i.e., there must exist $a_i \in F$, not all zero, such that

$$a_n T^n + \cdots + a_1 T + a_0 I = 0$$

which shows that the annihilator ideal of any operator on a finite dimensional space contains at least one nonzero polynomial.

A celebrated theorem due to Cayley and Hamilton states that the *characteristic* polynomial of T,

$$\phi_T(x) = \det(T - xI), \tag{6}$$

which is of degree $n = \dim V$, belongs to $\operatorname{ann} T$ but we shall not need this classical result of Linear Algebra.

5 Principal ideals For *any* polynomial $g(x)$, the set of polynomials $f(x)$ divisible by $g(x)$,

$$(g(x)) := \{f(x) = \rho(x)g(x) \mid \text{ for some } \rho(x) \in F[x]\} \tag{7}$$

is obviously an ideal. Such ideals are called *principal*. It immediately follows from the definition that two principal ideal $(g(x))$ and $(h(x))$ are equal *if and only if* $h(x)$ is divisible by $g(x)$ and $g(x)$ is divisible by $g'(x)$, which is possible precisely when $h(x)/g(x)$ is an invertible polynomial, i.e., a nonzero constant (polynomial) $c \in F$. If

$$g(x) = b_m x^m + \cdots + b_1 x + b_0$$

is a polynomial of exactly degree m, then the polynomial

$$g_0 := x^m + \frac{b_{m-1}}{b_m} x^{m-1} + \cdots + \frac{b_1}{b_m} x + \frac{b_0}{b_m} \tag{8}$$

generates the same ideal as $g(x)$ does:

$$(g(x)) = (g_0(x)). \tag{9}$$

Polynomials with the *leading* coefficients equal to 1 are called *monic*. Because of (9) it is often assumed that a generator of a principal ideal is monic. This is convenient because for monic polynomials, the ideals are equal *if and only if* the generating polynomials are equal:

$$(g_1(x)) = (g_2(x)) \qquad \text{if and only if} \qquad g_1(x) = g_2(x).$$

6 The minimal polynomial (of an operator) It is a remarkable property of the ring of polynomials that every ideal, J, in $F[x]$ is principal. This is a very special property shared with the ring of integers $\mathbb{Z}$.

Thus also the annihilator ideal of an operator T is principal, hence there exists a (unique) monic polynomial $p_T(x)$ that generates $\operatorname{ann} T$ when $\operatorname{ann} T$ is not zero, and the latter is the case for any operator on a finite dimensional vector space.

This monic polynomial is unique, see Sect. 5, and is referred to as the *minimal polynomial* of operator T.

7 Let $f(x)$ be any nonzero polynomial that annihilates T. We know from Sect. 4 that, for every operator on a finite dimensional vector space, such polynomials exist.

Suppose that $f(x)$ can be factored

$$f(x) = g(x)h(x) \tag{10}$$

into the product of *relatively prime* polynomials $g(x)$ and $h(x)$. The latter means that the only common divisor of both can be a constant nonzero polynomial. In this case, the ideal generated by $g(x)$ and $h(x)$,

$$(g(x), h(x)) := \{\rho(x)g(x) + \sigma(x)h(x) \mid \rho(x), \sigma(x) \in F[x]\}, \tag{11}$$

being principal, must coincide with $(1) = F[x]$. Thus, there exist polynomials $r(x)$ and $s(x)$ such that

$$1 = r(x)g(x) + s(x)h(x).$$

In particular,

$$I = r(T)g(T) + s(T)h(T). \tag{12}$$

Denote operator $r(T)g(T)$ by P. It follows from (12) that $s(T)h(T) = I - P$ and

$$\begin{aligned} P &= PI = P(P + (I - P)) = P^2 + P(I - P) = P^2 + (r(T)g(T))(s(T)h(T)) \\ &= P^2 + r(T)g(T)h(T)s(T) = P^2 + r(T)f(T)s(T) \\ &= P^2. \end{aligned}$$

In other words, P is a projection and, being polynomial in T, commutes with T.

Using P we obtain, as was explained in Sect. 2, a decomposition of V into the direct sum

$$V = V_1 \oplus V_2 \tag{13}$$

of T-invariant subspaces

$$V_q := \mathsf{N}[P] \qquad \text{and} \qquad V_2 := \mathsf{R}[P]$$

as in (3).

Denote by $T_1 \colon V_1 \to V_1$ the restriction of T to V_1, and by T_2, the corresponding restriction of T to V_2. Note that if we decompose any vector $v \in V$ as the sum $v_1 + v_2$ for $v_1 \in V_1$ and $v_2 \in V_2$, then

$$Tv = T(v_1 + v_2) = Tv_1 + Tv_2 = T_1(v_1) + T_2(v_2).$$

It is common to say in this case that operator T decomposes into a *direct sum* of operators $T_1 \colon V_1 \to V_1$ and $T_2 \colon V_2 \to V_2$. We express this by writing

$$T = T_1 \oplus T_2. \tag{14}$$

Since $v = Pv$ for any $v \in \mathsf{R}[P] = V_2$, we have

$$h(T)v = h(T)Pv = (h(T)r(T)g(T))v = (r(T)g(T)h(T))v = r(T)(f(T)v) = 0 \tag{15}$$

for $v \in V_2$. And since $\mathsf{N}[P] = \mathsf{R}[I - P]$ and $I - P$ is a projection as well, we have likewise

$$g(T)v = 0 \tag{16}$$

for $v \in V_1$. Since $g(T_1)$ is the restriction of $g(T)$ to V_1 and $h(T_2)$ is the restriction of $h(T)$ to V_2, formula (16) means that polynomial $g(x)$ annihilates operator T_1 while formula (15) means that $h(x)$ annihilates operator T_2.

We estabilished the following important result

8 Operator Decomposition Theorem *Let $f(x)$ be any polynomial that annihilates operator $T\colon V \to V$. Then, for any factorization* (10) *of $f(x)$ into a product of two relatively prime polynomials $g(x)$ and $h(x)$, there exists a decomposition of T into a direct sum* (14) *such that*

$$g(x) \text{ annihilates } T_1 \quad \text{and} \quad h(x) \text{ annihilates } T_2.$$

By applying this theorem several times, we obtain also the following corollary.

9 Corollary *Let $f(x)$ be any polynomial that annihilates operator $T\colon V \to V$. Then, for any factorization of $f(x)$ into a product of pairwise relatively prime polynomials,*

$$f(x) = g_1(x) \cdots g_r(x) \tag{17}$$

there exists a decomposition of T into a direct sum

$$T = T_1 \oplus \cdots \oplus T_r \tag{18}$$

corresponding to a decompostion of vector space V into a direct sum of certain T-invariant subsapces,

$$V =_1 \oplus \cdots \oplus V_r,$$

such that

$$g_1(x) \text{ annihilates } T_1, \ \ldots, \ g_r(x) \text{ annihilates } T_r.$$

10 Primary decomposition Every nonzero polynomial, (4), admits a factorization

$$f(x) = a_n (p_1(x))^{m_1} \cdots (p_r(x))^{m_r} \tag{19}$$

for a certain number of distinct irreducible monic polynomials $p_i(x)$. Factorization (19) is unique in the sense that the irreducible polynomials, $p_i(x)$, their number, r, and their exponents, m_i, are determined by $f(x)$ uniquely (up to permutation of factors in (19)). This is the so called *primary decomposition* of a polynomial $f(x)$.

Any two primary factors $(p_i(x))^{m_i}$ and $(p_j(x))^{m_j}$ corresponding to distinct $p_i(x)$ and $p_j(x)$ are relatively prime.

If $f(x)$ annihilates operator T we can apply Corollary 9 to obtain the corresponding decomposition of operator T such that each T_i is annihilated by the corresponding primary factor $(p_i(x))^{m_i}$ of the primary decomposition of polynomial $f(x)$.

It is not hard to see that if we disregard that some V_i may be zero subspaces, the obtained decomposition, (18), of operator T will not depend on the initial choice of $f(x)$! This follows from the fact that the annihilator ideal, $\operatorname{ann} T$, is generated by a unique monic polynomial, namely by the minimal polynomial of operator T, see Sect. 6 above.

11 This is as much as the method of factorization of a polynomial that annihilates T can yield. What remains to be done is to describe the structure of the "primary" components $T_1, \ldots, T_r$.

As a minimum we should know all the irreducible polynomials with coefficients in a given field of scalars F. For general fields this may be a very complicated task.

Fortunately, there are fields where all irreducible polynomials are known and their structure is as simple as possible.

The best in this regard are so called *algebraically closed fields*.

12 Algebraically closed fields Any polynomial of degree exactly 1 is always automatically irreducible. This follows from the fact that if it were reducible the degrees of its nontrivial factors would have to be less than 1 and greater than 0 which is clearly not possible as the degrees are integers.

A field F is said to be *algebraically closed* if only polynomials of degree 1 are irreducible. For example, the field of complex numbers, $\mathbb{C}$, is algebraically closed while the field of real numbers, $\mathbb{R}$, is not. Over $\mathbb{R}$, a polynomial is irreducible if it is either of degree 1, or of degree 2,

$$ax^2 + bx + c,$$

with no real roots (i.e., when $b^2 - 4ac < 0$).

13 The primary decomposition of an operator (algebraically closed field case) Let us assume that the scalar field F be algebraically closed. The primary decomposition of any monic nonzero polynomial $f(x)$ has the form

$$f(x) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_r)^{m_r} \tag{20}$$

where $\{\lambda_1, \ldots, \lambda_r\}$ is the set of all distinct roots of $f(x)$, and exponents $m_1, \ldots, m_r$ are their multiplicities.

Since $(x - \lambda_r)^{m_r}$ annihilates the corresponding *primary* component, T_i, of operator T, we know that each such component has the form

$$T_i = \lambda_i I + N_i \tag{21}$$

where

$$N_i^{m_i} = 0$$

Operators whose certain power is zero are called *nilpotent*. An operator is nilpotent if it is annihilated by a *monomial*.

Thus the only task left in the case when the scalar field is algebraically closed is to describe the structure of a nilpotent operator. And this can be done in exactly the same way for all fields.

14 Nilpotent operators Over any field F, an operator $n\colon V \to V$ with the matrix

$$\begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} \tag{22}$$

in some basis is nilpotent. We will call such operators *nilpotent cells* of size $n = \dim V$.

15 Nilpotent Operator Structure Theorem *Any nilpotent operator N on a finite dimensional vector space is the direct sum of nilpotent cells. In other words, for every nilpotent operator, there exists a basis β in which its matrix $[N]_\beta$ is the block diagonal matrix with blocks being matrices* (22) *of varying sizes.*

This is not difficult to prove but requires a rather careful analysis.

As a corollary, we obtain the following classical result

16 Jordan cell decomposition of an operator An operator T on a finite dimensional vextor space V is called a *Jordan cell* if it is of the form

$$\lambda I + N$$

for some $\lambda \in F$ and a nilpotent cell N.

Equivalently, T is a Jordan cell if it admits a basis β in which its matrix $[T]_\beta$ has the form

$$\begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix} \tag{23}$$

17 Jordan Canonical Form Theorem *Every operator T on a finite dimensional vector space V over an algebraically closed field is a dirct sum of Jordan cells. in other words, T admits a basis β in which its matrix $[T]_\beta$ is the block-diagonal matrix with diagonal blocks being of the form* (23).

Scalars λ are all the possible eigenvalues of T, the size an number of cells can vary. The sum of their sizes, of course, equals $\dim V$.