Lecture 18: The minimal Polynomial of a Linear Transformation

Subsituting a Linear Transformation into a Polynomial

Let V be a vector space over F of dimension n. $T \in L(V, V)$ and $f(x) \in F[x]$. We want to define $f(T) \in L(V, V)$.

Definition

If $f(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$ then

$$f(T) = a_k T^k + a_{k-1} T^{k-1} + \ldots + a_1 T + a_0 I$$

We could also evaluate at a square matrix A:

$$f(A) = a_k A^k + a_{k-1} A^{k-1} + \ldots + a_1 A + a_0 I$$

Proposition

The matrix of $f(T)$ relative to the basis $\mathscr{B}$ is $f(A)$, where A is the matrix of T relative to the basis $\mathscr{B}$.

Let $\Phi_T : F[x] \longrightarrow L(V, V)$ be given by

$$\Phi_T(f) = f(T).$$

Proposition

Φ_T is is linear and satisfies

$$\Phi_T(fg) = \Phi_T(f)\Phi_T(g). \tag{1}$$

Φ_T is not onto (for n strictly greater than 1) and has an infinite dimensional kernel (null-space).

Proof. It is clear that Φ_T is linear. We first prove Equation (1). The left-hand side of Equation (1) is $\Phi_T(fg) = (fg)(T)$ and the right-hand side of Equation (1) is f(T)g(T). So we must prove that $(fg)(T) = f(T)g(T)$. Suppose $f(x) = \sum_{i=0}^{k} a_i x^i$ and $g(x) = \sum_{j=0}^{\ell} a_j x^j$. Then

$$(fg)(x) = \sum_{m=0}^{k+\ell} \Big(\sum_{i,j:i+j=m} a_i b_j \Big) x^m. \tag{2}$$

We continue the proof of the Proposition.

From Equation (2) we obtain

$$(fg)(T) = \sum_{m=0}^{k+\ell} \Big(\sum_{i,j:i+j=m} a_i b_j \Big) \, T^m .$$

But $f(T) = \sum_{i=0}^{k} a_i T^i$ and $g(T) = \sum_{j=0}^{\ell} a_j T^j$ and hence

$$f(T)g(T) = \sum_{m=0}^{k+\ell} \Big(\sum_{i,j:i+j=m} a_i b_j \Big) \, T^m = fg(T).$$

$\square$

Now we prove that Φ_T is not onto. Note that

$$f(T)g(T) = (fg)(T) = (gf)(T) = g(T)f(T).$$

So any two elements in the image of Φ commute. So take two non-commuting elements in $L\left(V, V\right)$ (we need $n > 1$ to do this.) They cannot both be in the image of Φ_T.

We next prove that Φ_T has a nonzero kernel - in fact we show how to construct elements of that kernel. Take any subset $\{f_1, f_2, \cdots, f_{n^2+1}\}$ of n^2+1 elements of $F[x]$ (e.g. $\{1, x, x^2, \cdots, x^{n^2}\}$). Then the set $\{f_1(T), f_2(T), \cdots, f_{n^2+1}(T)\}$ is a subset of $L(V, V)$ containing n^2+1 elements. But the dimension of $L(V, V)$ is n^2 so there must be a linear relation among the elements of this set.
Hence there is a relation

$$\sum_{i=1}^{n^2+1} c_i f_i(T) = 0, \quad c_i \neq 0.$$

Then $\sum_{i=1}^{n^2+1} c_i f_i$ is a nonzero element in $\mathrm{Ker}(\Phi_\mathrm{T})$. So we have proved $\mathrm{Ker}(\Phi_\mathrm{T})$ is nonzero. To see that it is infinite dimensional see the remark on the next slide. □

Remark:Why does Φ_T have an infinite - dimensional nullspace?
The dimension of F[x] is infinite dimensional and the dimension of $L\,(V,\,V)$. Any linear map from an infinite dimensional space to a finite dimensional space has an infinite dimensional kernel.

The Minimal Polynomial

We just saw $I, T, T^2, \ldots, T^{n^2}$ must be linearly dependent since $\dim L(V, V) = n^2$. Hence there exist scalars $a_0, a_1, \ldots, a_{n^2}$ so that

$$a_0 I + a_1 T + \ldots + a_{n^2} T^{n^2} = 0.$$

So $f(x) = a_0 I + a_1 x + \ldots + a_{n^2} x^{n^2}$ is in $\mathrm{Ker}(\Phi_\mathrm{T})$. In other words, there is a linear relation between the power $I, T, T^2, \ldots, T^{n^2}$

Remark: We just showed there is always always a linear relation between the powers

$$I, T, T^2, \ldots, T^{n^2}.$$

We will now see that often we can get a even smaller power degree relation.

Fundamental Question

What is the smallest power k so that there is a nontrivial linear relation among I, T, T^2, $\ldots$, T^k?

First–there is a unique such k. Let

$$R = \left\{ \ell : \text{ there is a linear relation among the powers } I, T, T^2, \ldots, T^\ell \right\}$$

Since $n^2 \in R$, R is nonempty.

The smallest possible is $k = 1$.

- If $k = 0$, we would have

$$a_0 T^0 = 0, \quad a_0 \neq 0.$$

  But $T^0 = I$, a contradiction.

- If $k = 1$, we would have

$$a_0 T^0 + a_1 T = 0 \Longleftrightarrow T \text{ is a scalar (a multiple of)} I.$$

If T is not scalar, $k \geq 2$.

Choose a minimal degree linear relation

$$a_k T^k + a_{k-1} T^{k-1} + \ldots + a_1 T + a_0 I = 0$$

Divide by a_k to make it monic:

$$T^k + b_{k-1} T^{k-1} + \ldots + b_1 T + b_0 I = 0$$

Define

$$m(x) = x^k + b_{k-1} x^{k-1} + \ldots + b_1 x + b_0 I = 0$$

so $m(T) = 0$.

We need

Lemma

Suppose $f(x)$ *satisfies* $\deg(f) < k$. *Then*

$$f(T) = 0 \Longleftrightarrow f(x) = 0 (= \text{ the zero-polynomial}).$$

Proof. By definition, k is the smallest degree so that there is a nonzero polynomial satisfying $f(T) = 0$. $\square$

Theorem

Suppose $0 \neq f(x) \in F[x]$ *satisfies* $f(T) = 0$. *Then* $m(x) | f(x)$.

Proof. By the lemma, $\deg(f) \geq \deg(m)$. So we can divide f by m.

$$f(x) = Q(x)m(x) + R(x)$$

with $\deg(R(x)) < \deg(m(x))$. Now evaluate

$$f(T) = Q(T)m(T) + R(T)$$

But $f(T) = m(T) = 0$. Hence $R(T) = 0$. But $\deg(R(x)) < \deg(m(x))$, so $R(T) = 0 \implies R(x) = 0$ by the lemma. $\square$

Corollary

$m(x)$ is unique.

Proof. Suppose $m_1(x)$ is another monic polynomial of degree k so that $m_1(T) = 0$. Then $m(x)|m_1(x)$ so (since we have the same degree), $m_1(x) = cm(x)$. But since both $m(x)$ and $m_1(x)$ are monic, we have $c = 1$. $\square$

Definition

$m(x)$ is called the miniminal polynomial of the linear transformation T. Sometimes we will write m_T.

Note: It's hard to compute–it is even hard to compute $k = \deg(m_T)$. Now let $A \in M_n(F)$. We can repeat the whole theory to define

$$m_A = \text{ the monic polynomial } f \text{ of smallest degree such that } f(A) = 0.$$

Theorem

Suppose $T \in L(V, V)$, $\mathscr{B} = (b_1, b_2, \ldots, b_n)$ *is an ordered basis of* V *and* $A = M(T) = {}_{\mathscr{B}}[T]_{\mathscr{B}}$.
Then

$$m_T = m_A$$

We will need

Lemma

Let $f(x) \in F[x]$, A, T, $\mathscr{B}$ *be as above. Then*

$$M(f(T)) = f(A).$$

Proof of Lemma. $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 I$. So

$$f(T) = a_k T^k + a_{k-1}T^{k-1} + \ldots + a_1 T + a_0 I$$

But M satisfies M(ST)= M(S)M(T), so $M(T^j) = M(T)^j$ so

$$\begin{aligned} M(f(T)) &= M(a_k T^k + a_{k-1}T^{k-1} + \ldots + a_1 T + a_0 I) \\ &= M(a_k T^k) + M(a_{k-1}T^{k-1}) + \ldots + M(a_1 T) + M(a_0 I) \\ &= a_k M(T^k) + a_{k-1}M(T^{k-1}) + \ldots + a_1 M(T) + a_0 M(I) \\ &= a_k A^k + a_{k-1}A^{k-1} + \ldots + a_1 A + a_0 I = f(A). \quad \square \end{aligned}$$

Corollary

$f(T) = 0 \iff f(A) = 0.$

m_T is the monic nonzero polynomial of lowest degree in the space

$$\mathcal{N}_T = \{f \in F[x] : f(T) = 0\}$$

m_A is the monic polynomial of lowest degree in the space

$$\mathcal{N}_A = \{f \in F[x] : f(A) = 0\}$$

But we just saw that $\mathcal{N}_T = \mathcal{N}_A$ so the smallest degree monic polynomial in each of the subspaces is the same.

We now show that if a matrix A is similar to a matrix B (this means $B = PAP^{-1}$) then A and B have the same minimal polynomials.

Proposition

$m_{PAP^{-1}}(x) = m_A(x)$

Proof of the Proposition We will show

$$\mathcal{N}_A = \mathcal{N}_{PAP^{-1}}.$$

Then the unique lowest lowest degree monic polynomial in in each space must be the same.

Suppose $f \in F[x]$. We wish to show

$$f(PBP^{-1}) = Pf(B)P^{-1}, \text{ for all } n \text{ by } n \text{ matrices } B. \tag{3}$$

We first claim we have

$$(PBP^{-1})^k = PB^kP^{-1} \tag{4}$$

Indeed

$$(PBP^{-1})^k = (PBP^{-1})(PBP^{-1}) \cdots (PBP^{-1})$$

But note that the k-1 adjacent P's and P^{-1}'s cancel and the claim follows.

Now we prove Equation (3). Suppose $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$. Then

$$f(PBP^{-1}) = a_k(PBP^{-1})^k + a_{k-1}(PBP^{-1})^{k-1} + \cdots + a_0 I.$$

Apply the above claim to each of the first k terms on the right-hand side of the previous equation and use $PIP^{-1} = I$ to obtain

$$f(PBP^{-1}) = a_k PB^k P^{-1} + a_{k-1}PB^{k-1}P^{-1} + \cdots + a_0 PIP^{-1}.$$

Now factor P from the left and P^{-1} from the right in the right-hand side of the peevious equation to obtain

$$f(PBP^{-1}) = Pf(B)P^{-1}.$$

Now we can prove $\mathcal{N}_A = \mathcal{N}_{PAP^{-1}}$ and hence the Proposition. Indeed,

$$f \in \mathcal{N}_A \iff f(A) = 0 \iff Pf(A)P^{-1} = 0 \iff f(PAP^{-1}) = 0.$$

But $f(PAP^{-1}) = \iff f \in \mathcal{N}_{PAP^{-1}}$. Hence

$$\mathcal{N}_A = \mathcal{N}_{PAP^{-1}}$$

and the Proposition follows. $\square$