Lecture 17: 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 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ then

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

We could also evaluate at a square matrix A:

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

Theorem

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 an F-algebra homomorphism. Φ_T is not onto (for n ¿1) and had a big kernel.

Why isn't it onto?

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

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

Why does Φ_T have a big nullspace?
Take any set of $n^2 + 1$ linearly independent elements of $F[x]$, $\{f_1, f_2, \ldots, f_{n^2+1}\}$ (e.g. $1, x, x^2, \ldots, x^{n^2}$). Then

$$\{f_1(T), f_2(T), \ldots, f_{n^2+1}(T)\}$$

is a set of $n^1 + 1$ elements in $L(V, V)$, an n^2 dimensional vector space.

Hence there is a relation

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

Then $\sum_{i=1}^{n^2+1} c_i f_i \in \mathrm{Ker}(\Phi_\mathrm{T})$ is a non-zero elements is an infinite dimensional vector space?

The Minimal Polynomial

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

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

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: In fact, we will see later that there is always a linear relation between the powers

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

and often we can get a even smaller power k.

Fundamental Question

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

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*

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

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

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. □

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 $c = 1$. □

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 is a ring homomorphism, so

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

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.