Lecture 18

The Minimal Polynomial of a Linear Transformation

Substituting 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 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ then

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

(we could also evaluate at a square matrix A.

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

Proposition

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

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 has 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 any 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 null-space?

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

Hence there is a relation

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

Then $\left(\sum_{i=1}^{n^2+1} c_i f_i\right) \in \ker \Phi_T$ is a non-zero element of the kernel.

How many ways are there of picking n^2+1 linearly independent elements in an infinitie dimensional vector space?

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

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

So $f(x) = a_0 + a_1 x + \cdots + a_{n^2} x^{n^2}$ is in $\ker \Phi_T$

So any multiple of $f(x)$ is in $\ker \Phi_T$.

In other words, there is always a linear relation between the powers

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

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

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

and often we can get an even smaller power k.

Fundamental Question

What is the smallest power k so that there is a nontrivial linear relation among $1, T, T^2, \dots, T^k$?

First - there is a unique such k:

Let $R = \{ l : \text{there is a linear relation among the powers } 1, T, \dots, T^l \}$

Since $n^2 \in R$, R is non-empty.

The smallest possible is $k=1$.

If $\underline{k=0}$, we would have

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

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

If $\underline{k=1}$, we have

$$a_0 I + a_1 T = 0 \iff T \text{ is scalar} \left(\begin{matrix}\text{a multiple} \\ \text{of } I\end{matrix}\right)$$

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

Choose a minimal degree linear relation

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

Divide by a_k to make it monic:

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

Define:

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

So $m(T) = 0$.

We need

Lemma

Suppose $f(x)$ satisfies $\deg f < k$

Then $f(T) = 0 \iff f(x) = 0$ (the zero polynomial)

Proof By definition k is the smallest degree for which there is a nonzero polynomial satisfying $f(T)=0$ (at least) □

Theorem

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

Then $m(x) \mid f(x)$.

Proof:

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

$$f(x) = Q(x)\, m(x) + R(x) \quad \text{with } \deg R(x) < \deg m(x).$$

Now evaluate both sides at T.

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

But $f(T) = m(T) = 0$, hence $R(T) = 0$.

But $\deg R < \deg m$ so $R(T) = 0 \Rightarrow R(x) = 0$ 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 $m(x) \mid m_1(x)$ so (since they have the same degree) $m_1(x) = c\,m(T)$. But since both $m(x)$ and $m_1(x)$ are monic we have $c = 1$.

□

Definition:

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

It is 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 = the monic polynomial f of smallest degree so that $f(A) = 0$.

Theorem

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

Then $m_T = m_A$

We will need

Lemma

Let $f \in F[x]$, $A, T, \mathcal{B}$ be as above.

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

proof

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

So $f(T) = a_k T^k + \cdots + a_1 T + a_0 I$

But M is a ring homomorphism, so

$$M(f(T)) = M(a_k T^k + \cdots + a_1 T + a_0 I)$$

$$= M(a_k T^k) + \cdots + M(a_1 T) + M(a_0 I)$$

$$= a_k M(T)^k + \cdots + a_1 M(T) + a_0 M(I)$$

$$= a_k A^k + \cdots + a_1 A + a_0 I = f(A).$$

□

Corollary

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

---

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

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

m_A is the monic polynomial of lowest degree in the space

$$N_A = \{ f \in F[x] : f(A) = 0 \}.$$

But we just saw $N_T = N_A$ so the smallest degree monic polynomial in each of the two subspaces is the same.