1 Minimal Polynomials

1.1 Review

- There is a factorisation of any non-zero polynomial into distinct monic irreducible polynomials unique up to the ordering of the factors.
- Let $T \in \text{End}(V)$ be arbitrary.

  Note that a *minimal polynomial* of T is a monic polynomial $p(t)$ of the least degree such that $p(T) = 0$.

  Cayley-Hamilton Theorem gives us an upper bound on the degree of a monic polynomial:

$$\deg p(t) \leq \dim V$$

1.2 Uniqueness of the Minimal Polynomial

Theorem 1.1

Assume $p(t)$ is a minimal polyonmial of T.

a) If $g(t) \in \mathcal{P}(\mathbb{F})$ is a ny polynomial such that $g(T) = 0$, then $p(t)|g(t)$

b) $p(t)$ is the unique minimal polynomial

Remark 1.2. Note that a) implies by Cayley-Hamilton Theorem that $p(t)|f(t)$, where $f(t)$ is a characteristic polynomial.

Proof.

Using the division algorithm, we know that $g(t) = q(t)p(t) + r(t)$, where $\deg(r) < \deg(p)$.

Plugging in T, we know that $g(T) = q(T)p(T) + r(T)$.

Since $g(T) = 0$ and $p(T)$, then $r(T) = 0$.

If $r(t) \neq 0$, it can be rescaled to be monic, but $\deg r < \deg p$, which contradicts that $p(t)$ is minimal, and hence we can deduce that $r(t) = 0$.

Therefore, $r(t) = 0$, so $p(t)|g(t)$.

Suppose now that $p'(t)$ is another minimal polynomial. Therefore, $\deg p'(t) = \deg p(t)$.

Moreover, $p(T) = p'(T) = 0$, and thus $p(T)|p'(T)$. But p and p' have the same degree, and thus $p'(t) = cp(t)$ for $c \in \mathbb{F} \setminus \{0\}$. Since p and p' are monic, then $c = 1$, and hence $p(t) = p'(t)$. ☐

Theorem 1.3

The characteristic polynomial $f(t)$ and the minimal polynomial $p(t)$ have the same zeroes ni $\mathbb{F}$.

Proof.

If a minimal polynomial $p(t)$ has a zero, since $p(t)|f(t)$, then $f(t)$ also has a zero.

Suppose now that λ is a zero of $f(t)$, so λ is an eigenvector of T.

Pick $x \neq 0$ such that $Tx = \lambda x$. Therefore, $p(T)x = 0$, since p is a minimal polynomial.

Since x is an eigenvector, we get that $p(\lambda)x = 0$, and since $x \neq 0$, then $p(\lambda) = 0$. □

Corollary 1.4

If the characteristic polynomial $f(t) = (-1)^n \prod_{i=1}^{n}(t-\lambda_i)^{n_i}$, where λ_i are the distinct eigenvalues, then the minimal polynomial is $p(t) = \prod_{i=1}^{n}(t-\lambda_i)^{d_i}$, where $1 \leq d_i \leq n_i$.

Proof.

Use $p(t)|f(t)$ by Theorem 1.3 and unique factorisation.

□

Example 1.5

Let A be equal to $\begin{pmatrix} 2 & 2 & 3 \\ 1 & 3 & 3 \\ -1 & -2 & -2 \end{pmatrix}$ over $\mathbb{F} = \mathbb{Q}$.

We have already seen that $f(t) = -(t-1)^3$.

Therefore, $p(t) = (t-1)^d$ for $1 \leq d \leq 3$.

The dot diagram is $\begin{pmatrix} \bullet & \bullet \\ \bullet & \end{pmatrix}$, which means that $A - I \neq 0$ and the nullity is 2.

Therefore, $(A-I)^2 = 0$.

Theorem 1.6

Suppose $\dim V = n$ and V is the T-cyclic subspace generated by $x \in V$. Then the minimal polynomial has a degree of n and $f(t) = (-1)^n p(t)$.

Proof.

We know that $\beta = \{x, Tx, \ldots, T^{n-1}x\}$ is a basis of V.

Suppose that $g(t)$ is a polynomial of degree less that n, so $g(t) = \sum_{i=0}^{n-1} a_i t^i$ for some $a_i \in \mathbb{F}$.

Then $g(T) = a_0 I + \sum_{i=1}^{n-1} a_i T^i$, and hence $g(T) = 0$, which means that $g(T)(x) = 0$, and thus $a_{n-1} = \cdots = a_0 = 0$, because β is a basis.

Therefore, the minimal polynomial has a degree of n. □

Theorem 1.7

T is diagonalisable if and only if them minimal polynomial of T is of the form $\prod_{i=1}^{s}(t-\lambda_i)$, where $\lambda_i \in \mathbb{F}$ are distinct.

e.g. $T = \lambda I$ if and only if the minimal polynomial is $(t-\lambda)$

Proof.

Suppose that $\lambda_1, \ldots, \lambda_s \in \mathbb{F}$ are distinct eigenvalues of T.

Therefore, $V = \bigoplus_{i=1}^s E_{\lambda_i}$.

By Theorem 1.3, $g(t) = \prod_{i=1}^s (t - \lambda_i) | p(t)$.

We need to show that $g(t)$ is indeed a minimal polynomial.

It is enough to show that $g(T)(x) = 0$ for all $x \in E_{\lambda_i}$ for all possible λ_i.

But $g(T)(x) = g(\lambda_i)(x)$, since x is an eigenvector. But $g(\lambda_i) = 0$, and therefore $g(T) = 0$.

Exercise: Prove the other direction. $\square$