14. The minimal polynomial

For an example of a matrix which cannot be diagonalised, consider the matrix

\[ A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \]

The characteristic polynomial is \( \lambda^2 = 0 \) so that the only eigenvalue is \( \lambda = 0 \). The corresponding eigenspace \( E_0(A) \) is spanned by \((1, 0)\). In particular \( E_0(A) \) is one dimensional. But if \( A \) were diagonalisable then it would have a basis of eigenvectors. So \( A \) cannot be diagonalisable. Thus at the very least we must allow an extra matrix

\[ A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}. \]

This behaves exactly the same as before, since when we subtract \( \lambda I_2 \), we are back to the case of

\[ A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \]

In fact

**Lemma 14.1.** Let \( A \in M_{n,n}(F) \) and let \( \lambda \in F \).

\( A \) is similar to \( B \) iff \( A - \lambda I_n \) is similar \( B - \lambda I_n \).

*Proof.* There are two ways to see this.

First we proceed directly. Suppose that \( A \) is similar to \( B \). Then we may find an invertible matrix \( P \in M_{n,n}(F) \) such that \( B = PAP^{-1} \). In this case

\[
P(A - \lambda I_n)P^{-1} = PAP^{-1} - \lambda PI_nP^{-1} = B - \lambda I_n.
\]

Thus \( A - \lambda I_n \) is similar to \( B - \lambda I_n \).

The converse is clear, since

\[ A = (A - \lambda I_n) - \mu I_n \quad \text{and} \quad B = (B - \lambda I_n) - \mu I_n, \]

where \( \mu = -\lambda \). So much for the direct approach.

The other way to proceed is as follows. \( A \) and \( B \) correspond to the same linear function \( \phi: V \to V \), where \( V = F^n \). To get \( A \) we might as well suppose that we take \( f \) to be the identity map. To get \( B \) we take \( f' \) corresponding to the matrix \( P \) such that \( A = PBP^{-1} \). But then \( A - \lambda I_n \) and \( B - \lambda I_n \) correspond to the same linear function \( \phi - \lambda \), where \( I: V \to V \) is the identity function. \( \square \)
What are the possibilities for $n \geq 3$? Again we know that we must have repeated eigenvalues (in some sense). By (14.1) we know that we might as well suppose we have eigenvalue $\lambda = 0$. Here then are some possibilities:

$$A_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$  

It is interesting to consider the eigenspaces in all three cases. In the first case every vector is an eigenvector with eigenvalue 0, $E_0(A_0) = F^3$. In the second case the kernel is $z = 0$ so that $(1, 0, 0)$ and $(0, 1, 0)$ span $E_0(A_1)$. In the third case the kernel is $y = z = 0$, so that $E_0(A_2)$ is spanned by $(1, 0, 0)$. But we already know that similar matrices have eigenspaces of the same dimension. So $A_0$, $A_1$ and $A_2$ are inequivalent matrices.

In fact there is another way to see that these matrices are not similar.

**Definition 14.2.** Let $\phi : V \rightarrow V$ be a linear transformation. We say that $\phi$ is **nilpotent** if $\phi^k = 0$ for some positive integer $k$. The smallest such integer is called the **order** of $\phi$.

We say that a matrix is **nilpotent** if the corresponding linear function is nilpotent.

Almost by definition, if $A$ and $B$ are similar matrices then $A$ is nilpotent if and only if $B$ is nilpotent and the order is then the same. $A_0 = 0$, $A_1^2 = 0$ and $A_2^3 = 0$. In fact $A_2^2 \neq 0$. So $A_0$, $A_1$ and $A_2$ are not similar matrices, since they have different orders (of nilpotency).

In general then we should look at

$$(A - \lambda I)^k.$$  

Or what comes to the same thing

$$(\phi - \lambda I)^k.$$  

This in fact suggests that we should consider polynomials in $A$ (or $\phi$). Given a polynomial $m(x) \in P(F)$, we first note that it makes sense to consider $m(\phi)$. We can always compute powers of $\phi$, we can always multiply by a scalar and we can always add linear functions (or matrices). For example, if

$$m(x) = 3x^3 - 5x + 7 \quad \text{then} \quad 3\phi^3 - 5\phi + 7,$$

is a linear function. To see that there is something non-trivial going on here, note that by contrast it makes no sense to think about polynomials in two linear transformations. The problem is that $\phi \circ \psi \neq \psi \circ \phi$ and
yet the variables $x$ and $y$ are supposed to commute for any polynomial in these variables.

**Definition-Lemma 14.3.** Let $V$ and $W$ be vector spaces over the same field $F$. $\text{Hom}(V,W)$ denotes the set of all linear transformations $\phi: V \to W$. $\text{Hom}(V,W)$ is a vector space over $F$, with the natural rules for addition and scalar multiplication. If $V$ and $W$ are finite dimensional then so is $\text{Hom}(V,W)$ and

$$\dim \text{Hom}(V,W) = \dim V \dim W.$$  

**Proof.** In fact the set of all functions $W^V$ is a vector space with addition and scalar multiplication defined pointwise. Since the subset of linear transformations is closed under addition and scalar multiplication, $\text{Hom}(V,W)$ is a linear subspace of $W^V$. In particular it is a vector space.

Now suppose that $V$ and $W$ are finite dimensional. Pick isomorphisms $f: V \to F^n$ and $g: W \to F^m$. This induces a natural map

$$\Phi: \text{Hom}(V,W) \to \text{Hom}(F^n,F^m).$$

Given $\phi$ we send this to $\Phi(\phi) = g \circ \phi \circ f^{-1}$. Suppose that $\phi_1$ and $\phi_2 \in \text{Hom}(V,W)$. Pick $v \in V$. Then

$$\Phi(\phi_1 + \phi_2)(v) = g \circ (\phi_1 + \phi_2) \circ f^{-1}(v)$$
$$= g((\phi_1 + \phi_2)(f^{-1}(v)))$$
$$= g(\phi_1(f^{-1}(v))) + g(\phi_2(f^{-1}(v)))$$
$$= (g \circ \phi_1 \circ f^{-1})(v) + (g \circ \phi_2 \circ f^{-1})(v)$$
$$= \Phi(\phi_1)(v) + \Phi(\phi_2)(v).$$

But then $\Phi(\phi_1 + \phi_2) = \Phi(\phi_1) + \Phi(\phi_2)$. Therefore $\Phi$ respects addition. Similarly $\Phi$ respects scalar multiplication. It follows that $\Phi$ is linear. It is easy to see that $\Phi$ is a bijection. Thus $\Phi$ is a linear isomorphism.

Thus we might as well assume that $V = F^n$ and $W = F^m$. Now define a map

$$\Psi: \text{Hom}(F^n,F^m) \to M_{m,n}(F),$$

by sending a linear map $\phi$ to the associated matrix $A$. It is again straightforward to check that $\Psi$ is linear. We already know $\Psi$ is bijective. Hence $\Psi$ is a linear isomorphism. So the vector space $\text{Hom}(V,W)$ is isomorphic to $M_{m,n}(F)$. But the latter has dimension $mn = \dim W \dim V$. \qed
Proposition 14.4. Let $V$ be a finite dimensional vector space over a field and let $\phi : V \rightarrow V$ be a linear function.

Then there is a polynomial $m(x) \in P(F)$ such that $m(\phi) = 0$.

Proof. Consider the linear transformations

$$1, \phi, \phi^2, \ldots$$

Since this is an infinite set of vectors in the finite dimensional vector space $\text{Hom}(V, V)$ it follows that there are scalars $a_0, a_1, a_2, \ldots, a_d$, not all zero, such that

$$a_0 + a_1 \phi + a_2 \phi^2 + \cdots + a_d \phi^d = 0.$$ 

Let

$$m(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \in P(F).$$

Then $m(\phi) = 0$ by construction. \hfill \Box

Definition 14.5. Let $\phi : V \rightarrow V$ be a linear transformation, where $V$ is a finite dimensional vector space. The minimal polynomial of $\phi$ is the smallest degree monic polynomial $m(x)$ such that

$$m(\phi) = 0.$$ 

Clearly the minimal polynomials of $A_0, A_1$ and $A_2$ above, are $x$, $x^2$ and $x^3$. In what follows we will adopt the convention that the degree of the zero polynomial is undefined.

Lemma 14.6 (Division Algorithm). Let $F$ be a field. Let $a(x)$ and $b(x) \in P(F)$. Suppose $a(x) \neq 0$.

Then we may find $q(x)$ and $r(x) \in P(F)$ such that

$$b(x) = q(x)a(x) + r(x),$$

where either $r(x) = 0$ or $\deg r(x) < \deg a(x)$.

Proof. By induction on the degree of $b(x)$. If either $b(x) = 0$ or $\deg b(x) < \deg a(x)$ then take $q(x) = 0$ and $r(x) = b(x)$.

Otherwise we may assume that $\deg b(x) \geq \deg a(x)$ and that the result holds for any polynomial $c(x)$ of smaller degree than $b(x)$. Suppose that

$$a(x) = \alpha x^d + \ldots \quad \text{and} \quad b(x) = \beta x^e + \ldots,$$

where dots indicate lower degree terms. By assumption $d \leq e$. Let

$$c(x) = b(x) - (\gamma x^f)a(x),$$

where $\gamma = \frac{a}{e}$ and $f = e - d \geq 0$. Then either $c(x) = 0$ or $c(x)$ has smaller degree than the degree of $b(x)$. By induction there are polynomials $q_1(x)$ and $r(x)$ such that

$$c(x) = q_1(x)a(x) + r(x),$$
where either \( r(x) = 0 \) or \( \deg r(x) < d \). Then

\[
\begin{align*}
b(x) &= c(x) + \gamma x^f a(x) \\
b(x) &= q_1(x)a(x) + r(x) + \gamma x^f a(x) \\
&= (q_1(x) + \gamma x^f) a(x) + r(x).
\end{align*}
\]

So if we take \( q(x) = q_1(x) + \gamma x^f \) then we are done by induction. \( \square \)

**Theorem 14.7.** Let \( \phi : V \to V \) be a linear function, where \( V \) is a finite dimensional vector space.

The minimal polynomial \( m(x) \) of \( \phi \) is the unique monic polynomial such that

- \( m(\phi) = 0 \) and,
- if \( n(x) \) is any other polynomial such that \( n(\phi) = 0 \) then \( m(x) \) divides \( n(x) \).

**Proof.** Suppose that \( m(x) \) is the minimal polynomial. Then \( m(x) \) is monic and \( m(\phi) = 0 \). Suppose that \( n(x) \) is another polynomial such that \( n(\phi) = 0 \). By (14.6) we may find \( q(x) \) and \( r(x) \) such that

\[
n(x) = q(x)m(x) + r(x),
\]

where \( \deg r(x) < \deg m(x) \) (or \( r(x) = 0 \)). Now

\[
n(\phi) = q(\phi)m(\phi) + r(\phi).
\]

By assumption \( n(\phi) = m(\phi) = 0 \). But then \( r(\phi) = 0 \). By minimality of the degree of \( m(x) \) the only possibility is that \( r(x) = 0 \), the zero polynomial. But then \( m(x) \) divides \( n(x) \).

Now suppose that \( n(x) \) is monic, \( n(\phi) = 0 \) and \( n(x) \) divides any polynomial which vanishes when evaluated at \( \phi \). Let \( m(x) \) be the minimal polynomial. As \( m(\phi) = 0 \), \( n(x) \) divides \( m(x) \). But then the degree of \( n(x) \) is at most the degree of \( m(x) \). By minimality of the degree of the monic polynomial, \( n(x) \) and \( m(x) \) have the same degree. As both are monic, it follows that \( n(x) = m(x) \). \( \square \)

**Example 14.8.** Consider the matrices \( A_0, A_1 \) and \( A_2 \) above. Now \( n_i(x) = x^{i+1} \) is a polynomial such that \( n_i(A_i) = 0 \). So the minimal polynomial \( m_i(x) \) must divide \( x^{i+1} \) in each case. From this it is easy to see that the minimal polynomials are in fact \( n_i(x) \), so that \( m_0(x) = x \), \( m_1(x) = x^2 \) and \( m_2(x) = x^3 \).

For a more involved example consider the matrix \( B = B_k(\lambda) \in M_{k,k}(F) \), where \( \lambda \) is a scalar and we have a trailing sequence of 1’s on the main diagonal. First consider

\[
N = B_k(0) = B_k(\lambda) - \lambda I_k = B - \lambda I_k.
\]
This matrix is nilpotent. In fact $N^k = 0$, but $N^{k-1} \neq 0$. So if we set $n(x) = (x - \lambda)^k$ then $n(B) = 0$. Once again, the minimal polynomial $m(x)$ of $B$ must divide $n(x)$. So $m(x) = (x - \lambda)^i$, some $i \leq k$. But since $N^{k-1} \neq 0$, in fact $i = k$, and the minimal polynomial of $B$ is precisely $m(x) = (x - \lambda)^k$. 