Lecture VIII: Diagonalization and Canonical Forms of Matrices and Linear Transformations in General

If $T: V \to V$ is a linear transformation of a finite-dimensional vector space*, then it may not be possible to find a basis, orthonormal or not, $v_1, \ldots, v_n$ such that T is "diagonal" relative to $v_1, \ldots, v_n$, i.e., such that for some numbers $\lambda_1, \ldots, \lambda_n$ (not necessarily all distinct from each other) $Tv_i = \lambda_i v_i$, $i = 1, \ldots, n$.

Consider for example the transformation T from $\mathbb{R}^2$ to $\mathbb{R}^2$ with matrix $\begin{pmatrix} \lambda_0 & 1 \\ 0 & \lambda_0 \end{pmatrix}$, $\lambda \in \mathbb{R}$. The kernel $\ker(T - \lambda I)$ is larger than $\{\vec{0}\}$, positive dimensional, if and only if $\lambda = \lambda_0$ since $\det \begin{pmatrix} \lambda_0 - \lambda & 1 \\ 0 & \lambda_0 - \lambda \end{pmatrix} = (\lambda - \lambda_0)^2$

which is 0 only if $\lambda = \lambda_0$. But if there were a basis v_1, v_2 with $Tv_1 = \lambda_0 v_1$ and $Tv_2 = \lambda_0 v_2$, then T would equal $\lambda_0 I$, which is clearly not the case. Note that passing to the complex numbers and considering $T^{\mathbb{C}}: \mathbb{C}^2 \to \mathbb{C}^2$ would not in any sense improve this situation! The difficulty lies not in that $\det(T - \lambda I) = 0$ has complex roots that are not real — it does not. The difficulty is that $\det(T - \lambda I) = 0$ has a multiple root! This lecture is about how to deal with this situation — to the extent that one can

*over a field F: F need not be $\mathbb{R}$ or $\mathbb{C}$ in most of what follows.

It turns out that the most effective way to look at this is to move into a somewhat more algebraic setting than we have encountered so far. No really heavy-duty algebra is involved, but a little more algebraic generality will make life simpler. In particular, given $T: V \to V$ (or $A: \mathbb{R}^n \to \mathbb{R}^n$, a matrix-generated transformation, A an $n \times n$ matrix), we want to consider polynomials (with $\mathbb{R}$-coefficients) in T as a variable. For this, we define T^2 to be the linear transformation $v \to T(T(v))$ $v \in V$, T^3 to be $v \to T(T(T(v)))$ and so on: powers are to be interpreted as compositions. Since such "powers" of T commute and behave "normally" so that $T^{n+m} = T^n(T^m(\cdot))$, we can think of polynomials in T as a commutative ring with these operations. However, it may be that elements of this ring which are formally nonzero are $= 0$ as linear transformations. For example if T is the linear transformation $\mathbb{R}^2$ to $\mathbb{R}^2$ with matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then $(T-I)^2 = T^2 - 2T + I$ is actually 0:

$T^2((1,0)) = (1,0)$ $T((0,1)) = (1,1)$ so $T^2((0,1)) = T((1,1)) = (1,0) + (1,1) = (2,1)$. Hence

$(T^2 - 2T + I)(1,0) = (1,0) - 2(1,0) + (1,0) = (0,0)$

while

$(T^2 - 2T + I)(0,1) = (2,1) - 2(1,1) + (0,1) = (0,0)$

Note that "powers" of T in the composition sense correspond to powers in the matrix multiplication

with the constant term of a polynomial being interpreted as the constant times the identity, i.e. $c \leftrightarrow cI$.

sense of the matrix A of T: thus, we get, for a fixed A, a commutative subring of the noncommutative ring of nxn matrices.

Actually, it always happens that there is some nonzero polynomial which becomes the zero linear transformation when T is substituted into it for the variable. 8.3

Lemma: If $T: V \to V$ is a linear transformation then there is a polynomial P, not (identically) zero, such that $P(T): V \to V$ is the 0 linear transformation [V is finite-dimensional here! This is required!]

Proof: Choose a basis $v_1, \ldots, v_n$. It suffices to find for each $i = 1, \ldots, n$, a polynomial P_i, not (identically) zero with $P_i(T)(v_i) = 0$, since then we can take $P = P_1 \times \ldots \times P_n$ for the P of the Lemma. Fix an i. Then consider the vectors v_i, $T(v_i)$, $T(T(v_i))$ etc. or v_i, Av_i, $A^2 v_i$, $A^3 v_i \ldots$ in "matrix notation". This set must contain a dependent subset. Indeed, the set $v_i, Av_i, A^2 v_i \ldots A^{n-1} v_i, A^n v_i$ must be dependent since contains n+1 vectors (and n = dimension of V). A dependence relation $\sum_{j=0}^{n} \beta_j A^j v_i = 0$, not all β's $= 0$ gives a polynomial $\sum_{j=0}^{n} \beta_j A^j$ of degree at most n, call it $P_i(A)$, such that $P_i(A) v_i = 0$, as desired. □

We shall see later that there is a single polynomial $P(\cdot)$ of degree $\leq n$ such that $P(A)$ is in fact the 0 linear transformation of V to V. For the moment, we have shown only that there is a polynomial $P_1 \cdot \ldots \cdot P_r$ of degree $\leq n^2$ with this property.

The algebra of polynomials in one variable comes into the picture strongly in the following important lemma.

Composition Lemma: If P_1 and P_2 are polynomials over a field F in one variable which are relatively prime in the ring of polynomials over F (i.e. greatest common divisor of P_1 and $P_2 = 1$) and if $T : V \to V$ is a linear transformation from a vector space V over F to itself

Then

(1) $\ker P_1(T) \cap \ker P_2(T) = \{\vec{0}\}$

and

(2) if $P_1(T) \times P_2(T) = 0$, then

$$V = \ker P_1(T) \oplus \ker P_2(T)$$

[Here we say as usual that a vector space $V = W_1 \oplus W_2$, W_1, W_2 subspaces if every element v is uniquely expressible as $v = w_1 + w_2$, $w_1 \in W_1$, $w_2 \in W_2$.]

Proof: Since P_1 and P_2 are relative prime, $\exists$ Q_1 and Q_2 polynomials such that (in the ring of polynomials over F)

$$Q_1 P_1 + Q_2 P_2 = 1$$

This is a familar consequence of the euclidean algorithm for polynomials over a field.
This gives that for each $v \in \ker P_1(T)$

$$\begin{aligned} v &= Q_1(T) P_1(T) v + Q_2(T) P_2(T) v \\ &= Q_1(T)(\vec{0}) + Q_2(T) P_2(T) v \\ &= Q_2(T)(P_2(T) v). \end{aligned}$$

So $v \in \ker P_2(T)$ also would imply $v = \vec{0}$.
Thus $\ker P_1 \cap \ker P_2 = \{\vec{0}\}$. This proves (1).

For (2), note that for all $v \in V$:
$Q_1(T)P_1(T)v \in \ker P_2(T)$ since $P_2(T)\, Q_1(T) P_1(T) v = Q_1(T)(P_1(T) P_2(T) v) = Q_1(T)(\vec{0}) = \vec{0}$.
Similarly $Q_2(T) P_2(T) v \in \ker P_1$ for all $v \in V$. Thus for all $v \in V$

$$v = \underbrace{Q_2(T) P_2(T) v}_{\in \ker P_1(T)} + \underbrace{Q_1(T) P_1(T) v}_{\in \ker P_2(T)}.$$

Uniqueness of the decomposition follows from $\ker P_1(T) \cap \ker P_2(T) = \{\vec{0}\}$. Thus

$$V = \ker P_1(T) \oplus \ker P_2(T) \text{ as desired.}$$

□

Now fix $T: V \to V$ and consider all the one-variable polynomials $P \not\equiv 0$ such that $P(T): V \to V$ is the 0 linear transformation. Among these, there is one P_0 of minimal degree (this degree is necessarily positive of course, since $cI: V \to V$ is not zero if $c \neq 0$). Note that if $Q(T)$ is a (nonzero) polynomial with $Q(T) = 0$ on V, then P_0 divides Q as a polynomial over F: the reason is that the one-variable polynomials, call it R that is the remainder when Q is divided by P_0.

Then $R = P_1 P_0 + Q_1 Q$ (Euclidean algorithm again). Now $\deg R < \deg P_0$. But clearly $Q(T) = 0$ and $P_0(T) = 0$ together imply $R(T) = 0$. Since $\deg P_0$ is minimal among nonzero polynomials P such that $P(T) = 0$, it must be that $R = 0$ as a polynomial so that P_0 divides Q.

Thus:

Lemma: The minimal degree polynomial P_0 [minimal degree nonzero polynomial P with $P(T) = 0$] is unique up to a nonzero constant factor (in F).

Definition: The minimal polynomial of T is the unique monic (first coefficient $= 1$) polynomial among the minimal-degree $P_0 \not\equiv 0$ with $P_0(T) = 0$.

The minimal polynomial can have degree $< \dim V$.

Examples: (1) The minimal polynomial of I is $P_0(t) = t - 1$.

(2) The minimal polynomial of $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

(T = corresponding transformation of $\mathbb{R}^3 \to \mathbb{R}^3$) is $P(t) = (t-1)^2$ (check this! (see below, example 3))

Note that the minimal polynomial need not be irreducible!

(3) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ has minimal polynomial $(t-1)^3$.

[How to check this: The polynomial $P(t) = (t-1)^3$ has the property $P(A) = 0$: checking directly is easy. So if $P_0(t)$ is the minimal polynomial for A, then P_0 divides $(t-1)^3$. So $P(t)$ is $t-1$ or $(t-1)^2$ or $(t-1)^3$. But the first two of these do not work: $A - I$ and $(A-I)^2$ do not vanish on $(0,0,1)$.]

Similarly, the minimal polynomial of

$n \times n$ $\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & & 0 \\ 0 & 0 & \lambda & \ddots & \vdots \\ \vdots & \vdots & 0 & \ddots & 1 \\ 0 & \vdots & 0 & \cdots & \lambda \end{pmatrix}$ is $P(t) = (t-\lambda)^n$.

This example is important! Think it through

Now let us consider the situation where F is algebraically closed, i.e., every polynomial of degree k over F has k roots in F, counting multiplicities. ($F = \mathbb{C}$ is the example we are most interested in).

If $T: V \to V$ over F is a linear transformation of a finite-dimensional vector space and if P_0 is the minimal polynomial of T, then $P_0(t)$ can be expressed as

$$P_0(t) = (t-\lambda_1)^{k_1} \cdots (t-\lambda_\ell)^{k_\ell}$$

k_i's > 0 and the λ_i's distinct.

Indeed, this expression is unique up to order of the $(t-\lambda_i)^{k_i}$ factors: this is just the usual factoring of monic polynomials over an algebraically closed field.

Note that Σk_i may be $<$ dim V: see example 2 on the previous page!

Now repeated application of the Decomposition Lemma given earlier shows that in this situation

$$V = W_1 \oplus \cdots \oplus W_\ell$$

where $W_i =$

$$\ker (T - \lambda_i)^{k_i}.$$

Thus we can understand the "structure" of T if we understand the possibilities for how T behaves on each W_i: Note that the W_i are "T-invariant" here: $T(W_i) \subset W_i$

because if $w \in W_i$, then Tw satisfies

$$(T - \lambda_i I)^{k_i}(Tw) = T(T - \lambda_i I)^k w = \vec{0}.$$

So T acting on $W_1 \oplus \dots \oplus W_\ell$

is in an obvious since the direct sum $T_1 \oplus \dots \oplus T_\ell$ where $T_i : W_i \to W_i$. $(T_1 \oplus \dots \oplus T_\ell)(w_1 + \dots + w_\ell)$ being $\sum T_i w_i$.
Also the minimal polynomial of $T_i = T|W_i$ is exactly $(t - \lambda_i)^{k_i}$.

So our program of understanding T, which amounts to trying to find a basis of V relative to which T looks comprehensible, is reduced to the following problem:

Try to understand linear transformations $T : V \to V$, V finite dimensional, such that the minimal polynomial of T acting on V has the form $P_0(t) = (t - \lambda)^k$ for some $\lambda \in F$ and positive integer k.

This problem turns out to be solvable.

Now we have seen examples a few pages back of transformations (in the form of matrices) that have minimal polynomial $(t - \lambda)^k$ given λ, k.

They were $k \times k$ matrices of the form

Usual terminology called "Jordan block" →

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & & \\ & & \ddots & \\ & & & 1 \\ 0 & & & \lambda \end{pmatrix} \quad k \times k \text{ matrix.}$$

Of course if $k \geq 2$, then there are matrices of similar form but $k_1 \times k_1$, $k_1 < k$: These have minimal polynomial $(t-\lambda)^{k_1}$. We can thus generate matrices with minimal polynomial $(t-\lambda)^k$ by stringing together $k \times k$ Jordan blocks (λ as given) together with some other Jordan blocks, same λ, but smaller size $k_1 < k$ (when $k \geq 2$). There can be lots of blocks! V can have arbitrarily large dimension. But there has to be one $k \times k$ block and all blocks have to be no bigger than k. (All blocks have same λ).

Perhaps surprisingly, these are the only possibilities:

Theorem: If $T: V \to V$ is a linear (Jordan) transformation of a finite-dimensional vector space over an algebraically closed field F and if the minimal polynomial of V has the form $(t-\lambda)^k$, $\lambda \in F$, k a positive integer, then there

is a basis for V relative to which the matrix of T is a (diagonal) union of Jordan blocks of size $\leq k$ and with at least one block of size $= k$.

This, together with the decomposition into T-invariant subspaces with minimal polynomials $(t-\lambda)^k$ some k, λ already established is called the Jordan canonical form: every linear transformation is "equivalent" (= looks like in some basis) a union of diagonal Jordan blocks.

Before beginning the proof of Jordan canonical form, it is useful to think about how Jordan blocks arise. This will be the starting point of the next lecture.