Lecture 6. Diagonalization of Matrices
October 2022

DEFINITION 6.1 We say that a polynomial

$$P_n(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad n > 0,\ a_n \neq 0$$

with $a_i \in \mathbb{R}$, $i = 0, \ldots, n$, **factors completely** over $\mathbb{R}$ if it can be represented as

$$P_n(x) = a_n(x - x_1)(x - x_2)\ldots(x - x_n),$$

where the x_i are real numbers (not necessarily distinct).

EXAMPLE 6.2 Consider two matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Show that $p_B(\lambda)$ factors completely over $\mathbb{R}$, but $p_A(\lambda)$ does not.

THEOREM 6.3 (Diagonalization Theorem) The following are equivalent for a square matrix A for which $p_A(\lambda)$ factors completely.

1. A is diagonalizable.
2. $\gamma(\lambda_i) = \mu(\lambda_i)$ for every eigenvalue λ_i of the matrix A.

Proof. Let A be $n \times n$ and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the distinct eigenvalues of A. For each i, let m_i and d_i denote the algebraic and geometric multiplicities of λ_i, respectively. Then

$$p_A(\lambda) = (-1)^n(\lambda - \lambda_1)^{m_1}(\lambda - \lambda_2)^{m_2}\ldots(\lambda - \lambda_k)^{m_k}$$

so $m_1 + \cdots + m_k = n$ because $p_A(\lambda)$ has degree n. Moreover, $d_i \leqslant m_i$ for each i by Lemma 5.17.

(1) $\Longrightarrow$ (2). By (1), V has a basis of n eigenvectors of f, so let t_i of them lie in E_{λ_i} for each i. Since the subspace spanned by these t_i eigenvectors has dimension t_i, we have $t_i \leqslant d_i$ for each i by Fundamental Theorem. Hence

$$n = t_1 + \cdots + t_k \leqslant d_1 + \cdots + d_k \leqslant m_1 + \cdots + m_k = n.$$

It follows that $d_1 + \cdots + d_k = m_1 + \cdots + m_k$ so, since $d_i \leqslant m_i$ for each i, we must have $d_i = m_i$. This is (2).

(2) $\Longrightarrow$ (1). Let B_i denote a basis of E_{λ_i} for each i, and let $B = B_1 \cup \cdots \cup B_k$. Since each B_i contains m_i vectors by (2), and since the B_i are pairwise disjoint (the λ_i are distinct), it follows that B contains n vectors. So it suffices to show that B is linearly independent (then B is a basis of $\mathbb{R}^n$). Suppose a linear combination of the vectors in B vanishes, and let $\mathbf{y}_i$ denote the sum of all terms that come from B_i. Then $\mathbf{y}_i$ lies in E_{λ_i} for each i, so the nonzero $\mathbf{y}_i$ are independent by Theorem 5.11 (as the λ_i are distinct). Since the sum of the $\mathbf{y}_i$ is zero, it follows that $\mathbf{y}_i = \mathbf{0}$ for each i. Hence all coefficients of terms in $\mathbf{y}_i$ are zero (because B_i is independent). Since this holds for each i, it shows that B is independent. $\square$

Complex Vector Spaces

Nearly everything in this course would remain true if the phrase **real number** were replaced by **complex number** wherever it occurs. Then we would deal with matrices with complex entries, systems of linear equations with complex coefficients (and complex solutions), determinants of complex matrices, and vector spaces with scalar multiplication by any complex number allowed. The methods are the same; the only difference is that the arithmetic is carried out with complex numbers rather than real ones. For example, the gaussian algorithm works in exactly the same way to solve systems of linear equations with complex coefficients, matrix multiplication is defined the same way, and the matrix inversion algorithm works in the same way. Moreover, the proofs of most theorems about (the real version of) these concepts extend easily to the complex case.

Let A be an $n \times n$ complex matrix. As in the real case, a complex number λ is called an **eigenvalue** of A if $A\mathbf{x} = \lambda\mathbf{x}$ holds for some column $\mathbf{x} \neq \mathbf{0}$ in $\mathbb{C}^n$. In this case $\mathbf{x}$ is called an **eigenvector** of A corresponding to λ. The **characteristic polynomial** $p_A(\lambda)$ is defined by

$$p_A(\lambda) = \det(A - \lambda I).$$

This polynomial has complex coefficients (possibly nonreal). The eigenvalues of A are the roots (possibly complex) of $p_A(\lambda)$.

However the complex numbers are better than the real numbers in one respect. The real numbers are incomplete in the sense that the characteristic polynomial of a real matrix may fail to have all its roots real. However, this difficulty does not occur for the complex numbers. The so-called **Fundamental Theorem of Algebra** ensures that every polynomial of positive degree with complex coefficients has a complex root, and hence factors completely as a product of linear factors. Hence every square complex matrix A has n (complex) eigenvalues: $\lambda_1, \lambda_2, \ldots, \lambda_n$ with possible repetitions due to multiple roots.

EXAMPLE 6.4 The matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is diagonalizable in complex numbers.

Recall that a matrix is called **upper triangular** if every entry below the main diagonal is zero.

LEMMA 6.5 Suppose V is a finite-dimensional complex vector space and $f : V \to V$ is a linear operator. Then f has an upper-triangular matrix with respect to some basis of V.

Proof. We use induction on the dimension of V. Clearly the desired result holds if $\dim V = 1$.

Suppose now that $\dim V = n > 1$ and the statement holds for all complex vector spaces whose dimension is less than n. Let λ be an eigenvalue of f, and let $\mathbf{x}$ be an associated eigenvector. Let $U = \operatorname{Im}(f - \lambda 1_V)$. Because $f - \lambda 1_V$ is not surjective, $\dim U < \dim V$. By Theorem 5.9, U is invariant under f.

Thus $f|_U$ is an operator on U. By induction hypothesis, there is a basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$

of U with respect to which $f|_U$ has an upper-triangular matrix. Thus for each j we have

$$f(\mathbf{u}_j) = f|_U(\mathbf{u}_j) \in \operatorname{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_j\}.$$

Extend $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ to a basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{v}_1, \ldots, \mathbf{v}_r\}$ of V. For each k, $1 \leqslant k \leqslant m$, we have

$$f(\mathbf{v}_k) = (f(\mathbf{v}_k) - \lambda\mathbf{v}_k) + \lambda\mathbf{v}_k.$$

From the definition of U it follows that $(f - \lambda 1_V)\mathbf{v}_k \in U = \operatorname{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$. Thus the equation above shows that

$$f(\mathbf{v}_k) \in \operatorname{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{v}_1, \ldots, \mathbf{v}_k\}.$$

Therefore, we can conclude that f has an upper triangular matrix with respect to the basis $\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{v}_1, \ldots, \mathbf{v}_r\}$ of V, as desired. □

Now we will prove a famous Cayley–Hamilton theorem about matrices.

THEOREM 6.6 (Cayley–Hamilton Theorem) Every square matrix A satisfies its own characteristic equation, i.e. $p(A) = 0$.

Proof Any square matrix A induces a linear operator $f : V \to V$ of a finite-dimensional complex vector space V. Then by Lemma 6.5, there is a basis of V with respect to which the matrix B of V is upper triangular. The matrices A and B are similar, $A = P^{-1}BP$ for some invertible complex matrix P, and $p(A) = P^{-1}p(B)P$. Since B is upper triangular, the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ of f appear along the main diagonal, so

$$p(\lambda) = (-1)^n(\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3)\ldots(\lambda - \lambda_n).$$

Thus

$$p(B) = (-1)^n(B - \lambda_1 I)(B - \lambda_2 I)(B - \lambda_3 I)\ldots(B - \lambda_n I).$$

Note that each matrix $B - \lambda_i I$ is upper triangular. Now observe:

1. $B - \lambda_1 I$ has zero first column because column 1 of B is $(\lambda_1, 0, 0, \ldots, 0)^T$.
2. Then $(B - \lambda_1 I)(B - \lambda_2 I)$ has the first two columns zero because column 2 of $(B - \lambda_2 I)$ is $(b, 0, 0, \ldots, 0)^T$ for some constant b.
3. Next $(B - \lambda_1 I)(B - \lambda_2 I)(B - \lambda_3 I)$ has the first three columns zero because column 3 of $(B - \lambda_3 I)$ is $(c, d, 0, \ldots, 0)^T$ for some constants c and d.

Continuing in this way we see that $(B - \lambda_1 I)(B - \lambda_2 I)(B - \lambda_3 I)\ldots(B - \lambda_n I)$ has all n columns zero; that is, $p(B) = 0$, so $p(A) = 0$. □

EXAMPLE 6.7 For a generic 2×2 matrix, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ the characteristic polynomial is given by $p(\lambda) = \lambda^2 - (a + d)\lambda + (ad - bc)$, so the Cayley–Hamilton theorem states that

$$p(A) = A^2 - (a + d)A + (ad - bc)I_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$