# THE MINIMAL POLYNOMIAL AND SOME APPLICATIONS

KEITH CONRAD

## 1. Introduction

The easiest matrices to compute with are the diagonal ones. The sum and product of diagonal matrices can be computed componentwise along the main diagonal, and taking powers of a diagonal matrix is simple too. All the complications of matrix operations are gone when working only with diagonal matrices. If a matrix $A$ is not diagonal but can be conjugated to a diagonal matrix, say $D := PAP^{-1}$ is diagonal, then $A = P^{-1}DP$ so $A^k = P^{-1}D^kP$ for all integers $k$, which reduces us to computations with a diagonal matrix. In many applications of linear algebra (*e.g.*, dynamical systems, differential equations, Markov chains, recursive sequences) powers of a matrix are crucial to understanding the situation, so the relevance of knowing when we can conjugate a nondiagonal matrix into a diagonal matrix is clear.

We want look at the coordinate-free formulation of the idea of a diagonal matrix, which will be called a diagonalizable operator. There is a special polynomial, the minimal polynomial (generally not equal to the characteristic polynomial), which will tell us exactly when a linear operator is diagonalizable. The minimal polynomial will also give us information about nilpotent operators (those having a power equal to $O$).

*All linear operators under discussion are understood to be acting on nonzero finite-dimensional vector spaces over a given field $F$.*

## 2. Diagonalizable Operators

**Definition 2.1.** We say the linear operator $A\colon V \to V$ is *diagonalizable* when it admits a diagonal matrix representation with respect to some basis of $V$: there is a basis $\mathcal{B}$ of $V$ such that the matrix $[A]_{\mathcal{B}}$ is diagonal.

Let's translate diagoinalizability into the language of eigenvectors rather than matrices.

**Theorem 2.2.** *The linear operator $A\colon V \to V$ is diagonalizable if and only if there is a basis of eigenvectors for $A$ in $V$.*

*Proof.* Suppose there is a basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of $V$ in which $[A]_{\mathcal{B}}$ is diagonal:

$$[A]_{\mathcal{B}} = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & a_n \end{pmatrix}.$$

Then $Ae_i = a_ie_i$ for all $i$, so each $e_i$ is an eigenvector for $A$. Conversely, if $V$ has a basis $\{v_1, \ldots, v_n\}$ of eigenvectors of $A$, with $Av_i = \lambda_iv_i$ for $\lambda_i \in F$, then in this basis the matrix representation of $A$ is $\text{diag}(\lambda_1, \ldots, \lambda_n)$. $\square$

A basis of eigenvectors for an operator is called an *eigenbasis*.

An example of a linear operator that is *not* diagonalizable over any field $F$ is $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ acting on $F^2$. Its only eigenvectors are the vectors $\left(\begin{smallmatrix} x \\ 0 \end{smallmatrix}\right)$. There are not enough eigenvectors to form a basis for $F^2$, so $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ on $F^2$ does not diagonalize. Remember this example! Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$