

10.5 Cyclic Subspaces and Companion Matrices

The Jordan form of Section 3 exists only when the characteristic polynomial splits, because its building block $\mathbf{J}_k(\lambda)$ needs an eigenvalue λ in F . To build a normal form over **every** field we need a block that does not name a scalar. Look again at what a Jordan block really is: reading its columns, $\mathbf{J}_k(\lambda)$ is the matrix of T on the span of $u, Tu, \dots, T^{k-1}u$ for the top u of a chain. That description — *one vector and everything T can make of it* — mentions no eigenvalue at all. This section studies those subspaces, computes their dimension and their matrix, and decides when a single vector generates the whole space.

10.5.1 The subspace generated by one vector

Chapter 9 called a subspace U **invariant** when $Tu \in U$ for every $u \in U$ (Definition 9.1.1). Given one vector v , what is the smallest invariant subspace containing it? It must contain v , hence Tv , hence T^2v , and so on, hence every linear combination of these. That list is already closed under T , so nothing more is forced. So the answer is a span, and it deserves a name.

The cyclic subspace generated by a vector is everything that can be reached from it by applying the operator and taking combinations.

Definition 10.5.1. Cyclic Subspace

Let V be a vector space over F , let $T \in \mathcal{L}(V)$, and let $v \in V$. The **cyclic subspace generated by v** is

$$Z(v; T) := \text{span}(v, Tv, T^2v, \dots) = \text{span}(\{T^j v : j \geq 0\}),$$

where $T^0 = \text{id}_V$. For $\mathbf{A} \in M_n(F)$ we write $Z(v; \mathbf{A}) = Z(v; T_{\mathbf{A}})$.

In words: we apply T to v over and over, collect all the vectors obtained, and take their span — so $Z(v; T)$ is a subspace by Theorem 1.3.1, whatever v is. The spanning list may be infinite, but we shall see in a moment that in finite dimension its first few entries already suffice. Note $Z(0; T) = \text{span}(\emptyset) = \{0\}$ and $v \in Z(v; T)$.

Proposition 10.5.1. The Cyclic Subspace Is the Smallest Invariant Subspace Containing the Vector

Let V be a vector space over F , $T \in \mathcal{L}(V)$, and $v \in V$. Then:

- (a) $Z(v; T) = \{p(T)v : p \in F[x]\}$;
- (b) $Z(v; T)$ is T -invariant;
- (c) if U is a T -invariant subspace of V with $v \in U$, then $Z(v; T) \subseteq U$.

Proof.

- (a) A linear combination of the vectors $T^j v$ is $\sum_j a_j T^j v = p(T)v$ with $p = \sum_j a_j x^j$, and conversely (Definition 2.4.2). By Definition 1.3.2, these combinations are exactly the elements of $Z(v; T)$.

- (b) For $p \in F[x]$, $T(p(T)v) = (xp)(T)v \in Z(v; T)$ by Theorem 6.7.1 (b) and (a). (Or: T maps each spanning vector $T^j v$ to $T^{j+1} v \in Z(v; T)$, so Lemma 9.1.1 applies.)
- (c) Let U be invariant with $v \in U$. By induction on j , $T^j v \in U$: this holds for $j = 0$, and if $T^j v \in U$, then $T^{j+1} v = T(T^j v) \in U$ by invariance. So U contains the spanning list of $Z(v; T)$, and hence its span (Theorem 1.3.1, Proposition 1.3.4). ■

Examples. Throughout, V is finite-dimensional over F .

- **An eigenvector generates a line.** If $Tv = \lambda v$ with $v \neq 0$, then $T^j v = \lambda^j v$, so $Z(v; T) = \text{span}(v)$, of dimension 1. The smallest invariant subspace containing an eigenvector is its own line (Proposition 9.1.2).
- **The top of a Jordan chain generates the block.** Let T have matrix $\mathbf{J}_k(\lambda)$ in the basis $\mathcal{B} = (b_1, \dots, b_k)$. Then b_k is the top of the chain (Definition 10.2.2), and $b_{k-1} = (T - \lambda \text{id}_V)b_k = Tb_k - \lambda b_k \in \text{span}(b_k, Tb_k)$; continuing downwards, every b_j lies in $\text{span}(b_k, Tb_k, \dots, T^{k-j} b_k)$. So $Z(b_k; T) = V$: a single Jordan block is one cyclic subspace.
- **Differentiation.** For differentiation $D \in \mathcal{L}(\mathbb{R}[x]_{\leq 3})$, $Z(x^3; D) = \text{span}(x^3, 3x^2, 6x, 6)$ is everything, while $Z(x^2; D) = \text{span}(x^2, 2x, 2) = \mathbb{R}[x]_{\leq 2}$ is a proper subspace.
- **A companion matrix.** Let $\mathbf{A} \in M_n(F)$ have 1 in each position just below the diagonal, so that $\mathbf{A}\mathbf{e}_j = \mathbf{e}_{j+1}$ for $j \leq n-1$ (Exercise (C1: Companion matrices)). Then $\mathbf{A}^j \mathbf{e}_1 = \mathbf{e}_{j+1}$ for $j \leq n-1$, so $Z(\mathbf{e}_1; \mathbf{A})$ contains every standard basis vector and equals F^n .
- **The degenerate case.** $Z(0; T) = \{0\}$, the smallest invariant subspace of all.

Nonexample by minimal change. Truncate the spanning list: $\text{span}(\mathbf{v}, T\mathbf{v})$ need **not** be

invariant. For $\mathbf{A} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and $\mathbf{v} = \mathbf{e}_1$ we get $\text{span}(\mathbf{e}_1, \mathbf{A}\mathbf{e}_1) = \text{span}(\mathbf{e}_1, \mathbf{e}_2)$, and $\mathbf{A}\mathbf{e}_2 = \mathbf{e}_3$

is outside it. What fails is closure: cutting the list short loses exactly the vectors that invariance demands. The correct statement is that the list may be cut short at the right place, which is the subject of the next subsection.

Warning. $Z(v; T)$ depends on T as much as on v , and the spanning list $(v, Tv, T^2v, \dots)$ is almost never independent. For $\mathbf{v} = \mathbf{e}_1$ and $T = \text{id}$ the list is $(\mathbf{e}_1, \mathbf{e}_1, \mathbf{e}_1, \dots)$ and the cyclic subspace is a line; for the same $\mathbf{v}$ and the companion matrix above it is all of F^3 . In finite dimension the list must become dependent by step $\dim V$ at the latest (Theorem 1.6.3), and where it first does is the only thing that matters.

10.5.2 The annihilator of a vector

The examples suggest measuring v by the first dependence in the list $v, Tv, T^2v, \dots$. A dependence is a polynomial relation: $\sum_j a_j T^j v = 0$ says that the polynomial $p = \sum_j a_j x^j$ kills v , not necessarily all of V . Chapter 6 taught us what to do with such a set of polynomials.

The T -annihilator of v is the minimal polynomial of T as seen by the single vector v .

Definition 10.5.2. The T -Annihilator of a Vector

Let V be a **finite-dimensional** vector space over F , let $T \in \mathcal{L}(V)$, and let $v \in V$. The set

$$I_v := \{ p \in F[x] : p(T)v = 0 \}$$

is a nonzero ideal of $F[x]$, and the T -**annihilator** of v , written $m_{T,v}$, is its unique **monic** generator:

$$I_v = \langle m_{T,v} \rangle.$$

Equivalently, $m_{T,v}$ is the monic polynomial of **least degree** with $m_{T,v}(T)v = 0$. For $\mathbf{A} \in M_n(F)$ we write $m_{\mathbf{A},v}$.

Well-definedness. Three checks. *Ideal:* if $p, q \in I_v$, then $(p+q)(T)v = p(T)v + q(T)v = 0$, and for any $h \in F[x]$, $(hp)(T)v = h(T)(p(T)v) = 0$, using Theorem 6.7.1 (a), (b); so I_v is an ideal (Definition 6.2.1). *Nonzero:* $m_T \in I_v$, since $m_T(T) = 0$ as an operator (Definition 9.5.1), and $m_T \neq 0$. *Monic generator:* a nonzero ideal of $F[x]$ has exactly one monic generator, which is its nonzero element of least degree (Theorem 6.2.2). As with the minimal polynomial, the divisibility statement is the one we use:

$$p(T)v = 0 \iff m_{T,v} \mid p. \quad (*)$$

In words: $m_{T,v}$ records which polynomials in T kill this one vector. Two degenerate cases: $m_{T,0} = 1$, because every polynomial kills 0; and if $v \neq 0$, then $\deg m_{T,v} \geq 1$, since the constant 1 does not kill v . If v is an eigenvector for λ , then $m_{T,v} = x - \lambda$.

Why this definition. The minimal polynomial m_T is the “annihilator of all of V at once”: m_T kills every vector, so $m_{T,v} \mid m_T$ for every v by (*). The individual annihilators are finer, and they differ from vector to vector: for $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ we have $m_{\mathbf{J},\mathbf{e}_1} = x - 1$ but $m_{\mathbf{J},\mathbf{e}_2} = (x - 1)^2 = m_{\mathbf{J}}$. This spread is exactly what will let us split V into cyclic pieces in Section 6.

Now the payoff: the annihilator computes the dimension of the cyclic subspace, hands us a basis, and hands us the matrix.

Theorem 10.5.2. Basis and Matrix of a Cyclic Subspace

Let V be a finite-dimensional vector space over F , let $T \in \mathcal{L}(V)$, and let $v \in V$ with $v \neq 0$. Write $Z = Z(v; T)$ and

$$m_{T,v} = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0, \quad k = \deg m_{T,v} \geq 1.$$

Then:

- (a) $(v, Tv, \dots, T^{k-1}v)$ is a basis of Z ; in particular $\dim Z = \deg m_{T,v}$;
- (b) $T^k v = -(a_0v + a_1Tv + \cdots + a_{k-1}T^{k-1}v)$, and the matrix of $T|_Z$ in the basis of (a) is the companion matrix of $m_{T,v}$ (Exercise (C1: Companion matrices); the definition is repeated in full as [Definition 10.5.3](#) below);
- (c) $m_{T|_Z} = p_{T|_Z} = m_{T,v}$;
- (d) $m_{T,v} \mid m_T$, and $\deg m_{T,v} \leq \deg m_T \leq \dim V$.

Idea. For spanning, divide: any p is $q m_{T,v} + r$ with $\deg r < k$, and the $q m_{T,v}$ part dies on v , so $p(T)v = r(T)v$ uses only the first k powers. For independence, a shorter dependence would be a nonzero polynomial of degree $< k$ in I_v , and $m_{T,v}$ has the least degree there.

Part (b) is the definition of $m_{T,v}$ rearranged, read as the last column of a matrix; (c) says that on Z the vector v already sees everything, so its annihilator is the minimal polynomial of the restriction, and a degree count makes it the characteristic polynomial too.

Proof.

- (a) *Spanning.* Let $z \in Z$, say $z = p(T)v$ with $p \in F[x]$ ([Proposition 10.5.1](#) (a)). Divide by $m_{T,v}$: there are $q, r \in F[x]$ with $p = q m_{T,v} + r$ and $\deg r < k$ ([Theorem 6.1.1](#)). Then

$$z = p(T)v = q(T)(m_{T,v}(T)v) + r(T)v = r(T)v,$$

by [Theorem 6.7.1](#) (a), (b) and $m_{T,v}(T)v = 0$. As $\deg r < k$, the vector $r(T)v$ is a combination of $v, Tv, \dots, T^{k-1}v$.

Independence. Suppose $c_0v + c_1Tv + \dots + c_{k-1}T^{k-1}v = 0$ with the $c_j \in F$ not all zero. Then $q = \sum_{j < k} c_j x^j$ is a nonzero element of I_v of degree less than k , contradicting the fact that $m_{T,v}$ has least degree among the nonzero elements of I_v ([Theorem 6.2.2](#)). So all $c_j = 0$.

- (b) The identity $m_{T,v}(T)v = 0$ reads $T^k v + a_{k-1}T^{k-1}v + \dots + a_0v = 0$, which is the display. Write $z_j = T^{j-1}v$ for $j = 1, \dots, k$, the basis of (a). For $j \leq k-1$, $Tz_j = T^jv = z_{j+1}$, so the j -th column of the matrix is $\mathbf{e}_{j+1}$; and $Tz_k = T^k v = -a_0z_1 - \dots - a_{k-1}z_k$, so the last column is $(-a_0, -a_1, \dots, -a_{k-1})$. That is exactly the companion matrix of $m_{T,v}$ in the sense of Exercise (C1: Companion matrices), whose definition is recalled in full in the next subsection. For $k = 1$ the matrix is the 1×1 matrix $(-a_0)$.
- (c) Let $p \in F[x]$. If $p(T)v = 0$, then for every $q \in F[x]$,

$$p(T)(q(T)v) = q(T)(p(T)v) = 0$$

by [Theorem 6.7.1](#) (c), so $p(T)$ kills all of Z by [Proposition 10.5.1](#) (a). Since Z is T -invariant, $(T|_Z)^j z = T^j z$ for every $j \geq 0$ and $z \in Z$, hence $g(T|_Z) = g(T)|_Z$ for every $g \in F[x]$; with $g = p$ this reads $p(T|_Z) = 0$. Conversely, if $p(T|_Z) = 0$, then in particular $p(T)v = 0$, as $v \in Z$. So the annihilating ideals of v and of $T|_Z$ coincide, and their monic generators agree: $m_{T|_Z} = m_{T,v}$ ([Definition 9.5.1](#), [Theorem 6.2.2](#)). Finally $m_{T|_Z} \mid p_{T|_Z}$ ([Corollary 9.6.2](#)), both are monic, and $\deg p_{T|_Z} = \dim Z = k = \deg m_{T|_Z}$ by (a) and [Theorem 7.10.2](#); so they are equal ([Proposition 6.1.2](#) (c), (d)).

- (d) $m_T \in I_v$ as noted after [Definition 10.5.2](#), so $m_{T,v} \mid m_T$ by (*), and the degrees compare by [Proposition 6.1.2](#) (c). And $\deg m_T \leq \deg p_T = \dim V$ by [Corollary 9.6.2](#) and [Theorem 7.10.2](#). ■

Quick check. Let T be the operator on $\mathbb{Q}^2$ with matrix $\text{diag}(2, 5)$, and let $\mathbf{v} = (1, 1)$. Find $m_{T,\mathbf{v}}$ and $Z(\mathbf{v}; T)$. Then do the same for $\mathbf{v} = \mathbf{e}_1$.

Solution. $(T - 2 \text{ id})(T - 5 \text{ id})\mathbf{v} = \mathbf{0}$, as one checks entry by entry, so $m_{T,\mathbf{v}} \mid (x - 2)(x - 5)$. Neither factor alone kills $\mathbf{v}$: $(T - 2 \text{ id})\mathbf{v} = (0, 3) \neq \mathbf{0}$ and $(T - 5 \text{ id})\mathbf{v} = (-3, 0) \neq \mathbf{0}$. So $m_{T,\mathbf{v}} = (x - 2)(x - 5)$, of degree 2, and $Z(\mathbf{v}; T) = \mathbb{Q}^2$ by [Theorem 10.5.2](#) (a); the basis it provides is $(\mathbf{v}, T\mathbf{v}) = ((1, 1), (2, 5))$. For $\mathbf{v} = \mathbf{e}_1$, an eigenvector, $m_{T,\mathbf{e}_1} = x - 2$ and

$Z(\mathbf{e}_1; T) = \text{span}(\mathbf{e}_1)$ is a line.

10.5.3 Companion matrices

The matrix in [Theorem 10.5.2](#) (b) appeared in Chapter 7 as an exercise; it is the block we were looking for, and it deserves a definition of its own.

Definition 10.5.3. Companion Matrix

Let $n \geq 1$ and let $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$ be **monic** of degree n . The **companion matrix** of p is the matrix $\mathbf{C}(p) \in M_n(F)$ with 1 in each position $(j+1, j)$ just **below** the diagonal, last column $(-a_0, -a_1, \dots, -a_{n-1})$, and 0 elsewhere:

$$\mathbf{C}(p) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

For $n = 1$ and $p = x + a_0$ this reads $\mathbf{C}(p) = (-a_0)$.

This is the convention of Exercise (C1: Companion matrices), where the $n \geq 2$ case was introduced: the subdiagonal ones shift the standard basis forward, $\mathbf{C}(p)\mathbf{e}_j = \mathbf{e}_{j+1}$ for $j \leq n-1$, and the last column records the coefficients of p with their signs changed. Some books use the transpose, or put the coefficients in the last row; nothing changes but the bookkeeping, since a matrix and its transpose have the same characteristic polynomial (Exercise (B2: Transpose)).

Theorem 10.5.3. The Companion Matrix Realizes Its Polynomial Twice

Let $p \in F[x]$ be monic of degree $n \geq 1$ and $\mathbf{C} = \mathbf{C}(p)$. Then

$$p\mathbf{C} = m_{\mathbf{C}} = p,$$

and $\mathbf{e}_1$ satisfies $Z(\mathbf{e}_1; \mathbf{C}) = F^n$ with $m_{\mathbf{C}, \mathbf{e}_1} = p$. Consequently every monic polynomial over F is both the characteristic and the minimal polynomial of some square matrix over F .

Proof. For $n = 1$ the matrix is $(-a_0)$, with $p\mathbf{C} = m_{\mathbf{C}} = x + a_0 = p$. Let $n \geq 2$. Since $\mathbf{C}\mathbf{e}_j = \mathbf{e}_{j+1}$ for $j \leq n-1$, induction gives $\mathbf{C}^j\mathbf{e}_1 = \mathbf{e}_{j+1}$ for $0 \leq j \leq n-1$. Hence $Z(\mathbf{e}_1; \mathbf{C})$ contains $\mathbf{e}_1, \dots, \mathbf{e}_n$, so $Z(\mathbf{e}_1; \mathbf{C}) = F^n$, and by [Theorem 10.5.2](#) (a),

$$\deg m_{\mathbf{C}, \mathbf{e}_1} = \dim Z(\mathbf{e}_1; \mathbf{C}) = n.$$

Applying [Theorem 10.5.2](#) (c) with $Z = F^n$, so that $T_{\mathbf{C}}|_Z = T_{\mathbf{C}}$,

$$m_{\mathbf{C}} = m_{T_{\mathbf{C}}} = m_{\mathbf{C}, \mathbf{e}_1} = p_{T_{\mathbf{C}}} = p\mathbf{C},$$

where $m_{\mathbf{C}} = m_{T_{\mathbf{C}}}$ and $p_{T_{\mathbf{C}}} = p\mathbf{C}$ hold by definition (Definition 9.5.1, Definition 7.10.2), the matrix of $T_{\mathbf{C}}$ in the standard basis being $\mathbf{C}$. Finally $m_{\mathbf{C}, \mathbf{e}_1} = p$. Indeed, the basis of $Z(\mathbf{e}_1; \mathbf{C})$ supplied by [Theorem 10.5.2](#) (a) is $(\mathbf{e}_1, \mathbf{C}\mathbf{e}_1, \dots, \mathbf{C}^{n-1}\mathbf{e}_1) = (\mathbf{e}_1, \dots, \mathbf{e}_n)$, the standard basis,

so by [Theorem 10.5.2](#) (b) the matrix of $T_{\mathbf{C}}$ in the standard basis is the companion matrix of $m_{\mathbf{C}, \mathbf{e}_1}$; and that matrix is $\mathbf{C} = \mathbf{C}(p)$. Two companion matrices of monic polynomials of degree n are equal only if the polynomials are, since the last column of $\mathbf{C}(f)$ lists the coefficients of f with their signs changed ([Definition 10.5.3](#)). Hence $m_{\mathbf{C}, \mathbf{e}_1} = p$, and $m_{\mathbf{C}} = p_{\mathbf{C}} = p$. The last sentence follows by taking $\mathbf{C}(p)$ for the given p . ■

So the companion matrix is the field-free analogue of a Jordan block: $\mathbf{J}_k(\lambda)$ and $\mathbf{C}((x - \lambda)^k)$ both have characteristic and minimal polynomial $(x - \lambda)^k$, and they are similar, as we will see in Section 6. The difference is that $\mathbf{C}(p)$ is available for **every** monic p , whether or not p has a root in F .

10.5.4 Cyclic operators

One block is one cyclic subspace. Before assembling many of them, we should know when a single one already fills the space.

Definition 10.5.4. Cyclic Vector, Cyclic Operator

Let V be a finite-dimensional vector space over F with $\dim V = n \geq 1$, and let $T \in \mathcal{L}(V)$. A vector $v \in V$ is a **cyclic vector** for T if

$$Z(v; T) = V.$$

We call T **cyclic** if it has a cyclic vector, and $\mathbf{A} \in M_n(F)$ **cyclic** if $T_{\mathbf{A}}$ is.

By [Theorem 10.5.2](#) (a), v is cyclic exactly when $\deg m_{T,v} = n$, and then $(v, Tv, \dots, T^{n-1}v)$ is a basis of V . That is the definition used in Exercise (C1: Cyclic vectors), so the two agree. Reading [Theorem 10.5.2](#) (b) with $Z = V$: **in the basis generated by a cyclic vector, the matrix of T is a companion matrix.**

The key to the existence of cyclic vectors is a lemma about adding vectors whose annihilators have no common factor. It says that annihilators multiply, exactly as one hopes.

Lemma 10.5.4. Annihilator of a Sum with Coprime Annihilators

Let V be finite-dimensional, $T \in \mathcal{L}(V)$, and $u, w \in V$ with $f = m_{T,u}$ and $g = m_{T,w}$ **coprime**. Then

$$m_{T,u+w} = fg.$$

More generally, if $v_1, \dots, v_k \in V$ have pairwise coprime T -annihilators $f_1, \dots, f_k$, then $m_{T,v_1+\dots+v_k} = f_1 f_2 \cdots f_k$.

Idea. Write $h = m_{T,u+w}$. That h divides fg is immediate, since fg kills both summands. For the other direction, multiply the relation $h(T)(u + w) = 0$ by $g(T)$: the w part dies, leaving $(hg)(T)u = 0$, so $f \mid hg$; and since f and g are coprime we may cancel g and conclude $f \mid h$. Symmetrically $g \mid h$, and two coprime divisors multiply.

Proof. Polynomials in T commute (Theorem 6.7.1 (c)). Hence

$$(fg)(T)(u+w) = g(T)(f(T)u) + f(T)(g(T)w) = 0,$$

so $h \mid fg$, where $h = m_{T,u+w}$. Conversely, applying $g(T)$ to $h(T)(u+w) = 0$ and using $g(T)w = 0$,

$$0 = g(T)h(T)(u+w) = (hg)(T)u + h(T)(g(T)w) = (hg)(T)u.$$

Therefore $f \mid hg$, and since $\gcd(f, g) = 1$, Theorem 6.2.8 gives $f \mid h$. Swapping the roles of u and w gives $g \mid h$. As f and g are coprime and both divide h , their product divides h (Lemma 6.6.3 (b)). With $h \mid fg$, and all three polynomials monic, $h = fg$ (Proposition 6.1.2 (d)).

For k vectors, induct on k . The case $k = 1$ is trivial. Assume $m_{T,v_1+\dots+v_{k-1}} = f_1 \cdots f_{k-1}$. Each f_i with $i \leq k-1$ is coprime to f_k , so $f_1 \cdots f_{k-1}$ is coprime to f_k (Lemma 6.6.3 (a)), and the two-vector case applies to $u = v_1 + \dots + v_{k-1}$ and $w = v_k$. ■

Quick check. Let $\mathbf{A} = \text{diag}(2, 2, 5)$ on $\mathbb{Q}^3$. Find $m_{\mathbf{A}, \mathbf{e}_1}$, $m_{\mathbf{A}, \mathbf{e}_3}$, and $m_{\mathbf{A}, \mathbf{e}_1 + \mathbf{e}_3}$. Is $\mathbf{e}_1 + \mathbf{e}_3$ a cyclic vector for $\mathbf{A}$?

Solution. The vectors $\mathbf{e}_1$ and $\mathbf{e}_3$ are eigenvectors, for 2 and for 5, so $m_{\mathbf{A}, \mathbf{e}_1} = x - 2$ and $m_{\mathbf{A}, \mathbf{e}_3} = x - 5$. These are distinct monic linear polynomials, hence coprime, so Lemma 10.5.4 gives

$$m_{\mathbf{A}, \mathbf{e}_1 + \mathbf{e}_3} = (x - 2)(x - 5),$$

of degree 2. By Theorem 10.5.2 (a), $\dim Z(\mathbf{e}_1 + \mathbf{e}_3; \mathbf{A}) = 2 < 3$, so $\mathbf{e}_1 + \mathbf{e}_3$ is **not** cyclic; indeed $Z(\mathbf{e}_1 + \mathbf{e}_3; \mathbf{A}) = \text{span}(\mathbf{e}_1, \mathbf{e}_3)$. The lemma makes the annihilator as large as the two pieces allow, and here that is still not all of $\mathbb{Q}^3$ — the eigenvalue 2 is repeated, so $m_{\mathbf{A}} = (x - 2)^2(x - 5)$ has degree 3 and no vector can do better.

The lemma turns the primary decomposition into a supply of vectors with the largest possible annihilator.

Proposition 10.5.5. Some Vector Has the Minimal Polynomial as Its Annihilator

Let $V \neq \{0\}$ be a finite-dimensional vector space over F and $T \in \mathcal{L}(V)$. Then there is $v \in V$ with

$$m_{T,v} = m_T.$$

Idea. The minimal polynomial factors as $m_T = p_1^{e_1} \cdots p_k^{e_k}$, and the primary decomposition supplies an invariant piece V_i on which T has minimal polynomial exactly $p_i^{e_i}$. Inside V_i some vector must need the full exponent e_i , or $p_i^{e_i-1}$ would kill the whole piece. Then add up one such vector from each piece: the annihilators are powers of distinct irreducibles, hence pairwise coprime, so Lemma 10.5.4 multiplies them back into m_T .

Proof. Write $m_T = p_1^{e_1} \cdots p_k^{e_k}$ with $p_1, \dots, p_k$ distinct monic irreducibles and $e_i \geq 1$ (Theorem 6.3.5; $\deg m_T \geq 1$ because $V \neq \{0\}$, by Theorem 9.5.1). By Theorem 9.8.1, $V = V_1 \oplus \cdots \oplus V_k$ with $V_i = \ker p_i(T)^{e_i}$ invariant and $m_{T|_{V_i}} = p_i^{e_i}$.

Fix i . *Claim:* some $v_i \in V_i$ has $m_{T,v_i} = p_i^{e_i}$. For $v \in V_i$ we have $p_i^{e_i}(T)v = 0$ by the definition of V_i , so $m_{T,v} \mid p_i^{e_i}$ and hence $m_{T,v} = p_i^f$ with $0 \leq f \leq e_i$ (Lemma 9.5.2). Suppose no $v \in V_i$ has $f = e_i$. Then $m_{T,v} \mid p_i^{e_i-1}$ for every $v \in V_i$, so $p_i^{e_i-1}(T)v = 0$ for every $v \in V_i$; as V_i is T -invariant, $(T|_{V_i})^j v = T^j v$ for every $j \geq 0$ and $v \in V_i$, so $g(T|_{V_i}) = g(T)|_{V_i}$ for every $g \in F[x]$, and therefore $p_i^{e_i-1}(T|_{V_i}) = 0$. By Theorem 9.5.1 this forces $p_i^{e_i} = m_{T|_{V_i}}$ to divide $p_i^{e_i-1}$, which is false by degrees (Proposition 6.1.2 (c)). This proves the claim.

Pick such a v_i for each i and put $v = v_1 + \cdots + v_k$. The polynomials $p_1^{e_1}, \dots, p_k^{e_k}$ are pairwise coprime: a monic common divisor of $p_i^{e_i}$ and $p_j^{e_j}$ with $i \neq j$ is both a power of p_i and a power of p_j (Lemma 9.5.2), hence is 1 by the uniqueness of factorization (Theorem 6.3.5 (b)). So Lemma 10.5.4 gives

$$m_{T,v} = p_1^{e_1} \cdots p_k^{e_k} = m_T,$$

as claimed. ■

An operator is generated by one vector exactly when its minimal polynomial is as large as it can be.

Theorem 10.5.6. Cyclic Operators

Let V be a finite-dimensional vector space over F with $\dim V = n \geq 1$, and let $T \in \mathcal{L}(V)$. The following are equivalent:

- (a) T is cyclic, that is, T has a cyclic vector;
- (b) $\deg m_T = n$;
- (c) $m_T = p_T$.

In that case v is a cyclic vector if and only if $m_{T,v} = m_T$, and in the basis $(v, Tv, \dots, T^{n-1}v)$ the matrix of T is $\mathbf{C}(m_T)$. The same holds for $\mathbf{A} \in M_n(F)$.

Proof.

- (b) $\Leftrightarrow$ (c). Always $m_T \mid p_T$ with both monic and $\deg p_T = n$ (Corollary 9.6.2, Theorem 7.10.2). So $\deg m_T = n$ if and only if $m_T = p_T$ (Proposition 6.1.2 (c), (d)).
- (c) $\Rightarrow$ (b). Let v be cyclic. Then $v \neq 0$, since $Z(0; T) = \{0\} \neq V$, and by Theorem 10.5.2 (a), (d),

$$n = \dim V = \dim Z(v; T) = \deg m_{T,v} \leq \deg m_T \leq n.$$

So all these numbers are equal; in particular $\deg m_T = n$ and $m_{T,v} = m_T$, the two being monic with $m_{T,v} \mid m_T$ of equal degree.

- (d) $\Rightarrow$ (a). By Proposition 10.5.5 there is v with $m_{T,v} = m_T$, and then $\dim Z(v; T) = \deg m_T = n$ by Theorem 10.5.2 (a). A subspace of the same dimension as V is V (Theorem 1.6.8), so $Z(v; T) = V$ and v is cyclic.

For the final statements, the computation in (a) $\Rightarrow$ (b) shows a cyclic vector has $m_{T,v} = m_T$;

conversely if $m_{T,v} = m_T$ and (b) holds, the argument of (b) $\Rightarrow$ (a) shows v is cyclic. The matrix is then $\mathbf{C}(m_{T,v}) = \mathbf{C}(m_T)$ by Theorem 10.5.2 (b). For a matrix $\mathbf{A}$, apply all of this to $T_{\mathbf{A}}$, using $m_{\mathbf{A}} = m_{T_{\mathbf{A}}}$ and $p_{\mathbf{A}} = p_{T_{\mathbf{A}}}$. ■

The implication (a) $\Rightarrow$ (b) was Exercise (C1: Cyclic vectors) (a) in Chapter 9, where the converse was promised for this chapter; the promise is now paid off, and the proof shows what the missing vector is made of — one contribution from each primary piece, chosen to need the full exponent. Two consequences are worth naming. First, an operator with n distinct eigenvalues is cyclic, since then $m_T = p_T$ has n distinct roots (Theorem 9.8.2). Second, **a matrix is similar to a companion matrix if and only if $m_{\mathbf{A}} = p_{\mathbf{A}}$** : one direction is the last sentence of the theorem, and the other follows from Theorem 10.5.3 together with the fact that similar matrices share both polynomials. Section 6 makes this the first case of a general normal form.

Warning. **A cyclic vector need not exist, and when it exists it is far from unique.** For $T = \text{id}$ on F^2 we have $m_T = x - 1$ of degree $1 < 2$, so no vector is cyclic: indeed $Z(\mathbf{v}; \text{id}) = \text{span}(\mathbf{v})$ is a line for every $\mathbf{v} \neq \mathbf{0}$. At the other extreme, if v is cyclic, then so is cv for every $c \neq 0$, and usually many more vectors are: for $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ over $\mathbb{Q}$, a vector (s, t) is cyclic exactly when $t \neq 0$, since $((s, t), (s+t, t))$ has determinant $-t^2$. So “the” cyclic vector is never a well-defined object; only the polynomial m_T is.

Example. A Cyclic Subspace and a Cyclic Vector

Let

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \in M_3(\mathbb{Q}).$$

- Find $p_{\mathbf{A}}$ and $m_{\mathbf{A}}$.
- Find $m_{\mathbf{A}, \mathbf{e}_1}$, the subspace $Z(\mathbf{e}_1; \mathbf{A})$, and the matrix of $T_{\mathbf{A}}$ restricted to it.
- Find a cyclic vector for $\mathbf{A}$ and an invertible $\mathbf{P}$ with $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ a companion matrix.

Solution.

- Expanding $\det(x\mathbf{I} - \mathbf{A})$ along the second row, whose only nonzero entry is $x - 1$ in position $(2, 2)$ (Theorem 7.6.1),

$$p_{\mathbf{A}} = (x - 1) \det \begin{pmatrix} x - 1 & 0 \\ -1 & x - 2 \end{pmatrix} = (x - 1)^2(x - 2).$$

For $m_{\mathbf{A}}$, the roots 1 and 2 must both occur (Theorem 9.5.3), so the first candidate is $(x - 1)(x - 2)$. With

$$\mathbf{A} - \mathbf{I} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathbf{A} - 2\mathbf{I} = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

the product $(\mathbf{A} - \mathbf{I})(\mathbf{A} - 2\mathbf{I})$ has rows: row 1 of $\mathbf{A} - \mathbf{I}$ is $(0, 1, 0)$, which picks out row 2 of $\mathbf{A} - 2\mathbf{I}$, namely $(0, -1, 0)$; row 2 is zero; row 3 is $(1, 0, 1)$, which gives row 1 plus row 3 of $\mathbf{A} - 2\mathbf{I}$, namely $(0, 1, 0)$. So

$$(\mathbf{A} - \mathbf{I})(\mathbf{A} - 2\mathbf{I}) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \neq \mathbf{O},$$

and by Lemma 9.5.2 the only remaining candidate is $m_{\mathbf{A}} = (x - 1)^2(x - 2) = p_{\mathbf{A}}$. So $\mathbf{A}$ is cyclic by Theorem 10.5.6.

(b) $\mathbf{A}\mathbf{e}_1 = (1, 0, 1)$, the first column, and

$$\mathbf{A}^2\mathbf{e}_1 = \mathbf{A}(1, 0, 1) = (\text{column 1}) + (\text{column 3}) = (1, 0, 1) + (0, 0, 2) = (1, 0, 3).$$

Now $(1, 0, 3) = -2\mathbf{e}_1 + 3(1, 0, 1)$, so $(\mathbf{A}^2 - 3\mathbf{A} + 2\mathbf{I})\mathbf{e}_1 = \mathbf{0}$ and $m_{\mathbf{A}, \mathbf{e}_1} \mid x^2 - 3x + 2 = (x - 1)(x - 2)$. Neither factor kills $\mathbf{e}_1$: $(\mathbf{A} - \mathbf{I})\mathbf{e}_1 = (0, 0, 1) \neq \mathbf{0}$ and $(\mathbf{A} - 2\mathbf{I})\mathbf{e}_1 = (-1, 0, 1) \neq \mathbf{0}$. Hence

$$m_{\mathbf{A}, \mathbf{e}_1} = (x - 1)(x - 2) = x^2 - 3x + 2,$$

and by Theorem 10.5.2, $Z(\mathbf{e}_1; \mathbf{A}) = \text{span}(\mathbf{e}_1, (1, 0, 1)) = \text{span}(\mathbf{e}_1, \mathbf{e}_3)$, of dimension 2, with basis $\mathcal{B}_1 = (\mathbf{e}_1, \mathbf{A}\mathbf{e}_1)$ and

$$[T_{\mathbf{A}}|_{Z(\mathbf{e}_1; \mathbf{A})}]_{\mathcal{B}_1}^{\mathcal{B}_1} = \mathbf{C}(x^2 - 3x + 2) = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}.$$

In particular $\mathbf{e}_1$ is **not** cyclic for $\mathbf{A}$: its cyclic subspace is a plane, not $\mathbb{Q}^3$.

(c) Try $\mathbf{v} = \mathbf{e}_2$. Then

$$\mathbf{A}\mathbf{e}_2 = (1, 1, 0), \quad \mathbf{A}^2\mathbf{e}_2 = \mathbf{A}(1, 1, 0) = (1, 0, 1) + (1, 1, 0) = (2, 1, 1).$$

The matrix with these three columns is

$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \det \mathbf{P} = -\det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = -1 \neq 0,$$

expanding along the first column, whose only nonzero entry is the 1 in position $(2, 1)$. So $(\mathbf{e}_2, \mathbf{A}\mathbf{e}_2, \mathbf{A}^2\mathbf{e}_2)$ is a basis and $\mathbf{e}_2$ is a cyclic vector. By Theorem 10.5.6, $m_{\mathbf{A}, \mathbf{e}_2} = m_{\mathbf{A}} = (x - 1)^2(x - 2) = x^3 - 4x^2 + 5x - 2$ and

$$\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{C}(m_{\mathbf{A}}) = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -5 \\ 0 & 1 & 4 \end{pmatrix}.$$

The check. The identity $\mathbf{A}\mathbf{P} = \mathbf{P}\mathbf{C}(m_{\mathbf{A}})$ reads, column by column, $\mathbf{A}\mathbf{e}_2 = \mathbf{A}\mathbf{e}_2$, $\mathbf{A}(\mathbf{A}\mathbf{e}_2) = \mathbf{A}^2\mathbf{e}_2$ — both true by construction — and

$$\mathbf{A}(\mathbf{A}^2\mathbf{e}_2) = 2\mathbf{e}_2 - 5\mathbf{A}\mathbf{e}_2 + 4\mathbf{A}^2\mathbf{e}_2,$$

which is the annihilator relation. Verifying it: $\mathbf{A}(2, 1, 1) = 2(1, 0, 1) + (1, 1, 0) + (0, 0, 2) = (3, 1, 4)$, while

$$2(0, 1, 0) - 5(1, 1, 0) + 4(2, 1, 1) = (0 - 5 + 8, 2 - 5 + 4, 4) = (3, 1, 4). \checkmark$$

10.5.5 Exercises

10.5.5.1 A. Check your understanding

Exercise. A1

- Define $Z(v; T)$ and the T -annihilator $m_{T,v}$.
- State the formula for $\dim Z(v; T)$ and say which basis of $Z(v; T)$ the theorem provides.
- Write down $\mathbf{C}(p)$ for $p = x^3 - 2x + 5$, and say what $p_{\mathbf{C}(p)}$ and $m_{\mathbf{C}(p)}$ are.
- True or false: every operator on a space of dimension $n \geq 2$ has a cyclic vector. Justify your answer.
- What is $m_{T,v}$ when v is an eigenvector of T for λ ? What is $Z(v; T)$ then?
- True or false: if $m_{T,v} = m_T$ for some v , then v is a cyclic vector. Justify your answer.

Solution.

- $Z(v; T) = \text{span}(v, Tv, T^2v, \dots) = \{p(T)v : p \in F[x]\}$ (Definition 10.5.1, Proposition 10.5.1); $m_{T,v}$ is the monic generator of the ideal $\{p : p(T)v = 0\}$, equivalently the monic polynomial of least degree killing v (Definition 10.5.2).
- $\dim Z(v; T) = \deg m_{T,v} = k$, with basis $(v, Tv, \dots, T^{k-1}v)$ (Theorem 10.5.2 (a)).
- Here $a_0 = 5$, $a_1 = -2$, $a_2 = 0$, so

$$\mathbf{C}(p) = \begin{pmatrix} 0 & 0 & -5 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix},$$

and $p_{\mathbf{C}(p)} = m_{\mathbf{C}(p)} = x^3 - 2x + 5$ (Theorem 10.5.3).

- False. id_V has $m_T = x - 1$ of degree $1 < n$, so no cyclic vector (Theorem 10.5.6). More generally any T with $\deg m_T < n$ fails.
- $m_{T,v} = x - \lambda$, and $Z(v; T) = \text{span}(v)$ is the eigenline.
- False. By Theorem 10.5.2 (a), $\dim Z(v; T) = \deg m_{T,v} = \deg m_T$, which need not be n . For $T = \text{id}$ on F^2 and $\mathbf{v} = \mathbf{e}_1$ we have $m_{T,\mathbf{v}} = x - 1 = m_T$, yet $Z(\mathbf{v}; T) = \text{span}(\mathbf{e}_1)$ is a line. The statement is true when $\deg m_T = \dim V$ (Theorem 10.5.6).

10.5.5.2 B. Practice

Exercise. B1: Annihilators of vectors

Let

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in M_3(\mathbb{Q}).$$

- Write down $p_{\mathbf{A}}$.
- Find $m_{\mathbf{A}, \mathbf{e}_1}$, $m_{\mathbf{A}, \mathbf{e}_2}$, and $m_{\mathbf{A}, \mathbf{e}_3}$.
- For each of the three vectors, give $\dim Z(\mathbf{e}_j; \mathbf{A})$ and identify the subspace.
- Write down the matrix of $T_{\mathbf{A}}$ restricted to $Z(\mathbf{e}_2; \mathbf{A})$ in the basis $(\mathbf{e}_2, \mathbf{A}\mathbf{e}_2)$, and say which companion matrix it is.

Solution.

- $\mathbf{A}$ is upper triangular, so $p_{\mathbf{A}} = (x - 1)^2(x - 2)$ (Theorem 7.4.6).
- $\mathbf{A}\mathbf{e}_1 = \mathbf{e}_1$, so $\mathbf{e}_1$ is an eigenvector and $m_{\mathbf{A}, \mathbf{e}_1} = x - 1$.
 $\mathbf{A}\mathbf{e}_2 = (1, 1, 0) = \mathbf{e}_1 + \mathbf{e}_2$, so $(\mathbf{A} - \mathbf{I})\mathbf{e}_2 = \mathbf{e}_1 \neq \mathbf{0}$ and $(\mathbf{A} - \mathbf{I})^2\mathbf{e}_2 = (\mathbf{A} - \mathbf{I})\mathbf{e}_1 = \mathbf{0}$.
Hence $(x - 1)^2$ kills $\mathbf{e}_2$ but $x - 1$ does not, and $m_{\mathbf{A}, \mathbf{e}_2} = (x - 1)^2$ by Lemma 9.5.2.
 $\mathbf{A}\mathbf{e}_3 = (1, 1, 2)$ and $\mathbf{A}^2\mathbf{e}_3 = \mathbf{A}(1, 1, 2) = (1, 0, 0) + (1, 1, 0) + 2(1, 1, 2) = (4, 3, 4)$. The
matrix with columns $\mathbf{e}_3, (1, 1, 2), (4, 3, 4)$ is $\begin{pmatrix} 0 & 1 & 4 \\ 0 & 1 & 3 \\ 1 & 2 & 4 \end{pmatrix}$, of determinant $\det \begin{pmatrix} 1 & 4 \\ 1 & 3 \end{pmatrix} = -1 \neq 0$ by expansion along the first column. So the three vectors are independent, $\deg m_{\mathbf{A}, \mathbf{e}_3} = 3$, and since $m_{\mathbf{A}, \mathbf{e}_3} \mid m_{\mathbf{A}} \mid p_{\mathbf{A}}$ with $\deg p_{\mathbf{A}} = 3$ we get $m_{\mathbf{A}, \mathbf{e}_3} = p_{\mathbf{A}} = (x - 1)^2(x - 2)$.
- $\dim Z(\mathbf{e}_1; \mathbf{A}) = 1$ and $Z(\mathbf{e}_1; \mathbf{A}) = \text{span}(\mathbf{e}_1)$. $\dim Z(\mathbf{e}_2; \mathbf{A}) = 2$ and $Z(\mathbf{e}_2; \mathbf{A}) = \text{span}(\mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_2) = \text{span}(\mathbf{e}_1, \mathbf{e}_2)$. $\dim Z(\mathbf{e}_3; \mathbf{A}) = 3$, so $Z(\mathbf{e}_3; \mathbf{A}) = \mathbb{Q}^3$ and $\mathbf{e}_3$ is a cyclic vector.
- $(x - 1)^2 = x^2 - 2x + 1$, so by Theorem 10.5.2 (b) the matrix is

$$\mathbf{C}((x - 1)^2) = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}.$$

Exercise. B2: Cyclic or not?

Determine whether each matrix is cyclic. For those that are, find a cyclic vector; for those that are not, say which condition fails.

- $\text{diag}(1, 2, 3) \in M_3(\mathbb{Q})$.
- $\text{diag}(1, 1, 2) \in M_3(\mathbb{Q})$.
- $\mathbf{B} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{Q})$, for which $p_{\mathbf{B}} = m_{\mathbf{B}} = (x - 2)^2(x - 1)$. Check first that none of $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ is cyclic.
- $\mathbf{J}_2(0) \oplus \mathbf{J}_1(0) \in M_3(\mathbb{Q})$.

Hint: for (c), compute the three annihilators $m_{\mathbf{B}, \mathbf{e}_j}$ and use Lemma 10.5.4.

Solution.

- (a) Cyclic. The three eigenvalues are distinct, so $m = (x-1)(x-2)(x-3) = p$ (Theorem 9.8.2), of degree 3. A cyclic vector is $\mathbf{v} = (1, 1, 1)$: the matrix with columns $\mathbf{v}, \mathbf{A}\mathbf{v} = (1, 2, 3), \mathbf{A}^2\mathbf{v} = (1, 4, 9)$ is a Vandermonde matrix with distinct nodes 1, 2, 3, hence invertible (Corollary 7.8.2).
- (b) Not cyclic. Here $m = (x-1)(x-2)$ has degree $2 < 3$, so condition (b) of Theorem 10.5.6 fails.
- (c) *The standard basis vectors.* $\mathbf{B}\mathbf{e}_1 = (2, 0, 1)$ and $\mathbf{B}^2\mathbf{e}_1 = \mathbf{B}(2, 0, 1) = 2(2, 0, 1) + (0, 0, 1) = (4, 0, 3)$. Since $(4, 0, 3) = -2\mathbf{e}_1 + 3(2, 0, 1)$, the vector $\mathbf{e}_1$ is killed by $x^2 - 3x + 2 = (x-1)(x-2)$, and by neither factor alone ($(\mathbf{B} - \mathbf{I})\mathbf{e}_1 = (1, 0, 1) \neq \mathbf{0}$, $(\mathbf{B} - 2\mathbf{I})\mathbf{e}_1 = (0, 0, 1) \neq \mathbf{0}$); so $m_{\mathbf{B}, \mathbf{e}_1} = (x-1)(x-2)$, of degree 2.
 $\mathbf{B}\mathbf{e}_2 = (1, 2, 1)$ and $\mathbf{B}^2\mathbf{e}_2 = \mathbf{B}(1, 2, 1) = (2, 0, 1) + 2(1, 2, 1) + (0, 0, 1) = (4, 4, 4)$. As $(4, 4, 4) = -4\mathbf{e}_2 + 4(1, 2, 1)$, the vector $\mathbf{e}_2$ is killed by $x^2 - 4x + 4 = (x-2)^2$, and not by $x-2$; so $m_{\mathbf{B}, \mathbf{e}_2} = (x-2)^2$.
 $\mathbf{B}\mathbf{e}_3 = \mathbf{e}_3$, so $m_{\mathbf{B}, \mathbf{e}_3} = x-1$.

All three degrees are less than 3, so none of $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ is cyclic (Theorem 10.5.2 (a)).

A cyclic vector. The annihilators $(x-2)^2$ of $\mathbf{e}_2$ and $x-1$ of $-\mathbf{e}_3$ — note $m_{T, -\mathbf{v}} = m_{T, \mathbf{v}}$, since $p(T)(-\mathbf{v}) = -p(T)\mathbf{v}$ — are coprime, so Lemma 10.5.4 gives

$$m_{\mathbf{B}, \mathbf{e}_2 - \mathbf{e}_3} = (x-2)^2(x-1) = m_{\mathbf{B}}.$$

By Theorem 10.5.6, $\mathbf{v} = \mathbf{e}_2 - \mathbf{e}_3 = (0, 1, -1)$ is a cyclic vector. As a check, $\mathbf{B}\mathbf{v} = (1, 2, 1) - (0, 0, 1) = (1, 2, 0)$ and $\mathbf{B}^2\mathbf{v} = \mathbf{B}(1, 2, 0) = (2, 0, 1) + 2(1, 2, 1) = (4, 4, 3)$, and the matrix with columns $(0, 1, -1), (1, 2, 0), (4, 4, 3)$ has determinant

$$-\det \begin{pmatrix} 1 & 4 \\ -1 & 3 \end{pmatrix} + 4 \det \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix} = -(3+4) + 4 \cdot 2 = 1 \neq 0$$

by expansion along the first row.

- (d) Not cyclic: $m = x^2$ (Proposition 9.5.6) has degree $2 < 3$.

Exercise. B3: Cyclic subspaces for differentiation

Let $V = \mathbb{R}[x]_{\leq 3}$ and let $D \in \mathcal{L}(V)$ be differentiation.

- (a) Find $m_{D, q}$ for $q = 1, q = x, q = x^2$, and $q = x^3$.
 (b) Find $Z(x^2; D)$ and the matrix of D restricted to it in the basis (x^2, Dx^2, D^2x^2) .
 (c) Is x^3 a cyclic vector for D ? What is m_D ?

Solution.

- (a) $D1 = 0$, so $m_{D, 1} = x$. $Dx = 1 \neq 0$ and $D^2x = 0$, so $m_{D, x} = x^2$. Likewise $D^2x^2 = 2 \neq 0$ and $D^3x^2 = 0$, so $m_{D, x^2} = x^3$; and $D^3x^3 = 6 \neq 0$ with $D^4x^3 = 0$, so $m_{D, x^3} = x^4$. (In each case the annihilator is a monic divisor of x^4 , hence a power of x , by Lemma 9.5.2.)
 (b) $Z(x^2; D) = \text{span}(x^2, 2x, 2) = \mathbb{R}[x]_{\leq 2}$, of dimension $3 = \deg m_{D, x^2}$. With $z_1 = x^2$,

$z_2 = Dx^2 = 2x$, $z_3 = D^2x^2 = 2$ we have $Dz_1 = z_2$, $Dz_2 = z_3$, $Dz_3 = 0$, so the matrix is

$$\mathbf{C}(x^3) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \mathbf{J}_3(0)^\top.$$

- (c) Yes: $\dim Z(x^3; D) = \deg m_{D, x^3} = 4 = \dim V$. Hence $m_D = m_{D, x^3} = x^4 = p_D$ by [Theorem 10.5.6](#), which agrees with Example (Differentiation Is Nilpotent).

10.5.5.3 C. Going deeper

Exercise. C1: What commutes with a cyclic operator

Let V be finite-dimensional with $\dim V = n \geq 1$ and let $T \in \mathcal{L}(V)$ satisfy $m_T = p_T$.

- Prove that every $S \in \mathcal{L}(V)$ with $ST = TS$ is a polynomial in T , that is, $S = q(T)$ for some $q \in F[x]$.
- Deduce that the set $\{S \in \mathcal{L}(V) : ST = TS\}$ is a subspace of $\mathcal{L}(V)$ of dimension exactly n .
- Show that (a) fails without the hypothesis $m_T = p_T$, by taking $T = \text{id}_V$ with $n \geq 2$.

Hint for (a): apply S to a cyclic vector.

Solution.

- By [Theorem 10.5.6](#) there is a cyclic vector v , and $\mathcal{B} = (v, Tv, \dots, T^{n-1}v)$ is a basis of V . Since $\mathcal{B}$ spans V , there is $q \in F[x]$ with $Sv = q(T)v$ ([Proposition 10.5.1](#) (a)). For each $j \geq 0$, using $ST = TS$ and hence $ST^j = T^jS$ (induction on j), and that polynomials in T commute with T ([Theorem 6.7.1](#) (c)),

$$S(T^jv) = T^j(Sv) = T^jq(T)v = q(T)(T^jv).$$

So S and $q(T)$ agree on the basis $\mathcal{B}$, hence $S = q(T)$ ([Theorem 2.1.5](#)).

- The set is a subspace: it contains 0, and if $S_1T = TS_1$ and $S_2T = TS_2$, then $(S_1 + cS_2)T = T(S_1 + cS_2)$. By (a) it equals $\{q(T) : q \in F[x]\} = \text{span}(\text{id}_V, T, \dots, T^{n-1})$, where we used [Theorem 6.1.1](#) to reduce q modulo m_T , whose degree is n . That spanning list is independent: a vanishing combination would give a nonzero polynomial of degree less than $n = \deg m_T$ annihilating T , contradicting [Theorem 9.5.1](#). So the dimension is n .
- For $T = \text{id}_V$ every S commutes with T , so the commutant is all of $\mathcal{L}(V)$, of dimension $n^2 \geq 4$. But the polynomials in id_V are just the scalar operators $c \text{id}_V$, a subspace of dimension 1. Here $m_T = x - 1 \neq (x - 1)^n = p_T$.

Exercise. C2: How many cyclic vectors?

Let V be finite-dimensional with $\dim V = n \geq 1$ and $T \in \mathcal{L}(V)$.

- Prove that v is a cyclic vector for T if and only if v lies in no T -invariant subspace U with $U \neq V$.

- (b) Prove that if v is cyclic, then so is cv for every $c \in F$ with $c \neq 0$. Deduce that over an infinite field a cyclic operator has infinitely many cyclic vectors.
- (c) Let $F = \mathbb{F}_2$ and $T = T_{\mathbf{J}}$ with $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Find **all** cyclic vectors of T .
- (d) Deduce from (c) that the set of cyclic vectors, together with 0, need not be a subspace.

Solution.

- (a) ($\Rightarrow$) Let v be cyclic and let U be T -invariant with $v \in U$. By [Proposition 10.5.1](#) (c), $V = Z(v; T) \subseteq U$, so $U = V$. ($\Leftarrow$) If v is not cyclic, then $U = Z(v; T)$ is itself a T -invariant subspace containing v with $U \neq V$ ([Proposition 10.5.1](#) (b)).
- (b) For $c \neq 0$, $p(T)(cv) = cp(T)v$, so $p(T)(cv) = 0$ if and only if $p(T)v = 0$ (as $c \neq 0$ and by [Theorem 1.1.9](#)). Hence $m_{T,cv} = m_{T,v}$, and [Theorem 10.5.6](#) makes cv cyclic as well. Over an infinite field the vectors cv , $c \neq 0$, are pairwise distinct (if $cv = c'v$ with $v \neq 0$, then $c = c'$), so there are infinitely many.
- (c) Write $\mathbf{v} = (s, t)$ with $s, t \in \mathbb{F}_2$. Then $\mathbf{J}\mathbf{v} = (s + t, t)$, and $(\mathbf{v}, \mathbf{J}\mathbf{v})$ is a basis of $\mathbb{F}_2^2$ if and only if

$$\det \begin{pmatrix} s & s+t \\ t & t \end{pmatrix} = st - t(s+t) = -t^2 = t^2 \neq 0,$$

that is, if and only if $t = 1$. So the cyclic vectors are exactly $(0, 1)$ and $(1, 1)$, two of the four vectors of $\mathbb{F}_2^2$.

- (d) The set $\{\mathbf{0}, (0, 1), (1, 1)\}$ has 3 elements, and a subspace of $\mathbb{F}_2^2$ has 1, 2, or 4 elements. Concretely, $(0, 1) + (1, 1) = (1, 0)$, which is an eigenvector of $\mathbf{J}$ and hence not cyclic. So the set is not closed under addition.