

9.5 The Minimal Polynomial

Section 4 decided diagonalizability by counting eigenvectors, one eigenspace at a time. There is a second source of information about an operator, which Chapter 6 set up: the polynomials that kill it. On a finite-dimensional space they form an ideal of $F[x]$, and that ideal has a single monic generator. This section gives the generator its name, the minimal polynomial, and shows that its roots are exactly the eigenvalues. We learn two ways to compute it and check that similar matrices share it. The next section compares it with the characteristic polynomial, and Section 8 reads diagonalizability off its factorization.

9.5.1 The polynomial that divides all the others

Chapter 6 turned every polynomial identity satisfied by an operator into a statement about one ideal. For $T \in \mathcal{L}(V)$, the set

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

is an ideal of $F[x]$ (Theorem 6.7.3 (a)). If V is finite-dimensional, it contains a nonzero polynomial (Theorem 6.7.3 (c)). Then it consists of the multiples of a unique monic polynomial (Theorem 6.7.3 (b)).

Look at what this says for one operator. A projection P with $P \neq 0, \text{id}_V$ satisfies $P^2 = P$, so $x^2 - x$ kills it. So do $x^3 - x^2$, $(x^2 - x)(x + 5)$, and $x^{10} - x^9$, and a short calculation shows each one is a multiple of $x^2 - x$. This is no accident. Every annihilating polynomial of P is a multiple of $x^2 - x$, which Chapter 6 found to be the monic generator of I_P . One polynomial controls the whole list, and whenever something in mathematics is unique we give it a name.

The minimal polynomial of T is the one monic polynomial that kills T and divides every other polynomial that kills T .

Definition 9.5.1. Minimal Polynomial

Let V be a **finite-dimensional** vector space over F and $T \in \mathcal{L}(V)$. The **minimal polynomial** of T is the unique **monic** polynomial $m_T \in F[x]$ with

$$I_T = \{p \in F[x] : p(T) = 0\} = \langle m_T \rangle.$$

Equivalently, m_T is the monic polynomial of **least degree** with $m_T(T) = 0$.

For $\mathbf{A} \in M_n(F)$, the minimal polynomial is $m_{\mathbf{A}} := m_{T_{\mathbf{A}}}$: the monic polynomial of least degree with $m_{\mathbf{A}}(\mathbf{A}) = \mathbf{O}$.

In words: we look at **all** polynomials p with $p(T) = 0$, where $p(T)$ replaces x^k by T^k and the constant term c by $c \text{id}_V$ (Definition 2.4.2). They are exactly the multiples of one polynomial m_T . Among the generators of this ideal, which differ by nonzero constant factors, we pick **the monic** one. The second sentence of the definition gives the same polynomial described by size: it is the monic polynomial of **least degree** that kills T .

Well-definedness. Three things need checking, and Chapter 6 did all three. *Existence:* $I_T \neq \{0\}$ because V is finite-dimensional (Theorem 6.7.3 (c)). *Uniqueness:* a nonzero ideal of $F[x]$ has exactly one monic generator (Theorem 6.2.2). *The two descriptions agree:* the same theorem says that the monic generator is the unique monic polynomial of least degree in the ideal. For a matrix, $p(T_{\mathbf{A}}) = 0$ if and only if $p(\mathbf{A}) = \mathbf{O}$, because $[p(T_{\mathbf{A}})]_{\mathcal{E}}^{\mathcal{E}} = p(\mathbf{A})$ in the standard basis $\mathcal{E}$ (Corollary 4.1.3). So $I_{T_{\mathbf{A}}} = \{p : p(\mathbf{A}) = \mathbf{O}\}$, and the matrix version is the operator version for

T_A .

The name records the second description: m_T is the annihilating polynomial of minimal degree. The first description is the one we use in proofs, because it hands us a divisibility for free.

Theorem 9.5.1. Annihilating Polynomials Are Multiples of the Minimal Polynomial

Let V be finite-dimensional and $T \in \mathcal{L}(V)$. For every $p \in F[x]$,

$$p(T) = 0 \iff m_T \mid p.$$

In particular, a nonzero polynomial that annihilates T has degree at least $\deg m_T$. If $V \neq \{0\}$, then $\deg m_T \geq 1$.

Proof. By Definition 9.5.1, $p(T) = 0$ means $p \in \langle m_T \rangle$, that is, $p = q m_T$ for some $q \in F[x]$, that is, $m_T \mid p$. If $p \neq 0$ and $m_T \mid p$, then $\deg m_T \leq \deg p$ by Proposition 6.1.2 (c). Finally, the only monic polynomial of degree 0 is the constant 1, and $1(T) = \text{id}_V \neq 0$ when $V \neq \{0\}$; so $m_T \neq 1$ and $\deg m_T \geq 1$. ■

This is the move we will use again and again: **a polynomial relation becomes a divisibility**. If we learn that $T^3 = T$, we do not need to know anything else about T to conclude that $m_T \mid x^3 - x = x(x-1)(x+1)$. That leaves only finitely many candidates for m_T . To list candidates like these we need to know the monic divisors of a factored polynomial, and unique factorization describes them exactly.

Lemma 9.5.2. Monic Divisors of a Factored Polynomial

Let $f = p_1^{e_1} \cdots p_k^{e_k} \in F[x]$, where $k \geq 1$, $p_1, \dots, p_k$ are **distinct** monic irreducible polynomials, and $e_i \geq 1$. Then the monic divisors of f are exactly the polynomials

$$p_1^{f_1} \cdots p_k^{f_k} \quad \text{with } 0 \leq f_i \leq e_i \text{ for each } i.$$

Idea. One direction is a product: the missing factors form the cofactor. For the other, factor a monic divisor d into irreducibles, multiply that factorization by one of the cofactor, and compare the result with the factorization of f . Uniqueness says the two lists of irreducibles agree, so the irreducibles in d are among the p_i , and none can occur more often in d than in f .

Proof. Each such product divides f , with cofactor $p_1^{e_1-f_1} \cdots p_k^{e_k-f_k}$. Conversely, let d be monic with $f = dh$. If $d = 1$, take every $f_i = 0$. Otherwise d is nonconstant, and by Theorem 6.3.5 (a) it is a product $q_1 \cdots q_s$ of monic irreducibles; the constant in front is the leading coefficient of d , which is 1. The cofactor h is nonzero (as $f \neq 0$), so it is either a nonzero constant c or, by the same theorem, $c r_1 \cdots r_t$ with r_j monic irreducible. Multiplying, $f = c q_1 \cdots q_s r_1 \cdots r_t$ (with no r 's in the first case) is a factorization of f into a constant and monic irreducibles. By Theorem 6.3.5 (b), after renumbering it is the factorization $f = 1 \cdot p_1^{e_1} \cdots p_k^{e_k}$, in which p_i occurs exactly e_i times. So each q_j is one of the p_i , and p_i

occurs at most e_i times among $q_1, \dots, q_s$. Hence $d = p_1^{f_1} \cdots p_k^{f_k}$ with $0 \leq f_i \leq e_i$. ■

Examples. Each computation follows the same plan: find one annihilating polynomial, list its monic divisors with [Lemma 9.5.2](#), and discard those that do not annihilate.

- **A diagonal matrix with a repeated entry.** Let $\mathbf{A} = \text{diag}(1, 1, 2)$. Diagonal matrices multiply entry by entry, so

$$(\mathbf{A} - \mathbf{I})(\mathbf{A} - 2\mathbf{I}) = \text{diag}(0, 0, 1) \text{diag}(-1, -1, 0) = \mathbf{O}.$$

By [Theorem 9.5.1](#), $m_{\mathbf{A}}$ is a monic divisor of $(x - 1)(x - 2)$: one of $1, x - 1, x - 2, (x - 1)(x - 2)$. None of the first three annihilates $\mathbf{A}$, since $\mathbf{I}, \mathbf{A} - \mathbf{I} = \text{diag}(0, 0, 1)$, and $\mathbf{A} - 2\mathbf{I} = \text{diag}(-1, -1, 0)$ are nonzero. So $m_{\mathbf{A}} = (x - 1)(x - 2)$. The repeated diagonal entry 1 appears only **once** in $m_{\mathbf{A}}$, while the characteristic polynomial is $p_{\mathbf{A}} = (x - 1)^2(x - 2)$.

- **A matrix with too few eigenvectors.** Let $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ over any field. Then $\mathbf{J} - \mathbf{I} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \mathbf{O}$, and $(\mathbf{J} - \mathbf{I})^2 = \mathbf{O}$. So $m_{\mathbf{J}}$ is a monic divisor of $(x - 1)^2$, namely $1, x - 1$, or $(x - 1)^2$, and the first two do not annihilate $\mathbf{J}$. Hence $m_{\mathbf{J}} = (x - 1)^2$, which equals $p_{\mathbf{J}}$.
- **Projections.** Chapter 6 found, by this plan, that a projection P with $P \neq 0$ and $P \neq \text{id}_V$ has $m_P = x^2 - x$ (the examples after [Theorem 6.7.3](#)).
- **Differentiation.** Let D be differentiation on $\mathbb{R}[x]_{\leq n}$. Then $D^{n+1} = 0$ and $D^n \neq 0$ (Example (Differentiation Is Nilpotent)). By [Lemma 9.5.2](#), the monic divisors of x^{n+1} are the powers x^j with $0 \leq j \leq n+1$. For $j \leq n$, $D^j \neq 0$, since $D^n = D^{n-j}D^j$ would otherwise be 0. Hence $m_D = x^{n+1}$, of degree $n+1 = \dim \mathbb{R}[x]_{\leq n}$.
- **Degenerate cases.** On $V \neq \{0\}$, the identity has $m = x - 1$ and the zero operator has $m = x$: each is killed by a polynomial of degree 1, which is the least possible degree. More generally $m_{c \text{id}_V} = x - c$, and every 1×1 matrix (c) has $m = x - c$. On $V = \{0\}$, even the constant 1 annihilates, so $m_T = 1$. This last case is the reason for the hypothesis $V \neq \{0\}$ in [Theorem 9.5.1](#).

Nonexample by minimal change. For $\mathbf{J}$ above, take $q = x - 1$ instead of $(x - 1)^2$. It is still monic, it has the least degree a minimal polynomial can have on a nonzero space, and its only root is the eigenvalue 1 of $\mathbf{J}$. What fails is the clause $q(\mathbf{J}) = \mathbf{O}$: $q(\mathbf{J}) = \mathbf{J} - \mathbf{I} \neq \mathbf{O}$. In the other direction, $(x - 1)^3$ is monic and does annihilate $\mathbf{J}$, but it fails the clause $I_{\mathbf{J}} = \langle q \rangle$: the annihilating polynomial $(x - 1)^2$ is not a multiple of $(x - 1)^3$.

Quick check. Find the minimal polynomial of $2\mathbf{I}_3$ and of $\mathbf{N} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(F)$.

Solution. $2\mathbf{I}_3 - 2\mathbf{I}_3 = \mathbf{O}$, so $m_{2\mathbf{I}_3}$ divides $x - 2$; it is not 1, since $\mathbf{I}_3 \neq \mathbf{O}$. Hence $m_{2\mathbf{I}_3} = x - 2$. For $\mathbf{N}$: $\mathbf{N}\mathbf{e}_1 = \mathbf{O}$, $\mathbf{N}\mathbf{e}_2 = \mathbf{e}_1$, $\mathbf{N}\mathbf{e}_3 = \mathbf{e}_2$, so $\mathbf{N}^2\mathbf{e}_3 = \mathbf{e}_1 \neq \mathbf{O}$ and $\mathbf{N}^3$ kills $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$. Thus $\mathbf{N}^3 = \mathbf{O} \neq \mathbf{N}^2$. By [Lemma 9.5.2](#), $m_{\mathbf{N}} \in \{1, x, x^2, x^3\}$, and only x^3 annihilates $\mathbf{N}$ (the others give $\mathbf{I}_3, \mathbf{N}, \mathbf{N}^2 \neq \mathbf{O}$). So $m_{\mathbf{N}} = x^3$.

Why this definition. Each clause has a job.

- *Monic.* The polynomials m and $5m$ generate the same ideal, so “a generator” is determined only up to a nonzero constant. Insisting on leading coefficient 1 picks one, and makes statements like “ $m_{\mathbf{A}} = (x-1)(x-2)$ ” meaningful.
- *Generator, not only least degree.* The two descriptions give the same polynomial. Stating the definition through the ideal puts [Theorem 9.5.1](#) in front of us, and divisibility is the property we use.
- *Finite dimension.* Without it, I_T can be $\{0\}$, and then there is nothing to name. For multiplication by x on $F[x]$, $p(S)(1) = p$, so $p(S) \neq 0$ for every $p \neq 0$ (the remark after [Theorem 6.7.2](#)). The same happens for the right shift on $F^{\mathbb{N}}$.

Warning. The minimal polynomial is not the characteristic polynomial. For $\mathbf{I}_2$, $m = x-1$ while $p = (x-1)^2$; for $\text{diag}(1, 1, 2)$ above, $m = (x-1)(x-2)$ while $p = (x-1)^2(x-2)$. The two can differ in their exponents, and m can have smaller degree than the size of the matrix. How they are related is the subject of the next section. Its main theorem is one that Chapter 7 warned against “proving” by substituting $x = \mathbf{A}$ into $\det(x\mathbf{I} - \mathbf{A})$; that shortcut is not a proof and must not be used here either.

9.5.2 The roots are the eigenvalues

The minimal polynomial is defined by an ideal, and eigenvalues by vectors. They are closely linked.

Theorem 9.5.3. Roots of the Minimal Polynomial

Let V be finite-dimensional, $T \in \mathcal{L}(V)$, and $\lambda \in F$. Then $m_T(\lambda) = 0$ if and only if λ is an eigenvalue of T . Consequently, if $\dim V \geq 1$, then m_T and p_T have the same roots in F .

Idea. ($\Leftarrow$) is a one-liner: apply $m_T(T) = 0$ to an eigenvector v . Since T scales v by λ , every polynomial in T scales v by the value of the polynomial at λ . For ($\Rightarrow$), a root gives a factor: $m_T = (x - \lambda)q$. The cofactor q has smaller degree, so by minimality it does **not** kill T , and some vector w survives it. Then $q(T)w$ is nonzero and is killed by $T - \lambda \text{id}_V$. The eigenvector is manufactured by the part of m_T we removed.

Proof. ($\Leftarrow$) Let $v \neq 0$ with $Tv = \lambda v$. Then $T^j v = \lambda^j v$ for every $j \geq 0$, by induction: it holds for $j = 0$, and $T^{j+1}v = T^j(Tv) = T^j(\lambda v) = \lambda T^j v = \lambda^{j+1}v$, the first equality by Definition 2.4.2. Writing $p = \sum_j c_j x^j$, Definition 2.4.2 gives $p(T)v = \sum_j c_j T^j v = p(\lambda)v$ for every $p \in F[x]$. With $p = m_T$,

$$0 = m_T(T)v = m_T(\lambda)v.$$

Since $v \neq 0$, [Theorem 1.1.9](#) gives $m_T(\lambda) = 0$.

($\Rightarrow$) Suppose $m_T(\lambda) = 0$. By [Theorem 6.1.3 \(b\)](#), $m_T = (x - \lambda)q$ for some $q \in F[x]$, and q is monic with $\deg q = \deg m_T - 1$ by [Theorem 0.8.3](#). By [Theorem 9.5.1](#), a nonzero polynomial of degree less than $\deg m_T$ does not annihilate T ; so $q(T) \neq 0$, and there is $w \in V$ with $v := q(T)w \neq 0$. By [Theorem 6.7.1 \(b\)](#),

$$(T - \lambda \text{id}_V)v = (T - \lambda \text{id}_V)q(T)w = m_T(T)w = 0.$$

So $Tv = \lambda v$ with $v \neq 0$, and λ is an eigenvalue of T .

If $\dim V \geq 1$, the eigenvalues of T are exactly the roots of p_T in F (Theorem 9.2.1, (a) $\Leftrightarrow$ (e)), so m_T and p_T have the same roots in F . This proves the theorem. ■

So the minimal polynomial knows the spectrum, just as the characteristic polynomial does, although the multiplicities of the roots may differ. The examples bear this out. $\text{diag}(1, 1, 2)$ has spectrum $\{1, 2\}$, the roots of $(x - 1)(x - 2)$. $\mathbf{J}$ has spectrum $\{1\}$, the root of $(x - 1)^2$. The rotation R of $\mathbb{R}^2$ by a right angle has $m_R = x^2 + 1$ (the check after Theorem 6.7.3), with no real root, and indeed $\text{spec}(R) = \emptyset$ over $\mathbb{R}$. Its minimal polynomial has no linear factor at all.

Two consequences are worth stating.

- **Invertibility.** Taking $\lambda = 0$: for $V \neq \{0\}$, T is invertible if and only if $m_T(0) \neq 0$. Indeed $m_T(0) = 0$ if and only if $0 \in \text{spec}(T)$, if and only if $T = T - 0 \text{id}_V$ is not invertible (Theorem 9.2.1, (a) $\Leftrightarrow$ (c) with $\lambda = 0$; for matrices this is Theorem 9.2.6). Chapter 6 proved the same statement without eigenvalues (Exercise (C1: Inverses are polynomials) (c)).
- **Over $\mathbb{C}$.** If $F = \mathbb{C}$ and $V \neq \{0\}$, then m_T splits (Corollary 6.5.5), and its roots are the distinct eigenvalues $\lambda_1, \dots, \lambda_k$. So

$$m_T = (x - \lambda_1)^{s_1} \cdots (x - \lambda_k)^{s_k} \quad \text{with every } s_i \geq 1.$$

Only the exponents remain to be found.

9.5.3 Computing the minimal polynomial

There are two practical methods. The first needs nothing but elimination. The second uses the eigenvalues, when we know them, to cut the search down to a few candidates.

Method 1: the first dependence among powers. The proof of Theorem 6.7.2 searched for a dependence among $\text{id}_V, T, T^2, \dots$. The **first** dependence that appears gives m_T exactly.

Proposition 9.5.4. The First Dependence Among the Powers

Let V be finite-dimensional and $T \in \mathcal{L}(V)$. Let $d \geq 0$ be the **least** integer such that the list $(\text{id}_V, T, \dots, T^d)$ in $\mathcal{L}(V)$ is linearly dependent. Then there are unique $c_0, \dots, c_{d-1} \in F$ with

$$T^d = c_0 \text{id}_V + c_1 T + \cdots + c_{d-1} T^{d-1},$$

and $m_T = x^d - c_{d-1}x^{d-1} - \cdots - c_1x - c_0$. In particular $\deg m_T = d$. The same holds for $\mathbf{A} \in M_n(F)$, with powers of $\mathbf{A}$ in $M_n(F)$.

Proof. Such a d exists: with $n = \dim V$, the space $\mathcal{L}(V)$ has dimension n^2 (Theorem 4.1.4), so the list $(\text{id}_V, T, \dots, T^{n^2})$, of length $n^2 + 1$, is linearly dependent (Theorem 1.6.3 (a)). By minimality of d , the list $(\text{id}_V, \dots, T^{d-1})$ is independent (for $d = 0$ it is empty). By Lemma 1.5.3, since appending T^d makes it dependent, $T^d \in \text{span}(\text{id}_V, \dots, T^{d-1})$. The coefficients are unique by Theorem 1.4.3.

Let $q = x^d - c_{d-1}x^{d-1} - \cdots - c_0$. It is monic, and $q(T) = 0$ by the displayed relation. Let $p \neq 0$ with $\deg p < d$. Then $p(T) = \sum_{k < d} a_k T^k$ with the a_k not all zero, and this is not

0 because $(\text{id}_V, \dots, T^{d-1})$ is independent. So no nonzero polynomial of degree less than d annihilates T , and q is the monic annihilating polynomial of least degree. By [Definition 9.5.1](#), $q = m_T$. ■

Example. The Minimal Polynomial from the First Dependence

Find the minimal polynomial of

$$\mathbf{A} = \begin{pmatrix} 3 & 2 & -2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix} \in M_3(\mathbb{R}),$$

the matrix of Example (Diagonalizing a 3×3 Matrix with a Repeated Eigenvalue), without using its eigenvalues.

Solution. *Degree 1.* $\mathbf{A}$ is not a scalar multiple of $\mathbf{I}_3$, since its $(1,2)$ -entry is nonzero. So $(\mathbf{I}_3, \mathbf{A})$ is independent.

Degree 2. Multiplying out,

$$\mathbf{A}^2 = \begin{pmatrix} 9 & 8 & -8 \\ -8 & -7 & 8 \\ -8 & -8 & 9 \end{pmatrix}.$$

We look for a, b with $\mathbf{A}^2 = a\mathbf{A} + b\mathbf{I}_3$. The $(1,2)$ -entries give $8 = 2a$, so $a = 4$. The $(1,1)$ -entries give $9 = 3a + b$, so $b = -3$. Now check every entry of $4\mathbf{A} - 3\mathbf{I}_3$:

$$4\mathbf{A} - 3\mathbf{I}_3 = \begin{pmatrix} 12-3 & 8 & -8 \\ -8 & -4-3 & 8 \\ -8 & -8 & 12-3 \end{pmatrix} = \begin{pmatrix} 9 & 8 & -8 \\ -8 & -7 & 8 \\ -8 & -8 & 9 \end{pmatrix} = \mathbf{A}^2.$$

So $(\mathbf{I}_3, \mathbf{A}, \mathbf{A}^2)$ is dependent, and $d = 2$. By [Proposition 9.5.4](#),

$$m_{\mathbf{A}} = x^2 - 4x + 3 = (x-1)(x-3).$$

This fits [Theorem 9.5.3](#): Example (Diagonalizing a 3×3 Matrix with a Repeated Eigenvalue) found the eigenvalues 1 and 3, and $p_{\mathbf{A}} = (x-1)^2(x-3)$. Once again the repeated eigenvalue 1 appears only once in $m_{\mathbf{A}}$. Section 8 explains that this is exactly why $\mathbf{A}$ was diagonalizable.

Method 2: eigenvalues and trial exponents. Suppose p_T splits, $p_T = (x - \lambda_1)^{a_1} \cdots (x - \lambda_k)^{a_k}$ with distinct λ_i . By [Theorem 9.5.3](#), every $x - \lambda_i$ divides m_T . If we find **any** annihilating polynomial of the form $q = (x - \lambda_1)^{t_1} \cdots (x - \lambda_k)^{t_k}$, then $m_T \mid q$. By [Lemma 9.5.2](#), $m_T = (x - \lambda_1)^{s_1} \cdots (x - \lambda_k)^{s_k}$ with $1 \leq s_i \leq t_i$, so only finitely many candidates remain, and we test them from the smallest degree up. The next section proves that $q = p_T$ always annihilates T , so the search always succeeds with $t_i \leq a_i$. Here we verify that directly.

Example. The Minimal Polynomial from the Eigenvalues

Let $\mathbf{A} = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 3 & 1 \\ 1 & 0 & 2 \end{pmatrix} \in M_3(\mathbb{R})$, with $p_{\mathbf{A}} = (x-1)(x-3)^2$ (Example (A 3×3 Characteristic Polynomial)). Find $m_{\mathbf{A}}$.

Solution. By [Theorem 9.5.3](#), both $x-1$ and $x-3$ divide $m_{\mathbf{A}}$, so the candidate of least degree is $(x-1)(x-3)$. With

$$\mathbf{A} - \mathbf{I} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \mathbf{A} - 3\mathbf{I} = \begin{pmatrix} -1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix},$$

the product is

$$(\mathbf{A} - \mathbf{I})(\mathbf{A} - 3\mathbf{I}) = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \neq \mathbf{O}.$$

So $m_{\mathbf{A}} \neq (x-1)(x-3)$. Raise one exponent and try $(x-1)(x-3)^2$ (had this failed, the other candidate of degree 3, namely $(x-1)^2(x-3)$, would come next). Polynomials in $\mathbf{A}$ commute ([Theorem 6.7.1 \(c\)](#)), so we can multiply the matrix just found by $\mathbf{A} - 3\mathbf{I}$ on the right:

$$(\mathbf{A} - \mathbf{I})(\mathbf{A} - 3\mathbf{I})^2 = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ -2+2 & 0 & 2-2 \\ 0 & 0 & 0 \end{pmatrix} = \mathbf{O}.$$

So $m_{\mathbf{A}} \mid (x-1)(x-3)^2$, and by [Lemma 9.5.2](#), $m_{\mathbf{A}} = (x-1)^s(x-3)^t$ with $1 \leq s \leq 1$ and $1 \leq t \leq 2$. The case $t = 1$ was excluded, so

$$m_{\mathbf{A}} = (x-1)(x-3)^2 = p_{\mathbf{A}}.$$

In Section 3 we found $g(3) = 1 < 2 = a(3)$ for this matrix. The exponent 2 of $x-3$ in $m_{\mathbf{A}}$ is the polynomial trace of the same shortage of eigenvectors.

The product in Method 2 need not be multiplied out completely: to rule out a candidate it is enough to find **one** nonzero entry, and to confirm one, the factored form usually makes the zero visible.

9.5.4 Similar matrices and block diagonal matrices

The minimal polynomial belongs to the operator, not to a basis. That is what makes it an invariant of similarity.

Theorem 9.5.5. Similar Matrices Have the Same Minimal Polynomial

Let V be finite-dimensional with a basis $\mathcal{B}$, and let $T \in \mathcal{L}(V)$. Then $m_T = m_{[T]_{\mathcal{B}}^{\mathcal{B}}}$. If $\mathbf{A}, \mathbf{B} \in M_n(F)$ are similar, then $m_{\mathbf{A}} = m_{\mathbf{B}}$.

Proof. By Corollary 4.1.3, $[p(T)]_{\mathcal{B}}^{\mathcal{B}} = p([T]_{\mathcal{B}}^{\mathcal{B}})$ for every $p \in F[x]$. An operator is zero exactly when its matrix is zero (Theorem 4.1.4), so $p(T) = 0$ if and only if $p([T]_{\mathcal{B}}^{\mathcal{B}}) = \mathbf{O}$. Thus T and $[T]_{\mathcal{B}}^{\mathcal{B}}$ have the same ideal of annihilating polynomials, and hence the same monic generator. If $\mathbf{B} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$, then $p(\mathbf{B}) = \mathbf{P}^{-1}p(\mathbf{A})\mathbf{P}$ by Proposition 4.2.6 (c), so again $p(\mathbf{A}) = \mathbf{O}$ if and only if $p(\mathbf{B}) = \mathbf{O}$, and $m_{\mathbf{A}} = m_{\mathbf{B}}$. ■

The theorem gives a quick nonsimilarity test. For instance $\mathbf{I}_2$ and $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ have the same characteristic polynomial, but $m_{\mathbf{I}_2} = x - 1 \neq (x - 1)^2 = m_{\mathbf{J}}$, so they are not similar.

Chapter 8 showed that a block diagonal matrix computes polynomials blockwise: $p(\mathbf{A} \oplus \mathbf{B}) = p(\mathbf{A}) \oplus p(\mathbf{B})$ (Theorem 8.1.4 (b)). So a polynomial kills $\mathbf{A} \oplus \mathbf{B}$ exactly when it kills both blocks. In the language of ideals, the answer is the least common multiple.

Proposition 9.5.6. Minimal Polynomial of a Block Diagonal Matrix

Let $\mathbf{A} \in M_k(F)$ and $\mathbf{B} \in M_l(F)$ with $k, l \geq 1$. Then $m_{\mathbf{A} \oplus \mathbf{B}} = \text{lcm}(m_{\mathbf{A}}, m_{\mathbf{B}})$.

Proof. Let $p \in F[x]$. By Theorem 8.1.4 (b), $p(\mathbf{A} \oplus \mathbf{B}) = p(\mathbf{A}) \oplus p(\mathbf{B})$, which is zero if and only if $p(\mathbf{A}) = \mathbf{O}$ and $p(\mathbf{B}) = \mathbf{O}$. By Theorem 9.5.1, this holds if and only if $p \in \langle m_{\mathbf{A}} \rangle \cap \langle m_{\mathbf{B}} \rangle$. So $I_{\mathbf{A} \oplus \mathbf{B}} = \langle m_{\mathbf{A}} \rangle \cap \langle m_{\mathbf{B}} \rangle$. This ideal contains $m_{\mathbf{A} \oplus \mathbf{B}} \neq 0$, and by Definition 6.2.4 its monic generator is $\text{lcm}(m_{\mathbf{A}}, m_{\mathbf{B}})$. By Definition 9.5.1 its monic generator is also $m_{\mathbf{A} \oplus \mathbf{B}}$, and the monic generator is unique (Theorem 6.2.2). ■

For example, $\text{diag}(1, 1, 2) = \mathbf{I}_2 \oplus (2)$ has $m = \text{lcm}(x - 1, x - 2) = (x - 1)(x - 2)$, as computed above. And $\mathbf{J} \oplus (1)$ has $m = \text{lcm}((x - 1)^2, x - 1) = (x - 1)^2$: a block can contribute a factor that the other block already contains, and then the factor is not repeated. This is the difference from the characteristic polynomial, which multiplies: $p_{\mathbf{A} \oplus \mathbf{B}} = p_{\mathbf{A}} p_{\mathbf{B}}$.

Warning. Equal minimal polynomials do not make matrices similar. $\text{diag}(1, 1, 2)$ and $\text{diag}(1, 2, 2)$ both have minimal polynomial $(x - 1)(x - 2)$, by Proposition 9.5.6. But their characteristic polynomials $(x - 1)^2(x - 2)$ and $(x - 1)(x - 2)^2$ differ, so they are not similar (Theorem 7.10.3).

Remark. Even the minimal and characteristic polynomials **together** do not decide similarity. With $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, the matrices $\mathbf{J} \oplus \mathbf{J}$ and $\mathbf{J} \oplus \mathbf{I}_2$ in $M_4(F)$ both have characteristic polynomial $(x - 1)^4$ and, by Proposition 9.5.6, minimal polynomial $(x - 1)^2$, as $\text{lcm}((x - 1)^2, (x - 1)^2)$ and $\text{lcm}((x - 1)^2, x - 1)$ are both $(x - 1)^2$. Yet $(\mathbf{J} \oplus \mathbf{J}) - \mathbf{I}_4$ has rank 2 and $(\mathbf{J} \oplus \mathbf{I}_2) - \mathbf{I}_4$ has rank 1; if $\mathbf{B} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$, then $\mathbf{B} - \mathbf{I} = \mathbf{P}^{-1}(\mathbf{A} - \mathbf{I})\mathbf{P}$, so these ranks would have to agree (Proposition 4.2.6 (a)), and the two matrices are not similar. The invariant that does decide similarity is the subject of Chapter 10.

9.5.5 Exercises

9.5.5.1 A. Check your understanding

Exercise. A1

- (a) Define the minimal polynomial of an operator T on a finite-dimensional space, and give its two equivalent descriptions.
- (b) True or false: $m_{\mathbf{A}} = p_{\mathbf{A}}$ for every $\mathbf{A} \in M_n(F)$. Justify your answer.
- (c) State the relation between the roots of m_T and the eigenvalues of T .
- (d) Let $\mathbf{A} \neq \mathbf{O}$ satisfy $\mathbf{A}^3 = \mathbf{O}$. Which polynomials can $m_{\mathbf{A}}$ be?
- (e) True or false: if $m_{\mathbf{A}} = m_{\mathbf{B}}$, then $\mathbf{A} \sim \mathbf{B}$. Justify your answer.
- (f) Explain why multiplication by x on $F[x]$ has no minimal polynomial.

Solution.

- (a) m_T is the unique monic polynomial with $\{p : p(T) = 0\} = \langle m_T \rangle$; equivalently, the monic polynomial of least degree with $m_T(T) = 0$ (Definition 9.5.1).
- (b) False. For $\mathbf{I}_2$, $m = x - 1$ and $p = (x - 1)^2$.
- (c) They coincide: $m_T(\lambda) = 0$ if and only if λ is an eigenvalue of T (Theorem 9.5.3).
- (d) By Theorem 9.5.1, $m_{\mathbf{A}} \mid x^3$, so $m_{\mathbf{A}} \in \{1, x, x^2, x^3\}$ by Lemma 9.5.2. It is not 1 (as $\mathbf{I} \neq \mathbf{O}$) and not x (as $\mathbf{A} \neq \mathbf{O}$). So $m_{\mathbf{A}} = x^2$ or $m_{\mathbf{A}} = x^3$, and both occur: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and the matrix $\mathbf{N}$ of the Quick check.
- (e) False. $\text{diag}(1, 1, 2)$ and $\text{diag}(1, 2, 2)$ have the same minimal polynomial but different characteristic polynomials.
- (f) For $S(f) = xf$, we have $p(S)(1) = p$, so $p(S) \neq 0$ for all $p \neq 0$. The ideal I_S is $\{0\}$ and has no monic generator. The space $F[x]$ is infinite-dimensional, so the definition does not apply.

9.5.5.2 B. Practice

Exercise. B1: Computing minimal polynomials

Find the minimal polynomial of each real matrix.

- (a) $\mathbf{A}_1 = \begin{pmatrix} 4 & -1 \\ 1 & 2 \end{pmatrix}$.
- (b) $\mathbf{A}_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.
- (c) $\mathbf{A}_3 = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$, given that $p_{\mathbf{A}_3} = (x - 1)^2(x - 2)$.

(d) $\mathbf{A}_4 = \begin{pmatrix} 2 & 1 & 1 \\ -1 & 0 & -1 \\ 1 & 1 & 2 \end{pmatrix}$, given that $p_{\mathbf{A}_4} = (x-1)^2(x-2)$.

Hence decide whether $\mathbf{A}_3$ and $\mathbf{A}_4$ are similar.

Solution.

- (a) $\mathbf{A}_1$ is not scalar, so $\deg m_{\mathbf{A}_1} \geq 2$. Here $\text{tr } \mathbf{A}_1 = 6$ and $\det \mathbf{A}_1 = 9$, and $\mathbf{A}_1^2 = \begin{pmatrix} 15 & -6 \\ 6 & 3 \end{pmatrix} = 6\mathbf{A}_1 - 9\mathbf{I}_2$, as one checks entry by entry. By [Proposition 9.5.4](#), $m_{\mathbf{A}_1} = x^2 - 6x + 9 = (x-3)^2$.
- (b) $\mathbf{A}_2$ is not scalar. Every entry of $\mathbf{A}_2^2$ is $1+1+1=3$, so $\mathbf{A}_2^2 = 3\mathbf{A}_2$. By [Proposition 9.5.4](#), $m_{\mathbf{A}_2} = x^2 - 3x = x(x-3)$.
- (c) By [Theorem 9.5.3](#), $(x-1)(x-2) \mid m_{\mathbf{A}_3}$. First candidate:

$$\begin{aligned} (\mathbf{A}_3 - \mathbf{I})(\mathbf{A}_3 - 2\mathbf{I}) &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & -1 & -1 \\ -1 & -1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & -1 & -1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \neq \mathbf{O}. \end{aligned}$$

Next candidate: multiplying this on the left by $\mathbf{A}_3 - \mathbf{I}$, the rows of the result are $(1, 1, 1)\mathbf{M}$, $(0, 0, -1)\mathbf{M}$, and $(-1, -1, 0)\mathbf{M}$, where $\mathbf{M}$ is the matrix just found. Since the rows of $\mathbf{M}$ sum to zero and its third row is zero, all three products are $\mathbf{O}$. So $(\mathbf{A}_3 - \mathbf{I})^2(\mathbf{A}_3 - 2\mathbf{I}) = \mathbf{O}$, and by [Lemma 9.5.2](#), $m_{\mathbf{A}_3} = (x-1)^2(x-2)$.

- (d) Again $(x-1)(x-2) \mid m_{\mathbf{A}_4}$, and

$$(\mathbf{A}_4 - \mathbf{I})(\mathbf{A}_4 - 2\mathbf{I}) = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ -1 & -2 & -1 \\ 1 & 1 & 0 \end{pmatrix} = \mathbf{O},$$

since each column of the second matrix has entries summing to 0 and each row of the first is a multiple of $(1, 1, 1)$. So $m_{\mathbf{A}_4} = (x-1)(x-2)$.

Hence $m_{\mathbf{A}_3} \neq m_{\mathbf{A}_4}$, and by [Theorem 9.5.5](#) $\mathbf{A}_3$ and $\mathbf{A}_4$ are **not** similar, although their characteristic polynomials agree. (This matches Exercise (B1: Computing multiplicities), where the same two matrices appear as $\mathbf{A}_2$ and $\mathbf{A}_3$, with $g(1) = 1$ for the first and $g(1) = 2$ for the second.)

Exercise. B2: Operators with $T^2 = T$

Let $V \neq \{0\}$ be finite-dimensional and $T \in \mathcal{L}(V)$ with $T^2 = T$.

- (a) Show that $m_T \in \{x, x-1, x(x-1)\}$.
- (b) Show that $m_T = x$ exactly when $T = 0$, and $m_T = x-1$ exactly when $T = \text{id}_V$.
- (c) What is m_T on $V = \{0\}$?

Solution.

- (a) $x^2 - x = x(x - 1)$ annihilates T , so $m_T \mid x(x - 1)$ by Theorem 9.5.1. By Lemma 9.5.2, the monic divisors are $1, x, x - 1, x(x - 1)$. Since $V \neq \{0\}$, $\deg m_T \geq 1$, so $m_T \neq 1$.
- (b) If $m_T = x$, then $T = m_T(T) = 0$. Conversely, if $T = 0$, then x annihilates T , so $m_T \mid x$, and $m_T = x$ by (a). Likewise $m_T = x - 1$ if and only if $T - \text{id}_V = 0$. In all other cases $m_T = x(x - 1)$.
- (c) On $V = \{0\}$, $1(T) = \text{id}_V = 0$, so $m_T = 1$.

Exercise. B3: Companion matrices

Let $n \geq 2$, $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$, and let $\mathbf{C} = \mathbf{C}(p)$ be its companion matrix (Exercise (C1: Companion matrices)).

- (a) Show that $\mathbf{C}\mathbf{e}_k = \mathbf{e}_{k+1}$ for $1 \leq k \leq n - 1$, so $\mathbf{C}^k\mathbf{e}_1 = \mathbf{e}_{k+1}$ for $0 \leq k \leq n - 1$.
- (b) Deduce that no nonzero polynomial of degree less than n annihilates $\mathbf{C}$.
- (c) Show that $p(\mathbf{C})\mathbf{e}_1 = \mathbf{0}$, and hence $p(\mathbf{C})\mathbf{e}_{k+1} = \mathbf{0}$ for all $k \leq n - 1$.
- (d) Deduce that $m_{\mathbf{C}} = p = p_{\mathbf{C}}$.

Solution.

- (a) Column k of $\mathbf{C}$, for $k \leq n - 1$, has a single 1 in row $k + 1$, so $\mathbf{C}\mathbf{e}_k = \mathbf{e}_{k+1}$. By induction on k , $\mathbf{C}^k\mathbf{e}_1 = \mathbf{C}(\mathbf{C}^{k-1}\mathbf{e}_1) = \mathbf{C}\mathbf{e}_k = \mathbf{e}_{k+1}$.
- (b) Let $q = \sum_{k=0}^d b_k x^k \neq 0$ with $d \leq n - 1$. By (a), $q(\mathbf{C})\mathbf{e}_1 = \sum_k b_k \mathbf{C}^k\mathbf{e}_1 = \sum_k b_k \mathbf{e}_{k+1}$, which is not $\mathbf{0}$ because some $b_k \neq 0$. So $q(\mathbf{C}) \neq \mathbf{0}$.
- (c) By (a), $\mathbf{C}^n\mathbf{e}_1 = \mathbf{C}\mathbf{e}_n$, the last column $(-a_0, \dots, -a_{n-1}) = -\sum_{k=0}^{n-1} a_k \mathbf{e}_{k+1}$. Hence

$$p(\mathbf{C})\mathbf{e}_1 = \mathbf{C}^n\mathbf{e}_1 + \sum_{k=0}^{n-1} a_k \mathbf{C}^k\mathbf{e}_1 = -\sum_k a_k \mathbf{e}_{k+1} + \sum_k a_k \mathbf{e}_{k+1} = \mathbf{0}.$$

For $k \leq n - 1$, polynomials in $\mathbf{C}$ commute (Theorem 6.7.1 (c)), so $p(\mathbf{C})\mathbf{e}_{k+1} = p(\mathbf{C})\mathbf{C}^k\mathbf{e}_1 = \mathbf{C}^k p(\mathbf{C})\mathbf{e}_1 = \mathbf{0}$.

- (d) By (c), $p(\mathbf{C})$ kills the standard basis, so $p(\mathbf{C}) = \mathbf{0}$ and $m_{\mathbf{C}} \mid p$. By (b), $\deg m_{\mathbf{C}} \geq n = \deg p$. Two monic polynomials, one dividing the other, with $\deg m_{\mathbf{C}} \geq \deg p$, are equal (Proposition 6.1.2 (c), (d)). So $m_{\mathbf{C}} = p$, and $p = p_{\mathbf{C}}$ by Exercise (C1: Companion matrices) (b). Every monic polynomial of degree $n \geq 2$ is therefore the minimal polynomial of some $n \times n$ matrix.

9.5.5.3 C. Going deeper

Exercise. C1: Cyclic vectors

Let $\dim V = n \geq 1$ and $T \in \mathcal{L}(V)$. A vector v is a **cyclic vector** for T if $(v, Tv, \dots, T^{n-1}v)$ is a basis of V .

- (a) Prove that if T has a cyclic vector, then $\deg m_T \geq n$.
- (b) Suppose v is cyclic and $T^n v = -(a_0 v + a_1 T v + \cdots + a_{n-1} T^{n-1} v)$. Show that the matrix

of T in the basis $(v, \dots, T^{n-1}v)$ is the companion matrix of $p = x^n + a_{n-1}x^{n-1} + \dots + a_0$ (for $n \geq 2$), and deduce $m_T = p_T = p$.

- (c) Find a cyclic vector for $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and show that $\mathbf{I}_2$ has none.

(The converse of (a), that $\deg m_T = n$ forces a cyclic vector, is proved in Chapter 10.)

Solution.

- (a) Let $q = \sum_{k=0}^d b_k x^k \neq 0$ with $d \leq n-1$. Then $q(T)v = \sum_k b_k T^k v \neq 0$, because the vectors $T^k v$, $k \leq n-1$, are independent and some $b_k \neq 0$. So $q(T) \neq 0$, and by [Theorem 9.5.1](#), $\deg m_T \geq n$.
- (b) Let $\mathcal{B} = (v, Tv, \dots, T^{n-1}v)$. For $k \leq n-2$, $T(T^k v) = T^{k+1}v$, the $(k+2)$ -th basis vector, so column $k+1$ of $[T]_{\mathcal{B}}$ is $\mathbf{e}_{k+2}$. The last column is $[T^n v]_{\mathcal{B}} = (-a_0, \dots, -a_{n-1})$. This is $\mathbf{C}(p)$. By [Theorem 9.5.5](#) and [Exercise \(B3: Companion matrices\)](#) (d), $m_T = m_{\mathbf{C}(p)} = p$. By Definition 7.10.2 and [Exercise \(C1: Companion matrices\)](#) (b), $p_T = p_{\mathbf{C}(p)} = p$. (For $n=1$, $Tv = -a_0 v$ and $T = -a_0 \text{id}_V$, so $m_T = p_T = x + a_0$ directly.)
- (c) $\mathbf{J}\mathbf{e}_2 = (1, 1)$, and $(\mathbf{e}_2, (1, 1))$ is independent, so $\mathbf{e}_2$ is cyclic. For $\mathbf{I}_2$, every $\mathbf{v}$ has $\mathbf{I}_2 \mathbf{v} = \mathbf{v}$, so $(\mathbf{v}, \mathbf{I}_2 \mathbf{v})$ is dependent. This matches (a): $\deg m_{\mathbf{I}_2} = 1 < 2$.

Exercise. C2: Minimal polynomials of the pieces

Let V be finite-dimensional, $T \in \mathcal{L}(V)$, and U a T -invariant subspace, with restriction $T|_U$ and induced operator $\bar{T}$ on V/U (Definition 9.1.2).

- (a) Prove that $p(T|_U) = p(T)|_U$ and $p(\bar{T})(v+U) = p(T)v + U$ for every $p \in F[x]$.
- (b) Deduce that $m_{T|_U} \mid m_T$ and $m_{\bar{T}} \mid m_T$.
- (c) Prove that $m_T \mid m_{T|_U} m_{\bar{T}}$.
- (d) For $\mathbf{J} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U = \text{span}(\mathbf{e}_1)$, compute all three minimal polynomials, and show that m_T need not equal $\text{lcm}(m_{T|_U}, m_{\bar{T}})$.

Hint: for (c), apply $m_{\bar{T}}(T)$ to v and ask where the result lies.

Solution.

- (a) First, $(T|_U)^k = T^k|_U$ by induction on k : for $u \in U$, $(T|_U)^{k+1}u = T|_U((T|_U)^k u) = T(T^k u) = T^{k+1}u$. Taking linear combinations, $p(T|_U)u = p(T)u$. For the quotient, $\bar{T}^k(v+U) = T^k v + U$ by the same induction, using Definition 9.1.2 (b) at each step, and $p(\bar{T})(v+U) = \sum_k c_k (T^k v + U) = p(T)v + U$ by the coset operations (Theorem 4.4.4).
- (b) By (a), $m_T(T|_U) = m_T(T)|_U = 0$ and $m_T(\bar{T})(v+U) = 0 + U$ for all v . By [Theorem 9.5.1](#), applied to $T|_U \in \mathcal{L}(U)$ and to $\bar{T} \in \mathcal{L}(V/U)$, both finite-dimensional, $m_{T|_U} \mid m_T$ and $m_{\bar{T}} \mid m_T$.
- (c) Let $v \in V$. By (a), $m_{\bar{T}}(T)v + U = m_{\bar{T}}(\bar{T})(v+U) = 0 + U$, so $u := m_{\bar{T}}(T)v \in U$. By (a) again, $m_{T|_U}(T)u = m_{T|_U}(T|_U)u = 0$. Hence $(m_{T|_U} m_{\bar{T}})(T)v = m_{T|_U}(T) m_{\bar{T}}(T)v = 0$ (Theorem 6.7.1 (b)). As v was arbitrary, $m_{T|_U} m_{\bar{T}}$ annihilates T , and $m_T \mid m_{T|_U} m_{\bar{T}}$ by [Theorem 9.5.1](#).

- (d) $\mathbf{J}\mathbf{e}_1 = \mathbf{e}_1$, so $T|_U = \text{id}_U$ and $m_{T|_U} = x - 1$. The quotient F^2/U has basis $\mathbf{e}_2 + U$, and $\bar{T}(\mathbf{e}_2 + U) = (1, 1) + U = \mathbf{e}_2 + U$, so $\bar{T} = \text{id}$ and $m_{\bar{T}} = x - 1$. But $m_{\mathbf{J}} = (x - 1)^2$, computed earlier. So $m_{\mathbf{J}} = m_{T|_U} m_{\bar{T}}$, while $\text{lcm}(m_{T|_U}, m_{\bar{T}}) = x - 1 \neq m_{\mathbf{J}}$. Compare [Proposition 9.5.6](#): when U has an invariant complement the lcm is right, but in general it is not.