

6.7 Polynomials of an Operator

Chapter 2 taught us to substitute an operator into a polynomial: for $T \in \mathcal{L}(V)$ and $p \in F[x]$, the operator $p(T)$ replaces each x^k by T^k (Definition 2.4.2). That section used the idea for a few examples. With the arithmetic of this chapter in hand, the idea becomes a method. Divisibility, ideals, and Bézout's identity in $F[x]$ turn into statements about T : every operator on a finite-dimensional space satisfies a polynomial equation, the polynomials it satisfies form an ideal, and a factorization of such a polynomial into coprime pieces splits the space. The last statement, the kernel splitting lemma, is the engine that Chapter 9 will run to take operators apart.

6.7.1 Evaluating at an operator

Fix $T \in \mathcal{L}(V)$, where V is any vector space over F . Theorem 2.4.3 already says that substituting T respects sums and products of polynomials, and that any two polynomials in T commute. The new point of view is to treat “substitute T ” as a single map from $F[x]$ to $\mathcal{L}(V)$, and to ask what it preserves. Both sides are vector spaces, and both have a multiplication. The map respects all of the structure.

Theorem 6.7.1. Evaluation at an Operator

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

$$F[x] \rightarrow \mathcal{L}(V), \quad p \mapsto p(T),$$

has the following properties.

- (a) It is **linear**: $(cp + q)(T) = cp(T) + q(T)$ for all $p, q \in F[x]$ and $c \in F$.
- (b) It is **multiplicative** and sends 1 to id_V : $(pq)(T) = p(T)q(T)$ and $1(T) = \text{id}_V$.
- (c) Its image $\{p(T) : p \in F[x]\}$ is a subspace of $\mathcal{L}(V)$, closed under composition, in which any two operators commute.
- (d) If $S \in \mathcal{L}(V)$ commutes with T , then S commutes with $p(T)$ for every $p \in F[x]$.

Proof.

- (a) Let $p = \sum_k a_k x^k$ and $q = \sum_k b_k x^k$. The coefficient of x^k in $cp + q$ is $ca_k + b_k$, so by Definition 2.4.2 and the vector space laws in $\mathcal{L}(V)$ (Theorem 2.4.1),

$$(cp + q)(T) = \sum_k (ca_k + b_k)T^k = c \sum_k a_k T^k + \sum_k b_k T^k = cp(T) + q(T).$$

- (b) The product rule is Theorem 2.4.3 (b). The constant polynomial 1 gives $1 \cdot T^0 = \text{id}_V$.
- (c) The image of a linear map is a subspace (Theorem 2.2.2). For polynomials p, q , the composite $p(T)q(T)$ equals $(pq)(T)$ by (b), so it lies in the image, and $p(T)q(T) = q(T)p(T)$ by Theorem 2.4.3 (c).
- (d) Suppose $ST = TS$. We show $ST^k = T^k S$ by induction on k . For $k = 0$, both sides are S . If $ST^k = T^k S$, then by associativity (Theorem 2.4.2)

$$ST^{k+1} = (ST^k)T = T^k(ST) = T^k(TS) = T^{k+1}S.$$

For $p = \sum_k a_k x^k$, distributivity (Theorem 2.4.2) gives $Sp(T) = \sum_k a_k ST^k = \sum_k a_k T^k S = p(T)S$.



Parts (a) and (b) together say that $p \mapsto p(T)$ is a **homomorphism of algebras**: it translates every identity built from sums, scalar multiples, and products of polynomials into the same identity for operators. (This map should not be confused with the evaluation map $V \rightarrow V^{**}$ of Chapter 5; here we evaluate polynomials, not functionals.) Part (d) is what we will use most. It says that anything commuting with T commutes with the whole family of polynomials in T .

For matrices nothing new is needed. If V is finite-dimensional with basis $\mathcal{B}$, then $[p(T)]_{\mathcal{B}}^{\mathcal{B}} = p([T]_{\mathcal{B}}^{\mathcal{B}})$ by Corollary 4.1.3. So every statement in this section holds verbatim for $\mathbf{A} \in M_n(F)$, applied to the operator $T_{\mathbf{A}}$.

Example. Two Ways to Evaluate

Let $\mathbf{A} = \begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix} \in M_2(\mathbb{Q})$. Compute $p(\mathbf{A})$ for $p = x^2 - 4x + 4$ and $q = x^2 - 3x$, once by expanding and once by factoring.

Solution. Expanding. $\mathbf{A}^2 = \begin{pmatrix} 9-1 & 3+1 \\ -3-1 & -1+1 \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ -4 & 0 \end{pmatrix}$. Hence

$$p(\mathbf{A}) = \begin{pmatrix} 8-12+4 & 4-4 \\ -4+4 & 0-4+4 \end{pmatrix} = \mathbf{O},$$

$$q(\mathbf{A}) = \begin{pmatrix} 8-9 & 4-3 \\ -4+3 & 0-3 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & -3 \end{pmatrix}.$$

Factoring. $p = (x-2)^2$, so $p(\mathbf{A}) = (\mathbf{A}-2\mathbf{I})^2$ by Theorem 6.7.1 (b). Here $\mathbf{A}-2\mathbf{I} = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$, whose square is $\begin{pmatrix} 1-1 & 1-1 \\ -1+1 & -1+1 \end{pmatrix} = \mathbf{O}$. Likewise $q = x(x-3)$, so

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

in agreement with the expansion. The factored form showed at a glance why $p(\mathbf{A}) = \mathbf{O}$: the matrix $\mathbf{A} - 2\mathbf{I}$ squares to zero.

Warning. A product of polynomials in T can vanish without either factor vanishing. In $F[x]$, $pq = 0$ forces $p = 0$ or $q = 0$ (Corollary 0.8.4). Evaluation at T does not carry this over. For the projection $P(x, y) = (x, 0)$ on F^2 , the polynomials $p = x$ and $q = x - 1$ give $p(P)q(P) = P^2 - P = 0$, while $p(P) = P \neq 0$ and $q(P) = P - \text{id} \neq 0$. The map $p \mapsto p(T)$ respects products, but it is not injective, and it is exactly its kernel that makes this possible.

6.7.2 Annihilating polynomials

In Chapter 2 we saw operators satisfying polynomial equations: a projection satisfies $P^2 - P = 0$, the rotation of $\mathbb{R}^2$ by a right angle satisfies $R^2 + \text{id} = 0$ (Example (Operators That Satisfy a Polynomial)), and differentiation on $F[x]_{\leq n}$ satisfies $D^{n+1} = 0$ (Example (Differentiation Is Nilpotent)). Each such equation is a nonzero polynomial in the kernel of $p \mapsto p(T)$. Does every operator have one? We need a word for these polynomials.

Definition 6.7.1. Annihilating Polynomial

Let $T \in \mathcal{L}(V)$. A polynomial $p \in F[x]$ **annihilates** T if $p(T) = 0$, the zero operator on V .

For example, $x^2 - x$ annihilates every projection, $x^2 + 1$ annihilates the rotation R , and the zero polynomial annihilates every operator. On the zero space $V = \{0\}$, even the constant 1 annihilates T , because $1(T) = \text{id}_V$ is the zero map there. On $V \neq \{0\}$, a nonzero constant c never annihilates, since $c \text{id}_V \neq 0$. (The word “annihilate” is also used for the annihilator U^0 of Chapter 5; the two uses share the idea “sends to zero” and nothing more.)

In finite dimension a counting argument settles existence. The space $\mathcal{L}(V)$ is finite-dimensional, so the powers of T cannot all be independent.

Theorem 6.7.2. Every Operator Satisfies a Polynomial

Let V be a finite-dimensional vector space over F with $\dim V = n$, and let $T \in \mathcal{L}(V)$. Then there is a **nonzero** $p \in F[x]$ with $\deg p \leq n^2$ and $p(T) = 0$. The same holds for every $\mathbf{A} \in M_n(F)$.

Proof. If $n = 0$, the constant 1 works, as noted above. Let $n \geq 1$. By Theorem 4.1.4, $\dim \mathcal{L}(V) = n \cdot n = n^2$. The list $(\text{id}_V, T, T^2, \dots, T^{n^2})$ in $\mathcal{L}(V)$ has length $n^2 + 1 > n^2$, so it is linearly dependent by Theorem 1.6.3 (a). Hence there are $a_0, \dots, a_{n^2} \in F$, **not all zero**, with $a_0 \text{id}_V + a_1 T + \dots + a_{n^2} T^{n^2} = 0$. The polynomial $p = a_0 + a_1 x + \dots + a_{n^2} x^{n^2}$ is nonzero, has degree at most n^2 , and satisfies $p(T) = 0$ by Definition 2.4.2. For $\mathbf{A} \in M_n(F)$, apply the same argument in $M_n(F)$, which has dimension n^2 (Example (Dimensions of the Running Examples)).

■

The bound n^2 is crude. In Chapter 9, the Cayley–Hamilton Theorem will produce an annihilating polynomial of degree exactly n . The finite dimension is essential: on $F[x]$, let S be multiplication by x , $S(f) = xf$. Then $S^k(1) = x^k$, so $p(S)(1) = p$ for every $p \in F[x]$, and $p(S) \neq 0$ whenever $p \neq 0$.

The proof is also an algorithm: search for the first power of $\mathbf{A}$ that is a combination of the earlier ones. This is a question about linear dependence, which elimination answers (Theorem 3.5.10).

Example. Finding an Annihilating Polynomial

Find a nonzero polynomial of least possible degree that annihilates $\mathbf{B} = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Q})$.

Solution. *Degree 1.* $\mathbf{B}$ is not a scalar multiple of $\mathbf{I}_3$ (its $(1, 2)$ -entry is nonzero), so $(\mathbf{I}_3, \mathbf{B})$ is independent, and no nonzero polynomial of degree at most 1 annihilates $\mathbf{B}$.

Degree 2. Compute

$$\mathbf{B}^2 = \begin{pmatrix} 4 & 3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We look for a, b, c with $a\mathbf{I}_3 + b\mathbf{B} + c\mathbf{B}^2 = \mathbf{O}$. Reading entries: position $(1, 2)$ gives $b + 3c = 0$; position $(1, 1)$ gives $a + 2b + 4c = 0$; position $(2, 2)$ gives $a + b + c = 0$. The positions $(1, 3)$ and $(3, 3)$ repeat the $(1, 2)$ and $(2, 2)$ equations, and all other entries are $0 = 0$. With $c = 1$: $b = -3$ and $a = 2$, and indeed $2 - 6 + 4 = 0$. So

$$\mathbf{B}^2 - 3\mathbf{B} + 2\mathbf{I}_3 = \mathbf{O},$$

and $p = x^2 - 3x + 2 = (x - 1)(x - 2)$ annihilates $\mathbf{B}$. Check with the factored form: $\mathbf{B} - \mathbf{I}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $\mathbf{B} - 2\mathbf{I}_3 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, whose product is $\begin{pmatrix} 0 & 1 - 1 & 1 - 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \mathbf{O}$.

The bound of [Theorem 6.7.2](#) allowed degree 9; the search stopped at degree 2.

Annihilating polynomials are far from unique: if p annihilates T , so does every multiple qp , since $(qp)(T) = q(T)p(T) = q(T) \cdot 0 = 0$. In [Example \(Finding an Annihilating Polynomial\)](#), $x^3 - 3x^2 + 2x$ annihilates $\mathbf{B}$ too. This closure under multiplication is the defining property of an ideal, and ideals of $F[x]$ are completely understood ([Theorem 6.2.2](#)).

Theorem 6.7.3. The Annihilating Polynomials Form an Ideal

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

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

- (a) I_T is an ideal of $F[x]$.
- (b) Either $I_T = \{0\}$, or there is a **unique monic** $m \in F[x]$ with $I_T = \langle m \rangle$. In the second case, for every $p \in F[x]$,

$$p(T) = 0 \iff m \mid p,$$

and m has the least degree among the nonzero polynomials annihilating T .

- (c) If V is finite-dimensional, then $I_T \neq \{0\}$, and $\deg m \leq (\dim V)^2$.

Proof.

- (a) By [Theorem 6.7.1](#) (a), I_T is the kernel of a linear map, so it is a subspace ([Theorem 2.2.1](#)); in particular it contains 0 and is closed under addition. If $p \in I_T$ and

$q \in F[x]$, then $(qp)(T) = q(T)p(T) = 0$ by [Theorem 6.7.1](#) (b), so $qp \in I_T$. By Definition 6.2.1, I_T is an ideal.

- (b) By Theorem 6.2.2, either $I_T = \{0\}$, or $I_T = \langle m \rangle$ for a unique monic m , which has least degree among the nonzero elements of I_T . In the second case, $p(T) = 0$ means $p \in \langle m \rangle$, that is, $p = qm$ for some q , that is, $m \mid p$.
- (c) By [Theorem 6.7.2](#), I_T contains a nonzero polynomial of degree at most $(\dim V)^2$. So $I_T \neq \{0\}$, and $\deg m \leq (\dim V)^2$ because m has the least degree.

■

This monic generator is one of the most important invariants of an operator. **Chapter 9** names it the **minimal polynomial** of T and relates its roots to eigenvalues; here it is simply “the monic generator of I_T ”. Part (b) turns every polynomial identity satisfied by T into a divisibility statement about one fixed polynomial.

Examples.

- **Projections.** Let P be a projection with $P \neq 0$ and $P \neq \text{id}_V$. Then $x^2 - x = x(x-1) \in I_P$, so the monic generator divides $x(x-1)$. By unique factorization (Theorem 6.3.5), its monic divisors are 1, x , $x-1$, and $x(x-1)$. The first three do not annihilate P : $1(P) = \text{id}_V \neq 0$, $x(P) = P \neq 0$, and $(x-1)(P) = P - \text{id}_V \neq 0$. So the generator is $x^2 - x$.
- **Degenerate cases.** For the identity on $V \neq \{0\}$, the generator is $x-1$; for the zero operator on $V \neq \{0\}$, it is x ; on $V = \{0\}$, it is 1.
- **The matrix B.** In [Example \(Finding an Annihilating Polynomial\)](#), no nonzero polynomial of degree at most 1 annihilates **B**, and $x^2 - 3x + 2$ does, so the generator is $x^2 - 3x + 2$.
- **Infinite dimension.** For multiplication by x on $F[x]$, we saw that $I_S = \{0\}$.

Quick check. Let $R(x, y) = (-y, x)$ be the rotation of $\mathbb{R}^2$ by a right angle. What is the monic generator of $I_R \subseteq \mathbb{R}[x]$?

Solution. $R^2 = -\text{id}$, so $x^2 + 1 \in I_R$, and the generator divides $x^2 + 1$. Over $\mathbb{R}$, $x^2 + 1$ has no root, so its only monic divisors are 1 and $x^2 + 1$ (a monic divisor of degree 1 would be $x - c$ with c a root). Since $1(R) = \text{id} \neq 0$, the generator is $x^2 + 1$.

6.7.3 Kernels of polynomials in T

The subspaces we can build from T and a polynomial p are $\ker p(T)$ and $\text{im } p(T)$. For $p = x - \lambda$, the kernel $\ker(T - \lambda \text{id}_V)$ consists of the vectors that T merely scales by λ ; for a projection, $\ker P$ and $\ker(P - \text{id}_V)$ are the two pieces of the direct sum. These subspaces have a property that general subspaces lack: T does not move vectors out of them.

Theorem 6.7.4. T Preserves Kernels and Images of Polynomials in T

- (a) Let $R, S \in \mathcal{L}(V)$ with $SR = RS$. Then $Sv \in \ker R$ for every $v \in \ker R$, and $Sw \in \text{im } R$ for every $w \in \text{im } R$.
- (b) In particular, for $T \in \mathcal{L}(V)$ and $p, q \in F[x]$, the operator $q(T)$ maps $\ker p(T)$ into $\ker p(T)$ and $\text{im } p(T)$ into $\text{im } p(T)$. Taking $q = x$: T maps $\ker p(T)$ and $\text{im } p(T)$ into

themselves.

Proof.

- (a) Let $v \in \ker R$. Then $R(Sv) = S(Rv) = S0 = 0$, so $Sv \in \ker R$. Let $w = Ru \in \operatorname{im} R$. Then $Sw = S(Ru) = R(Su) \in \operatorname{im} R$.
- (b) By [Theorem 6.7.1](#) (c), $q(T)$ commutes with $p(T)$, so (a) applies with $R = p(T)$ and $S = q(T)$. For $q = x$, $q(T) = T$.

■

In Chapter 9, a subspace that an operator maps into itself will be called an invariant subspace, and the notion will be developed properly there. For now the theorem is what matters: whenever $U = \ker p(T)$, the rule $u \mapsto Tu$ is an operator on U , and so is $u \mapsto q(T)u$.

The inclusion can fail for subspaces not built from T . For the rotation R of the check above, R moves the x -axis to the y -axis, so the x -axis is not of the form $\ker p(R)$ or $\operatorname{im} p(R)$ for any p .

6.7.4 The kernel splitting lemma

Chapter 2 contains two theorems with the same shape. A projection satisfies $P(P - \operatorname{id}_V) = 0$, and [Theorem 4.5.1](#) splits V as $\operatorname{im} P \oplus \ker P$. An involution in characteristic not 2 satisfies $(T - \operatorname{id}_V)(T + \operatorname{id}_V) = 0$, and [Theorem 4.5.5](#) splits V as $\ker(T - \operatorname{id}_V) \oplus \ker(T + \operatorname{id}_V)$. In both, a polynomial annihilating T factors into two pieces with no common factor, and V is the direct sum of the kernels of the pieces. In both, the projections turned out to be polynomials in T : P itself, and $\frac{1}{2}(\operatorname{id}_V + T)$. The general statement needs only the arithmetic of $F[x]$.

Theorem 6.7.5. Kernel Splitting Lemma

Let V be a vector space over F , let $T \in \mathcal{L}(V)$, and let $p, q \in F[x]$ be **coprime**. Choose $a, b \in F[x]$ with $ap + bq = 1$ ([Corollary 6.2.4](#)), and put

$$W = \ker(pq)(T), \quad E_1 = b(T)q(T), \quad E_2 = a(T)p(T).$$

Then:

- (a) $W = \ker p(T) \oplus \ker q(T)$;
- (b) $E_1 + E_2 = \operatorname{id}_W$, and for every $w \in W$, the splitting of w in (a) is

$$w = E_1w + E_2w, \quad E_1w \in \ker p(T), \quad E_2w \in \ker q(T);$$

so E_1 maps W into W and acts on W as the projection onto $\ker p(T)$ along $\ker q(T)$, and E_2 acts on W as the projection onto $\ker q(T)$ along $\ker p(T)$;

- (c) in particular, if $(pq)(T) = 0$, then

$$V = \ker p(T) \oplus \ker q(T),$$

and the projections of V onto the two summands along each other are the polynomials $(bq)(T)$ and $(ap)(T)$ in T .

Idea. Substitute T into Bézout's identity: $\text{id}_V = a(T)p(T) + b(T)q(T)$. Applied to a vector w , this writes $w = E_1w + E_2w$, and it does so for **every** vector of V . Now look at the pieces. ① $p(T)$ kills $E_1w = b(T)q(T)w$, because $p(T)b(T)q(T) = b(T)(pq)(T)$ and $(pq)(T)w = 0$ for $w \in W$: the factor q in E_1 combines with p to the whole product. Symmetrically $q(T)$ kills E_2w . ② If w is killed by both $p(T)$ and $q(T)$, then both pieces are 0, so $w = 0$. ③ Direct sum by the intersection criterion; the projections are read off from uniqueness. Coprimality enters only through the identity $ap + bq = 1$, and without it step ② has nothing to stand on.

Proof. Since $ap + bq = 1$, Theorem 6.7.1 gives

$$\text{id}_V = a(T)p(T) + b(T)q(T) = E_2 + E_1.$$

Throughout, polynomials in T commute with each other (Theorem 6.7.1 (c)).

The kernels lie in W . If $p(T)v = 0$, then $(pq)(T)v = q(T)p(T)v = 0$; so $\ker p(T) \subseteq W$, and likewise $\ker q(T) \subseteq W$.

The pieces. Let $w \in W$. Then $w = \text{id}_V w = E_1w + E_2w$. Moreover

$$p(T)(E_1w) = p(T)b(T)q(T)w = b(T)(pq)(T)w = b(T)0 = 0,$$

so $E_1w \in \ker p(T)$, and similarly $q(T)(E_2w) = a(T)(pq)(T)w = 0$, so $E_2w \in \ker q(T)$. Hence $W = \ker p(T) + \ker q(T)$.

The intersection. Let $v \in \ker p(T) \cap \ker q(T)$. Then $E_1v = b(T)q(T)v = 0$ and $E_2v = a(T)p(T)v = 0$, so $v = E_1v + E_2v = 0$. By Theorem 1.7.4, the sum is direct, which proves (a).

The projections. The splitting of $w \in W$ in (a) is unique (Definition 1.7.2), and we have exhibited it as $w = E_1w + E_2w$; this proves the formula in (b). In particular $E_1w \in \ker p(T) \subseteq W$, so E_1 maps W into W . As an operator on W , E_1 is linear, fixes every $u \in \ker p(T)$ (whose splitting is $u = u + 0$), and kills every vector of $\ker q(T)$ (whose splitting is $0 + v$). By the uniqueness in Theorem 4.5.1 (b), applied to $W = \ker p(T) \oplus \ker q(T)$, it is the projection onto $\ker p(T)$ along $\ker q(T)$. Swapping the roles of p and q gives the statement for E_2 .

(c) If $(pq)(T) = 0$, then $W = V$, and (a) and (b) become the statements in (c), with $E_1 = (bq)(T)$ and $E_2 = (ap)(T)$ by Theorem 6.7.1 (b). This proves the theorem. ■

Bézout's coefficients a, b are not unique, but the projections on W are, by Theorem 4.5.1 (b). So different choices of a, b give polynomials bq that may differ, while $(bq)(T)$ always does the same thing on W . When $(pq)(T) = 0$, the lemma turns a factorization of an annihilating polynomial into a direct sum decomposition of the whole space, with explicit projections, and each summand is carried into itself by T (Theorem 6.7.4).

Example. Recovering Projections and Direct Sums

Let $P \in \mathcal{L}(V)$ be a projection. Apply Theorem 6.7.5 with $p = x$ and $q = x - 1$, and compare with Theorem 4.5.1 (a).

Solution. Coprime. $1 \cdot x + (-1)(x - 1) = 1$, so we may take $a = 1$, $b = -1$, and any common divisor of x and $x - 1$ divides 1. *Annihilating.* $(pq)(P) = P^2 - P = 0$ because P is a projection.

By Theorem 6.7.5 (c),

$$V = \ker P \oplus \ker(P - \text{id}_V),$$

with projection $E_1 = b(P)q(P) = -(P - \text{id}_V) = \text{id}_V - P$ onto $\ker P$ along $\ker(P - \text{id}_V)$, and $E_2 = a(P)p(P) = P$ onto $\ker(P - \text{id}_V)$ along $\ker P$.

To compare, note that $\ker(P - \text{id}_V) = \text{im } P$. ($\subseteq$) If $Pv = v$, then $v \in \text{im } P$. ($\supseteq$) If $v = Pu$, then $Pv = P^2u = Pu = v$. So the lemma gives $V = \text{im } P \oplus \ker P$, with P the projection onto $\text{im } P$ along $\ker P$: this is Theorem 4.5.1 (a). It also reproves Exercise (B2: The complementary projection), that $\text{id}_V - P$ is the complementary projection.

Example. Recovering the Involution Decomposition

Let F have characteristic not 2, and let $T \in \mathcal{L}(V)$ with $T^2 = \text{id}_V$. Apply Theorem 6.7.5 with $p = x - 1$ and $q = x + 1$, and compare with Theorem 4.5.5. What goes wrong in characteristic 2?

Solution. Coprime. Since $2 \neq 0$ in F (Definition 0.7.2),

$$-\frac{1}{2}(x - 1) + \frac{1}{2}(x + 1) = 1,$$

so $a = -\frac{1}{2}$ and $b = \frac{1}{2}$ work, and a common divisor of p and q divides 1. *Annihilating.* $(pq)(T) = T^2 - \text{id}_V = 0$.

By Theorem 6.7.5 (c),

$$V = \ker(T - \text{id}_V) \oplus \ker(T + \text{id}_V) = E_+ \oplus E_-,$$

and the projection onto E_+ along E_- is $b(T)q(T) = \frac{1}{2}(T + \text{id}_V)$. These are exactly the conclusions of Theorem 4.5.5. The other projection is $a(T)p(T) = \frac{1}{2}(\text{id}_V - T)$.

In characteristic 2, $x + 1 = x - 1$, so $p = q$ and $\gcd(p, q) = x - 1 \neq 1$. The lemma does not apply, and the warning after Theorem 4.5.5 shows that the conclusion really fails there.

The lemma applies just as well when neither factor is linear, and then it finds subspaces that are not visible from single vectors.

Example. A Splitting with a Repeated Factor

Let $\mathbf{A} = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Q})$. Verify that $\mathbf{A}^2(\mathbf{A} - \mathbf{I}_3) = \mathbf{O}$, and use Theorem 6.7.5 with $p = x^2$, $q = x - 1$ to split $\mathbb{Q}^3$, giving both projections as polynomials in $\mathbf{A}$.

Solution. The relation. $\mathbf{A}^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, and $\mathbf{A}^3 = \mathbf{A} \cdot \mathbf{A}^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \mathbf{A}^2$. So

$$\mathbf{A}^2(\mathbf{A} - \mathbf{I}_3) = \mathbf{A}^3 - \mathbf{A}^2 = \mathbf{O}.$$

Bézout. $x^2 = (x+1)(x-1) + 1$, so $1 \cdot x^2 + (-(x+1))(x-1) = 1$: take $a = 1$, $b = -(x+1)$. Then

$$\mathbf{E}_1 = b(\mathbf{A})q(\mathbf{A}) = -(\mathbf{A} + \mathbf{I}_3)(\mathbf{A} - \mathbf{I}_3) = \mathbf{I}_3 - \mathbf{A}^2$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\mathbf{E}_2 = a(\mathbf{A})p(\mathbf{A}) = \mathbf{A}^2.$$

The summands. $\ker \mathbf{A}^2 = \{(x, y, z) : z = 0\} = \text{span}(\mathbf{e}_1, \mathbf{e}_2)$, and $\ker(\mathbf{A} - \mathbf{I}_3)$ is cut out by $-x + y - z = 0$, $-y + z = 0$, $0 = 0$, so it is $\text{span}((0, 1, 1))$. By [Theorem 6.7.5 \(c\)](#),

$$\mathbb{Q}^3 = \text{span}(\mathbf{e}_1, \mathbf{e}_2) \oplus \text{span}((0, 1, 1)),$$

and for $\mathbf{v} = (x, y, z)$, the splitting is $\mathbf{E}_1\mathbf{v} + \mathbf{E}_2\mathbf{v} = (x, y - z, 0) + (0, z, z)$. One checks directly that $(x, y - z, 0)$ has third entry 0 and $(0, z, z)$ is a multiple of $(0, 1, 1)$.

Note that $\ker \mathbf{A} = \text{span}(\mathbf{e}_1)$ is strictly smaller than $\ker \mathbf{A}^2$. The factor $p = x^2$ could not be replaced by x : the polynomial $x(x-1)$ does not annihilate $\mathbf{A}$, since $\mathbf{A}^2 - \mathbf{A} \neq \mathbf{O}$.

Warning. Without coprimality the kernels need not fill $\ker(pq)(T)$, or even form a direct sum. Let $T = T_{\mathbf{N}}$ with $\mathbf{N} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ on F^2 , and $p = q = x$. Then $(pq)(T) = \mathbf{N}^2 = \mathbf{O}$, so $\ker(pq)(T) = F^2$. But $\ker p(T) = \ker q(T) = \ker \mathbf{N} = \text{span}(\mathbf{e}_1)$. The two kernels are equal, so their sum is not direct, and $\text{span}(\mathbf{e}_1) + \text{span}(\mathbf{e}_1) = \text{span}(\mathbf{e}_1) \neq F^2$. Here $\gcd(x, x) = x$, and no identity $ax + bx = 1$ exists, since its left side vanishes at 0.

Quick check. Let $T \in \mathcal{L}(V)$ satisfy $T^2 = 3T$, over a field with $3 \neq 0$. Split V with the lemma, and write the projection onto $\ker T$ as a polynomial in T .

Solution. $x(x-3)$ annihilates T . Since $\frac{1}{3}x - \frac{1}{3}(x-3) = 1$, $p = x$ and $q = x-3$ are coprime with $a = \frac{1}{3}$, $b = -\frac{1}{3}$. By [Theorem 6.7.5 \(c\)](#), $V = \ker T \oplus \ker(T - 3\text{id}_V)$, and the projection onto $\ker T$ along $\ker(T - 3\text{id}_V)$ is $b(T)q(T) = -\frac{1}{3}(T - 3\text{id}_V) = \text{id}_V - \frac{1}{3}T$.

In Chapter 9 the lemma is used with an annihilating polynomial factored into powers of distinct irreducibles, $m = p_1^{e_1} \cdots p_k^{e_k}$. Distinct monic irreducibles are coprime, and so are their powers, so the lemma with k factors ([Exercise \(C2: Splitting with \$k\$ coprime factors\)](#)) splits V into the pieces $\ker p_i(T)^{e_i}$. That is the primary decomposition, and the canonical forms of Chapter 10 are built on it.

6.7.5 Exercises

6.7.5.1 A. Check your understanding

Exercise. A1

- (a) State what it means that $p \mapsto p(T)$ is linear and multiplicative.
- (b) True or false: if $p(T)q(T) = 0$, then $p(T) = 0$ or $q(T) = 0$. Justify your answer.
- (c) Why does every operator on a finite-dimensional space have a nonzero annihilating polynomial? Is the same true on $F[x]$?
- (d) True or false: if p annihilates T and $p \mid q$, then q annihilates T . Justify your answer.
- (e) State the kernel splitting lemma for $(pq)(T) = 0$, and say where coprimality is used in its proof.
- (f) True or false: for every subspace U of V and every $T \in \mathcal{L}(V)$, T maps U into U . Justify your answer.

Solution.

- (a) $(cp + q)(T) = cp(T) + q(T)$ and $(pq)(T) = p(T)q(T)$ for all $p, q \in F[x]$ and $c \in F$ ([Theorem 6.7.1](#)).
- (b) False. For the projection $P(x, y) = (x, 0)$, $P(P - \text{id}) = 0$ while $P \neq 0$ and $P - \text{id} \neq 0$.
- (c) $\mathcal{L}(V)$ has dimension n^2 , so the $n^2 + 1$ operators $\text{id}_V, T, \dots, T^{n^2}$ are linearly dependent, and a dependence is a nonzero annihilating polynomial ([Theorem 6.7.2](#)). On $F[x]$, multiplication by x has no nonzero annihilating polynomial, since $p(S)(1) = p$.
- (d) True. If $q = hp$, then $q(T) = h(T)p(T) = 0$. This is the ideal property ([Theorem 6.7.3](#)).
- (e) If p, q are coprime and $(pq)(T) = 0$, then $V = \ker p(T) \oplus \ker q(T)$, and the projections are polynomials in T ([Theorem 6.7.5](#)). Coprimality gives $ap + bq = 1$, hence $\text{id}_V = a(T)p(T) + b(T)q(T)$, which both produces the splitting of each vector and shows the intersection is $\{0\}$.
- (f) False. The rotation $R(x, y) = (-y, x)$ maps the x -axis to the y -axis. The statement is true for $U = \ker p(T)$ and $U = \text{im } p(T)$ ([Theorem 6.7.4](#)).

6.7.5.2 B. Practice

Exercise. B1: A polynomial of a 2×2 matrix

Let $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} \in M_2(\mathbb{Q})$.

- (a) Compute $p(\mathbf{A})$ for $p = x^2 - 7$ and for $q = x^2 + x - 5$.
- (b) Hence show that $\mathbf{A}$ is invertible and find $\mathbf{A}^{-1}$ as a polynomial in $\mathbf{A}$.

Solution.

- (a) $\mathbf{A}^2 = \begin{pmatrix} 1+6 & 2-2 \\ 3-3 & 6+1 \end{pmatrix} = 7\mathbf{I}_2$. Hence $p(\mathbf{A}) = \mathbf{A}^2 - 7\mathbf{I}_2 = \mathbf{O}$. For q , divide: $q =$

$(x^2 - 7) + (x + 2)$, so by [Theorem 6.7.1](#) $q(\mathbf{A}) = p(\mathbf{A}) + \mathbf{A} + 2\mathbf{I}_2 = \begin{pmatrix} 3 & 2 \\ 3 & 1 \end{pmatrix}$. (Directly:

$$7\mathbf{I}_2 + \mathbf{A} - 5\mathbf{I}_2 = \mathbf{A} + 2\mathbf{I}_2.)$$

- (b) From $\mathbf{A}^2 = 7\mathbf{I}_2$, $\mathbf{A}(\frac{1}{7}\mathbf{A}) = (\frac{1}{7}\mathbf{A})\mathbf{A} = \mathbf{I}_2$. So $\mathbf{A}$ is invertible with $\mathbf{A}^{-1} = \frac{1}{7}\mathbf{A} = \begin{pmatrix} \frac{1}{7} & \frac{2}{7} \\ \frac{3}{7} & -\frac{1}{7} \end{pmatrix}$.

Exercise. B2: An annihilating polynomial by elimination

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

- Compute $\mathbf{C}^2$ and $\mathbf{C}^3$, and show that $(\mathbf{I}_3, \mathbf{C}, \mathbf{C}^2)$ is linearly independent.
- Find a linear dependence among $\mathbf{I}_3, \mathbf{C}, \mathbf{C}^2, \mathbf{C}^3$, and hence a monic polynomial p of degree 3 with $p(\mathbf{C}) = \mathbf{O}$.
- Hence show that $\mathbf{C}$ is invertible and write $\mathbf{C}^{-1}$ as a polynomial in $\mathbf{C}$.

Solution.

- (a) Multiplying out,

$$\mathbf{C}^2 = \begin{pmatrix} 0 & 2 & 4 \\ 0 & -1 & 0 \\ 1 & 2 & 3 \end{pmatrix}, \quad \mathbf{C}^3 = \mathbf{C} \cdot \mathbf{C}^2 = \begin{pmatrix} 2 & 4 & 6 \\ -1 & 0 & 1 \\ 2 & 3 & 6 \end{pmatrix}.$$

Let $a\mathbf{I}_3 + b\mathbf{C} + c\mathbf{C}^2 = \mathbf{O}$. The $(2, 1)$ -entry gives $b = 0$; the $(3, 1)$ -entry gives $c = 0$; then the $(1, 1)$ -entry gives $a = 0$. So the list is independent.

- (b) Let $a\mathbf{I}_3 + b\mathbf{C} + c\mathbf{C}^2 + d\mathbf{C}^3 = \mathbf{O}$. Reading entries: $(2, 1)$: $b - d = 0$; $(3, 1)$: $c + 2d = 0$; $(1, 1)$: $a + 2d = 0$. With $d = 1$: $b = 1$, $c = -2$, $a = -2$. Check all entries of $-2\mathbf{I}_3 + \mathbf{C} - 2\mathbf{C}^2 + \mathbf{C}^3$: row 1 is $(-2 + 0 - 0 + 2, 0 - 4 + 4, 2 - 8 + 6) = (0, 0, 0)$; row 2 is $(1 - 0 - 1, -2 + 0 + 2 + 0, -1 - 0 + 1) = (0, 0, 0)$; row 3 is $(0 - 2 + 2, 1 - 4 + 3, -2 + 2 - 6 + 6) = (0, 0, 0)$. Hence

$$p = x^3 - 2x^2 + x - 2 = (x - 2)(x^2 + 1)$$

satisfies $p(\mathbf{C}) = \mathbf{O}$. By (a) no nonzero polynomial of degree at most 2 annihilates $\mathbf{C}$, so p is the monic generator of $I_{\mathbf{C}}$ ([Theorem 6.7.3](#)).

- (c) $\mathbf{C}^3 - 2\mathbf{C}^2 + \mathbf{C} = 2\mathbf{I}_3$, that is, $\mathbf{C}(\mathbf{C}^2 - 2\mathbf{C} + \mathbf{I}_3) = (\mathbf{C}^2 - 2\mathbf{C} + \mathbf{I}_3)\mathbf{C} = 2\mathbf{I}_3$, using [Theorem 6.7.1](#) (c) for the second equality. Since $2 \neq 0$ in $\mathbb{Q}$, $\mathbf{C}$ is invertible with

$$\mathbf{C}^{-1} = \frac{1}{2}(\mathbf{C}^2 - 2\mathbf{C} + \mathbf{I}_3) = \begin{pmatrix} \frac{1}{2} & 1 & 0 \\ -1 & 0 & 1 \\ \frac{1}{2} & 0 & 0 \end{pmatrix}.$$

Exercise. B3: Operators with $T^3 = T$

Let F have characteristic not 2, and let $T \in \mathcal{L}(V)$ with $T^3 = T$.

- (a) Use [Theorem 6.7.5](#) with $p = x$ and $q = x^2 - 1$ to show $V = \ker T \oplus \ker(T^2 - \text{id}_V)$, with projection $\text{id}_V - T^2$ onto $\ker T$.
- (b) Show that $V = \ker T \oplus \ker(T - \text{id}_V) \oplus \ker(T + \text{id}_V)$.
- (c) Verify that the projections onto the three summands in (b) are $\text{id}_V - T^2$, $\frac{1}{2}(T^2 + T)$, and $\frac{1}{2}(T^2 - T)$, in the sense that these three operators sum to id_V and each maps V into the corresponding kernel.

Solution.

- (a) $x \cdot x + (-1)(x^2 - 1) = 1$: take $a = x$, $b = -1$. Then p and q are coprime, and $(pq)(T) = T^3 - T = 0$. By [Theorem 6.7.5](#) (c), $V = \ker T \oplus \ker(T^2 - \text{id}_V)$, and the projection onto $\ker T$ is $b(T)q(T) = -(T^2 - \text{id}_V) = \text{id}_V - T^2$.
- (b) Let $W = \ker(T^2 - \text{id}_V)$. Apply [Theorem 6.7.5](#) (a) with $p_1 = x - 1$, $q_1 = x + 1$, which are coprime as in [Example \(Recovering the Involution Decomposition\)](#): $W = \ker(p_1 q_1)(T) = \ker(T - \text{id}_V) \oplus \ker(T + \text{id}_V)$. Write $K_0 = \ker T$, $K_+ = \ker(T - \text{id}_V)$, $K_- = \ker(T + \text{id}_V)$. Then $V = K_0 + K_+ + K_-$ by (a). If $u_0 + u_+ + u_- = 0$ with $u_0 \in K_0$, $u_{\pm} \in K_{\pm}$, then $u_+ + u_- \in W$, so directness in (a) gives $u_0 = 0$ and $u_+ + u_- = 0$, and directness of $W = K_+ \oplus K_-$ gives $u_+ = u_- = 0$. By [Theorem 1.7.5](#) ((b) $\Rightarrow$ (a)), the sum is direct.
- (c) The sum is $\text{id}_V - T^2 + \frac{1}{2}T^2 + \frac{1}{2}T + \frac{1}{2}T^2 - \frac{1}{2}T = \text{id}_V$. Using $T^3 = T$: $T(\text{id}_V - T^2) = T - T^3 = 0$; $(T - \text{id}_V)\frac{1}{2}(T^2 + T) = \frac{1}{2}(T^3 - T) = 0$; $(T + \text{id}_V)\frac{1}{2}(T^2 - T) = \frac{1}{2}(T^3 - T) = 0$. So the three operators map V into K_0 , K_+ , K_- respectively. For $v \in V$, v is the sum of its three images, and by the uniqueness of the splitting in (b) these are the components of v . Hence each operator is the projection onto its summand along the sum of the other two.

6.7.5.3 C. Going deeper

Exercise. C1: Inverses are polynomials

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

- (a) Suppose $p(T) = 0$ for some $p \in F[x]$ with $p(0) \neq 0$. Prove that T is invertible and that $T^{-1} = g(T)$ for some $g \in F[x]$.
- (b) Deduce that if V is finite-dimensional and T is invertible, then T^{-1} is a polynomial in T .
- (c) Show that the monic generator m of I_T , for V finite-dimensional and nonzero, satisfies $m(0) \neq 0$ if and only if T is invertible.

Hint: for (b), write a nonzero annihilating polynomial as $x^k p_1$ with $p_1(0) \neq 0$.

Solution.

- (a) Write $p = c + xg_0$, where $c = p(0) \neq 0$ and $g_0 \in F[x]$. Then $0 = p(T) = c \text{id}_V + T g_0(T)$, so $T g_0(T) = -c \text{id}_V$. Put $g = -c^{-1}g_0$. Then $T g(T) = \text{id}_V$, and $g(T) T = T g(T) = \text{id}_V$ by [Theorem 6.7.1](#) (c). Hence T is invertible with $T^{-1} = g(T)$.
- (b) If $V = \{0\}$, then $T^{-1} = \text{id}_V = 1(T)$. Otherwise, by [Theorem 6.7.2](#) there is a nonzero p

with $p(T) = 0$. Let k be the least index with a nonzero coefficient in p ; then $p = x^k p_1$ with $p_1(0) \neq 0$. Now $0 = p(T) = T^k p_1(T)$. Since T is invertible, so is T^k , with inverse $(T^{-1})^k$, and composing on the left with it gives $p_1(T) = 0$. By (a), T^{-1} is a polynomial in T .

- (c) $(\Rightarrow)$ If $m(0) \neq 0$, apply (a) to m . $(\Leftarrow)$ Suppose T is invertible and $m(0) = 0$. Then $m = x m_1$ with m_1 monic of degree $\deg m - 1$, and $0 = m(T) = T m_1(T)$. Composing with T^{-1} gives $m_1(T) = 0$, so $m \mid m_1$ by Theorem 6.7.3 (b). Since $V \neq \{0\}$, m is not constant, so $m_1 \neq 0$ and $\deg m \leq \deg m_1 = \deg m - 1$ by Theorem 0.8.3, a contradiction. Hence $m(0) \neq 0$.

Exercise. C2: Splitting with k coprime factors

Let $T \in \mathcal{L}(V)$, and let $p_1, \dots, p_k \in F[x]$ be nonzero and pairwise coprime, with $k \geq 2$. Put $p = p_1 \cdots p_k$ and $W = \ker p(T)$.

- Use Theorem 6.6.4 to find $e_1, \dots, e_k \in F[x]$ with $e_i \equiv 1 \pmod{p_i}$ and $e_i \equiv 0 \pmod{p_j}$ for $j \neq i$. Show that $p \mid e_1 + \cdots + e_k - 1$ and that $p \mid p_i e_i$ for each i .
- Prove that for every $w \in W$, $w = e_1(T)w + \cdots + e_k(T)w$ with $e_i(T)w \in \ker p_i(T)$.
- Prove that $W = \ker p_1(T) \oplus \cdots \oplus \ker p_k(T)$, and that $e_i(T)$ is the identity on $\ker p_i(T)$ and zero on $\ker p_j(T)$ for $j \neq i$.
- Deduce: if $p(T) = 0$, then $V = \ker p_1(T) \oplus \cdots \oplus \ker p_k(T)$, and the projection onto the i -th summand along the others is the polynomial $e_i(T)$.

Hint: for the second divisibility in (a), use Lemma 6.6.3 (b).

Solution.

- By Theorem 6.6.4 (a), applied to the pairwise coprime moduli $p_1, \dots, p_k$ with $r_i = 1$ and $r_j = 0$ for $j \neq i$, such an e_i exists. The sum $s = e_1 + \cdots + e_k$ satisfies $s \equiv 1 \pmod{p_j}$ for each j , since exactly one summand is $\equiv 1$ and the others are $\equiv 0$. The constant 1 satisfies the same congruences, so $s \equiv 1 \pmod{p}$ by Theorem 6.6.4 (b). For the second claim, $p_j \mid e_i$ for every $j \neq i$, and these p_j are pairwise coprime, so $\prod_{j \neq i} p_j \mid e_i$ by Lemma 6.6.3 (b). Multiplying by p_i , $p \mid p_i e_i$.
- Write $e_1 + \cdots + e_k = 1 + hp$ and $p_i e_i = h_i p$. By Theorem 6.7.1, for $w \in W$,

$$\begin{aligned} e_1(T)w + \cdots + e_k(T)w &= w + h(T)p(T)w = w, \\ p_i(T)(e_i(T)w) &= h_i(T)p(T)w = 0. \end{aligned}$$

- Each $\ker p_i(T) \subseteq W$, since $p(T) = (\prod_{j \neq i} p_j)(T)p_i(T)$. With (b), $W = \ker p_1(T) + \cdots + \ker p_k(T)$. Let $u_j \in \ker p_j(T)$. For $j \neq i$, $p_j \mid e_i$, say $e_i = g p_j$, so $e_i(T)u_j = g(T)p_j(T)u_j = 0$. And $e_i = 1 + g' p_i$, so $e_i(T)u_i = u_i + g'(T)p_i(T)u_i = u_i$. This proves the second statement. Now suppose $u_1 + \cdots + u_k = 0$ with $u_j \in \ker p_j(T)$. Applying $e_i(T)$ gives $u_i = 0$, for each i . By Theorem 1.7.5 ((b) $\Rightarrow$ (a)), the sum is direct.
- If $p(T) = 0$, then $W = V$. By (c), V is the direct sum, and $e_i(T) \in \mathcal{L}(V)$ is the identity on the i -th summand and zero on the others. For $v = u_1 + \cdots + u_k$, $e_i(T)v = u_i$, which is the projection onto $\ker p_i(T)$ along the sum of the other summands. For $k = 2$ this is Theorem 6.7.5 (c).

Exercise. C3: The same rotation over $\mathbb{R}$ and over $\mathbb{C}$

Let $\mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, so that $\mathbf{A}^2 + \mathbf{I}_2 = \mathbf{O}$.

- (a) Over $\mathbb{C}$, apply [Theorem 6.7.5](#) to $T_{\mathbf{A}}$ on $\mathbb{C}^2$ with $p = x - i$ and $q = x + i$. Find both kernels and write the projection onto $\ker(\mathbf{A} - i\mathbf{I}_2)$ as a polynomial in $\mathbf{A}$.
- (b) Over $\mathbb{R}$, show that the only subspaces of $\mathbb{R}^2$ that $T_{\mathbf{A}}$ maps into themselves are $\{\mathbf{0}\}$ and $\mathbb{R}^2$. Explain why this matches the fact that $x^2 + 1$ admits no factorization into coprime nonconstant factors in $\mathbb{R}[x]$.

Solution.

- (a) $(x + i) - (x - i) = 2i$, so $\frac{i}{2}(x - i) - \frac{i}{2}(x + i) = \frac{i}{2}(-2i) = 1$: take $a = \frac{i}{2}$ and $b = -\frac{i}{2}$. So p, q are coprime, and $(pq)(\mathbf{A}) = \mathbf{A}^2 + \mathbf{I}_2 = \mathbf{O}$. By [Theorem 6.7.5](#) (c), $\mathbb{C}^2 = \ker(\mathbf{A} - i\mathbf{I}_2) \oplus \ker(\mathbf{A} + i\mathbf{I}_2)$. Solving, $(\mathbf{A} - i\mathbf{I}_2)(z, w) = (-iz - w, z - iw) = \mathbf{0}$ gives $w = -iz$, so $\ker(\mathbf{A} - i\mathbf{I}_2) = \text{span}((1, -i))$; similarly $\ker(\mathbf{A} + i\mathbf{I}_2) = \text{span}((1, i))$. The projection onto $\ker(\mathbf{A} - i\mathbf{I}_2)$ is

$$b(\mathbf{A})q(\mathbf{A}) = -\frac{i}{2}(\mathbf{A} + i\mathbf{I}_2) = \frac{1}{2}(\mathbf{I}_2 - i\mathbf{A}) = \begin{pmatrix} \frac{1}{2} & \frac{i}{2} \\ -\frac{i}{2} & \frac{1}{2} \end{pmatrix}.$$

Check: it sends $(1, -i)$ to $(\frac{1}{2} + \frac{1}{2}, -\frac{i}{2} - \frac{i}{2}) = (1, -i)$ and $(1, i)$ to $(\frac{1}{2} - \frac{1}{2}, -\frac{i}{2} + \frac{i}{2}) = \mathbf{0}$.

- (b) A subspace of $\mathbb{R}^2$ other than $\{\mathbf{0}\}$ and $\mathbb{R}^2$ has dimension 1 ([Theorem 1.6.7](#)), so it is $\text{span}(\mathbf{v})$ with $\mathbf{v} = (s, t) \neq \mathbf{0}$. If $\mathbf{A}\mathbf{v} \in \text{span}(\mathbf{v})$, then $(-t, s) = c(s, t)$ for some $c \in \mathbb{R}$, so $-t = cs$ and $s = ct$, giving $s = -c^2s$ and $t = -c^2t$. Since $1 + c^2 > 0$, $s = t = 0$, a contradiction. So only $\{\mathbf{0}\}$ and $\mathbb{R}^2$ are mapped into themselves.

Over $\mathbb{R}$, $x^2 + 1$ has no root, so its only monic divisors are 1 and $x^2 + 1$, and the only factorizations $x^2 + 1 = pq$ into monic factors have $p = 1$ or $q = 1$. The lemma then gives only $\ker p(T) \oplus \ker q(T) = \{\mathbf{0}\} \oplus \mathbb{R}^2$, and by (b) there is no finer splitting into subspaces preserved by $T_{\mathbf{A}}$ at all. Enlarging the field to $\mathbb{C}$ creates the coprime factors $x \mp i$, and with them the splitting of (a).