

## VI. Canonical forms

### VI.A. The minimal polynomial of a transformation

The statement that  $\vec{v}_0$  is an eigenvector of  $A \in M_n(\mathbb{R})$  with eigenvalue 3 can be written

$$(3\mathbb{I} - A)\vec{v}_0 = 0.$$

That is, if you plug  $A$  into the polynomial  $3 - x$ , then the resulting matrix annihilates  $\vec{v}_0$ . Is there a corresponding statement for *all* vectors  $\vec{v} \in \mathbb{R}^n$ ? That is, a polynomial into which we may plug  $A$  to get the *zero* matrix (which is the only matrix annihilating all vectors)?

Consider  $M_n(\mathbb{R})$  as a vector space over  $\mathbb{R}$  of dimension  $n^2$ .<sup>1</sup> Apparently the  $n^2 + 1$  “vectors”

$$\mathbb{I}, A, A^2, \dots, A^{(n^2)}$$

cannot all be independent. So there is a relation

$$\alpha_0\mathbb{I} + \alpha_1 A + \alpha_2 A^2 + \dots + \alpha_{(n^2)} A^{(n^2)} = 0,$$

where not all  $\alpha_i$  are zero. That is,  $A$  is “annihilated” by a polynomial  $q(x)$  of degree  $n^2$ , in the sense that  $q(A)$  is the zero matrix.

However we should (at least some of the time) be able to do better than this. If  $A$  is diagonalizable with eigenvalues  $\lambda_1, \lambda_2, \dots, \lambda_n$ , then

$$(\lambda_1\mathbb{I} - A)(\lambda_2\mathbb{I} - A) \cdots (\lambda_n\mathbb{I} - A)\vec{v} = 0$$

for all  $\vec{v} \in \mathbb{R}^n$ . (Write  $\vec{v} = \beta_1\vec{v}_1 + \dots + \beta_n\vec{v}_n$  in terms of the eigenbasis; then use the fact that all the  $(\lambda_i\mathbb{I} - A)$  commute with one another.) Multiplying this out gives a polynomial in  $A$  of degree  $n$ , not  $n^2$ .

---

<sup>1</sup>The “standard” basis of this vector space would be the matrices with 1 in the  $ij^{\text{th}}$  place and 0’s in the other places,  $i, j = 1, \dots, n$ . Clearly there are  $n^2$  of these.

Similarly, if  $A$  is of the (non-diagonalizable!) form

$$\begin{pmatrix} 0 & 1 & & * \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

then we find it satisfies  $A^n = 0$  ( $A$  is *nilpotent*). In fact, the characteristic polynomials ( $= \det(\lambda \mathbb{I} - A)$ ) in these two cases are

$$(\lambda - \lambda_1) \cdots (\lambda - \lambda_n) \quad \text{and} \quad \lambda^n,$$

so the following more general result should not surprise you:

**VI.A.1. THEOREM (Cayley-Hamilton).** *Let  $A \in M_n(F)$  be a square matrix over any field. Then  $A$  is annihilated by its own characteristic polynomial, i.e. if  $f_A(\lambda) := \det(\lambda \mathbb{I} - A)$  then  $f_A(A) = 0$ .*

**VI.A.2. REMARK.** Thus we can always do much better than  $n^2$ , since  $\deg f_A = n$ . However, the proof is not as easy as

$$\det(A\mathbb{I} - A) = \det 0 = 0.$$

This is cheating. Substituting in  $A$  before you take the determinant is not the same as doing so *after* taking the determinant. We now give two correct proofs.

**FIRST PROOF OF VI.A.1.** We need to introduce (a little more consciously than before) matrices whose entries are *polynomials in  $\lambda$* . Let  $F[\lambda]$  denote polynomials of arbitrary degree in  $\lambda$  with coefficients in  $F$ , and consider  $M \in M_n(F[\lambda])$ . The tricky thing is that we must *avoid* dividing by  $\lambda$  — polynomials are not invertible like real numbers.

One definition that involved no inverting of anything was that of the adjugate of  $A$ , whose  $ij^{\text{th}}$  entry was defined to be

$$\det\{ji^{\text{th}} \text{ minor of } A\} \times (-1)^{i+j}.$$

In §IV.C, we had from Cramer's rule (assuming  $A \in M_n(F)$ , not  $M_n(F[\lambda])$ ) the relationship

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A, \quad \text{i.e. } A \left( \frac{1}{\det A} \operatorname{adj} A \right) = \mathbb{I}.$$

Clearing the denominator yields something which still holds<sup>2</sup> for  $M$ :

$$M(\operatorname{adj} M) = (\det M)\mathbb{I}.$$

Now let  $M = \lambda\mathbb{I} - A$ . We have

$$(\lambda\mathbb{I} - A)[\operatorname{adj}(\lambda\mathbb{I} - A)] = \det(\lambda\mathbb{I} - A)\mathbb{I} = f_A(\lambda) \cdot \mathbb{I}.$$

One may decompose any  $M \in M_n(F[\lambda])$  into powers of  $\lambda$ ,  $M = \sum \lambda^k B_k$  where  $B_k \in M_n(F)$ : for example,

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \lambda \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

We do this for

$$\operatorname{adj}(\lambda\mathbb{I} - A) = \sum_{k=0}^{n-1} \lambda^k S_k,$$

and write also

$$f_A(\lambda) = \sum_{j=0}^n a_j \lambda^j.$$

We have

$$(\lambda\mathbb{I} - A) \left( \sum_{k=0}^{n-1} \lambda^k S_k \right) = \sum_{j=0}^n a_j \lambda^j \mathbb{I}$$

or

$$\begin{aligned} & -AS_0 + \lambda(S_0 - AS_1) + \lambda^2(S_1 - AS_2) + \dots \\ & \quad + \lambda^{n-1}(S_{n-2} - AS_{n-1}) + \lambda^n S_{n-1} \\ & = a_0\mathbb{I} + a_1\lambda\mathbb{I} + a_2\lambda^2\mathbb{I} + \dots + a_{n-1}\lambda^{n-1}\mathbb{I} + a_n\lambda^n\mathbb{I}. \end{aligned}$$

---

<sup>2</sup>Technically, applying Cramer as we did in §IV.C requires knowing  $A$  is invertible, which typically won't be true for  $M$ . See Exercise (5) below for a way around this.

You may equate “coefficients” of like powers of  $\lambda$ , even though they are matrices (just by doing so entry by entry):

$$\begin{aligned} a_0\mathbb{I} &= -AS_0, \quad a_1\mathbb{I} = S_0 - AS_1, \quad a_2\mathbb{I} = S_1 - AS_2, \dots, \\ a_{n-1}\mathbb{I} &= S_{n-2} - AS_{n-1}, \quad a_n\mathbb{I} = S_{n-1}. \end{aligned}$$

To show  $f_A(A) = 0$ , write

$$\begin{aligned} f_A(A) &= f_A(A)\mathbb{I} = a_0\mathbb{I} + a_1A\mathbb{I} + a_2A^2\mathbb{I} + \dots + a_nA^n\mathbb{I} \\ &= a_0\mathbb{I} + A(a_1\mathbb{I}) + A^2(a_2\mathbb{I}) + \dots + A^{n-1}(a_{n-1}\mathbb{I}) + A^n(a_n\mathbb{I}) \\ &= -AS_0 + A(S_0 - AS_1) + A^2(S_1 - AS_2) + \dots \\ &\quad + A^{n-1}(S_{n-2} - AS_{n-1}) + A^nS_{n-1} \\ &= -AS_0 + AS_0 - AS_1 + AS_1 - AS_2 + \dots \\ &\quad + A^{n-1}S_{n-2} - A^nS_{n-1} + A^nS_{n-1} \\ &= 0. \end{aligned} \quad \square$$

SECOND PROOF OF VI.A.1. Here’s a more abstract approach.

Start with a basis  $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$  of  $F^n$ , and a transformation  $T : F^n \rightarrow F^n$ , with  $[T]_{\mathcal{B}} = A$ . We show  $f_A(T)$  is the zero transformation. By definition

$$T\vec{v}_i = \sum_j A_{ji}\vec{v}_j,$$

which we can rewrite

$$\sum_j (\delta_{ij}T - A_{ji}) \vec{v}_j = 0.$$

Set  $B_{ij} = \delta_{ij}T - A_{ji}$  (or  $B = T\mathbb{I} - {}^tA$ ); the entries of  $B$  are formal polynomials in the transformation  $T$ . The above equation becomes

$$\sum_j B_{ij}\vec{v}_j = 0$$

while we have also

$$\det(B) = f_A(T).$$

It is therefore sufficient to show  $(\det B)\vec{v}_k = 0$  for all  $k$ .

Let  $\tilde{B} = \text{adj}B$ , so that

$$\sum_i \tilde{B}_{ki} B_{ij} = \delta_{kj} \det B.$$

This time the calculation is far less messy:

$$\begin{aligned} (\det B)\vec{v}_k &= \sum_j \delta_{kj} (\det B)\vec{v}_j = \sum_j \left( \sum_i \tilde{B}_{ki} B_{ij} \right) \vec{v}_j \\ &= \sum_{i,j} \tilde{B}_{ki} B_{ij} \vec{v}_j = \sum_i \tilde{B}_{ki} \left( \sum_j B_{ij} \vec{v}_j \right) = \sum_i \tilde{B}_{ki} \cdot 0 = 0. \end{aligned}$$

□

The obvious question after Cayley-Hamilton is “can we ever do better than a polynomial of degree  $n$ ?”, i.e. find a nonzero polynomial of lower degree that annihilates  $A$ .

VI.A.3. EXAMPLE. Consider the matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Since

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 3 \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

or  $A^2 - 3A = 0$ , we find that  $q(x) = x^2 - 3x$  annihilates  $A$ . Notice that  $x^2 - 3x = x(x - 3)$  divides the characteristic polynomial  $f_A(x) = x^2(x - 3)$  for this  $A$ .

VI.A.4. DEFINITION. The **minimal polynomial**  $m_A$  of  $A$  is the (unique) nonzero monic<sup>3</sup> polynomial  $m$  of lowest possible degree, such that  $m(A) = 0$ . Cayley-Hamilton  $\implies \deg m_A \leq n$  for  $n \times n$  matrices  $A$ .

---

<sup>3</sup>*Monic* means that the coefficient of the highest power of  $\lambda$  (or  $x$ ) in the polynomial is 1.

**Uniqueness of  $m_A$ .** Let  $d$  = the lowest possible degree mentioned above. If  $'m$  and  $m$  are two distinct *monic* polynomials of degree  $d$ , which annihilate  $A$ , then  $'m(x) - m(x) =$

$$\begin{aligned} &= (x^d + 'a_{d-1}x^{d-1} + \dots + 'a_0) - (x^d + a_{d-1}x^{d-1} + \dots + a_0) \\ &= ('a_{d-1} - a_{d-1})x^{d-1} + \dots + ('a_0 - a_0). \end{aligned}$$

Dividing by the first nonzero  $'a_i - a_i$  (reading from left to right) gives a monic polynomial annihilating  $A$ :

$$''m(A) = \frac{1}{'a_i - a_i} ('m(A) - m(A)) = 0.$$

But  $\deg(''m) < d$ , which contradicts the definition (that is, the minimality) of  $d$ .

**Further properties of  $m_A$ .** Now recall that *long division* of polynomials, say of  $g$  into  $f$ , gives a quotient  $q$  and remainder  $r$  (where the remainder has degree strictly less than that of  $g$ ), such that  $\frac{f}{g} = q + \frac{r}{g}$ . If  $r = 0$  then we write  $g \mid f$  ( $g$  divides  $f$ ), otherwise  $g \nmid f$ . We may write this “division algorithm” as a polynomial equation

$$\boxed{f = gq + r, \deg r < \deg g.}$$

VI.A.5. PROPOSITION. *The minimal polynomial of  $A$  divides its characteristic polynomial,  $m_A(\lambda) \mid f_A(\lambda)$ .*

PROOF. By the division algorithm we may write

$$f_A(\lambda) = m_A(\lambda) \cdot q(\lambda) + r(\lambda), \quad \deg r < \deg m_A.$$

But then

$$r(A) = f_A(A) - m_A(A) \cdot q(A) = 0 - 0 \cdot q(A) = 0,$$

and  $r$  annihilates  $A$ . Because its degree is less than that of  $m_A$ ,  $r$  must be zero (as a polynomial) — otherwise we have contradicted minimality of  $m_A$ . Therefore  $f_A = m_A \cdot q$  and we’re done.  $\square$

VI.A.6. REMARK. By the same proof,  $m_A$  divides any polynomial  $p$  satisfying  $p(A) = 0$ .

In §VI.B we shall give an algorithm for finding  $m_A$ . The idea is to perform elementary row *and column* operations (suitably defined) on  $\lambda\mathbb{I} - A$  to put it in a new form:

VI.A.7. DEFINITION. A matrix  $M \in M_n(F[\lambda])$  (with polynomial entries) is in **normal form** iff it looks like this:

$$\begin{pmatrix} f_1(\lambda) & & 0 \\ & \ddots & \\ 0 & & f_n(\lambda) \end{pmatrix}$$

where  $f_1 \mid f_2 \mid \dots \mid f_n$  and each  $f_i$  is a monic polynomial or zero.<sup>4</sup> (So the only possible nonzero scalar is 1, and in the sorts of normal forms we'll encounter the first few  $\{f_i\}$  will usually be 1.) A typical example is  $\text{diag}\{1, 1, 1, \lambda, \lambda(\lambda - 2)^2\}$ .

In fact we shall give an algorithm associating to any square matrix  $M$  with entries in  $F[\lambda]$ , a matrix  $nf(M)$  in normal form.

We need one more

VI.A.8. DEFINITION. For  $M \in M_n(F[\lambda])$ , let

- $\delta_k(M) :=$  the monic *gcd* (= greatest common divisor) of the determinants of all  $k \times k$  submatrices<sup>5</sup> of  $M$ , and
- $\Delta_k(M) := \delta_k(M) / \delta_{k-1}(M)$ . These  $\Delta_k$  are called the **invariant factors** of  $M$ .

VI.A.9. REMARK. The  $\Delta_k(M)$  are polynomials (as will be implied by the Theorem below). Note that

$$\delta_{n-1} = \text{the monic gcd of the entries of } \text{adj}(M),$$

and

$$\delta_n(M) = C^{-1} \cdot \det(M)$$

<sup>4</sup>The “zero” possibility will not occur when  $M = nf(\lambda\mathbb{I} - A)$  (the main application), but must be included to state more general results. Note that if  $f_k = 0$ , then  $f_{k+1} = \dots = f_n = 0$  as well, as 0 only divides 0.

<sup>5</sup>The submatrices are obtained by blocking out any  $(n - k)$  rows and  $(n - k)$  columns. Their determinants are frequently called  $k \times k$  *minors*. If these are all zero, we put  $\delta_k = 0 = \Delta_k$ ; but again, this cannot happen for  $M = \lambda\mathbb{I} - A$ .

where  $C$  is a scalar – namely, the coefficient of the highest power of  $\lambda$  in  $\det(M)$ . If  $M = \lambda\mathbb{I} - A$  then  $\det(M)$  is monic; thus  $C = 1$  and

$$\delta_n(\lambda\mathbb{I} - A) = \det(\lambda\mathbb{I} - A) = f_A(\lambda).$$

VI.A.10. THEOREM. *If*

$$nf(M) = \begin{pmatrix} f_1(\lambda) & & \\ & \ddots & \\ & & f_n(\lambda) \end{pmatrix}$$

*then  $\Delta_k(M) = f_k(\lambda)$ . That is, the invariant factors of  $M$  are given by the diagonal entries of  $nf(M)$ .*

The Theorem will be proved in the next section.

Clearly then  $f_1(\lambda) \cdots f_n(\lambda) =$

$$\Delta_1(M) \cdots \Delta_n(M) = \delta_1(M) \cdot \frac{\delta_2(M)}{\delta_1(M)} \cdots \frac{\delta_n(M)}{\delta_{n-1}(M)} = \delta_n(M)$$

and we have a

VI.A.11. COROLLARY. *If  $M = \lambda\mathbb{I} - A$  then  $f_1(\lambda) \cdots f_n(\lambda) = \det(\lambda\mathbb{I} - A)$ . That is, the product of the (diagonal) entries of  $nf(\lambda\mathbb{I} - A)$  is  $f_A(\lambda)$ .*

Set

$$\delta_A(\lambda) := \delta_{n-1}(\lambda\mathbb{I} - A) = \text{monic gcd of entries of } \text{adj}(\lambda\mathbb{I} - A).$$

What we would like now is to prove the following

VI.A.12. PROPOSITION. *The top invariant factor of  $\lambda\mathbb{I} - A$  is the minimal polynomial of  $A$ :*

$$m_A(\lambda) = \Delta_n(\lambda\mathbb{I} - A) = \frac{f_A(\lambda)}{\delta_A(\lambda)}.$$

According to this statement, in order to find  $m_A(\lambda)$  it suffices to row/column-reduce  $\lambda\mathbb{I} - A$  to normal form (as described in the next section), and pick out the last (diagonal) entry. The proof will be independent of Theorem VI.A.10.



For small  $n$ , it can actually be practical to apply the Proposition directly to compute  $m_A$ . For  $A$  as in Example VI.A.3, the entries of  $\text{adj}(\lambda\mathbb{I} - A)$  are all  $\lambda^2 - 2\lambda$  or  $\lambda$ , whose gcd is  $\lambda$ . Dividing  $f_A(\lambda) = \lambda^2(\lambda - 3)$  by this gives  $m_A(\lambda) = \lambda(\lambda - 3)$ .

PROOF OF PROP. VI.A.12 (IN FOUR STEPS).

**Step I** Show  $f_A(\lambda)/\delta_A(\lambda)$  is a polynomial (that is,  $\delta_A \mid f_A$ ).

Let

$$(VI.A.13) \quad B := \text{adj}(\lambda\mathbb{I} - A) = \delta_A(\lambda)M$$

where the gcd of the entries of  $M$  is 1 (see definition of  $\delta_A(\lambda)$  above). By “Cramer’s rule” (cf. Exercise (5) below) we know the adjoint gives a “partial” inverse to  $(\lambda\mathbb{I} - A)$ , i.e.

$$\det(\lambda\mathbb{I} - A)\mathbb{I} = (\lambda\mathbb{I} - A)B$$

or (using (VI.A.13))

$$(VI.A.14) \quad f_A(\lambda)\mathbb{I} = \delta_A(\lambda)(\lambda\mathbb{I} - A)M.$$

So  $(\lambda\mathbb{I} - A)M$  must be of the form  $\Delta(\lambda) \cdot \mathbb{I}$  (for some polynomial  $\Delta$ ), and the polynomial equation

$$f_A(\lambda) = \delta_A(\lambda)\Delta(\lambda)$$

must hold, and we have finished the first step. (Notice we have proved directly that  $\Delta_n(\lambda\mathbb{I} - A) [= \Delta(\lambda)]$  is a polynomial.)

**Step II** Show  $m_A(\lambda) \mid \Delta(\lambda)$ .

From (VI.A.14) we have that

$$(\delta_A(\lambda)\Delta(\lambda))\mathbb{I} = \delta_A(\lambda)(\lambda\mathbb{I} - A)M$$

or

$$(VI.A.15) \quad \Delta(\lambda)\mathbb{I} = (\lambda\mathbb{I} - A)M.$$

Now while one cannot simply substitute  $A$  for  $\lambda$  (the entries of  $M$  are polynomials in  $\lambda$  too!), one may essentially repeat the argument we used in our first proof of Cayley-Hamilton (writing out  $\Delta(\lambda) =$

$\sum b_j \lambda^j$  and  $M = \sum \lambda^k B_k$ ) to show that

$$\Delta(A) = 0.$$

But then by Remark VI.A.6 above,  $m_A$  divides any polynomial with this property, and we are done.

**Step III** Show  $\Delta(\lambda) \mid m_A(\lambda)$ .

Since by definition

$$m_A(A) = 0,$$

we have for some matrix  $Q \in M_n(F[\lambda])$

$$m_A(\lambda)\mathbb{I} = Q(\lambda\mathbb{I} - A).$$

(See Remark VI.A.16.) Multiplying on the right by  $M$  and using (VI.A.15) gives

$$m_A(\lambda)M = \Delta(\lambda)Q.$$

Consider the monic  $\gcd$ 's of the entries of the matrices on either side:

$$m_A(\lambda) = \Delta(\lambda) \cdot \gcd\{\text{entries of } Q\},$$

since  $\gcd\{\text{entries of } M\}$  was 1. This concludes step III.

**Step IV** The end.

Since  $m_A$  and  $\Delta$  are both monic ( $\Delta$  is the quotient of two monic polynomials), and both divide each other, they must be equal.  $\square$

VI.A.16. REMARK. How do we know that  $m_A(A) = 0$  means that  $m_A(\lambda)\mathbb{I}$  is “divisible” by  $(\lambda\mathbb{I} - A)$  in a matrix ring which is not even commutative? The trick is to look just at the (commutative) subring  $R$  consisting of polynomials in  $A$  and  $\lambda$ . If you are comfortable with rings, then consider the homomorphism  $\theta : R \twoheadrightarrow R/(\lambda - A)$ , with kernel simply the ideal  $(\lambda - A)$  consisting of multiples of  $\lambda - A$ . In the quotient,  $\lambda$  is identified with  $A$ ; and so  $\theta(m_A(\lambda)) = \theta(m_A(A)) = 0$ . Consequently  $m_A(\lambda)$  is a multiple of  $\lambda - A$ , as required.

Alternatively, writing  $m_A(\lambda)\mathbb{I} = \lambda^\mu\mathbb{I} + \sum_{k=0}^{\mu-1} \lambda^k \alpha_k \mathbb{I}$  and

$$Q(\lambda\mathbb{I} - A) = \sum_{k=0}^{\mu-1} \lambda^k Q_k(\lambda\mathbb{I} - A),$$

with  $Q_k \in M_n(F)$ , we can try to solve for  $Q_k$  such that these two expressions are equal. One finds that  $Q_{\mu-1} = \mathbb{I}$ ,  $Q_{\mu-2} = \alpha_{\mu-1}\mathbb{I} + A$ ,  $Q_{\mu-3} = \alpha_{\mu-2}\mathbb{I} + \alpha_{\mu-1}A + A^2, \dots$ , and

$$Q_0 = \alpha_1\mathbb{I} + \alpha_2A + \dots + \alpha_{\mu-1}A^{\mu-2} + A^{\mu-1}.$$

This leaves the equality of the constant terms, which is

$$\alpha_0\mathbb{I} = -Q_0A.$$

As you will readily verify, this is just the statement that  $m_A(A) = 0$ .

### Exercises

(1) Verify Cayley-Hamilton for

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then use Prop. VI.A.12 and Defn. VI.A.8 to directly find  $m_A$ .

(2) Same as the last Exercise, for

$$A = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}.$$

(3) Suppose  $\det A \neq 0$ . Use Cayley-Hamilton to show that  $A$  is invertible and that  $A^{-1}$  is given by a certain polynomial in  $A$ .

(4) Let  $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  be a polynomial, and  $V$  be a vector space with basis  $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$ . Define  $T: V \rightarrow V$  by  $T\vec{v}_i = \vec{v}_{i+1}$  ( $i = 1, \dots, n-1$ ) and

$$T\vec{v}_n = -a_{n-1}\vec{v}_n - a_{n-2}\vec{v}_{n-1} - \dots - a_1\vec{v}_2 - a_0\vec{v}_1.$$

(a) Show that  $p(T) = 0$ . [Hint: substitute  $\vec{v}_2 = T\vec{v}_1$ , etc., into the equation for  $T\vec{v}_n$ .]

(b) Determine  $A := [T]_{\mathcal{B}}$ .

(c) Show that  $p(x) = m_A(x) = f_A(x)$ . [Hint: suppose that  $q(T) = 0$  for a polynomial  $q$  of degree  $< n$ .]

- (5) Prove that for a matrix with entries in  $F[\lambda]$  (or really, any commutative ring), we have

$$M \cdot \text{adj}(M) = \det(M)\mathbb{I} = \text{adj}(M) \cdot M.$$

[Hint: all you need is the fact that by definition,  $[\text{adj}(M)]_{ij} = (-1)^{i+j} \det(M_{ji})$ , together with the Laplace expansion formulas for  $\det$  and the property of  $\det$  that a repeated row makes it zero.<sup>6</sup> The point is to *not* use Cramer's rule.]

---

<sup>6</sup>Both of these follow from the definition (IV.A.5) of  $\det$  for matrices with coefficients in any commutative ring, like  $F[\lambda]$ .