1.7. Jordan normal form and finitely generated $\mathbb{F}[x]$-modules

1.7.1. Minimal and characteristic polynomials (annihilators of $\mathbb{F}[x]$-modules).

— Let $A \in M_n(\mathbb{F})$. Let

$$\begin{array}{rccc} \mathrm{ev}_A\colon & \mathbb{F}[x] & \to & M_n(\mathbb{F}) \\ & c_0 + c_1x + \cdots + c_rx^r & \mapsto & c_0 + c_1A + \cdots c_rA^r \end{array}$$

The *kernel* of ev_A is

$$\ker(\mathrm{ev}_A) = \{p(x) \in \mathbb{F}[x] \mid \mathrm{ev}_A(p(x)) = 0.\}$$

Proposition 1.7.1. — *There exists a unique monic polynomial $m(x) \in \mathbb{F}[x]$ such that* $\ker(\mathrm{ev}_A) = m(x)\mathbb{F}[x]$.

Let $A \in M_n(\mathbb{F})$.

- The **minimal polynomial** of A is the monic polynomial $m(x) \in \mathbb{F}[x]$ such that
$$\ker \mathrm{ev}_A = m_A(x)\mathbb{F}[x].$$
- The matrix $x - A \in M_n(\mathbb{F}[x])$. The **characteristic polynomial** of A is $\det(x-A)$.

Proposition 1.7.2. — *(Cayley-Hamlton theorem) Let $A \in M_n(\mathbb{F})$ and let $m(x)$ be the minimal polynomial of A. Then*

$$\det(x - A) \in \ker(\mathrm{ev}_A).$$

HW: Show that

$$\det(x - (A_1 \oplus A_2)) = \det(x - A_1)\det(x - A_2) \quad \text{and} \quad m_{A_1 \oplus A_2}(x) = \mathrm{lcm}(m_{A_1}(x), m_{A_2}(x)).$$

HW: Show that

$$\det(x - (P^{-1}AP)) = \det(x - A) \quad \text{and} \quad m_{P^{-1}AP}(x) = m_A(x).$$

Proposition 1.7.3. — *(Chinese block decomposition) Let $\mathbb{F}$ be a field, let $n \in \mathbb{Z}_{>0}$ and let $V = \mathbb{F}^n$. Let $A \in M_n(\mathbb{F})$ and let $m_A(x)$ be the minimal polynomial of A. Assume*

$$m_A(x) = p(x)q(x) \qquad \textit{with} \quad \gcd(p(x), q(x)) = 1.$$

Use the Euclidean algorithm for $\mathbb{F}[x]$ to construct $r(x), s(x) \in \mathbb{F}[x]$ such that

$$1 = p(x)r(x) + q(x)s(x) \qquad \textit{and let} \quad P_U = p(A)r(A) \qquad \textit{and} \qquad P_W = q(A)s(A).$$

Then

$$P_U^2 = P_U, \quad P_W^2 = P_W, \quad P_UP_W = P_WP_U = 0, \quad \textit{and} \quad P_U + P_W = 1.$$

Let

$$U = p(A)r(A)V \quad \textit{and} \quad W = q(A)s(A)V. \qquad \textit{Then} \quad V = U \oplus W$$

and both U and W are A-invariant.

Proof. — Let $P_U = p(A)r(A)$ and $P_W = q(A)s(A)$. Then

$$P_U + P_W = \mathrm{ev}_A(p(x)r(x) + q(x)s(x)) = \mathrm{ev}_A(1) = 1.$$

Let $v \in V$. Then

$$P_UP_Wv = p(A)r(A)q(A)s(A)v = p(A)q(A)r(A)s(A)v = m_A(A)r(A)s(A)v = 0.$$

Using $P_UP_W = 0$, then

$$P_Uv = P_U(P_U + P_W)v = P_U^2 v \qquad \text{and} \qquad P_Wv = P_W(P_U + P_W)v = P_W^2 v.$$

So $P_U^2 = P_U$ and $P_W^2 = P_W$.
If $u \in U$ then there exists $v \in V$ such that $u = P_Uv$. So

$$P_Uu = P_U^2 v = P_Uv = u, \quad \text{and similarly} \qquad \text{if } w \in W \text{ then } P_Ww = w.$$

Assume $z \in U \cap W$. Then $z = P_Uz = P_UP_Wz = 0$. So $U \cap W = 0$.
Assume $v \in V$. Then $v = 1 \cdot v = (P_U + P_W)v = P_Uv + P_Wv \in U + W$. So $V = U + W$.
Thus $V = U \oplus W$. □

Corollary 1.7.4. — *(Generalized eigenspaces and simsimple+nilpotent decomposition) Let $\overline{\mathbb{F}}$ be an algebraically closed field and let $n \in \mathbb{Z}_{>0}$. Let $V = \overline{\mathbb{F}}^n$ and let $A \in M_n(\overline{\mathbb{F}})$. Let $k \in \mathbb{Z}_{>0}$ and $\lambda_1, \ldots, \lambda_k \in \mathbb{F}$ and $c_1, \ldots, c_k \in \mathbb{Z}_{>0}$ so that*

$$m_A(x) = (x - \lambda_1)^{c_1} \cdots (x - \lambda_k)^{c_k}$$

is the prime factorization of the minimal polynomial of A. For $j \in \{1, \ldots, k\}$ define

$$V_{\lambda_j}^{\mathrm{gen}} = \{v \in V \mid \textit{there exists } k \in \mathbb{Z}_{>0} \textit{ such that } (A - \lambda_j)^k v = 0\}.$$

Define $S \in M_n(\overline{\mathbb{F}})$ by setting $Sv = \lambda_j v$ if $v \in V_{\lambda_j}^{\mathrm{gen}}$, and let $N = A - S$. Then

$$V = V_{\lambda_1}^{\mathrm{gen}} \oplus \cdots \oplus V_{\lambda_k}^{\mathrm{gen}}$$

$$S \textit{ is semisimple}, \quad N \textit{ is nilpotent}, \quad SN = NS \quad \textit{and} \quad A = S + N.$$

1.7.2. Diagonalization (simple and semisimple $\mathbb{F}[x]$-modules). — Let $\mathbb{F}$ be a field and let $n \in \mathbb{Z}_{>0}$.

$$\text{Let} \quad V = \mathbb{F}^n \quad \text{and} \quad A \in M_n(\mathbb{F}).$$

- A subspace $U \subseteq \mathbb{F}^n$ is *A-invariant*, or U is an *A-submodule of V*, if U satisfies:

$$\text{if } u \in U \text{ then } Au \in U.$$

- An *eigenvector of A* is a nonzero element of a 1-dimensional A-invariant subspace of V.
- Let $\lambda \in \mathbb{F}$. An *eigenvector of A of eigenvalue λ* is $p \in V$ such that

$$p \neq 0 \quad \text{and} \quad Ap = \lambda p.$$

- The matrix A is *semisimple*, or *diagonalizable*, if there exist $P \in GL_n(\mathbb{F})$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ such that

$$P^{-1}AP = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

- The matrix A is *nilpotent* if there exists $k \in \mathbb{Z}_{>0}$ such that $A^k = 0$.

HW: Show that p is an eigenvector of A if and only if $\mathbb{F}p$ is A-invariant.

HW: Show that p is an eigenvector of A if and only if $p \in \ker(A - \lambda)$.

HW: Show that if $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ and $P^{-1}AP = D$ then

$$\det(A) = \lambda_1 \cdots \lambda_n \quad \text{and} \quad \det(x - A) = (x - \lambda_1) \cdots (x - \lambda_n).$$

Proposition 1.7.5. — *Let $\mathbb{F}$ be a field and let $n \in \mathbb{Z}_{>0}$. Let $A \in M_n(\mathbb{F})$.*
(a) If $p_1, \ldots, p_k$ are eigenvectors of A with eigenvalues $\lambda_1, \ldots, \lambda_k$ and $\lambda_1, \ldots, \lambda_k$ are all distinct then $p_1, \ldots, p_k$ are linearly independent.

(b) Let $\lambda \in \mathbb{F}$. Then A has an eigenvector of eigenvalue λ if and only if λ is a root of $m_A(x)$.
(c) Let $\lambda \in \mathbb{F}$. Then A has an eigenvector of eigenvalue λ if and only if λ is a root of $\det(x - A)$.

Corollary 1.7.6. — *Let $\mathbb{F}$ be a field and let $n \in \mathbb{Z}_{>0}$. Let $A \in M_n(\mathbb{F})$. If $\mathbb{F}$ is algebraically closed then A has an eigenvector.*

HW: Let $A \in M_n(\mathbb{F})$. Show that A is diagonalizable if and only if there exist n linearly independent eigenvectors of A.

1.7.3. Jordan normal form (indecomposable $\mathbb{F}[x]$-modules). — Assume that $\mathbb{F}$ is algebraically closed. Let $d \in \mathbb{Z}_{>0}$ and let $\lambda \in \mathbb{F}$. The *Jordan block of size d and eigenvalue λ* is

$$J_d^\lambda \in M_d(\mathbb{F}) \qquad \text{given by} \qquad J_d^\lambda(i,j) = \begin{cases} \lambda, & \text{if } i = j, \\ 1, & \text{if } j = i+1, \\ 0, & \text{otherwise.} \end{cases}$$

$$J_d^\lambda = \begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ & & & \lambda & 1 & 0 \\ & & & 0 & \lambda & 1 \\ 0 & & \cdots & & 0 & \lambda \end{pmatrix}, \qquad \text{a } d \times d \text{ matrix.}$$

Theorem 1.7.7. — *(Jordan normal form) Let $n \in \mathbb{Z}_{>0}$ and let $A \in M_n(\mathbb{F})$. Then there exists $P \in GL_n(\mathbb{F})$, $k \in \mathbb{Z}_{>0}$ and $\{(\lambda_1, d_1), \ldots, (\lambda_k, d_k)\} \subseteq \mathbb{F} \times \mathbb{Z}_{>0}$ such that*

$$P^{-1}AP = J_{d_1}^{\lambda_1} \oplus \cdots \oplus J_{d_k}^{\lambda_k}.$$

Up to reordering, the Jordan blocks for A are unique (don't depend on the choice of P).

HW: Show that if $J = J_d^\lambda$ then $m_J(x) = (x-\lambda)^d$ and $det(x - J) = (x-\lambda)^d$.

HW: *(The waterfall basis)* Show that if $J = J_d^\lambda$ then

$$Je_1 = \lambda e_1, \quad Je_2 = \lambda e_2 + e_1, \quad \ldots, \quad Je_d = \lambda e_d + e_{d-1}, \qquad \text{and}$$
$$(J-\lambda)e_1 = 0, \quad (J-\lambda)e_2 = e_1, \quad \ldots, \quad (J-\lambda)e_d = e_{d-1}.$$

HW: Let $S \in M_n(\mathbb{F})$. Show that S is semisimple if and only if all Jordan blocks for S have size 1.

HW: Let $N \in M_n(\mathbb{F})$. Show that N is nilpotent if and only if all Jordan blocks for N have eigenvalue 0.