Lecture 33: Examples of Modules over PID

Given a matrix $A \in F^{n\times n}$ we may discuss the $F[x]$-module which it generates under $f(x)v = f(A)v$, the Smith Normal Form derived from row and column operations on $xI - A$ gives a unique set of invariant factors $a_1(x), a_2(x), \dots, a_m(x) \in F[x]$ where these factors are nonzero, non-units for which

$$a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$$

Moreover, it turns out that

$$\underbrace{m_A(x) = a_m(x)}_{\substack{\text{minimal polynomial,} \\ \text{monic polynomial} \\ \text{in } F[x] \text{ of least} \\ \text{degree with} \\ m_A(A) = 0.}} \qquad \underbrace{\overbrace{char_A(x) = a_1(x)a_2(x)\cdots a_m(x)}^{\text{this will also be the product of elem. divisors.}}}_{\substack{\text{characteristic polynomial} \\ char_A(x) = \det(xI - A) \\ \deg(char_A(x)) = n}}$$

In Math 321 we saw $m_A(x)$ and $char_A(x)$ share the same zeros and $\boxed{char_A(A) = 0}$ ← Cayley Hamilton Th^{m}

The elementary divisors are $a_1(x), a_2(x), \dots, a_m(x)$ subdivided into their factors (primes), the elementary factors are powers of primes forming $a_1(x), \dots, a_m(x)$.

$\boxed{E1}$ $char_A(x) = (x-1)^2(x+1)$ $\xrightarrow{\text{I}}$ $m_A(x) = (x-1)(x+1)$

$\xrightarrow{\text{II}}$ $m_A(x) = (x-1)^2(x+1)$

I $a_2(x) = (x-1)(x+1)$ and $a_1(x) = x-1$, $\underbrace{(x-1), (x-1), (x+1)}_{\text{elementary divisors}}$

II $a_1(x) = (x-1)^2(x+1)$, $\underbrace{(x-1)^2, (x+1)}_{\text{elementary divisors.}}$

The Fundamental Th$^{\underline{m}}$ indicates,

$$F^n \cong \frac{F[x]}{(a_1(x))} \oplus \frac{F[x]}{(a_2(x))} \oplus \cdots \oplus \frac{F[x]}{(a_m(x))}$$

we can build a basis for F^n which respects the above decomposition, this is the <u>rational</u> <u>canonical</u> <u>form</u>

$\underbrace{\text{we assume } a(A) = A^n + \cdots + c_1 A + c_0 I = 0}$

Th$^{\underline{m}}$/ If $\langle\langle v \rangle\rangle = \text{span}_F\{v, Av, A^2v, \ldots, A^{n-1}v\}$ given $\deg(a(x)) = n$ and $a(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ then $\beta = \{v, Av, \ldots, A^{n-1}v\}$ is basis for $\langle\langle v \rangle\rangle$ and if $L_A : \langle\langle v \rangle\rangle \longrightarrow \langle\langle v \rangle\rangle$ is $L_A(x) = Ax$ then

$$[L_A]_{\beta,\beta} = \begin{bmatrix} 0 & 0 & & 0 & -c_0 \\ 1 & 0 & & 0 & -c_1 \\ 0 & 1 & & 0 & -c_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{bmatrix} = C_{a(x)}$$

<u>Proof</u>: $A^j v = (j+1)$-th basis vector in β and $A(A^{j-1}v) = A^j v$ for $j = 1, 2, \ldots, n-1$ thus for $j = 1, 2, \ldots, n-1$

$$[L_A(\underbrace{A^{j-1}v}_{j^{\text{th}} \text{ basis element}})]_\beta = [A^j v]_\beta = e_{j+1}$$

When we reach the $n^{\underline{\text{th}}}$ basis element of $A^{n-1}v$ then

$$[L_A(A^{n-1}v)]_\beta = [A^n v]_\beta = [-c_{n-1}A^{n-1}v - \cdots - c_2 A^2 v - c_1 Av - c_0 v]_\beta$$

$$= \underbrace{-c_0 e_1 - c_1 e_2 - \cdots - c_{n-1} e_n}_{\text{gives last column of } C_{a(x)}.}$$

Continuing, if we have divisors $a_1(x) / a_2(x) / \cdots / a_m(x)$ for $A \in F^{n \times n}$ then $\text{char}_A(x) = a_1(x)\, a_2(x) \cdots a_m(x)$ and if we construct a basis $\beta = \beta_1 \cup \beta_2 \cup \cdots \cup \beta_m$ where $L_A : \langle\langle v_j \rangle\rangle \longrightarrow \langle\langle v_j \rangle\rangle$ has $[L_A]_{\beta_j, \beta_j} = C_{a_j(x)}$ for $j = 1, 2, \ldots, m$ then ~~(oops! I've assumed $a_1(x)$, $a_2(x), \ldots, a_m(x)$ are irreducible)~~

~~see E3 for how to deal with product of primes... well...~~

$$[L_A]_{\beta, \beta} = \underbrace{\boxed{C_{a_1(x)} \oplus C_{a_2(x)} \oplus \cdots \oplus C_{a_m(x)}}}_{\text{rational canonical form of } A}$$

Remark: I believe § 12.2 describes method to create β as a side-product of calculating SMITH NORMAL FORM from row/column op's over $F[x]$ on $xI - A$. I'm probably not working a problem complicated enough to warrant my attention to this calculation.

$\boxed{\text{E2}}$ $\text{char}_A(x) = (x-1)^2(x-1)$

$m_A(x) = (x-1)^2(x-1) = a_1(x)$

$d_1(x) = (x-1)^2, \quad d_2(x) = x - 1$

$$A \sim \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{bmatrix} = C_{x^3 - 3x^2 + 3x - 1}$$

$$\boxed{A \sim \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right]}$$

$a_1(x) = (x^2 - 2x + 1)(x-1) = x^3 - 3x^2 + 3x - 1$

$m_A(x) = (x-1)(x+1) = a_2(x), \quad a_1(x) = x - 1$

$a_2(x) = x^2 - 1, \quad a_1(x)$

$d_1(x) = (x-1), \quad d_2(x) = x+1, \quad d_3(x) = x - 1$

$$A \sim \left[\begin{array}{c|cc} 1 & & \\ \hline & 0 & 1 \\ & 1 & 0 \end{array}\right] = C_{a_1(x)} \oplus C_{a_2(x)} \quad \leftarrow \text{rational canonical form}$$

$$\boxed{A \sim \begin{bmatrix} 1 & & \\ & -1 & \\ & & 1 \end{bmatrix}} \quad \leftarrow \text{Jordan Form}$$

(explain next ↷)

The elementary divisors are prime powers which appear in the invariant factors $a_1(x), \dots, a_m(x)$. Notice $a_m(x)$ has <u>all</u> possible factors since $a_1(x) \,/\, a_2(x) \,/\, \cdots \,/\, a_m(x)$. Suppose $\underbrace{r_1^m, r_2^m, \dots, r_s^m}_{\text{exponents for distinct prime powers forming } a_m(x)} \geq 1$

$$a_m(x) = p_1^{r_1^m}(x)\, p_2^{r_2^m}(x) \cdots p_s^{r_s^m}(x)$$

$$a_{m-1}(x) = p_1^{r_1^{m-1}}(x)\, p_2^{r_2^{m-1}}(x) \cdots p_s^{r_s^{m-1}}(x)$$

$$a_{m-2}(x) = p_1^{r_1^{m-2}}(x)\, p_2^{r_2^{m-2}}(x) \cdots p_s^{r_s^{m-2}}(x)$$

$$\vdots$$

$$a_1(x) = p_1^{r_1^1}(x)\, p_2^{r_2^1}(x) \cdots p_s^{r_s^1}(x)$$

Here $r_j^m \geq r_j^{m-1} \geq \cdots \geq r_j^2 \geq r_j^1 \geq 0$ for $j = 1, 2, \dots, s$.

The elementary divisors are $(p_j(x))^{r_j^k}$ where $r_j^k \neq 0$.

<u>Remark</u>: Let $d_1(x), d_2(x), \dots, d_s(x)$ denote the prime powers which form factors of $a_1(x), \dots, a_m(x)$ hence $d_1(x)\, d_2(x) \cdots d_s(x) = \text{char}_A(x)$.

Fundamental Th^m, elem. divisors form applied to pure torsion $F[x]$-mod.

$$\boxed{\text{Th}^m / \; F^n \cong \frac{F[x]}{(d_1(x))} \oplus \frac{F[x]}{(d_2(x))} \oplus \cdots \oplus \frac{F[x]}{(d_s(x))}}$$

<u>Remark</u>: the decomposition above is not unique, unless we have some adhoc scheme to order the elementary divisors.... we next see the basis built to reflect this decomp. the basis will similarity transform A to Jordan Form (provided $d_1(x), \dots, d_s(x)$ <u>split</u> over F)

Suppose $d_j(x) = (x-\lambda_j)^{n_j}$ for $j = 1, 2, .., s$ are the elementary divisors over F $(\lambda_j \in F)$ then we can form basis for F^n via n_j-chains for A according to the chain-equations,

$$(A-\lambda_j)V_{j,1} = 0$$

($V_{j,1}$ e-vector with e-value λ_j for A)

$$\left.\begin{aligned} (A-\lambda_j)V_{j,2} &= V_{j,1} \\ &\vdots \\ (A-\lambda_j)V_{j,n_j} &= V_{j,n_j-1} \end{aligned}\right\} \quad (A-\lambda_j)V_{j,k} = V_{j,k-1}$$

$\boxed{\text{Th}^{\underline{m}}/ \ \beta_j = \{V_{j,1}, V_{j,2}, .., V_{j,n_j}\} \text{ a } n_j\text{-chain for } A \text{ then } L_A : \text{span}(\beta_j) \longrightarrow \text{span}(\beta_j) \text{ has } [L_A]_{\beta_j,\beta_j} = \lambda_j I_{n_j} + N_{n_j} = \underbrace{J_{n_j}}_{(n_j \times n_j)\text{-Jordan Block matrix}}(\lambda_j)}$

Here N_{n_j} is the <u>nilpotent</u> <u>matrix</u> for which $(N_{n_j})^{n_j-1} = E_{1,n_j}$ and $(N_{n_j})^{n_j} = 0$.

$$\boxed{\text{Def}^{\underline{n}}/ \ N_k = [0|e_1|e_2|\cdots|e_{k-1}] \in F^{k\times k}}$$

Note, $N_k^2 = N_k N_k = [0|Ne_1|Ne_2|\cdots|Ne_{k-1}] = [0|0|e_1|e_2|\cdots|e_{k-2}]$ etc...

Jordan Form for A is given by joining collection of n_j - chains for λ_j for $j = 1, 2, .., s$ and for

$\beta_1 \cup \beta_2 \cup .. \cup \beta_s = \beta$ we find

$$[L_A]_{\beta,\beta} = \underbrace{\boxed{J_{n_1}(\lambda_1) \oplus J_{n_2}(\lambda_2) \oplus \cdots \oplus J_{n_s}(\lambda_s) = J_A}}_{\text{Jordan Form of } A}$$

$$\boxed{\begin{array}{l} \text{Th}^{m}/ \ [\beta]^{-1} A [\beta] = J_A \ \text{ hence} \\ \quad \det(A) = \lambda_1^{n_1} \lambda_2^{n_2} \cdots \lambda_s^{n_s} \ \text{ and} \\ \quad \text{trace}(A) = n_1\lambda_1 + n_2\lambda_2 + \cdots + n_s\lambda_s \end{array}}$$

Remark: $\frac{dx}{dt} = Ax$ has general sol.$^{\underline{n}}$

$$x = e^{tA}c \quad \text{where } e^{tA} = \sum_{n=0}^{\infty} \frac{t^n}{n!} A^n$$

and
$$\exp(tA) = \exp\left(t[\beta]J_A[\beta]^{-1}\right) = [\beta] \underbrace{\exp(tJ_A)}_{\text{actually easy to calculate.}} [\beta]^{-1}$$

actually easy to calculate.

see p. 504 for formula.

E3 Suppose A has $\mathrm{char}_A(x) = x^4+1$ discuss the possible rational cannonical forms and Jordan forms for such A over $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

$\mathbb{Q}$: observe $x^4+1 \in \mathbb{Q}[x]$ is irreducible hence prime and so $a_1(x) = a_m(x) = x^4+1$

$$A \sim C_{x^4+1} = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

there is no Jordan form to find in this context since x^4+1 does not split over $\mathbb{Q}$.

$\mathbb{R}$: $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$ $(\mathbb{R}[x])$

Thus $a_1(x) = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$ but this is it since $\nexists$ factors to use for $a_2(x)$. Once more no Jordan form either and so,

$$A \sim C_{x^2+\sqrt{2}x+1} \oplus C_{x^2-\sqrt{2}x+1}$$

$$\underbrace{A \sim \begin{bmatrix} 0 & -1 \\ 1 & -\sqrt{2} \end{bmatrix} \oplus \begin{bmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{bmatrix}}_{\text{RCF over } \mathbb{R}}$$

If $a_m(x) = d_1(x)d_2(x)\cdots d_q(x)$ all irreducible over F then the RCF for $C_{a_m(x)} = C_{d_1(x)} \oplus C_{d_2(x)} \oplus \cdots \oplus C_{d_q}(x)$.

We could do this, but then it's not the rational canonical form.

E3 continued

$\mathbb{C}: \; x^4+1 = (x-\omega)(x-\omega^3)(x-\omega^5)(x-\omega^7)$

where $\omega = \exp\left(\frac{i\pi}{4}\right)$ has $\omega^4 = \exp(i\pi) = -1$

x^4+1 splits over $\mathbb{C}$ hence

$a_1(x) = x^4+1 = (x-\omega)(x-\omega^3)(x-\omega^5)(x-\omega^7)$

$$A \sim C_{x-\omega} \oplus C_{x-\omega^3} \oplus C_{x-\omega^5} \oplus C_{x-\omega^7}$$

$$\underbrace{A \sim \begin{bmatrix} \omega & & & \\ & \omega^3 & & \\ & & \omega^5 & \\ & & & \omega^7 \end{bmatrix}}$$

RCF for x^4+1 over $\mathbb{C}$ is the same as the Jordan form,

$$J_1(\lambda) = [\lambda]$$

$$A \sim J_1(\omega) \oplus J_1(\omega^3) \oplus J_1(\omega^5) \oplus J_1(\omega^7)$$

elementary divisors: $x-\omega, \; x-\omega^3, \; x-\omega^5, \; x-\omega^7$