Alg 551 12/4/2017

R commutative ring, M R-module

<u>Def</u> M is <u>free</u> of (finite) <u>rank</u> $n \iff M \cong R^n$.

rank(M) well def: (R domain $\Rightarrow \operatorname{rank}_R(M) = \dim_K(M \otimes_R K)$

K = field of fractions.)

Assume $R^n \cong R^m$, $m < n$.

$$R^n \xrightarrow{A} R^m \xrightarrow{B} R^n$$
$$x \longmapsto Ax \qquad y \longmapsto By$$

A $m \times n$, B $n \times m$, $BA = I_n$

$$A' = \begin{bmatrix} A \\ \hline 0 \end{bmatrix} \qquad B' = \left[\begin{array}{c|c} B & 0 \end{array}\right]$$

$B'A' = I_n \qquad \det(B')\det(A') = \det(I_n)$ ↯

<u>Example</u> $\exists$ non-commutative ring R and $m \neq n$ such that $R^m \cong R^n$ as left R-modules

<u>Def</u> M is <u>finitely generated</u> if $M = \langle x_1, \dots, x_n \rangle$, $x_i \in M$.

<u>Def</u> M is <u>Noetherian</u> if every submodule $N \subseteq M$ is fin. gen.

$\iff$ Ascending chain condition holds for submodules of M

$\iff$ Every nonempty collection of submodules of M has max elt.

<u>Def</u> $0 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \longrightarrow 0$ is short exact seq. of R-modules if

- ι injective R-hom,
- π surjective R-hom,
- $\iota(M') = \operatorname{Ker}(\pi)$.

Equivalent: $M' \subseteq M$ submodule and $M/M' \xrightarrow[\pi]{\cong} M''$ iso.

<u>Exer</u> M' and M'' f.g. $\Rightarrow$ M f.g. $\Rightarrow$ M'' f.g.

<u>Exer</u> M Noetherian $\iff$ M' and M'' Noetherian

<u>Exer</u> R Noetherian and M f.g. R-module $\Rightarrow$ M Noetherian

Finite presentation

A $m\times n$, $A \in \mathrm{Mat}(m\times n; R)$

$\mathrm{coker}(A) = R^m / \langle \text{columns of } A \rangle$

$$R^n \xrightarrow{A} R^m \longrightarrow \mathrm{Coker}(A) \longrightarrow 0$$

Def M is finitely presented if $M \cong \mathrm{coker}(A)$ for some A.

Exer R Noetherian, M f.g. R-module $\Rightarrow$ M finitely presented.

$$R^m \overset{\varphi}{\twoheadrightarrow} M. \qquad R^n \overset{A}{\twoheadrightarrow} \mathrm{Ker}(\varphi) \subseteq R^m$$

Def $A, A' \in \mathrm{Mat}(m\times n; R)$ are equivalent
if $\exists$ invertible $Q \in GL(n,R)$, $P \in GL(m,R)$: $A' = PAQ^{-1}$.

E.g. A' obtained by applying invertible row/column ops. to A.

Note A, A' equivalent $\Rightarrow$ $\mathrm{Coker}(A) \cong \mathrm{coker}(A')$

$$\begin{tikzcd}
R^n \arrow[r, "A"] \arrow[d, "\cong"', "Q"] & R^m \arrow[r, "\pi"] \arrow[d, "\cong"', "P"] & \mathrm{Coker}(A) \arrow[r] \arrow[d, dashed, "\cong"'] & 0 \\
R^n \arrow[r, "A'"] & R^m \arrow[r, "\pi'"] & \mathrm{Coker}(A') \arrow[r] & 0
\end{tikzcd}$$

($\pi' P$ factors through π and πP^{-1} factors through π'!)

$\Leftarrow$ NOT true! But true if R is PID.

Def R UFD, $A = (a_{ij}) \in \mathrm{Mat}(m\times n; R)$.
$\gcd(A) = \gcd(\{a_{ij}\})$ – well defined up to units.

Exer A, A' equivalent $\Rightarrow$ $\gcd(A) = \gcd(A')$
($\gcd(A)$ divides all entries of PAQ^{-1}.)

Lemma R PID, $A \in Mat(m \times n; R)$. Assume $a_{11} \nmid a_{ij}$ for some i, j. Then A is equiv. to some $A' \in Mat(m \times n, R)$ for which $\langle a_{11} \rangle \subsetneq \langle a'_{11} \rangle \subseteq R$. $A = (a_{ij})$, $A' = (a'_{ij})$

Proof WLOG $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 2×2 matrix.

Case 1: $a \nmid b$. $x = \gcd(a, b) = sa + tb$, $s, t \in R$.

$$Q = \begin{bmatrix} s & -b/x \\ t & a/x \end{bmatrix} \quad \det(Q) = \frac{sa}{x} + \frac{tb}{x} = 1 \Rightarrow Q \text{ invertible.}$$

$$A' = AQ = \begin{bmatrix} x & * \\ * & * \end{bmatrix} \qquad \langle a \rangle \subsetneq \langle a, b \rangle = \langle x \rangle$$

Case 2: $a \nmid c$. $x = \gcd(a, c) = sa + tc$. $\begin{bmatrix} s & t \\ -\frac{c}{x} & \frac{a}{x} \end{bmatrix} A = \begin{bmatrix} x & * \\ * & * \end{bmatrix}$

Case 3: $a \mid b$, $a \mid c$, $a \nmid d$.

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \sim \begin{bmatrix} a & 0 \\ c & d' \end{bmatrix} \sim \begin{bmatrix} a & 0 \\ 0 & d' \end{bmatrix} \sim \begin{bmatrix} a & d' \\ 0 & d' \end{bmatrix}, \quad d' = d - \frac{b}{a}\frac{c}{a}a$$

$a \nmid d'$. Use Case 1. □

Thm R PID, $A \in Mat(m \times n, R)$. Then A is equivalent to a "diagonal" matrix D such that $\langle d_1 \rangle \supseteq \langle d_2 \rangle \supseteq \cdots \supseteq \langle d_m \rangle$.

$$D = \begin{bmatrix} d_1 & 0 & \cdots & & 0 \\ 0 & d_2 & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots 0 & d_m & 0 \cdots 0 \end{bmatrix}$$

(If $m > n$, set $d_i = 0$ for $i > n$.)

Proof Lemma + R Noetherian $\Rightarrow$
A equiv. to $\overset{\text{some}}{} A'$ for which $a'_{11} \mid a'_{ij}$ $\forall i, j$. $a'_{11} = \gcd(A')$.

$$A' \sim \left[\begin{array}{c|ccc} a'_{11} & 0 & 0 \cdots & 0 \\ \hline 0 & & & \\ 0 & & B & \\ \vdots & & & \\ 0 & & & \end{array}\right]$$

where $a'_{11} \mid \gcd(B)$.

Diagonalize B by induction. □

<u>Note</u> $\operatorname{Coker}(A) \cong \operatorname{Coker}(D) \cong R/\langle d_1\rangle \oplus R/\langle d_2\rangle \oplus \cdots \oplus R/\langle d_m\rangle$

Assume $d_1, \dots, d_k \in R^\times$, $d_{k+1} \notin R^\times$ <u>and</u> $d_\ell \neq 0$, $d_{\ell+1} = \cdots = d_m = 0$.

$\operatorname{Rank}(M) = m - \ell$

<u>Invariant factors</u> of M: $d_{k+1}, d_{k+2}, \dots, d_\ell$, $M = \operatorname{Coker}(A)$.

$$M \cong R^{\operatorname{rank}(M)} \oplus R/\langle d_{k+1}\rangle \oplus \cdots \oplus R/\langle d_\ell\rangle$$

<u>Next</u>: Unique up to units.

R PID, M R-module, $p \in R$ prime elt.

$F = R/\langle p\rangle$ field.

$pM = \{px \mid x \in M\} \subseteq M$ submodule.

M/pM F-vector space. [redacted] $p^kM/p^{k+1}M$ F-vector space.

<u>Lemma</u> $M = R/\langle a\rangle$, $a \in R$. Then $p^kM/p^{k+1}M \cong \begin{cases} R/\langle p\rangle & \text{if } p^{k+1} \mid a \\ 0 & \text{else.} \end{cases}$

<u>Proof</u>

$$p^kM = \langle p^k, a\rangle / \langle a\rangle$$

$$p^kM/p^{k+1}M = \langle p^k, a\rangle / \langle p^{k+1}, a\rangle$$

$$p^{k+1} \mid a \Rightarrow p^kM/p^{k+1}M \cong \langle p^k\rangle/\langle p^{k+1}\rangle \cong R/\langle p\rangle.$$

Assume $p^{k+1} \nmid a$.

write $a = p^n b$ where $\langle p, b\rangle = \langle 1\rangle \subseteq R$. $\gcd(p,b) = 1$.

Then $n \le k$ and [redacted] $\gcd(p^{k+1}, a) = p^n = \gcd(p^k, a)$.

$\langle p^k, a\rangle = \langle p^n\rangle = \langle p^{k+1}, a\rangle \Rightarrow p^kM/p^{k+1}M = 0.$

$\square$

Choose complete set of non-associated primes $\mathcal{P} \subseteq R$.

Given $a \in R$, $\exists!\ u \in R^\times$ and $F: \mathcal{P} \longrightarrow \mathbb{N}$ such that

$$a = u \prod_{p \in \mathcal{P}} p^{F(p)}.$$

For $I \subseteq R$ ideal, set $\Phi(I) = \{(p,k) \in \mathcal{P} \times \mathbb{N} \mid I \leq \langle p^{k+1} \rangle\}$

<u>Note</u>: I is uniquely determined by $\Phi(I)$.

$$I = 0 \iff \Phi(I) = \mathcal{P} \times \mathbb{N}.$$

$$I = \langle a \rangle : \quad p^{k+1} \mid a \iff I \subseteq \langle p^{k+1} \rangle$$

<u>Note</u>: Set $M = R/I$. $\quad p^k M / p^{k+1} M \neq 0 \iff (p,k) \in \Phi(I)$.

<u>Note</u>: If $M \cong M_1 \oplus M_2$ then

$$p^k M / p^{k+1} M \cong p^k M_1 / p^{k+1} M_1 \oplus p^k M_2 / p^{k+1} M_2$$

<u>Thm</u> R PID, M f.g. R-module. Then $\exists!$ chain of <u>proper</u> ideals $R \supsetneq I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ such that $M \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_m$.

<u>Proof</u>

<u>Existence</u>: $R^n \xrightarrow{A} R^m \longrightarrow M \longrightarrow 0$, $\quad A \in \mathrm{Mat}(m \times n, R)$

A equiv. to $\mathrm{diag}(d_1, d_2, \ldots, d_m)$, $\quad \langle d_1 \rangle \supseteq \langle d_2 \rangle \supseteq \cdots \supseteq \langle d_m \rangle$.

$M \cong \mathrm{Coker}(A) \cong R/\langle d_1 \rangle \oplus \cdots \oplus R/\langle d_m \rangle$.

Drop $R/\langle d_i \rangle$ if $\langle d_i \rangle = R$.

<u>Uniqueness</u>: $\Phi(I_1) \subseteq \Phi(I_2) \subseteq \cdots \subseteq \Phi(I_m)$.

For $(p,k) \in \mathcal{P} \times \mathbb{N}$: $\quad \dim_{R/\langle p \rangle} \left(p^k M / p^{k+1} M \right) = \#\{ j \mid (p,k) \in \Phi(I_j) \}$

$\therefore$ The sets $\Phi(I_j)$ are uniquely determined by the integers $\dim_{R/\langle p \rangle} \left(p^k M / p^{k+1} M \right)$.

$\square$

R PID, M f.g. R-module.

$\mathrm{tor}(M) = \{x \in M \mid \exists\, 0 \neq a \in R : ax = 0\} = \mathrm{Ker}(M \longrightarrow M \otimes_R K(R))$

Example $R = \mathbb{Z}$. $\mathrm{tor}(\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}) = \mathbb{Z}/20\mathbb{Z}$.

Cor $M \cong R^{\mathrm{rank}(M)} \oplus \mathrm{tor}(M). \cong M/\mathrm{tor}(M) \oplus \mathrm{tor}(M)$

Note $\mathrm{tor}(M)$ is well def. submodule of M, $R^{\mathrm{rank}(M)}$ is not.

Chinese Remainder Thm

R commutative ring, $I, J \subseteq R$ ideals, $I + J = R$.
Then $R/I \cap J \cong R/I \oplus R/J$ and $I \cap J = IJ$

Proof

Choose $a \in I$, $b \in J$ such that $a + b = 1$.

$IJ \subseteq I \cap J$ always true.

Let $x \in I \cap J$. $x = (a+b)x = ax + bx \in IJ$. $\therefore IJ = I \cap J$.

$\phi : R \longrightarrow R/I \oplus R/J$, $\phi(x) = (x + I, x + J)$.

$\mathrm{Ker}(\phi) = I \cap J$

Let $(y + I, z + J) \in R/I \oplus R/J$.

$x = by + az$. $\quad x + I = by + ay + I = y + I$

$\phi(x) = (y + I, z + J)$. $\quad x + J = bz + az + J = z + J$.

□

Cor $\exists$ prime powers $q_1, \dots, q_k \in R \setminus R^\times$, unique up to units/reordering, such that $M \cong R^{\mathrm{rank}(M)} \oplus R/\langle q_1 \rangle \oplus \cdots \oplus R/\langle q_k \rangle$.

Proof WLOG $\mathrm{rank}(M) = 0$, $M = \mathrm{tor}(M)$.

Existence: $M = R/\langle d_1 \rangle \oplus \cdots \oplus R/\langle d_m \rangle$, $d_1, \dots, d_m$ invariant factors.

$d_i = q_1 q_2 \cdots q_\ell$ product of prime powers. CRT $\Rightarrow$ $R/\langle d_i \rangle = R/\langle q_1 \rangle \oplus \cdots \oplus R/\langle q_\ell \rangle$
For distinct primes.

<u>Uniqueness</u>: Assume $M \cong R/\langle q_1 \rangle \oplus \cdots \oplus R/\langle q_k \rangle$.

WLOG: $q_1, \ldots, q_{l_1}$ powers of a maximal set of distinct primes, and highest powers of these primes.

WLOG: $q_{l_1+1}, \ldots, q_{l_2}$ highest powers remaining of primes dividing $\prod_{j=l_1+1}^{k} q_j$.

etc.

$$M \cong R/\langle q_1 q_2 \cdots q_{l_1} \rangle \oplus R/\langle q_{l_1+1} q_{l_1+2} \cdots q_{l_2} \rangle \oplus \cdots$$

$$\langle q_1 q_2 \cdots q_{l_1} \rangle \subseteq \langle q_{l_1+1} q_{l_1+2} \cdots q_{l_2} \rangle \subseteq \cdots \subseteq R.$$

Ideals are unique, and $q_1, \ldots, q_k$ are determined by ideals. $\square$

$\hat{R} = \mathrm{End}_R(M) = \{ \phi : M \to M \text{ R-homomorphism} \}$

$\hat{R}$ is an R-algebra: $\mu : R \longrightarrow \hat{R}$, $\mu(a)(x) = ax$, $a \in R$, $x \in M$

$\phi\, \mu(a) = \mu(a)\, \phi$ since $\phi(ax) = a\,\phi(x)$.

<u>Thm</u> R PID, M f.g. R-module. Then $Z(\hat{R}) = \mu(R)$.

<u>Proof</u> $M = R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_m$, $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$.

$\iota_j : R/I_j \xrightarrow{\subseteq} M$, $\pi_j : M \twoheadrightarrow R/I_j$

Set $e_j = \iota_j(1 + I_j) = (0, \ldots, 0, \bar{1}, 0, \ldots, 0) \in M$
j-th entry.

M gen. by $e_1, \ldots, e_m$.

Def: $\varepsilon_j : M \xrightarrow{\pi_m} R/I_m \longrightarrow R/I_j \xrightarrow{\iota_j} M$

$(\bar{x}_1, \ldots, \bar{x}_m) \longmapsto (0, \ldots, 0, \bar{x}_m, 0, \ldots, 0)$
j-th entry.

$\varepsilon_j \in \hat{R} = \mathrm{End}_R(M)$.

Let $\phi \in Z(\hat{R})$.

$\varepsilon_m \phi(e_m) = a\, e_m$ for some $a \in R$.

<u>Claim:</u> $\phi = \mu(a)$.

Show: $\phi(x) = ax \quad \forall x \in M$.

$\phi(e_m) = \phi(\varepsilon_m(e_m)) = \varepsilon_m(\phi(e_m)) = a\, e_m$

$\phi(e_j) = \phi(\varepsilon_j(e_m)) = \varepsilon_j(\phi(e_m)) = \varepsilon_j(a\, e_m) = a\, e_j$

$\square$

<u>Endomorphisms of vector spaces</u>

k Field, V k-vector space, $\dim(V) < \infty$.

Let $\varphi \in \mathrm{End}_k(V)$

$R = k[x]$ PID, $\quad \mu : R \longrightarrow \mathrm{End}_k(V)$, $x \mapsto \varphi$, $f(x) \mapsto f(\varphi)$.

V R-module. $x.v = \varphi(v)$ for $v \in V$.

$\hat{R} = \mathrm{End}_R(V) = \{\psi \in \mathrm{End}_k(V) \mid \psi\varphi = \varphi\psi\} \subseteq \mathrm{End}_k(V)$.

<u>Cor</u> Let $\varphi, \psi \in \mathrm{End}_k(V)$. Assume: $\forall h \in \mathrm{End}_k(V)$: $h\varphi = \varphi h \Rightarrow h\psi = \psi h$.
Then $\psi = f(\varphi)$ for some $f \in k[x]$.

<u>Proof</u>

$h\varphi = \varphi h \iff h \in \mathrm{End}_R(V)$

Assumption: $\psi \in Z(\mathrm{End}_R(V))$

$\Rightarrow \psi = \mu(f)$ for some $f \in k[x]$ by Thm.

$\square$

<u>Cor</u> $Z(\mathrm{End}_k(V)) = k$.

<u>Proof</u> Take $\varphi = 1$. $\square$

Basis of V: $\{v_1, \dots, v_n\}$

$$\varphi(v_j) = \sum_{i=1}^{n} a_{ij} v_i \quad , \qquad A = (a_{ij}) \in \mathrm{Mat}(n \times n, k)$$

<u>Lemma</u> $V \cong \mathrm{Coker}(xI_n - A)$ as R-module.

<u>Proof</u> Show $0 \xrightarrow{\text{[redacted]}} R^n \xrightarrow{xI-A} R^n \xrightarrow{\pi} V \longrightarrow 0$ is exact.

$$e_i \mapsto v_i$$

$$f(x)\, e_i \mapsto f(\varphi)(v_i).$$

$$\pi\big((xI-A)\, e_i\big) = \pi(x e_i - A e_i) = \varphi(v_i) - \varphi(v_i) = 0$$

Assume $\mathrm{Im}(xI-A) \subsetneq \mathrm{Ker}(\pi)$.

Let $u = u_0 + x u_1 + \dots + x^d u_d \in \mathrm{Ker}(\pi) - \mathrm{Im}(xI-A)$

with $u_i \in k^n \subseteq R^n$ and d <u>minimal</u>.

$$u - (xI-A)\, x^{d-1} u_d = u - x^d u_d + x^{d-1} A u_d \in \mathrm{Ker}(\pi) - \mathrm{Im}(xI-A) \ \lightning$$

$\square$

<u>Def</u> The invariant factors of $\varphi \in \mathrm{End}_k(V)$ are the $\boxed{\text{monic}}$ invariant factors $d_1, d_2, \dots, d_m \in R$ of V as R-module.

$$V \cong R/\langle d_1 \rangle \oplus R/\langle d_2 \rangle \oplus \dots \oplus R/\langle d_m \rangle \ , \quad \langle d_1 \rangle \supseteq \langle d_2 \rangle \supseteq \dots \supseteq \langle d_m \rangle.$$

<u>Note</u> $xI_n - A \in \mathrm{Mat}(n \times n, R)$ equivalent to $\mathrm{diag}(\underbrace{1, 1, \dots, 1}_{n-m}, d_1, d_2, \dots, d_m)$

Characteristic polynomial of φ:

$$\chi_\varphi(x) = \det(xI_n - A) = d_1 d_2 \cdots d_m \quad \text{product of invariant factors.}$$

<u>Claim</u> Minimal poly of φ = last **inv.** factor $d_m \in \mathbf{R}$.

Show: $\varphi_i : R/\langle d_i \rangle \xrightarrow{x\cdot} R/\langle d_i \rangle$ has min. poly d_i.

$$f(\varphi_i) = 0 \iff f(\varphi_i)(\bar{1}) = 0 \iff \overline{f(x)} = 0 \iff f(x) \in \langle d_i \rangle$$

Example $M = \mathbb{Z}^4 / \langle 2e_1 + 3e_2 + 4e_3 + 5e_4 ,\ 4e_1 + 5e_2 + 6e_3 + 7e_4 ,\ 20e_2 \rangle$

$M \cong \mathrm{Coker}(A)$

$$A = \begin{bmatrix} 2 & 4 & 0 \\ 3 & 5 & 20 \\ 4 & 6 & 0 \\ 5 & 7 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 20 \\ 2 & 4 & 0 \\ 4 & 6 & 0 \\ 5 & 7 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 2 & 2 & -40 \\ 4 & 2 & -80 \\ 5 & 2 & -100 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 40 \\ 0 & 2 & 80 \\ 0 & 2 & 100 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 40 \\ 0 & 0 & 40 \\ 0 & 0 & 60 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 20 \\ 0 & 0 & 0 \end{bmatrix}$$

Invariant factors of $\mathbb{Z}$-module M: 2, 20

$M \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$

Example $V = k^3$, $\varphi = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix} \in \mathrm{End}_k(V)$

As $k[x]$-module: $V \cong \mathrm{Coker}(A)$

$$A = xI - \varphi = \begin{bmatrix} x-\lambda & -1 & 0 \\ 0 & x-\lambda & -1 \\ 0 & 0 & x-\lambda \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \lambda - x \\ \lambda - x & 1 & 0 \\ 0 & \lambda - x & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \lambda - x \\ 0 & 1 & -(\lambda - x)^2 \\ 0 & \lambda - x & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & \lambda - x \\ 0 & 1 & -(\lambda - x)^2 \\ 0 & 0 & (\lambda - x)^3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-\lambda)^3 \end{bmatrix}$$

Invariant factor of φ: $(x-\lambda)^3$

Isomorphism of vector spaces:

$$\mu : V \xrightarrow{\cong} k[x]/\langle (x-\lambda)^3 \rangle$$

$e_1 \longmapsto \overline{(x-\lambda)^2}$

$e_2 \longmapsto \overline{x-\lambda}$

$e_3 \longmapsto \overline{1}$

$\varphi(e_1) = \lambda e_1$ $\qquad x \cdot \overline{(x-\lambda)^2} = \lambda \overline{(x-\lambda)^2}$

$\varphi(e_2) = \lambda e_2 + e_1$ $\qquad x \cdot \overline{x-\lambda} = \lambda \overline{x-\lambda} + \overline{(x-\lambda)^2}$

$\varphi(e_3) = \lambda e_3 + e_2$ $\qquad x \cdot \overline{1} = \lambda \overline{1} + \overline{x-\lambda}$

Canonical forms of matrices

$V = k^n$, $\varphi \in \mathrm{End}_k(V)$, $R = k[x]$. PID.

$V \cong R/\langle f_1 \rangle \oplus \cdots \oplus R/\langle f_m \rangle$, $f_1, \ldots, f_m \in R$.

$\varphi(v) = xv$. WLOG $f_1, \ldots, f_m$ prime powers in R.

Idea: Pick basis of V by picking basis of each $R/\langle f_i \rangle$, then express φ in this basis.

WLOG $V = R/\langle f \rangle$, $f = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, $a_i \in k$

Basis: $\{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \overline{x^{d-1}}\}$

$\varphi(\overline{x^i}) = x \cdot \overline{x^i} = \overline{x^{i+1}}$, $\varphi(\overline{x^{d-1}}) = \overline{x^d} = -a_0 - a_1\bar{x} - \cdots - a_{d-1}\overline{x^{d-1}}$

$$\varphi = \begin{bmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & 0 & \vdots \\ 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & -a_{d-1} \end{bmatrix}$$ (Rational canonical form)

Jordan Normal Form

Assume $k = \bar{k}$ alg. closed.

$V = R/\langle f \rangle$, $f \in R$ prime power.

$f = (x-\lambda)^d$, $\lambda \in k$

Basis: $\{\overline{(x-\lambda)^{d-1}}, \overline{(x-\lambda)^{d-2}}, \ldots, \overline{x-\lambda}, \bar{1}\}$

$\varphi(\overline{(x-\lambda)^{d-i}}) = x\,\overline{(x-\lambda)^{d-i}} = \lambda\,\overline{(x-\lambda)^{d-i}} + \overline{(x-\lambda)^{d-i+1}}$

$$\varphi = \begin{bmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & & 0 \\ 0 & 0 & \lambda & 1 & & \vdots \\ \vdots & \vdots & & \ddots & & \\ \vdots & \vdots & & & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}$$ $d \times d$ Jordan block.

Lemma R PID, $a, b \in R$, $b \neq 0$.

Then $\mathrm{Hom}_R(R/\langle a\rangle, R/\langle b\rangle) \cong \langle c\rangle/\langle b\rangle$, $c = \frac{b}{\gcd(a,b)}$

Proof

$$\mathrm{Hom}_R(R/a, R/b) \xrightarrow{\subseteq} R/b, \quad \varphi \longmapsto \varphi(\bar{1}).$$

If $\varphi(\bar{1}) = r + \langle b\rangle$ then $\varphi(x + \langle a\rangle) = xr + \langle b\rangle$.

$r + \langle b\rangle \in \text{Image} \iff ar \in \langle b\rangle \iff r \in \langle c\rangle$.

□

Cor Let $a, b \in R$, $a \mid b$. Then

$$\mathrm{Hom}_R(R/\langle a\rangle, R/\langle b\rangle) \cong \mathrm{Hom}_R(R/\langle b\rangle, R/\langle a\rangle) \cong R/\langle a\rangle.$$

Proof $\gcd(a,b) = a$. $\langle b/a\rangle/\langle b\rangle \cong \langle a/a\rangle/\langle a\rangle \cong R/\langle a\rangle$. □

Frobenius' Thm

Let $\varphi \in \mathrm{End}_k(V)$ have invariant factors $f_1, \dots, f_m \in k[x]$.

Then $\dim_k \{\psi \in \mathrm{End}_k(V) \mid \psi\varphi = \varphi\psi\} = \sum_{i=1}^{m} (2m - 2i + 1) \deg(f_i)$.

Proof

$R = k[x]$, $V \cong R/\langle f_1\rangle \oplus \cdots \oplus R/\langle f_m\rangle$.

LHS $= \dim_k \mathrm{End}_R(V)$.

$$\mathrm{End}_R(V) \cong \bigoplus_{i,j} \mathrm{Hom}_R(R/\langle f_i\rangle, R/\langle f_j\rangle)$$

$$\mathrm{Hom}_R(R/\langle f_i\rangle, R/\langle f_j\rangle) \cong R/\langle f_{\min(i,j)}\rangle \qquad \dim = \deg(f_{\min(i,j)})$$

$$\sum_{i,j} \deg(f_{\min(i,j)}) = (2m-1)\deg(f_1) + (2m-3)\deg(f_2) + \cdots + \deg(f_m)$$

□

Note V is a cyclic R-module (gen. by 1 elt)
$\Leftrightarrow$ φ has one **invariant** factor.

Cor V cyclic R-module $\Leftrightarrow$ All $\psi \in End_k(V)$ that commute with φ are polynomials in φ.

Proof
$\Rightarrow$: If $V = R/\langle f \rangle$ then $End_R(V) \cong R/\langle f \rangle$

$$\varphi \longleftrightarrow \bar{x}$$

$\Leftarrow$: Let $f_1, \ldots, f_m \in R$ be inv. factors of φ.

f_m = min. poly of φ

$End_R(V) = k[\varphi] \Rightarrow$

$$\sum_{i=1}^{m} (2m-2i+1)\deg(f_i) = \deg(f_m) \Rightarrow m = 1.$$

$\square$