2/22

Friday, February 22, 2019 11:30

$M = R/(a)$

$$\boxed{\begin{array}{c} p^k R \cong R \\ p^k \longleftrightarrow 1 \end{array}}$$

Some isomorphism theorem

$$p^k(R/(a)) \big/ p^{k+1}(R/(a)) \cong \left(p^k R / p^{k+1} R\right) \big/ (a, p^{k+1})$$
$$\cong R/p \big/ \left(\tfrac{a}{p^k}, p\right)$$

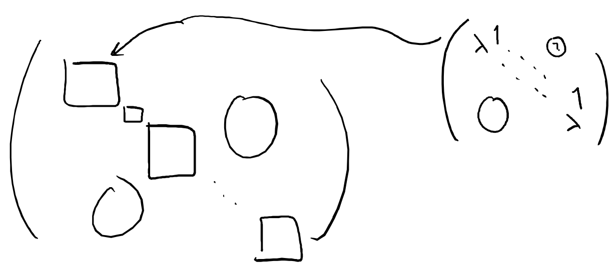
F - field, V - F-vector space, $\dim_F(V) < \infty$.

$\varphi : V \longrightarrow V$, $\varphi \in \mathrm{End}_F(V)$.

$A_\varphi = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$. Find the simplest form of the matrix.

Jordan Normal Form :

(but you need an algebraically closed field).



V is an $F[x]$ module where $x \cdot u = \varphi(u)$.

$p(x) \cdot u = (p(\varphi))(u)$.

W is a submodule of V iff it's a subspace & $\varphi(W) \subseteq W$.

that is, W is a φ-invariant subspace of V.

If $\{u_1, \dots, u_n\}$ is a basis in V s.t. $\{u_1, \dots, u_k\}$ is a basis in W,

then A_φ in this basis is

$$\begin{array}{cc} \left(\begin{array}{c|c} A_1 & * \\ \hline O & A_2 \end{array}\right) & \begin{array}{c} \vdots \\ k \end{array} \\ 1 \dots k & \end{array}$$

A_1 is matrix of $\varphi\big|_W$,

A_2 is matrix of $\tilde{\varphi} : V/W \to V/W$ where $\tilde{\varphi}(u + W) = \varphi(u) + W$.

If $V = W_1 \oplus W_2$, $\varphi(W_1) \subseteq W_1$, $\varphi(W_2) \subseteq W_2$.

Then let $\{u_1, \dots, u_k\}$ be a basis in W_1, $\{u_{k+1}, \dots, u_n\}$ a basis in W_2.

Then in the basis $\{u_1, \dots, u_n\}$, $A_\varphi = \begin{pmatrix} A_1 & O \\ O & A_2 \end{pmatrix}$.

$A_1 \leftrightarrow \varphi\big|_{W_1}$ $A_2 \leftrightarrow \varphi\big|_{W_2}$.

Since V is finite-dim, it has rank 0 as an $F[x]$-module.

(Otherwise, it would contains a copy of $F[x]^k$, $k = \operatorname{rank}_{F[x]}(V)$.)

but $F[x]$ is ∞-dim over F.

So V is a torsion module.

Let $I = \mathrm{Ann}(V) \subseteq F[X]$. $F[X]$ is a PID, so $I = (m_\varphi(x))$.

$m_\varphi(x) \cdot u = 0 \quad \forall u \in V.$

$(m_\varphi(\varphi))(u) = 0 \quad \forall u \in V.$

So $m_\varphi(\varphi) = 0$ transformation.

If $P(\varphi) = 0$ then $p(x)$ is a multiple of $m_\varphi(x)$.

m_φ is called the minimal polynomial of φ.

$F[x]$ is a PID so:

<u>Theorem</u>: $V = V_1 \oplus \cdots \oplus V_m$ where V_i are cyclic $F[x]$-modules.

$V_i \cong F[x]/(P_i(x)) \quad \forall i$, and $P_1(x) \mid P_2(x) \mid \cdots \mid P_m(x)$.

So V is a direct sum of φ-invariant subspaces $V_1, \dots, V_k$.

$\forall i$, $P_i(x)$ generates $\mathrm{Ann}(V_i)$, so $P_i(x) = m_{\varphi|_{V_i}}(x)$.

And $m_\varphi(x) = P_m(x)$.

In the basis of V that agrees with $V = V_1 \oplus \cdots \oplus V_m$,

the matrix of φ is $\begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_m} \end{pmatrix}$ - block diagonal,

$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_m \end{pmatrix}$ - block diagonal,

where $\forall i$, $A_i = A_{\varphi|_{V_i}}$.

Let V be a cyclic $F[x]$ module. $V \cong F[x]/(p)$

$u \leftrightarrow 1 \bmod p$.

$$V = F[x]u = \{f(\varphi)(u),\ f \in F[x]\}.$$

$$V = \text{Span}\{u, \varphi(u), \varphi^2(u), \dots\}$$

u is called a cyclic vector for φ.

$V \cong F[x]/(p(x))$. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

basis is $\{1, x, x^2, \dots, x^{n-1}\}$.

$u \longleftrightarrow 1$

$\varphi(u) \leftrightarrow x$

$\forall f \in F[x]$, $f = pg + r$ where $\deg(r) < \deg(p) = n$.

So basis in V is $\{u, \varphi(u), \varphi^2(u), \dots, \varphi^{n-1}(u)\}$.

In $F[x]/(p(x))$, $x^n = -a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$,

so in V, $\varphi^n(u) = -a_{n-1}\varphi^{n-1}(u) - \cdots - a_1\varphi(u) - a_0 u$.

(so $p(\varphi) = 0$ transfm).

$$\begin{array}{ccccccc} u & \varphi(u) & \varphi^2(u) & \cdots & \varphi^{n-1}(u) & & \\ \varphi \downarrow & & & & & & \\ \varphi(u) & \varphi^2(u) & \varphi^3(u) & \cdots & \varphi^n(u) & = & -\sum_0^{n-1} a_i \varphi^i(u) \end{array}$$

The matrix of φ is

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & & \vdots & -a_1 \\ 0 & 1 & 0 & & \vdots & \vdots \\ \vdots & 0 & 1 & & \vdots & \vdots \\ \vdots & \vdots & 0 & & 0 & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} = \left(\begin{array}{cccc|c} 0 & & & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ 0 & & \ddots & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{array}\right)$$ - companion matrix of p.

So,

<u>Theorem</u>: $\forall\, \varphi \in \mathrm{End}(V)$, $\exists$ basis s.t. A_φ looks like

$$\begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_m} \end{pmatrix} \text{ where } A_i = \left(\begin{array}{cccc|c} 0 & & & 0 & * \\ 1 & \ddots & & & * \\ & \ddots & \ddots & & \vdots \\ 0 & & \ddots & 0 & \vdots \\ & & & 1 & * \end{array}\right),$$

The companion matrix of pol-l $p_i \neq$ const, and $p_1 | p_2 | \cdots | p_m = m_\varphi$.

This is the "rational normal form" of φ.

Note: p_i can be taken monic, and then they are uniquely defined.

Also, there is another form $\begin{pmatrix} \boxed{B_1} & & & 0 \\ & \boxed{B_2} & & \\ & & \ddots & \\ 0 & & & \boxed{B_\ell} \end{pmatrix}$ where each B_j is the companion matrix of the pol-l $q_j(x)^{r_j}$ where q_j is an irreducible polynomial, and $r_j \in \mathbb{N}$.

Such a form is also unique (up to permutation of blocks).

Note: P_i are invariant factors

$q_{ij}^{r_{ij}}$ are elementary divisors