Modules?

What is a module?

What can we do to one?

Examples

1) Vector spaces

2) A-invariant subspaces: modules over $\mathbb{F}[A]$, e.g.

(a) walk modules: $\mathrm{span}\{A^r x : r \geq 0\} =: \langle x \rangle_A$

(b) equitable partitions

3) $Mat_{d\times d}(\mathbb{F})$; $R = Mat_{d\times d}(\mathbb{F})$

$M \in Mat_{d\times d}(\mathbb{F})$; $A, B \in Mat_{d\times d}(\mathbb{F})$

$L_A : M \longmapsto AM$; $R_B : M \to MB$

$L_A L_B : M = A(BM) = (AB)M = L_{AB}(M)$ $L_A L_B = L_{AB}$

$R_A R_B (M) = MBA = R_{BA}(M)$ opposite ring

redefine R

$R_A(M) = MA^*$, $R_A R_B (M) = MB^* A^* = M(AB)^*$

Operations

1) submodules

2) sums, direct sums, $M \oplus N$

3) quotients: M/N

4) homomorphisms: $\varphi : M \to N$

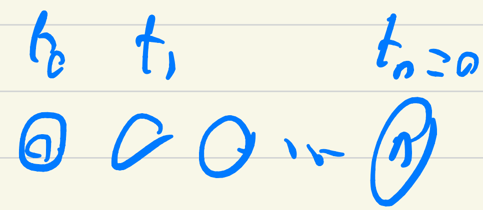
$$\varphi(rm) = r\varphi(m), \quad r \in R$$

Module example: control theory

We have a system of $n+1$ bodies arranged in a line. At time r, the temperature of the i-th body is $t_i(r)$ $(r \in \mathbb{Z})$. Assumptions:

(a) we control the temperature of the 0-th body; at time r it is $u(r)$.

(b) $t_n(r) = 0$ for all r.



(c) If $0 < i < n$, then

$$t_i(r+1) = \frac{1}{4} t_{i-1}(r) + \frac{1}{2} t_i(r) + \frac{1}{4} t_{i+1}(r)$$

Assume $t = (t_0, \ldots, t_n)^T$. Then

$$t(r+1) = A\,t(r) + u(r)\,b.$$

If $n = 4$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} & 0 & 0 \\ 0 & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} & 0 \\ 0 & 0 & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad b = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

By choosing different sequences $u(0), u(1), \ldots, u(n)$ we can reach a variety of different temperature distributions. Which ones?

Assume $t(0) = 0$. Then

$$t(1) = u(0)b$$

$$t(2) = u(1)b + u(0)Ab$$

$$t(3) = u(2)b + u(1)Ab + u(0)A^2b$$

$$\vdots$$

and if

$$W_r = (b \; Ab \cdots A^{r-1}b)$$

then

$$t(r+1) = W_r \begin{bmatrix} u(0) \\ \vdots \\ u(r) \end{bmatrix}$$

Conclusion We can reach a state $t(r+1)$ if & only if it lies in the A-module $\langle b \rangle_A$.

Problem Suppose we start in some (non-zero) state $t(0)$ and the system state at time r is $t(r) = A^r t(0)$. If we are given the average values $\frac{1}{n+1}\sum_{i=0}^{n} t_i(r)$ at each time, can we deduce the initial state?

controllable

$\langle b \rangle_A = \mathbb{R}^{n+1}$

$\langle c \rangle_{A^T} = \mathbb{R}^{n+1}$

observable

START 27-09-21

Complements $\longleftrightarrow$ Sums $\longleftrightarrow$ Idempotents

Complements → direct sums

If $M_1, M_2 \leq V$, their sum $M_1 + M_2$ is

$$\{u_1 + u_2 : u_1 \in M_1, \ u_2 \in M_2\}$$

If $M_1 \cap M_2 = \langle 0 \rangle$ and $M_1 + M_2 = V$, then M_2 is a complement to M_1.

If M_1 has a complement M_2, then V is isomorphic to the direct sum of M_1 & M_2. We may write this as $M_1 \oplus M_2$.

Assume $M_1, \dots, M_k \leq V$. Define $M_i' = \sum_{r \neq i} M_r$

Then V is the direct sum of $M_1, \dots, M_k$ ($V \cong M_1 \oplus \dots \oplus M_k$) if V is the direct sum of M_i & M_i', for each i.

Sums → idempotents

If $V = M_1 + M_2$ and $w \in V$, then $v = v_1 + v_2$ $(v_i \in M_i)$. If also $v = v_1' + v_2'$ $(v_i' \in M_i)$, then

$$v_1 - v_1' = v_2' - v_2$$

in M_1

in M_2

and so $v_1 - v_1', v_2' - v_2 \in M_1 + M_2$. Hence if $M_1 \cap M_2 = \langle 0 \rangle$, the decomposition of v is unique and the map $\pi_1 : V \to V$ given by

$$\pi_1(v) = v_1$$

is an idempotent.

$\pi_1^2 = \pi_1$

$(1 - \pi_1)^2 = (1 - \pi_1)$

If $r \in R$, then $rw = rw_1 + rw_2$

and $\pi_1(rw) = r\pi_1(w)$.

Moral Direct sum decompositions correspond to idempotents in $\operatorname{End}(M)$ abelian group that commute with R, i.e. in $\operatorname{End}_R(M)$.

Given such π, decomposition is

$$V = \pi(V) + (1-\pi)V$$

Lemma Assume $V = U_1 \oplus U_2$ and π is the projection onto U_1. Then an endomorphism A fixes U_1 & U_2 if and only if $A\pi = \pi A$.

If P is the matrix representing π, then

$$A = PAP + (I-P)A(I-P)$$

(A is block diagonal)

Remark: $x_1, \dots, x_d$ is a basis for V if & only if $V = \langle x_1 \rangle \oplus \cdots \oplus \langle x_d \rangle$

Primary Decomposition

(decomposing modules for $\mathbb{F}[A]$)

Minimal polynomials

- ψ_A monic polynomial ψ of least degree such that $\psi(A) = 0$. (Existence uses the fact that $\mathbb{F}[t]$ is a principal ideal domain.)

- $\psi_{A,x}$ monic polynomial of least degree such that $\psi(A)x = 0$.

Clearly $\psi_{A,x}$ divides ψ_A. Also $\psi_{A,x}$ is minimal polynomial of restriction of A to $\operatorname{span}\{A^r x : r \geq 0\}$

Lemma: $\mathbb{F}[A] \cong \mathbb{F}[t]/(\psi_A(t))$

Hence an $\mathbb{F}[A]$-module is an $\mathbb{F}[t]$-module.

Lemma Any polynomial $\psi(t)$ in $\mathbb{F}[t]$ admits a factorization $\psi(t) = \prod_{i=1}^{m} \psi_i(t)$ where $\psi_i(t) \in \mathbb{F}$ and $\psi_i(t)$ is a power of an irreducible.

If $\psi_i' := \psi/\psi_i$, then:

$$\mathbb{F}[t]/(\psi(t)) \cong \bigoplus_{i=1}^{m} \mathbb{F}[t]/\psi_i'(t)$$

Theorem Assume $\psi(t)$ has primary factorization $\psi = \prod_{i=1}^{r} \psi_i$. Set $\psi_i' = \psi/\psi_i$. Then there are polynomials $a_i(t)$ such that

$$\sum_i a_i \psi_i' = 1.$$

Set $E_i := a_i(A)\psi_i'(A)$. Then

$$E_i^2 = E_i, \quad E_i E_j = 0 \ (i \neq j), \quad \sum E_i = I$$

The minimal polynomial of $A\restriction \mathrm{im}(E_i)$ is ψ_i.

Degree of $\psi_A(t)$?

Lemma If $T \in \mathrm{End}(V)$, there is a vector x in V such that $\psi_{T,x} = \psi_T$.

$\mathbb{F}$

Proof. Assume first that $\psi_T = p(t)^m$, where p is irreducible. Then $p(T)^m = 0$ and $p(T)^{m-1} \neq 0$. Choose x so that $p(T)^{m-1}x \neq 0$.

Suppose φ is monic and $\varphi(T)x = 0$. Set $\gamma(t) = \gcd(p^m, \varphi)$. Then $\gamma = p^m$ or $\gamma \mid p^{m-1}$. As $p(T)^{m-1}x \neq 0$, we have $\gamma = p^m$ and $\psi_T \mid \varphi$. So $\psi_T = \psi_{T,x}$.

Assume ψ_T has coprime factorization $\psi_T = \psi_1 \psi_2$ and U_1, U_2 are the direct summands corresponding to ψ_1 & ψ_2. Let E_1 & E_2 be the associated idempotents. Choose $x_i \in U_i$ so that the minimal polynomial of T on U_i is ψ_i.

If φ is monic & $\varphi(T)(x_1+x_2)=0$, then $\varphi \mid \psi_T$. Now

$$0 = E_1 \varphi(T)(x_1+x_2) = \varphi(T) E_1 (x_1+x_2) = \varphi(T) x_1$$

and so $\psi_1 \mid \varphi$. Similarly $\psi_2 \mid \varphi$ and hence $\psi_T \mid \varphi$.

$\square$

Root spaces

we work over $\mathbb{C}$,
any alg. closed
field will do.

$T \in \mathrm{End}(V)$

$$\psi_T = \prod_{i=1}^{k} (t-\theta_i)^{m_i}$$

Then $V = \bigoplus_{i=1}^{k} \ker((T-\theta_i)^{m_i})$. We say

$\ker((T-\theta_i I)^{m_i})$ is a root space. If

$(T-\theta_i I)^r v = 0$ for some r then v is a root vector; the least value of r is its index.

The 0-vector is a root vector of index 0 (the only one).

A root vector of index one is an eigenvector.

Theorem If $T \in \mathrm{End}(V)$, then V has a basis consisting of root vectors for T.

Lemma If $v_1, \dots, v_m$ are non-zero root vectors with distinct eigenvalues $\theta_1, \dots, \theta_m$, they are linearly independent.

Examples

(a) Suppose V has basis $e_1, \dots, e_n$. Define T in $\mathrm{End}(V)$ by

$$Te_i = \begin{cases} e_{i+1}, & i < n; \\ 0, & i = n. \end{cases}$$

Then the minimal polynomial of T is t^n, and V is a root space for T

$\mathbb{F}[t]/(t^n)$

(b) $V = C^\infty(\mathbb{R})$. D is differentiation.

Define an operator M_λ on V by

$$M_\lambda(f) = e^{\lambda t} f$$

Claim $M_\lambda D M_{-\lambda} = D - \lambda I$

Claim $\ker(D-\lambda I)^r = \{ e^{-\lambda t} p : p \in \mathbb{R}[t],\ \deg(p) < r \}$

(c) $V = \mathbb{C}^{\mathbb{N}}$, S is left shift

$$S : (a_0, a_1, \dots) \longmapsto (a_1, a_2, \dots)$$

Define M_λ by

$$M_\lambda (a_0, a_1, \dots) = (a_0, \lambda a_1, \lambda^2 a_2, \dots)$$

Claims:

$$S - \lambda I = M_\lambda (S - I) M_{-\lambda}$$

$$\ker (S - \lambda I)^r = \{ (p(0), \lambda p(1), \lambda^2 p(2), \dots) : \deg(p) < r \}$$

Example: solving linear recurrences

Consider

$$f_{n+1} = f_n + f_{n-1}$$

(why be original?)

If $f = (f_0, f_1, \ldots)$, then f satisfies this recurrence if & only if $(S^2 - S - I)f = 0$, i.e. $f \in \ker(S^2 - S - I)$.

Set $K = \ker(S^2 - S - I)$. Then

(a) K is S-invariant

(b) $\dim(K) = 2$.

(c) minimal polynomial S on K is $t^2 - t - 1$.

Therefore K has a basis of root vectors.

The zero of χ_S are

θ, τ

$$\frac{1}{2}(1 \pm \sqrt{5})$$

Since zeros of ψ are simple, all non-zero root vectors are eigenvectors. Therefore

$$f = A(1, \theta, \theta^2, \dots) + B(1, \tau, \tau^2, \dots)$$

$$f_{n+1} = 3f_{n-1} - f_{n-2}$$

$$(S^3 - 3S + 2) f = 0$$

$$t^3 - 3t + 2 = (t-1)^2 (t+2)$$

$$C(1, -2, 4, -8, \dots)$$

$$(p(0), p(1), \dots) \qquad \deg(p) = 0, 1$$

$$f_n = A + nB + C(-2)^n$$

Diagonalizabity

A matrix is diagonalizable if it is similar to a diagonal matrix

What is the minimal polynomial of $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$?

Theorem Let A be an $n \times n$ matrix over an algebraically closed field $\mathbb{F}$. The following are equivalent:

(a) A is diagonalizable

(b) $\mathbb{F}^n$ has a basis that consists of eigenvectors of A

(c) The minimal polynomial ψ of A has no repeated factors

(a) $\Rightarrow$ (c) If two matrices are similar, they have the same minimal polynomial. The minimal poly of a diagonal matrix has no repeated factors. So (a) $\Rightarrow$ (c)

(c) $\Rightarrow$ (b) If ψ has no repeated factors, all non-zero root vectors are eigenvectors. Hence (c) $\Rightarrow$ (b).

(b) $\Rightarrow$ (a) Let the columns of L be eigenvectors. Then $AL = L$ where D is diagonal.

So we have a useful criterion for deciding if A is similar to a diagonal matrix.

What about a condition for deciding if matrices A & B are similar?

$$A = A^*$$

$$A^2 x = 0$$

$$A^* A x = 0$$

$$x^* A^* A x = 0$$

$$Ax = 0 \quad \Rightarrow \text{ no root vectors for } 0 \text{ with index} \geq 2$$

$$(A - \lambda I)^2 x = 0 \Rightarrow (A - \lambda I) x = 0$$