Lecture 13: Rational canonical form

Tuesday, February 6, 2018 11:27 PM

Let k be a field and $A \in M_n(k)$. Then $\phi_A : k[x] \to \mathrm{End}(k^n)$

$\phi_A(f(x)) := f(A)$

turns k^n to a $k[x]$-module. We denote this $k[x]$-mod by V_A. In the previous lecture we proved:

<u>Claim 1.</u> $\operatorname{rank}_{k[x]} V_A = 0$

<u>Claim 2.</u> $\exists\, f_1 | f_2 | \cdots | f_m$ s.t. $V_A \simeq k[x]/\langle f_1\rangle \oplus \cdots \oplus k[x]/\langle f_m\rangle$

<u>Claim 3,4</u> Suppose $f(x) = x^{\ell} + c_{\ell-1}x^{\ell-1} + \cdots + c_0$; and $c(f)$ is the companion matrix of f; that means

$$c(f) = \begin{bmatrix} 0 & & \mathbf{0} & -c_0 \\ 1 & \ddots & & -c_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 1 & -c_{\ell-1} \end{bmatrix}.$$ Then $V_{c(f)} \simeq k[x]/\langle f(x)\rangle$ (as $k[x]$-mod.)

<u>Theorem.</u> Let k be a field and $A \in M_n(k)$. Then there are unique monic polynomials $f_1, \ldots, f_m \in k[x]$ such that

(a) $f_1 | f_2 | \cdots | f_m$

(b) A is similar to $\begin{bmatrix} c(f_1) & & \\ & \ddots & \\ & & c(f_m) \end{bmatrix}$.

(This is called the rational canonical form of A; and f_i's are called the invariant factors of A.)

Lecture 13: Rational canonical form

Tuesday, February 6, 2018 11:45 PM

<u>Proof</u>. <u>Existence</u>. By Claim 2,3,4, we have

$$V_A \simeq V_{c(f_1)} \oplus \cdots \oplus V_{c(f_m)}, \quad \text{as } k[x]\text{-mod}.$$
$$\simeq V_{\underbrace{\operatorname{diag}(c(f_1),\ldots,c(f_m))}_{B}}$$

That means $\exists$ a $k[x]$-mod isomorphism

$$V_A \xrightarrow[\sim]{\Phi} V_B .$$

Hence $\Phi(x\cdot v) = x\cdot\Phi(v)$; this implies $\Phi(Av) = B\Phi(v)$.

$$\begin{tikzcd} k^n \arrow[r, "\Phi"] \arrow[d, "A"'] \arrow[dr, phantom, "\circlearrowleft"] & k^n \arrow[d, "B"] \\ k^n \arrow[r, "\Phi"', "\sim"] & k^n \end{tikzcd}$$

Hence $A = X_\Phi^{-1} B X_\Phi$, where $X_\Phi \in GL_n(k)$ is the matrix associated to Φ w.r.t. the standard basis.

<u>Uniqueness</u>. Suppose $g_1 | g_2 | \cdots | g_s$ are monic and

$$A = X^{-1}\begin{bmatrix} c(g_1) & & \\ & \ddots & \\ & & c(g_s)\end{bmatrix} X.$$

Then

$$\begin{tikzcd} k^n \arrow[r, "X"] \arrow[d, "A"'] \arrow[dr, phantom, "\circlearrowleft"] & k^n \arrow[d, "\operatorname{diag}(c(g_1),\ldots,c(g_s))"] \\ k^n \arrow[r, "X"] & k^n \end{tikzcd}$$

Then $V_A \simeq V_{\operatorname{diag}(c(g_1),\ldots,c(g_s))}$

$$\simeq V_{c(g_1)} \oplus \cdots \oplus V_{c(g_s)} \simeq k[x]/\langle g_1\rangle \oplus \cdots \oplus k[x]/\langle g_s\rangle$$

Now by the uniqueness part of f.g. mod. over a PID claim follows. ∎

Lecture 13: Minimal polynomial and invariant factors

Sunday, February 4, 2018 10:46 PM

Proposition. Let k be a field, and $A \in M_n(k)$. Suppose $f_1 | f_2 | \cdots | f_m$ are invariant factors of A. Then

(1) $f_m(A) = 0$

(2) $\{g(x) \in k[x] \mid g(A) = 0\} = \langle f_m(x) \rangle$; in particular f_1 is the smallest degree monic polynomial that vanishes at A.

Pf. • As we have seen, $V_A \simeq k[x]/\langle f_1(x)\rangle \oplus \cdots \oplus k[x]/\langle f_m(x)\rangle$.

$\Rightarrow f_m(x) \cdot V_A = 0 \Rightarrow f_m(A) = 0$

• $g(A) = 0 \Rightarrow g(x) \cdot V_A = 0 \Rightarrow g(x) \in \langle f_m(x) \rangle \Rightarrow f_m(x) | g(x)$. ∎

How can we find the invariant factors?

In your HW assignment, you will prove that

if $xI - A = \gamma_1 \begin{bmatrix} f_1(x) & & \\ & \ddots & \\ & & f_n(x) \end{bmatrix} \gamma_2$ for some $\gamma_1, \gamma_2 \in GL_n(k[x])$, and $f_1 | f_2 | \cdots | f_n$, then $f_{m+1}, \ldots, f_n$ are the invariant forms of A where $\deg f_m = 0$ and $\deg f_{m+1} > 0$.

This gives an algorithmic way of computing invariant factors.

Did not mention this in class

Lecture 13: Cayley-Hamilton's theorem

Sunday, February 4, 2018 10:55 PM

Theorem. Let k be a field, and $A \in M_n(k)$. Let $f(x)$ be the characteristic polynomial of A; that means

$$f_A(x) = \det(xI - A).$$

Let $m_A(x)$ be the minimal polynomial of A. Then

(1) $m_A(x) \mid f_A(x)$ (2) Any irreducible factor of $f_A(x)$ is an irreducible factor of $m_A(x)$.

Pf. (method 1, based on a HW assignment.)

Did not mention the 1st method in class

$\exists$ monic $f_1 \mid f_2 \mid \cdots \mid f_n$ and $\gamma_1, \gamma_2 \in GL_n(k[x])$ s.t.

$$xI - A = \gamma_1 \begin{bmatrix} f_1 & & \\ & \ddots & \\ & & f_n \end{bmatrix} \gamma_2 \quad \text{and}$$

the invariant factors are all the non-constant f_i's.

In particular $m_A(x) = f_n(x)$.

Then $$\underbrace{\det(xI - A)}_{\text{monic}} = \underbrace{\det(\gamma_1)}_{\text{in } k^\times} \cdot f_1(x) \cdots f_n(x) \cdot \underbrace{\det(\gamma_2)}_{\text{in } k^\times}$$

$\Rightarrow \det(xI - A) = f_{m+1}(x) \cdots f_n(x) \Rightarrow m_A(x) \mid f_A(x)$.

And, if $p(x)$ is irred. and $p(x) \mid f_A(x)$, then $\exists i$, $p(x) \mid f_i(x)$.

Hence $p(x) \mid f_n(x) = m_A(x)$. ∎

Lecture 13: Cayley-Hamilton's theorem

Monday, February 5, 2018 11:49 AM

<u>method 2</u>. Let $g_1 | g_2 | \cdots | g_m$ be the invariant factors of A.

Then $A \sim \mathrm{diag}(c(g_1), \ldots, c(g_m))$. Then

(1) $m_A(x) = g_m(x)$ and (2) $f_A(x) = f_{c(g_1)}(x) \cdot f_{c(g_2)}(x) \cdot \ldots \cdot f_{c(g_m)}(x)$.

$$f_{c(g)}(x) = \det \begin{bmatrix} x & & & c_0 \\ -1 & x & & c_1 \\ & -1 & \ddots & \vdots \\ 0 & & \ddots & \\ & & -1 & x+c_{\ell-1} \end{bmatrix}$$

$$= x \det \begin{bmatrix} x & & c_1 \\ -1 & \ddots & \vdots \\ & \ddots & \\ & -1 & x+c_{\ell-1} \end{bmatrix} + \det \begin{bmatrix} & & & c_0 \\ -1 & x & \cdots & c_2 \\ & \ddots & \ddots & \vdots \\ & & -1 & x+c_{\ell-1} \end{bmatrix}$$

$$= x\,(x^{\ell-1} + c_{\ell-1} x^{\ell-2} + \cdots + c_1) + (-1)^{\ell} c_0 (-1)^{\ell-2}$$

induction hypothesis

$$= x^{\ell} + c_{\ell-1} x^{\ell-1} + \cdots + c_1 x + c_0 = g(x).$$

Hence $f_A(x) = g_1(x)\, g_2(x) \cdots g_m(x)$. Now the rest of the argument goes as in method 1. ∎

We have proved the following stronger result:

<u>Theorem</u>. Let k be a field, $A \in M_n(k)$, and $g_1 | \cdots | g_m$ be the invariant factors of A. Then

$$m_A(x) = g_m(x) \quad \text{and} \quad f_A(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_m(x).$$

(And g_i's uniquely determine A upto similarity.)

Lecture 13: Jordan form

Monday, February 5, 2018 8:51 AM

Now suppose $f_A(x) = \prod (x-\lambda_i)^{n_i}$ $(\lambda_i \neq \lambda_j)$. Then the invariant factors are of the form $g_j(x) = \prod (x-\lambda_i)^{m_{ij}}$.

And $m_{i1} \leq m_{i2} \leq \cdots \leq m_{is}$ for any i.

So $V_A \simeq k[x]/\langle g_1(x)\rangle \oplus \cdots \oplus k[x]/\langle g_s(x)\rangle$

$$\simeq \bigoplus_i \bigoplus_j k[x]/\langle (x-\lambda_i)^{m_{ij}} \rangle .$$

why? A version of Chinese Remainder Theorem

So we need to find out how multiplication by x acts on $k[x]/\langle (x-\lambda)^m \rangle$. We will do this in the next lecture and find out that multiplication by x can be represented by $\begin{bmatrix} \lambda & & \\ 1 & \ddots & \\ & \ddots & \ddots \\ & & 1 \quad \lambda \end{bmatrix}$ which is called a Jordan block.

In the proof of Rational Canonical Form theorem, in lecture the following is proved which is of independent interest: for $A, B \in M_n(k)$,

$V_A \simeq V_B$ as $k[x]$-mod $\Leftrightarrow$ A and B are similar.