Lecture 10: Cayley-Hamilton and Friends

Friday, April 3, 2015 2:37 PM

(Reduced) norm, trace, cha poly

Recall: $a \in M_n(F)$ can $\chi_a(x) \in F[t]$ via $\chi_A(x) = \det(xI - a)$

Motive: doesn't depend on change of basis.

$\chi_a(x) = \prod (x - a_i)$

$a = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$

It follows if a is diagonalizable (over $\bar{F}$) then $\chi_a(a) = 0$

Thm (Cayley-Hamilton) $\chi_a(a) = 0$ if $a \in M_n(F)$.

Pf: true if $\chi_a(x)$ has distinct roots.

Consider $X = (x_{ij}) \in M_n(F[x_{ij}]) \subset M_n(F(x_{ij}))$

$\chi_X(t) \in F[x_{ij}][t]$ $\qquad \chi_a(t) = \chi_X(t)\Big|_{x_{ij} = a_{ij}}$

$a = (a_{ij})$

and consequently $\chi_a(a) = \chi_X(X)\Big|_{x_{ij} = a_{ij}}$

suffices to show $\chi_X(X) = 0$

true if X is diagonalizable at alg. closure.

true if X has dist. e.vals. $\iff$ χ_X has distinct roots.

$\mathrm{disc}(\chi_X(t)) \in F[x_{ij}]$

$\mathrm{disc} \neq 0 \iff \chi_X(t) \in \overline{F(x_{ij})}(t)$ has distinct roots.

Same nonsense as above $\quad \mathrm{disc}(\chi_a(t)) = \mathrm{disc}(\chi_X(t))\Big|_{x_{ij}=a_{ij}}$

$\mathrm{disc}(\chi_X(t)) = 0 \Rightarrow \mathrm{dis}(\chi_a(t)) = 0$ all $a \in M_n(F)$.

~~moreover~~ $= 0$ for any field ext. of F. $\quad \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}$ all distinct

$\swarrow$

$\mathrm{disc}(\chi_X(t)) \neq 0$.

$\Rightarrow \chi_X(X) = 0$ dist. roots $\Rightarrow \chi_a(a) = 0$ all a. $\square$.

<u>Observation:</u> $m_a(t) = \chi_a(t)$ if evals. are distinct.

$X = (x_{ij}) \in F[x_{ij}]$ then $m_X(t) = \chi_X(t)$ (in $M_n(F(x_{ij}))$)

Let A/F be a CSA of deg n, choose $\varphi : A \otimes \overline{F} \xrightarrow{\sim} M_n(\overline{F})$

$Z = \sum x_{ij} a_{ij} \in A \otimes_F F[x_{ij}]$ where a_{ij} some basis for A.

note the iso φ extends to an iso $A \otimes \overline{F}[x_{ij}] \xrightarrow{\sim} M_n(\overline{F}[x_{ij}])$

$m_Z(t) = m_{\varphi(Z)}(t)$.

Claim $\quad m_{\varphi(Z)}(t) = \chi_{\varphi(Z)}(t)$

$m_{\varphi(Z)}(t)\Big|_{x_{ij}=z_{ij}} (\sum z_{ij} a_{ij}) = 0, \ \forall\, z_{ij} \in \overline{F}$

$\cdots \varphi(z) \Big|_{x_{ij}=z_{ij}}$

$$m_{\sum_i z_{ij}a_{ij}} \,\Big|\, \left(m_{\varphi(z)}(t) \Big|_{x_{ij}=z_{ij}} \right) \qquad \deg m_{\sum z_{ij}a_{ij}} \le \deg m_{\varphi(z)}(t)$$

in $M_n(\overline{F})$ can choose some matrix $b = (b_{ij})$ w/ $\chi_b = m_b$

$$b = \varphi(\bar{a}) \quad \bar{a} \in A \otimes \overline{F} \qquad \bar{a} = \sum \lambda_{ij} a_{ij} \quad \lambda_{ij} \in \overline{F}$$

$\bar{a} = Z \Big|_{x_{ij} = \lambda_{ij}}$ consider $z_{ij} = \lambda_{ij}$ then

$$\deg m_{\sum \lambda_{ij} a_{ij}} = \deg m_{\bar{a}} = n$$

$$\Longrightarrow \quad n = \deg m_{\varphi(z)}(t) \quad \Rightarrow \quad m_{\varphi(z)}(t) = \chi_{\varphi(z)}(t)$$

<u>Define</u>: $\chi_a(t) = m_Z(t) \Big|_{x_{ij} = \lambda_{ij}}$

$a \in A$, $a = \sum_i \lambda_{ij} a_{ij}$

norm, trace = appropriate coeffs (w/ sign) of χ_a

We've shown: coincides w/ defn:

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, "N_A"'] & A \otimes \overline{F} \simeq M_n(\overline{F}) \arrow[d, "\det"] \\ F \arrow[r, hook] & \overline{F} \end{tikzcd}$$

Skip Garibaldi (Monthly) : "The determinant is not an ad hoc construction"

Pfaffian Cayley Hamilton thm

Thm If (A,τ) is a central simple algebra w/ sympectic involution τ, and $a \in \mathrm{Symd}(A,\tau)$, $P\chi_a(t)^2 = \chi_a(t)$, then $P\chi_a(a) = 0$.

Claim/Def If (A,τ) CSA w/ symp. inv., $a \in \mathrm{Symd}(A,\tau)$ then $\chi_a(t)$ is the square of a unique monic poly $P\chi_a(t)$.

$\mathbb{H}$ = standard real quaternions

$A = M_m(\mathbb{H}) \hookrightarrow \mathrm{End}_{\mathbb{H}}(\mathbb{H}^m)$ $\quad \tau = t \otimes \overline{}$ $\quad$ inv. defined by

$\tau(a_{ij}) = (\overline{a_{ji}})$ $\quad$ $\overline{a+bi+cj+dk} = a-bi-cj-dk$.

symplectic since sym stuff has dim $\frac{2(2-1)}{2} = 1$

can check τ is symplectic also.

Note: τ is adjoint inv. w/ respect to the quaternionic form

$h(x,y) = x^t \cdot \overline{y} \in \mathbb{H}$ $\quad$ $h(Tx,y) = h(x,\tau(T)y)$

h is also positive-definite! $h(x,x) \geq 0$ $\quad$ 0 only if $x=0$

h is also positive-definite: $h(x,x) \neq 0$ ...

$$x = \begin{bmatrix} x_1 \\ | \\ x_m \end{bmatrix} \quad x_i \in \mathbb{H} \qquad h(x,x) = \sum_i |x_i|^2.$$

<u>Claim:</u> Let $T \in A$ be τ-symmetric. Then $T^2 x = 0 \Rightarrow Tx = 0$.

<u>Pf:</u> $h(Tx, Tx) = h(T^2 x, x) = 0 \Rightarrow Tx = 0$ by pos def. $\square$.

<u>Cor:</u> consider $T \in A$ τ-symmetric

$$T \in A \hookrightarrow \mathrm{End}_{-\mathbb{H}}(\mathbb{H}^m) \hookrightarrow \mathrm{End}_{-\mathbb{C}}(\mathbb{H}^m) = M_{2m}(\mathbb{C})$$

$$\mathbb{C} = \mathbb{R} + i\mathbb{R}$$

then $m_T(t)$ has no repeated roots!

(in $M_{2n}(\mathbb{C})$)

Pf: if $m_T(t) = n(x)(x-\alpha)^2$ set $p(t) = n(x)(x-\alpha)$

$p(T) \neq 0$ but $p(T)^2 = 0$

$p(T)v \neq 0 \quad p(T)^2 v = 0$ ↯.

Consequently, since $P\chi_T(x)^2 = \chi_T(x)$

$m_T(x)$ & $\chi_T(x)$ have same roots all appear in $m_T(x)$ w/ mult. 1 $\Rightarrow m_T \mid P\chi_T$

$$\Rightarrow P\chi_T(T) = 0 \quad T \in \mathrm{Sym}(M_m(\mathbb{H}), \tau).$$

Next, consider $M_{2m}(\mathbb{C})$, ω = standard symp. form

$\omega(x,y) = x^t \Omega y \qquad \Omega = \begin{pmatrix} 0 & I \\ -I & \end{pmatrix} \qquad \sigma$ = adj. invol. w/ resp to ω.

$\omega(x,y) = x^t \Omega y \qquad \Omega = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ $\qquad \sigma =$ adj. invol. w/ resp to ω.

Let $X = (x_{ij}) \in M_{2m}(\mathbb{C}[x_{ij}]) \qquad Y = X + \sigma(X) \in M_{2m}(\mathbb{C}[x_{ij}])$

$\chi_Y \in \mathbb{C}[x_{ij}][t] \qquad (P\chi_Y)^2 = \chi_Y \quad (\text{in } \mathbb{C}(x_{ij})[t])$

follows that $P\chi_Y \in \mathbb{C}[x_{ij}][t]$

$$\begin{tikzcd}
 & \mathrm{End}_{-\mathbb{H}}(\mathbb{H}^m) \arrow[r, hook] & \mathrm{End}_{-\mathbb{C}}(\mathbb{H}^m) \arrow[d, phantom, "="] & \\
M_m(\mathbb{H}) \arrow[ur, "\sim"] \arrow[urr, bend right] \arrow[dr, hook] & & M_m(\mathrm{End}_{-\mathbb{C}}(\mathbb{H})) \arrow[d, phantom, "//"] \arrow[r, phantom, "\cong"] & M_{2m}(\mathbb{C}) \arrow[d, "\wr"] \\
\tau & M_m(\mathbb{H}) \otimes \mathbb{C} & M_m(\mathbb{H} \otimes \mathbb{C}) \arrow[l, "\sim"'] & M_{2m}(\mathbb{C}) \\
 & & & \sigma
\end{tikzcd}$$

τ'

$$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathrm{End}_{-\mathbb{C}}(\mathbb{H})$$
$$x \otimes \lambda \longmapsto (y \mapsto xy\lambda)$$

$\Rightarrow (M_m(\mathbb{H}), \tau) \otimes_{\mathbb{R}} \mathbb{C} \simeq (M_{2m}(\mathbb{C}), \sigma)$

preserve symm. stuff, χ, $P\chi$

$P\chi_Y(Y)$ poly function on $\mathrm{Sym}(M_{2m}(\mathbb{C}), \sigma)$

$\;\;\; = \qquad\qquad\qquad\qquad =$

$\;\;\; G \qquad\qquad W \otimes \mathbb{C} = \mathrm{Sym}(M_m(\mathbb{H}), \tau) \otimes_{\mathbb{R}} \mathbb{C}$

$$\uparrow$$

G fcn on $W \otimes \mathbb{C} \qquad W = \mathrm{Sym}(M_m(\mathbb{H}), \tau)$

$$G|_W \equiv 0 \implies G \equiv 0$$

$\therefore\ P\chi_Y(Y) = 0$

consider inv σ on $M_{2m}(\mathbb{Z})$ given by $\Omega = \begin{pmatrix} & I \\ -I & \end{pmatrix}$

$X = (x_{ij})$ $\quad Y = X + \sigma(X)$, $\quad P\chi_Y(Y)$ is 0 when eval. on $\forall$ values of Y.

$\implies P\chi_Y(Y) = 0$.

for gen field / alg (A, τ)

$$(A, \tau) \hookrightarrow (A, \tau) \otimes \bar{F} \simeq (M_{2m}(\bar{F}), \sigma)$$

$P\chi_Y(Y) = 0$ there

$\Downarrow$

same in (A, τ) $\square$.

<u>Consequence</u>: Let A be a CDA of period 2.

Then $\exists$ (separable) subfields $L \subset A$ s.t. $2[L:F] = \deg A$.

<u>Pf</u>: WLOG $|F| = \infty$

Consider τ symplectic inv on A. consider $\mathrm{Symd}(A, \tau)$

some "typical" $a \in \mathrm{Symd}(A, \tau)$ has $\min_a = \mathrm{Prd}_a$ / distinct roots

(consider $\mathrm{disc}(P\chi_X(t))$) $\quad F(a) \simeq F[x]/\min_a(x) = P\chi_a(x)$ $\subset A$ division

$\neq 0$ generically $\quad$ " subfield

degree as claimed

—

(consider disc( ) $\neq 0$ generically " subfield

degree as claimed

$$\begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_m \end{bmatrix} \in M_m(\mathbb{H})$$

$\square$.

<u>For Fun:</u> Given $m \mid n$, construct a div. alg w/ per m i, ind n.

(same prime factors)

consider case m, n are powers of same prime p $\quad m = p^r \quad n = p^s$

(p, p^a)

Skew <u>Polynomials</u>.

R ring, $\sigma \in \mathrm{Aut}(R)$ order$(\sigma) = n$

<u>Define</u> $R[t;\sigma] = \left\{ \sum_{i=0}^{k} r_i t^i \mid r_i \in R \right\}$

$$(rt^i)(st^j) = r\,\sigma^i(s)\,t^{i+j}$$

$$t^n \in Z(R[t;\sigma]) = Z(R)^\sigma \oplus Z(R)^\sigma t^n \oplus \dots$$

$Z(R)^\sigma$ ✓ $\qquad = Z(R)^\sigma[t^n]$

if R a domain so is $R[t;\sigma]$

$F(x_1, \ldots, x_a) \circlearrowleft \sigma_i \qquad \sigma_i(x_j) = \begin{cases} x_j & \text{if } i \neq j \\ \rho x_i & \text{if } i = j \end{cases}$

$\underset{\mathbb{C}}{\overset{\shortparallel}{\ }} \quad \underbrace{\qquad}_{E}$

ρ a primitive pth root of 1.

$A = E[t_1; \sigma_1][t_2; \sigma_2] \cdots [t_a; \sigma_a]$

$Z(\qquad) = F(x_1^p, \ldots, x_a^p)[t_1^p, \ldots, t_a^p] = R$

observe: A/R is a finite free R-mod of rank p^{2a}

R domain = polys in a vars / rat'l fns in a vars.

$L = \mathrm{frac}(R)$ = rat'ls in $2a$ variables.

$\Rightarrow A \otimes_R L$ is a domain. also f. dim'l / L.

& a finite dim'l domain / field is a div. alg!

$\Longrightarrow A \otimes_R L$ is a d. alg. degree p^a

A = tensor prod of $(x_i, t_i)_{L, \rho}$
deg p so per $| p$.

$\Rightarrow \mathrm{per} A | p$

Specific fields:

D # field $\qquad \mathrm{per} D = \mathrm{ind} D$

$F = \mathbb{Q}(x)$ $\exists$ examples w/ ind D = (per D)

Conj: ind $D \mid (\mathrm{per}\, D)^2$ OPEN!

$\mathbb{C}(t_1, \ldots, t_n)$ ind $D \mid (\mathrm{per}\, D)^{n-1}$ $\leftarrow$ conj OPEN! "

$\exists$ examples w/ $=$.

Known if $n = 1$ or 2.

Tsen's thm dejong ~15 yrs ago.

Known for any p $\exists\, n(p)$ s.t. if per $D = p^{k}$

ind $D \mid (\mathrm{per}\, D)^{n(p)}$ E. Matzri

~3 yrs ago.

$\mathbb{Q}_p$ ind = per

$\mathbb{Q}_p(t)$ ind $\mid$ per^2 Saltman late 90's.

$\mathbb{Q}_p((x_1))((x_2)) \ldots ((x_n))(t)$ ind $\mid$ per^{2+n} Lieblich/, K-, Harb-Hartmann '09.

Ref/Claim $\chi_a(t) = \mathrm{P}\chi_a(t)^2$ $a \in \mathrm{Symd}(A, \tau)$ symplectic.

Reduce to case of 1 example A, τ, and generic elmt. in char 0.

$(M_m(\mathbb{H}), \tau)$

given $M \in \mathrm{Sym}(M_m(\mathbb{H}), \tau)$, this defines a $\mathbb{H}$-hermitian form

$h: \mathbb{H}^m \times \mathbb{H}^m \longrightarrow \mathbb{H}$ $h(x, y) = \overline{h(y, x)}$

$$h : \mathbb{H}^n \times \mathbb{H}^n \longrightarrow \mathbb{H} \qquad h(x,y) = \overline{h(y,x)}$$

$$h(x,y) = x^t M \bar{y}$$

<u>Now:</u> Do Gram-Schmidt & show:

$$T^t M \bar{T} = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \qquad d_i \in \mathbb{R}.$$

$$\begin{array}{c} \cap \\ M_n(\mathbb{H}) \\ \cap \\ M_n(M_2(\mathbb{C})) \\ \| \\ M_{2n}(\mathbb{C}) \end{array}$$