Lecture 3: Noether-Skolem and examples

Friday, January 23, 2015 2:34 PM

Stuff from last time

$$A \text{ CSA} \iff \exists B \text{ s.t. } A \otimes B \; M_n(F) \iff A \otimes A^{op} \simeq \operatorname{End}(A)$$

$$\Updownarrow$$

$$\exists B \text{ s.t. } A \otimes B \text{ CSA} \iff A \otimes_F L \simeq M_n(F) \iff A \otimes_F \bar{F} \simeq M_n(\bar{F})$$

some L/F

$$\Updownarrow$$

$$\forall B \text{ CSA} \; A \otimes B \text{ CSA} \iff A \otimes L \text{ CSA}$$

$\forall L/F$

$\exists L/F$

If A, B CSA $\Rightarrow A \otimes B$ CSA

$A \sim B \iff M_n(A) \simeq M_m(B)$

$\operatorname{Br}(F)$

$[A] + [B] = [A \otimes B]$

Lem A/F CSA, B/F simple (f.dim'l) $\Rightarrow A \otimes B$ simple.

Pf: If $L = Z(B)$ then B/L CSA

$$A \otimes_F B \simeq A \otimes_F (L \otimes_L B) \simeq \underbrace{(A \otimes_F L)}_{\text{CSA}/L} \otimes_L B \Leftarrow \text{CSA}/L$$

CSA$/L$ in particular, simple $\checkmark$.

Lem (Almost DCT 2)

$A = B \otimes C$ CSA's. then $C = C_A(B)$

Pf: By def $C \subset C_A(B)$

But $\dim_F C_A(B) = \dim_{\bar{F}} C_A(B) \otimes_F \bar{F} = \dim_{\bar{F}} C_{A\otimes\bar{F}}(B\otimes\bar{F})$

WLOG, $B \underset{\bar{F}}{=} M_n(\bar{F})$ $C_{\bar{F}} = M_m(\bar{F})$

$$A = M_n(\bar{F}) \otimes M_m(\bar{F}) = M_m(M_n(\bar{F}))$$

$$C_{M_m(M_n(\bar{F}))}(M_n(\bar{F})) = M_m(C_{M_n(\bar{F})}M_n(\bar{F})) = M_m(Z(M_n(\bar{F})))$$

diagonally $\begin{pmatrix} a & & & \\ & a & & \\ & & a & \\ & & & \ddots \end{pmatrix}$ $= M_m(\bar{F})$

$= C_{\bar{F}}$

dimensions match! $\triangle$

Theorem (Noether - Skolem)

Suppose A/F CSA, $B, B' \subset A$ simple subalgebra, and $\psi : B \xrightarrow{\sim} B'$. Then $\exists\, a \in A^*$ s.t. $\psi(b) = aba^{-1}$

Pf: $B \hookrightarrow A \hookrightarrow A \otimes A^{op} \simeq \mathrm{End}_F(A) = \mathrm{End}_F(V)$ $V = A$

$B' \hookrightarrow A$

V is a A-A bimod $\Rightarrow$ it is a B-A mod or $B \otimes A^{op}$ left module.

B simple A^{op} CSA $\Rightarrow$ $B \otimes A^{op}$ simple $\Rightarrow$ unique simple left module

V determined by its dim as a $B \otimes A^{op}$ module. $(b\otimes a)(v)$

V also a $B \otimes A^{op}$ via $(b \otimes a) \cdot v = (\psi(b) \otimes a)(v)$

these modules are isom

i.e. $\exists\ \varphi : V \xrightarrow{\sim} V$ s.t.

$$\forall b, a,\quad \varphi(b \otimes a'(v)) = \Psi(b) \otimes a'(\varphi(v))$$

$\varphi \in \mathrm{End}(V)^* = \mathrm{End}(A)^* = (A \otimes A^{op})^*$ via sandwich map

$\Rightarrow\ \varphi$ is a right A mod map. $\Rightarrow \varphi \in C_{A \otimes A^{op}}(A^{op})$

$$C_{A \otimes A^{op}}(A^{op}) = (A \otimes 1)^*$$

$\Rightarrow \varphi =$ left mult. by $a \in A^*$

$\forall b$ - $\quad \forall v \in A \qquad a' = 1$

$$a \otimes 1(b \otimes 1(v)) = \Psi(b) \otimes 1(a \otimes 1(v))$$

$$abv = \Psi(b)\, a v \quad \text{all } v$$

$v = 1$

$$ab = \Psi(b)\, a$$

$$aba^{-1} = \Psi(b) \quad \text{all } b \qquad \square.$$

Thm (DCT on approach, step 3)

A CSA, $B \subset A$ simple, then $(\dim_F C_A(B))(\dim_F B) = \dim_F A$

Pf: $B \hookrightarrow A \qquad L = Z(B)$, B/L CSA. say $\deg B = m$

B CSA$/L$, $\quad B \hookrightarrow A \otimes_F L$ (CSA$/L$)

$$\dim_F B = m^2 [L:F]$$

$$C_{A \otimes L}(B) = C_{A \otimes L}(B \otimes L) = C_A(B) \otimes L$$

$B \otimes_L \bar{L} \hookrightarrow A \otimes_F \bar{L} \qquad n = \deg A$

$$\overset{\shortparallel}{M_m(\overline{L})} \qquad \overset{\shortparallel}{M_n(\overline{L})} \Rightarrow m \mid n$$

$M_m(\overline{L}) \hookrightarrow M_n(\overline{L})$ block-scalar matrices

$$\overset{\shortparallel}{m \cdot \frac{n}{m}}$$

NS $\Rightarrow$ only need to compute centralizer here

Lemma (didn't get to last time) $\quad C_{A\otimes_F \overline{L}}(B \otimes_L \overline{L}) \simeq M_{\frac{n}{m}}(\overline{L})$

$\dim_L C_{A\otimes L}(B) = \left(\frac{n}{m}\right)^2 \qquad \dim_F (C_{A\otimes L}(B)) = \left(\frac{n}{m}\right)^2 [L:F]$

$$\shortparallel$$

$\dim_F C_A(B) \cdot [L:F]$

$\Rightarrow \dim_F C_A(B) = \left(\frac{n}{m}\right)^2 \quad \dim_F A$

ummm....

I owe you DCT later!

Existence of max'l subfields

If A/F a CSA, $E \subset A$ subfield, we say E is a max'l subfield if

$[E:F] = \deg A$.

E/F sep. ext.

Thm If A is a division algebra, then $\exists$ max'l separable subfields.

will show in case F is infinite.

Rem: $(\dim_F E)(\dim_F C_A(E)) = \dim_F A$

...: if $C_A(E) \supsetneq E$, then add another elmt, get a comm. subalg.

DCT says if $\dim_F E \leq \sqrt{\dim_F A}$ can always get bigger field.

why separable?

If F finite, all exts are separable, so done.

Pf: given $a \in A$, consider $F(a) = \text{span}\{1, a, a^2, \ldots, a^{n-1}\}$

$n = \deg A$

want: 1. these to be indep $/F$

2. want poly satisfied by a of deg n to be separable.

this poly at $\bar{F}$ ~~is~~ will be χ_a

if χ_a dist roots $\Rightarrow$ = min'l. $\Rightarrow \exists!$ poly deg n satisfied by $a_{\bar{F}}$

will be this one.

3. disc of poly gives poly in coeffs which are poly in coords of a

nonvanishing if distinct eigenvals.

$$A \xrightarrow[\text{Big Poly fcn}]{} F$$

Lem Suppose V a f.d. vspace$/F$ $F \subset L$ field ext. F infinite. If $f \in L[x_1, \ldots, x_n]$, $f \not\equiv 0$ then $\exists a_1, \ldots, a_n \in F$ $f(\vec{a}) \neq 0$.

Pf: $n=1$ any poly has only finitely many 0's if $\not\equiv 0$.

general: $F(x_1, \ldots, x_{n-1})[x_n]$. $\square$

Structure & Examples

degree 2 algebras

Def A Quaternion algebra is a deg 2 CSA.

Structure = $M_2(F)$ or D division.

$\exists$ quadratic separable subfields if division

(& usually w/ matrices)

Suppose A is a quat. $E \subset A$ sep. quadratic

(char $F \neq 2$) $E = F(\sqrt{a})$ $i = \sqrt{a}$

aut of E/F via $i \mapsto -i$

$NS \Rightarrow \exists\, j \in A^*$ s.t. $jij^{-1} = -i$ $ij = -ji$

j^2 commutes w/ i & j

Claim: $A = F \oplus Fi \oplus Fj \oplus Fij$

As a left $F(i)$ space 1 doesn't generate, & $\dim_{F(i)} A = 2$

$j \notin F(i)$ commutativity reasons.

$\Rightarrow A = F(i) \oplus F(i)j$

$\Rightarrow j^2$ comm w/ i, j $\Rightarrow j^2 \in Z(A) = F$, $j^2 = b \in F$.

$k = ij$

So: A generated by i, j

So: A generated by i, j

$$i^2 = a \in F^* \quad j^2 = b \in F^* \quad ij = -ji$$

$k = ij$ $\qquad -ab = k^2 \qquad ki = iji = -iij = -ik$

$ijij = -iijj$ $\qquad\qquad kj = ijj = -jij = -jk$

$= -ab$

<u>Conversely</u>: given any $a, b \in F^*$, define $\left(\frac{a,b}{F}\right)$ to be the algebra above. This is a CSA. (Quest)

ETS $\left(\frac{a,b}{F}\right)$ works $\qquad i \mapsto \frac{1}{\sqrt{a}} i = \tilde{i} \qquad \tilde{i}^2 = 1$

$\qquad j \mapsto \frac{1}{\sqrt{b}} j = \tilde{j} \qquad \tilde{j}^2 = 1$

so ETS $\left(\frac{1,1}{F}\right) \xrightarrow{\sim} \mathrm{End}_F(F[i])$ via

$F[i] \longrightarrow$ left mult.

$j \longrightarrow$ Gal action $i \mapsto -i$

exercise

<u>Symbol Algebras</u>

Given A/F CSA deg n.

Suppose $\exists E \subset A$ max'l subfield $E = F(\sqrt[n]{\alpha})$, $\alpha = a$

cyclic (Kummer) extn.

$\sigma \in \mathrm{Aut}(E/F)$ generator via $\sigma(\alpha) = \omega\alpha$ ω prim n^{th} root of 1.

$NS \Rightarrow \exists \beta \in A^*$ s.t. $\beta\alpha\beta^{-1} = \omega\alpha$

$\beta\alpha = \omega\alpha\beta$

$$A = E \oplus E\beta \oplus E\beta^2 \oplus \cdots \oplus E\beta^{n-1}$$

consider action of α on A via conjugation

$E\beta^i = E$ v.space $/E$ or $/F$

$\alpha(x\beta^i)\alpha^{-1} = \omega^{-i} x \beta^i$ $E\beta^i$ consist of e.vectors for conj by α w/ val ω^{-i}

$\Rightarrow \beta^n$ central $\Rightarrow \beta^n = b \in F^*$

$$A = \bigoplus_{i,j \in \{1,\dots,n\}} F\alpha^i\beta^j \qquad \beta\alpha = \omega\alpha\beta, \quad \alpha^n = a,\ \beta^n = b$$

---

turns out if we define

$(a,b)_\omega$ "symbol algebra"

to be $\bigoplus F\alpha^i\beta^j$ w/ $\alpha^n = a$ $\beta^n = b$

$\omega\alpha\beta = \beta\alpha$ is always a CSA/F.

Cyclic Algebras

E/F cyclic w/ $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ $\sigma^n = id_E$

E/F cyclic w/ $\mathrm{Gal}(E/F) = \langle \sigma \rangle$ $\quad \sigma^n = id_E$

suppose $E \subset A$ max'l subfield

choose $u \in A^*$ s.t. $ux = \sigma(x)u$ all $x \in E$ (N-Sk)

then we'll show: $A = E \oplus Eu \oplus Eu^2 \oplus \cdots \oplus Eu^{n-1}$

$\Rightarrow \underset{\substack{\parallel \\ b}}{u^n} \in F = Z(A)$

$A = \Delta(E, \sigma, b)$ "cyclic algebra"

turns out: over a # field, all CSA's are of this form!

Albert $\Rightarrow$ not all da's are cyclic!

E/F G-Galois $\quad E \subset A$ max'l

$\forall g \in G$, $\exists$ $u_g \in A$ s.t. $u_g x = g(x) u_g$

$A = \bigoplus_{g \in G} E u_g \quad \ldots$