Lecture 9: Existence of Involutions (and division algebras)

Friday, March 27, 2015 2:34 PM

Involutions (of the first kind)

Involution: anti-automorphism of order 2 on a CSA.

either $\mathrm{aut}|_{\mathrm{centr}} = \mathrm{id}$ 1st kind

$\mathrm{aut}|_{\mathrm{centr}} \neq \mathrm{id}$ 2nd kind

1st kind → orthogonal $\rightsquigarrow$ adjoint inv. for symm. bilinear forms $\otimes \bar{F}$

1st kind → symplectic $\rightsquigarrow$ adj. inv. for alternating forms

$$\dim(\mathrm{Symm}(A,\sigma)) = \begin{cases} n^2+n/2 & \text{if orth} \\ n^2-n/2 & \text{if symp} \end{cases} \quad ?$$

$\deg A = n$, σ inv

Given alg w/ inv (A,σ) $\quad \sigma : A \xrightarrow{\sim} A^{op}$

$\Rightarrow 2[A] = [A] + [A^{op}] = [A] - [A] = 0 \quad [A]$ per 1 or 2

Thm $\exists$ orth (symp) inv. on $A \iff \mathrm{per}\, A \mid 2$.

Pf: if $A \otimes E \simeq \mathrm{End}(V)$ (E/F G Galois)

$A^{op} \otimes E \simeq \mathrm{End}(V^*)$ (transpose)

$A^{op}_E \otimes_E A^{op}_E \simeq \mathrm{End}(V^* \otimes V^*)$ since $\mathrm{per}.\, A \mid 2$

$A^{op} \otimes A^{op} \simeq \mathrm{End}(W)$

$A^{op}_E \otimes_E A_E$ —

$A^{op} \otimes E$

$W_E \simeq V^* \otimes V^*$

$A^{op} \otimes A^{op} \simeq \mathrm{End}(W)$

W is a right $A \otimes A$-mod.

$W_E \simeq V^* \otimes V^*$ right $\mathrm{End}\,V \otimes \mathrm{End}\,V$-mod

$\ni b'$

$$(b' \cdot (a \otimes a'))(x \otimes x') = b'(ax \otimes a'x')$$

From this perspective, if $b \in V^* \otimes V^*$ then $\sigma_{b'}$ defined by, for $a \in \mathrm{End}(V)$

$$b'(1 \otimes a) = b'(\sigma_{b'}(a) \otimes 1)$$

Therefore, if $b \in W$, (corresp. to a nondeg. form $/E$)

defining σ_b via $b \cdot (1 \otimes a) = b \cdot (\sigma_b(a) \otimes 1)$ gives an anti-aut.!

(since extending to E, get an anti-aut.)

Want: describe a subspace

$$\begin{array}{ccc} \mathrm{SymmB}(V) & \longrightarrow & V^* \otimes V^* \\ \uparrow & & \uparrow \\ \mathrm{Symm}\,W & \longrightarrow & W \end{array}$$

i.e. $(\mathrm{Symm})_E \simeq \mathrm{SymmB}(V)$

Works via descent:

comes down to: describe a semilinear action of G on $\mathrm{SymmB}(V)$

comp. w/ semilinear action of G on $V^* \otimes V^*$ giving W

$$\mathrm{SymmB}(V) = \left(V \otimes V \big/ \mathrm{Skd}(V) \right)^*$$

$\mathrm{Skd}(V) = \langle v \otimes w - w \otimes v \rangle$ $\quad V^* \otimes V^*$

Summ (/Skd(V))

$$Skd(V) = \langle v\otimes w - w\otimes v \rangle$$

"have" an action (similar) on $V\otimes V$ w/ invariants W on $V^*\otimes V^*$

Claim: can choose this to promote $Skd(V)$

Have: actions on End V, End $V\otimes V$, End $V^*\otimes V^*$, End(Skd V)

$$Skd \hookrightarrow V\otimes V = W_E^*$$
$$\{z[A]=0\}$$

End(Skd) End$(V\otimes V)$

$\text{End}(Skd)^G = \text{End}(Summ(W^*))$

$G \circlearrowright A_E$

$G \circlearrowright A_E \otimes A_E$

$G \circlearrowright V\otimes V = W_E^*$

see video for details.

if $G \circlearrowright$ End V

s.t. $\text{End}(V)^G \cong \text{End}(W)$

then can choose iso, s.t. its induced by same action $G \circlearrowright V$

$V^G = W$

adjoints w/r/t b_6 Summ(W) are exactly orth. involutions

(promise: need b_E to be nonsingular.) singular ones given by vanishing of poly on $W_E = V^*\otimes V^*$

if poly vanished completely $\Rightarrow$ poly would be 0 (if $|F|$ not finite) if F finite $\Rightarrow \nexists$ div. algs (Wedd)

$\Rightarrow$ for $A=1 \Rightarrow A = \mathrm{End}(W)$ and we already have invs.

Symplectic Case:

$$\mathrm{Alt}(V) = \left({V \otimes V}/{\Delta_V} \right)^*$$

$\Delta_V = \langle v \otimes v \rangle$

2nd kind "Unitary Involutions"

Arise as adjoint inv's for Hermitian forms

Setup: L/F quadratic Gal extension, gp $\langle \tau \rangle = \mathrm{Gal}(L/F)$

Def A Hermitian form on an L-space V is a function

$V \times V \xrightarrow{h} L$ s.t. h is L-linear in 1st coord

$$h(v,w) = \tau(h(w,v))$$

$$\Rightarrow h(v,\lambda w) = \tau(h(\lambda w, v)) \; \tau(\lambda h(w,v)) = \tau(\lambda) \cdot \tau(h(w,v))$$
$$= \tau(\lambda) h(v,w)$$

Given a v.space V/E $\quad$ $E \,|\, G \; F$ $\quad$ $\sigma \in G$ define

$$\underline{{}^{\sigma}V}$$

${}^{\sigma}V = \{ {}^{\sigma}v \mid v \in V \}$ $\qquad$ ${}^{\sigma}v + {}^{\sigma}w = {}^{\sigma}(v+w)$

$${}^{\sigma}(\lambda x) = \sigma(\lambda)\,{}^{\sigma}(x)$$

i.e. v.space/L structure is via $\lambda \circ {}^{\sigma}x = \sigma(\sigma^{-1}(\lambda)\, x)$

<u>Def</u>: If A/E is an algebra.

$\bigotimes_{\sigma \in G} {}^{\sigma}A$ has a G-semilinear action by permuting factors

$$\tau(1 \otimes \dots \otimes {}^{\sigma}a \otimes \dots \otimes 1) \equiv (1 \otimes \dots \otimes {}^{\tau\sigma}a \otimes \dots \otimes 1)$$

$\uparrow$ σ place $\uparrow$ $\tau\sigma$ place

$$\mathrm{cor}_{E/F} A = \Big(\bigotimes_{\sigma \in G} {}^{\sigma}A \Big)^{G}$$

L / $k(\tau)$ / F

<u>Def</u>! a Hermitian form is a fcn

$$h : V \otimes_L {}^{\tau}V \longrightarrow L$$

$$h(v,w) \equiv h(v \otimes {}^{\tau}w)$$

h nondeg if induces

$${}^{\tau}V \xrightarrow{\sim} V^*$$

$${}^{\tau}w \longmapsto (v \mapsto h(v,w))$$

<u>Def</u> $\sigma_h : \mathrm{End}(V) \circlearrowleft$ defined by $h(v, Tw) = h(\sigma_h(T)v, w)$

(h nondeg)

σ_h is an involution

<u>Thm</u> if A/L CSA, L/F Gal. deg 2, then $\exists$ unitary inv

Thm if A/L ..., $F^{\otimes}$ inv

(w.r.t. to L/F) iff $\mathrm{cor}_{L/F} A$ is split.

Division algebras exist

$\exists$ division algebras of every index.

given n positive integer, $F = \mathbb{C}$

$L = F((t))$ $\qquad A = L \oplus Lu \oplus Lu^2 \oplus \cdots Lu^{n-1} \oplus Lu^n \cdots$

w/ $(\lambda u^i)(\mu u^j) = \lambda \sigma^i(\mu) u^{i+j}$

where $\sigma\left(\sum_{k \geq M} \lambda_k t^k\right) = \left(\sum \lambda_k \rho^k t^k\right)$

$\rho^n = 1$ is a prim nth root of 1.

Observations: A is a domain! (look at leading coeffs!)

$$Z(A) = F((t^n)) \oplus F((t^n)) u^n \oplus F((t^n)) u^{2n} \oplus \cdots$$

$$F((t^n))[u^n]$$

Notice: $A \otimes_{Z(A)} \mathrm{frac}(Z(A))$ $\qquad \mathrm{frac}\, Z(A) = F((t^n))(u^n)$

$\|$

cyclic algebra $(F((t))/F((t^n)), \mathrm{inn}_u, u^n)$

$\Rightarrow$ this is a CSA.

it's a domain (exercise $\qquad \mathrm{frac}(Z(\mathrm{dom}))$

$D^{op} \otimes_{Z(D^{op})} \quad = D^{op}!$

$\Rightarrow$ division!

Moreover: for every finite gp G, $\exists$ field F and a G crossed product division alg over F. (with per = ind)

$$H^2(G, E^*) = Br(E/F) \qquad \begin{array}{c} E \\ |\,G \\ F \end{array} \quad \text{Galois. finite.}$$

Start:

$$X_{g,h} \mapsto u_g - u_h \qquad g u_h = u_{gh}$$

$$0 \to I_G \to \mathbb{Z}G \xrightarrow{u_g \mapsto 1} \mathbb{Z} \to 0$$

$$\mathbb{Z}G = \{\textstyle\sum a_g u_g \mid a_g \in \mathbb{Z}\}$$

$$u_g \leftrightarrow g \in G$$

$$H^0(G, \mathbb{Z}G) \to H^0(G, \mathbb{Z}) \to H^1(G, I_G) \to H^1(G, \mathbb{Z}G) = 0 \quad \star$$

$$H^0(G, \mathbb{Z}G) = (\mathbb{Z}G)^G \ni \textstyle\sum a u_g, \qquad (\mathbb{Z}G)^G = \mathbb{Z}$$

$$H^0(G, \mathbb{Z}) = \mathbb{Z}^G = \mathbb{Z}$$

$$\mathbb{Z} \xrightarrow{\cdot |G|} \mathbb{Z}$$

$$\Rightarrow \boxed{H^1(G, I_G) = \mathbb{Z}/|G|\mathbb{Z}}$$

$$0 \to Q_G \to (\mathbb{Z}G)^{\oplus |G \times G|} \to \overset{X_{g,h}}{I_G} \to 0$$

$$(\underset{g,h}{\ldots, 1, 0, \ldots}) \mapsto X_{g,h}$$

$$H^1(G, (\mathbb{Z}G)^{?}) \to H^1(G, I_G) \to H^2(G, Q_G) \to H^2(G, (\mathbb{Z}G)^{?})$$

$\not{\emptyset} \overset{\shortparallel}{0}$ $\qquad \mathbb{Z}/|G|\mathbb{Z} \qquad \overset{\Psi}{\alpha}$

$\bar{1} \longmapsto \alpha$ order $|G|$

Q_G is a free Ab. gp w/ G-action!

$\overset{\shortparallel}{\mathbb{Z}}^{B|G}$

Pick my favorite $E \,|\, G \, F$ Galois. $\qquad E[Q_G] \hookleftarrow$ domain

$\cong E[t_1, t_1^{-1}, t_2, t_2^{-1} \ldots]$

G acts on coeffs & on "monomials" $\leftrightarrow$ elmts of Q_G

monic?

$\checkmark \; H^2(G, E[Q_G]^*)$

want $H^2(G, Q_G) \hookrightarrow H^2(G, E(Q_G)^*) = Br(E(Q_G)/E(Q_G)^G)$

$\overset{\Psi}{\alpha} \longmapsto$ alg of period $|G|$ $\qquad$ alg has deg $|G|$

$$0 \to Q_G \hookrightarrow E[Q_G]^* \longrightarrow E^* \to 1$$

monic monomials $\qquad \overset{\shortparallel}{\text{monomials}}$ $\qquad$ split ses.

$$0 \to H^2(G, Q_G) \hookrightarrow H^2(G, E[Q_G]^*) \twoheadrightarrow H^2(G, E^*) \to 0$$

split ses.

$$1 \to E[Q_G]^* \longrightarrow E(Q_G)^* \longrightarrow \frac{E(Q_G)^*}{E[Q_G]^*} \to 1$$

free ab gp gen by
primes in $E[Q_G]$

important fact: primes are permuted
by G

free ab gp of primes $= \bigoplus \mathbb{Z}[G/H_i]$

fact ☆ $H^1(G, \mathbb{Z}[G/H]) = 0$

$$\underset{\overset{\parallel}{0}}{H^1(G, \mathbb{Z}\langle\text{primes}\rangle)} \to H^2(G, E[Q_G]^*) \hookrightarrow H^2(G, E(Q_G)^*)$$

$\overset{\nearrow}{!}$

$\triangleright$.