Lecture 8: Involutions and other anti-automorphisms

Friday, February 27, 2015 2:36 PM

If E/F prime to ind A then ind $A\otimes E$ = ind A

If L/E splits $A\otimes E$ then L/F splits A

ind $A \mid (\text{ind } A\otimes E)\,[E:F]$

If E/F prime to per A then per $A\otimes E$ = per A

Bilinear forms on a vector space V = f. dim'l

Def: A bilinear form b is a function $b: V\times V \to F$ s.t. linear in each variable

i.e.
$$\begin{tikzcd} V\times V \arrow[r, "b"] \arrow[d] & F \\ V\otimes V \arrow[ur] & \end{tikzcd}$$
or $b\in (V\otimes V)^*$

Def: b is symmetric if $b(v,w)=b(w,v)$ i.e.

b factors through
$$\begin{tikzcd} V\otimes V \arrow[r] \arrow[d] & F \\ (V\otimes V)/\langle v\otimes w - w\otimes v\rangle \arrow[ur] & \end{tikzcd}$$

i.e. b symm $\iff$ $b\in (S^2V)^*$

$S^nV = \otimes^n V/S_n$

Def b is left nondegenerate if $V\to V^*$, $v\mapsto b(v,-)$ inj (iso.)

b is right " — — — — — $b(-,v)$

Def b, b' are isometric if $\exists\ \varphi: V \xrightarrow{\sim} V'$ s.t.
$V \quad V'$

$$b(v,w) = b'(\varphi(v), \varphi(w))$$

Def b, b' are right isometric if $\exists\ \varphi: V \to V$
on same V

s.t. $b(v,w) = b'(v, \varphi w)$ (similarly left isom).

Ex $\langle , \rangle$ on F^n $\quad \langle x,y \rangle = x^t y$ (column vectors)

this is both r & left nondg.

Lem If b, b' both left nondg $\Rightarrow$ they are left isometric.

Pf: $\forall x,\ b'(x, \_) \in V^*$

$$\begin{array}{c} \shortparallel \\ b(\varphi x, \_) \end{array} \quad \text{same } \varphi x \qquad b'(x,y) = b(\varphi x, y)$$

Can check: φ is a lnr map.

similarly $b(x,y) = b'(\psi x, y)$

$\Rightarrow b(x,y) = b'(\psi x, y) = b(\varphi \psi x, y)$

$\Rightarrow x = \varphi\psi x \Rightarrow \varphi\psi = id$, φ an isom. $\square$

In particular, any b left nondg

$b(x,y) = \langle \varphi x, y \rangle$ $\qquad$ write $\varphi = M^t$ matrix M

$= (M^t x)^t y = x^t M y$

M = Gram matrix for b. b left nondg $\Rightarrow \forall x$

$x^t M \neq 0$

$\Leftrightarrow M$ nonsing.

$\Leftrightarrow b$ right nondg.

So nondg = r. nondg = l. nondg.

Given b bilinr on V, can form $\sigma_b^L, \sigma_b^R \subset \operatorname{End} V$ l & r. adjoint anti-aut's.

Want to define

$$b(x, Ty) = b(\sigma_b^L(T)x, y) \qquad b(Tx, y) = b(x, \sigma_b^R(T)y)$$

$b(x, T(-)) \in V^*$

$$\Rightarrow b(x, T(-)) = b(\sigma_b^L(T)x, -)$$

can check $\sigma_b^L(T_1 + T_2) = \sigma_b^L(T_1)\,\sigma_b^L(T_2)$

$$\sigma_b^L(T_1 T_2) = \sigma_b^L(T_2)\,\sigma_b^L(T_1)$$

$$\sigma_b^R \circ \sigma_b^L = \sigma_b^L \circ \sigma_b^R = id_{\operatorname{End}(V)}$$

Given b, b' nondegenerate, know

$$b'(x,y) = b(x, uy)$$

$$b'(x, Ty) = b'(\sigma_{b'}^L(T)x, y) = b(\sigma_{b'}^L(T)x, uy)$$

$$\| \qquad\qquad = b(\sigma_b^L(u)\,\sigma_{b'}^L(T)\,x, y)$$

$b(x, uTy)$

$\|$

$b(\sigma_b^{-}(u)x, y)$

nondeg $\Rightarrow \sigma_b^L(uT) = \sigma_b^L(u)\,\sigma_{b'}^L(T)$

$(\sigma_b^L)^{-1}$ both sides

$$uT = (\sigma_b^L)^{-1}\left(\sigma_b^L(u)\,\sigma_{b'}^L(T)\right)$$

$$= (\sigma_b^L)^{-1}\left(\sigma_{b'}^L(T)\right) u$$

$$\mathrm{inn}_u(T) = uTu^{-1} = (\sigma_b^L)^{-1}\left(\sigma_{b'}^L(T)\right) = (\sigma_b^L)^{-1} \circ \sigma_{b'}^L(T)$$

$\Rightarrow (\sigma_b^L)^{-1}\sigma_{b'}^L = \mathrm{inn}_u \qquad u =$ "Noether-Skolem elmt"

$$\boxed{\sigma_{b'}^L = \sigma_b^L \circ \mathrm{inn}_u \text{ where } b'(x,y) = b(x, uy)}$$

{bilin forms nondeg} $\longrightarrow$ {anti-auts}

$b(x,y) = x^t M y \qquad b'(x,y) = b(x, uy) = x^t M u y$

if $\sigma_b = \sigma_{b'} \iff \mathrm{inn}_M = \mathrm{inn}_{Mu}$

$\sigma_b = t \circ \mathrm{inn}_M$, $\sigma_{b'} = t \circ \mathrm{inn}_{Mu} \iff \mathrm{inn}_u = id$

$\iff u \in Z(\mathrm{End}\, F) = F^*$, $u = \lambda$

$\sigma_b = \sigma_{b'} \iff$
$\exists \lambda$ s.t. $\forall x, y$ $b'(x,y) = b(x, \lambda y)$
$= \lambda b(x,y)$

<u>Def</u> b & b' are homothetic if $b = \lambda b'$ some $\lambda \in F^\times$

$$\left\{ \begin{matrix} \text{nondeg} \\ \text{hom. classes} \\ \text{of bilin} \end{matrix} \right\} \xleftrightarrow{\text{bijection}} \{\text{anti auts}\}$$

given any $\sigma \in \text{Anti-Aut}(\text{End}\,V)$, $t \circ \sigma \in \text{Aut}(\text{End}\,V)$

$\Rightarrow \exists M$, $t \circ \sigma = \text{inn}_M$

$\sigma = t \circ \text{inn}_M \Rightarrow \sigma$ adj to b

$b(x,y) = x^t M y$.

(Involutions)

<u>Def</u> A bilin form b is

- symmetric if $b(x,y) = b(y,x)$
- skew if $b(x,y) = -b(y,x)$
- alternating if $b(x,x) = 0$ all x.

alt $\Rightarrow$ skew. In each case, have

$$b(x,y) = \varepsilon\, b(y,x) \quad \varepsilon^2 = 1$$

"ε-symmetric"

If b is one of these, σ its adjoint

then $b(x,Ty) = b(\sigma T x, y) = \varepsilon\, b(y, \sigma T x)$

$= \varepsilon\, b(\sigma^2 T y, x) = \varepsilon^2 b(x, \sigma^2 T y)$

$= b(x, \sigma^2 T y)$

nandy $\Rightarrow \sigma^2 = id$

Def A is a ring, $\sigma : A \to A$ an antiaut is an involution if $\sigma^2 = 1$

Def if A is a CSA/F we say σ is of the first kind if $\sigma|_{Z(A)=F} = id$.

If not, $\sigma(F) \subset F$ $\quad \sigma(\lambda) a = \sigma(\lambda)\sigma^2 a$
λ $\quad = \sigma(\sigma(a)\lambda)$

$\Rightarrow \sigma|_F$ order 2 nontriv. aut $\quad \sigma(\lambda\sigma(a)) = a\,\sigma(\lambda)$

$\Rightarrow F/F^\sigma$ is Gal w/ gp $C_2 = \langle\sigma|_F\rangle$

This is called an inv of 2nd kind.

A matrix $T \in M_n(F)$ is
- symmetric if $T = T^t$
- skew if $T = -T^t$
- symmetrized if $T = S + S^t$ same S
- sk. sym'd if $T = S - S^t$ same S.

ex: $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ symm.

sym'd $\begin{pmatrix} 2a & b \\ b & 2a \end{pmatrix}$

skew char $\neq 2$ $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$

sk'd $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$

char 2 $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$

Q: Do all inv's come as adjoints to sym or sk. sym. bilinr forms?

Yes. if $\sigma \in \mathrm{Inv}_F(\mathrm{End}(V))$ (1^{st} kind)

$\sigma = \sigma_b$ some bilin b

$\sigma = \sigma_b = t \circ \mathrm{inn}_M$

$id = \sigma^2 = t \cdot \mathrm{inn}_M \cdot t\, \mathrm{inn}_M$

$$T = id(T) = \sigma^2(T) = \left(M\left(MTM^{-1}\right)^t M^{-1}\right)^t$$

$$= \left(M\left((M^t)^{-1} T^t M^t\right) M^{-1}\right)^t$$

$$= (M^t)^{-1} M T M^{-1} M^t$$

$$= \mathrm{inn}_{(M^t)^{-1}M}(T)$$

$$\Rightarrow (M^t)^{-1} M \in F^*$$

$$\underset{\varepsilon^{-1}}{\shortparallel}$$

$$M = \varepsilon^{-1} M^t$$

$$M^t = \varepsilon M$$

$$M = M^{tt} = (\varepsilon M)^t = \varepsilon^2 M \Rightarrow \varepsilon^2 = 1$$

(recall, M nonsing)

<u>Lem</u> Suppose M = Gram for b then

- b symm $\Leftrightarrow$ M symm
- b skew $\Leftrightarrow$ M skew

ω_b alt. $\Leftrightarrow$ M skew'd

Pf sym, skew easy. ✓

3^{rd} $\Leftarrow$ ✓ $\Rightarrow$?

Sublem M skew'd $\Leftrightarrow$ M skew & diagonal entries all 0.

if sk'd $\Rightarrow$ skew & Δ entries all 0

$S - S^t$

if Δ entries all 0 & skew

$\boxed{\begin{matrix} 0 & \text{stuff} \\ -\text{stuff} & 0 \end{matrix}}$ = skew'd of $\begin{bmatrix} 0 & \text{stuff} \\ 0 & 0 \end{bmatrix}$ D D ✓

Def If A is a CSA/F, σ an inv. on A of 1^{st} kind,
we say σ is orthogonal if σ_F = adj for symm.
sympectic if σ_F = adj for skew

Graham-Schmitt / Darboux

Lem: If ω is alternating nondg. then
can write $V = \langle x_1, y_1 \rangle \perp \langle x_2, y_2 \rangle \perp \cdots \perp \langle x_n, y_n \rangle$
(where $W_1 \perp W_2$ = means $W_1 \oplus W_2$ & $\omega(w_1, w_2) = 0$ all $w_i \in W_i$)
& where $\omega(x_i, y_i) = 1$

Pf: Induct on dim V, base case dim V = 0 ✓

choose $x_1 \in V \setminus \{0\}$, nondeg $\exists\, y_1$ $\omega(x_1, y_1) \neq 0$
scale, $\omega(x_1, y_1) = 1$

$\langle x_1, y_1 \rangle \cap \langle x_1, y_1 \rangle^{\perp} = 0$

$\lambda x_1 + \mu y_1 \ldots$ $\quad V = \langle x_1, y_1 \rangle \perp \underbrace{\langle x_1, y_1 \rangle^{\perp}}$ $\square$

<u>Prop</u> if b is ε-symm. then can write

$V = W \perp V^{alt}$ where V^{alt} is alternating &

$W = \langle z_1 \rangle \perp \langle z_2 \rangle \perp \cdots \perp \langle z_n \rangle$ $\,||\,$ $\langle a_1, \ldots, a_n \rangle$

$b(z_i, z_i) = a_i \neq 0$

<u>Pf:</u> induct on dim V

either V alt or $\exists\, z_1$ s.t. $b(z_1, z_1) \neq 0 = a_1$

$\langle z_1 \rangle \cap \langle z_1 \rangle^{\perp} = 0 \Rightarrow V = \langle z_1 \rangle \perp \langle z_1 \rangle^{\perp}$ $\square$

ω alternating $\rightsquigarrow$ after a change of basis

looks like $\langle x_1, y_1 \rangle \perp \cdots \perp$

$$\text{Gram matrix} = \begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & 0 \\ & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & \\ & & \ddots & \\ 0 & & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \end{pmatrix} = \Omega$$

<u>Pfaffian</u>

$\sqrt{\ }$ of det

M skew symmetrized, invertible matrix. $\Longleftrightarrow$ ω alternating

via Darboux $\Rightarrow$ $M \longleftrightarrow \Omega$ after chg of basis.

i.e. $\omega(x,y) = \text{stdalt.}(\varphi x, \varphi y) = (\varphi x)^t \Omega \varphi y$

A = matrix for φ $\qquad \omega(x,y) = x^t A^t \Omega A x$

So $\quad M = A^t \Omega A \qquad \det \Omega = 1 \qquad \det M = (\det A)^2$

<u>Def</u> $\quad Pf(M) = \det(A)$

$Pf(M)^2 = \det M$

general nonsense $\Rightarrow$

$Pf(M)$ = rat'l fcn in entries of M

$Pf(M)^2$ = poly fcn $\Rightarrow$

$Pf(M)$ poly (polys are a UFD)

If (V,ω) is a space w/ alt. form ω nondeg,

want to define, for $T \in \text{Sym'd}(\text{End}, \omega)$

" $S + \sigma_\omega(S)$

Pfaffian χ poly.

v = sk. sym'd.

write $\quad \omega(x,y) = x^t v y \quad$ then $\quad v^t = -v$

$\sigma_\omega = \text{inn}_v \circ t$

$$T = S + \sigma_\omega(S) = S + \text{inn}_v(S^t)$$
$$= S + v S^t v^{-1}$$

$$= (Sv + vS^t)\, v^{-1}$$

$$= \big(\underbrace{Sv - (Sv)^t}_{\text{sk symm'd}}\big)\, v^{-1}$$

$$\det T = \det\big(Sv - (Sv)^t\big)(\det v)^{-1}$$

$$= Pf(\quad)^2 \left(Pf(\,)^2\right)^{-1}$$

ignore this

$$\chi_T(x) = \det(X\cdot 1 - T)$$

$$= \det\left(X\cdot 1 - \big(Sv - (Sv)^t\big)v^{-1}\right)$$

$$= \det\big(\underset{\text{sk-sym}}{Xv} - \underbrace{(Sv - (Sv)^t)}_{\text{sk sym}}\big)(\det v)^{-1}$$

$$= Pf(\qquad\qquad)^2 \left((Pf\, v)^2\right)^{-1}$$

$\chi_T(x)$ is the square of a poly

let $P\chi_T(x)$ = monic sq. root.

have $P\mathrm{Norm}$ = last coeff

$P\mathrm{tr}$ = second etc...

Thm If T is symm'd for ω alt. then

$P\chi_T(T) = 0$.

Aside

Given $\begin{array}{c} A \\ \mid \deg 5 \\ F \end{array}$ given $E \subset A$ max'l

consider Gal closure $\begin{array}{c} L \\ \mid \\ E \\ \mid 5 \\ F \end{array}$ $G \subset S_5$

Open problem: if A is $\deg 5$ $\exists$? $E \subset A$ max'l s.t.

Gal closure $\begin{array}{c} L \\ \mid \\ E \\ \mid \\ F \end{array}$ G does not satisfy $G \cong S_5$.

if $\deg A = 8$ & $\operatorname{per} A \mid 2$ $\Rightarrow$ $\exists$ a $C_2 \times C_2 \times C_2$ Gal. max'l subfield.
(Rowen)

Open problem: if $\operatorname{ind} A \neq 4$ or $(\operatorname{ind} A, \operatorname{per} A) \neq (8,2)$
if $\operatorname{ind} A = p^n$ $n > 1$, $\exists$ nonmax'l subfields of A?
$(\operatorname{per} A, \operatorname{ind} A) = (p^m, p^n)$ $n > 1$

But if $\operatorname{per} A = 2$ $\operatorname{ind} = 2^n$, then $\exists$ "half-max'ls"
i.e. $\begin{array}{c} E \\ \mid 2 \\ L \\ \mid \\ F \end{array}$ E = max'l.

Lem (V,b) bilin $\dim V = n$

b symmetric $\Rightarrow \mathrm{Sym}(\mathrm{End}\,V, \sigma_b)$ has dim $\frac{n(n+1)}{2}$

b skew $\Rightarrow \mathrm{Skew}(\text{— " —})$ has dim — " —

Pf: $\mathrm{Sym}(M_n(F), t) \xrightarrow{\sim} \mathrm{Sym}^{\varepsilon}(\underset{\mathrm{End}\,V}{A}, \underset{\varepsilon\text{-sym}}{\sigma})$

$TM^{-1} \longleftarrow\!\shortmid\ T$

M = Gram for b.

Existence of invs.

Given A CSA period 2, $\exists\, \sigma \in \mathrm{Inv}_F(A)$ orthogonal.

$G = \mathrm{Gal}(E/F)$

Pf: $A \longleftrightarrow H^1(G, PGL(V \otimes E))$

$GL(V)$ acts on $(S^2 V)^*$

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
F^* & \xrightarrow{x \mapsto x^{-2}} & F^* \\
\downarrow & & \downarrow \\
GL(V) & \longrightarrow & GL((S^2V)^*) \\
\downarrow & & \downarrow \\
PGL(V) & \longrightarrow & PGL((S^2V)^*) \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}$$

$$H^1(G, GL(V\otimes E)) \longrightarrow \underset{[A]}{H^1}(G, PGL(V \otimes E)) \longrightarrow H^2(G, E^*)$$

$\downarrow \qquad\qquad\qquad \downarrow \cdot(-2)$

$H^1(G, GL($ ...

$$\downarrow \qquad\qquad\qquad \downarrow \qquad\qquad\qquad \downarrow$$

$$H^1(G, GL(S^2(V \otimes E)^*)) \to H^1(G, PGL(S^2 \quad)) \to H^2(G, E^*)$$

$$[S^2(V))^*$$

$$H^1(G, Aut(VS))$$