Lecture 7: Primary decomposition and some involutions

Friday, February 20, 2015 2:33 PM

Primary decomposition

M group $m \in M$ m torsion

$m = m_1 m_2 \cdots m_r$ m_i's commute

w/. prime order

m_i has prime power order.

$$\begin{tikzcd} \mathbb{Z} \arrow[r] & M \\ 1 \arrow[r, mapsto] \arrow[dr, bend right] & m \\ & \mathbb{Z}/n \quad 1 \arrow[u, bend right] \end{tikzcd}$$

m is n-torsion

$n = p_1^{r_1} \cdots p_s^{r_s}$

$\mathbb{Z}/n$

$\shortparallel$

$\mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_s^{r_s}$

$(a_1, \ldots, a_s)$

$b_i \in \mathbb{Z}/n$

$\uparrow$

$(0, \ldots, 1, \ldots, 0)$

$\uparrow$

i^{th} slot

$1 = \sum a_i b_i \in \mathbb{Z}/n$ $\qquad \overline{a_i b_i} = \overline{a_i}$ i^{th} slot

$\downarrow$

$\begin{cases} \overline{a_i} \text{ in } i^{th} \text{ slot} \\ 0 \text{ in } j \neq i^{th} \text{ slot} \end{cases}$

$m = m^{\sum a_i b_i} = m^{a_1 b_1} \cdots m^{a_s b_s}$ $\qquad m^{a_i b_i}$ order $| \, p_i^{r_i}$

In $Br(F)$:

Prop. If D a d.alg. then if we write $[D] = [D_1] + \cdots + [D_s]$

primary

Prop if D a d.alg. then if we write $[D] = [D_1] + \dots + [D_s]$ primary components

$\Rightarrow D = D_1 \otimes \dots \otimes D_s$

Some things we should have said.

If E/F is any field extension

Then: $\mathrm{Br}(F) \longrightarrow \mathrm{Br}(E)$
$[A] \longmapsto [A \otimes E]$ is a group homomorphism

$$(A \otimes B) \otimes E \cong (A \otimes E) \otimes_E (B \otimes E)$$

E splits $A \Leftrightarrow [A] \in \ker(\mathrm{Br}(F) \to \mathrm{Br}(E)) = \mathrm{Br}(E/F)$

Prop If E/F is a splitting field for A then $\exists B \sim A$ s.t.
E max'l subfield of B.

Pf: $E \hookrightarrow \mathrm{End}_F(E) = M_n(F)$

$E \subset A \otimes M_n(F) \supset C_{A \otimes M_n(F)}(E) \sim A \otimes M_n(F) \otimes E \sim A \otimes E$ split.

$$\Downarrow$$

$$M_{\deg A}(E) \supset M_{\deg A}(F)$$

$$E \subset C_{A \otimes M_n(F)}\left(M_{\deg A}(F)\right) = \text{CSA equiv. to } A$$

$$\text{degree} = n = [E:F] \quad \square$$

<u>Cor</u> Every CSA $\sim$ a crossed prod:

<u>Pf:</u> Given D, choose $L \subset D$ max'l sep. subfield

$$\begin{array}{c} E \\ | \\ L \\ | \\ F \end{array} \Big) G$$

Galois closure, $E \otimes D = E \otimes_L (L \otimes_F D)$

$D \sim B$, $E \subset B$ max'l subfield

$[D] \in Br(E/F)$

<u>Alternate characterization of index</u>

<u>Prop:</u> A/F CSA then

$\operatorname{ind} A = \min\{[E:F] \mid E/F \text{ finite w/ } A \otimes E \text{ split}\}$

$= \gcd\{$ ______ '' ______ $\}$

$= \min\{$ ______ $\mid E/F$ finite, sep, ______ $\}$

$= \gcd\{$ ______ $\}$

<u>Pf:</u> suppose E/F splits A

wLOG A division alg.

$B \sim A$ w/ $E \subset B$ max'l subfield

$$B = M_m(A) \Rightarrow [E:F] = m \cdot \deg A = m \, \mathrm{ind}\, A$$

$\Rightarrow \mathrm{ind}\, A \mid [E:F]$ every splitting field.

We know $\exists$ max'l sep. subfields of any div. alg.

$\Rightarrow$ everything. $\square$

Note: if $[A] \in Br(F)$, E/F then

$\mathrm{per}\, A \otimes E \mid \mathrm{per}\, A$

Lem $\mathrm{ind}(A \otimes E) \mid \mathrm{ind}\, A$

Pf: Suppose $K \subset A$ max'l sep. subfield, A div. alg.

$$\begin{tikzcd} & KE \arrow[dl, dash] \arrow[dr, dash, "\text{divides ind } A"] & \\ K \arrow[dr, dash, "\mathrm{ind}\, A"'] & & E \arrow[dl, dash] \\ & F & \end{tikzcd}$$

KE/E sp. field for A_E

$\mathrm{ind}\, A \otimes E \mid [KE:E] \mid \mathrm{ind}\, A$

$\square$

Lem if E/F finite field ext, then

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

Pf: Let L/E split $A\otimes E$, $[L:E] = \operatorname{ind} A\otimes E$

then L/F splits A $\Rightarrow$

$\operatorname{ind} A \mid [L:F] = [L:E][E:F] = \operatorname{ind}(A\otimes E)[E:F]$. Δ

Cor: if E/F is rel. prime to $\operatorname{ind} A$ then

$\operatorname{ind} A = \operatorname{ind} A\otimes E$

Lem: If $[E:F]$ rel. prime to $\deg A$ $\quad$ (E/F sep.)

($\Rightarrow$ $\operatorname{per} A\otimes E = \operatorname{per} A$.) $\Leftarrow$ will do later.

$\operatorname{ind} A\otimes E = \operatorname{ind} A$.

Lem: A per $n = p^k$ sp field

then A has index a p-pow.

Pf: Let

$$\begin{tikzcd}
L \arrow[d, dash] \arrow[dr, dash, "P - p\text{-sylow}"] & \\
E \arrow[d, dash, "\operatorname{ind}"] & K \arrow[dl, dash, "\text{prime to } p"] \\
F &
\end{tikzcd}$$

G Gal closure

choose E / F sp. field.

previous lemma

$\Downarrow$

$\operatorname{ind} A\otimes K = \operatorname{ind} A$

L/K splits $A\otimes K$ $\Rightarrow$ $\operatorname{ind} A\otimes K$ p-pow.

$\Rightarrow$ p_i primary part D_i of D has index p_i-pow.

know that if E/F max'l subfield for D, then E/F splits

D_i $\quad$ $\operatorname{ind} D_i \mid [E:F]$ & be a p_i^{th} power.

$\operatorname{ind} D = p_1^{t_1} \cdots p_s^{t_s}$ $\qquad$ $\operatorname{ind} D_i \mid p_i^{t_i}$

if smaller $\Rightarrow \bigotimes D_i$'s smaller degree than D.

can't happen since D has min'l degree in Br class

$\Rightarrow \operatorname{ind} D_i = p_i^{t_i}$

$\Rightarrow$ Both sides of $D \longleftrightarrow D_1 \otimes \cdots \otimes D_s$ same degree

$\Rightarrow$ isomorphic.

Let's move on

Given a vector space w/ a symm. bilinear form. (V, b)

$b : V \otimes V \longrightarrow F$ $\qquad$ $b(v,w) = b(w,v)$

need b nondegenerate if $V \longrightarrow V^*$

this is an iso. $\quad v \longmapsto b(v, -)$

Ex: recall standard inner product on $F^n \longleftrightarrow$ column vectors

$b(v,w) = v^t \cdot w$ $\quad$ then if

$$b(Tv,w) = (Tv)^t w = v^t T^t w = b(v, T^t w)$$

Similarly: given general b on V/F, given $T \in End(V)$

$$w \longmapsto b(w, T(\_)) \in V^*$$

by nondegeneracy,

$$b(w, T(-)) = b(v, -)$$

some v

define $\tau_b(T)(w) = v$

by def: $\quad b(w, Tu) = b(\tau_b(T)w, u)$

we call $\tau_b : End(V) \circlearrowleft$ is the adjoint involution associated to b.

Def an involution on a (CSA) A/F is a anti-homomorphism $\tau : A \xrightarrow{\sim} A^{op}$ w/ $\tau^2 = id_A$.

One should check:

τ_b defined above is:

- well defined ($\tau_b(T) \in End(V)$)
- anti-aut
- period 2

$$b(v, TSw) = b(\tau_b(T)v, Sw)$$
$$= b(\tau_b(S)\tau_b(T)v, w)$$
$$\parallel$$
$$b(\tau_b(TS), v, w)$$

all w, nondegenacy

$$\Rightarrow \tau_b(S)\tau_b(T) = \tau_b(TS) \quad \text{all } T, S.$$

Recall: Given b symm bilinr, define q_b by

$$q_b(x) = b(x,x)$$

q_b: deg 2 hom poly

Given q q. form, get symm bilinr form:

$$\tilde{b}_q(x,y) = q(x+y) - q(x) - q(y)$$

q nondg if $\tilde{b}_q$ nondg.

$$\tilde{b}_{(q_b)} = 2b$$

in chr $\neq 2$, $b_q = \dfrac{\tilde{b}_q}{2}$

get a bijective corresp.

Things to say:

- To what extent is b (or q) determined by τ_b
- Does every involution on $\mathrm{End}(V)$ come from bilnr form? (need skew forms)
- When do CSA's (not split) have involutions?

- What structural props of q. forms carry over to CSA's w/ involutions?

Understand groups defined by alg. eqns.

coords $x_1, \ldots, x_n$ on v. space $V = F^n$

$G(F)$ = solns to some set of poly eqns in V

w/ group law described by poly functions

ex: $GL_n(F) = (\det \neq 0)$

scalar matrices normal connected

$O_n(F) = \{TT^t = 1\}$

$SO_n(F)$ (char $\neq 2$)

$SL_n(F)$ simple

connected w/ no subgps normal, connected defined by eqns $f_1, \ldots, f_k = 0$

"simple"

A_n	B_n	C_n	D_n	G_2	F_4	E_6 ...
$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$	$\uparrow$		
SL_{n+1}	SO_{2n+1}	Sp_{2n}	SO_{2n}			
SU						

preserve Hermitian form.

$TT^\tau = 1$ appropriate τ

punchline: simple lin. alg. gps of types A, B, C, D (except D_4) come from CSA's w/ involution.

- $\tau_b = \tau_{b'} \iff b' = \lambda b$ some $\lambda \in F$.

- If τ is an inv. on A then

$$\tau : A \xrightarrow{\sim} A^{op}$$

$$A \otimes A \cong A \otimes A^{op} \simeq 1.$$

split

$\Rightarrow$ per $[A] = 2$ or 1.

conversely, if per $A \mid 2 \Rightarrow \exists$ involutions.