

Primary decomposition

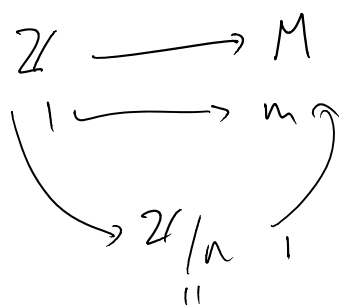
M group $m \in M$ m torsion

$$m = m_1 m_2 \dots m_r$$

m_i 's commute

wt. prime order

m_i has prime power order.



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

$$(a_1, \dots, a_s)$$

m is n -torsion

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

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

$$(0, \dots, 1, \dots, 0)$$

i -th slot

$$1 = \sum a_i b_i \in \mathbb{Z}/n$$

$\downarrow$
 a_i in i -th slot
 b_i in i -th slot

$$\overline{a_i b_i} = \overline{a_i}$$

$$m = m^{\sum a_i b_i} = m^{a_1 b_1} \dots m^{a_s b_s}$$

$$m^{a_i b_i} \text{ order } p_i^{r_i}$$

In $\mathcal{B}_c(P)$:

D_{ann} of D a d-aly. then if we write $[D] = [D_1] + \dots + [D_s]$

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

Some things we should have said.

If E/F is any field extension

then $\begin{matrix} \text{Br}(F) & \longrightarrow & \text{Br}(E) \\ [A] & \longmapsto & [A \otimes E] \end{matrix}$ is a group homomorphism

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

E splits $A \iff [A] \in \ker(\text{Br}(F) \rightarrow \text{Br}(E)) = \text{Br}(E/F)$

Prop If E/F is a splitting field for A then $\exists B \sim A$ s.t. E max l. subfield of B .

PF: $E \hookrightarrow \text{End}_F(E) = M_n(F)$

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

split.

$$M_{dg A}^{(E)} > M_{dg A}^{(F)}$$

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

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

Con Every CSA $\sim$ a crossed prod:

Pf. Given D , choose LCD max'l xp. subfield

$$\begin{array}{c} E \\ | \\ L \\ | \\ F \end{array} \Bigg) G \quad \text{Galois closure, } E \otimes D = E \otimes_L (L \otimes_F D)$$

$$D \sim B, \quad E \subset B \text{ max'l subfield}$$

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

Alternate characterization of index

Prop: A/F CSA then

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

$$= \gcd \{ \text{---} \mid \text{---} \}$$

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

$$= \gcd \{ \text{---} \}$$

Pf: suppose E/F splits A

1. Induction on

wlog A division alg.

$B \sim A$ w/ ECB max'l subfield

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

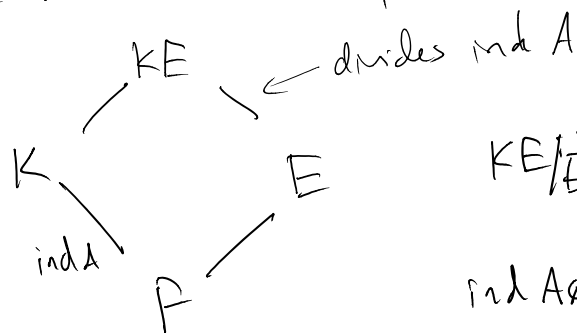
$\Rightarrow \text{ind } A \mid [E:F]$ every splitting field.

We know $\exists$ max'l sep. subfields of any div. alg.
 $\Rightarrow$ every th. $\square$

Note: if $(A \in Br(F))$ E/F then
 $\text{pr } A \otimes E \mid \text{pr } A$

Lemma $\text{ind}(A \otimes E) \mid \text{ind } A$

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



KE/E sp. field for $A \otimes E$
 $\text{ind } A \otimes E \mid [KE:E] \mid \text{ind } A$

$\square$

Lemma if E/F field ext, then
 $\text{ind } A \mid \text{ind}(A \otimes E) [E:F]$

$$\left(\text{ind } A \otimes E \mid \text{ind } A \right)$$

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

then L/F splits $A \Rightarrow$

$$\text{ind } A \mid [L:F] = [L:E][E:F] = \text{ind}(A \otimes E) [E:F]. \quad \Delta$$

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

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

Lem If $[E:F]$ rel. prime to $\deg A$ (E/F sep.)
 $(\Rightarrow \text{per } A \otimes E = \text{per } A.) \leftarrow \text{will do later.}$
 $\text{ind } A \otimes E = \text{ind } A. \leftarrow$

Lem A per $n = p^k$ sp. feld

then A has index a p -power.

Pf Let $L \mid E \mid K$
 L is p -p-sylow
 E is ind
 F is $\text{prime to } p$
 choose E as Gal. closure of F in L
 E is sp. feld.

previous lemma
 $\Downarrow$

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

$$L/K \text{ splits } A \otimes K \Rightarrow \text{ind } A \otimes K \text{ } p\text{-power.}$$

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

know that if E/F maximal subfield for D , then E/F sp¹¹¹³

D_i $\text{ind } D_i \mid [E:F]$ is be a p_i^{th} power.

$$\text{ind } D = p_1^{t_1} \cdots p_s^{t_s}$$

$$\text{ind } D_i \mid p_i^{t_i}$$

if smaller $\Rightarrow \otimes D_i$ is smaller degree than D .

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

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

$\Rightarrow$ Both sides of $D \iff D_1 \otimes \cdots \otimes D_s$ same degree $\Rightarrow$ isomorphic.

let's move on

Given a vector space w/ a ^{symmetric} b form. (V, b)

$$b: V \times V \rightarrow F \quad b(u, w) = b(w, u)$$

need b nondegenerate if $V \rightarrow V^*$
 this $\rightarrow$ is an iso. $v \mapsto b(v, -)$

Ex 1 recall standard inner product on $F^n \iff$ column vectors
 $b(u, w) = u^t \cdot w$ 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 $T \in \text{End}(V)$

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

by nondegeneracy,

$$b(w, T(-)) = b(\underset{\text{some } v}{v}, -)$$

$$\text{define } \tau_b(T)(w) = v$$

$$\text{by def: } b(w, Tu) = b(\tau_b(T)w, u)$$

we call $\tau_b: \text{End}(V) \ni$ is the adjoint involution associated to b .

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

One should check:

τ_b defined above is:

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

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

$$b(\tau_b(TS), v, w)$$

all w , nondegeneracy

$$\Rightarrow \tau_b(S)\tau_b(T) = \tau_b(TS) \quad \forall T, S.$$

Recall: Given b^{sym} bilinear, define q_b by

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

q_b : deg 2 hom poly

Given q q. form, get $\hat{b}$ bilinear form:

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

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

$$\tilde{b}_{(q_b)} = 2b \quad \text{in char } \neq 2, \quad b_q = \frac{\tilde{b}_q}{2}$$

get a bijective corresp.

Things to say:

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

- What structural props of $\mathfrak{g}$ -forms carry over to CSA's w/ involutions?

Understand groups defined by alg. eqns.

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

$G(F) =$ solns to some set of poly eqns in V
w/ graph law described by poly functions

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

$\left. \begin{array}{l} \text{scalar matrices} \\ \text{normal} \\ \text{connected} \end{array} \right\} \begin{array}{l} O_n(F) = \{TT^t = I\} \\ \vdots \\ SL_n(F) \text{ simple} \end{array}$

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

connected
w/ no subgrps
normal, connected
defined by eqns
 $f_1, \dots, f_r = 0$
"simple"

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

$TT^t = I$ appropriate τ

punchline: simple lnr alg. sps of types A, B, C, D (except D_4)
come from CSA's w/ involutions.

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

- If τ is an inv. on A then

$$\tau \cdot A \cong A^{\text{op}}$$

$$A \otimes A \cong A \otimes A^{\text{op}} \cong 1, \text{ split}$$

$$\Rightarrow \text{pr}[A] = 2 \text{ or } 1.$$

conversely, if $\text{pr}[A] \equiv 2 \Rightarrow \exists$ involutions.