

Lecture 19

11/9

Central simple algebras.

Recall:

$$\mathbb{R}/k \text{ c.s.a. } [R:k] = n^2.$$

$$k \subset L \subset R$$

commutative subalg.

① L is a field $\Rightarrow \underline{\underline{[L:k] \mid n}}$

② In general.

$$R = M_n(k).$$

A diagram of a square matrix of size $n \times n$. The matrix is divided into four quadrants by a horizontal line and a vertical line. The top-left quadrant is labeled $n/2$ on the left and contains the letter a . The bottom-left quadrant is labeled $n/2$ on the left. The bottom-right quadrant is labeled a and contains a diagonal sequence of dots and the letter a . The top-right quadrant is shaded with diagonal lines and is labeled a on the left. To the right of the matrix is the expression $\sim \frac{n^2}{4}$.

③ $L =$ product of fields.

$$\Rightarrow [L:k] \leq n.$$

Thm (Noether-Skolem)

R/k c.s.a. finite-dim'l / k ,

S : simple k -algebra.

$$S \begin{array}{c} \xrightarrow{\varphi_1} \\ \xrightarrow{\varphi_2} \end{array} R \quad (k\text{-alg maps})$$

$\Rightarrow \exists u \in R^{\times}$, s.t.

$$\varphi_1(s) = u \varphi_2(s) u^{-1}, \quad \forall s \in S.$$

Special case:

① $S = R$.

$$\varphi_1 = \varphi: R \xrightarrow{\sim} R \quad (k\text{-linear auto.})$$

$$\varphi_2 = \text{id}: R = R.$$

$\Rightarrow \exists u \in R^{\times}$ s.t.

$$\varphi(r) = u r u^{-1} \quad \forall r \in R.$$

\iff any automorphism of R is inner.

(2) $L = S =$ a ^{finite} field extension of k .

\Rightarrow Any two embeddings $L \hookrightarrow R$ are conjugate by some $u \in R^\times$.

Pf.

$$S \hookrightarrow R \hookrightarrow R$$

$\varphi_1 \qquad \uparrow \text{usual}$

$$\rightsquigarrow R \cong R' \cong S \otimes_k R^{\text{op}} \text{ - mod}$$

simple \downarrow *c.s.a./k*

simple k-als. finite-dim'l.

$$\left[\begin{array}{l} S \otimes_k R^{\text{op}} \text{ has a unique simple mod } \underline{M} \\ \underline{R'} \cong M^{\oplus a} \\ [R:k] = a \cdot \dim_k M \end{array} \right.$$

Using $S \hookrightarrow R \hookrightarrow R \Rightarrow$ same conclusion

$\varphi_2 \cong R''$

$$R'' \cong M^{\oplus a}$$

$\Rightarrow R' \cong R''$ as $S \otimes R^{\text{op}}$ -mod.

i.e., $\exists u: R' \xrightarrow{\sim} R''$ $S \otimes R^{\text{op}}$ -linear

$\parallel \quad \parallel$

$R \hookrightarrow$

R

$R \hookrightarrow$

R

Since u comm with right mult

$\Rightarrow u$ is left mult by $u \in R$

u is isom $\Rightarrow u \in R^{\times}$

u is S -linear

$$\begin{array}{ccc}
 R & \xrightarrow{\cdot u \cdot} & R \\
 \varphi_1(s) \cdot \downarrow & \circlearrowleft & \downarrow \varphi_2(s) \cdot \\
 R & \xrightarrow{\cdot u \cdot} & R
 \end{array}$$

$$\begin{array}{ccc}
 1 & \longrightarrow & u \\
 \downarrow & & \downarrow \\
 \varphi_1(s) & \longrightarrow & \boxed{u \varphi_1(s) = \varphi_2(s) u}
 \end{array}$$

$$\varphi_2(s) = u \varphi_1(s) u^{-1}$$

$$\forall s \in S$$

□

Thm (Wedderburn) Any finite division ring is a field.

Pf. D finite div. ring. $[D:k] = n^2$

$Z(D)$ finite field $= k = \mathbb{F}_q$.

$\forall x \in D$,

$k[x] \subset D$.

"finite field"

$k[x] \subset L = \text{max. comm. subring.}$
 $= \text{field.}$

$$\Rightarrow [L:k] = n.$$

$$L \cong \mathbb{F}_{q^n}.$$

Noether-Skolem:

$$\mathbb{F}_{q^n} \subset D.$$

unique up to conjugation by D^\times

$$\Rightarrow \text{Fix } i: \mathbb{F}_{q^n} \subset D.$$

$\forall x \in D$ can be conjugated to $i(\mathbb{F}_{q^n})$

$$G = D^\times \text{ gp of order } q^n - 1.$$

conjugates of $i(\mathbb{F}_{q^n}^\times)$ cover the whole D^\times .

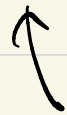
H

$H \subset G$ - Subgp.

$$\bigcup_{g \in G/H} \underline{gHg^{-1}} = G$$

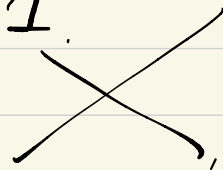
$$\underline{\underline{ghHh^{-1}g^{-1}}} = gHg^{-1}$$

$$|\text{LHS}| < |G/H| \cdot |H| = |G|$$



strict if $H \neq G$

'the gHg^{-1} all contain 1.'



$$\Rightarrow H = G \Rightarrow D = \mathbb{F}_{q^n}, n=1.$$



Reformulation:

$$\text{Br}(\mathbb{F}_q) = 0.$$

Ex of k s.t. $\text{Br}(k) = 0.$

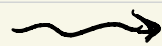
① $k = \text{alg. closed.}$

$$K = \underline{k(t)}$$

$$\Rightarrow \text{Br}(K) = 0.$$

similarly,

$$\mathbb{Q}_p$$



$$\mathbb{Q}_p^{\text{unr}}$$

max. unram.
extn of $\mathbb{Q}_p.$

$$\text{Br}(\mathbb{Q}_p^{\text{nr}}) = 0.$$

$$\text{Br}(\widehat{\mathbb{Q}_p^{\text{nr}}}) = 0.$$

More generally,

K : discrete valuation field.

residue is alg. closed.

complete.

$$\Rightarrow \text{Br}(K) = 0.$$

(2) $k = \text{alg. closed}$.

K/k transcendence degree 1.
(*fig. extn.*).

(i.e. $K/k(t)$ finite)

"1-dim'l function fields over k ".

(rational functions on alg curves/ k).

$$\text{Br}(K) = 0.$$

$$K = k(t).$$

Splitting fields of c.s.a. ← finite-dim'l.

R/k c.s.a. $[R:k] = n^2$.

L/k field extn is called a splitting field for R if $R \otimes_k L \cong M_n(L)$.

$$\left(\begin{array}{ccc} (\Leftrightarrow) & \text{Br}(k) & \longrightarrow \text{Br}(L) \\ & [R] & \longmapsto 0 \end{array} \right)$$

$$R = M_m(D).$$

If L/k is a splitting field for D .

$$D \otimes_k L \cong M_d(L).$$

$$\begin{aligned} R \otimes_k L &\cong M_m(D \otimes_k L) \\ &\cong M_m(M_d(L)) \cong M_{md}(L). \end{aligned}$$

Prop. D/k c.d.a.

$L \subset D$ max. subfield.

Then L is a splitting field of D .

(if $[D:k] = n^2 \Rightarrow \exists$ splitting field of deg n)

Pf.

$$\underset{=}{D} \underset{=}{\otimes_k} L \supseteq D$$

($D \subset D \subseteq L$)

$$\varphi: \underset{k}{D \otimes L} \rightarrow \text{End}_L(D)$$

c. simple L -algebra of dim n^2 over L .

right mult.

$$M_n(L)$$

φ injective

$\dim_L \Rightarrow \varphi$ is \cong .

$$n = \dim_L D$$

Using $[L:k] = n$.

$$\Rightarrow [D:L] = \frac{[D:k]}{[L:k]} = n$$

$$D \underset{k}{\otimes} L = M_n(L).$$

□

Thm (char $k = p > 0$),

D/k c.d.a.

Then D has a separable (finite) splitting field.

Recall:

L/k separable \iff
| finite.

any of the following holds.

• $\forall x \in L$, x is a root of a separable polynomial over k .
(no repeated roots)

• $L \otimes_k k'$ (k'/k ^{finite} extn)

has no nilpotent elements.
(\iff a product of fields)

• $L \otimes_k \bar{k}$ has no nilp. elements.
(\iff a product of \bar{k})

purely inseparable elts:

$$x^{p^e} = a :$$

$$L = k[x] / (x^{p^e} - a)$$

$$L \otimes_k \bar{k} = \bar{k}[x] / (x^{p^e} - a), \quad \text{let } \alpha^{p^e} = a.$$

$$= \bar{k}[x] / (x - \alpha)^{p^e}$$

$x - \alpha$ is nilpotent.

Pf of Thm.

$$D \text{ c.d.a. / } k, \quad [D:k] = n^2.$$

If $D \otimes_k k'$ has a zero divisor.

$$\cong M_m(\underline{D}')$$

c.d.a. / k' .

$$n^2 = m^2 \cdot [D':k']$$

$$[D':k'] < [D:k].$$

Induction on n .

inductive step: find $x \in D \setminus k$,

s.t. $k[x]$ is separable over k .

with such x . $k' = k[x]$.

$$D \otimes_k k' \supset \boxed{k' \otimes_k k'}$$

not a field.

$$k' \otimes_k k' \twoheadrightarrow k'$$

hence $k' \otimes_k k'$ has zero div.

$$\text{so does } \boxed{D \otimes_k k'} \cong M_m(D').$$

$$[D' : k'] < [D : k]. \quad (m > 1).$$

↑ use hypoth.

Suppose we can't find such x ,

$\Rightarrow \forall x \in D$ is purely inseparable / k .

($x \in D \Rightarrow x^{p^e}$ is separable / k
(some e)

$$x^{p^e} \notin k. \quad \checkmark$$

o/w: $x^{p^e} \in k. \quad \otimes$)

$$D \subset D \otimes_{\mathbb{k}} \bar{\mathbb{k}} \cong M_n(\bar{\mathbb{k}}).$$

$$\alpha \otimes 1 \rightarrow n \times n \text{ matrix } \Sigma$$

$$\Sigma^{p^e} \in \mathbb{k} I_n.$$

\Rightarrow all eigenvalues of Σ (in $\bar{\mathbb{k}}$) are the same.

$$p \mid n.$$

$$\text{Tr}(\Sigma) = \text{Tr} \begin{pmatrix} \lambda & & * \\ & \lambda & \\ 0 & & \ddots \\ & & & \lambda \end{pmatrix} = 0.$$

$M_n(\bar{\mathbb{k}})$ is the $\bar{\mathbb{k}}$ -span of D .

$$\Rightarrow \text{Tr}(M_n(\bar{\mathbb{k}})) = 0. \quad \square$$

Rk.

$$\mathbb{k} = \mathbb{F}_p((t)).$$

$$L = \mathbb{F}_{q^n}((t)).$$

$$D = L \langle x; \sigma \rangle / (x^n - t^a). \quad \sigma = \text{Frob}$$

$\gcd(a, n) = 1 \Rightarrow D$ is c.d.a./k.

$$n = p.$$

$$D \supset \underbrace{k[x] / (x^p - t^a)}_{\text{insep}/k} = L'$$

$$H^2(k, G_m).$$

L/k ~~sep~~ Galois.

$$H^p(\underline{L/k}, \underline{H^q(L, G_m)}) \Rightarrow \underline{H^{p+q}(k, G_m)}$$

$$H^1(L, G_m) = 1 \quad H^2(k, G_m)$$

$$H^2(k, G_m) \xrightarrow{\text{Gal}(L/k)} \underline{H^2(L, G_m)}$$

||
I