Lecture 19

11/9

Central simple algebras.

Recall:

R/k 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.

$$R = M_n(k).$$

$$\begin{array}{c} n/2 \\ \\ n/2 \end{array} \left[\begin{array}{c|c} \begin{matrix} a & & \\ & a & \\ & & \ddots \; a \end{matrix} & \boxed{} \\ \hline & \begin{matrix} a & & \\ & \ddots & \\ & & a \end{matrix} \end{array}\right] \qquad \sim \frac{n^2}{4}.$$

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.

$$S \underset{\varphi_2}{\overset{\varphi_1}{\rightrightarrows}} R \quad (k\text{-alg maps})$$

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

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

Special case:

① $S = R$.

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

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

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

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

$\Longleftrightarrow$ any automorphism of R is <u>inner</u>.

② $L = S$ = a finite field extension of k.

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

<u>Pf</u>:

$$S \overset{\varphi_1}{\curvearrowright} R \curvearrowleft R$$

usual.

$\rightsquigarrow$ $\underset{\substack{\| \\ R'}}{R}$ is $S \otimes_k R^{op}$ - mod.

simple   c.s.a/k

simple k-alg. finite-dim'l.

<u>$S \otimes_k R^{op}$</u> has a unique simple mod <u>M</u>.

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

$[R : k] = a \cdot \dim_k M$.

Using $S \overset{\varphi_2}{\curvearrowright} \underset{\substack{\| \\ R''}}{R} \curvearrowleft R$ $\Rightarrow$ same conclusion

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

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

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

$$\begin{tikzcd} R' \arrow[r, "\sim"] \arrow[d, equal] & R'' \arrow[d, equal] \\ R \circlearrowleft R & R \circlearrowleft R \end{tikzcd}$$

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

$$\begin{tikzcd} R \arrow[r, "u\cdot"] \arrow[d, "\varphi_1(s)\cdot"'] \arrow[dr, phantom, "\circlearrowright"] & R \arrow[d, "\varphi_2(s)\cdot"] \\ R \arrow[r, "u\cdot"] & R \end{tikzcd}$$

$$
\begin{tikzcd}
1 \arrow[r] \arrow[d] & u \arrow[d] \\
\varphi_1(s) \arrow[r] & \boxed{u\varphi_1(s) = \varphi_2(s)u}.
\end{tikzcd}
$$

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

$$\forall s \in S.$$

∎

<u>Thm</u> (Wedderburn) Any finite division ring is a field.

<u>Pf</u>. D finite div. ring. $[D:k] = n^2$.

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

$\forall x \in D$.

$k[x] \subset D$.

$\underset{\text{finite field}}{\overset{\parallel}{}}$.

$k[x] \subset L =$ max. comm. subring.

$=$ field.

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

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

Noether-Skolem:

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

unique up to conjugation by $D^\times$

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

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

$G = D^\times$ gp of order $q^{n^2} - 1$.

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

$$i(\mathbb{F}_{q^n}^\times) = H$$

$H \subset G$. subgp.

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

$$g\underbrace{hHh^{-1}}_{H}g^{-1} = gHg^{-1}$$

$$|LHS| < |G/H| \cdot |H| = |G|$$

strict if $H \neq G$

$\because$ the gHg^{-1} all contain 1.

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

Reformulation:

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

<u>Ex</u> of k s.t. $Br(k) = 0$.

① k = alg. closed.

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

$\Rightarrow Br(K) = 0$.

similarly, $\mathbb{Q}_p \rightsquigarrow \mathbb{Q}_p^{unr}$

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

$$\mathrm{Br}(\mathbb{Q}_p^{unr}) = 0.$$

$$\mathrm{Br}(\widehat{\mathbb{Q}_p^{unr}}) = 0.$$

More generally.

K: discrete valuation field.

residue is alg. closed.

complete.

$$\Longrightarrow \mathrm{Br}(K) = 0.$$

(2). k = alg. closed.

K/k transcendence degree 1.
(f.g. extn).

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

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

(rational functions on alg curves/k).

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

$$K = k(t).$$

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 $R \otimes_k L \simeq M_n(L)$.

$$\left(\iff \quad \begin{array}{ccc} Br(k) & \longrightarrow & Br(L) \\ [R] & \longmapsto & \overset{\Downarrow}{0} \end{array} \right)$$

$R = M_m(D)$.

If L/k is a splitting field for D.

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

$$R \otimes_k L \simeq M_m(D \otimes_k L)$$

$$\simeq M_m(M_d(L)) \simeq M_{md}(L).$$

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

$$\underset{=}{D} \otimes_k \underset{=}{L} \circlearrowleft \mathbf{D}$$

$$(D \subset \mathbf{D} \supset L)$$

$$\varphi : D \otimes_k L \longrightarrow \mathrm{End}_L(D)$$

right mult.

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

$$M_n(L)$$

φ injective

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

$n = \dim_L D$.

Using $[L:k] = n$.

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

$$\Downarrow$$

$$D \otimes_k L = M_n(L).$$

∎

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

D/k c.d.a.

Then D has a separable (finite) splitting field.

Recall:
$$\begin{array}{c} L \\ \Big| \text{ finite.} \\ k \end{array}$$
separable $\iff$ 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.

<u>Pf of Thm</u>.

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

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

$$\simeq M_m(D').$$

c.d.a. $/k'$.

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

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

Induction on n.

<u>inductive step: find $x \in D \setminus k$</u>,

<u>s.t. $k[x]$ is separable over k</u>.

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.

so does $\boxed{D \otimes_k k'} \simeq M_m(D')$. $(m > 1)$.

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

use hypoth.

Suppose we can't find such x.

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

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

$x^{p^e} \notin k$. ✓

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

$$D \subset D \otimes_k \bar{k} \simeq M_n(\bar{k}).$$

$$x \otimes 1 \longrightarrow n \times n \text{ matrix } X.$$

$$X^{p^e} \in k I_n.$$

$\Longrightarrow$ all eigenvalues of X (in $\bar{k}$) are the same.

$p \mid n$

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

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

$\Longrightarrow \mathrm{Tr}(M_n(\bar{k})) = 0$. $\times$ $\blacksquare$

<u>Rk</u>. $k = \mathbb{F}_p((t))$. $\boxed{L = \mathbb{F}_{q^n}((t)).}$ $\circlearrowleft \sigma = \mathrm{Frob}$

$$D = L\langle x; \sigma\rangle / (x^n - t^a).$$

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

$n=p$.

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

$$H^2(k,\mathbb{G}_m).$$

L/k ~~sep~~. Galois.

$$H^p(\underline{L/k}, \underbrace{H^q(L,\mathbb{G}_m)}) \Rightarrow \underline{H^{p+q}(k,\mathbb{G}_m)}$$

$H^1(L,\mathbb{G}_m)=1$. $\quad H^2(k,\mathbb{G}_m) = 1$.

$$H^2(k,\mathbb{G}_m) \longrightarrow \underbrace{H^2(L,\mathbb{G}_m)}^{\boxed{\mathrm{Gal}(L/k)}}$$