Lecture 20

11/16

- Splitting fields
- Reduced norm and trace
- C_1 fields

D/k. c.d.a. (always assumed to be f.d./k)

$$\begin{array}{c} L \\ | \\ k \end{array} \text{ field extn}$$

L is a <u>splitting field</u> of D if

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

<u>Lemma</u>. $L \subset D$ max subfield

$\Rightarrow$ L is a splitting field of D.

$$\left([L:k] = [D:k]^{1/2} \right).$$

<u>Prop 1</u> D/k. c.d.a. $[D:k] = n^2$.

1) Any splitting field L of D satisfies

$$n \mid [L:k]$$

2). If L is splitting field of D, and $[L:k] = n$

then L can be k-linearly embedded in D.

Warning: L splits D. $\not\Longrightarrow$ $\exists\, L' \subset L$.
s.t. L' embeddable into D.

Prop 2 D/k f.d. c.d.a. TFAE

1) L is a splitting field of D;

2) $\exists$ R/k c.s.a, $R \sim D$.
(i.e., $R \simeq M_m(D)$).
s.t. L is isom to a max comm subalg of R.
(i.e., $\exists\, L \hookrightarrow R$, $[L:k] = [R:k]^{1/2}$)

Prop 2 $\Longrightarrow$ Prop 1.

Ⓡ L splits D.

$L \subset M_m(D)$.

$[L:k] = [M_m(D):k]^{1/2} = m \cdot n$

If $[L:k] = n$. $\Rightarrow m=1$. $\Rightarrow L \subset D$. $\blacksquare$

Proof of Prop 2

1) $\Longrightarrow$ 2) $D \underset{k}{\otimes} L \cong \mathrm{End}_L(V)$
($V = L$-v.s.)

R = centralizer of D inside $\mathrm{End}_k(V)$.

$\boxed{D \subset \mathrm{End}_k(V)} \supset R$.

$D \circlearrowright V$, $R = \mathrm{End}_D(V) \simeq M_m(D^{op})$

$\Rightarrow$ R/k c.s.a.

$L \subset R \sim D^{op}$

$L \subset R^{op} \sim D$.

$\dim_k V = [D:k]\cdot \dim_D V$

$= n^2 \cdot m$.

$[R:k] = (mn)^2$

$[L:k]$

$D \otimes_k L \simeq \mathrm{End}_L(V)$.

$$n^2 \cdot [L:k] = \frac{\dim_k \mathrm{End}_k(V)}{[L:k]} = \frac{(n^2 \cdot m)^2}{[L:k]}$$

$\dim_k \mathrm{End}_k(V) = (n^2 \cdot m)^2$

$\Rightarrow [L:k]^2 = m^2 n^2 = [R:k]$.

2) $\Rightarrow$ 1). $\underset{\text{max comm}}{L \subset R} \sim \mathbf{D}$.

$\quad = M_m(\mathbf{D})$.

$$M_m(D \otimes_k L) \simeq R \otimes_k L \simeq M_{mn}(L).$$

c.s.a./L $\qquad$ L is max. comm in R.

$\Downarrow$

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

$\blacksquare$

Last time. $\exists$ separable splitting field.

Slightly stronger: D/k c.d.a.

$\Rightarrow \exists$ sep. extn L/k

$L \subset D$.

and L splits D.

$\underline{\text{Pf}}$: Last time: $\exists\ x_1 \in D \setminus k$, x_1 is sep. over k.

$k_1 = k(x_1)$. — field.

$D_1 = Z_D(k_1)$. c.d.a. $/ k_1$.

$[D_1 : k_1] < [D : k]$.

Find $x_2 \in D_1 \setminus k_1$, x_2 sep. over k_1.

$k_2 = k_1(x_2)$ ....

get $L = k(x_1, x_2, \ldots)$ max subfield $\subset D$.

$\blacksquare$

Reduced trace and norm.

R/k $\overset{\text{f.d.}}{\text{c.s.a.}}$

$R = M_n(k)$. $\xrightarrow{tr} k$.

will introduce (general R/k c.s.a.)

$$tr_R : R \longrightarrow k$$

characterized by: L splitting field of R.

$$\begin{tikzcd} R \otimes_k L \arrow[r, phantom, "\simeq"] \arrow[d, "tr_R \otimes 1_L"'] & M_n(L) \arrow[d, "tr"] \\ L \arrow[r, equal] & L \end{tikzcd}$$

Attempt: $x \in R$. $\ell_x : R \longrightarrow R$
left mult.

$$Tr(\ell_x | R). \in k.$$

Apply to $R = \underline{\underline{M_n(k)}}$. above gives n (usual trace)

Similarly. will define

$$Nm : R \longrightarrow k.$$

analogue of $\det : M_n(k) \longrightarrow k$.

More generally,

$$tr, \quad \ldots\ldots, \quad \det.$$

$\downarrow$

coeff. of char poly. of $A \in M_n(k)$.
all have analogues for R/k c.s.a.

Reduced trace: L splitting field of R

$$\begin{array}{c} L \\ | \\ k \end{array} \nwarrow \text{finite Galois.} \qquad Gal(L/k) = \Gamma.$$

$$R \otimes_k L \simeq M_n(L) \xrightarrow{tr} L$$

need to show this trace function is equivariant under Γ-action.

$$\mathrm{Hom}_L(\underset{\substack{\circlearrowleft \\ \Gamma}}{R \otimes L}, \underset{\substack{\circlearrowleft \\ \Gamma}}{L})^{\Gamma\text{-equiv}} = \mathrm{Hom}_k(R, k).$$

What's the Γ-action on $M_n(L)$?

$$\gamma \cdot (A_{ij})$$

$$\gamma \cdot (\underset{\substack{\cap \\ L}}{c} A) = \underline{\gamma(c)}(\gamma \cdot A) \quad \checkmark$$

$A \in M_n(L)$.

Consider another action of γ on $M_n(L)$

$$g_\gamma(A) = \gamma \cdot (\gamma^{-1}(A_{ij}))$$

new action is L-linear.

$$g_\gamma(cA) = c\, g_\gamma(A). \qquad A \in M_n(L).$$

i.e., $g_\gamma : M_n(L) \longrightarrow M_n(L)$

is an L-linear automorphism of rings.

Skolem-Noether $\Longrightarrow$ g_γ = conjugation by some matrix $\in M_n(L)$.

$$\begin{tikzcd} M_n(L) \arrow[rr, "g_\gamma"] \arrow[dr, "tr"'] & \arrow[d, phantom, "\circlearrowright"] & M_n(L) \arrow[dl, "tr"] \\ & L & \end{tikzcd}$$

$$\Longrightarrow \quad \begin{tikzcd} M_n(L) \arrow[r, "\gamma^{-1}", "\text{entrywise}"'] \arrow[rr, bend left, "g_\gamma"] \arrow[d, "tr"'] \arrow[dr, phantom, "\circlearrowright"] & M_n(L) \arrow[r, "\gamma\cdot"] \arrow[d, "tr"] \arrow[dr, phantom, "?"] & M_n(L) \arrow[d, "tr"] \\ L \arrow[r, "\gamma^{-1}"] \arrow[rr, bend right, "id"'] & L \arrow[r, "\gamma"] & L \end{tikzcd}$$

$\Longrightarrow$? is comm. i.e., $tr: M_n(L) \longrightarrow L$ is γ-equiv. $\forall \gamma \in \Gamma$.

$\Longrightarrow$ $R \otimes_k L \simeq M_n(L) \xrightarrow{tr} L$ is Γ-eq.

hence restricts to

$tr_R: \quad R = (R \otimes_k L)^\Gamma \longrightarrow L^\Gamma = k$.

Similarly, $R \otimes L \simeq M_n(L) \xrightarrow{\det} L$ is Γ-eq.

take Γ-invts get

$Nm_R: \ R \longrightarrow k$.

Stronger: $\mathrm{tr}_R : R \longrightarrow k$ (k-linear)

$\mathrm{Nm}_R : R \longrightarrow k$ polynomial function of deg n

$[R:k] = n^2$.

i.e., choose any basis $r_1, \dots, r_{n^2}$ of R over k.

$x = x_1 r_1 + \cdots + x_{n^2} r_{n^2} \in R$

Then $\mathrm{Nm}_R(x) = P(x_1, \dots, x_{n^2})$

homog. poly of deg n, coeff $\in k$.

uniquely determined by: L splits R

$$P(y_1, \dots, y_{n^2}) = \det(\varphi(y))$$

$y_i \in L$. poly. in $y_1, \dots, y_{n^2}$

$$\varphi : R \otimes_k L \xrightarrow{\sim} M_n(L).$$

$$y = \sum y_i r_i \longmapsto \varphi(y).$$

Examples of fields with $\mathrm{Br}(k) = 0$.

$k = \mathbb{F}_q$. $\quad \bar{k}((t))$. $\quad \widehat{\mathbb{Q}_p^{ur}}$

$\bar{k}(t)$ and its finite extensions (Tsen–Lang)

all these k satisfies $\mathrm{Br}(k') = 0 \ \forall \ k'/k$ algebraic extn.

(Auslander)

(Rk: $\exists$ k, s.t. $Br(k) = 0$.

but $Br(k') \neq 0$ for some finite k'/k.

See:

Serre, Galois Cohomology.

Ex. II. 3. 1 (1).

k_0, not algebraically closed

but no abelian extn

($\bigcup$ solvable extns of $\mathbb{Q}$ $\subset \overline{\mathbb{Q}}$)

$\boxed{k = k_0((t))}$.

$Br(k) = H^2(Gal(\bar{k}/k), \bar{k}^\times)$.

$Gal(\bar{k}/k) \simeq Gal(\bar{k_0}/k_0) \times \hat{\mathbb{Z}}$.)

C_1-condition:

A field k is $\underline{C_1}$ if $F(x_1, \dots, x_n)$, homog. deg d coeff in k.

If $d < n$, then $F(x_1, \dots, x_n) = 0$ has a nonzero solution in k^n.

Thm. If k is C_1, then $Br(k') = 0$ for any alg. extn k'/k.

Pf: First show $Br(k) = 0$.

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

want $n = 1$,

Idea: if $n > 1$, try to find $0 \neq x \in D$. s.t. $Nm_D(x) = 0$.

$$\left(\begin{array}{l} Nm_D(xy) = Nm_D(x) \cdot Nm_D(y). \\ Nm_D(1) = 1. \\ \Rightarrow Nm_D(x) = 0 \Rightarrow x = 0. \end{array} \right).$$

$Nm_D : D \longrightarrow k$. is a polynomial

$P(x_1, x_2, \ldots, x_{n^2})$. homog. deg n.

$n^2 > n$.

k is C_1 $\Rightarrow$ $P(x_1, \ldots, x_{n^2}) = 0$ has a nonzero sol. in k.

$$\left. \begin{array}{l} \Rightarrow x = \sum x_i r_i \in D \setminus \{0\}. \\ Nm_D(x) = 0 \end{array} \right\} \times$$

Next: k'/k alg. extn.

k is C_1 $\Rightarrow$ k' is C_1.

Suffices to treat k'/k is finite extn.

$F(x_1, \ldots, x_n) \in k'[x_1, \ldots, x_n]$. deg d.

$n > d$.

$F(x_1, \ldots, x_n) = 0$

$\Longleftrightarrow Nm_{k'/k}\big(F(x_1, \ldots, x_n)\big) = 0.$

choose k-basis of k'. $\{r_i\}_{i=1}^N$ $\quad x_i = y_{i1} r_1 + \cdots + y_{iN} r_N$

y_{ij} new variables.

$\underline{\underline{Nm_{k'/k}}}\, F(x_1, \ldots, x_n) = P(y_{ij}) \in k[y_{ij}]$

$n \cdot \underline{N}$ variables

$d \underline{N}$

$\Rightarrow$ nonzero sol. $(y_{ij}) \in k^{nN}$.

$\Rightarrow$ nonzero sol. $(x_i) \in \cancel{k}.(k')^n$.