Last time:

K finite field ext. of $\mathbb{Q}$ (a "number field")

$\mathcal{O}_K$ = integral closure of $\mathbb{Z}$ in K

$= \{x \in K \mid \text{min. poly of } x \text{ has coeff. in } \mathbb{Z}\}$

Example: $K = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}$ squarefree

⚠ $\Rightarrow \mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega_D$, $\omega_D = \begin{cases} \frac{1+\sqrt{D}}{2}, & D \equiv 1 \ (4) \\ \sqrt{D}, & D \equiv 2,3 \ (4) \end{cases}$

1.2. Traces and norms

K arbitrary field

Definition: L/K finite field ext, $x \in L$

Set $\varphi_x : L \to L, a \mapsto xa$ K-lin. endo.

of the K-v.s. L, i.e. $\varphi_x \in \mathrm{End}_K(L)$

Set $\mathrm{Tr}_{L/K}(x) := \mathrm{tr}(\varphi_x) \in K$

trace of x (relative to L/K)

$N_{L/K}(x) := \det(\varphi_x) \in K$ norm of x

(relative to L/K)

Note: $\mathrm{Tr}_{L/K} : L \to K$ K-linear, $N_{L/K} : L \to K$ multiplicativ

Lemma: L/M, M/K finite field ext., $x \in L$

1) $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}(x))$, $N_{L/K}(x) = N_{M/K}(N_{L/K}(x))$

2) If $x \in K$, then $\mathrm{Tr}_{L/K}(x) = [L:K] \cdot x$

$$N_{L/K}(x) = x^{[L:K]}$$

3) If $f(T) = T^n + a_1 T^{n-1} + \ldots + a_n \in K[T]$ min. poly of x over K, then

$$\mathrm{Tr}_{K(x)/K}(x) = -a_1 \quad , \quad N_{K(x)/K}(x) = (-1)^n \cdot a_n .$$

More generally, set $L = K(x)$, then

$$a_i = (-1)^i \,\mathrm{Tr}(\Lambda^i \varphi_x)$$

$$\Lambda^i \varphi_x : \Lambda^i_K L \to \Lambda^i_K L$$

Proof: Exercise $\square$

Proposition: L/K finite, sep. ext., $n = [L:K]$, Ω alg. cld. field, $\tau : K \hookrightarrow \Omega$ an embedding

1) there exist exactly n distinct embeddings $\sigma_1, \ldots, \sigma_n : L \hookrightarrow \Omega$ such that $\sigma_{i|K} = \tau$ for $1 \le i \le n$, i.e. $\#\mathrm{Hom}_{K\text{-alg}}(L, \Omega) = n$

2) $\sigma_1, \dots, \sigma_n$ are linearly independent over Ω in Ω-v.s. $\mathrm{Maps}(L, \Omega)$

Proof: 1) Via induction on n, reduce to $L = K(x)$ $(*)$

for some $x \in L$

Set $f(T) \in K[T]$ min. poly. of x over K:

Then $L \simeq K[T]/(f(T))$ and
$x \leftarrow T$

$$\mathrm{Hom}_{K\text{-alg}}(L, \Omega) \xleftrightarrow{1:1} \{\alpha \in \Omega \mid f(\alpha) = 0\}$$
$$\sigma \longmapsto \sigma(x)$$

f sep. of deg n $\Rightarrow$ f has n distinct roots in Ω

(Details on $(*)$: $x \in L \setminus K$, if $L = K(x)$ ✓,
if $L \neq K(x)$, then

extend γ to $\gamma_1, \dots, \gamma_{[K(x):K]} : K(x) \to \Omega$,

then extend $\gamma_i : L \to \Omega$ (by induction as $[L:K(x)] < [L:K]$)

Use $[L:K] = [L:K(x)] \cdot [K(x):K]$)

2) $n = 1$ ✓ Thus, assume $n \geq 2$ and that $\sigma_1, \dots, \sigma_n$ are lin. dep.

Pick a relation $\sum_{i=1}^{d} c_i \sigma_i = 0$, $c_i \in \Omega$ with d minimal

Choose $y \in L$, s.t. $\sigma_1(y) \neq \sigma_2(y)$ (recall $\sigma_1 \neq \sigma_2$)

$$\Rightarrow 0 = \sum_{i=1}^{d} c_i \sigma_i(x \cdot y) = \sum_{i=1}^{d} c_i \sigma_i(x) \cdot \sigma_i(y) \quad \forall x \in L$$

$$\Rightarrow 0 = \sum_{i=1}^{d} c_i (\sigma_i(y) - \sigma_1(y)) \cdot \sigma_i(x)$$

$$= \sum_{i=2}^{d} c_i (\sigma_i(y) - \sigma_1(y)) \cdot \sigma_i(x), \text{ i.e.}$$

we obtained a shorter relation $\lightning$ $\square$

Theorem: L/K fin. sep. ext of fields, Ω alg. cld $K \subseteq \Omega$, $n = [L:K]$, $\mathrm{Hom}_{K\text{-alg}}(L, \Omega) = \{\sigma_1, \dots, \sigma_n\}$

$\Rightarrow$ 1) $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$, $N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$

for all $x \in L$

⚠ 2) The K-bilinear form

$L \times L \to K$, $(x, y) \mapsto \mathrm{Tr}_{L/K}(x \cdot y)$

is non-deg, i.e if $x \in L$, s.t. $\mathrm{Tr}_{L/K}(x \cdot y) = 0$ for all $y \in L$, then $x = 0$

Proof: 1) Reduce to case $L = K(x)$
(either using induction on n, or existance of prim. elt.)

Let $f(T) = T^n + a_1 T^{n-1} + \ldots + a_n = \prod_{i=1}^{n} (T - x_i)$

min. poly of x

Then $\sigma_i(x) = x_i$

$\Rightarrow$ Apply prev. exercise $\Rightarrow \mathrm{Tr}_{L/K}(x) = -a_1 = \sum_{i=1}^{n} \sigma_i(x)$

2) Write

$$\mathrm{Tr}_{L/K}(x \cdot y) \overset{1)}{=} \sum_{i=1}^{n} \sigma_i(x \cdot y) = \sum_{i=1}^{n} \sigma_i(x) \cdot \sigma_i(y) \quad \forall y \in L$$

$\underset{\text{prev. prop.}}{\Rightarrow} \quad \sigma_i(x) = 0 \quad \forall i = 1, \ldots, n \Rightarrow x = 0$ $\square$

Remark: 1) K a field, A a fin. dim. comm. K-alg.

Then $A \simeq \prod_{i=1}^{n} L_i$ with L_i/K fin. sep. field ext.

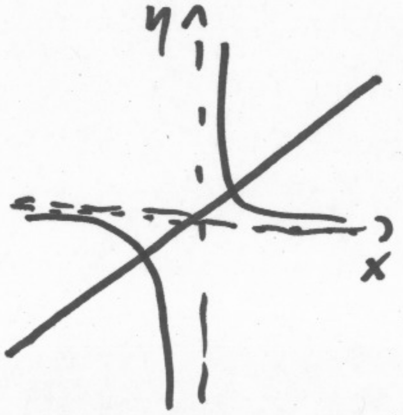
iff trace bilinear

$$A \times A \to K, \ (x, y) \mapsto \mathrm{Tr}_{A/K}(x \cdot y)$$

is non-degenerate

2) $K = \mathbb{F}_p(T)$, $L = \mathbb{F}_p(T^{\frac{1}{p}})$. Then $\mathrm{Tr}_{L/K}(x) = 0$ for $x \in L$, i.e.
p prime

second part of thm fails for insep. ext.



$$\begin{array}{ccc} k[x,y]/_{x\cdot y-1} & x & x+y \text{ integral} \\ \uparrow \sigma_1 & \uparrow & \nwarrow \\ k[x] \ni & x & \sigma_2 \quad k[x] \end{array}$$

$$\begin{array}{c} L \\ \tau \,|\, \text{trdeg } 1 \\ K \end{array}$$

Assume trdeg $K/_{\mathbb{Q}}$ infinite

$\Rightarrow \bar{K}, \bar{L}$ are isom. as they have same trdeg $/_{\mathbb{Q}}$

Pick isom. $\bar{K} \overset{\sigma_2}{\cong} \bar{L}$

$\sigma_1 : \bar{K} \hookrightarrow \bar{L}$ ext. of τ.
trdeg 1

Corollary: $L/_K$ fin. sep. field ext., $n = [L:K]$, $\alpha_1, \dots, \alpha_n \in L$. Then $\alpha_1, \dots, \alpha_n$ are a K-basis of $L \Leftrightarrow \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)) \neq 0$

Proof: Consider

$$K^n \xrightarrow{\varphi} L \xrightarrow{\psi} K^n$$

$$(x_1,\dots,x_n) \mapsto \sum_{i=1}^{n} x_i \alpha_i$$

$$x \mapsto \left(\mathrm{Tr}_{L/K}(x \cdot \alpha_i)\right)_{1 \leq i \leq n}$$

Note $\psi \circ \varphi$ is mult. by matrix $\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{i,j}$

"$\Rightarrow$" φ iso, and ψ inj.

$\Rightarrow \psi \circ \varphi$ inj. $\Rightarrow \psi \circ \varphi$ iso.

"$\Leftarrow$" $\psi \circ \varphi$ iso

$\Rightarrow \varphi$ inj. $\Rightarrow \alpha_1,\dots,\alpha_n$ basis ∎

Notation: $\alpha_1,\dots,\alpha_n \in L$ basis

$\Rightarrow \alpha_1^\vee,\dots,\alpha_n^\vee \in L$ dual basis w.r.t.

$\mathrm{Tr}_{L/K}(\cdot)$, i.e.

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_j^\vee) = \begin{cases} 1 & , i=j \\ 0 & , \text{otherwise.} \end{cases}$$

1.3. Discriminants and integral basis

K number field, $n=[K:\mathbb{Q}]$, $\mathcal{O}_K \subseteq K$ ring of integers

If $\alpha_1,\dots,\alpha_n \in K$, then

$$\mathrm{Disc}(\alpha_1,\dots,\alpha_n) := \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)\right)$$

the discriminant of $\alpha_1,\dots,\alpha_n$

Lemma: 1) $\alpha_1, \dots, \alpha_n \in K$ basis over $\mathbb{Q}$

$\iff \operatorname{Disc}(\alpha_1, \dots, \alpha_n) \neq 0$

2) Let $\operatorname{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$, then

$$\operatorname{Disc}(\alpha_1, \dots, \alpha_n) = \left(\det\left((\sigma_i(\alpha_j))_{i,j}\right)\right)^2$$

3) If $C \in \operatorname{Mat}_{n\times n}(\mathbb{Q})$, $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n) \cdot C$,

i.e. $\beta_i = \sum c_{ji} \alpha_j$, then

$$\operatorname{Disc}(\beta_1, \dots, \beta_n) = \operatorname{Disc}(\alpha_1, \dots, \alpha_n) \cdot \det(C)^2$$

Proof: 1) ✓

2) Prev. thm

$$\Rightarrow \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i) \cdot \sigma_k(\alpha_j)$$

Set $U := (\sigma_i(\alpha_j))_{i,j} \Rightarrow \left(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)\right)_{i,j} = U^{tr} \cdot U$

$\Rightarrow$ take det

3) $U \cdot C = (\sigma_i(\beta_j))_{i,j} \Rightarrow$ 3) follows from 2) $\square$

Proposition: $\alpha \in K$, $f \in \mathbb{Q}[T]$ its min. poly.

$$\Rightarrow \operatorname{Disc}(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$$

$$= \begin{cases} 0 & \text{if } \deg f < n \\ (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)), & \text{if } \deg f = n \end{cases}$$

Proof: ✓ if $\deg f < n$

Thus, assume $\deg f = n$, i.e. $K = \mathbb{Q}(\alpha)$.

Let $\{\sigma_1, \dots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{C})$

$\Rightarrow$ $\mathrm{Disc}(1, \alpha, \dots, \alpha^{n-1}) = \det(\sigma_i(\alpha^{j-1}))^2$

$$= \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

Vandermonde determinant

On the other hand,

$$N_{K/\mathbb{Q}}(f'(\alpha)) = \prod_{i=1}^{n} \sigma_i(f'(\alpha))$$

$$= \prod_{i=1}^{n} \prod_{j \neq i} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

$$f(T) = \prod_{i=1}^{n} (T - \sigma_i(\alpha))$$

$$\Rightarrow f'(T) = \sum_{j=1}^{n} \prod_{k \neq j} (T - \sigma_k(\alpha))$$

□

Theorem: $\mathcal{O}_K$ is a free abelian group of rk n

⚠ Proof: Pick basis $\alpha_1, \dots, \alpha_n \in K$ over $\mathbb{Q}$. Wlog $\alpha_i \in \mathcal{O}_K$, $i = 1, \dots, n$ (mult. with some integer)

Set $M := \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Z}} \subseteq \mathcal{O}_K$

Let $\alpha_1^\vee, \ldots, \alpha_n^\vee$ be the dual basis, $M^\vee = \langle \alpha_1^\vee, \ldots, \alpha_n^\vee \rangle_{\mathbb{Z}}$

Recall $\quad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^\vee \cdot \alpha_j) = \begin{cases} 1 & , i = j \\ 0 & , \text{otherwise} \end{cases}$

Claim: $M^\vee = \{ x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(x \cdot y) \in \mathbb{Z} \text{ for all } y \in M \}$

"$\subseteq$" ✓

"$\supseteq$" Write $x = \sum x_i \alpha_i^\vee$, $x_i \in \mathbb{Q}$

$\Rightarrow x_i = \mathrm{Tr}_{K/\mathbb{Q}}(x \cdot \alpha_i) \in \mathbb{Z}$ $\qquad \square_{\text{claim}}$

Claim $\Rightarrow$ $\mathcal{O}_K \subseteq M^\vee$, i.e. $M \subseteq \mathcal{O}_K \subseteq M^\vee$

free $\mathbb{Z}$-modules of rank n $\qquad \square$

Def: A basis $\alpha_1, \ldots, \alpha_n$ of K over $\mathbb{Q}$ is called an integral basis if $\alpha_1, \ldots, \alpha_n$ are a basis of $\mathcal{O}_K$ over $\mathbb{Z}$.

Prop: $\alpha_1, \ldots, \alpha_n \in K$ integral basis, $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$

$\Rightarrow$ 1) $\mathrm{Disc}(\beta_1, \ldots, \beta_n) = \mathrm{Disc}(\alpha_1, \ldots, \alpha_n) \cdot c^2$ for some $c \in \mathbb{Z}$

2) $\beta_1, \dots, \beta_n$ integral basis $\Leftrightarrow$
$\mathrm{Disc}(\beta_1, \dots, \beta_n) = \mathrm{Disc}(\alpha_1, \dots, \alpha_n)$

Proof: Prev. lemma

Definition: The discriminat $\Delta_K \in \mathbb{Z}$ of K is the discriminant of an integral basis.

Example: $n = 2$, $K = \mathbb{Q}(\sqrt{D})$, D squarefree

$$\Rightarrow \mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega_D, \quad \omega_D = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \ (4) \\ \sqrt{D}, & \text{if } D \equiv 2,3 \ (4) \end{cases}$$

$$\mathrm{Disc}(1, \omega_D) = -N_{K/\mathbb{Q}}(f'(\omega_D)), \quad f(T) = \begin{cases} T^2 - T + \frac{1-D}{4} \\ T^2 - D \end{cases}$$

$$= \begin{cases} -N_{K/\mathbb{Q}}(\overbrace{2\omega_D - 1}^{\sqrt{D}}) \\ -N_{K/\mathbb{Q}}(2 \cdot \omega_D) \end{cases} = \begin{cases} D \\ 4 \cdot D \end{cases}$$

Note: $K = \mathbb{Q}(\sqrt{\Delta_K})$ if $[K:\mathbb{Q}] = 2$