Lecture 4: Note: Office hours Thursday 2-4.

Last time: $\alpha_1, \dots, \alpha_n$ in L/K, $n = [L:K]$.

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(\operatorname{Tr}(\alpha_i \alpha_j)) = (\det \sigma_i(\alpha_j))^2$$

Today: Thm: K a number field.

$$(\mathcal{O}_K, +) \cong \mathbb{Z}^n \text{ where } n = [K:\mathbb{Q}]$$

Discriminant: $\Delta_K = \operatorname{disc}(\text{integral basis for } \mathcal{O}_K)$.

Lemma: L/K, char 0. For $\alpha_1, \dots, \alpha_n \in L$, $n = [L:K]$

$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = 0 \iff \alpha_i$ are linearly dependent (as elts of the K-vector space L).

(separable = really separable)

Proof: ($\Leftarrow$) If $\sum a_i \alpha_i = 0$ for $a_i \in K$, then the cols of $(\sigma_i(\alpha_j))$ sat the same relation

$\Rightarrow \operatorname{disc} = 0$.

($\Rightarrow$) $\operatorname{disc} = \det(\operatorname{Tr}(\alpha_i \alpha_j)) = 0$

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \ddots & \vdots \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

G = matrix of bilinear form w.r.t $\mathcal{B}$.

Suppose $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ is a basis for L.

For $\beta, \gamma \in L$, we have $(\beta, \gamma) = \operatorname{tr}(\beta\gamma) = (\beta)_{\mathcal{B}}^{t} \, G \, (\gamma)_{\mathcal{B}}$

($(\gamma)_{\mathcal{B}}$: column vector of γ w.r.t. $\mathcal{B}$)

Since $\det G = 0$, there is a $\gamma \neq 0$ in L that $G(\gamma)_{\mathcal{B}} = \vec{0}$ and hence $\operatorname{tr}(\beta\gamma) = 0$ for all $\beta \in L$. But $\operatorname{tr}(\frac{1}{\gamma}\gamma) = \operatorname{tr}(1) = n$, a contradiction ▨

Thm: $(\mathcal{O}_K, +) \cong \mathbb{Z}^n$ where $n = [K : \mathbb{Q}]$

Pf: Let $\alpha_1, \dots, \alpha_n$ be algebraic integers forming a $\mathbb{Q}$-basis for K. Let $A = \{\sum a_i \alpha_i \mid a_i \in \mathbb{Z}\}$

Claim: $A \leq \mathcal{O}_K \leq \frac{1}{d} A$ where $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$ ← not 0 by lemma.

[implies thm as $(A, +) \cong (\frac{1}{d}A, +) \cong \mathbb{Z}^n$]

Given $\alpha \in \mathcal{O}_K$ can write $\alpha = \sum a_i \alpha_i$, $a_i \in \mathbb{Q}$.

The a_i solve the system

$$G \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \operatorname{tr}(\alpha \alpha_1) \\ \vdots \\ \operatorname{tr}(\alpha \alpha_n) \end{pmatrix} = \vec{b}$$

all entries in $\mathbb{Z}$.

$\Rightarrow a_i \in \frac{1}{\det G}\mathbb{Z}$ by Cramer's Rule. $\left[a_i = \frac{\det G \text{ with } i^{\text{th}} \text{ col replaced by } \vec{b}}{\det G}\right]$ ▨

Ex: $K = \mathbb{Q}(\zeta)$, ζ a p^{th} root of unity, p prime.

Fact: $1, \zeta, \dots, \zeta^{p-1}$ is a int. basis for $\mathcal{O}_{\mathbb{Q}(\zeta)}$

$$\Delta_K = \operatorname{disc}(1, \zeta, \dots, \zeta^{p-1}) = \pm p^{p-2}$$

↑ + if $p \equiv 1 \bmod 4$.

as follows.

Prop: Suppose $L = K(\alpha)$ is separable. Let $\alpha_1, \dots, \alpha_n$ be the conj of α. Then

$$\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \le i < j < n} (\alpha_i - \alpha_j)^2$$

$$= \pm N_{L/K}(f'(\alpha))$$

$+$ if $n \equiv 0, 1 \bmod 4$

where f is the min poly of α.

Proof: Compute via the Vandermonde matrix $\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & & & & \vdots \end{pmatrix}$

$$N_{L/K}(f'(\alpha)) = \prod_i f'(\alpha_i) = \prod_i \prod_{j \neq i} (\alpha_i - \alpha_j) = \cdots$$

as $f(x) = \prod (x - \alpha_j)$. ∎

Returning to $\mathbb{Q}(\zeta)$:

$\leftarrow$ min poly of $\zeta = x^{p-1} + x^{p-2} + \cdots + 1$

Then $x^p - 1 = (x-1) f(x) \Rightarrow p x^{p-1} = f(x) + (x-1) f'(x)$

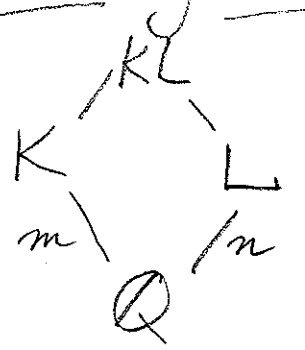
$$\Rightarrow f'(\zeta) = \frac{p \zeta^{p-1}}{\zeta - 1} \Rightarrow N(f'(\zeta)) = \frac{p^{p-1} \cdot 1}{p} = p^{p-2}$$

$$\operatorname{disc}(1, \zeta, \zeta^2, \dots, \zeta^{p-1}) = \pm p^{p-2}$$

$+$ when $p \equiv 1 \bmod 4$

from $\dfrac{x^p - 1}{x - 1} = (x - \zeta) \cdots (x - \zeta^{p-1})$

Combining Fields: $\mathcal{O}_{KL} \supseteq \mathcal{O}_K \mathcal{O}_L$



Thm: If $[KL:\mathbb{Q}] = mn$ then $\mathcal{O}_{KL} = \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$ where $d = \gcd(\Delta_K, \Delta_L)$.

When $d=1$, $\Delta_{KL} = \Delta_K^n \Delta_L^m$.

Pf: See text.

If time remains, discuss $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ as lead-in to Friday's class.