Different and discriminant (part 2)

From now on, I will try to start the post-lecture office hours as soon as possible after I end the lecture, rather than waiting until 11:00. They will still run until 11:30 as scheduled.

Reminder: different of a field extension

L/K be an extension of number fields

inverse different of L/K = fractional ideal $\{x \in L : \mathrm{Tr}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\}$

different $\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$ = inverse of this fractional ideal

(trace pairing defines an isomorphism $L \to \mathrm{Hom}_K(L,K)$
but not $\mathcal{O}_L \longrightarrow \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$)

~~Pf~~ if $\mathcal{O}_L = \mathcal{O}_K(\alpha)/(P(\alpha))$ ⟵ P monic polynomial

then $\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} = (P'(\alpha))$.

Reminder: different vs discriminant

$\mathcal{D}_{O_L/O_K}$ is an ideal of O_L

Disc_{O_L/O_K} is an ideal of O_K.

$\mathrm{Norm}_{M/K} = \mathrm{Norm}_{L/K} \circ \mathrm{Norm}_{M/L}$

Prop $\mathrm{Disc}_{O_L/O_K} = \mathrm{Norm}_{L/K}\, \mathcal{D}_{O_L/O_K}$

Cor Say $M/L/K$ tower number fields

then $\mathcal{D}_{O_M/O_K} = \mathcal{D}_{O_M/O_L}\, \mathcal{D}_{O_L/O_K}$

$\downarrow \mathrm{Norm}_{M/K}$

$\Rightarrow \mathrm{Disc}_{O_M/O_K} = \mathrm{Disc}_{O_L/O_K}^{[M:L]}\, \mathrm{Norm}_{L/K}\left(\mathrm{Disc}_{O_M/O_L}\right)$

Étale algebras

Let K be a field

An étale algebra over K is a ring which is a finite direct sum of finite separable field extensions of K.

e.g. $\mathbb{Q}(i) \oplus \mathbb{Q}(\zeta_3) \oplus \mathbb{Q}$ is an étale algebra over $\mathbb{Q}$ of degree $2+2+1=5$.

e.g. over $\mathbb{R}$, an étale algebra is a direct sum of copies of $\mathbb{R}$ and $\mathbb{C}$.

For K a # field, (or étale algebra over $\mathbb{Q}$)

$K \hookrightarrow K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$

$K_{\mathbb{R}}$ = Frob-invariants of $K_{\mathbb{C}}$ $= \oplus \mathbb{R} \oplus \mathbb{C}$

$K_{\mathbb{C}} = \bigoplus_{\tau} \mathbb{C}$

note:

$K_{\mathbb{R}} \cong K \otimes_{\mathbb{Q}} \mathbb{R}$

$K_{\mathbb{C}} \cong K \otimes_{\mathbb{Q}} \mathbb{C}$

Etale algebras and the trace pairing

For R an étale algebra over K,

define trace pairing $R \times R \to K$,

$\langle x, y \rangle = \mathrm{Trace}_{R/K}(xy)$.

This is a nondegenerate & perfect pairing:

$$R \longrightarrow \mathrm{Hom}_K(R, K) \qquad x \longmapsto (y \mapsto \langle x, y \rangle)$$

is an isomorphism.

Reduction modulo a prime

Let L/K be a finite separable extension,
$\mathcal{O}_K$ = Dedekind domain with function field K,
$\mathcal{O}_L$ = integral closure of $\mathcal{O}_K$ in L.

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime, factor

with all $\underline{e = 1}$

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r$$

(and $\mathcal{O}_L/\mathfrak{q}_i$ is separable over $\mathcal{O}_K/\mathfrak{p}$)

Then: $\prod_i \mathcal{O}_L/\mathfrak{q}_i \overset{\text{CRT}}{\cong} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is étale algebra over $\mathcal{O}_K/\mathfrak{p}$ $\Rightarrow$ trace pairing on $\mathcal{O}_L$ is perfect mod $\mathfrak{p}$!

Ramification, different, and discriminant

Thm let L/K be a extension of \# fields. $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime.

Then $\mathfrak{p}$ is ramified in $L \iff \mathfrak{p} \mid \mathrm{Disc}\, \mathcal{O}_L/\mathcal{O}_K$

$\iff \mathfrak{p}$ not coprime to $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$

We already know: if $\mathfrak{p}$ is ramified then $\mathfrak{p} \mid \mathrm{Disc}\, \mathcal{O}_L/\mathcal{O}_K$.

Need: if $\mathfrak{p}$ is unramified then $\mathfrak{p} \nmid \mathrm{Disc}\, \mathcal{O}_L/\mathcal{O}_K$

or $\mathfrak{p}$ coprime to $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$

Ramification, different, and discriminant

If $\mathfrak{p}$ is unramified then $\mathfrak{p}\mathcal{O}_L = \underbrace{\mathfrak{q}_1 \cdots \mathfrak{q}_r}_{\text{primes}}$

and $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \bigoplus_i \mathcal{O}_L/\mathfrak{q}_i$ is an étale algebra over $\mathcal{O}_K/\mathfrak{p}$

so Trace pairing mod $\mathfrak{p}$ perfect, that is,

$\mathcal{O}_L \to \operatorname{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$ becomes an isomorphism mod $\mathfrak{p}$

$\Rightarrow$ $\mathfrak{p}$ coprime to $\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$.

($\mathcal{O}_L$, choose a basis of L/K of elements of $\mathcal{O}_L$ which reduce mod $\mathfrak{p}$ to a basis of $\bigoplus_i \mathcal{O}_L/\mathfrak{q}_i$, Disc of this basis not divisible by $\mathfrak{p}$)

Preview: more on ramification and the different

Theorem (not proved yet) Let L/K be an extension of # fields

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime, let $\mathfrak{q}$ of L lying over $\mathfrak{p}$.

- $e(\mathfrak{q}/\mathfrak{p}) = 1$ iff $v_{\mathfrak{q}}(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}) = 0$.

- $v_{\mathfrak{q}}(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}) \geq e(\mathfrak{q}/\mathfrak{p}) - 1$ "usually" $=$

$\leq e(\mathfrak{q}/\mathfrak{p}) - 1 + v_{\mathfrak{q}}(e(\mathfrak{q}/\mathfrak{p}))$ "wild"

$e(\mathfrak{q}/\mathfrak{p}) \leq n = [L:K]$

Cor Can bound $v_{\mathfrak{q}}(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K})$ as a function of p, n

from above

The Hermite-Minkowski theorem

Fix $n \geq 1$

Thm (Hermite-Minkowski)

Let K = # field, let S = finite set of (nonzero) primes of O_K.

Then there are finitely many number fields L/K of (relative) degree n which are unramified outside S.

e.g. quadratic extensions of $\mathbb{Q}$

The Hermite-Minkowski theorem

$L - K - \mathbb{Q}$

WLOG assume $K = \mathbb{Q}$

Combine:

- bounding S also gives a bound on $(\mathrm{Disc}\, L/\mathbb{Q})$
- there are only finitely many $L/\mathbb{Q}$ of fixed degree and fixed discriminant.

(geometry of numbers)

Choose "small" element of $\mathcal{O}_L \subset L_\mathbb{R}$ primitive

$\rightarrow$ L defined by a "small" polynomial