Math 538, Lecture 13, 28/2/2024

Last time: Ramification

K complete wrt non-triv, non-arch abs value
k perfect, $|\cdot|$ discrete

Prop: L/K finite totally ramified iff $L = K(\pi)$ where π uniformiser; min poly is Eisenstein
any

Thm: $\mathbb{Q}_p$ has finitely many extensions of any fixed degree.

Today: Implications for number fields

Lemma: let L/K be an extension of fields, $|\cdot|_w$ an absolute value on L, trivial on K. Then $|\cdot|_w$ is trivial on the algebraic closure of K in L

Pf: $|\cdot|$ is non-arch. let $\alpha \in L$ with $|\alpha|_w > 1$
let $f \in K[x]$ be its min poly (assume α alg. $/K$)

$$f(x) = \sum_{i=0}^{d-1} a_i x^i + x^d.$$

$$|a_i \alpha^i|_w = |\alpha|_w^i < |\alpha|_w^d \quad \text{if } i<d.$$

$$\Rightarrow \quad |f(\alpha)|_w = |\alpha|_w^d \neq 0 \quad \text{contradiction} \quad \boxtimes$$

Fix a finite extension L/K of fields, v place of K ($|\cdot|_v$ is an absolute value)

Goal: Extend v to L

Can do this: say L gen by roots of some f. Then splitting field of f over K_v will contain a copy of L, so v extends to L.

<u>Lemma:</u> There is a bijection between

$$\{w \in |L| : w | v\} \leftrightarrow \mathrm{Hom}(L; \overline{K_v}) / \mathrm{Gal}(\overline{K_v}/K_v)$$

<u>Pf:</u> v extends uniquely to $\overline{K_v}$, so extension is $\mathrm{Gal}(\overline{K_v})$-inv't. Get map

$$\mathrm{Hom}(L; \overline{K_v}) / \mathrm{Gal}(\overline{K_v}/K_v) \to \{w : w|v\}$$

St is surjective, if $w|v$. (L_w is a finite extension of K_v) $L\cdot K_w \subset L_w$ is a f.d. K_v-vsp

$\Rightarrow$ closed in L_w, contains L, so $L_w = L\cdot K_v$

so L_w finite over K_v so algebraic

$\Rightarrow$ have embedding $L_w \hookrightarrow \overline{K_v}$

compatible with absolute values by uniqueness

For injectivity, suppose $L, L' \subset \overline{K_v}$ subfields finite $/K$, $\sigma : L \to L'$ isometric K-isom. Need to show σ extends to an aut. of $\overline{K_v}$.

First, σ extends to the topological closures of L, L' (finite extensions of K_v). These a fields, the extension is a K_v-isom. Done by Galois theory.

<u>Remarks</u> we implicitely assumed $\overline{K_v}/K_v$ is Galois. Check what happens otherwise

<u>Cor</u>: Suppose $L = K(\alpha)$ with min poly $f \in K[x]$. Then places of L above v are in bijection with irred factors of f in $K_v[x]$

(Recall: if $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ saw primes of $\mathcal{O}_L$ above $\mathfrak{p} \triangleleft \mathcal{O}_K$ are bijection with factors of f in $\mathcal{O}_K/\mathfrak{p}[x]$)

$\Rightarrow$ Get new proof of this fact, works even if $\mathfrak{p}$ is ramified in L/K.

Examples: (1) L/K # fields, $v \in |K|_\infty$.

If $K_v \cong \mathbb{C}$ then $L_w \cong \mathbb{C}$ for all $w|v$

if $L = K(\alpha)$, α has n embeddings to $\mathbb{C}$, $n = [L:K]$. Get n places, all complex, lying over v.

If $K_v \cong \mathbb{R}$ then f factors in $\mathbb{R}[x]$ into r linear, s quadratic factors $n = r + 2s$

Get r real places, s complex places, of L lying over v.

In particular if $K = \mathbb{Q}$, see that L has r real, s complex places where $r + 2s = n = [L:\mathbb{Q}]$

($\mathrm{Aut}_{cts}(\mathbb{C}) = \{1, c\}$ acts on embedding $L \hookrightarrow \mathbb{C}$, orbits are of size 1, 2)

(2) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, min poly $x^3 - 2$.

· Over $\mathbb{Q}_\infty \simeq \mathbb{R}$, $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$
so have one real place, one complex place

$(\dim_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C}) = 3 = [L : \mathbb{Q}])$

· Over $\mathbb{Q}_2$ $x^3 - 2$ is Eisenstein hence irred
($\Rightarrow$ irred in $\mathbb{Q}[x]$) get unique place $w_2 | 2$,
extension is totally (but tamely) ramified

· Over $\mathbb{Q}_3$ $x^3 - 2 \equiv x^3 + 1 \equiv (x+1)^3 \equiv (x-2)^3$

$f(2) = 6 = 3 \cdot 2$, $f'(2) = 3 \cdot 2^2$ so $\left| \frac{f(2)}{(f'(2))^2} \right|_3 \geq 1$

Hensel's lemma does not apply. In fact
$f(2) = 6$, $f(5) = 123 \equiv 6$ (9), $f(-1) \equiv -3 \equiv 6$ (9)

f has no root mod 9, hence in $\mathbb{Z}_3$, hence
in $\mathbb{Q}_3$, so f is irred in $\mathbb{Q}_3$.

Let $g(y) = f(y-1) = y^3 - 3y^2 + 3y - 3$
(min poly of $1+\sqrt[3]{2}$). Also Eisenstein, so irred
only one place over 3, which is totally ramified,
$1+\sqrt[3]{2}$ is a uniformiser.

$N^{L}_{\mathbb{Q}}(1+\sqrt[3]{2}) = 3$ so $(1+\sqrt[3]{2})$ is the prime ideal$/3$

· Over $\mathbb{Q}_5$; mod 5, $f \equiv (x-3)(x^2+3x+4)$
2nd factor is irred $f'(3) = 27 \equiv 2 \ (5)$
so by Hensel's Lemma, $f = f_1 f_2$ in $\mathbb{Q}_5[x]$
with f_1 of deg 1, f_2 deg 2 irred

$\Rightarrow$ two places over 5, one completion $\cong \mathbb{Q}_5$
other completion L_w is a quad extension of $\mathbb{Q}_5$,
the unramified extension since $\bar{f}_2$ is irred.

· Over $\mathbb{Q}_p$, $p \geq 5$, $\bar{f}' = 3x^2$ rel prime to $\bar{f}$
so any root of $\bar{f}$ mod p lifts to $\mathbb{Z}_p$, if $\bar{f} = \prod_i \bar{f}_i$
this lifts to $f = \prod_i f_i$

$\Rightarrow$ places of $\mathbb{Q}(\sqrt[3]{2})$ over p corresp to $\bar{f}_i$.

All unram since $\bar{f}_1$ irred mod p

(*) if $p \equiv 1\ (3)$, $\mathbb{Z}/p\mathbb{Z}$ has cube roots of unity.
$\Rightarrow \mathbb{Z}_p \subset \mathbb{Q}_p$ has cube roots of unity. $\Rightarrow \mathbb{Q}_p \supset \underset{M}{\overset{\shortparallel}{\mathbb{Q}(\omega)}}$

$\Rightarrow$ either $\underbrace{\bar{f} \text{ irred}}_{p \text{ is inert in } L/\mathbb{Q}}$ or has $\underbrace{3 \text{ linear factors}}_{p \text{ splits in } L/\mathbb{Q}}$

f splits iff $\bar{f}$ has a root iff 2 is cube mod p
let $p = \pi\bar{\pi}$ is $\mathbb{Z}[\omega]$ $f_{M/\mathbb{Q}}(\pi : p) = 1$ $efg = 2$, $g=2$

or: $\mathbb{Q}(\omega)$ completed at π is $\mathbb{Q}_p$ ~~so~~ $f = 1$
$\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \simeq \mathbb{Z}/p\mathbb{Z}$.

Need to decide if $\left(\frac{2}{\pi}\right)_3 = 1$. By cubic reciprocity
this is $\Leftrightarrow$ $\left(\frac{\pi}{2}\right)_3$ (choose $\pi \equiv \pm 2\ (3)$ in $\mathbb{Z}[\omega]$)

2 is prime in $\mathbb{Z}[\omega]$, $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega] \simeq \mathbb{F}_4$
Only cube there is 1 so $\left(\frac{2}{\pi}\right)_3 = 1$ iff $\pi \equiv 1\ (2)$

write $p = a^2 + 3b^2$ $(p = N\pi)$ ..
condition on splitting in terms of a, b

· $p \equiv 2$ (3) $(\mathbb{Z}/p\mathbb{Z})^*[3] = \{1\}$ so no cube root of unity in $\mathbb{Z}/p\mathbb{Z}$, so in $\mathbb{Z}_p$

so either p inert ($\bar{f}$ irred) or $f = f_1 f_2$.

Ireland - Rosen, A Classical Introduction to Modern Number Theory (GTM) 84

Return to general problem: L/K finite, v place of K. Saw: completions of L lie in $L \cdot K_v \subset \bar{K_v}$

Makes us automatically interested in the K_v-algebra

$$K_v \otimes_K L$$

for each $w | v$ get hom $K_v \otimes_K L \to L_w$
$\Rightarrow$ get hom

$$K_v \otimes_K L \to \prod_{w|v} L_w \qquad (*)$$

(from embedding $L_w \hookrightarrow \bar{K_v}$ get map back)

<u>Thm:</u> If L/K is separable, $(*)$ is an isom

<u>Pf:</u> Say $L = K(\alpha)$ with min poly $f \in K[x]$
Say $f = \prod_w f_w$ with $f_w \in K_v[x]$ irred
(distinct since f is separable). By CRT:

$$\prod_w L_w \cong \prod_w \left(K_v[x]/(f_w) \right) \cong K_v[x]/fK_v[x]$$
$$\cong K_v \otimes_K K[x]/fK[x] \cong K_v \otimes_K L.$$

<u>Cor:</u> If L/K is separable,

$$[L:K] = \sum_{w|v} [L_w : K_v] = \sum_{w|v} e(w|v) \cdot f(w|v)$$

valuation is discrete
residue field perfect

$SL_2(\mathbb{Z}[\sqrt{2}]) \circlearrowright \mathbb{H}^{(2)} \times \mathbb{H}^{(2)}$ action totally discontinuous,

quotient has finite volume,
$\rightsquigarrow$ Hilbert modular forms

R_v top rings, $K_v \subset R_v$ compact subrings

M_v R_v-modules

$\bigotimes'_v M_v$

this relates to the question on restricted tensor products in the adèle supplement

<u>Need:</u> $\xi_v \in M_v$ s.t. $K_v \circlearrowleft \xi_v$ for almost all v

$$\bigotimes_{v \in S} x_v \otimes \bigotimes_{v \notin S} \xi_v \;\leftarrow\; \bigotimes_{v \in S} M_v$$

<u>Eg:</u> G_v groups, K_v subgps, M_v rep'ns
$\xi_v \in M_v$ K_v-fixed.

$\bigotimes'_v M_v$ is a rep'n of $\prod'_v G_v$

<u>Thms</u> (Flath) F #field, G/F lin alg.

every irred adm rep'n of $G(\mathbb{A}) = \prod'_v (G(F_v) : G(\mathcal{O}_v))$

is of form $\bigotimes'_v \pi_v$ at almost all places π_v sph