Math 538, lecture 14, 1/3/2024

Last time: Places of # fields

Looked at finite extensions L/K of fields, studied places of L lying over a fixed place v of K.

Basic observation: any completion L_w would embed in subspace $L \cdot K_v \subset \overline{K_v}$ ← alg. closure

$\Rightarrow$ look at $K_v \otimes_K L$

Conclusions: (L/K separable: $L = K(\alpha)$)

(1) places of L over v $\overset{1:1}{\longleftrightarrow}$ irred factors of min poly of α in K_v

(2) $K_v \otimes_K L \cong \bigoplus_{w|v} L_w$

Cor: ($|K^\times|$ discrete, K_v perfect)

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

Cor: Take $\beta \in L$. $Tr^L_K \beta$, $N^L_K \beta$ are the trace/det of K-linear map of mult by β on L.

$$\Rightarrow Tr^L_K \beta = \sum_{w|v} Tr^{L_w}_{K_v} \beta, \quad N^L_K \beta = \prod_{w|v} N^{L_w}_{K_v} \beta$$

Galois Extensions: Assume L/K Galois, finite

Prop: $Gal(L/K)$ acts transitively on places of L over v.

Pf: Say there are disjoint orbits. By weak approx can find $\beta \in L$ s.t. $|\beta|_w > 1$ in one orbit
$|\beta|_w < 1$ in another.

$$N^L_K \beta = \prod_{\sigma \in Gal(L/K)} \sigma\beta \qquad \text{take norms.}$$

Def: The decomposition group is $G_w = Stab_G(w)$

If v is non-arch also have a map
$$G_w \to Aut(\lambda_w : k_v)$$
Kernel is the inertia subgroup
$$I_w = \{\sigma \in G_w \mid \sigma x \equiv x \ (P_w)\}$$

Lemma: L_w/K_v is Galois with Galois gp G_w

Pf:

Let $L = K(\alpha)$ with min poly f. Then L is the splitting field of f.

$L_w = K_v(L) = K_v(\alpha)$ so L_w is the splitting field of f over K_v, hence Galois

Let f_w be the irred factor of f st.

$$L_w = K_v[x]/(f_w)$$

wlog α is a root of f_w.

Then $G_w = \{\sigma \in G \mid f_w(\sigma\alpha) = 0\}$

$$|G_w| = \deg f_w = [L_w : K_v]$$

Lemma: Let $L_w : K_v$ be a Galois extension of complete fields. Then $\lambda_w : k_v$ is normal and the map

$$\mathrm{Gal}(L_w : K_v) \to \mathrm{Aut}(\lambda_w : k_v)$$

is surjective.

Pf: Given $\bar{\alpha} \in \lambda_w$, let $\alpha \in \mathcal{O}_w = \mathcal{O}_{L_w}$ be a preimage. Let $f \in k_v[x]$ be the min poly of α. Then f splits in $\mathcal{O}_w$ ($L_w : k_v$ Galois)
So $\bar{f}$ splits in λ_w, so min poly of $\bar{\alpha}$ splits & extension is normal.

Any aut of λ_w will map $\bar{\alpha}$ to the image of some other root of f, so to $\overline{\sigma\alpha}$ for some $\sigma \in Gal(L_w/k_v)$.

<u>Apply to # fields</u>

F # field

Call place v of F infinite if $v | \infty$ (∞ place) $\Leftrightarrow$ v is archimedean, finite otherwise

Write $|F| = |F|_\infty \sqcup |F|_f$.

<u>Prop:</u> (1) $|F|_\infty = Hom(F, \mathbb{C}) / Gal(\mathbb{C} : \mathbb{R})$

(2) $|F|_f = \{ |\cdot|_\mathfrak{p} : \mathfrak{p} \triangleleft \mathcal{O}_F \text{ prime} \}$

Pf: (1) just $\{ v \in |F| : v | \infty \} = Hom(F, \overline{\mathbb{Q}_\infty}) / Gal(\overline{\mathbb{Q}_\infty} / \mathbb{Q}_\infty)$

(2) For a prime $\mathfrak{p}$ of F, set for $x \in F^*$

$$v_{\mathfrak{p}}(x) = e \quad \text{if} \quad \mathfrak{p}^e \| x\mathcal{O}_F$$

This is a valuation $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$ follows from unique factorization

if $\mathfrak{p}^e \| x\mathcal{O}_F$, $\mathfrak{p}^e \| y\mathcal{O}_F$ $\Leftrightarrow$ $x\mathcal{O}_F, y\mathcal{O}_F \subseteq \mathfrak{p}^e$

so $(x+y)\mathcal{O}_F \subseteq \mathfrak{p}^e$ $\Rightarrow$ $v_{\mathfrak{p}}(x+y) \geq \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}$

If $\mathfrak{p} \neq \mathfrak{p}'$ $v_{\mathfrak{p}}, v_{\mathfrak{p}'}$ are distinct.

(CRT: have $x \in \mathfrak{p}$ $x \in \mathcal{O}_F \setminus \mathfrak{p}'$
$y \in \mathfrak{p}'$ $y \in \mathcal{O}_F \setminus \mathfrak{p}$

so $v_{\mathfrak{p}}(x) > 0$, $v_{\mathfrak{p}'}(x) = 0$
$v_{\mathfrak{p}}(y) = 0$, $v_{\mathfrak{p}'}(y) > 0$ $\Rightarrow$ $v_{\mathfrak{p}}, v_{\mathfrak{p}'}$ not proportional)

<u>Converse:</u> Let $|\cdot|$ be an absolute value on F (non-trivial). Then $|\cdot|\big|_{\mathbb{Q}}$ is a non-triv absolute value, either $|\cdot|_\infty$ or $|\cdot|_p$ for some rational prime p

If $|\cdot|$ is non-arch it extends $|\cdot|_p$ (renormalize)

Let $\alpha \in F$ have $|\alpha| > 1$; let $f \in \mathbb{Z}[x]$ be monic, of deg d. Then $|f(\alpha)| = |\alpha|^d > 0$ so $\alpha \notin \mathcal{O}_F \Rightarrow \mathcal{O}_F \subset \{\alpha \in F : |\alpha| \leq 1\}$.

$\Rightarrow \mathfrak{p} = \mathcal{O}_F \cap \{\alpha \in F : |\alpha| < 1\}$ is prime.

$\left(\mathcal{O}_F/\mathfrak{p} \hookrightarrow \{\alpha \in F : |\alpha| \leq 1\} / \{\alpha \in F : |\alpha| < 1\} \right)$

Want to show $|\cdot| = |\cdot|_{\mathfrak{p}}$.

First $|p| = |p|_p = \frac{1}{p} < 1$ so $p \in \mathfrak{p}$

i.e. $\mathfrak{p} \mid p$. Let $|\cdot|_{\mathfrak{p}}$ be the associated absolute value, normalized s.t. $|p|_{\mathfrak{p}} = \frac{1}{p}$.

Both $|\cdot|, |\cdot|_{\mathfrak{p}}$ agree on what

$$\{x \in \mathcal{O}_F : |x| < 1\}$$

is; agree on $\mathcal{O}_F \setminus \mathfrak{p}$ $|\cdot| = 1$.

$\Rightarrow$ agree on $\mathfrak{p} \setminus \mathfrak{p}^2$, on $\mathfrak{p}^2 \setminus \mathfrak{p}^3$, (first localise at $\mathfrak{p}$) after localization $(\mathcal{O}_F)_\mathfrak{p}$ is a local ring, $|\cdot|$, $|\cdot|_\mathfrak{p}$ agree on $(\mathcal{O}_F)_\mathfrak{p}^\times$.

so both determined by values on uniformizer.
Some power of u is associate to $\mathfrak{p}$
so $|\cdot| = |\cdot|_\mathfrak{p}$.

$\boxtimes$

<u>Lemma</u>: (completion includes localization)
Let $v \in \mathcal{V}_F$ corresp. to $\mathfrak{p} \triangleleft \mathcal{O}_F$. Then $\mathcal{O}_F$ is dense in $\mathcal{O}_v \subset F_v$, $\mathfrak{p}$ is dense in $\mathfrak{p}_v \triangleleft \mathcal{O}_v$

More generally if $\mathfrak{a} \subset F$ is a fractional ideal of order e at $\mathfrak{p}$, have $\overline{\mathfrak{a}} = \mathfrak{p}_v^e$

closure in F_v

<u>converse</u>: $\mathfrak{p}_v^e \cap \mathcal{O}_F = \mathfrak{p}_v^e$.

<u>Pf</u>: Checked above $\mathcal{O}_F \subset \mathcal{O}_v$, $\mathfrak{p} \subset \mathfrak{p}_v$.
Let $x \in F$ have $|x|_\mathfrak{p} \leq 1$.
Know: order of $\mathfrak{p}$ at $x\mathcal{O}_F$ is at least 0
$\Rightarrow$ have $\mathfrak{a}$ prime to $\mathfrak{p}$ s.t. $x\mathcal{O}_F = \mathfrak{p}^e \mathfrak{a}$
$\Rightarrow$

$$\mathfrak{a}^{-1} x = \mathfrak{p}^e \subseteq \mathcal{O}_F$$

So $\mathfrak{a}^{-1}$ prime to $\mathfrak{p}$ so have $\alpha \in \mathfrak{a}^{-1}, \alpha \notin \mathfrak{p}$

$\alpha x \in \mathcal{O}_F$.

since α is prime to $\mathfrak{p}$, it's prime to $\mathfrak{p}^k$.
$(\alpha) + \mathfrak{p}^k = (1)$

So given k can find $\bar{\alpha} \in \mathcal{O}_F$ s.t. $\alpha\bar{\alpha} \equiv 1 \ (\mathfrak{p}^k)$

then $v_p(\underbrace{\alpha\bar{\alpha}x}_{\in \mathcal{O}_F} - x) = v_p(x) + v_p(\alpha\bar{\alpha} - 1)$
$\geq v_p(x) + k \xrightarrow[k\to\infty]{} \infty$

$\Rightarrow \mathcal{O}_F$ is dence in $\mathcal{O}_v$.

If $\mathfrak{a}$ is fractional ideal, $\bar{\mathfrak{a}} \subset F_v$ is
$\mathcal{O}_F$-inv't $\Rightarrow \mathcal{O}_v$ inv't

Also $\mathfrak{a} \subset \alpha\mathcal{O}_F$ for some $\alpha \in F^\times$
so $\bar{\mathfrak{a}} \subset \alpha\mathcal{O}_v$.
so $\bar{\mathfrak{a}}$ is a fractional ideal of F_v

$\Rightarrow \bar{\mathfrak{a}} = \mathfrak{p}_v^{e'}$ want: $e' = e$.

claim is inv't by mult by elements of $\mathbb{Q}^\times$.
so can assume $\mathfrak{a} \subset \mathcal{O}_F$
then if $\mathfrak{a} \subset \mathfrak{p}^e$, $\bar{\mathfrak{a}} \subset \overline{\mathfrak{p}^e} = \bar{\mathfrak{p}}^e = \mathfrak{p}_v^e$

$\Rightarrow e' \geq e$

<u>converse:</u> $\bar{\mathfrak{a}} \subset \mathfrak{p}_v^{e'} \Rightarrow \mathfrak{a} \subset \bar{\mathfrak{a}} \cap \mathcal{O}_F \subset \mathfrak{p}^{e'}$.
$\Rightarrow e \geq e'$

<u>Lemma:</u> let L/K be number fields, $[L:K]=n$
let $w \in |L|_f$, $v \in |K|_f$, $w|v$, assoc to primes $\mathfrak{P}, \mathfrak{p}$

Then $e(L_w : K_v) = e(\mathfrak{P}/\mathfrak{p})$
$f(L_w : K_v) = f(\mathfrak{P}/\mathfrak{p})$.

<u>Pf:</u> By previous lemma map $\mathcal{O}_K \to \mathcal{O}_v/\mathfrak{p}_v$ is surjective, kernel $\mathfrak{p}$.

so $K_v \cong \mathcal{O}_K/\mathfrak{p} \Rightarrow f(L_w : K_v) = f(\mathfrak{P}/\mathfrak{p})$

For ramification, localize at $\mathfrak{P}, \mathfrak{p}$ resp

then $\mathfrak{P}^e = \mathfrak{p}\mathcal{O}_L$, both principal

$\Rightarrow$ | gen of $\mathfrak{p}$ | = e-th power of | of gen of $\mathfrak{P}$ |.

$\blacksquare$

Def: Let v be a place of F.
Write

$|\cdot|_v$ for the absolute value in the class that restricts to $|\cdot|_p$ on $\mathbb{Q}$

$(|p|_v = \frac{1}{p})$

$\|\cdot\|_v$ for absolute value $\|\cdot\|_v = |\cdot|_v^{[F_v:\mathbb{Q}_p]}$

Lemma: If v is infinite, assoc to $\varphi: F \to \mathbb{C}$
have $\|x\|_v = \begin{cases} |\varphi(x)|_{\mathbb{R}} & \text{if } v \text{ real} \\ \varphi(x)\overline{\varphi(x)} & \text{if } v \text{ complex} \end{cases}$

(if $\varphi(x) = a+bi$, v complex, $\|x\|_v = a^2+b^2$)

For a finite place v assoc to $\mathfrak{p} \triangleleft \mathcal{O}_F$,
let $q = \# k_v = [\mathcal{O}_F : \mathfrak{p}] = [\mathcal{O}_v : \mathfrak{p}_v]$.
Then

$$\|x\|_v = q_v^{-v_{\mathfrak{p}}(x)}.$$

$(\|p\|_v = p^{-e_{\mathfrak{p}} f_{\mathfrak{p}}})$ $\qquad e_{\mathfrak{p}} f_{\mathfrak{p}} = [F_v : \mathbb{Q}_p]$

Prop (Product formula)
For all $x \in F^\times$

$$\prod_{v \in |F|} \|x\|_v = 1$$

Pf Claim for $\mathbb{Q}$ is just unique factorization (HW)

If $v \in F$ is above $|\cdot|_p$ (maybe $p = \infty$)

$$|x|_v = |N^{F_v}_{\mathbb{Q}_p} x|_p^{1/[F_v : \mathbb{Q}_p]}$$

$$\Rightarrow \|x\|_v = |N^{F_v}_{\mathbb{Q}_p}|_p$$

$$\Rightarrow \prod_{v|p} \|x\|_v = \prod_{v|p} |N^{F_v}_{\mathbb{Q}_p} x|_p = |\prod_{v|p} N^{F_v}_{\mathbb{Q}_p} x|_p$$

$$= |N^F_{\mathbb{Q}} x|_p$$

Now mult over p, use formula for $\mathbb{Q}$.

(for almost all v, $\|x\|_v = 1$)