Math 538, lecture 7, 31/1/2024

Last time: primes in Galois extensions

$G \left(\begin{array}{c} L \\ | \\ K \end{array} \right.$ Galois extension of # fields, $p \triangleleft \mathcal{O}_K$ prime lying below $\mathfrak{P} \triangleleft \mathcal{O}_L$.

Thms: (1) G acts transitively on primes of L above p

$\Rightarrow$ **Def:** $G_{\mathfrak{P}} = \mathrm{Stab}_G(\mathfrak{P})$ is the decomposition group

(2) Map $G_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}} : k_p)$ is surjective.

$\Rightarrow$ **Def:** $\mathrm{Ker} = \{ \sigma \in G \mid \sigma x \equiv x \ (\mathfrak{P}) \} = I_{\mathfrak{P}}$ is the inertia group

Any $\sigma \in G_{\mathfrak{P}}$ s.t. $\sigma x \equiv x^q \ (\mathfrak{P})$, $q = \# k_p$ is a Frobenius element.

Today: Start Chapter 2: Local fields

- valuations

Valuations and absolute values

Theme: encode algebra in analysis.
arithmetic

Fix a field F.

Def: A valuation is a map $v: F \to \mathbb{R} \cup \{\infty\}$
s.t.:

(1) $v(xy) = v(x) + v(y)$

(2) $v(x)+v(y) \geq \min\{v(x), v(y)\}$

(3) $v^{-1}(\{\infty\}) = \{0\}$

Examples: (1) $F = \mathbb{Q}$, $v_p(p^r \frac{a}{b}) = r$ if $p \nmid ab$
"p-adic valuation of $\mathbb{Q}$", K. Hensel.

(2) $F = k(t)$ (k = any field), $p \in k[t]$ irred,
$v_p(p^r \frac{a}{b}) = r$ is $p \nmid ab$ ($k[t]$ is a UFD)

(3) $F = k(t)$ $v_\infty(\frac{a}{b}) = \deg b - \deg a$

In fact 2,3 same thing: think of elements of $k(t)$ as rational functions on $\mathbb{P}^1(\bar{k})$
for any point, have valuation = order of vanishing.

But: to $\mathbb{Z}$ associate space $\mathrm{Spec}(\mathbb{Z}) = \{\text{primes}\} \cup \{0\}$

interpret each $n \in \mathbb{Z}$ as a function on $\mathrm{Spec}(\mathbb{Z})$

value of n at p is residue $n \bmod p$.

To get full "Taylor expansion" need to reduce mod $p^2, p^3, \ldots$, "order of vanishing" = largest r s.t. $n \equiv 0 \ (p^r)$.

Def: An absolute value on F is a function

$$|\cdot| : F \to \mathbb{R}_{\geq 0}$$

s.t.

(1) $|xy| = |x| \cdot |y|$

(2) $|x+y| \leq |x| + |y|$

(3) $|x| = 0$ iff $x = 0$

Call the absolute value trivial (nondiscrete) if $|x| = 1$ for all $x \neq 0$

ultrametric or non-archimedean if $|x+y| \leq \max\{|x|, |y|\}$

Ex: $|1| = |1^2| = |1|^2$ so $|1| \in \{0, 1\}$ but $|1| \neq 0$

so $|1| = 1$

if $\exists x$ with $|x| \neq \{0, 1\}$, either x or $\frac{1}{x}$ has $0 < |x| < 1$ then $|x^n| \to 0$ so $x^n \to 0$.

Example: (1) usual absolute value on $\mathbb{Q}$, $|\cdot|_\infty$
(2) let v be a valuation on F, $q>1$.
Set
$$|x|_v = q^{-v(x)}.$$
Then $|\cdot|_v$ is a nonarchimedean absolute value

On $\mathbb{Q}$ set $|x|_p = p^{-v_p(x)}$ i.e. $|p^r| = p^{-r}$

Observation: ("product formula") for $x \in \mathbb{Q}^\times$
$$|x|_\infty \cdot \prod_p |x|_p = 1$$

lemma: let $|\cdot|$ be an absolute value. Then $|\cdot|$ is non arch iff the set $\{|n \cdot 1_F| : n \geq 1\}$ is bounded, which is implied by $|n \cdot 1_F| \leq 1$ for some $n \geq 2$

Pf: If $|\cdot|$ in non-arch $\left(|\sum_{i=1}^{r} x_i| \leq \max_{1 \leq i \leq r} |x_i| \right)$

Then $|n \cdot 1_F| = |1_F + \cdots + 1_F| \leq |1_F| = 1$

Conversely suppose $|n \cdot 1_F| \leq M$ for all $n \in \mathbb{Z}_{\geq 1}$.
Then for any $x, y \in F$,

$$|(x+y)^N| = \left|\sum_{k=0}^{N} \binom{N}{k} x^k y^{N-k}\right|$$

$$\leq \sum_{k=0}^{N} \left|\binom{N}{k}\right| |x|^k |y|^{N-k}$$

$$\leq (N+1)\cdot M \left(\max\{|x|,|y|\}\right)^N$$

so $|x+y| \leq (N+1)^{1/N} \cdot M^{1/N} \cdot \max\{|x|,|y|\}$

$\to \max\{|x|,|y|\}$ as $N \to \infty$

Suppose we only know $|b| \leq 1$ for some $b \geq 2$

Let $M = \max\{|a| : 0 \leq a < b\}$

Writing any $n \in \mathbb{Z}_{\geq 1}$ as $n = \sum_{i=0}^{\log_b n} a_i b^i$

have $|n| \leq \sum_{i=0}^{\log_b n} |a_i| \cdot |b|^i \leq M \cdot (\log_b n + 1)$

$$\Rightarrow |n| = |n^d|^{1/d} \leq \left(M(d\log_b n + 1)\right)^{1/d} \xrightarrow[d\to\infty]{} 1 \quad \blacksquare$$

<u>Cor:</u> If $\mathrm{char}(F) > 0$, any absolute value on F is non-arch (set $\{n \cdot 1_F\}$ is finite)

Ex: $\mathrm{char}(F)=0$, $|F|\le \aleph$ then F has a non-ultrametric absolute value.
Pf: $\overline{F}$ is an alg. closed field of cardinality $\aleph$ so $\overline{F}\cong \mathbb{C}$ as fields. Take $|\cdot|_\infty$ on $\mathbb{C}$.

Given an absolute value $|\cdot|$ on F, $d(x,y)=|x-y|$ is a metric, it's an ultrametric iff $|\cdot|$ is

(ultrametric : $d(x,z)\le \max\{d(x,y),d(y,z)\}$)
$\Rightarrow$ $|y|<|x|$ then $|x+y|=|x|$
$\Rightarrow$ if $s<r$, $x\in B_r(0)$, $B_s(x)\subset B_r(0)$)
if two balls intersect, one is contained in the other)

Def: Two absolute values on F are equivalent if they induce same topology on F.

Lemma: (Snowflake construction) If $|\cdot|$ is an absolute value on F, then so is $|\cdot|^\lambda$ for any $\lambda<1$.

Lemma: Let $|\cdot|_1$, $|\cdot|_2$ be equivalent non-trivial absolute values then $|\cdot|_1=|\cdot|_2^\lambda$ for some $\lambda>0$

Pf: Observe $|x^n| \to 0$ iff $|x| < 1$, so sets

$\{x : |x| < 1\}$, $\{x : |x| = 1\}$, $\{x : |x| > 1\}$

only depend on the topology. Fix $a \in F$ s.t. $|a|_1 > 1$. Then $|a|_2 > 1$, set λ s.t. $|a|_1 = |a|_2^\lambda$.

Let $b \in F^\times$

For any k, l whether $|a^k b^l| > 1$ or < 1 same for $|\cdot|_1$, $|\cdot|_2$ if $|b|_2^\lambda \neq |b|_1$:

say $\log|b|_1 \neq \lambda \cdot \log|b|_2$

take l large s.t. $l(\log|b|_1 - \lambda \log|b|_2) > \log|a|_1$

take k s.t. $l \log|b|_1 + k \log|a|_1$

$\lambda l \log|b|_2 + k \lambda \log|a|_2$

have different signs $\Rightarrow\Leftarrow$ ∎

Def: $|F|$ will denote the set of equivalence classes of non discrete absolute values on F.

Theorem: (Ostrowski) $|\mathbb{Q}| = \{|\cdot|_p\}_{p \leq \infty}$

Pf: HW.

Theorem: ("Weak approximation"; Artin-Whaples) Let $\{|\cdot|_i\}_{i=1}^n$ be pairwise inequivalent nondiscrete absolute values on F, let $\underline{x} \in F^n$, let $\varepsilon > 0$. Then there is $y \in F$ s.t. $|x_i - y|_i < \varepsilon$

Remark: If $F = \mathbb{Q}$, see given any classes mod $p_i^{r_i}$ can find $y \in \mathbb{Q}$ in those classes.

CRT = "strong" approx: can also insist $|y|_\ell \leq 1$ for $\ell \neq p_i$.

Set-theory notation: $|A|$ = cardinality of set A.

$\aleph_0$ = cardinality of $\mathbb{N}$.

$\aleph$ = cardiality of the continuum

hebrew letter Aleph.

$\aleph_\alpha$ = α'th cardinal

$\beth_0 = \aleph_0$, $\beth_{\alpha+1} = 2^{\beth_\alpha}$ + limit