COURS 5

lunedì 15 marzo 2021 13:58

References: • ROBERT : A course in p-adic analysis chap. 1-2-3

• KOBLITZ: p-adic numbers, p-adic analysis and ζ-functions chap. 1-2

Recall

valued field: $(K, |\cdot|)$

• archimedean $|n \cdot 1| > 1$ for some $n \in \mathbb{N}$, if complete $\Rightarrow \simeq \mathbb{R}$ or $\mathbb{C}$ with $|\cdot|_\infty$.

• non-archimedean $|x+y| \leq \max\{|x|, |y|\}$ Ex: $\mathbb{Q}_p = (\mathbb{Q}, |\cdot|_p)^{\text{completion}}$.

The field $\mathbb{C}_p$: "p-adic complex field"

$(\mathbb{Q}, |\cdot|_\infty) \xrightarrow{\text{complete}} \mathbb{R} \xrightarrow{\text{alg. closure}} \mathbb{C}$

$(\mathbb{Q}, |\cdot|_p) \hookrightarrow \mathbb{Q}_p \hookrightarrow \mathbb{Q}_p^{alg}$

Rem: $\mathbb{Q}_p^{alg}$ is endowed with a unique norm that is multiplicative and extends $|\cdot|_p$ on $\mathbb{Q}_p$. Fact: $\mathbb{Q}_p^{alg}$ is NOT complete.

Idea 1. KOBLITZ, §III.4.

or. Baire category argument: $F_n = \{x \in \mathbb{Q}_p^{alg}, \deg_{\mathbb{Q}_p}(x) = n\}$ is closed, non-empty, with empty interior, use Baire Theorem.

Def: $\mathbb{C}_p$ is the completion of $\mathbb{Q}_p^{alg}$

Thm: $\mathbb{C}_p$ is complete and algebraically closed. (in fact, this holds $\forall$ K algebraically closed valued field)

Rem: • value group $|\mathbb{C}_p^\times| = \{|x|_p, x \in \mathbb{C}_p^\times\}$

$|\mathbb{C}_p^\times| = |(\mathbb{Q}_p^{alg})^\times| = p^{\mathbb{Q}}$ exercise (recall $|\mathbb{Q}_p^\times| = p^{\mathbb{Z}}$)

since $|x-y|_p < |y|_p \Rightarrow |x|_p = |y|_p$.

• residue field $\tilde{\mathbb{C}}_p = \mathbb{C}_p^\circ / \mathbb{C}_p^{\circ\circ} = \{x \in \mathbb{C}_p : |x| \leq 1\} / \{|x| < 1\}$

$\tilde{\mathbb{C}}_p \simeq \tilde{\mathbb{Q}}_p^{alg} \simeq (\tilde{\mathbb{Q}}_p)^{alg} = \mathbb{F}_p^{alg}$

density of $\mathbb{Q}_p^{alg}$ inside $\mathbb{C}_p$ — non-trivial exercise.

Fact: $\mathbb{C}_p$ is NOT locally compact (exercise III.5)

Fact: $\mathbb{C}_p$ is NOT locally compact (exercise III.5)

(locally compact $\Rightarrow$ $|K^\times|$ discrete and $\tilde{K}$ finite. Here both don't hold)

Fact: $\mathbb{C}_p$ as a field is isomorphic to $\mathbb{C}$ (ROBERT, §3.3.5)

Proof: $a_0 \dots a_{d-1} \in \mathbb{C}_p$. $x^d + a_{d-1}x^{d-1} + \dots + a_0 = 0$. (*)

Want to show that (*) has at least a solution in $\mathbb{C}_p$.

For each i, $a_i^{(n)} \in \overline{\mathbb{Q}}_p$, $|a_i^{(n)} - a_i|_p \to 0$.

$E_n := \max_i |a_i^{(n)} - a_i^{(n+1)}| \to 0$. Consider

$P_n(x) = x^d + a_{d-1}^{(n)} x^{d-1} + \dots + a_0^{(n)} \in \overline{\mathbb{Q}}_p[x]$.

By induction we construct a sequence $x_n \in \overline{\mathbb{Q}}_p$ such that $|x_{n+1} - x_n|_p \le \varepsilon_n^{\frac{1}{d}} A$ where A is some fixed positive real number, and $P_n(x_n) = 0$

$\Rightarrow (x_n)_n$ is a Cauchy sequence, converges to x_∞. By continuity, $P(x_\infty) = 0$.

$\{P_n = 0\} = \{x_1^{(n)}, \dots, x_d^{(n)}\} \subseteq \overline{\mathbb{Q}}_p$.

Fact: $\sup_n \max_{i=1\dots d} \{|x_i^{(n)}|_p\} < +\infty$.

$A := \max\{\dots, 1\}$

Proof: suppose x_n has been chosen. Evaluate

$|P_{n+1}(x_n)| = \left|\prod_{j=1}^{d} (x_j^{(n+1)} - x_n)\right| \le |(P_{n+1} - P_n)(x_n)| \le \varepsilon_n A^d \Rightarrow$

$\exists j,\ |x_j^{(n+1)} - x_n| \le \varepsilon_n^{\frac{1}{d}} A \quad \Rightarrow \quad x_{n+1} = x_j^{(n+1)}$.

Proof of the fact: $P_n(x) = x^d + a_{d-1}^{(n)} x^{d-1} + \dots + a_0^{(n)}$. $a_j^{(n)} \to a_j$

$A' = \sup_{n,j} \max\{1, |a_j^{(n)}|\}$. $J := \{1 \le j \le d,\ \bullet\ |x_j^{(n)}| > A,\ \bullet\ |x_j^{(n)}| = \max_{1 \le \ell \le d} |x_\ell^{(n)}|\}$.

look at the symmetric polynomial. $|\sigma_{|J|}(x_j^{(n)})|_p = |a_{d-|J|}^{(n)}|$

a sum of terms.

- exactly one of them has norm $|x_j^{(n)}|^{|J|}$
- all others have norm $< |x_j^{(n)}|^{|J|}$ $\Rightarrow |x_j^{(n)}|^{|J|} \le A'$. □

3) Norms on number fields.

$K = \mathbb{Q}$

3) Norms on number fields.

$\mathbb{K} = \mathbb{Q}$

Theorem (OSTROWSKI) Any multiplicative norm on $\mathbb{Q}$ is either:

- the trivial norm $|\cdot|_0$.
- $|\cdot|_\infty^\varepsilon$ $\varepsilon \in (0,1]$ archimedean
- $|\cdot|_p^\lambda$ $\lambda > 0$ p prime : N.A.

Proof (KOBLITZ §1.2)

If $|\cdot|$ is non trivial and not archimedean, then it is N.A.

$\rightarrow |x| \leq 1$ for any integer $x \in \mathbb{Z}$ $\rightsquigarrow \exists\, x_0 \in \mathbb{Z}$, $|x_0| < 1$

$\Rightarrow \exists p$ prime, $|p| < 1$

If $m \wedge p = 1$ then $|m| = 1$.

The fact is that m has finite order in $\mathbb{F}_p^\times$ $\Rightarrow \exists\, a \geq 1$, $p \mid m^a - 1$.

$\rightsquigarrow |m^a - 1| < 1 \Rightarrow |m^a| = |1| = 1 \rightsquigarrow |m| = 1$

In the general case write $m = p^{v_p(m)} \cdot m'$. Use multiplicative property of $|\cdot|$ and proceed by induction on $v_p(m)$. □

Goal: extend this to any number field

Set $M_{\mathbb{Q}} = \{\infty\} \cup P$ = primes.

We have a bijection: $v \in M_{\mathbb{Q}} \mapsto |\cdot|_v$

$|\cdot|_v$ is a nontrivial multiplicative norm on $\mathbb{Q}$, modulo a natural equivalence relation (which allows to normalize by $|p|_p = \frac{1}{p}$)

We say that $|\cdot|_1 = |\cdot|_2 \Leftrightarrow |\cdot|_1^\alpha = |\cdot|_2^\beta$ for some $\alpha, \beta > 0$.

($\Leftrightarrow$ they define the same topology on $\mathbb{Q}$).

Let now $\mathbb{K}$ be any number field.

$M_{\mathbb{K}} = \{$nontrivial multiplicative norms on $\mathbb{K}$, $|\cdot|_{\mathbb{K}} = |\cdot|_v$ for some $v \in M_{\mathbb{Q}}\}$.

Restriction: $M_{\mathbb{K}} \rightarrow M_{\mathbb{Q}}$

$|\cdot| \mapsto |\cdot|_{\mathbb{Q}}$ $(= |\cdot|_v)$.

Restriction: $|\cdot|_K \rightsquigarrow |\cdot|_{\mathbb{Q}}$

$|\cdot| \mapsto |\cdot|_{\mathbb{Q}}$ $(= |\cdot|_v)$.

The archimedean case: want to describe $M_{K,\infty} = \text{rest}^{-1}(\infty)$.

$K = \mathbb{Q}[T]/(P)$ $P \in \mathbb{Z}[T]$ irreducible.

$P^{-1}(0) \cap \mathbb{C} = \{ \underbrace{x_1 \dots x_r}_{\in \mathbb{R}}, \underbrace{y_1, \bar{y}_1, \dots, y_s, \bar{y}_s}_{\in \mathbb{C} \setminus \mathbb{R}} \}$

Embeddings of K in $\mathbb{C}$.

- real: $\forall\, 1 \le i \le r$ $\sigma_i : K \hookrightarrow \mathbb{R}$ unique embedding in $\mathbb{R}$ s.t. $\sigma_i(T) = x_i$.
If $x \in K$, $|x|_{i,\mathbb{R}} := |\sigma_i(x)|_\infty$ Then $|\cdot|_{i,\mathbb{R}} \in M_{K,\infty}$.
- complex: $\forall\, 1 \le j \le s$, $\tau_j : K \hookrightarrow \mathbb{C}$ unique embedding s.t. $\tau_j(T) = y_j$.
$|x|_{j,\mathbb{C}} := |\tau_j(x)|_\infty$, $|\cdot|_{j,\mathbb{C}} \in M_{K,\infty}$.

We will show that these are the only elements in $M_{K,\infty}$.

Rem: if $\tau_{\bar{j}}(T) = \bar{y}_j$, then $\tau_{\bar{j}} \neq \tau_j$, but $|\tau_j(x)|_\infty = |\tau_{\bar{j}}(x)|_\infty$ $\forall x$.

Theorem: $M_{K,\infty} = \{ |\cdot|_{i,\mathbb{R}},\ i = 1 \dots r \} \cup \{ |\cdot|_{j,\mathbb{C}},\ j = 1 \dots s \}$.

In particular, $\text{Card}(M_{K,\infty}) = r + s \le r + 2s = [K : \mathbb{Q}]$.

For any $v \in M_{K,\infty}$, set $n_v = \begin{cases} 1 & |\cdot|_v = |\cdot|_{i,\mathbb{R}} \\ 2 & |\cdot|_v = |\cdot|_{j,\mathbb{C}} \end{cases}$. More obstractly:

$n_v = [K_v : \mathbb{Q}_v]$

↑ completion of K w.r.t. $|\cdot|_v$.

Corollary: $\forall x \in K$, $\prod_{v \in M_{K,\infty}} |x|_v^{n_v} = |N_{K/\mathbb{Q}}(x)|_\infty$

$|\tau_j(x)|\,|\bar{\tau}_j(x)|$

Proof (cor) $\prod_{v \in M_{K,\infty}} |x|_v^{n_v} = \prod_{i=1}^{r} |\sigma_i(x)|_v \times \prod_{j=1}^{s} |\tau_j(x)|^2$

But $\{ \sigma_i(x), \tau_j(x), \bar{\tau}_j(x) \} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})(x)$.

We conclude by the Red thm $N_{K/\mathbb{Q}}(x) = \prod_i \sigma_i(x) \prod_j \tau_j(x)\bar{\tau}_j(x)$ □.

↑ $\in \mathbb{Q}$

We conclude by the Kod that $N_{K/\mathbb{Q}}(x) = \prod_i \sigma_i(x) \prod_j \tau_j(x)\overline{\tau_j(x)}$ □.

↑ relative norm

Proof of the Thm. 2 steps:

1) $M_{K,\infty} \subseteq \{|\cdot|_{i,\mathbb{R}}, |\cdot|_{j,\mathbb{C}}\}$. 2) all these norms are different.

1) $f \in M_{K,\infty}$. $f : K \to \mathbb{R}_+$ multiplicative norm $f(x) = |x|_\infty$ $\forall x \in \mathbb{Q}$.

Want $f(x) = |x|_{i,\mathbb{R}}^{\alpha} = |x|_{j,\mathbb{C}}^{\alpha}$.

$\hat{K}$ = completion of K w.r.t. f.

$\hat{K} \supseteq$ completion of $(\mathbb{Q}, |\cdot|_\infty) = (\mathbb{R}, |\cdot|_\infty)$.

By Gelfand-Mazur, $\hat{K} = (\hat{K}, |\cdot|_\infty) = (\mathbb{R}, |\cdot|_\infty)$ or $= (\mathbb{C}, |\cdot|_\infty)$.

$K = \mathbb{Q}[T]/(P) \subseteq \hat{K} \hookrightarrow \mathbb{C}$ isomorphic embedding, with $\sigma(T) \in P^{-1}(0)$

$\leadsto f(x) = |\sigma(x)|_\infty \Rightarrow \sigma = \sigma_{i,\mathbb{R}}$ or $= \tau_{j,\sigma}$ or $\bar{\tau}_{j,\sigma} \Rightarrow f = |\cdot|_{i,\mathbb{R}}$ or $|\cdot|_{j,\mathbb{C}}$.

2) Suppose now two embeddings $\sigma, \sigma' : K \hookrightarrow \mathbb{C}$ define the same norm:

$|\sigma(x)|_\infty = |\sigma'(x)|_\infty$ $\forall x \in K$. Conclusion: $\sigma' = \sigma$ or $\bar{\sigma} = \bar{\sigma}$.

$K \xrightarrow{\sigma} \mathbb{C} \supseteq \hat{K}_\sigma$

$\downarrow$ field iso. isometry

$\xrightarrow{\sigma'} \mathbb{C} \supseteq \hat{K}_{\sigma'}$

One concludes by the following facts:

- the only field isometry of $\mathbb{R}$ is id,
- of $\mathbb{C}$ is id or $z \mapsto \bar{z}$.

The non-archimedean case:

We do the same with $M_{K,p} = \text{rest}^{-1}(p)$.

$K = \mathbb{Q}[T]/(P)$ P irreducible.

Write $P = \prod_{i=1}^{i_p} P_i$ where $P_i \in \mathbb{Q}_p[T]$ irreducible.

$\deg P_i =: n_i$, $\sum n_i = [K : \mathbb{Q}_p]$

Thm: $M_{K,p}$ possesses exactly i_p elements. For all $v \in M_{K,p}$, set $n_v = [K_v : \mathbb{Q}_p] \geq 1$.

Then $\prod_{v \in M_{K,p}} |x|_v^{n_v} = |N_{K/\mathbb{Q}}(x)|_p$

Rem: at ∞: $n_v \in \{1, 2\}$. at p, $n_v \in \mathbb{N}$ can be arbitrarily large.

Rem: of ∞: $n_v \in \{1,2\}$. of p, $n_v \in \mathbb{N}$ can be arbitrarily large.

Proof: analog to the $\mathbb{C}$ case!

$f \in M_{K,p}$. $\mathbb{Q} \subseteq \mathbb{Q}_p \subseteq \overline{\mathbb{Q}}_p^{alg} \subseteq \mathbb{C}_p$.

$K \subseteq K_f \subseteq \overline{K}_f$ ← choose any isometry.

Fact: $[\hat{K}_f : \mathbb{Q}_p] < +\infty$.

$\exists \sigma : K \hookrightarrow \mathbb{C}_p$, $\forall x \in K$, $f(x) = |\sigma(x)|_p$ (by uniqueness of the p-adic norm on $\hat{K}_f$).

$\exists$ root x_i of P inside $\overline{\mathbb{Q}}_p^{alg}$.

$|f(x)| = |\sigma_i(x)|_p$, $\sigma_i(\tau) = x_i$.

2) Suppose now $\sigma_i, \sigma_j : K \hookrightarrow \mathbb{C}_p$ such that $|\sigma_i(x)| = |\sigma_j(x)|$

$\hat{K}_i$ = completion of K w.r.t. $|\sigma_i|$

$\hat{K}_j$ = " " " $|\sigma_j|$ $\hat{K}_i \simeq \hat{K}_j$ field isometry

You may assume $\hat{K}_i$, $\hat{K}_j \subseteq \overline{\mathbb{Q}}_p^{alg}$.

$\exists \varphi \in Gal(\overline{\mathbb{Q}}_p^{alg}/\mathbb{Q}_p)$ s.t. $\sigma_i = \varphi \circ \sigma_j$ (i.e. we extend to the algebraic closure as an isometry).

Let $x_i = \sigma_i(\tau)$, $x_j = \sigma_j(\tau) \in \overline{\mathbb{Q}}_p^{alg}$

Then $\sigma_i = \varphi \circ \sigma_j \iff x_i$ and x_j are Galois conjugate $/\mathbb{Q}_p$.

They are root of one of the factors of P inside $\mathbb{Q}_p[\tau]$.

- The product formula is analogous to the ∞-case. □

Proof of: $[\hat{K}_f : \mathbb{Q}_p] < \infty$.

$K/\mathbb{Q}$ finite extension, $f : K \to \mathbb{R}_+$ mult. norm., $f|_{\mathbb{Q}} = |\cdot|_p$.

- $K = \mathbb{Q} e_1 \oplus \dots \oplus \mathbb{Q} e_s$. $\cdot |$

V = Vector space generated by $e_1 \dots e_s$ inside $\hat{K}_f$.

$= \mathbb{Q}_p e_1 + \dots + \mathbb{Q}_p e_s \subseteq \hat{K}_f$

$\dim_{\mathbb{Q}_p} V$ is finite $\Rightarrow V$ is complete (for the product norm for some basis)

(because $\mathbb{Q}_p$ is locally compact).

(because $\mathbb{Q}_p$ is locally compact).

But $K \subset V \Rightarrow |K_p = V$. □

Theorem (product formula).

$\forall x \in K^\times$, $K/\mathbb{Q}$ finite extension, $\prod_{v \in M_K} |x|_v^{n_v} = 1$

Proof: $M_K = M_{K,\infty} \sqcup \bigsqcup_{p \in P} M_{K,p}$. To make sense of the ∞ product, we need to show that:

$\{v \in M_K : |x|_v \neq 1\}$ is finite.

$P \in \mathbb{Q}[T]$ minimal monic polynomial. $P(T) = T^d + a_{d-1}T^{d-1} + \dots + a_0$.

$P_0 = \{p \in P,\ |a_i|_p = 1 \text{ or } 0\}$. $M_{\mathbb{Q}} \setminus P_0$ is finite.

If $v \in M_{K,p}$, $p \in P_0$, then $|\cdot|_v = 1$ (some argument using symmetric polynomials)

Then, $\prod_{v \in M_K} |x|_v^{n_v} = \prod_{p \in P_0} \prod_{v \in M_{K,p}} |x|_v^{n_v} \cdot \prod_{v \in M_{K,\infty}} |x|_v^{n_v} = \prod_{w \in M_{\mathbb{Q}}} |N_{K/\mathbb{Q}}(x)|_w$.

For any rational number $y \in \mathbb{Q}$, $\prod_{w \in M_{\mathbb{Q}}} |y|_w = 1$ (Claim to prove)

$y = \pm \prod_{p \in P} p^{v_p(y)}$ $\quad v_p(y) \in \mathbb{Z}$, $\quad |v|_p = p^{-v_p(y)}$ $\quad \forall p \in P$.

$|y|_\infty = \prod_{p \in P} p^{v_p(y)}$

Definition of the height.

$x \in \mathbb{Q}^{alg}$. Let K be a number field s.t. $x \in K$. We set

$h_K(x) = \frac{1}{[K:\mathbb{Q}]} \cdot \sum_{v \in M_K} n_v \log^+ |x|_v$ $\quad n_v = [K_v : \mathbb{Q}_v]$

For $x \in \mathbb{Q}$, $h(x) = \sum_{v \in M_{\mathbb{Q}}} \log^+ |x|_v$. $\quad \log^+ f = \max\{0, \log f\}$.

Rem: the product formula shows that $\sum_{v \in M_K} n_v \log |x|_v = 0 \quad \forall\, x \in K^\times$

↑ without the $+$.

Rem: $h_K(x)$ does not depend on K, we'll see it next time.