Théorie des Nombres TD2

M2 AAG 2021-2022

Warm-up

1. Let L/K be an algebraic extension of complete non-archimedian fields. Show that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.
2. Show that if L/K is a finite extension of local fields, then L/K is totally ramified if and only if $\mathcal{O}_L = \mathcal{O}_K[\pi]$ with π a root of an Eisenstein polynomial in $K[X]$.
3. Show that if K is a finite extension of $\mathbb{C}((t))$ then there exists n such that $K \simeq \mathbb{C}((t^{1/n}))$.

Exercices

Exercice 1. Let $L = \overline{\mathbf{Q}_p}$ be an algebraic closure of $\mathbf{Q}_p$.

1. Show that the p-adic absolute value $|\cdot|_p$ extends uniquely to L.

We are going to give two proofs that L is not complete.

For all prime number $\ell > 2$ let ζ_ℓ be a primitive ℓ-th root of 1. Assume that L is complete and let Liouville's number

$$\alpha = \sum_{\ell \notin \{2,p\}} \zeta_\ell p^\ell.$$

2. Show that the series converges in L.

Let $K = \mathbf{Q}_p(\alpha) \subset L$. Let ℓ_1 the least prime $\notin \{2, p\}$ such that $\zeta_{\ell_1} \notin K$.

3. Show that $\zeta_{\ell_1} \in \mathcal{O}_L$ and that there exists $\beta \in \mathcal{O}_K$ satisfying $\beta \equiv \zeta_{\ell_1} \mod p$.
4. Deduce that K contains a ℓ_1-th root of 1 congruent to ζ_{ℓ_1} modulo p.
5. For $\ell \neq p$, show that roots of unity of order ℓ are distinct modulo p. Deduce that $\zeta_{\ell_1} \in K$ and thus that the residue field of K is infinite.
6. Get a contradiction.

Second proof :

7. For $d \geqslant 1$, show that $\mathbf{Q}_p$ has only a finite number of non isomorphic extensions of degree d.

8. For $d \geqslant 1$, let $L_d \subset L$ the compositum of all degree $\leqslant d$ extensions of $\mathbb{Q}_p$. Show that L_d is a closed subset of L with empty interior.

9. Conclude.

Exercice 2. Show that $\mathbb{C}_p$ is not spherically complete. *Hint : Choose a sequence* $(a_n)_n$ *which is dense in* $\mathbb{C}_p$.

Exercice 3 (Ax-Sen-Tate). Let K be a complete non archimedean field. Let $K^{sep} \subset \overline{K}$ a separable and algebraic closure. Let $G_K = \mathrm{Gal}(\overline{K}/K) = \mathrm{Gal}(K^{sep}/K)$ the Galois group.

1. Show that the action of G_K extends to $\widehat{\overline{K}}$.

2. Show that if M/L is a separable extension of fields, then $\mathrm{tr}_{M/L} = M \longrightarrow L$ is surjective.

Our goal is to prove the following theorem of Ax-Sen-Tate,

Theorem 1 (Ax-Sen-Tate). *Let H be a closed subgroup of G_K. Then $(\widehat{\overline{K}})^H$ is the completion of $\overline{K}^H$, i.e. $\overline{K}^H$ is dense in $(\widehat{\overline{K}})^H$.*

The reader who wants to focus of the case of extensions of $\mathbb{Q}_p$ can forget about questions 3.-6. We introduce $L = \overline{K}^H$. If $\alpha \in \overline{K}$, denote $\Delta_L(\alpha) = \inf_{\sigma \in H} v(\sigma(\alpha) - \alpha)$, the *diameter* of α w.r.t. L. Clearly, $\Delta_L(\alpha) = 0$ iff $\alpha \in L$.

3. Show that L is perfect.

To prove the theorem, we will need to first prove the following theorem of Ax

Theorem 2 (Ax). *There exists a constant C such that for $\alpha \in \overline{K}$, there is $a \in L$ such that $v(\alpha - a) \geqslant \Delta_L(\alpha) - C$.*

Fix a α and denote $M = L(\alpha)$, it is a finite separable extension of L by the previous question.

4. Assume K is of equal characteristics zero. Show that setting $a = \mathrm{tr}_{M/L}(\frac{1}{[M:L]}\alpha)$ we have
$$v(a - \alpha) \geqslant \Delta_L(\alpha).$$

5. Now assume K is of equal characteristics $p > 0$. Show that for all $\delta > 0$ there exists $y \in M$ such that $v(y) > -\delta$ and $\mathrm{tr}_{M/L}(y) = 1$.

6. Setting $a = \mathrm{tr}_{M/L}(y\alpha)$, show that for all $\delta > 0$ there exists $a \in L$ such that
$$v(a - \alpha) \geqslant -\delta + \Delta_L(\alpha).$$

For the next two questions, we assume that K is of characteristic zero and its residue field is of characteristic $p > 0$. We also assume $v(p) = 1$.

7. Let $P \in \overline{K}[X]$ unitary of degree n such that all its roots α satisfies $v(\alpha) \geqslant u$. Show that
   (a) if $n = p^k d, p \nmid d$ and $d \geqslant 2$, then $P^{(p^k)}$ has at least one root β such that $v(\beta) \geqslant u$.
   (b) if $n = p^{k+1}$ for $k \geqslant 0$, then $P^{(p^k)}$ has at least one root β such that $v(\beta) \geqslant u - \frac{1}{p^{k+1}-p^k}$.

8. Denote $[L(\alpha) : L] = n$ and $\ell(n)$ the maximal power such that $p^{\ell(n)} \leqslant n$. Prove that there exists $a \in L$ such that

$$v_p(\alpha - a) \geqslant \Delta_L(\alpha) - \sum_{i=1}^{\ell(n)} \frac{1}{p^i - p^{i-1}}.$$

   In particular we can prove Ax's theorem with $C = \frac{p}{(p-1)^2}$. ***Hint : We can use strong induction on n.***

9. Prove the theorem of Ax-Sen-Tate.

10. What is $(\mathbb{C}_p)^{G_{\mathbb{Q}_p}}$?

Exercice 4. Let A be a discrete valuation ring (DVR), i.e. a ring with a discrete (non trivial) valuation[1], K its fraction field and denote by $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ the valuation. If $P = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ with $a_0 \neq 0$, we define $\mathcal{N}\mathrm{ewt}_P$ the Newton polygone of P as the unique maximal continuous fonction, piecewise linear with breakpoint at integral abscissas, $\mathcal{N}\mathrm{ewt}_P : [0, d] \longrightarrow \mathbb{R}$ such that

- $\mathcal{N}\mathrm{ewt}_P(0) = v(a_0)$ et $\mathcal{N}\mathrm{ewt}_P(d) = v(a_d)$.
- $\mathcal{N}\mathrm{ewt}_P(j) \leqslant v(a_j) \forall j \in \{0, \ldots, d\}$.
- The graph of $\mathcal{N}\mathrm{ewt}_P$ is convex (i.e. has increasing slopes).

Another way to say it is that $\mathcal{N}\mathrm{ewt}_P$ is the ***lower convex hull*** of points $(i, v(a_i))$.

1. Draw the polygon of $X^3 - X^2 - 2X + 8 \in \mathbb{Q}_2[X]$ and of $X^3 + 2X^2 - 2X + 4 \in \mathbb{Q}_2[X]$.

2. Assume given a factorisation $P(X) = \prod_{i=1}^{d}(X - x_i) \in K[X], x_i \neq 0$ and denote $\gamma_1 \leqslant \gamma_2 \leqslant \cdots \leqslant \gamma_d$ the slopes of $\mathcal{N}\mathrm{ewt}_P$ (with multiplicity). Show that, up to reorder the x_i, we have $\gamma_i = -v(x_i)$. ***Hint : we can introduce the piecewise linear function on $[0, d]$ starting at $v(a_0)$ and with increasing slopes $v(x_i)$ (with multiplicities) and try to compare its position to $\mathcal{N}\mathrm{ewt}_P$***

3. Deduce that if $P \in K[X]$ is irreducible, then its Newton polygon is a line. What are the possible reductions of P if $P \in \mathcal{O}_K[X]$ and irreducible in $K[X]$?

[1] Prove if you want that it is the same as an integral, local, dimension one ring

4. Let $P = X^d + a_1 X^{d-1} + \dots + a_d \in K[X]$ with $a_d \neq 0$ a separable polynomial (or assume K of characteristic zero). Assume that the slopes of $\mathcal{N}\mathrm{ewt}_P$ are $\lambda_1 < \dots < \lambda_k$, with multiplicities $w_1, \dots, w_k$. Then there exists a unique factorisation $P(X) = \prod_{i=1}^k g_i(X)$ with g_i unitary, $\deg g_i = w_i$ et $\mathcal{N}\mathrm{ewt}_{g_i}$ isoclinic of slope λ_i. Can you extend it to the general case ?

5. Show that $X^3 - X^2 - 2X + 8$ has three distinct roots in $\mathbb{Q}_2$.

6. Deduce the following version of Hensel's Lemma : if $P \in \mathcal{O}_K$, such that

$$P \equiv \overline{h}\overline{g} \pmod{\mathfrak{m}_K},$$

with $\overline{h}, \overline{g}$ coprime, then there exists $h, g \in \mathcal{O}_K[X]$ such that $P = hg$ and $h \equiv \overline{h}, g \equiv \overline{g} \pmod{\mathfrak{m}_K}$. ***Hint : We can start by writing*** $P = \prod_{i=1}^r P_i$ ***as a product of irreducible***

7. Prove Eisenstein-Dumas criterion :

Theorem 5. *Let* $P \in K[X]$*. Assume its Newton polygon is a line from* $(0, n)$ *to* $(d, 0)$ *with* $n, d = 1$*. Then* P *is irreducible.*

Deduce the classical Eisenstein criterion.