University of Bordeaux **Number Theory**
M2 AGNT/ALGANT, 2025–2026

Exercise sheet n°5

Local fields

Exercice 1 – Let K be a complete discrete valuation field with *perfect* residue field k_K of characteristic p.

1) Show that if $a, b \in O_K$ are such that $a \equiv b \pmod{\mathfrak{m}_K}$, then $a^{p^n} \equiv b^{p^n} \pmod{\mathfrak{m}_K^n}$ for each $n \geq 1$.

2) Let $\xi \in k_K$. For any $n \geq 1$, let $a_n \in O_K$ denote a lifting of $\xi^{p^{-n}}$ under the reduction map $O_K \to k_K$. Show that the sequence $(a_n^{p^n})_n$ converges in O_K to an element $[\xi]$ which does not depend on the choice of $(a_n)_n$.

3) Show that $[\xi]$ is a lifting of ξ and that $[\xi_1\xi_2] = [\xi_1][\xi_2]$ for all $\xi_1, \xi_2 \in k_K$.

4) Assume, in addition, that $\mathrm{char}(k_K) = p$. Show that K contains a subfield isomorphic to k_K and that $O_K \simeq k_K[[X]]$. Deduce that K is isomorphic to $k_K((X))$.

Exercice 2 – Let K be a complete discrete valued field. Fix an algebraic closure $\overline{K}/K$. Let k/k_K be a Galois extension.

1) Recall why there exists a unique subfield $L \subset \overline{K}$ such that L/K is unramified with residue field k.

2) Show that L/K is a Galois extension and $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(k/k_K)$.

Exercice 3 – Let K be a complete discrete valued field. Let $L, M \subset \overline{K}$ be finite extensions of K. Assume that L/K is unramified. Show that LM/M is unramified.

Exercice 4 – Let $L \subset \overline{\mathbf{Q}}_p$ be a finite extension of $\mathbf{Q}_p$. Prove that there exists a finite extension K of $\mathbf{Q}$ such that $K \subset L$, $[K : \mathbf{Q}] = [L : \mathbf{Q}_p]$, and $L = K\mathbf{Q}_p$.

Exercice 5 – Let $P(X) = X^3 - 17 \in \mathbf{Q}_3[X]$.

1) Compute $P(5)$ and give the degrees of the irreducible factors of P in $\mathbf{Q}_3[X]$.

2) Show that the 3-adic absolute value on $\mathbf{Q}$ has exactly two extensions to $\mathbf{Q}[\sqrt[3]{17}]$.

Exercice 6 – Let C denote the completion of an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. Let $v : C \to \mathbf{R} \cup \{+\infty\}$ denote the extension to C of the standard p-adic valuation on $\mathbf{Q}_p$; hence $v(p) = 1$. We write O_C for its ring of integers and $\mathfrak{m}_C$ for the maximal ideal of O_C. Consider the formal power series

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}, \qquad \log(1+X) = \sum_{n=0}^{\infty} (-1)^{n+1} \frac{X^n}{n}.$$

We assume that the following formulas hold true in $\mathbf{Q}[[X,Y]]$:

$\exp(X+Y) = \exp(X)\exp(Y), \quad \log((1+X)(1+Y) = \log(1+X)+\log(1+Y).$

(They can be proved by a direct computation involving binomial coefficients.)

1) Show that $\log(1+X)$ converges on $\mathfrak{m}_C$.

2) Let $U_C^1 = \{x \in O_C \mid x \equiv 1 \pmod{\mathfrak{m}_C}\}$. Show that the rule $x \mapsto \log(x)$ defines a morphism $\log : (U_C^1, *) \to (C, +)$.

3) Show that the series $\exp(X)$ converges on the set

$$\left\{ x \in O_C \mid v(x) > \frac{1}{p-1} \right\}.$$

4) Show that the multiplicative group $(1+p^2O_C)^*$ is isomorphic to the additive group p^2O_C.

5) Let $\mu_{p^\infty} = \overset{\infty}{\underset{n}{\cup}} \mu_{p^n}$, where μ_{p^n} denotes the group of p^nth roots of unity. Show that $\ker(\log) = \mu_{p^\infty}$.

Exercice 7 – Let K be a finite extension of $\mathbf{Q}_p$ with the residue field k_K. Fix a uniformizer π of K and denote by v_K the discrete valuation on K such that $v_K(\pi) = 1$. Let e denote the ramification index and f the residue degree of K over $\mathbf{Q}_p$. For each $i \geq 1$, set $U_K^{(i)} = \{x \in K \mid v_K(x-1) \geq i\}$.

1) Show that for each $i \geq 1$, the set U_K^i is a multiplicative subgroup of U_K.

2) Show that $U_K/U_K^{(1)}$ is isomorphic to the multiplicative group k_K^*.

3) Show that $U_K^{(i)}/U_K^{(i+1)}$ is isomorphic to the additive group $(k_K, +)$ for each $i \geq 1$.

4) Let $a \in \mathbf{Z}_p$. Write a as $a = \lim_{n\to+\infty} a_n$ with $a_n \in \mathbf{Z}$. Show that for each $x \in U_K^{(1)}$, the sequence x^{a_n} converges to some element $x^a \in U_K^{(1)}$, which does not depend on the choice of (a_n). Check that the rule $(a, x) \mapsto x^a$ equips $U_K^{(1)}$ with a structure of $\mathbf{Z}_p$-module.

5) Show that the group $U_K^{(i)p} = \{x^p \mid x \in U_K^{(i)}\}$ coincides with $U_K^{(i+e)}$ if $i > \frac{e}{p-1}$.

6) Let $\{\theta_i\}_{i=1}^f$ denote a lifting of a basis of k_K over $\mathbf{F}_p$ under the reduction map $O_K \to k_K$. Show that the family

$$\{1 + \theta_i \pi^j \mid 1 \leq i \leq f, \quad 1 \leq j \leq \frac{pe}{p-1}\}$$

is a system of generators of the $\mathbf{Z}_p$-module $U_K^{(1)}$.

Exercice 8 –

1) Show that $U_{\mathbf{Q}_p}^{(1)}$ is a free $\mathbf{Z}_p$-module of rank one if $p \neq 2$. Show that $U_{\mathbf{Q}_2}^{(1)} = U_{\mathbf{Q}_2}$ is isomorphic to $\mathbf{Z}_2 \times \{\pm 1\}$ as $\mathbf{Z}_2$-module.

2) Compute the index $(\mathbf{Q}_p^* : (\mathbf{Q}_p^*)^2)$ for each prime p.

3) Show that $\mathbf{Q}_p$ has 3 quadratic extensions if $p \geq 3$ and 7 quadratic extensions if $p = 2$.

Exercice 9 – Show that there exists exactly two non-isomorphic extensions of $\mathbf{Q}_2$ of degree 3.