Théorie des nombres - TD6

Exercise 1 (p-adic remarks). 1. Show that for all $N \in \mathbb{N}_{>1}$, we have an isomorphism

$$\operatorname{proj}\lim_{i \geqslant 0} \mathbb{Z}/N^i\mathbb{Z} \simeq \prod_{p|N} \mathbb{Z}_p.$$

2. Show that for all sequence $(u_n)_{n\in\mathbb{N}}$, $u_n \in \mathbb{Q}_p$ (or in $\mathbb{Q}$), $\sum_n u_n$ converges in $\mathbb{Q}_p$ if and only if $u_n \longrightarrow 0$ in $\mathbb{Q}_p$. Find an example of a sequence of rational whose sum converge in $\mathbb{Q}_p$ but not in $\mathbb{R}$.
3. Show that writing $x = \sum_i a_i p^i \in \mathbb{Q}_p$, with $a_i \in \{0, \dots, p-1\}$ we have $x \in \mathbb{Q}$ if and only if the sequence $(a_i)_i$ is eventually periodic.
4. Show that there exists a continuous surjection $\mathbb{Z}_p \longrightarrow [0,1]$. Is there a continuous surjection $[0,1] \longrightarrow \mathbb{Z}_p$?

Exercise 2. 1. For which $x \in \mathbb{Q}_p$ does the following series converges

$$\exp(x) = \sum_{n \geqslant 0} \frac{x^n}{n!}?$$

2. For which $x \in \mathbb{Q}_p$ does the following series converges

$$\log(x) = \sum_{n \geqslant 1} \frac{(-1)^{n-1}}{n}(x-1)^n?$$

3. Generalize these results for (finite) extensions of $\mathbb{Q}_p$.
4. Show that $\exp(x+w) = \exp(x)\exp(w)$ for $x, w \in 2p\mathbb{Z}_p$. *Hint : You can first prove that if a_n, b_m are such that $\sum_n a_n$ and $\sum_m b_n$ converges then $\sum_n \sum_m a_n b_m = \sum_m \sum_n a_n b_m = \sum_\ell (\sum_{n,m|\ n+m=\ell} a_n b_m)$.*
5. Show that $\log(xw) = \log(x) + \log(w)$ for $x, w \in 1 + p\mathbb{Z}_p$.

Exercise 3 (Krasner). Let K be a p-adic field and $\overline{K}$ a separable (algebraic) closure.

1. Let $x \in \overline{K}$ with conjugates $x_2, \dots, x_n \in \overline{K}$. Let $y \in \overline{K}$ such that $|y - x| < |y - x_i|$ for all $i \in \{2, \dots, n\}$. Then show that $K(x) \subset K(y)$.
2. Recall that $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}_p$ in K. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_K[X]$ be a monic irreducible polynomial, and α a root of f. Show that there exists $N \in \mathbb{N}$ such that if $g = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in \mathcal{O}_K[X]$ satisfies $f \equiv g \pmod{p}^N$, then g is irreducible, and there exists a root β of g such that $K(\alpha) = K(\beta)$.
3. Deduce that there are only finitely many extensions of $\mathbb{Q}_p$ of degree n.

Exercise 4 (Exposant 2 extensions of $\mathbb{Q}_p$.). Show that $\mathbb{Q}_p$ has 3 (up to isomorphism) quadratic extensions for $p \neq 2$ and $\mathbb{Q}_2$ has 7 quadratic extensions. Show that there is a unique extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$ (up to isomorphism). What can you say for $\mathbb{Z}/p\mathbb{Z}$ extensions of $\mathbb{Q}_p$?

Exercise 5 ($\overline{K}/K$ is prosolvable). Let $K/\mathbb{Q}_p$ a finite extension. The goal is to prove that any finite (Galois) extension L/K is solvable.

1. For $\sigma \in G = \mathrm{Gal}(L/K)$ denote by σ_n its restriction/quotient to $\mathcal{O}_L/\pi_L^{n+1}$. Show that if we denote G_n the kernel of $\sigma \mapsto \sigma_n$ then G_n is a decreasing sequence of normal subgroup which is eventually stationary.
2. Identify G_0. What is its index in G?
3. Denote $U_0 = \mathcal{O}_L^\times$ and by $U_n = 1 + (\pi_L^n) \subset L^\times$ for $n \geqslant 1$. Construct a morphism
$$G_n \longrightarrow U_n/U_{n+1}$$
which is independant of the choice of π_L.
4. Deduce that G is solvable. *Hint : prove that* $G_n/G_{n+1} \hookrightarrow U_n/U_{n+1}$.

Remark 0.1. The analogous result for $\mathbb{Q}$, or any number field, is completely false! This is one aspect for which the local situation ($\mathbb{Q}_p$) is way easier that then global one ($\mathbb{Q}$).

Exercise 6 (The extension $\mathbb{Q}_p(\zeta_{p^\infty})$)**.** Let $\zeta_p^\infty = (\zeta_{p^n})_n$ with ζ_{p^n} a primitive p^n-th roots of 1, such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. Denote $\mathbb{Q}_p(\zeta_{p^\infty}) = \cup_{n \geqslant 0}\mathbb{Q}_p(\zeta_{p^n})$.

1. Show that p is a norm in $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$
2. Deduce that $\mathbb{Q}_p(\zeta_{p^\infty})$ is the subfield of $\mathbb{Q}_p^{ab}$ fixed by $\mathrm{rec}(p)$.