

Exercise sheet n°3

p -adic fields, polynomials over non-Archimedean fields

Exercise 1 –

- 1) Determine the p -adic expansion of -2 .
- 2) Determine the 5-adic expansion of $-2/3$.
- 3) Show that a p -adic integer with an eventually periodic p -adic expansion (that is, $a_{n+m} = a_n$ for some positive m and all sufficiently large n) belongs to $\mathbb{Q}$.
- 4) Show that conversely, every $x \in \mathbb{Z}_p \cap \mathbb{Q}$ has an eventually periodic p -adic expansion.

Exercise 2 – Let $\overline{\mathbb{Q}_p}$ is an algebraic closure of $\mathbb{Q}_p$ and let ζ_3 denote a primitive cubic root of unity.

- 1) Show that $\zeta_3 \notin \mathbb{Q}_3$.
- 2) What are the degrees of the irreducible factors of the polynomial $f(X) = X^3 - 17$ in $\mathbb{Q}_3[X]$? (Hint : compute $f(5)$.)

Exercise 3 – In this exercise, we show that the polynomial $(X^2 - 13)(X^2 - 17)(X^2 - 221)$ has a root in every $\mathbb{Q}_p$. Since it has no root in $\mathbb{Q}$, this provides a counter-example to the "local-global principle for polynomials in one variable".

- 1) Show that 17 is a square in $\mathbb{Q}_2$ and in $\mathbb{Q}_{13}$, and that 13 is a square in $\mathbb{Q}_{17}$.
- 2) Let p be a prime distinct from 2, 13, 17. Using properties of Legendre symbol, show that one of the numbers 13, 17, 221 is a square in $\mathbb{Q}_p$.
- 3) Conclude.

Exercise 4 – Let $\mathbb{Z}_p^*$ denote the group of units of $\mathbb{Z}_p$.

- 1) Show that each $x \in \mathbb{Z}_p^*$ can be uniquely written as $x = \xi u$, where $\xi^{p-1} = 1$ and $u \equiv 1 \pmod{p}$.
- 2) Let $a \in \mathbb{Z}_p^*$ be such that $a \equiv 1 \pmod{p}$. Show that for any m coprime with p , there exists exactly one $b \in \mathbb{Z}_p^*$ such that $b^m = a$ and $b \equiv 1 \pmod{p}$.
- 3) Show that for $p \neq 2$, the only roots of unity contained in $\mathbb{Q}_p$ are the $(p-1)$ th roots of unity. Show that the only roots of unity in $\mathbb{Q}_2$ are ± 1 .
- 4) Let m be a positive integer coprime with $p(p-1)$. Show that every p -adic unit is an m -th power in $\mathbb{Q}_p$.

Exercise 5 –

- 1) Prove that the field $\mathbb{R}$ has no nontrivial automorphisms.

2) Prove that the field $\mathbb{Q}_p$ has no nontrivial automorphisms.

Exercise 6 –

1) Prove that the fields $\mathbb{R}$ and $\mathbb{Q}_p$ are not isomorphic.

2) Prove that the fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic if $p \neq q$.

Exercise 7 – Let $(K, |\cdot|)$ be a non-Archimedean field and let $\widehat{K}$ denote the completion of K . Show that $|\widehat{K}^*| = |K^*|$ and that the residue fields of K and $\widehat{K}$ are isomorphic.

Exercise 8 – Let $(K, |\cdot|)$ be a complete non-Archimedean field and let $f(X) = \sum_{k=0}^n a_k X^k$ be an irreducible monic polynomial. Show that $|a_k|^n \leq |a_0|^{n-k}$ for all $0 \leq k \leq n-1$.

Exercise 9 – Let $(K, |\cdot|)$ be a complete ultrametric valued field and let $f(X)$ be a monic polynomial. Prove that if $f(X)$ is irreducible in $O_K[X]$, its image in $k_K[X]$ is the power of an irreducible polynomial.

Exercise 10 – Check that the Eisenstein criterion holds for any discrete valuation ring. Namely, let A be a DVR and let π denote a uniformizer of A . Assume that the coefficients of a monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ satisfy the following properties : a) $\pi \mid a_i$ for all $0 \leq i \leq n-1$; b) $\pi^2 \nmid a_0$. Then $f(X)$ is irreducible over the field of fractions of A .

Exercise 11 – Let p be a prime number.

1) Show that the polynomial $\Phi_p(X) = \frac{X^p-1}{X-1}$ is irreducible over $\mathbb{Q}_p$.

2) Show that, more generally, $\Phi_{p^n}(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$ is irreducible over $\mathbb{Q}_p$ for all $n \geq 1$.

Exercise 12 – (**Newton polygons**) Let K be a field complete for a nontrivial valuation v . Recall that v has a unique extension to the algebraic closure $\overline{K}$ of K , which we denote again by v . Let $f(X) = \sum_{k=0}^n a_k X^k \in K[X]$

be a polynomial. Assume that $a_0, a_n \neq 0$. To each nonzero term $a_k X^k$ we attach the point $(k, v(a_k)) \in \mathbf{R}^2$, and denote by D the set of such points. The Newton polygon of f is defined as the lower convex envelope of D . It consists of line segments joining two points of D . Assume that the segment S joining the points $(j, v(a_j))$ and $(i, v(a_i))$ with $j > i$ appears in the Newton polygon, and call the slope of S the number

$$s = \frac{v(a_j) - v(a_i)}{j - i}.$$

Show that f has exactly $j - i$ roots of value $-s$.