BMST 2025: p-ADIC NUMBERS
EXERCISE SHEET 2

Exercise 1. (1) Let $p \neq 2$ be a prime and let $u \in \mathbb{Z}_p$ such that $u \equiv 1 \mod (p)$. Show that for any $n \geq 1$ not divisible by p, u is an n-th power in $\mathbb{Z}_p^\times$.

(2) Let $p \neq 2$. Show that there is an element of $\mathbb{Z}/(p^2)$ that is not a p-th power; deduce a counterexample to the above for $n = p$. (*Hint*: you might want to show that if $v \equiv 1 \mod (p)$ then $v^p \equiv 1 \mod (p^2)$.)

(3) Let $p \neq 2$ be a prime and let $u \in \mathbb{Z}_p$ such that $u \equiv 1 \mod (p^2)$. Show that u has a p-th root. (*Hint*: Write $u = 1 + kp^2$ and consider the element $1 + kp$.)

Remark. We actually have the sharper result that u has a p-th root if and only if u is a p-th power modulo p^2.

Exercise 2. (1) Let $u \in \mathbb{Q}_p \setminus \{0\}$ and write $u = p^k v$, $k \in \mathbb{Z}$, $v \in \mathbb{Z}_p^\times$. Show that u is a square if and only if

(i) for p odd, k is even and v is a square modulo p;

(ii) for $p = 2$, k is even and $v \equiv 1 \mod (8)$.

(2) (If you know about quadratic residues) Denote by $(\mathbb{Q}_p^\times)^2$ the multiplicative group of non-zero elements which are squares. Show that for $p \neq 2$, $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(3) Show that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

Exercise 3. Factor the polynomial $P(X) = X^4 - 7X^3 + 2X^2 + 2X + 1 \in \mathbb{Z}[X]$ into a product of irreducible polynomials over $\mathbb{F}_3$. Show that P has a root in $\mathbb{Z}_3$.

Exercise 4 (If you know about quadratic residues)**.** Show that the equation $(X^2 - 2)(X^2 - 17)(X^2 - 34)$ has roots in $\mathbb{Q}_p$ for all p prime and in $\mathbb{R}$, but not in $\mathbb{Q}$. (*Hint*: first treat the case of $\mathbb{R}$ and $\mathbb{Q}_2$, then do a general argument for $\mathbb{Q}_p$ using that $34 = 2 \times 17$.)

In a non-archimedean field with a discrete valuation, a generator π of the maximal ideal $\mathfrak{m}$, i.e. an element of maximal absolute value strictly less than 1, is called a uniformizer.

Exercise 5. (1) Let K be a complete non-archimedean field with a discrete valuation. Let π be a uniformizer. Show the following version of Eisenstein's criterion: for $f = \sum_{k=0}^{n} a_k X^k \in \mathcal{O}_K[X]$, if $a_n \not\equiv 0 \mod (\pi)$, $a_k \equiv 0 \mod (\pi)$ for all $k < n$ and $a_0 \not\equiv 0 \mod (\pi^2)$ then f is irreducible in $\mathcal{O}_K[X]$ and in $K[X]$. (for that last statement, you will need Gauss' lemma)

(2) Deduce that the p-th cyclotomic polynomial Φ_p is irreducible over $\mathbb{Q}_p$ for $p \neq 2$ prime. (*Hint*: the usual trick is to look at $\Phi_p(X+1)$.)

Exercise 6 (Uses Hensel's lemma for polynomials and the Gauss norm)**.** Let K be a complete non-archimedean field. Show that if $f \in \mathcal{O}_K[X]$ is monic, then

(1) f is irreducible in $\mathcal{O}_K[X]$ if and only if it is irreducible in $K[X]$;
(2) if f is irreducible modulo $\mathfrak{m}$, then f is irreducible in $\mathcal{O}_K[X]$;
(3) conversely, if f is irreducible in $\mathcal{O}_K[X]$ and has no multiple roots modulo $\mathfrak{m}$, then it is irreducible modulo $\mathfrak{m}$.

Exercise 7. Let K be a complete normed field and consider the subring $\mathcal{O}_K\langle T\rangle := \left\{ f = \sum a_k T^k \in \mathcal{O}_K[[T]], \quad |a_k| \xrightarrow[n\to\infty]{} 0 \right\}$ of formal power series with coefficients in $\mathcal{O}_K$ converging on the closed unit ball, i.e. on $\mathcal{O}_K$.

(1) Show that for any $f \in \mathcal{O}_K\langle T\rangle$, $f(X+Y) = f(X) + f'(X)Y + R(X,Y)Y^2$ for some $Y \in \mathcal{O}_K\langle T\rangle$.
(2) Show that for any $f \in \mathcal{O}_K\langle T\rangle$ and $x, y \in \mathcal{O}_K$, we have
$$|f(x) - f(y)| \leq |x - y|.$$
In particular f defines a uniformly continuous function $\mathcal{O}_K \to K$.
(3) Deduce that Hensel's lemma applies to formal power series in $\mathcal{O}_K\langle T\rangle$.

Exercise 8 (Canonical lifts)**.** Let p be a prime and let K be a non-archimedean normed field such that $p \in \mathfrak{m}$. Recall that for $1 \leq k \leq p$, the binomial coefficient $\binom{p}{k}$ is divisible by p.

(1) Show that for $x, y \in \mathcal{O}_K$, if $|x-y| < 1$ then for $t = \max(|p|, |x-y|) < 1$ we have$|x^{p^k} - y^{p^k}| \leq t^{k+1}$ for all $k \geq 1$.
(2) Reformulate this in terms of congruences in the case where the valuation is discrete.
(3) Suppose that K is complete and that the residue field k of K is perfect, that is such that any $x \in k$ has a (unique) p-th root (i.e. $y \mapsto y^p$ is an automorphism of k, since $p = 0$ in k). For $x \in k$, let $x^{p^{-k}}$ denote its unique p^k-th root. For each $k \in \mathbb{N}$, choose a lift $\widetilde{x^{p^{-k}}} \in \mathcal{O}_K$ of $x^{p^{-k}}$. Show that the expression
$$\tau(x) := \lim_{k\to\infty} \left(\widetilde{x^{p^{-k}}}\right)^{p^k}$$
is well-defined and independent of the choice of lifts.
(4) Deduce that the map $\tau : k \to \mathcal{O}_K$ is a multiplicative injection with image a complete set of representative of classes modulo $\mathfrak{m}$.
(5) Show that if K is of characteristic p, τ is a field embedding of k in K.
(6) If the valuation on K is discrete, let $\pi \in \mathfrak{m}$ be a uniformizer. Show that every element of $\mathcal{O}_K$ has a unique representation in base π with coefficients in the image of τ.

(7) Deduce that if K is a complete non-archimedean normed field of characteristic p with a discrete valuation, there are isomorphisms $\mathcal{O}_K \simeq k[[X]]$ and $K \simeq k((X))$ inducing the X-adic valuation on $k[[X]]$ and $k((X))$.

Exercise 9 (End of classification of locally compact non-archimedean fields. You need to have read section 9 of the notes)**.** Let K be a locally compact non-archimedean field with a non-trivial absolute value.

(1) If K is of characteristic p prime, use the previous exercise to conclude that K is isomorphic to $\mathbb{F}_q((T))$ with the T-adic absolute value, for q a power of p.

(2) Suppose now that K is of characteristic 0. Show that K contains $\mathbb{Q}_p$ for a prime p.

(3) Using Riesz's theorem, deduce that K is a finite extension of $\mathbb{Q}_p$.