CHAPTER 2

p-adic numbers

1. Different absolute values, different distances

An absolute value $|.|_v$ defines a distance on $\mathbb{Q}$ by setting

$$d_v(x,y) = |x-y|_v.$$

This gives $\mathbb{Q}$ the structure of a topological metric space. Different absolute values yield rather different topologies:

- the trivial valuation gives the discrete topology;
- the archimedean valuation $|.|_\infty$ gives the usual topology;
- the p-adic absolute value yields the *p-adic topology.* This topology is rather different from the usual one. For instance, one has $p^n \to \infty$ (as $n \to \infty$) in the usual topology, but $p^n \to 0$ in the p-adic topology. More generally, an integer m has small p-adic absolute value if and only if it is divisible by a large power of p: for $k \geqslant 0$, one has
$$|m|_p \leqslant p^{-k} \iff p^k | m.$$
Similarly, two integers are close to each other p-adically if and only if they are congruent to each other modulo a large power of p:
$$d_p(m,n) = |m-n|_p \leqslant p^{-k} \iff p^k | m-n \Leftrightarrow m \equiv n \,(\mathrm{mod}\, p^k).$$
In particular, integers can be arbitrarily close to one other for the p-adic distance, while they are always separated by at least 1 for the usual distance.

Exercise 2.1. Prove that equivalent valuations yield the same topology on $\mathbb{Q}$ and that inequivalent valuation yield distinct topologies.

As we know already the field of real numbers $\mathbb{R}$ is obtained by completion of the metric space $(\mathbb{Q}, d_\infty)$. In this chapter, we discuss what happens when we replace the usual distance by a p-adic distance.

2. Normed rings and their ompletion

Let us first recall the following

Definition 2.1. *Let (X, d_X) be metric space. A completion of (X, d_X), is a metric space $(\overline{X}, d_{\overline{X}})$ with is complete (i.e., every Cauchy sequence in $\overline{X}$ is convergent in $\overline{X}$) together with an isometry $(X, d_X) \hookrightarrow (\overline{X}, d_{\overline{X}})$ with dense image.*

A completion always exists, and is unique up to isometry. It can be constructed as the space of equivalence classes of Cauchy sequences $(x_n)_{n\geqslant 1},\ x_n \in X$, two Cauchy sequences $(x_n)_n,\ (y_n)_n$ being equivalent if and only if $d_X(x_n, y_n) \to 0$. The inclusion $X \hookrightarrow \overline{X}$ is then given by the map

$$x \in X \mapsto \text{equivalence class of the constant sequence } (x)_n.$$

The completion has the following property

PROPOSITION 2.1. *Any (uniformly) continuous map $X \to Y$ to a complete metric space (Y, d_Y) extends uniquely to a (uniformly) continuous map $\overline{X} \to Y$.*

2.1. Normed rings. A normed ring $(R, |.|)$ is a unital ring equipped with a *norm*, that is a map

$$|.| : R \mapsto \mathbb{R}_{\geqslant 0}$$

such that

- $|x| = 0 \Leftrightarrow x = 0$,
- $|x + y| \leqslant |x| + |y|$,
- $|xy| \leqslant |x||y|$.

The norm defines a distance on R given by

$$d_R(x, y) = |x - y|.$$

Let $(R^\times, \times)$ denote the group of units (i.e., invertible elements) of R. Recall that R is a *field* if $R^\times = R - \{0\}$.

PROPOSITION 2.2. *The addition, multiplication, and inversion maps*

$$+, \times : R \times R \to R,$$

$$(\cdot)^{-1} : R^\times \to R^\times$$

are continuous with respect to to the corresponding topology.

EXERCISE 2.1. Prove the above proposition.

We may give the completion $\overline{R}$ of a normed ring $(R, |.|)$ the structure of a ring by defining the addition and multiplication laws on $\overline{R}$ to be those induced by elementwise addition and multiplication on the space of Cauchy sequences, i.e.,

$$(a_n)_n + (b_n)_n = (a_n + b_n)_n,\ (a_n)_n \times (b_n)_n = (a_n \times b_n)_n.$$

PROPOSITION 2.3. *The completion of a normed ring $(R, |.|)$ is a normed ring for the norm*

$$|x| = d_{\overline{R}}(0, x).$$

If R is a field, then $\overline{R}$ is also a field.

PROOF. This is a consequence of Proposition 2.1 applied to the addition, multiplication and inversion maps using Proposition 2.2. □

One reason to work with rings is that one can also consider series. Let us say that a series $\sum_n a_n$ with terms $a_n \in R$ (taken over $n \in \mathbb{N}$, say) is *absolutely convergent* if $\sum_n |a_n| < \infty$. Recall also that $\sum a_n$ is *convergent* (in R) if its partial sums converge to some element of R.

PROPOSITION 2.4. *In a complete normed ring $(R, |.|)$, an absolutely convergent series is convergent.*

2.2. p-adic numbers. We apply the above results to the normed ring $(\mathbb{Q}, |.|_v)$ and its subring $(\mathbb{Z}, |.|_v)$ for $v = 0, \infty$ or p a prime number.

We denote the corresponding normed field and ring by $(\mathbb{Q}_v, |.|_v)$ and $(\mathbb{Z}_v, |.|_v)$. Note that $\mathbb{Z}_v$ is naturally a subring of $\mathbb{Q}_v$: in fact, it is the closure of $\mathbb{Z}$ in $\mathbb{Q}_v$.

We have

$$\mathbb{Z}_0 = \mathbb{Z}, \mathbb{Q}_0 = \mathbb{Q},\ \mathbb{Z}_\infty = \mathbb{Z},\ \mathbb{Q}_\infty = \mathbb{R}.$$

For the p-adic valuation $|\cdot|_p$ one obtains a new type of ring and field:

DEFINITION 2.2. *The completion $\mathbb{Q}_p$ of $\mathbb{Q}$ relative to $|.|_p$ is called* the field of p-adic numbers. *The subring $\mathbb{Z}_p \subset \mathbb{Q}_p$ is* the ring of p-adic integers.

3. Arithmetic and analysis on p-adic numbers

In this section we discuss in greater detail the topology and the arithmetic of $\mathbb{Q}_p$ and $\mathbb{Z}_p$. We make the following

DEFINITION 2.3. *For $r > 0$ and $x \in \mathbb{Q}_p$, the open ball of radius r centered at x is the set*

$$B_o(x, r) = \{y \in \mathbb{Q}_p, |y - x|_p < r\} = x + B_o(0, r)$$

and the closed ball is the set

$$B_c(x, r) = \{y \in \mathbb{Q}_p, |y - x|_p \leqslant r\} = x + B_c(0, r).$$

Thus for $x \in \mathbb{Q}_p$ and $r > 0$, the open and closed balls $B_o(x, r)$, $B_c(x, r)$ form a basis of respectively open and compact neighborhoods of $\mathbb{Q}_p$. In fact, since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, it suffices to consider only those $x \in \mathbb{Q}$.

3.1. p-adic expansion. Let us make the completion process a bit more explicit. Let (x_n) (taken over $n \geqslant 0$, say) be a Cauchy sequence in $(\mathbb{Z}, |.|_p)$; by definition, this sequence represents some element $x \in \mathbb{Q}_p$. For each $k \geqslant 1$, there exists $N_k \geqslant 0$ such that for $m, n \geqslant N_k$, one has $|x_m - x_n|_p \leqslant p^{-k}$, or in other words,

$$x_m \equiv x_n \,(\mathrm{mod}\, p^k).$$

We expand the integers x_m, x_n in base p, as follows:

$$x_m = \sum_{j \geqslant 0} a_{m,j} p^j,\ x_n = \sum_{j \geqslant 0} a_{n,j} p^j,\ a_{m,j},\ a_{n,j} \in [0, p-1].$$

The above congruence then implies that

$$\sum_{j \leqslant k-1} a_{m,j} p^j = \sum_{j \leqslant k-1} a_{n,j} p^j,$$

or in other words, that $a_{m,j} = a_{n,j}$ for all $m, n \geqslant N_k$ and $j \leqslant k - 1$. In particular, for each $j \geqslant 0$, the sequence $(a_{n,j})_n$ (which takes values in the finite set $\{0, \cdots, p-1\}$) is eventually stationary. We let a_j denote its limit. Consider the series

$$\sum_{j \geqslant 0} a_j p^j.$$

This series is absolutely convergent, since

$$\sum_{j \geqslant 0} |a_j p^j|_p \leqslant \sum_{j \geqslant 0} p^{-j} < \infty.$$

We claim that

$$\sum_{j\geqslant 0} a_j p^j = x.$$

Indeed, from the above discussion we have that for every $k \geqslant 1$ and $j \leqslant k-1$, there exists N_k such that for $n \geqslant N_k$, $a_{n,j} = a_j$, hence for such n,

$$|x_n - \sum_{j\leqslant k-1} a_j p^j|_p = |\sum_{j\geqslant k} a_{n,j} p^j|_p \leqslant p^{-k}.$$

In particular

$$x_{k+N_k} - \sum_{j\leqslant k-1} a_j p^j \to 0,\ k \to \infty.$$

Since $x_{N_k+k} \to x$, the claim follows. We have proven the main part of the following result:

PROPOSITION 2.5. *Any p-adic integer x can be written in a unique way as a convergent series*

$$x = \sum_{j\geqslant v_p(x)} a_j(x) p^j,\ a_j(x) \in \{0, \cdots, p-1\},\ a_{v_p(x)}(x) \neq 0.$$

Here $v_p(x)$ is the p-adic valuation of x and is defined by the formula

$$|x|_p = p^{-v_p(x)}.$$

This series is called the p-adic expansion of x and the $a_j(x)$ are the coefficients of this expansion.

PROOF. Given $x \neq 0$, we have proven that there exists a sequence $(a_k(x))_k \geqslant 0 \in \{0, \cdots, p-1\}^{\mathbb{N}}$ such that

$$x = \lim_{k\to\infty} x_k,\ x_k = \sum_{j\leqslant k} a_j(x) p^j.$$

Let $k_0 = \inf\{k \geqslant 0,\ a_k(x) \neq 0\}$; for $k \geqslant k_0$ we have

$$v_p(x_k) = k_0,\ |x_k|_p = p^{-k_0} = |x|_p,$$

which prove that the expansion of x starts precisely at the index $v_p(x)$ defined above.

Let us show that this expansion is unique. Suppose that x has two distinct expansions

$$x = \sum_{j\geqslant 0} a_j p^j = \sum_{j\geqslant 0} a'_j p^j$$

and let $j_0 = \inf\{j,\ a_j \neq a'_j\} \geqslant 0$. We consider the partial sums of these series

$$x_k = \sum_{j\leqslant k} a_j p^j,\ x'_k = \sum_{j\leqslant k} a'_j p^j;$$

for $k \geqslant j_0$ we have $|x_k - x'_k|_p = p^{-j_0}$ contradicting that $\lim_{k\to\infty} |x_k - x'_k|_p = 0$. □

We can extend this result to a full p-adic expansion of p-adic numbers:

PROPOSITION 2.6. *Any p-adic number x can be represented in a unique way by a convergent series*

$$x = \sum_{k\in\mathbb{Z}} a_k(x) p^k,\ a_k(x) \in \{0 \cdots, p-1\};$$

in this summation, it is understood that the coefficient $a_k(x)$ are zero for all $k \leqslant K_x$ for some value K_x depending on x. More precisely one has

$$|x|_p = p^{-v_p(x)},\ v_p(x) = \inf\{j \geqslant 0,\ a_j(x) \neq 0\} \in \mathbb{Z}.$$

The proof follows immediately from the following important

THEOREM 2.1. *One has the equality*

$$\mathbb{Z}_p = B_c(0,1)$$

where $B_c(0,1) = \{x \in \mathbb{Q}_p,\ |x|_p \leqslant 1\}$ denote the closed unit ball of $\mathbb{Q}_p$.

PROOF. (of Prop. 2.6) Since multiplication by a power of p result in a shift in a p-adic expansion:

$$p^m \sum_{k \in \mathbb{Z}} a_k(x) p^k = \sum_{k \in \mathbb{Z}} a_{k-m}(x) p^k,$$

we may assume that $|x|_p = 1$ and therefore that x belongs to $\mathbb{Z}_p$ hence admits a unique p-adic expansion. □

COROLLARY 2.1. *For $x \in \mathbb{Q}_p$ we have*

$$|x|_p = p^{-v_p(x)},\ v_p(x) = \sup\{k \in \mathbb{Z},\ p^{-k} x \in \mathbb{Z}_p\}.$$

EXERCISE 2.1.

3.2. The structure of the ring of p-adic integers. In this section, we prove Theorem 2.1: obviously one has $\mathbb{Z}_p \subset B_c(0,1)$ (since $\mathbb{Z} \subset B_c(0,1)$). To prove the converse we note that

$$\mathbb{Q} \cap B_c(0,1) = \mathbb{Z}_{(p)} = \{\frac{a}{b},\ a, b \in \mathbb{Z},\ (b,p) = 1\}.$$

Since $\mathbb{Z}_{(p)}$ is dense in $B_c(0,1)$ it will suffice to show that any element of this set can be approximated by an element of $\mathbb{Z}$ to arbitrary precision. Since is coprime with p it is coprime with p^n for any $n \geq 1$ and there exist (Bezout) $u, v \in \mathbb{Z}$ such that

$$ub + vp^n = 1$$

and hence

$$\frac{1}{b} = u + \frac{v}{b} p^n$$

and

$$\frac{a}{b} = au + \frac{v}{b} p^n.$$

therefore

$$|\frac{a}{b} - au|_p = |\frac{v}{b} p^n| \leqslant p^{-n}.$$

□

REMARK 3.1. The set $\mathbb{Z}_{(p)} = \mathbb{Q} \cap B_c(0,1)$ of rational numbers whose denominator is prime to p is a ring (this is the intersection of two rings): this is the *localization* of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$. As such this is a local ring (it has only one maximal ideal $p\mathbb{Z}_{(p)}$).

Theorem 2.1 is an illustration of how different the p-adic topology is from the usual one: this theorem shows the equality of two objects of fairly different nature: the ring $\mathbb{Z}_p$ which is an algebraic object and the unit ball $B_c(0,1)$ which is of a more geometric nature (but still is invariant under addition !)

This theorem is consequence of two rather distinguished features of $|\cdot|_p$ by comparison with the usual absolute value which we now spell out:

- $|\cdot|_p$ satisfies the *ultrametric inequality*

$$\forall x, y \in \mathbb{Q}_p,\ |x+y|_p \leqslant \max(|x|_p, |y|_p). \tag{3.1}$$

  Note that if $|x|_p \neq |y|_p$ this inequality is an equality.
- The restriction to $\mathbb{Q}_p^\times$ of $|\cdot|_p$ takes *discrete* values:

$$|\mathbb{Q}_p^\times|_p = p^{\mathbb{Z}}. \tag{3.2}$$

Using these we complete our study of the structure of $\mathbb{Z}_p$:

THEOREM 2.2. *The ring $\mathbb{Z}_p$ enjoy the following properties:*

1. *$\mathbb{Z}_p$ is a compact subring of $\mathbb{Q}_p$ and is maximal for this property (any compact subring of $\mathbb{Q}_p$ is contained in $\mathbb{Z}_p$).*
2. *$\mathbb{Z}_p$ is open.*
3. *The group of units $\mathbb{Z}_p^\times$ is precisely the unit circle $C(0,1) = \{x \in \mathbb{Z}_p,\ |x|_p = 1\}$.*
4. *The ideals of $\mathbb{Z}_p$ are exactly the closed balls*

$$B_c(0,r) = \{x \in \mathbb{Q}_p,\ |x|_p \leqslant r\}$$

   for some $r \leqslant 1$. More generally, the $\mathbb{Z}_p$-module $M \subset \mathbb{Q}_p$ distinct from $\mathbb{Q}_p$ are exactly the closed balls $B_c(0,r)$ for some $r \geqslant 0$.
5. *$\mathbb{Z}_p$ is a principal ideal domain with a unique maximal ideal,*

$$p\mathbb{Z}_p = B_c(0, 1/p)$$

   and any $\mathbb{Z}_p$-module contained in -but distinct from- $\mathbb{Q}_p$ is generated by p^k for some $k \in \mathbb{Z}$.
6. *For any $k \geqslant 0$, the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ induce the isomorphism*

$$\mathbb{Z}_p/p^k\mathbb{Z}_p \simeq \mathbb{Z}/p^k\mathbb{Z}.$$

   In particular $\mathbb{Z}_p/p\mathbb{Z}_p$ is the finite field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

PROOF. - Since $\mathbb{Z}_p = B_c(0,1)$, $\mathbb{Z}_p$ is closed, bounded, hence compact. Let $R \subset \mathbb{Q}_p$ be a compact subring, then it is bounded. Suppose that there exist $x \in R$ with $|x|_p > 1$ then $|x^n|_p = |x|_p^n \to \infty$ contradicting the boundedness of R, therefore $R \subset B_c(0,1) = \mathbb{Z}_p$.

- $\mathbb{Z}_p = B_c(0,1) = B_o(0,p)$ is open.

- Since $|x^{-1}|_p = |x|_p^{-1}$, $C(0,1) \subset \mathbb{Z}_p$ is stable under multiplicative inversion and therefore contained in $\mathbb{Z}_p^\times$. Conversely given $x, y \in \mathbb{Z}_p$ such that $xy = 1$, we have $|x|_p|y|_p = 1$ and $|x|_p, |y|_p \leqslant 1$ which imply that $|x|_p = |y_p| = 1$; this implies that $\mathbb{Z}_p^\times = C(0,1)$.

- Let $M \subset \mathbb{Q}_p$ be a $\mathbb{Z}_p$-module distinct from $\{0\}$ and $\mathbb{Q}_p$ and let $x \in \mathbb{Q}_p - M$. Given $y \in M - \{0\}$ we have $\mathbb{Z}_p.y \subset M$ and $\mathbb{Z}_p.y = B_c(0, |y|_p)$. This imply that $|x|_p > |y|_p$ and therefore $M \subset B_c(0, |x_p|/p)$. If $M \neq \{0\}$ (otherwise we are done), $|x|_p$ is bounded from below by a positive number and since $|x|_p \in p^{\mathbb{Z}}$ we may assume that $x \in \mathbb{Q}_p - M$ is of minimal absolute value with this property and if follows that

$$M = \mathbb{Z}_p y = B_c(0, |y|_p)$$

for any y of valuation $|x|_p/p$.

- The isomorphism $\mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}$ follows from the density of $\mathbb{Z}$ in $\mathbb{Z}_p$. □

EXERCISE 2.2. Show that if $A = \{a_0, \cdots, a_{p-1}\} \subset \mathbb{Z}_p$ is a set of representatives of $\mathbb{Z}_p/p\mathbb{Z}_p$, any $x \in \mathbb{Q}_p$ can be represented in a unique way as a series of the shape

$$\sum_{k \geqslant v_p(x)} a_k(x; A)p^k, \; a_k(x; A) \in A, \; a_{v_p(x)}(x; A) \not\equiv 0(p\mathbb{Z}_p).$$

EXERCISE 2.2. Compute the 7-adic expansion of -6, -1, $1/3$ for the usual set of representatives; same question for $-2/3$.

3.3. $\mathbb{Z}_p$ as an inverse limit. The ring $\mathbb{Z}_p$ can be given a purely algebraic construction as an inverse limit: Let $(N, \leqslant)$ be a partially ordered set and let $(R_n)_{n\in N}$ be a colection of rings indexed by N; for each pair $(m, n) \in N^2$ with $m \leqslant n$ we are given a map

$$r_{n,m} : R_n \to R_m$$

such that

$$r_{m,m} = \mathrm{Id}_{R_m}, \;\text{ for each } k \leqslant m \leqslant n \in N, \; f_{n,k} = f_{n,m} \circ f_{m,k}$$

then the inverse limit of the $(R_n)_{n\in N}$ with respect to the system of maps $(r_{n,m})_{\substack{(m,n)\in N^2\\ m\leqslant n}}$ is the following subring of the direct product ring $\prod_{n\in N} R_n$

$$\varprojlim_{n\in N} R_n = \{(x_n)_{n\in N} \in \prod_{n\in N} R_n, \; \forall m \leqslant n, \; x_m = r_{n,m}x_n\} \subset \prod_{n\in N} R_n.$$

If $N = \mathbb{N}$ (equipped with the natural ordering) we have setting $r_n = r_{n+1,n}$

$$\varprojlim_{n\in N} R_n = \{(x_n)_{n\in N} \in \prod_{n\in N} R_n, \; \forall n \geqslant 0, \; x_n = r_n x_{n+1}\}.$$

EXERCISE 2.3. Prove that $\mathbb{Z}_p \simeq \varprojlim_{n\geqslant 1} \mathbb{Z}/p^n\mathbb{Z}$ where $r_{n,m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ is the reduction modulo p^m map.

3.3.1. *The profinite completion.* The above construction of $\mathbb{Z}_p$ as an additive group is also a special case of another example of inverse limit: the profinite completion of a group: given G a group, let $N = \{H \subset G, \; H \text{ normal}, \; |G/H| < \infty\}$ be the partially ordered set of the normal subgroups of G of finite index inversely ordered by inclusion (for $H, H' \subset G$ two normal subgroups of finite index, we declare that $H \leqslant H'$ iff $H \supset H'$). For $H \leqslant H'$ ($H' \subset H$) we let

$$r_{H',H} : G/H' \mapsto G/H$$

be the canonical map. The inverse limit

$$\widehat{G} = \varprojlim_{H} G/H$$

is the profinite completion of G.

3.4. Further surprises with the p-adic topology.

PROPOSITION 2.7. *Open balls are closed and closed ball are open (for the p-adic topology). In particular $\mathbb{Q}_p$ is totally disconnected (the only connected subsets are points). Every point of an open ball is a center of that ball:*

$$\forall y \in B_o(x, r), \; B_o(x, r) = B_o(y, r),$$

Any ball is of the shape

$$x + p^k B_c(0, 1), \; k \in \mathbb{Z}.$$

EXERCISE 2.4. Prove the proposition.

Concerning suite and series p-analysis look like a "student dream":

PROPOSITION 2.8. *A sequence in $\mathbb{Q}_p$, $(a_n)_n$ is Cauchy if and only if $a_{n+1} - a_n \to 0$. A series in $\mathbb{Q}_p$, $\sum_{n=1}^{\infty} a_n$ is convergent if and only if $\lim_n a_n = 0$.*

For instance

$$\sum_{n=0}^{\infty} p^n = \frac{1}{1-p}$$

while the series

$$\sum_{n\geqslant 1} \frac{1}{n^2}$$

is diverging.

EXERCISE 2.3. Show that the series

$$\exp_p(x^{p-1}) = \sum_{n\geqslant 0} \frac{(x^{p-1})^n}{n!} \quad \log_p(x) = \sum_{n\geqslant 1} \frac{(-1)^{n-1}x^n}{n}$$

converge for $|x|_p < p^{-1}$ and $|x|_p < 1$ respectively.

3.5. Continuous functions. The space of continuous function on $\mathbb{Q}_p$ or on an open subset of $\mathbb{Q}_p$ is fairly rich: it contains obviously the polynomial as well as power series

$$\sum_{n\geqslant 0} a_n x^n$$

if $|a_n x^n|_p \to 0$ for some $x \neq 0$.

Another class of continuous functions are the locally constant functions:

DEFINITION 2.4. *Let $\Omega \subset \mathbb{Q}_p$ an open subset. A function $f : \Omega \to \mathbb{C}$ is locally constant if for any $x \in \Omega$ there exist an open neighborhood $\Omega_x \subset \Omega$ on which f is constant.*

A locally constant function is clearly continuous however unlike over the reals, there are plenty of locally constant functions which are not constant. For instance the characteristic function of $\mathbb{Z}_p$ in $\mathbb{Q}_p$ is continuous !

4. Newton's method and Hensel's lemma

In archimedean analysis, Newton's method is a way to find approximation to a solution of the equation $P(x) = 0$ for some function P starting from a point x_0 close enough to that solution. The principle is to consider the intersection of tangent to the graph of f through the point $(x_0, P(x_0))$ with the horizontal axis which gives the point $(x_1, 0)$ and to iterate the process with x_1... In this section we provide an analog to Newton's method in the p-adic setting for $P \in \mathbb{Z}_p[X]$ is a polynomial and when we search for a root in $\mathbb{Z}_p$.

THEOREM 2.3. *Let $P \in \mathbb{Z}_p[X]$ and $x_0 \in \mathbb{Z}_p$ such that*

$$|P(x_0)|_p < 1, \ |P'(x_0)|_p = 1$$

then the sequence defined recursively by

$$x_{n+1} = x_n - \frac{P(x_n)}{P'(x_n)}$$

is well defined for every $n \geqslant 0$, belong to $\mathbb{Z}_p$ and converge to a root x_∞ of P in $\mathbb{Z}_p$ which satisfy $|x_\infty - x_0|_p < 1$.

Let us give an arithmetic interpretation of this result: consider the reduction modulo p map which takes value in the finite field $\mathbb{F}_p$:

$$\cdot \,(\mathrm{mod}\, p) : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

Any polynomial $P \in \mathbb{Z}_p[X]$ define a polynomial $P\,(\mathrm{mod}\, p) \in \mathbb{F}_p[X]$ by reduction of the coefficient modulo p. The condition

$$|P(x_0)|_p < 1,\ |P'(x_0)|_p = 1$$

is equivalent to

$$x_0\,(\mathrm{mod}\, p) \text{ is a simple root of } P\,(\mathrm{mod}\, p).$$

The above theorem says that a simple root $\overline{x} \in \mathbb{F}_p$ of a polynomial with integral coefficients $P(X) \in \mathbb{Z}_p[X]$ ($\overline{P}(\overline{x}) = 0_{\mathbb{F}_p}$) can be "lifted" to a root $x \in \mathbb{Z}_p$ (such that $x\,(\mathrm{mod}\, p) = \overline{x}$).

PROOF. To give a fell of what is going on we start by checking that the sequence is well defined: let $h_n = -P(x_n)/P'(x_n)$ whenever it is defined so that

$$x_{n+1} = x_n + h_n.$$

By assumption we have $|h_0|_p < 1 \Leftrightarrow h_0 \equiv 0\,(\mathrm{mod}\, p)$ and therefore (since $P, P' \in \mathbb{Z}_p[X]$)

$$P(x_1) \equiv P(x_0)\,(\mathrm{mod}\, p),\ P'(x_1) \equiv P'(x_0)\,(\mathrm{mod}\, p)$$

showing that $|P(x_1)|_p < 1,\ |P'(x_1)|_p = 1$. Clearly this generalize to any n showing that that $(x_n)_n$ is well defined. Let us assume that $|h_n|_p \leqslant p^{-k_n}$, we will evaluate $P(x_{n+1}) = P(x_n + h_n)$ using the Taylor expansion of P. For this we use the general lemma:

LEMMA 2.1. *Let R be a ring and $P \in R[X]$, one has the following identity*

$$P(X+Y) = \sum_{k=0}^{\deg P} P^{[k]}(X) Y^k$$

where

$$P^{[k]}(X) \in R[X],\ P^{[0]}(X) = P(X),\ P^{[1]}(X) = P'(X).$$

REMARK 4.1. If R is contained in a field of characteristic 0,

$$P^{[k]}(X) = P^{(k)}(X)/k!.$$

By this lemma we have

$$P(x_{n+1}) = P(x_n) - \frac{P(X_n)}{P'(x_n)} P'(x_n) + \sum_{k \geqslant 2} P^{[k]}(x_n) h_n^k = \sum_{k \geqslant 2} P^{[k]}(x_n) h_n^k \equiv 0\,(\mathrm{mod}\, p)^{2k_n};$$

therefore we have proven that

$$|P(x_{n+1})|_p = |h_{n+1}|_p = |x_{n+1} - x_n|_p \leqslant |h_n|_p^2.$$

It follows that for all $n \geqslant 0$

$$|h_n|_p = |P(x_n)|_p = |x_{n+1} - x_n|_p \leqslant p^{-2^n} \to 0.$$

Therefore $(x_n)_n$ is a Cauchy sequence converging to x_∞ satisfying

$$|x_\infty - x_n|_p \leqslant p^{-2^n},\ P(x_\infty) = 0.$$

□

EXERCISE 2.4. Prove that $\sqrt{2}$ exists in $\mathbb{Q}_7$ and compute its 7-adic expansion up to 10 digits.

4.1. The Teichmueller character. We apply this to the polynomial

$$P(X) = X^{p-1} - 1.$$

COROLLARY 2.2. *There exists an injective group homomorphism (called the Teichmueller character):*

$$\omega_p : \mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$$

whose image is the group of $p-1$-roots of 1

$$\omega_p(\mathbb{F}_p^\times) = \mu_{p-1}(\mathbb{Q}_p) = \{x \in \mathbb{Q}_p,\ x^{p-1} = 1\} \subset \mathbb{Z}_p^\times$$

which is an inverse for the reduction modulo p map on $\mu_{p-1}(\mathbb{Q}_p)$

$$\forall u \in \mathbb{F}_p^\times,\ \omega_p(u) \,(\mathrm{mod}\, p) = u.$$

In particular $\{0\} \cup \omega_p(\mathbb{F}_p^\times)$ is a sytem of representatives of $\mathbb{Z}_p/p\mathbb{Z}_p$.

EXERCISE 2.5. Prove that for any $a \in \mathbb{Z}_p^\times$ with $|a|_p = 1$, the sequence $(a^{p^n})_{n\geqslant 1}$ converge to $\omega_p(a \,(\mathrm{mod}\, p))$.

4.2. Points on hypersurfaces. Hensel's lemma can be generalized in several dimensions and makes it possible to prove the existence of point on *algebraic varieties* over $\mathbb{Q}_p$. We discuss here the case of *hypersurfaces*: given $P(X_1, \cdots X_n) \subset \mathbb{Q}_p[X_1, \cdots, X_n]$, the set of $\mathbb{Q}_p$-point of the hypersurface defined by P is the set

$$V_P(\mathbb{Q}_p) = \{\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Q}_p^n,\ P(\mathbf{x}) = 0\} \subset \mathbb{Q}_p^n.$$

We denote by

$$V_P(\mathbb{Z}_p) = V_P(\mathbb{Q}_p) \cap \mathbb{Z}_p^n$$

the set of $\mathbb{Z}_p$-point. We are looking for sufficient condition to guaranty that

$$V_P(\mathbb{Q}_p) \neq \emptyset.$$

Obviously it is sufficient to show that $V_P(\mathbb{Z}_p) \neq \emptyset$; up to multipliying P by a scalar we may assume that $P \in \mathbb{Z}_p[X_1, \cdots, X_n]$. If $\mathbf{x} \in V_P(\mathbb{Z}_p)$ we have $P(\mathbf{x}) = 0$ and in particular, considering reduction modulo p, $\overline{x} = \mathbf{x} \,(\mathrm{mod}\, p) \in (\mathbb{Z}_p/p\mathbb{Z}_p)^n = \mathbb{F}_p^n$ and $\overline{P} = P \,(\mathrm{mod}\, p)$ we have

$$\overline{P}(\overline{\mathbf{x}}) = 0_{\mathbb{F}_p}.$$

In other terms we have

$$V_P(\mathbb{Z}_p) \neq \emptyset \Rightarrow V_{\overline{P}}(\mathbb{F}_p) \neq \emptyset$$

where

$$V_{\overline{P}}(\mathbb{F}_p) = \{\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_p^n,\ \overline{P}(\mathbf{x}) = 0\}$$

is the set of $\mathbb{F}_p$-points of the hypersurface defined by the equation:

$$\overline{P}(\mathbf{x}) = 0$$

We would like to go in the reverse direction and find sufficient conditions to insure that

$$V_{\overline{P}}(\mathbb{F}_p) \neq \emptyset \Rightarrow V_P(\mathbb{Z}_p) \neq \emptyset.$$

For this we use an extension and Hensel's lemma and we make the following definitions:

DEFINITION 2.5. *A point* $\mathbf{x} \in V_{\overline{P}}(\mathbb{F}_p)$ *is critical if is satisfies*

$$\nabla \overline{P}(\mathbf{x}) = (\frac{\partial P}{\partial x_1}(\mathbf{x}), \cdots, \frac{\partial P}{\partial x_n}(\mathbf{x})) = 0.$$

The hypersurface $V_{\overline{P}}$ *is* non-singular over $\mathbb{F}_p$ *if* $V_{\overline{P}}(\mathbb{F}_p)$ *does not have any critical points.*

THEOREM 2.4 (Higher dimensional Hensel's Lemma). *Let* $P \in \mathbb{Z}_p[\mathbf{X}]$. *We have the lower bound*

$$|V_P(\mathbb{Z}_p)| \geqslant |V_{\overline{P}}^{nc}(\mathbb{F}_p)|$$

where $V_{\overline{P}}^{nc}(\mathbb{F}_p)$ *denote the set of non-critical points of* $V_{\overline{P}}(\mathbb{F}_p)$.

EXERCISE 2.5. Prove the Theorem.

4.3. The Chevalley-Warning theorem. We now look for conditions to insure that $V_{\overline{P}}(\mathbb{F}_p) \neq \emptyset$ and a simple criterion comes from the

THEOREM 2.5 (Chevalley-Warning). *Let* $P(\mathbf{x}) \in \mathbb{F}_p[x_1, \cdots, x_n]$ *be a polynomial in* n *variables of degree* $d < n$, *then*

$$|V_P(\mathbb{F}_p)| \equiv 0 \,(\mathrm{mod}\, p).$$

in particular if $|V_P(\mathbb{F}_p)| > 0$ *then* $|V_P(\mathbb{F}_p)| \geqslant p$.

EXERCISE 2.6. Prove the theorem. For this one introduce the polynomial

$$Q(\mathbf{x}) = 1 - P(\mathbf{x})^{p-1} \in \mathbb{F}_p[X_1, \cdots, X_n];$$

it has degree $d(p-1) < n(p-1)$.

(1) Prove that

$$Q(\mathbf{x}) = \begin{cases} 1_{\mathbb{F}_p} & \text{if } \mathbf{x} \in V_P(\mathbb{F}_p) \\ 0_{\mathbb{F}_p} & \text{if } \mathbf{x} \notin V_P(\mathbb{F}_p) \end{cases}$$

(2) Deduce that

$$|V_P(\mathbb{F}_p)| \equiv \sum_{\mathbf{x} \in \mathbb{F}_p^n} Q(\mathbf{x}) \,(\mathrm{mod}\, p).$$

(3) Prove the following

LEMMA 2.2. *Given* $k \geqslant 0$ *be an integer we have*

$$\sum_{x \in \mathbb{F}_p} x^k = \begin{cases} -1 & \text{if } p-1 | k \\ 0 & \text{if } p-1 \not| k. \end{cases}$$

(4) Prove that

$$\sum_{\mathbf{x} \in \mathbb{F}_p^n} Q(\mathbf{x}) = 0$$

and conclude. For the later, one can proceed by decomposing $Q(X_1, \cdots, X_n)$ into monomials and use the previous Lemma.

COROLLARY 2.3. *Let* $P \in \mathbb{F}_p[X_1, \cdots, X_n]$ *be an homogeneous polynomial of degree* $0 < d < n$, *then*

$$|V_P(\mathbb{F}_p)| \geqslant p.$$

COROLLARY 2.4. *Let $P \in \mathbb{Z}_p[X_1, \cdots, X_n]$ be an homogeneous polynomial of degree $0 < d < n$, such that $\overline{P} \in \mathbb{F}_p[X_1, \cdots, X_n]$ has no critical points except for $(0, \cdots, 0)$, then there exists $\mathbf{x} \in \mathbb{Z}_p^n - \{(0, \cdots, 0)\}$ such that $P(\mathbf{x}) = 0$.*

EXERCISE 2.7. Prove these two corollaries