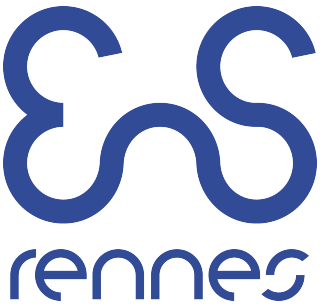
**ANNÉE 2017**


RAPPORT DE LECTURE DIRIGÉE

par

**Rémi Moreau, Antoine Sabut et Pierre Houédry**

---

# Nombres $p$-adiques
# Lemme de Hensel

sous la tutelle de
**Yvan Ziegler**

## Table des matières

Dans tout ce qui suit, $p$ désigne un entier premier.

# 1. Anneau des entiers $p$-adiques

## 1.1. Généralités

**Définition 1.1.** Un entier $p$-adique est une série formelle $\sum_{i=0}^{\infty} a_i p^i$ où $0 \leq a_i < p$. L'ensemble des entiers p-adiques est alors noté $\mathbb{Z}_p$.
On remarque qu'un entier $p$-adique s'identifie à la suite de ses coefficients $(a_i)_{i\in\mathbb{N}}$ : $\mathbb{Z}_p$ correspond ensemblistement à $[\![0, p-1]\!]^{\mathbb{N}}$.

La décomposition en base $p$ assure une injection de $\mathbb{N}$ dans $\mathbb{Z}_p$.

**Théorème 1.2.** *$\mathbb{Z}_p$ n'est pas dénombrable.*

*Démonstration.* On raisonne par un argument diagonal. Pour toute séquence d'entiers $p$-adiques,

$$a = \sum_{i=0}^{\infty} a_i p^i,\ b = \sum_{i=0}^{\infty} b_i p^i,\ c = \sum_{i=0}^{\infty} c_i p^i,\ ...$$

on peut construire un $x = \sum_{i=0}^{\infty} x_i p^i$ en choisissant $x_0 \neq a_0$, $x_1 \neq b_1$, $x_2 \neq c_2$, ... Ainsi construit, $x$ est différent de tout élément existant. Il n'existe donc pas de surjection de $\mathbb{N}$ dans $\mathbb{Z}_p$. □

On peut munir $\mathbb{Z}_p$ d'une addition $+$ et d'une multiplication $\times$ définies sur le modèle des opérations en base $p$ : les algorithmes usuels sont poursuivis à l'infini. L'élément neutre pour l'addition est 0 et tout entier $p$-adique admet un opposé :

$$\sum_{i=0}^{\infty}(p-1)p^i = -1 \text{ et } \sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty}(p-1-a_i)p^i + 1 = 0$$

Il existe également des éléments inversibles au sens de la multiplication.

**Exemple 1.3.** $(1-p)^{-1} = \frac{1}{1-p} = \sum_{i=0}^{\infty} p^i$ et pour $\alpha \in \mathbb{Z}_p$, $(1+\alpha p)^{-1} = \sum_{i=0}^{\infty}(-1)^i(\alpha p)^i$.

**Théorème 1.4.** *$(\mathbb{Z}, +, \times)$ est un anneau commutatif.*

## 1.2. Propriétés de l'anneau $\mathbb{Z}_p$

**Définition 1.5.** Soit $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$.
La *valuation* (aussi appelée *ordre*) de $a$, notée $\nu(a)$, est définie par

$$\nu(a) = \begin{cases} \min\{i \in \mathbb{N} \mid a_i \neq 0\} & \text{si } a \neq 0 \\ \infty & \text{si } a = 0 \end{cases}$$

**Proposition 1.6.**

*(i) $\mathbb{Z}_p$ est intègre.*

*(ii)* $\forall a, b \in \mathbb{Z}_p,\ \nu(ab) = \nu(a) + \nu(b)$ *et* $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$

*Démonstration.* $\mathbb{Z}_p$ est non nul. Soient $a = \sum_{i=0}^{\infty} a_i p^i$, $b = \sum_{i=0}^{\infty} b_i p^i$ non nuls. $a_{\nu(a)}$ (resp. $b_{\nu(b)}$) est le premier coefficient non nul de $a$ (resp. $b$). $p$ ne divise ni $a_{\nu(a)}$, ni $b_{\nu(b)}$, donc $p$ ne divise pas leur produit $a_{\nu(a)}b_{\nu(b)}$. $a_{\nu(a)}b_{\nu(b)}$ est le premier coefficient non nul de $a \times b$. En particulier, $a \times b \neq 0$. Ainsi $\mathbb{Z}_p$ ne contient pas de diviseur de zéro. $\mathbb{Z}_p$ est intègre. □

**Définition 1.7.** L'application $\varepsilon : \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ donnée par $\varepsilon(\sum_{i=0}^{\infty} a_i p^i) = a_0 \ mod\ p$ définit un morphisme d'anneaux, de noyau $\ker \varepsilon = p\mathbb{Z}_p$. C'est le morphisme de réduction modulo $p$.

**Proposition 1.8.** *L'ensemble des inversibles de* $\mathbb{Z}_p$ *est* $\mathbb{Z}_p^\times = \{\sum_{i=0}^{\infty} a_i p^i \mid a_0 \neq 0\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

*Démonstration.* Si $a \in \mathbb{Z}_p$ est inversible, alors son image $\varepsilon(a) \in \mathbb{Z}/p\mathbb{Z}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$, ce qui prouve la première inclusion : $\mathbb{Z}_p^\times \subset \{\sum_{i=0}^{\infty} a_i p^i \mid a_0 \neq 0\}$.

Réciproquement, soit $a \in \mathbb{Z}_p$ avec $a_0 \neq 0$. $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc $\exists \overline{b_0} \in \mathbb{Z}/p\mathbb{Z}$, $\overline{a_0 b_0} = \overline{1}$. Pour $b_0 \in [\![1, p-1]\!]$, $ab_0 = 1 + \alpha p \in \mathbb{Z}_p^\times$ puisque $(1+\alpha p)\sum_{i=0}^{\infty}(-1)^i(\alpha p)^i = 1$.

Donc $a$ est inversible, d'inverse $a^{-1} = b_0(1+\alpha p)^{-1}$, $\{\sum_{i=0}^{\infty} a_i p^i \mid a_0 \neq 0\} \subset \mathbb{Z}_p^\times$. □

**Proposition 1.9.**

*(i)* $\mathbb{Z}_p$ *est principal.*

*(ii) Les seuls idéaux de* $\mathbb{Z}_p$ *sont les* $(p^k) = p^k\mathbb{Z}_p$, $k \in \mathbb{N}$. *Ils sont principaux.*

*(iii)* $p\mathbb{Z}_p$ *est le seul idéal maximal.*

*Démonstration.* Il est facile de voir que les seuls sous-groupes de $\mathbb{Z}_p$ sont les $p^k\mathbb{Z}_p$, $k \in \mathbb{N}$. Ceux-ci vérifient en particulier le caractère absorbant et sont principaux. □

## 2. Topologie de $\mathbb{Z}_p$

$X_p = [\![0, p-1]\!]^{\mathbb{N}}$ est compact en tant que produit de compacts pour la topologie produit (théorème de Tychonoff, version dénombrable). (La topologie sur $[\![0, p-1]\!]$ est la topologie discrète.) $\mathbb{Z}_p$ est donc aussi compact pour cette topologie.
Toutes les métriques sur un espace compact métrisable sont équivalentes : on introduit ici la distance $p$-adique, pour laquelle la topologie est équivalente à celle présentée ci-dessus.

### 2.1. Propriétés de la distance

**Proposition 2.1.** *$d : (x, y) \mapsto p^{-\nu(x-y)}$ définit une distance sur $\mathbb{Z}_p$, la distance $p$-adique.*
*Muni de cette métrique, la multiplication par $p$ est $\frac{1}{p}$-contractante, donc continue.*

Désormais, $\mathbb{Z}_p$ est muni de la distance $p$-adique.

*Démonstration.* On vérifie sans difficulté les propriétés de distance pour $d$.

$$d(px, py) = p^{-\nu(px-py)} = p^{-\nu(p(x-y))} = p^{-\nu(x-y)-\nu(p)} = p^{-\nu(x-y)-1} = \frac{1}{p} p^{-\nu(x-y)} = \frac{1}{p} d(x, y)$$

□

**Théorème 2.2.** *$\mathbb{N}$ est une partie dense de $\mathbb{Z}_p$.*

*Démonstration.* $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ est limite de la suite d'entiers naturels $(\sum_{i=0}^{n} a_i p^i)_{n\in\mathbb{N}}$. □

**Proposition 2.3.** *La distance $p$-adique définit une distance ultramétrique sur $\mathbb{Z}_p$ :*

$$\forall x, y, z \in \mathbb{Z}_p,\ d(x, y) = 0 \Leftrightarrow x = y \ \ ; \ \ d(x, y) = d(y, x) \ \ ; \ \ d(x, y) \leq \max\{d(x, z), d(z, y)\}$$

*Cette dernière propriété, plus forte que l'inégalité triangulaire, est appelée inégalité ultramétrique.*

*Démonstration.*
$\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$ donc $p^{-\nu(x-y)} \leq \max\{p^{-\nu(x-z)}, p^{-\nu(z-y)}\}$ où $a = x - z$ et $b = z - y$. □

**Proposition 2.4.** *Soit $(X, d)$ un espace ultramétrique.*

*(i) Pour qu'une suite $(x_n) \in \mathbb{X}^{\mathbb{N}}$ soit de Cauchy, il suffit que $d(x_n, x_{n+1}) \to 0$.*

*(ii) Tout point d'une boule en est son centre.*

*(iii) Toute boule ouverte est fermée. Toute boule fermée est ouverte.*

*(iv) Tout triangle de $X$ est isocèle. De plus, sa base est au plus égale aux côtés égaux.*

*Démonstration.*

(i) Pour $p, q \in \mathbb{N},\ p > q : d(x_p, x_q) \leq \max\{d(x_p, x_{p-1}), ..., d(x_{q+1}, x_q)\}$.

(ii) Soient $x \in \mathbb{Z}_p$, $r \in \mathbb{R}_+^*$, $y \in \mathcal{B}(x, r)$. Montrons $\mathcal{B}(x, r) = \mathcal{B}(y, r)$. Soit $z \in \mathcal{B}(y, r)$ (resp. $z \in \mathcal{B}(x, r)$).

$d(z, y) \leq \max\{d(z, x), d(x, y)\} \leq r$ (resp. $d(z, x) \leq \max\{d(z, y), d(y, x)\} \leq r$) : $\mathcal{B}(x, r) = \mathcal{B}(y, r)$

(iii) Soit $\mathcal{B}_f(x,r)$ boule fermée de $\mathbb{Z}_p$. Soit $z \in \mathcal{B}(x,r)$.
$\mathcal{B}_f(z,r) = \mathcal{B}_f(x,r)$ donc $\mathcal{B}(z,\frac{r}{2}) \subset \mathcal{B}_f(x,r)$. Donc $\mathcal{B}_f(x,r)$ ouverte. Soit $\mathcal{B}(x,r)$ boule ouverte de $\mathbb{Z}_p$. Soit $(x_n) \in \mathcal{B}(x,r)^{\mathbb{N}}$, $x_n \to x_\infty$.
$\forall n \in \mathbb{N},\ d(x,x_\infty) \leq \max\{d(x,x_n), d(x_n,x_\infty)\} < r$ donc $x_\infty \in \mathcal{B}(x,r)$. Donc $\mathcal{B}(x,r)$ fermée.

(iv) Soit $(x,y,z) \in \mathbb{Z}_p$. Supposons (sans perte de généralités) que $d(x,y) \leq d(x,z) \leq d(y,z)$. $d(y,z) \leq \max\{d(x,y), d(x,z)\} = d(x,z)$ car $d$ est ultramétrique. Ainsi $d(x,z) = d(y,z)$.

□

**Corollaire 2.5.** *Les boules ouvertes de $\mathbb{Z}_p$ sont exactement les boules fermées de $\mathbb{Z}_p$.*

$\mathbb{Z}_p$ est totalement discontinu (car ultramétrique) : ses composantes connexes sont les singletons.

## 2.2. Espace de Cantor - Analogie avec $\mathbb{Z}_2$

**Définition 2.6.** L'espace de Cantor est la limite $C$ de la suite de compacts $(C_n)_n$ définie par :

$$C_0 = [0,1] \text{ et } \forall n \in \mathbb{N},\ C_{n+1} = \frac{C_n}{3} \cup \frac{2 + C_n}{3}$$

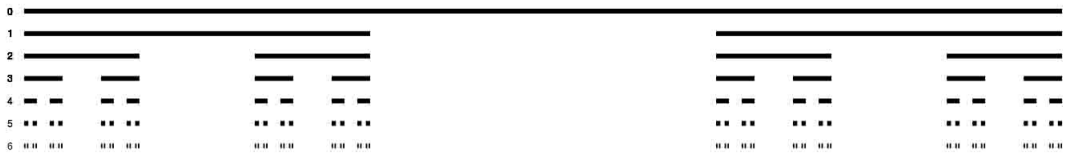


FIGURE 1 – Représentation des 6 premières itérations

**Proposition 2.7.** *L'espace de Cantor est un compact non vide de $[0,1]$, de mesure nulle, non dénombrable et d'intérieur vide. De plus :*

$$C = \{\sum_{i=1}^{\infty} \frac{2\alpha_i}{3^i} \mid \forall i \in \mathbb{N},\ \alpha_i \in \{0,1\}\}$$

*Démonstration.*

(i) $C$ est compact car il est fermé borné dans $[0,1]$ de dimension finie.

(ii) $C = \bigcap_{n\in\mathbb{N}} C_n$ donc $\lambda(C) = \lim_{n\to\infty} \lambda(C_n) = \lim_{n\to\infty} \left(\frac{2}{3}\right)^n = 0$. $\mathring{C}$ est un ouvert de mesure nulle, $C$ est d'intérieur vide.

(iii) Notons $I_n$ l'un des $2^n$ intervalles composant $C_n$.
Soit $\Phi : x \in C \mapsto (\alpha_n^x)_n$ défini par : $\alpha_n^x = 0$ si $x$ est dans le premier tiers de $I_n$, $\alpha_n^x = 2$ sinon. $\Phi$ définit une bijection entre $[0,1]$ et $C$ : $C$ est non dénombrable.

(iv) Par récurrence, $\forall n \in \mathbb{N},\ K = \{\sum_{i=1}^{\infty} \frac{\alpha_i}{3^i} \mid \forall i \in \mathbb{N},\ \alpha_i \in \{0,2\}\} \subset C_n$ donc $K \subset C$.

De plus, tout $x \in C$ est limite de $(\sum_{i=1}^{n} \frac{\alpha_i^x}{3^i})_n$ donc $C \subset \overline{K} = K$.

□

**Lien avec $\mathbb{Z}_2$**

La preuve précédente introduit l'homéomorphisme $\psi : \sum_{i=0}^{\infty} a_i 2^i \mapsto \sum_{i=0}^{\infty} \frac{2a_i}{3^{i+1}}$ de $\mathbb{Z}_2$ dans $C$.

Considérons aussi la surjection $\varphi : \sum_{i=0}^{\infty} a_i 2^i \mapsto \sum_{i=0}^{\infty} \frac{a_i}{2^{i+1}}$ de $\mathbb{Z}_2$ dans $[0,1]$. Notons que $\varphi$ n'est pas injective : $\sum_{i>j} 2^i$ et $2^j$ ont la même image par $\varphi$.

Le modèle précédent est résumé dans le schéma (commutatif) suivant :

$$\begin{array}{ccccc} \psi : \mathbb{Z}_2 & \to & C & \subset & [0,1] \\ \| & & \downarrow & & \\ \varphi : \mathbb{Z}_2 & \to & [0,1] & & \end{array}$$

On identifie comme ci-dessous les extrémités de $C$ sur les $\frac{a}{2^j}$ de $[0,1]$.

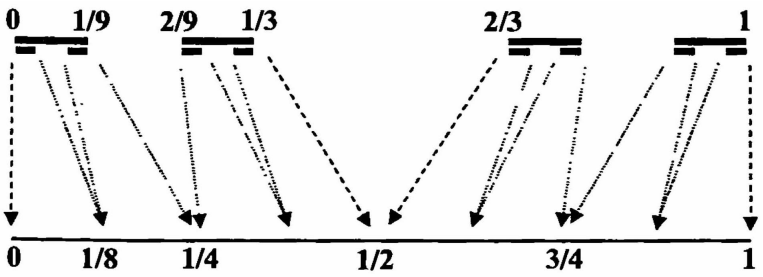



FIGURE 2 – Recollement des extrémités de $C$

# 3. Algèbre topologique

## 3.1. Groupes topologiques

### 3.1.1. Groupes et sous-groupes topologiques

**Définition 3.1.** Un groupe topologique $G$ est un groupe muni d'une topologie qui rend l'application $(x, y) \in G \times G \mapsto xy^{-1}$ continue.
Dans ce cas, les translations et $x \mapsto x^{-1}$ sont des homéomorphismes.
Un sous-groupe $H$ d'un groupe topologique $G$ est un groupe topologique pour la topologie induite par $G$ sur $H$.

**Exemples 3.2.** $(\mathbb{Z}_p, +)$, $(\mathbb{R}, +)$ et $(\mathbb{Z}_p^\times, \times)$ sont des groupes topologiques.

**Définition 3.3.** Un espace est dit localement compact si chacun de ses points admet un voisinage compact.

**Proposition 3.4.** *Si un groupe topologique admet un voisinage compact d'un de ses points, alors il est localement compact.*

*Démonstration.* Les translations (homéomorphes) envoient ce voisinage compact sur un voisinage compact de tout point du groupe topologique. □

**Lemme 3.5.** *Soit $G$ un groupe topologique. Soit $H$ un sous-groupe de $G$.*

*(i) L'adhérence $\overline{H}$ de $H$ est un sous-groupe de $G$.*

*(ii) $G$ est séparé si et seulement si $\{e_G\}$ est fermé.*

*Démonstration.*

(i) Notons $\varphi : (x, y) \in G \times G \mapsto xy^{-1}$. $H$ est un sous-groupe donc $\varphi(H \times H) \subset H$.

$$\varphi(\overline{H} \times \overline{H}) = \varphi(\overline{H \times H}) \subset \overline{\varphi(H \times H)} \subset \overline{H}$$

Cela montre que $\overline{H}$ est un sous-groupe de $G$.

(ii) Rappelons que $G$ est séparé si et seulement si la diagonale $\Delta_G$ est fermée dans $G \times G$. De là :

$$G \text{ séparé } \Rightarrow \{e_G\} \text{ fermé } \Rightarrow \Delta_G = \varphi^{-1}(\{e\}) \text{ fermé dans } G \times G \Rightarrow G \text{ séparé}$$

□

**Théorème 3.6.** *Soit $H$ un sous-groupe d'un groupe topologique $G$.*
*Si $H$ contient un voisinage du neutre $e_G$, alors $H$ est à la fois ouvert et fermé dans $G$.*

*Démonstration.*

(i) *$H$ est ouvert* Notons $V$ un voisinage de $e_G$ contenu dans $H$. Puisque $V \subset H$ et les translations sont des homéomorphismes, pour tout $h \in H$, $hV$ est un voisinage de $h$ contenu dans $H$. $H$ est ouvert car voisinage de chacun de ses points.

(ii) *$H$ est fermé* Pour $g \in H$, $gH$ est ouvert et $H = \big(\bigcup_{gH \neq H} gH\big)^c$. $H$ est fermé en tant que complémentaire d'un ouvert.

□

**Exemples 3.7.** Les sous-groupes $p^n\mathbb{Z}_p$ (resp. $1+p^n\mathbb{Z}_p$) sont des sous-groupes ouverts et fermés de $\mathbb{Z}_p$ (resp. $1+p\mathbb{Z}_p$).

**Définition 3.8.** Un sous-espace topologique $Y$ de $X$ est dit localement fermé dans $X$ si tout point $y \in Y$ admet un voisinage ouvert $V$ dans $X$ tel que $V \cap Y$ est fermé dans $V$.

**Proposition 3.9.** *Un sous-groupe localement fermé d'un groupe topologique est fermé.*

*Démonstration.* $H$ est localement fermé dans $G$ donc ouvert dans $\overline{H}$. Or $\overline{H}$ est un sous-groupe topologique de $G$, donc $H$ est fermé dans $\overline{H}$, i.e. $H = \overline{H}$, $H$ fermé dans $G$. □

**Corollaire 3.10.** *Soit $G$ un groupe topologique. Soit $H$ un sous-groupe de $G$.*

*(i) Si $G$ est séparé et $H$ localement compact, alors $H$ est fermé.*

*(ii) Si $G$ est séparé et $H$ discret, alors $H$ est fermé.*

*(iii) $G/H$ est séparé si et seulement si $H$ est fermé.*

**Proposition 3.11.** *Tout groupe topologique métrisable localement compact est complet.*

*Démonstration.* Le complété de $G$, groupe métrisable localement compact, est aussi topologique, donc $G$ est fermé dans son complété, d'où le résultat. □

Les résultats précédents sont résumés dans le schéma suivant :

$$\begin{array}{ccc} G/H \text{ fini et séparé} & \Leftrightarrow & H \text{ fermé d'indice fini} \\ \Downarrow & & \Downarrow \\ G/H \text{ discret} & \Leftrightarrow & H \text{ ouvert} \\ \Downarrow & & \Downarrow \\ G/H \text{ séparé} & \Leftrightarrow & H \text{ fermé} \end{array}$$

### 3.1.2. Sous-groupes fermés de $\mathbb{R}$ et de $\mathbb{Z}_p$

**Proposition 3.12.** *Les sous-groupes discrets de $\mathbb{R}$ sont les $a\mathbb{Z}$, où $a \in \mathbb{R}$.*

*Démonstration.* Soit $H$ un sous-groupe discret non trivial de $\mathbb{R}$. Il est fermé. Soit $h \neq 0$ dans $H$. $H \cap [0, |h|]$ est dicret et compact donc fini. Il admet donc un plus petit élément non nul noté $a \in H$. Par stabilité du sous-groupe, $a\mathbb{Z} \subset H$. De plus, pour $b \in H$, $b = ma + r$ avec $0 \leq r < a$ où $m$ est la partie entière de $b/a$. $r = b - ma \in H$ et $0 \leq r < a$ donc $r = 0$. Ainsi $b \in a\mathbb{Z}$. □

**Corollaire 3.13.** *Le quotient de $\mathbb{R}$ par un sous-groupe discret non trivial est compact.*

*Démonstration.* Il suffit de considérer $\varphi : \mathbb{R} \to \mathbb{U}\,;\, x \mapsto \exp(\frac{2i\pi x}{a})$ de noyau $H = a\mathbb{Z}$. □

**Proposition 3.14.** *Tout sous-groupe de $\mathbb{R}$ non discret est dense dans $\mathbb{R}$.*

*Démonstration.* C'est le cas où $\inf H \cap [0, |h|] = 0$.
Pour $x, y$ distincts dans $\mathbb{R}$, $\exists h \in H,\ 0 < h < |x - y|$. Posons $n = \lfloor \frac{x}{h} + 1 \rfloor$.

$$x < nh = (n-1)h + h \leq x + h < x + (y - x) = y \text{ donc } x < nh < y : H \text{ est dense dans } \mathbb{R}.$$

En effet, entre deux réels $x$ et $y$, on réussit à placer un élément de $H$. □

**Corollaire 3.15.** *Les sous-groupes fermés propres de $\mathbb{R}$ sont les sous-groupes discrets $a\mathbb{Z}$. Le seul sous-groupe compact de $\mathbb{R}$ est $\{0\}$.*

**Proposition 3.16.** *Les sous-groupes fermés de $(\mathbb{Z}_p, +)$ sont $\{0\}$ et les $p^m\mathbb{Z}_p$, $m \in \mathbb{N}$. Ce sont des idéaux.*

*Démonstration.* Un sous-groupe fermé $H$ de $\mathbb{Z}_p$ vérifie $\mathbb{Z}H = H$ donc pour $h \in H$,
$h\mathbb{Z}_p \subset \overline{h\mathbb{Z}} \subset \overline{H} = H$ car $H$ fermé. Donc tout sous-groupe fermé de $\mathbb{Z}_p$ est un idéal de $\mathbb{Z}_p$. □

**Corollaire 3.17.** *Le quotient de $\mathbb{Z}_p$ par un sous-groupe fermé $H$ non trivial est discret.*
*Le seul sous-groupe discret de $(\mathbb{Z}, +)$ est le sous-groupe trivial $\{0\}$.*

## 3.2. Anneaux topologiques

**Définition 3.18.** Un anneau topologique est un anneau $(A, +, .)$ muni d'une topologie qui rend les applications $(x, y) \mapsto x + y$ et $(x, y) \mapsto x.y$ continues sur $A \times A$.
En particulier, un anneau topologique est un groupe topologique muni d'une multiplication continue sur $A \times A$.

**Proposition 3.19.** *Muni de la métrique p-adique, $\mathbb{Z}_p$ est un anneau topologique. $(\mathbb{Z}_p, d)$ est un espace complet et compact.*

*Démonstration.*
$(\mathbb{Z}_p, +)$ est topologique ce qui assure la continuité de l'addition. Soit $(a, b, k, h) \in \mathbb{Z}_p$.

$$|(a+h)(b+k) - ab| = |ak + hb - hk| \leq \max\{|a|, |b|\}(|h| + |k|) + |h||k| \xrightarrow[|h|,|k|\to 0]{} 0$$

Cela assure la continuité de la multiplication sur $A \times A$.
Par Tychonoff, $\mathbb{Z}_p$ est compact. Muni de la métrique $d$, il est donc complet (toute suite de Cauchy admettant une valeur d'adhérence est convergente). □

**Corollaire 3.20.**

*(i) Le groupe topologique $\mathbb{Z}_p$ est le complété de $\mathbb{Z}$ pour la topologie induite.*

*(ii) La suite $(x_n = \sum_{i=0}^{n} x_i p^i)$ est de Cauchy dans $\mathbb{Z}_p$ complet, de limite $x = \sum_{i\geq 0} x_i p^i$.*

*(iii) L'addition et la multiplication d'entiers p-adiques sont les seules opérations continues sur $\mathbb{Z}_p$ prolongeant l'addition et la multiplication des entiers naturels.*

## 3.3. Corps topologiques - Corps valués

**Définition 3.21.** Un corps topologique $K$ est un corps muni d'une topologie qui rend les applications $(x, y) \mapsto x + y$, $(x, y) \mapsto xy$ continues sur $K \times K$ et le passage à l'inverse continu sur $K^\times$.

**Définition 3.22.** Soit $K$ un corps. Une valeur absolue sur $K$ est un morphisme de groupes $|\,.\,| : K^\times \to \mathbb{R}_+^*$ étendu par $|\,0\,| = 0$ vérifiant l'inégalité triangulaire.
$(K^\times, |\,.\,|)$ est appelé corps valué. Dans ce contexte, $d : (x, y) \mapsto |x - y|$ définit une distance sur $K$.

**Proposition 3.23.**

*(i) Un corps valué muni d'une telle distance est un corps topologique.*

*(ii) Le complété d'un corps valué est encore un corps valué.*

# 4. Limites projectives

La réduction modulo $p^n$ $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$, qui à un entier$p$-adique $x = \sum_{i=0}^{\infty} a_i p^i$ associe $\overline{\sum_{i=0}^{n-1} a_i p^i}$, et le morphisme canonique $\varphi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ donnent le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathbb{Z}_p & \xrightarrow{\varepsilon_{n+1}} & \mathbb{Z}/p^{n+1}\mathbb{Z} \\ & {\scriptstyle \varepsilon_n} \searrow \quad \swarrow {\scriptstyle \varphi_n} & \\ & \mathbb{Z}/p^n\mathbb{Z} & \end{array}$$

$\mathbb{Z}_p$ semble "plus proche" de $\mathbb{Z}/p^{n+1}\mathbb{Z}$ que de $\mathbb{Z}/p^n\mathbb{Z}$. Si $x = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ alors $\lim_{n\to\infty} \sum_{i<n} a_i p^i = x$, où chaque $\sum_{i<n} a_i p^i$ peut être vu comme un élément de $\mathbb{Z}/p^n\mathbb{Z}$.
On aimerait pouvoir dire, dans un sens à expliciter, que $\mathbb{Z}/p^n\mathbb{Z}$ converge vers $\mathbb{Z}_p$.

## 4.1. Existence et propriétés d'une limite projective

**Définition 4.1.** Un système d'ensembles et d'applications $(E_n, \varphi_n)_{n\in\mathbb{N}}$ avec $\varphi_n : E_{n+1} \to E_n$ est appelé *système projectif*.

**Définition 4.2.** La donnée d'un ensemble $E$ et d'applications $\psi_n : E \to E_n$ est appelée *limite projective* de $(E_n, \varphi_n)_{n\in\mathbb{N}}$ si pour tout ensemble $X$ et toutes applications $f_n : X \to E_n$ tels que $\forall n \in \mathbb{N}$ $f_n = \varphi_n \circ f_{n+1}$, il existe une unique factorisation $f : X \to E$ telle que :

$$f_n = \psi_n \circ f \quad \text{pour tout } n \geq 0$$

La limite projective est notée $\varprojlim E_n$. La situation est résumée par le schéma suivant :

$$\begin{array}{ccccccccc} & & X & & & & & & \\ & & {\scriptstyle f}\downarrow & \searrow^{f_n} & & & & & \\ \varprojlim E_n & \cdots & \xrightarrow{\varphi_{n+1}} & E_{n+1} & \xrightarrow{\varphi_n} & E_n & \longrightarrow & \cdots & \end{array}$$

**Théorème 4.3.** *Pour tout système projectif $(E_n, \varphi_n)_{n\in\mathbb{N}}$, il existe une limite projective $\varprojlim E_n \subset \prod_{n\geq 0} E_n$ avec $\psi_n$ données par les restrictions des projections.*
*De plus, si $(E'_n, \psi'_n)$ est une autre limite projective du même système, alors il existe une unique bijection $f : E' \to E$ telle que $\psi'_n = \psi_n \circ f$.*

*Démonstration.*

(i) *Existence.* Posons

$$E = \{(x_n)_{n\in\mathbb{N}},\ \varphi_n(x_{n+1}) = x_n\} \subset \prod_{n\geq 0} E_n$$

Ce sont les *suites cohérentes* relativement aux $\varphi_n$. Si $x \in E$ alors $\varphi_n(p_{n+1}(x)) = p_n(x)$. On peut donc considérer les restrictions $\psi_n$ des projections $p_n$ à $E$ et alors $\varphi_n \circ \psi_{n+1} = \psi_n$.

Montrons que l'ensemble $E$ ainsi construit muni des $\psi_n$ possède la propriété universelle requise. Considérons $E'$ et des applications $\psi_n^{'} : E' \to E_n$ tels que $\forall n \in \mathbb{N} \;\; \psi_n^{'} = \varphi_n \circ \psi_{n+1}^{'}$.

$$\psi^{'} : E' \to \prod_{n\geq 0} E_n, \; y \mapsto \psi_n^{'}(y)$$

La relation $\varphi_n(\psi_{n+1}^{'}(y)) = \psi^{'}$ implique que l'image de $\psi^{'}$ est incluse dans $E$. Il existe donc bien $f : E' \to E$ ayant la propriété voulue et c'est $\psi_n^{'}$ avec $E$ comme ensemble d'arrivée.

(ii) *Unicité.* Si $(E, (\psi_n))$ et $(E', (\psi_n^{'}))$ possède la propriété universelle de factorisation, alors il y a aussi une unique application $f' : E \to E'$ tel que $\psi_n = \psi_n^{'} \circ f'$. Par substitution :

$$\psi_n^{'} = \psi_n \circ f = \psi_n^{'} \circ f' \circ f$$

$f' \circ f$ est donc une factorisation de l'identité et puisque $(E', (\psi_n^{'}))$ est une limite projective du système, nécessairement $f' \circ f = Id_{E'}$. De la même manière, $f \circ f' = Id_E$. La preuve de l'unicité montre que le diagramme suivant est commutatif.

$$\begin{array}{ccccc} E & \xrightarrow{f} & E' & \xrightarrow{f'} & E \\ & \searrow & & \nearrow & \\ & & Id & & \end{array}$$

□

**Corollaire 4.4.** *Si pour un système projectif $(E_n, \varphi_n)_{n\in\mathbb{N}}$ les applications $\varphi_n$ sont surjectives, alors les projections $\psi_n$ de la limite projective $(E, \psi_n)$ le sont aussi. En particulier, $E$ est non vide.*

*Démonstration.* Par construction de $E$ par rapport à $\prod E_n$, il suffit de montrer que pour tout $x_n \in E_n$, il existe un élément de $E$ avec $x_n$ pour $n$-ème composantes. Par surjectivité des $\varphi_n$, on choisit $x_{n+1} \in E_{n+1}$ tel que $\varphi_n(x_{n+1}) = x_n$ et l'axiome du choix dénombrable permet de conclure. □

Si le système projectif $(E_n, \varphi_n)_{n\in\mathbb{N}}$ est formé d'espaces topologiques et d'applications continues, alors la construction précédente assure que la limite projective $(E, \psi_n)$ est un espace topologique muni d'applications continues.

**Proposition 4.5.** *Une limite projective de compacts non vides est non vide.*

*Démonstration.* Soit $(K_n, \varphi_n)$ un sytéme projectif constitué d'ensembles compacts. $\prod K_n$ est compact par le théorème de Tychonoff, et la limite projective du système est un fermé par construction ( $\cap_{n\geq 0}(\varphi_n \circ p_{n+1} - p_n)^{-1}(0)$ ). Donc $\varprojlim K_n$ est compact. Posons

$$\ldots \; K_n'' = \varphi_n(\varphi_{n+1}(K_{n+2})) \subset K_n' = \varphi_n(K_{n+1})$$

Ces ensembles sont compacts et non vides. Leurs intersection $L_n$ est non vide dans $K_n$. De plus $\varphi_n(L_{n+1}) = L_n$, et les restrictions des $\varphi_n$ aux $L_n$ nous donnent un système projectif avec des applications surjectives. Par le corollaire précédent on peut en déduire que la limite projective de ce système est non vide. De plus, $\varprojlim L_n \subset \varprojlim K_n$ ce qui conclut. □

**Corollaire 4.6.** *La limite projective d'ensembles non vides est non vide.*

## 4.2. Retour à $\mathbb{Z}_p$

Nous savons alors en partant des considérations précédentes que le système $(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n)$, avec $\varphi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ le morphisme canonique, admet une limite projective. Une conséquence est que l'on peut donner une seconde définition, équivalente à la première, des entiers $p$-adiques.

**Théorème 4.7.** *L'application* $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ *;* $x = \sum_{i=0}^{\infty} a_i p^i \mapsto (x_n = \sum_{i=0}^{n-1} a_i p^i)_{n\geq 0}$ *est un isomorphisme d'anneaux topologiques.*

*Démonstration.*

$$\varphi_n : \sum_{i=0}^{n} a_i p^i \mapsto \sum_{i=0}^{n-1} a_i p^i$$

Les séquences cohérentes dans $\prod \mathbb{Z}/p^n\mathbb{Z}$ sont les sommes partielles des séries formelles $\sum_{i=0}^{\infty} a_i p^i$ où $0 \leq a_i < p$, précisément les entiers $p$-adiques.

$$x_1 = a_0,\ x_2 = a_0 + a_1 p,\ \ldots \text{ et inversement } a_0 = x_1,\ a_1 = \frac{x_2 - x_1}{p},\ \ldots$$

Ces relations montrent que la factorisation $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ est bijective. C'est une application continue entre deux compacts, c'est donc un homéomorphisme. □

# 5. Corps des $p$-adiques $\mathbb{Q}_p$

**Définition 5.1.** $\mathbb{Z}_p$ est intègre donc le corps des fractions $Frac(\mathbb{Z}_p)$ est bien défini. Il est noté $\mathbb{Q}_p$.

**Proposition 5.2.** *Tout élément $x \in \mathbb{Z}_p$ peut se décomposer de façon unique $x = p^m u$ où $u \in \mathbb{Z}_p^\times$. A partir de cette écriture, $1/x = p^{-m}u^{-1} \in \mathbb{Q}_p$. Ainsi, $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$.*

De plus, écrit sous cette forme, $1/x \in p^{-m}\mathbb{Z}_p$ ce qui assure l'écriture $\mathbb{Q}_p = \bigcup_{m\in\mathbb{N}} p^{-m}\mathbb{Z}_p = \bigsqcup_{m\in\mathbb{Z}} p^m\mathbb{Z}_p^\times$.
La notion de valuation est étendue à $\mathbb{Q}_p$ : $\nu(x = p^m u) = m \in \mathbb{Z}$. Ainsi $\nu^{-1}(\{m\}) = p^m\mathbb{Z}_p^\times$.

$$\nu(x) \geq 0 \Leftrightarrow x \in \mathbb{Z}_p \;\; ; \;\; a,b\in \mathbb{Z}_p, b \neq 0 \Rightarrow \nu(\frac{a}{b}) = \nu(a) - \nu(b) \;\; ; \;\; \nu(x+y) \geq \min\{\nu(x),\nu(y)\}$$

**Proposition 5.3.** *La valuation $\nu : \mathbb{Q}_p \to \mathbb{Z}$ définit un morphisme et $\forall x \in \mathbb{Q}_p \;\; x = \sum_{k=\nu(x)}^{\infty} x_k p^k$.*

## 5.1. Parties entière et fractionnaire sur $\mathbb{Q}_p$

**Définition 5.4.** Soit $x = \sum_{\nu(x)}^{\infty} x_i p^i \in \mathbb{Q}_p$. On définit partie entière et partie fractionnaire de $x$ par :

$$[x] = \sum_{i\geq 0} x_i p^i \in \mathbb{Z}_p \text{ et } \langle x\rangle = \sum_{i<0} x_i p^i \in \mathbb{Z}[1/p] \quad : \quad x = [x] + \langle x\rangle \text{ assure } \mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p]$$

$$0 \leq \langle x\rangle = \sum_{i=\nu(x)}^{-1} x_i p^i < (p-1)\sum_{i\geq 1}\frac{1}{p^i} = 1 \text{ donc } \langle x\rangle \in [0,1[\cap\mathbb{Z}[1/p]$$

**Définition 5.5.** Notons, pour $m \in \mathbb{N}$, $\mu_m = \{z \in \mathbb{C},\ z^m = 1\}$, $\mu = \bigcup_{m\geq 1} \mu_m$ et $\mu_{p^\infty} = \bigcup_{k\geq 0} \mu_{p^k}$.

**Proposition 5.6.** *L'application $\tau : x \in \mathbb{Q}_p \mapsto \exp(2i\pi\langle x\rangle)$ est un morphisme de groupes de noyau $\mathbb{Z}_p$.*

En particulier, $\mathbb{Q}_p/\mathbb{Z}_p \simeq \mu_{p^\infty}$ et $x \in p^k\mathbb{Z}_p \Leftrightarrow \tau(x)^{p^k} = 1 \Leftrightarrow \tau(x) \in \mu_{p^k}$.

## 5.2. Structures sur $\mathbb{Q}_p$

### 5.2.1. Structure ultramétrique

**Définition 5.7.** L'application $x \mapsto |x| = p^{-\nu(x)}$ définit un morphisme $\mathbb{Q}_p^\times \to \mathbb{R}_+^*$ appelé valeur absolue $p$-adique. Par convention, $|\,0\,| = 0$.

$$x \neq 0 \Rightarrow |x| > 0 \;\; ; \;\; |xy| = |x|.|y| \;\; ; \;\; |x+y| \leq \max\{|x|,|y|\}$$

$|\,.\,|$ permet de définir une distance $d : (x,y) \mapsto |x-y|$ sur $\mathbb{Q}_p$ vérifiant pour $x,y,z \in \mathbb{Q}_p$ :

$x = y \Leftrightarrow d(x,y) = 0 \;\; ; \;\; d(x,y) = d(y,x) \;\; ; \;\; d(x,y) \leq \max\{d(x,y),d(z,y)\} \;\; ; \;\; d(zx,zy) = |z|d(x,y)$

**Proposition 5.8.** *$(\mathbb{Q}_p, d)$ est un corps (ultra)métrique muni d'une valuation, donc un corps topologique, localement compact.*

### 5.2.2. Structure additive

$$\mathbb{Q}_p = \mathbb{Z}_p + \mathbb{Z}[1/p] \text{ mais } \mathbb{Q}_p \neq \mathbb{Z}_p \oplus \mathbb{Z}[1/p] \text{ car } \mathbb{Z}_p \cap \mathbb{Z}[1/p] = \mathbb{Z}$$

Pour une décomposition $\mathbb{Q}_p = \mathbb{Z}_p \oplus \Gamma$, il faudrait : $\Gamma \cap \mathbb{Z}_p = \{0\}$ ce qui implique $\Gamma = \{0\}$.

L'unicité de la décomposition sur $\mathbb{Z}_p + [0,1) \cap \mathbb{Z}[1/p]$ donne le meilleur candidat 'supplémentaire', $[0,1) \cap \mathbb{Z}[1/p]$, qui n'est pas un sous-groupe de $(\mathbb{Q}_p^\times, \times)$.

## 5.3. Caractérisation des rationnels dans $\mathbb{Q}_p$

**Théorème 5.9.** *Soit* $x = \sum_{\nu(x)}^{\infty} x_i p^i \in \mathbb{Q}_p$. $x \in \mathbb{Q} \Leftrightarrow (x_i)$ *périodique à partir d'un certain rang.*

*Démonstration.* Quitte à multiplier par une puissance de $p$, on peut supposer $\nu(x) \geq 0$, i.e. $x \in \mathbb{Z}_p$. Si la suite $(x_i)$ est périodique à partir d'un certain rang $s$, alors $x$ est la somme d'un entier et d'une combinaison linéaire d'éléments de la forme $\sum_{j\geq 0} p^{s+jt} = \frac{p^s}{1-p^t} \in \mathbb{Q}$, et donc $x \in \mathbb{Q}$.
Réciproquement, supposons $x = \sum_{i\geq 0} x_i p^i = \frac{a}{b} \in \mathbb{Q}$.
On peut choisir $a$ et $b$ premiers entre eux. $b$ et $p$ sont aussi premiers entre eux. En ajoutant un entier suffisamment grand, on se ramène au cas $a$ et $b$, donc $x$, strictement positifs.

$$\sum_{j\leq\beta} b_j p^j . \sum_{i\geq 0} x_i p^i = \sum_{k\leq\alpha} a_k p^k \text{ donc } \sum_{k=0}^{l} b_k x_{l-k} = a_l + r_{l+1} p$$

De là, pour $l > \max\{\alpha, \beta\}$, $b_0 x_l + ... + b_\beta x_{l-\beta} + r_l = r_{l+1} p$. Il suffit de calculer $x_l \ mod\ p$ en fonction des termes précédents. Cet algorithme permet de calculer $(x_l, ..., x_{l-\beta}, r_l) \in (\mathbb{Z}/p\mathbb{Z})^{\beta+1}$. L'ensemble $(\mathbb{Z}/p\mathbb{Z})^{\beta+1}$ étant fini, l'algorithme produit un résultat cyclique. □

**Exemple 5.10.** Les entiers $p$-adiques $\sum_{n=0}^{\infty} p^{n^2}$ et $\sum_{n=0}^{\infty} p^{n!}$ ne sont pas rationnels.

## 6. Lemme de Hensel

**Proposition 6.1.** *Les propriétés suivantes sont équivalentes pour $P \in \mathbb{Z}[X,Y]$ :*

*(i)* *$P$ a une racine dans $\mathbb{Z}_p$.*

*(ii)* *$\forall n \geq 0$, $P = 0$ a une solution dans $\mathbb{Z}/p^n\mathbb{Z}$.*

*(iii)* *$\forall n \geq 0$, il existe $(a_n, b_n) \in \mathbb{Z}^2$ tel que $P(a_n, b_n) = 0 \ (mod\ p^n)$.*

*Démonstration.* $(iii) \Leftrightarrow (ii)$ Clair.
$(i) \Rightarrow (ii)$ Pour $x = \sum_{i \geq 0} a_i p^i$ posons $x_n = \sum_{i<n} a_i p^i \ (mod\ p^n) \ \in \mathbb{Z}/p^n\mathbb{Z}$. Ainsi pour $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p$, on a

$$P(x_n, y_n) = P(x,y) \ (mod\ p^n)$$

$(ii) \Rightarrow (i)$ Considérons les ensembles suivants

$$X_n = \{(x,y) \in \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}; P(x,y) = 0\}$$

La réduction modulo $p^n$ fournit une application $\varphi_n : X_{n+1} \to X_n$ qui nous donne un système projectif. Ce système admet une limite projective $X \subset \mathbb{Z}_p \times \mathbb{Z}_p$. Les éléments de $X$ sont solutions de $P = 0$. $X$ est non vide par le corollaire de la proposition 4.4. □

**Proposition 6.2.** *Soit $A$ un anneau, $P \in A[X]$ alors il existe $P_1, P_2 \in A[X,Y]$ tel que*

$$P(X+h) = P(X) + hP_1(X,h) = P(X) + hP'(X) + h^2 P_2(X,h)$$

*Démonstration.* En posant $P(X) = \sum a_n X^n$ alors

$$\begin{aligned} P(X+h) = \sum a_n (X+h)^n &= \sum a_n (X^n + nX^{n-1}h + h^2(\ldots)) \\ &= \sum a_n X^n + \sum n a_n X^{n-1} + h^2 P_2(X,h) \end{aligned}$$

□

La proposition suivante permet de montrer que l'on peut toujours obtenir une meilleure approximation d'une racine d'un polynôme à coefficients $p$-adiques.

**Proposition 6.3.** *Soit $P \in \mathbb{Z}_p[X]$ et $x \in \mathbb{Z}_p$ tel que $P(x) \equiv 0$ mod $p^n$ pour un certain $n \in \mathbb{N}$. Si $k = \nu(P'(x)) < n/2$, alors $x_1 = x - P(x)/P'(x)$ satisfait*

*(i)* *$P(x_1) \equiv 0 \ (mod\ p^{n+1})$*

*(ii)* *$x_1 \equiv x \ (mod\ p^{n-k})$*

*(iii)* *$\nu(P'(x_1)) = \nu(P'(x))$*

*Démonstration.* Posons $P(x) = p^n y$ pour $y \in \mathbb{Z}_p$, et $P'(x) = p^k u$ pour $u \in \mathbb{Z}_p^*$. Par définition de $x_1$ dans la proposition précédente

$x_1 - x = -P(x)/P'(x) = p^{n-k} y u^{-1} \in p^{n-k}\mathbb{Z}_p$ et $P(x_1) = P(x) - P(x)/P'(x)P'(x) + (x_1 - x)^2 t$ où $t \in \mathbb{Z}_p$

Ainsi

$$P(x_1) = (x_1 - x)^2 t \in p^{2n-2k}\mathbb{Z}_p \subset p^{n+1}\mathbb{Z}_p \ n > 2k$$

De plus

$$P'(x_1) = P'(x + (x_1 - x)) = P'(x) + (x_1 - x)s = p^k u + p^{n-k} zs = p^k v$$

On a alors

$$v = u + p^{n-2k} zs \in up\mathbb{Z}_p \in \mathbb{Z}_p^\times$$

Cela montre que $\nu(P'(x_1)) = \nu(P'(x))$ comme voulu. □

Ce résultat est à mettre en rapport avec la méthode de Newton sur $\mathbb{R}$ pour trouver les zéros d'une fonction $f$, $C^1$. Cette méthode consiste à supposer que l'on part d'un réel $x_0$ proche d'un zéro de $f$ où la pente $f'(x_0)$ ne soit pas nulle. On définit alors par récurrence $x_{n+1}$ comme l'abscisse à laquelle la tangente à $f$ en $x_n$ coupe l'axe des abscisses. La suite ainsi définie converge quadratiquement vers une zéro de $f$.

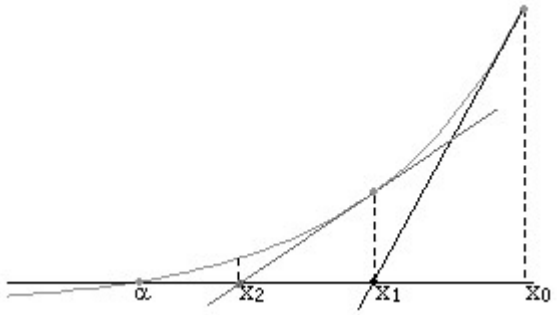



FIGURE 3 – Illustration de la méthode de Newton

Le résultat suivant permet de construire une racine à un polynôme dont on connaît une "racine approchée".

**Théorème 6.4** (**Lemme de Hensel**). *Soit $P \in \mathbb{Z}_p[X]$. S'il existe $a \in \mathbb{Z}_p[X]$ et $N \in \mathbb{N}$ tels que $P(a) \equiv 0 \ mod\ p^N$ et si $k = \nu(P'(a)) < N/2$, alors il existe une unique racine $\varepsilon$ de $P$ dans $\mathbb{Z}_p$ tel que*

$$\varepsilon \equiv a \ mod\ p^{N-k} \ et\ \nu(P'(a)) = \nu(P'(\varepsilon))$$

*Démonstration.*

(i) *Existence* Pour $x_0 = a$, construisons $x_1 \in \mathbb{Z}_p$ une racine "plus précise" (On utilise la proposition précédente), c'est-à-dire une racine vérifiant :

$$x_1 \equiv x_0 \ mod\ p^{N-k} \quad P(x_1) \equiv 0 \ mod\ p^{N+1} \text{ et } \nu(P'(x_0)) = \nu(P'(x_1))$$

De façon similaire on peut obtenir un entier $p$-adique $x_2$ satisfaisant

$$x_2 \equiv x_1 \ mod\ p^{N+1-k} \quad P(x_2) \equiv 0 \ mod\ p^{N+2}$$

En itérant cette construction on obtient une suite de Cauchy $(x_n)_{n\geq 0}$ ayant une limite $p$-adique car $\mathbb{Z}_p$ est complet. Cette limite $\varepsilon$ satisfait $\varepsilon \equiv a \ mod\ p^{N-k}$ et $P(\varepsilon) = 0$.

(ii) *Unicité* Soit $\varepsilon$ et $\eta$ deux racines de $P$ satisfaisant les conditions du théorème. Alors en particulier, $\eta \equiv \varepsilon \ (mod\ p^{N-k})$, et comme $n > 2k$ on a $n - k > k$. Et donc $\eta \equiv \varepsilon \ (mod\ p^{k+1})$. Alors

$$P(\eta) = P(\varepsilon) + P'(\varepsilon)(\eta - \varepsilon) + (\eta - \varepsilon)^2 b$$

pour un certain entier $p$-adique $b$. Ainsi

$$(\eta - \varepsilon)(P'(\varepsilon) + (\eta - \varepsilon)b) = 0$$

Mais en raisonnant sur l'ordre, $P'(\varepsilon) + (\eta - \varepsilon)b \neq 0$. Par intégrité de $\mathbb{Z}_p$, $\eta = \varepsilon$.

□

# 7. Applications du lemme de Hensel

## 7.1. Inversibles de $\mathbb{Z}_p$

Considérons le polynôme $P = aX - 1$, avec $a \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. $P$ admet une racine approchée *mod* $p$ car $a_0$ est non nul, donc inversible dans le corps $\mathbb{F}_p$.
De plus, $P'(x) = a$ et $\nu(a) = 0$ ($a$ inversible), donc cette racine *mod* $p$ peut être améliorée en une racine *mod* $p^n$ pour $n \in \mathbb{N}$.
Par le lemme de Hensel, il existe $\xi \in \mathbb{Z}_p$ tel que $P(\xi) = 0$, i.e. $a\xi = 1$. $\xi$ fournit un inverse pour $a$.
D'où l'inclusion $\mathbb{Z}_p \setminus p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$.

Réciproquement, $a$ inversible $\Rightarrow \varepsilon(a)$ inversible dans $\mathbb{F}_p \Rightarrow a_0 \neq 0$. Donc $\mathbb{Z}_p^\times \subset \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

## 7.2. Racines $n$-ièmes de l'unité dans $\mathbb{Z}_p$

Soit $\xi$ une racine $n$-ième de l'unité dans $\mathbb{Q}_p$ : $\xi^n = 1$. $n\nu(\xi) = \nu(1) = 0$ donc $\nu(\xi) = 0$.
Les racines $n$-ièmes de l'unité de $\mathbb{Q}_p$ sont donc des inversibles de $\mathbb{Z}_p$. En particulier, chaque racine a une réduction *mod* $p$ dans $\mathbb{F}_p^\times$.

Considérons le polynôme $P = X^{p-1} - 1$. $P' = (p-1)X^{p-2}$ et $x \in \mathbb{Z}_p^\times \Rightarrow x^{p-2} \in \mathbb{Z}_p^\times \Rightarrow \nu(P'(x)) = 0$.
Les $p-1$ éléments de $\mathbb{F}_p^\times$ fournissent des racines distinctes de $P$ dans $\mathbb{F}_p$. Le lemme de Hensel assure alors l'existence de $p-1$ racines distinctes dans $\mathbb{Z}_p^\times$. Autrement dit, $\mathbb{Q}_p$ contient toujours un groupe cyclique d'ordre $p-1$ constitué de racines de l'unité.

**Proposition 7.1.** *Si $p$ est impair (i.e. $p \neq 2$), alors le groupe des racines de l'unité de $\mathbb{Q}_p$, noté $\mu(\mathbb{Q}_p)$, est $\mu_{p-1}$, les racines $p-1$-ièmes de l'unité.*

*Démonstration.* Montrons que la réduction *mod* $p$ $\varepsilon : \mu(\mathbb{Q}_p) \to \mathbb{F}_p^\times$ est bijective.

(i) Par ce qui précède, $\varepsilon$ est surjective.

(ii) Soit $\zeta = 1 + pt \in \ker \varepsilon$ une racine de l'unité d'ordre $n$ : $\zeta^n = 1$. Puisque $p \neq 0$, en développant :

$$t\Big(n + \binom{n}{2}pt + ... + p^{n-1}t^{n-1}\Big) = 0 \text{ donc } t = 0 \text{ ou } p|n$$

Si $t = 0$ alors $\zeta = 1$ et on conclut : $\ker \varepsilon = \{1\}$, $\varepsilon$ est injective.
Sinon, la relation précédente pour $\zeta^{\frac{n}{p}}$ et $\frac{n}{p}$ donne $t = 0$ ou $p^2|n$. En itérant, on se ramène à $n = p$.

$$t\Big(p + \binom{p}{2}pt + ... + p^{p-1}t^{p-1}\Big) = 0 \text{ et } p + \binom{p}{2}pt + ... + p^{p-1}t^{p-1} \neq 0 \text{ donc } t = 0$$

□

## 7.3. Automorphisme(s) de corps de $\mathbb{Q}_p$

**Lemme 7.2.** *Soit $x \in \mathbb{Q}_p^\times$. $x \in \mathbb{Z}_p^\times \Leftrightarrow x^{p-1}$ possède une racine $n$-ième pour une infinité de $n$.*

*Démonstration.*

(i) Si $x \in \mathbb{Z}_p^\times$ alors $x \not\equiv 0 \ mod\ p$ et $x^{p-1} \equiv 1 \ mod\ p$. Soit $a = x^{p-1}$.
1 est une racine approchée *mod* $p$ du polynôme $P = X^n - a$ et $P'(1) = n$ qui ne s'annule pas *mod* $p$ si $n$ n'est pas multiple de $p$. Le lemme de Hensel fournit alors une racine $\xi \in \mathbb{Z}_p$ vérifiant $\xi^n = a = x^{p-1}$.

(ii) Réciproquement, si $x^{p-1} = y_n^n$ avec $\forall n \in \mathbb{N} \quad y_n \in \mathbb{Q}_p^\times$, alors $(p-1)\nu(x) = n\nu(y_n)$, donc $n$ divise $(p-1)\nu(x)$. Ceci étant vrai pour une infinité de $n$, $\nu(x) = 0$, i.e. $x \in \mathbb{Z}^\times$.

□

**Théorème 7.3.** *Le seul automorphisme de corps de $\mathbb{Q}_p$ est l'identité.*

*Démonstration.* Soit $\varphi$ un automorphisme de corps de $\mathbb{Q}_p$. Le lemme précédent assure que $\mathbb{Z}_p^\times$ est stable par $\varphi$. De plus, $\varphi$ est trivial sur $\mathbb{Q}$.
Soit $x \in \mathbb{Q}_p^\times$. Il existe une décomposition $x = p^m u$ avec $m = \nu(x)$ et $u \in \mathbb{Z}_p^\times$.

$$\varphi(x) = \varphi(p^m u) = \varphi(p^m)\varphi(u) = p^m \varphi(u) \text{ avec } \varphi(u) \in \mathbb{Z}_p^\times$$

$\nu(\varphi(x)) = \nu(x)$ et $\varphi$ préserve la valuation des $p$-adiques, donc $\varphi$ est continu.
Soit $y \in \mathbb{Q}_p$. Soit $(r_n) \in \mathbb{Q}^{\mathbb{N}}$, $r_n \xrightarrow[n\to\infty]{} y$. Par continuité :

$$\varphi(y) = \varphi(\lim_{n\to\infty} r_n) = \lim_{n\to\infty} \varphi(r_n) = \lim_{n\to\infty} r_n = y$$

□