Le bâton des aveugles

« Il faut que les mathématiques domptent les écarts de notre raison; c'est le bâton des aveugles, on ne marche point sans elles... » Voltaire.

Introduction à l'étude des nombres *p*-adiques

Jean DE BIASI
Faculté des Sciences de Toulouse.

K est un corps supposé commutatif. Ses éléments neutres sont respectivement notés 0 et 1. L'entier n de K est l'élément ainsi défini :

$$n = \underbrace{1 + 1 + \ldots + 1}_{n \text{ fois}}$$

$\mathbb{Q}$ et $\mathbb{R}$ sont respectivement le corps des rationnels et le corps des réels.

1. Corps valués.

1.1. Définitions.

• *Une valeur absolue* φ *sur un corps K est une application de K dans* $\mathbb{R}$ *satisfaisant aux axiomes suivants.*

$$a_1 \begin{cases} \varphi(x) > 0 & \forall x \neq 0 \\ \varphi(0) = 0 \end{cases}$$

$$a_2 : \varphi(x + y) \leqslant \varphi(x) + \varphi(y)$$

$$a_3 : \varphi(x\,y) = \varphi(x).\varphi(y)$$

• *Un corps K muni d'une valeur absolue* φ *est un corps valué noté* $K(\varphi)$.

• *Un corps valué est immédiatement muni d'une métrique (ou distance)* d_φ *grâce à la définition :*

$$d_\varphi(x,\ y) = \varphi(x - y)$$

(Il est aisé de constater que les axiomes

$$d_1 \begin{cases} d_\varphi(x, y) \in \mathbb{R}^+ \\ d_\varphi(x, y) = 0 \Leftrightarrow x = y \end{cases}$$
$$d_2 : d_\varphi(x, y) = d_\varphi(y, x)$$
$$d_3 : d_\varphi(x, z) \leqslant d_\varphi(x, y) + d_\varphi(y, z)$$

sont bien vérifiés et que par suite d_φ est une distance).

• *Un corps valué est ainsi un espace métrique particulier appelé corps métrique.*

1.2. Exemples.

1.2.1. Pour tout corps K, la métrique triviale t définie par

$$t(0) = 0; \quad \forall x \neq 0 \qquad t(x) = 1$$

1.2.2. $\mathbb{Q}$ et $\mathbb{R}$ avec la valeur absolue habituelle définie par

$$|x| = \text{Max } (x, -x)$$

1.3. Propriétés immédiates.

• $\varphi(1) = 1$ car $\varphi(1) = \varphi(1.1) = \varphi(1).\varphi(1) = \varphi(1)^2$

d'où $\varphi(1)[1 - \varphi(1)] = 0$ et comme $\varphi(1) \neq 0$ on a $\varphi(1) = 1$.

• $\varphi(-x) = \varphi(x)$ car $[\varphi(-x)]^2 = \varphi((-x)^2) = \varphi(x^2) = [\varphi(x)]^2$

d'où $\varphi(-x) = \pm\varphi(x)$ et d'après a_1 : $\varphi(-x) = \varphi(x)$.

• $\varphi(n) \leqslant n$ car $\varphi(n) = \varphi\left(\underbrace{1 + 1 + \ldots + 1}_{n \text{ fois}}\right) \leqslant \underbrace{\varphi(1) + \ldots + \varphi(1)}_{n \text{ fois}} = n$

• $|\varphi(x) - \varphi(y)| \leqslant \varphi(x - y)$

car $\begin{cases} \varphi(x) \leqslant \varphi(x - y) + \varphi(y) \Rightarrow \varphi(x) - \varphi(y) \leqslant \varphi(x - y) \\ \varphi(y) \leqslant \varphi(y - x) + \varphi(x) \Rightarrow \varphi(y) - \varphi(x) \leqslant \varphi(y - x) = \varphi(x - y) \end{cases}$

Conséquence importante :
Si (x_n) est une suite de Cauchy de $K(\varphi)$, $(\varphi(x_n))$ est une suite de Cauchy de $\mathbb{R}$.

2. Complétion d'un corps valué.

2.1. Suites de Cauchy dans un corps valué.

Une suite (x_n) d'éléments d'un corps valué $K(\varphi)$ est dite de Cauchy pour la métrique associée à φ si $\varphi(x_n - x_m)$ tend vers zéro quand n et m tendent vers $+\infty$.

Toutes les propriétés des suites de Cauchy d'un espace métrique sont évidemment valables ici.

2.2. *Corps valué complet.*

Un corps valué $K(\varphi)$ est dit complet pour la métrique associée à φ si toute suite de Cauchy pour cette métrique est convergente dans K.

2.3. *Théorème de complétion.*

Pour tout corps valué $K(\varphi)$ il existe un corps valué complet $\widehat{K}(\widehat{\varphi})$ contenant K comme sous corps partout dense. Ce corps $\widehat{K}$ est unique à tout isomorphisme près laissant fixes les éléments de K. $\widehat{K}$ est le complété de K pour la métrique associée à φ.

Disons qu'un corps valué $K_1(\varphi_1)$ est un sous-corps du corps valué $K_2(\varphi_2)$ si

$$x \in K_1 \Rightarrow x \in K_2$$
$$\forall x \in K_1 \ : \varphi_1(x) = \varphi_2(x)$$

Disons de plus que K_1 est partout dense dans K_2 si, au sens habituel des espaces topologiques, $\overline{K}_1 = K_2$.

Démonstration : Elle est calquée presque mot pour mot sur la démonstration de l'existence et sur la construction de $\mathbb{R}$ corps des réels à partir de $\mathbb{Q}$ corps des rationnels. Nous renvoyons le lecteur à un ouvrage quelconque du premier cycle ou de Spéciales par exemple (I). Indiquons rapidement les différentes étapes :

• Dans l'ensemble $\mathcal{S}_c(K)$ des suites de Cauchy d'éléments de K on démontre que l'ensemble I des suites de Cauchy équivalentes à zéro ($\varphi(x_n) \xrightarrow[n \to \infty]{} 0$) est un idéal maximal.

• Dans $\mathcal{S}_c(K)$ la relation

$$(x_n)\, \mathcal{R}(y_n) \Leftrightarrow (x_n - y_n) \in I$$

est alors une relation d'équivalence qui, parce que $\mathcal{S}_c(K)$ admet un élément unité ($x_n = 1$ pour tout n) et I est maximal fait de $\dfrac{\mathcal{S}_c(K)}{I}$ un corps $\widehat{K}$.

Après l'identification classique de l'élément x de K avec la classe d'équivalence de la suite (x) ($x_n = x$ pour tout n), identification faisant de K un sous ensemble de $\dfrac{\mathcal{S}_c(K)}{I} = \widehat{K}$ et l'extension de la valeur absolue φ à $\widehat{K}$ de la manière suivante :

[Soit x un élément de $\widehat{K}$ défini par la classe d'équivalence $\mathcal{C}(x)$ de suites de Cauchy d'éléments de K et soit (x_n) l'une de ces suites :

— $\varphi(x_n)$ est une suite de Cauchy dans $\mathbb{R}$ et converge donc vers un nombre réel que l'on note par définition $(\widehat{\varphi}x)$;

— $\widehat{\varphi}(x)$ ne dépend pas de la suite choisie dans $\mathcal{C}(x)$: en effet pour deux telles suites (équivalentes par hypothèse) on a :

$$|\varphi(x_n) - \varphi(y_n)| \leqslant \varphi(x_n - y_n) \xrightarrow[n \to \infty]{} 0;$$

— on contrôle alors que $\widehat{\varphi}$ est bien une valeur absolue et que $\widehat{\varphi}(x) = \varphi(x)$ pour x dans K.]

On constate que $\widehat{K}$ est le corps cherché.

$\widehat{K}(\varphi)$ sur-corps de $K(\varphi)$ étant construit on vérifie alors que :

• *$K(\varphi)$ est partout dense dans $\widehat{K}(\widehat{\varphi})$.* En effet, montrons que toute suite (x_n) de la classe $\mathcal{C}(x)$ définissant x converge vers x au sens de la métrique $\widehat{\varphi}$ de $\widehat{K}$. (x_n) étant une suite de Cauchy on a :

$$\forall \varepsilon > 0 \ \exists N;\ n,\ m > N \Rightarrow \varphi(x_n - x_m) < \varepsilon$$

Fixant n et faisant tendre m vers $+\infty$, par définition même de $\widehat{\varphi}$, $\varphi(x_n - x_m)$ tend vers $\widehat{\varphi}(x_n - x)$ et l'inégalité se conservant on a démontré que :

$$\forall \varepsilon > 0 \ \exists N;\ n > N \Rightarrow \widehat{\varphi}(x_n - x) < \varepsilon$$

et par suite (x_n) converge vers x dans $\widehat{K}(\varphi)$.

• *$\widehat{K}(\varphi)$ est complet.* Soit (X_n) une suite de Cauchy dans $\widehat{K}(\varphi)$. Puisque X_n est limite d'une suite d'éléments de K il existe un élément x_n de K tel que $\widehat{\varphi}(X_n - x_n) < \frac{1}{n}$. La suite (X_n) étant de Cauchy la suite (x_n) l'est aussi et converge donc vers un élément X de $\widehat{K}$. On vérifie alors sans difficulté que (X_n) converge vers X dans $\widehat{K}$.

• *$\widehat{K}(\varphi)$ est unique à un isomorphisme près laissant K invariant.* Soit K_1 un autre corps complet tel que K soit partout dense dans K_1 et dans $\widehat{K}$. Pour α élément de $\widehat{K}$ il existe une suite de Cauchy (x_n) de K convergente vers α; mais (x_n) converge également vers un élément α_1 de K_1. On vérifie que α_1 ne dépend que de la classe de (x_n) et donc que de α et ensuite que la correspondance $\alpha \mapsto \alpha_1$ réalise un isomorphisme entre $\widehat{K}$ et K_1 laissant K invariant.

$\widehat{K}$ est le *complété* de K pour la métrique associée à la valeur absolue φ. On peut alors le noter classiquement $\overline{K}$; d'autre part comme $\widehat{\varphi} = \varphi$ sur K on notera φ également la valeur absolue prolongée à $\overline{K}$.

3. Les valeurs absolues du corps Q des nombres rationnels.

Dans le corps $\mathcal{Q}$, nous connaissons :

3.1. La valeur absolue triviale.

3.2. La valeur absolue $\varphi_\alpha(x) = |x|^\alpha$ avec $0 < \alpha \leqslant 1$.

En effet on sait déjà que $\varphi_1(x) = |x|$ est une valeur absolue. Montrons que $\varphi_\alpha(x) = |x|^\alpha$ avec $0 < \alpha \leqslant 1$ en est encore une.

Seul a_2 n'est pas évident; démontrons-le en supposant, ce qui ne restreint pas la généralité, que $|x| \geqslant |y| > 0$ on a :

$$|x+y|^\alpha = \left|x\left(1+\frac{y}{x}\right)\right|^\alpha = |x|^\alpha \left|1+\frac{y}{x}\right|^\alpha \leqslant |x|^\alpha \left(1+\left|\frac{y}{x}\right|\right)^\alpha$$

$$\leqslant |x|^\alpha \left(1+\left|\frac{y}{x}\right|\right) \leqslant |x|^\alpha \left(1+\left|\frac{y}{x}\right|^\alpha\right) = |x|^\alpha + |y|^\alpha$$

Remarquons que $\varphi_\alpha(x)$ définit la même notion de convergence que $\varphi_1(x)$ puisque

$$\varphi_1(x) \to 0 \Leftrightarrow |x| \to 0 \Leftrightarrow |x|^\alpha \to 0 \Leftrightarrow \varphi_\alpha(x) \to 0.$$

Les espaces métriques $\mathcal{Q}(d\varphi_1)$ et $\mathcal{Q}(d\varphi_\alpha)$ sont donc identiques.

3.3. La valeur absolue p-adique $\varphi_p(x)$.

Celle-ci est définie, p étant un nombre premier quelconque, par

$$\begin{cases} \varphi_p(0) = 0 \\ \varphi_p(x) = \rho^{v_p(x)} \end{cases}$$

où ρ est un nombre donné tel que $0 < \rho < 1$ et $v_p(x)$ est l'exposant de p dans la décomposition de x en facteurs premiers (ainsi $\varphi_3(4) = 1$; $\varphi_5\left(\frac{1}{5}\right) = \frac{1}{\rho}$; $\varphi_2(8) = \rho^3$ ...).

Montrons que φ_p est bien une valeur absolue. Ici encore démontrons seulement a_2.

Tout nombre rationnel $x \neq 0$, s'écrit :

$$x = \frac{s}{t}p^n \text{ où } n \in \mathbb{N} \text{ et } s \text{ et } t \text{ sont premiers avec } n.$$

Dans ces conditions pour

$$x = \frac{s}{t}p^n \quad \text{et} \quad y = \frac{u}{v}p^m$$

où l'on suppose par exemple $\varphi_p(y) \geqslant \varphi_p(x)$, c'est-à-dire $n \geqslant m$, on a :

$$x + y = \frac{svp^{n-m} + tu}{tv} p^m$$

d'où $\varphi_p(x + y) = \rho^{m'}$ avec $m' \geqslant m$ (car tv est premier avec p) et par suite

$$\varphi_p(x + y) \leqslant \varphi_p(y) = \text{Max}[\varphi_p(x), \varphi_p(y)] \leqslant \varphi_p(x) + \varphi_p(y)$$

La métrique introduite par φ_p vérifie aussi l'inégalité

$$d_\varphi(x, z) \leqslant \text{Max } [d_\varphi(x, y), d_\varphi(y, z)]$$

plus forte due d_2. Une telle métrique est appelée une *ultramétrique*.

Remarquons ici aussi que pour deux nombres ρ_1 et ρ_2 compris entre 0 et 1 les métriques définies par un même nombre premier p et par ces deux nombres définissent la même notion de convergence dans $\mathbb{Q}$ puisque :

$$\varphi_p^{(1)}(x) \to 0 \Leftrightarrow \rho_1^{(x)} \to 0 \Leftrightarrow \rho_2^{(x)} \to 0 \Leftrightarrow \varphi_p^{(2)}(x) \to 0$$

On choisit en général $\rho = \frac{1}{p}$ et φ_p est alors la *valeur absolue p-adique normalisée.*

3.4. Théorème d'Ostrowski (II).

Les valeurs absolues du type $\varphi_\alpha(x) = |x|^\alpha$ *et les valeurs absolues* p-*adiques pour tout entier premier p sont les seules valeurs absolues non triviales du corps* $\mathbb{Q}$ *des nombres rationnels.*

Soit φ une valeur absolue non triviale de $\mathbb{Q}$. Deux cas sont possibles :

— ou bien il existe $a \in \mathbb{N}$ tel que $\varphi(a) > 1$ (Remarquer que nécessairement : $a \geqslant 2$);

— ou bien $\varphi(n) \leqslant 1$ quel que soit $n \in \mathbb{N}$.

• *Premier cas.* Il existe $a \in \mathbb{N}$ tel que $\varphi(a) > 1$.

Puisque (1, 3), $\varphi(n) \leqslant n$, quel que soit n, il existe α réel avec $0 < \alpha \leqslant 1$ tel que $\varphi(a) = a^\alpha$.

Décomposons alors tout entier n suivant les puissances successives de a.

$$n = n_0 + n_1 a + n_2 a^2 + \ldots n_{k-1} a^{k-1}$$

avec $a^{k-1} \leqslant n < a^k$; $0 \leqslant n_i \leqslant a - 1$; $n_{k-1} \geqslant 1$.

(C'est l'écriture de n dans le système de base a.)

Les propriétés de la valeur absolue et les affirmations précédentes permettent d'écrire :

$$\varphi(n) \leqslant \varphi(n_0) + \sum_{i=1}^{i=k-1} \varphi(n_i)\varphi(a)^i$$

$$\varphi(n) \leqslant (a-1)(1 + a^{\alpha} + \ldots + a^{(k-1)\alpha}) = (a-1)\frac{a^{k\alpha}-1}{a^{\alpha}-1}$$
$$< (a-1)\frac{a^{k\alpha}}{a^{\alpha}-1} = \frac{(a-1)a^{\alpha}}{a^{\alpha}-1}\, a^{(k-1)\alpha}$$
$$\leqslant \frac{(a-1)a^{\alpha}}{a^{\alpha}-1}\, n^{\alpha} = \mu n^{\alpha}$$

Ainsi on a :

$$\varphi(n) \leqslant \mu n^{\alpha} \qquad \text{avec } \mu \text{ indépendant de } n.$$

Mais remplaçant n par n^m il vient :

$$\varphi(n^m) = (\varphi(n))^m \leqslant \mu n^{m\alpha}$$

d'où

$$\varphi(n) \leqslant \mu^{\frac{1}{m}} n^{\alpha}$$

Lorsque m augmente indéfiniment $\mu^{\frac{1}{m}}$ tend vers 1 et par suite :

$$\underline{\varphi(n) \leqslant n^{\alpha}} \qquad (1)$$

Posons maintenant $n = a^k - b$ avec $0 < b \leqslant a^k - a^{k-1}$; on a :

$$\varphi(n) \geqslant \varphi(a^k) - \varphi(b) = a^{k\alpha} - \varphi(b)$$

Mais

$$\varphi(b) \leqslant b^{\alpha} \leqslant (a^k - a^{k-1})^{\alpha}$$

d'où :

$$\varphi(n) \geqslant a^{k\alpha} - (a^k - a^{k-1})^{\alpha} = a^{k\alpha}\left[1 - \left(1 - \frac{1}{a}\right)^{\alpha}\right] = \mu_1 a^{k\alpha} \geqslant \mu_1 n^{\alpha}$$

Ainsi

$$\varphi(n) \geqslant \mu_1 n^{\alpha} \quad \text{avec } \mu_1 \text{ indépendant de } n$$

Remplaçant ici encore n par n^m et faisant tendre m vers $+\infty$, on aboutit à l'inégalité

$$\boxed{\varphi(n) \geqslant n^{\alpha}} \qquad (2)$$

(1) et (2) impliquent alors :

$$\boxed{\forall n \in \mathbb{N} : \ \varphi(n) = n^{\alpha} \quad (0 < \alpha \leqslant 1)} \qquad (3)$$

x étant maintenant un nombre rationnel quelconque, $\pm \frac{p}{q}$ avec p et q positifs, on déduit de (3) que :

$$\varphi(x) = \varphi\left(\frac{p}{q}\right) = \frac{\varphi(p)}{\varphi(q)} = \frac{p^{\alpha}}{q^{\alpha}} = \left(\frac{p}{q}\right)^{\alpha}$$

d'où la

***Proposition 1** : S'il existe un nombre entier naturel a tel que $\varphi(a) < 1$ la valeur absolue φ est alors du type :*

$$\varphi(x) = |x|^{\alpha} \quad \textit{avec} \quad 0 < \alpha \leqslant 1.$$

$\mathbb{Q}$ n'est pas complet pour la métrique associée à φ_α; son complété est $\mathbb{R}$.

• *Deuxième cas :* $\varphi(n) \leqslant 1 \quad \forall n \in \mathbb{N}$.

Si l'on a $\varphi(p) = 1$ pour tout nombre premier p, alors pour tout nombre entier naturel n dont la décomposition en facteurs premiers est

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

on a :

$$\varphi(n) = \varphi(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = \varphi(p_1)^{\alpha_1} \varphi(p_2)^{\alpha_2} \dots \varphi(p_k)^{\alpha_k} = 1$$

et par suite pour $x = \pm \frac{p}{q}$, il vient

$$\varphi(x) = \varphi\left(\frac{p}{q}\right) = \frac{\varphi(p)}{\varphi(q)} = 1$$

et φ est la valeur absolue triviale, cas écarté.

Il existe donc un nombre premier p tel que $\varphi(p) < 1$. Montrons qu'il ne peut pas en exister un autre, q, vérifiant cette inégalité stricte.

En effet si

$$\varphi(p) < 1 \quad \text{et} \quad \varphi(q) < 1$$

Choisissant k et l entiers naturels assez grands on réaliserait

$$(\varphi(p))^k < \frac{1}{3} \quad \text{et} \quad (\varphi(q))^l < \frac{1}{3}$$

or p et q étant premiers sont premiers entre eux et il en est de même de p^k et de q^l. Alors l'identité de Bezout implique l'existence de deux entiers relatifs u et v tels que

$$up^k + vq^l = 1$$

Mais dans ces conditions

$$\varphi(1) = 1 = \varphi(up^k + vq^l) \leqslant \varphi(up^k) + \varphi(vq^l)$$
$$\leqslant \varphi(u)(\varphi(p))^k + \varphi(v)(\varphi(q))^l < 1 \cdot \frac{1}{3} + 1 \cdot \frac{1}{3} = \frac{2}{3}$$

Cette contradiction démontre l'unicité du nombre premier p tel que $\varphi(p) = p < 1$.

Alors pour tout autre nombre premier q, $\varphi(q) = 1$ et il en est de même pour tout nombre entier relativement premier avec p (ne contenant pas p comme facteur premier).

Enfin pour tout nombre rationnel x on a :

$$x = \pm p^m \frac{a}{b} \text{ où } a \text{ et } b \text{ sont premiers avec } p$$

d'où $$\varphi(x) = \varphi(p)^m \varphi\left(\frac{a}{b}\right) = \rho^m \frac{\varphi(a)}{\varphi(b)} = \rho^m = \rho^{v_p(x)}$$

d'où la

Proposition 2 : *Si pour tout entier naturel n on a* $\varphi(n) \leqslant 1$ *il existe un nombre premier unique p tel que* $\varphi(p) = \rho < 1$ *et la valeur absolue* φ *coïncide avec la valeur absolue p-adique* φ_p *définie par* $\varphi_p(x) = \rho^{v_p(x)}$

Les propositions (1) et (2) démontrent le théorème d'Ostrowski.

$\mathbb{Q}$ n'est pas complet pour la métrique associée à φ_p; ceci justifie la définition suivante :

4. Le corps des nombres *p*-adiques.

4.1. Définition.

Le complété de $\mathbb{Q}$ *pour la valeur absolue p-adique* φ_p *associée au nombre premier p est le corps des nombres p-adiques. Il est noté* $\mathbb{Q}_p$.

4.2. Remarques.

On démontre que $\mathbb{Q}_p$ a la même puissance que $\mathbb{R}$, c'est-à-dire celle du continu.

Il existe une infinité de corps de nombres *p*-adiques, un pour chaque nombre premier *p*.

Deux corps de nombres *p*-adiques correspondant à des nombres premiers distincts ne sont pas isomorphes.

4.3. Convergences de suites et de séries dans $\mathbb{Q}_p$.

4.3.1. Suites.

Proposition 3 : *Pour qu'une suite* (x_n) *de nombres p-adiques soit convergente il faut et il suffit que* $\varphi_p(x_n - x_{n+1})$ *tende vers zéro quand n tend vers* $+\infty$.

Comme $\mathbb{Q}_p$ est complet il suffit de démontrer l'équivalence :

$$\varphi_p(x_{n+1} - x_n) \to 0 \Leftrightarrow (x_n) \text{ suite de Cauchy.}$$

L'implication $\Leftarrow$ étant évidente il reste à démontrer l'autre :

Or $\mathbb{Q}_p$ étant ultramétrique, on a :

$$\varphi_p(x_n - x_m) \leqslant \text{Max } [\varphi(x_n - x_{n+1}), \varphi(x_{n+1} - x_{n+2}), \ldots, \varphi(x_{m-1} - x_m)]$$

Par suite si l'on a l'implication

$$\forall \varepsilon > 0 \ \exists N_\varepsilon ; k \geqslant N_\varepsilon \Rightarrow \varphi_p(x_k - x_{k+1}) < \varepsilon$$

on a aussi (même ε et même N_ε)

$$\forall \varepsilon > 0 \ \exists N_\varepsilon ; n, m \geqslant N_\varepsilon \Rightarrow \varphi_p(x_n - x_m) < \varepsilon$$

et (x_n) est une suite de Cauchy.

4.3.2. Séries.

Proposition 4 : *Pour que la série* $\sum_1^\infty u_n$ *soit convergente dans* $\mathcal{Q}_p$ *il faut et il suffit que son terme général* u_n *tende vers zéro.*

En effet cette convergence équivaut au fait que la suite $S_n = \sum_1^n u_k$ est convergente ce qui d'après 4, 3, 1 équivaut à $S_{n+1} - S_n = u_n$ tend vers zéro quand n tend vers $+\infty$.

Exemple :

La série $\sum_1^\infty p^n$ est convergente puisque

$$\varphi_p(p^n) = \frac{1}{p^n} \xrightarrow[n \to \infty]{} 0$$

De l'égalité

$$1 + p + \ldots + p^n = \frac{1 - p^{n+1}}{1 - p}$$

où $p^{n+1} \xrightarrow[n \to \infty]{}$ (dans $\mathcal{Q}_p$) on déduit que

$$\boxed{\sum_0^\infty p^n = \frac{1}{1-p}}$$

4.4. *Écriture d'un nombre* p-*adique.*

Théorème (Développement de Hensel).

Tout nombre p-adique $x \neq 0$ *s'écrit de manière unique sous la forme :*

$$x = p^m(x_o + x_1 p + \ldots + x_n p^n + \ldots)$$

où $m = v_p(x)$; $1 \leqslant x_o \leqslant p-1$; $0 \leqslant x_1 \leqslant p-1$; $\ldots$; $0 \leqslant x_n \leqslant p-1$

Pour la démonstration de ce théorème nous renvoyons à II ou à III. Nous allons simplement l'illustrer par quelques exemples.

4.4.1. Écriture de $\frac{3}{10}$ dans $\mathcal{Q}_5$.

Comme $v_5\left(\frac{3}{10}\right) = -1$ on aura $\frac{3}{10} = \frac{1}{5}\ x_0 + 5x_1 \ \ldots$

Remarquons que déterminer x_o revient à déterminer *le* nombre entier x_o compris entre 0 et 4 tel que $\frac{3}{10} - \frac{x_o}{5} = x_1 + 5x_2 + \ldots$ ne contienne plus le facteur 5 en dénominateur. On veut donc avoir

$\frac{3}{10} - \frac{x_o}{5} = \frac{5}{10}$ soit $3 - 2x_o \equiv 0$ (5) dont l'unique solution comprise entre 0 et 4 est $x_o = 4$.

$\frac{3}{10} - \frac{x_o}{5}$ étant alors égal à $-\frac{1}{2}$, déterminer x_1 revient à déterminer le nombre x_1 tel que $-\frac{1}{2} - x_1$ contienne 5 comme facteur premier en numérateur.

On a ainsi :

$$-\frac{1}{2} - x_1 = -\frac{1 + 2x_1}{2}$$

d'où $2x_1 + 1 \equiv 0$ (5) dont l'unique solution comprise entre 0 et 4 est $x_1 = 2$. Itérant ce procédé on trouve $x_n = 2$ pour tout $n \geqslant 1$. On écrit alors :

$$\frac{3}{10} = \frac{1}{5}(4 + 2.5 + 2.5^2 + \ldots 2.5^n + \ldots) = 42{,}22\ldots$$

Vérification :

$$\begin{aligned} 42{,}22\ldots &= \frac{4}{5} + 2 + 2.5 + \ldots + 2.5^n + \ldots \\ &= \frac{4}{5} + 2(1 + 5 + \ldots + 5^n + \ldots) \\ &= \frac{4}{5} + 2 \lim_{n \to \infty} \frac{1 - 5^{n+1}}{1 - 5} = \frac{4}{5} - \frac{1}{2} = \frac{3}{10} \end{aligned}$$

4.4.2. Calcul de $\sqrt{2}$ dans Q_7.

Le problème est de trouver un nombre p-adique

$$x = 7^m(x_o + 7x_1 + \ldots)$$

tel que $(x^2 - 2)$ soit « aussi petit que l'on veut » c'est-à-dire contienne en facteur une puissance de 7 aussi grande que l'on veut.

Comme $v_7(2) = 0$ on cherche a_o tel que

$a_o^2 - 2 \equiv 0$ (7) : seule solution $a_o = 3$;

ensuite on cherche a_1 tel que

$(a_o + 7a_1)^2 - 2 \equiv 0$ (7^2) ce qui conduit à

$6a_1 + 1 \equiv 0$ (7) et $a_1 = 1$.

On cherche alors a_2 tel que

$(a_o + 7a_1 + 7^2a_2)^2 - 2 \equiv 0$ (7^3) ce qui conduit à

$1 + 3a_1 \equiv 0$ (7) et $a_2 = 2$.

Puis a_3 tel que

$(a_o + 7a_1 + 7^2a_2 + 7^3a_3)^2 - 2 \equiv 0\ (7^3)$ pour lequel on trouve $a_3 = 3$; etc...

Ainsi dans $\mathcal{Q}_7$ on a :

$$\boxed{\sqrt{2} = 3{,}123...}$$

On remarquera bien que dans $\mathcal{Q}_p$, (x_n) tend vers x si et seulement si $(x_n - x)$ contient en facteur une puissance de p arbitrairement grande.

Le lecteur trouvera dans II et III une théorie approfondie de ces nombres.

Bibliographie

I. *Leçons d'Algèbre moderne*, par MM. LENTIN et RIVAUD (Vuibert).
II. *Théorie des nombres*, par MM. BOREVITCH et CHAFAREVITCH (Gauthier-Villars).
III. *Théorie des nombres*. Séminaire Delange-Pisot (Paris 1960).

La mathématique parlée
par ceux qui l'enseignent

le troisième ouvrage de notre collection
Bibliothèque d'Enseignement Mathématique

parution prévue : **mai 1969**

Souscrivez en remplissant dès aujourd'hui le *bulletin de souscription* encarté dans ce *Bulletin 266*

Souscrire, c'est participer à l'édition d'un ouvrage conçu par ceux qui enseignent pour ceux qui enseignent