Principes transversaux en mathématiques

Série 6, corrigé

Partie I : Quelques normes sur $\mathbb{Q}$

1. Clair.

2. Soit r et s deux rationnels quelconques. Il est clair que $N_\alpha(r) = 0 \Leftrightarrow r = 0$ et que $N_\alpha(rs) = N_\alpha(r)N_\alpha(s)$. Montrons l'inégalité triangulaire. On sait que $|r + s| \leq |r| + |s|$. En passant à la puissance α , on obtient donc $|r + s|^\alpha \leq (|r| + |s|)^\alpha$. Il suffit donc de montrer $(x + y)^\alpha \leq x^\alpha + y^\alpha$ pour tout $a, b \in \mathbb{R}^+$. Si $a = b = 0$, le résultat est clair, sinon, il est équivalent à $1 \leq \left(\frac{a}{a+b}\right)^\alpha + \left(\frac{b}{a+b}\right)^\alpha$. Or $\frac{a}{a+b}, \frac{b}{a+b} \leq 1$ et $\alpha \in (0, 1]$, donc $\left(\frac{a}{a+b}\right)^\alpha \geq \frac{a}{a+b}$ et $\left(\frac{b}{a+b}\right)^\alpha \geq \frac{b}{a+b}$, ce qui, en sommant, donne bien le résultat voulu.

3. Commençons par montrer que v_p est bien défini :

sur $\mathbb{Z}$: Pour tout $n \in \mathbb{Z}^*$, l'ensemble $\{k \in \mathbb{N} | p^k \text{ divise } n\}$ est non vide car il contient 0. Il est de plus majoré car si p^k divise n , alors $p^k \leq |n|$ et donc $k \leq \frac{\ln(|n|)}{\ln(p)}$. Or un sous-ensemble borné de $\mathbb{N}$ est fini, si de plus il est non vide, il admet bien un élément maximum.

sur $\mathbb{Q}$: Pour $r \in \mathbb{Q}^*$, la valeur $v_p(r)$ pourrait, *a priori*, dépendre de son représentant sous la forme $r = a/b$. Supposons donc $a_1/b_1 = a_2/b_2$. On a alors $a_1 b_2 = a_2 b_1$ et ainsi $v_p(a_1 b_2) = v_p(a_2 b_1)$. Or nous allons bientôt montrer que $v_p(xy) = v_p(x) + v_p(y)$ pour tout $x, y \in \mathbb{Z}^*$, cela impliquera alors que $v_p(a_1) - v_p(b_1) = v_p(a_2) - v_p(b_2)$.

Par définition, pour $r \in \mathbb{Q}$, on a $v(r) = \infty \Leftrightarrow r = 0$ et donc $N_{p,\alpha}(r) = 0 \Leftrightarrow r = 0$.

Montrons la multiplicativité. Soit r, s deux rationnels. Si $r = 0$ ou $s = 0$ alors clairement $N_{p,\alpha}(rs) = N_{p,\alpha}(r)N_{p,\alpha}(s)$. Sinon, on remarque que pour $r = a_r/b_r$, on a $N_{p,\alpha}(r) = \alpha^{v_p(a_r) - v_p(b_r)} = \frac{N_{p,\alpha}(a_r)}{N_{p,\alpha}(b_r)}$. Il suffit donc de vérifier la multiplicativité pour r et s entiers. Or, si $p^{k_r} | r$ et $p^{k_s} | s$, alors $p^{k_r + k_s} | rs$. Réciproquement, si $p^k | rs$, alors $p^{\min(k, v_p(r))} | r$ et $p^{k - \min(k, v_p(r))} | s$. On en déduit que

$$\{k \in \mathbb{N} | p^k \text{ divise } rs\} = \{k_r + k_s | k_r, k_s \in \mathbb{N}, p^{k_r} \text{ divise } r \text{ et } p^{k_s} \text{ divise } s\}$$

et donc que $v_p(rs) = v_p(r) + v_p(s)$, ce qui permet de conclure.

Montrons enfin l'inégalité triangulaire ultramétrique. Soit $r, s \in \mathbb{Q}$. Si $r = 0$ ou $s = 0$ alors le résultat est clair. Sinon, on a $p^k | r, s \Rightarrow p^k | (r + s)$ et donc $v_p(r + s) \geq \min(v_p(r), v_p(s))$. En passant à l'exponentiel, on obtient bien $N_{p,\alpha}(r + s) \leq \max(N_{p,\alpha}(r), N_{p,\alpha}(s))$ car l'application $(t \mapsto \alpha^{-t})$ est décroissante sur $\mathbb{R}_+^*$.

4. Une topologie est déterminé par l'ensemble des suites convergentes. Soit $(r_n)_{n \in \mathbb{N}}$ une suite de rationnels et $r \in \mathbb{Q}$.

Pour la norme triviale, on a

$$\lim_{n \rightarrow \infty} r_n = r \Leftrightarrow (r_n) \text{ est constante égale à } r \text{ à partir d'un certain rang.}$$

Pour la norme N_α , on a

$$\lim_{n \rightarrow \infty} r_n = r \Leftrightarrow \lim_{n \rightarrow \infty} |r_n - r| = 0.$$

Enfin, pour la norme $N_{p,\alpha}$, on a

$$\lim_{n \rightarrow \infty} r_n = r \Leftrightarrow \forall k \in \mathbb{Z}, \exists n_0 \in \mathbb{N}, \forall n \geq n_0, \exists a \in \mathbb{Z}, b \in \mathbb{N}^* \text{ t.q. } b \wedge p = 1 \text{ et } (r_n - r) = p^k \frac{a}{b}.$$

Bien que non équivalentes, Les normes N_α induisent donc la même topologies, de même que les normes $N_{p,\alpha}$ pour un même nombre premier p . Montrons que les topologies restantes sont toutes différentes en exhibant des suites qui convergent pour l'une mais pas pour les autres :

- pour p premier, $(p^n)_{n \in \mathbb{N}}$ converge vers 0 pour $N_{p,\alpha}$ mais pas pour les autres ;
- $(\frac{1}{n+1})_{n \in \mathbb{N}}$ converge vers 0 pour N_α mais pas pour les autres ;
- toute suite convergeant pour N_{triviale} converge pour les autres normes, mais les exemples ci-dessus montrent que sa topologie est néanmoins différentes de toutes les autres.

5 Considérons une suite de Cauchy pour N_{triviale} . Elle est alors constante à partir d'un certain rang et donc convergeante. Donc $(\mathbb{Q}, N_{\text{triviale}})$ est complet.

Considérons maintenant la norme N_1 . Pour tout $n \in \mathbb{N}^*$, on choisit r_n dans l'ensemble

$$\left\{ \frac{a}{b} \mid a, b \in \mathbb{N}^*, \left| \frac{a}{b} \right|^2 \in \left(2 - \frac{1}{n}, 2 + \frac{1}{n} \right) \right\}$$

qui est clairement non vide. Alors la suite $(r_n)_{n \in \mathbb{N}^*}$ est de Cauchy, mais toute limite éventuelle satisfait l'équation $x^2 = 2$ qui n'a pourtant pas de solution dans $\mathbb{Q}$. La suite ne converge donc pas et, pour tout $\alpha \in (0, 1]$, $(\mathbb{Q}, N_\alpha)$, homéomorphe à $(\mathbb{Q}, N_1)$, n'est pas complet.

Considérons enfin la série $\sum_0^\infty p^i$. Elle est de Cauchy pour la norme $N_{p,\alpha}$ avec p premier et $\alpha \in (0, 1)$. Supposons qu'elle converge vers $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors, pour tout $n \in \mathbb{N}$, $(\sum_{n+1}^N p^i)_{N>n}$ est une suite d'éléments du fermé $N_{p,\alpha}^{-1}([0, \alpha^{(n+1)!}])$ convergeant vers $(\frac{a}{b} - \sum_0^\infty p^i)$ qui est donc un élément de $N_{p,\alpha}^{-1}([0, \alpha^{(n+1)!}])$. Autrement dit, $(\frac{a}{b} - \sum_0^\infty p^i)$ s'écrit sous la forme $p^{(n+1)!} \frac{a_n}{b_n}$ avec $a_n \in \mathbb{Z}$ et $b_n \in \mathbb{N}^*$ premier avec p . On en déduit que $p^{(n+1)!}$ divise $a - b \sum_0^\infty p^i$.

Or $\sum_0^n p^i \leq \sum_0^n p^i = \frac{p^{n+1}-1}{p-1} \leq p^{n+1}$, et donc, $|a - b \sum_0^n p^i| \leq \max\{|a|, b\}(1 + p^{n+1})$. Pour n_1, n_2 suffisamment grand et distincts, on a donc $|a - b \sum_0^{n_1} p^i| < p^{(n_1+1)!}$ et $|a - b \sum_0^{n_2} p^i| < p^{(n_2+1)!}$ ce qui, d'après ce qui précède, implique que $a - b \sum_0^{n_1} p^i = 0 = a - b \sum_0^{n_2} p^i$ ce qui est absurde car $b \neq 0$.

La série $\sum_0^\infty p^i$ ne converge donc pas et $(\mathbb{Q}, N_{p,\alpha})$ n'est pas complet.

Partie II : Le théorème d'Ostrowski

1. On raisonne par récurrence sur $n \in \mathbb{N}$.

Cas $n = 0$: clair.

Supposons le résultat vrai au rang n : alors d'après l'inégalité triangulaire, on a

$$N(n+1) \leq N(n) + N(1).$$

Or, $N(1) = N(1^2) = N(1)^2$. Donc $N(1) = 0$ ou 1 mais d'après le point i. de la définition d'une norme, $N(1) \neq 0$. De plus, par hypothèse de récurrence, $N(n) \leq n$, on en conclut donc que $N(n+1) \leq n+1$.

2. a. On a $\alpha = \frac{\ln(b_0)}{\ln(N(b_0))}$ avec $b_0 > 1$, et $1 < N(b_0) \leq b_0$. Au final, $\alpha \in (0, 1]$.

b. On a

$$\begin{aligned} N(k) &= N\left(\sum_{i=0}^d k_i b_0^i\right) \leq \sum_{i=0}^d N(k_i) N(b_0)^i \\ &\leq \sum_{i=0}^d k_i b_0^{i\alpha} \leq (b_0 - 1) \sum_{i=0}^d (b_0^\alpha)^i \\ &\leq (b_0 - 1) \frac{b_0^{\alpha(d+1)} - 1}{b_0^\alpha - 1}. \end{aligned}$$

Or $b_0^d \leq k$ donc $b_0^{\alpha d} \leq k^\alpha$ et

$$N(k) \leq (b_0 - 1) \frac{b_0^{\alpha(d+1)} - 1}{b_0^\alpha - 1} \leq (b_0 - 1) \frac{b_0^{\alpha(d+1)}}{b_0^\alpha - 1} \leq C k^\alpha$$

en posant $C = \frac{b_0(b_0-1)}{b_0^\alpha-1}$ qui est une constante strictement positive indépendante de k .

- c. Pour tout $n \in \mathbb{N}^*$, on a $N(k)^n = N(k^n) \leq Ck^{n\alpha}$. En prenant la racine $n^{\text{ième}}$, on trouve $N(k) \leq \sqrt[n]{C}k^\alpha$ et en faisant tendre n vers l'infini $N(k) \leq k^\alpha$.
- d. Par inégalité triangulaire, on a

$$\begin{aligned} N(k) &= N(b_0^{d+1} - (b_0^{d+1} - k)) \geq N(b_0^{d+1}) - N(b_0^{d+1} - k) \\ &\geq b_0^{\alpha(d+1)} - (b_0^{d+1} - k)^\alpha \geq b_0^{\alpha(d+1)} - (b_0^{d+1} - b_0^d)^\alpha \end{aligned}$$

en réutilisant l'inéquation de la question précédente ainsi que $b_0^{d+1} - k \leq b_0^{d+1} - b_0^d$. Au final, on obtient

$$N(k) \geq b_0^{\alpha(d+1)} \left(1 - \frac{(b_0^{d+1} - b_0^d)^\alpha}{b_0^{\alpha(d+1)}} \right).$$

- e. En posant $D = \left(1 - \frac{(b_0^{d+1} - b_0^d)^\alpha}{b_0^{\alpha(d+1)}} \right) > 0$, on a, puisque $k^\alpha < b_0^{\alpha(d+1)}$,

$$N(k) \geq Db_0^{\alpha(d+1)} \geq Dk^\alpha.$$

La constante D étant indépendante de k , on raisonne comme pour la question c. et on obtient $N(k) \geq k^\alpha$.

On en déduit que $N(k) = |k|^\alpha$ pour tout $k \in \mathbb{N}$. Or $N(-1)^2 = N(1) = 1$ donc $N(-1) = 1$ et pour tout $k \in \mathbb{N}^*$, on a aussi $N(-k) = N(-1)N(k) = N(k) = |-k|^\alpha$.

Enfin, pour tout a/b avec $a, b \in \mathbb{Z}^*$, on a $N(a/b)N(b) = N(a)$ ou encore $N(a/b)|b|^\alpha = |a|^\alpha$ et donc $N(a/b) = |a/b|^\alpha$.

3. a. Supposons par l'absurde que $N(p) = 1$ pour tout nombre premier p . Alors, en décomposant tout entier $k \in \mathbb{N}^*$ en ses facteurs premiers, on obtient $N(k) = \prod N(p_i)^{k_{p_i}} = 1$. Mais alors, en raisonnant comme pour la question 2.e., on obtient $N(k) = 1$ pour tout $k \in \mathbb{Z}^*$ puis $N(x) = 1$ pour tout $x \in \mathbb{Q}^*$ ce qui est absurde puisque N a été supposé non trivial.
- b. Supposons encore par l'absurde qu'il existe p et q entiers premiers distincts tels que $N(p), N(q) < 1$. Puisque p et q sont premiers et distincts, pour tout $n \in \mathbb{N}^*$, p^n et q^n sont premiers entre eux et d'après le théorème de Bézout, il existe deux entiers $a_n, b_n \in \mathbb{Z}$ tels que $a_n p^n + b_n q^n = 1$. On en déduit que

$$1 = N(1) \leq N(a_n)N(p)^n + N(b_n)N(q)^n \leq N(p)^n + N(q)^n \xrightarrow{n \rightarrow \infty} 0,$$

ce qui est absurde.

- c. En décomposant tout $k \in \mathbb{Z}^*$ en facteurs premiers, on obtient

$$N(k) = N(\pm 1) \prod N(p_i)^{v_{p_i}(k)} = N(p)^{v_p(k)}.$$

Pour a/b avec $a, b \in \mathbb{Z}^*$, on a $N(a/b)N(b) = N(a)$ et donc $N(a/b) = \alpha^{v_p(a/b)}$ avec $\alpha = N(p) \in (0, 1)$.

Partie III : Les nombres p -adiques

1. a. La somme et le produit terme à terme induisant déjà une structure d'anneau sur les suites d'entiers, il suffit de vérifier que ces opérations sont internes pour $\mathbb{Z}_p$ et qu'elles sont compatibles avec la relation $\sim$. Or, pour ces deux points, cela provient de ce que somme et produit sont compatibles avec les relations de congruence.
- L'élément unité est la projection dans $\mathbb{Z}_p$ de la suite constante égale à 1.

b. Posons d'abord $\widetilde{\psi}: \mathbb{Z} \rightarrow \mathbb{Z}_p$ qui à $k \in \mathbb{Z}$ associe $\widetilde{\psi}(k)$ la suite constante égale à k qui est clairement un élément de $\mathbb{Z}_p$. Au final, on définit $\psi: \mathbb{Z} \rightarrow \mathbb{Z}_p$ par $\psi = \pi \circ \widetilde{\psi}$ où π est la projection canonique de $\mathbb{Z}_p$ dans $\mathbb{Z}_p$. Cette application est clairement un morphisme d'anneau. Elle est de plus injective. En effet, pour tout $k \in \mathbb{Z}^*$, il existe $n \in \mathbb{N}^*$ tel que $p^n > |k|$ et alors, à partir du $n^{\text{ième}}$ terme, la suite $\psi(k)$ est non nulle. Autrement dit, $\psi(k) \neq 0$.

c. On travaille par récurrence sur n .

Cas $n = 0$: On pose $\widetilde{x}_0$ l'unique représentant dans $\llbracket 0, p-1 \rrbracket$ de x_0 modulo p .

Supposons $\widetilde{x}_0, \dots, \widetilde{x}_n$ contruits : alors $(x_{n+1} - x_n)$ et $(x_n - \sum_0^n \widetilde{x}_i p^i)$ sont divisibles par p^{n+1} , l'entier $x_{n+1} - \sum_0^n \widetilde{x}_i p^i$ l'est donc lui aussi et on pose $\widetilde{x}_{n+1}$ l'unique représentant dans $\llbracket 0, p-1 \rrbracket$ de $\frac{x_{n+1} - \sum_0^n \widetilde{x}_i p^i}{p^{n+1}}$ modulo p . On a alors bien $\sum_0^{n+1} \widetilde{x}_i p^i$ congru à x_{n+1} modulo p^{n+2} .

2. a. Supposons d'abord que $(x_n) \in \mathbb{Z}_p$ est inversible. Alors il existe $(y_n) \in \mathbb{Z}_p$ tel que, pour tout $n \in \mathbb{N}$, $x_n y_n \equiv 1 [p^{n+1}]$. C'est notamment vrai pour $n = 0$ et donc $x_0 \not\equiv 0 [p]$.

Supposons maintenant que $x_0 \not\equiv 0 [p]$. On montre facilement par récurrence sur $n \in \mathbb{N}$ que $x_n \equiv x_0 \not\equiv 0 [p]$. De fait $x_n \not\equiv 0 [p^{n+1}]$ et on pose y_n un inverse de x_n modulo p^{n+1} . Mais alors $x_{n+1} y_{n+1} \equiv x_n y_{n+1} \equiv 1 [p^{n+1}]$, et donc par unicité de l'inverse dans $\mathbb{Z}/p^{n+1}\mathbb{Z}$, on a $y_{n+1} \equiv y_n [p^{n+1}]$. Autrement dit, $(y_n) \in \mathbb{Z}_p$ et par construction son image dans $\mathbb{Z}_p$ est un inverse pour (x_n) .

b. Soit x un élément non nul de $\mathbb{Z}_p$. Puisqu'il est non nul, $E_x = \{k \in \mathbb{Z} | x_k \not\equiv 0 [p^{k+1}]\} \neq \emptyset$. On peut donc poser $\mu_p(x) = \min E_x$ ainsi que $x_* = (x_{n-\mu_p(x)})$ qui est bien un élément de $\mathbb{Z}_p$ car, pour tout $n \geq \mu_p(x)$, $(x_{n+1} \equiv x_n [p^{n+1}]) \Rightarrow (x_{n+1} \equiv x_n [p^{n+1-\mu_p(x)}])$. De plus, par construction, le premier terme de x_* est non nul modulo $p^{\mu_p(x)+1}$, donc non nul modulo p , par construction. L'image de x_* dans $\mathbb{Z}_p$ est inversible d'après la question précédente. Enfin, il est clair d'après l'écriture sous forme de série que $x = p^{\mu_p(x)} x_*$.

Montrons que l'entier $\mu_p(x)$ est unique. Pour cela, supposons $p^m x'_* = x = p^{\mu_p(x)} x_*$ avec x'_* inversible. Si $m \geq \mu_p(x)$, alors $p^{m-\mu_p(x)} x'_* = x_*$ est inversible, son premier terme n'est donc pas divisible par p et, de fait, $m = \mu_p(x)$. Si $m \leq \mu_p(x)$, on montre de même que $m = \mu_p(x)$.

c. Soit $x, y \in \mathbb{Z}_p$. Si $x = 0$ ou $y = 0$, alors le produit est également nul et on a bien $\mu_p(xy) = \mu_p(x) + \mu_p(y)$. Autrement, d'après la question précédente, il existe x_* et y_* des éléments inversibles de $\mathbb{Z}_p$ tels que $x = p^{\mu_p(x)} x_*$ et $y = p^{\mu_p(y)} y_*$. On a alors $xy = p^{\mu_p(x)+\mu_p(y)} x_* y_*$ avec $x_* y_*$ inversible, et par unicité d'une telle décomposition, on a $\mu_p(xy) = \mu_p(x) + \mu_p(y)$.

d. Soit $x, y \in \mathbb{Z}_p$ tels que $xy = 0$, i.e. tels que $\mu_p(xy) = \infty$, alors $\mu_p(x)$ ou $\mu_p(y)$ est également infini.

3. a. Soit x/y avec $x, y \in \mathbb{Z}_p^*$. D'après la question 2.b., on a donc $x_*, y_* \in \mathbb{Z}_p$ inversibles tels que $x = p^{\mu_p(x)} x_*$, $y = p^{\mu_p(y)} y_*$ et donc

$$x/y = \left(p^{\mu_p(x)} / p^{\mu_p(y)} \right) \cdot \left(x_* / y_* \right) = p^{\mu_p(x)-\mu_p(y)} (x_* y_*^{-1})$$

avec $x_* y_*^{-1}$ inversible dans $\mathbb{Z}_p$.

Pour l'unicité, on travaille comme pour la question 2.b.

b. Les points i. et ii. de la définition d'une norme sont clairs. Montrons que $\widetilde{N}_p$ satisfait l'inégalité triangulaire ultramétrique. Pour cela, considérons x et y dans $\mathbb{Q}_p$. Si l'un des deux termes est nul, alors l'inégalité est évidente. Autrement, on a $x = p^{\mu_p(x)} x_*$ et $y = p^{\mu_p(y)} y_*$ avec x_*, y_* inversibles dans $\mathbb{Z}_p$. Supposons d'abord que $\mu_p(x) < \mu_p(y)$, on a alors

$$x + y = p^{\mu_p(x)} (x_* + p^{\mu_p(y)-\mu_p(x)} y_*)$$

où $x_* + p^{\mu_p(y)-\mu_p(x)} y_*$ est un élément de $\mathbb{Z}_p$ dont le premier terme est congru au premier terme de x_* modulo p , i.e. non congru à 0. L'élément $x_* + p^{\mu_p(y)-\mu_p(x)} y_*$ est donc inversible et on a $\mu_p(x+y) = \mu_p(x) = \min(\mu_p(x), \mu_p(y))$. On a donc $\widetilde{N}_p(x+y) = \max(\widetilde{N}_p(x), \widetilde{N}_p(y))$.

Si $\mu_p(x) > \mu_p(y)$, on raisonne de même.

Supposons maintenant $\mu_p(x) = \mu_p(y)$. On a alors

$$x + y = p^{\mu_p(x)}(x_* + y_*) = p^{\mu_p(x) + \mu_p(x_* + y_*)}(x_* + y_*)$$

avec $\mu_p(x_* + y_*) \geq 0$ puisque $x_* + y_* \in \mathbb{Z}_p$. Au final, on obtient bien là encore $\widetilde{N}_p(x+y) = \max(\widetilde{N}_p(x), \widetilde{N}_p(y))$.

- c. En reprenant les notations de la question 1.b., on étant ψ à $\mathbb{Q}$ par $\psi(a/b) = \psi(a)/\psi(b)$. L'application reste injective car

$$\begin{aligned} \psi(a_1/b_1) = \psi(a_2/b_2) &\Rightarrow \psi(a_1)/\psi(b_1) = \psi(a_2)/\psi(b_2) \\ &\Rightarrow \psi(a_1)\psi(b_2) = \psi(a_2)\psi(b_1) \\ &\Rightarrow \psi(a_1b_2) = \psi(a_2b_1) \\ &\Rightarrow a_1b_2 = a_2b_1. \end{aligned}$$

Soit $a \in \mathbb{Z}^*$, on a $a = p^{v_p(a)}b$ avec $b \not\equiv 0[p]$, donc $\psi(b)$ inversible dans $\mathbb{Z}_p$. Par l'unicité de la question 2.b., on a $v_p(a) = \mu_p(\psi(a))$ et donc $v_p(r) = \mu_p(\psi(r))$ pour tout $r \in \mathbb{Q}$. On en déduit l'égalité des normes.

- d. On a $\lim_{n \rightarrow \infty} \widetilde{N}_p(p^n) = \lim_{n \rightarrow \infty} p^{-n} = 0$. La suite converge donc vers 0.

Partie IV : Un peu de topologie sur $\mathbb{Q}_p$

- Multiplier un nombre p -adique par p divise sa norme par p . Quitte à multiplier tout ses termes par une puissance suffisamment grande de p , on peut donc ramener toute suite bornée à une suite bornée par 1. Or $\widetilde{N}_p^{-1}([0, 1]) = \mathbb{Z}_p$. Il suffit donc de montrer que toute suite d'entiers p -adiques admet une sous-suite convergente. Soit $(x^i)_{i \in \mathbb{N}} = (\sum_0^\infty x_n^i p^n)_{i \in \mathbb{N}}$ une telle suite avec $x_n^i \in \llbracket 0, p-1 \rrbracket$ pour tout $i, n \in \mathbb{N}$. On va extraire une sous-suite convergente par extraction diagonale. C'est à dire, on va construire une suite de fonctions strictement croissantes $(\varphi_i: \mathbb{N} \rightarrow \mathbb{N})_{i \in \mathbb{N}}$ telles que, pour tout $n \in \mathbb{N}$, la suite $(x_n^{\varphi_n \circ \dots \circ \varphi_0(i)})_{i \in \mathbb{N}}$ soit constante.

Cas i = 0 : La suite $(x^i)_{i \in \mathbb{N}}$ est une suite infinie prenant un nombre fini de valeurs. Il existe donc une extraction $\varphi_0: \mathbb{N} \rightarrow \mathbb{N}$ telle que la suite $(x_0^{\varphi_0(i)})_{i \in \mathbb{N}}$ soit constante.

Supposons φ_i construite : Alors on construit φ_{i+1} comme ci-dessus en regardant les coefficients de p^i .

Maintenant, on pose $x = \sum_0^\infty x_n^{\varphi_n \circ \dots \circ \varphi_0(n)} p^n$ dont les k premiers termes, pour tout $k \in \mathbb{N}$, coïncident par construction avec les k premiers termes des éléments de la suite extraite $(x^{\varphi_i \circ \dots \circ \varphi_0(i)})_{i \in \mathbb{N}}$ à partir du rang k . Autrement dit, pour tout $k \in \mathbb{N}$ et pour tout $n \geq k$, on a $\widetilde{N}_p(x^{\varphi_n \circ \dots \circ \varphi_0(n)} - x) \leq p^{-k}$. Cette suite extraite converge donc vers x .

- On vient de montrer que toute suite de $\mathbb{Z}_p$ admet une sous-suite convergente, $\mathbb{Z}_p$ est donc compact.

De plus, $\mathbb{Z}_p = \widetilde{N}_p^{-1}([0, 1]) = \widetilde{N}_p^{-1}\left(\left[0, 1, \frac{3}{2}p\right]\right)$. L'ensemble $\mathbb{Z}_p$ est donc également ouvert.

- Soit $B_\varepsilon(x)$ une boule ouverte de rayon $\varepsilon > 0$, centré en $x \in \mathbb{Q}_p$. Soit $y \in B_\varepsilon(x)$. Alors, pour tout $z \in B_\varepsilon(y)$, on a $\widetilde{N}_p(z-x) \leq \max(\widetilde{N}_p(z-y), \widetilde{N}_p(y-x)) \leq \varepsilon$ et donc $z \in B_\varepsilon(x)$. De fait, $B_\varepsilon(y) \subset B_\varepsilon(x)$. Mais si $y \in B_\varepsilon(x)$, alors $x \in B_\varepsilon(y)$ et en inversant les rôles de x et de y , on obtient $B_\varepsilon(x) \subset B_\varepsilon(y)$. Au final, $B_\varepsilon(y) = B_\varepsilon(x)$ et tout point de $B_\varepsilon(x)$ est centre de $B_\varepsilon(x)$.

- Il est toujours vrai que le terme général d'une série de Cauchy tend vers 0.

Réciproquement, supposons que $\sum_0^\infty x_i$ est une série d'éléments de $\mathbb{Q}_p$ vérifiant $\lim_{i \rightarrow \infty} x_i = 0$. Alors, pour tout $\varepsilon > 0$, il existe un rang $i_0 \in \mathbb{N}$ tel que pour tout $i \geq i_0$, $\widetilde{N}_p(x_i) \leq \varepsilon$. Mais alors, pour tout $j, k \in \mathbb{N}$ vérifiant $k > j \geq i_0$, on a

$$\widetilde{N}_p\left(\sum_{i=0}^k x_i - \sum_{i=0}^j x_i\right) = \widetilde{N}_p\left(\sum_{i=j}^k x_i\right) \leq \max_{i \in \llbracket j, k \rrbracket} (\widetilde{N}_p(x_i)) \leq \varepsilon.$$

La série est donc de Cauchy.

5. Toute suite de Cauchy est bornée. D'après la question 1., toute suite de Cauchy admet donc une sous-suite convergente. Or si une suite de Cauchy admet une valeur d'adhérence, alors cette valeur est unique et la suite converge vers cette valeur.

L'espace $\mathbb{Q}_p$ est donc complet. Or, on a vu que $\mathbb{Q}$ muni de la topologie induite par la norme p -adique s'injectait naturellement dans $\mathbb{Q}_p$. Pour montrer que $\mathbb{Q}_p$ est la complétion de $\mathbb{Q}$ pour cette norme, il suffit donc de montrer que tout élément $\sum_{i=0}^{\infty} x_i p^i$ de $\mathbb{Q}_p$, avec $N \in \mathbb{N}$ et $x_i \in \llbracket 0, p-1 \rrbracket$ pour tout $i \in \mathbb{N}$, est limite d'une suite d'éléments de $\mathbb{Q}$. Or $\sum_{i=0}^{\infty} x_i p^i$ est limite de ses sommes tronquées, qui correspondent justement à des éléments de $\mathbb{Q}$.