Problème 1 - Entiers et rationnels p-adiques

Ce sujet a été inspiré par l'une des deux épreuves de l'Agrégation interne de 2023.

Si K est un corps, on appelle valeur absolue sur K toute application $|\,.\,|$ de K dans $\mathbb{R}_+$ qui satisfait les axiomes suivants :

séparation : pour tout $x \in K$, $|x| = 0 \iff x = 0$

inégalité triangulaire : pour tout $(x, y) \in K^2$, $|x + y| \leqslant |x| + |y|$

homogénéité interne : pour tout $(x, y) \in K^2$, $|xy| = |x| \times |y|$

Dans un corps K muni d'une valeur absolue, on définit alors classiquement les notions de limites de suites. Formellement, tous les théorèmes valables pour les suites réelles (ou dans un espace normé quelconque) restent valables, hormis bien sûr ceux qui font intervenir la relation d'ordre sur les éléments de K (comme le th. de la limite monotone). On peut aussi définir la notion de boule ouverte dans K, de boule fermée, d'ouvert, de fermé, etc, comme dans un espace vectoriel normé.

Par exemple, pour $a \in K$ et $r > 0$, on pose comme d'habitude $B(a, r) = \{x \in K \;/\; |x - a| < r\}$ la boule ouverte de centre a et de rayon r.

Dans tout le problème p désigne un nombre premier. On note aussi $S_p = [\![0, p-1]\!]^{\mathbb{N}}$ l'ensemble des suites d'entiers naturels compris entre 0 et $p - 1$.

L'objectif de ce problème est de construire un corps $\mathbb{Q}_p$ qui contient $\mathbb{Q}$, muni d'une valeur absolue différente de la valeur absolue usuelle et dont les propriétés topologiques sont étudiées dans la dernière partie.

I. Généralités

Dans cette partie, K est un corps.

Q 1. En notant 1 le neutre de K pour la multiplication, montrer que pour toute valeur absolue $|\,.\,|$ sur K, $|1| = 1$ et pour tout $x \in K$, $|-x| = |x|$.

Dans la suite de cette partie, on suppose que $|\,.\,|$ est une application qui vérifie les axiomes de séparation et d'homogénéité interne, qui vérifie de plus la propriété suivante

inégalité ultramétrique : pour tout $(x, y) \in K^2$, $|x + y| \leqslant \max(|x|, |y|)$.

Q 2. Montrer que $|\,.\,|$ est une valeur absolue, dite ultramétrique.

Q 3. Montrer alors que pour tout $a, b \in K$ et $r > 0$, si $b \in B(a, r)$, alors $B(a, r) = B(b, r)$.

Q 4. Montrer que si on considère deux boules ouvertes de K, alors elles sont disjointes ou l'une des deux est incluse dans l'autre.

Q 5. Montrer que toute boule ouverte est à la fois une partie ouverte et une partie fermée. Montrer la même chose pour les boules fermées.

II. Valuation et valeur absolue p-adiques sur $\mathbb{Q}$

Q 6. Soit n un entier relatif non nul. Montrer qu'il existe un unique entier k tel que p^k divise n et p^{k+1} ne divise pas n.

L'unique entier k ainsi défini est appelé valuation p-adique de n et on le note $v_p(n)$.

Q 7. Soient a et b deux entiers relatifs non nuls. Montrer l'égalité $v_p(ab) = v_p(a) + v_p(b)$.

Soit r un rationnel non nul, qu'on écrit sous la forme $\dfrac{a}{b}$ où a, b sont deux entiers : on pose alors $v_p(r) = v_p(a) - v_p(b)$. Et par convention, on pose $v_p(0) = +\infty$.

Q 8. Montrer que cette définition n'est pas ambigüe et qu'elle permet de définir une application $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$.

Q 9. Soient r, s deux rationnels. En prenant soin de préciser les inégalités et les règles de calcul dans $\mathbb{Z} \cup \{+\infty\}$, montrer les résultats suivants :

a) $v_p(rs) = v_p(r) + v_p(s)$.

b) $v_p(r + s) \geqslant \min(v_p(r), v_p(s))$.

On définit l'application $|\,.\,|_p : \mathbb{Q} \to \mathbb{R}_+$ par $|0|_p = 0$ et pour tout nombre rationnel x non nul, $|x|_p = \dfrac{1}{p^{v_p(x)}}$.

Q 10. Montrer que l'application $|\,.\,|_p$ est une valeur absolue ultramétrique sur $\mathbb{Q}$, appelée valeur absolue p-adique. La définition a été donnée en question **Q 2**.

Q 11. Étudier la convergence de la suite (p^n) pour cette valeur absolue, puis celle de la série $\sum_{n \geqslant 0} p^n$. Étudier la convergence de la suite $(n!)$.

III. Les entiers p-adiques

On note $\mathbb{Z}_p$ l'ensemble des suites d'entiers naturels (a_n) telles que
- pour tout $n \in \mathbb{N}$, $a_n \in [\![0, p^{n+1} - 1]\!]$
- pour tout $(m, n) \in \mathbb{N}^2$, si $m \geqslant n$, alors $a_m \equiv a_n\ [p^{n+1}]$.

III.A - Représentations des éléments de $\mathbb{Z}_p$

Q 12. Soit (a_n) une suite d'entiers naturels tels que pour tout $n \in \mathbb{N}$, $a_n \in [\![0, p^{n+1} - 1]\!]$.

Montrer que la suite (a_n) est dans $\mathbb{Z}_p$ si et seulement si pour tout $n \in \mathbb{N}$, $a_{n+1} \equiv a_n\ [p^{n+1}]$.

Q 13. Soit $x \in \mathbb{Z}$. Pour $n \in \mathbb{N}$, on pose a_n le reste de la division euclidienne de x par p^{n+1}. Montrer que la suite (a_n) appartient à $\mathbb{Z}_p$. Cette suite est désormais notée $\theta(x)$.

On définit ainsi une application $\theta : \mathbb{Z} \to \mathbb{Z}_p$.

Q 14. Dans cette question uniquement, fixons $p = 5$. Déterminer les éléments $\theta(1)$, $\theta(-1)$, $\theta(27)$ et $\theta(-7)$ de $\mathbb{Z}_5$.

Q 15. Soit $u = (u_i) \in S_p$. On pose pour tout $n \in \mathbb{N}$, $a_n = \sum_{i=0}^{n} u_i p^i$. On définit ainsi une suite d'entiers naturels, qu'on note $\sigma(u)$. Montrer que σ est une application bijective de S dans $\mathbb{Z}_p$.

Cette bijection permet de représenter les éléments de $\mathbb{Z}_p$ comme des suites d'entiers compris entre 0 et $p - 1$. Si $a \in \mathbb{Z}_p$ et $u = \sigma^{-1}(a)$, on dit que u est la suite des chiffres en base p de a et on écrit symboliquement

$$a = [\ldots\, u_{i+1}\, u_i\, u_{i-1}\, \ldots\, u_2\, u_1\, u_0]$$

comme si a était une sorte de nombre ayant une infinité de chiffres en base p.

Q 16. Si $x \in \mathbb{N}$, donner l'écriture symbolique de $\theta(x)$. Faire de même si $x \in \mathbb{Z}_-^*$.

Avec $p = 5$, donner l'écriture symbolique de $\theta(27)$, $\theta(-1)$ et $\theta(-27)$.

III.B - Valuation p-adique dans $\mathbb{Z}_p$

Q 17. Soit $a = (a_n) \in \mathbb{Z}_p$, $a \neq 0$. Montrer qu'il existe un unique entier $k \in \mathbb{N}$ tel que
- pour tout $n < k$, $v_p(a_n) = +\infty$
- pour tout $n \geqslant k$, $v_p(a_n) = k$

Cet entier k est noté $\tilde{v_p}(a)$. Par convention, on pose de plus $\tilde{v_p}(0) = +\infty$.

Q 18. Montrer que θ est une application injective et vérifie la propriété : $\forall x \in \mathbb{Z} \quad \tilde{v_p}(\theta(x)) = v_p(x)$.

Ceci prouve qu'on peut identifier $\mathbb{Z}$ à une partie de $\mathbb{Z}_p$ et qu'alors $\tilde{v_p}$ prolonge l'application v_p. Désormais, dans toute la suite du problème, on notera v_p au lieu de $\tilde{v_p}$.

Q 19. Montrer que θ n'est pas une bijection.

III.C - Structure d'anneau

Soient $a = (a_n)$ et $b = (b_n)$ deux éléments de $\mathbb{Z}_p$.

Pour tout $n \in \mathbb{N}$, on pose c_n et d_n les restes des divisions euclidiennes de $a_n + b_n$ et $a_n \times b_n$ respectivement par p^{n+1}.

Q 20. Montrer que les suites $c = (c_n)$ et $d = (d_n)$ sont deux éléments de $\mathbb{Z}_p$.

Par définition, on pose $c = a + b$ et $d = a \times b = ab$.

On définit ainsi deux lois de composition interne dans $\mathbb{Z}_p$.

Q 21. Montrer que $(\mathbb{Z}_p, +)$ est un groupe commutatif dont on précisera le neutre ainsi que l'opposé de tout élément a de $\mathbb{Z}_p$.

On admettra, car cela ne pose aucune autre difficulté, que $(\mathbb{Z}_p, +, \times)$ est un anneau commutatif. Désormais, on sous-entend cette structure d'anneau quand on évoque $\mathbb{Z}_p$.

Q 22. Quel est le neutre pour la multiplication ? Montrer que $\mathbb{Z}_p$ est un anneau intègre.

Q 23. Montrer que pour tout $(a,b) \in \mathbb{Z}_p^2$, $v_p(a+b) \geqslant \min(v_p(a), v_p(b))$ et $v_p(ab) = v_p(a) + v_p(b)$.

Q 24. Montrer que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}_p$, c'est-à-dire que θ est un morphisme d'anneaux.

Q 25. Soit $a = (a_n) \in \mathbb{Z}_p$. Montrer que a est inversible dans $\mathbb{Z}_p$ si et seulement si $a_0 \neq 0$.

Q 26. Déterminer les idéaux de l'anneau $\mathbb{Z}_p$.

L'anneau $\mathbb{Z}_p$ étant un anneau commutatif intègre, il possède un corps de fractions noté $\mathbb{Q}_p$, qui est formellement défini comme l'ensemble des quotients $\dfrac{a}{b}$ où $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p^*$.

À tout couple $(x,y) \in \mathbb{Z} \times \mathbb{Z}^*$, on associe l'élément $\Theta(x/y) = \dfrac{\theta(x)}{\theta(y)}$. On définit ainsi une application de $\mathbb{Q}$ dans $\mathbb{Q}_p$.

Q 27. Montrer que l'application Θ est injective et qu'on peut prolonger naturellement la valuation v_p à $\mathbb{Q}_p$.

Comme pour $\mathbb{Z}$, on peut donc identifier $\mathbb{Q}$ à son image dans $\mathbb{Q}_p$ et on admet que $\mathbb{Q}$ est un sous-corps de $\mathbb{Q}_p$. On admet aussi que la valuation sur $\mathbb{Q}_p$ a les mêmes propriétés calculatoires que celles sur $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{Z}_p$. Enfin, on prolonge la définition de la valeur absolue : pour tout $r \in \mathbb{Q}_p$, on pose $|r|_p = \dfrac{1}{p^{v_p(r)}}$. Là encore, on admet que ce symbole est une valeur absolue ultramétrique sur $\mathbb{Q}_p$.

Q 28. Montrer que tout élément $r \in \mathbb{Q}_p$ s'écrit sous la forme $r = \dfrac{a}{p^k}$ où $a \in \mathbb{Z}_p$, $k \in \mathbb{N}$.

IV. Topologie dans $\mathbb{Q}_p$

On rappelle que les notions topologiques sont relatives à la valeur absolue $|\,.\,|_p$ dans $\mathbb{Q}_p$. Les définitions données dans le cours sur les espaces vectoriels normés se transposent mot pour mot dans l'ensemble $\mathbb{Q}_p$. En revanche, les théorèmes peuvent être tout à fait différents.

Q 29. Montrer que $\mathbb{Z}_p^\times$ (ensemble des inversibles de l'anneau $\mathbb{Z}_p$) est la sphère-unité de $\mathbb{Q}_p$.

Q 30. Montrer que $\mathbb{Z}_p$ est à la fois une boule ouverte de $\mathbb{Q}_p$ et une boule fermée dont on précisera un centre et un rayon.

Q 31. Soit $a = (a_n) \in \mathbb{Z}_p$. Montrer que la suite $(\theta(a_n))$ converge vers a. En déduire que $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$.

Q 32. Soit $a \in \mathbb{Z}_p$. Montrer qu'il existe une unique suite d'entiers naturels (u_i) telle que pour tout $i \in \mathbb{N}$, $u_i \in [\![0, p-1]\!]$ et $a = \displaystyle\sum_{i=0}^{+\infty} u_i p^i$. Dans le cas où $a \in \mathbb{Z}$, quelle est cette suite (u_i) ?

Donner une écriture des éléments de $\mathbb{Q}_p$ sous forme de somme d'une série indexée éventuellement par des entiers relatifs.

Q 33. Montrer que $\mathbb{Z}_p$ est un compact. En déduire que toutes les boules fermées sont compactes.

Q 34. Soit (x_n) une suite de $\mathbb{Q}_p$. Montrer que la série $\displaystyle\sum_{n \geqslant 0} x_n$ converge si et seulement si la suite (x_n) converge vers 0.

Problème 1

I.

Q 1. D'après l'axiome d'homogénéité interne, $|1| = |1 \times 1| = |1|^2$ donc comme $|1| \neq 0$ d'après l'axiome de séparation, on en déduit que $|1| = 1$.

De même, $1 = |1| = |(-1)^2| = |-1|^2$ donc $|-1| = 1$ puisque $|-1| \geqslant 0$. Enfin, pour tout $x \in K$, $|-x| = |-1 \times x| = |-1| \times |x| = |x|$.

Q 2. Soit $(x, y) \in K^2$. Comme $|x| \geqslant 0$ et $|y| \geqslant 0$, alors $\max(|x|, |y|) \leqslant |x| + |y|$ donc l'inégalité triangulaire est vérifiée dès que l'inégalité ultramétrique l'est. Donc une valeur absolue ultramétrique est aussi une valeur absolue.

Q 3. Soit $a, b \in K$ et $r > 0$ tels que $b \in B(a, r)$, donc $|a - b| < r$. Pour tout $x \in B(a, r)$, $|x - a| < r$, or $|x - b| = |(x - a) + (a - b)| \leqslant \max(|x - a|, |a - b|)$ donc $|x - b| < r$: ceci prouve l'inclusion $B(a, r) \subset B(b, r)$.

Comme $|b - a| < r$, alors $a \in B(b, r)$, donc en échangeant les rôles de a et b, on a aussi l'inclusion $B(b, r) \subset B(a, r)$. Conclusion : $B(a, r) = B(b, r)$.

Q 4. Soit $B(a, r)$ et $B(b, s)$ deux boules ouvertes de K ($r, s > 0$). On suppose par exemple que $r \leqslant s$. Si elles ne sont pas disjointes, alors il existe $c \in B(a, r) \cap B(b, s)$. D'après la question précédente, $B(c, r) = B(a, r)$ et $B(c, s) = B(b, s)$. Comme $B(c, r) \subset B(c, s)$, on en déduit que $B(a, r) = B(c, r) \subset B(c, s) = B(b, s)$.

Q 5. Comme dans le cours sur les espaces vectoriels normés, une boule ouverte est un ouvert et une boule fermée est un fermé (les démonstrations sont identiques au remplacement de la norme par la valeur absolue près).

Soit $a \in K$, $r > 0$ et (u_n) une suite à termes dans $B(a, r)$ qui converge vers x : on montre que $x \in B(a, r)$, ce qui prouvera que la boule $B(a, r)$ est un fermé.

Pour tout $\varepsilon > 0$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $|u_n - x| < \varepsilon$. On choisit $\varepsilon = r$. D'après la question **Q 3**, comme $u_N \in B(a, r)$, alors $B(u_N, r) = B(a, r)$, donc comme $x \in B(u_N, r)$, on a donc $x \in B(a, r)$.

Soit $a \in K$, $r > 0$ et $x \in \bar{B}(a, r)$: on montre qu'il existe $s > 0$ tel que $B(x, s) \subset \bar{B}(a, r)$, ce qui prouvera que $\bar{B}(a, r)$ est un ouvert.

On prend $s = r$: pour tout $y \in B(x, r)$, $|x - y| < r$ donc $|y - a| = |(y - x) + (x - a)| \leqslant \max(|y - x|, |x - a|) \leqslant r$ puisque $|x - y| < r$ et $|x - a| \leqslant r$, donc $y \in \bar{B}(a, r)$; ceci prouve bien que $B(x, r) \subset \bar{B}(a, r)$.

II.

Q 6. L'ensemble $\{k \in \mathbb{N} \ / \ p^k \mid n\}$ est une partie de $\mathbb{N}$, non vide (elle contient 0) et majorée, car si p^k divise n, alors $p^k \leqslant |n|$ donc $k \leqslant \dfrac{\ln |n|}{\ln p}$. D'après la propriété fondamentale de $\mathbb{N}$, cette partie possède un maximum.

Q 7. On pose $k = v_p(a)$ et $\ell = v_p(b)$. Alors par définition, p^k divise a et p^ℓ divise b, donc $p^{k+\ell} = p^k \times p^\ell$ divise ab. Ceci prouve donc que $v_p(ab) \geqslant k + \ell$.

Réciproquement, si $k + \ell + 1$ divise ab, alors $ab = p^{k+\ell+1} q$, donc $pq = \dfrac{a}{p^k} \times \dfrac{b}{p^\ell}$: p étant un nombre premier, il divise donc l'un des deux entiers $\dfrac{a}{p^k}$ ou $\dfrac{b}{p^\ell}$, donc p^{k+1} divise a ou $p^{\ell+1}$ divise b, ce qui est contradictoire.

Donc $v_p(ab) = k + \ell = v_p(a) + v_p(b)$.

Q 8. Si $r = \dfrac{a}{b} = \dfrac{c}{d}$ où a, b, c, d sont quatre entiers relatifs non nuls, alors $ad = bc$ donc $v_p(ad) = v_p(bc)$, donc $v_p(a) + v_p(d) = v_p(b) + v_p(c)$ donc $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

Ceci prouve que la définition de $v_p(r)$ ne dépend pas du choix des entiers a et b tels que $r = \dfrac{a}{b}$.

Q 9. Dans $\mathbb{Z} \cup \{+\infty\}$, on étend l'addition de $\mathbb{Z}$ en posant pour tout $a \in \mathbb{Z}$, $a + (+\infty) = (+\infty) + a = (+\infty) + (+\infty) = +\infty$ et on étend la relation d'ordre en posant $a < +\infty$.

a) Si r et s sont non nuls, alors on les écrit $r = \dfrac{a}{b}$ et $s = \dfrac{c}{d}$ où a, b, c, d sont quatre entiers relatifs non nuls. Alors $rs = \dfrac{ac}{bd}$, donc $v_p(rs) = v_p(ac) - v_p(bd) = (v_p(a) + v_p(c)) - (v_p(b) + v_p(d)) = v_p(a) - v_p(b) + v_p(c) - v_p(d) = v_p(r) + v_p(s)$.

Si r ou s est nul, alors $rs = 0$, donc $v_p(rs) = +\infty = v_p(r) + v_p(s)$.

b) Si r et s sont non nuls, alors on les écrit $r = \dfrac{a}{b}$ et $s = \dfrac{c}{d}$ où a, b, c, d sont quatre entiers relatifs non nuls. Alors $r + s = \dfrac{ad + bc}{bd}$, donc $v_p(r + s) = v_p(ad + bc) - v_p(bd)$.

Or si $k = v_p(ad)$ et $\ell = v_p(bc)$, alors $p^{\min(k,\ell)}$ divise à la fois p^k et p^ℓ donc divise ad et bc, donc divise $ad + bc$, donc $v_p(ad + bc) \geqslant \min(v_p(ad), v_p(bc))$. Donc $v_p(r + s) \geqslant \min(v_p(a) + v_p(d), v_p(b) + v_p(c)) - (v_p(b) + v_p(d)) = \min(v_p(a) - v_p(b), v_p(c) - v_p(d)) = \min(v_p(r), v_p(s))$.

Si r est nul, alors $r + s = s$, donc $v_p(r + s) = v_p(s) = \min(+\infty, v_p(s) = \min(v_p(r), v_p(s))$.

Q 10. Par définition de v_p, la seule valeur $x \in \mathbb{Q}$ telle que $v_p(x) = 0$ est $x = 0$: l'axiome de séparation est satisfait.

Soit $x, y \in \mathbb{Q}$, alors $|xy|_p = \dfrac{1}{p^{v_p(xy)}} = \dfrac{1}{p^{v_p(x)+v_p(y)}} = \dfrac{1}{p^{v_p(x)} \times p^{v_p(y)}} = |x|_p \times |y|_p$ d'après la question **Q 9** : l'axiome d'homogénéité interne est satisfait.

Et de même, $|x + y|_p = \dfrac{1}{p^{v_p(x+y)}} \leqslant \dfrac{1}{p^{\min(v_p(x),v_p(y))}} = \dfrac{1}{\min(p^{v_p(x)}, p^{v_p(y)})} = \max\left(\dfrac{1}{p^{v_p(x)}}, \dfrac{1}{p^{v_p(y)}}\right) = \max(|x|_p, |y|_p)$ d'après la question **Q 9** : l'inégalité ultramétrique est vraie.

Donc v_p est une valeur absolue ultramétrique.

Q 11. Pour tout $n \in \mathbb{N}$, $v_p(p^n) = n$ donc $|p^n|_p = \dfrac{1}{p^n} \xrightarrow[n\to+\infty]{} 0$ donc la suite (p^n) converge vers 0.

Pour tout $n \in \mathbb{N}^*$, si $n \geqslant p$, alors p divise $n!$: plus précisément, si $k = \left\lfloor \dfrac{n}{p} \right\rfloor$, alors $p, 2p, \ldots, kp$ apparaissent dans la liste des entiers $1, 2, \ldots, n$ donc $p \times 2p \times \ldots \times kp$ divise $n!$, autrement dit $v_p(n) \geqslant k \geqslant \dfrac{n}{p} - 1$, donc $v_p(n!) \xrightarrow[n\to+\infty]{} +\infty$ donc $|n!|_p \xrightarrow[n\to+\infty]{} 0$. La suite $(n!)$ converge donc vers 0.

III.

III.A -

Q 12. Le sens direct est immédiat (prendre $m = n + 1$).

Réciproquement, si pour tout $k \in \mathbb{N}$, $a_{k+1} \equiv a_k\ [p^{k+1}]$, alors soit $n \in \mathbb{N}$, on pose $\mathscr{P}(m)$ le prédicat $a_m \equiv a_n\ [p^{n+1}]$.

$\mathscr{P}(n + 1)$ est vraie par hypothèse et $\mathscr{P}(n)$ est trivialement vraie.

Si $\mathscr{P}(m)$ est vraie ($m \geqslant n$), alors comme $a_{m+1} \equiv a_m\ [p^{m+1}]$ et p^{n+1} divise p^{m+1} alors $a_{m+1} \equiv a_m\ [p^{n+1}]$. Par hypothèse de récurrence, on en déduit par transitivité de la congruence que $a_{m+1} \equiv a_m \equiv a_n\ [p^{n+1}]$. Donc $\mathscr{P}(m+1)$ est vraie.

D'après le principe de récurrence, on en déduit que pour tout $m \geqslant n$, $\mathscr{P}(m)$ est vraie.

Comme ceci est vrai pour tout $n \in \mathbb{N}$, on en déduit que $(a_n) \in \mathbb{Z}_p$.

Q 13. Par définition de la division euclidienne dans $\mathbb{Z}$, la suite (a_n) vérifie la propriété

« pour tout $n \in \mathbb{N}$, $a_n \in [\![0, p^{n+1} - 1]\!]$ ».

Pour tout $n \in \mathbb{N}$, il existe $q_n, q_{n+1} \in \mathbb{Z}$ tel que $x = p^{n+2}q_{n+1} + a_{n+1} = p^{n+1}q_n + a_n$

donc $a_{n+1} - a_n = p^{n+1}(q_n - pq_{n+1}) \equiv 0\ [p^{n+1}]$.

D'après la question précédente, la suite (a_n) appartient à $\mathbb{Z}_p$.

Q 14. Le reste de la division euclidienne de 1 par 5^{n+1} est toujours 1 donc $\theta(1) = (1, 1, 1, \ldots, 1, \ldots)$.

Le reste de la division euclidienne de -1 par 5^{n+1} est $5^{n+1} - 1$ donc $\theta(-1) = (4, 24, 124, \ldots, 5^{n+1} - 1, \ldots)$.

Le reste de la division euclidienne de 27 par 5^{n+1} est 27 dès que $n \geqslant 2$ (car $27 < 5^3$) donc $\theta(27) = (2, 2, 27, \ldots, 27, \ldots)$.

Le reste de la division de -7 par 5^{n+1} est $5^{n+1} - 7$ dès que $n \geqslant 1$ donc $\theta(-7) = (3, 18, 118, 618, \ldots, 5^{n+1} - 7, \ldots)$.

Q 15. D'abord, on verifie que σ est bien une application de S_p dans $\mathbb{Z}_p$, car

pour tout $n \in \mathbb{N}$, $a_{n+1} - a_n = u_{n+1}p^{n+1} \equiv 0\ [p^{n+1}]$ et $0 \leqslant a_n \leqslant \displaystyle\sum_{i=0}^{n}(p - 1)p^i = (p - 1)\frac{p^{n+1} - 1}{p - 1} = p^{n+1} - 1$.

Ensuite, on vérifie que σ est une surjection.

Soit $(b_n) \in \mathbb{Z}_p$. Pour tout $n \in \mathbb{N}$, $b_{n+1} - b_n \equiv 0 \ [p^{n+1}]$: on pose alors $u_0 = b_0 \in [\![0, p-1]\!]$ et $u_{n+1} = \dfrac{b_{n+1} - b_n}{p^{n+1}} \in \mathbb{Z}$.

On vérifie maintenant que la suite (u_n) est dans S_p et que $\sigma(u) = (b_n)$.

Par définition, pour tout $n \in \mathbb{N}$, $0 \leqslant b_{n+1} < p^{n+2}$ et $0 \leqslant b_n < p^{n+1}$ donc $-p^{n+1} < b_{n+1} - b_n < p^{n+2}$, donc $-1 < u_{n+1} < p$, or u_n est un entier donc $u_{n+1} \in [\![0, p-1]\!]$.

Ceci prouve que la suite u appartient à S_p.

De plus, pour tout $n \in \mathbb{N}$, $b_{n+1} - b_n = u_{n+1}p^{n+1}$ donc par télescopie, $b_n = b_0 + \displaystyle\sum_{i=1}^{n} u_i p^i = \sum_{i=0}^{n} u_i p^i$. Donc $(b_n) = \sigma(u)$.

Enfin, on conclut que σ est une injection car si on veut avoir pour tout $n \in \mathbb{N}$, $b_n = \displaystyle\sum_{i=0}^{n} u_i p^i$, alors il est nécessaire que $u_0 = b_0$ et que pour tout $n \in \mathbb{N}$, $b_{n+1} - b_n = u_{n+1}p^{n+1}$, ce qui est exactement le choix de u qui a été fait juste avant.

Q 16. On note $\theta(x) = a = (a_n)$ et u la suite $\sigma^{-1}(a)$.

Si $x = 0$, il est évident que $\theta(0)$ est la suite nulle donc la suite u associée est aussi la suite nulle

$$\theta(0) = [\dots 0\,0 \dots 0]$$

Si $x \in \mathbb{N}^*$, alors il existe un unique entier naturel k tel que $p^k \leqslant x < p^{k+1}$, donc pour tout $n \geqslant k$, $a_n = x$ donc $u_{n+1} = 0$, autrement dit $x = \displaystyle\sum_{i=0}^{k} u_i p^i$ est l'écriture de x en base b :

$$\theta(x) = [\dots 0\,0 \dots 0\, u_k\, u_{k-1} \dots u_0]$$

Si $x \in \mathbb{Z}_-^*$, alors on pose $y = -x$: il existe un unique entier naturel k tel que $p^k \leqslant y < p^{k+1}$, donc pour tout $n \geqslant k$, $a_n = p^{n+1} - y$ donc $u_{n+1} = p - 1$, et en particulier $a_k = p^{k+1} - y = \displaystyle\sum_{i=0}^{k} u_i p^i$ est l'écriture de $p^{k+1} - y$ en base b :

$$\theta(x) = [\dots p-1\, p-1 \dots p-1\, u_k\, u_{k-1} \dots u_0]$$

Exemples :

$$\theta(27) = [\dots 0\,2\,2]$$
$$\theta(-1) = [\dots 4\,4\,4]$$
$$\theta(-27) = [\dots 4\,4\,3\,4\,3]$$

III.B -

Q 17. Soit $u = \sigma^{-1}(a)$: comme $a \neq 0$, alors $u \neq 0$ et on pose alors $k = \min\{n \in \mathbb{N} \ / \ u_n \neq 0\}$.

Alors pour tout $n < k$, $a_n = \displaystyle\sum_{i=0}^{n} u_i p^i = 0$ donc $v_p(a_n) = +\infty$ et pour $n \geqslant k$, $a_n = p^k u_k + \displaystyle\sum_{i=k+1}^{n} u_i p^i$ est divisible par p^k mais pas par p^{k+1} puisque $u_k \neq 0$.

Q 18. Soit $x, y \in \mathbb{Z}$ tels que $\theta(x) = \theta(y)$. On pose $u = \sigma^{-1}(\theta(x))$. Alors

— soit la suite u se termine par des 0 dans le cas où x est positif et dans ce cas, y est aussi positif donc les autres termes de la suite u sont les chiffres en base p de x et de y, donc $x = y$ par unicité de l'écriture en base p

— soit la suite u se termine par des $p-1$ dans le cas où x est strictement négatif et dans ce cas, y est aussi strictement négatif et donc les autres termes de la suite u sont les chiffres en base p de $p^{v_p(x)+1} - x$ et de $p^{v_p(x)+1} - y$, donc $x = y$ par unicité de l'écriture en base p

De plus, si $x > 0$ et $k = v_p(x)$, alors p^k divise x et p^{k+1} ne divise pas x, donc les k premiers chiffres $u_0, \dots, u_{k-1}$ de l'écriture en base p de x sont nuls et le suivant u_k est non nul, donc $x = u_k p^k + \displaystyle\sum_{i=k+1}^{K} u_i p^i$ donc $a_0, \dots, a_{k-1}$ sont nuls et pour tout $n \geqslant k$, $a_n = u_k p^k + \displaystyle\sum_{i=k+1}^{n} u_i p_i$ est divisible par p^k mais pas par p^{k+1}, donc $\tilde{v}_p(\theta(x)) = v_p(x)$.

Si $x < 0$ et $k = v_p(x)$, alors on encadre $y = -x$: $p^\ell \leqslant y < p^{\ell+1}$: on sait que les $\ell + 1$ premiers chiffres $u_0, \dots, u_\ell$

sont les chiffres de $p^{\ell+1}-y$ et que les suivants sont tous égaux à $p-1$, donc $p^{\ell+1}-y=\sum_{i=0}^{\ell} u_i p^i$. Comme p^k divise y, on en déduit que $\ell \geqslant k$ et que les k premiers chiffres de l'écriture en base p de $p^{\ell+1}-y$ sont nuls, donc $p^{\ell+1}-y=u_k p^k+\sum_{i=k+1}^{\ell} u_i p^i$ donc $a_0,\ldots,a_{k-1}$ sont nuls ; or p^{k+1} ne divise par $p^{\ell+1}-y$, donc $u_k \neq 0$, donc pour $n \geqslant k+1$, $a_n=u_k p^k+\sum_{i=k+1}^{n} u_i p^i$ donc a_n est divisible par p^k mais pas par p^{k+1}, donc $\tilde{v}_p(\theta(x))=v_p(x)$.

Q 19. Soit u la suite qui vaut alternativement 1 aux rangs pairs et 0 aux rangs impairs. C'est une suite de S_p associé à un élément a de $\mathbb{Z}_p$ qui n'est ni l'image d'un entier naturel (puisque la suite u n'est pas stationnaire en 0), ni l'image d'un entier strictement négatif (puisqu'elle n'est pas stationnaire en $p-1$). Donc l'élément a n'est pas dans l'image de θ, *i.e.* θ n'est pas surjective.

III.C -

Q 20. D'après les propriétés de compatibilité de la congruence avec les opérations arithmétiques sur $\mathbb{Z}$, il est facile de montrer que les suites (c_n) et (d_n) satisfont la condition de la question **Q 12** et par définition de la division euclidienne, l'autre propriété $. \in [[0, p^{n+1}-1]]$ est aussi satisfaite.

Q 21. Il est évident que la suite nulle est neutre pour la loi $+$, que cette loi est commutative grâce à la commutativité de $+$ dans $\mathbb{Z}$. L'associativité découle des propriétés de la congruence et de l'associativité de $+$ dans $\mathbb{Z}$:

en effet, si $r(x)$ est le reste de la division euclidienne de x par un entier $q>0$ fixé, alors $r(x+y)\equiv r(x)+r(y)\ [q]$ donc $r(x+(y+z))=r((x+y)+z)$ par congruence et appartenance à l'ensemble $[\![0,q-1]\!]$.

Enfin, si $a\in\mathbb{Z}_p$, on pose (b_n) la suite définie par : $b_n=0$ si $a_n=0$ et sinon $b_n=p^{n+1}-a_n$ si $a_n\neq 0$. Il est facile de vérifier que b est un élément de $\mathbb{Z}_p$ et que $a+b=0$.

Q 22. Le neutre pour la multiplication est la suite constante égale à 1.

Soit a,b deux éléments non nuls de $\mathbb{Z}_p$. On pose $c=ab$. Si $c=0$, alors pour tout $n\in\mathbb{N}$, p^{n+1} divise a_nb_n. Or en posant $k=v_p(a)$ et $\ell=v_p(b)$ (qui sont deux entiers puisque a et b sont non nuls), on en déduit que pour tout $n\geqslant \max(k,\ell)$, $v_p(a_n)=k$ et $v_p(b_n)=\ell$ donc $v_p(a_nb_n)=k+\ell$ donc $n+1\leqslant k+\ell$, ce qui est contradictoire dès que $n>k+\ell$. Contradiction, donc $c\neq 0$.

Ceci prouve donc que $\mathbb{Z}_p$ est un anneau intègre.

Q 23. Si $a=0$, alors les règles de calcul dans $\mathbb{Z}\cup\{+\infty\}$ donnent directement le résultat. De même si $b=0$.

Soit a,b deux éléments non nuls de $\mathbb{Z}_p$. On pose $k=v_p(a)$ et $\ell=v_p(b)$, tous deux entiers naturels. On note $d=ab$.

Pour tout $n\geqslant k+\ell$, $n\geqslant k$ donc $v_p(a_n)=k$ et $n\geqslant \ell$ donc $v_p(b_n)=\ell$ donc $v_p(a_nb_n)=v_p(a_n)+v_p(b_n)=k+\ell$ donc $a_nb_n=p^{k+\ell}r$ où p ne divise pas r. Comme $d_n\equiv a_nb_n\ [p^{n+1}]$, alors $d_n=a_nb_n+p^{n+1}q=p^{k+\ell}r+p^{n+1}q$ est divisible par $p^{k+\ell}$ mais pas par $p^{k+\ell+1}$ puisque $n+1>k+\ell$. Donc $v_p(d_n)=k+\ell$.

Pour tout $n<k+\ell$, on a soit $v_p(a_n)=+\infty$ (c'est-à-dire $a_n=0$), soit $v_p(a_n)=k$, donc dans les deux cas, p^k divise a_n ; de même, p^ℓ divise b_n ; donc $p^{k+\ell}$ divise a_nb_n donc comme $n+1\leqslant k+\ell$, p^{n+1} divise a_nb_n donc le reste de la division euclidienne de a_nb_n par p^{n+1} est nul, donc $v_p(d_n)=+\infty$.

Ceci prouve que $v_p(d)=v_p(a)+v_p(b)$.

On pose maintenant $c=a+b$. Si $c=0$, alors on a directement le résultat. On suppose donc $c\neq 0$ et on pose $h=v_p(c)$ entier naturel.

Alors pour tout $n<\min(k,\ell)$, $a_n=b_n=0$ donc $c_n=0$ donc comme $c_h\neq 0$, $h\geqslant\min(k,\ell)$, donc $v_p(a+b)\geqslant \min(v_p(a),v_p(b))$.

Q 24. Soit $x,y\in\mathbb{Z}$, alors on pose $a=\theta(x)$, $b=\theta(y)$ et $c=\theta(x)+\theta(y)$.

Pour tout $n\in\mathbb{N}$, $c_n\equiv a_n+b_n\ [p^{n+1}]$, or $a_n\equiv x$ et $b_n\equiv y$ donc $c_n\equiv x+y\ [p^{n+1}]$, donc $c=\theta(x+y)$, ce qui prouve $\theta(x+y)=\theta(x)+\theta(y)$.

De même pour la multiplication. Et enfin, $\theta(1)=(1,1,\ldots)$ neutre pour la multiplication, donc finalement θ est un morphisme d'anneaux.

Q 25. Si a est inversible dans $\mathbb{Z}_p$, il existe $b\in\mathbb{Z}_p$ tel que $ab=1$ donc $v_p(a)+v_p(b)=v_p(1)=0$, donc nécessairement $v_p(a)=0$, donc a_0 est divisible par 1 mais pas par p tout en étant dans $[\![0,p-1]\!]$, donc $a_0\neq 0$.

Réciproquement, si $a_0\neq 0$, alors on construit une suite $b=(b_n)$ de $\mathbb{Z}_p$ telle que $ab=1$, c'est-à-dire pour tout $n\in\mathbb{N}$, $a_nb_n\equiv 1\ [p^{n+1}]$ et $b_{n+1}\equiv b_n[p^{n+1}]$:

$a_0\neq 0$ et $a_0\in[\![0,p-1]\!]$, donc a_0 est premier avec p donc est inversible modulo p : il existe $b_0\in[\![0,p-1]\!]$ tel que $a_0b_0\equiv 1\ [p]$.

Si on suppose avoir construit $b_0, \ldots, b_{n-1}$ ($n \geqslant 1$), alors on cherche $b_n \in \mathbb{Z}$ tel que $a_n b_n \equiv 1$ $[p^{n+1}]$ et en même temps $b_n \equiv b_{n-1}$ $[p^n]$. On cherche donc b_n sous la forme $b_{n-1} + qp^n$ tel que $a_n \times (b_{n-1} + qp^n) = 1 + rp^{n+1}$ où q et r sont deux entiers. Or $a_n = a_{n-1} + sp^n$ donc on veut $(a_{n-1} + sp^n) \times (b_{n-1} + qp^n) = 1 + rp^{n+1}$,

c'est-à-dire $a_{n-1}b_{n-1} + b_{n-1}sp^n + a_{n-1}qp^n + sqp^{2n} = 1 + rp^{n+1}$.

Or $a_{n-1}b_{n-1} = 1 + up^n$, donc il vient l'équation $(u + b_{n-1}s + a_{n-1}q)p^n + sqp^{2n} = rp^{n+1}$ d'inconnue q et r entiers,

c'est-à-dire l'équation $u + b_{n-1}s + qa_{n-1} + sqp^n) = rp$ d'inconnue q et r entiers.

On veut donc que $qa_{n-1} \equiv -u - b_{n-1}s$ $[p]$. Or puisque $a_{n-1}b_{n-1} = 1 + up^n$, a_n est inversible modulo p et son inverse modulo p est b_{n-1}. Donc il suffit que $q \equiv -ub_{n-1} - b_{n-1}^2 s$ $[p]$ pour avoir ce qu'on souhaite.

Ceci justifie donc l'existence de b_n (en réduisant ensuite modulo p^{n+1}). Par récurrence, on construit donc l'inverse de a dans $\mathbb{Z}_p$.

Q 26. On montre que les seuls idéaux de $\mathbb{Z}_p$ sont les idéaux principaux $p^k\mathbb{Z}_p$ pour tout $k \in \mathbb{N}$ et $\{0\}$.

D'abord, ce sont bien des idéaux de $\mathbb{Z}_p$ (ce sont des idéaux principaux).

Réciproquement, soit I un idéal de $\mathbb{Z}_p$, autre que $\{0\}$. On considère l'ensemble $\{k \in \mathbb{N} \ / \ \exists a \in I \quad v_p(a) = k\}$: c'est une partie de $\mathbb{N}$, non vide car $I \neq \{0\}$. Il possède donc un minimum $r \geqslant 0$. Et il existe donc un élément $a \in I$ tel que $v_p(a) = r$, *i.e.* $a = (0, 0, \ldots, 0, a_r, a_{r+1}, \ldots)$ où $v_p(a_n) = r$ dès que $n \geqslant r$.

On pose alors b la suite $\left(\dfrac{a_r}{p^r}, \ldots, \dfrac{a_n}{p^r}, \ldots\right)$ qui est alors une suite de $\mathbb{Z}_p$ dont le premier terme est non nul. C'est donc un inversible de $\mathbb{Z}_p$ et il vérifie $p^k \times b = a$.

Comme I est un idéal, $a \times b^{-1} \in I$, c'est-à-dire $p^k \in I$, donc on a l'inclusion $p^k\mathbb{Z}_p \subset I$.

Tout élément z de I a une valuation au moins égale à k, donc est factorisable par p^k, donc appartient à $p^k\mathbb{Z}_p$, ce qui prouve l'inclusion $I \subset p^k\mathbb{Z}_p$.

Au total, $I = p^k\mathbb{Z}_p$.

Q 27. On note que comme en **Q 8**, l'application Θ est bien définie (elle ne dépend pas du choix des entiers x, y représentant la fraction $\dfrac{x}{y}$.

Ensuite on prolonge v_p de la même façon en posant $v_p(\Theta(x/y)) = v_p(\theta(x)) - v_p(\theta(y))$: elle vérifie les mêmes propriétés et les démonstrations sont identiques, elles reposent sur les propriétés de v_p sur les éléments de $\mathbb{Z}_p$.

Enfin, si $\Theta(x/y) = \Theta(w/z)$, alors $\theta(x)\theta(z) = \theta(y)\theta(w)$ donc $\theta(xz) = \theta(yw)$ d'après **Q 24**, donc comme θ est injective, on en déduit que $xz = yw$ donc $x/y = w/z$: ceci prouve l'injectivité de Θ.

Q 28. Soit $r \in \mathbb{Q}_p$. Il existe $x, y \in \mathbb{Z}_p$ tel que $r = \dfrac{x}{y}$. Or comme en **Q 26**, on peut écrire $y = p^k z$ où z est un inversible de $\mathbb{Z}_p$, donc finalement en posant $a = xz^{-1} \in \mathbb{Z}_p$, on a $r = \dfrac{a}{p^k}$.

IV.

Q 29. D'abord, on remarque que $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \ / \ v_p(a) \geqslant 0\}$.

Donc $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \ / \ a_0 \neq 0\} = \{a \in \mathbb{Z}_p \ / \ v_p(a) = 0\} = \{a \in \mathbb{Q}_p \ / \ |a|_p = 1/p^0 = 1\} = S(0, 1)$.

Q 30. De même, $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \ / \ v_p(a) \geqslant 0\} = \{a \in \mathbb{Q}_p \ / \ |a|_p \leqslant 1\}$ est la boule fermée de centre 0 et de rayon 1.

Or la valeur absolue est à valeurs discrètes dans $\left\{\dfrac{1}{p^n} \ / \ n \in \mathbb{Z}\right\}$, donc $|a|_p \leqslant 1 \iff |a|_p < p$ donc $\mathbb{Z}_p$ est aussi la boule ouverte de centre 0 et de rayon p.

Q 31. Soit $a \in \mathbb{Z}_p$. Pour tout $n \in \mathbb{N}$, $a_n \in \mathbb{N}$ donc $\theta(a_n) = (a_0, a_1, \ldots, a_n, a_n, \ldots)$ d'après **Q 13**. Donc $a - \theta(a_n) = (0, 0, \ldots, 0, a_{n+1}, a_{n+2}, \ldots)$: la valuation de $a - \theta(a_n)$ est donc au moins égale à n, *i.e.* $|a - \theta(a_n)| \leqslant \dfrac{1}{p^n}$, donc par encadrement, $\lim\limits_{n \to +\infty} \theta(a_n) = a$.

Ceci prouve que $\mathbb{Z}$ identifié à $\theta(\mathbb{Z})$ est dense dans $\mathbb{Z}_p$ (et on a même montré mieux : $\mathbb{N}$ est dense dans $\mathbb{Z}_p$!).

Q 32. On pose $u = \sigma^{-1}(a)$. Alors pour tout $n \in \mathbb{N}$, $a_n = \displaystyle\sum_{i=0}^{n} u_i p^i$. Or la suite (a_n) converge vers a (question précédente), donc $a = \displaystyle\lim_{n \to +\infty} \sum_{i=0}^{n} u_i p^i = \sum_{i=0}^{+\infty} u_i p^i$.

Dans le cas où $a \in \mathbb{N}$, la suite (u_i) est la suite des chiffres en base p de a. Dans le cas où $a \in \mathbb{Z}_-^*$, la suite (u_i) a été explicitée en **Q 16**.

Q 33. Soit $(a(n))$ une suite de $\mathbb{Z}_p$ (j'écris $a(n)$ pour bien distinguer les notions de $(a_n) \in \mathbb{Z}_p$ et $(a(n)) \in \mathbb{Z}_p^{\mathbb{N}}$). D'après la question **Q 30**, $\mathbb{Z}_p$ est la boule de centre 0 et de rayon 1.

Pour $n \in \mathbb{N}$, on pose $u(n) = \sigma^{-1}(a(n))$, autrement dit pour tout $k \in \mathbb{N}$, $a(n)_k = \displaystyle\sum_{i=0}^{k} u(n)_i p^i$.

Les suites $(u(n)_i)_{n\in\mathbb{N}}$ sont des suites à termes dans $[\![0, p-1]\!]$, donc elles ne prennent qu'un nombre fini de valeurs, ce qui les oblige à prendre une infinité de fois la même valeur : on va construire une suite d'extractrices bien choisies.

La suite $(u(n)_0)$ prend une infinité de fois la même valeur λ_0 : il existe donc une extractrice φ_0 telle que la suite $(u(\varphi_0(n))_0)$ soit constante égale à λ_0.

La suite $(u(\varphi_0(n))_1)$ prend alors une infinité de fois la la même valeur λ_1 : il existe donc une extractrice ψ_1 telle que la suite $(u(\varphi_0 \circ \psi_1(n))_1)$ soit constante égale à λ_1. Mais alors la suite $u(\varphi_0 \circ \psi_1(n))_0)$, extraite de $(u(\varphi_0(n))_0)$, est aussi constante égale à λ_0. En posant $\varphi_1 = \varphi_0 \circ \psi_1$, on a donc construit une extractrice telle que les deux suites $(u(\varphi_1(n)_0)$ et $(u(\varphi_1(n)_1)$ sont constantes.

Pour $k \in \mathbb{N}$, on suppose avoir construit une extractrice φ_k telle que pour tout $i \in [\![0, k]\!]$, la suite $(u(\varphi_k(n))_i)$ soit constante égale à λ_i. La suite $(u(\varphi_k(n))_{k+1})$ prend une infinité de fois la même valeur donc il existe une extractrice ψ_{k+1} telle que la suite $(u(\varphi_k \circ \psi_{k+1}(n))_{k+1})$ soit constante égale à λ_{k+1}. Mais alors pour tout $i \in [\![0, k]\!]$, la suite $u(\varphi_k \circ \psi_{k+1}(n))_i)$, extraite de $(u(\varphi_k(n))_i)$, est aussi constante égale à λ_i. En posant $\varphi_{k+1} = \varphi_k \circ \psi_{k+1}$, on a donc construit une extractrice telle que toutes les suites $(u(\varphi_{k+1}(n)_i)$ sont constantes quand $i \in [\![0, k+1]\!]$.

Par récurrence, on a donc construit une famille d'extractrices $(\varphi_k)_{k\in\mathbb{N}}$ et une famille de constantes entières $\lambda = (\lambda_k)$ telles que

$$\text{pour tout } k \in \mathbb{N}, \text{ pour tout } i \in [\![0, k]\!], \text{ la suite } (u(\varphi_k(n))_i) \text{ soit constante égale à } \lambda_i,$$
$$\text{ou encore : pour tout } i \in \mathbb{N}, \text{ pour tout } k \geqslant i, \text{ pour tout } n \in \mathbb{N},\ u(\varphi_k(n))_i = \lambda_i.$$

On pose alors $b = \sigma(\lambda) = \displaystyle\sum_{i=0}^{+\infty} \lambda_i p^i \in \mathbb{Z}_p$ et on considère la suite $(a(\varphi_n(n))_{n\in\mathbb{N}}$, qui est extraite de la suite $(a(n))$.

Par construction, pour tout $n \in \mathbb{N}$, si $i \leqslant n$, alors $u(\varphi_n(n))_i = \lambda_i$, autrement dit $a(\varphi_n(n))$ et b ont les mêmes $n+1$ premiers chiffres en base p, donc $v_p\left(a(\varphi_n(n)) - b\right) \geqslant n$, *i.e.* $|a(\varphi_n(n)) - b|_p \leqslant \dfrac{1}{p^n}$.

Par encadrement, la suite $(a(\varphi_n(n)))_{n\in\mathbb{N}}$ est une suite extraite de $(a(n))$ qui converge vers $b \in \mathbb{Z}_p$.

On a donc montré que toute suite de $\mathbb{Z}_p$ possède une sous-suite convergente dans $\mathbb{Z}_p$, ce qui signifie que $\mathbb{Z}_p$ est un compact.

Q 34. On a montré que la boule fermée $\mathbb{Z}_p$ est un compact, donc par continuité de la somme et du produit dans $\mathbb{Q}_p$, toute boule fermée est encore compacte (l'image continue d'un compact est un compact).

Si la série $\displaystyle\sum_{n\geqslant 0} x_n$ converge, alors la suite (x_n) converge vers 0 : c'est exactement la même démonstration que le résultat habituel dans un espace vectoriel normé.

Réciproquement, si la suite (x_n) est converge vers 0, alors elle est bornée : il existe $i \in \mathbb{Z}$ telle que pour tout $n \in \mathbb{N}$, $|x_n|_p \leqslant \dfrac{1}{p^i} = r$, ce qui est équivalent à $v_p(x_n) \geqslant i$, donc d'après la propriété sur la valuation d'une somme, $v_p\left(\displaystyle\sum_{k=0}^{n} x_k\right) \geqslant \displaystyle\min_{0\leqslant k\leqslant n} v_p(x_k) \geqslant i$, donc les sommes partielles s_n de la série sont toutes de valeurs absolues majorées par $\dfrac{1}{p^i} = r$.

Autrement dit, la suite (s_n) des sommmes partielles est à valeurs dans le compact $\bar{B}(0, r)$ donc elle possède une sous-suite convergente $(s_{\varphi(n)})$ qui converge vers ℓ.

Soit $k \in \mathbb{N}$. Comme la suite (x_n) converge vers 0, il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $|x_n|_p \leqslant \dfrac{1}{p^k}$.

Pour $n \geqslant N$, on a $\varphi(n) \geqslant n \geqslant N$, donc pour tout $i \in [\![n+1, \varphi(n)]\!]$, $v_p(x_i) \geqslant k$, donc par le même raisonnement sur les valuations que précédemment, $v_p\left(\displaystyle\sum_{i=n+1}^{\varphi(n)} x_i\right) \geqslant k$. Ceci prouve alors que $|s_{\varphi(n)} - s_n|_p \leqslant \dfrac{1}{p^k}$.

On a donc montré que la suite $(s_{\varphi(n)} - s_n)$ converge vers 0.

Par opérations sur les limites, la suite (s_n) converge donc vers ℓ, *i.e.* la série $\sum x_n$ converge.